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

Table des matières

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 l'appliance Web sécurisé Cisco.
- Connaissance de la configuration des stratégies d'authentification et d'autorisation sur ISE.
- Connaissances de base de RADIUS.

Cisco vous recommande également de disposer des éléments suivants :

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

Composants utilisés

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

- SWA 14.0.2-012
- ISE 3.0.0

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

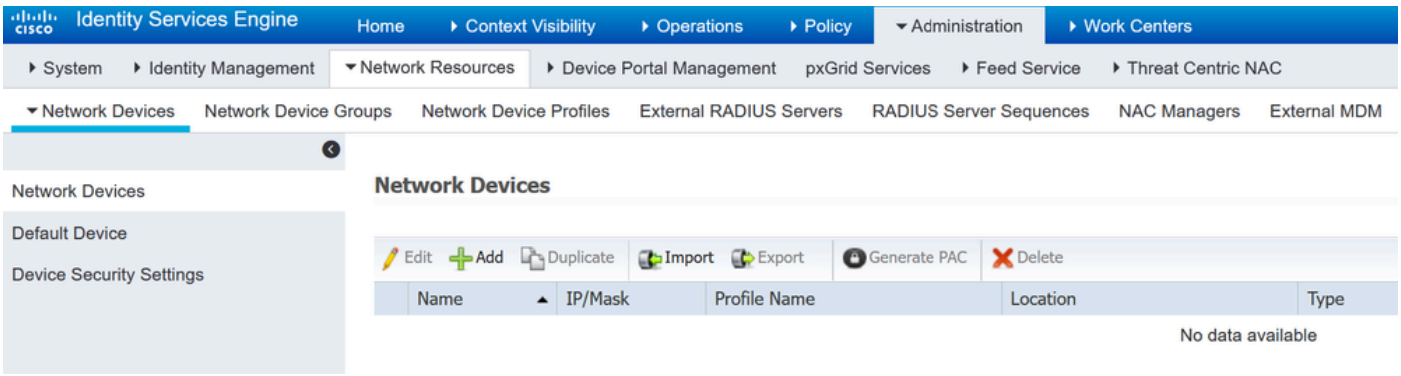
Schéma de topologie du réseau

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

Configurer

Configuration ISE

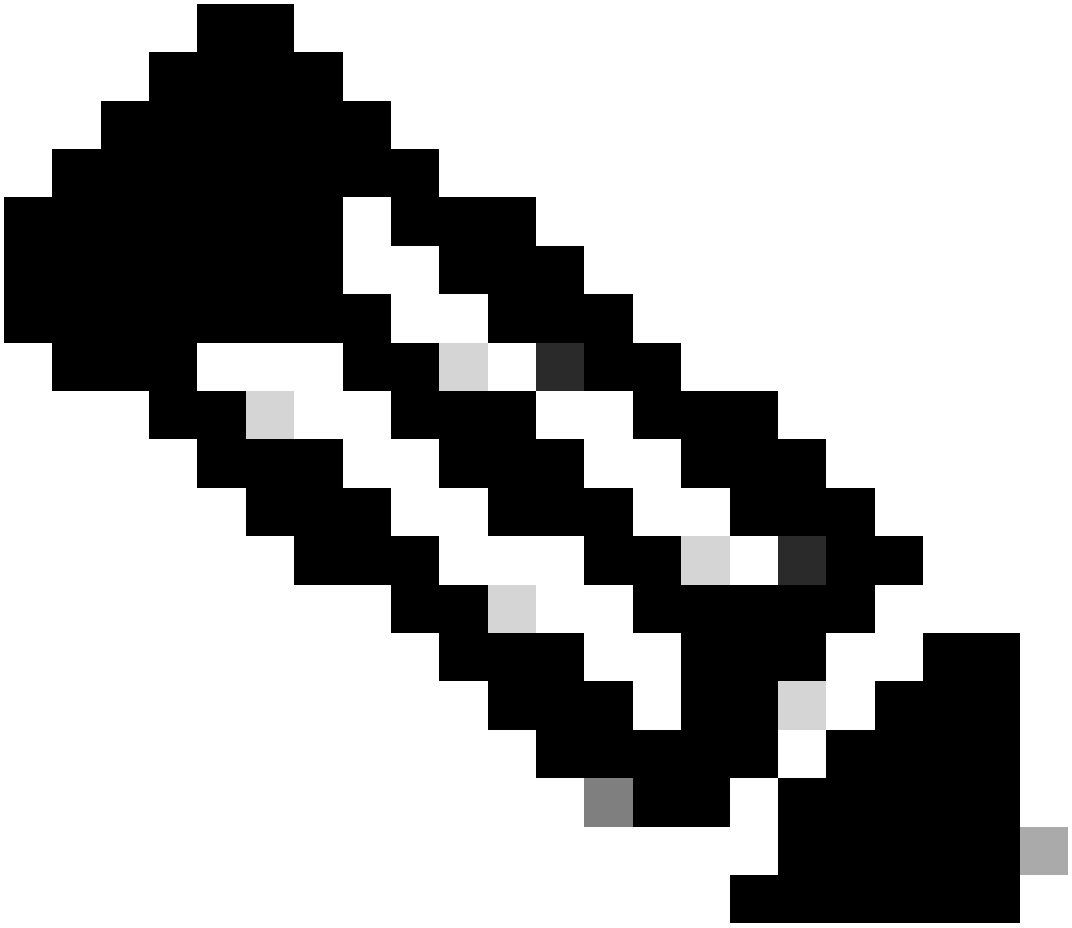
Étape 1. Ajoutez un nouveau périphérique réseau. Accédez à Administration > Network Resources > Network Devices > +Add.



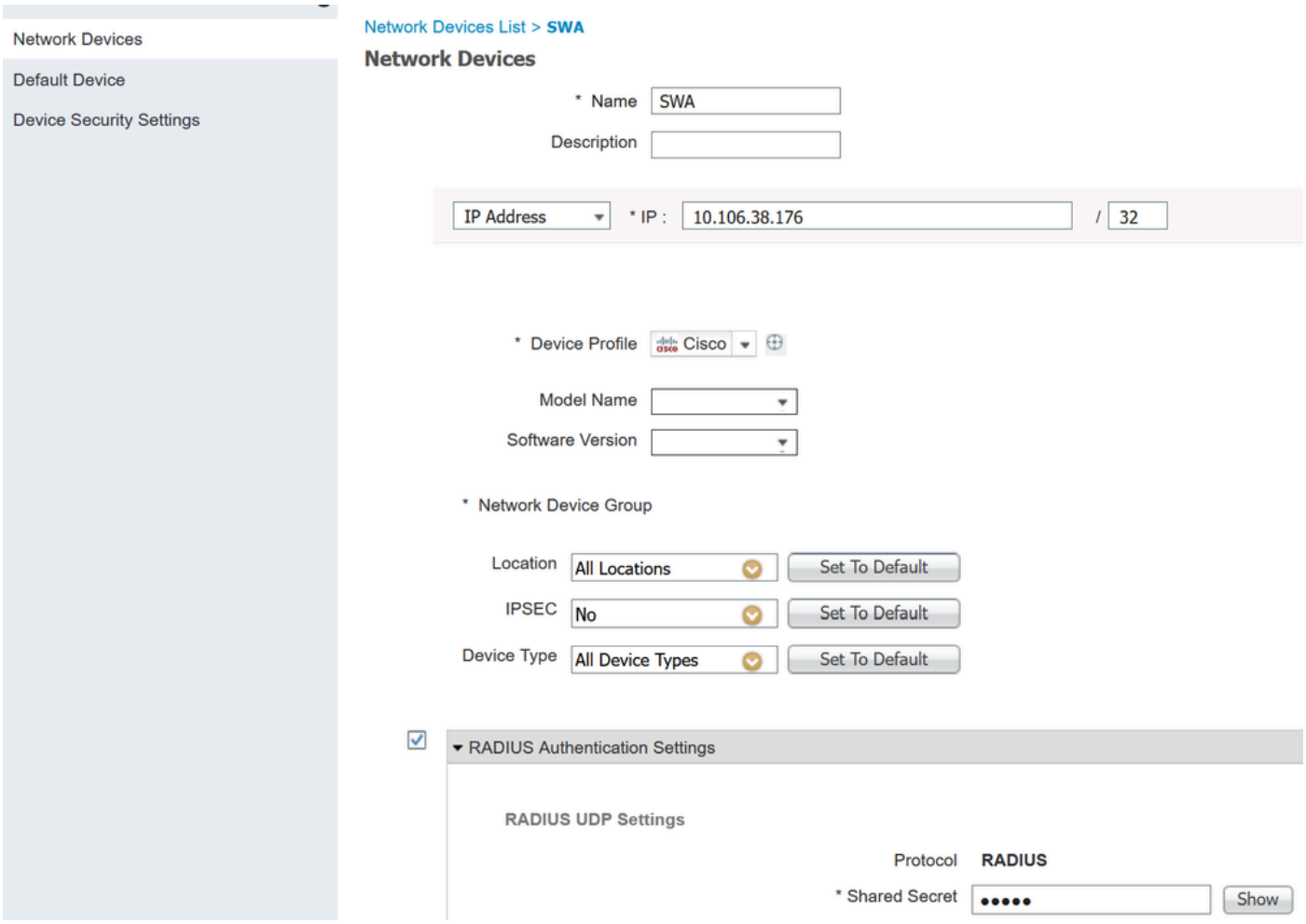
Ajouter SWA en tant que périphérique réseau dans ISE

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

Cochez la case RADIUS et définissez un secret partagé.

