Configuration du BYOD ISE avec SSID simple et double dans ISE 3.3

Table des matières

- Introduction
- Fond
  - Mécanisme D'Authentification À Clé D'Accès
- Conditions préalables
  - Exigences
  - Composants utilisés
- Qu'est-ce que le BYOD avec SSID unique et SSID double sur ISE ?
  - SSID unique BYOD
  - BYOD à double SSID
- Configuration WLC
  - Créer un WLAN pour CWA
  - Configuration des serveurs RADIUS
  - Configuration des serveurs AAA
  - Configuration des stratégies de sécurité pour le WLAN
  - Configurer une liste de contrôle d'accès pré-authentification
  - Configurer le profil de stratégie
  - Appliquer les balises et déployer
  - Configurer un SSID ouvert/non sécurisé
- Configuration ISE
  - Conditions préalables
  - Certificats
  - Configuration DNS
- Configuration du périphérique réseau ISE
- Créer un portail BYOD
- Télécharger la dernière version de Cisco IOS®
- Créer un profil de terminal
  - Modèle de certificat
- Mappage d'un profil de point de terminaison au portail d'approvisionnement client
- Configuration des ensembles de stratégies ISE pour le BYOD avec un seul SSID
- Configuration des ensembles de stratégies ISE pour le BYOD à double SSID
- Journalisation
- Dépannage
- Extrait de journal
  - Journaux invités
  - Journaux Ise-Psc
  - Téléchargement du profil de terminal

Introduction

Le document décrit comment configurer et dépanner les problèmes liés au BYOD sur ISE.

Fond

Le BYOD est une fonctionnalité qui permet à l'utilisateur d'intégrer ses appareils personnels sur Cisco Identity Services Engine (ISE) afin qu'il puisse utiliser les ressources réseau de l'environnement. Il aide également l'administrateur réseau à empêcher l'utilisateur d'accéder à la ressource critique à partir des périphériques personnels.

Contrairement au flux invité où le périphérique est authentifié avec la page Invité en utilisant le magasin interne ou Active Directory sur ISE. Le BYOD permet à l'administrateur réseau d'installer un profil de point de terminaison sur le point de terminaison pour choisir le type de méthode EAP. Dans des scénarios comme EAP-TLS, le certificat client est signé par l'ISE lui-même pour créer une confiance entre le point d'extrémité et l'ISE.

Mécanisme D'Authentification À Clé D'Accès

Un nouveau mécanisme d'authentification de clé d'accès a été introduit sur la page d'installation du portail BYOD pour améliorer la sécurité et empêcher le détournement de session entre le navigateur et l'assistant de configuration du réseau.

Lorsqu'un utilisateur accède à la page d'installation du BYOD, une clé d'accès est générée et affichée de manière dynamique dans le portail BYOD. Cette clé est unique par session et sert de jeton pour valider le processus d'intégration. L'utilisateur doit noter cette clé d'accès et la saisir dans l'assistant de configuration du réseau pendant le processus d'intégration du périphérique.

Lors du lancement, l'assistant de configuration du réseau invite l'utilisateur à saisir la clé d'accès. L'assistant de configuration du réseau valide la clé d'accès entrée par rapport à la clé générée par le portail BYOD avant de procéder à l'intégration. Si la clé d'accès correspond, le processus d'intégration se poursuit. Si la clé ne correspond pas, l'utilisateur est invité à saisir la clé correcte.

Si votre version de Cisco ISE ne prend pas en charge l'authentification par clé d'accès, l'assistant de configuration du réseau présente l'option No Token Authentication. Cette option permet aux utilisateurs de contourner l'entrée de clé d'accès et de poursuivre l'intégration sans la clé d'accès.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- contrôleur WLC
- Connaissances de base sur ISE

Composants utilisés

Les périphériques utilisés ne sont pas limités à une version particulière du flux BYOD :

- Contrôleur sans fil Catalyst 9800-CL (17.12.3)
- Machine virtuelle ISE (3.3)

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.

Qu'est-ce que le BYOD avec SSID unique et SSID double sur ISE ?

SSID unique BYOD

Dans une configuration BYOD à SSID unique, les utilisateurs connectent leurs périphériques personnels directement au réseau sans fil de l'entreprise. Le processus d'intégration se déroule sur le même SSID, où ISE facilite l'enregistrement, le provisionnement et l'application des politiques des périphériques. Cette approche simplifie l'expérience utilisateur, mais nécessite une intégration sécurisée et des méthodes d'authentification appropriées pour garantir la sécurité du réseau.

BYOD à double SSID

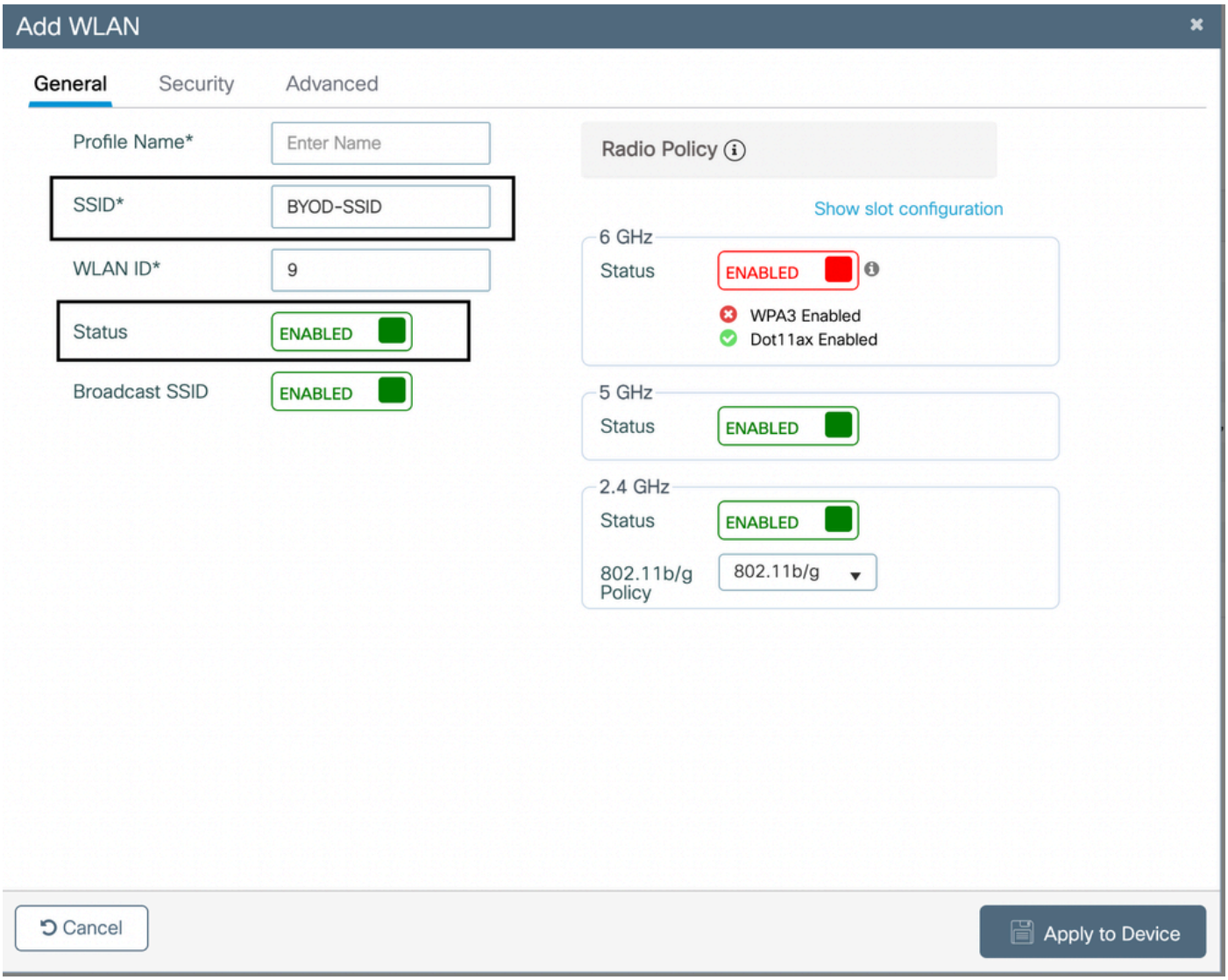
Dans une configuration BYOD à double SSID, deux SSID distincts sont utilisés : une pour l'intégration (accès non sécurisé ou restreint) et une autre pour l'accès au réseau d'entreprise. Les utilisateurs se connectent d'abord au SSID d'intégration, effectuent l'enregistrement et le provisionnement des périphériques via ISE, puis basculent vers le SSID d'entreprise sécurisé pour accéder au réseau. Cela permet d'obtenir une couche de sécurité supplémentaire en séparant le trafic d'intégration du trafic de production.

Configuration WLC

Créer un WLAN pour CWA

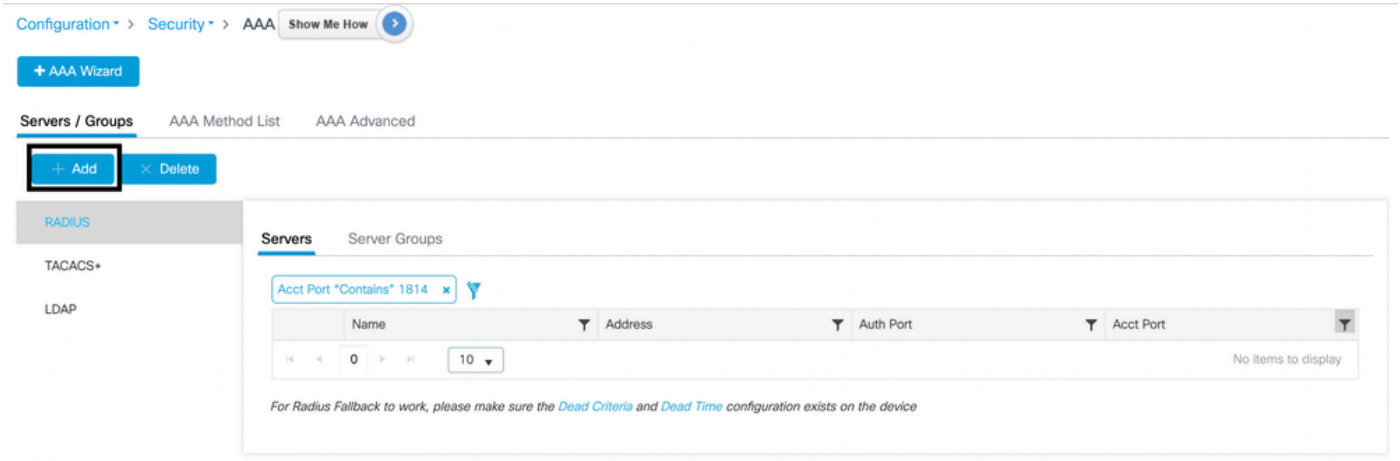
1. Accédez à Configuration > Tags & Profiles > WLANs.
2. Cliquez sur Add pour créer un nouveau WLAN.

    - Définissez un nom WLAN et un SSID (par exemple, BYOD-WiFi).
    - Activez le WLAN.

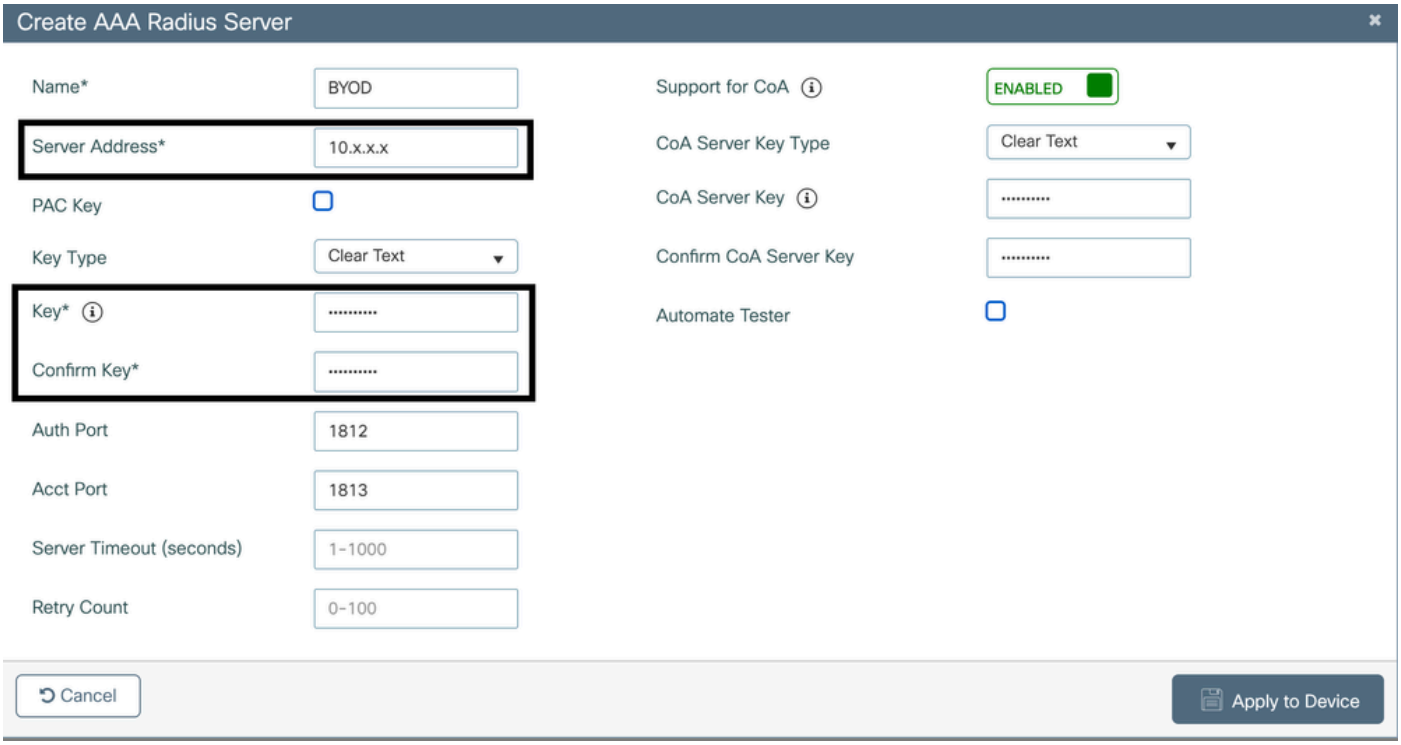


Configuration des serveurs RADIUS

1. Accédez à Configuration > Security > AAA > RADIUS > Servers.

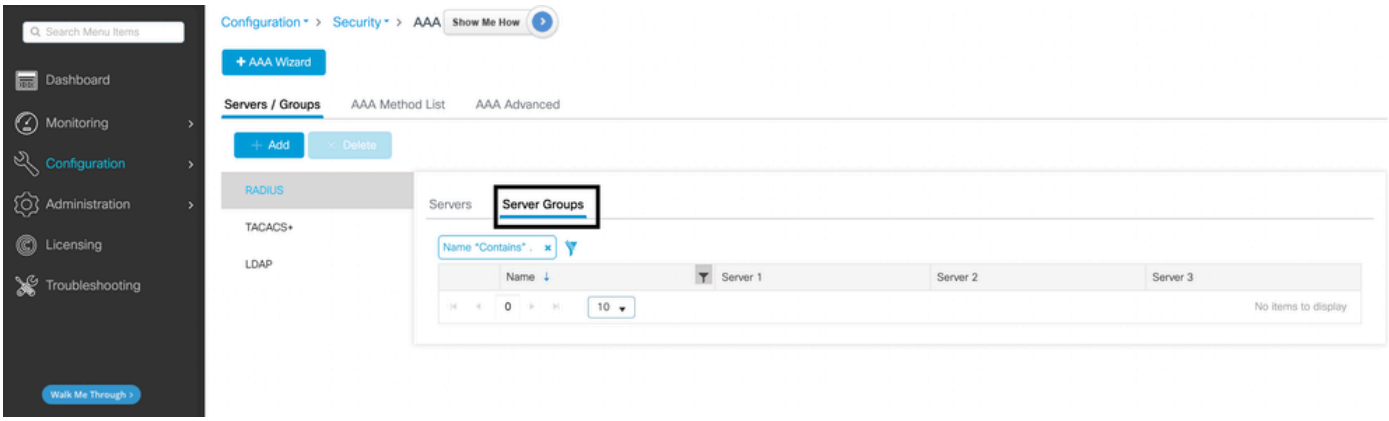


2. Cliquez sur Add pour configurer ISE en tant que serveur RADIUS :
    - Adresse IP du serveur : Adresse IP d'ISE.
    - Secret partagé : Associez les secrets partagés configurés sur ISE.

