Configurer le certificat de l'interface graphique Secure Web Appliance

Table des matières

Introduction

Ce document décrit les étapes de configuration des certificats pour l'interface Web de gestion de l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration SWA.

Cisco recommande que vous ayez :

- SWA physique ou virtuel installé.
- Accès administratif à l'interface utilisateur graphique (GUI) de SWA.
- Accès administratif à l'interface de ligne de commande (CLI) SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Certificat d'interface utilisateur Web

Nous devons d'abord choisir le type de certificats que nous voulons utiliser dans l'interface utilisateur Web de gestion SWA.

Par défaut, SWA utilise le « Certificat de démonstration d'appareil Cisco : »

- CN = Certificat de démonstration d'appareil Cisco
- O = Cisco Systems, Inc
- L = San Jose
- S = Californie
- C = US

Vous pouvez créer un certificat auto-signé dans SWA ou importer votre propre certificat qui a été généré par votre serveur d'autorité de certification interne.

Le SWA ne prend pas en charge l'inclusion d'autres noms de sujet (SAN) lors de la génération d'une demande de signature de certificat (CSR). En outre, les certificats auto-signés SWA ne prennent pas en charge les attributs SAN non plus. Pour utiliser des certificats avec des attributs SAN, vous devez créer et signer le certificat vous-même, en vous assurant qu'il inclut les détails SAN nécessaires. Une fois que vous avez généré ce certificat, vous pouvez le télécharger sur le SWA à utiliser. Cette approche vous permet de spécifier plusieurs noms d'hôte, adresses IP ou autres identificateurs, offrant ainsi une plus grande flexibilité et une plus grande sécurité pour votre environnement réseau.

Remarque : les certificats doivent inclure la clé privée au format PKCS#12.

Étapes de modification du certificat d'interface Web

Étape 1. Connectez-vous à l'interface utilisateur graphique et sélectionnez Network dans le menu supérieur.

Étape 2. Sélectionnez Certificate Management.

Étape 3. Dans Appliance Certificates, Sélectionnez Add Certificate.

Étape 4. Sélectionnez le type de certificat (certificat auto-signé ou certificat d'importation).

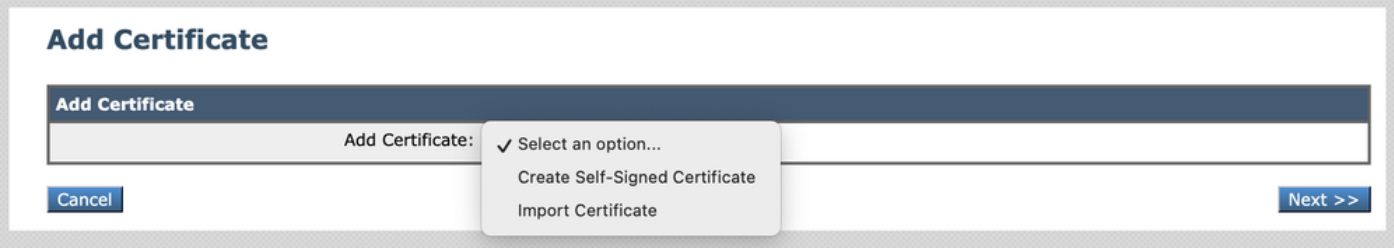


Image - Choisir le type de certificat

Étape 5. Si vous sélectionnez le certificat auto-signé, procédez comme suit. Sinon, passez à l'étape 6.

Étape 5.1. Renseignez les champs.

