Generar y agregar certificados necesarios para la instalación de Secure Endpoint Private Cloud 3.x en adelante

Contenido

Introducción

Este documento describe el proceso para generar certificados que deben cargarse con cada instalación nueva de Secure Console Private Cloud o para renovar los Servicios de Certificate Server instalados.

Prerequisites

Requirements

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Windows Server 2008
- CentOS 7/8
- Secure Console Virtual Private Cloud 3.0.2 (en adelante)
- OpenSSL 1.1.1

Componentes Utilizados

Cisco recomienda que tenga conocimiento sobre estos temas:

- Windows Server 2008 (versiones posteriores)
- Instalación de Secure Console Private Cloud
- Infraestructura de clave pública
- OpenSSL
- Linux CLI

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.

Antecedentes

Con la introducción de Secure Console Private Cloud 3.X, se requieren nombres de host y pares de certificado/clave para todos los servicios siguientes:

- Portal de administración
- Autenticación (novedad en la nube privada 3.X)
- Consola segura
- Servidor de disposición
- Servidor de disposición - Protocolo extendido
- Servicio de actualización de disposición
- Centro de administración FirePOWER

En este documento se describe una forma rápida de generar y cargar los certificados requeridos. Puede ajustar cada uno de los parámetros, incluidos el algoritmo de hash, el tamaño de clave y otros, según la política de su organización, y es posible que el mecanismo de generación de estos certificados no coincida con lo que se detalla aquí.

> **Advertencia**: el procedimiento que se menciona a continuación puede variar según la configuración del servidor de la CA. Se espera que el servidor de la CA de su elección ya esté aprovisionado y que la configuración del mismo se haya completado. La siguiente nota técnica describe un ejemplo de generación de certificados y Cisco TAC no participa en la resolución de problemas relacionados con la generación de certificados y/o problemas de servidor de la CA de ningún tipo.

Creación de certificados

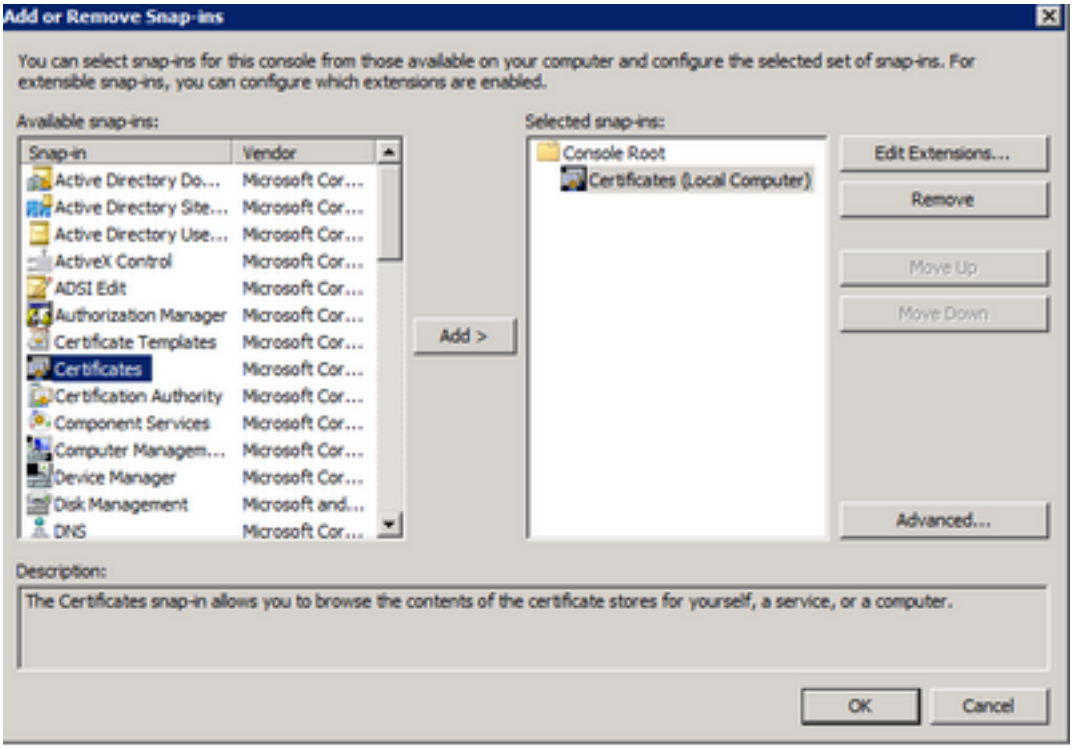
Generar certificados en el servidor de Windows

Asegúrese de que las siguientes funciones están instaladas y configuradas en Windows Server.

- Servicios de certificados de Active Directory
- Entidad emisora de certificados
- Inscripción en la Web de entidad de certificación
- Respondedor en línea
- Servicio web de inscripción de certificados
- Servicio web de directiva de inscripción de certificados
- Servicios de dominio de Active Directory
- Servidores DNS
- Servidor Web (IIS)

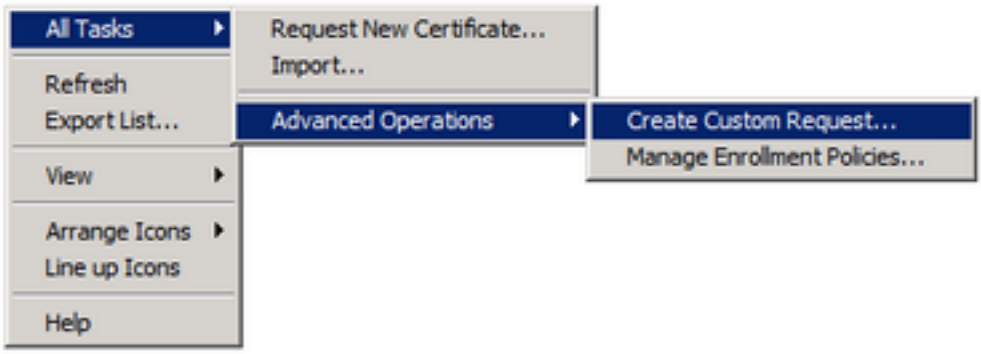
Generar una solicitud de firma de certificado (CSR)

Paso 1. Vaya a la consola de MMC y agregue el complemento Certificados para la cuenta de equipo, como se muestra en la imagen.