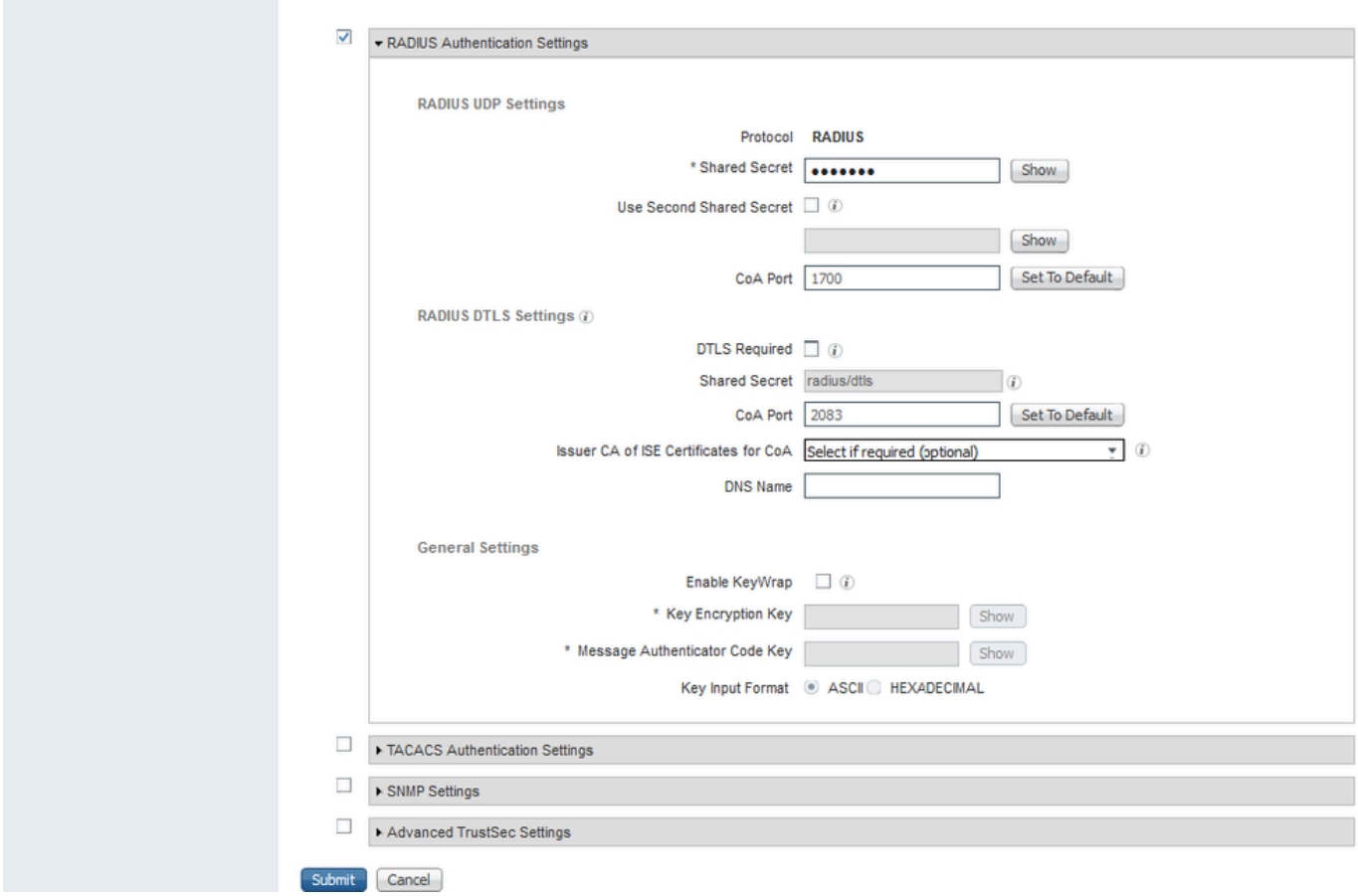


Remarque : la même clé doit être utilisée ultérieurement pour configurer le serveur RADIUS dans SWA.



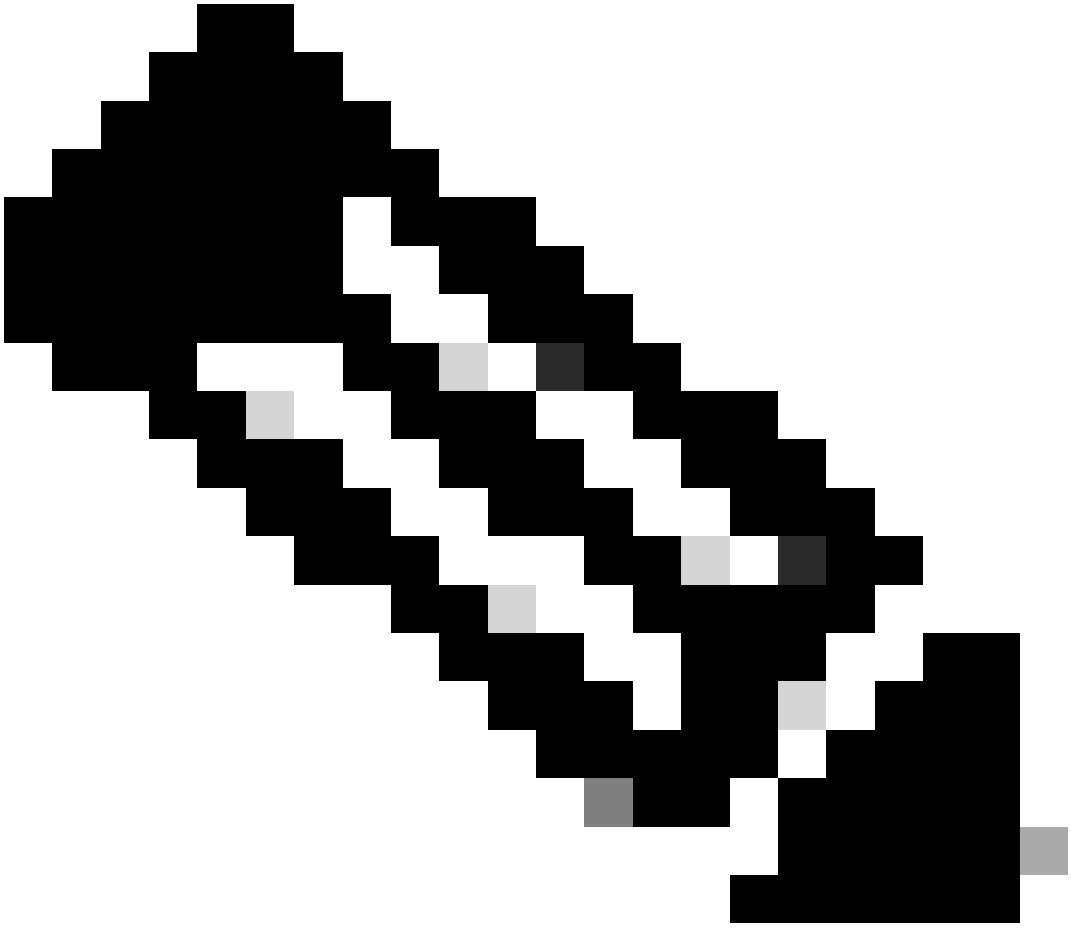
Configurer la clé partagée du périphérique réseau SWA

Étape 2.1. Cliquez sur Submit.

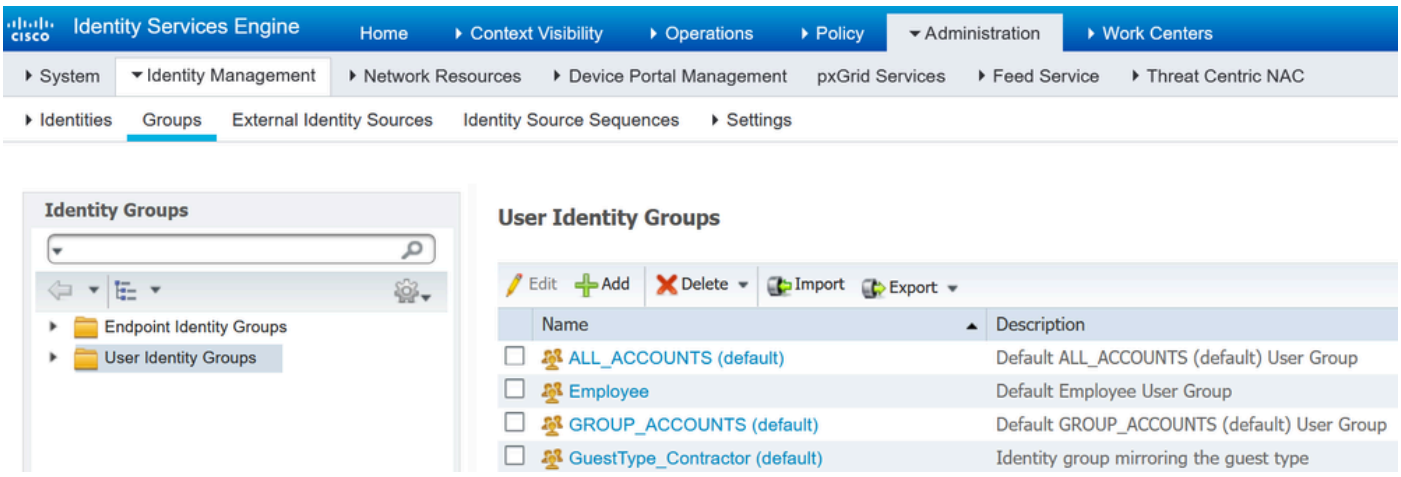


Envoyer la configuration des périphériques réseau

Étape 3. Créez les groupes d'identités utilisateur requis. Accédez à Administration > Identity Management > Groups > User Identity Groups > + Add.



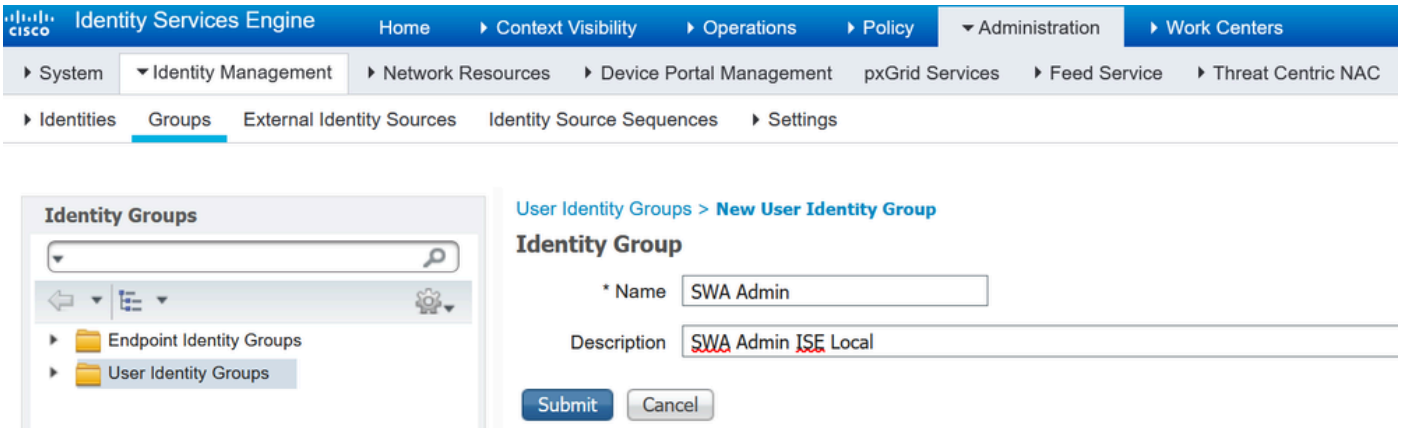
Remarque : vous devez configurer différents groupes d'utilisateurs pour qu'ils correspondent à différents types d'utilisateurs.



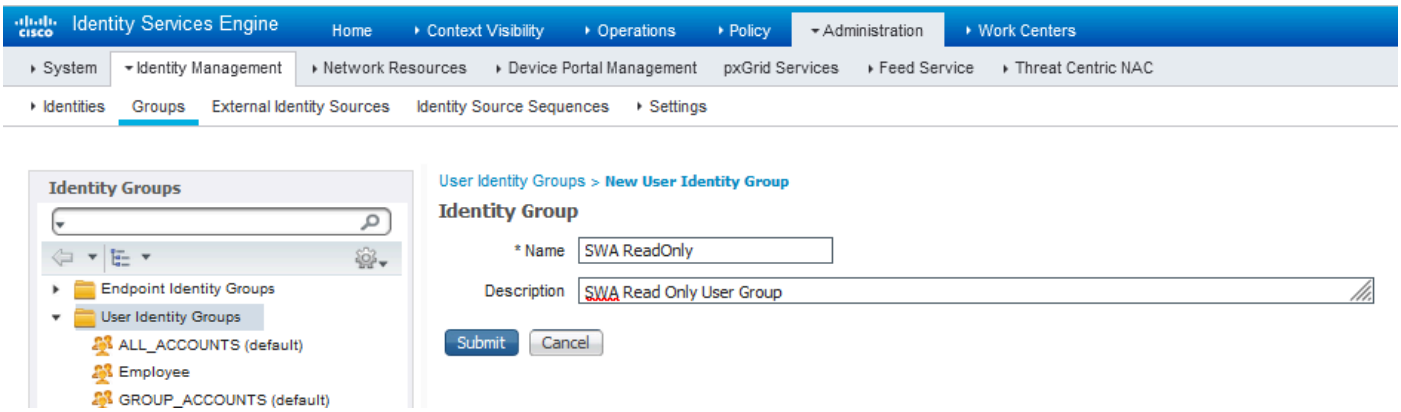
Ajouter un groupe d'identités utilisateur

Étape 4. Saisissez le nom du groupe, sa description (facultatif) et Submit. Répétez ces étapes

pour chaque groupe. Dans cet exemple, vous créez un groupe pour les utilisateurs administrateurs et un autre pour les utilisateurs en lecture seule.



