Configurer APIC pour l'administration des périphériques avec ISE et TACACS+

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Diagramme du réseau
- Procédure D'Authentification
- Configuration APIC
- Configuration ISE

Vérifier

Dépannage

Introduction

Ce document décrit la procédure pour intégrer APIC avec ISE pour l'authentification des utilisateurs administrateurs avec le protocole TACACS+.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur des infrastructures des politiques relatives aux applications (APIC)
- Moteur du service de vérification des identités (ISE)
- protocole TACACS

Composants utilisés

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

- APIC version 4.2(7u)
- ISE version 3.2 Patch 1

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

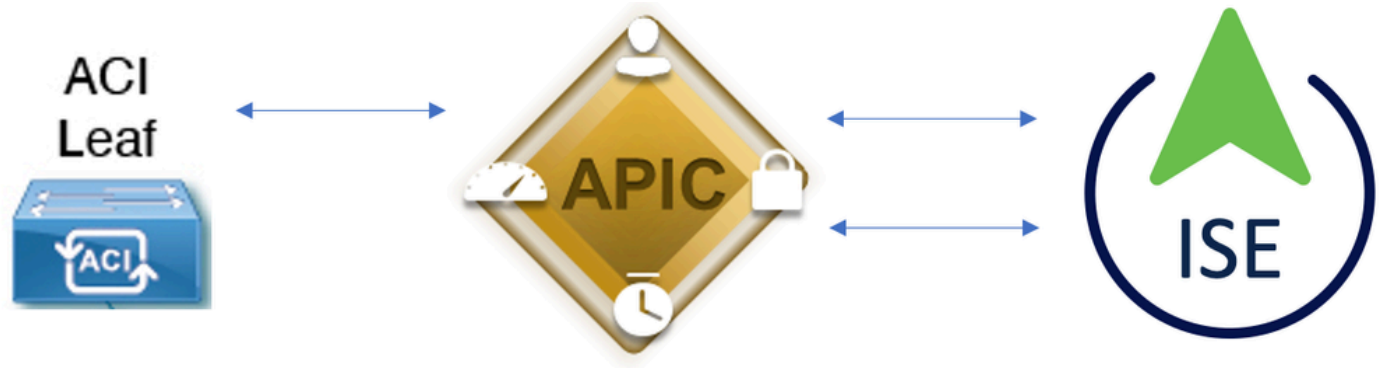


Diagramme D'Intégration

Procédure D'Authentification

Étape 1.Connectez-vous à l'application APIC avec les informations d'identification utilisateur Admin.

Étape 2. Le processus d'authentification déclenche et ISE valide les informations d'identification localement ou via Active Directory.

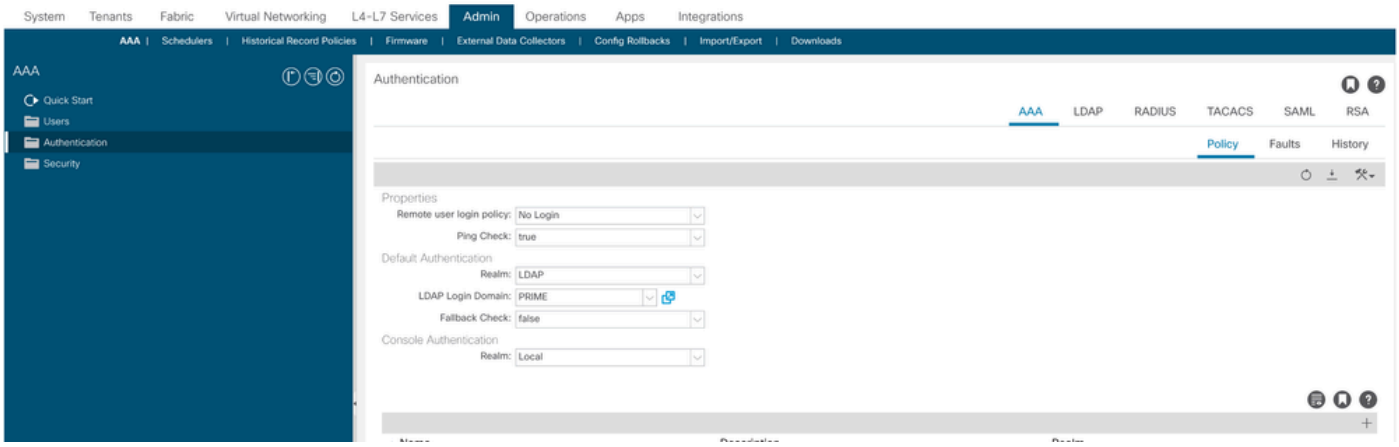
Étape 3. Une fois l'authentification réussie, ISE envoie un paquet d'autorisation pour autoriser l'accès au contrôleur APIC.

Étape 4. ISE affiche un journal en direct d'authentification réussi.

Remarque : Le contrôleur APIC réplique la configuration TACACS+ sur les commutateurs Leaf qui font partie du fabric.

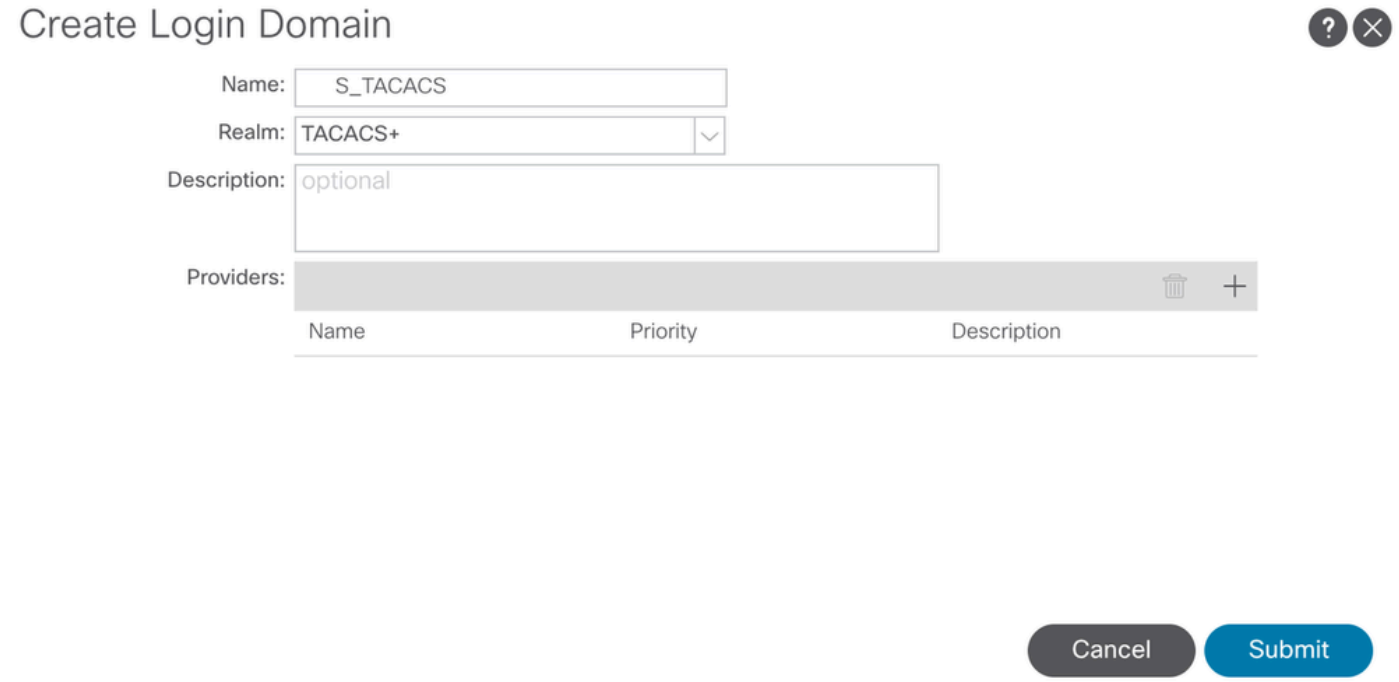
Configuration APIC

Étape 1. Naviguez jusqu'à Admin > AAA > Authentication > AAA et choisissez + l'icône afin de créer un nouveau domaine de connexion.

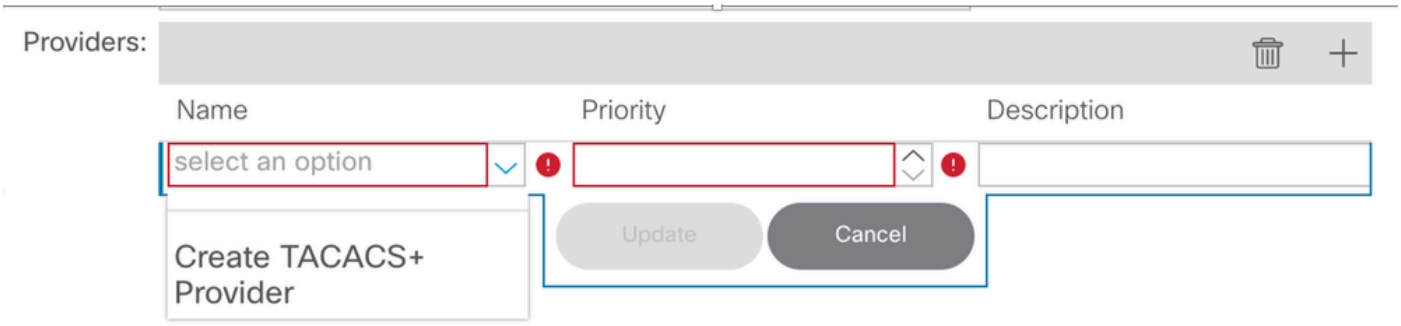


Configuration admin de connexion APIC

Étape 2. Définissez un nom et un domaine pour le nouveau domaine de connexion et cliquez sur+Providers afin de créer un nouveau fournisseur.



