Configurer l'authentification externe SWA avec ISE en tant que serveur RADIUS

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Topologie du réseau

Configurer

- Configuration ISE
- Configuration SWA

Vérifier

Autres informations utiles

Introduction

Ce document décrit les étapes pour configurer l'authentification externe sur Secure Web Access (SWA) avec Cisco ISE® comme serveur RADIUS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de RADIUS
- Connaissances de base de Cisco SWA
- Connaissance des stratégies de configuration d'authentification et d'autorisation sur Cisco Identity Services Engine® (ISE)

Cisco vous recommande également de disposer des éléments suivants :

- Versions SWA et ISE compatibles
- Accès à l'administration SWA et ISE

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles suivantes :

- ISE 3.0.0
- SWA 14.0.2-012

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

Lorsque vous activez l'authentification externe pour les utilisateurs administratifs de votre SWA, le périphérique vérifie les informations d'identification de l'utilisateur avec un serveur LDAP (Lightweight Directory Access Protocol) ou RADIUS comme spécifié dans la configuration de l'authentification externe.

Topologie du réseau



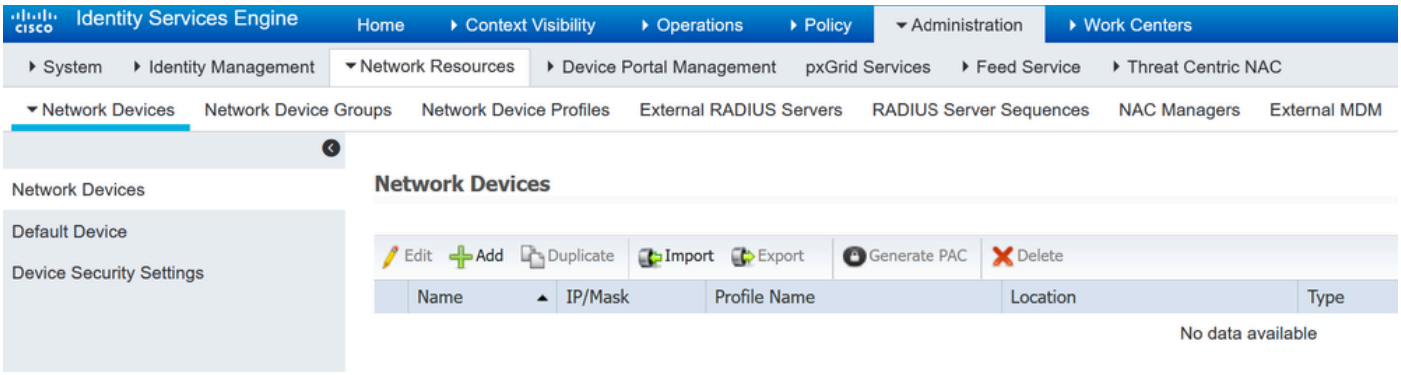
Schéma de topologie du réseau

Les utilisateurs administratifs accèdent à SWA sur le port 443 avec leurs informations d'identification et SWA vérifie ces informations d'identification avec le serveur RADIUS.

Configurer

Configuration ISE

1. Ajoutez un nouveau périphérique réseau et accédez à Administration > Network Resources > Network Devices > +Add.

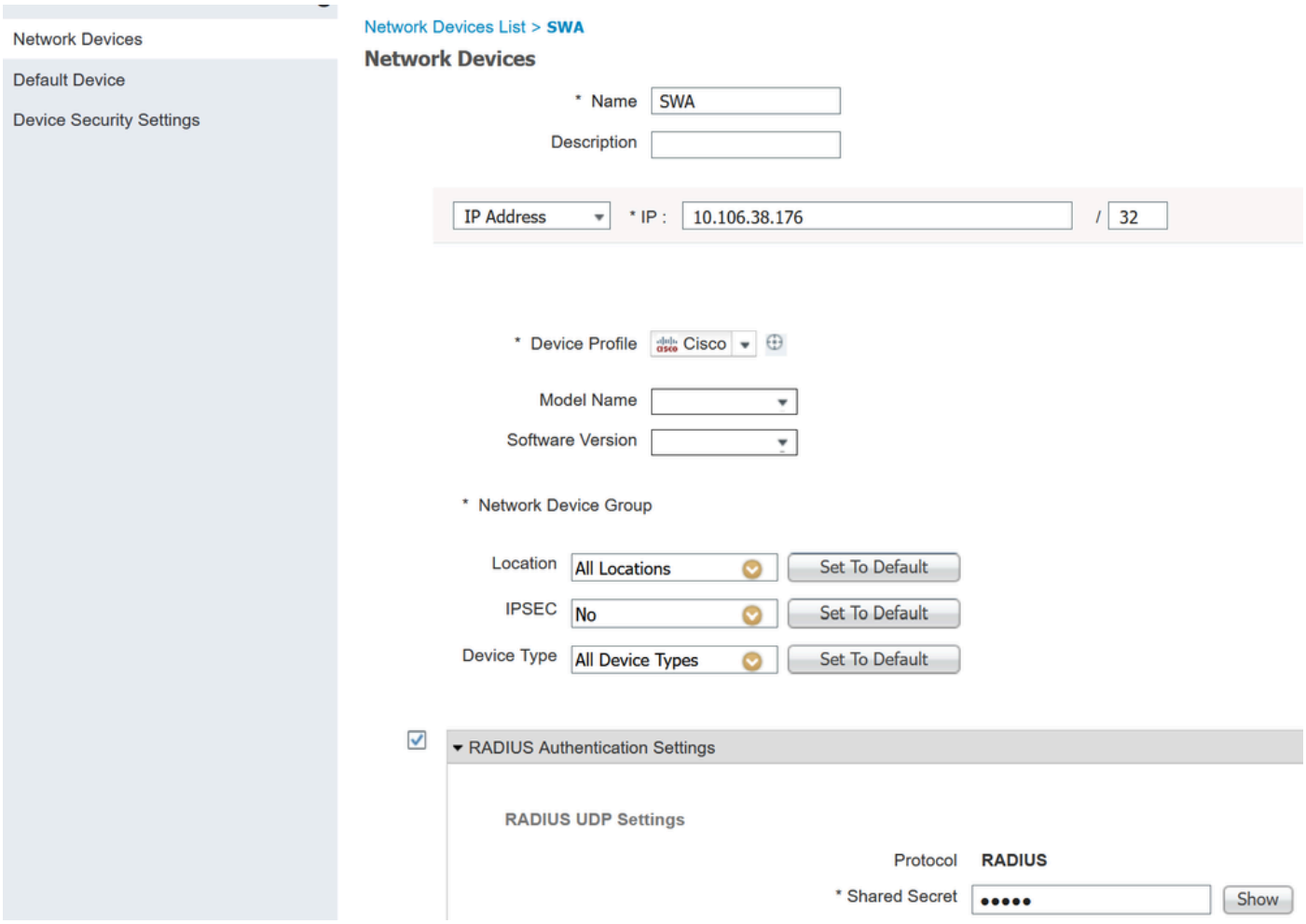


Ajouter SWA en tant que périphérique réseau dans ISE

2. Attribuez un nom à l'objet périphérique réseau et insérez l'adresse IP SWA.

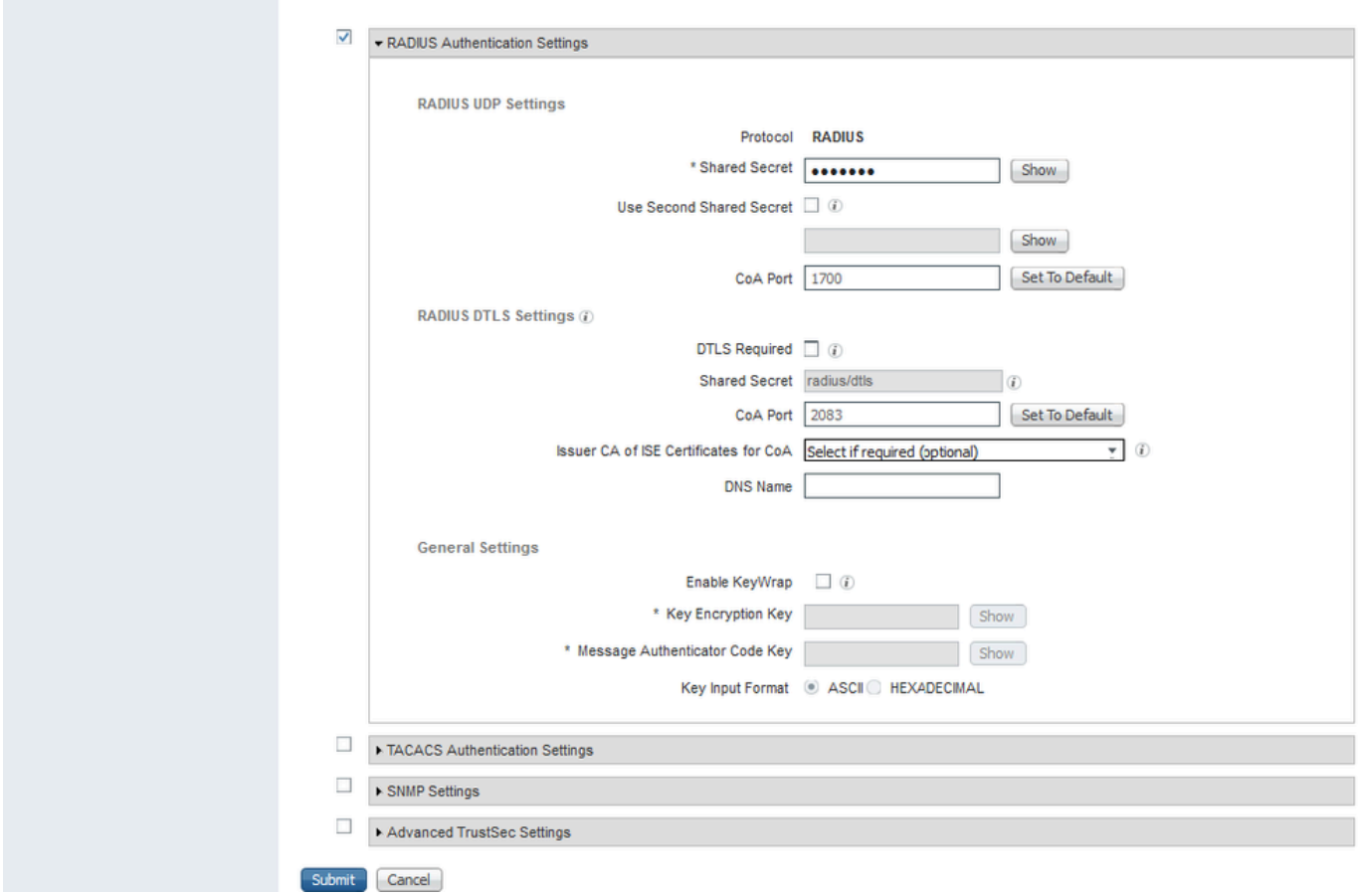
2.1. Cochez la case RADIUS et définissez un secret partagé.

