Configurar certificado de GUI do Secure Web Appliance

Contents

Introdução

Este documento descreve as etapas para configurar certificados para a interface da Web de gerenciamento do Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração SWA.

A Cisco recomenda que você:

- SWA físico ou virtual instalado.
- Acesso administrativo à interface gráfica do usuário (GUI) do SWA.
- Acesso administrativo à interface de linha de comando (CLI) do SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Certificado de interface de usuário da Web

Primeiro, precisamos escolher o tipo de certificados que queremos usar na interface de usuário da Web (IU da Web) de gerenciamento do SWA.

Por padrão, o SWA usa o "Certificado de demonstração do dispositivo Cisco:"

- CN = Certificado de demonstração do dispositivo Cisco
- O = Cisco Systems, Inc
- L = São José
- S = Califórnia
- C = EUA

Você pode criar um certificado com assinatura automática no SWA ou importar seu próprio certificado que foi gerado pelo servidor da Autoridade de certificação interna (CA).

O SWA não suporta a inclusão de SAN (Subject Alternative Names, nomes alternativos da entidade) ao gerar uma CSR (Certificate Signing Request, solicitação de assinatura de certificado). Além disso, os certificados autoassinados do SWA também não oferecem suporte a atributos SAN. Para utilizar certificados com atributos de SAN, você mesmo deve criar e assinar o certificado, garantindo que ele inclua os detalhes de SAN necessários. Depois de gerar esse certificado, você pode carregá-lo no SWA a ser usado. Essa abordagem permite que você especifique vários nomes de host, endereços IP ou outros identificadores, fornecendo maior flexibilidade e segurança para seu ambiente de rede.

 Observação: os certificados devem incluir a chave privada e devem estar no formato PKCS#12.

Etapas para modificar o certificado da interface da Web

Etapa 1. Faça login na GUI e selecione Network no menu superior.

Etapa 2. Escolha Gerenciamento de Certificados.

Etapa 3. Em Appliance Certificates Selecione Add Certificate.

Etapa 4. Selecione o tipo de certificado (certificado autoassinado ou certificado de importação).

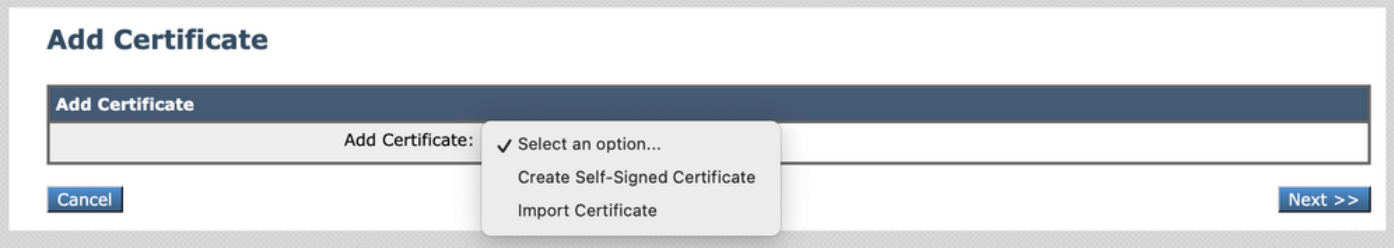


Imagem - Escolher tipo de certificado

Etapa 5. Se você selecionar o certificado autoassinado, use estas etapas. Caso contrário, vá para o passo 6.

Etapa 5.1. Complete os campos.