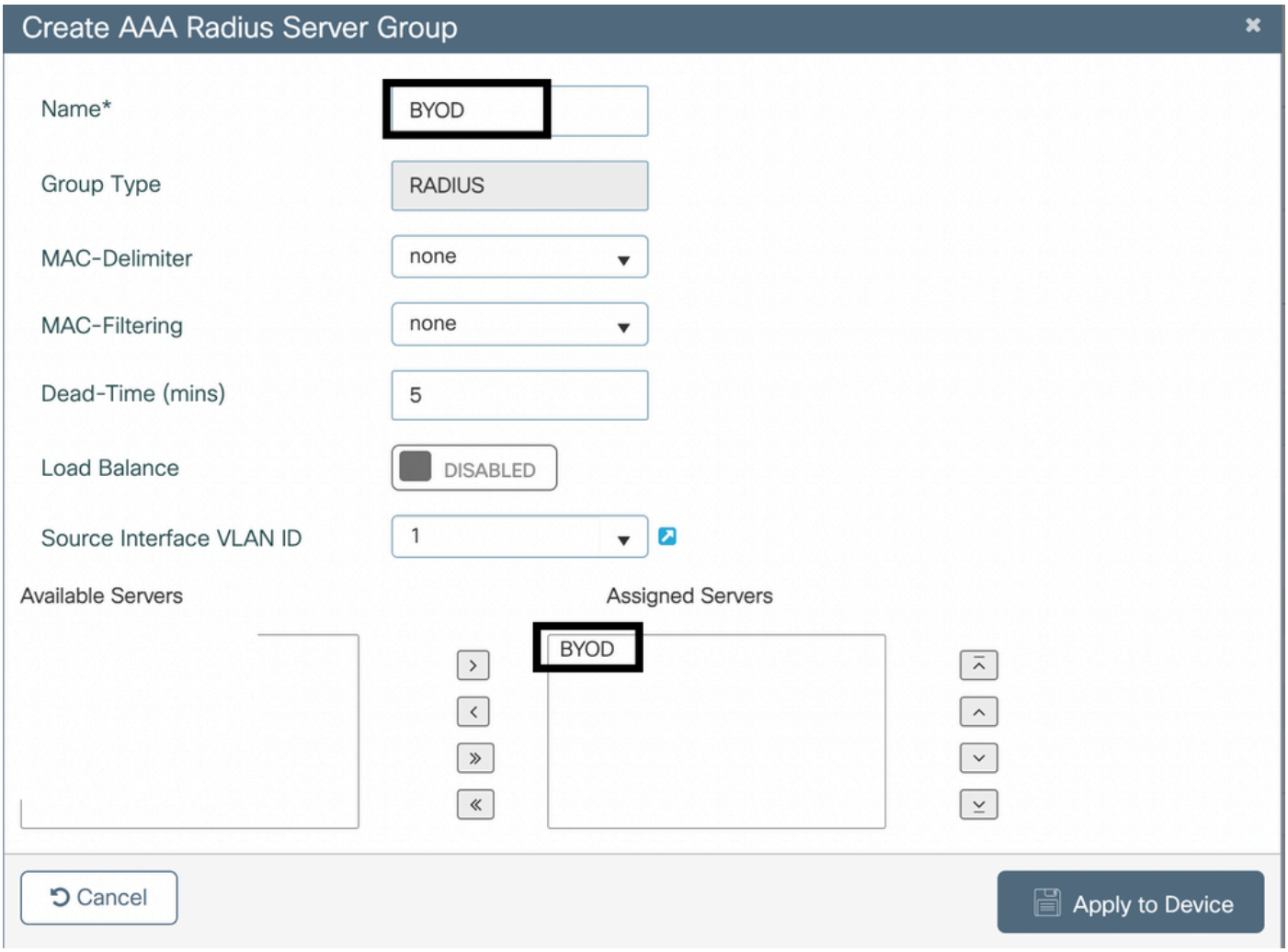


Configuration des serveurs AAA

1. Accédez à Configuration > Security > AAA > Servers/Groups.



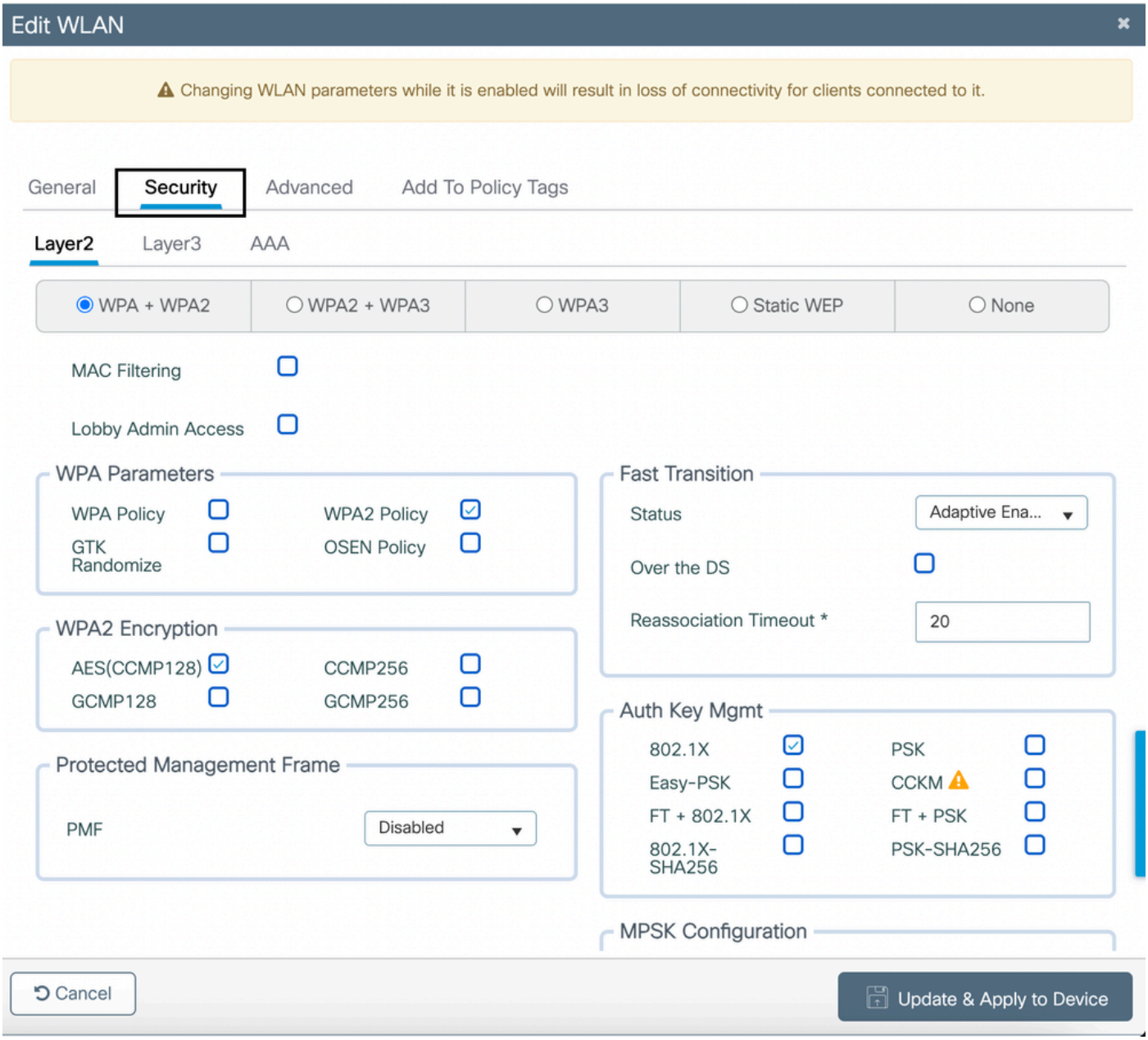
2. Attribuez le serveur RADIUS à un groupe de serveurs nouveau ou existant.



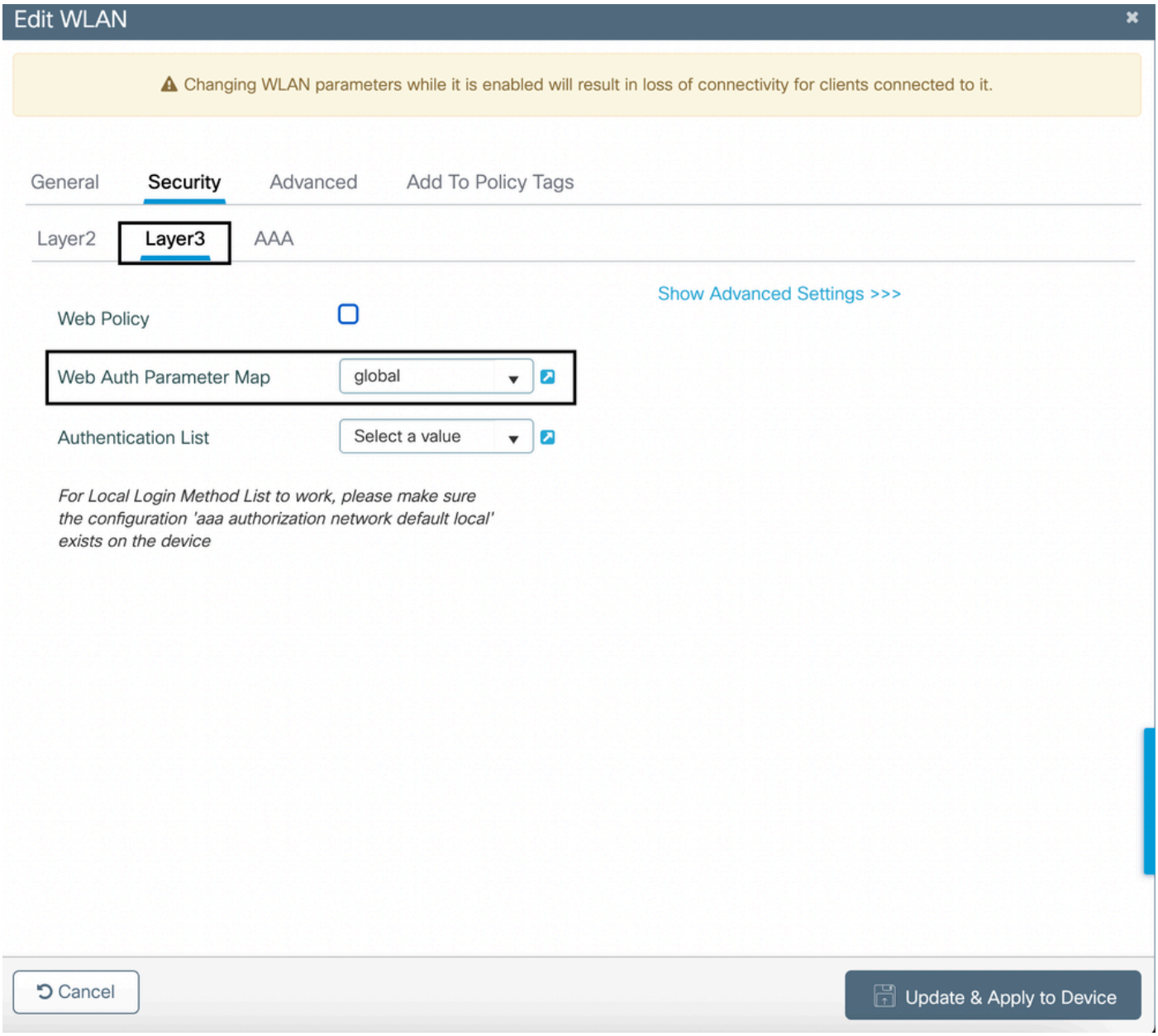
Configuration des stratégies de sécurité pour le WLAN

1. Accédez à Configuration > Tags & Profiles > WLANs. Modifiez le WLAN créé précédemment.

2. Sous l'onglet Security > Layer 2 :
   - Activez WPA+WPA2.
   - Définissez AES(CCMP128) sous Cryptage WPA2.
   - Définissez Auth Key Mgmt sur 802.1X.



3. Sous l'onglet Security > Layer 3, sélectionnez global dans la liste déroulante pour Web Auth Parameter Map.



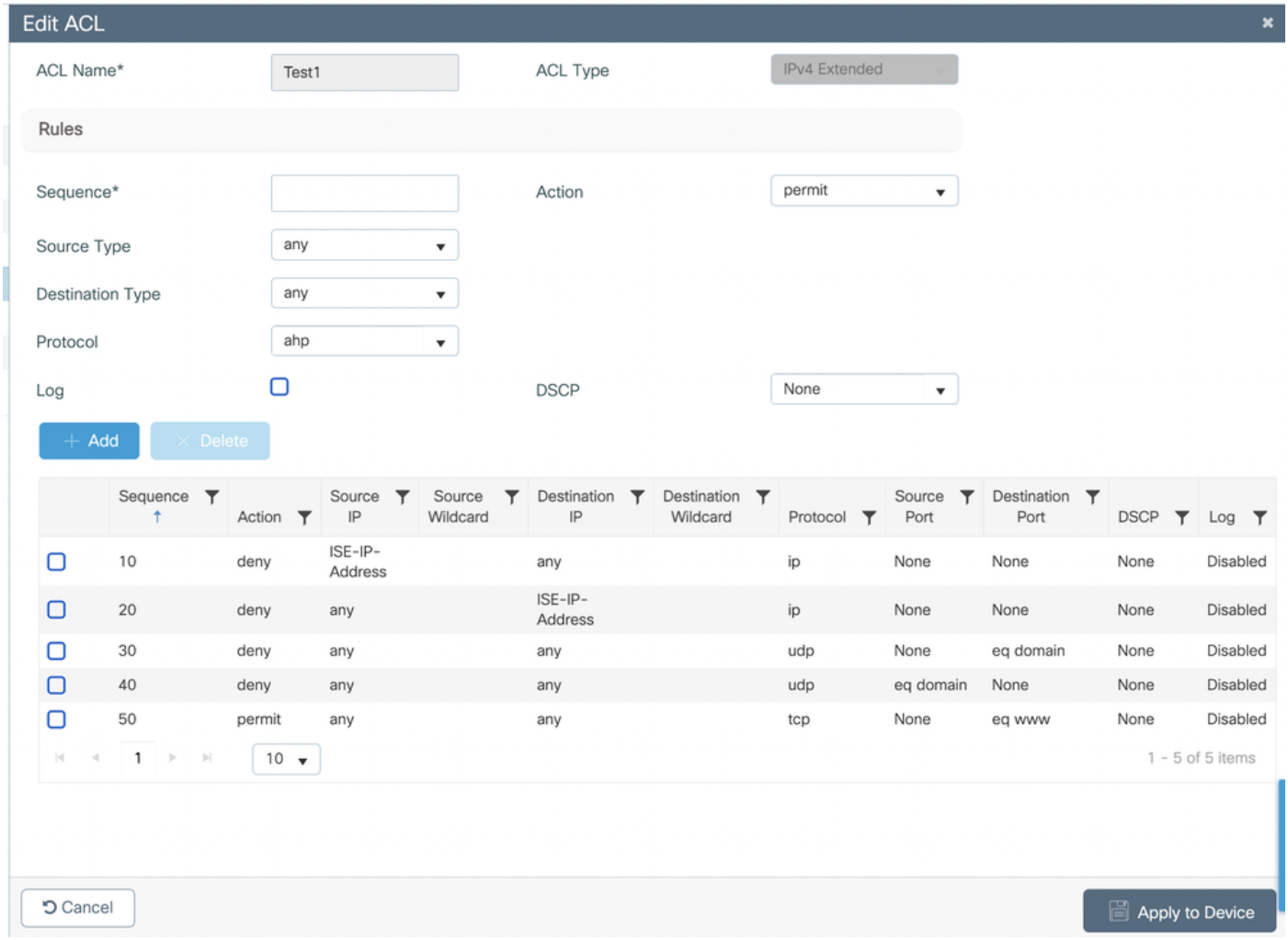
Configurer une liste de contrôle d’accès pré-authentification

Créez une liste de contrôle d’accès pour autoriser ces actions de redirection :

- Trafic DNS.
- HTTP/HTTPS vers le portail ISE.
- Tous les services back-end requis.

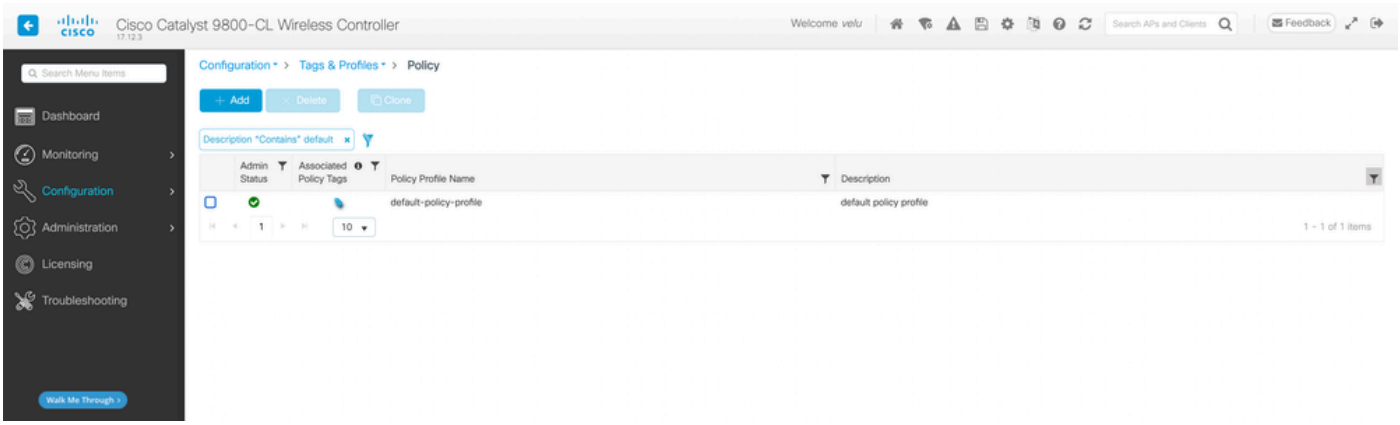
Pour ce faire :

1. Accédez à Configuration > Security > ACLs > Access Control Lists.
2. Créez une nouvelle liste de contrôle d’accès avec des règles pour autoriser le trafic nécessaire.