Remarque : La même clé doit être utilisée ultérieurement pour configurer le serveur RADIUS dans SWA.



Configurer la clé partagée du périphérique réseau SWA

2.2. Cliquez sur Envoyer.

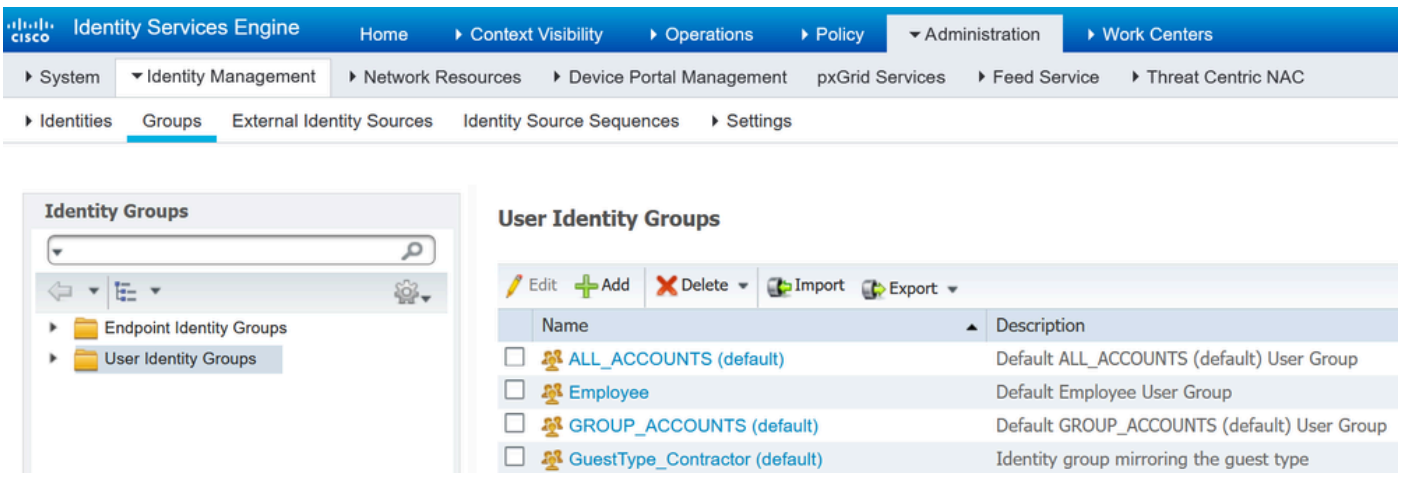


Envoyer la configuration des périphériques réseau

---

3. Créez les groupes d'identités utilisateur requis et accédez à Administration > Gestion des identités > Groupes > Groupes d'identités utilisateur > +Ajouter.

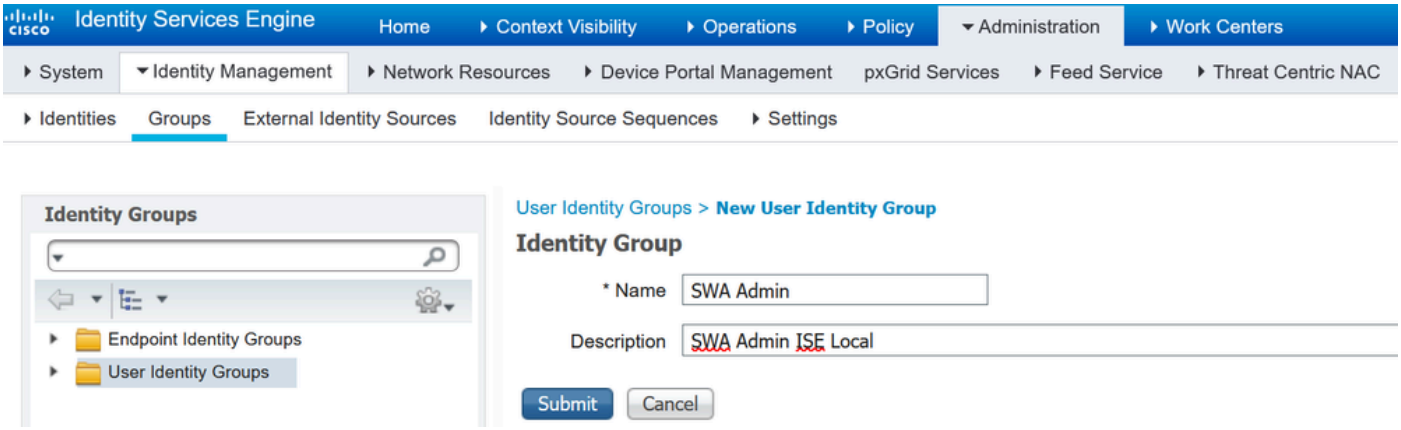
Remarque : Vous devez configurer différents groupes d'utilisateurs pour qu'ils correspondent aux différents types d'utilisateurs.



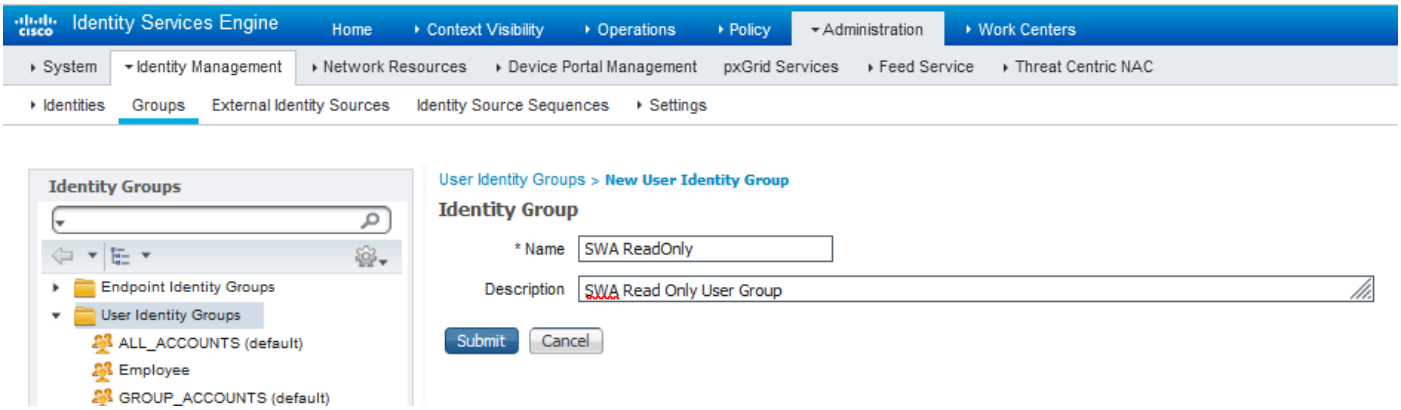
Ajouter un groupe d'identités utilisateur

---

4. Entrez le nom du groupe, sa description (facultatif) et Soumettre. Répétez ces étapes pour chaque groupe. Dans cet exemple, créez un groupe pour les utilisateurs administrateurs et un autre pour les utilisateurs en lecture seule.



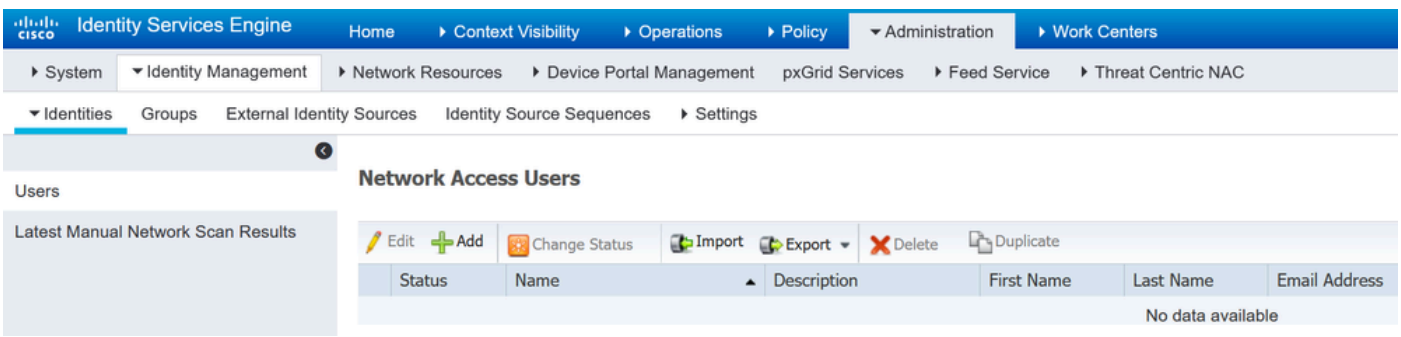
Ajouter un groupe d'identités utilisateur



Ajouter un groupe d'identités utilisateur pour les utilisateurs en lecture seule SWA

