

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

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Topologie du réseau](#)

[Configuration Steps](#)

[Configuration ISE](#)

[Configuration SWA](#)

[Vérifier](#)

[Références](#)

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices

Default Device

Device Security Settings

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type
No data available				

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.

Network Devices

Default Device

Device Security Settings

[Network Devices List > SWA](#)

Network Devices

* Name

Description

IP Address * IP : /

* Device Profile  Cisco

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Configurer la clé partagée du périphérique réseau SWA

Étape 2.5. Cliquez sur Submit.

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: **RADIUS**

* Shared Secret: Show

Use Second Shared Secret: ⓘ

Show

CoA Port: Set To Default

RADIUS DTLS Settings ⓘ

DTLS Required: ⓘ

Shared Secret: ⓘ

CoA Port: Set To Default

Issuer CA of ISE Certificates for CoA: ⓘ

DNS Name:

General Settings

Enable KeyWrap: ⓘ

* Key Encryption Key: Show

* Message Authenticator Code Key: Show

Key Input Format: ASCII HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

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.

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | Threat Centric NAC

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Network Access Users

Users

Latest Manual Network Scan Results

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address
No data available					

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name:

Status: Enabled

Email:

Passwords

Password Type:

Password:
 Re-Enter Password:
 ⓘ

* Login Password:
 ⓘ

Enable Password:
 ⓘ

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.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

+	Status	Policy Set Name	Description	Conditions
Search				

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.



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.

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.

The screenshot shows the Cisco Secure Web Appliance (S100V) administration interface. The top navigation bar includes 'Reporting', 'Web Security Manager', 'Security Services', 'Network', and 'System Administration'. The 'Users' section is active, displaying a table of users with columns for 'Accounts', 'User Name', 'Full Name', 'User Type', 'Account Status', 'Passphrase Expires', and 'Delete'. Below the table are sections for 'Local User Account & Passphrase Settings', 'External Authentication', and 'Second Factor Authentication Settings'. The 'Second Factor Authentication Settings' section shows 'Two Factor Authentication is disabled' and an 'Enable...' button, which is highlighted by a blue arrow.

Accounts	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	

Local User Account & Passphrase Settings

Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. Additional rules configured...

External Authentication

External Authentication is disabled.