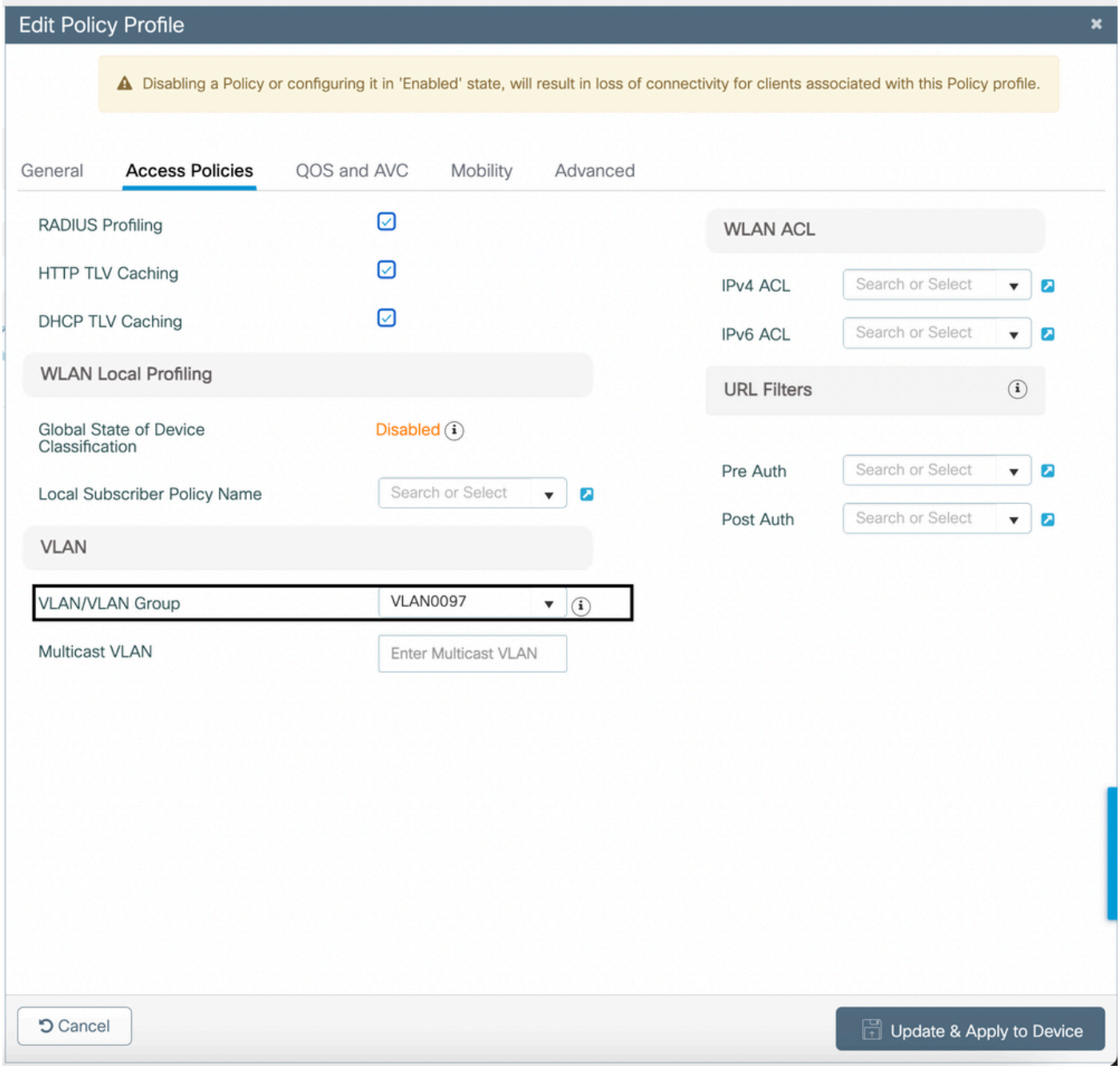


Configurer le profil de stratégie

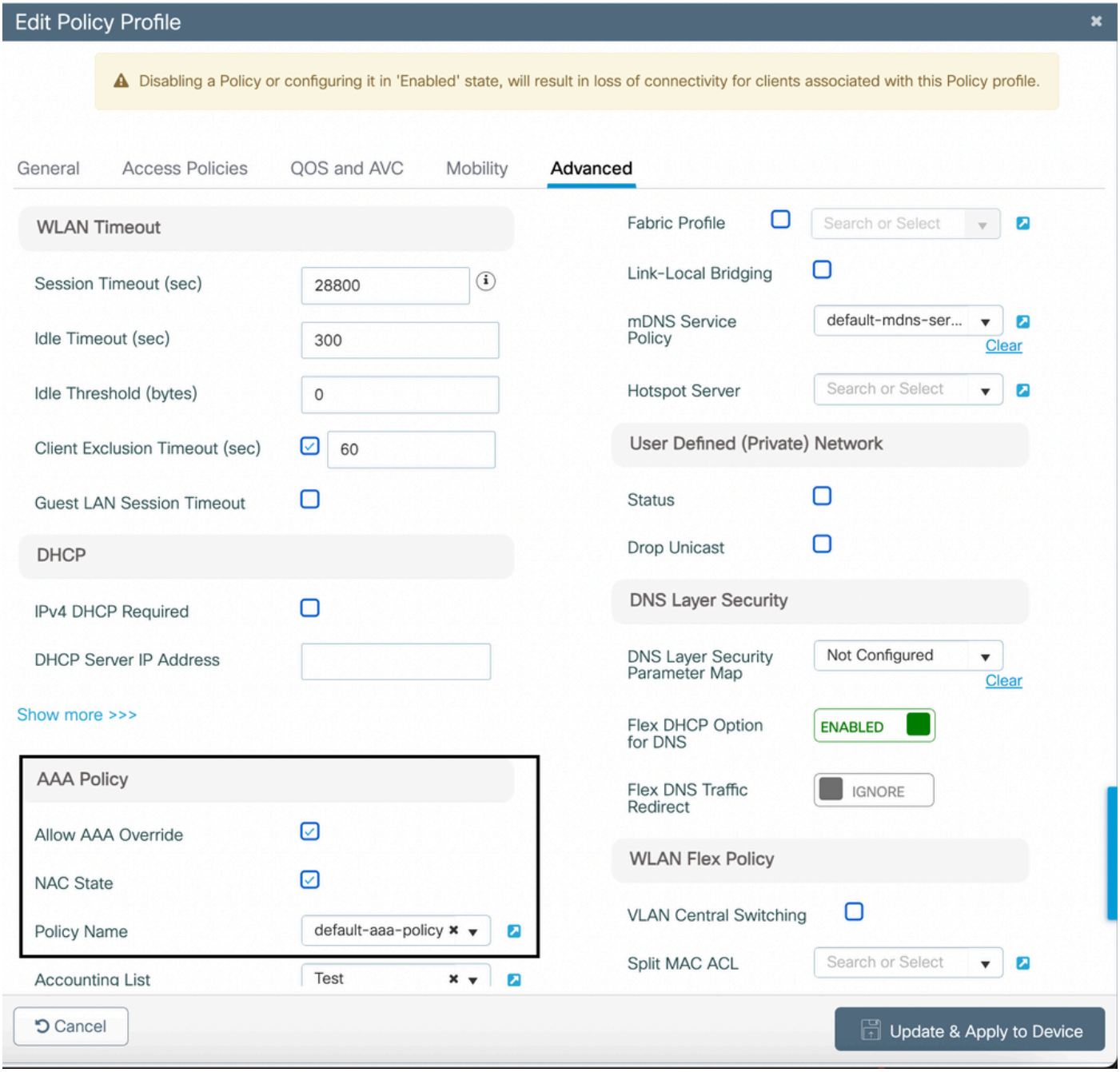
1. Accédez à Configuration > Tags & Profiles > Policy. Vous pouvez créer ou utiliser la stratégie par défaut :



2. Attribuez le VLAN approprié sous Access Policies :

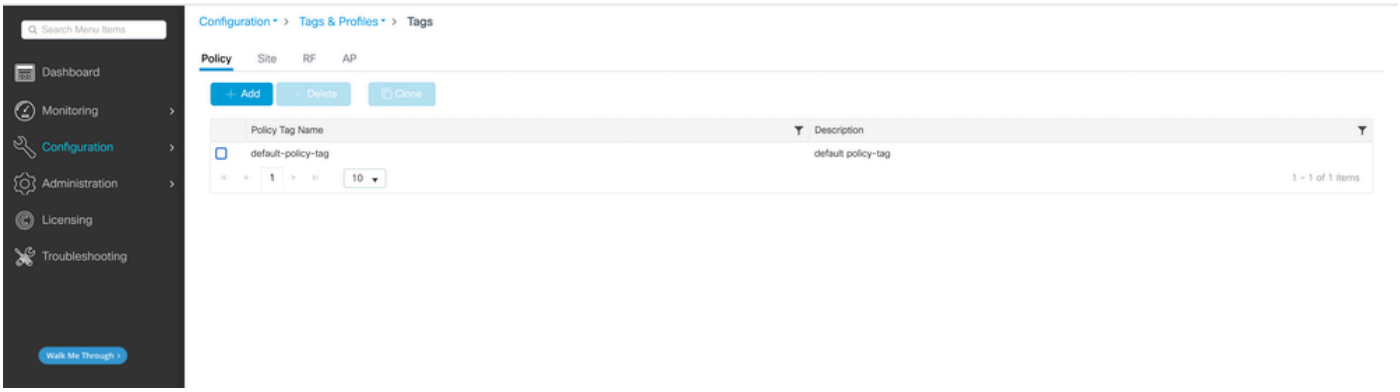


3. Activez également Allow AAA Override et l'état NAC sous Advanced de la stratégie.



Appliquer les balises et déployer

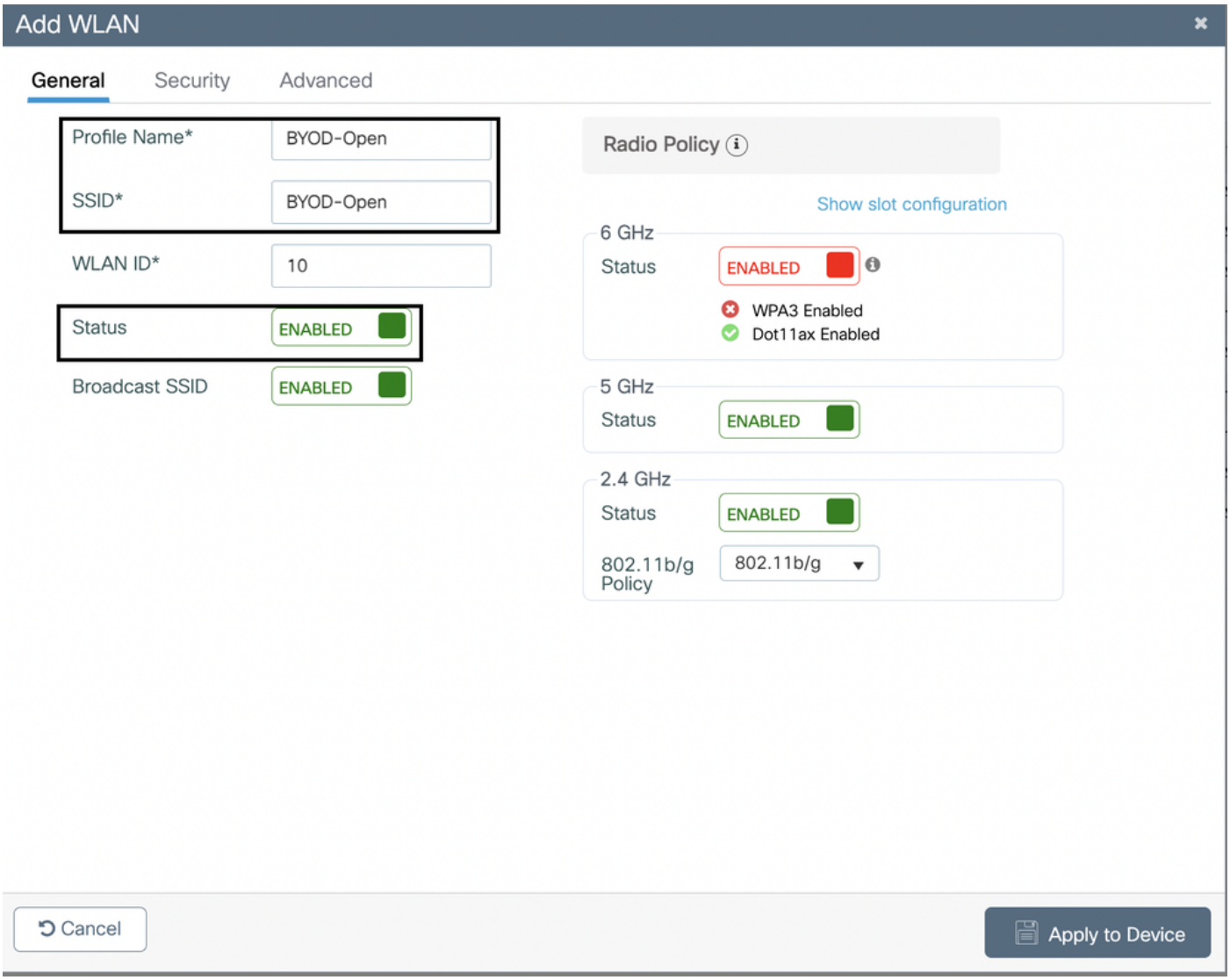
- Accédez à Configuration > Tags & Profiles > Tags.
- Créez ou modifiez une balise pour inclure le WLAN et le profil de stratégie.
- Attribuez la balise aux points d'accès.



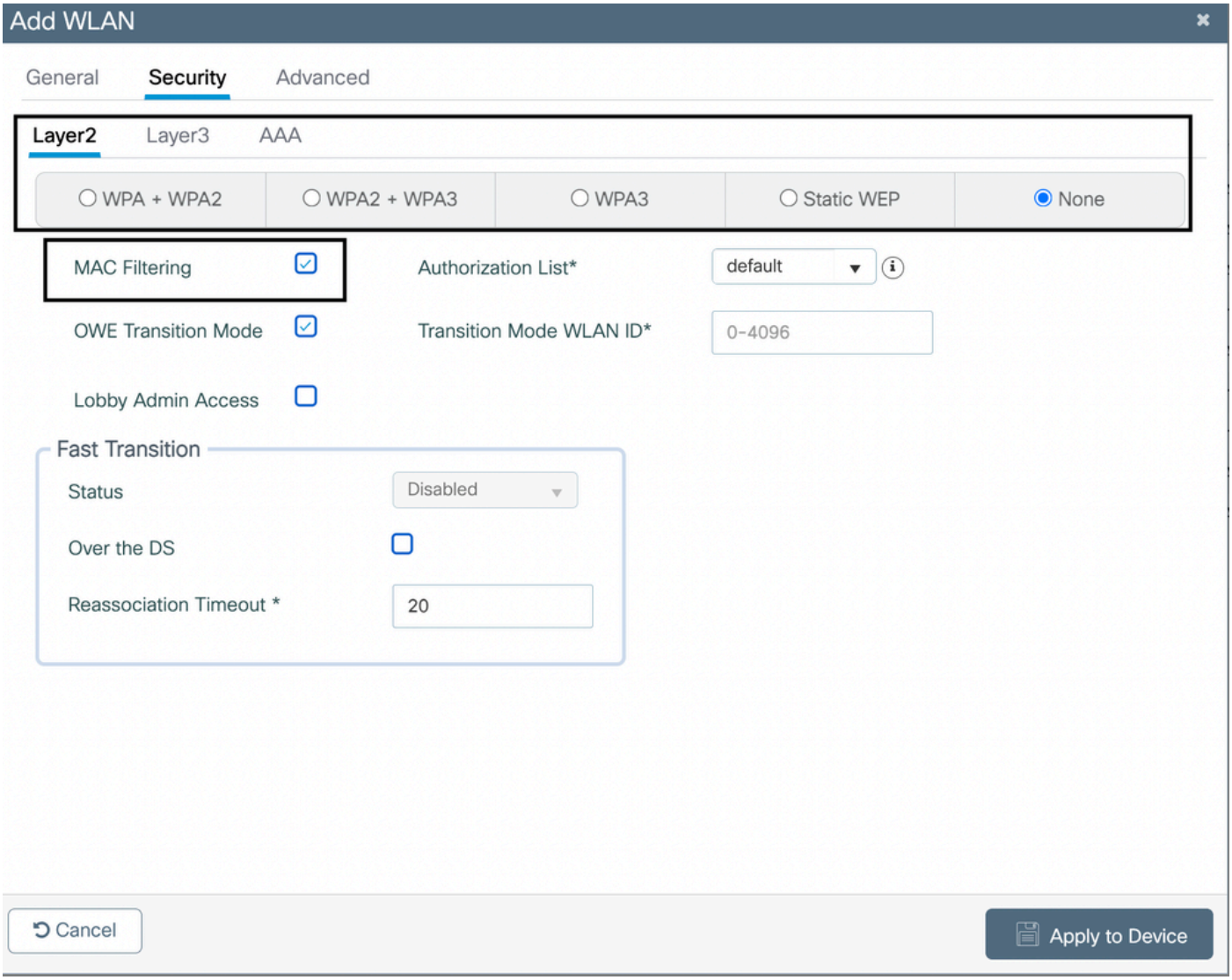
Configurer un SSID ouvert/non sécurisé

Le SSID ouvert est créé uniquement lorsque vous décidez d'avoir une configuration BYOD à double SSID sur votre environnement.

