Configurer l'authentification SWA à facteur 2 avec ISE en tant que serveur RADIUS

Table des matières

Introduction

Ce document décrit comment configurer l'authentification de second facteur sur l'appareil Web sécurisé avec Cisco Identity Service Engine comme serveur RADIUS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base en SWA.
- 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 de l'appliance Web sécurisée (SWA) et du moteur Cisco Identity Service Engine (ISE).
- Votre ISE est intégré à Active Directory ou LDAP.
- Active Directory ou LDAP est configuré avec un nom d'utilisateur « admin » pour authentifier le compte « admin » par défaut de SWA.
- 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 par le second facteur pour les utilisateurs administratifs sur SWA, le périphérique vérifie les informations d'identification de l'utilisateur avec le serveur RADIUS pour la seconde fois après avoir vérifié les informations d'identification configurées dans SWA.

Topologie du réseau

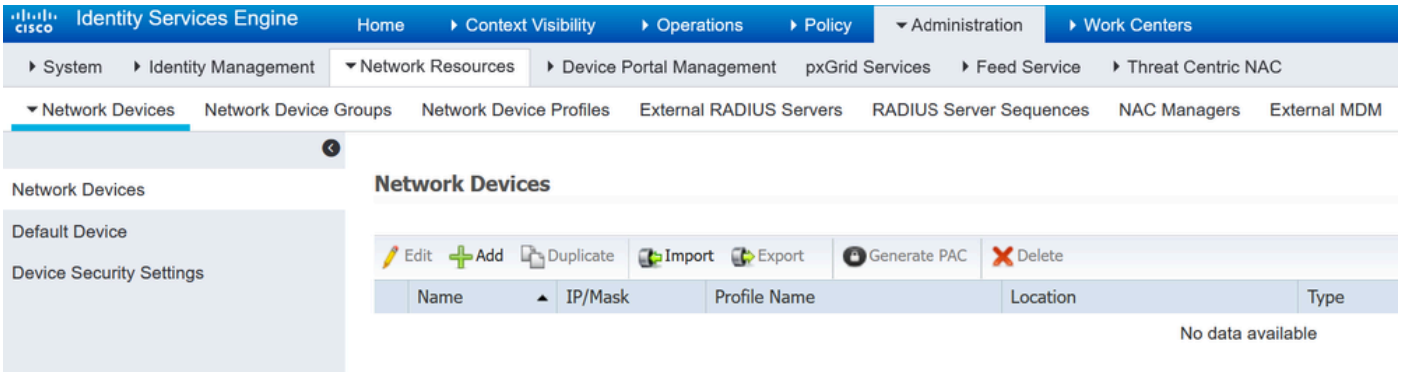
Image - Schéma de topologie du réseau

Les utilisateurs administratifs accèdent à SWA sur le port 443 avec leurs informations d'identification. SWA vérifie les informations d'identification auprès du serveur RADIUS pour l'authentification du second facteur.

Configuration Steps

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

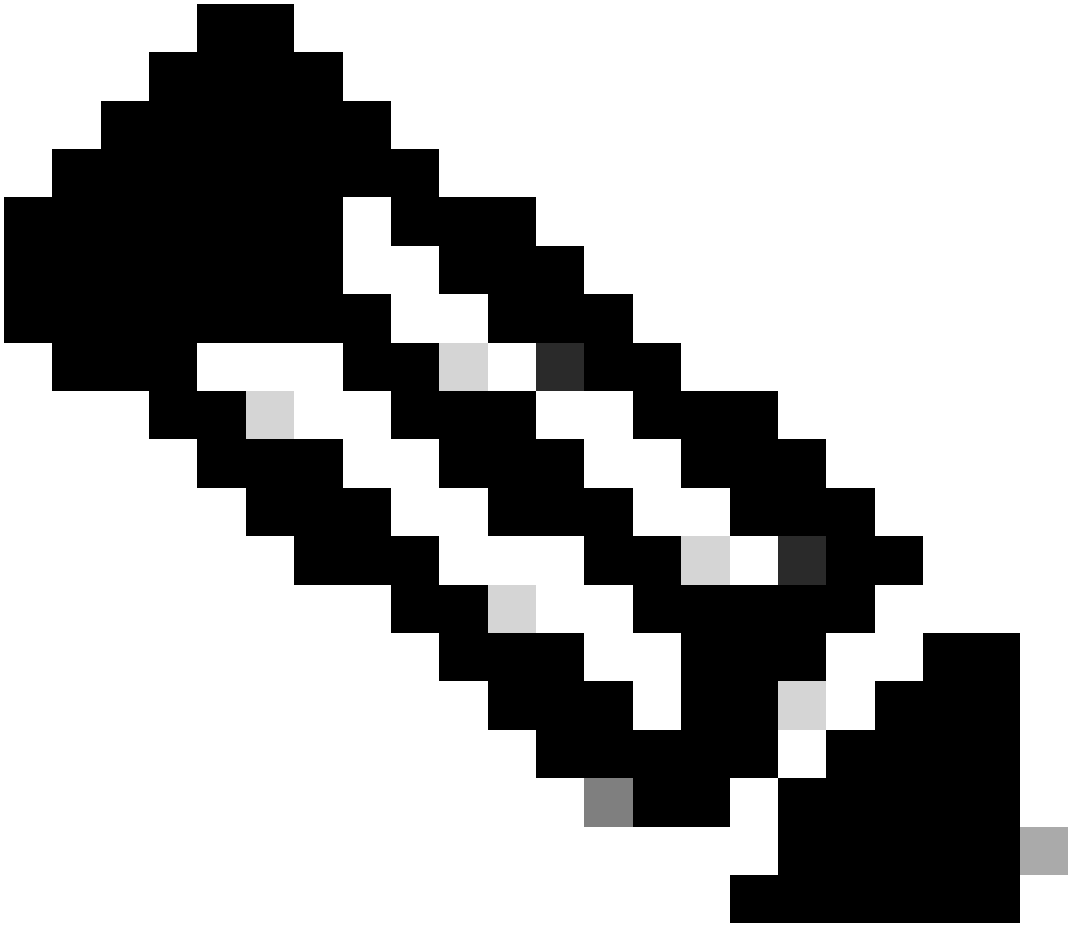
Étape 2. Configurez le périphérique réseau dans ISE.

Étape 2.1. Attribuez un nom à l'objet périphérique réseau.

