Configurazione del certificato GUI di Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritta la procedura per configurare i certificati per l'interfaccia Web di gestione di Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione della SWA.

Cisco raccomanda:

- SWA fisico o virtuale installato.
- Accesso amministrativo all'interfaccia grafica (GUI) SWA.
- Accesso amministrativo all'interfaccia CLI (Command Line Interface) SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Certificato interfaccia utente Web

Innanzitutto è necessario scegliere il tipo di certificati che si desidera utilizzare nell'interfaccia utente Web di gestione SWA.

Per impostazione predefinita, SWA utilizza il certificato demo dell'accessorio Cisco:

- CN = Certificato demo dell'appliance Cisco
- O = Cisco Systems, Inc
- L = San Jose
- S = California
- C = US

È possibile creare un certificato autofirmato in SWA o importare il proprio certificato generato dal server CA (Certification Authority) interno.

L'inclusione di nomi alternativi soggetto (SAN, Subject Alternative Names) non è supportata dal programma SWA durante la generazione di una richiesta di firma del certificato (CSR, Certificate Signing Request). Inoltre, i certificati autofirmati SWA non supportano nemmeno gli attributi SAN. Per utilizzare i certificati con attributi SAN, è necessario creare e firmare il certificato personalmente, verificando che includa i dettagli SAN necessari. Una volta generato il certificato, è possibile caricarlo nell'SWA per utilizzarlo. Questo approccio consente di specificare più nomi host, indirizzi IP o altri identificatori, fornendo una maggiore flessibilità e sicurezza per l'ambiente di rete.

 Nota: i certificati devono includere la chiave privata e deve essere in formato PKCS#12.

Procedura per la modifica del certificato dell'interfaccia Web

Passaggio 1. Accedere alla GUI e selezionare Network (Rete) dal menu in alto.

Passaggio 2. Scegliere Gestione certificati.

Passaggio 3. In Certificati Accessorio Selezionare Aggiungi Certificato.

Passaggio 4. Selezionare il tipo di certificato (certificato autofirmato o certificato di importazione).

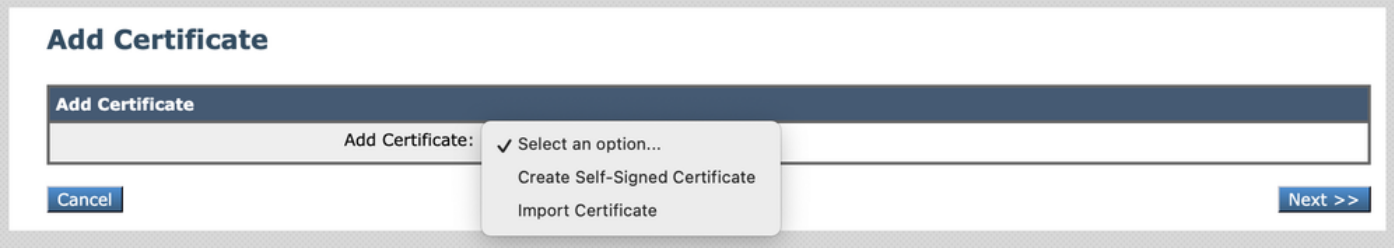


Immagine - Scegli tipo di certificato

Passaggio 5. Se si seleziona il certificato autofirmato, attenersi alla seguente procedura. In caso contrario, andare al Passaggio 6.

Passaggio 5.1. Completare i campi.