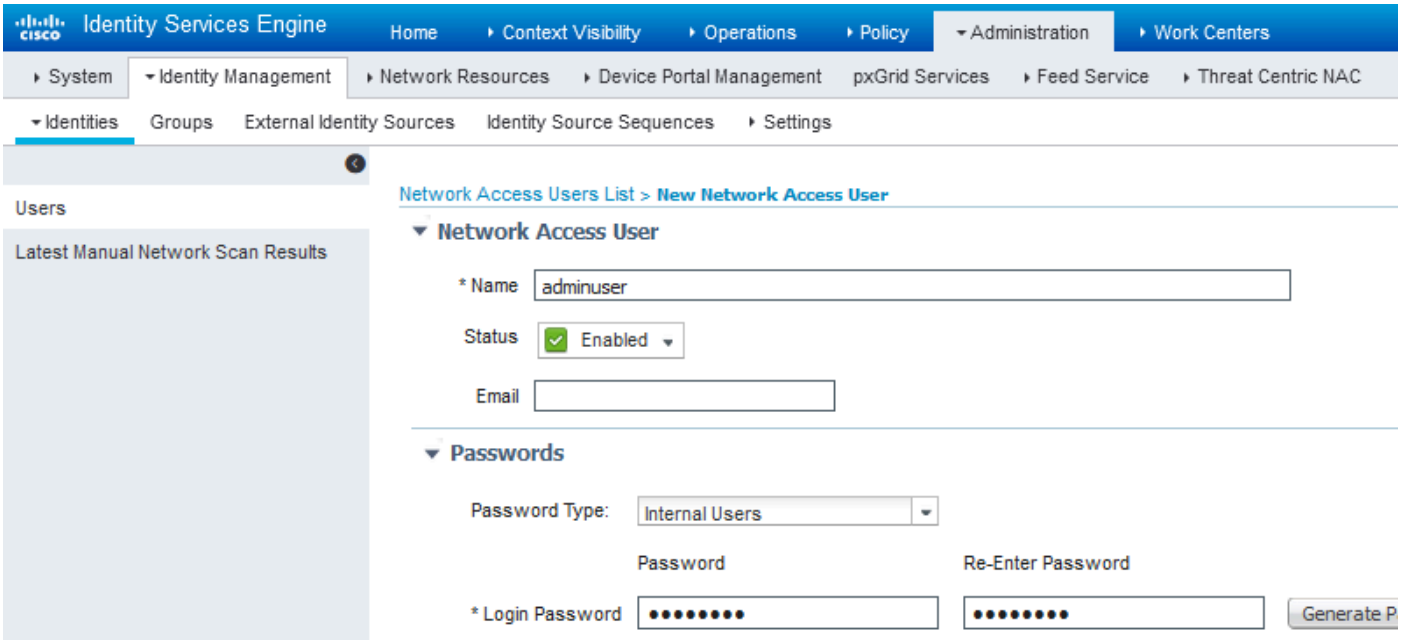
5. Vous devez créer des utilisateurs d'accès réseau correspondant au nom d'utilisateur configuré dans SWA.

5.1. Créez les utilisateurs d'accès réseau et ajoutez-les à leur groupe correspondant. Accédez à Administration > Identity Management > Identities > +Add.



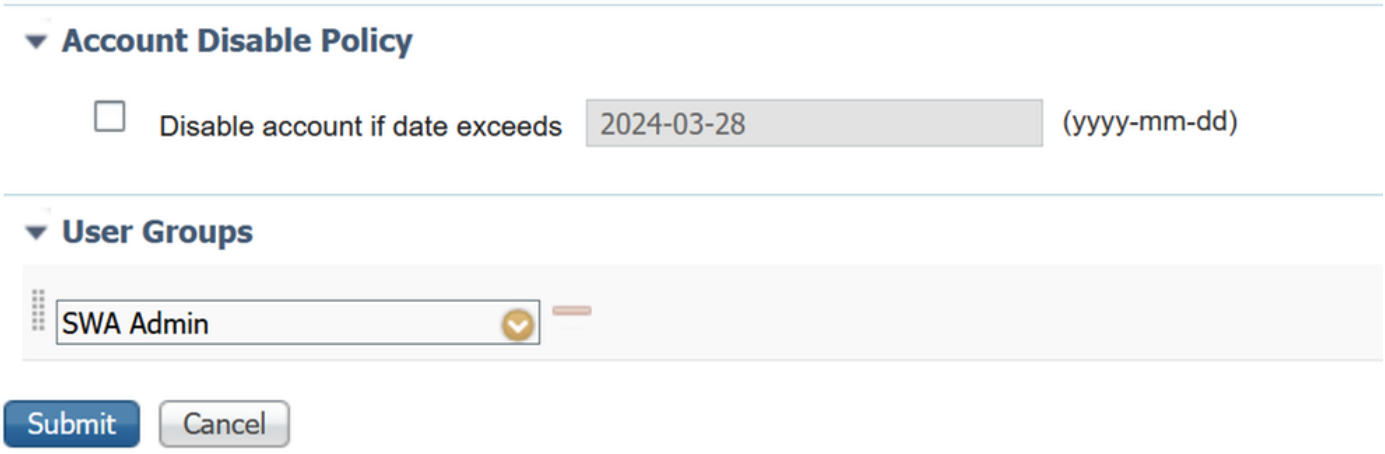
Ajouter des utilisateurs locaux dans ISE

5.2. Vous devez créer des utilisateurs d'accès réseau avec des droits d'administrateur et attribuer un nom et un mot de passe.



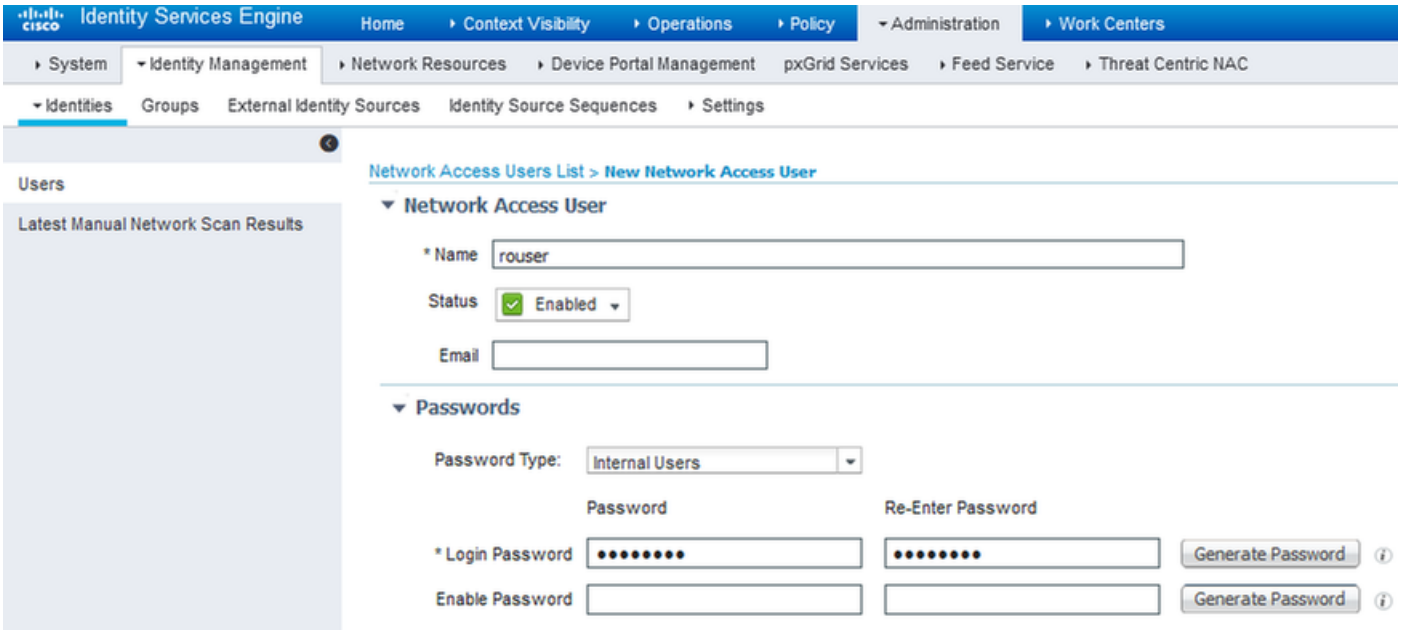
Ajouter un utilisateur Admin

5.3. Choisissez SWA Admin dans la section User Groups.



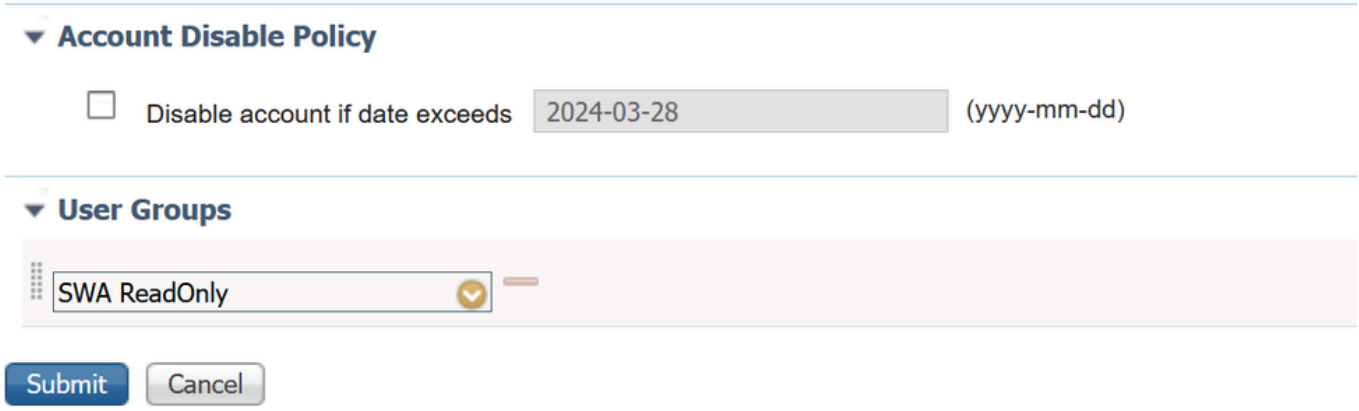
Attribuer un groupe d'administrateurs à l'utilisateur Admin