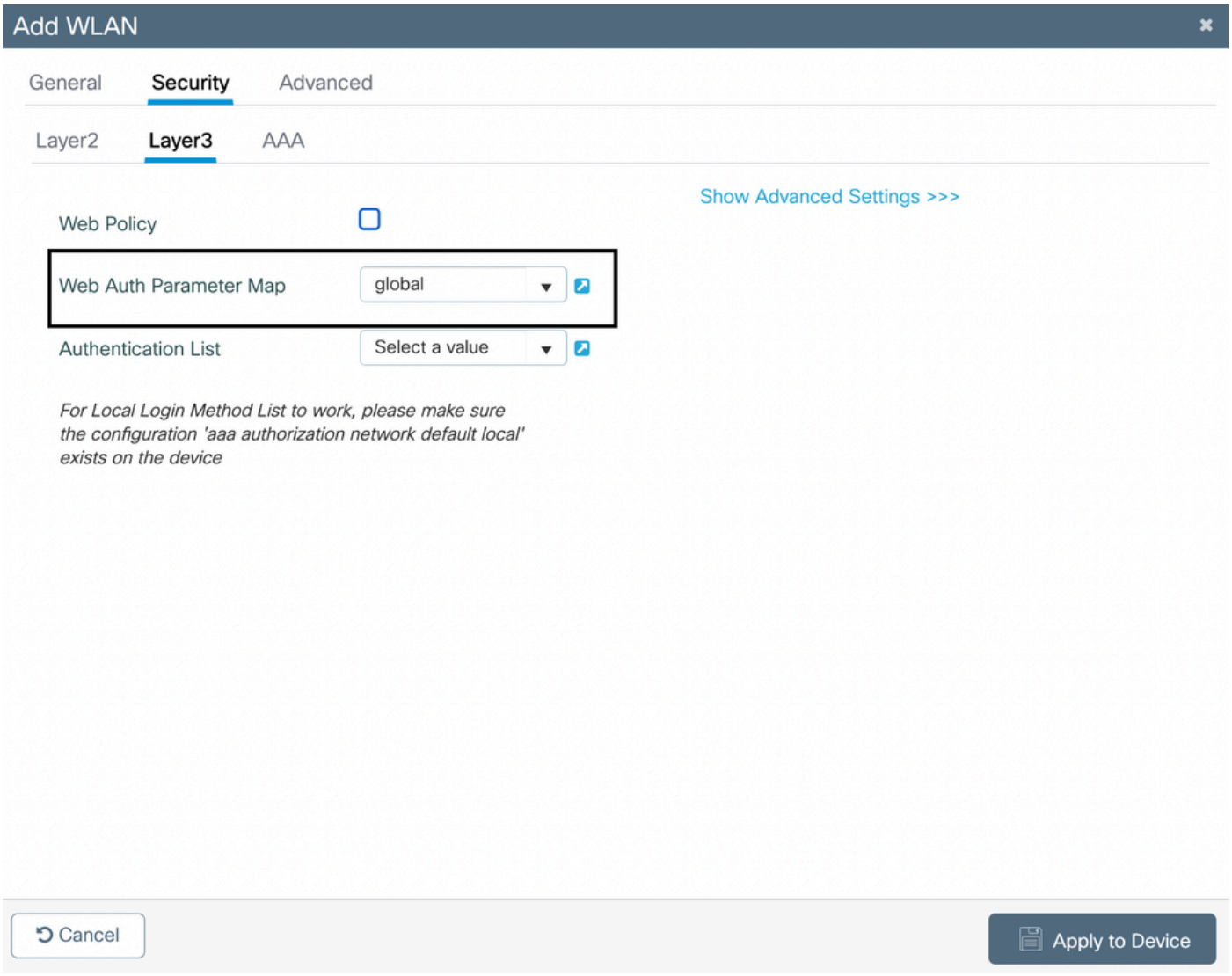
1. Accédez à Configuration > Tags & Profiles > WLANs. Cliquez sur le bouton Ajouter.
2. Entrez un nom SSID dans l'onglet General et activez le bouton WLAN.



3. Cliquez sur l'onglet Sécurité de la même fenêtre. Sélectionnez la case d'option None et activez le filtrage Mac.



4. Dans la couche 3, sous Sécurité, sélectionnez le paramètre global de la carte de paramètres d'authentification Web. Si un autre profil d'authentification Web est configuré sur le WLC, vous pouvez également le mapper ici :



Configuration ISE

Conditions préalables

- S'assurer que Cisco ISE est installé et sous licence pour la fonctionnalité BYOD.
- Ajoutez votre WLC à ISE en tant que périphérique réseau avec le secret partagé RADIUS.

Certificats

- Installez un certificat de serveur valide sur ISE pour éviter les avertissements de sécurité du navigateur.
- Assurez-vous que le certificat est approuvé par les terminaux (signé par une autorité de certification connue ou une autorité de certification interne avec une racine

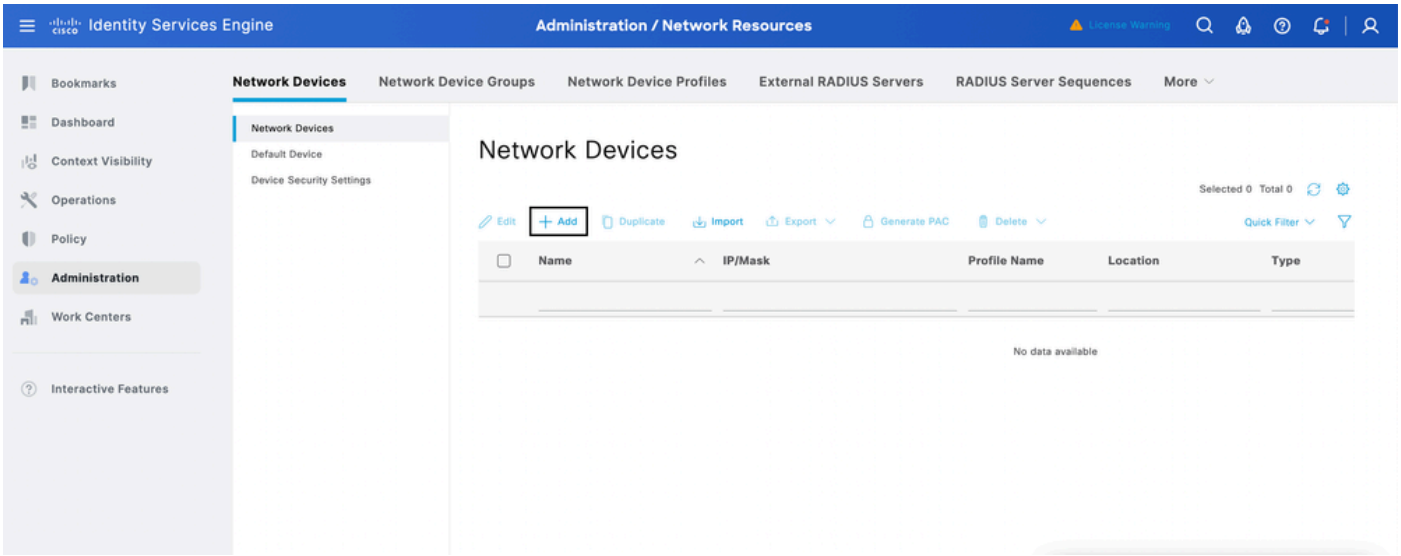
approuvée).

Configuration DNS

- Assurez-vous que DNS résout le nom d'hôte ISE pour le portail BYOD.

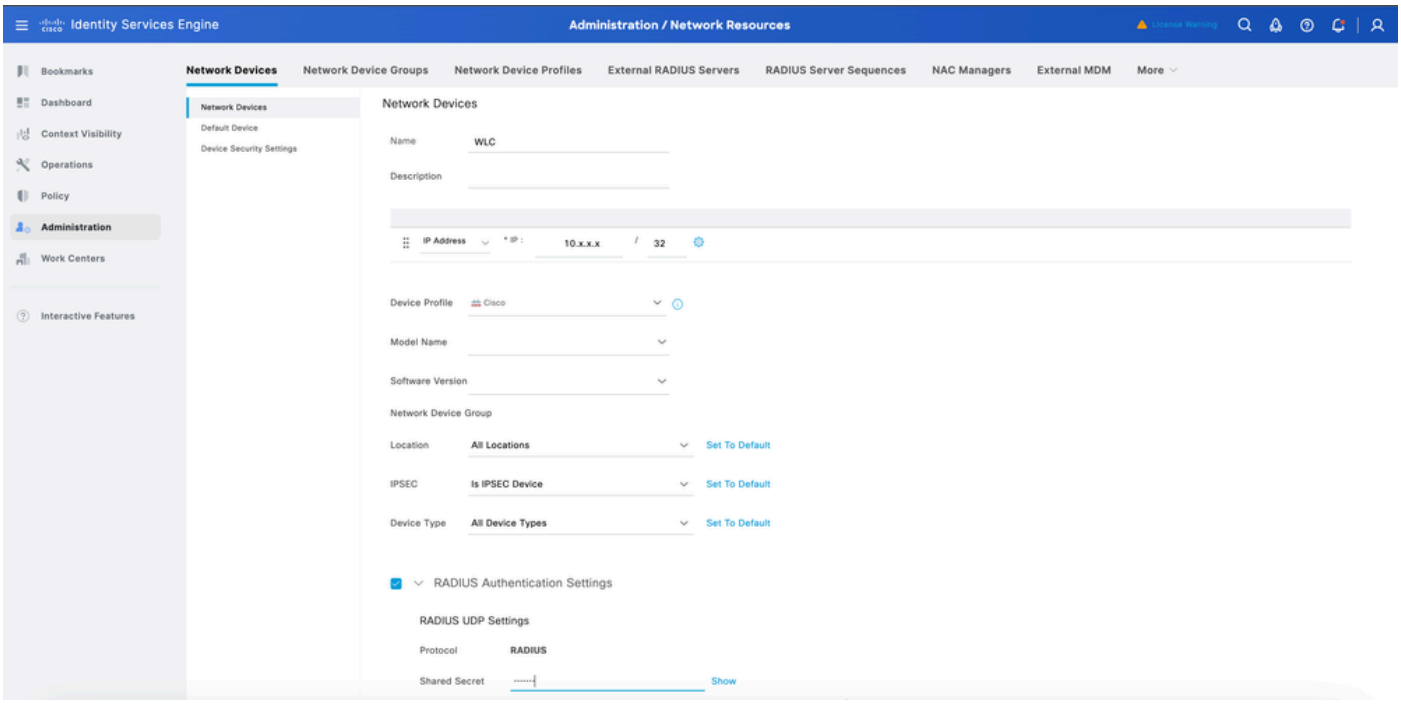
Configuration du périphérique réseau ISE

1. Connectez-vous à l'interface utilisateur Web ISE.
2. Accédez à Administration > Network Resources > Network Devices.



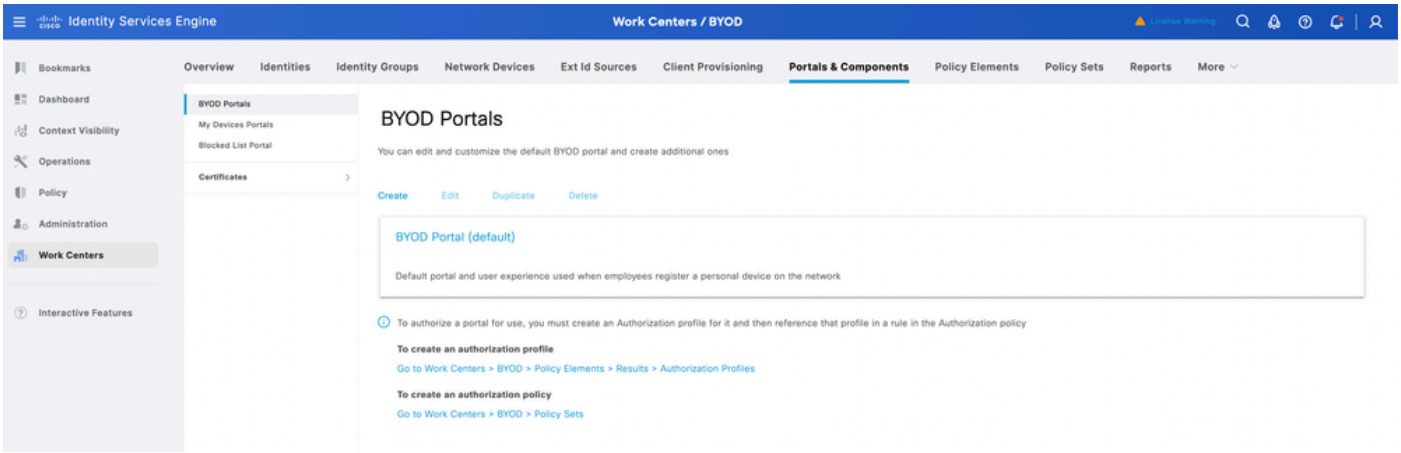
3. Ajoutez votre WLC en tant que périphérique réseau :

- Name : Entrez un nom pour le WLC.
- Adresse IP: Saisissez l'adresse IP de gestion WLC.
- Secret partagé RADIUS : Entrez le même secret partagé que celui configuré sur le WLC.
- Cliquez sur Submit.



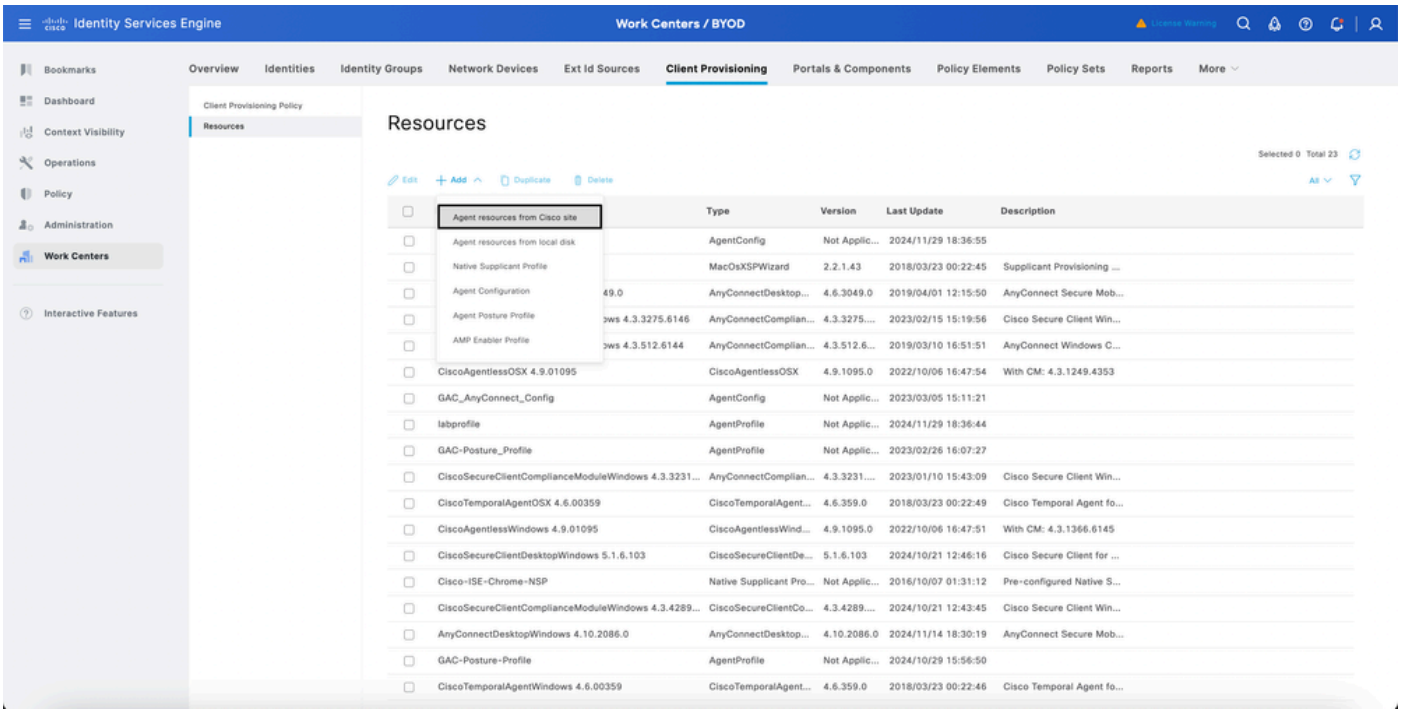
Créer un portail BYOD

1. Accédez à Work Centers > BYOD > Settings > Portals & Components > BYOD Portals.
2. Cliquez sur Add pour créer un portail BYOD ou vous pouvez utiliser le portail par défaut existant sur ISE.

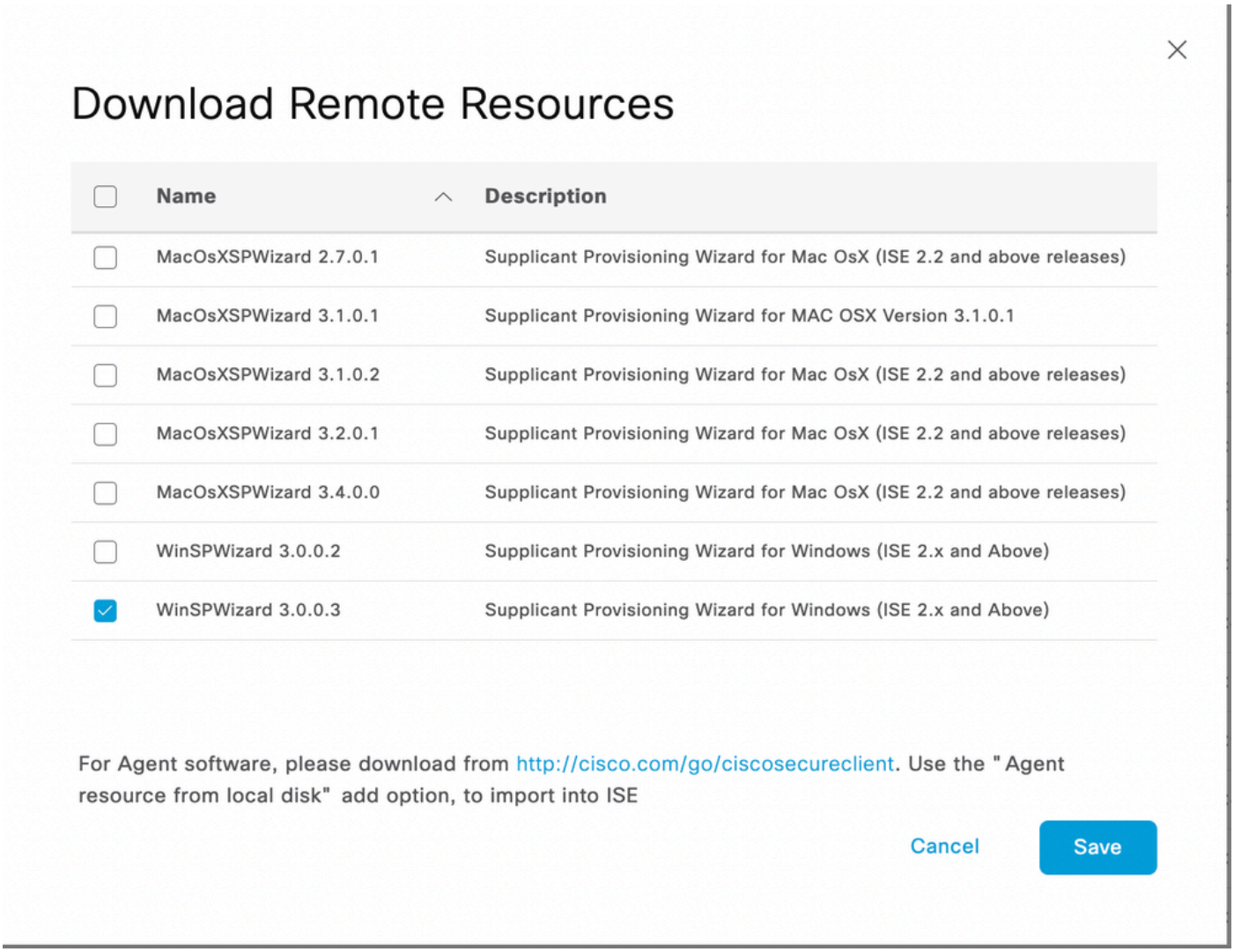


Télécharger la dernière version de Cisco IOS®

1. Accédez à Work Centers > BYOD > Client provisioning > Resources.
2. Cliquez sur le bouton Add et sélectionnez agent resources from the Cisco site.