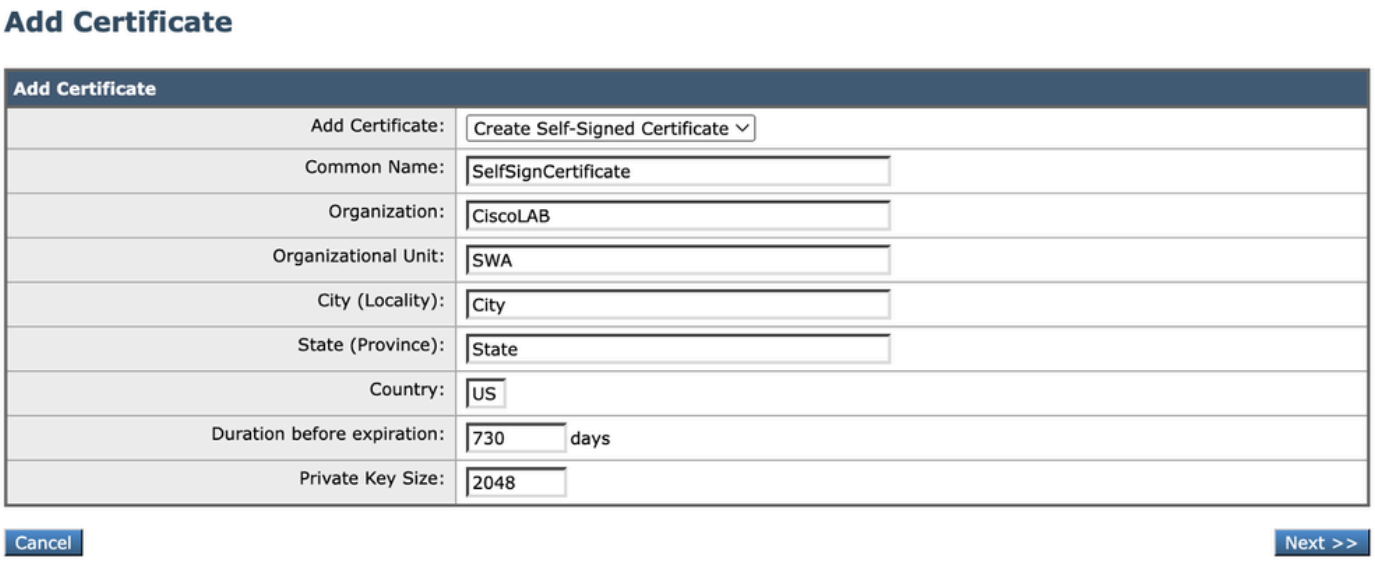


Immagine - Dettagli certificato autofirmato

Nota: le dimensioni della chiave privata devono essere comprese tra 2048 e 8192.

Passaggio 5.2. Fare clic su Next (Avanti).