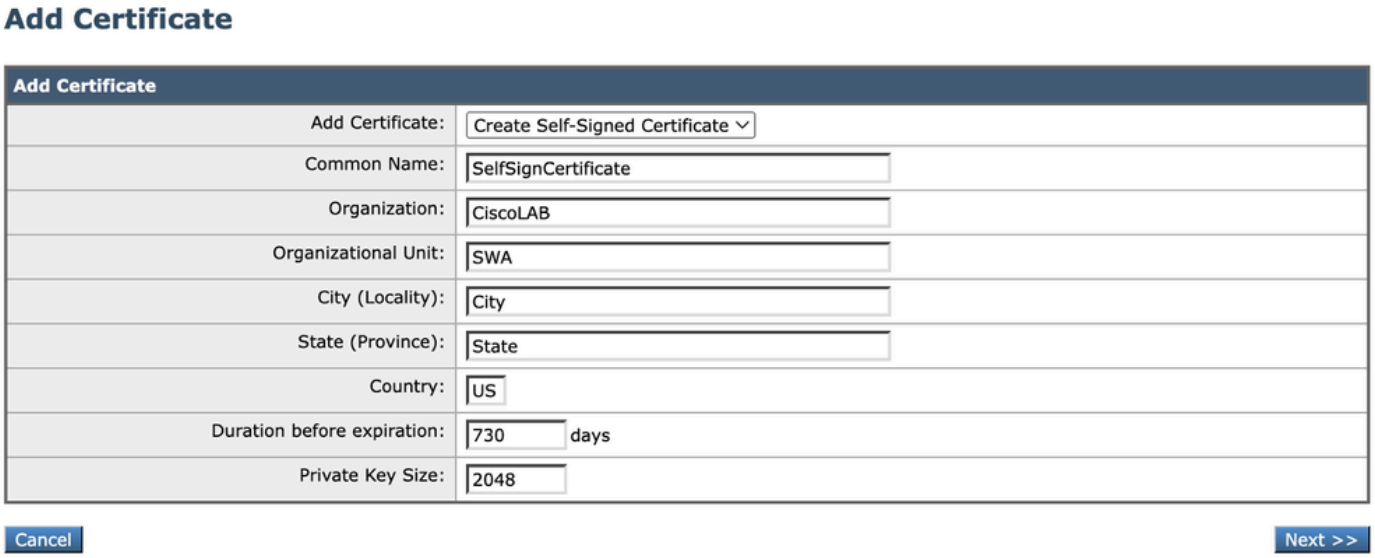


Image - Détails du certificat d'auto-signature

Remarque : la taille de la clé privée doit être comprise entre 2048 et 8192.

Étape 5.2. Cliquez sur Next (Suivant).