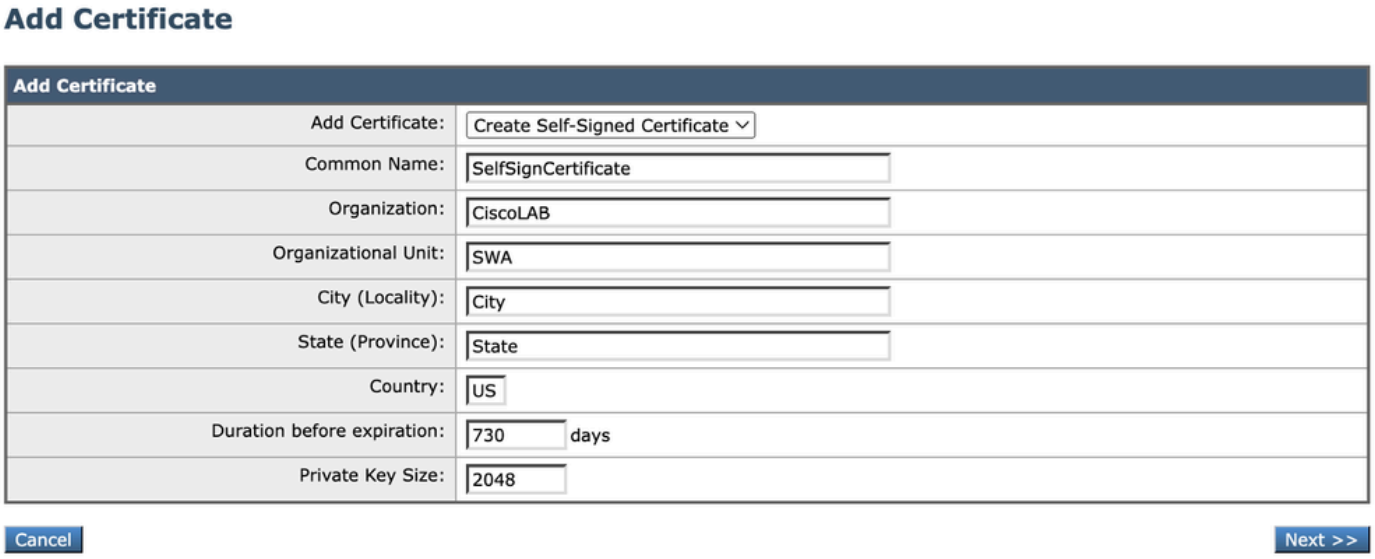


Imagem - Detalhes do certificado de autoassinatura

Observação: o tamanho da chave privada deve estar no intervalo de 2048 a 8192.

Etapa 5.2. Clique em Next.

