Configuration de l'authentification à deux facteurs SWA avec ISE RADIUS

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Topologie du réseau

Configuration Steps

- Configuration ISE
  - 2. Configuration du périphérique réseau dans ISE
- Configuration SWA

Vérifier

Autres informations utiles

Introduction

Ce document décrit comment configurer l'authentification de second facteur sur l'appareil Web sécurisé avec Cisco ISE® en tant que serveur RADIUS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Cisco vous recommande également de disposer des éléments suivants :

- Versions compatibles WSA et ISE
- Votre ISE est intégré à Active Directory ou LDAP
- Accès à l'administration de Secure Web Appliance (SWA) et de Cisco Identity Service Engine (ISE)
- Active Directory ou LDAP est configuré avec un nom d'utilisateur « Admin » pour authentifier le compte « Admin » par défaut de SWA

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 à second facteur pour les utilisateurs administratifs sur SWA, le périphérique vérifie les informations d'identification de l'utilisateur avec le serveur RADIUS une seconde fois une fois que les informations d'identification configurées dans SWA sont vérifiées.

Topologie du réseau



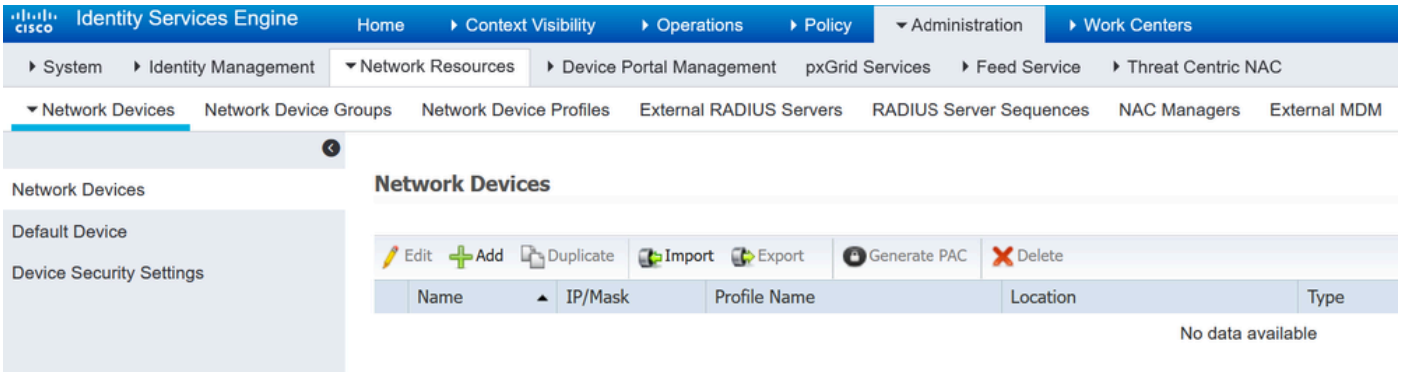
Image - Schéma de topologie du réseau

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

Configuration Steps

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. Configuration du périphérique réseau dans ISE

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

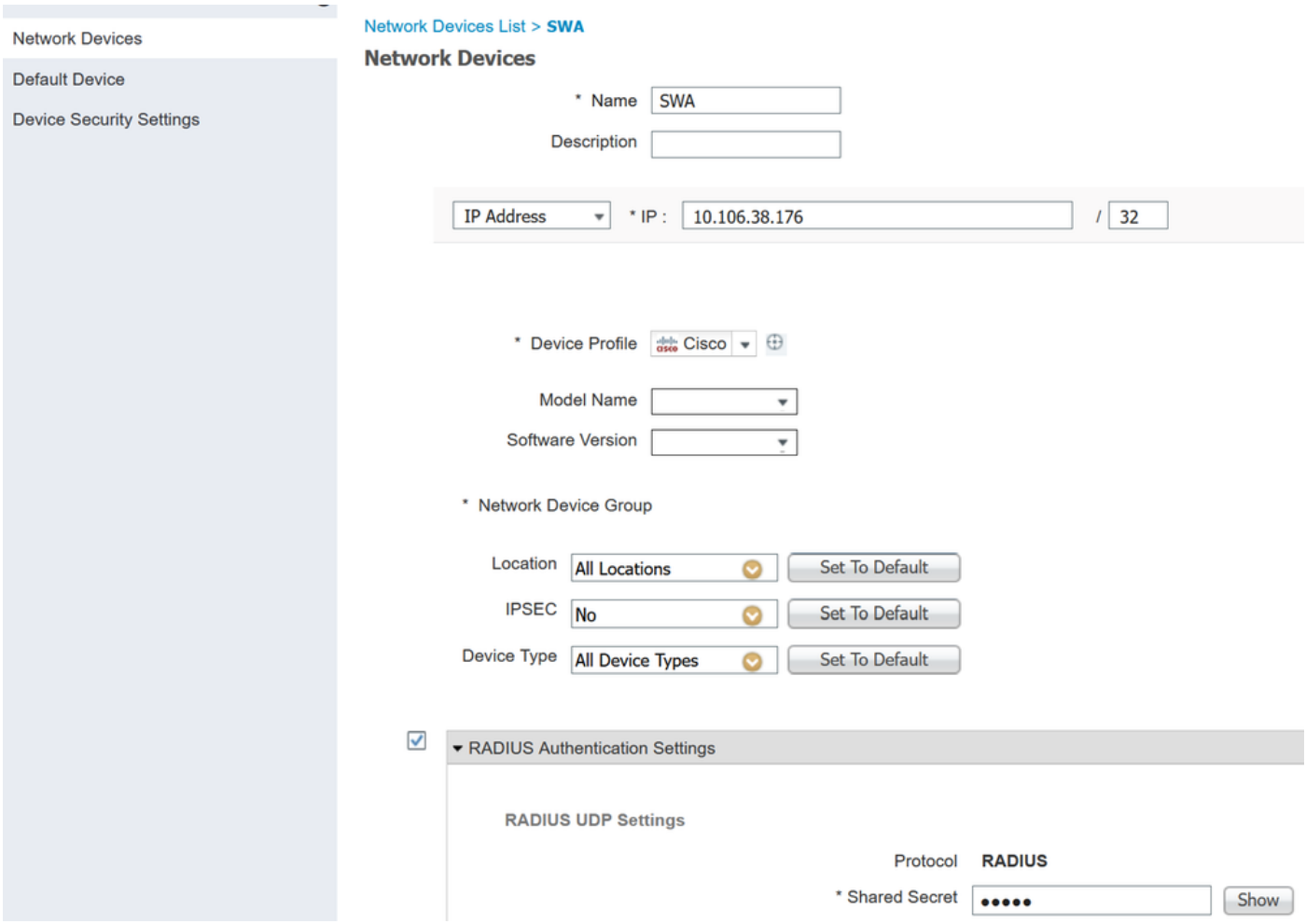
2.2. Insérez l'adresse IP SWA.

