Configurar certificado GUI de dispositivo web seguro

Contenido

Introducción

Este documento describe los pasos para configurar certificados para la interfaz web de administración de dispositivos web seguros (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA.

Cisco recomienda que tenga:

- SWA físico o virtual instalado.
- Acceso administrativo a la interfaz gráfica de usuario (GUI) de SWA.
- Acceso administrativo a la interfaz de línea de comandos (CLI) SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Certificado de interfaz de usuario web

Primero tenemos que elegir el tipo de certificados que queremos utilizar en la interfaz de usuario web (interfaz de usuario web) de administración SWA.

De forma predeterminada, SWA utiliza el "Cisco Appliance Demo Certificate:".

- CN = certificado de demostración del dispositivo de Cisco
- O = Cisco Systems, Inc.
- L = San José
- S = California
- C = US

Puede crear un certificado autofirmado en SWA o importar su propio certificado generado por el servidor de la autoridad de certificación interna (CA).

El SWA no admite la inclusión de nombres alternativos de asunto (SAN) al generar una solicitud de firma de certificado (CSR). Además, los certificados autofirmados SWA tampoco admiten atributos SAN. Para utilizar certificados con atributos SAN, debe crear y firmar el certificado usted mismo, asegurándose de que incluya los detalles de SAN necesarios. Una vez que haya generado este certificado, puede cargarlo en el SWA que se utilizará. Este enfoque permite especificar varios nombres de host, direcciones IP u otros identificadores, lo que proporciona una mayor flexibilidad y seguridad para el entorno de red.

Nota: Los certificados deben incluir la clave privada y debe estar en formato PKCS#12.

Pasos para Modificar el Certificado de Interfaz Web

Paso 1. Inicie sesión en la GUI y seleccione Network en el menú superior.

Paso 2. Elija Administración de certificados.

Paso 3. En Appliance Certificates, Seleccione Add Certificate.

Paso 4. Seleccione Tipo de certificado (Certificado autofirmado o Certificado de importación).

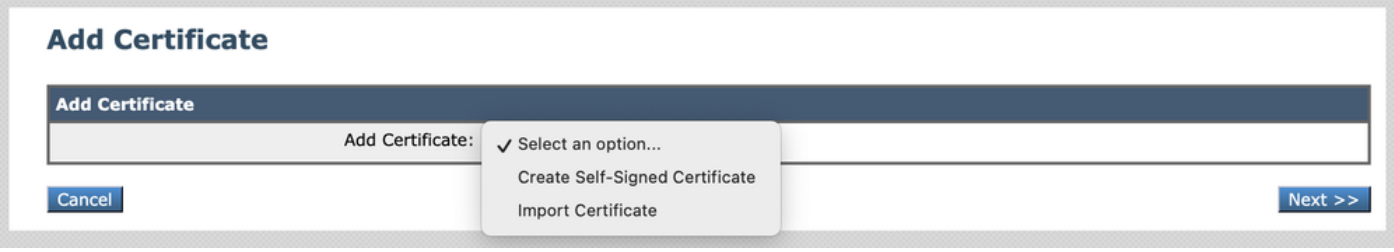


Imagen - Elegir tipo de certificado

Paso 5. Si selecciona el certificado autofirmado, siga estos pasos. Caso contrario, siga con el paso 6.

Paso 5.1. Complete los campos.

