

Instalación y renovación de certificados en ASA administrados por ASDM

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Solicitud e instalación de un nuevo certificado de identidad con ASDM](#)

[Solicitar e instalar un nuevo certificado de identidad con solicitud de firma de certificado \(CSR\)](#)

[Generación de un CSR con ASDM](#)

[Crear un punto de confianza con un nombre específico](#)

[\(Opcional\) Creación de un nuevo par de claves](#)

[Elija el nombre del par de claves](#)

[Configure el asunto del certificado y el nombre de dominio completamente calificado \(FQDN\)](#)

[Generar y guardar el CSR](#)

[Instalación del Certificado de Identidad en formato PEM con ASDM](#)

[Instalar el certificado de CA que firmó el CSR](#)

[Instalar certificado de identidad](#)

[Enlace del Nuevo Certificado a la Interfaz con ASDM](#)

[Instalación de un Certificado de Identidad Recibido en Formato PKCS12 con ASDM](#)

[Instalar la identidad y los certificados de CA desde un archivo PKCS12](#)

[Enlace del Nuevo Certificado a la Interfaz con ASDM](#)

[Renovación de certificados](#)

[Renovación de un certificado inscrito con solicitud de firma de certificado \(CSR\) con ASDM](#)

[Generación de un CSR con ASDM](#)

[Cree un nuevo punto de confianza con un nombre específico.](#)

[\(Opcional\) Creación de un nuevo par de claves](#)

[Seleccione el nombre del par de claves](#)

[Configure el asunto del certificado y el nombre de dominio completamente calificado \(FQDN\)](#)

[Generar y guardar el CSR](#)

[Instalación del Certificado de Identidad en Formato PEM con ASDM](#)

[Instalar el certificado de CA que firmó el CSR](#)

[Instalar certificado de identidad](#)

[Enlace del Nuevo Certificado a la Interfaz con ASDM](#)

[Renovación de un Certificado Inscrito con el Archivo PKCS12 con ASDM](#)

[Instalación del certificado de identidad renovado y los certificados de CA desde un archivo PKCS12](#)

[Enlace del Nuevo Certificado a la Interfaz con ASDM](#)

[Verificación](#)

[Ver certificados instalados mediante ASDM](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo solicitar, instalar, confiar y renovar ciertos tipos de certificados en el software Cisco ASA administrado con ASDM.

Prerequisites

Requirements

- Antes de comenzar, compruebe que el dispositivo de seguridad adaptable (ASA) tiene la hora, fecha y zona horaria del reloj correctas. Con la autenticación de certificados, se recomienda utilizar un servidor de protocolo de tiempo de la red (NTP) para sincronizar la hora en el ASA. Marque Información relacionada para referencia.
- Para solicitar un certificado que utilice la Solicitud de firma de certificado (CSR), es necesario tener acceso a una Autoridad de certificación (CA) interna o de terceros de confianza. Algunos ejemplos de proveedores de CA de terceros son, entre otros, Entrust, Geotrust, GoDaddy, Thawte y VeriSign.

Componentes Utilizados

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

- ASA 9.18.1
- Para la creación de PKCS12, se utiliza OpenSSL.

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

Los tipos de certificados a los que se dirige este documento son:

- Certificados con firma automática
- Certificados firmados por una autoridad de certificación externa o una CA interna

Los protocolos de autenticación Secure Socket Layer (SSL), Transport Layer Security (TLS) e IKEv2 RFC7296 para EAP exigen que el servidor SSL/TLS/IKEv2 proporcione al cliente un certificado de servidor para que el cliente realice la autenticación del servidor. Se recomienda utilizar CA de terceros de confianza para emitir certificados SSL al ASA con este fin.

Cisco no recomienda el uso de un certificado autofirmado debido a la posibilidad de que un

usuario pueda configurar inadvertidamente un navegador para confiar en un certificado de un servidor no autorizado. También existe la molestia para los usuarios de tener que responder a una advertencia de seguridad cuando se conecta al gateway seguro.

Solicitud e instalación de un nuevo certificado de identidad con ASDM

Se puede solicitar un certificado a una autoridad de certificación (CA) e instalarlo en un ASA de dos maneras:

- Utilizar la solicitud de firma de certificado (CSR). Genere un par de claves, solicite un certificado de identidad de CA con una CSR e instale el certificado de identidad firmado obtenido de CA.
- Utilice el archivo PKCS12 obtenido de una CA o exportado desde un dispositivo diferente. El archivo PKCS12 contiene pares de claves, certificados de identidad y certificados de CA.