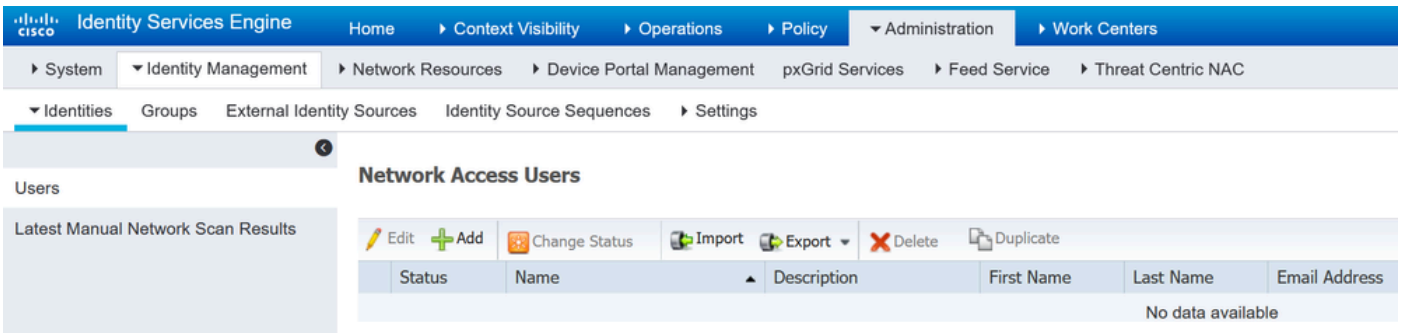
Ajouter un groupe d'



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

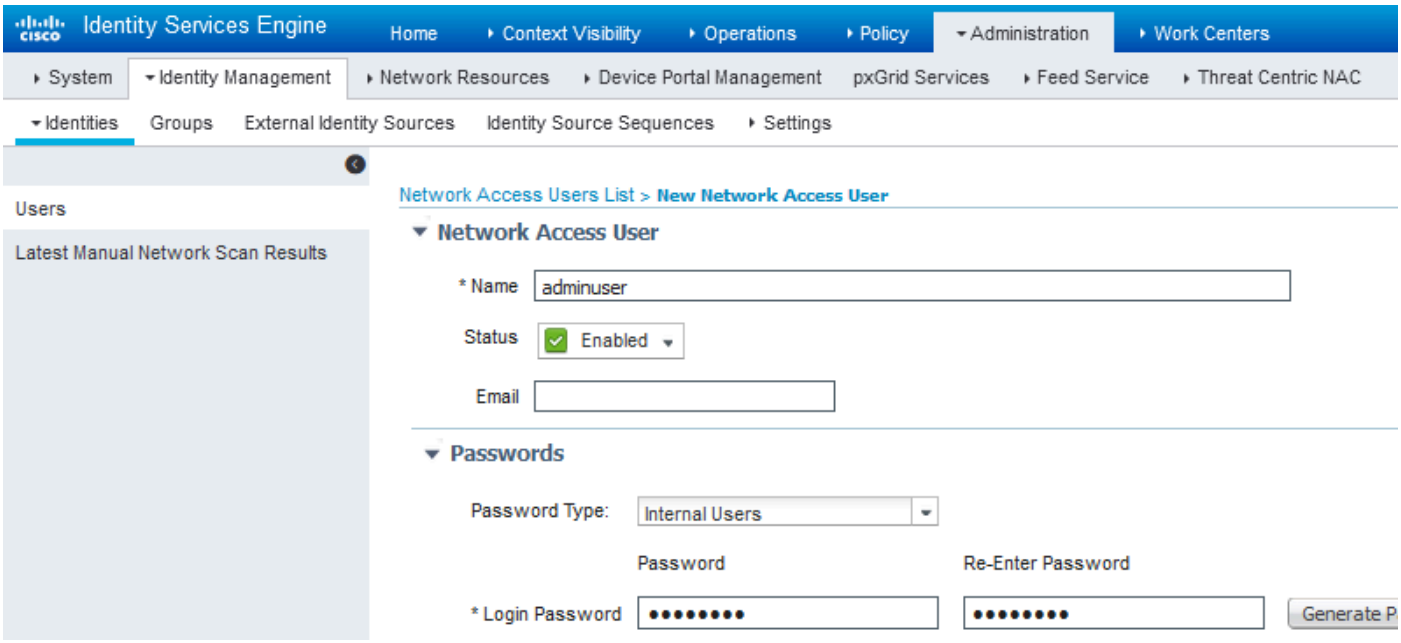
Étape 5. Vous devez créer des utilisateurs d'accès réseau correspondant au nom d'utilisateur configuré dans SWA.

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



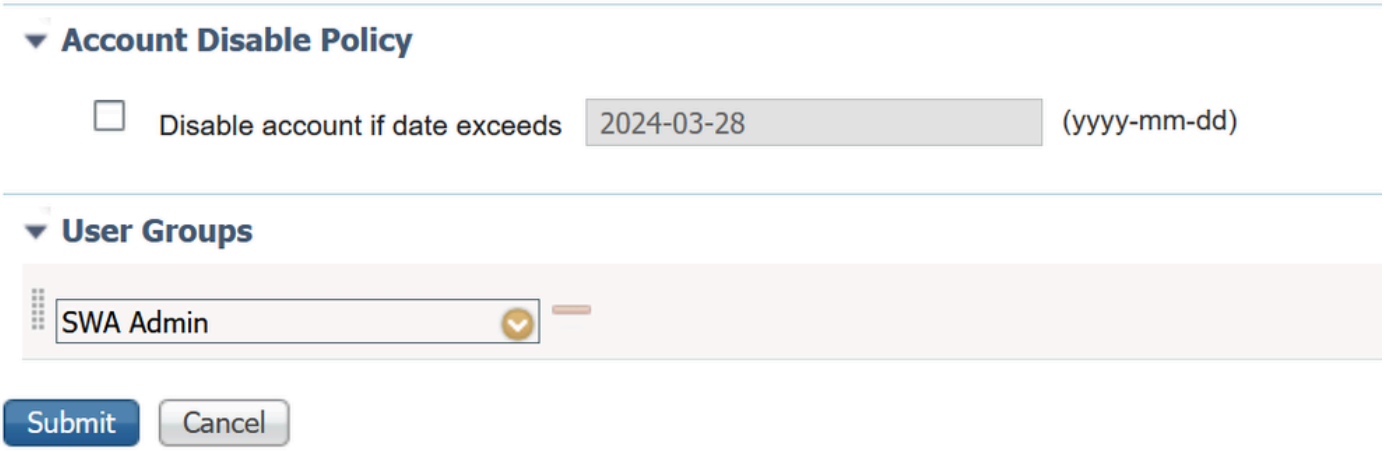
Ajouter des utilisateurs locaux dans ISE

Étape 5.1. Vous devez créer des utilisateurs d'accès réseau avec des droits d'administrateur. Attribuez un nom et un mot de passe.



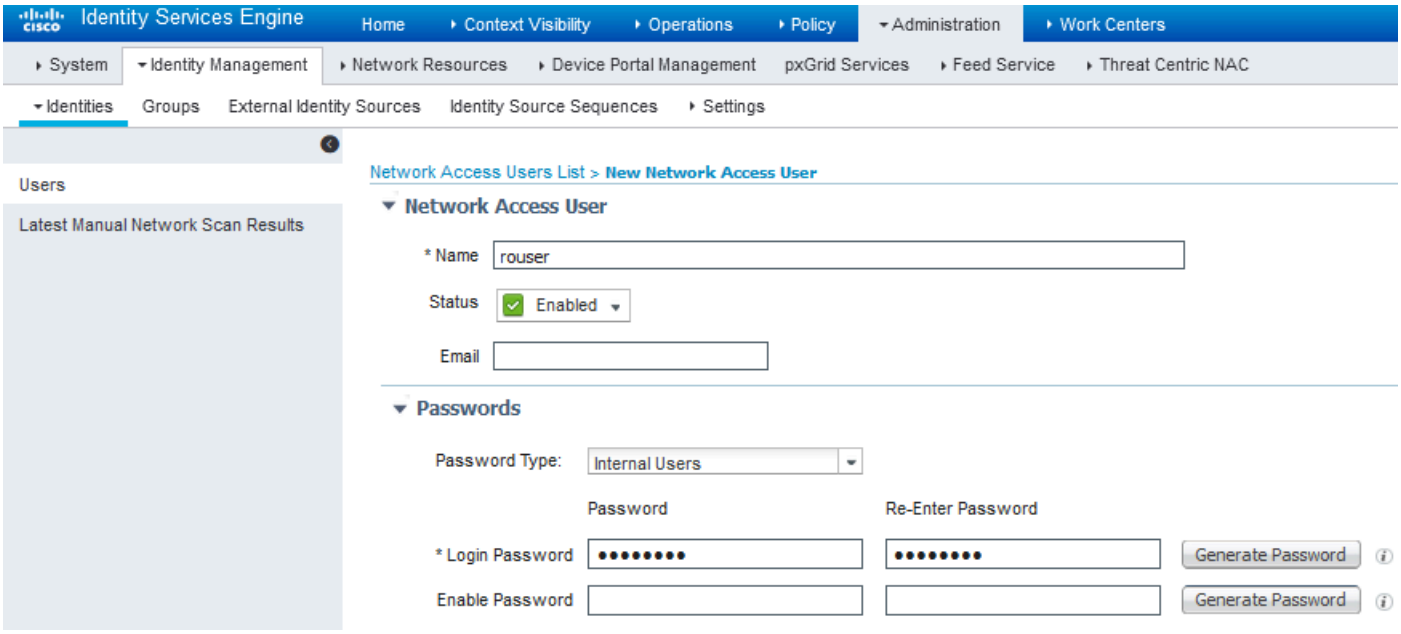
Ajouter un utilisateur Admin

Étape 5.2. Choisissez SWA Admin dans la section User Groups.



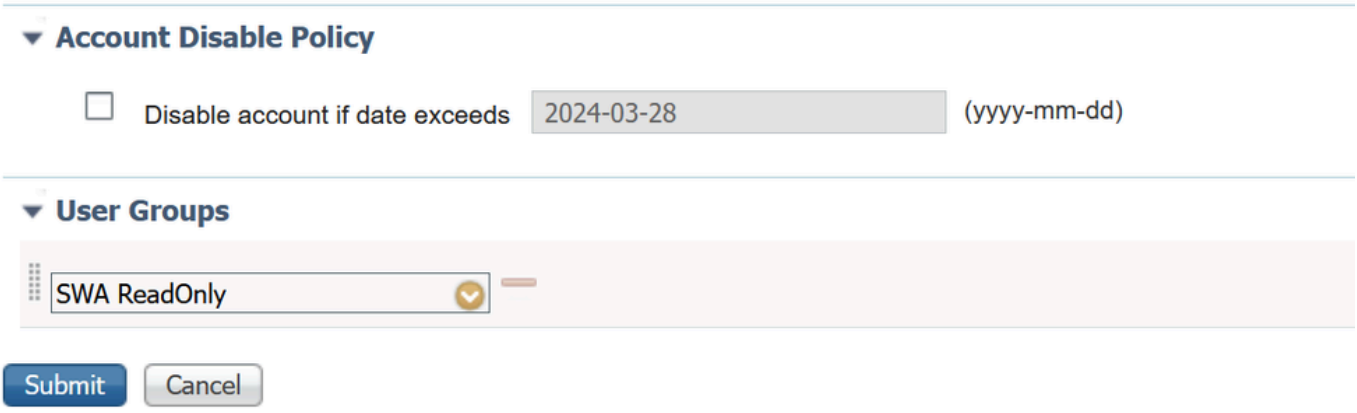
Assign Admin Group to the Admin User

Étape 5.3. Vous devez créer un utilisateur avec des droits en lecture seule. Attribuez un nom et un mot de passe.