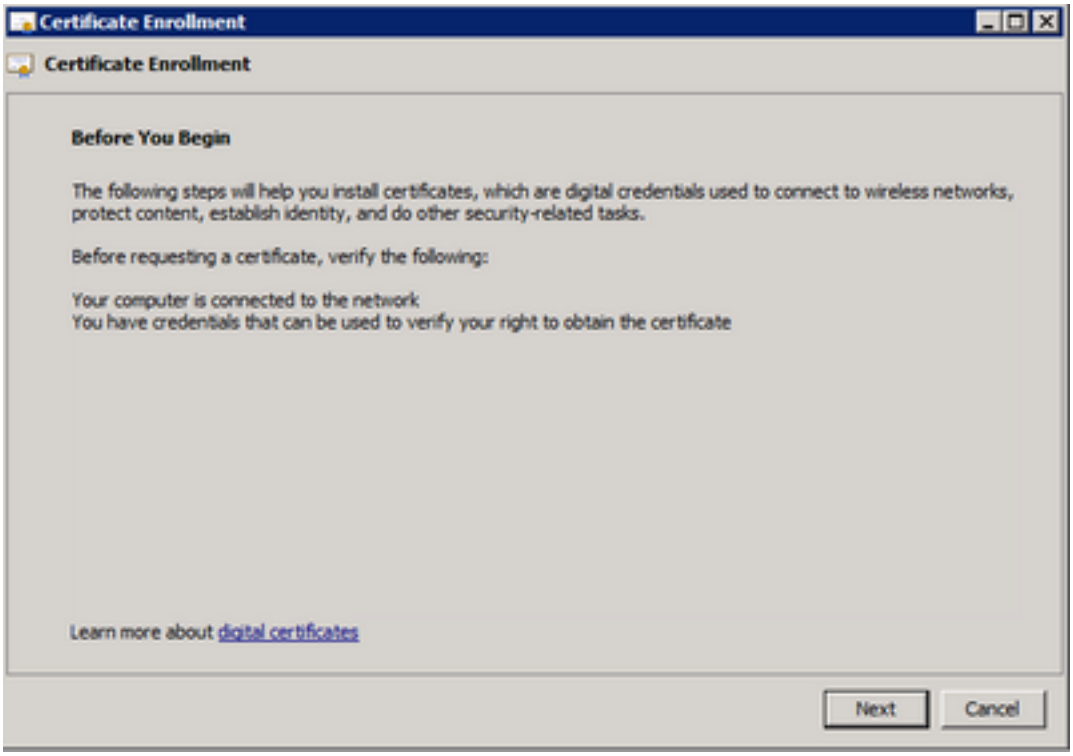


Paso 2. Acceder a **Certificados (Equipo local) > Personal > Certificados**.

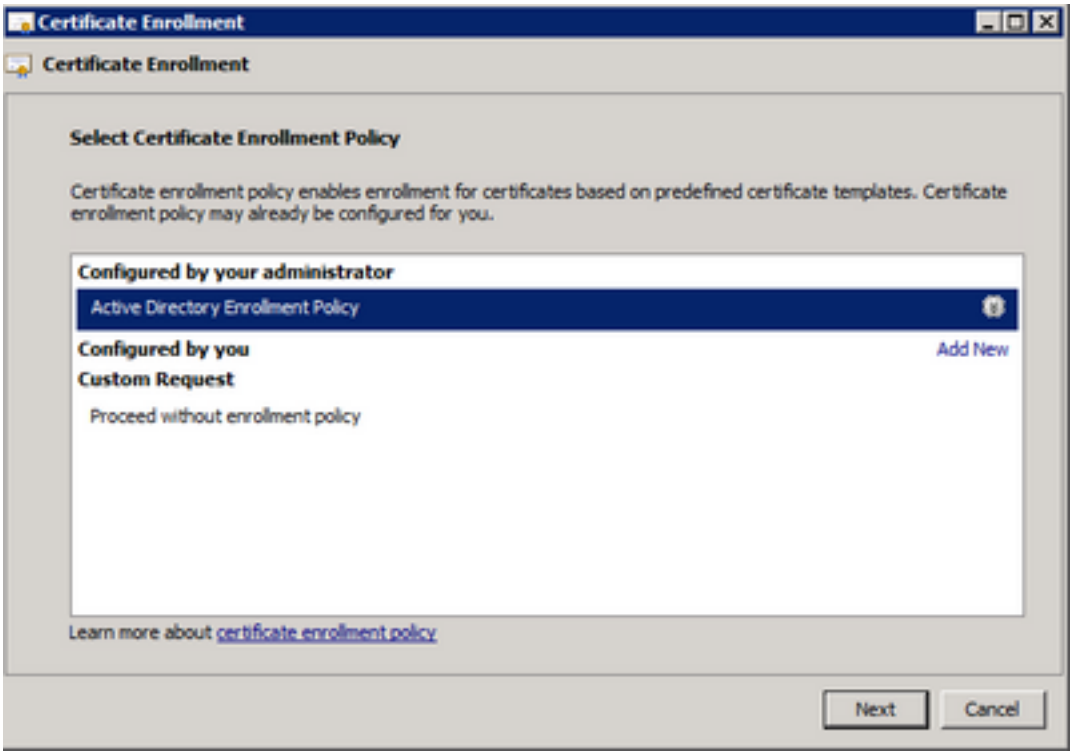
Paso 3. Haga clic con el botón derecho del ratón en el espacio vacío y seleccione **Todas las tareas > Operaciones avanzadas > Crear solicitud personalizada.**



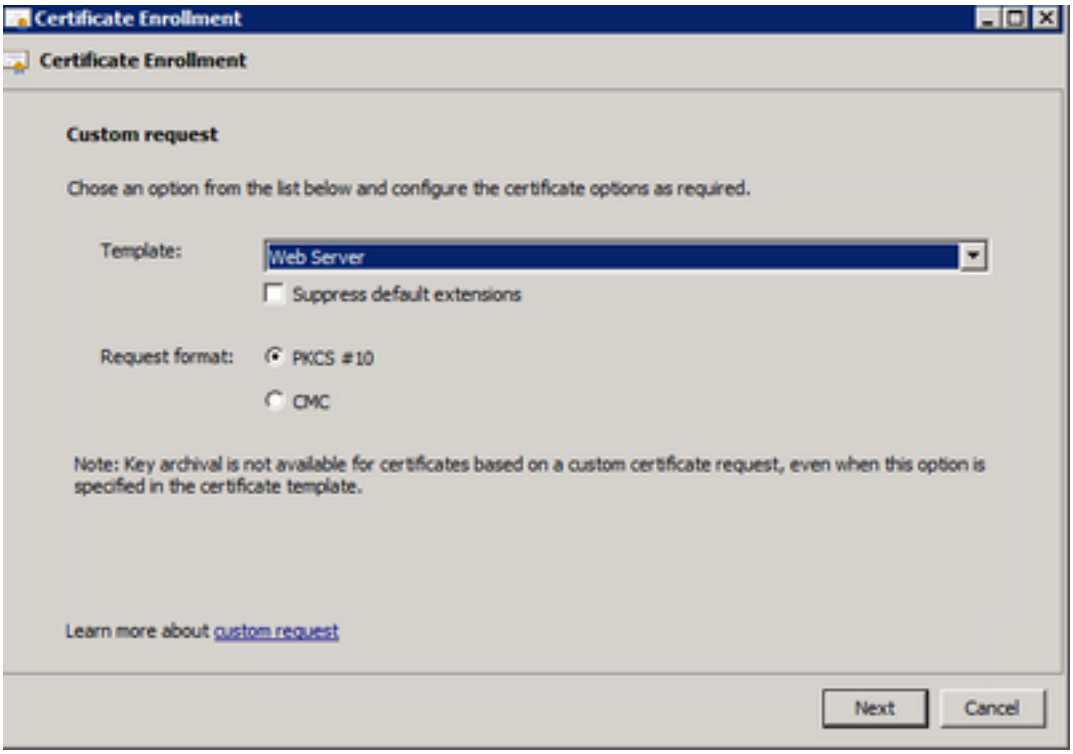
Paso 4. Seleccione **Next** en la ventana Enrollment.