Solicitar e instalar un nuevo certificado de identidad con solicitud de firma de certificado (CSR)


Se crea una CSR en el dispositivo que necesita un certificado de identidad; utilice un par de claves creado en el dispositivo.

Una CSR contiene:

- información de solicitud de certificado: asunto solicitado y otros atributos, clave pública del par de claves,
- información del algoritmo de firma,
- firma digital de la información de solicitud de certificado, firmada con la clave privada del par de claves.

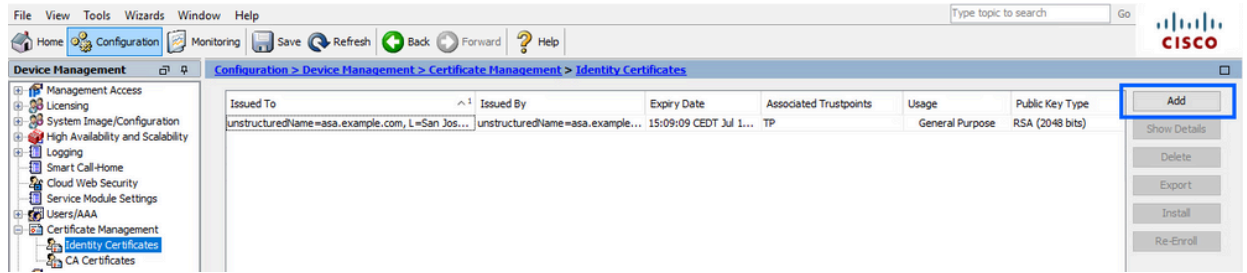
La CSR se pasa a la Autoridad de Certificación (CA), para que la firme, en un formulario PKCS#10.

El certificado firmado se devuelve desde la CA en un formulario PEM.

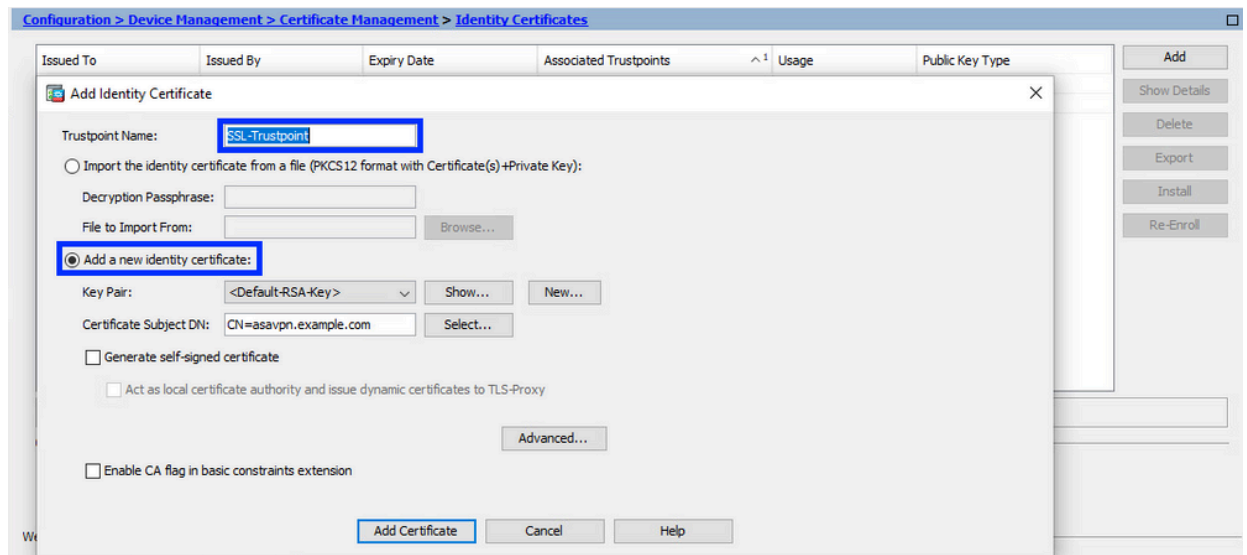
 Nota: CA puede modificar los parámetros FQDN y nombre de sujeto definidos en el punto de confianza cuando firma el CSR y crea un certificado de identidad firmado.

