Secure Web applicatie GUI-certificaat configureren

Inhoud

Inleiding

In dit document worden de stappen beschreven voor het configureren van certificaten voor de Secure Web Appliance (SWA) Management Web Interface.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toediening van SWA.

Cisco raadt u aan het volgende te doen:

- Fysieke of virtuele SWA geïnstalleerd.
- Administratieve toegang tot de grafische gebruikersinterface van de SWA (GUI).
- Administratieve toegang tot de SWA Command Line Interface (CLI).

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Web gebruikersinterfacecertificaat

Eerst moeten we het type certificaten kiezen dat we willen gebruiken in SWA Management Web Gebruikersinterface (Web UI).

Standaard gebruikt SWA het "Cisco Application Demo Certificate:"

- CN = Cisco-democertificaat voor applicatie
- O = Cisco Systems, Inc.
- L = San Jose
- S = Californië
- C = VS

U kunt een zelfondertekend certificaat maken in SWA of uw eigen certificaat importeren dat is gegenereerd door uw interne certificaatinstantie (CA) server.

De SWA ondersteunt het opnemen van alternatieve onderwerpnamen (SAN's) bij het genereren van een aanvraag voor het ondertekenen van een certificaat (CSR) niet. Bovendien ondersteunen de zelfondertekende certificaten van de SWA de SAN-eigenschappen ook niet. Als u certificaten met SAN-kenmerken wilt gebruiken, moet u het certificaat zelf maken en ondertekenen, waarbij u ervoor moet zorgen dat het de benodigde SAN-gegevens bevat. Zodra u dit certificaat hebt gegenereerd, kunt u het uploaden naar de SWA voor gebruik. Deze benadering stelt u in staat om meerdere hostnamen, IP-adressen of andere identifiers te specificeren, waardoor u meer flexibiliteit en beveiliging voor uw netwerkomgeving kunt bieden.

 Opmerking: de certificaten moeten een privé-sleutel bevatten en in PKCS#12-formaat.

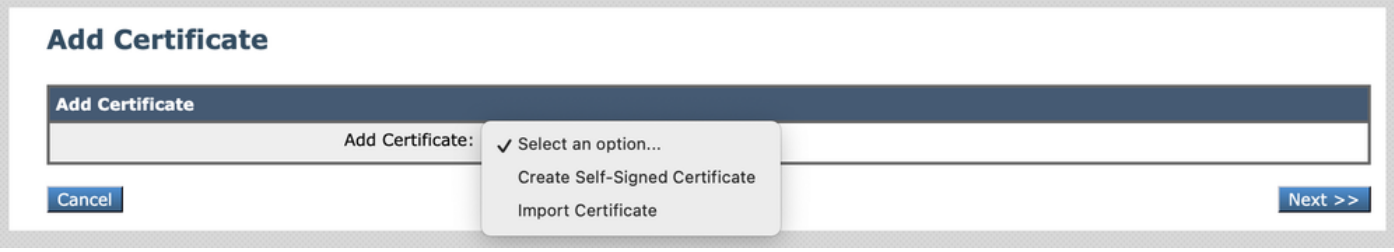
Stappen om webinterfacecertificaat te wijzigen

Stap 1. Log in op GUI en selecteer Netwerk in het bovenste menu.

Stap 2. Kies certificaatbeheer.

Stap 3. Selecteer Certificaat toevoegen van applicatie certificaten.