Ajouter un utilisateur en lecture seule

Étape 5.4. Sélectionnez SWA ReadOnly dans la section User Groups.

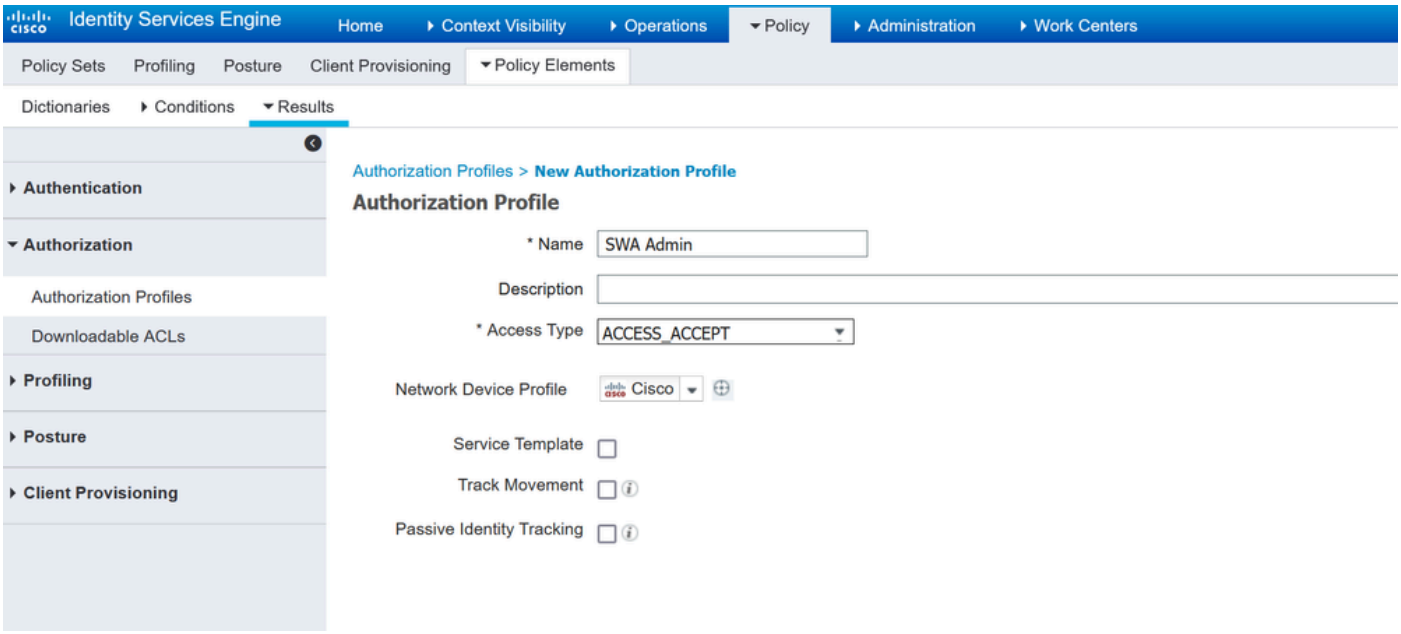


Attribuer un groupe d'utilisateurs en lecture seule à l'utilisateur en lecture seule

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

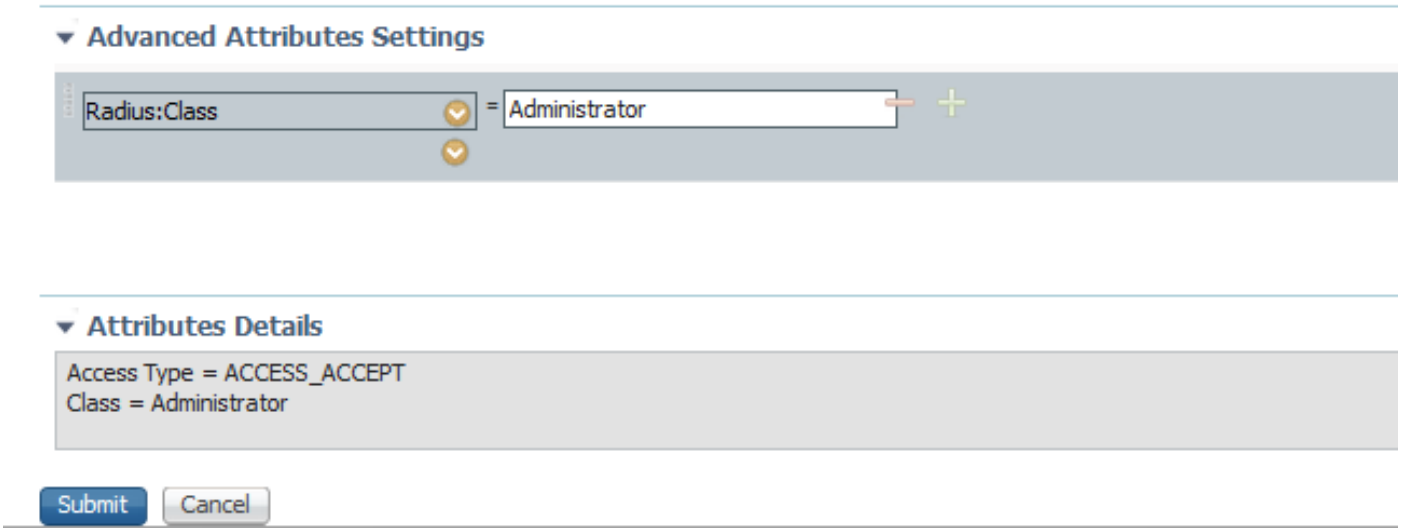
Accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles > +Add.

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



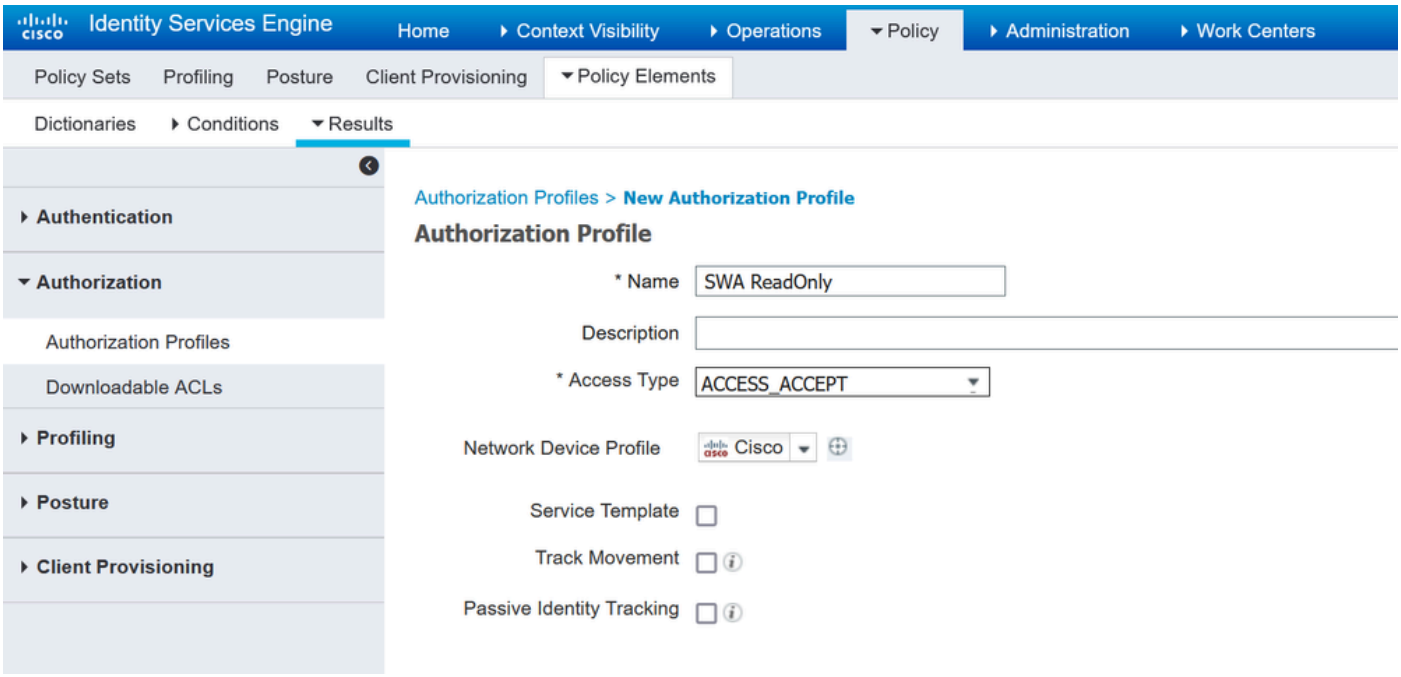
Ajouter un profil d'autorisation pour les administrateurs

Étape 6.1. Dans les paramètres d'attributs avancés, accédez à Radius > Class—[25] et entrez la valeur Administrator et cliquez sur Submit.



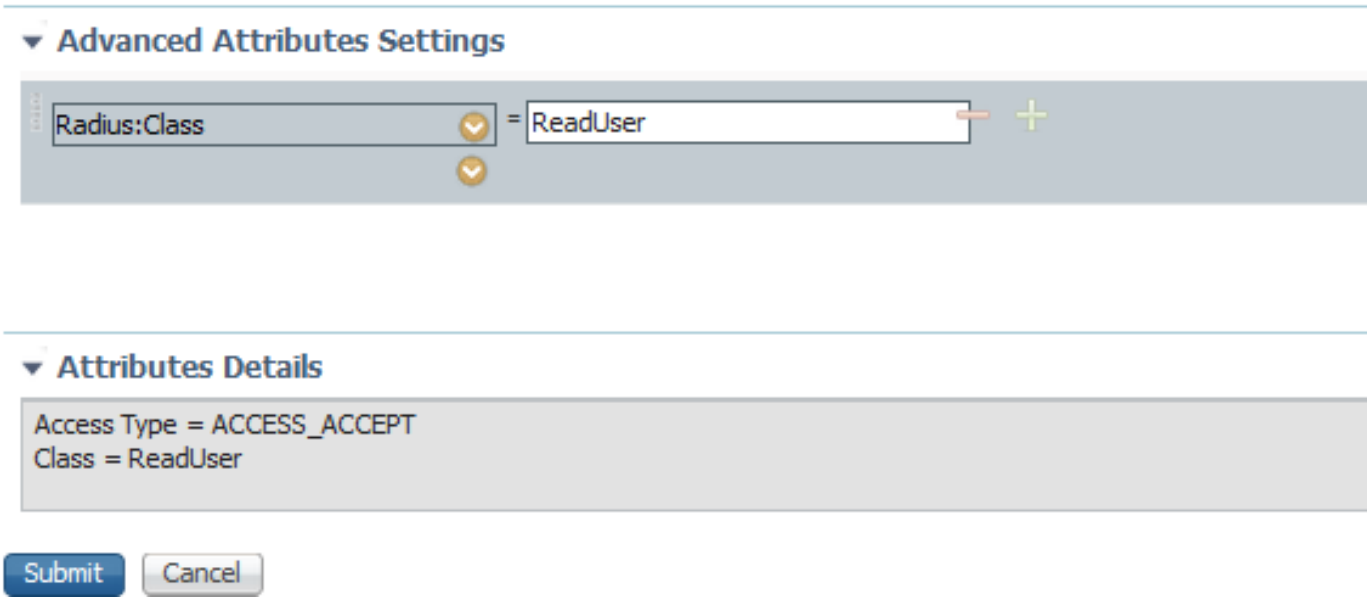
Add Authorization Profile for Admin Users