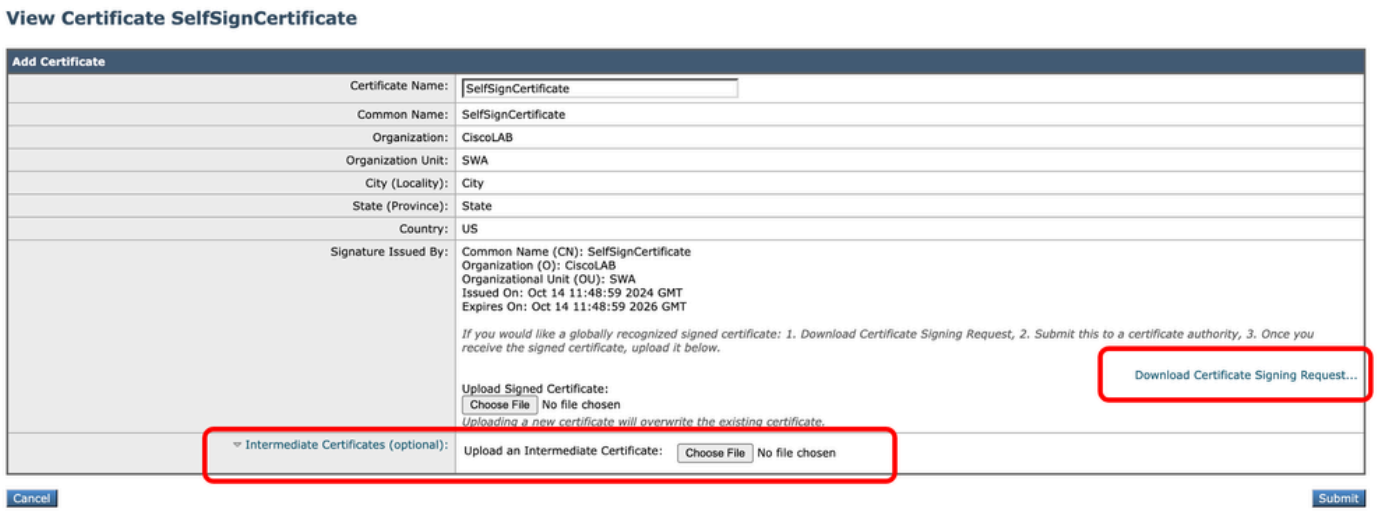
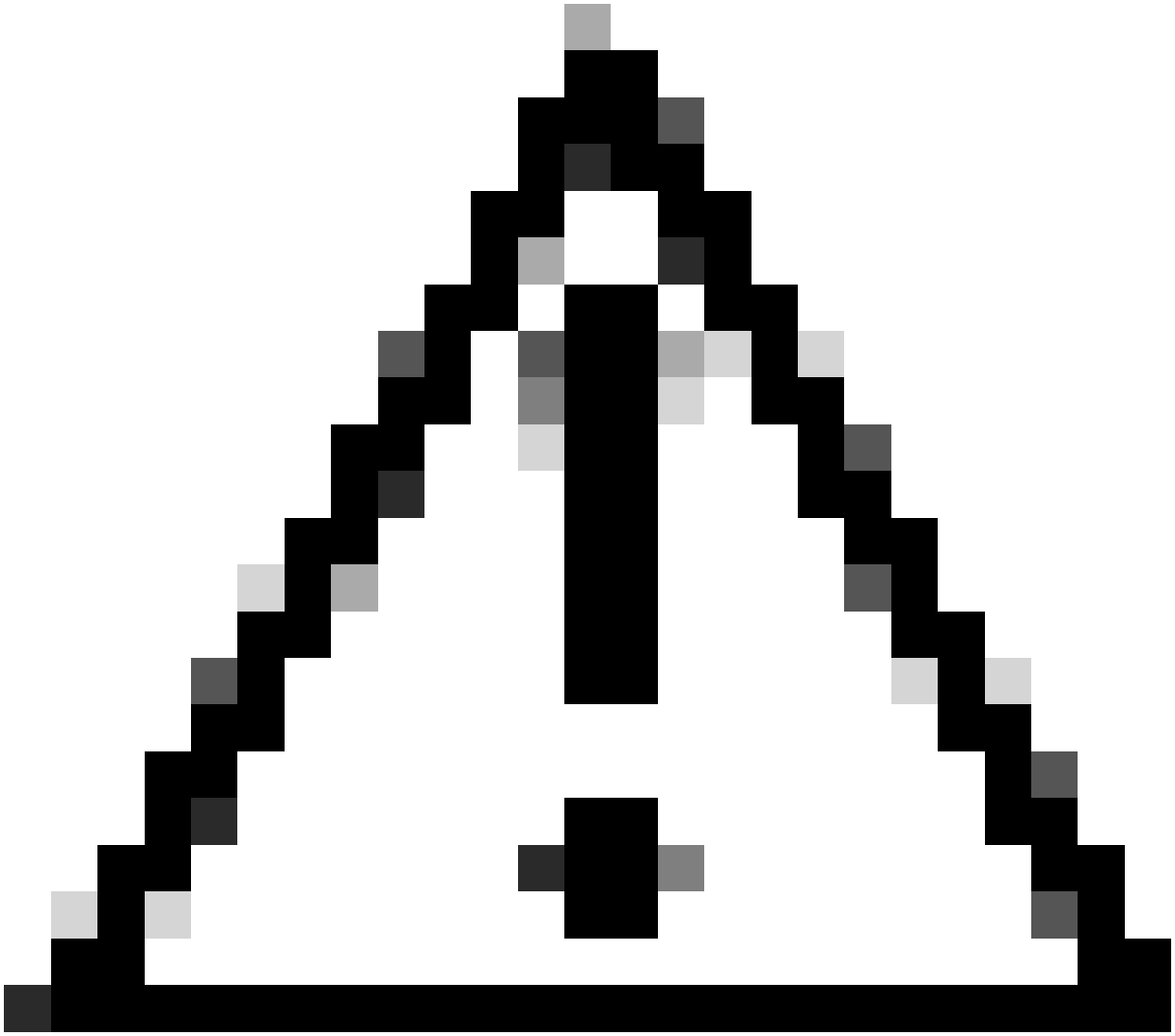


Imagem - Faça download do CSR

Etapa 5.3. (Opcional) Você pode fazer download do CSR e assiná-lo com o servidor CA da sua organização, depois carregar o certificado assinado e enviar.



Cuidado: se quiser assinar o CSR com o servidor de CA, certifique-se de Enviar e Confirmar a página antes de assinar ou carregar o certificado assinado. O perfil que você criou durante o processo de geração de CSR inclui sua chave privada.