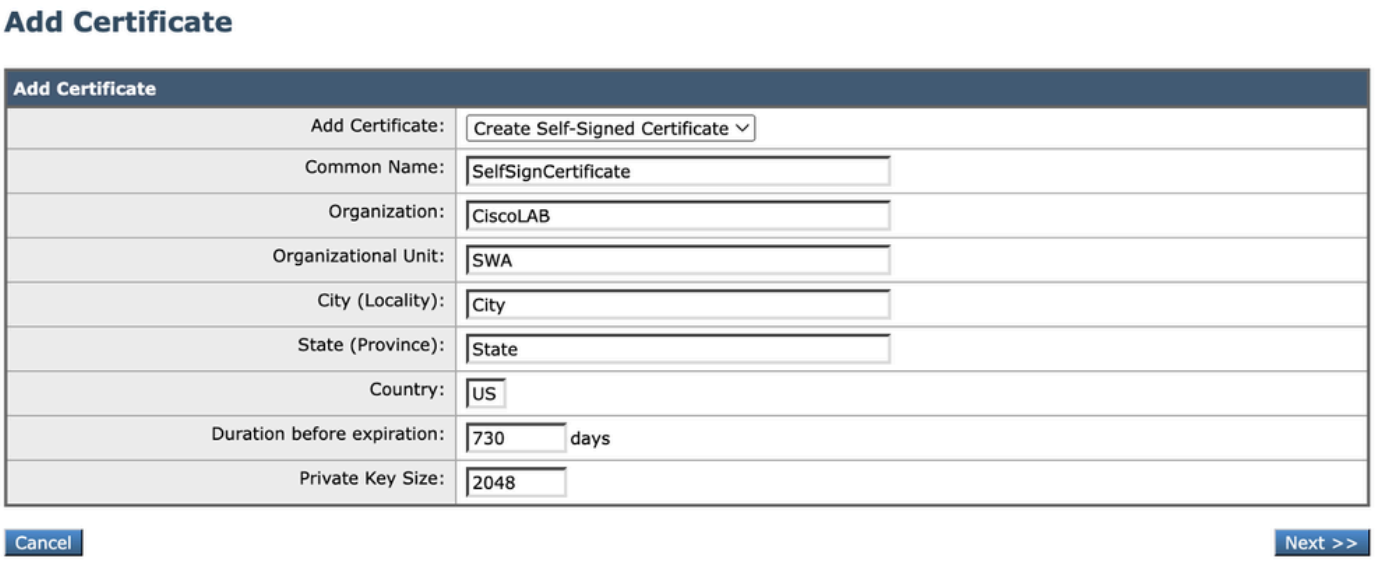
Stap 4. Selecteer certificaattype (zelfondertekend certificaat of invoercertificaat).



Afbeelding - Certificaattype kiezen

Stap 5. Als u het zelfondertekende certificaat selecteert, gebruikt u deze stappen. Anders gaat u naar stap 6.

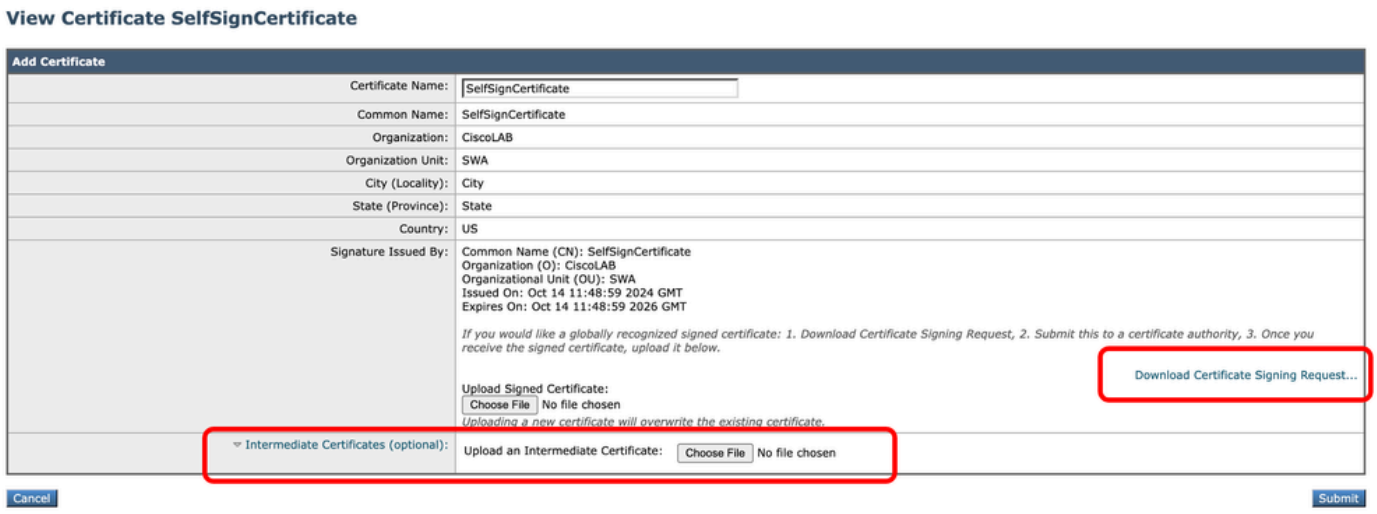
Stap 5.1. Vul de velden in.