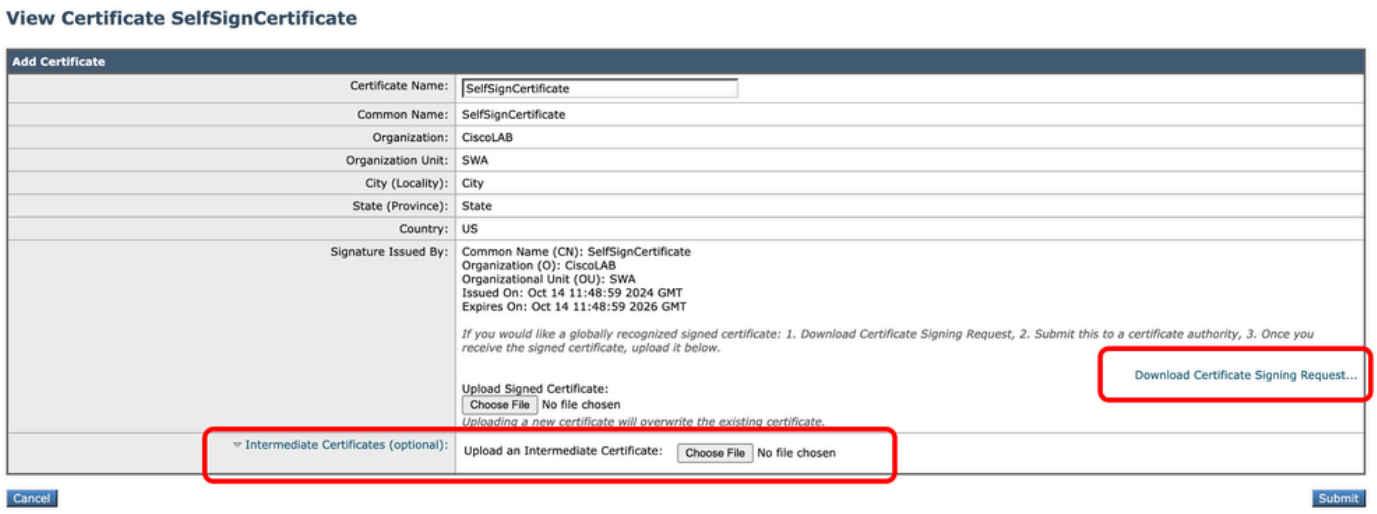
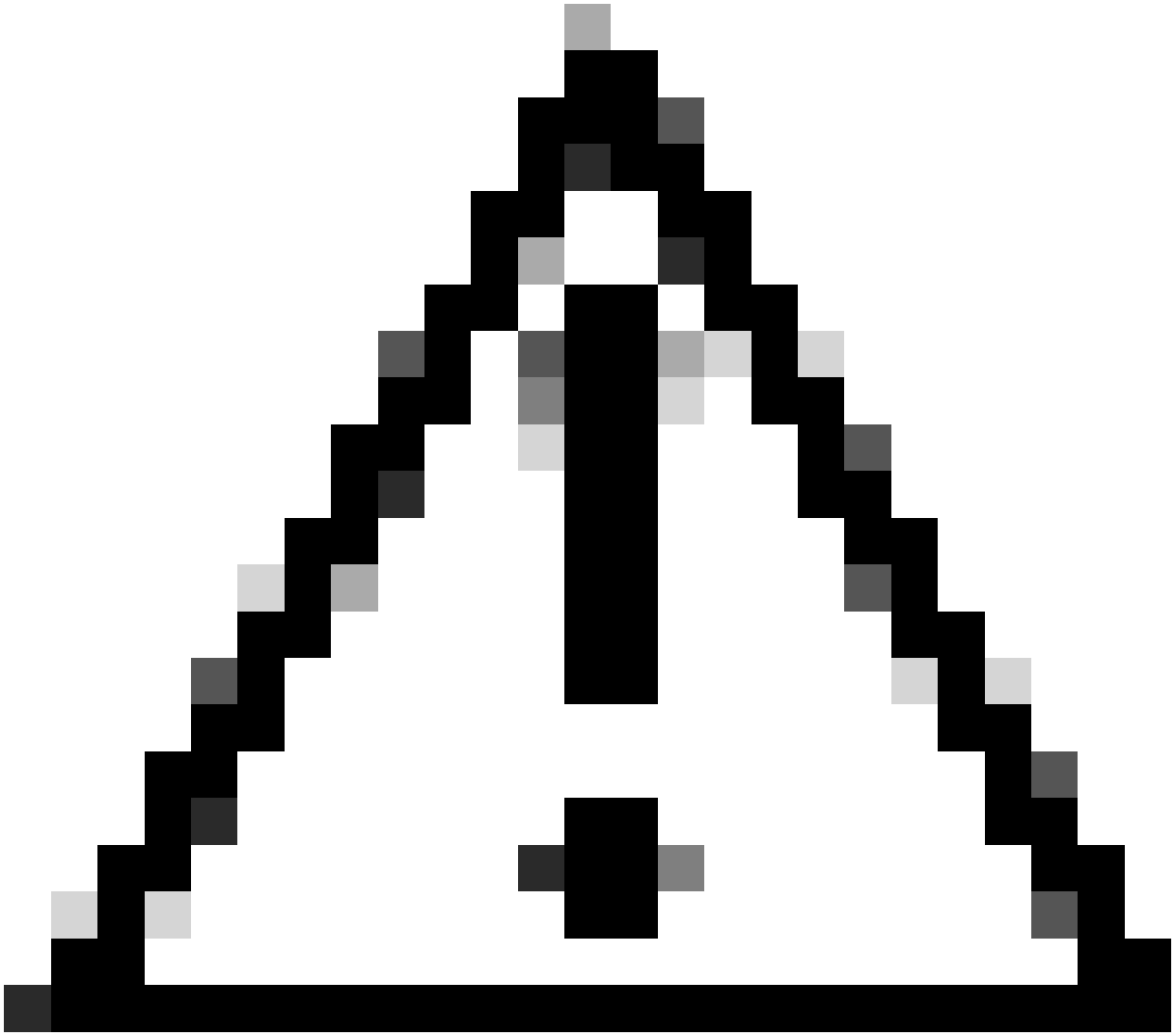


Image - Télécharger CSR

Étape 5.3. (Facultatif) Vous pouvez télécharger le CSR et le signer avec le serveur AC de votre organisation, puis télécharger le certificat signé et l'envoyer.



Attention : si vous souhaitez signer le CSR avec votre serveur AC, veillez à envoyer et à valider la page avant de signer ou de télécharger le certificat signé. Le profil que vous avez créé lors du processus de génération CSR inclut votre clé privée.

Étape 5.4.Envoyer si le certificat auto-signé actuel est approprié.

Étape 5.5. Passez à l'étape 7.

Étape 6. Si vous choisissez Importer un certificat.

Étape 6.1. Importer le fichier de certificat (le format PKCS#12 est requis).

Étape 6.2. Saisissez le mot de passe du fichier de certificat.