Etapa 5.4.Enviar se o certificado autoassinado atual for apropriado.

Etapa 5.5. Vá para a Etapa 7.

Etapa 6. Se você escolher Importar certificado.

Etapa 6.1. Importar arquivo de certificado (o formato PKCS#12 é obrigatório).

Etapa 6.2. Insira a senha para o arquivo de certificado.

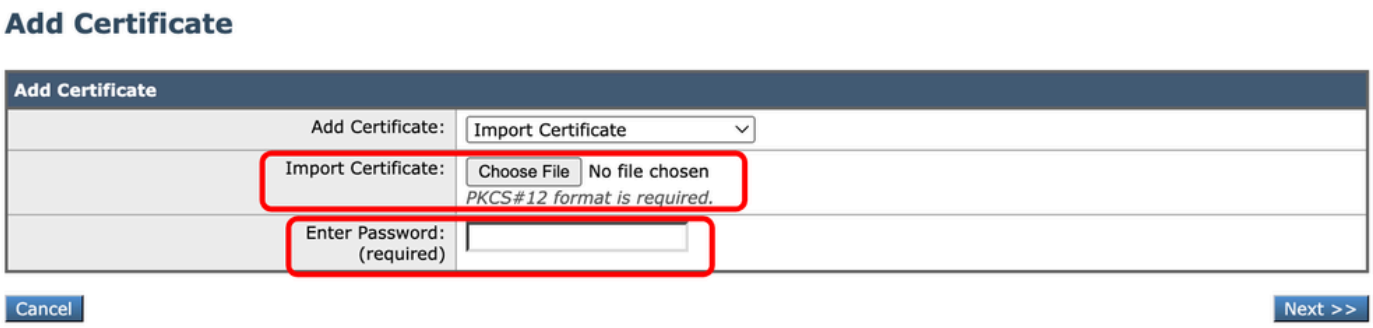


Imagem - Importar certificado

Etapa 6.3. Clique em Next.

Etapa 6.4. Enviar alterações.

Passo 7. Confirmar alterações.

Etapa 8. Faça login na CLI.

Etapa 9. Digite certconfig e pressione Enter.

Etapa 10. Digite SETUP.

Etapa 11. Digite Y e pressione Enter.

Observação: quando o certificado é alterado, os usuários administrativos que estão atualmente conectados à interface de usuário da Web podem experimentar um erro de conexão e podem perder alterações não enviadas. Isso ocorrerá somente se o certificado ainda não estiver marcado como confiável pelo navegador.

Etapa 12. Escolha 2 para selecionar na lista de certificados disponíveis.

Etapa 13. Selecione o Número do Certificado desejado a ser usado para a GUI.

Etapa 14. Se você tiver um certificado intermediário e quiser adicioná-lo, digite Y ou digite N .

Observação: se você precisar adicionar o certificado intermediário, você terá que colar o certificado intermediário no formato PEM e terminar com '.' (Somente ponto).

```
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.
```

Etapa 15. Digite commit para salvar as alterações.

Testar o certificado a partir da linha de comando

Você pode verificar o certificado usando o comando openssl:

```
 openssl s_client -connect




      :
```

Neste exemplo, o nome do host é SWA.cisco.com e a interface de gerenciamento é definida como padrão (porta TCP 8443).

Na segunda linha da saída, você pode ver os detalhes do certificado:

```
openssl s_client -connect SWA.cisco.com:8443
CONNECTED(00000003)
depth=0 C = US, CN = SelfSignCertificate, L = City, O = CiscoLAB, ST = State, OU = SWA
```

Erros comuns

Aqui estão alguns erros comuns que você pode enfrentar ao tentar criar ou modificar seu certificado de GUI.