5.4. Créer un utilisateur avec des droits en lecture seule et attribuer un nom et un mot de passe.



Ajouter un utilisateur en lecture seule

5.5. Choisissez SWA ReadOnly dans la section User Groups.



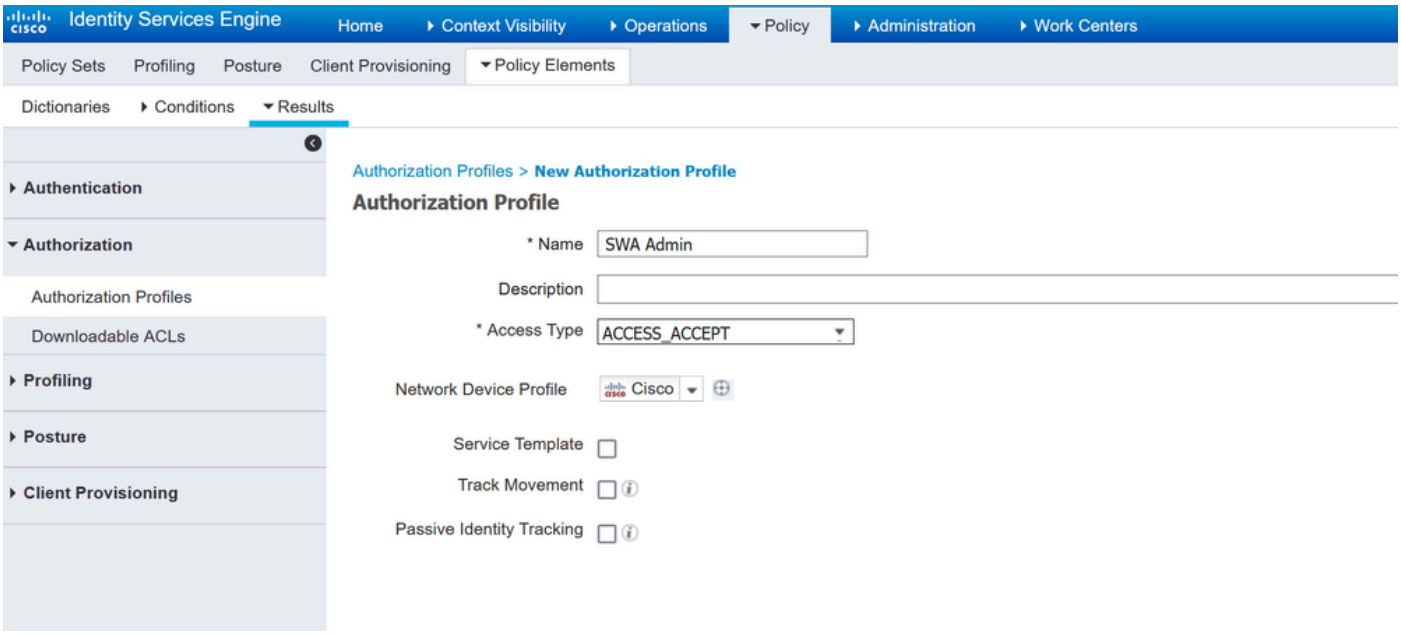
Attribuer un groupe d'utilisateurs en lecture seule à l'utilisateur en lecture seule

---

6. Créez le profil d'autorisation pour l'utilisateur Admin.

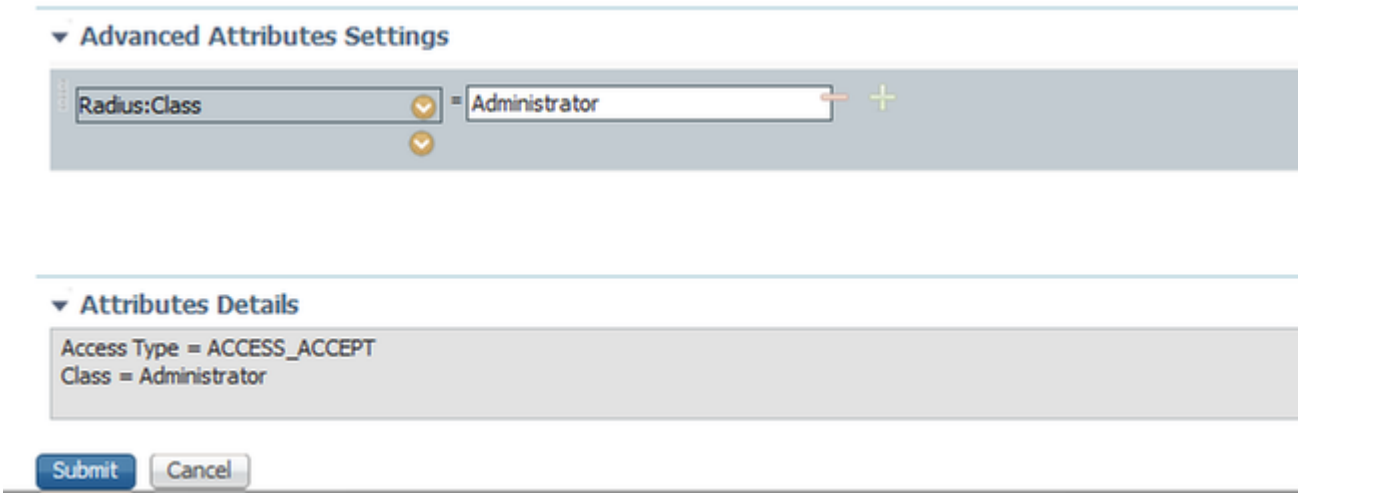
6.1. Accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.

6.2. Définissez un nom pour le profil d'autorisation et assurez-vous que le type d'accès est défini sur ACCESS_ACCEPT.



Ajouter un profil d'autorisation pour les administrateurs

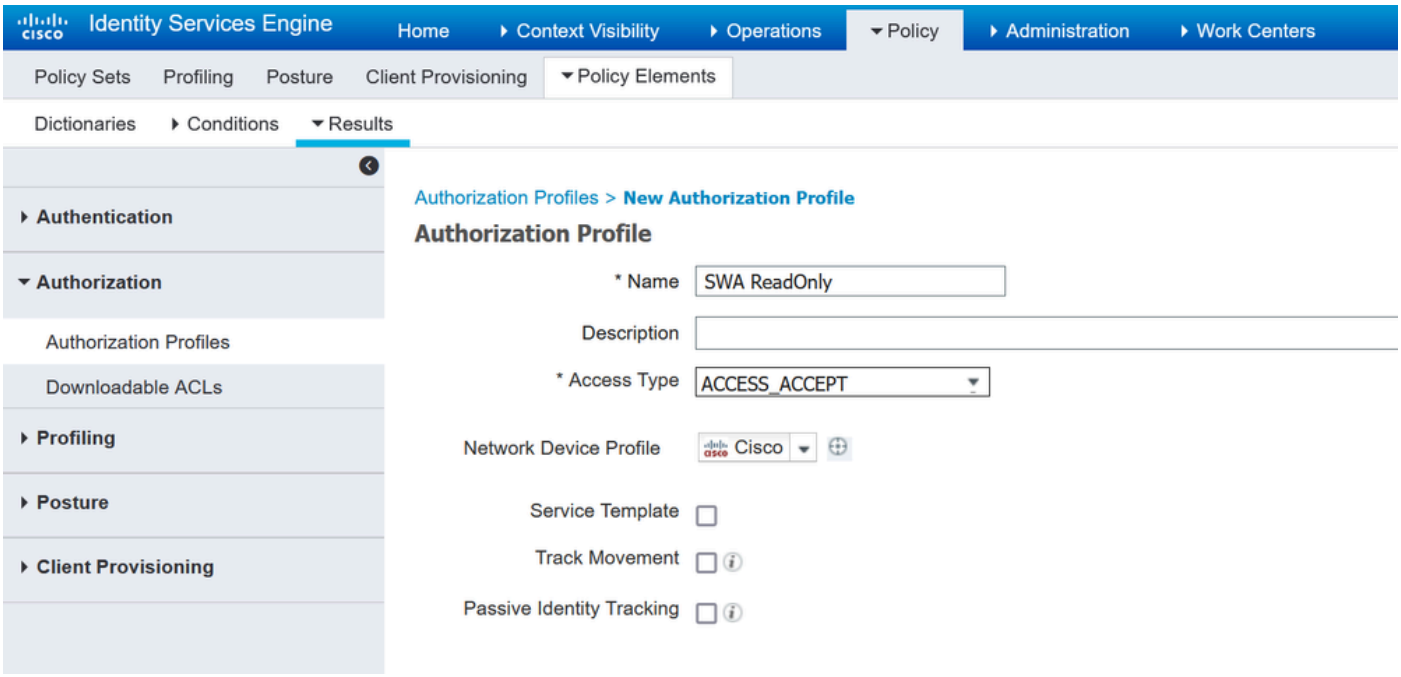
6.3. Dans les paramètres d'attributs avancés, naviguez jusqu'à Radius > Class—[25] et entrez la valeur Administrator et cliquez sur Submit.



Ajouter un profil d'autorisation pour les administrateurs

---

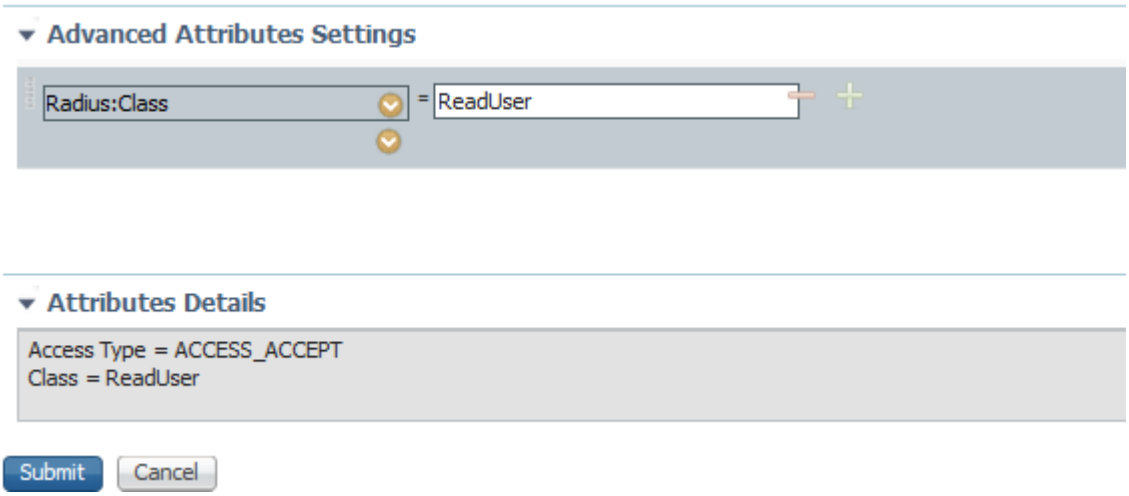
7. Répétez l'étape 6 pour créer le profil d'autorisation pour l'utilisateur en lecture seule.