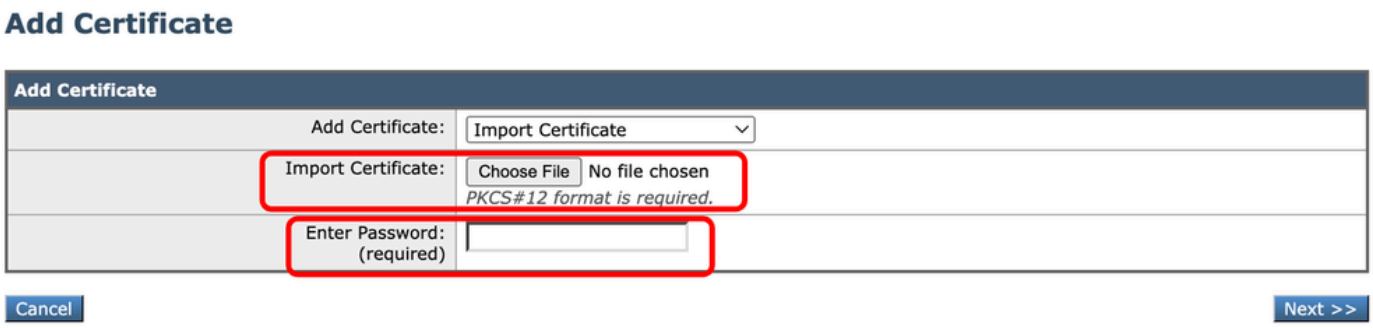


Image - Importer le certificat

Étape 6.3. Cliquez sur Next (Suivant).

Étape 6.4. Soumettre les modifications.

Étape 7. Valider les modifications.

Étape 8. Connectez-vous à la CLI.

Étape 9. Tapez certconfig et appuyez sur Entrée.

Étape 10. Tapez SETUP.

Étape 11. Tapez Y, puis appuyez sur Entrée.

Remarque : lorsque le certificat est modifié, les utilisateurs administratifs actuellement connectés à l'interface utilisateur Web peuvent rencontrer une erreur de connexion et perdre les modifications non envoyées. Cela se produit uniquement si le certificat n'est pas déjà marqué comme approuvé par le navigateur.

Étape 12. Choisissez 2 pour effectuer votre sélection dans la liste des certificats disponibles.

Étape 13. Sélectionnez le numéro du certificat à utiliser pour l'interface utilisateur graphique.

Étape 14. Si vous avez un certificat intermédiaire et que vous voulez les ajouter, tapez Y sinon tapez N .

Remarque : si vous devez ajouter le certificat intermédiaire, vous devez coller le certificat intermédiaire au format PEM et terminer par '.' (point uniquement).

```
SWA_CLI> certconfig

Choose the operation you want to perform:
- SETUP - Configure security certificate and key.
- OCSPVALIDATION - Enable OCSP validation of certificates during upload
- RESTRICTCERTSIGNATURE - Enable restricted signature validation of certificates during upload
- OCSPVALIDATION_FOR_SERVER_CERT - Enable OCSP validation for server certificates
- FQDNVALIDATION - FQDN validation for certificate
[]> SETUP
```

```
Currently using the demo certificate/key for HTTPS management access.

When the certificate is changed, administrative users who are currently logged in to the web user inter
occurs only if the certificate is not already marked as trusted by the browser.

Do you want to continue? [Y]> Y

Management (HTTPS):
Choose the operation you want to perform:
1. PASTE - Copy paste cert and key manually
2. SELECT - select from available list of certificates
[1]> 2

Select the certificate you want to upload
1. SelfSignCertificate
2. SWA_GUI.cisco.com
[1]> 1

Do you want add an intermediate certificate? [N]> N

Successfully updated the certificate/key for HTTPS management access.
```

Étape 15. Tapez commit pour enregistrer les modifications.

Tester le certificat à partir de la ligne de commande

Vous pouvez vérifier le certificat en utilisant la commande openssl :

```
 openssl s_client -connect
```

```
      :
```

Dans cet exemple, le nom d'hôte est SWA.cisco.com et l'interface de gestion est définie par défaut (port TCP 8443).

Sur la deuxième ligne du résultat, vous pouvez voir les détails du certificat :

```
openssl s_client -connect SWA.cisco.com:8443
CONNECTED(00000003)
```

```
depth=0 C = US, CN = SelfSignCertificate, L = City, O = CiscoLAB, ST = State, OU = SWA
```

Erreurs courantes

Voici quelques erreurs courantes que vous pouvez rencontrer lors de la tentative de création ou de modification de votre certificat GUI.