2.3. Cochez la case RADIUS.

2.4. Définir un secret partagé.

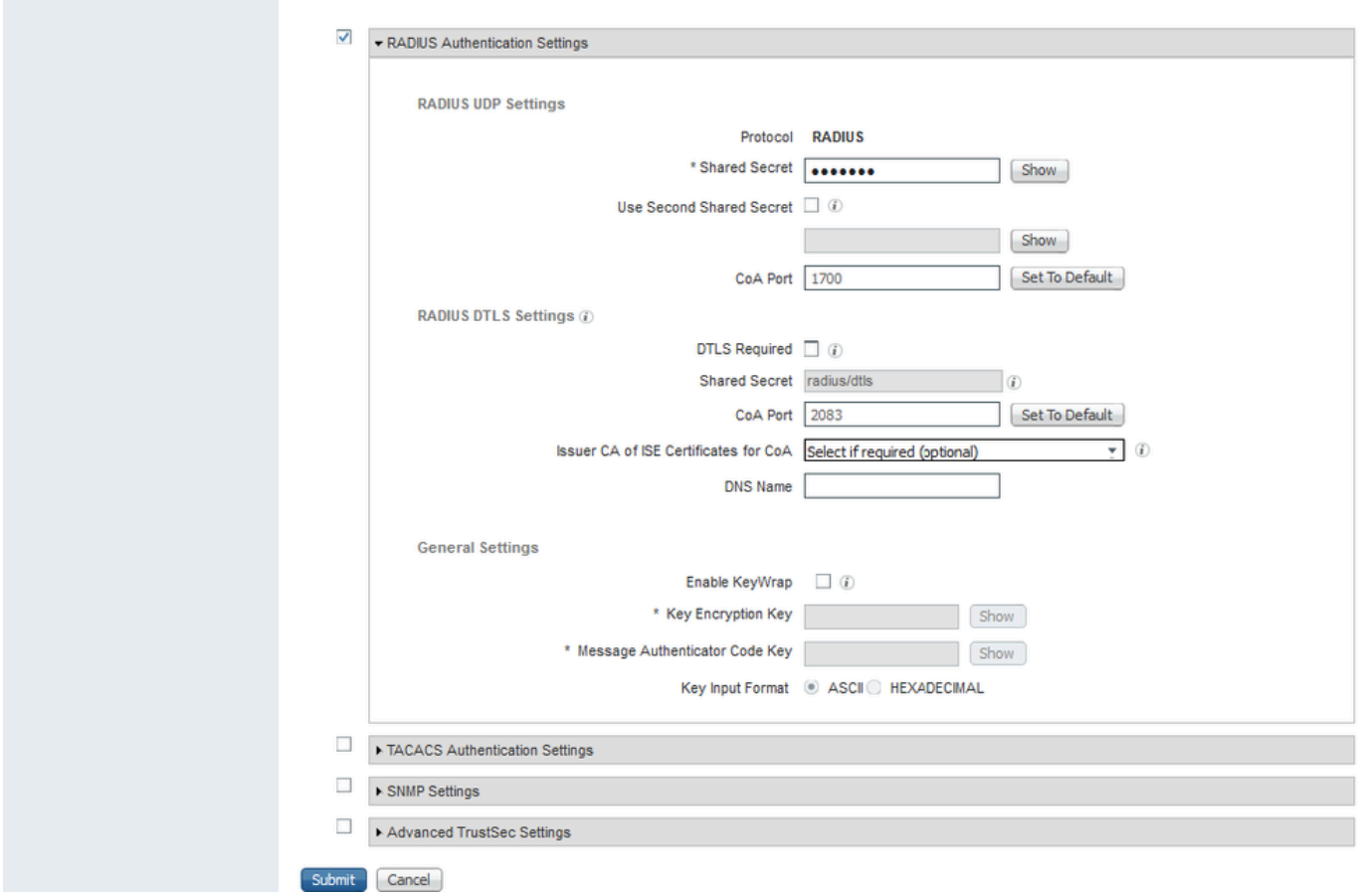


Remarque : La même clé doit être utilisée ultérieurement pour configurer le SWA.