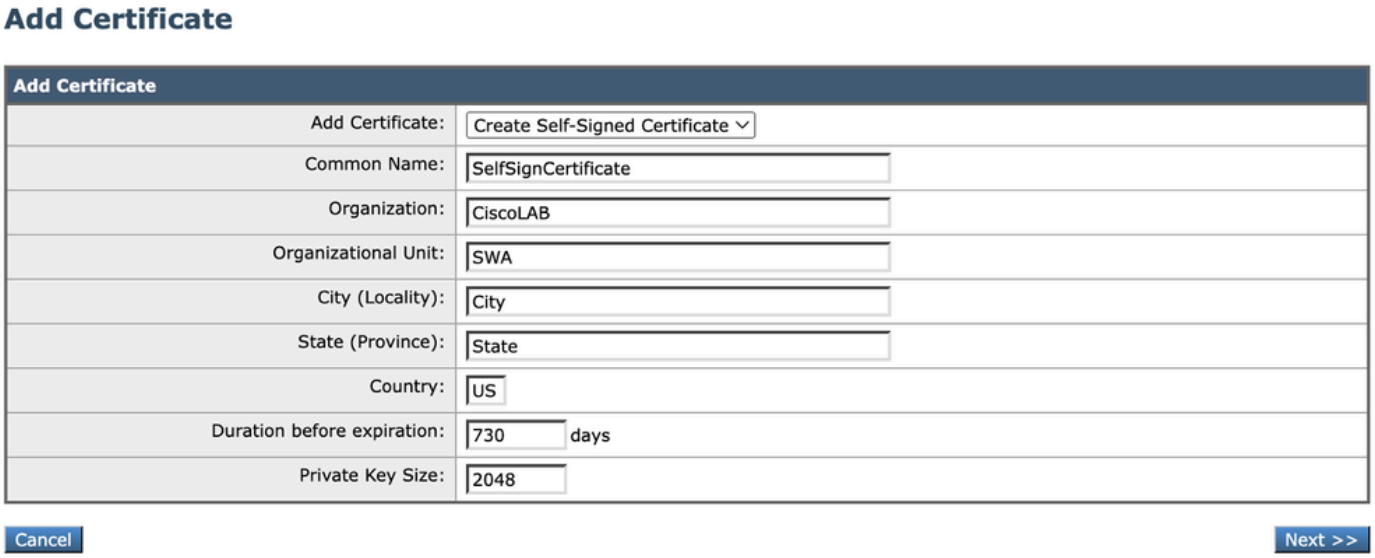


Imagen - Detalles del certificado de firma automática

Nota: el tamaño de la clave privada debe estar entre 2048 y 8192.

Paso 5.2. Haga clic en Next (Siguiente).