Afbeelding - Certificaatgegevens zelfondertekening

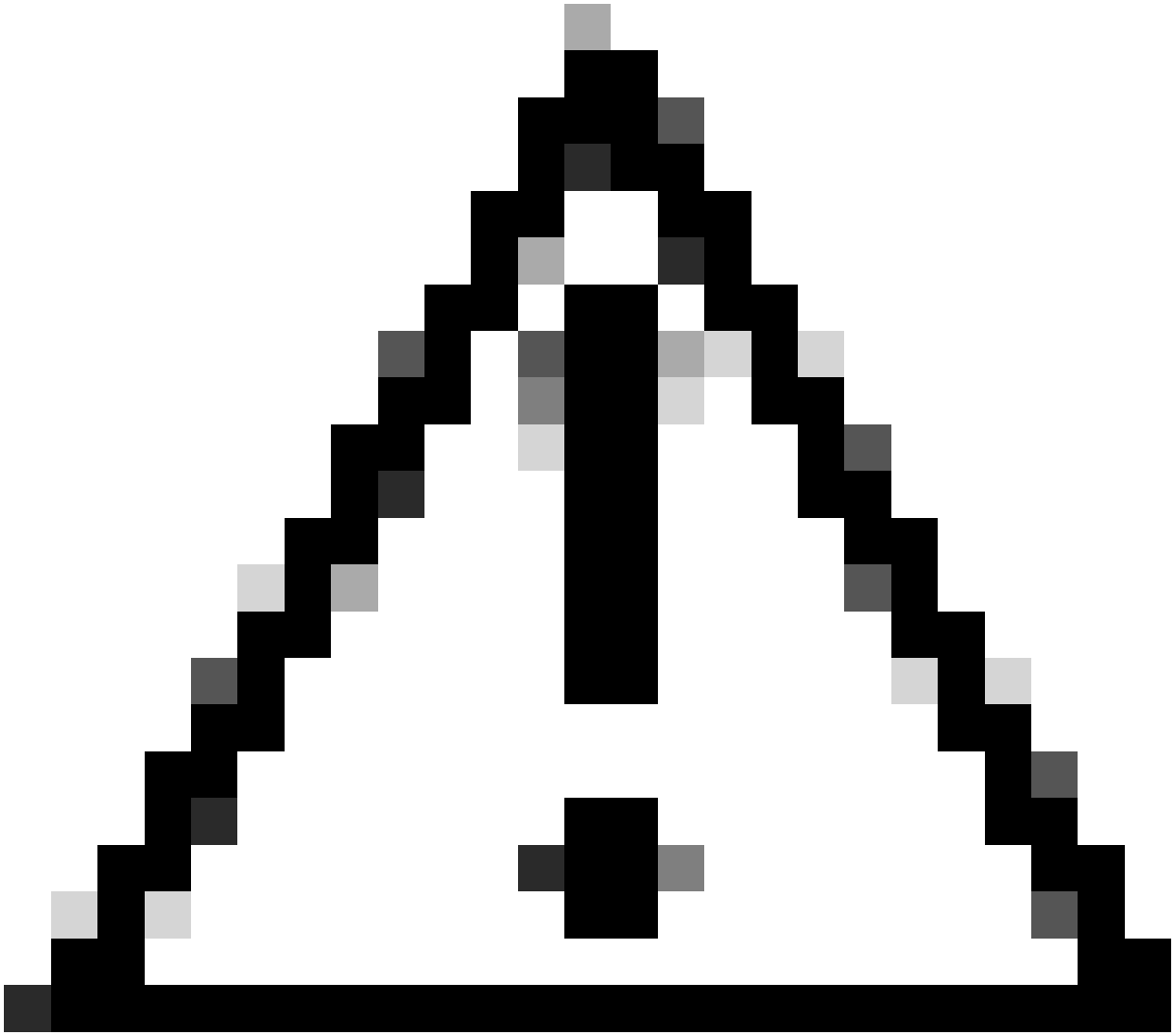
Opmerking: de grootte van de persoonlijke sleutel moet tussen 2048 en 8192 liggen.

Stap 5.2. Klik op Next (Volgende).



Afbeelding - CSR downloaden

Stap 5.3. (Optioneel) U kunt de CSR downloaden en ondertekenen met uw organisatie CA Server, vervolgens het ondertekende certificaat uploaden en verzenden.



Waarschuwing: als u de CSR wilt ondertekenen met uw CA-server, zorg er dan voor dat u de pagina indient en vastlegt voordat u het ondertekende certificaat ondertekent of uploadt. Het profiel dat u tijdens het MVO-generatieproces hebt gemaakt, bevat uw privé-sleutel.