Generación de un CSR con ASDM

1. Crear un punto de confianza con un nombre específico
 - a. Vaya a Configuración > Administración de dispositivos > Administración de certificados > Certificados de identidad.




- b. Haga clic en Add (Agregar).
- c. Defina un nombre de punto de confianza.

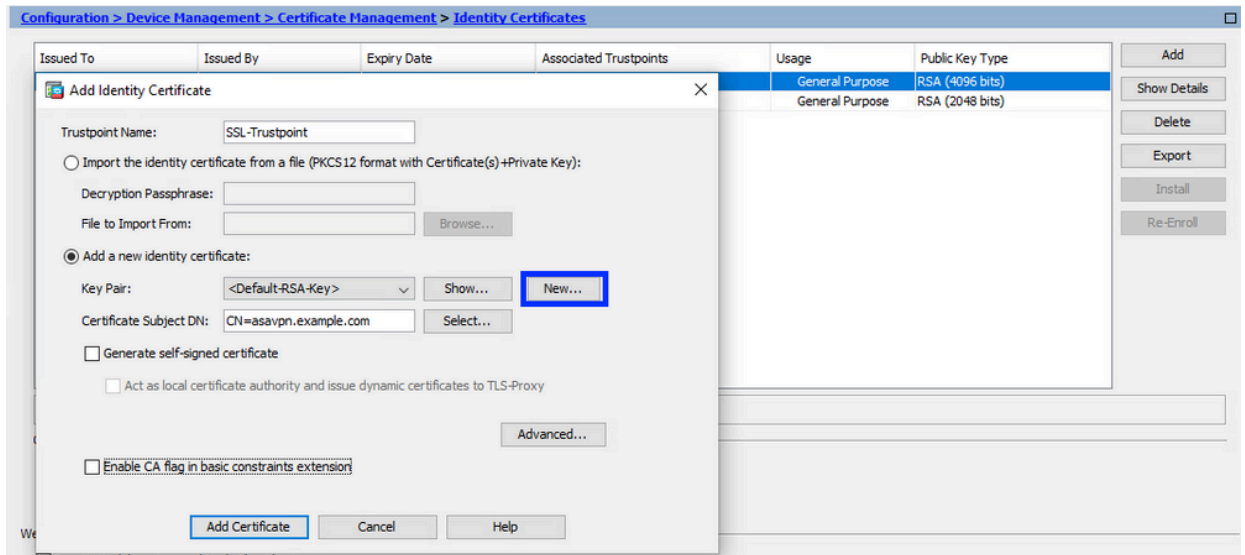


- d. Haga clic en el botón de opción Add a New Identity Certificate .

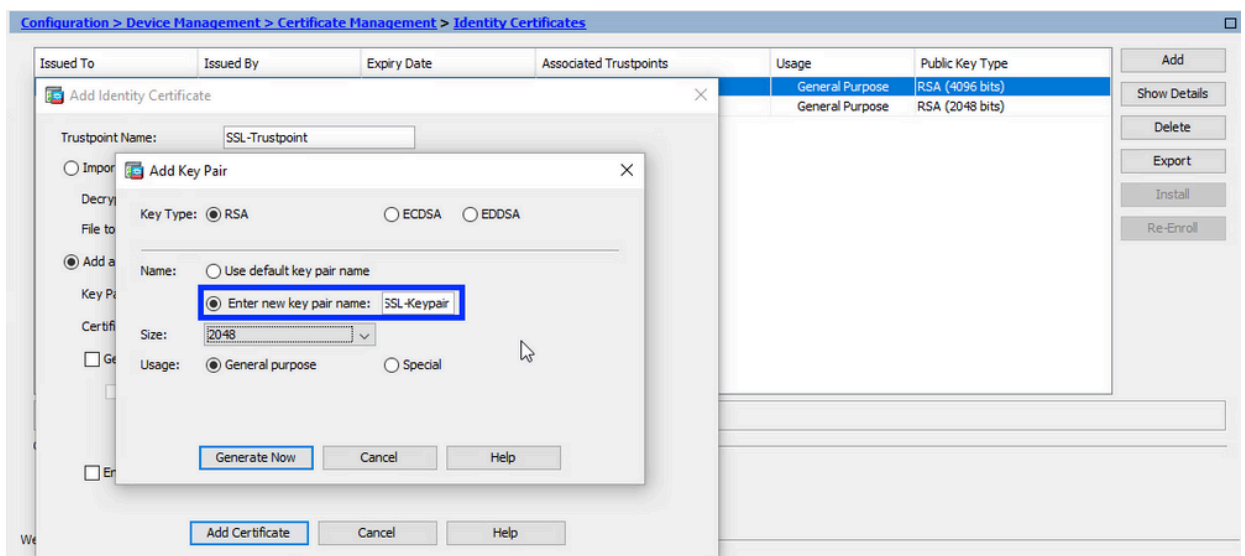
2. (Opcional) Creación de un nuevo par de claves