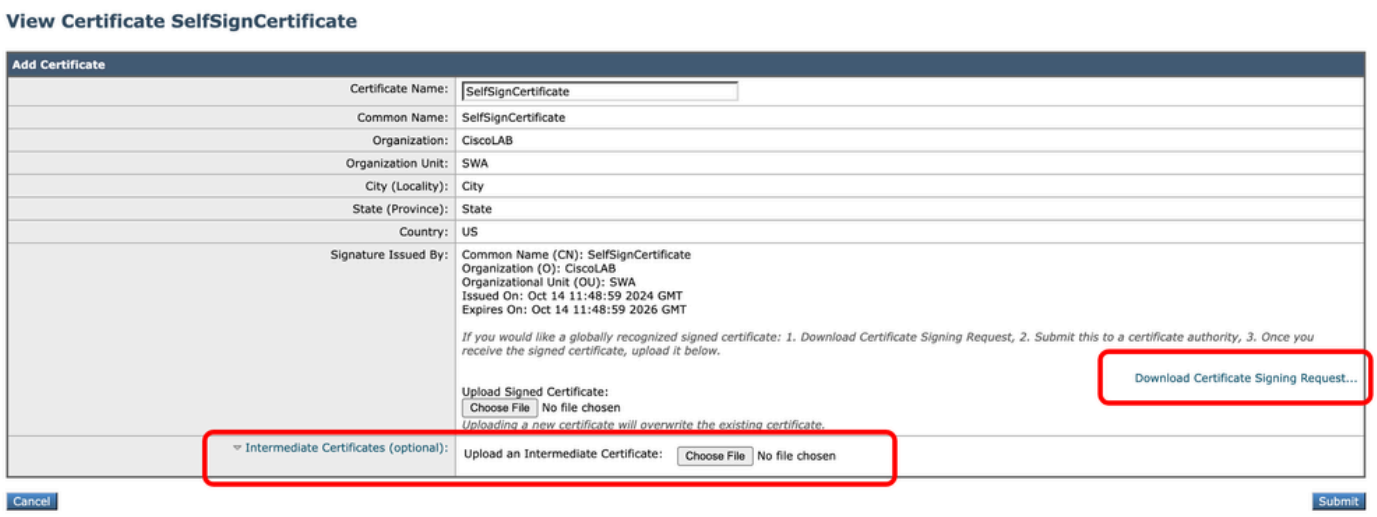
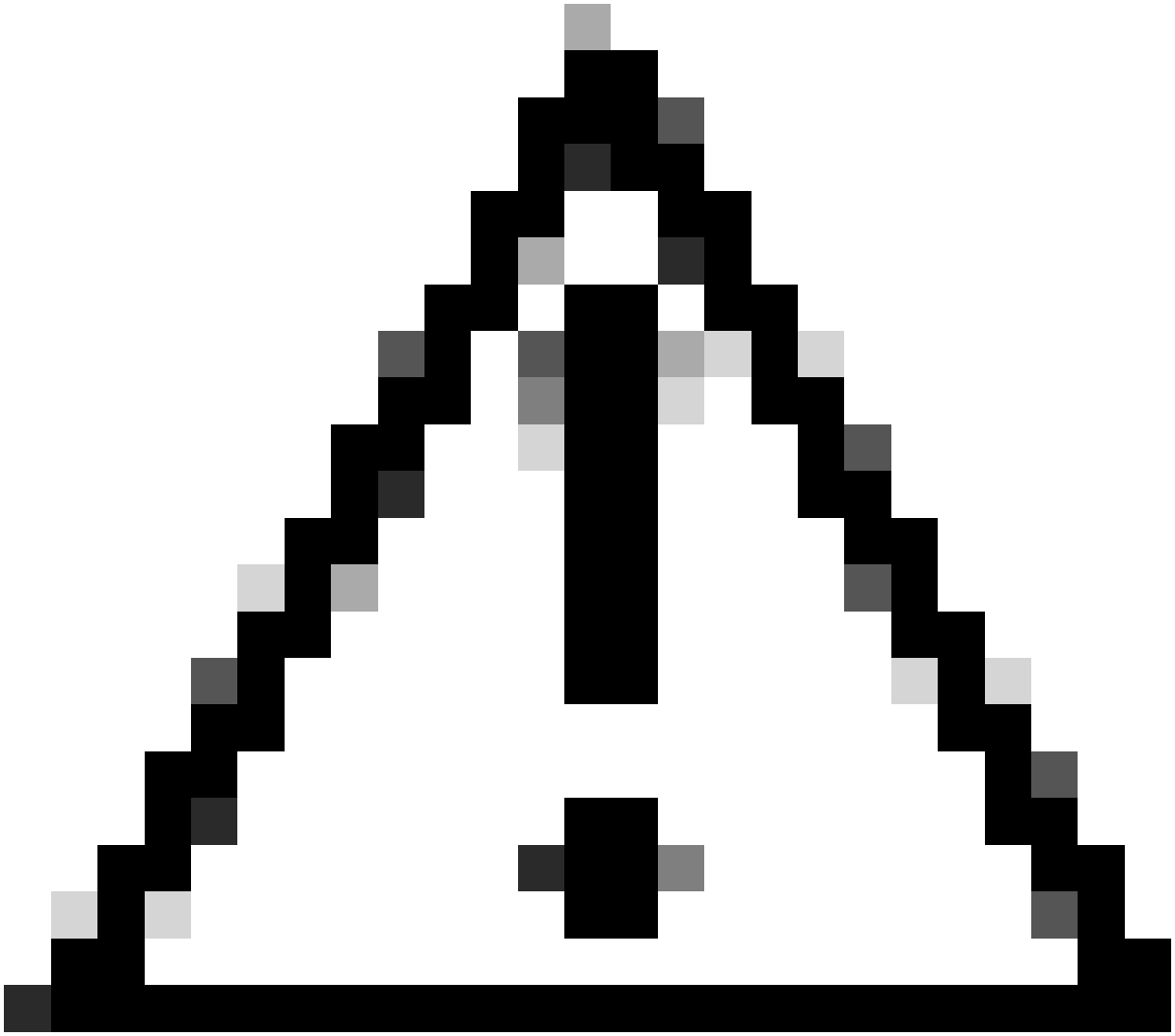


Imagen - Descargar CSR

Paso 5.3. (Opcional) Puede descargar el CSR y firmarlo con el servidor de la CA de su organización, luego Cargar el certificado firmado y Enviar.



Precaución: si desea firmar el CSR, con el servidor de la CA, asegúrese de Enviar y Confirmar la página antes de firmar o cargar el certificado firmado. El perfil que ha creado durante el proceso de generación de CSR incluye su clave privada.