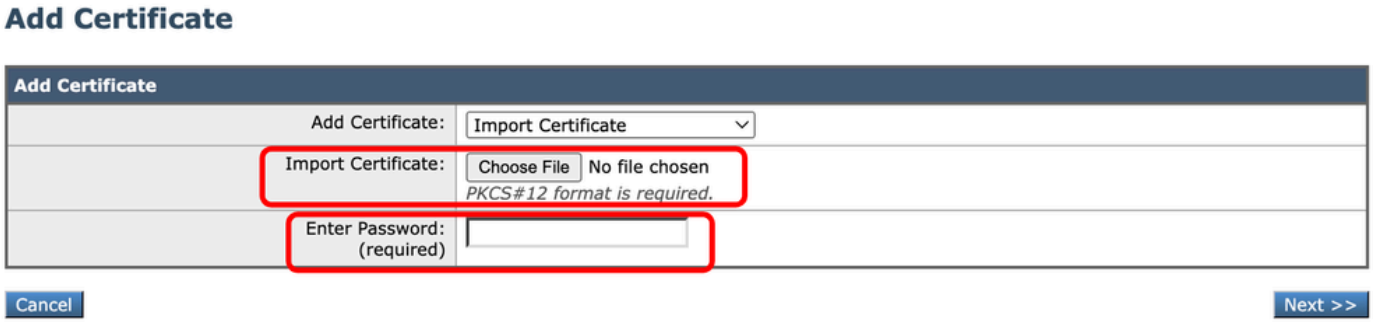
Stap 5.4.Indienen als het huidige zelfondertekende certificaat van toepassing is.

Stap 5.5. Naar Stap 7.

Stap 6. Als u Certificaat importeren kiest.

Stap 6.1. Het bestand met het invoercertificaat (PKCS#12-formaat is vereist).

Stap 6.2. Voer het wachtwoord voor het certificaatbestand in.



Afbeelding - Certificaat importeren

Stap 6.3. Klik op Next (Volgende).

Stap 6.4. Wijzigingen verzenden.

Stap 7. Wijzigingen vastleggen.

Stap 8. Log in op de CLI.

Stap 9. Typ certconfig en druk op ENTER.

Stap 10. Type INSTALLATIE.

Stap 11. Typ Y en druk op ENTER.

Opmerking: wanneer het certificaat wordt gewijzigd, kunnen beheergebruikers die momenteel zijn aangemeld bij de webgebruikersinterface een verbindingsfout ondervinden en kunnen niet-ingediende wijzigingen verloren gaan. Dit gebeurt alleen als het certificaat nog niet is gemarkeerd als vertrouwd door de browser.

Stap 12. Selecteer 2 om een van de beschikbare certificaten te selecteren.

Stap 13. Selecteer het aantal gewenste certificaten dat u voor GUI wilt gebruiken.

Stap 14. Als u een tussentijds certificaat heeft en deze wilt toevoegen Type Y anders type N .

Opmerking: als u het tussencertificaat moet toevoegen, moet u de tussenkern in PEM-formaat plakken en eindigen met '.' (Alleen punt).

```
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.
```

Stap 15. Type commit om de wijzigingen op te slaan.

Certificaat vanaf opdrachtregel testen

U kunt het certificaat controleren met de opdracht openssl:

```
 openssl s_client -connect

      :
```

In dit voorbeeld is de hostnaam SWA.cisco.com en is de beheerinterface standaard ingesteld (TCP-poort 8443).

Op de tweede regel in het uitvoerdocument ziet u de certificaatgegevens:

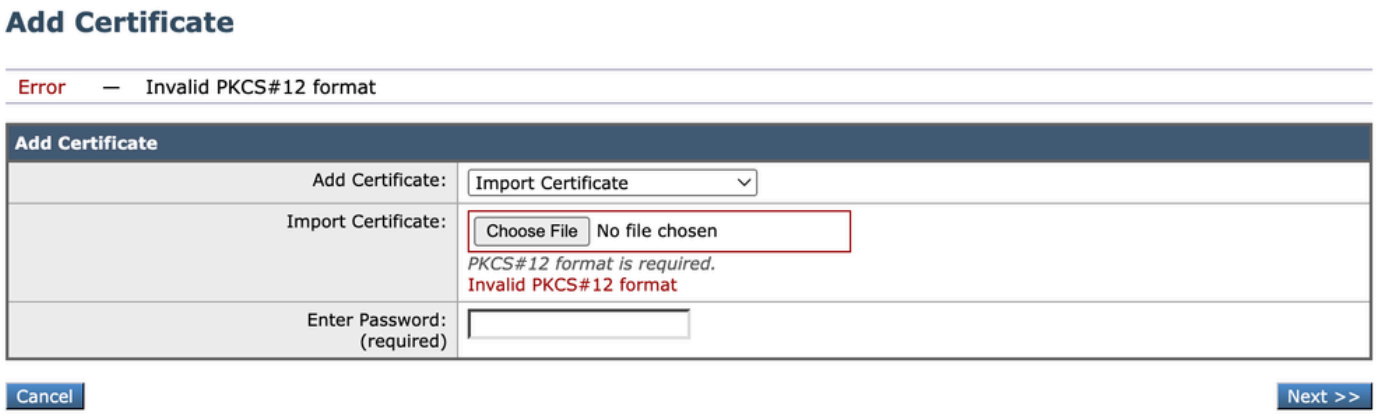
```
openssl s_client -connect SWA.cisco.com:8443
```

```
CONNECTED(00000003)
depth=0 C = US, CN = SelfSignCertificate, L = City, O = CiscoLAB, ST = State, OU = SWA
```

Veelvoorkomende fouten

Hier zijn een aantal veelvoorkomende fouten die u kunt tegenkomen tijdens het maken of wijzigen van uw GUI-certificaat.

Fout Ongeldig PKCS#12 formaat



Afbeelding - Ongeldige PKCS#12-indeling

Er kunnen twee oorzaken voor deze fout zijn:

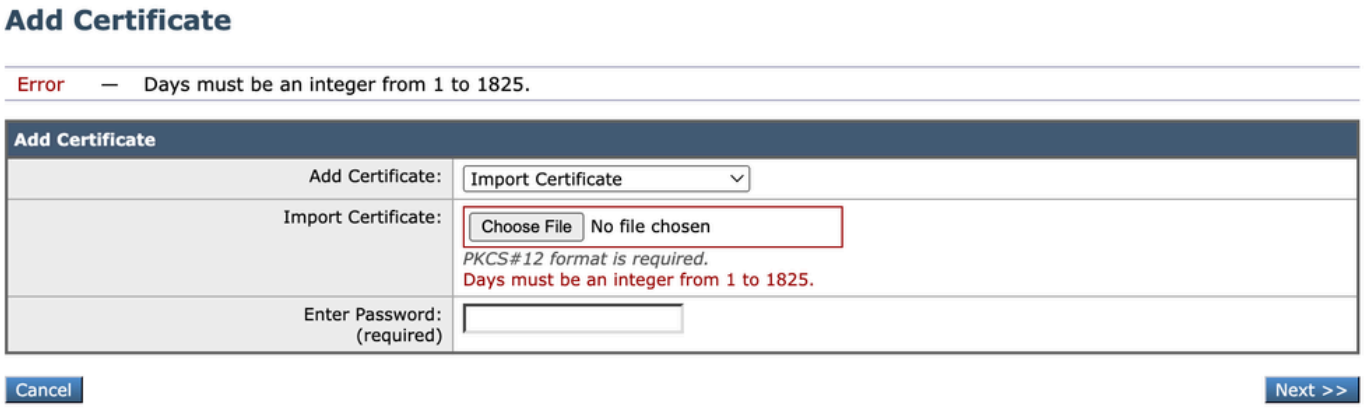
1. Het certificaatbestand is beschadigd en is niet geldig.

   Probeer het certificaat te openen. Als u een fout krijgt tijdens het openen, kunt u het certificaat opnieuw genereren of downloaden.

2. De MVO die eerder werd opgesteld, is niet langer geldig.

   Wanneer u een MVO genereert, moet u ervoor zorgen om uw veranderingen te verzenden en toe te leggen. De reden is dat uw CSR niet werd opgeslagen toen u uitlogde of pagina's veranderde. Het profiel dat u hebt gemaakt toen u de CSR genereerde, bevat de persoonlijke sleutel die vereist is voor het succesvol uploaden van uw certificaat. Zodra dit profiel is verdwenen, is de privésleutel verdwenen. Daarom moet er een andere CSR worden gegenereerd en dan opnieuw worden meegenomen naar uw CA.