 Nota: De forma predeterminada, se utiliza la clave RSA con el nombre Default-RSA-Key y un tamaño de 2048. Sin embargo, se recomienda utilizar un único par de claves pública y privada para cada certificado de identidad.

- a. Haga clic en Nuevo para generar un nuevo par de claves.

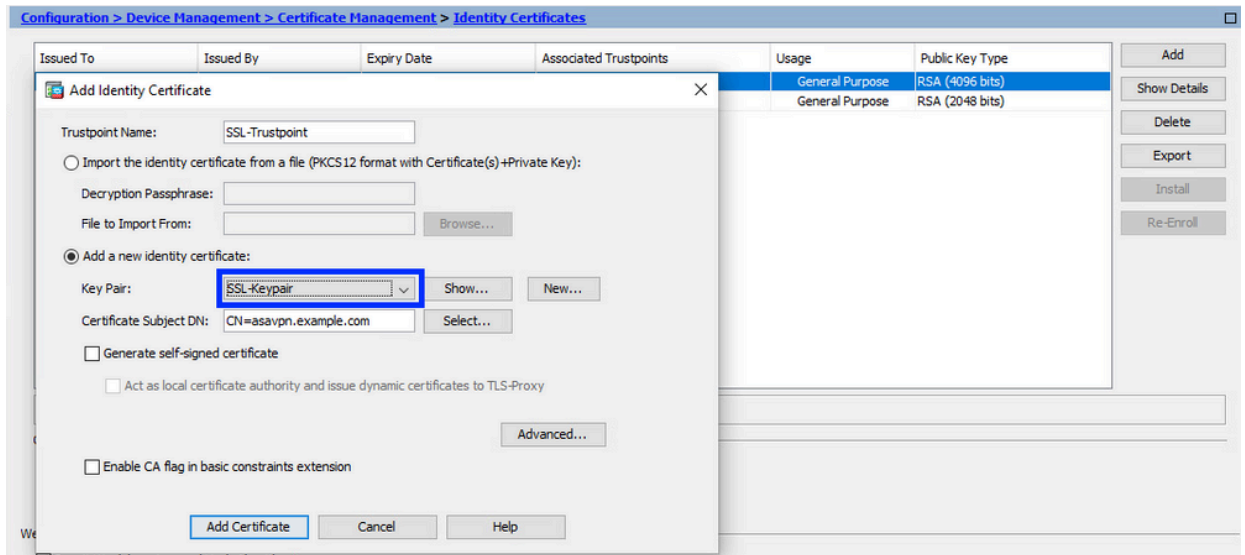


- b. Elija la opción Enter new Key Pair name e ingrese un nombre para el nuevo Key Pair.
- c. Elija el Tipo de clave: RSA o ECDSA.
- d. Elija el tamaño de clave; para RSA, elija propósito general para uso.
- e. Haga clic en Generar ahora. Ya se ha creado el par de claves.