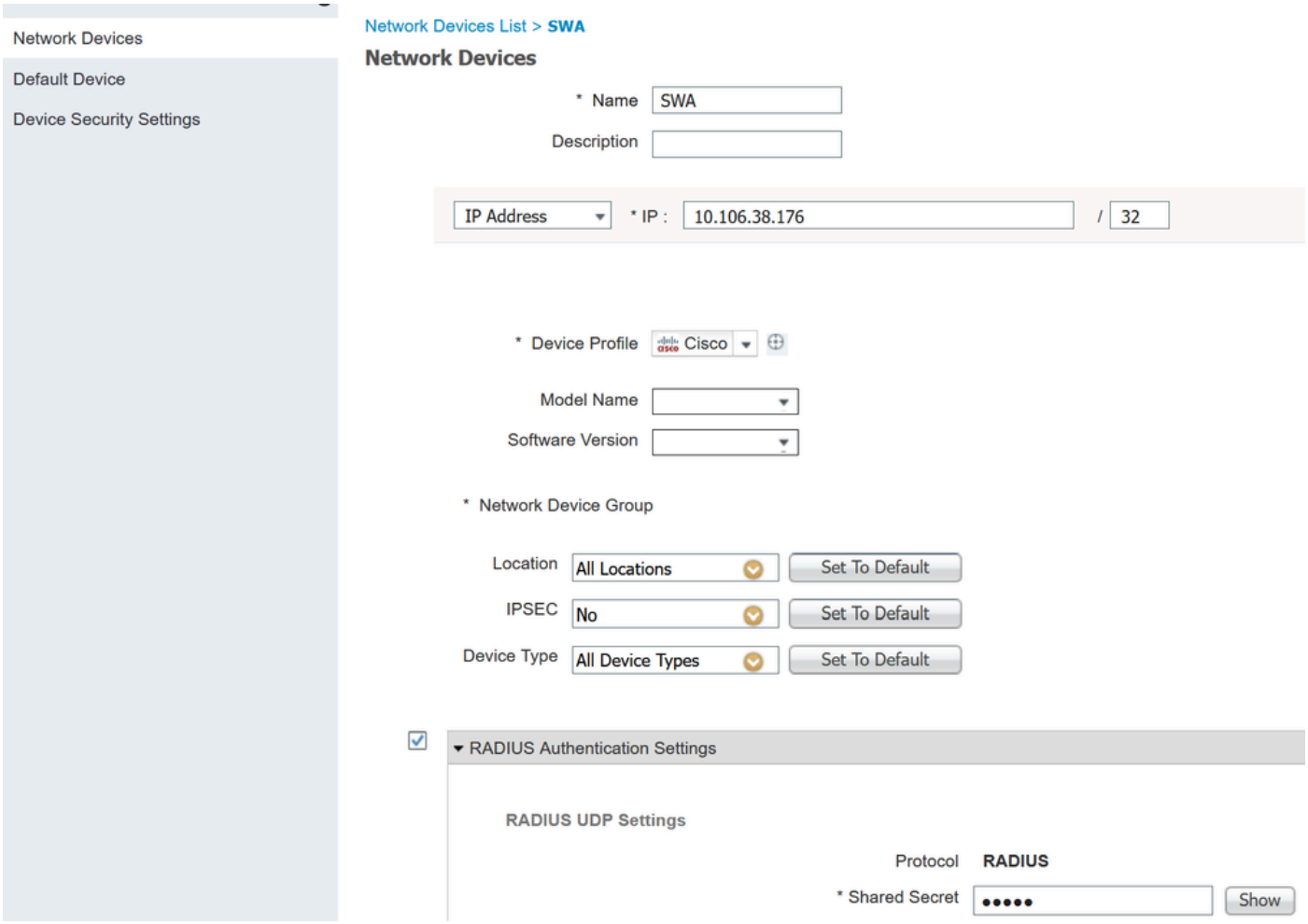
Étape 2.2. Insérez l'adresse IP SWA.

Étape 2.3. Cochez la case RADIUS.

Étape 2.4. Définissez un secret partagé.

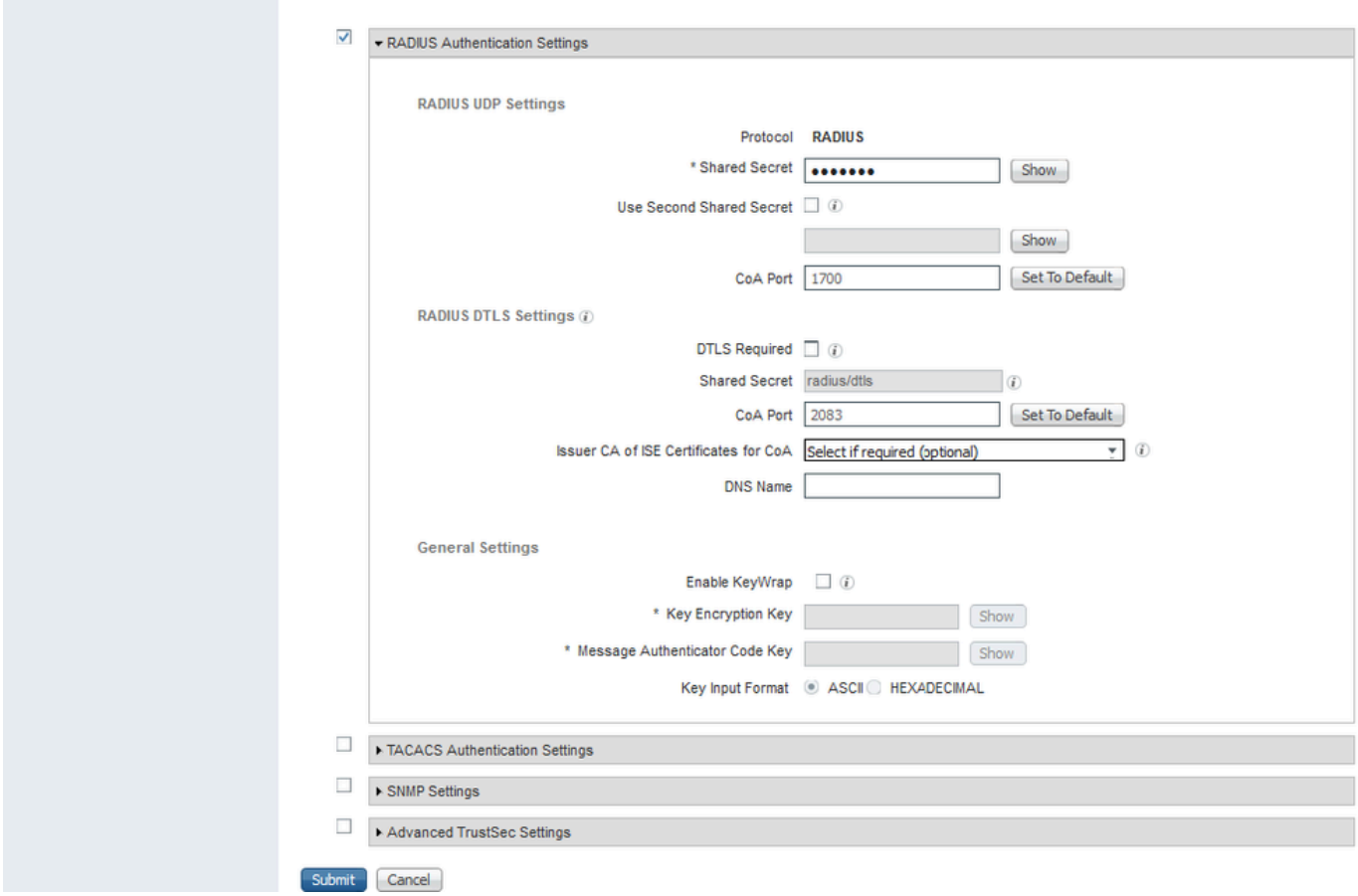


Remarque : la même clé doit être utilisée ultérieurement pour configurer le SWA.



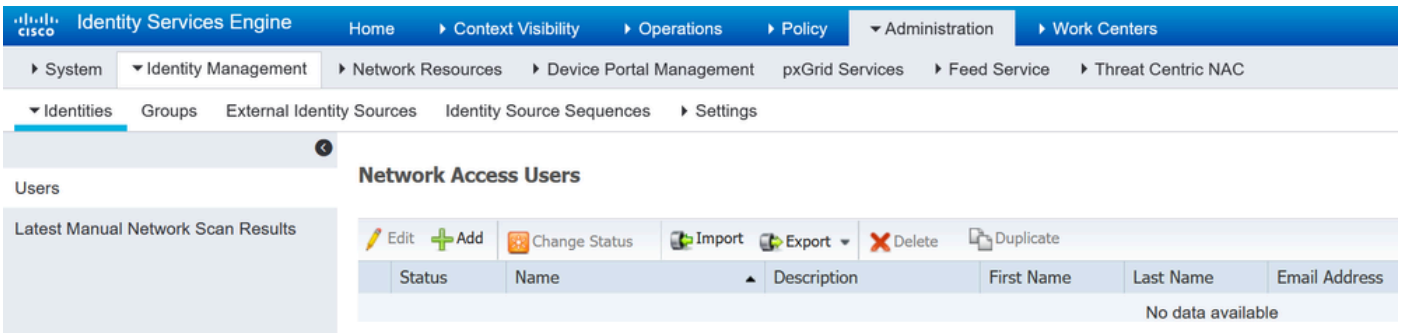
Configurer la clé partagée du périphérique réseau SWA

Étape 2.5. Cliquez sur Submit.