Configurer la clé partagée du périphérique réseau SWA

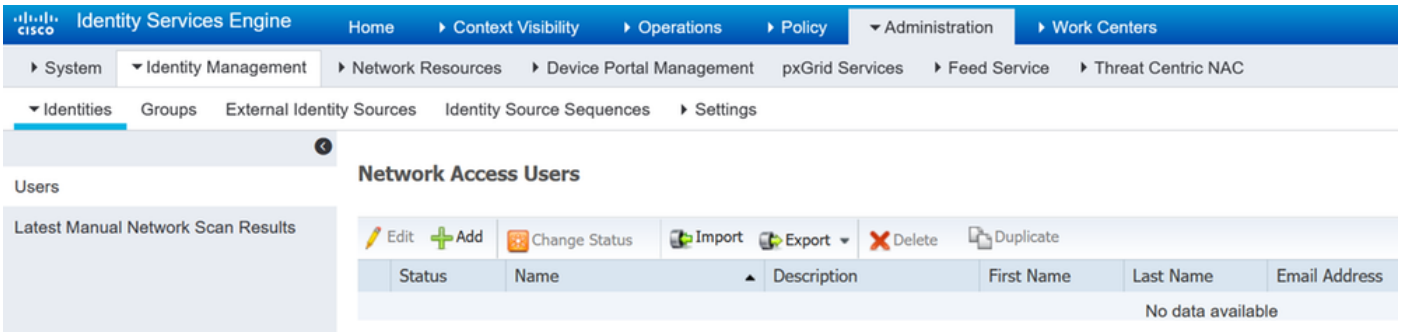
2.5. Cliquez sur Envoyer.



Envoyer la configuration des périphériques réseau

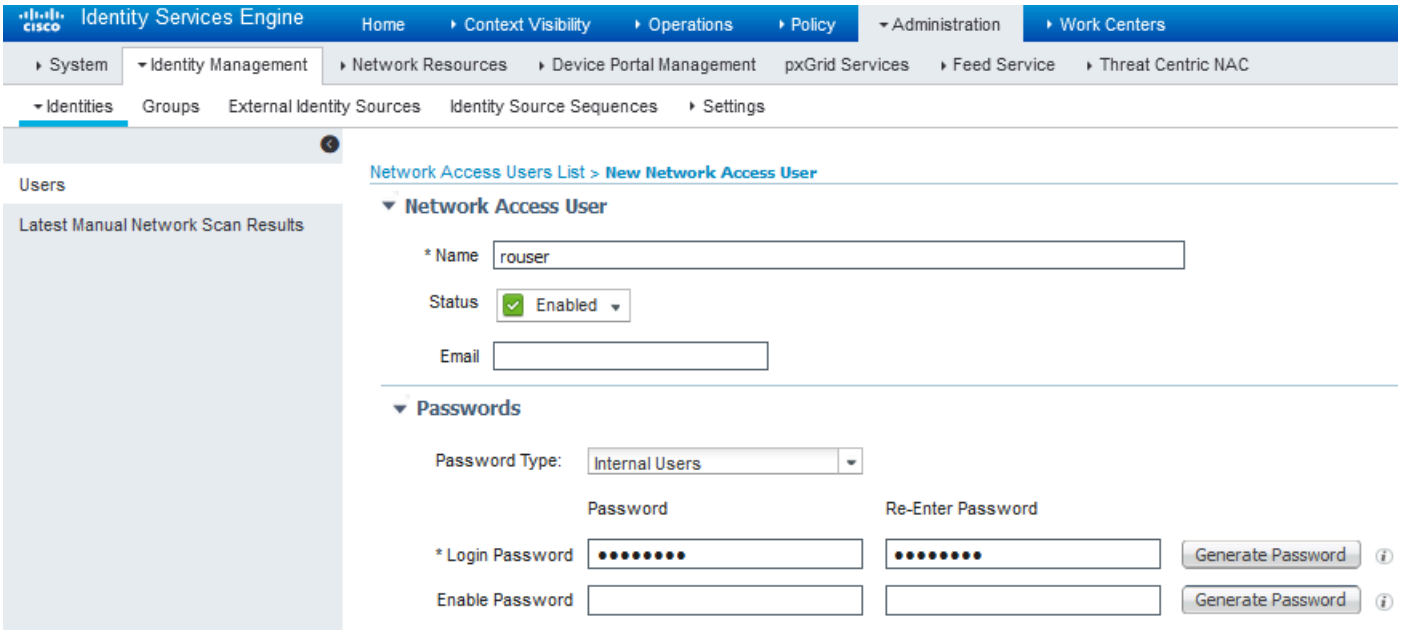
---

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

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

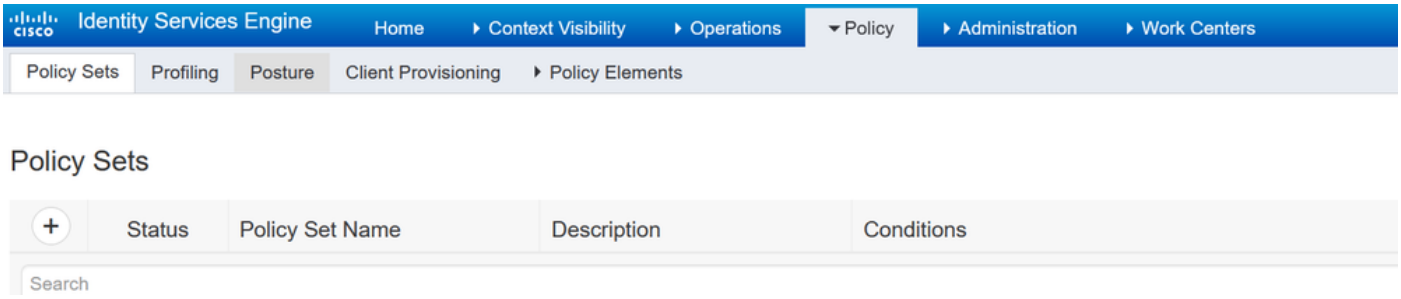


Ajouter un utilisateur local dans ISE

---

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.