Dagen moeten een geheel zijn



Afbeelding - Dagen moeten een integratiefout zijn

Deze fout is te wijten aan het geüploade certificaat dat is verlopen of dat een geldigheid van 0 dagen heeft.

Om het probleem op te lossen, controleert u de verloopdatum van het certificaat en controleert u of uw SWA-datum en -tijd juist zijn.

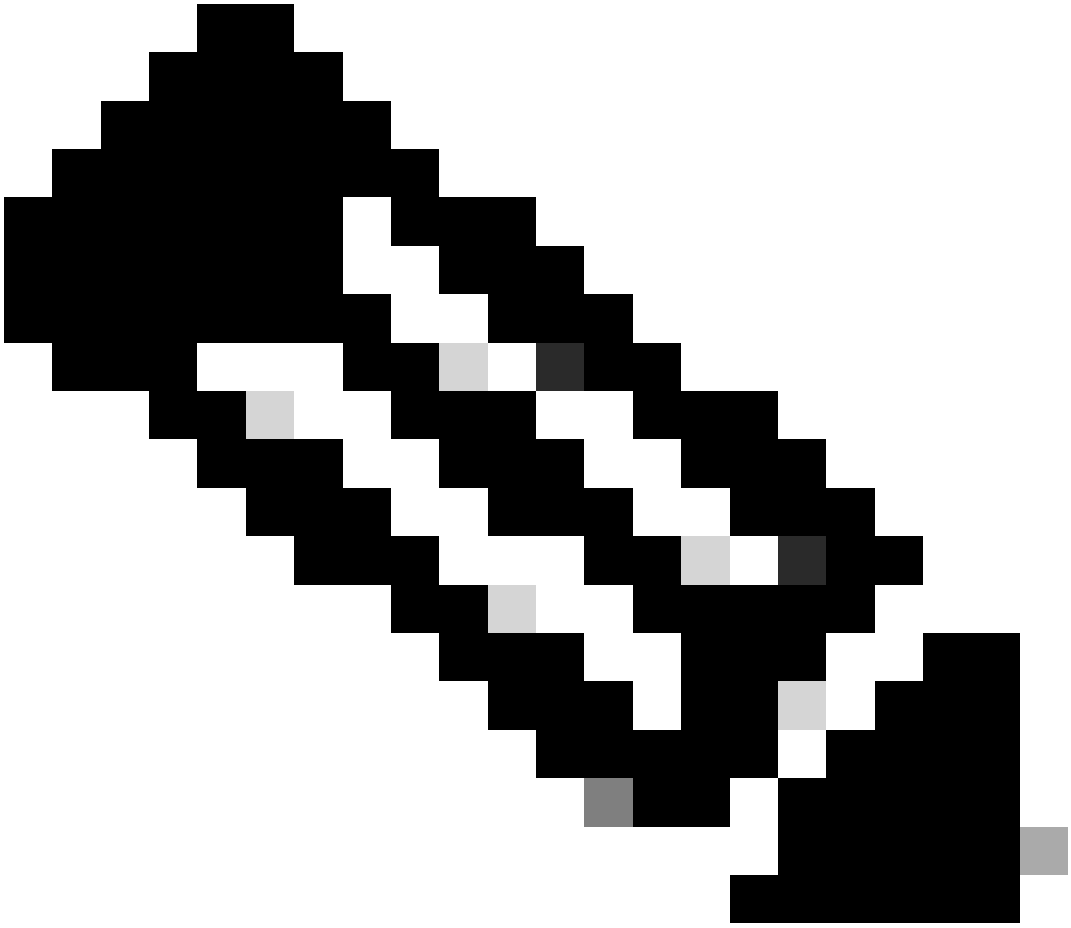
Fout bij certificaatvalidatie

Deze fout betekent dat de Root CA of de Intermediate CA niet worden toegevoegd in de lijst met Trusted Root Certificate in SWA. Om het probleem op te lossen, als u zowel Root CA als Intermediate CA gebruikt:

1. Upload de root-CA naar SWA en voer vervolgens Commit.

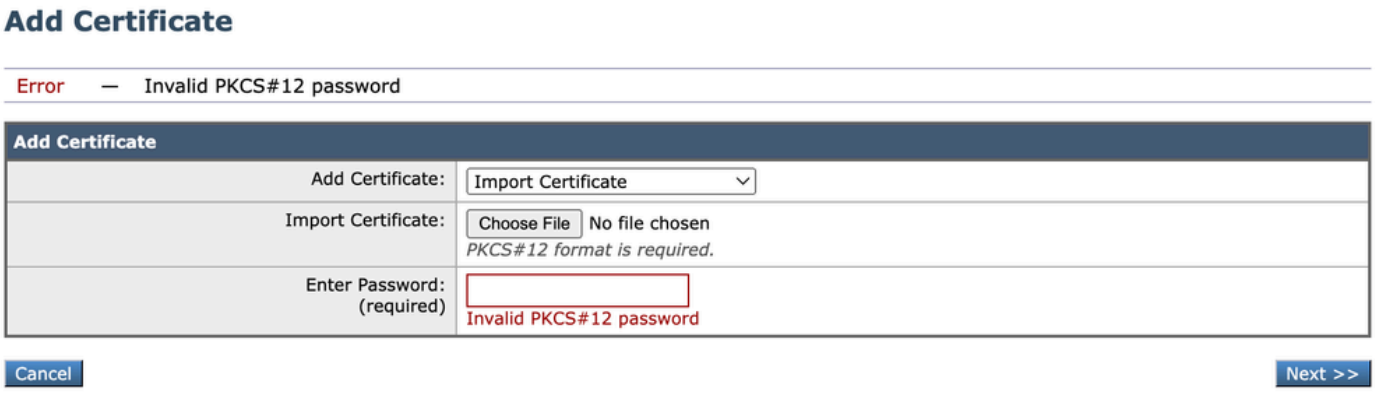
2. Upload de tussenliggende CA en leg de wijzigingen opnieuw vast.

3. Upload uw GUI-certificaat.



Opmerking: U kunt de root of tussenliggende CA uploaden via de GUI: Network. In de sectie Certificaatbeheer kiest u Trusted Root-certificaten beheren. Klik in Custom Trusted Root op Importeren om uw CA-certificaten te uploaden.

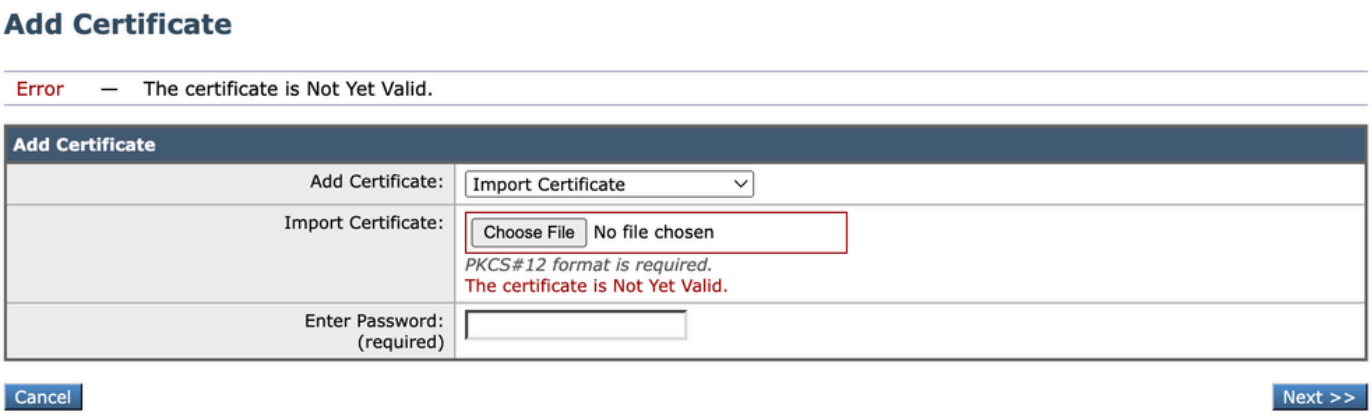
Ongeldig wachtwoord



Afbeelding - Ongeldig wachtwoord

Deze fout geeft aan dat het wachtwoord voor het PKCS#12-certificaat niet correct is. Om de fout op te lossen, typt u het juiste wachtwoord of regenereert u het certificaat.