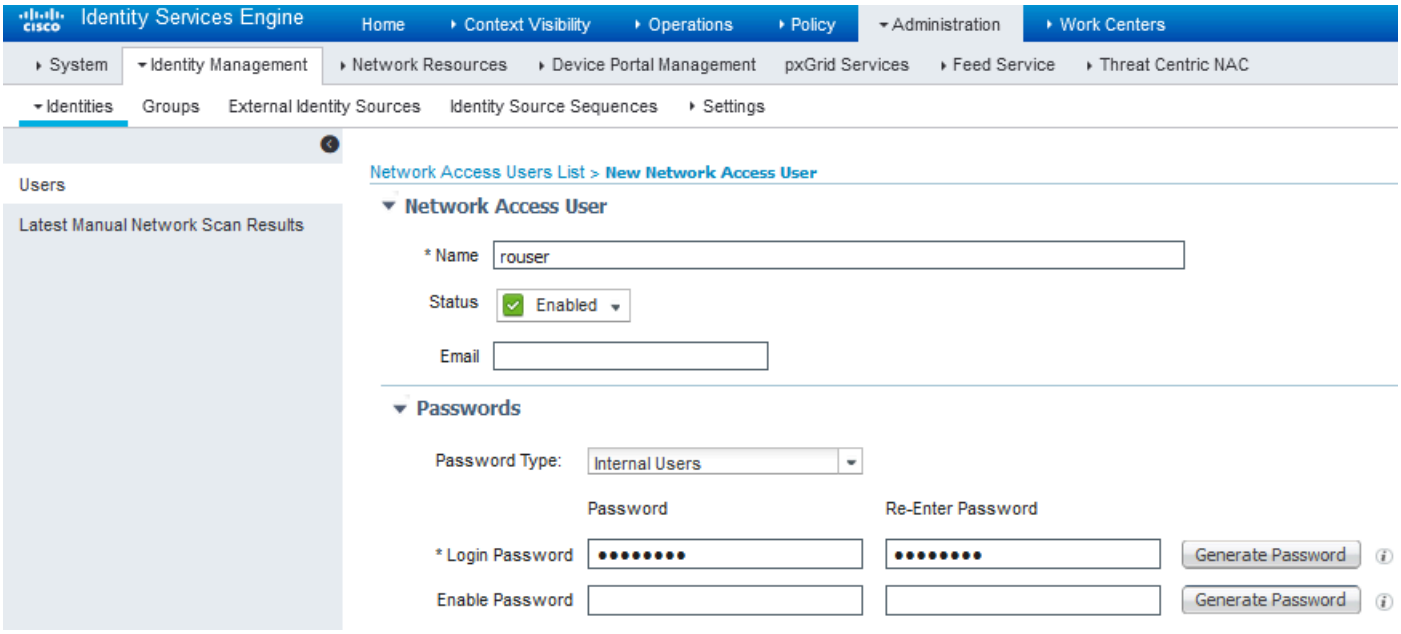
Envoyer la configuration des périphériques réseau

Étape 3. Vous devez créer des utilisateurs d'accès réseau qui correspondent au nom d'utilisateur configuré dans SWA. Accédez à Administration > Identity Management > Identities > + Add.



Ajouter des utilisateurs locaux dans ISE

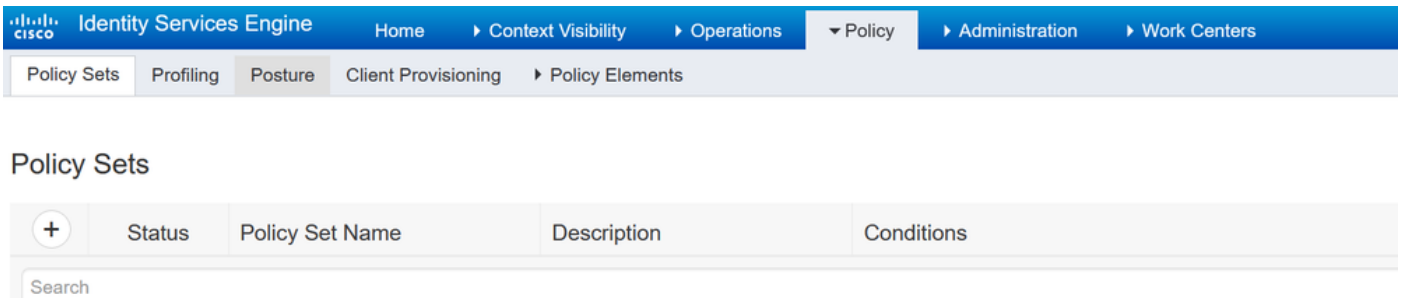
Étape 3.1. Attribuez un nom.
Étape 3.2. (Facultatif) Saisissez l'adresse e-mail de l'utilisateur.
Étape 3.3. Définir un mot de passe.
Étape 3.4. Cliquez sur Save.



Ajouter un utilisateur local dans ISE

Étape 4. Créez un ensemble de stratégies correspondant 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.