4.1. Accédez à Policy > Policy Sets et cliquez sur l'icône + située dans le coin supérieur gauche.

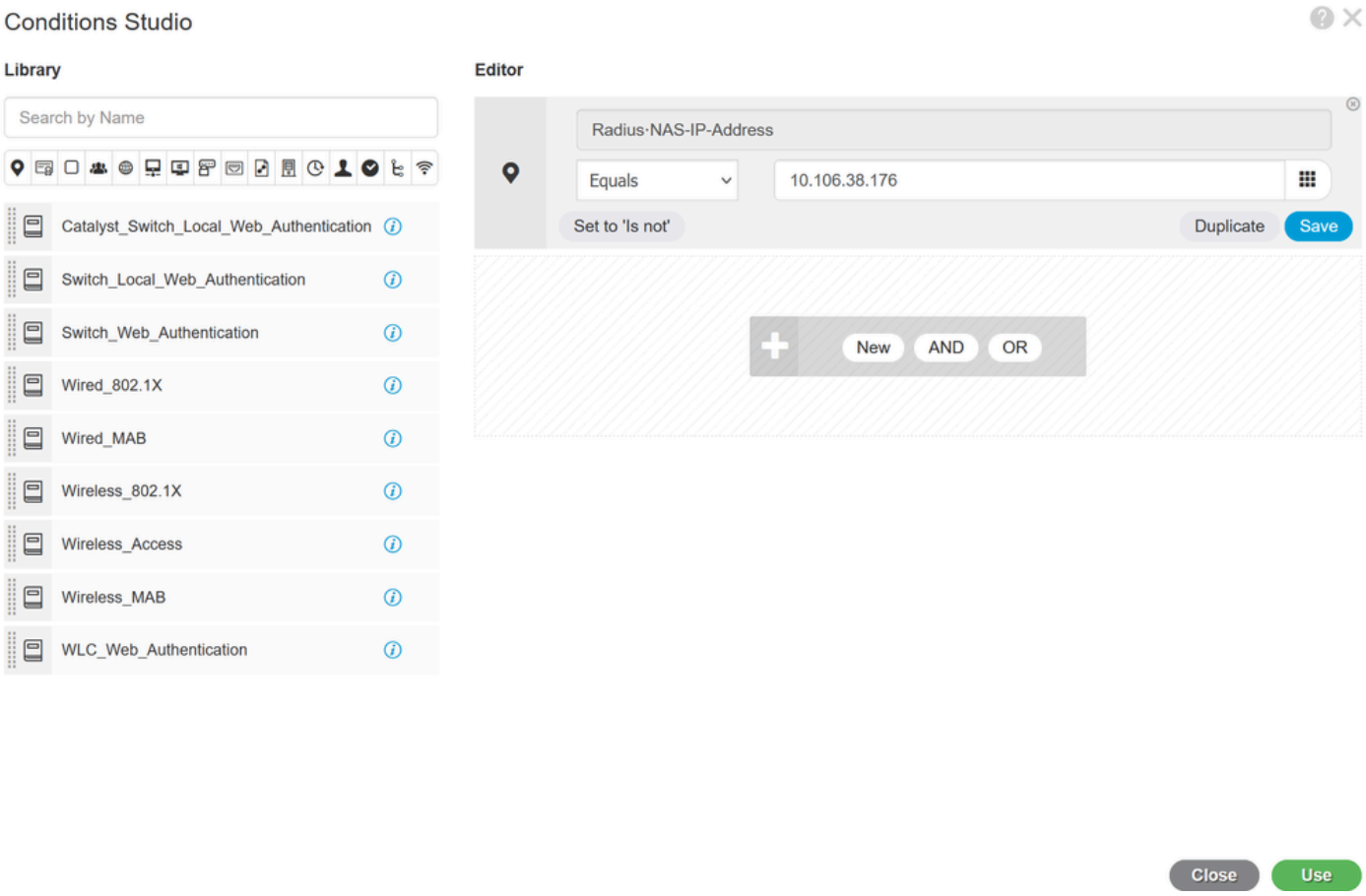


Ajouter un jeu de stratégies dans ISE

4.2. Une nouvelle ligne est placée en haut de vos ensembles de stratégies. Entrez un nom pour la nouvelle stratégie.

4.3. Ajoutez une condition pour que l'attribut RADIUS NAS-IP-Address corresponde à l'adresse IP SWA.

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



Ajouter une stratégie pour mapper un périphérique réseau SWA