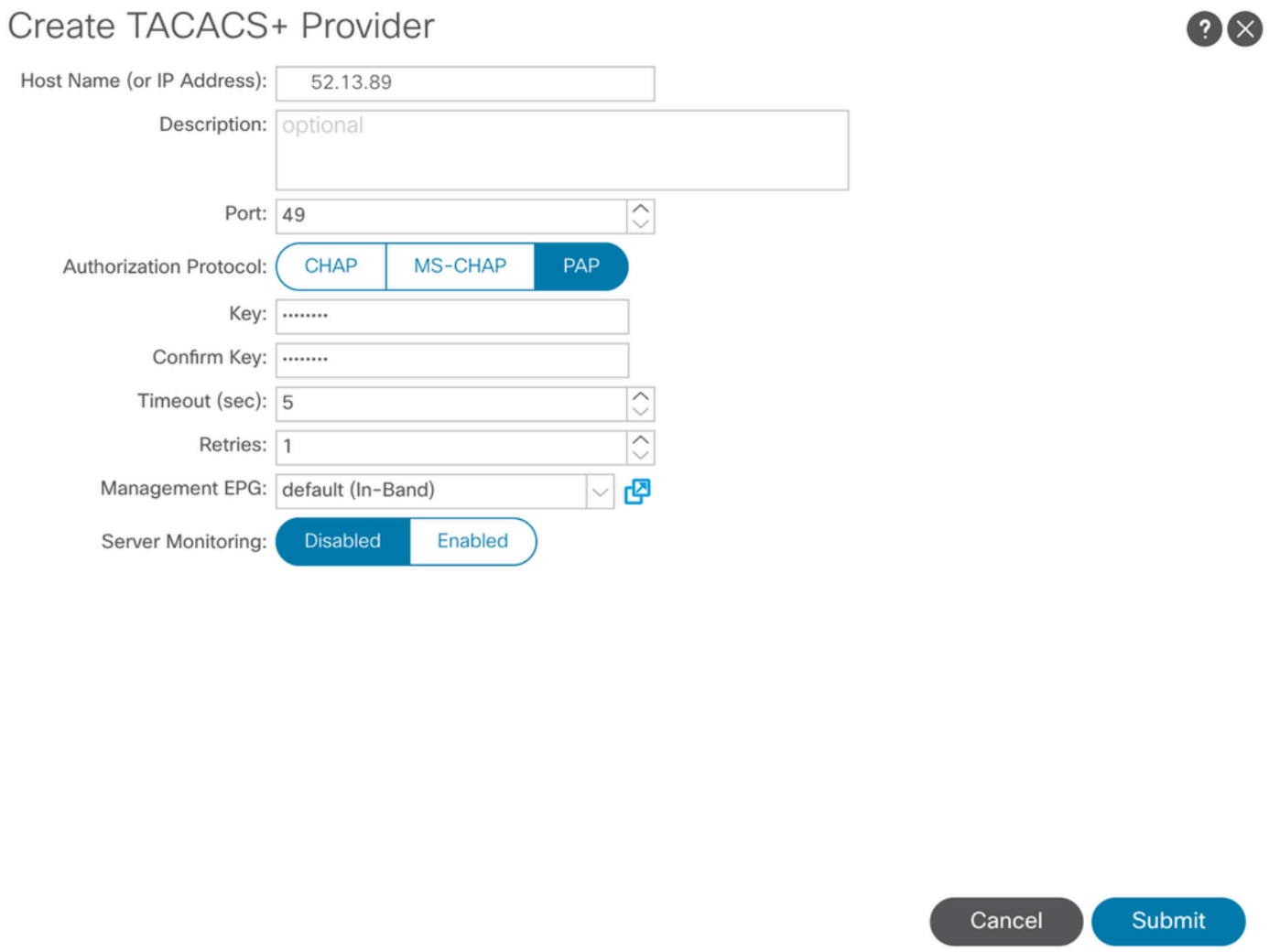
Administrateur de connexion APIC



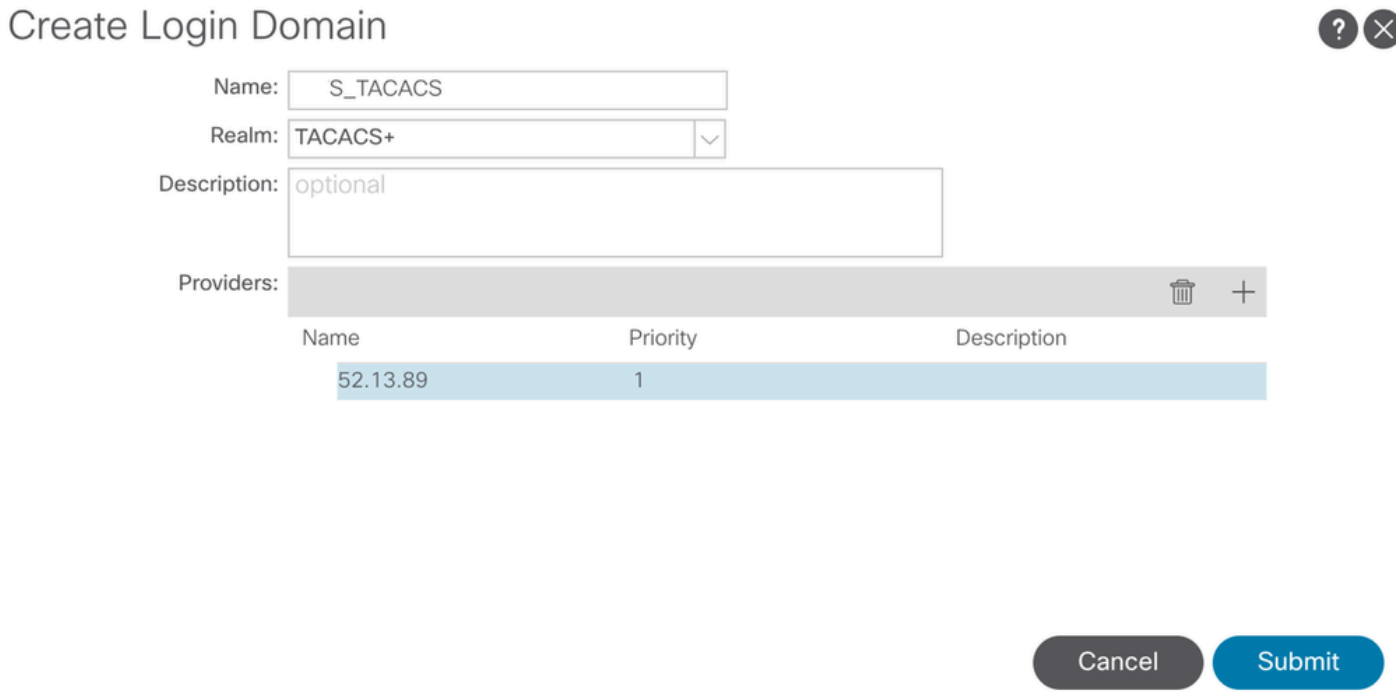
Fournisseur TACACS APIC

Étape 3 : définition de l'adresse IP ISE ou du nom d'hôte, définition d'un secret partagé et

sélection du groupe de stratégie de point de terminaison (EPG) de gestion Cliquez pour Submit ajouter TACACS+ Provider à login admin.