3. Dans la liste des logiciels, sélectionnez la dernière version de Cisco IOS à télécharger.

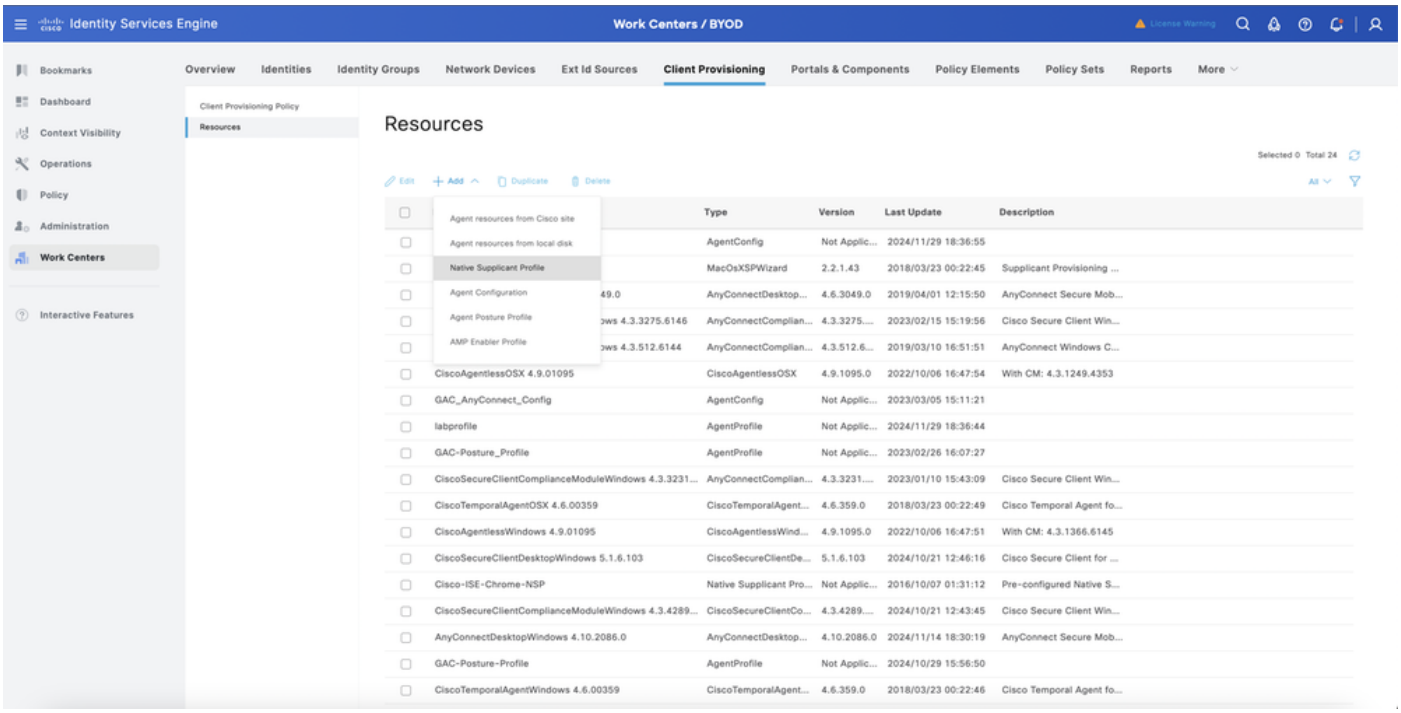


Remarque : Le logiciel Cisco IOS est téléchargé sur ISE pour les terminaux Windows et MacOS. Pour Apple iPhone IOS, il utilise un supplicant natif pour provisionner l'appareil et Pour appareil Android, vous avez Network setup assistant qui doit être téléchargé à partir de Play Store.

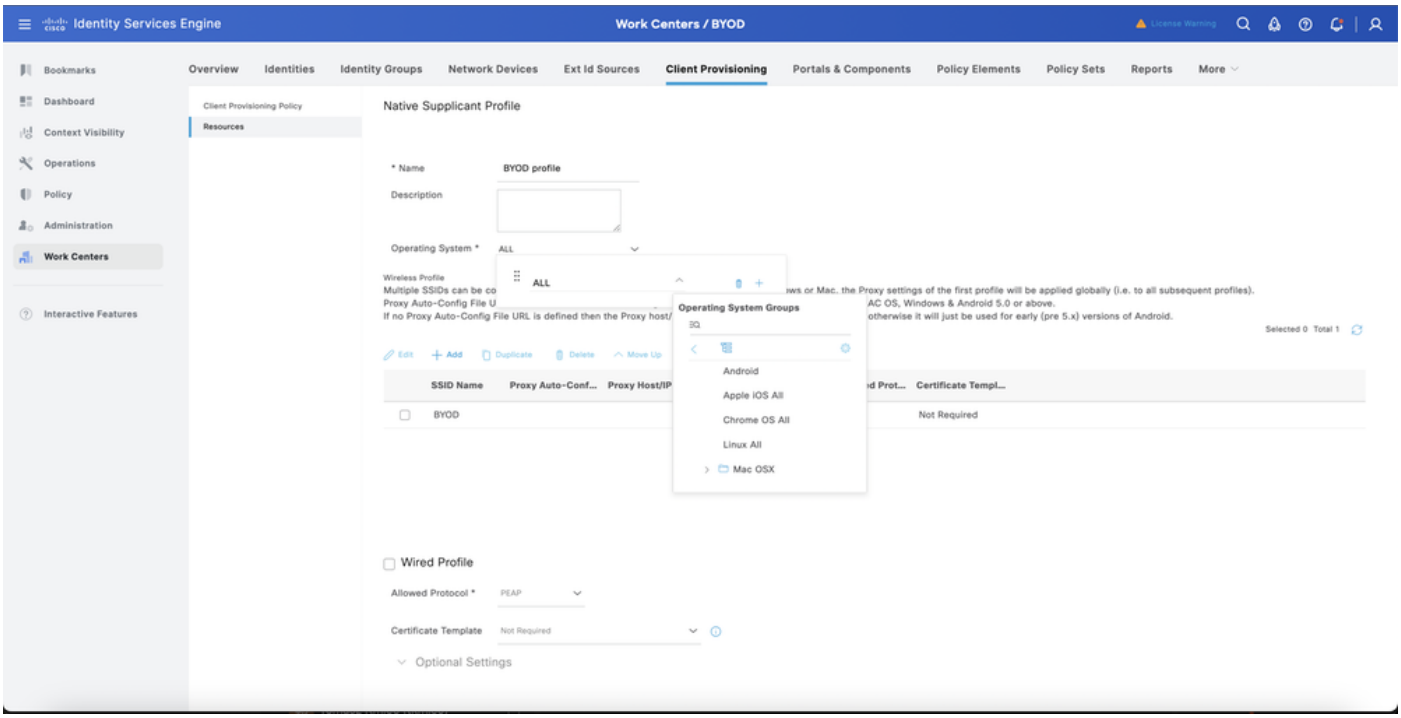
Créer un profil de terminal

1. Accédez à Work Centers > BYOD > Client provisioning > Resources.

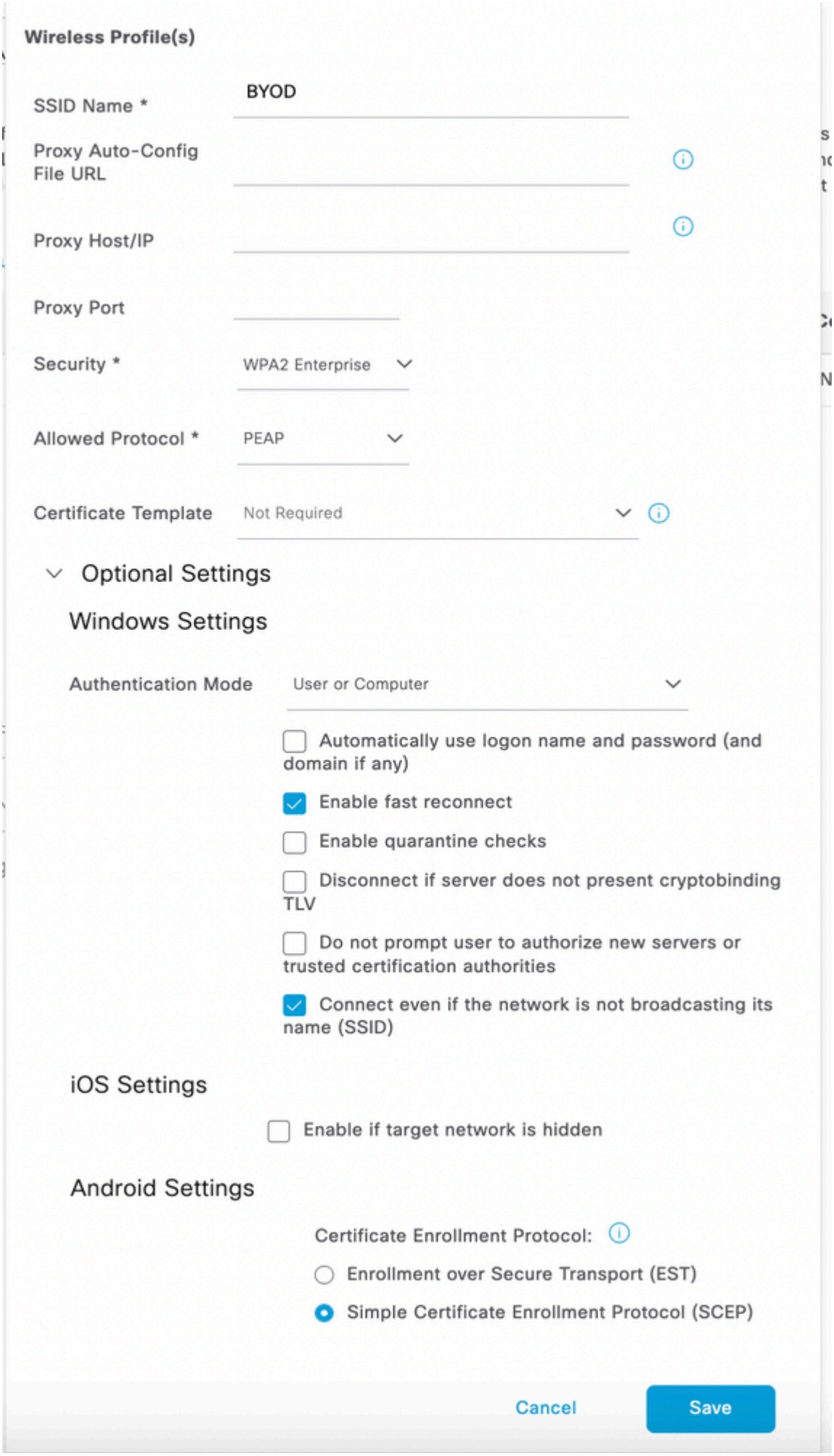
2. Cliquez sur Add, sélectionnez Native supplicant profile dans le menu déroulant.



3. Dans la liste déroulante Operating system (Système d'exploitation), sélectionnez le système d'exploitation requis que vous souhaitez intégrer au périphérique ou définissez-le sur ALL (TOUT) pour intégrer tous les terminaux de votre environnement :



4. Cliquez sur Add dans la page pour créer le profil de point de terminaison afin de configurer la norme 802.1X pour le point de terminaison :

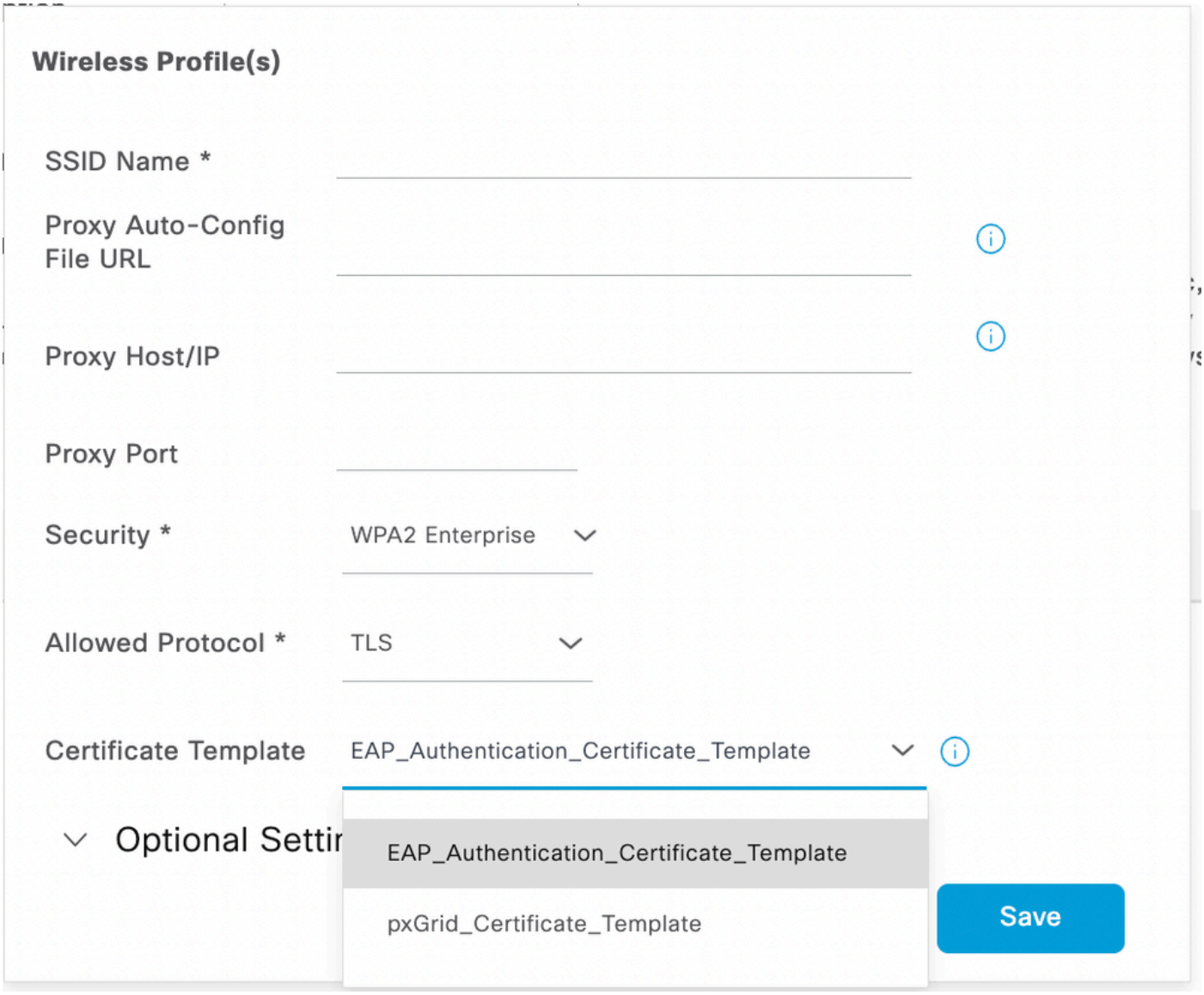

Wireless Profile(s)
SSID Name *
BYOD
Proxy Auto-Config File URL
Proxy Host/IP
Proxy Port
Security *
WPA2 Enterprise
Allowed Protocol *
PEAP
Certificate Template
Not Required
Optional Settings
Windows Settings
Authentication Mode
User or Computer
Automatically use logon name and password (and domain if any)
Enable fast reconnect
Enable quarantine checks
Disconnect if server does not present cryptobinding TLV
Do not prompt user to authorize new servers or trusted certification authorities
Connect even if the network is not broadcasting its name (SSID)
iOS Settings
Enable if target network is hidden
Android Settings
Certificate Enrollment Protocol:
Enrollment over Secure Transport (EST)
Simple Certificate Enrollment Protocol (SCEP)
Cancel
Save

Remarque : En fonction de vos besoins, configurez le profil de point de terminaison pour le point de terminaison dans votre environnement. Le profil de terminaux nous permet de configurer EAP-PEAP, EAP-TLS.

5. Cliquez sur Enregistrer, puis sur Soumettre sur le profil de point de terminaison.

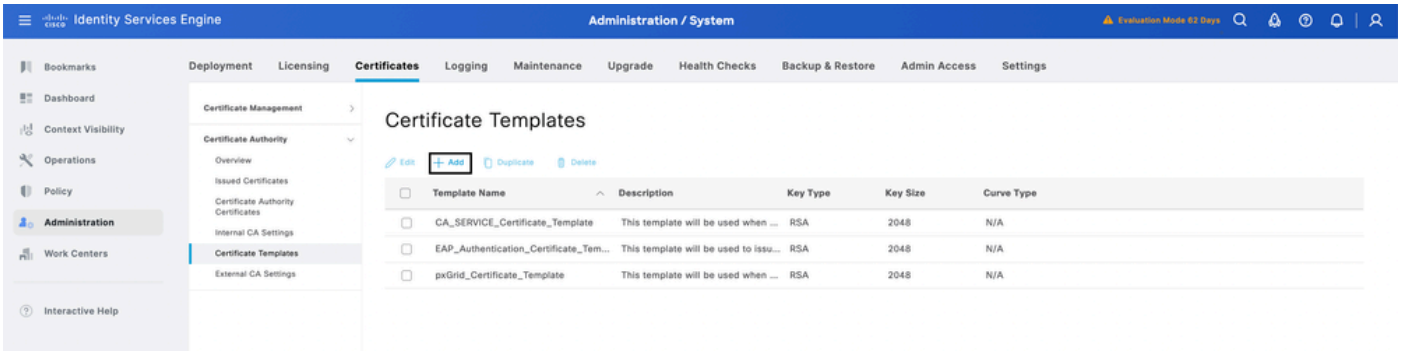
Modèle de certificat

Le profil de point de terminaison est préconfiguré pour exécuter EAP-TLS. Un modèle de certificat doit être ajouté au profil. Par défaut, ISE dispose de deux modèles prédéfinis qui peuvent être sélectionnés dans la liste déroulante.