Étape 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

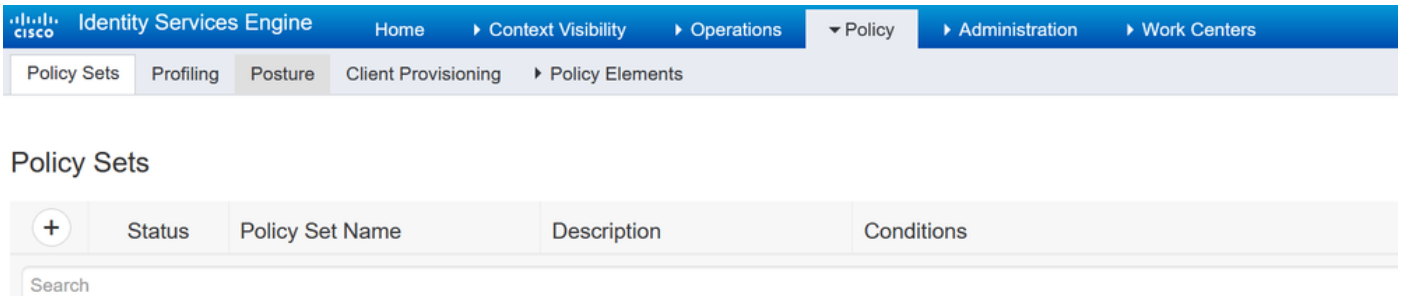
ÉTAPE 7.1. Cette fois, créez Radius : Class avec la valeur ReadUser à la place de Administrator.



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

Étape 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.

Accédez à Policy > PolicySets et cliquez sur l'icône + placée dans l'angle supérieur gauche.

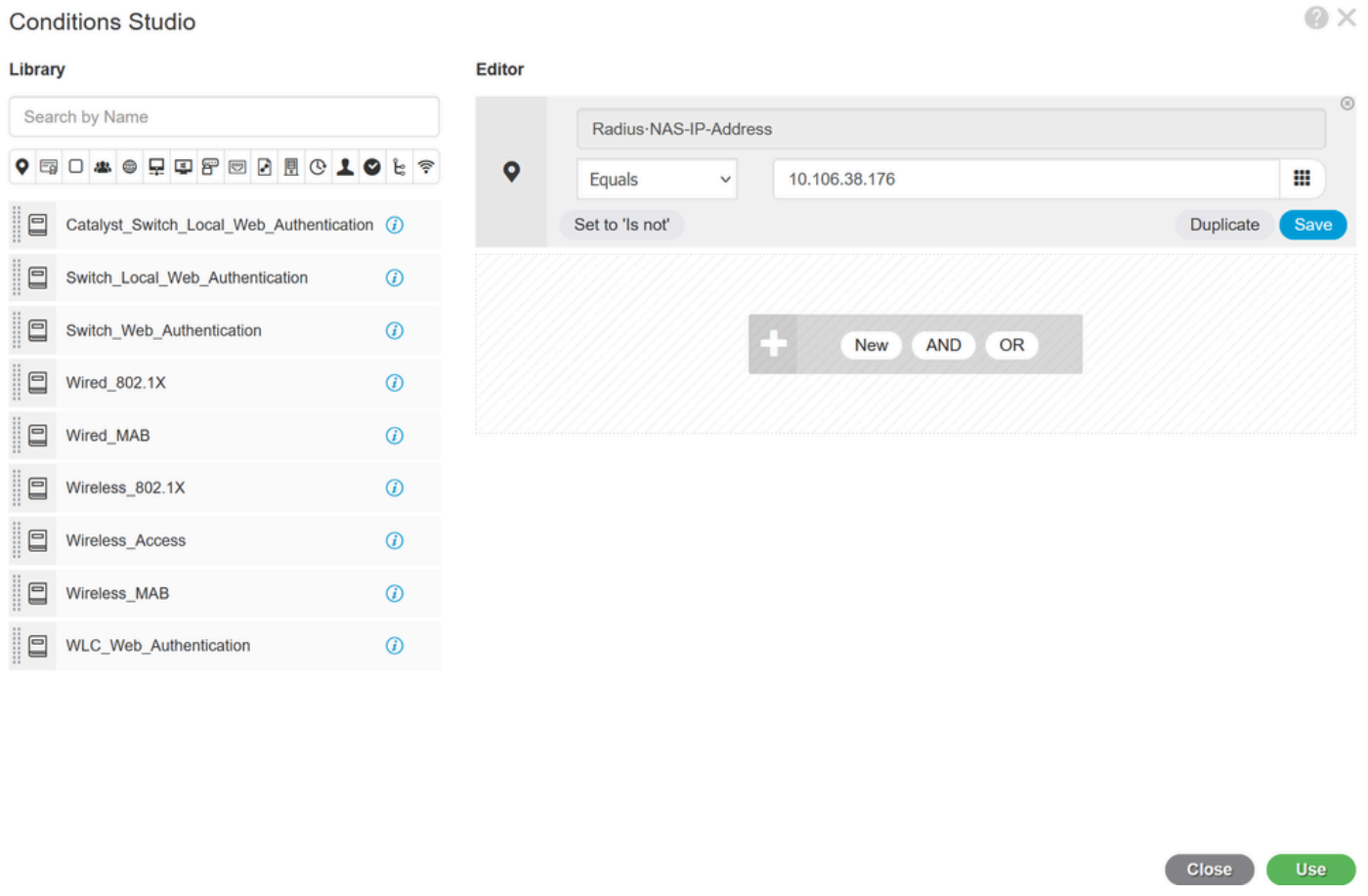


Ajouter un jeu de stratégies dans ISE

Étape 8.1. Une nouvelle ligne est placée en haut de vos ensembles de stratégies.

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

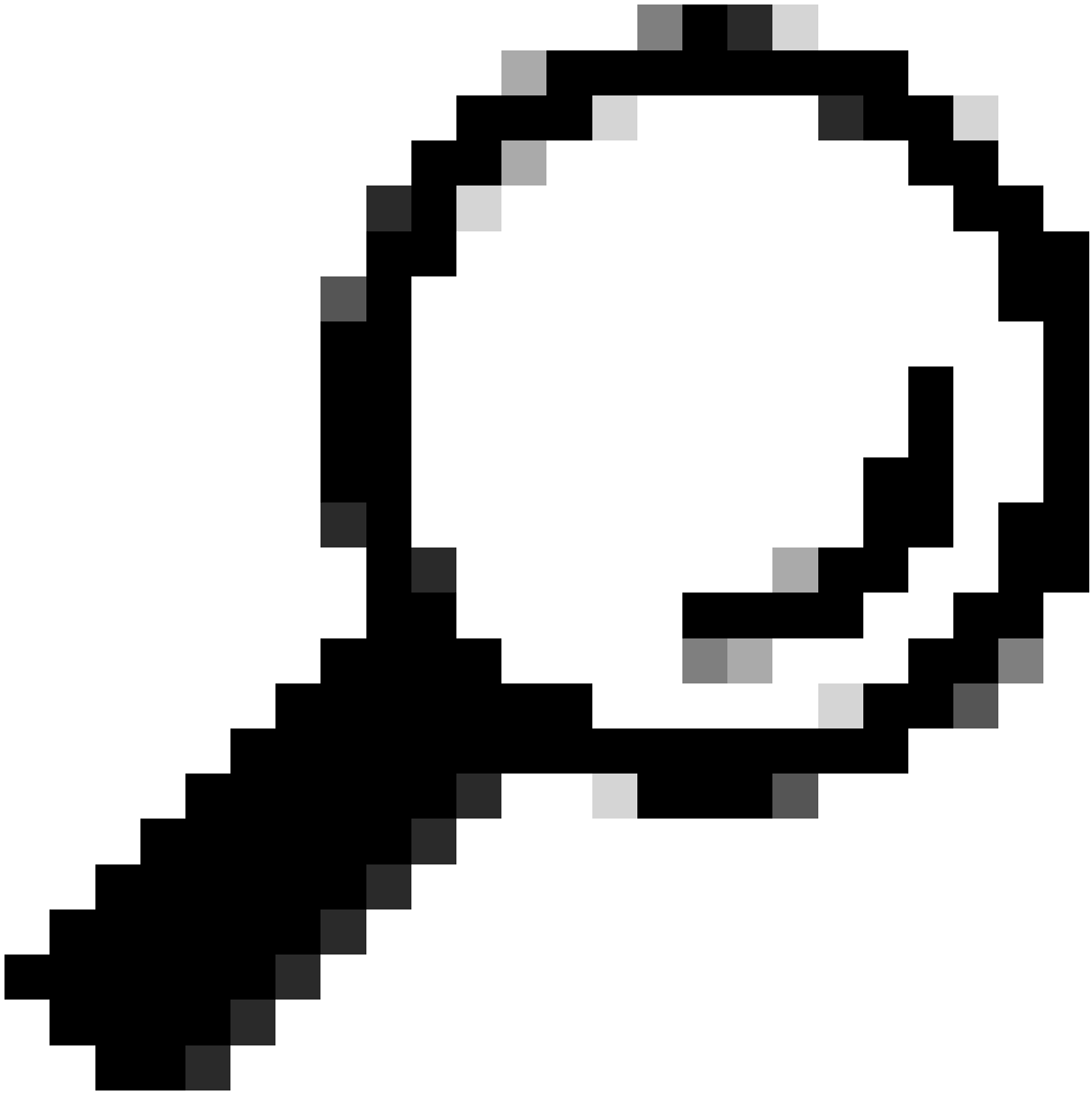
Cliquez sur Utiliser pour conserver les modifications et quitter l'éditeur.



Ajouter une stratégie pour mapper un périphérique réseau SWA

Étape 8.2. Cliquez sur Save.

Enregistrer la stratégie



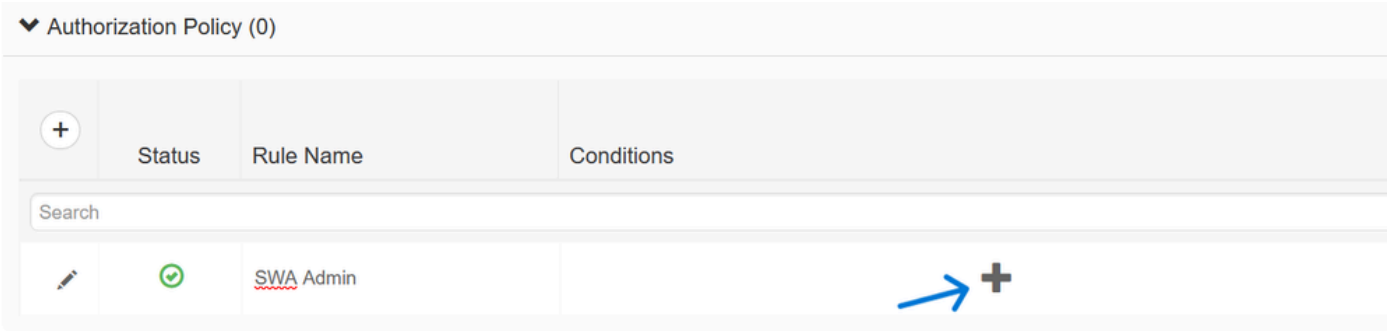
Conseil : dans cet article, la liste des protocoles d'accès réseau par défaut est autorisée. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.