Erreur Format PKCS#12 non valide

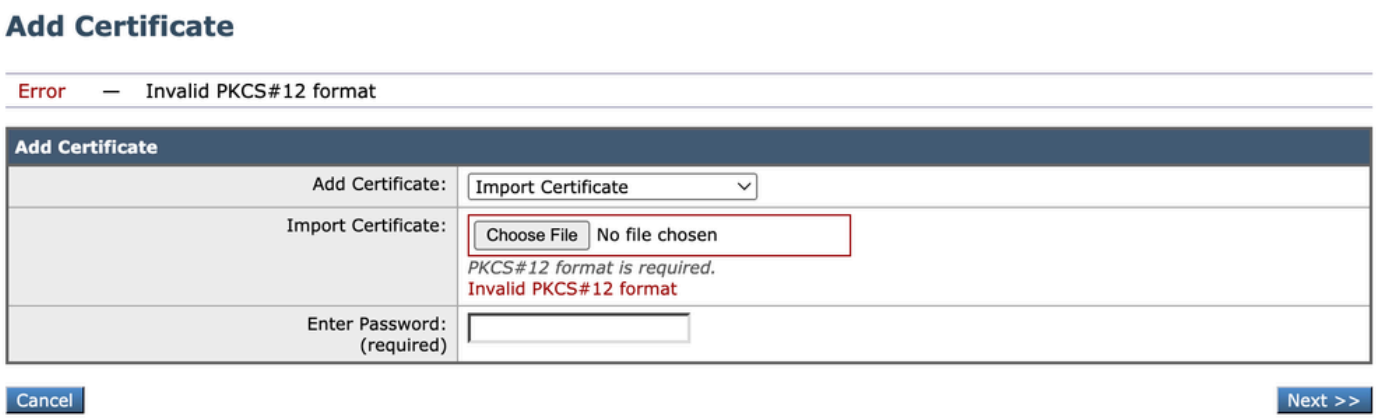


Image - Format PKCS#12 non valide

Il peut y avoir deux causes de cette erreur :

1. Le fichier de certificat est endommagé et n'est pas valide.

   Essayez d'ouvrir le certificat. Si une erreur se produit lors de l'ouverture, vous pouvez le régénérer ou le télécharger à nouveau.

2. Le CSR précédemment généré n'est plus valide.

   Lorsque vous générez un CSR, vous devez vous assurer de Soumettre et Valider vos modifications. La raison en est que votre CSR n'a pas été enregistré lorsque vous vous êtes déconnecté ou avez modifié des pages. Le profil que vous avez créé lors de la génération du CSR contient la clé privée requise pour télécharger correctement votre certificat. Une fois ce profil supprimé, la clé privée disparaît. Par conséquent, une autre CSR doit être générée, puis de nouveau transmise à votre CA.

Les jours doivent être des entiers

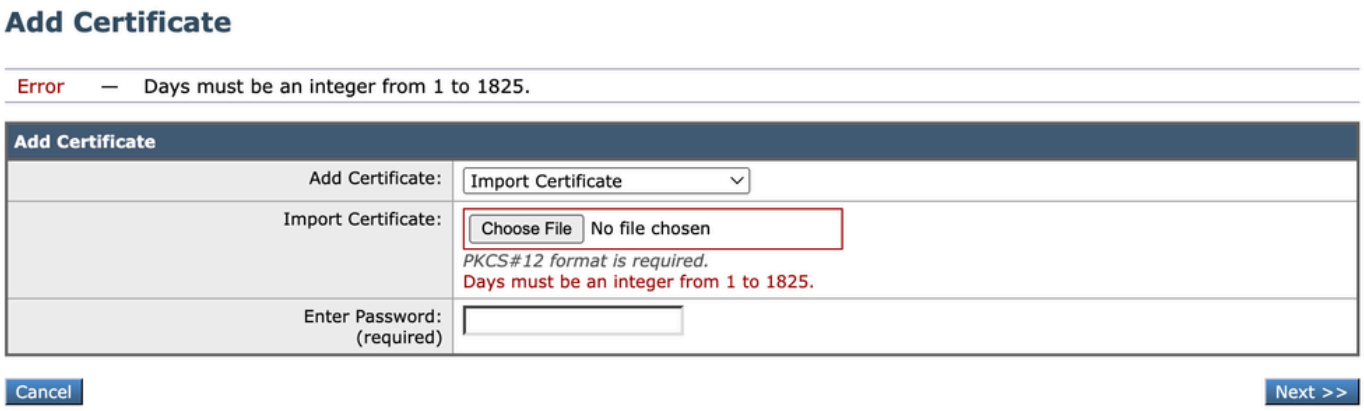


Image - Les jours doivent être une erreur d'entier

Cette erreur est due au fait que le certificat téléchargé a expiré ou a une validité de 0 jour.