3. Elija el nombre del par de claves

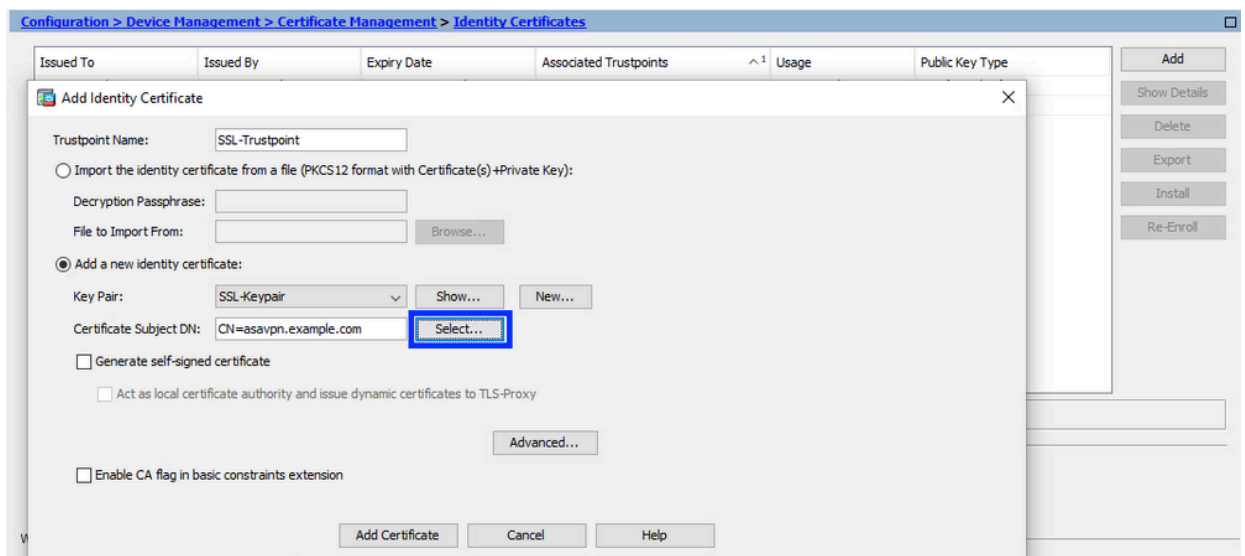
Elija el par de claves con el que firmar el CSR y al que se vinculará con el nuevo certificado.



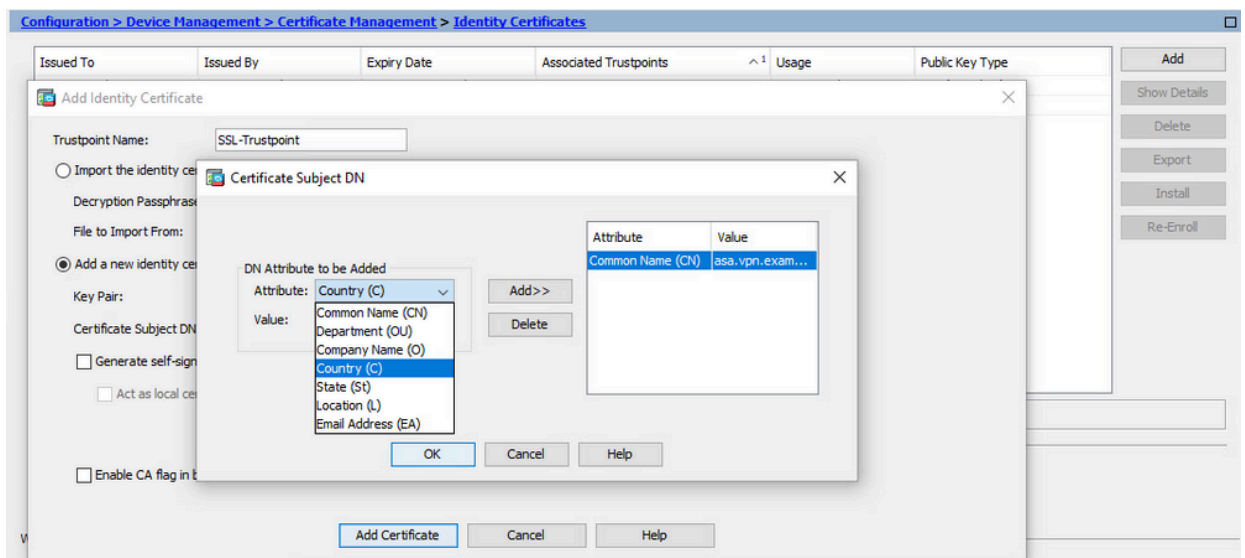
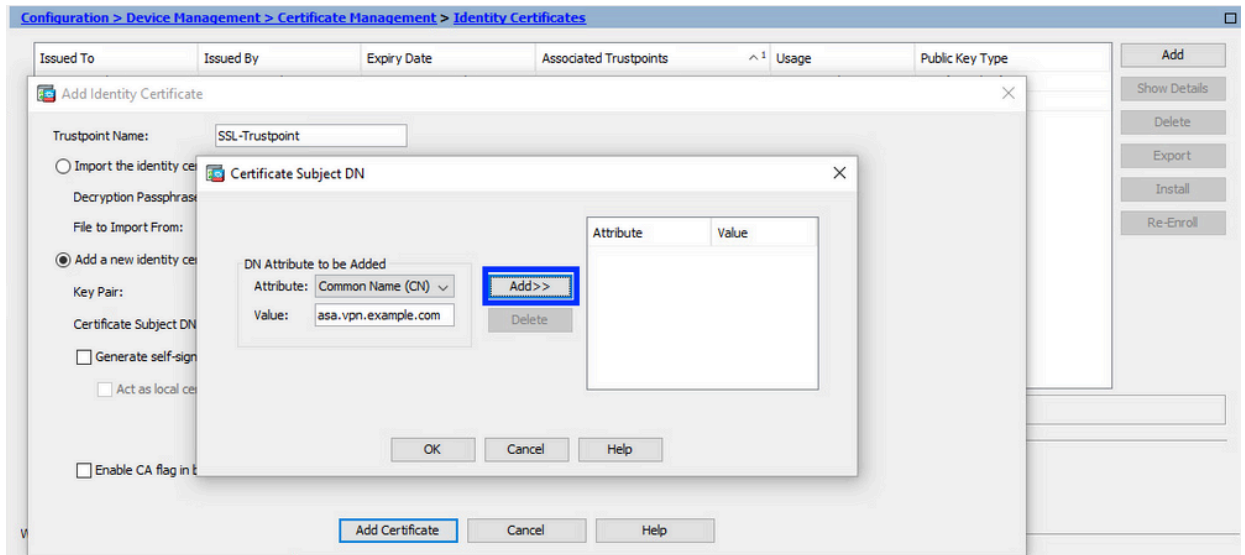
4. Configure el asunto del certificado y el nombre de dominio completamente calificado (FQDN)