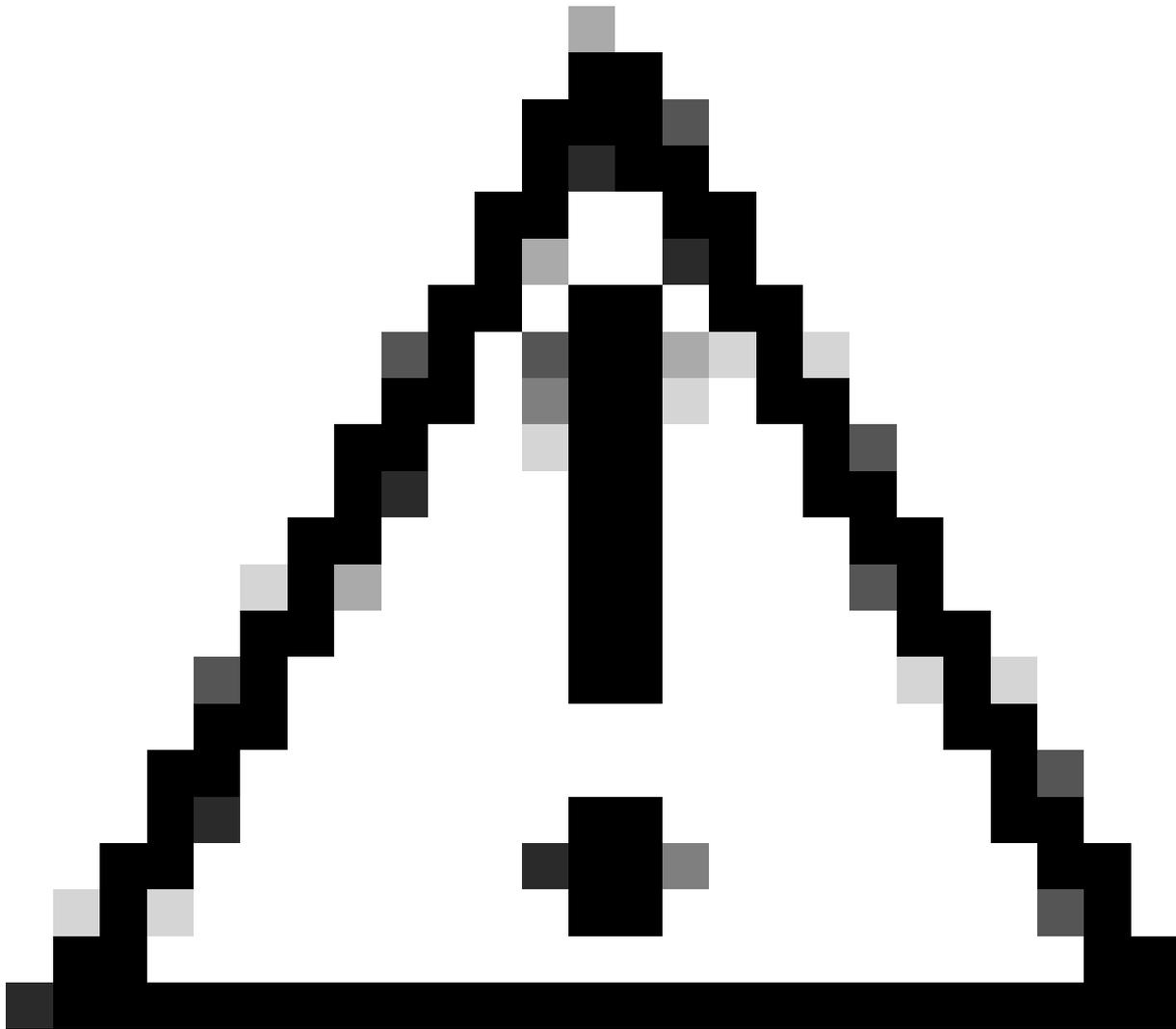
Second Factor Authentication Settings

Two Factor Authentication is disabled.

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.



Users

Users						
Add User...						
<input type="checkbox"/>	User Name	Full Name	User Type	Account Status	Passphrase Expires	Delete
<input type="checkbox"/>	admin	Administrator	Administrator	Active	n/a	
Enforce Passphrase Changes						