Pour résoudre le problème, vérifiez la date d'expiration du certificat et assurez-vous que votre date et heure SWA sont correctes.

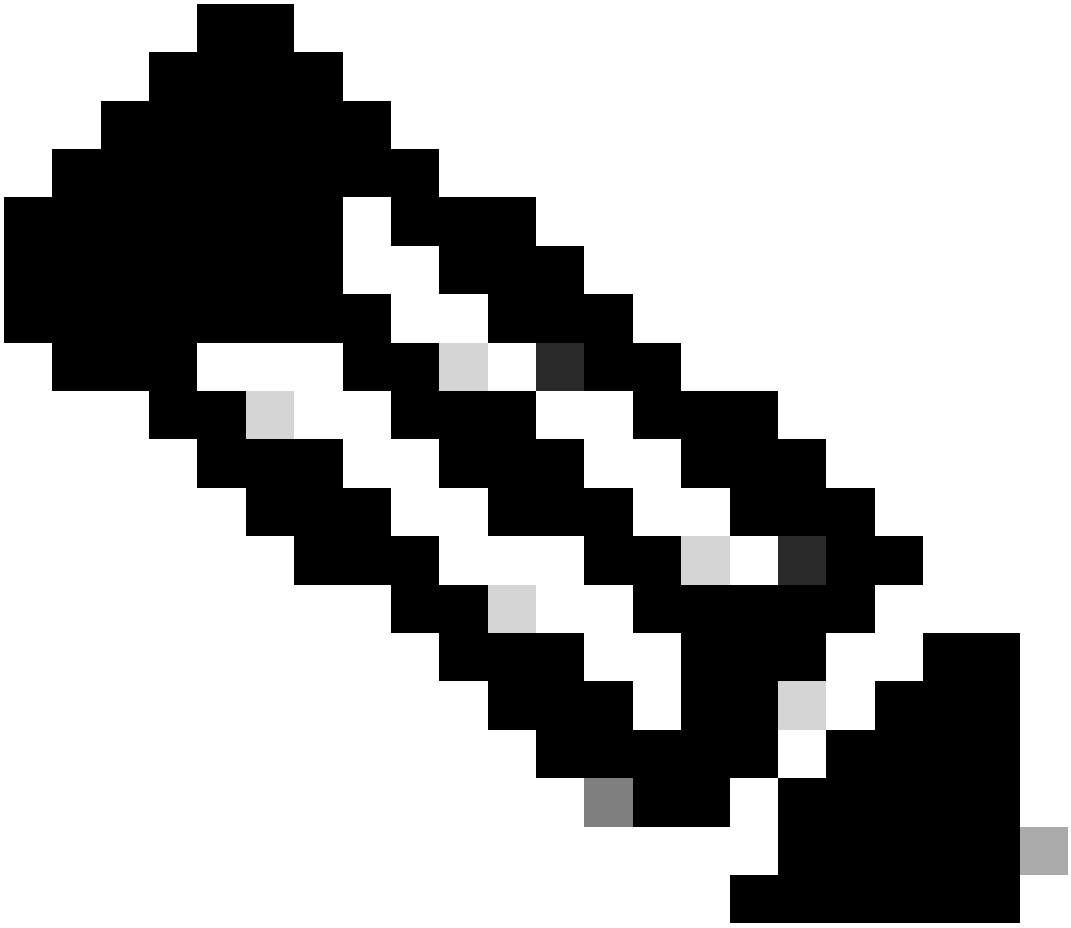
Erreur de validation du certificat

Cette erreur signifie que l'autorité de certification racine ou l'autorité de certification intermédiaire ne sont pas ajoutées à la liste des certificats racines de confiance dans SWA. Pour résoudre le problème, si vous utilisez à la fois l'autorité de certification racine et l'autorité de certification intermédiaire :

1. Téléchargez l'autorité de certification racine dans SWA, puis validez.

2. Téléchargez l'autorité de certification intermédiaire, puis confirmez à nouveau les modifications.

3. Téléchargez votre certificat GUI.



Remarque : pour télécharger l'autorité de certification racine ou intermédiaire, à partir de l'interface utilisateur graphique : Réseau. Dans la section Gestion des certificats, choisissez Gérer les certificats racine approuvés. Dans Certificats racine de confiance personnalisés, cliquez sur Importer pour télécharger vos certificats CA.