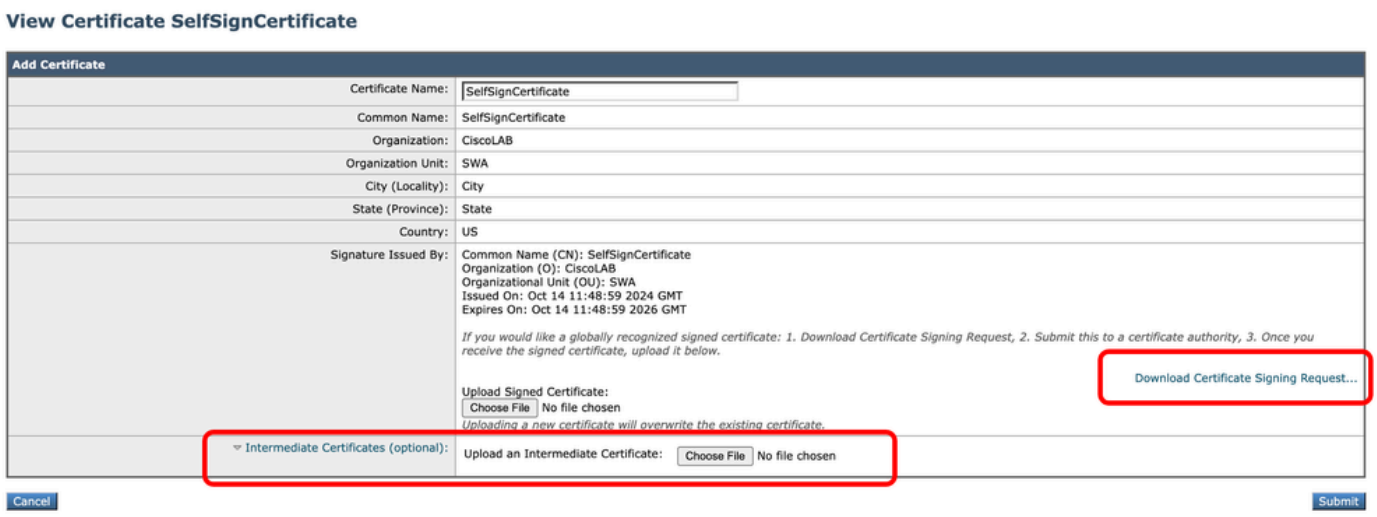
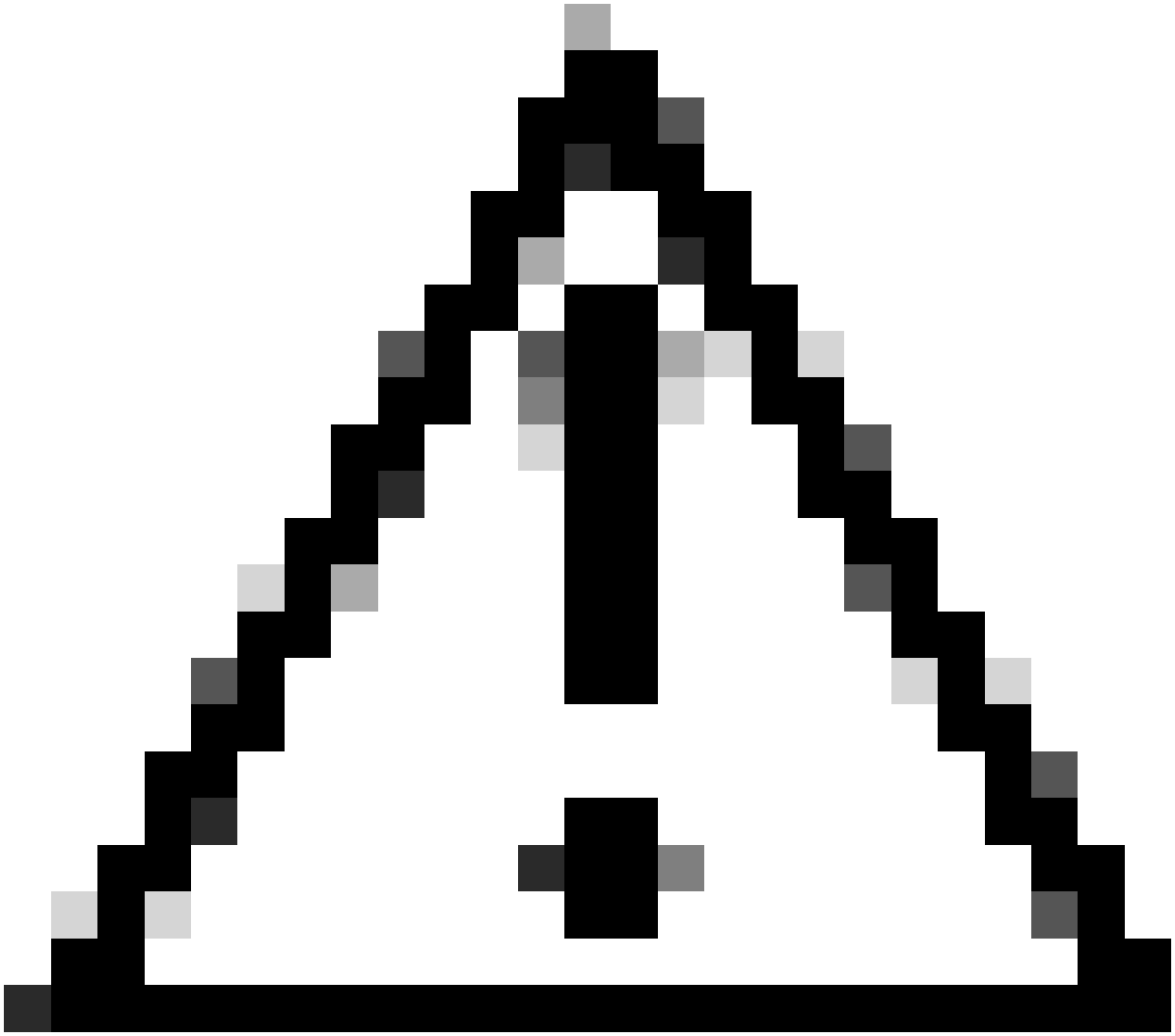


Immagine - Scarica CSR

Passaggio 5.3. (Facoltativo) È possibile scaricare il CSR e firmarlo con il server CA dell'organizzazione, quindi caricare il certificato firmato e inviare.



Attenzione: per firmare il CSR con il server CA, assicurarsi di inviare e confermare la pagina prima di firmare o caricare il certificato firmato. Il profilo creato durante il processo di generazione di CSR include la chiave privata.