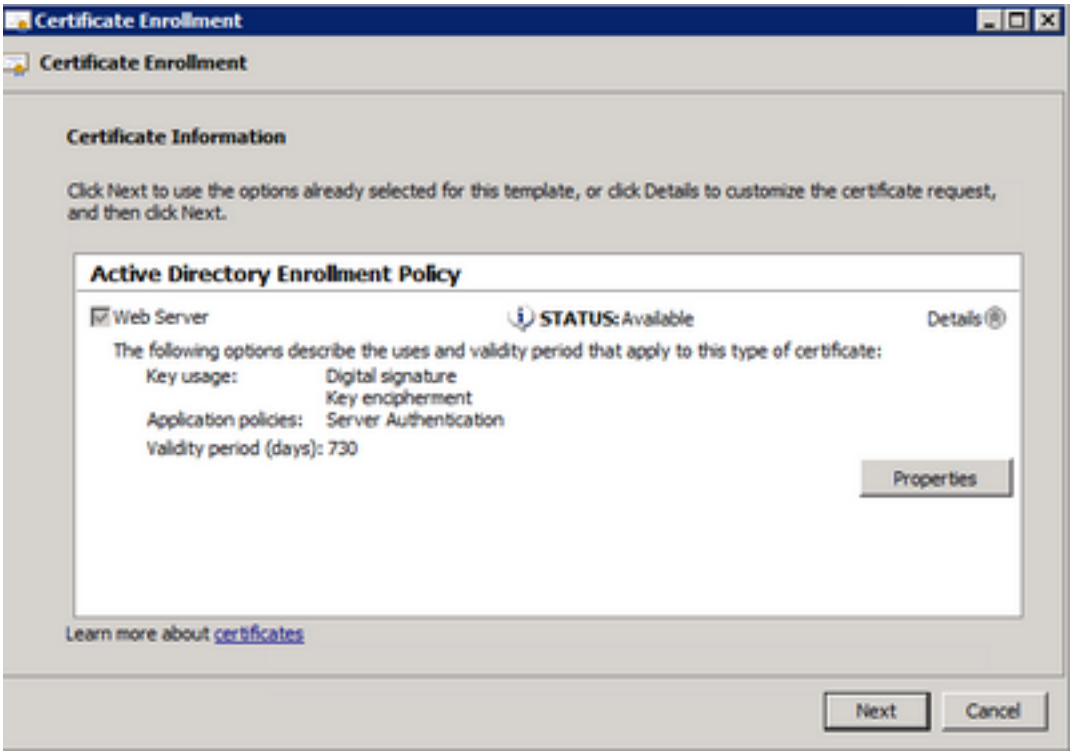
Paso 5. Seleccione su directiva de inscripción de certificados y seleccione **Siguiente**.



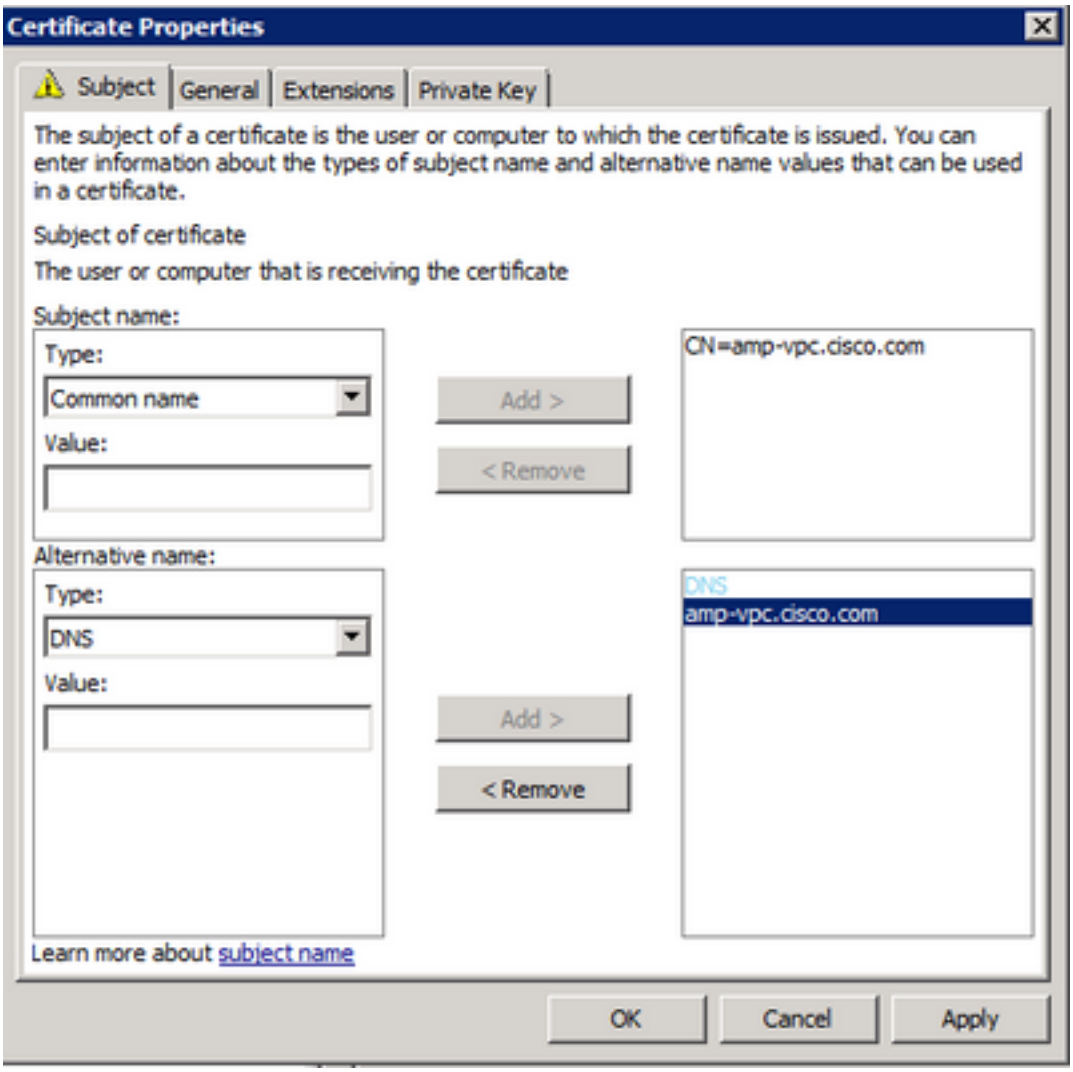
Paso 6. Elija la plantilla como **Web Server** y seleccione **Next**.