Étape 9. Pour afficher les nouveaux ensembles de stratégies, cliquez sur l'icône > dans la colonne View. Développez le menu Politique d'autorisation et cliquez sur l'icône + pour ajouter une

nouvelle règle permettant l'accès à l'utilisateur disposant de droits d'administrateur.

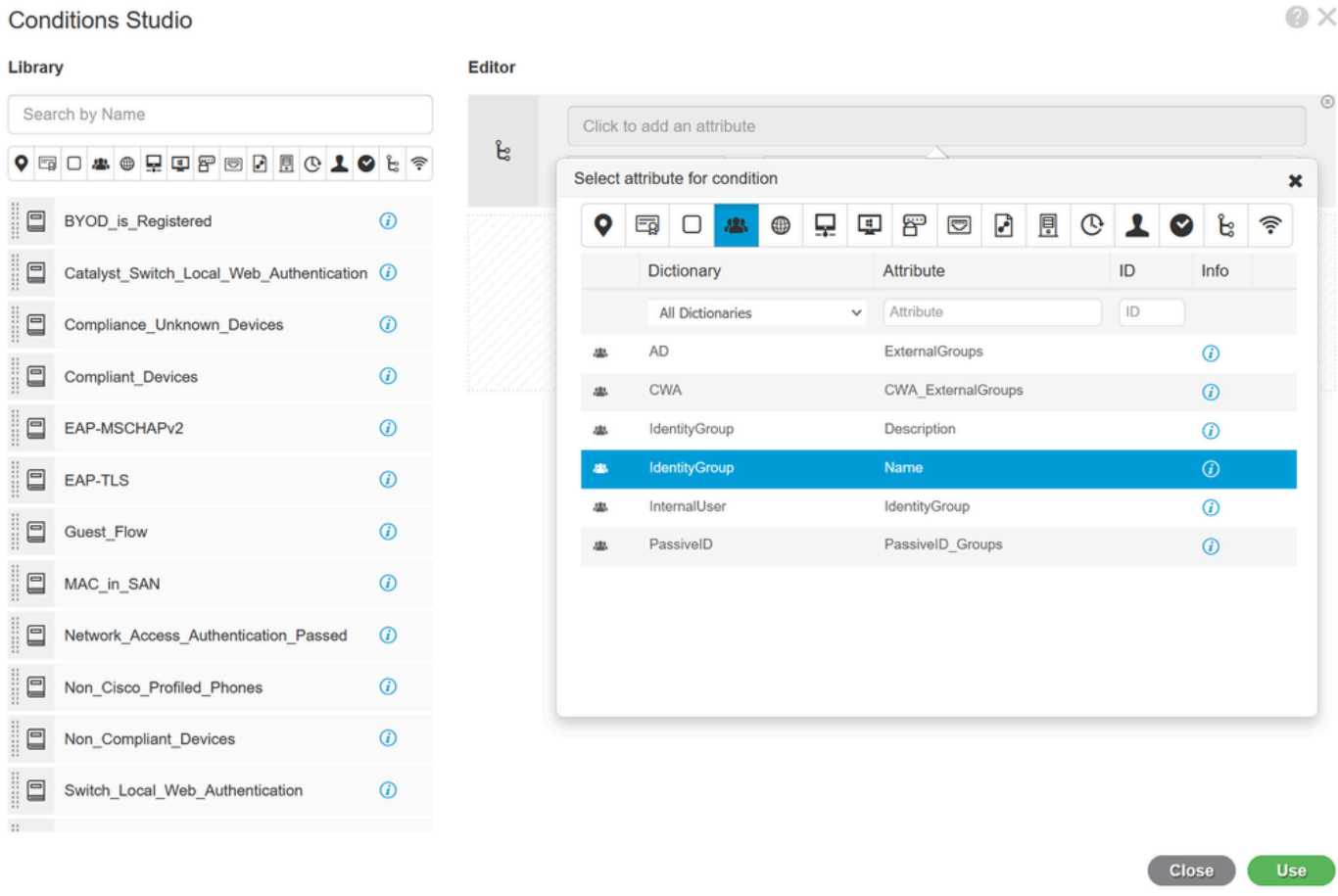
Définissez un nom.

Étape 9.1. Pour créer une condition correspondant au groupe d'utilisateurs Admin, cliquez sur l'icône +.



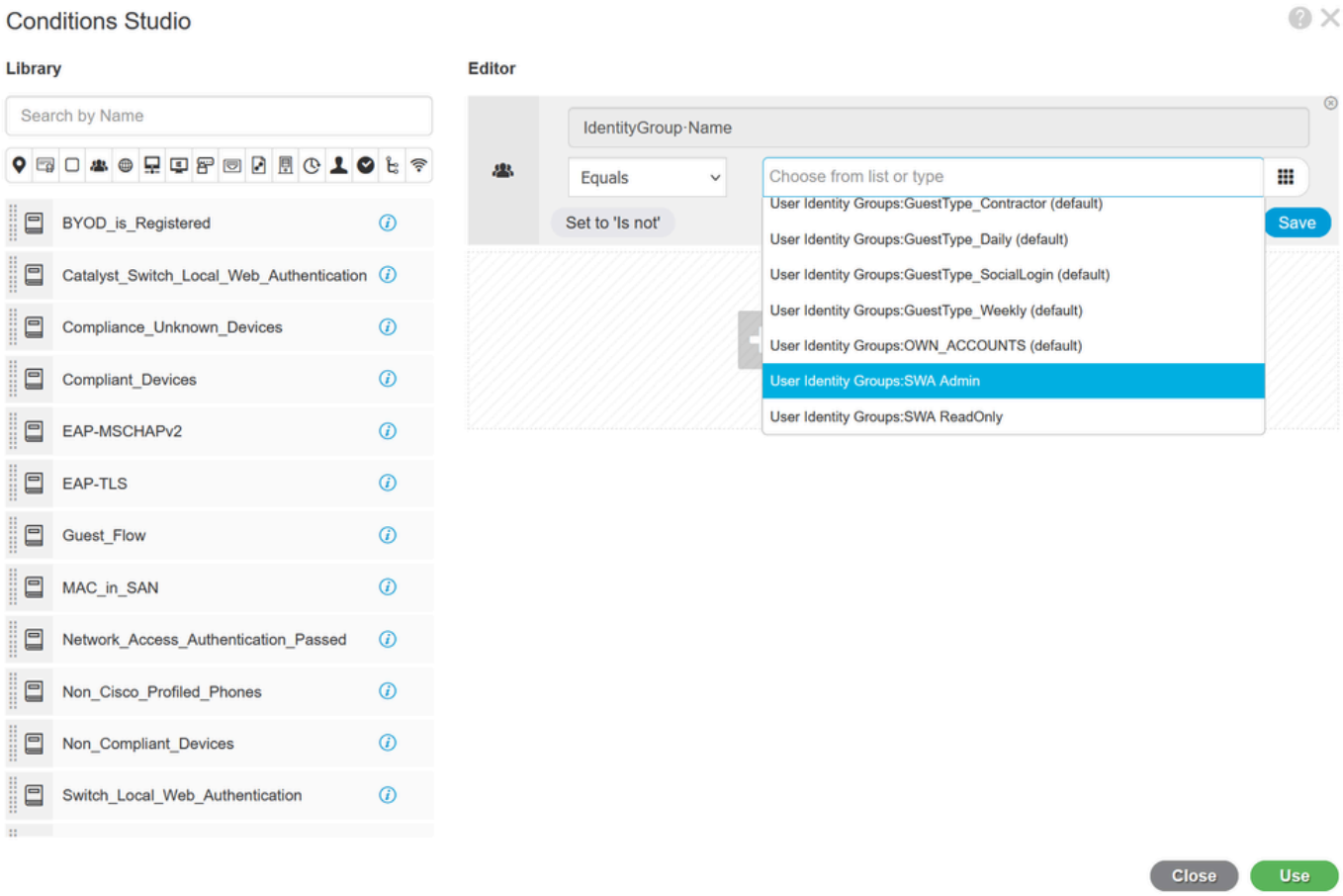
Ajouter une condition de stratégie d'autorisation

Étape 9.2. Définissez les conditions pour faire correspondre le groupe d'identités de dictionnaire avec le groupe d'identités Attribute Name Equals User Identity Groups : SWA admin.



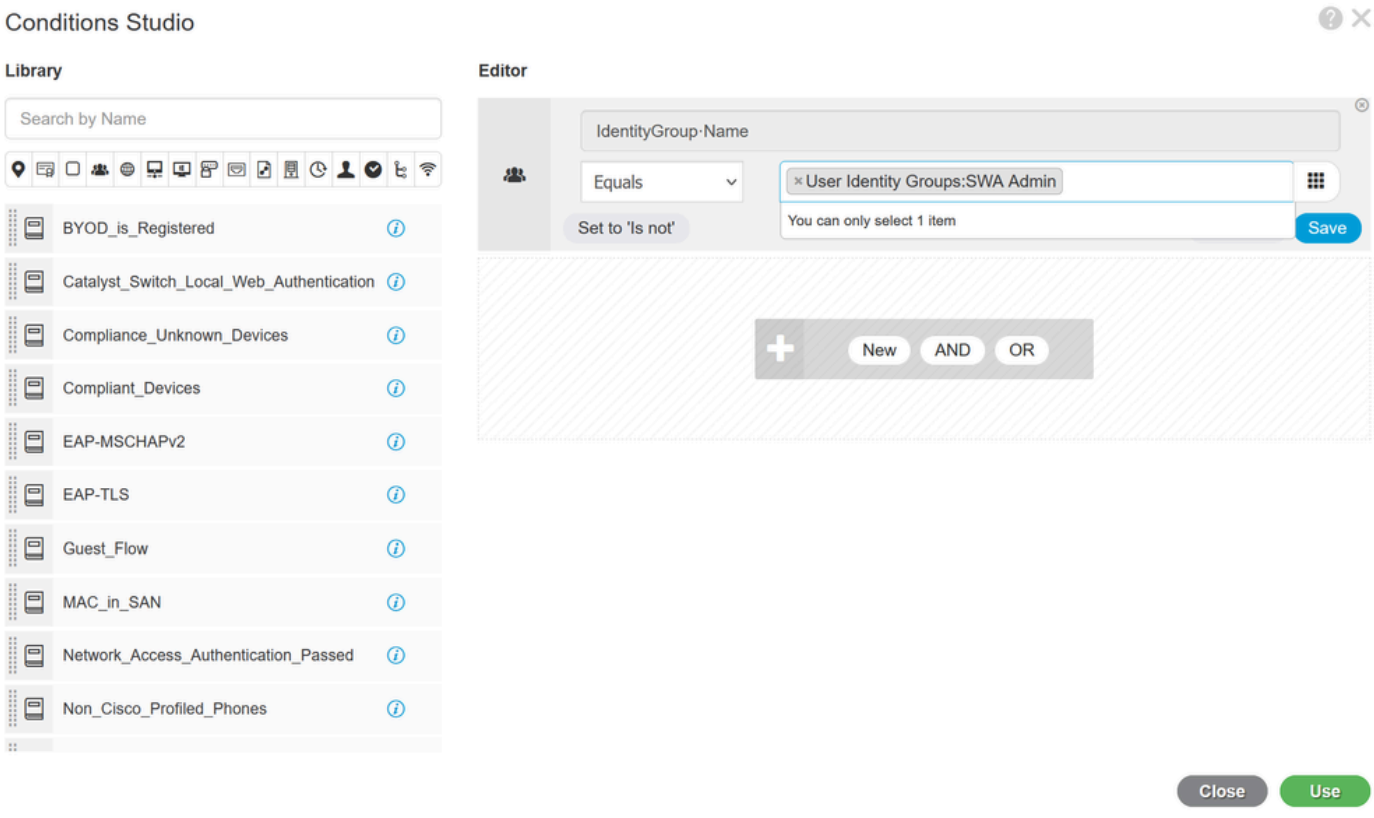
Sélectionnez Identity Group comme condition

Étape 9.3. Faites défiler vers le bas et sélectionnez User Identity Groups : SWA admin.