Paramètres du fournisseur TACACS APIC

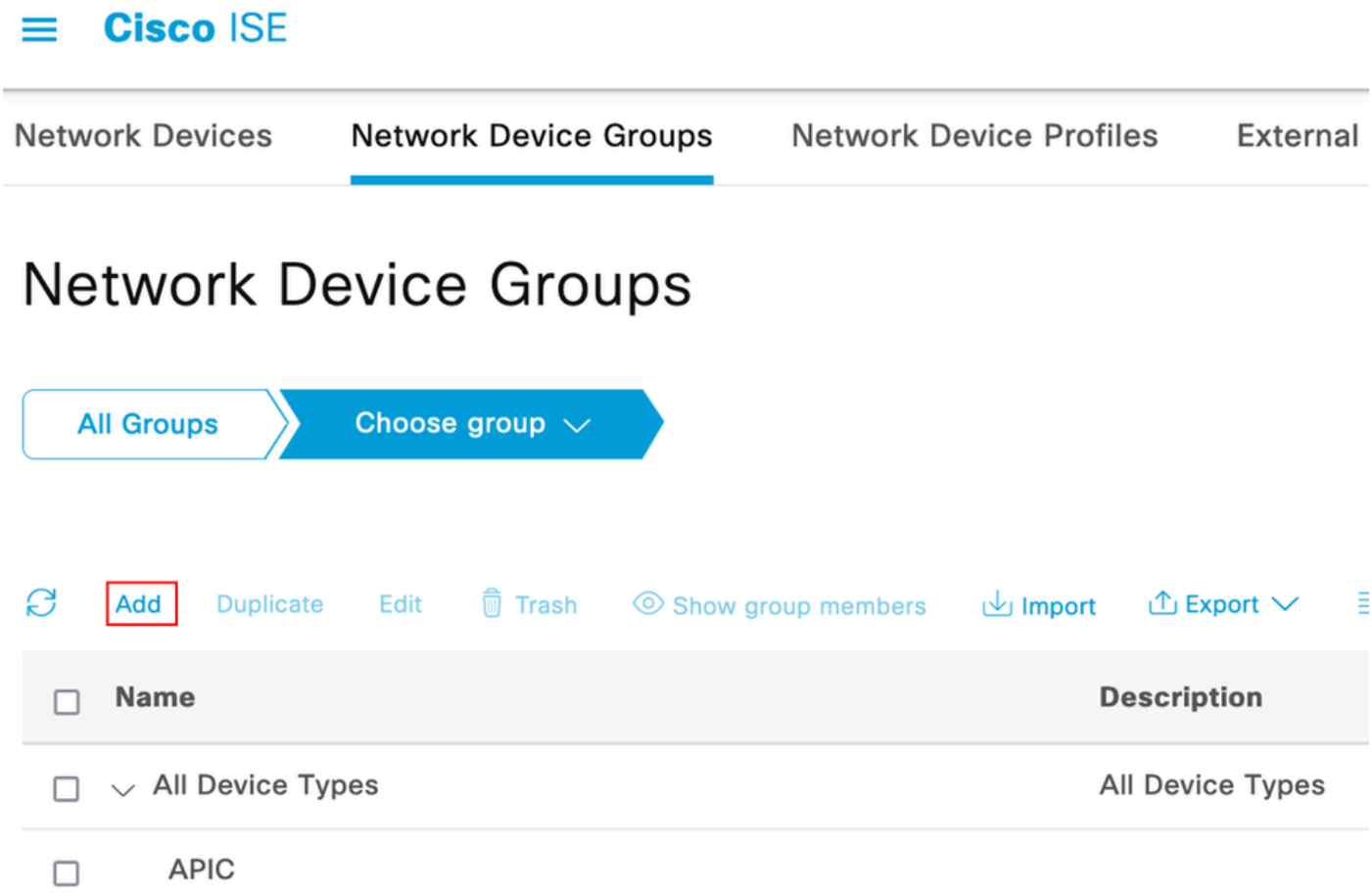




Vue Fournisseur TACACS

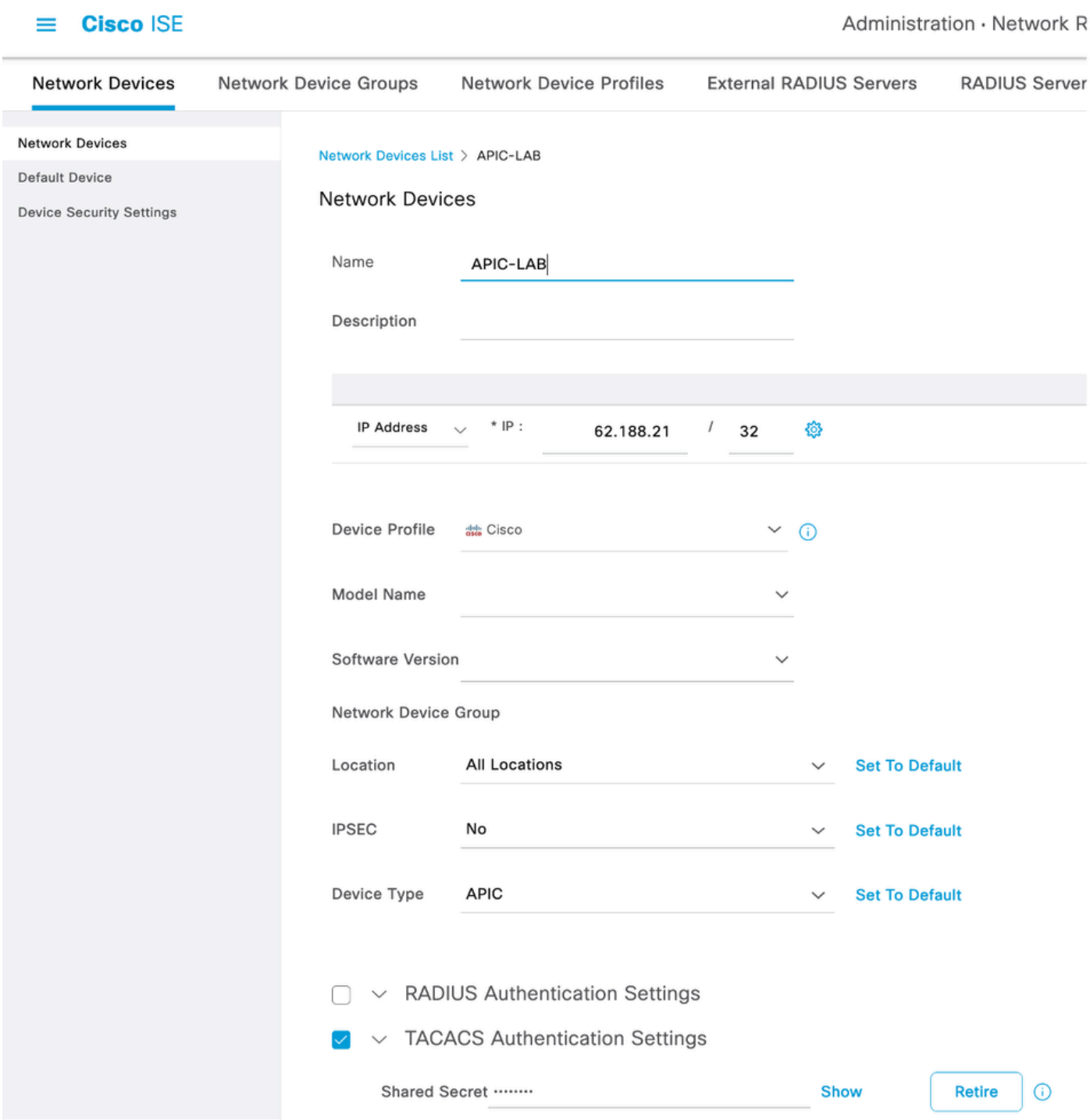
Configuration ISE

Étape 1. Accédez à ☰>Administration > Network Resources > Network Device Groups. Créez un groupe de périphériques réseau sous Tous les types de périphériques.



Groupes de périphériques réseau ISE

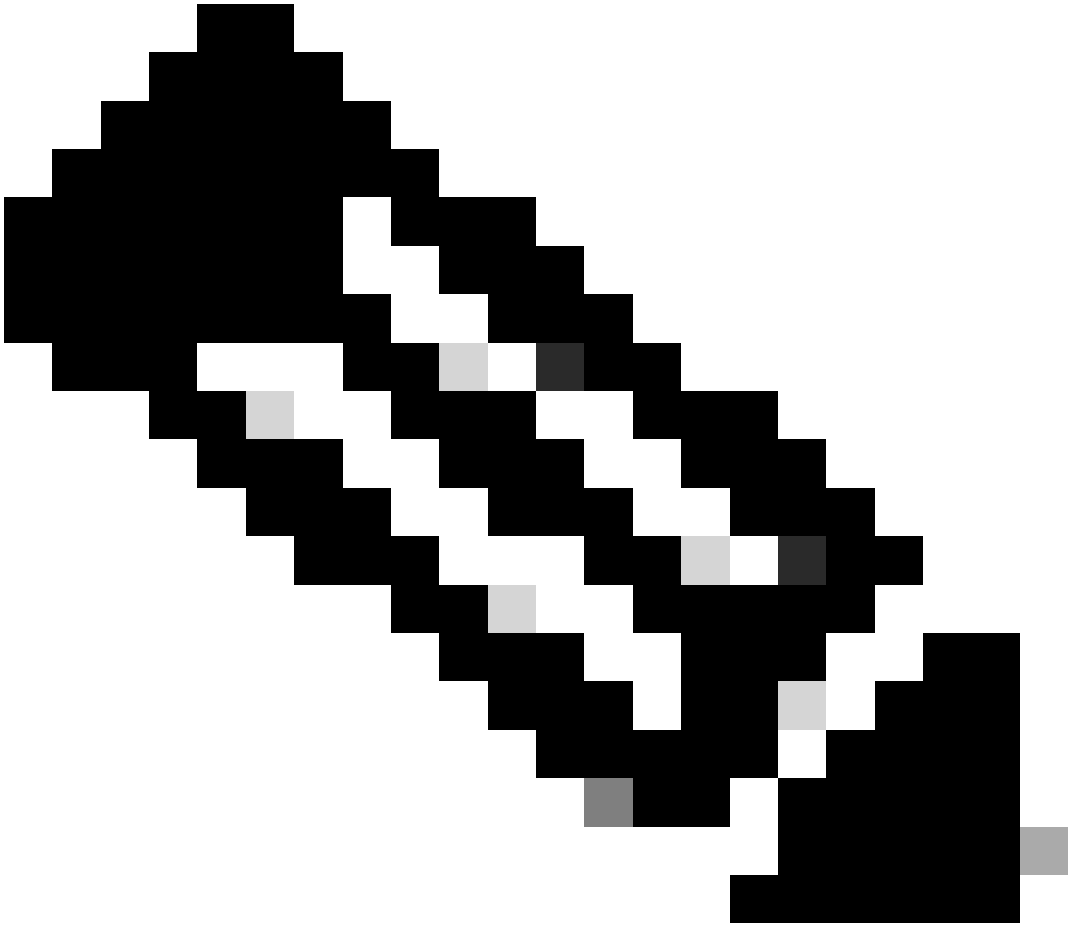
Étape 2. Accédez àAdministration > Network Resources > Network Devices. ChoisissezAdddefine APIC Name and IP address, choisissez APIC sous Device Type et TACACS+ case à cocher, et définissez le mot de passe utilisé sur la configuration du fournisseur APIC TACACS+. Cliquez surSubmit.



Répétez les étapes 1 et 2 pour les commutateurs Leaf.