Paso 5.4.Enviar si el certificado autofirmado actual es apropiado.

Paso 5.5. Vaya al paso 7.

Paso 6. Si elige Importar certificado.

Paso 6.1. Importar archivo de certificado (se requiere el formato PKCS#12).

Paso 6.2. Introduzca la contraseña para el archivo de certificado.

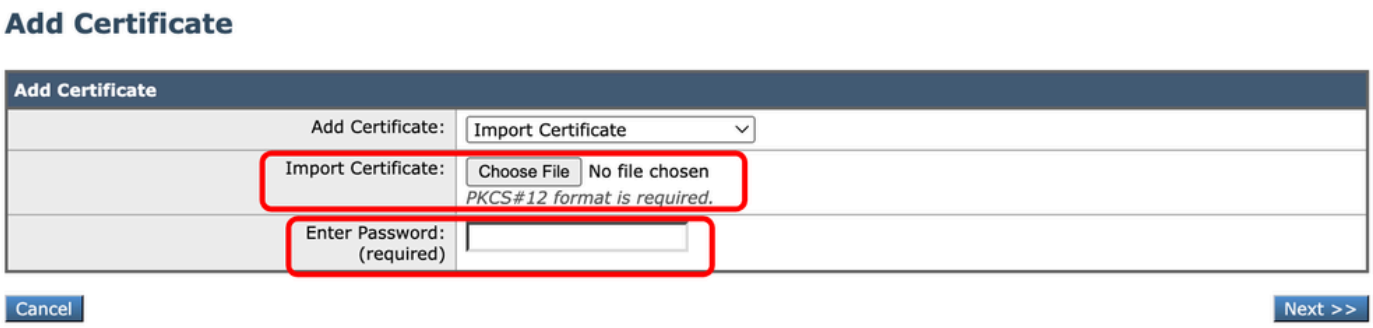


Imagen - Importar certificado

Paso 6.3. Haga clic en Next (Siguiente).

Paso 6.4. Enviar cambios.

Paso 7. Registrar cambios.

Paso 8. Inicie sesión en la CLI.

Paso 9. Escriba certconfig y presione Enter.

Paso 10. Escriba SETUP.

Paso 11. Escriba Y y, a continuación, presione Intro.

Nota: cuando se cambia el certificado, los usuarios administrativos que están conectados actualmente a la interfaz de usuario web pueden experimentar un error de conexión y podrían perder los cambios no enviados. Esto ocurre sólo si el explorador no ha marcado ya el certificado como de confianza.

Paso 12. Elija 2 para seleccionar de la lista de certificados disponibles.

Paso 13. Seleccione el número de certificado que desea utilizar para la GUI.

Paso 14. Si tiene un certificado intermedio y desea agregarlo, escriba Y; de lo contrario, escriba N .

Nota: si necesita agregar el certificado intermedio, debe pegarlo en formato PEM y terminar con '.' (sólo con 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.
```

Paso 15. Escriba commit para guardar los cambios.

Probar el certificado desde la línea de comandos

Puede verificar el certificado mediante el comando openssl:

```
 openssl s_client -connect

      :
```

En este ejemplo, el nombre de host es SWA.cisco.com y la interfaz de administración se establece como predeterminada (puerto TCP 8443).

En la segunda línea de la salida, puede ver los detalles del 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
```

Errores comunes

Estos son algunos errores comunes que puede encontrar al intentar crear o modificar su certificado de GUI.