Erro: formato PKCS#12 inválido

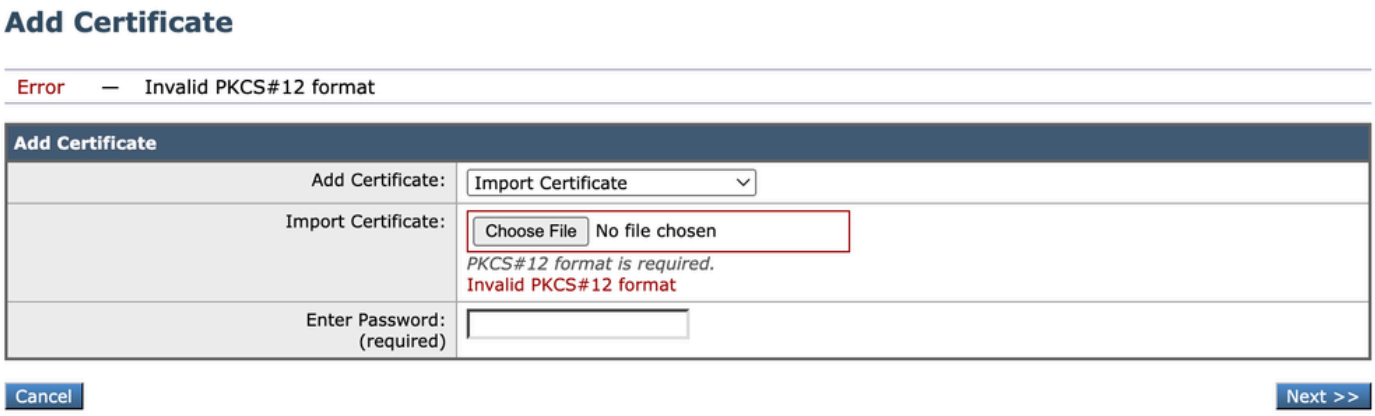


Imagem - Formato PKCS#12 inválido

Pode haver duas causas para esse erro:

1. O arquivo de certificado está danificado e não é válido.

   Tente abrir o certificado. Se você receber um erro ao abri-lo, poderá gerá-lo novamente ou baixá-lo novamente.

2. O CSR gerado anteriormente não é mais válido.

   Ao gerar um CSR, certifique-se de Enviar e Confirmar suas alterações. O motivo é que seu CSR não foi salvo quando você fez logoff ou alterou páginas. O perfil que você criou quando gerou o CSR contém a chave privada necessária para carregar o certificado com êxito. Quando esse perfil desaparecer, a chave privada desaparecerá. Portanto, outro CSR deve ser gerado e, em seguida, levado novamente para o CA.

Dias deve ser um inteiro

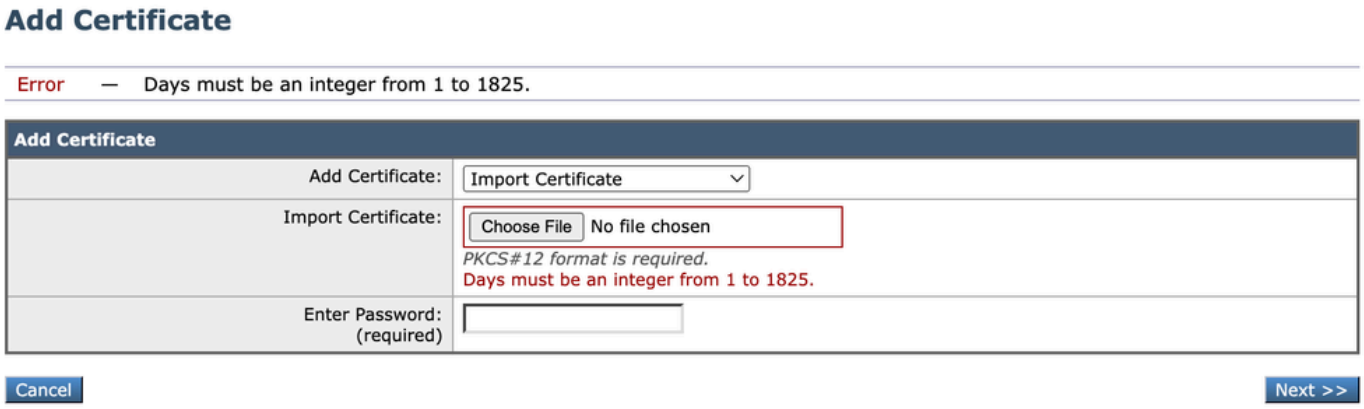


Imagem - Dias devem ser um erro inteiro

Este erro ocorre porque o certificado carregado expirou ou tem validade de 0 dias.

Para resolver o problema, verifique a data de expiração do certificado e se a data e a hora do SWA estão corretas.