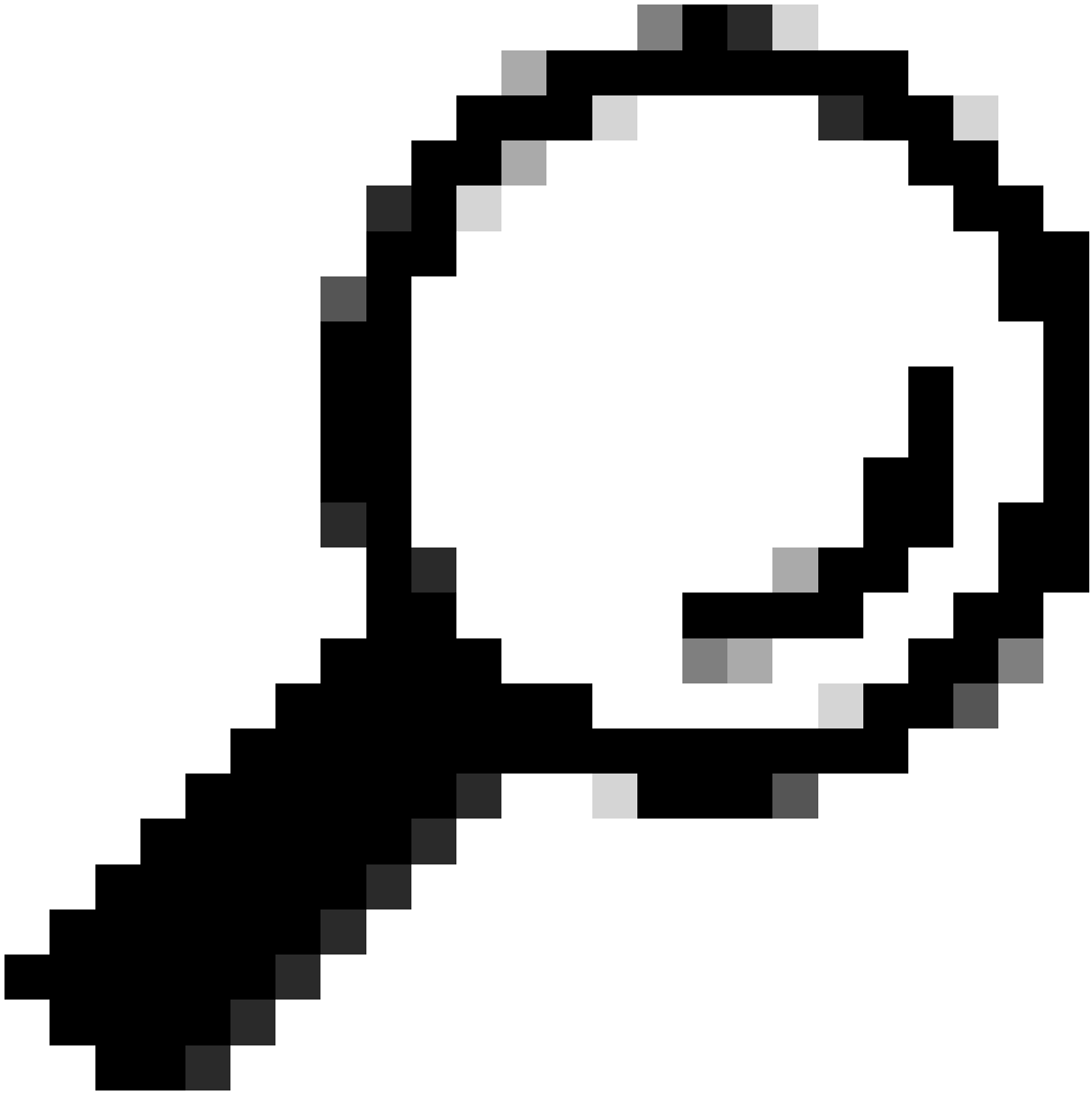
Het certificaat is nog niet geldig



Afbeelding - Het certificaat is nog niet geldig

1. Controleer of de SWA-datum en -tijd juist zijn.

2. Controleer de datum van het certificaat en controleer of de datum en het tijdstip van het certificaat "Niet voor" juist zijn.



Tip: Als u zojuist het certificaat hebt gegenereerd, wacht dan een minuut om het certificaat te uploaden.

GUI-service opnieuw starten vanaf CLI

Om de WebUI-service opnieuw te starten, kunt u deze stappen van CLI gebruiken:

Stap 1. Log in op CLI.

Stap 2. Type diagnose (Dit is een verborgen opdracht en niet automatisch met TAB).

Stap 3. Kies SERVICES.

Stap 4. Selecteer WEBUI.

Stap 5. Kies OPNIEUW STARTEN.

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Applicatie - GD (Algemene implementatie) - Classificatie van eindgebruikers voor beleidstoepassing [Cisco Secure Web Applicatie] - Cisco

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.