Ajouter un profil d'autorisation pour les utilisateurs en lecture seule

---

7.1. Cette fois, créez le Radius : Class avec la valeur ReadUser au lieu de Administrator.

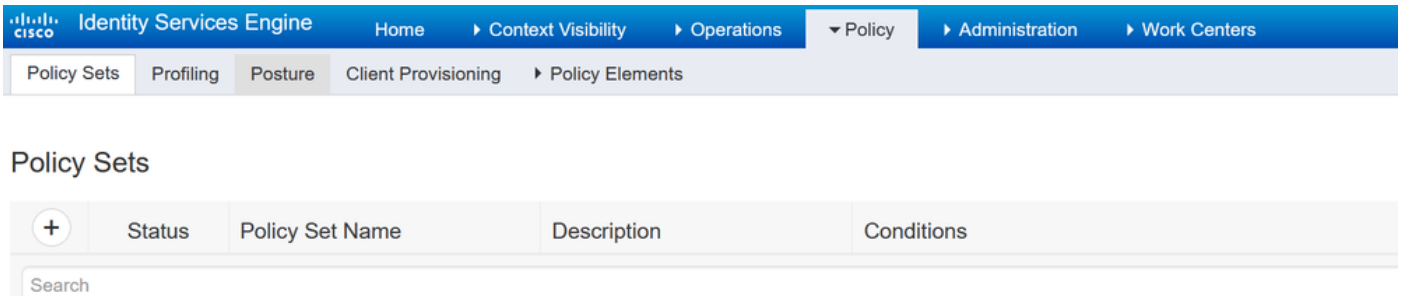


Ajouter un profil d'autorisation pour les utilisateurs en lecture seule

---

8. Créez des ensembles de stratégies qui correspondent à l'adresse IP SWA. Cela empêche l'accès à d'autres périphériques avec ces informations d'identification utilisateur.

8.1. Accédez à Policy > Policy Sets et cliquez sur l'icône + située dans l'angle supérieur gauche.

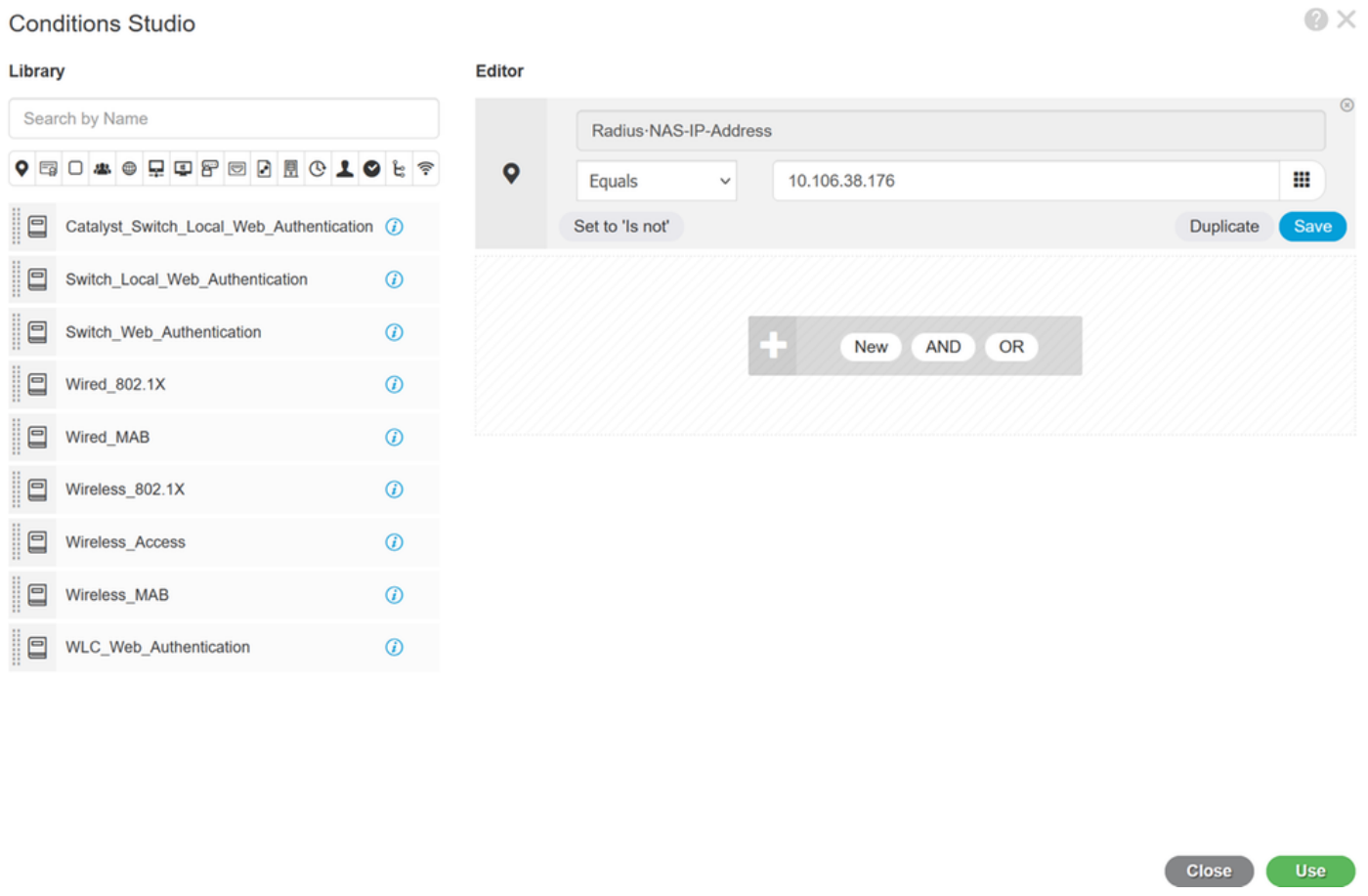


Ajouter un jeu de stratégies dans ISE

8.2. Une nouvelle ligne est placée en haut de vos ensembles de stratégies.

8.3. Entrez un nom pour la nouvelle stratégie et ajoutez une condition pour l'attribut RADIUS NAS-IP-Address afin qu'il corresponde à l'adresse IP SWA.

8.4. Cliquez sur Use pour conserver les modifications et quitter l'éditeur.



Ajouter une stratégie pour mapper un périphérique réseau SWA

8.5. Cliquez sur Save.



Enregistrer la stratégie

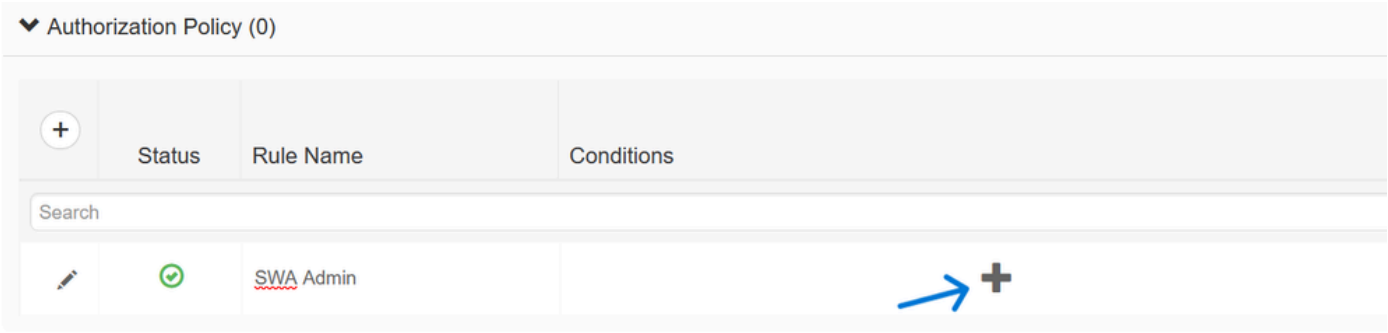
Conseil : Dans cet article, la liste des protocoles d'accès réseau par défaut est autorisée. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.

---

9. Pour afficher les nouveaux ensembles de stratégies, cliquez sur l'icône > dans la colonne Afficher. Développez le menu Stratégie d'autorisation et cliquez sur l'icône + pour ajouter une nouvelle règle permettant d'autoriser l'accès à l'utilisateur disposant de droits d'administrateur.

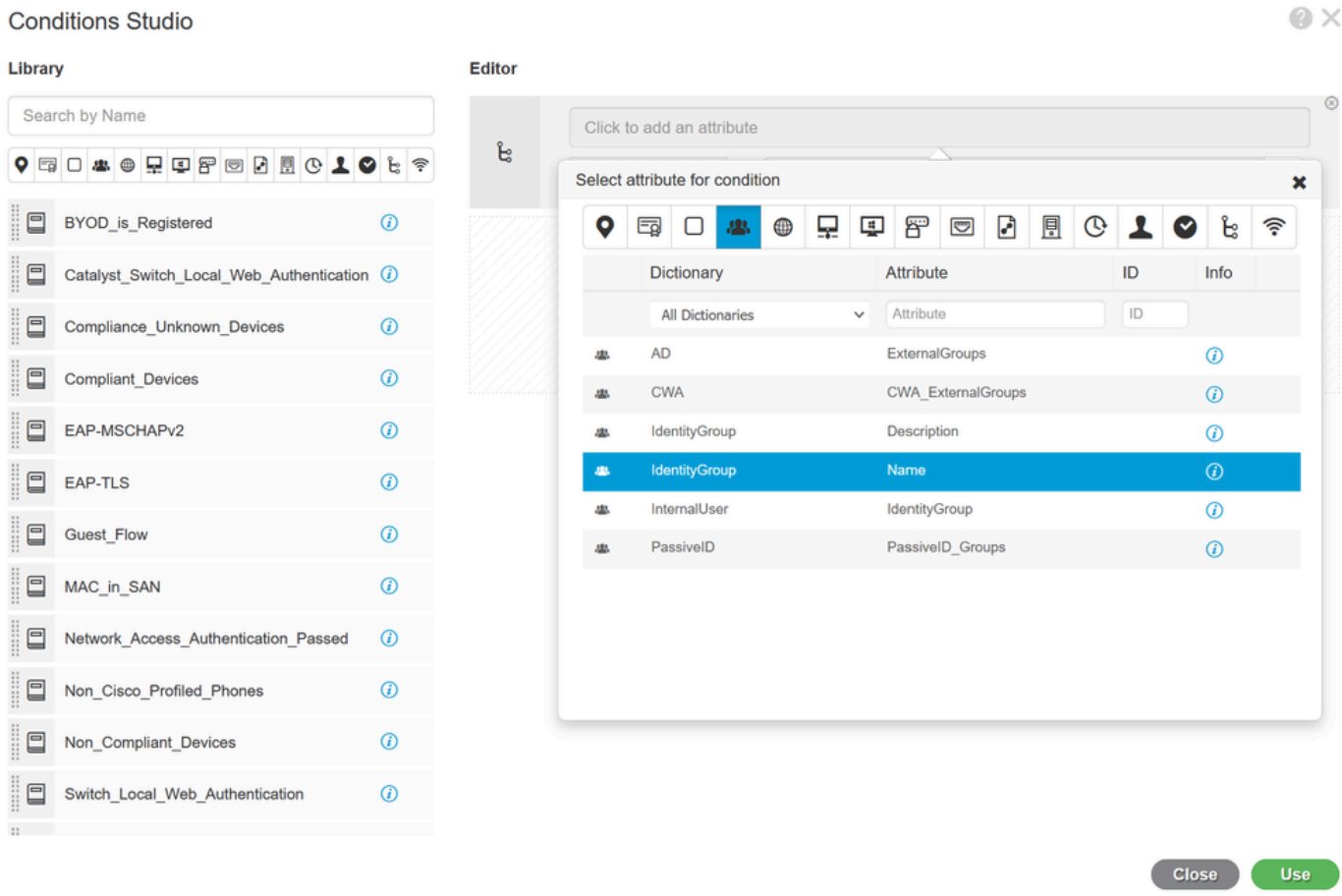
9.1.Entrez un nom.