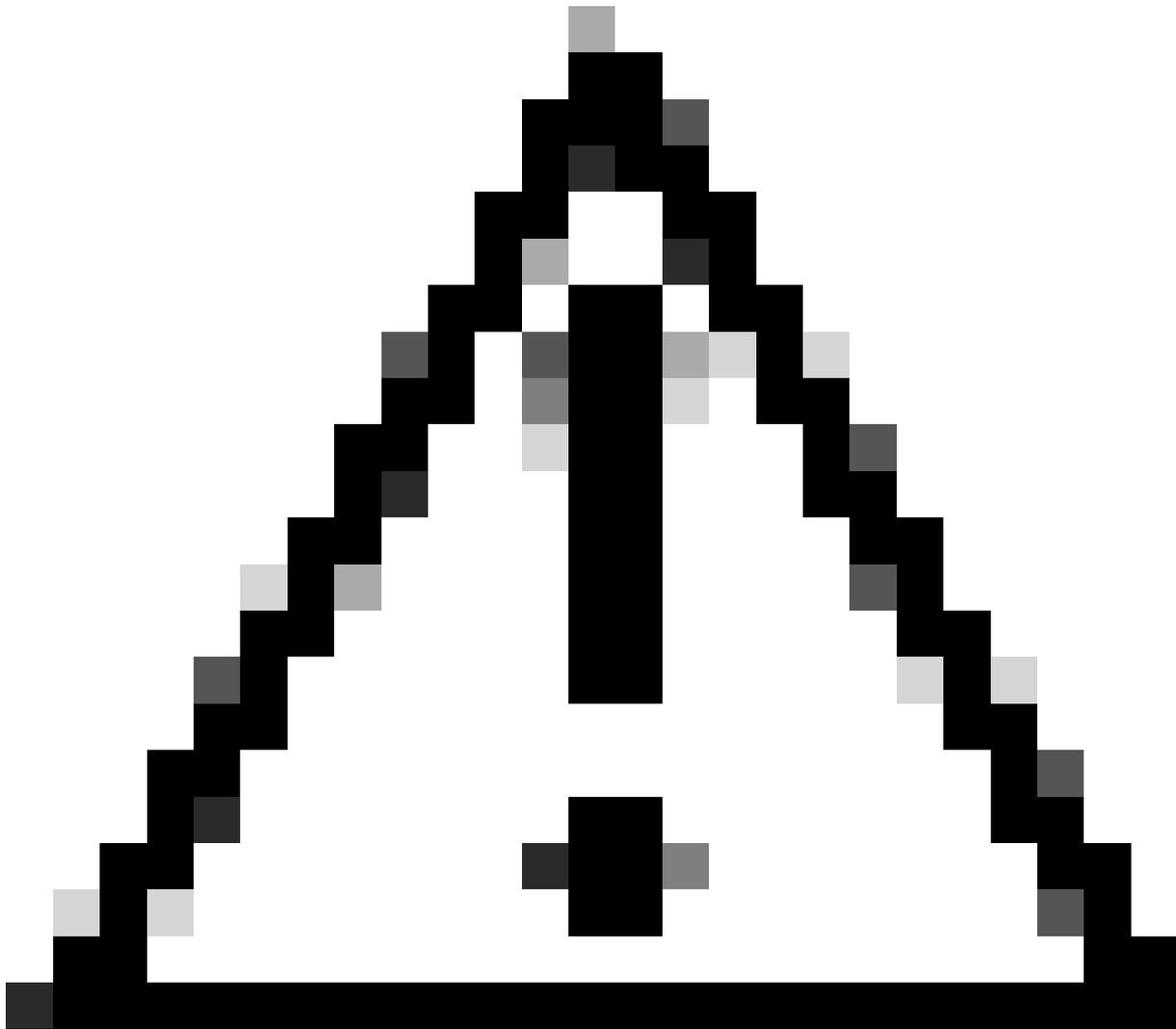
Local User Account & Passphrase Settings	
Account Lock:	Not configured.
Passphrase Reset:	Not configured.
Passphrase Rules:	Require at least 8 characters. <i>Additional rules configured...</i>
Edit Settings...	

External Authentication
<i>External Authentication is disabled.</i>
Enable...

Second Factor Authentication Settings
<i>Two Factor Authentication is disabled.</i>
Enable...



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.

Second Factor Authentication

Second Factor Authentication Settings

Enable Second Factor Authentication

Authentication Type: RADIUS

Protocol: UDP

RADIUS Server Information:	RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Add Row
	10.106.38.150	1812	*****	5	PAP	🗑️

User Role Privileges

Configure user roles for Second Factor Authentication

Second Factor Authentication is enforced to:

Predefined Roles

- Administrator
- Operator
- Read-Only Operator
- Guest

Two Factor Login Page

Appearance:

Current Logo:

Use Current Logo

Upload Custom Logo from Local Computer: Browse... No file selected.

Company Name:
(Max 150 characters only)

Custom text Information:
(Max 500 characters only)

Login help Information:
(Examples: For login trouble Please contact, Contact Name ,123-1234-123,admin@example.com or help URL. Note:Max 500 characters only)

[View Existing Two Factor Login Page](#)

Cancel
Submit

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.

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
<input type="checkbox"/>	adminuser	Admin User	Administrator	Active	n/a	🗑️
<input type="checkbox"/>	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 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.



Passcode:

Login

Copyright © 2003-2022 Cisco Systems, Inc. All rights reserved. | [Privacy Statement](#)

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.