Mot de passe incorrect

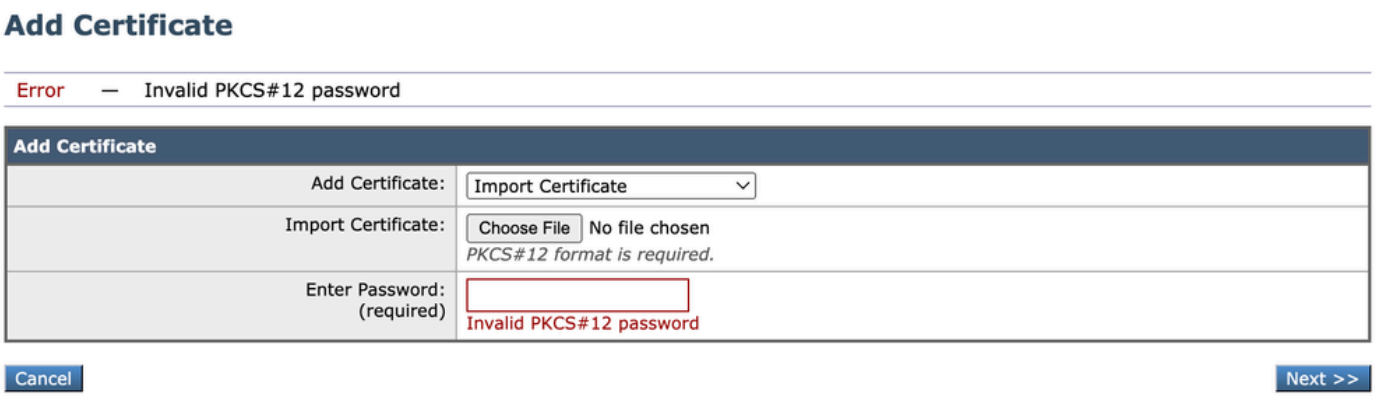


Image - Mot de passe incorrect

Cette erreur indique que le mot de passe du certificat PKCS#12 est incorrect. Pour résoudre l'erreur, tapez le mot de passe correct ou régénérez le certificat.