Paso 7. Si la plantilla "Servidor web" se ha configurado correctamente y está disponible para su inscripción, se muestra el estado Disponible. Seleccione **Details** para expandir Properties.

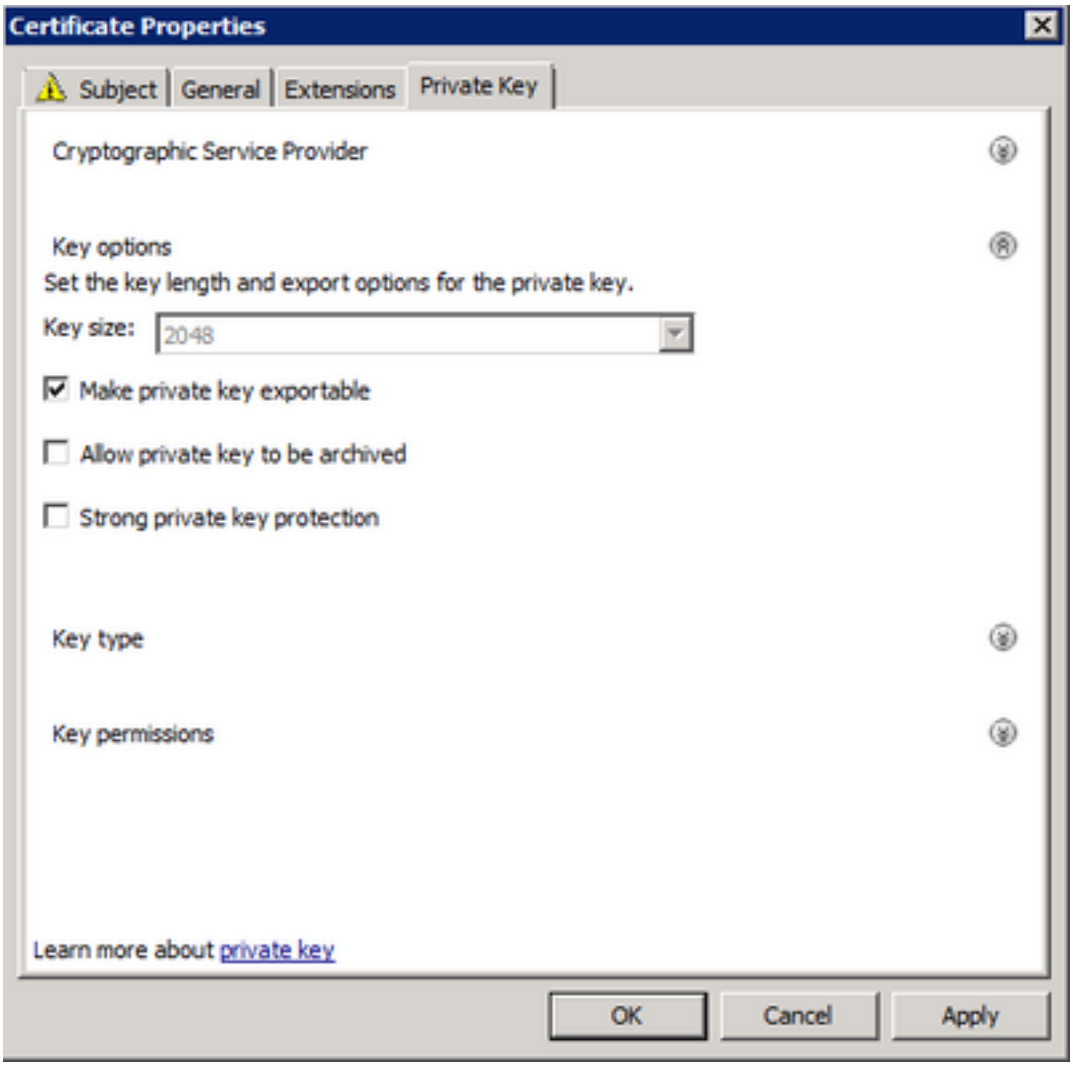


Paso 8. Como mínimo, agregue los atributos CN y DNS. El resto de los atributos se pueden agregar según sus requisitos de seguridad.



Paso 9. De manera opcional, asigne un nombre descriptivo en la ficha **General**.

Paso 10. Seleccione en la pestaña **Private Key** y asegúrese de que está habilitando la opción Make private key exportable **en la sección Key Options**.

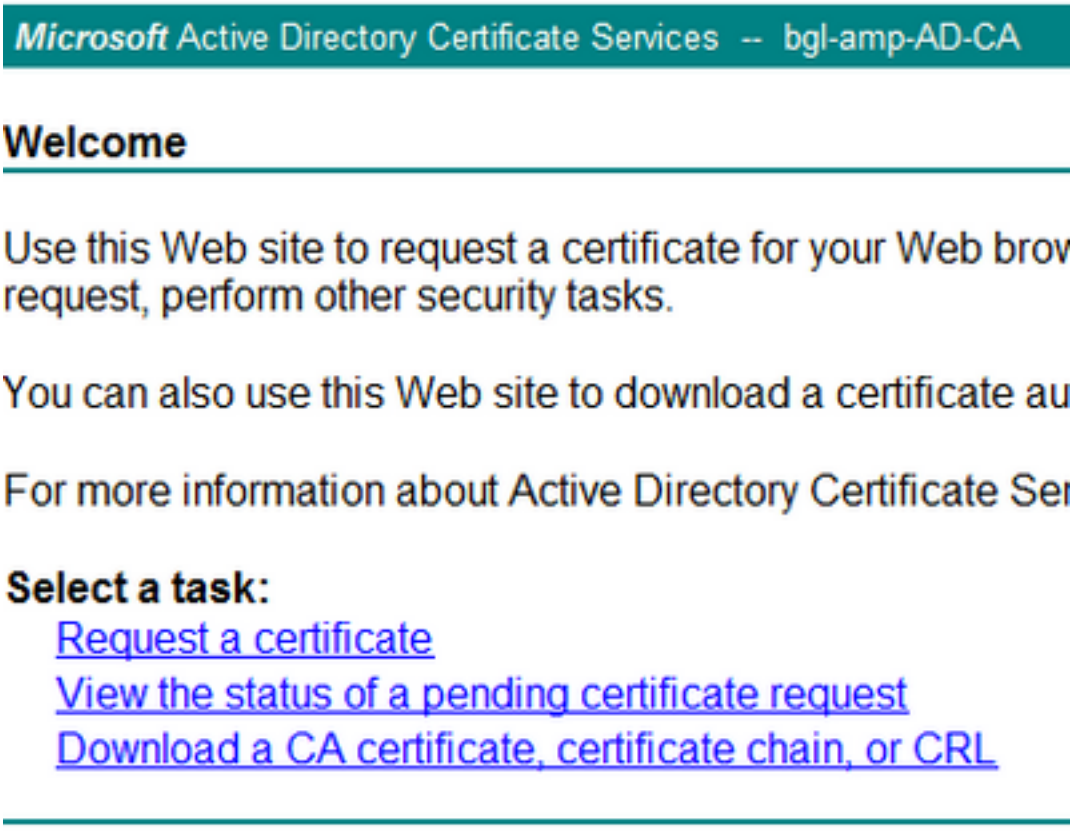


Paso 11. Por último, seleccione en **Aceptar**. Esto debe conducirle al cuadro de diálogo Inscripción de certificados desde donde puede seleccionar **Siguiente**.