Error Formato PKCS#12 no válido

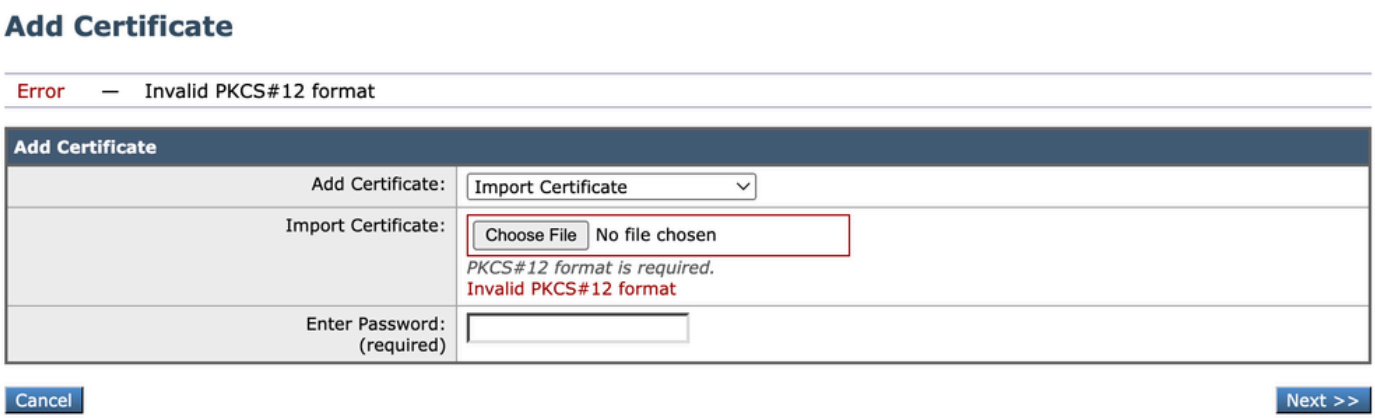


Imagen: formato PKCS#12 no válido

Puede haber dos causas de este error:

1. El archivo de certificado está dañado y no es válido.

   Intente abrir el certificado. Si se produce un error durante la apertura, puede volver a generar o descargar el certificado.

2. La CSR generada anteriormente ya no es válida.

   Cuando genere una CSR, debe asegurarse de Enviar y Registrar los cambios. El motivo es que su CSR no se guardó cuando cerró sesión o cambió de página. El perfil que creó al generar el CSR contiene la clave privada necesaria para cargar correctamente el certificado. Una vez que este perfil se ha ido, la clave privada se ha ido. Por lo tanto, se debe generar otra CSR y, a continuación, volver a llevarla a la CA.

Los días deben ser enteros

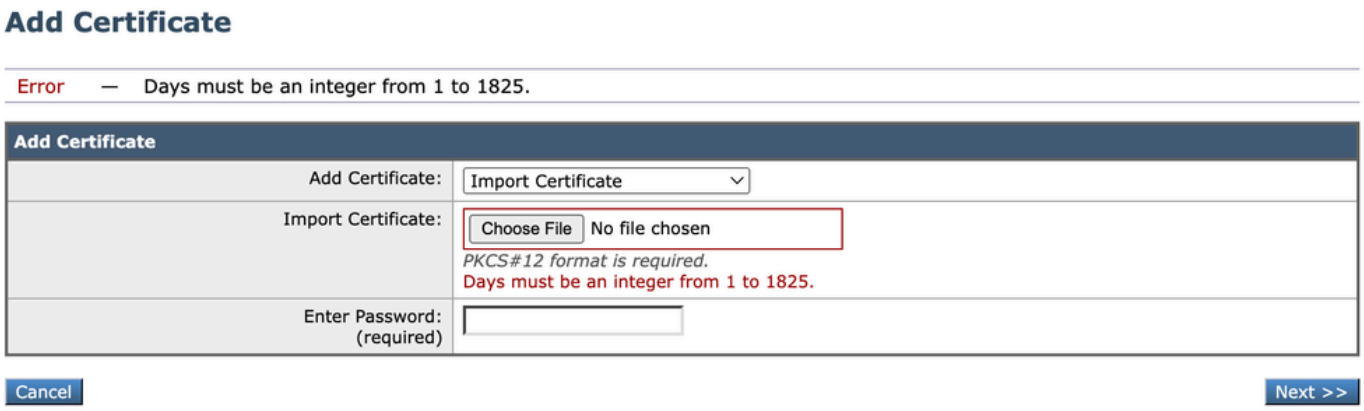


Imagen: los días deben ser un error entero

Este error se debe a que el certificado cargado ha caducado o tiene una validez de 0 días.

Para solucionar el problema, compruebe la fecha de vencimiento del certificado y asegúrese de que la fecha y hora SWA sean correctas.