Le certificat n'est pas encore valide

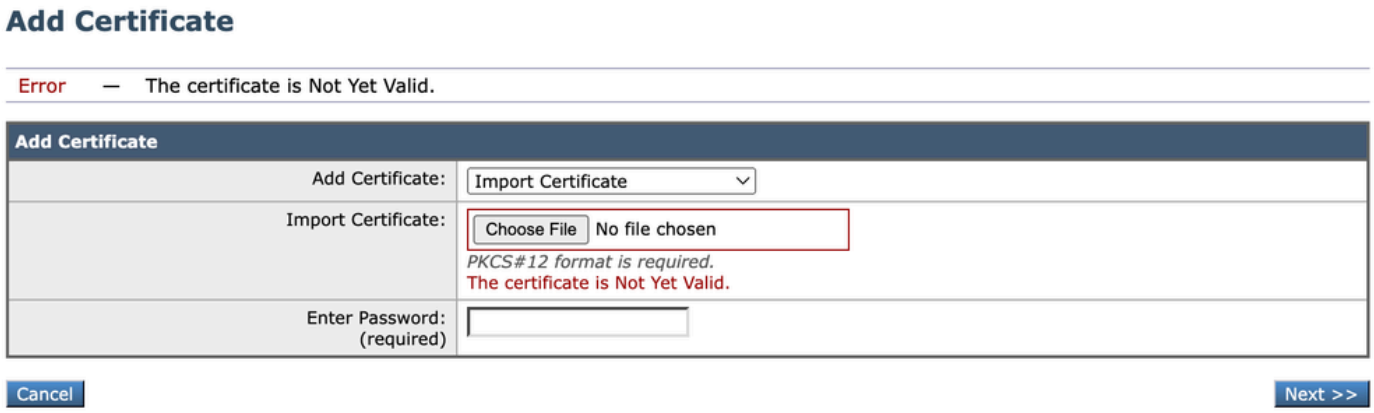
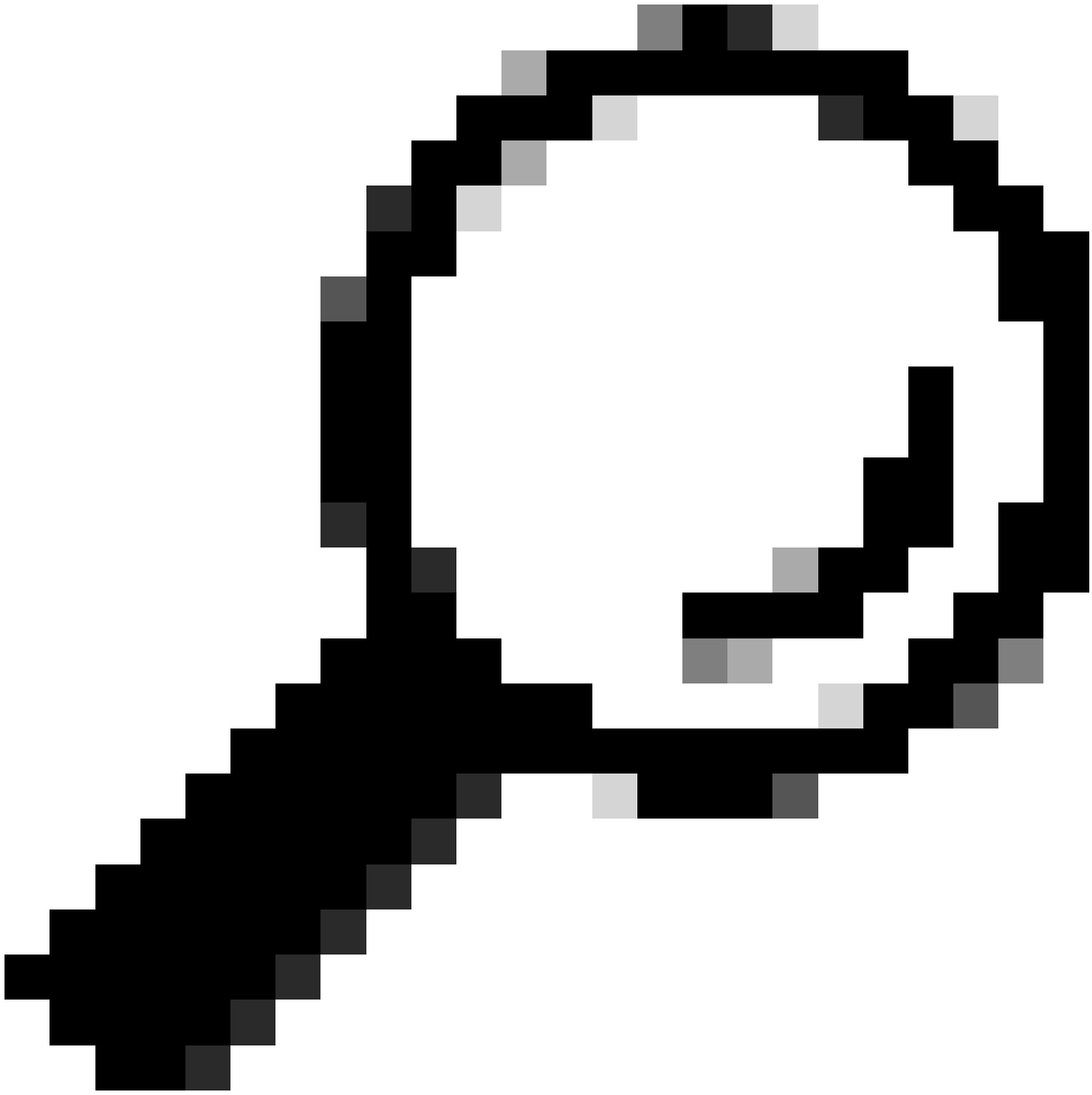


Image - Le certificat n'est pas encore valide

1. Assurez-vous que la date et l'heure de SWA sont correctes.

2. Vérifiez la date du certificat et assurez-vous que la date et l'heure « Not Before » sont correctes.



Conseil : si vous venez de générer le certificat, patientez une minute, puis téléchargez le certificat.

Redémarrer le service GUI à partir de CLI

Pour redémarrer le service WebUI, vous pouvez utiliser les étapes suivantes à partir de l'interface de ligne de commande :

Étape 1. Connectez-vous à CLI.

Étape 2. Tapez diagnostic (Il s'agit d'une commande masquée et ne saisit pas automatiquement avec TAB).

Étape 3. Sélectionnez SERVICES.

Étape 4. Sélectionnez WEBUI.

Étape 5. Sélectionnez RESTART.

Informations connexes

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance - GD(General Deployment) - Classify End-Users for Policy Application [Cisco Secure Web Appliance] - Cisco

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.