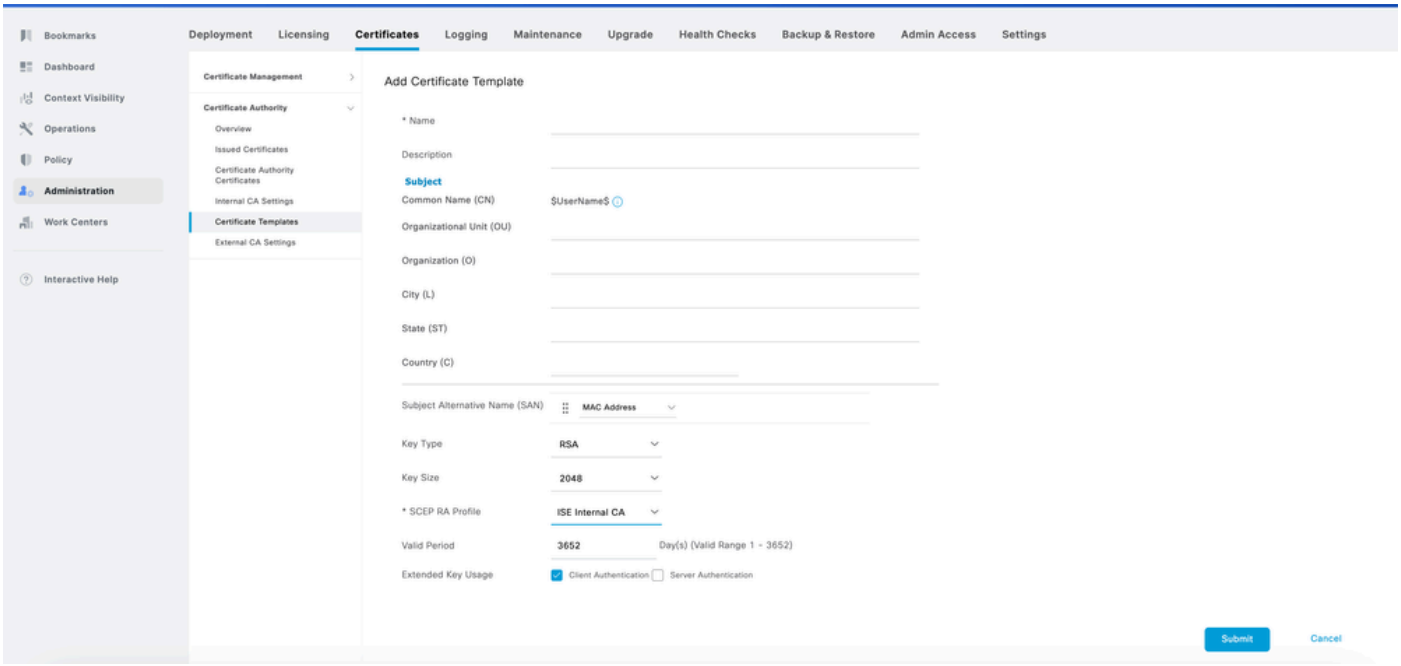


Pour créer un nouveau modèle de certificat, procédez comme suit :

1. Accédez à Administration > System > Certificates > Certificate Authority > Certificate Templates.
2. Cliquez sur le bouton Ajouter de la page.



3. Renseignez les détails adaptés aux besoins spécifiques de votre organisation.



4. Cliquez sur Soumettre pour enregistrer les modifications.

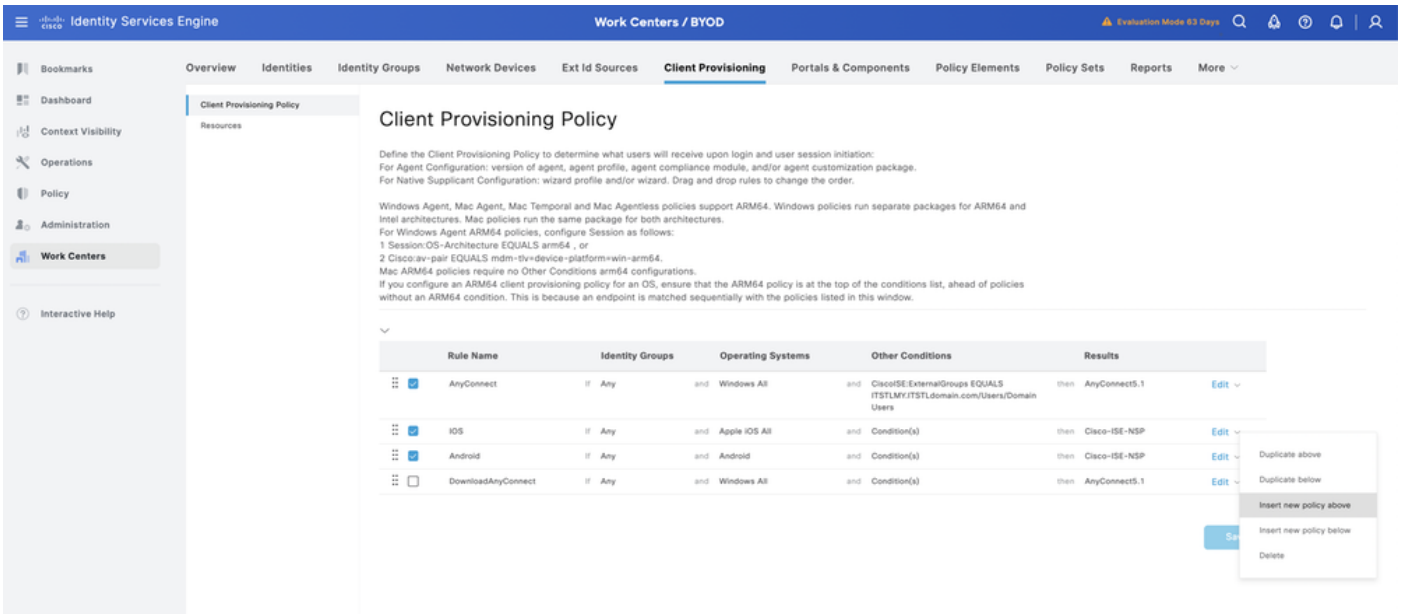
Remarque : Le modèle de certificat peut être utile dans un scénario où vous avez différents domaines et où vous segmentez l'utilisateur en ajoutant une valeur différente

---

dans l'unité d'organisation du certificat.

Mappage d'un profil de point de terminaison au portail d'approvisionnement client

1. Accédez à Work Centers > BYOD > Client provisioning > Client provisioning Policy.
2. Cliquez sur v on des règles pour créer une nouvelle règle d'approvisionnement de client.

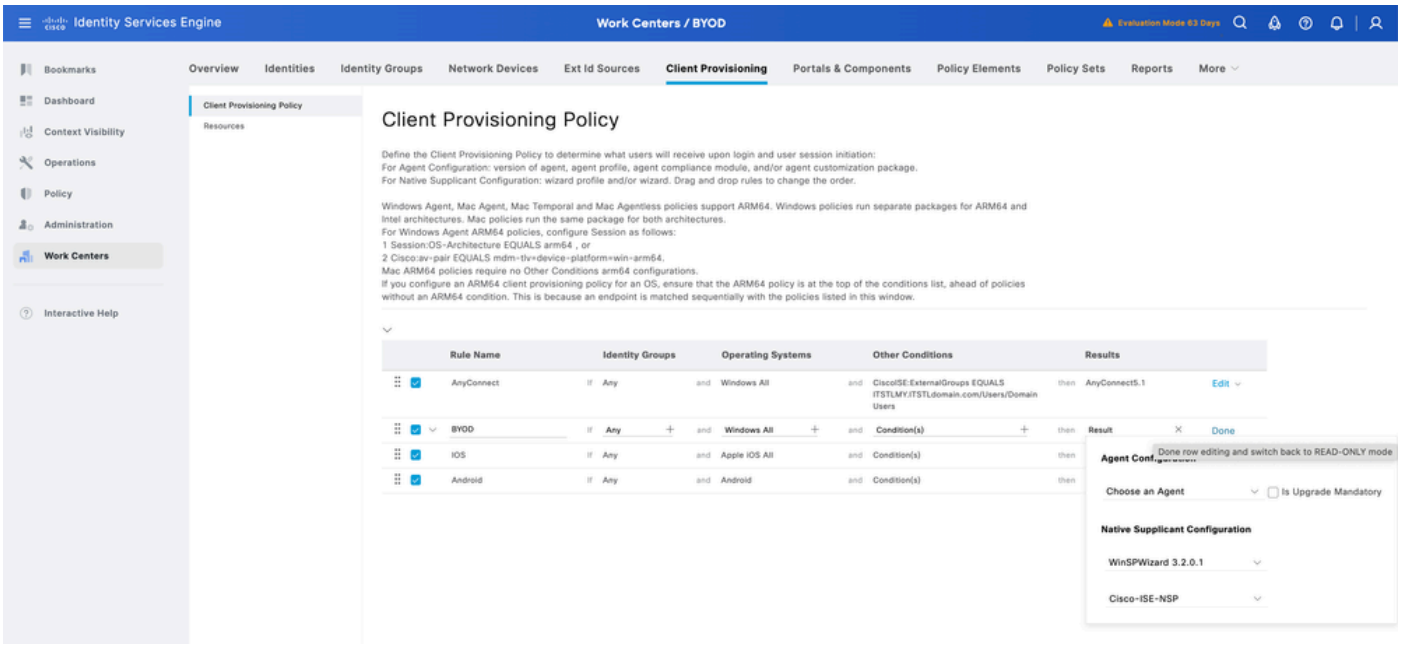


3. Publiez la création de la nouvelle règle sur la page

4. Ajoutez le groupe d'identité si vous souhaitez restreindre l'accès au portail BYOD à certains utilisateurs.

5. Ajoutez le système d'exploitation auquel vous souhaitez accéder au portail BYOD.

6. Mappez la version de Cisco IOS à partir de la liste déroulante et sélectionnez également le profil de point de terminaison que vous avez créé à partir du résultat.



7. Cliquez sur Terminé, puis sur le bouton Enregistrer.

Remarque : Cette stratégie a un impact sur l'approvisionnement du client de posture et sur l'approvisionnement BYOD, où la section Configuration de l'agent détermine l'agent de posture et le module de conformité appliqués pour les vérifications de posture, tandis que la section Configuration du demandeur natif gère les paramètres des flux d'approvisionnement BYOD

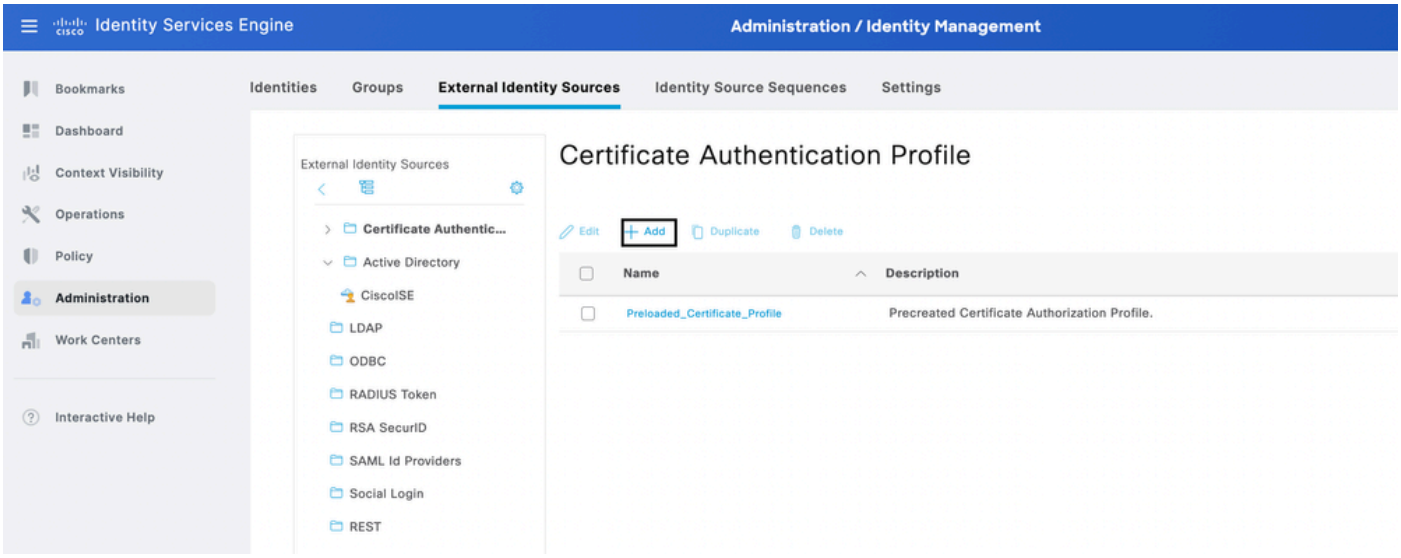
Configuration des ensembles de stratégies ISE pour le BYOD avec un seul SSID

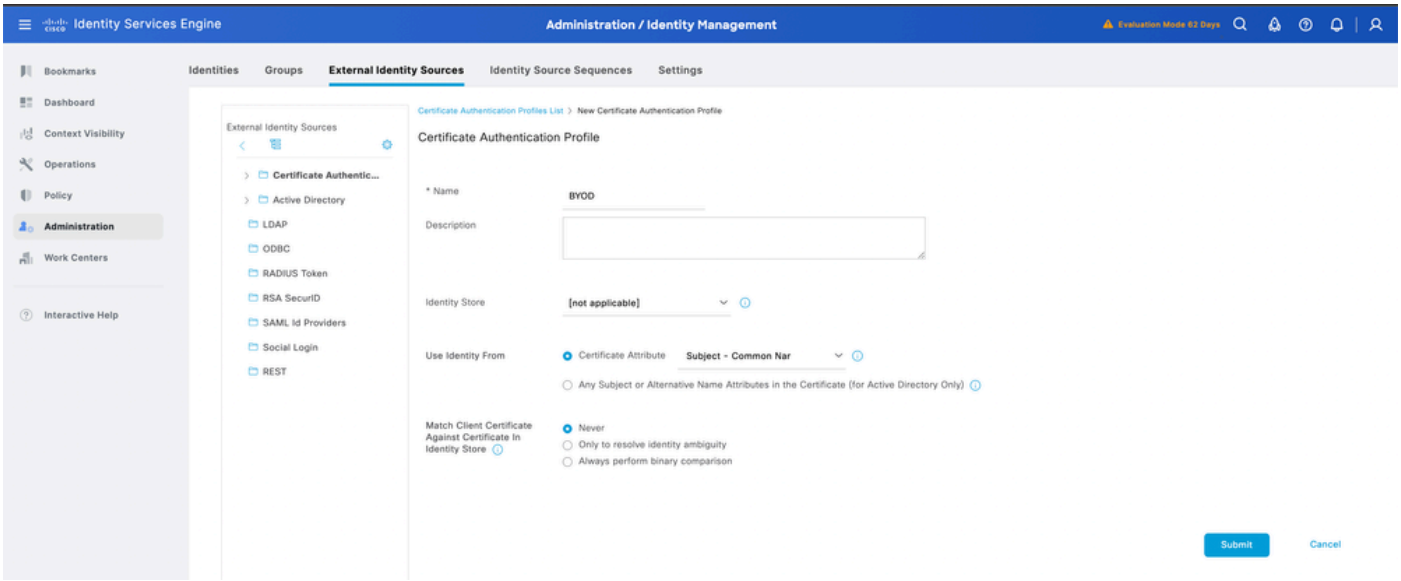
1. Accédez à Policy > Policy Set et créez une stratégie pour le flux BYOD sur ISE :



2. Ensuite, accédez à Administration > Gestion des identités > Sources d'identité externes > Profil

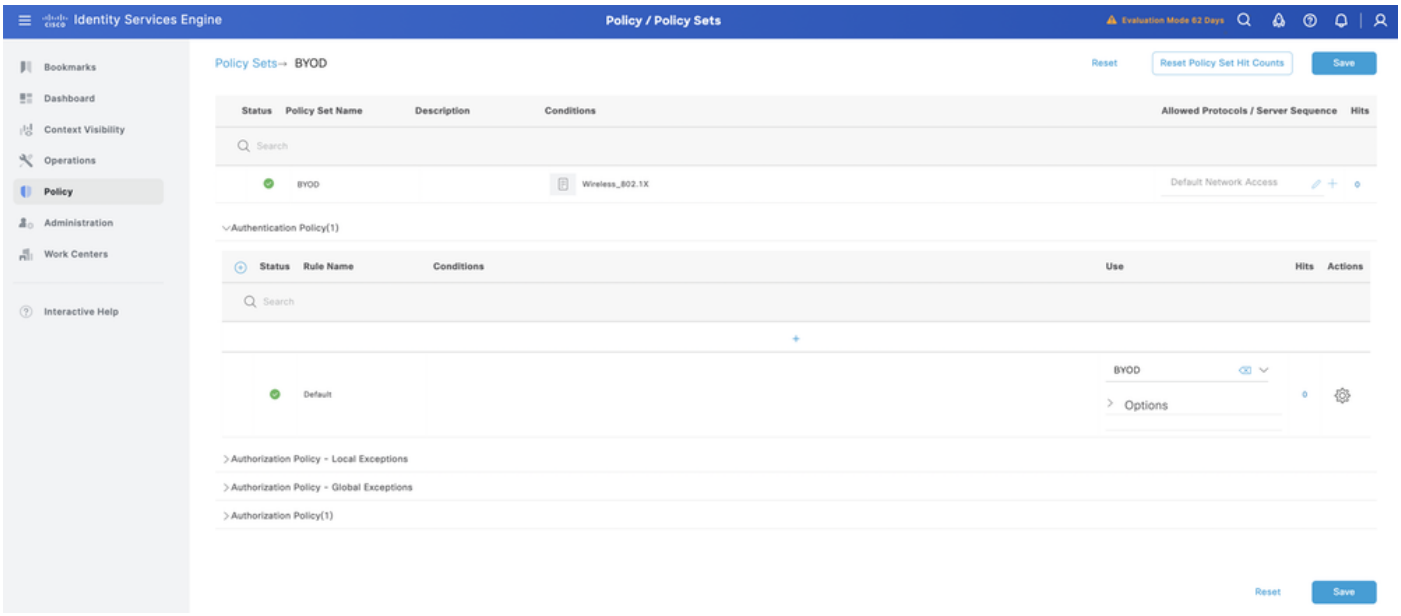
d'authentification de certificat. Cliquez sur le bouton Add pour créer le profil de certificat :