9.2. Pour créer une condition correspondant au groupe d'utilisateurs Admin, cliquez sur l'icône +.



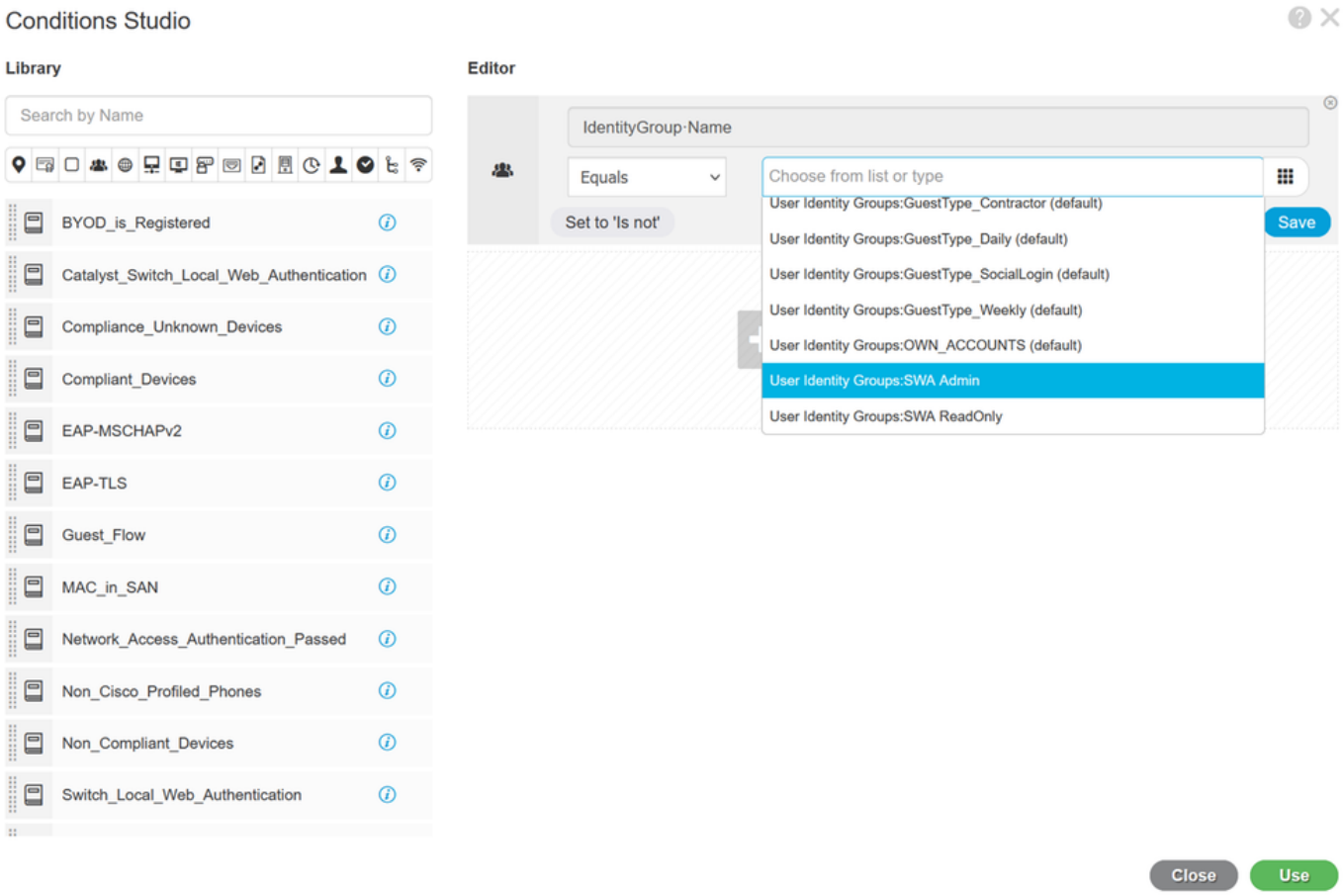
Ajouter une condition de stratégie d'autorisation

9.3. Définissez les conditions pour faire correspondre le groupe d'identité du dictionnaire avec les groupes d'identité d'attribut Nom égal utilisateur : Administrateur SWA.



Sélectionner le groupe d'identités comme condition

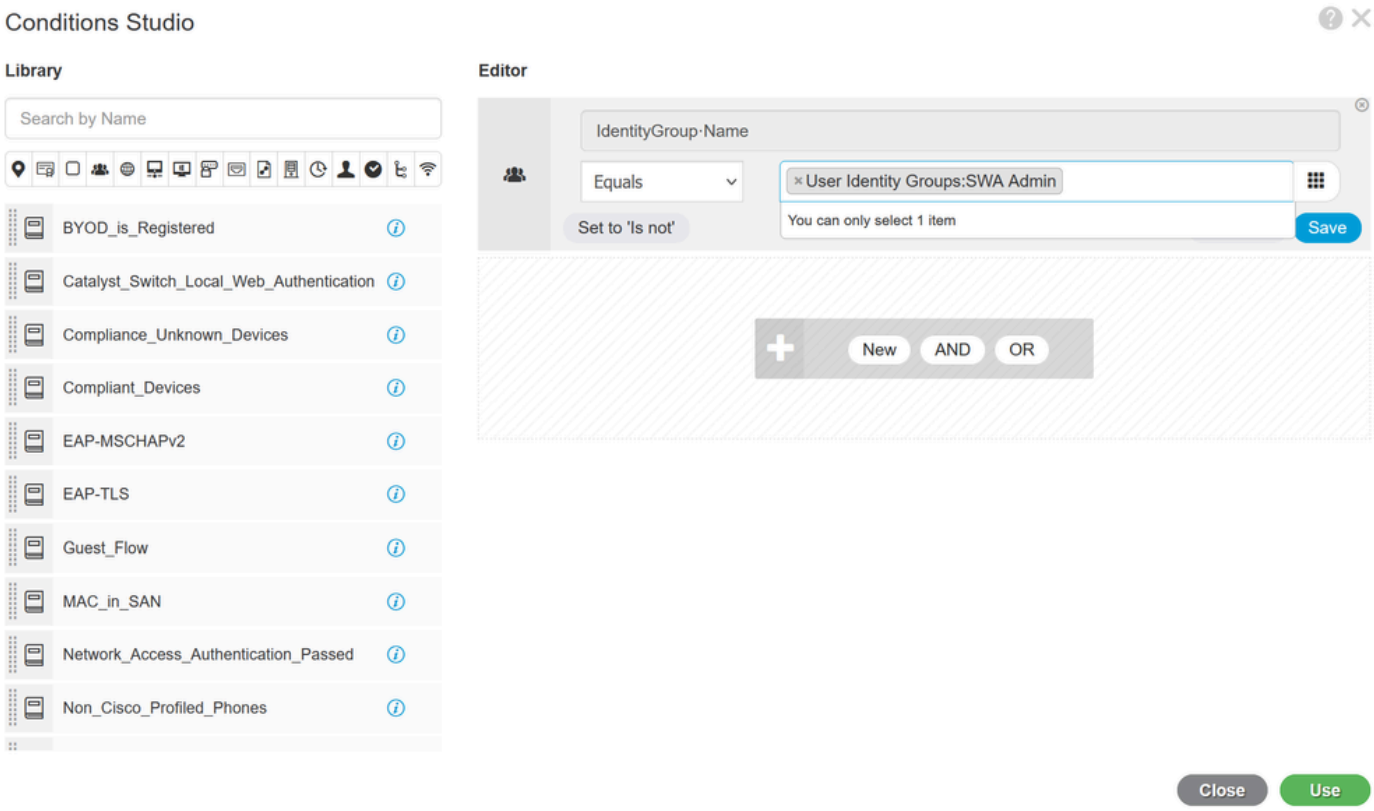
9.4. Faites défiler vers le bas et sélectionnez User Identity Groups : Administrateur SWA.