Passaggio 5.4.Inviare se il certificato autofirmato corrente è appropriato.

Passaggio 5.5. Andare al passo 7.

Passaggio 6. Se si sceglie Importa certificato.

Passaggio 6.1. Importa file di certificato (è necessario il formato PKCS#12).

Passaggio 6.2. Immettere la password per il file del certificato.

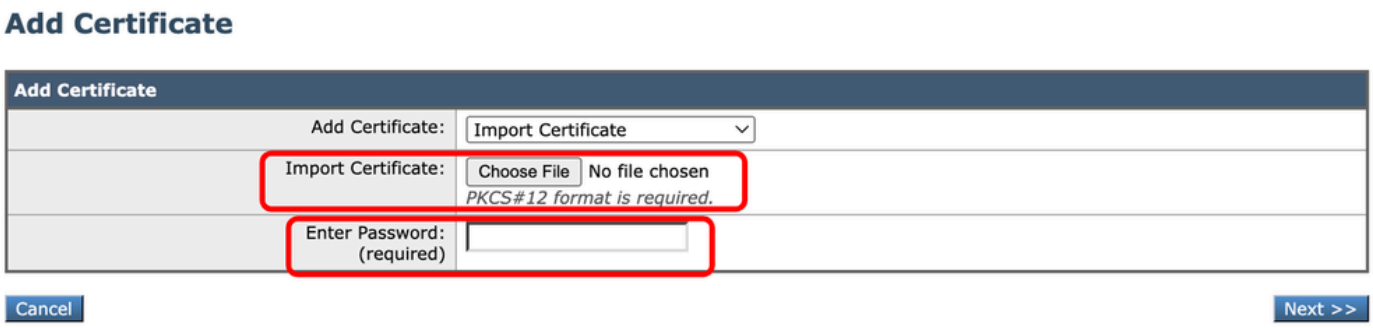


Immagine - Importa certificato

Passaggio 6.3. Fare clic su Next (Avanti).

Passaggio 6.4. Invia modifiche.

Passaggio 7. Eseguire il commit delle modifiche.

Passaggio 8. Accedere alla CLI.

Passaggio 9. Digitare certconfig e premere Invio.

Passaggio 10. Digitare SETUP.

Passaggio 11. Digitare Y, quindi premere Invio.

Nota: quando il certificato viene modificato, gli utenti amministratori che hanno eseguito l'accesso all'interfaccia utente Web possono riscontrare un errore di connessione e perdere le modifiche non inviate. Questo si verifica solo se il certificato non è già contrassegnato come attendibile dal browser.

Passaggio 12. Scegliere 2 per selezionare dall'elenco dei certificati disponibili.

Passaggio 13. Selezionare il numero del certificato desiderato da utilizzare per la GUI.

Passaggio 14. Se si dispone di un certificato intermedio e si desidera aggiungerlo Digitare Y, altrimenti digitare N .

Nota: se è necessario aggiungere il certificato intermedio, è necessario incollarlo nel formato PEM e terminare con '.' (solo punto).

```
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.
```

Passaggio 15. Digitare commit per salvare le modifiche.

Verifica certificato dalla riga di comando

È possibile controllare il certificato utilizzando il comando openssl:

```
 openssl s_client -connect

      :
```

Nell'esempio, il nome dell'host è SWA.cisco.com e l'interfaccia di gestione è impostata come predefinita (porta TCP 8443).

Nella seconda riga dell'output è possibile visualizzare i dettagli del certificato:

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

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

Errori comuni

Di seguito sono riportati alcuni errori comuni che è possibile riscontrare durante il tentativo di creare o modificare il certificato GUI.