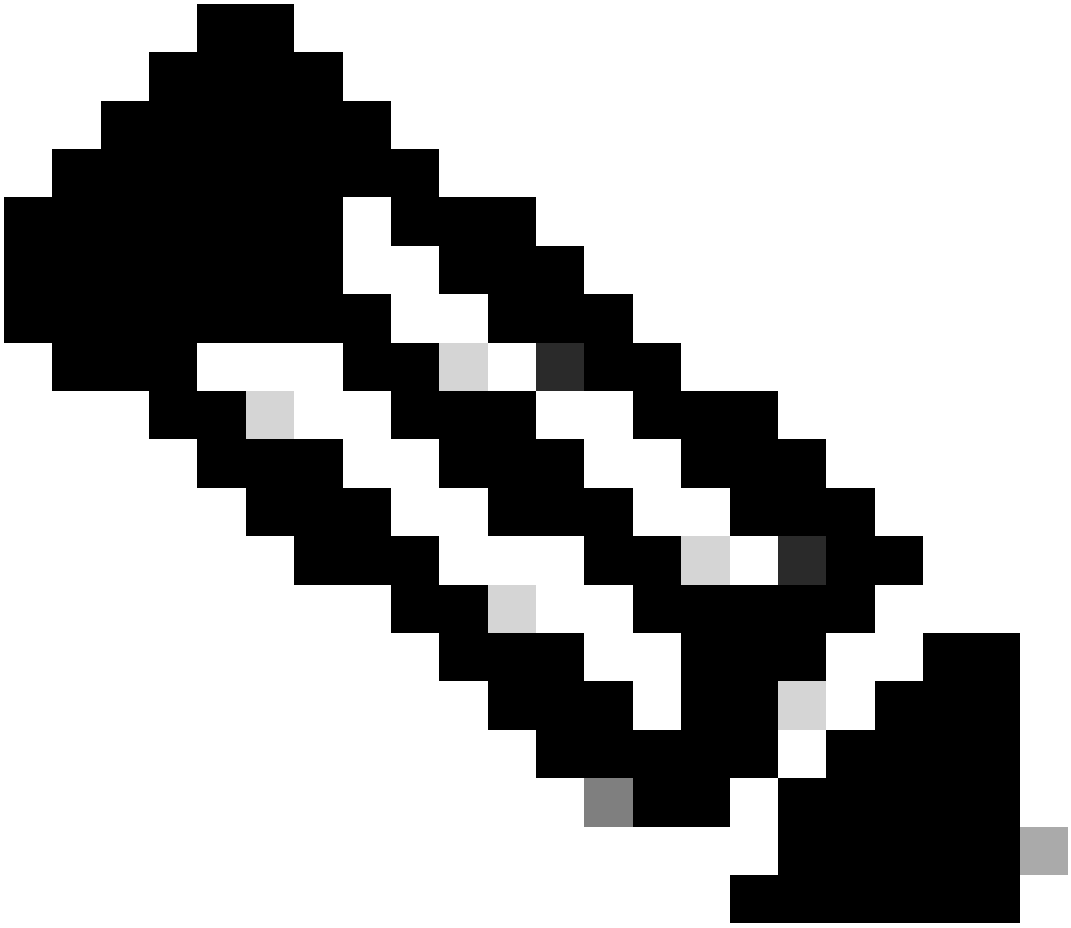
Erro de validação de certificado

Este erro significa que a CA raiz ou a CA intermediária não foram adicionadas à lista Certificado raiz confiável no SWA. Para resolver o problema, se você estiver usando CA raiz e CA intermediária:

1. Carregue a CA raiz no SWA e confirme.

2. Carregue a CA Intermediária e confirme as alterações novamente.

3. Carregue seu certificado de GUI.



Observação: para fazer upload da CA raiz ou intermediária, na GUI: Rede. Na seção Gerenciamento de Certificados, escolha Gerenciar Certificados Raiz Confiáveis. Em Custom Trusted Root Certificates, clique em Import para carregar seus certificados CA.