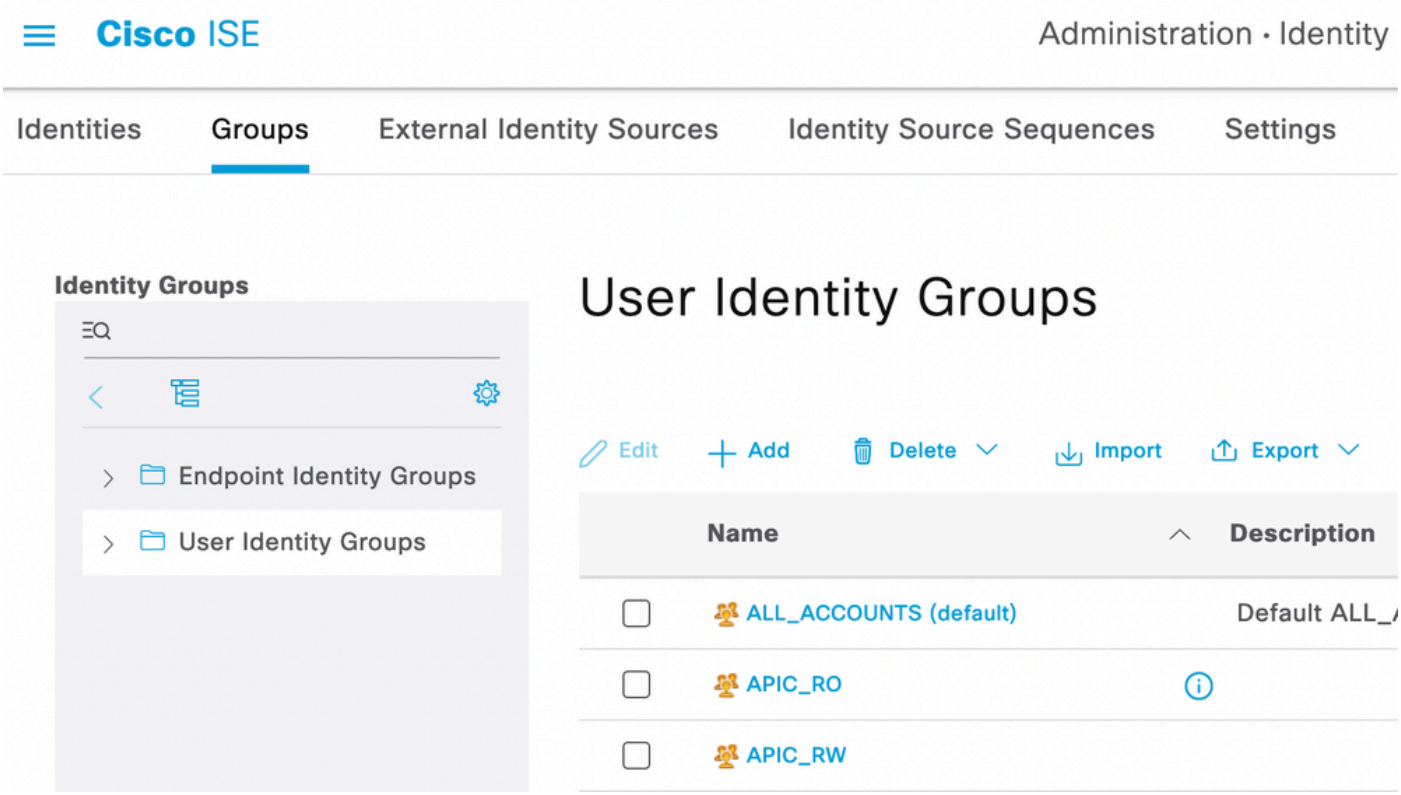
Étape 3. Utilisez les instructions sur ce lien afin d'intégrer ISE avec Active Directory ;

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html.



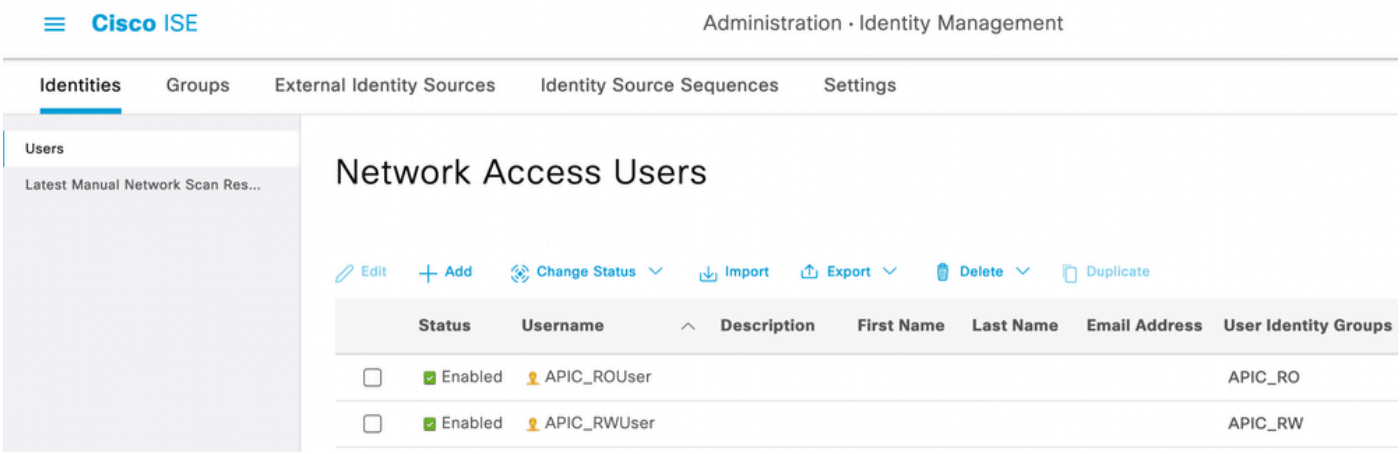
Remarque : Ce document inclut des utilisateurs internes et des groupes d'administrateurs AD en tant que sources d'identité. Toutefois, le test est effectué avec la source d'identité des utilisateurs internes. Le résultat est le même pour les groupes AD.

Étape 4. (Facultatif) Accédez à ☰>Administration > Identity Management > Groups. SélectionnezUser Identity Groups et cliquez sur Add. Créez un groupe pour les utilisateurs Admin en lecture seule et les utilisateurs Admin.

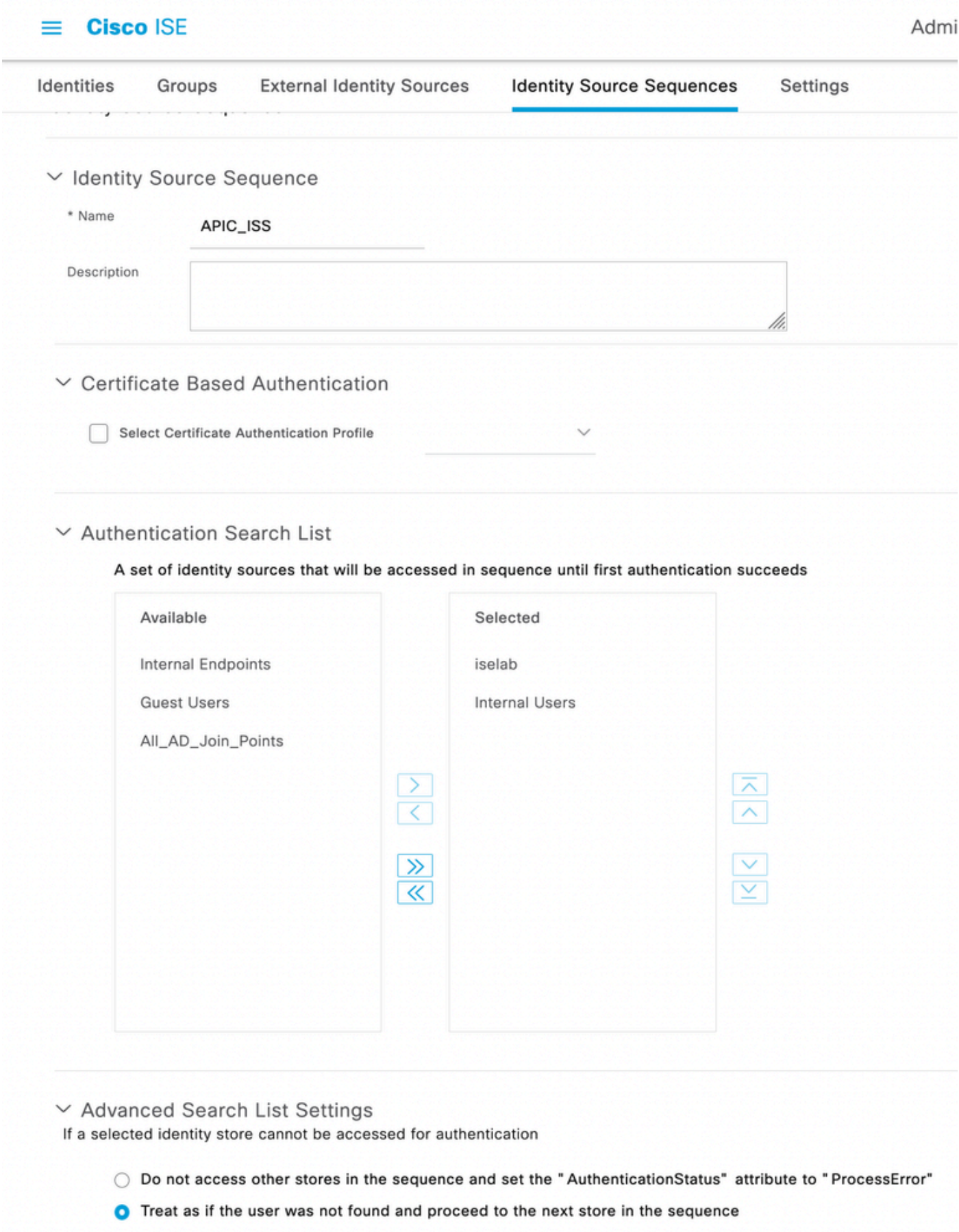


Groupe d'identité

Étape 5. (Facultatif) Accédez à ☰>Administration > Identity Management > Identity.Cliquez surAddet créez unRead Only Adminutilisateur et unAdminutilisateur. Attribuez chaque utilisateur à chaque groupe créé à l'étape 4.