Errore formato PKCS#12 non valido

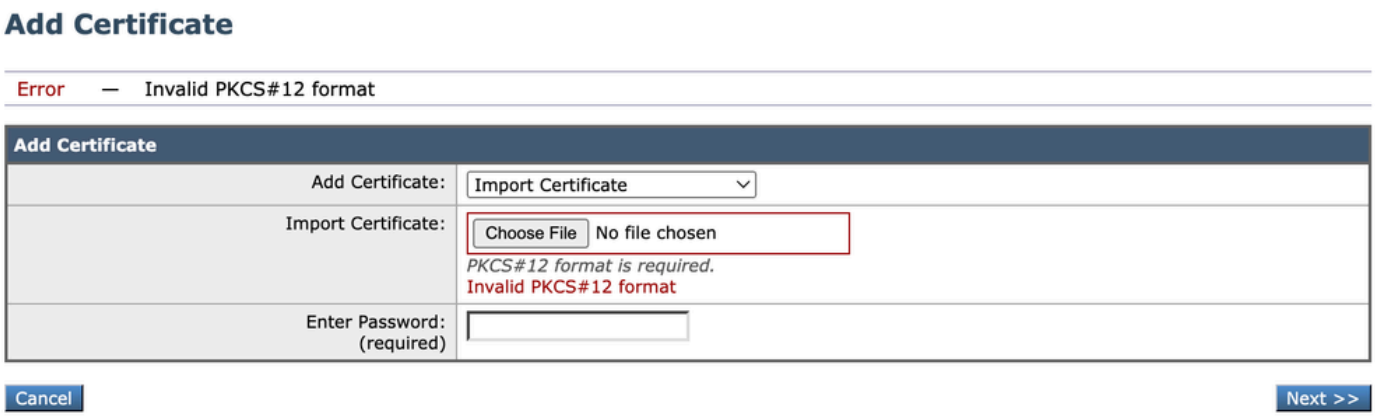


Immagine - Formato PKCS#12 non valido

L'errore può essere causato da due cause:

1. Il file del certificato è danneggiato e non è valido.

   Provare ad aprire il certificato. Se si verifica un errore durante l'apertura, sarà possibile rigenerare o scaricare di nuovo il certificato.

2. Il CSR generato in precedenza non è più valido.

   Quando si genera un CSR, è necessario assicurarsi di inviare e confermare le modifiche. Il motivo è che il CSR non è stato salvato al momento della disconnessione o della modifica delle pagine. Il profilo creato al momento della generazione del CSR contiene la chiave privata necessaria per caricare correttamente il certificato. Quando il profilo non è più disponibile, la chiave privata non è più disponibile. Pertanto, è necessario generare un altro CSR e quindi trasferirlo nuovamente alla CA.

I giorni devono essere un numero intero

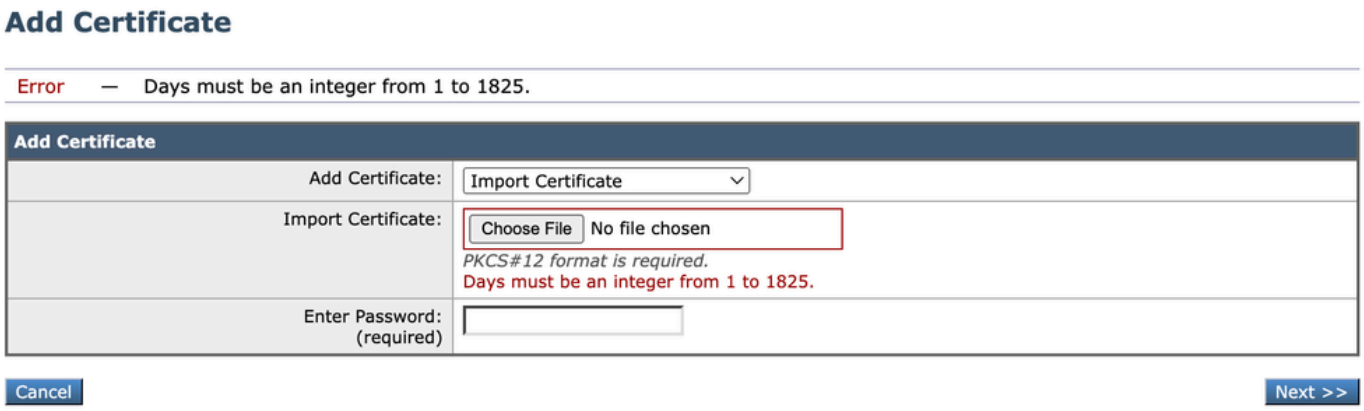


Immagine - I giorni devono essere un errore intero

Questo errore è dovuto alla scadenza o alla validità di 0 giorni del certificato caricato.

Per risolvere il problema, controllare la data di scadenza del certificato e assicurarsi che la data e l'ora SWA siano corrette.