Senha inválida

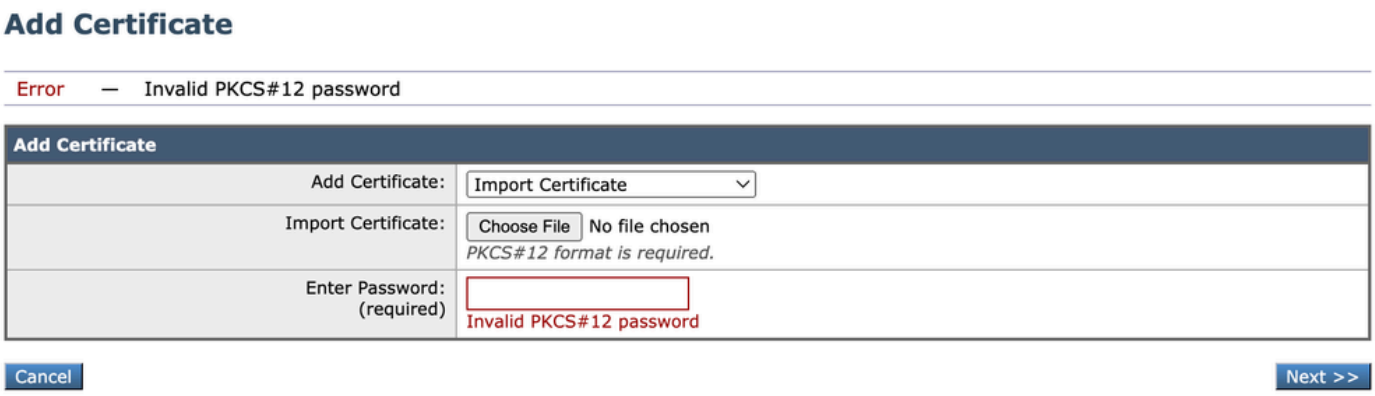


Imagem - Senha inválida

Este erro indica que a senha do certificado PKCS#12 está incorreta. Para resolver o erro, digite a senha correta ou gere novamente o certificado.