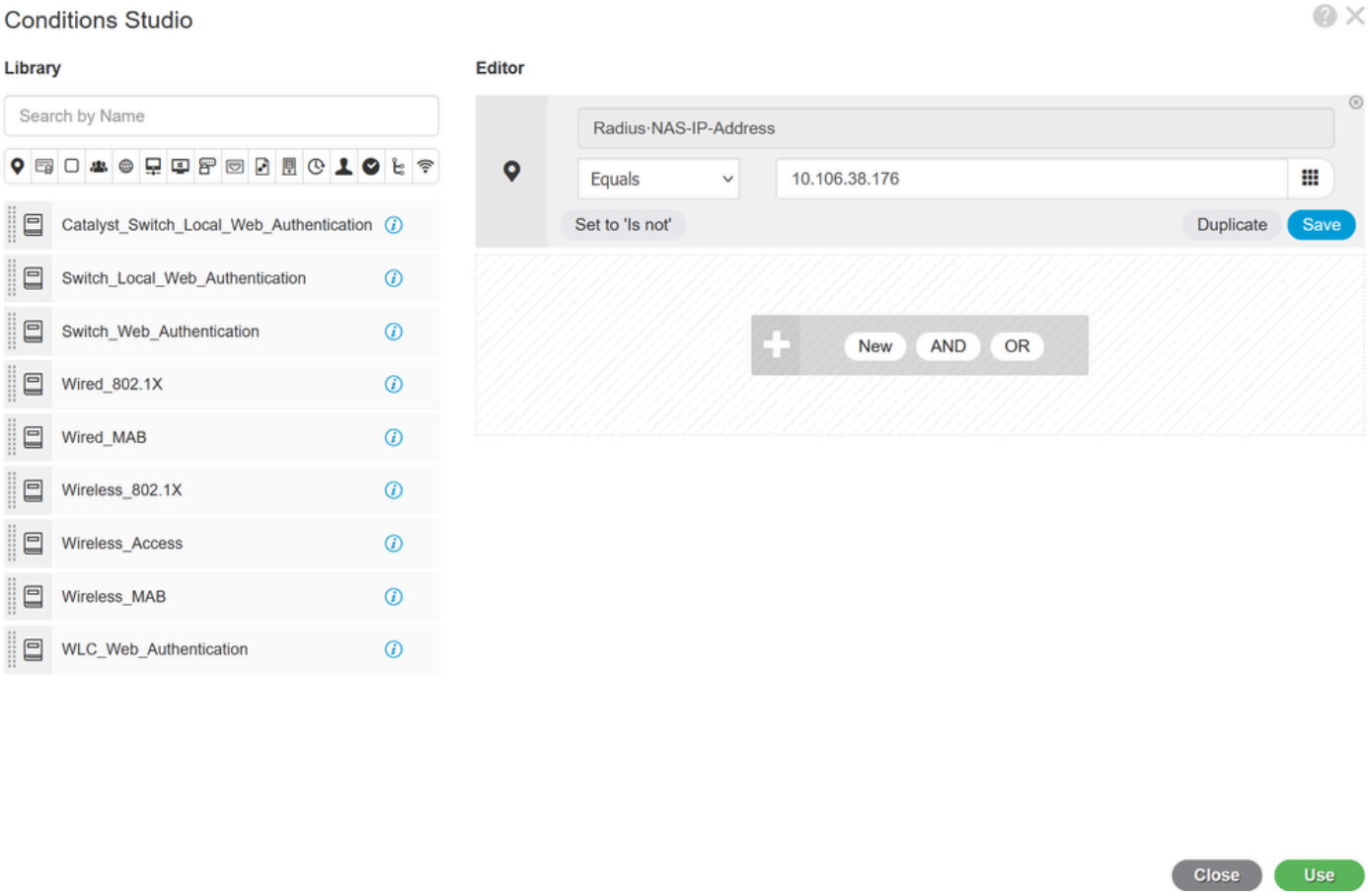


Ajouter un jeu de stratégies dans ISE

Étape 4.1. Une nouvelle ligne est placée en haut de vos ensembles de stratégies. Saisissez le nom de la nouvelle stratégie.

Étape 4.2. Ajoutez une condition pour l'attribut RADIUS NAS-IP-Address afin qu'il corresponde à l'adresse IP SWA.

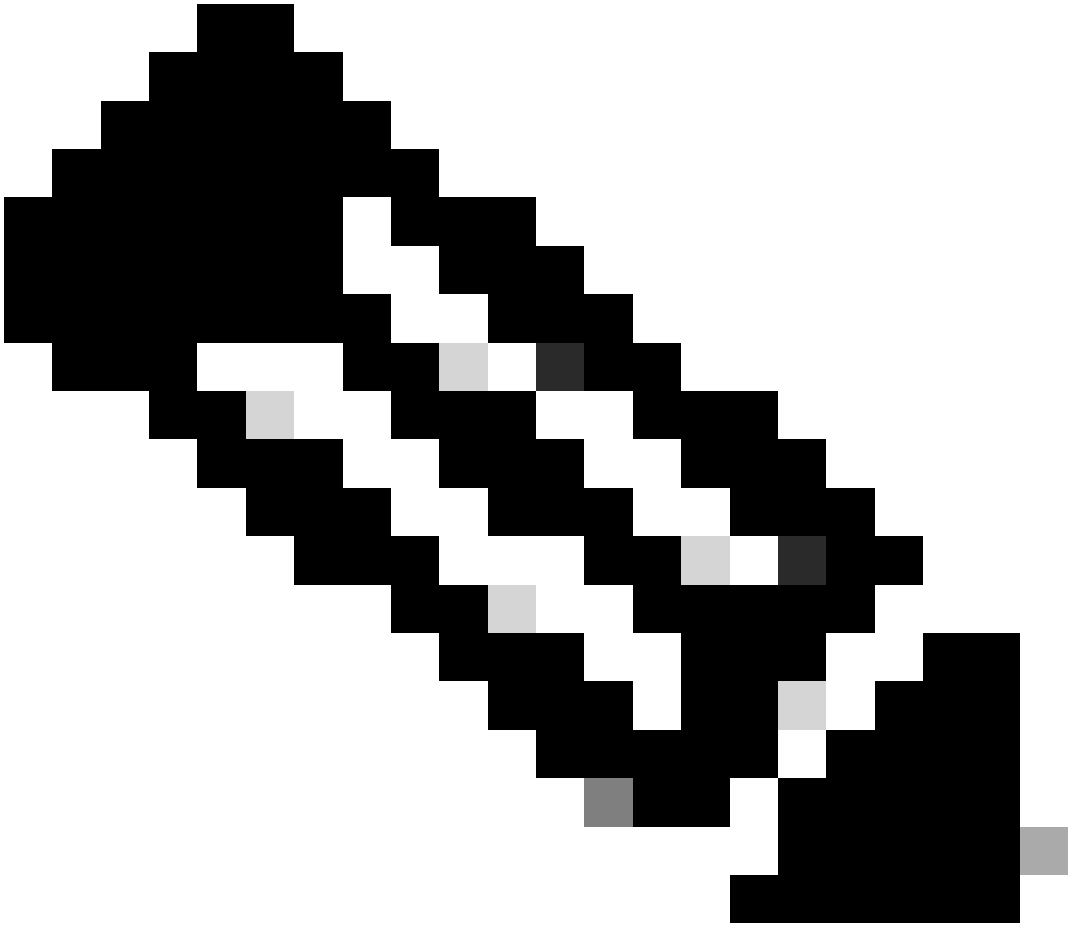
Étape 4.3. Cliquez sur Utiliser pour conserver les modifications et quitter l'éditeur.



Ajouter une stratégie pour mapper un périphérique réseau SWA

Étape 4.4. Cliquez sur Save.

Enregistrer la stratégie



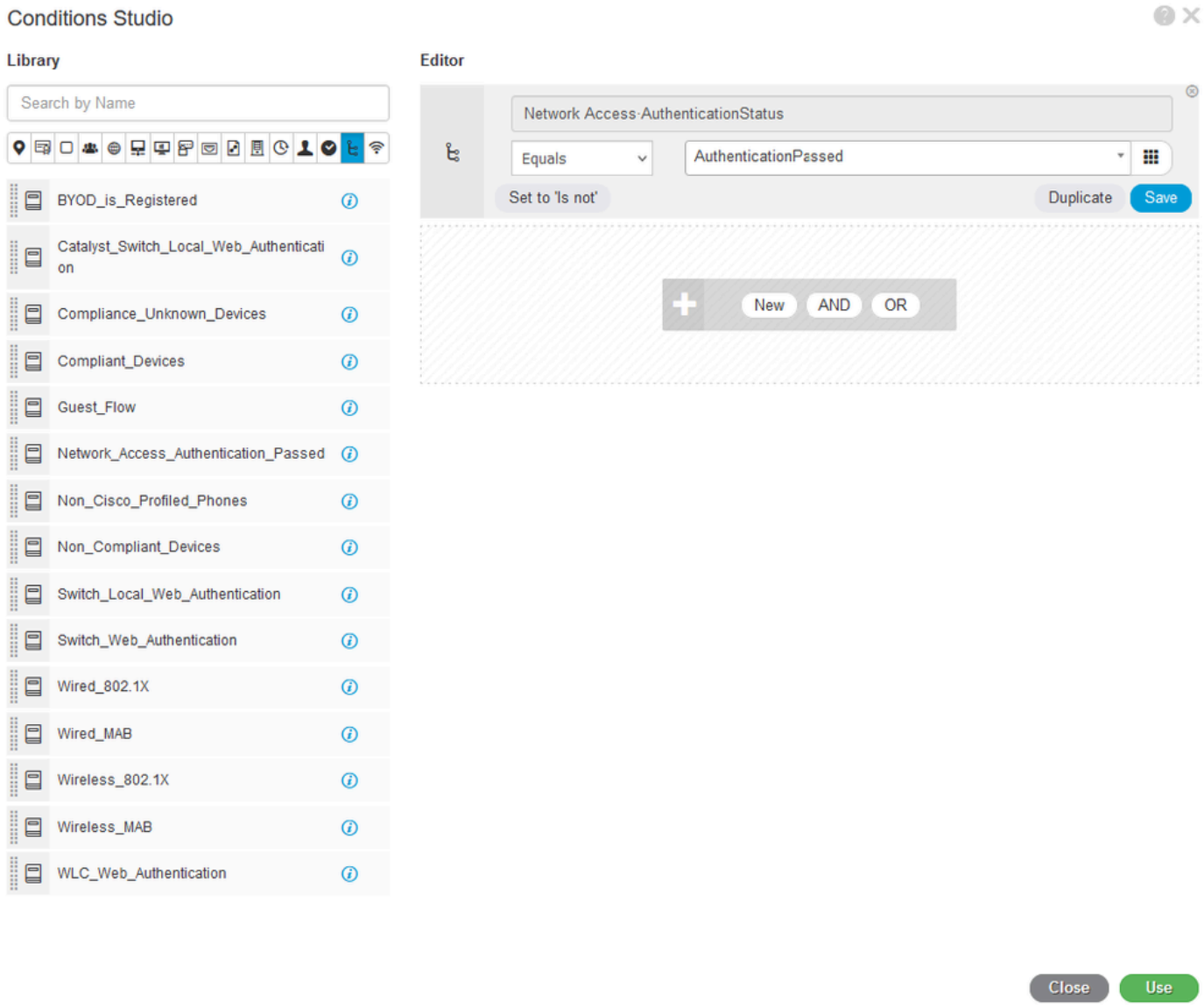
Remarque : cet exemple a autorisé la liste des protocoles d'accès réseau par défaut. Vous pouvez créer une nouvelle liste et la réduire si nécessaire.