Faites défiler vers le bas et sélectionnez Identity Group Name

Étape 9.4. Cliquez sur Utiliser.

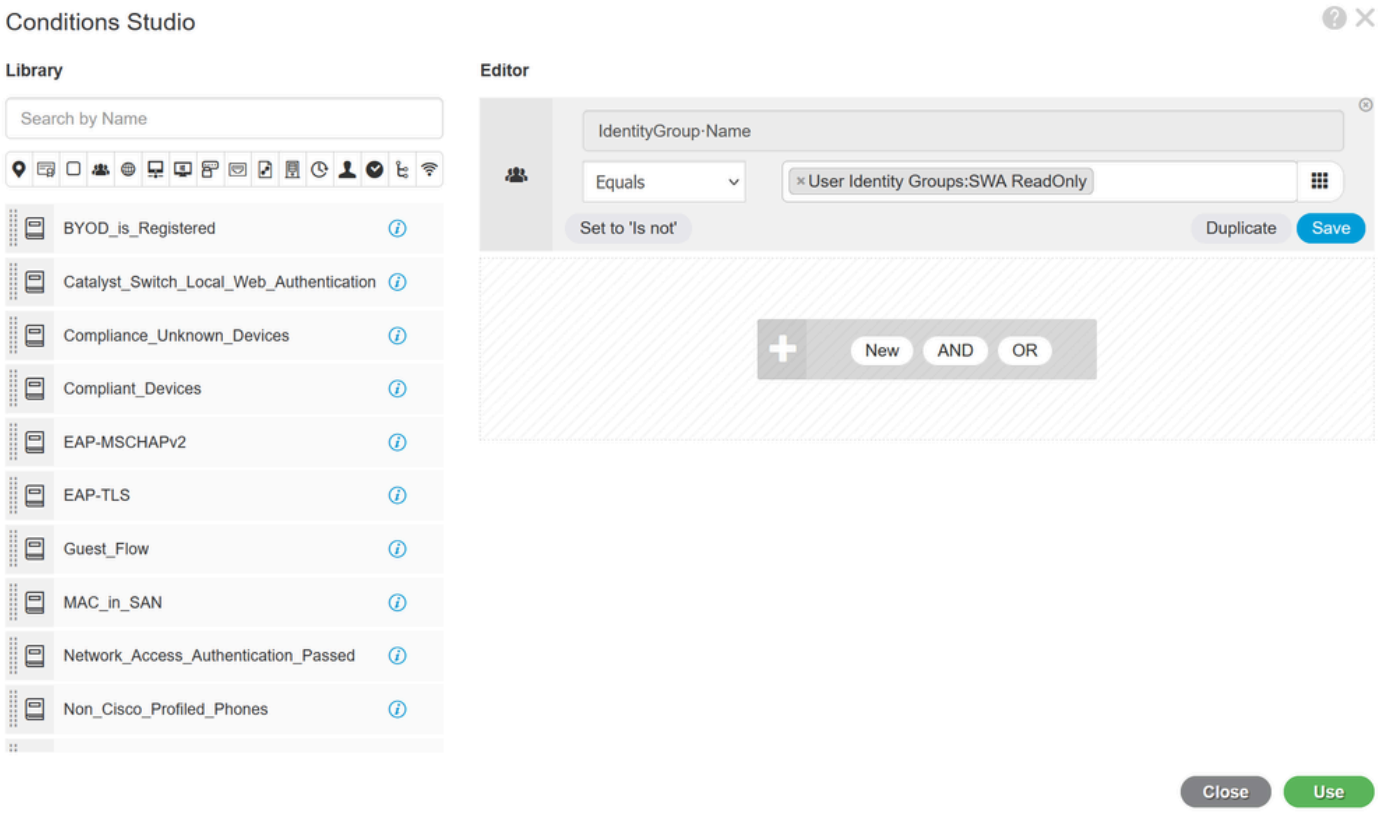


Sélectionner la stratégie d'autorisation pour le groupe d'utilisateurs Admin SWA

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

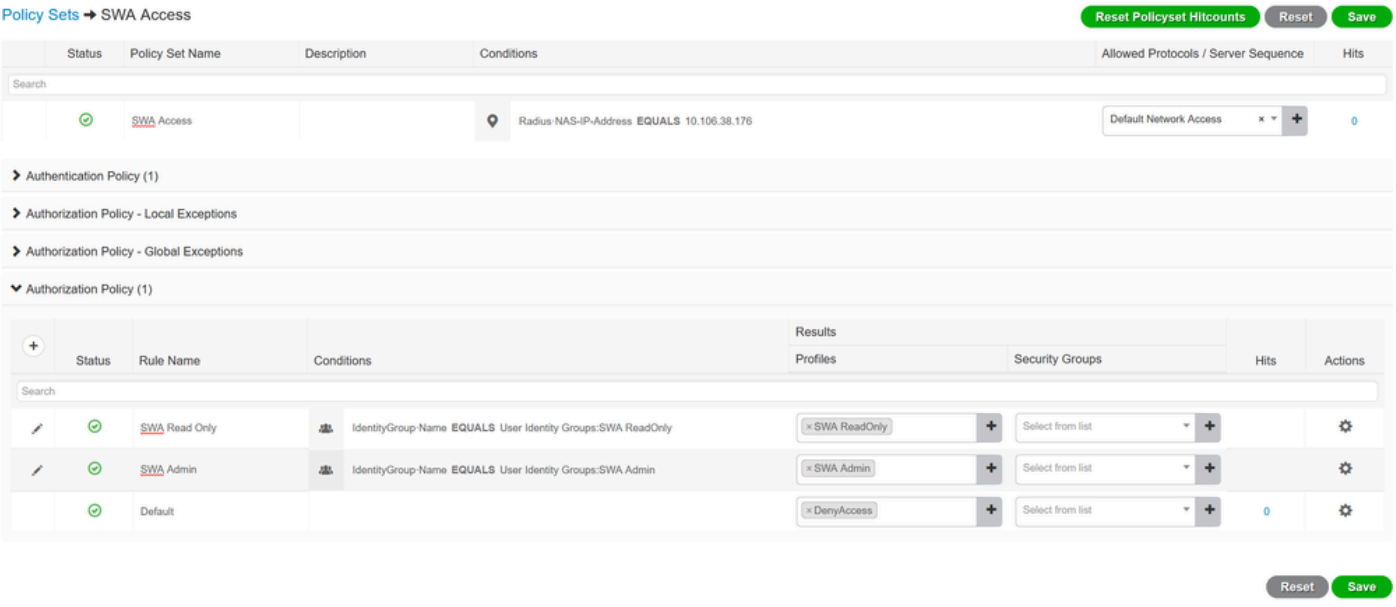
Définissez un nom.

Définissez les conditions pour faire correspondre le groupe d'identités de dictionnaire avec le groupe d'identités Attribute Name Equals User Identity Groups : SWA ReadOnly et cliquez sur Use.



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

Étape 11. Définissez le profil d'autorisation pour chaque règle, puis cliquez sur Enregistrer.

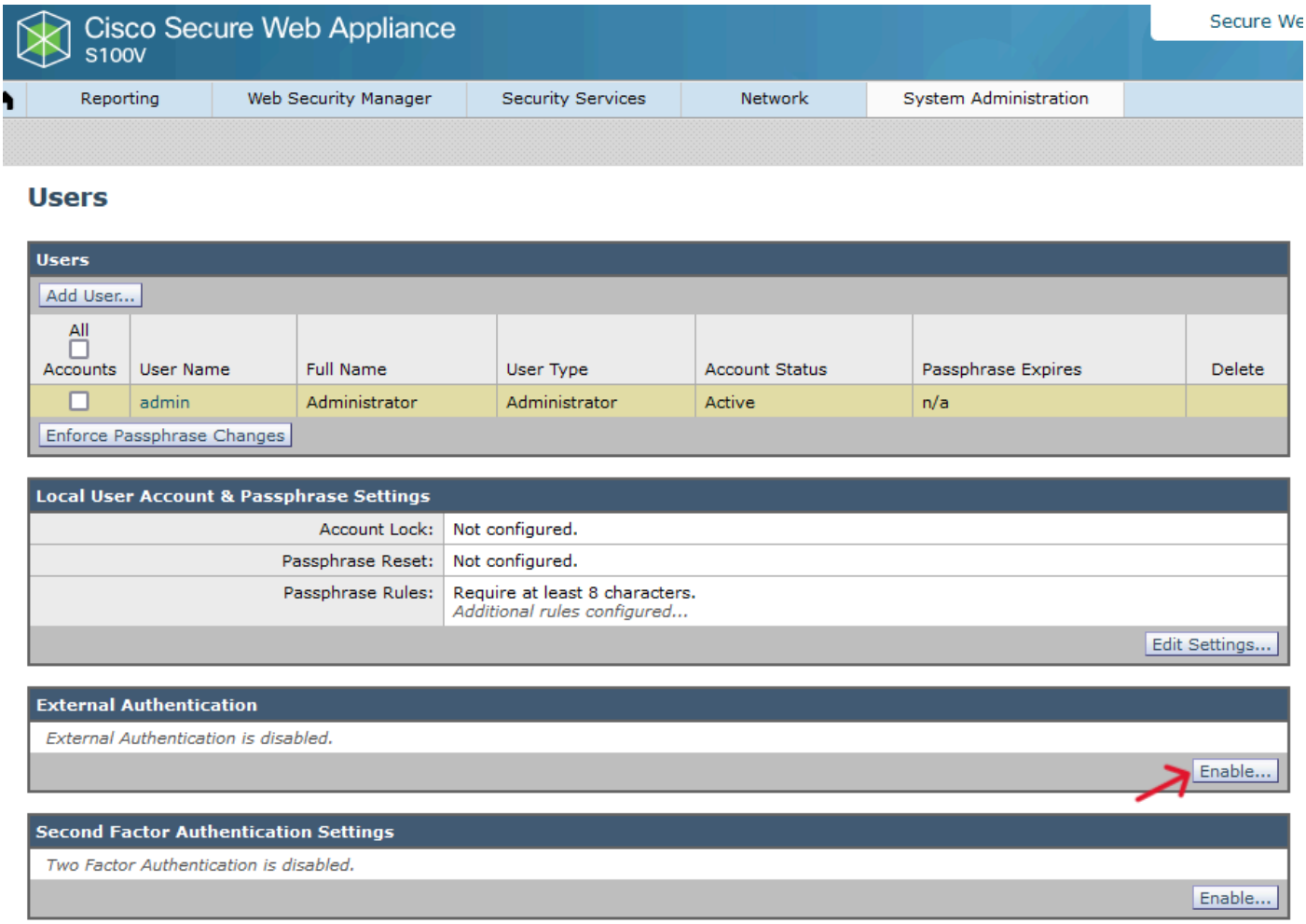


Sélectionner le profil d'autorisation

Configuration SWA

Étape 1. Dans l'interface utilisateur graphique de SWA, accédez à Administration système et cliquez sur Users.