O certificado ainda não é válido

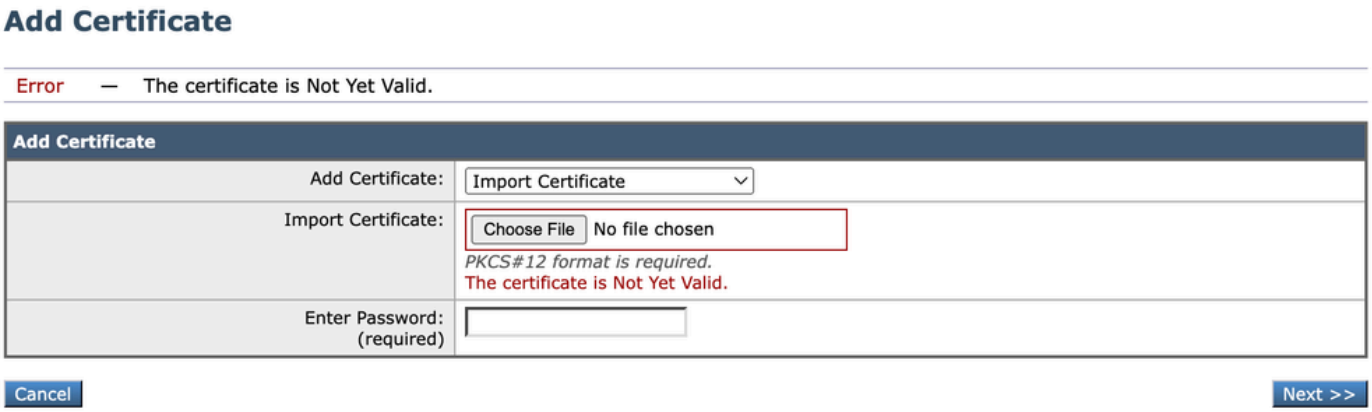
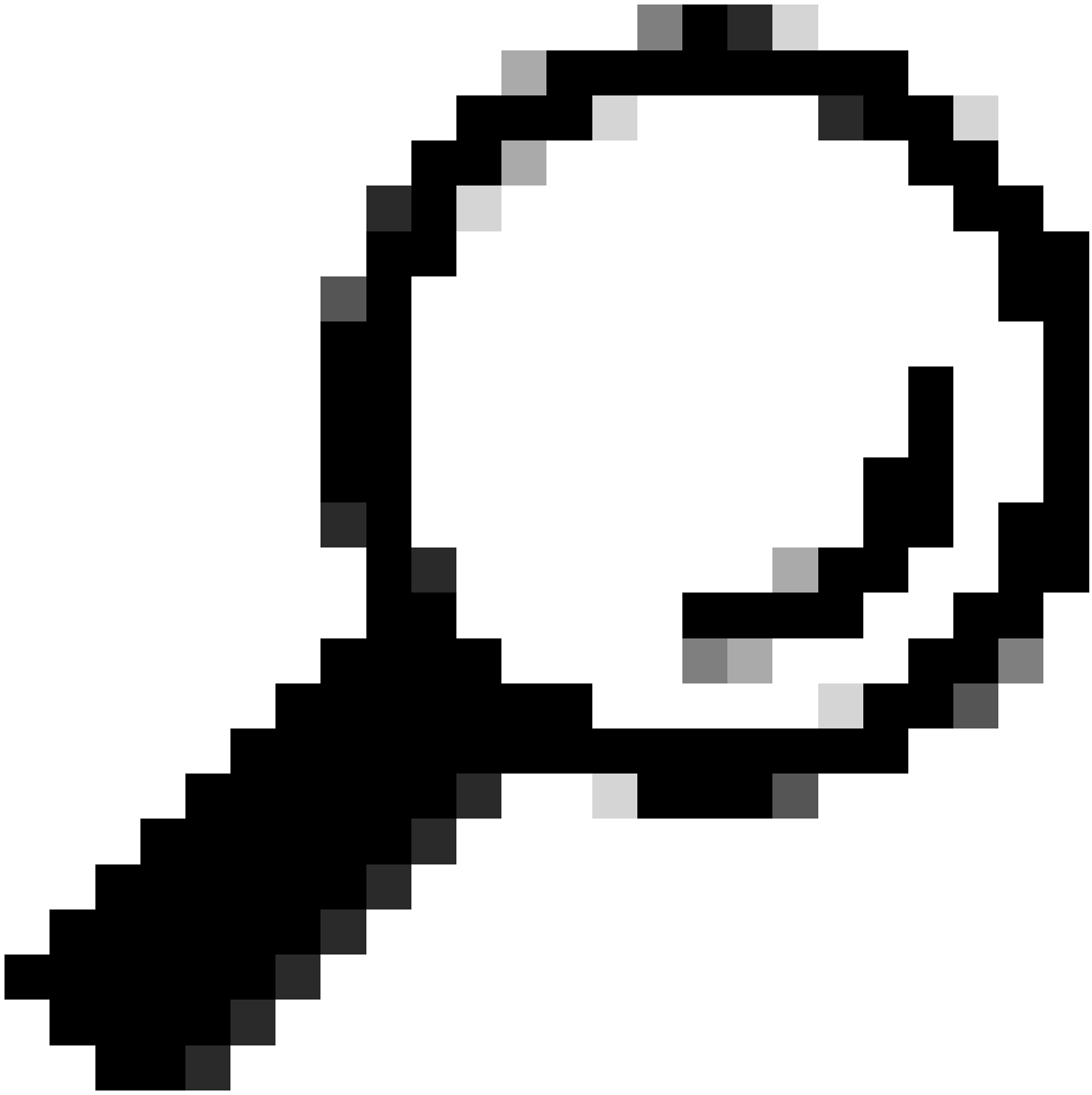


Imagem - O certificado ainda não é válido

1. Verifique se a data e a hora do SWA estão corretas.

2. Verifique a data do certificado e certifique-se de que a data e a hora "Não Antes" estejam corretas.



Dica: se você acabou de gerar o certificado, aguarde um minuto e carregue o certificado.

Reiniciar o serviço de GUI a partir do CLI

Para reiniciar o serviço WebUI, você pode usar estas etapas do CLI:

Etapa 1. Faça login na CLI.

Etapa 2. Type diagnostic (Este é um comando oculto e não digita automaticamente com TAB).

Etapa 3. Selecione SERVICES.

Etapa 4. Selecione WEBUI.

Etapa 5. Escolha REINICIAR.

Informações Relacionadas

- Guia do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - GD (General Deployment) - Classifique os usuários finais para aplicação de política [Cisco Secure Web Appliance] - Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.