Étape 5. Pour afficher les nouveaux ensembles de stratégies, cliquez sur l'icône ">" dans la colonne Afficher.

Étape 5.1. Développez le menu Stratégie d'autorisation et cliquez sur l'icône + pour ajouter une nouvelle règle autorisant l'accès à tous les utilisateurs authentifiés.

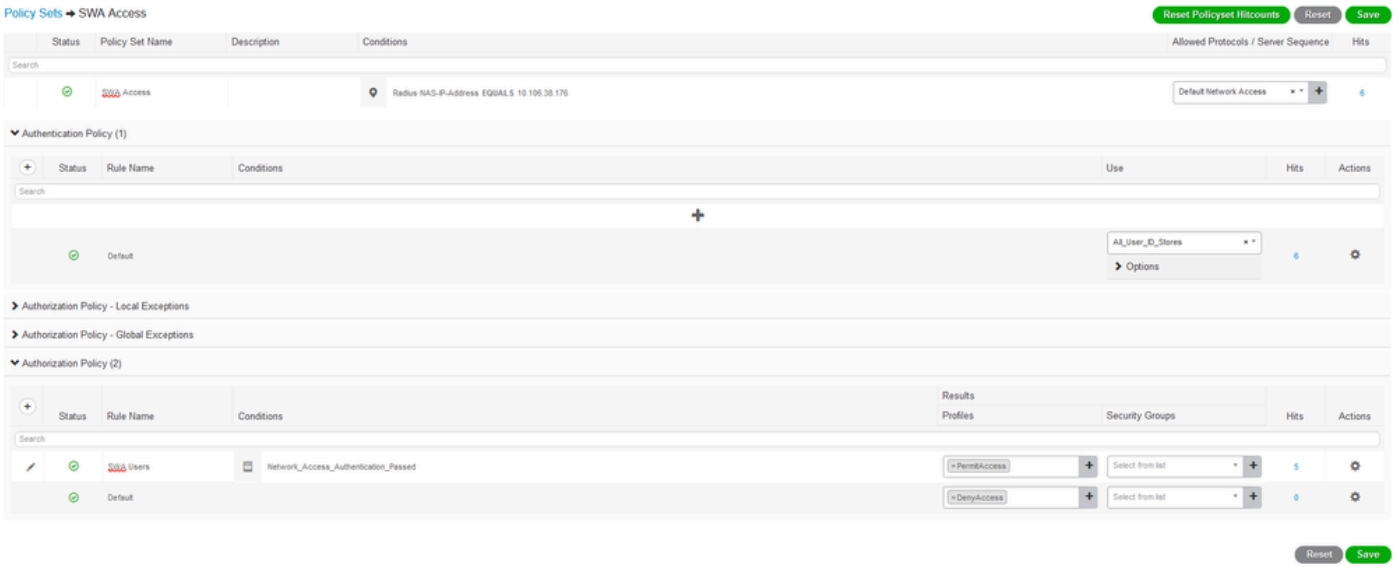
Étape 5.2. Définissez un nom.

Étape 5.3. Définissez les conditions pour faire correspondre l'accès réseau du dictionnaire avec l'attribut AuthenticationStatus est égal à AuthenticationPassed et cliquez sur Use.



Sélectionner une condition d'autorisation

Étape 6. Définissez PermitAccess comme profil d'autorisation par défaut et cliquez sur Save.