Étape 2. Cliquez sur Enable dans External Authentication.



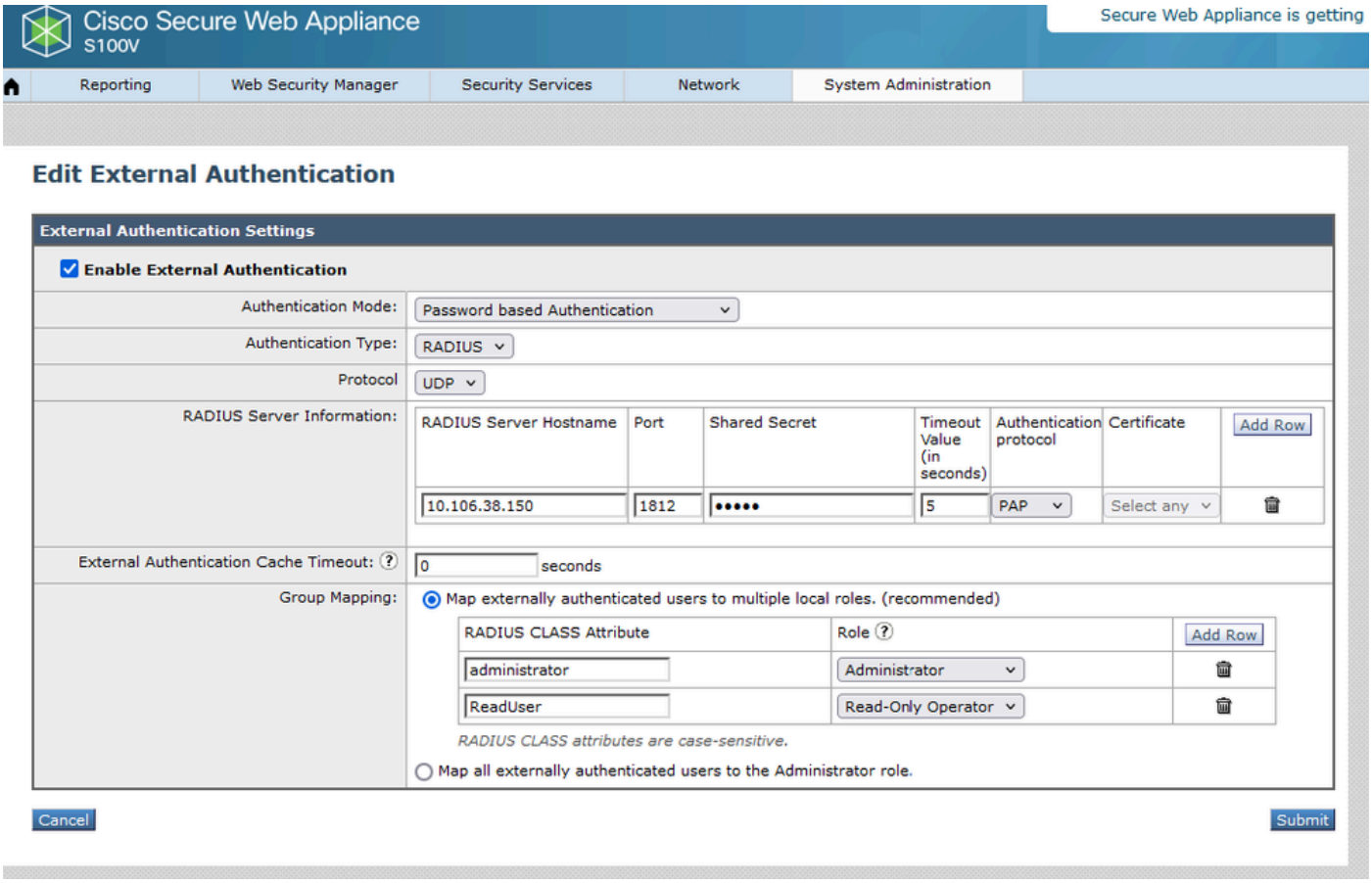
Activer l'authentification externe dans SWA

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

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

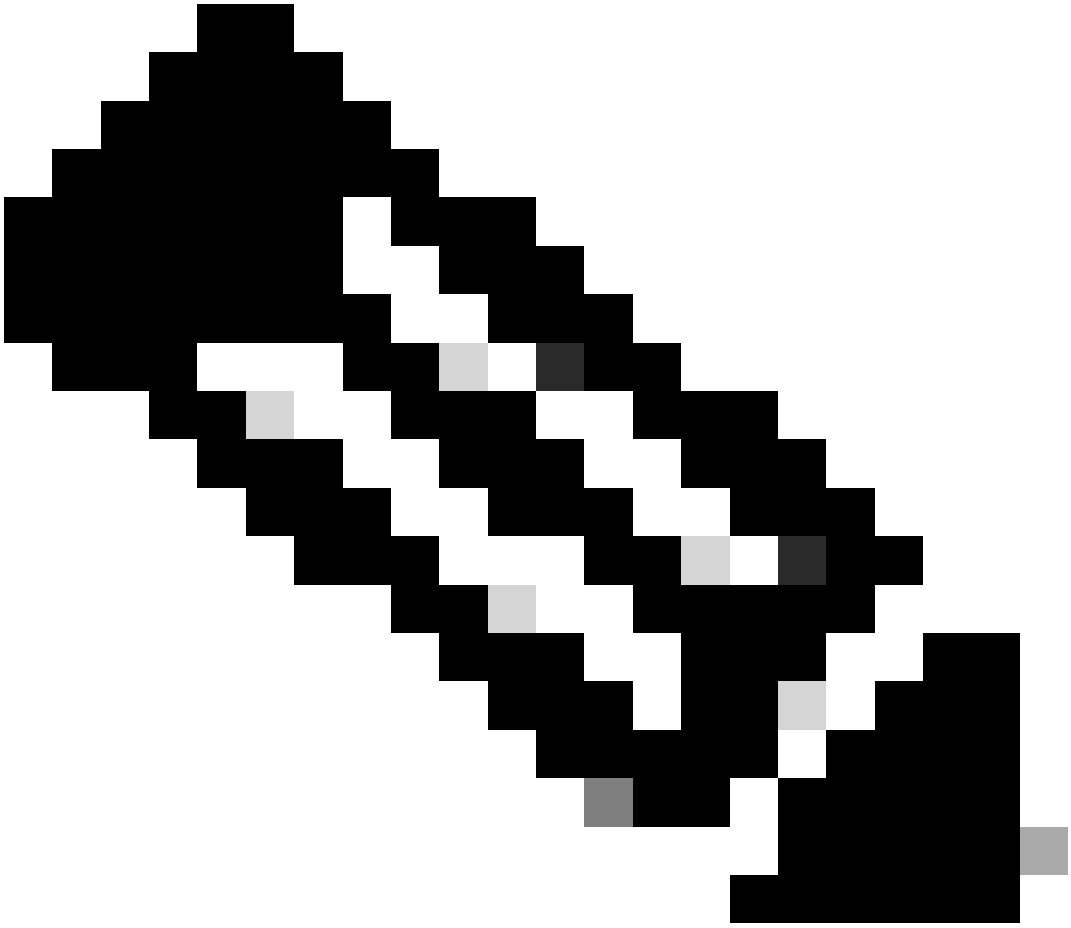
Étape 4.1. Saisissez Administrator dans le champ RADIUS CLASS Attribute et sélectionnez Role Administrator.

Étape 4.2. Saisissez ReadUser dans le champ RADIUS CLASS Attribute et sélectionnez Role Read-Only Operator.



Configuration de l'authentification externe pour le serveur RADIUS

Étape 5 : pour configurer les utilisateurs dans SWA, cliquez sur Add User. Entrez User Name et sélectionnez User Type requis pour le rôle souhaité. Entrez Passphrase et Retype Passphrase, qui est requis pour l'accès à l'interface utilisateur graphique 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.

Users

Users

Add User...

** When RADIUS external authentication is enabled, all local user accounts except "admin" are disabled. If all RADIUS services fail, local user accounts will be used for authentication.*

All Accounts	User Name	Full Name	User Type*	Account Status	Passphrase Expires	Delete
☐	adminuser	Admin User	*Administrator*	Active	n/a	🗑
☐	rouser	RO User	*Read-Only Operator*	Active	n/a	🗑

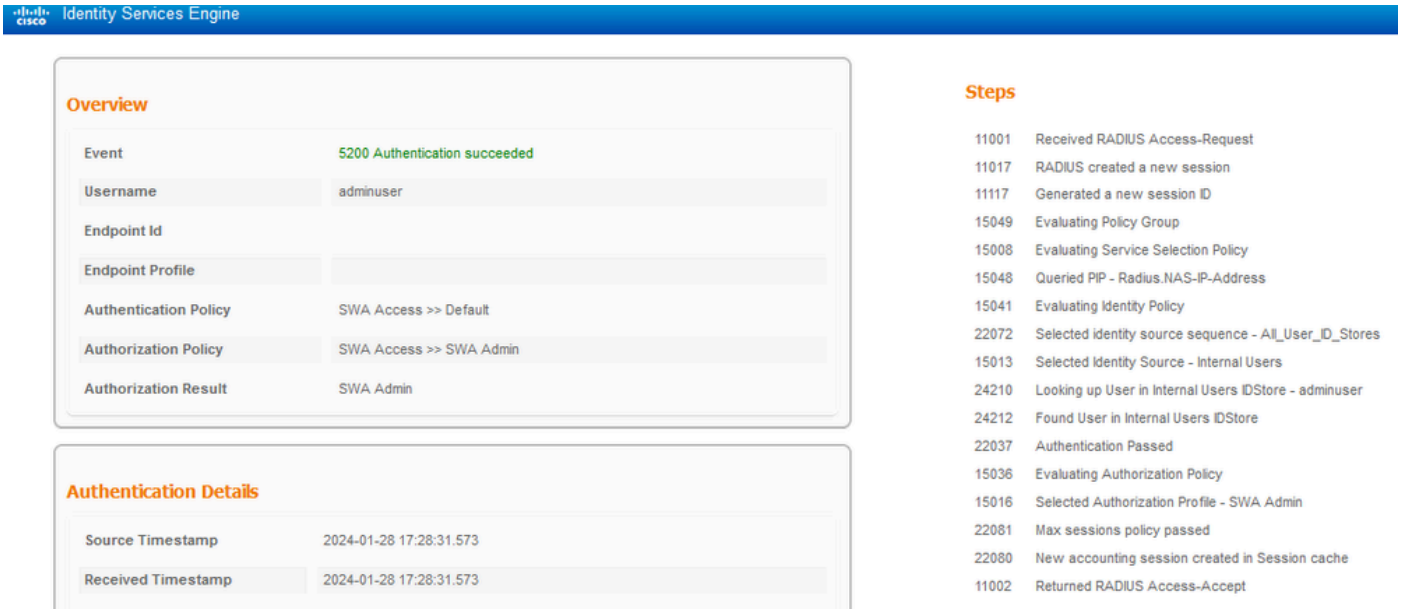
Configuration utilisateur dans SWA

Étape 6 : cliquez sur Submit and Commit Changes.

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

Informations connexes

- 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.