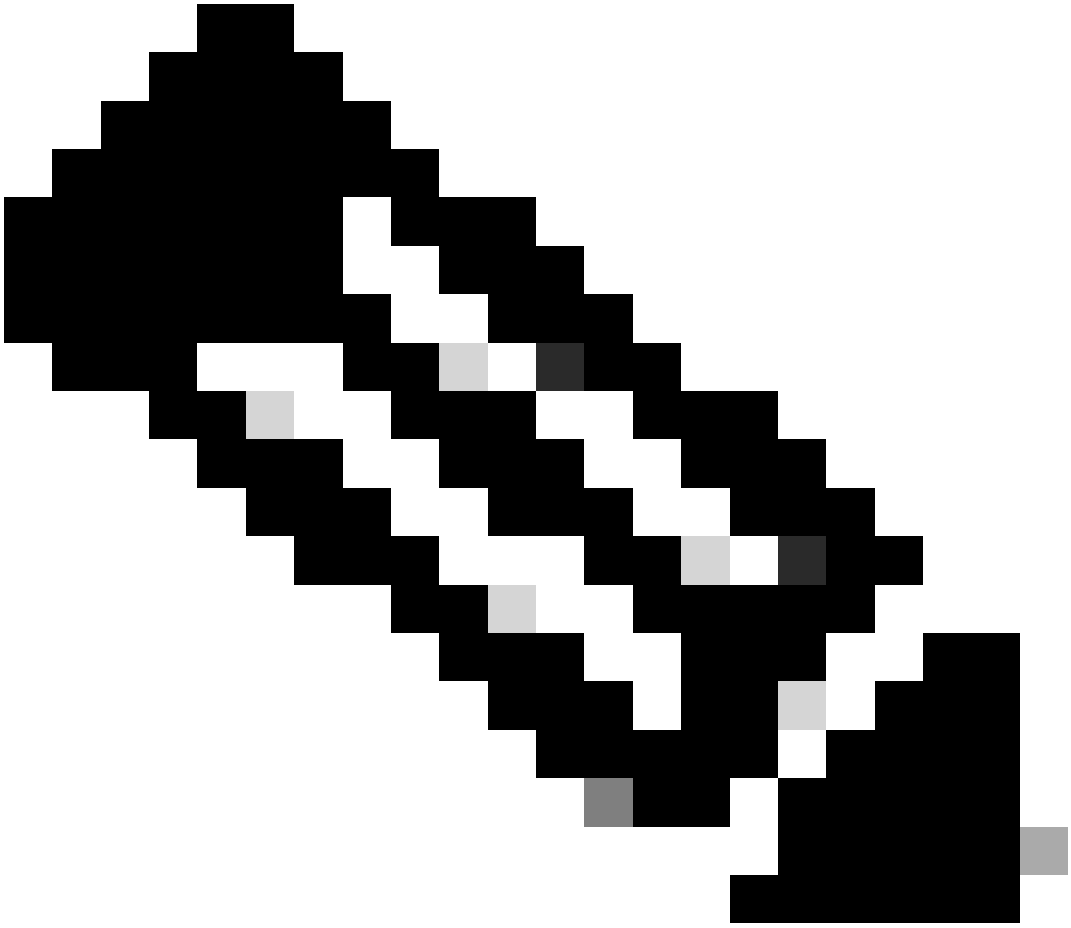
Errore di convalida del certificato

Questo errore indica che la CA radice o la CA intermedia non vengono aggiunte all'elenco dei certificati radice attendibili in SWA. Per risolvere il problema, se si utilizzano sia la CA radice che la CA intermedia:

1. Caricare la CA radice nell'SWA, quindi eseguire il commit.

2. Caricare la CA intermedia, quindi eseguire nuovamente il commit delle modifiche.

3. Caricare il certificato GUI.



Nota: per caricare la CA radice o intermedia dalla GUI: Network. Nella sezione Gestione certificati scegliere Gestisci certificati radice attendibili. In Certificati radice attendibili personalizzati fare clic su Importa per caricare i certificati CA.