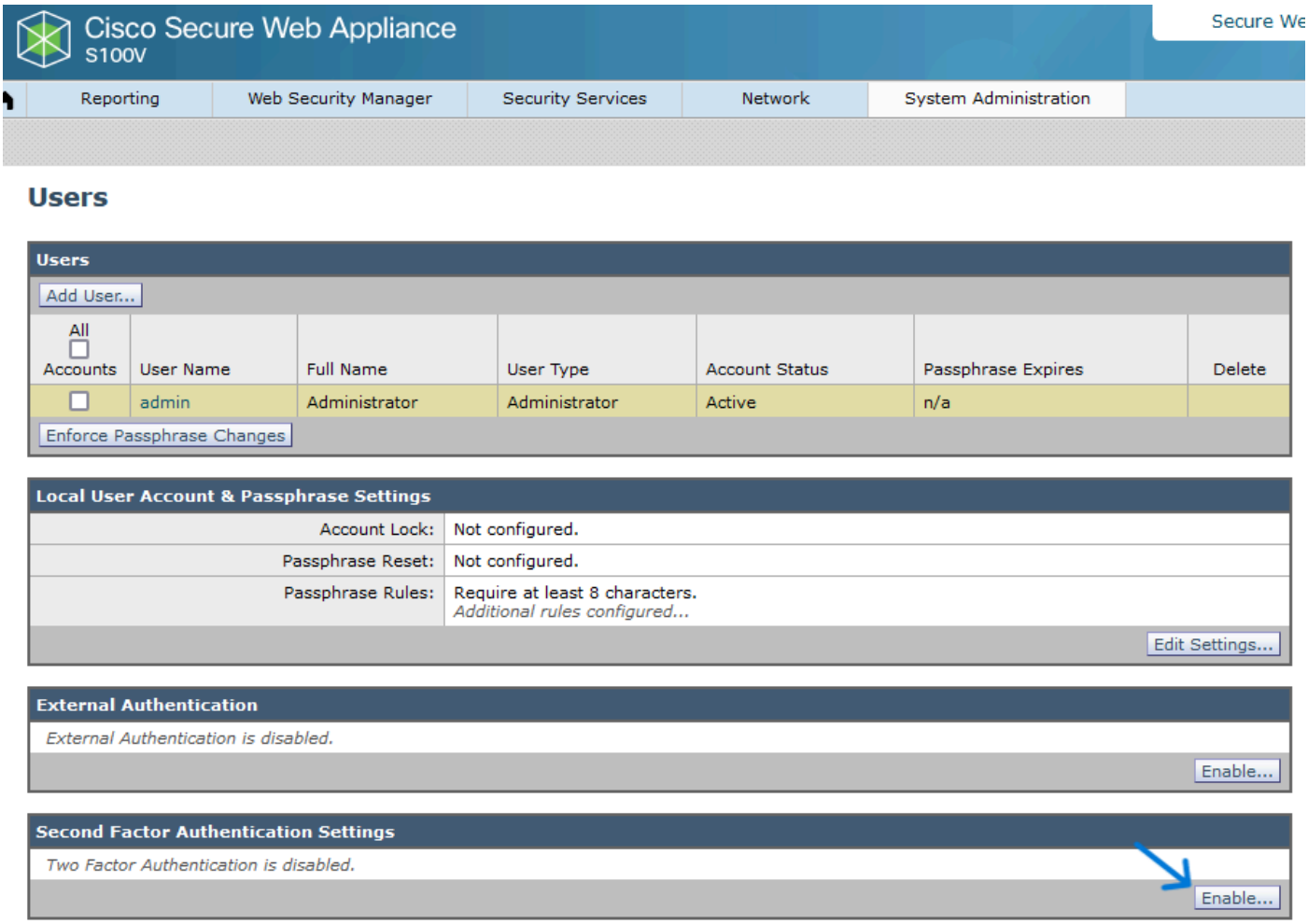


Sélectionner le profil d'autorisation

Configuration SWA

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

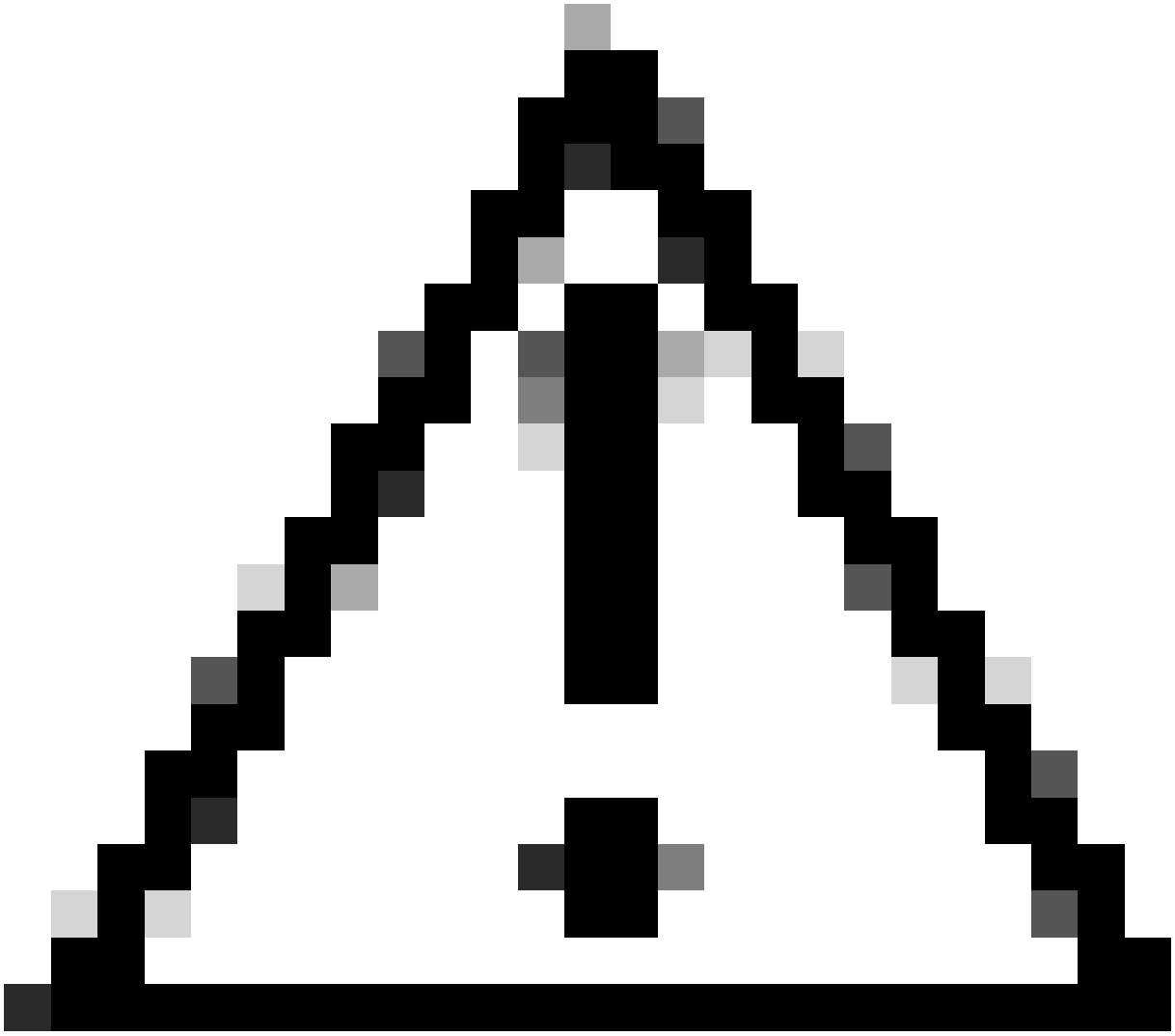
Étape 2. Cliquez sur Enable dans Second Factor Authentication Settings.



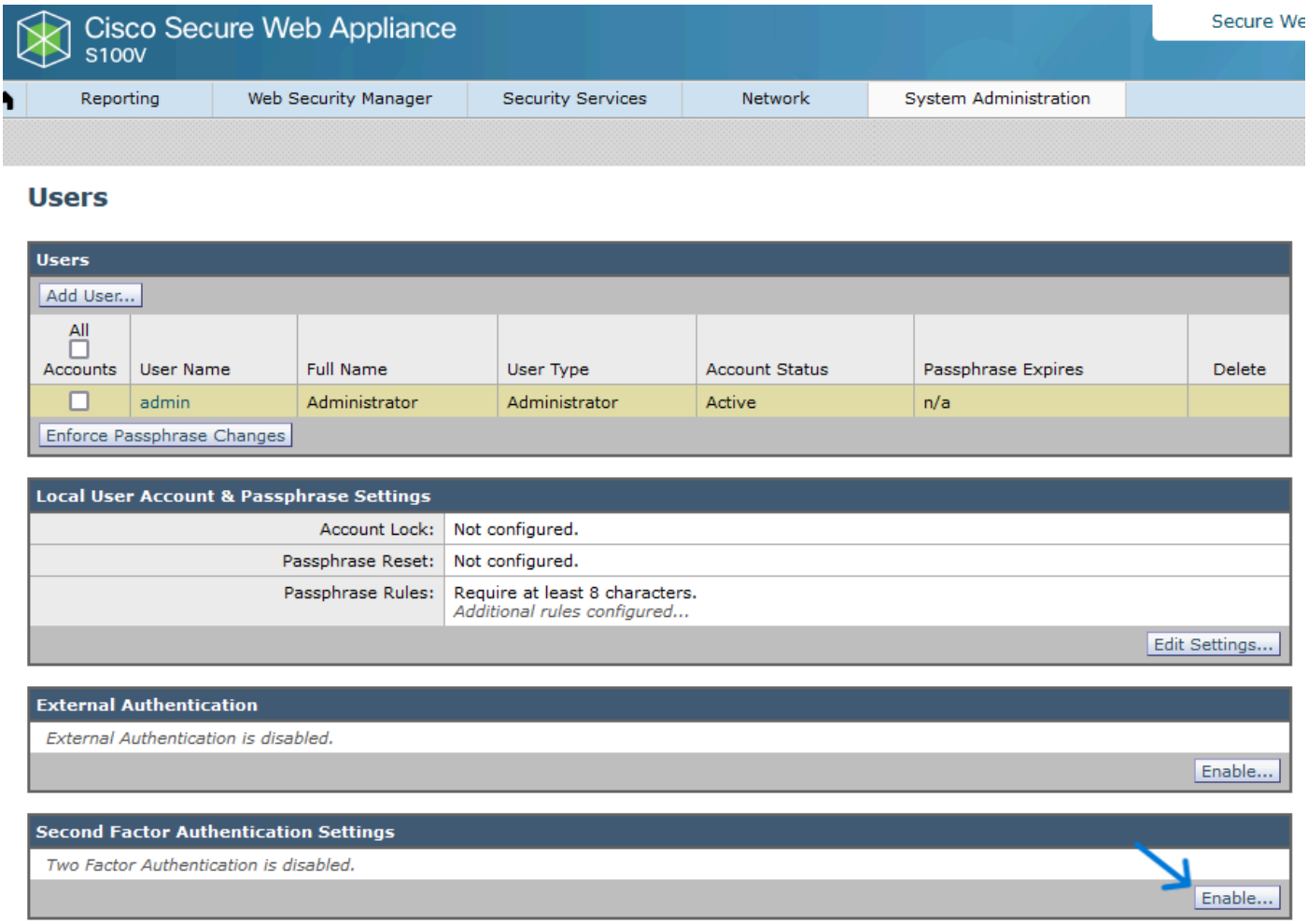
Activer l'authentification du second facteur dans SWA

Étape 3. Entrez l'adresse IP de l'ISE dans le champ RADIUS Server Hostname et entrez Shared Secret qui est configuré à l'étape 2 de la configuration de l'ISE.