Faites défiler vers le bas et sélectionnez Nom du groupe d'identités

---

9.5. Cliquez sur Utiliser.



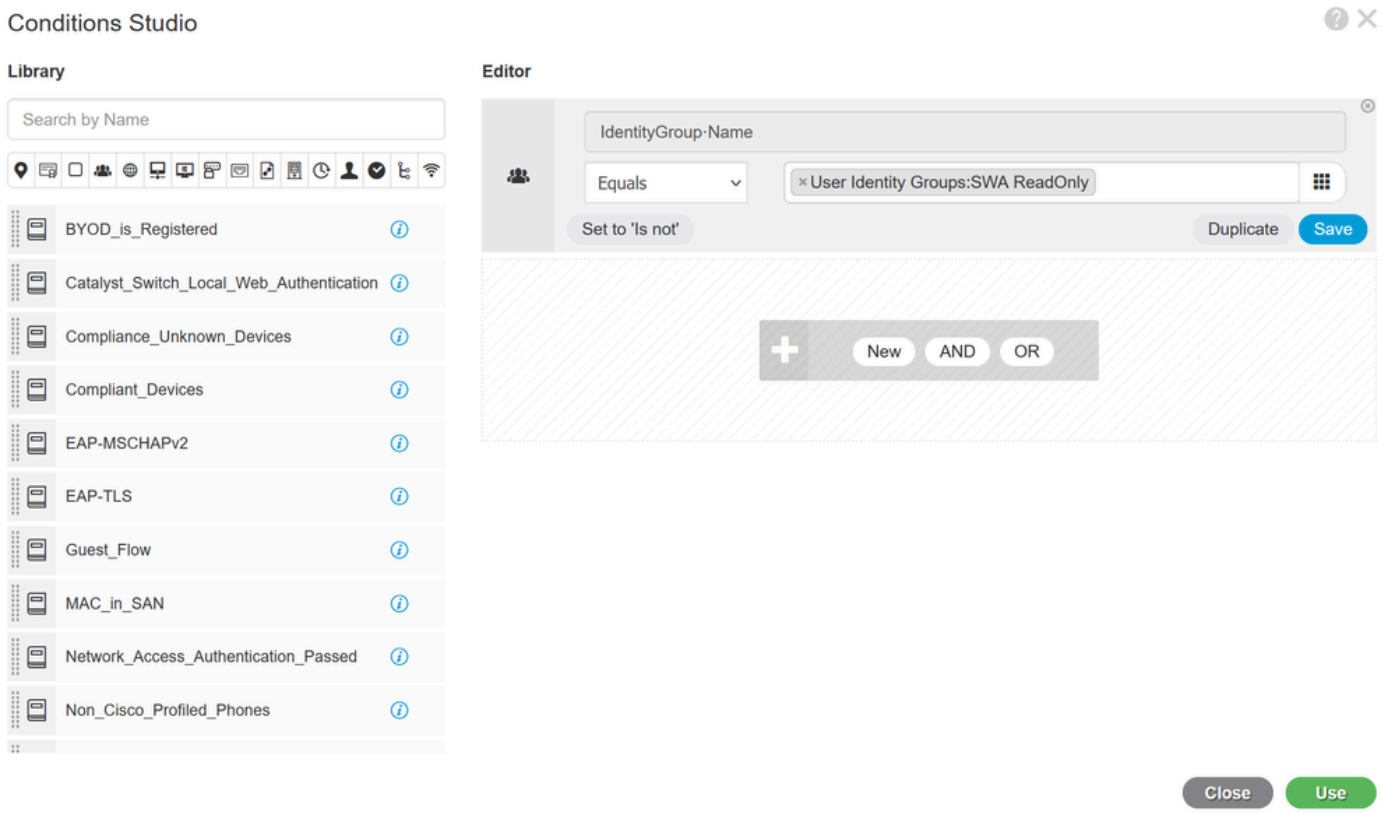
Sélectionner la stratégie d'autorisation pour le groupe d'utilisateurs Admin SWA

---

10. Cliquez sur l'icône + pour ajouter une deuxième règle permettant d'autoriser l'accès à l'utilisateur avec des droits en lecture seule.

10.1. Entrez un nom.

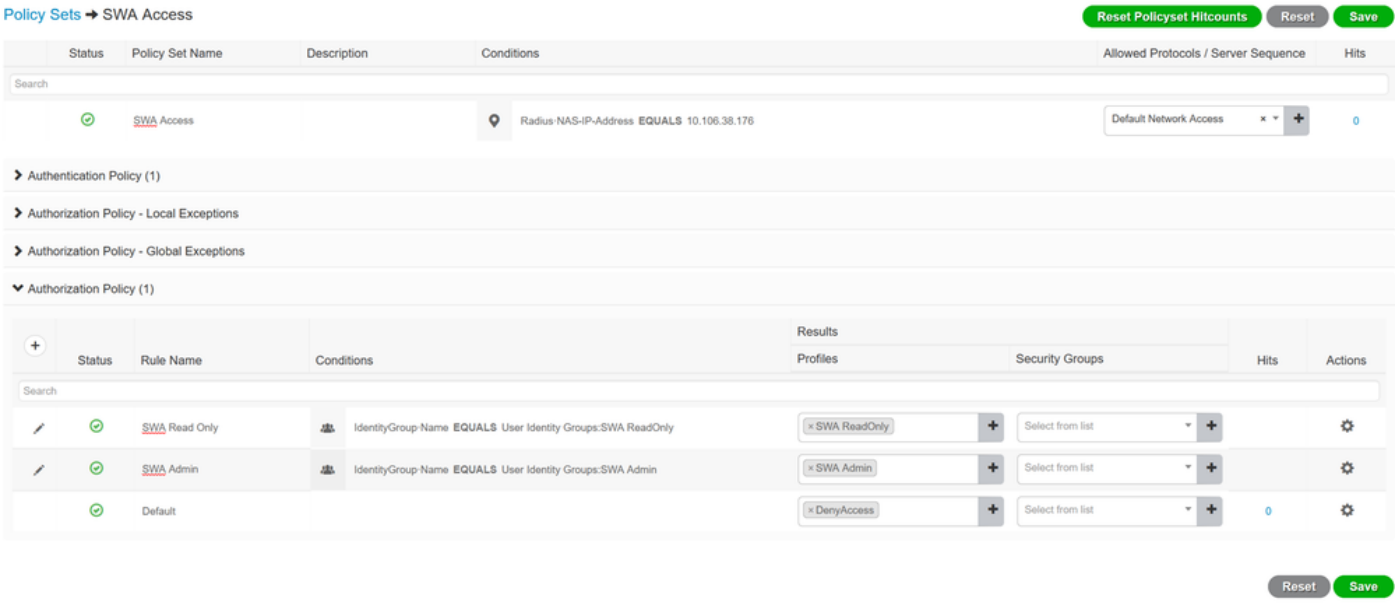
10.2. Définir les conditions pour faire correspondre le groupe d'identités du dictionnaire avec le groupe d'identités Attribut Nom égal Groupes d'identités d'utilisateurs : SWA ReadOnly et cliquez sur Use.



Sélectionner la stratégie d'autorisation pour le groupe d'utilisateurs en lecture seule