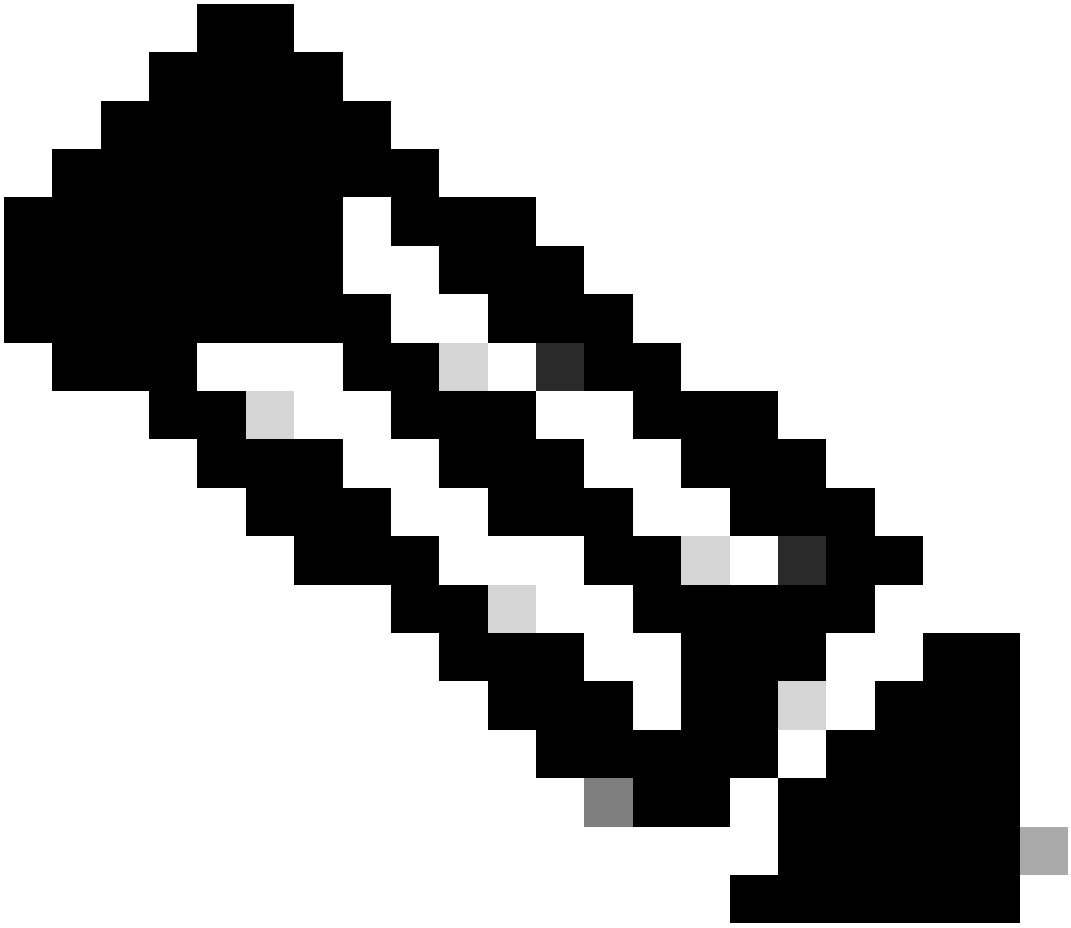
Error de validación de certificado

Este error significa que la CA raíz o la CA intermedia no se agregan a la lista de certificados raíz de confianza en SWA. Para solucionar el problema, si utiliza tanto la CA raíz como la CA intermedia:

1. Cargue la CA raíz en SWA y, a continuación, Confirme.

2. Cargue la CA intermedia y, a continuación, vuelva a registrar los cambios.

3. Cargue el certificado de la GUI.



Nota: Para cargar la CA raíz o intermedia, desde la GUI: Red. En la sección Administración de certificados, elija Administrar certificados raíz de confianza. En Certificados raíz de confianza personalizados, haga clic en Importar para cargar sus certificados de CA.