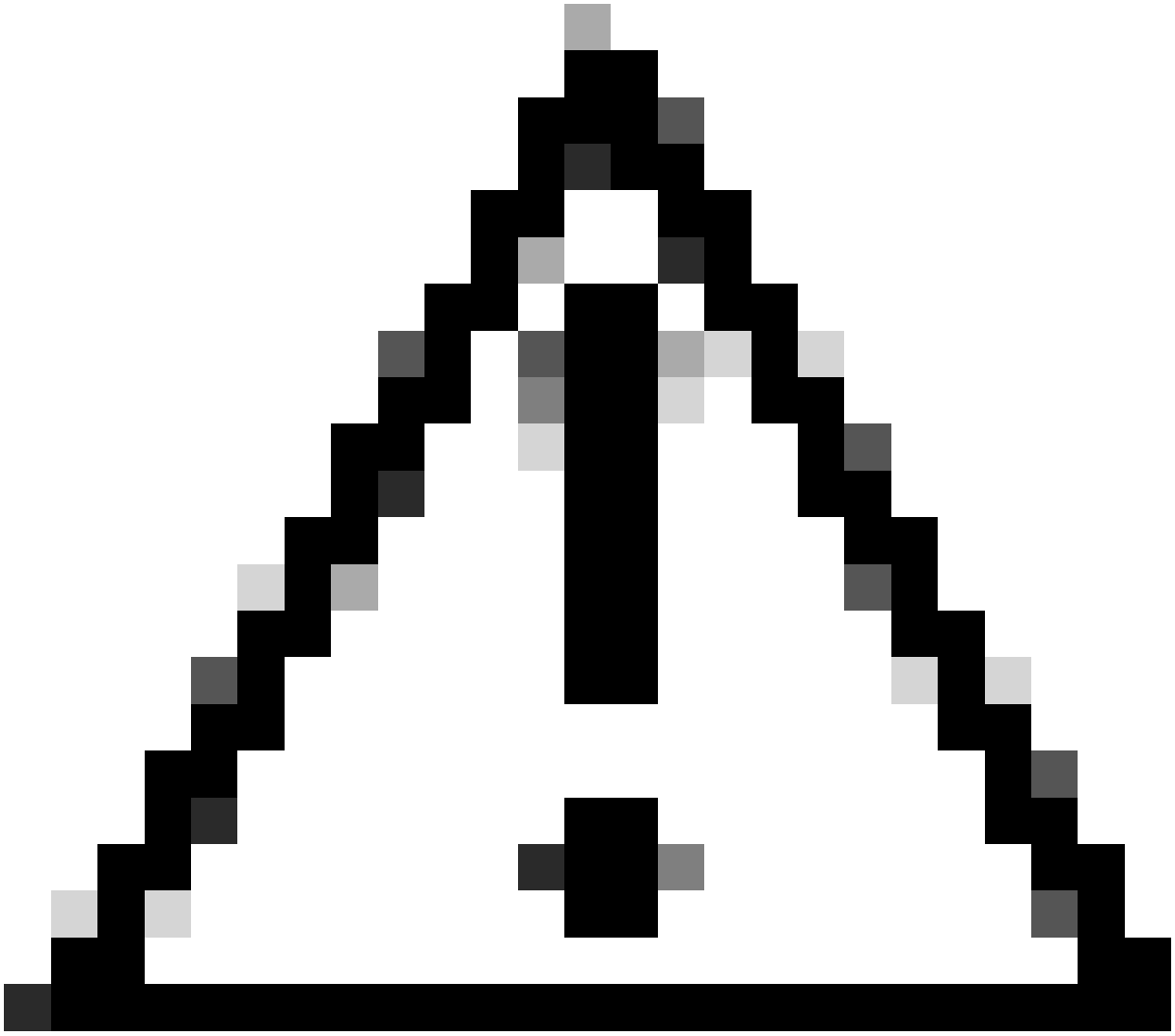
Étape 4. Sélectionnez les rôles prédéfinis requis pour lesquels l'application du second facteur doit être activée.



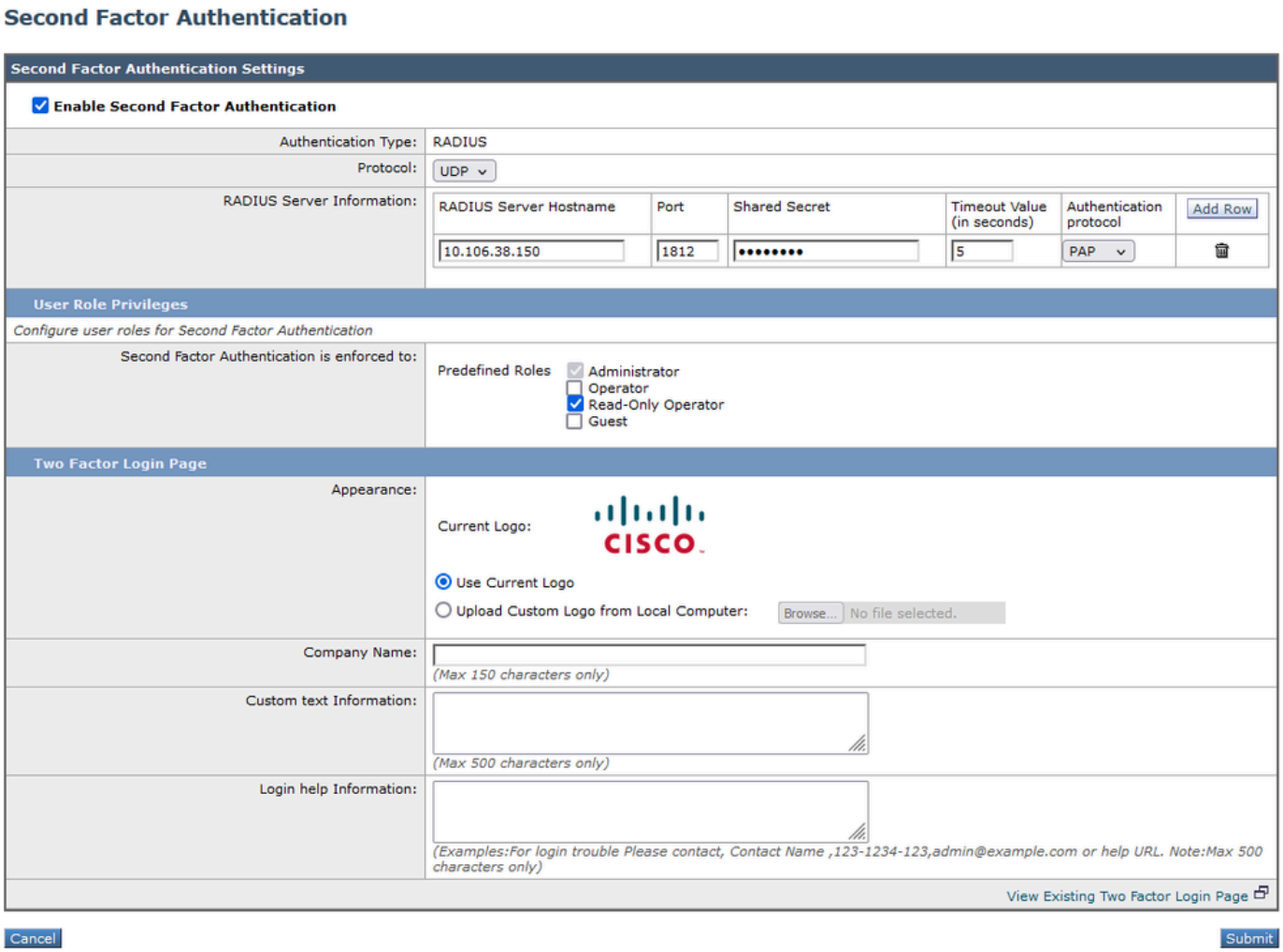
Attention : si vous activez l'authentification du second facteur dans SWA, le compte 'admin' par défaut sera également activé avec l'application du second facteur. Vous devez intégrer ISE avec LDAP ou Active Directory (AD) pour authentifier les informations d'identification d'« admin », car ISE ne vous permet pas de configurer « admin » en tant qu'utilisateur d'accès réseau.