Password non valida

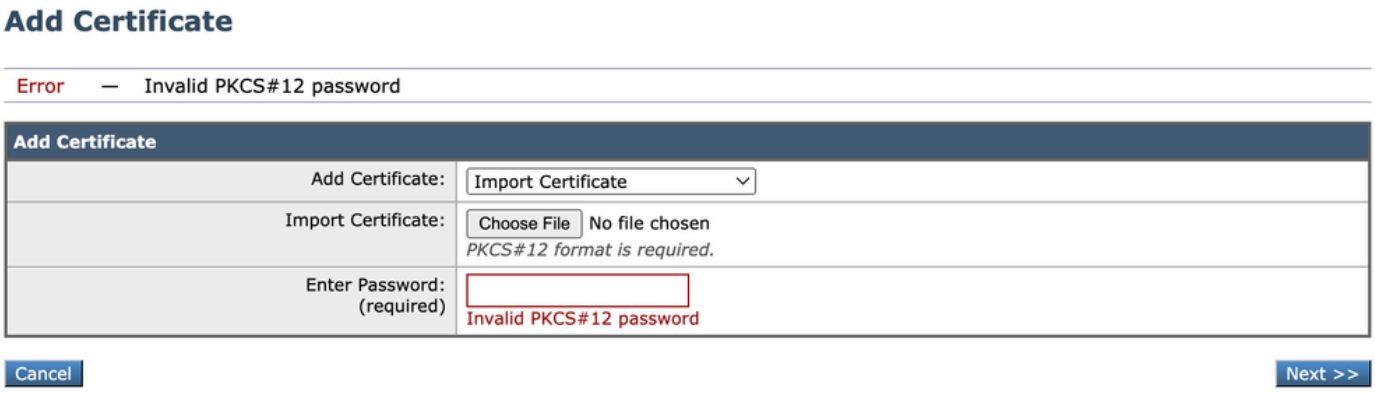


Immagine - Password non valida

Questo errore indica che la password del certificato PKCS#12 non è corretta. Per risolvere l'errore, digitare la password corretta o rigenerare il certificato.