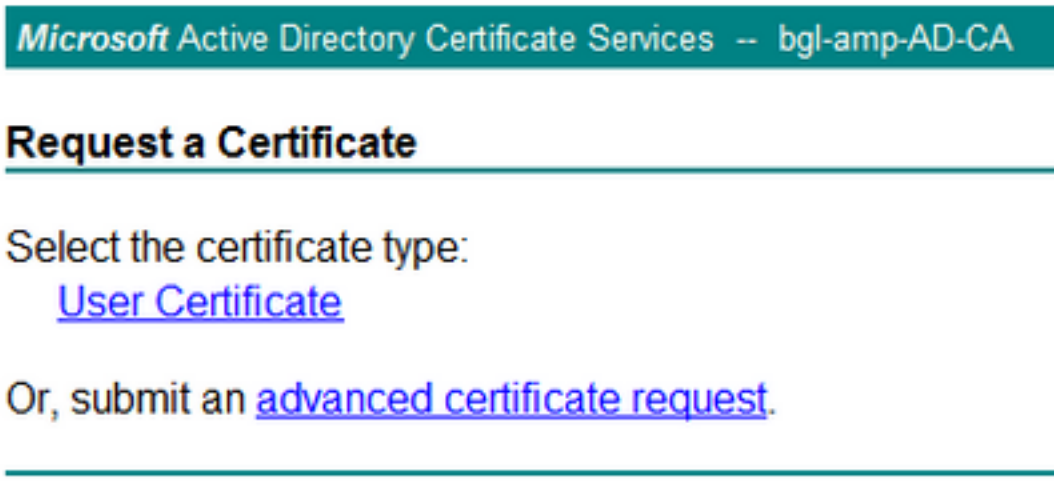
Paso 12. Busque una ubicación para guardar el archivo .req que se envía al servidor de la CA para su firma.

Enviar la CSR a la CA y generar el certificado

Paso 1. Navegue hasta la página web de Servicios de Certificate Server de MS AD como se muestra a continuación y seleccione **Solicitar un certificado**.

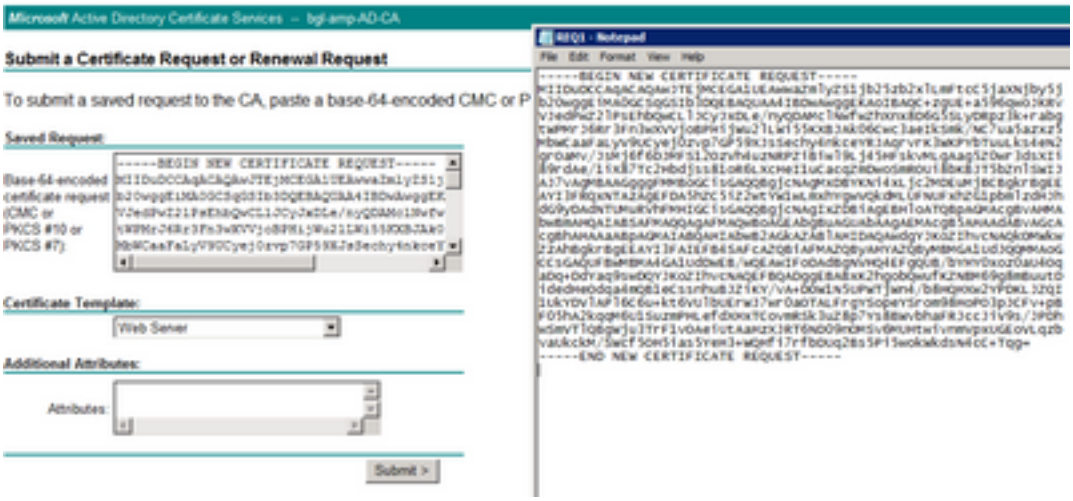


Paso 2. Seleccione en el enlace **solicitud de certificado avanzado**.



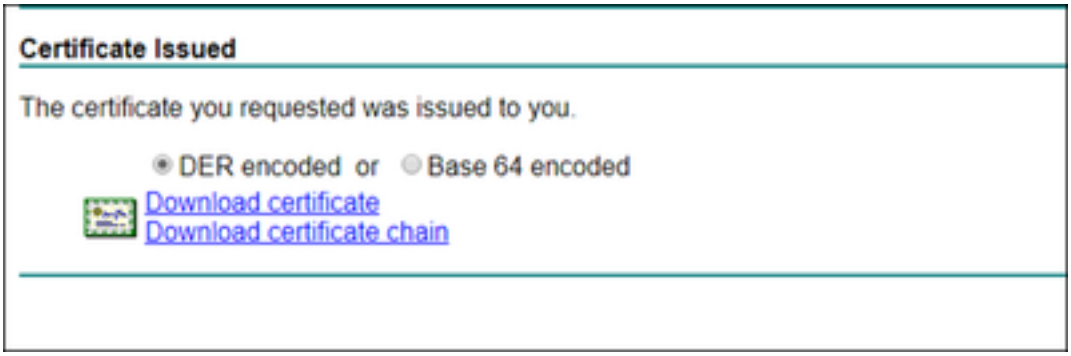
Paso 3. Seleccione en **Enviar una solicitud de certificado mediante un archivo CMC o PKCS #10 codificado en base 64, o envíe una solicitud de renovación mediante un archivo PKCS #7 codificado en base 64**.

Paso 4. Abra el contenido del archivo .req (CSR) guardado anteriormente mediante el Bloc de notas. Copie el contenido y péguelo aquí. Asegúrese de que la plantilla de certificado esté seleccionada como **servidor web**



Paso 5. Por último, seleccione **Submit**.

Paso 6. En este punto, debe poder **Descargar** el certificado, como se muestra en la imagen.