Activer l'authentification du second facteur dans SWA

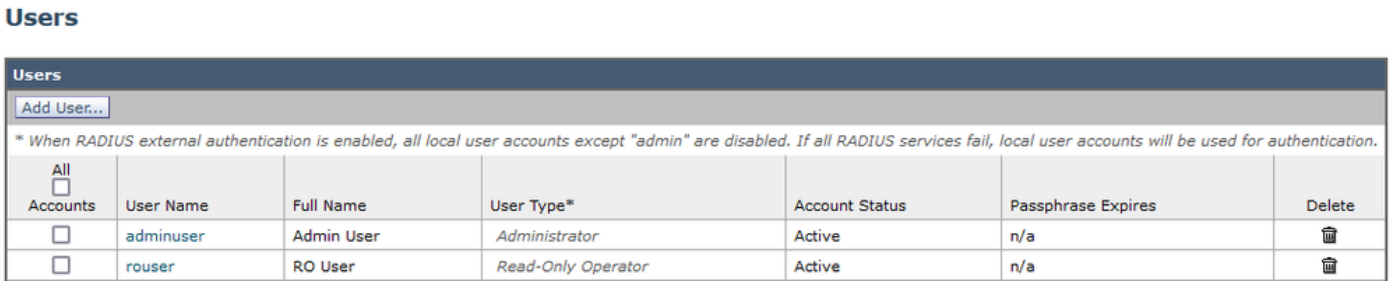


Attention : si vous activez l'authentification du second facteur dans SWA, le compte 'admin' par défaut sera également activé avec l'application du second facteur. Vous devez intégrer ISE avec LDAP ou Active Directory (AD) pour authentifier les informations d'identification d'« admin », car ISE ne vous permet pas de configurer « admin » en tant qu'utilisateur d'accès réseau.



Configuration de Second Factor Authentication

Étape 5 : pour configurer les utilisateurs dans SWA, cliquez sur Add User. Entrez User Name et sélectionnez User Type requis pour le rôle souhaité. Saisissez Passphrase et retapez Passphrase.

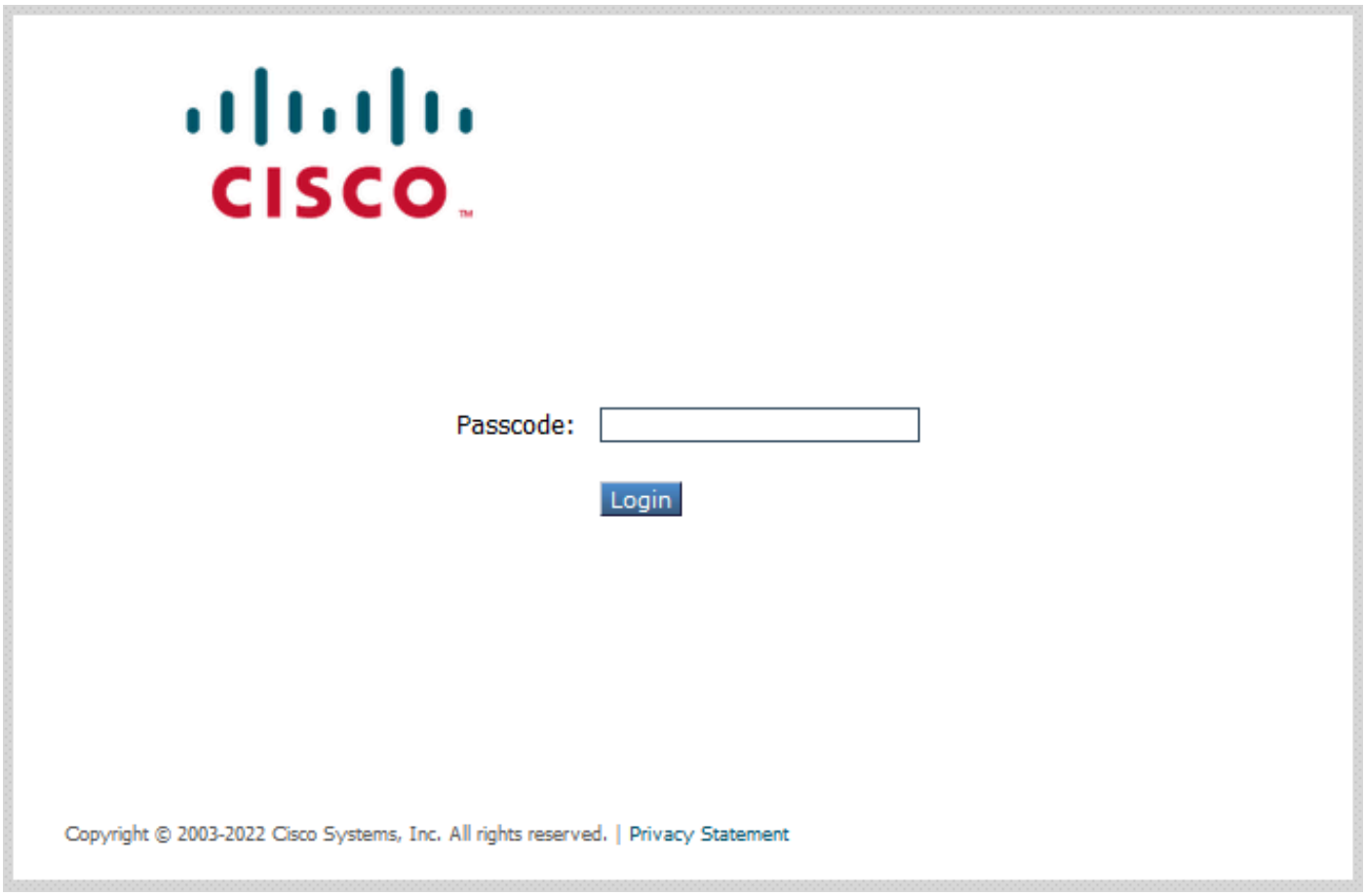


Configuration utilisateur dans SWA

Étape 6 : cliquez sur Submit and Commit Changes.

Vérifier

Accédez à l'interface utilisateur SWA avec les informations d'identification configurées. Une fois l'authentification réussie, vous êtes redirigé vers la page d'authentification secondaire. Ici, vous devez entrer les informations d'identification d'authentification secondaires configurées dans ISE.



Vérification de la connexion au second facteur

Références

- 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
- Intégration d'AD pour interface utilisateur ISE et connexion CLI

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.