4.5. Cliquez sur Enregistrer.



Enregistrer la stratégie

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

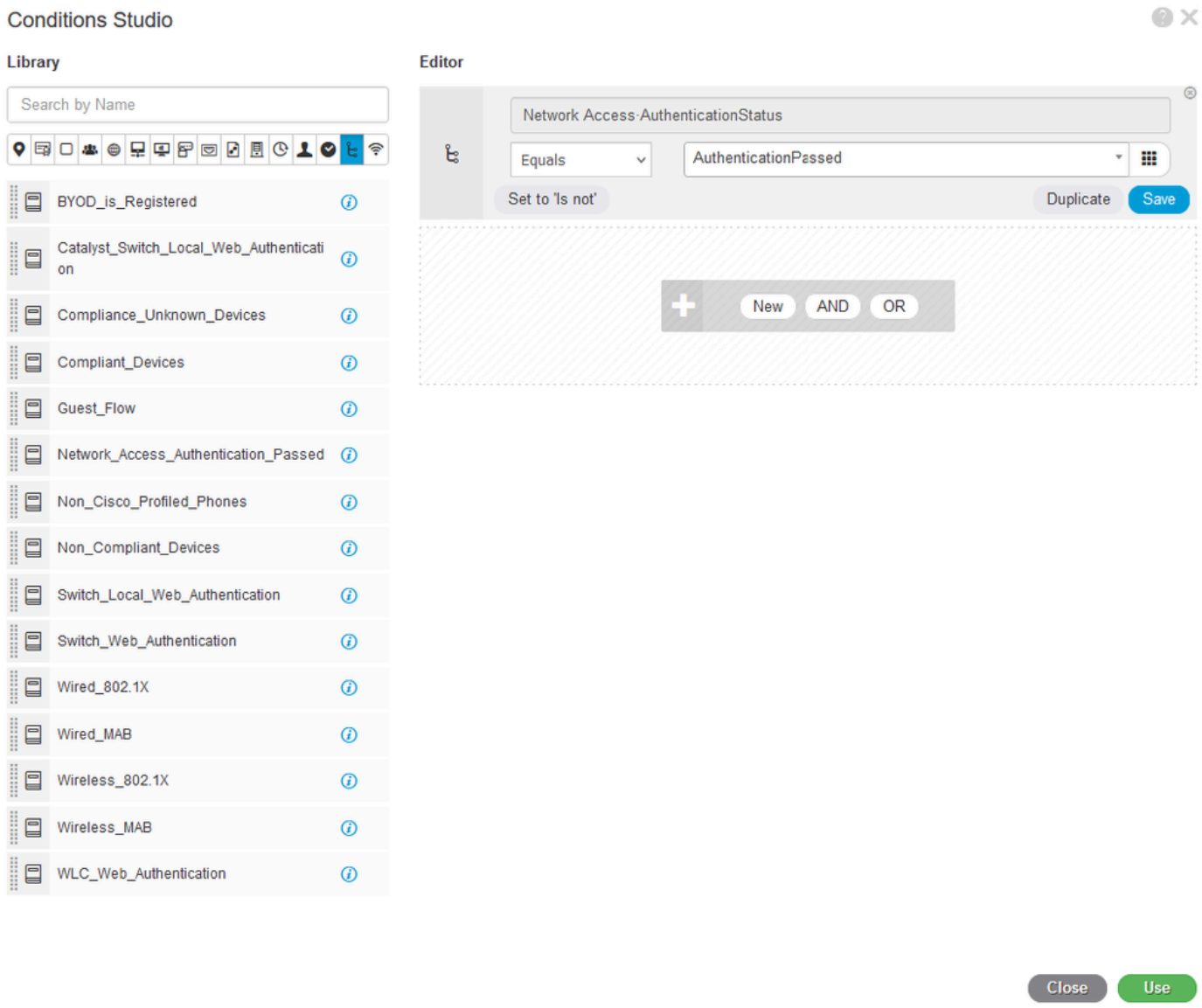
---

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

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.

5.2. Entrez un nom.

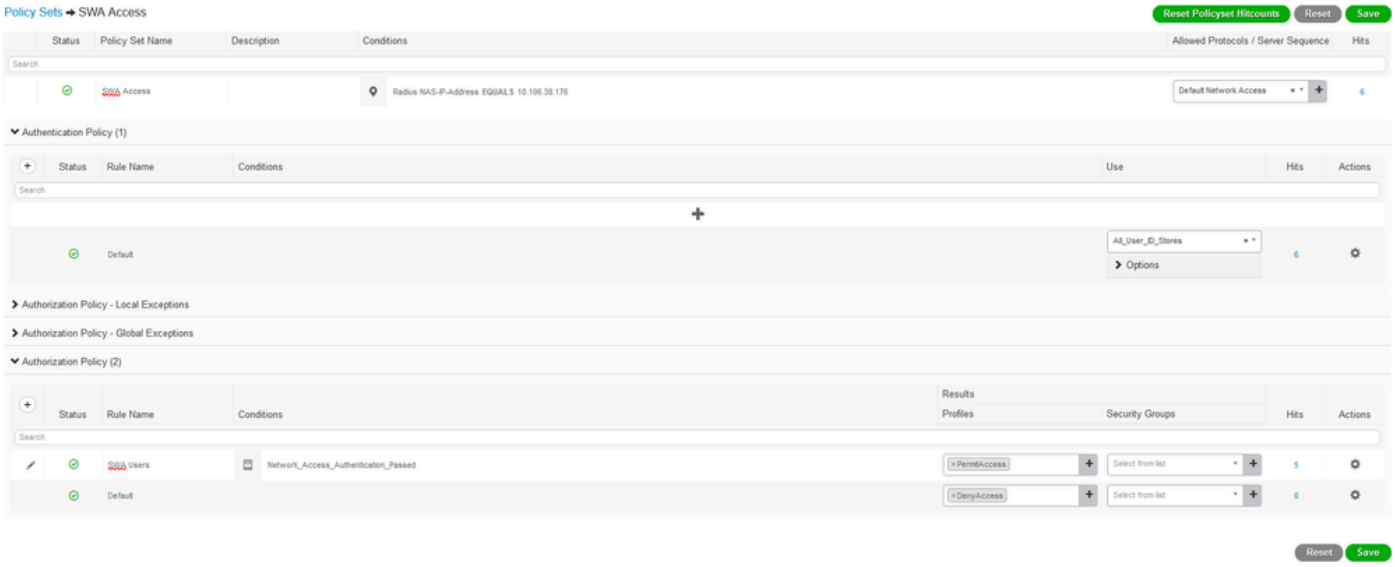
5.3. Définissez les conditions pour faire correspondre le dictionnaire Accès réseau avec Attribut AuthentificationÉtat est égal à AuthentificationPassé et cliquez sur Utiliser.