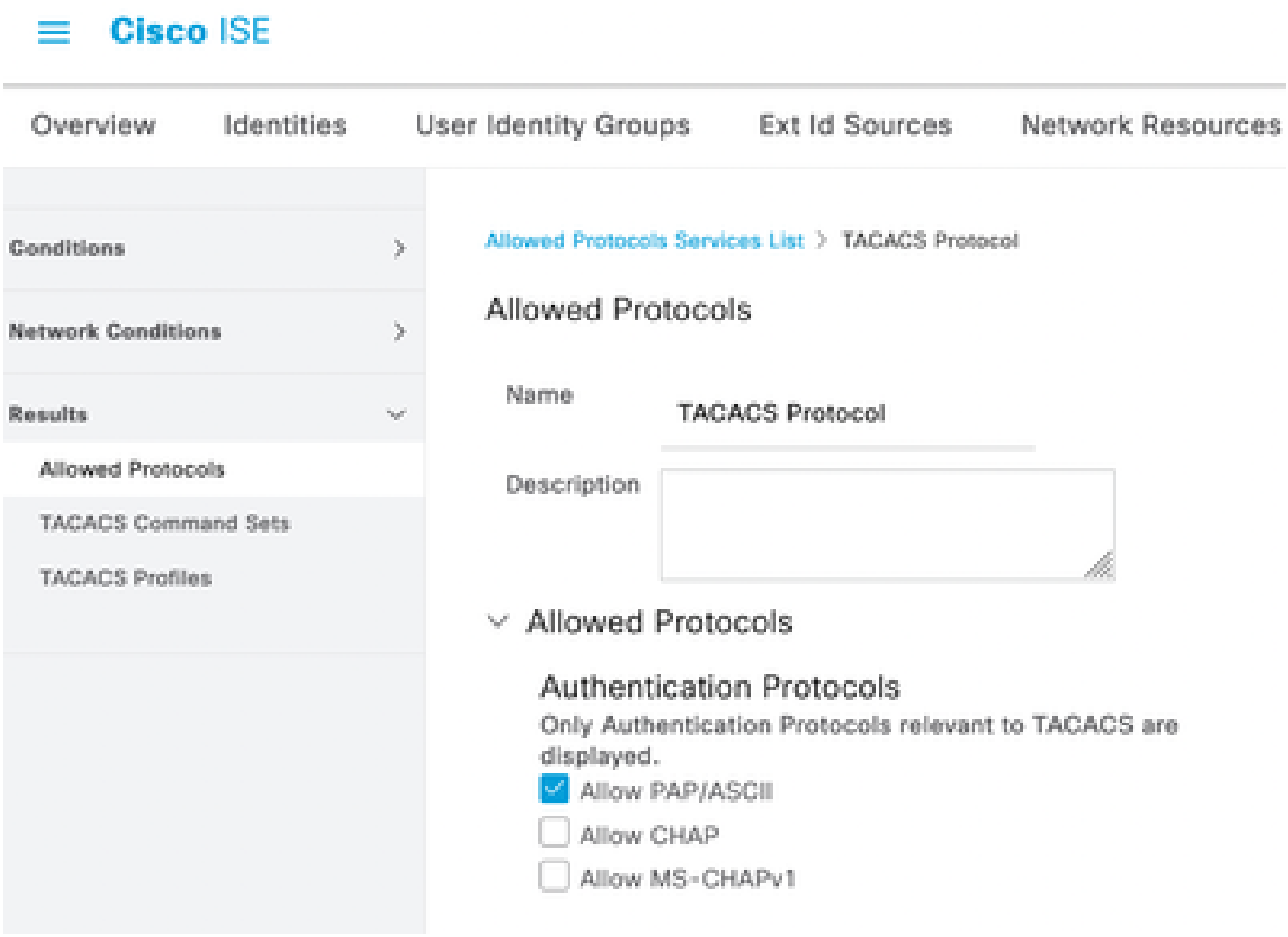
Étape 6. Accédez à ☰>Administration > Identity Management > Identity Source Sequence. ChoisissezAdd, définissez un nom, puis choisissezAD Join PointsetInternal UsersSource d'identité dans la liste. ChoisissezTreat as if the user was not found and proceed to the next store in the sequencesousAdvanced Search List Settingset cliquez surSave.



Séquence source d'identité

7. Accédez à ☰>**Work Centers** > **Device Administration** > **Policy Elements** > **Results** > **Allowed Protocols**. Sélectionnez

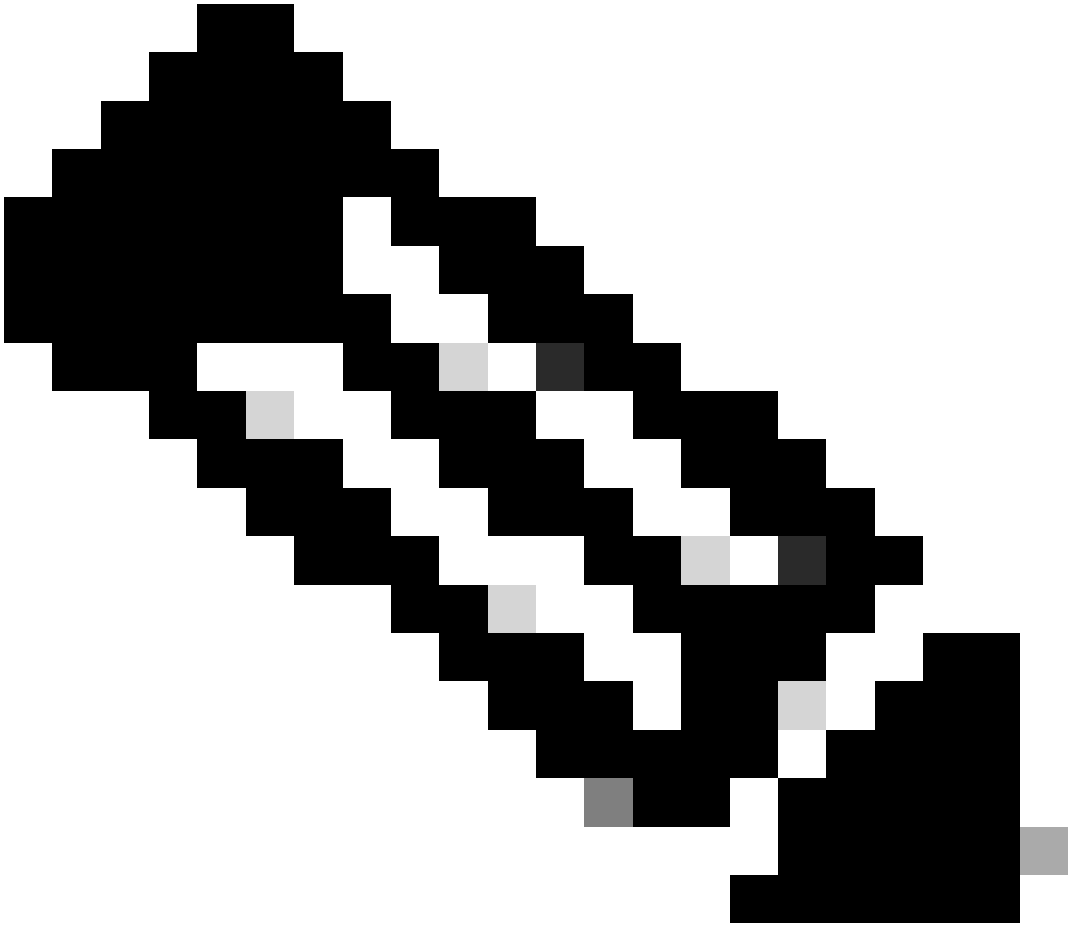
Ajouter, définissez un nom et décochez Autoriser CHAP et Autoriser MS-CHAPv1 dans la liste des protocoles d'authentification. Sélectionnez Enregistrer.



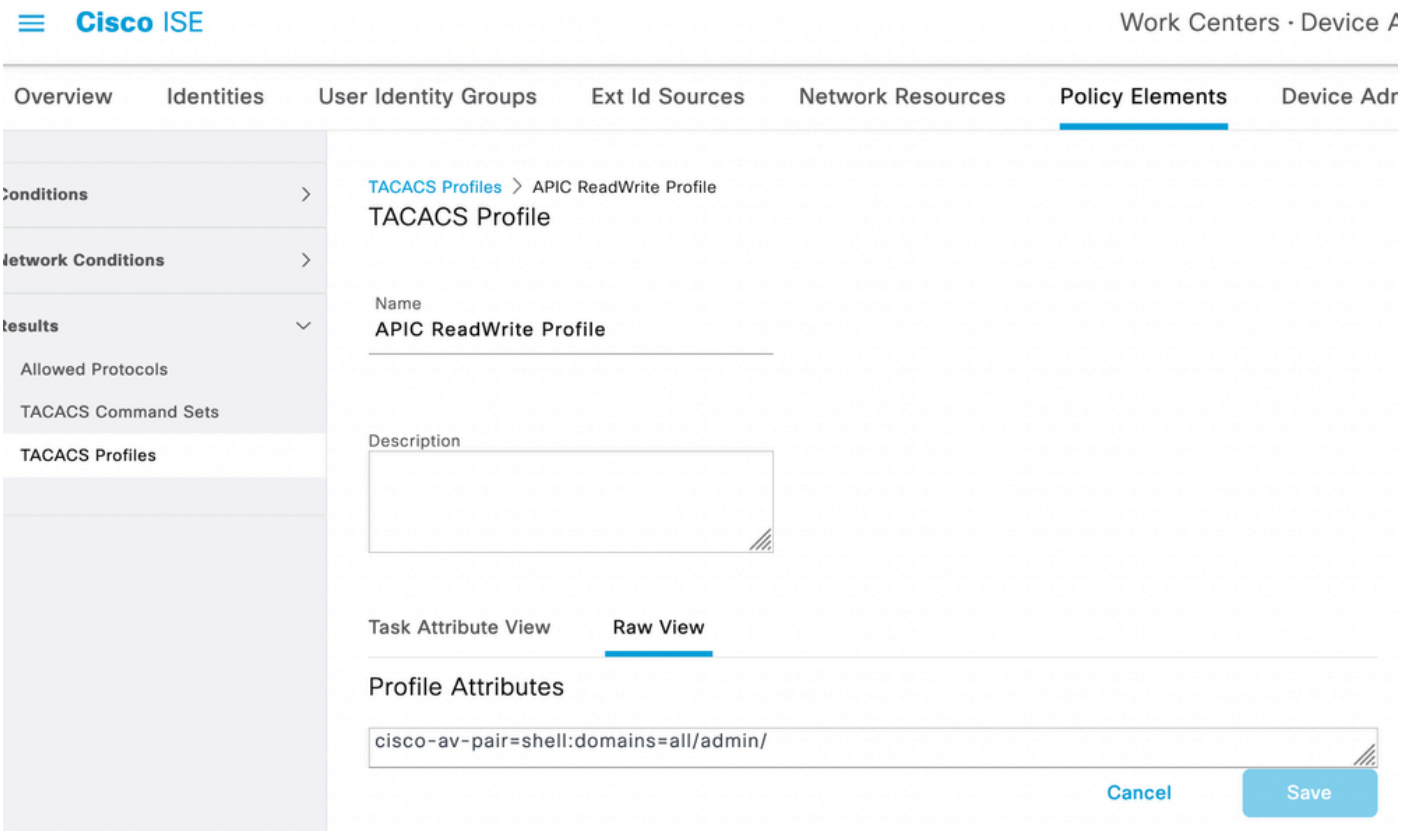
Protocole TACACS Allow

8. Accédez à ☰>Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. Cliquez suraddet créez deux profils en fonction des attributs de la liste située sousRaw View. Cliquez surSave.