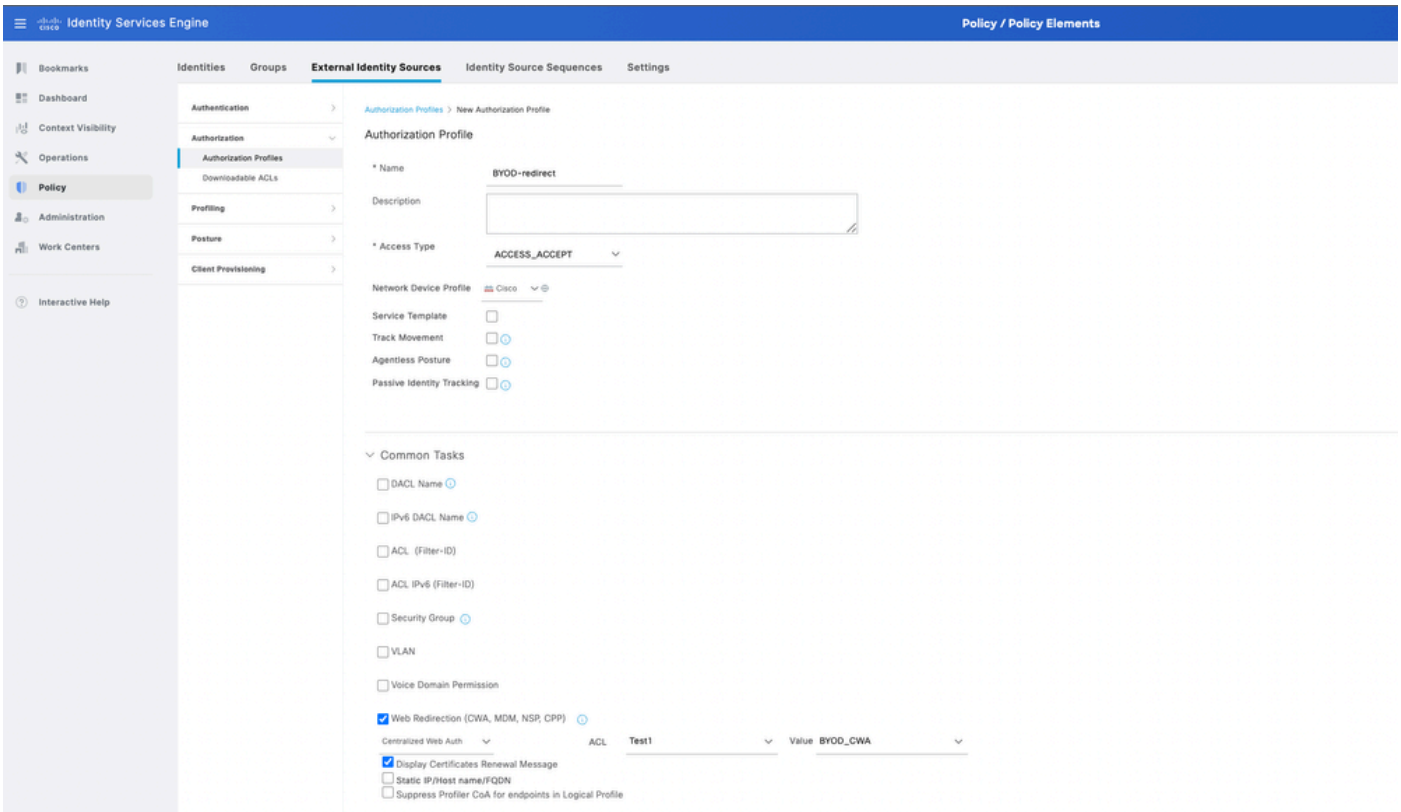
Remarque : Dans le magasin d'identités, vous pouvez toujours sélectionner votre Active Directory qui a été intégré à ISE pour effectuer une recherche d'utilisateur à partir du certificat pour plus de sécurité.

3. Cliquez sur Soumettre pour enregistrer la configuration. Ensuite, mappez le profil de certificat à la stratégie définie pour le BYOD :

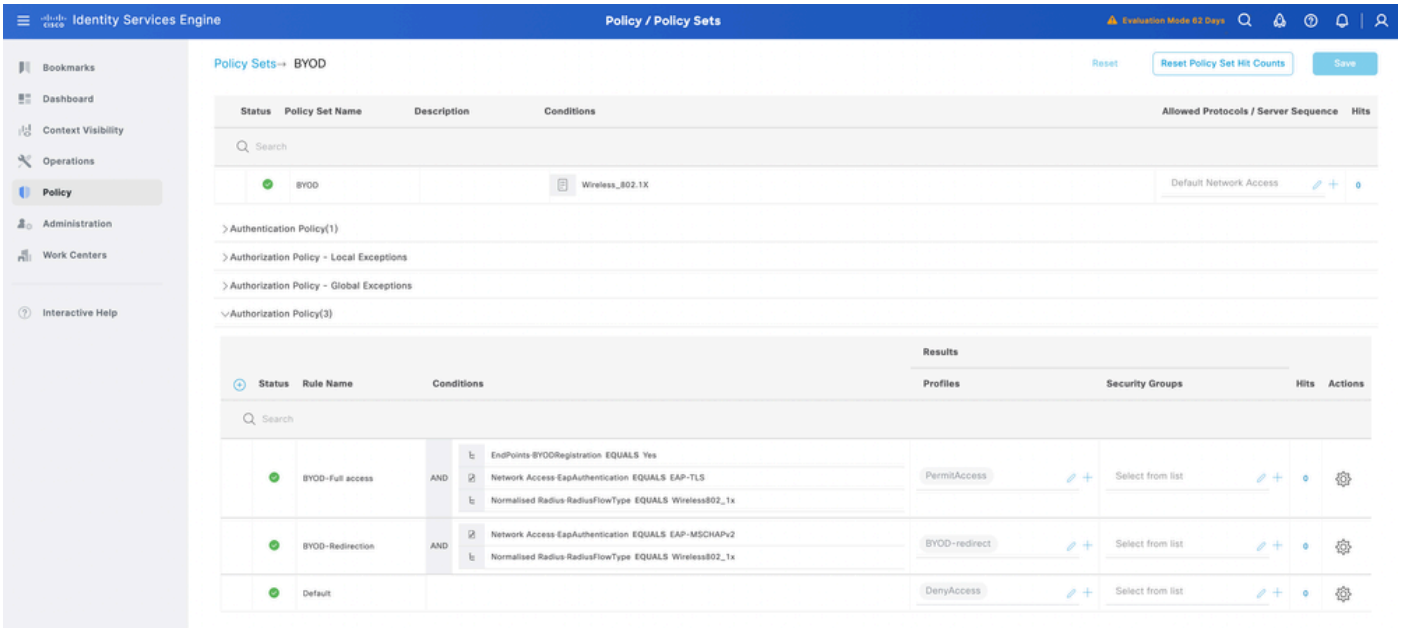


4. Configurez le profil d'autorisation pour la redirection BYOD et l'accès complet après le flux BYOD. Allez à Policy > Policy Elements > Results > Authorization > Authorization Profiles (politique > éléments de politique > résultats > autorisation > profils d'autorisation).

5. Cliquez sur Ajouter et créez un profil d'autorisation. Vérifiez la redirection Web (CWA, MDM, NSP, CPP) et mappez la page BYOD Portal. Ajoutez également le nom de la liste de contrôle d'accès de redirection du WLC au profil. Pour le profil d'accès complet, configurez un accès autorisé avec le VLAN d'entreprise correspondant dans le profil.



6. Mappez le profil d'autorisation à la règle d'autorisation. L'accès complet au BYOD doit avoir la règle EndPoints·BYODegistration égale à yes afin que l'utilisateur obtienne un accès complet au réseau après le flux BYOD.

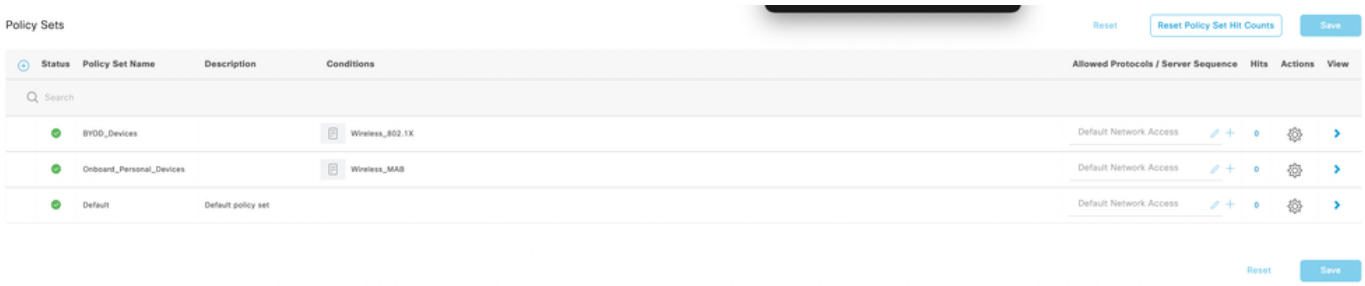


Configuration des ensembles de stratégies ISE pour le BYOD à double SSID

Dans la configuration BYOD à double SSID, le jeu de deux stratégies est configuré sur ISE. Le premier jeu de stratégies est pour le SSID ouvert/non sécurisé, où la configuration du jeu de stratégies redirige l'utilisateur vers la page BYOD Portal lors de la connexion au SSID ouvert/non sécurisé :

1. Accédez à Policy > Policy Set et créez une politique pour le flux BYOD sur ISE.

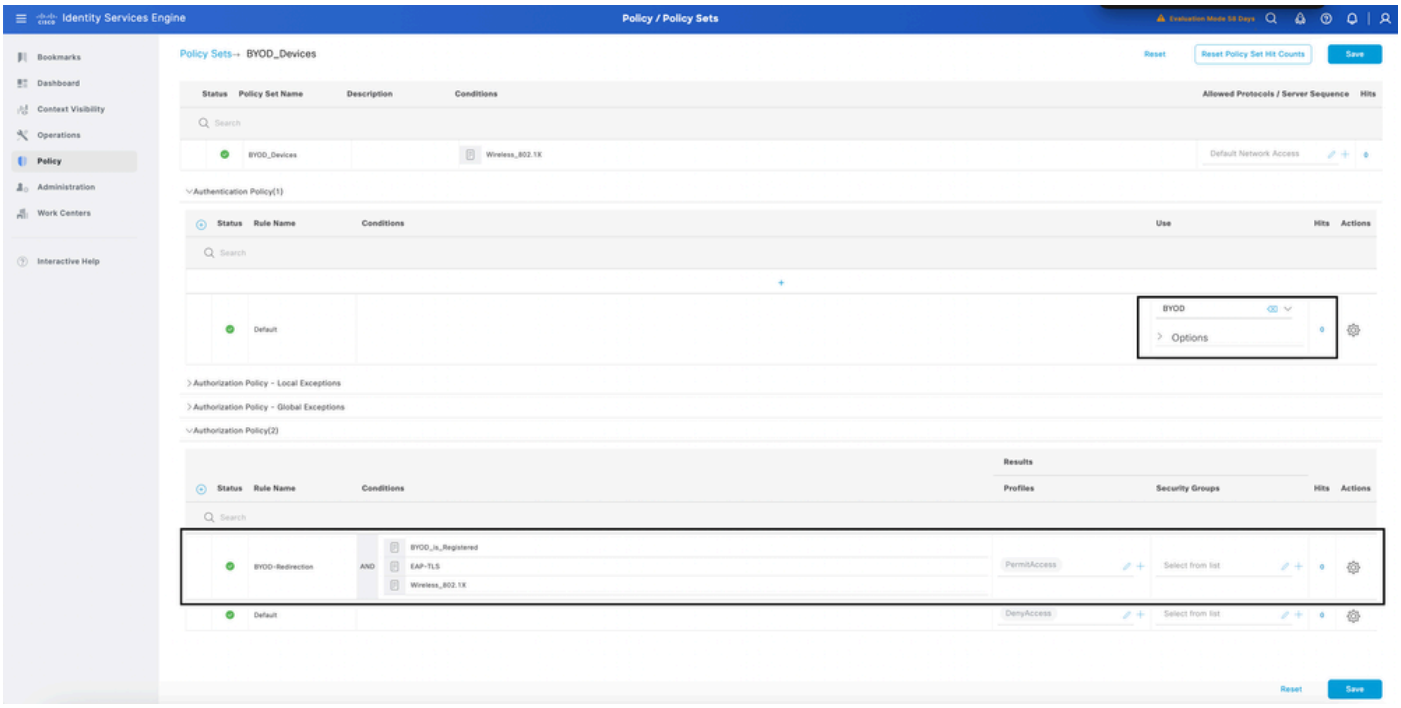
2. Créez un ensemble de stratégies pour le SSID ouvert/non sécurisé et le SSID d'entreprise qui authentifie l'utilisateur BYOD enregistré sur ISE.



3. Dans l'ensemble Politique d'intégration, sélectionnez Continuer sous les options. Pour la stratégie d'autorisation, créez une condition et mappez le profil d'autorisation de redirection. Les mêmes étapes sont impliquées dans la création du profil d'autorisation, que l'on peut trouver au point 4.

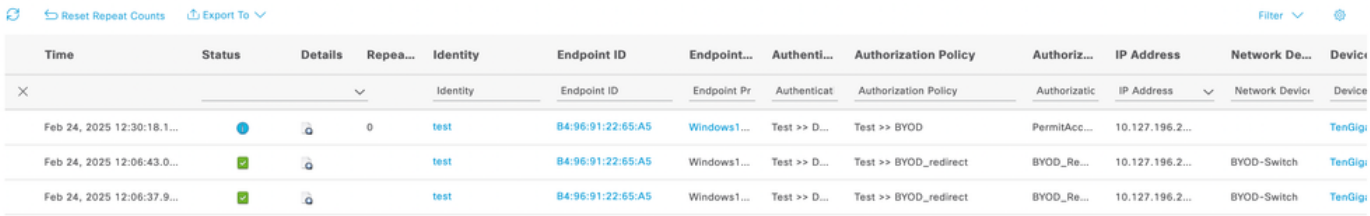


4. Dans l'ensemble de stratégies enregistré pour le BYOD, configurez la stratégie d'authentification avec le profil de certificat identique à celui indiqué dans Configurer les ensembles de stratégies ISE pour le BYOD avec SSID unique au point 2. Créez également une condition pour la stratégie d'autorisation et mappez le profil d'accès complet à la stratégie.