Sélectionner une condition d'autorisation

---

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

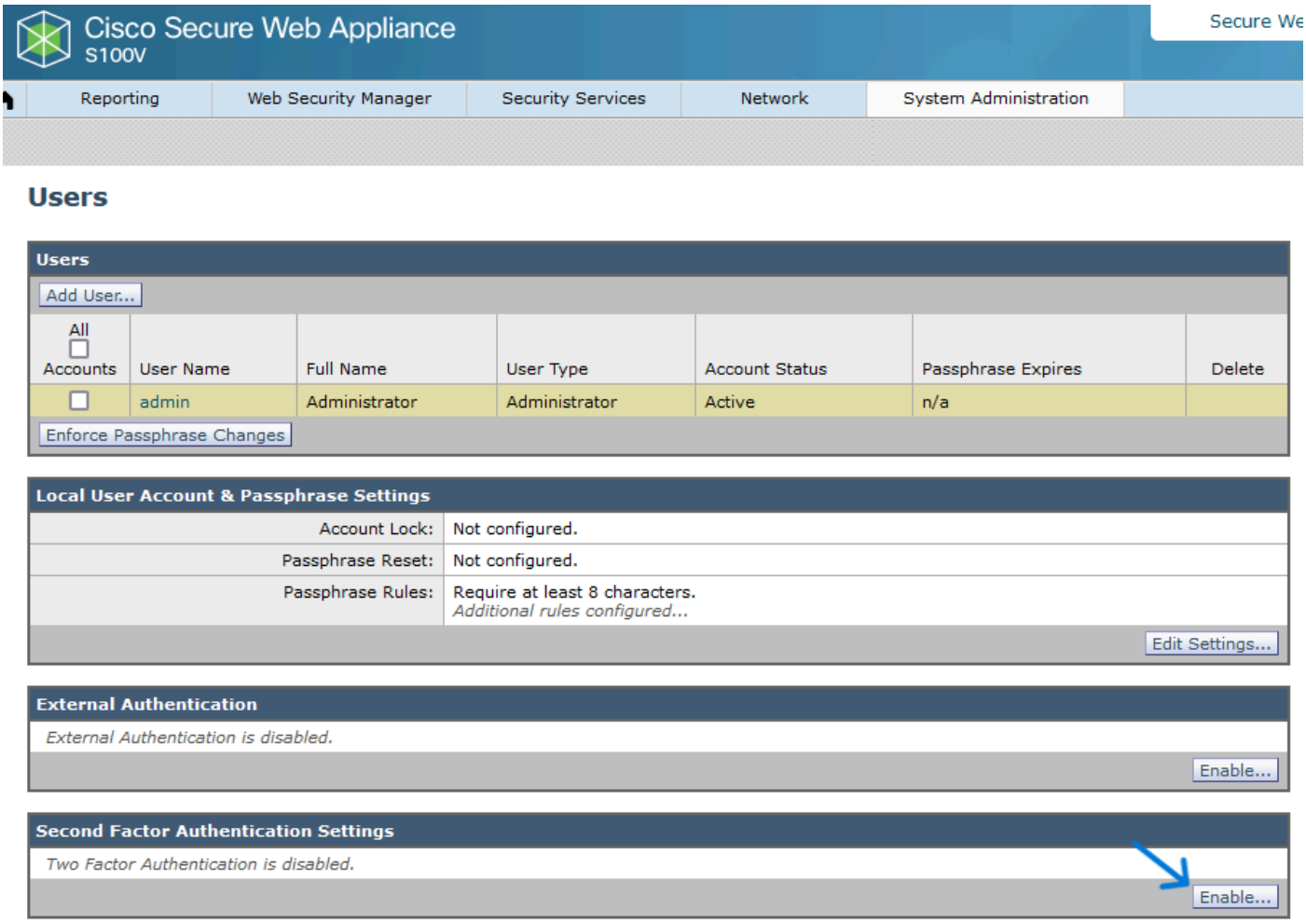


Sélectionner le profil d'autorisation

Configuration SWA

1. Dans l'interface utilisateur graphique de SWA, accédez à Administration système et sélectionnez Utilisateurs.

2. Cliquez sur Activer dans les paramètres Second Factor Authentication.



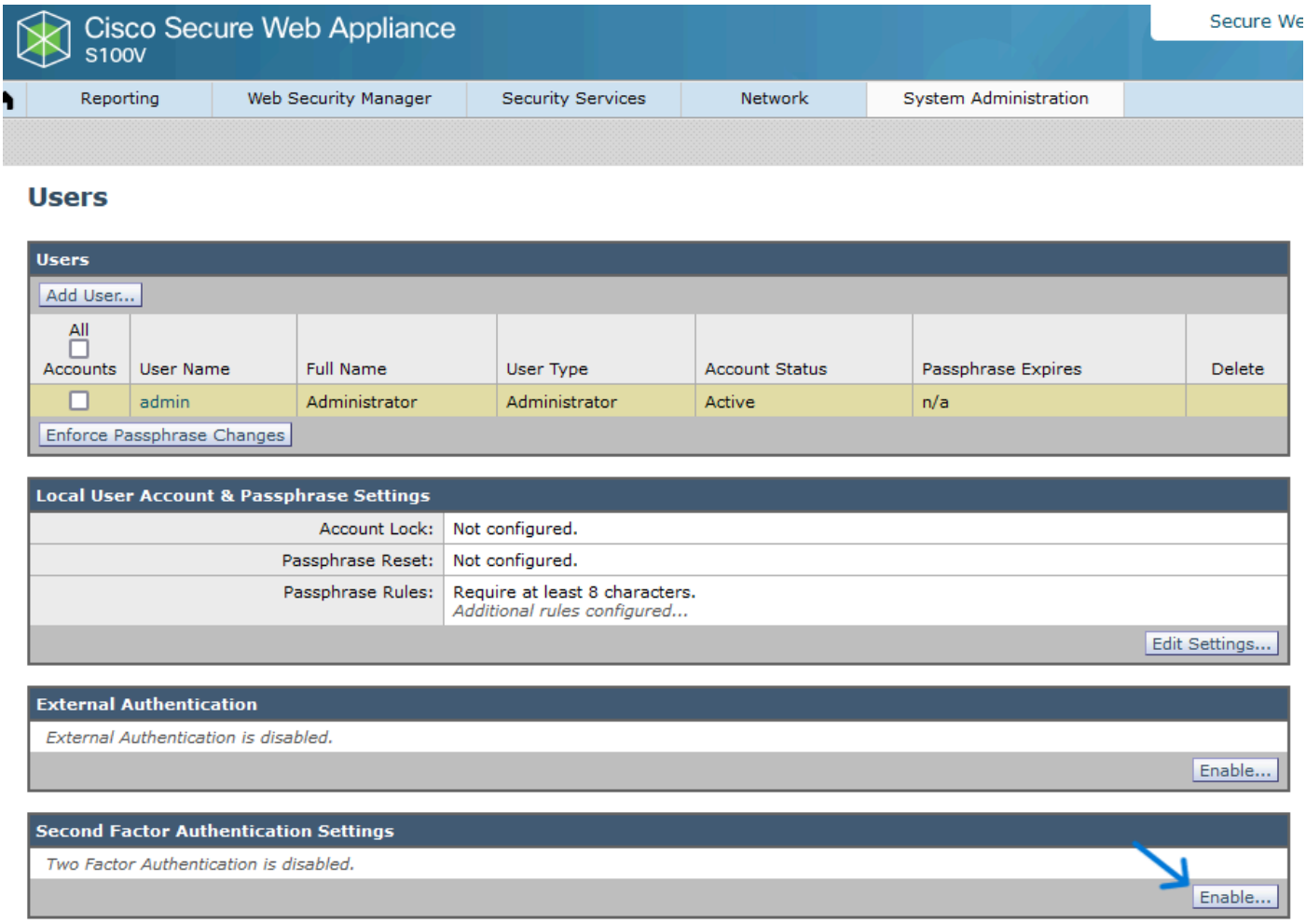
Activer l'authentification du second facteur dans SWA