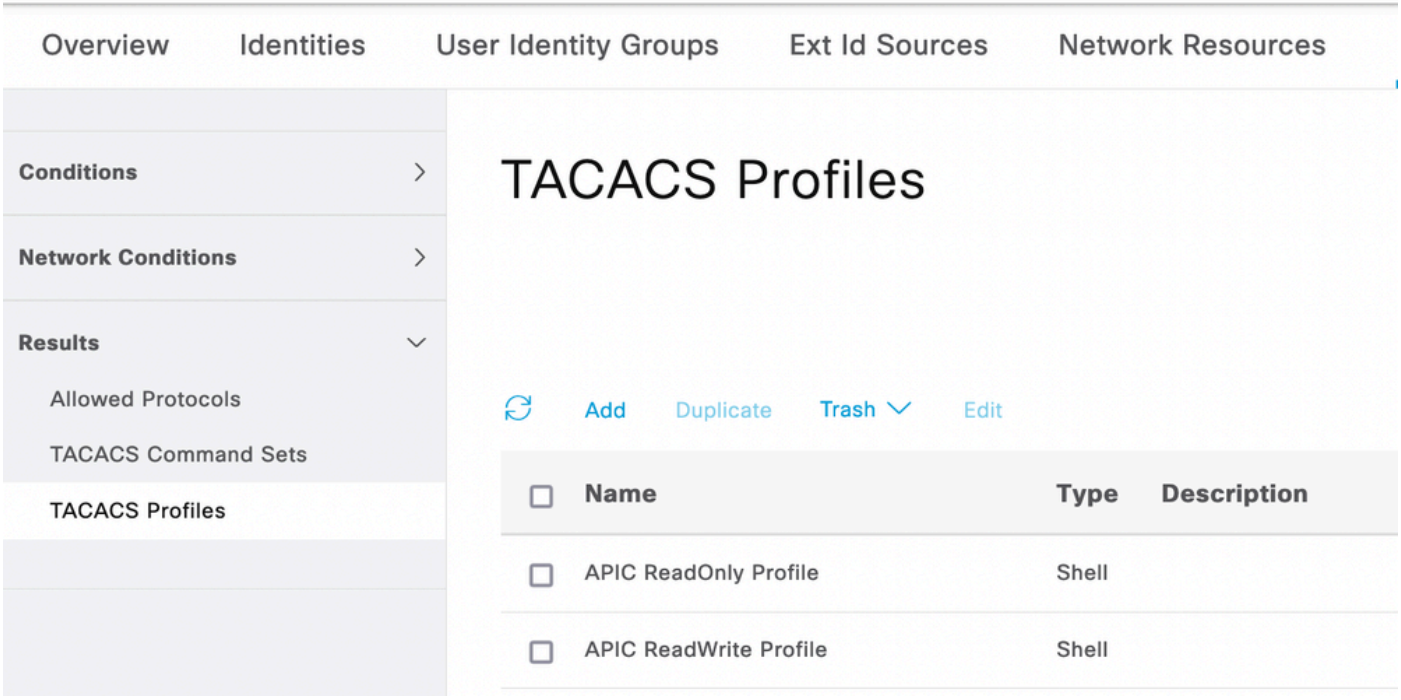
- Utilisateur admin : cisco-av-pair=shell:domains=all/admin/
- Utilisateur admin en lecture seule : cisco-av-pair=shell:domains=all//read-all



Remarque : En cas d'espace ou de caractères supplémentaires, la phase d'autorisation échoue.

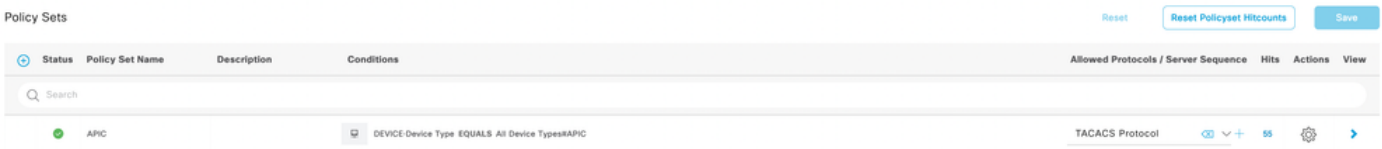


Profil TACACS



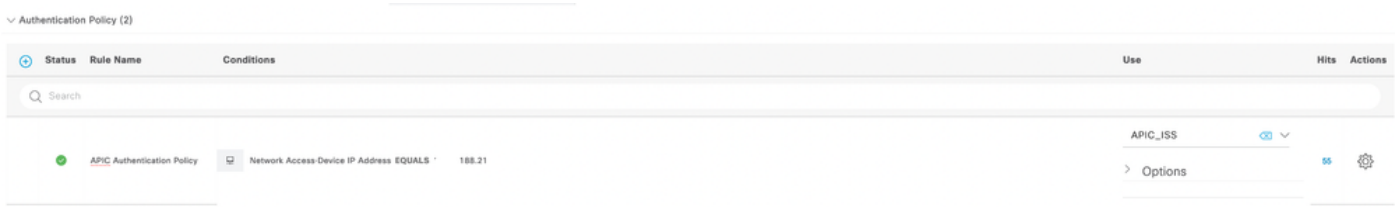
Profils admin TACACS et admin en lecture seule

Étape 9. Accédez à ☰>Work Centers > Device Administration > Device Admin Policy Set. Créez un nouvel ensemble de stratégies, définissez un nom et choisissez le type de périphériqueAPICcréé à l'étape 1. ChoisissezTACACS Protocolcréé à l'étape 7. comme protocole autorisé, puis cliquez surSave.

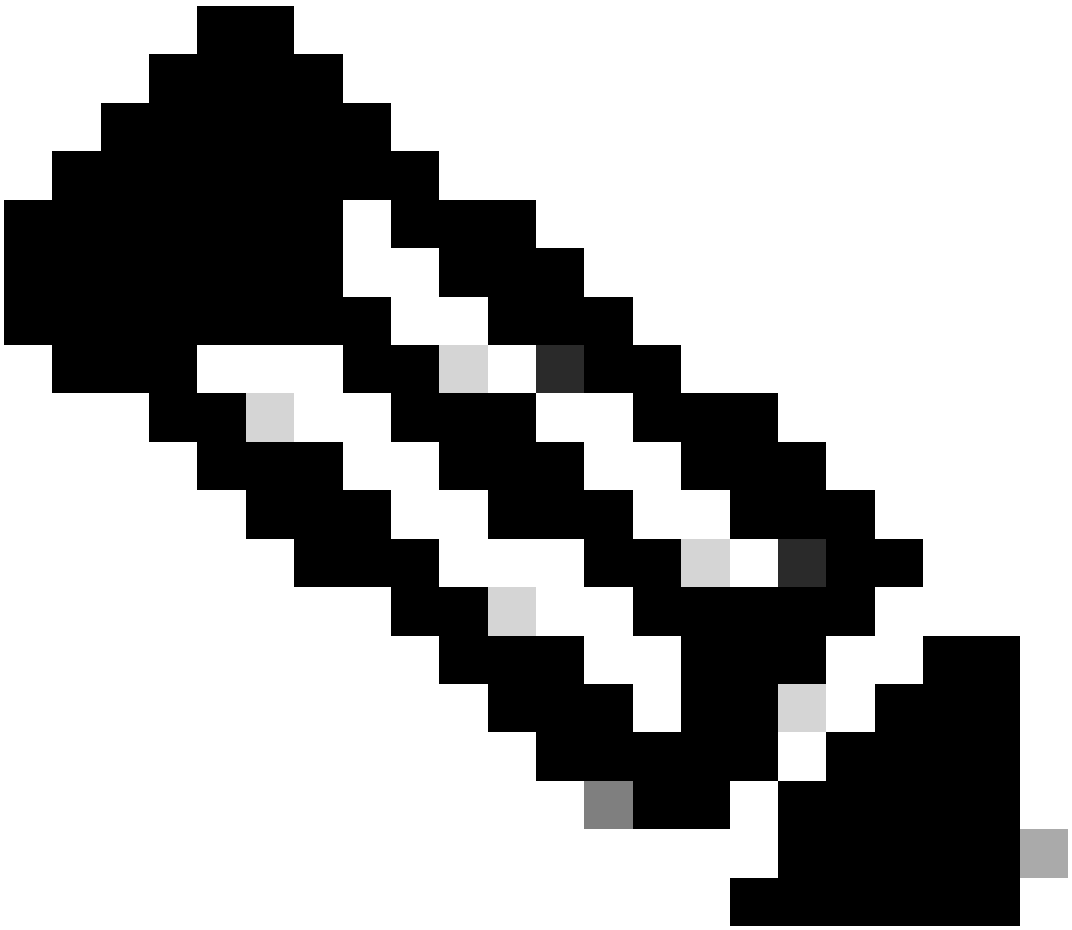


Ensemble de politiques TACACS

Étape 10. Sous newPolicy Set, cliquez sur la flèche droite>et créez une stratégie d'authentification. Définissez un nom et choisissez l'adresse IP du périphérique comme condition. Sélectionnez ensuite la séquence source d'identité créée à l'étape 6.