---

11. Définissez le profil d'autorisation respectivement pour chaque règle et cliquez sur Enregistrer.

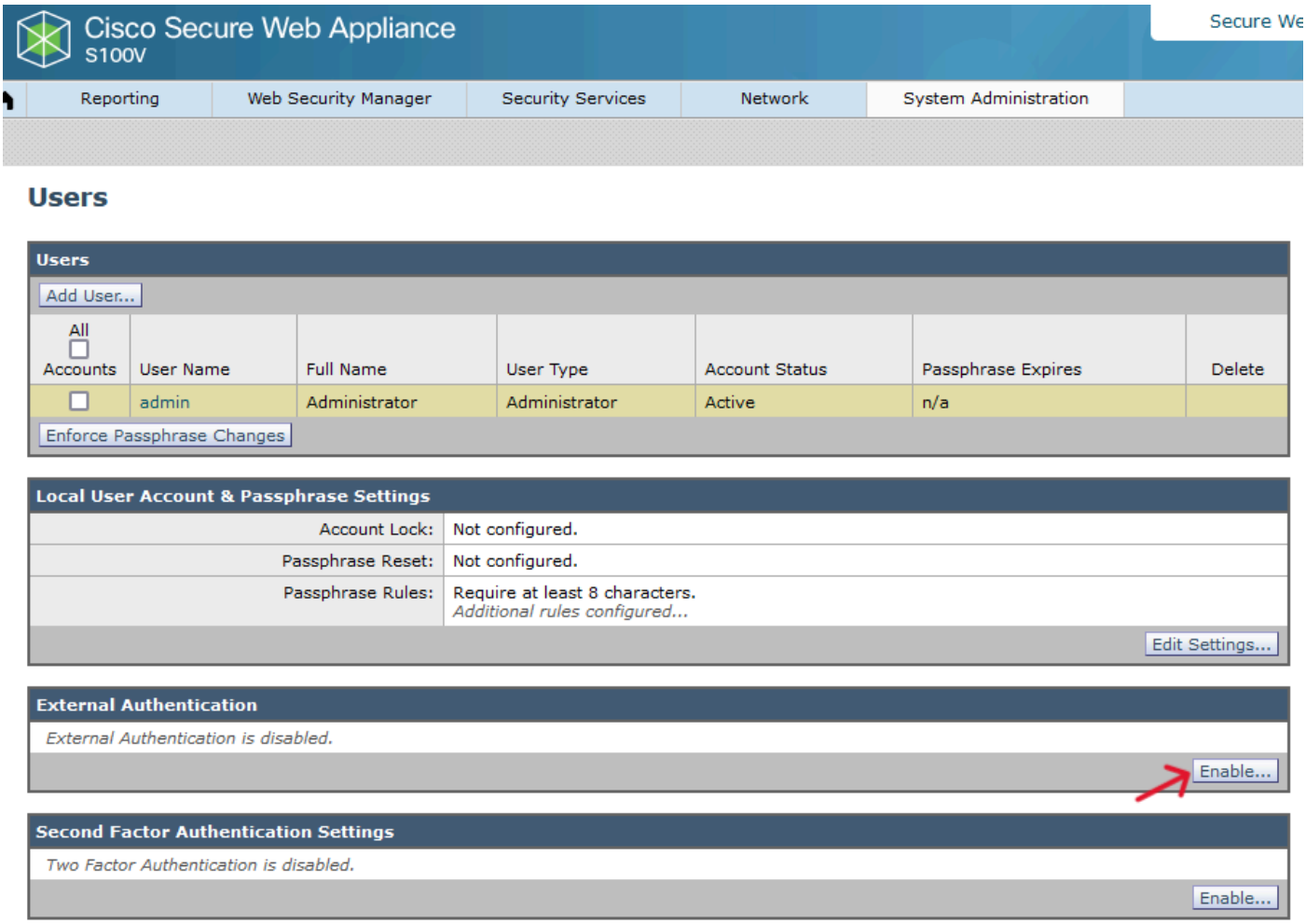


Sélectionner le profil d'autorisation

Configuration SWA

1. Dans l'interface utilisateur graphique de SWA, sélectionnez System Administration, puis Users.

2. Cliquez sur Activer dans Authentification externe.



Activer l'authentification externe dans SWA

---

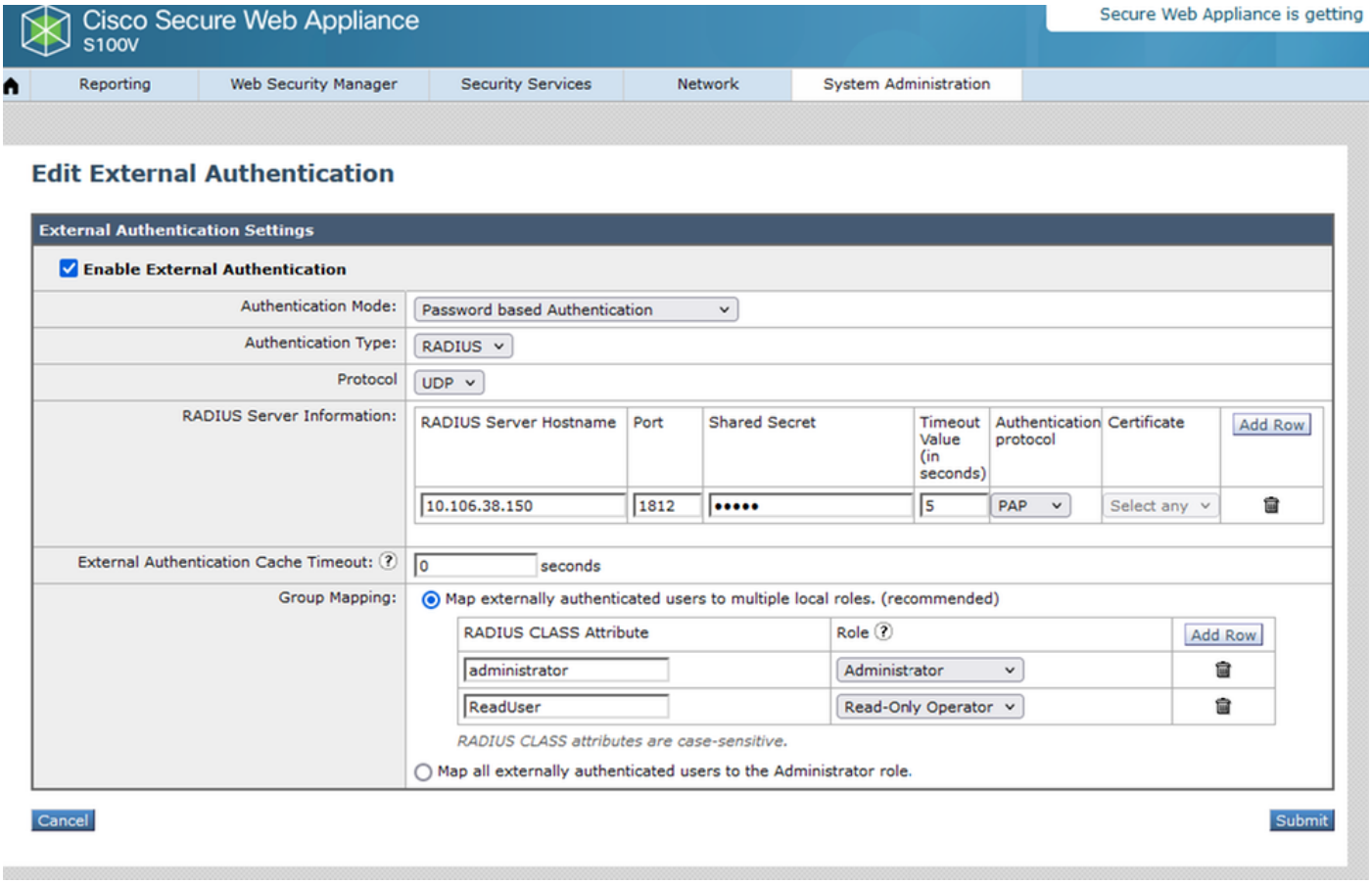
3. Entrez l'adresse IP ou le nom de domaine complet (FQDN) de l'ISE dans le champ RADIUS Server Hostname et entrez le même secret partagé que celui configuré à l'étape 2, Configuration ISE.

4. Sélectionnez Mapper des utilisateurs authentifiés en externe à plusieurs rôles locaux dans Mappage de groupe.

4.1. Saisissez Administrator dans le champ RADIUS CLASS Attribute et sélectionnez le Role Administrator.

4.2. Saisissez ReadUser dans le champ RADIUS CLASS Attribute et sélectionnez le rôle Read-

Only Operator.

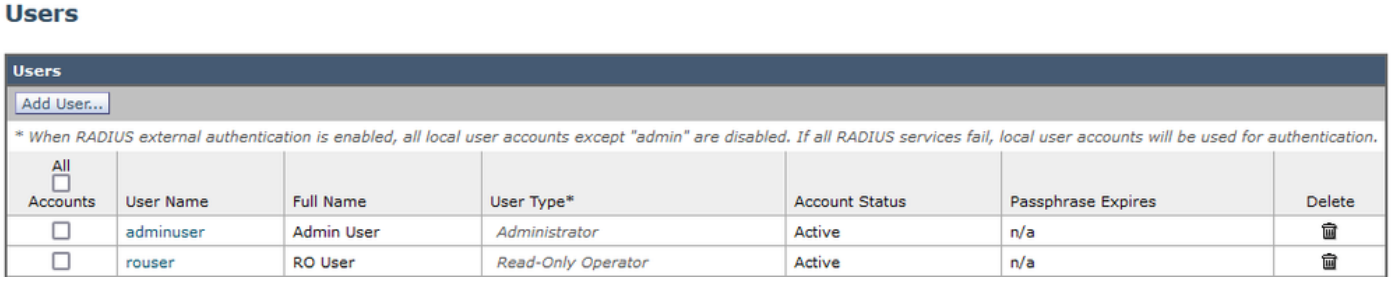


Configuration de l'authentification externe pour le serveur RADIUS

---

5. Pour configurer les utilisateurs dans SWA, cliquez sur Add User. Entrez le Nom d'utilisateur et sélectionnez User Type1, qui est requis pour le rôle souhaité. Saisissez la phrase de passe et la retapez la phrase de passe, qui est requise pour l'accès à l'interface graphique utilisateur, si l'appliance ne peut pas se connecter à un serveur RADIUS externe.

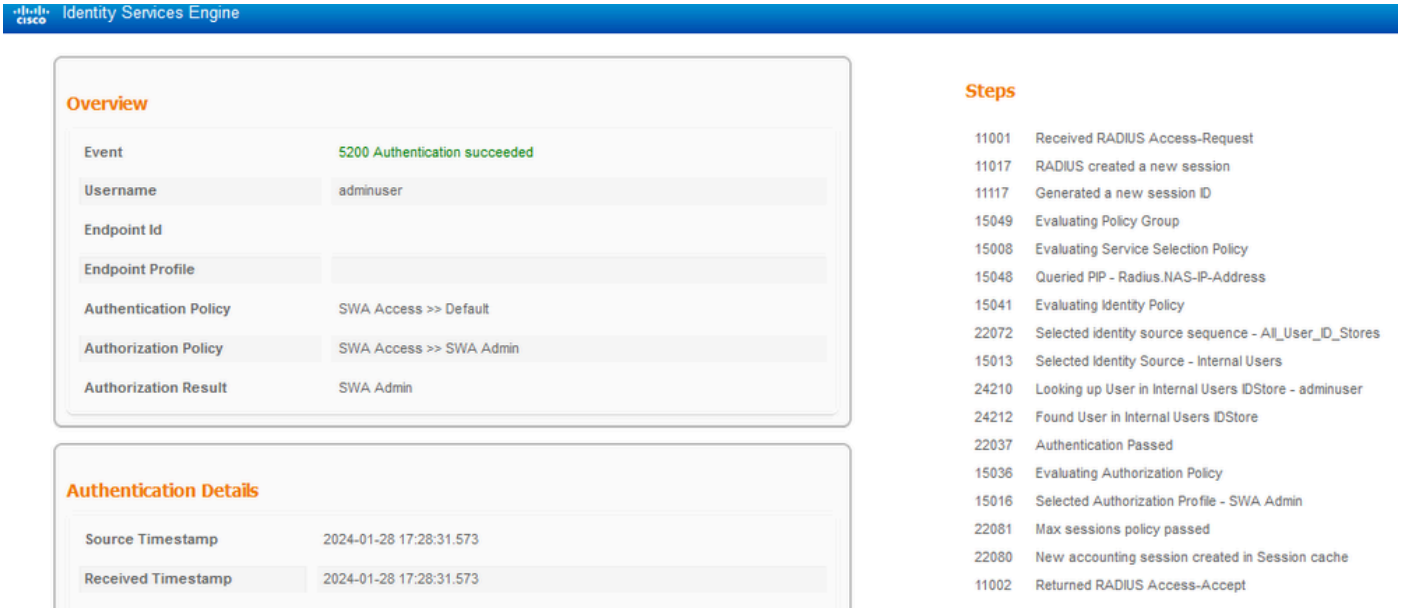
Remarque : Si l'appliance ne parvient pas à se connecter à un serveur externe, elle tente d'authentifier l'utilisateur en tant qu'utilisateur local défini sur l'appliance Web sécurisée.



6. Cliquez sur Soumettre et valider les modifications.

Vérifier

Accédez à l'interface utilisateur graphique SWA avec les informations d'identification utilisateur configurées et vérifiez les journaux actifs dans ISE. Pour vérifier les journaux en direct dans ISE, accédez à Operations > Live Logs :



Vérification de la connexion utilisateur ISE

Autres informations utiles

- Guide de l'utilisateur d'AsyncOS 14.0 pour Cisco Secure Web Appliance
- Guide d'administration ISE 3.0
- Matrice de compatibilité ISE pour l'appliance Web sécurisée
- 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.