Il certificato non è ancora valido

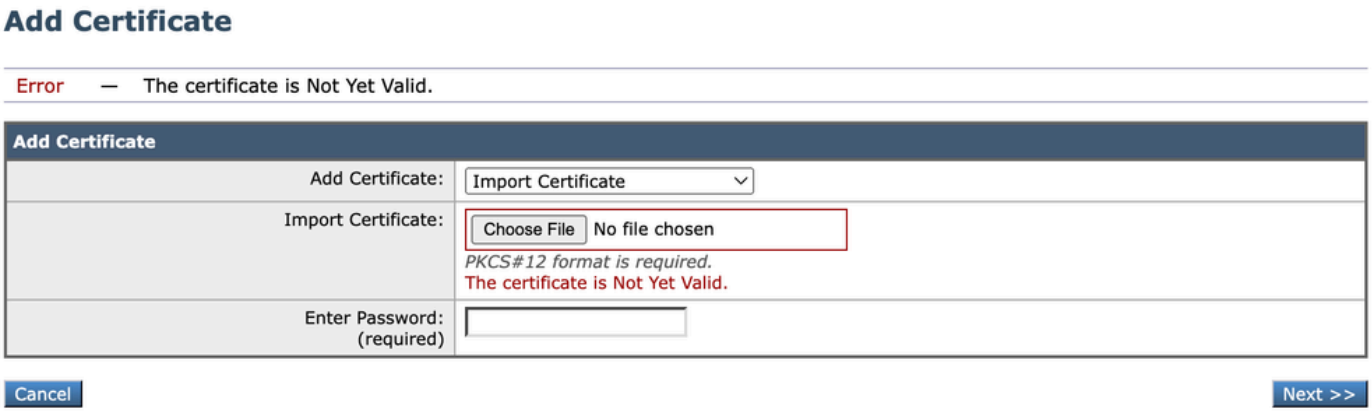
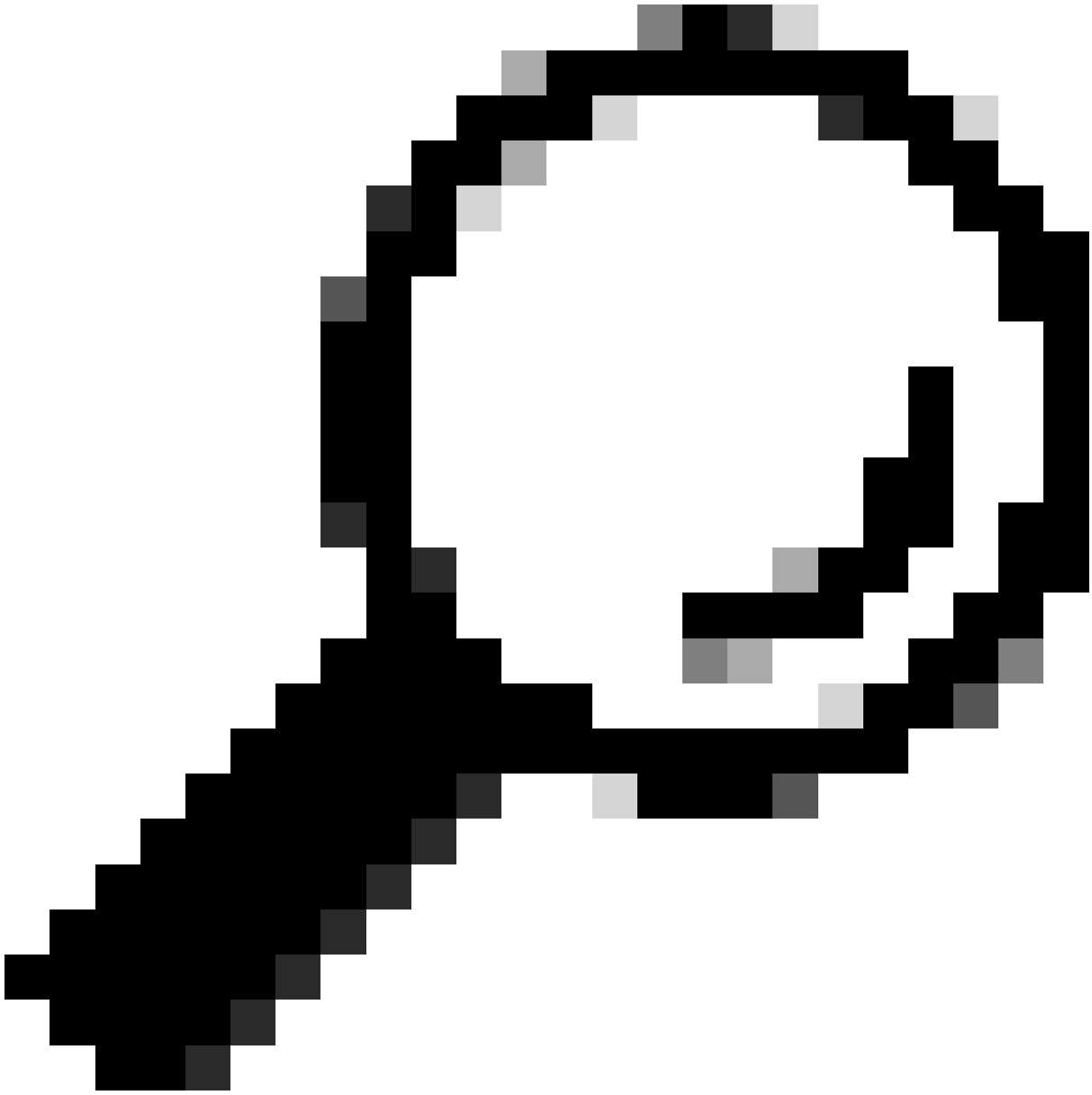


Immagine - Il certificato non è ancora valido

1. Assicurarsi che la data e l'ora SWA siano corrette.

2. Controllare la data del certificato e assicurarsi che la data e l'ora "Non prima" siano corrette.



Suggerimento: se il certificato è appena stato generato, attendere qualche minuto, quindi caricare il certificato.

Riavviare il servizio GUI dalla CLI

Per riavviare il servizio WebUI, è possibile eseguire i seguenti passaggi dalla CLI:

Passaggio 1. Accedere alla CLI.

Passaggio 2. Diagnostica tipo (comando nascosto e non digitato automaticamente con TAB).

Passaggio 3. Scegliere SERVIZI.

Passaggio 4. Selezionare WEBUI.

Passaggio 5. Scegliere RIAVVIA.

Informazioni correlate

- Guida per l'utente di AsyncOS 15.0 per Cisco Secure Web Appliance - GD (General Deployment) - Classify End-Users for Policy Application [Cisco Secure Web Appliance] - Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).