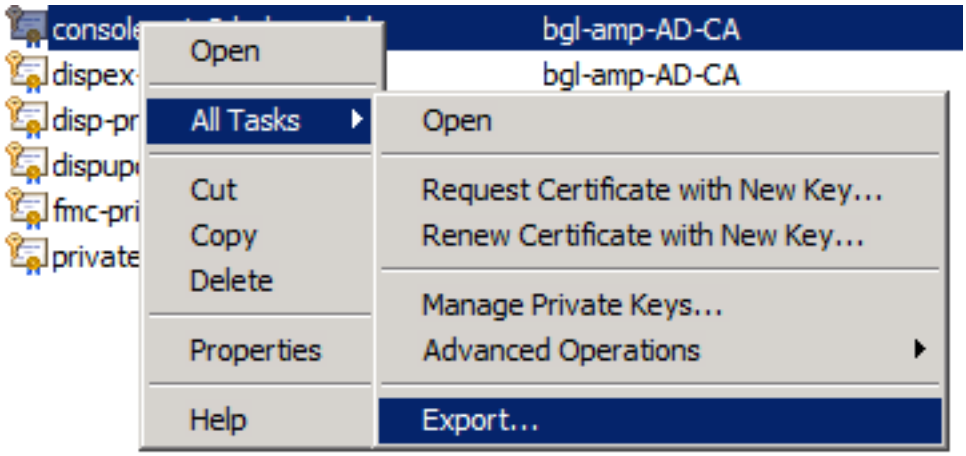
Exportación de la clave privada y conversión al formato PEM

Paso 1. Instale el certificado en el almacén de certificados abriendo el archivo .cer y seleccione **Install Certificate**.

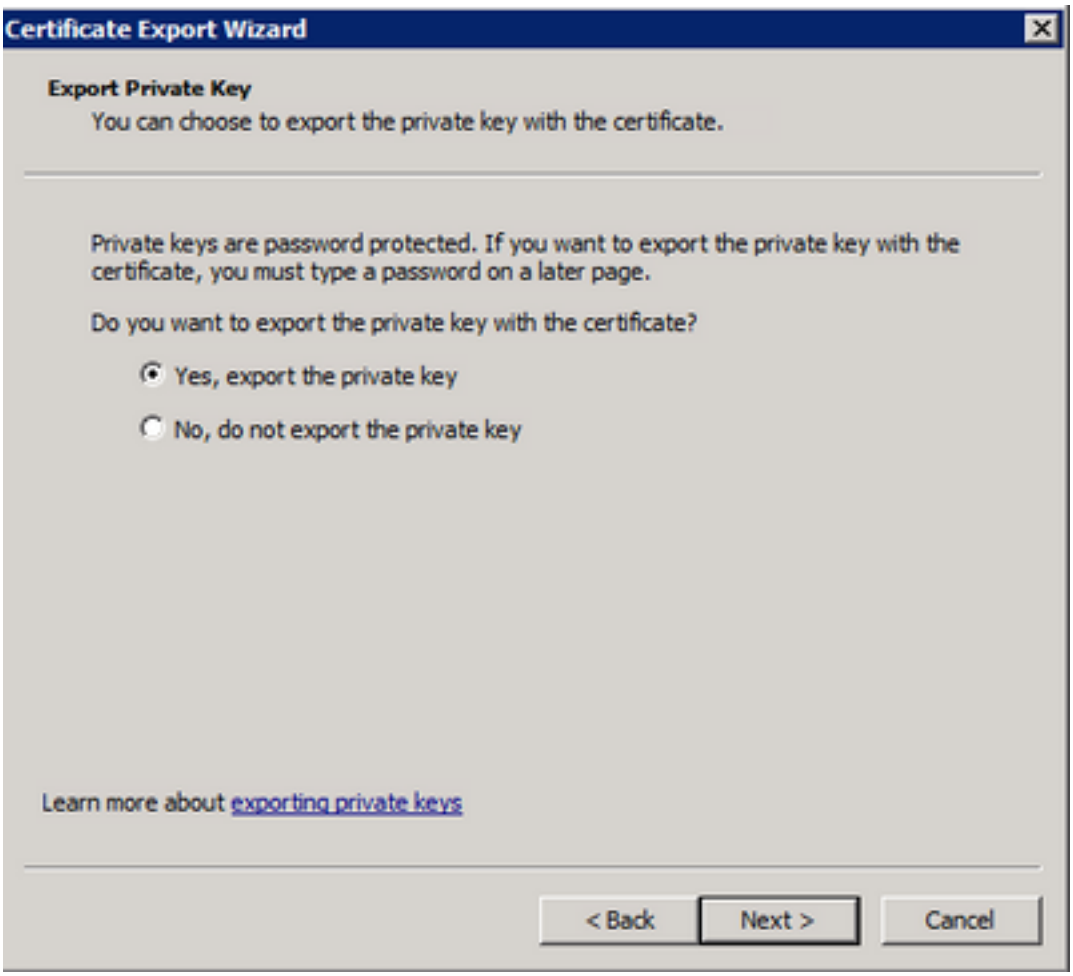
Paso 2. Vaya al complemento MMC seleccionado anteriormente.

Paso 3. Vaya al almacén donde se instaló el certificado.

Paso 4. Haga clic con el botón derecho en el certificado correcto, seleccione **Todas las tareas > Exportar**.



Paso 5. En el Asistente para exportación de certificados, confirme que desea exportar la clave privada, como se muestra en la imagen.



Paso 6. Introduzca una contraseña y seleccione **Next** para guardar la clave privada en el disco.

Paso 7. Esto guarda la clave privada en formato .PFX; sin embargo, debe convertirla al formato .PEM para utilizarla con Secure Endpoint Private Cloud.

Paso 8. Instale las bibliotecas de OpenSSL.

Paso 9. Abra una ventana del símbolo del sistema y cambie al directorio donde instaló OpenSSL.

Paso 10. Ejecute el siguiente comando para extraer la clave privada y guardarla en un nuevo archivo: (Si su archivo PFX no está en la misma ruta que donde se almacena la biblioteca OpenSSL, debe especificar la ruta exacta junto con el nombre de archivo)

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out privatekey.pem -nodes
```

Paso 11. Ahora ejecute el siguiente comando para extraer también el certificado público y guardarlo en un nuevo archivo:

```
openssl pkcs12 -in yourpfxfile.pfx -nokeys -out publiccert.pem -nodes
```

Generar certificado en servidor Linux (verificación SSL estricta DESACTIVADA)

Nota: La verificación TLS estricta verifica que el certificado cumpla los requisitos de TLS de Apple. Consulte la Guía de administración para obtener más información.

Asegúrese de que el servidor Linux en el que está intentando generar los certificados requeridos tenga instaladas las bibliotecas de OpenSSL 1.1.1. La verificación de si esto y el procedimiento que se muestra a continuación pueden variar de la distribución de Linux que está ejecutando. Esta parte se ha documentado, como se hace en un servidor CentOS 8.4.

Generar CA raíz autofirmada

Paso 1. Genere la clave privada para el certificado de CA raíz.

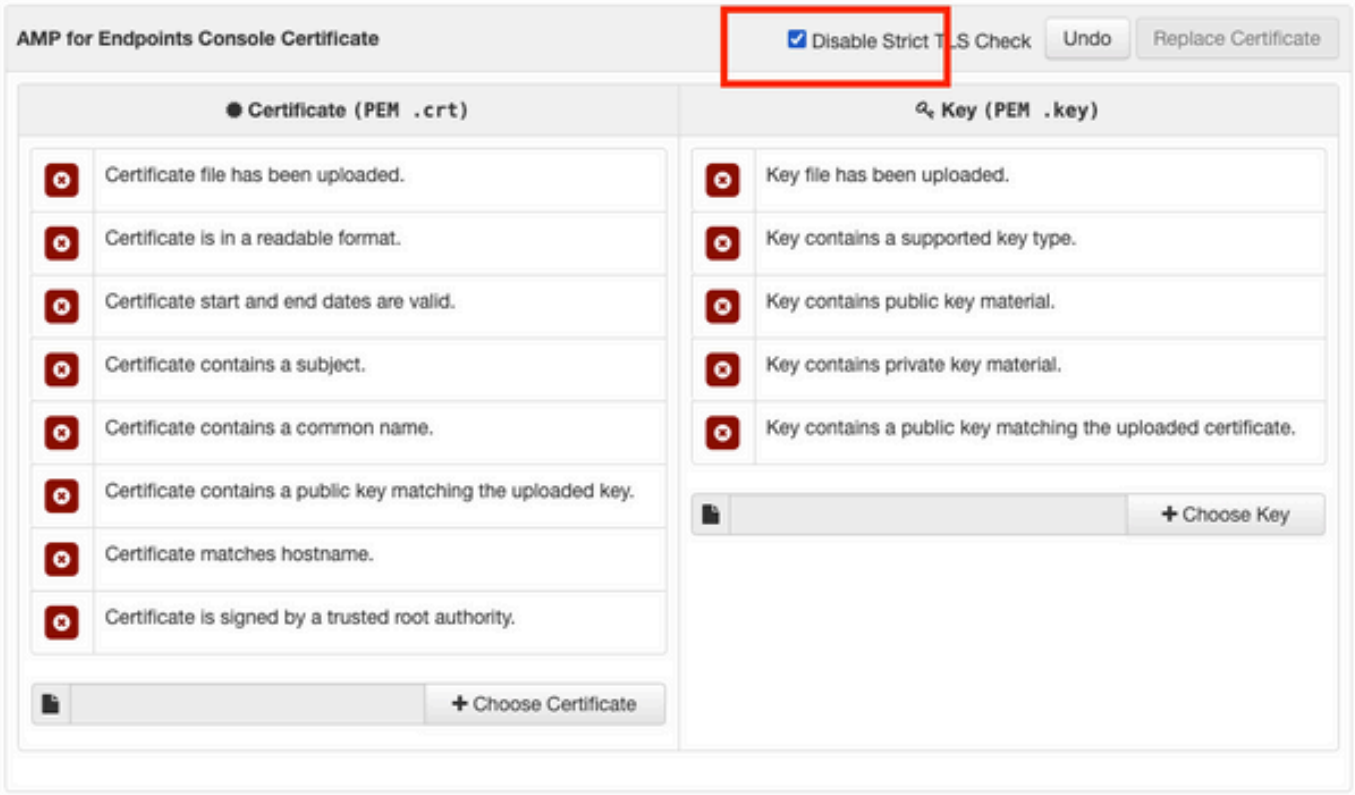
```
openssl genrsa -out
```

Paso 2. Genere el certificado de la CA.

```
openssl req \
-subj '/CN=
-addext "extendedKeyUsage = serverAuth, clientAuth" \
-outform pem -out
-key
-days "1000"
```

Generar un certificado para cada servicio

Cree el certificado para el servicio Autenticación, Consola, Disposición, Disposición ampliada, Actualizar servidor, Firepower Management Center (FMC) según la entrada de nombre DNS. Debe repetir el siguiente proceso de generación de certificados para cada servicio (autenticación, consola, etc.).



Generar clave privada

```
openssl genrsa -out
```

Sustituya <YourServiceName.key> por el nuevo nombre de archivo KEY que se creará como Auth-Cert.key

Generar CSR

```
openssl req -new \
-subj '/CN=
-key
```

Sustituya el <YourServiceName.key> con el archivo KEY del certificado actual (o nuevo), como Auth-Cert.key

Sustituya <YourServiceName.csr> por el nombre de archivo CSR que se va a crear, como Auth-Cert.crt

Generar certificado

```
openssl x509 -req \
-in
-CAkey
-days 397 -sha256
```

Reemplace <YourServiceName.csr> por un CSR de certificado real (o nuevo) como Auth-Cert.csr

Sustituya <YourRootCAName.pem> por el nombre de archivo PEM real (o nuevo) como RootCAName.pem

Reemplace <YourServiceName.key> por el archivo KEY del certificado actual (o nuevo), como Auth-Cert.key

Sustituya <YourServiceName.crt> por el nombre de archivo que se va a crear, como Auth-Cert.crt

Generar certificado en servidor Linux (verificación SSL estricta HABILITADA)

> **Nota**: La verificación TLS estricta verifica que el certificado cumpla los requisitos de TLS de Apple. Consulte la Guía de administración para obtener más información.

Generar CA raíz autofirmada

Paso 1. Genere la clave privada para el certificado de CA raíz.

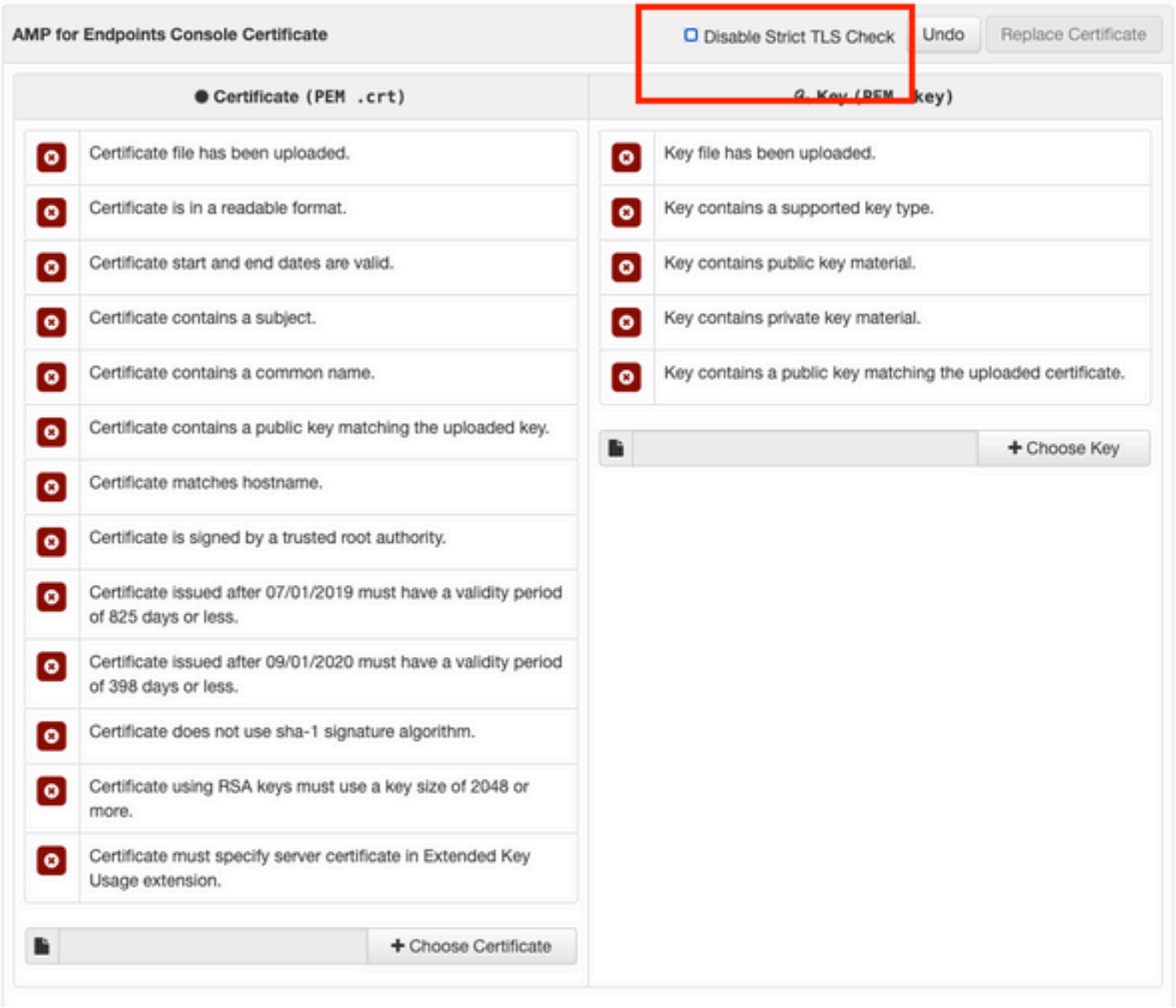
```
openssl genrsa -out
```

Paso 2. Genere el certificado de la CA.