Contraseña no válida

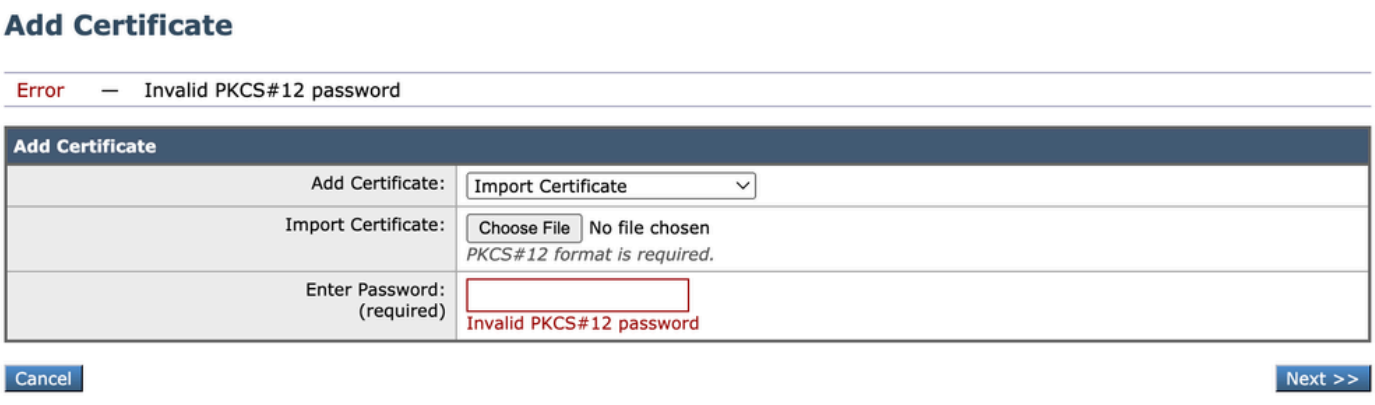


Imagen - Contraseña no válida

Este error indica que la contraseña del certificado PKCS#12 es incorrecta. Para solucionar el error, escriba la contraseña correcta o vuelva a generar el certificado.