---

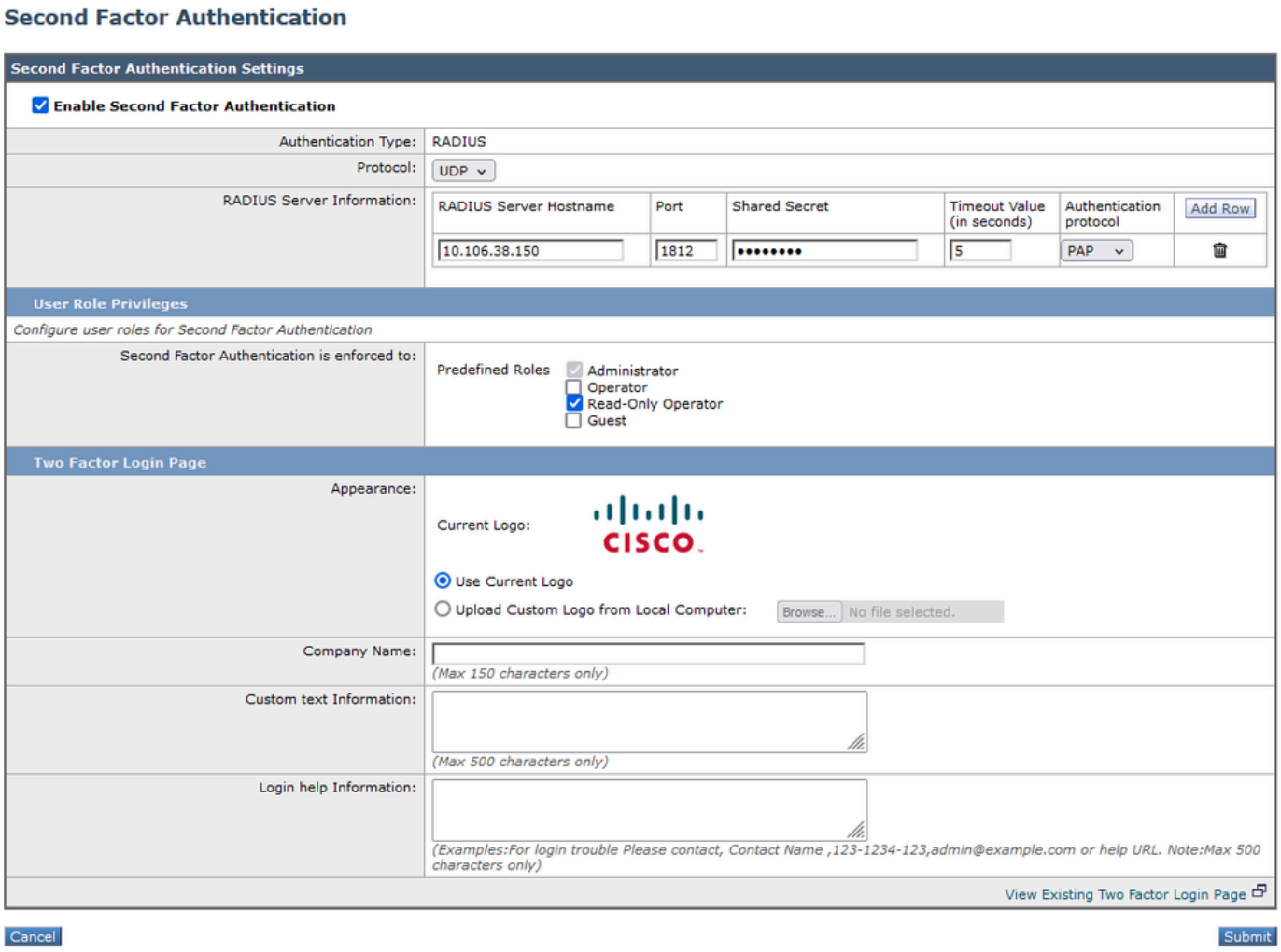
3. Entrez l'adresse IP de l'ISE dans le champ RADIUS Server Hostname et entrez le secret partagé qui a été configuré à l'étape 2 de la configuration d'ISE.

4. Sélectionnez les rôles prédéfinis que vous souhaitez activer l'application du second facteur.

⚠ Mise en garde : Si vous activez l'authentification du second facteur dans SWA, le compte Admin par défaut est également activé pour l'application du second facteur. Vous devez intégrer ISE avec LDAP ou Active Directory (AD) pour authentifier les informations d'identification d'administrateur car ISE ne vous permet pas de configurer Admin en tant qu'utilisateur d'accès au réseau.