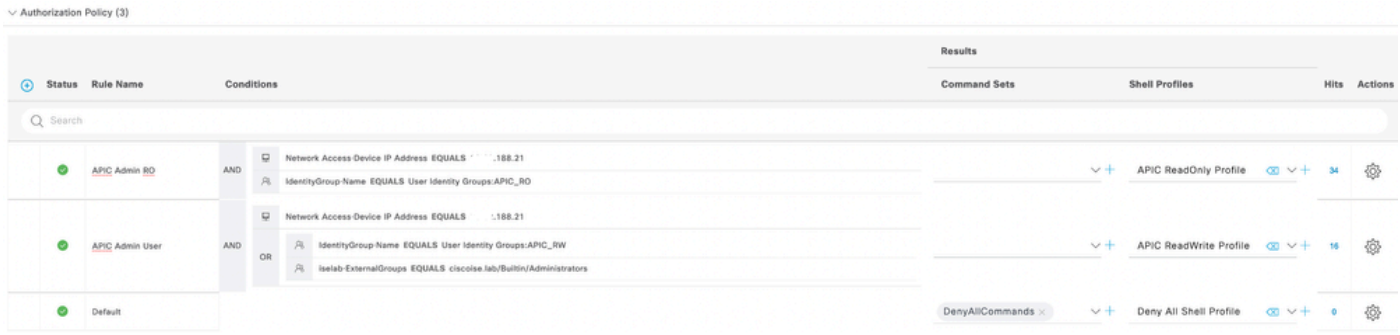


Stratégie d'authentification



Remarque : L'emplacement ou d'autres attributs peuvent être utilisés comme condition d'authentification.

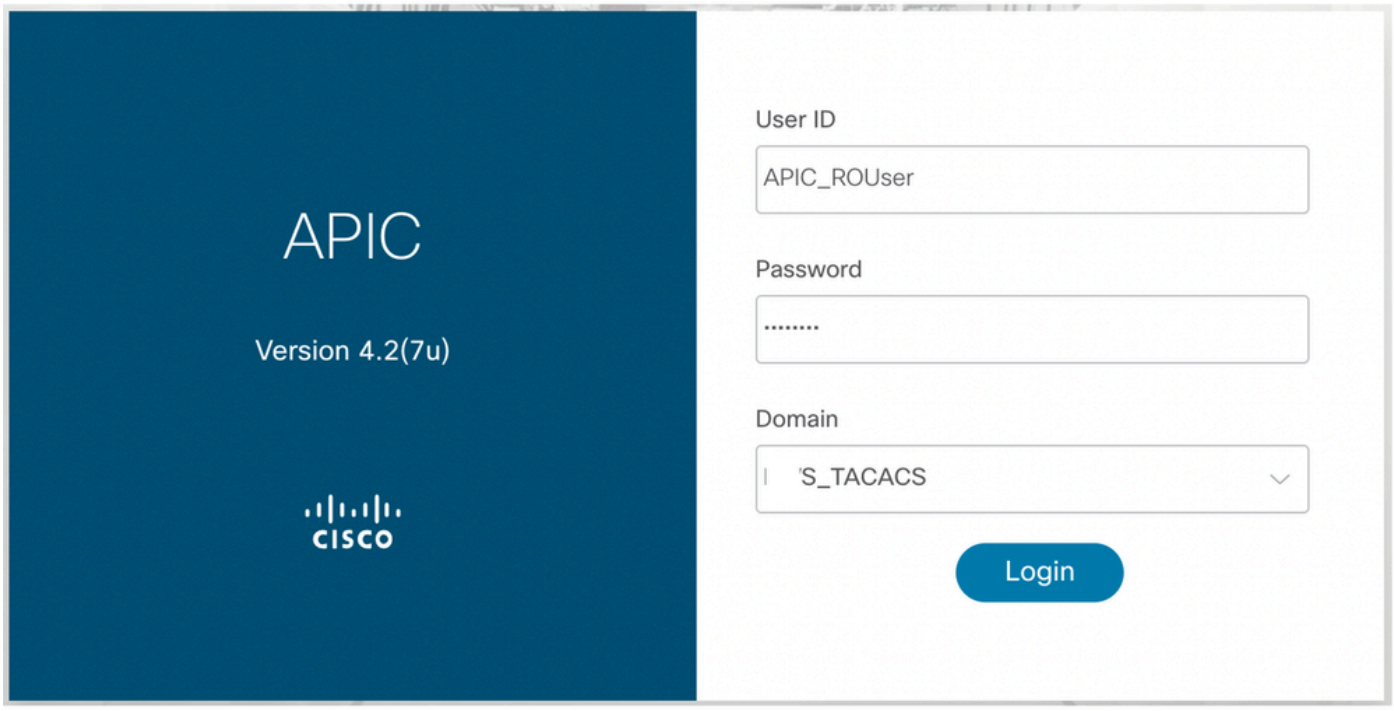
Étape 11. Créez un profil d'autorisation pour chaque type d'utilisateur Admin, définissez un nom et choisissez un utilisateur interne et/ou un groupe d'utilisateurs AD comme condition. D'autres conditions, telles qu'un APIC, peuvent être utilisées. Sélectionnez le profil d'environnement approprié pour chaque stratégie d'autorisation et cliquez surSave.



Profil d'autorisation TACACS

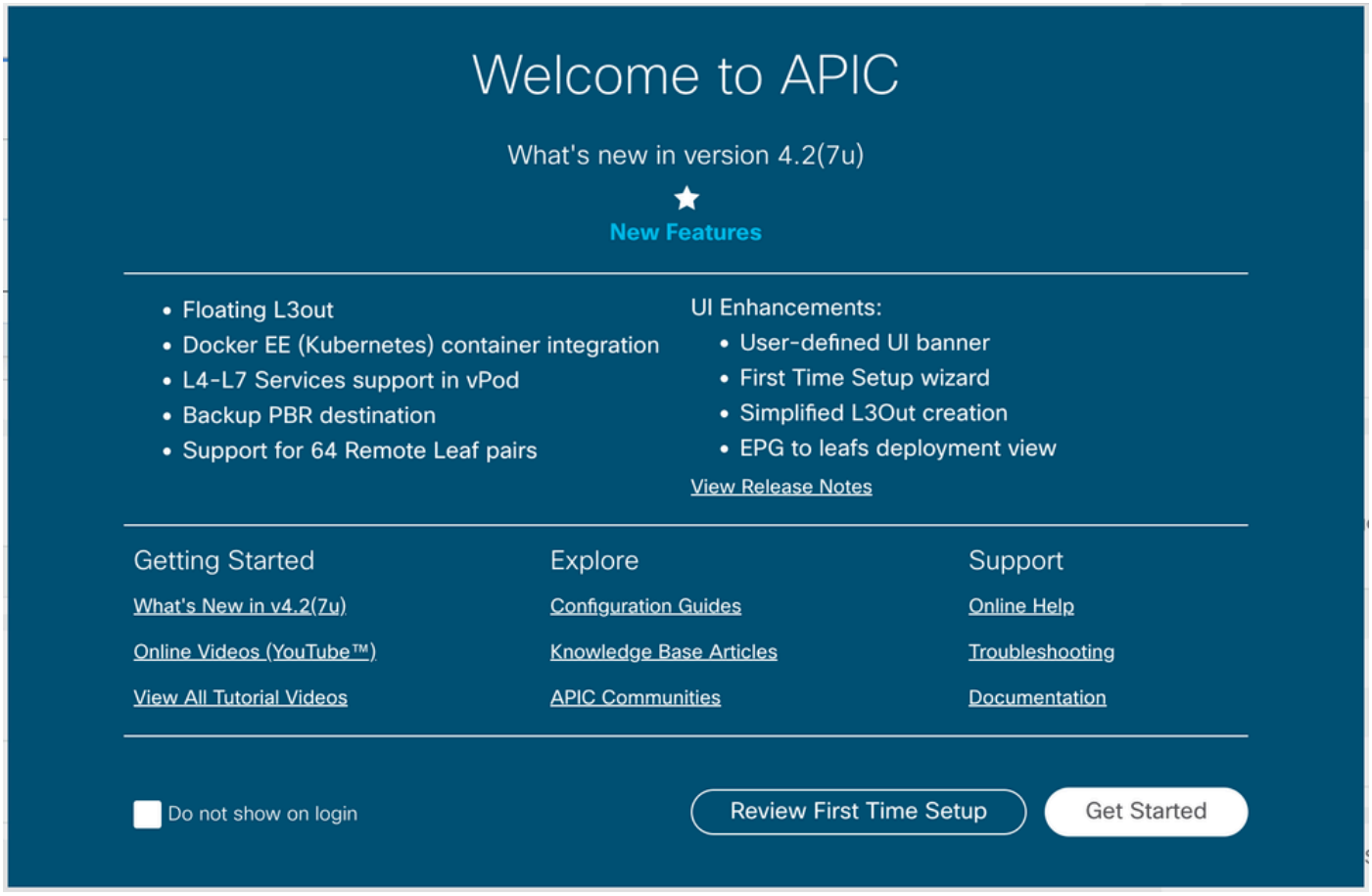
Vérifier

Étape 1. Connectez-vous à l'interface utilisateur APIC avec les informations d'identification administrateur utilisateur. Sélectionnez l'option TACACS dans la liste.