El certificado aún no es válido

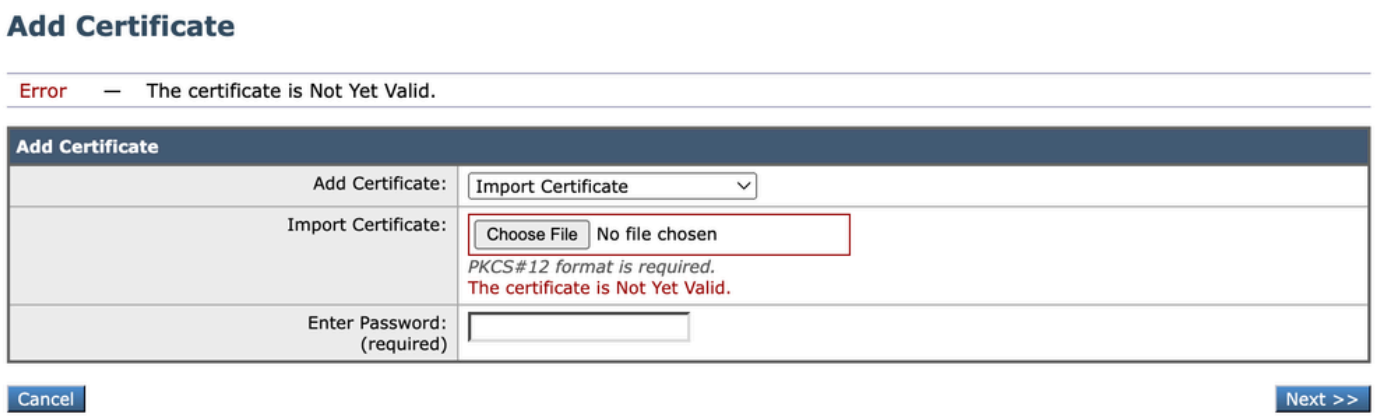
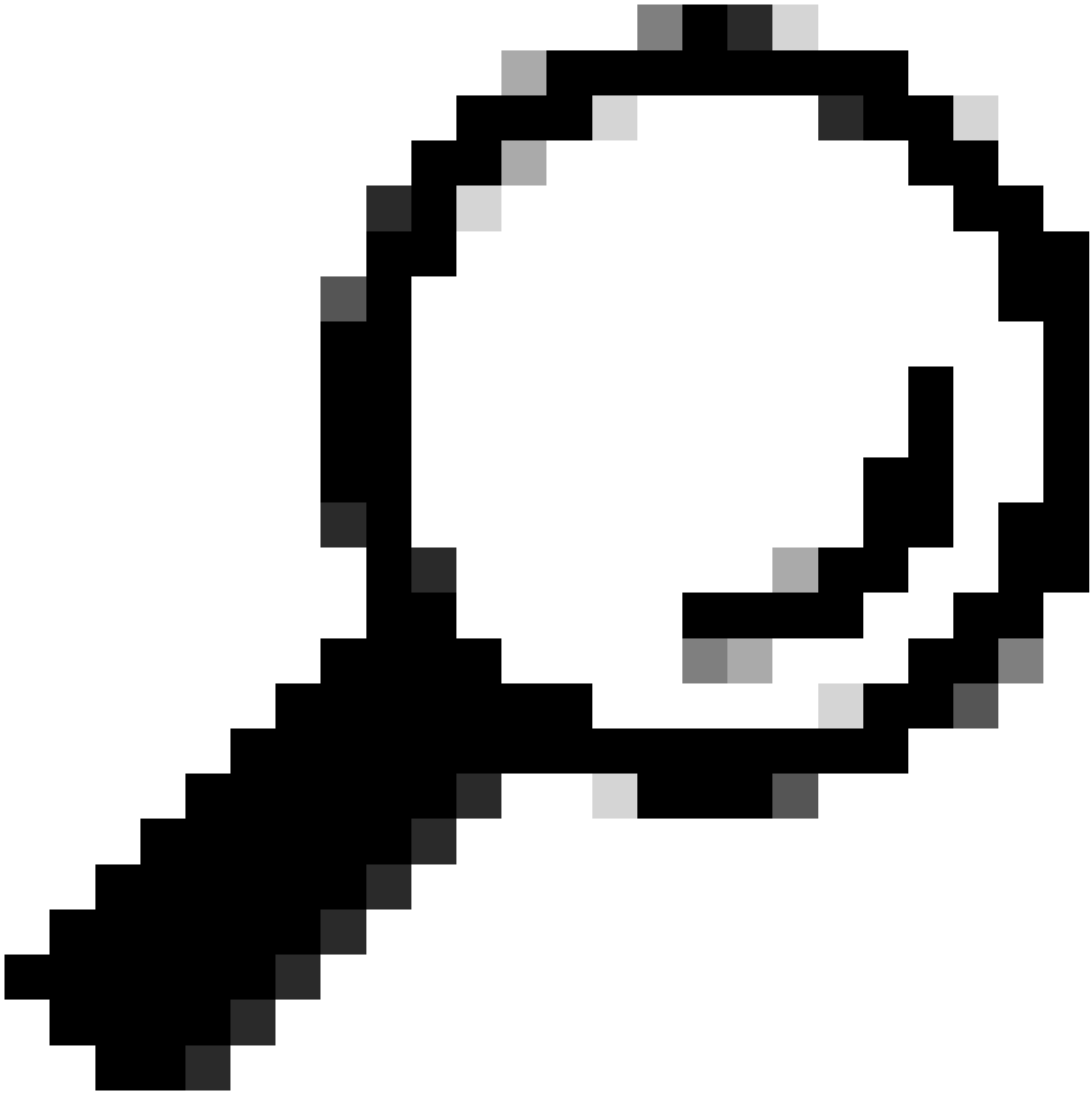


Imagen: el certificado aún no es válido

1. Asegúrese de que la fecha y hora SWA sean correctas.

2. Compruebe la fecha del certificado y asegúrese de que la fecha y la hora "No antes de" sean correctas.



Consejo: Si acaba de generar el certificado, espere un minuto y, a continuación, cargue el certificado.

Reiniciar el servicio GUI desde CLI

Para reiniciar el servicio WebUI, puede seguir estos pasos desde la CLI:

Paso 1. Inicie sesión en CLI.

Paso 2. Escriba diagnostic (Este es un comando oculto y no escribe automáticamente con TAB).

Paso 3. Elija Servicios.

Paso 4. Seleccione WEBUI.

Paso 5. Elija REINICIAR.

Información Relacionada

- Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - GD(General Deployment) - Clasificación de usuarios finales para la aplicación de políticas [Cisco Secure Web Appliance] - Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).