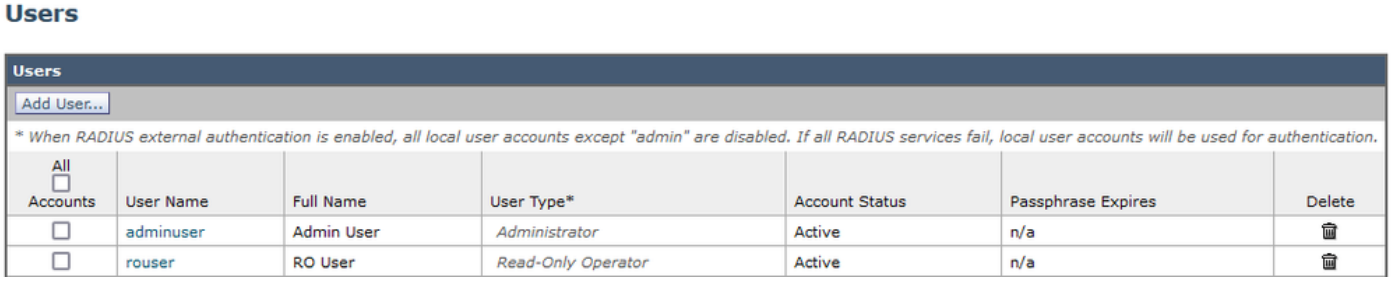
Activer l'authentification du second facteur dans SWA



Configuration de Second Factor Authentication

---

5. Pour configurer les utilisateurs dans SWA, cliquez sur Ajouter un utilisateur. Entrez le Nom d'utilisateur et sélectionnez le Type d'utilisateur requis pour le rôle souhaité. Saisissez la phrase de passe et retapez la phrase de passe.



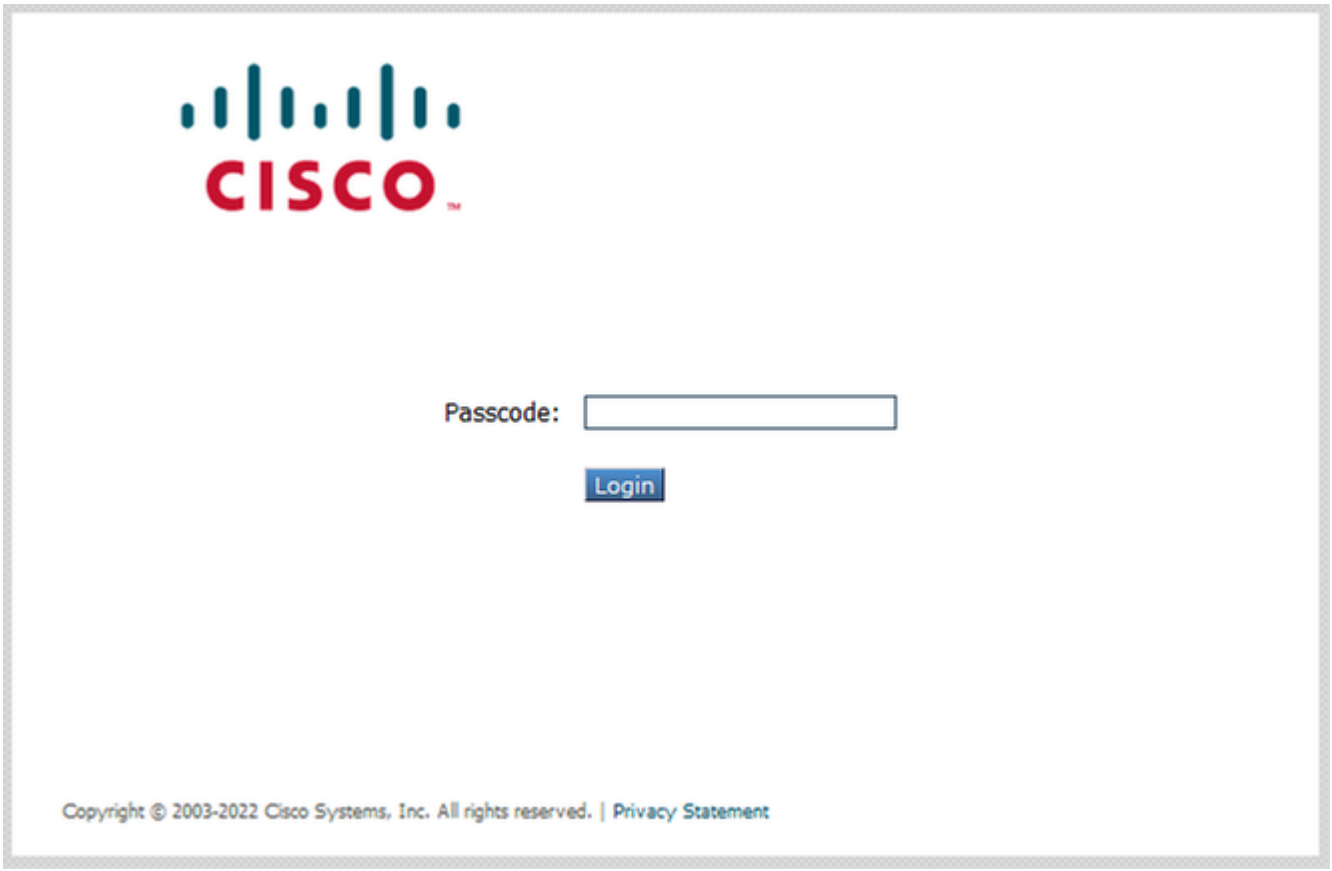
Configuration utilisateur dans SWA

---

6. Cliquez sur Soumettre et valider les modifications.

Vérifier

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



Vérification de la connexion au second facteur

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
- 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.