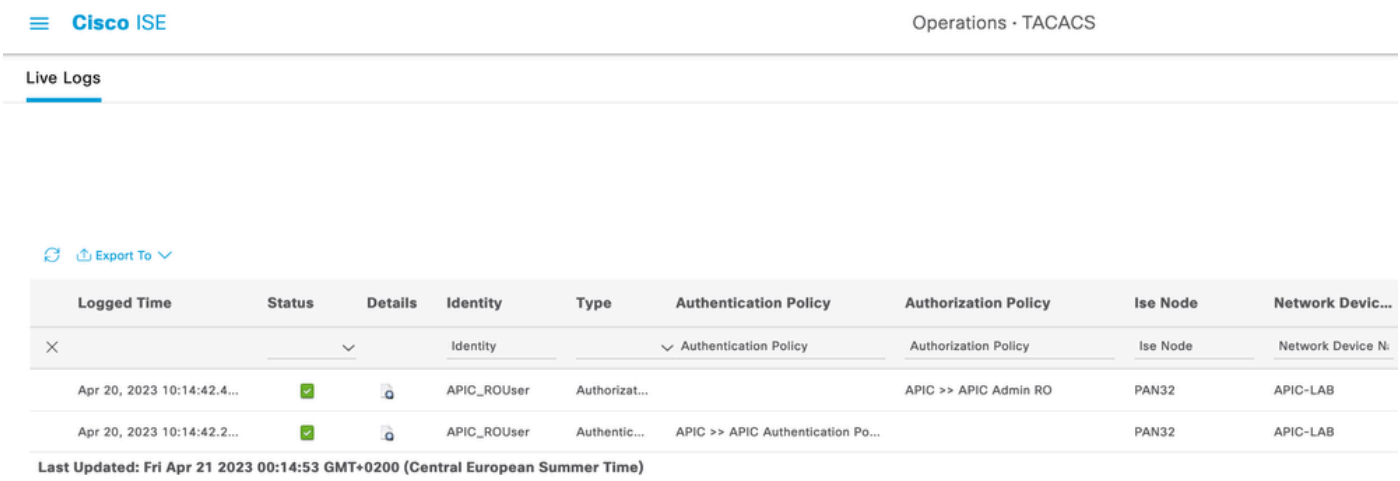
Connexion APIC

Étape 2 : vérification de l'accès à l'interface utilisateur APIC et application des stratégies appropriées aux journaux TACACS Live



Message de bienvenue APIC

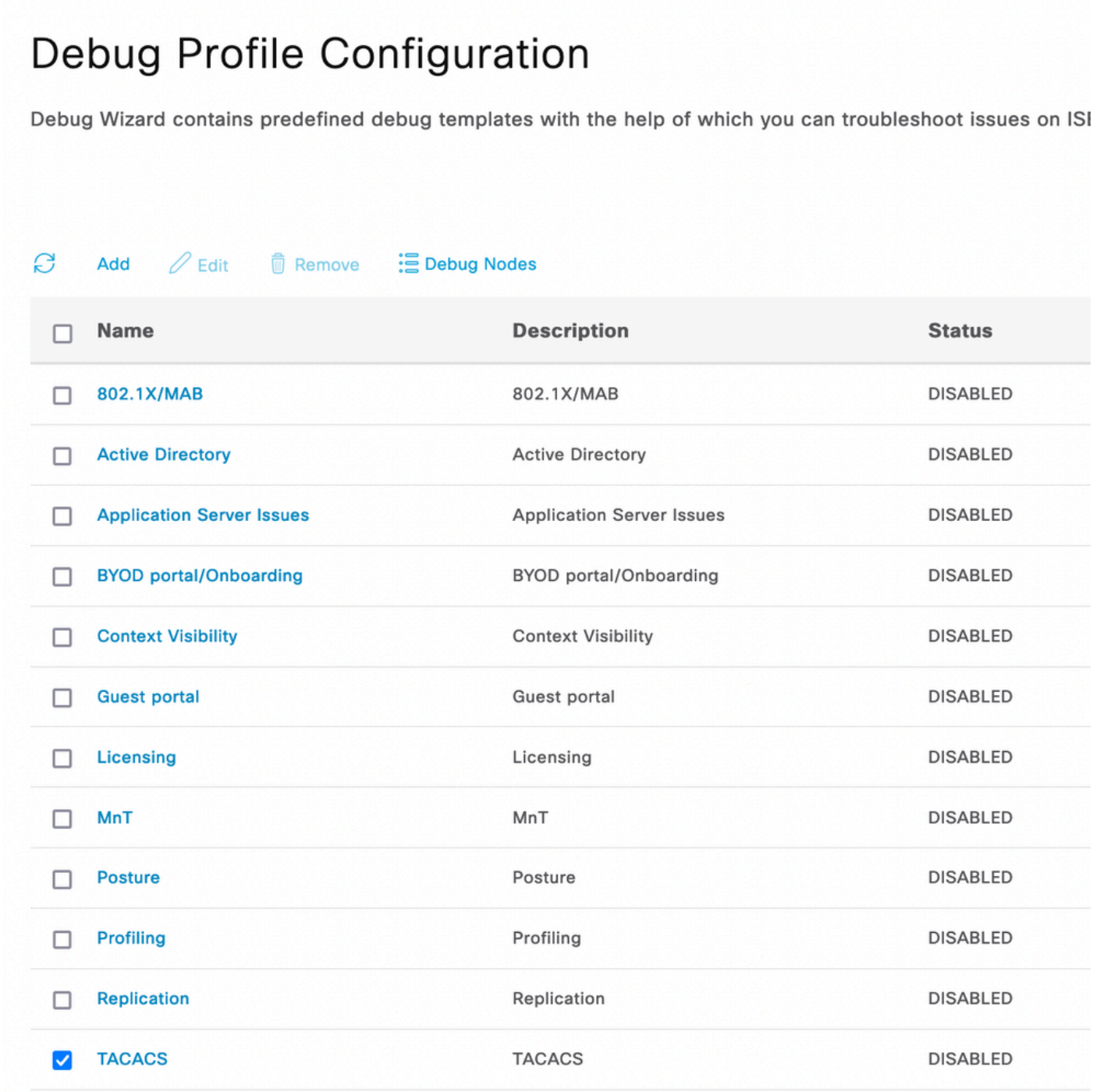
Répétez les étapes 1 et 2 pour les utilisateurs Admin en lecture seule.



Journaux TACACS+ en direct

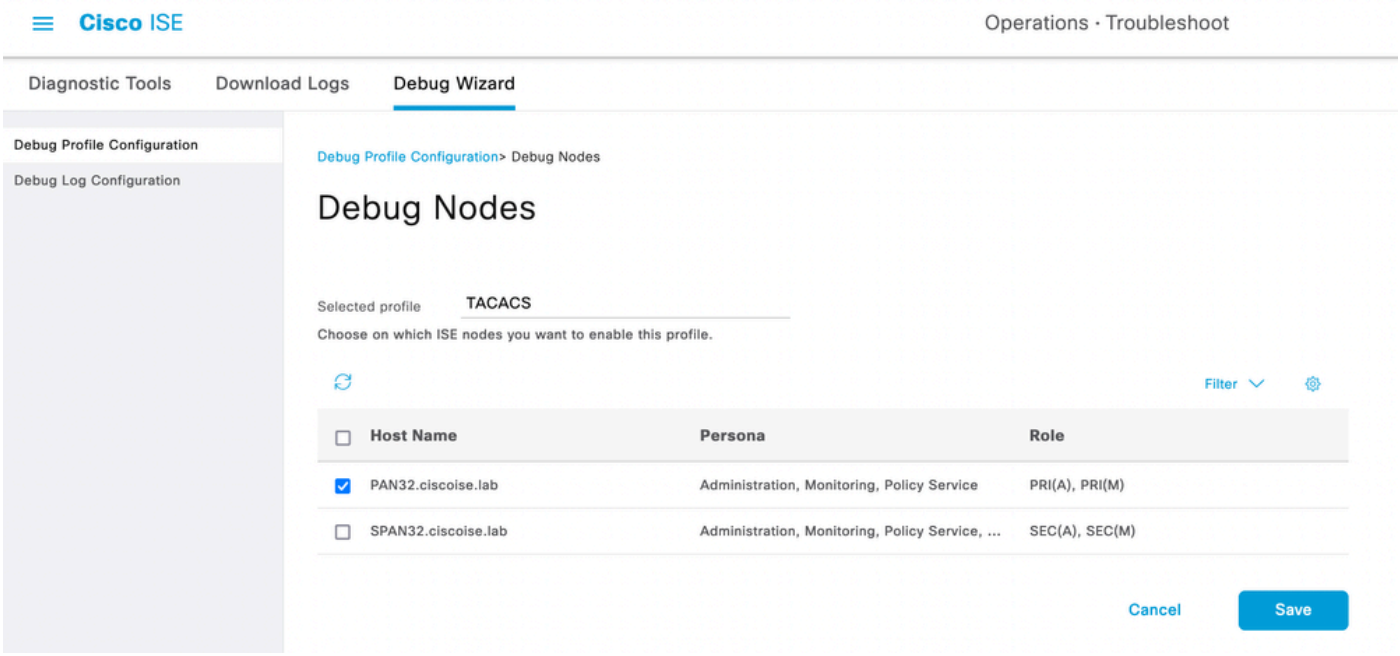
Dépannage

Étape 1. Accédez à ☰>Operations > Troubleshoot > Debug Wizard. SélectionnezTACACSet cliquez sur Debug Nodes.



Configuration du profil de débogage

Étape 2. Choisissez le noeud qui reçoit le trafic et cliquez surSave.



Sélection des noeuds de débogage

Étape 3. Effectuez un nouveau test et téléchargez les journaux sousOperations > Troubleshoot > Download logs comme indiqué :

```
AcsLogs,2023-04-20 22:17:16,866,DEBUG,0x7f93cabc7700,cntx=0004699242,sesn=PAN32/469596415/70,CPMSession
```

Si les débogages n'affichent pas les informations d'authentification et d'autorisation, validez ceci :

1. Le service d'administration des périphériques est activé sur le noeud ISE.
2. L'adresse IP ISE correcte a été ajoutée à la configuration APIC.
3. Si un pare-feu se trouve au milieu, vérifiez que le port 49 (TACACS) est autorisé.

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.