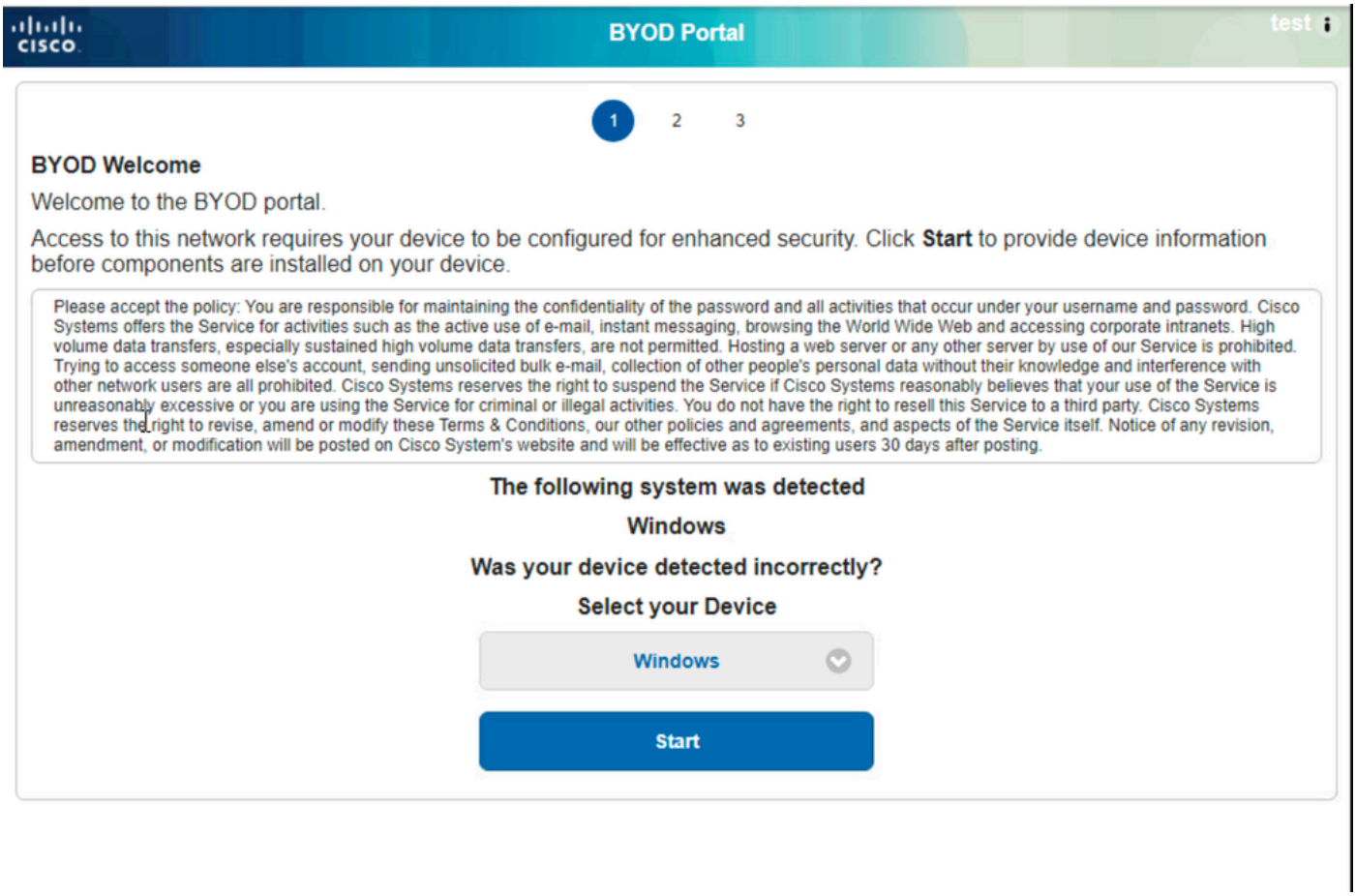


Journalisation

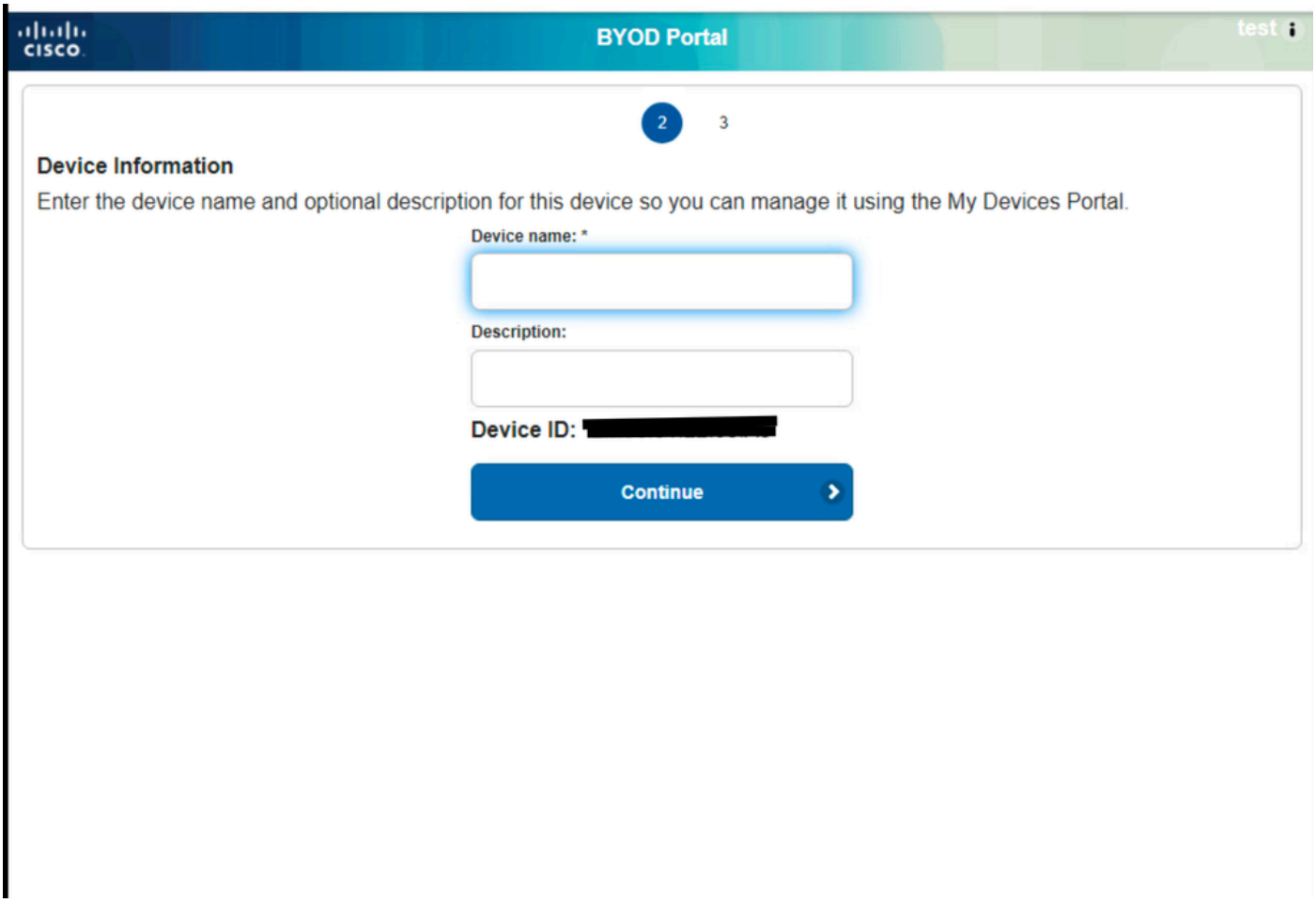
À partir du journal en direct d'ISE, l'authentification de l'utilisateur est réussie et redirige vers la page BYOD Portal. Une fois le flux BYOD terminé, l'utilisateur se voit accorder l'accès au réseau :



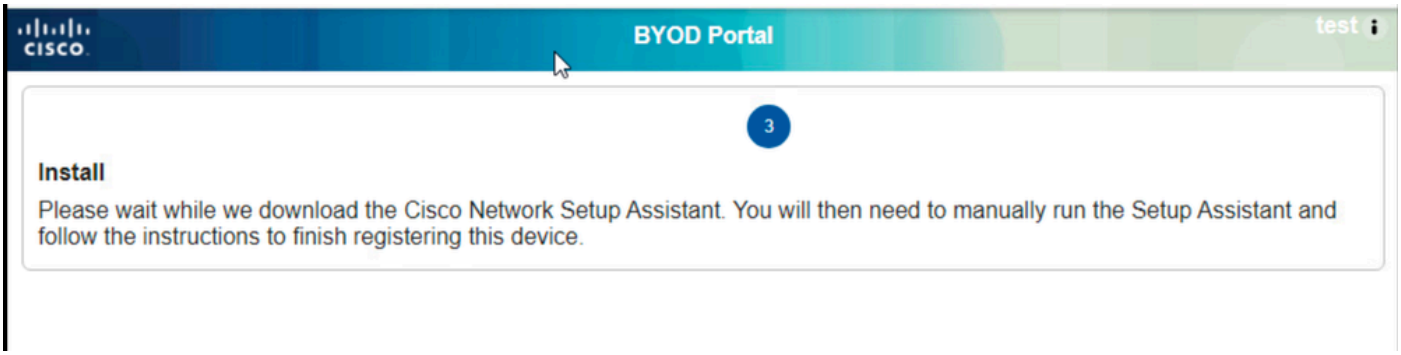
Du point de vue de l'utilisateur, ils sont d'abord redirigés vers la page BYOD Portal et le périphérique approprié doit être sélectionné à partir de la page Web. Pour les tests, un périphérique Windows 10 a été utilisé :



Après avoir cliqué sur le bouton Next (Suivant), vous êtes redirigé vers une page où l'utilisateur est invité à saisir le nom du périphérique et sa description :

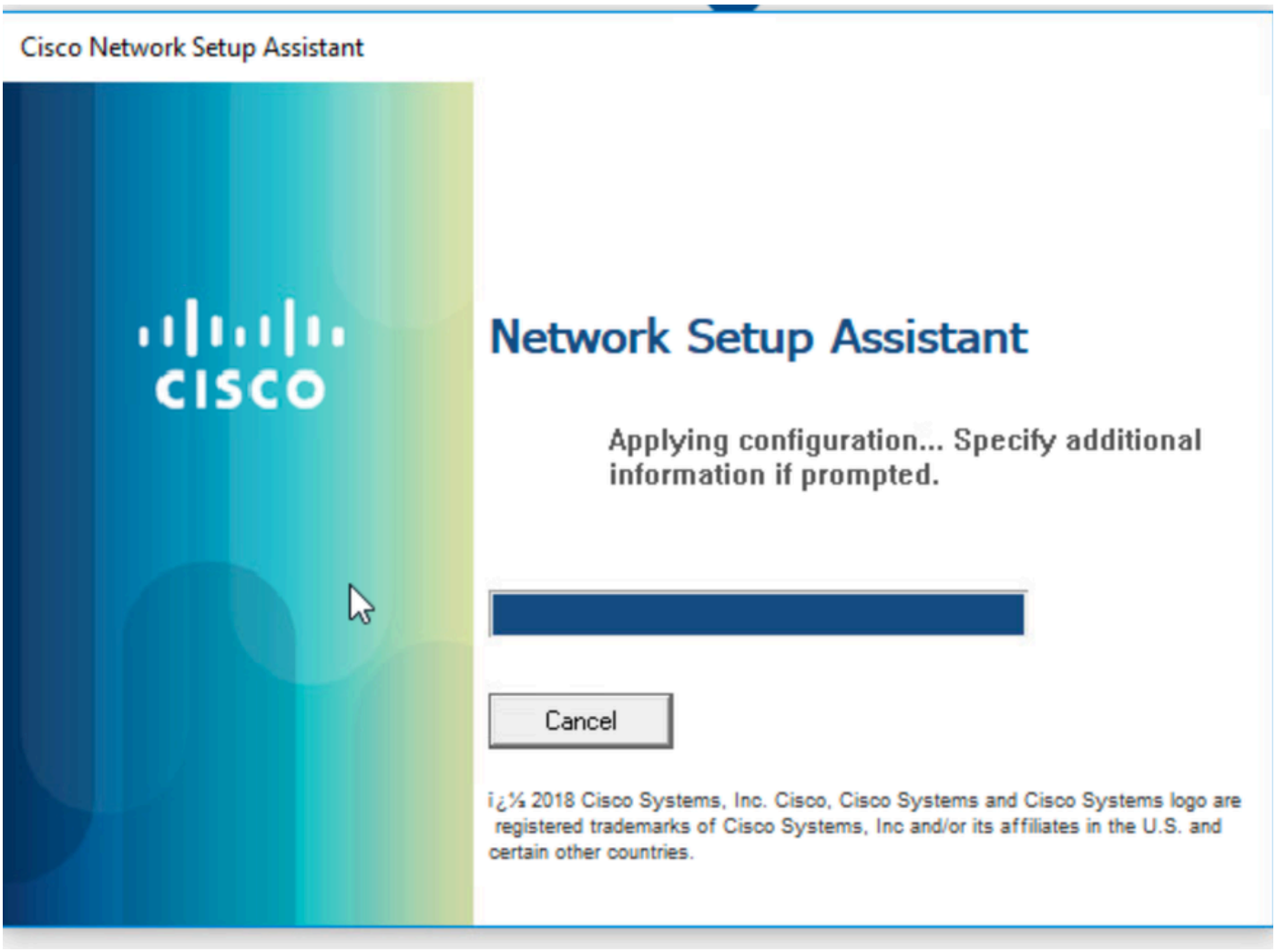


Indiquez que l'utilisateur doit télécharger l'outil Network Assistant pour télécharger le profil de point de terminaison et le certificat EAP TLS pour l'authentification si le profil est configuré pour effectuer l'authentification EAP-TLS :



Exécutez l'application Network Assistant dans les privilèges d'administration et cliquez sur le bouton Démarrer pour démarrer le flux d'intégration :


Cisco Network Setup Assistant
Network Setup Assistant
This application automatically configures network settings.
Start
Quit
i¿¼ 2018 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



L'utilisateur a été correctement intégré au réseau avec son périphérique personnel pour accéder aux ressources.

Dépannage

Pour résoudre le problème du BYOD, activez ce débogage sur ISE

Attributs à définir au niveau de débogage :

- client (guest.log)
- client-webapp (guest.log)
- scep (ise-psc.log)
- ca-service (ise-psc.log)
- admin-ca (ise-psc.log)
- runtime-AAA (prt-server.log)

- nsf (ise-psc.log)
- nsf-session (ise-psc.log)
- profiler (profiler.log)

Extrait de journal

Journaux invités

Ces journaux indiquent que l'utilisateur a correctement redirigé la page et téléchargé l'application Network Assistant :

2025-02-24 12:06:08,053 INFO [https-jsse-nio-10.127.196.172-8443-exec-4][] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::- chemin de mappage trouvé dans action-forwards, transfert vers : pages/byodWelcome.jsp // Page d'accueil du BYOD
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- Taille de pTranSteps:1
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, pTranSteps:[id: d2513b7b-7249-4bc3-a423-0e7d9a0b2500]
2025-02-24 12:06:09,968 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, stepTran : d2513b7b-7249-4bc3-a423-0e7d9a0b2500
2025-02-24 12:06:09,979 INFO [https-jsse-nio-10.127.196.172-8443-exec-8][[]] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::- chemin de mappage trouvé dans action-forwards, transfert vers : pages/byodRegistration.jsp
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- Taille de pTranSteps:1
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, pTranSteps:[id: f203b757-9e8a-473e-abdc-879d0cd37491]
2025-02-24 12:06:14,643 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][] cpm.guestaccess.flowmanager.step.StepExecutor -:000000000000000B30D59CC5::test:- getNextFlowStep, stepTran : f203b757-9e8a-473e-abdc-879d0cd37491
2025-02-24 12:06:14,647 INFO [https-jsse-nio-10.127.196.172-8443-exec-2][] portalwebaction.utils.portal.spring.ISEPortalControllerUtils -:000000000000000B30D59CC5::- chemin de mappage trouvé dans action-forwards, transfert vers : pages/byodInstall.jsp
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::- Session = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][]

cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::- portalSessionId = null
2025-02-24 12:06:14,713 DEBUG [https-jsse-nio-10.127.196.172-8443-exec-10][[]] cisco.cpm.client.provisioning.StreamingServlet -:000000000000000B30D59CC5::- StreamingServlet URI:/auth/provisioning/download/f6b73ef8-4502-4d50-81aa-bbb91e8828da/NetworkSetupAssistant.exe // L'application d'assistance réseau a été envoyée au point d'extrémité

Journaux Ise-Psc

Lorsque l'application est téléchargée sur le terminal, elle lance un flux SCEP pour obtenir le certificat client auprès d'ISE.

2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- CertStore contient 4 certificat(s) :
2025-02-24 12:04:39,807 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 1. '[issuer=CN=Certificate Services Root CA - iseguest ; serial=322815127387689606282525327846633020 89]'
2025-02-24 12:04:39,808 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 2. '[issuer=CN=Certificate Services Endpoint Sub CA - iseguest ; serial=131900858749761727853768227590303808637]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 3. '[issuer=CN=Certificate Services Root CA - iseguest ; serial=68627620160586308685849818775100698224]'
2025-02-24 12:04:39,810 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 4. '[issuer=CN=Certificate Services Node CA - iseguest ; serial=729347676986030971539324822275488749 53]'
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Sélection du certificat de chiffrement
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Sélection du certificat avec la clé keyEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- 1 certificat(s) trouvé(s) avec keyEncipherment keyUsage
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Utilisation de [issuer=CN=Certificate Services Endpoint Sub CA - iseguest ; serial=131900858749761727853768227590303808637] pour le chiffrement des messages
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Sélection du certificat du vérificateur
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]] org.jscep.client.CertStoreInspector -::::- Sélection du certificat avec la clé de signature

numériqueUtilisation
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 1 certificat(s) trouvé(s) avec la clé de signature
numériqueUtilisation
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Utilisation de [issuer=CN=Certificate Services Endpoint Sub CA - iseguest ; serial=131900858749761727853768227590303808637] pour la vérification des messages
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Sélection du certificat de l'émetteur
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Sélection d'un certificat avec basicConstraints
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- 3 certificat(s) trouvé(s) avec basicConstraints
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
org.jscep.client.CertStoreInspector -::::- Utilisation de [issuer=CN=Certificate Services Endpoint Sub CA - iseguest ; serial=131900858749761727853768227590303808637] pour l'émetteur
2025-02-24 12:04:39,812 DEBUG [DefaultQuartzScheduler_Worker-5][[]]
com.cisco.cpm.scep.PKIServerLoadBalancer -::::- Mesures de performances des serveurs SCEP : name[actif/inactif, nombre total de demandes, nombre total de défaillances, nombre de demandes en vol, moyenne RTT]
http://127.0.0.1:9444/caservice/scep[actif,96444,1,0,120]

Téléchargement du profil de terminal

Une fois le processus SCEP terminé et le terminal installé le certificat, l'application télécharge le profil du terminal pour une authentification ultérieure qui serait effectuée par le périphérique :

2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Référent = Windows // Le périphérique Windows a été détecté en fonction de la page Web
24-02-2025 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 000000000000000B30D59CC5
24-02-2025 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- Session = 000000000000000B30D59CC5
2025-02-24 12:06:26,539 DEBUG [https-jsse-nio-8905-exec-1][[]]
cisco.cpm.client.provisioning.EvaluationServlet -::::- provisionner le profil nsp
24-02-2025 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- Session = 000000000000000B30D59CC5
24-02-2025 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- portalSessionId = null
2025-02-24 12:06:26,546 DEBUG [https-jsse-nio-8905-exec-2][[]]
cisco.cpm.client.provisioning.StreamingServlet -::::- StreamingServlet

URI:/auth/provisioning/download/b8ce01e6-b150-4d4e-9698-40e48d5e0197/Cisco-ISE-NSP.xml //Le profil NSP est téléchargé sur le point d'extrémité
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::- Diffusion en continu sur IP: type de fichier : NativeSPProfile, nom de fichier : Cisco-ISE-NSP.xml //Application Network Assistant
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::- BYODStatus:INIT_PROFILE
2025-02-24 12:06:26,547 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -:::- userId a été défini pour tester
2025-02-24 12:06:26,558 DEBUG [https-jsse-nio-8905-exec-2][[]] cisco.cpm.client.provisioning.StreamingServlet -::::- le type de redirection est : SUCCESS_PAGE, l'URL de redirection est : pour mac :

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.