```
openssl req \
-subj '/CN=
-outform pem -out
-key
-days "1000"
```

Generar un certificado para cada servicio

Cree el certificado para el servicio Autenticación, Consola, Disposición, Disposición ampliada, Actualizar servidor, Firepower Management Center (FMC) según la entrada de nombre DNS. Debe repetir el siguiente proceso de generación de certificados para cada servicio (autenticación, consola, etc.).



Crear un archivo de configuración de extensiones y guardarlo (extensions.cnf)

```
[v3_ca]
basicConstraints = CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = critical, serverAuth, clientAuth
```

Generar clave privada

```
openssl genrsa -out
```

Sustituya <YourServiceName.key> por un nuevo nombre de archivo KEY que se creará como Auth-Cert.key

Generar CSR

```
openssl req -new \
-key
-subj '/CN=
-out
```

Sustituya el <YourServiceName.key> con la CLAVE de certificado actual (o nueva), como Auth-Cert.key

Sustituya <YourServiceName.csr> por el CSR de certificado actual (o nuevo), como Auth-Cert.csr.

Generar certificado

```
openssl x509 -req -in
-CA
-CAcreateserial -out
-extensions v3_ca -extfile extensions.cnf \
-days 397 -sha256
```

Sustituya <YourServiceName.csr> por el CSR de certificado actual (o nuevo), como Auth-Cert.csr.

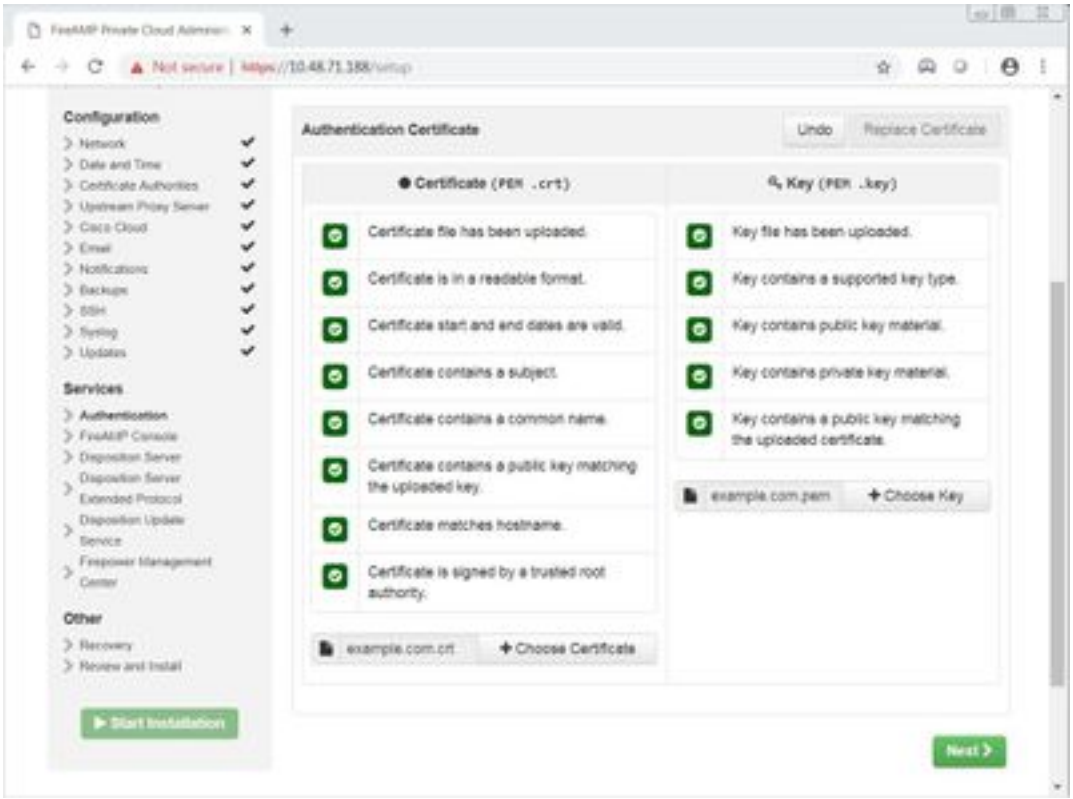
Sustituya <YourRootCAName.pem> por el nombre de archivo PEM actual (o nuevo) como RootCAName.pem

Reemplace <YourServiceName.key> por el archivo de clave de certificado actual (o nuevo), como Auth-Cert.key

Sustituya <YourServiceName.crt> por el nombre de archivo que se va a crear, como Auth-Cert.crt

Adición de certificados a la nube privada de consola segura

Paso 1. Una vez generados los certificados a partir de cualquiera de los métodos anteriores, cargue el certificado correspondiente para cada uno de los servicios. Si se han generado correctamente, todas las marcas de verificación están habilitadas como se ve en la imagen aquí.



Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

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).