⚠️ Precaución: el parámetro FQDN debe coincidir con el FQDN o la dirección IP de la interfaz ASA para la que se utiliza el certificado de identidad. Este parámetro establece la extensión de nombre alternativo de sujeto (SAN) solicitada para el certificado de identidad. El cliente SSL/TLS/IKEv2 utiliza la extensión SAN para verificar si el certificado coincide con el FQDN al que se conecta.


a. Haga clic en Seleccionar.



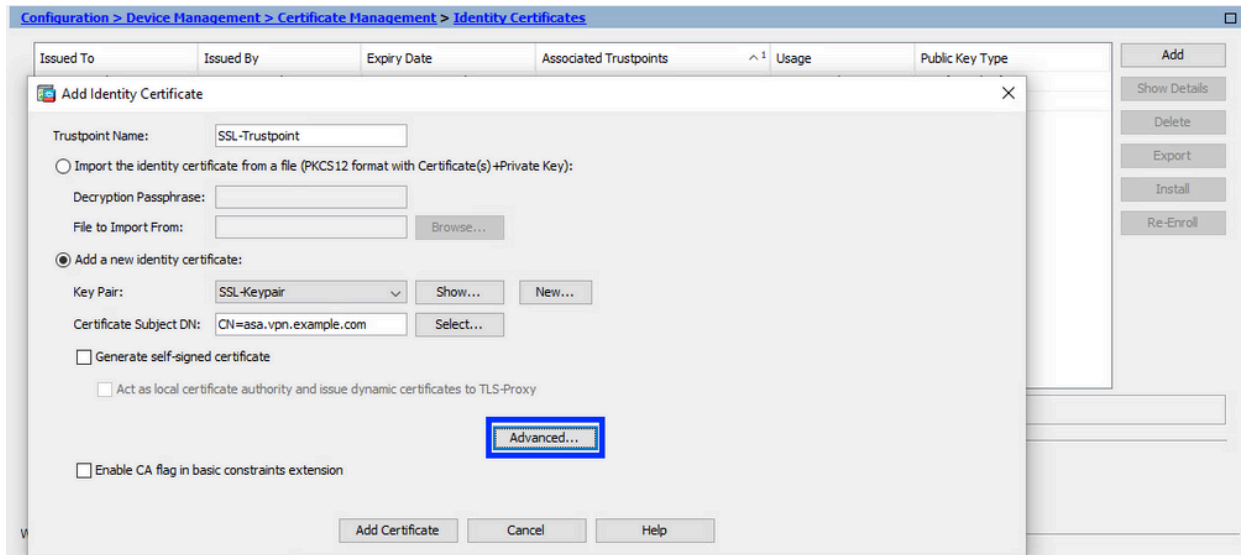
b. En la ventana Certificate Subject DN, configure certificate attributes - choose attribute from drop-down list, ingrese el valor, haga clic en Add.



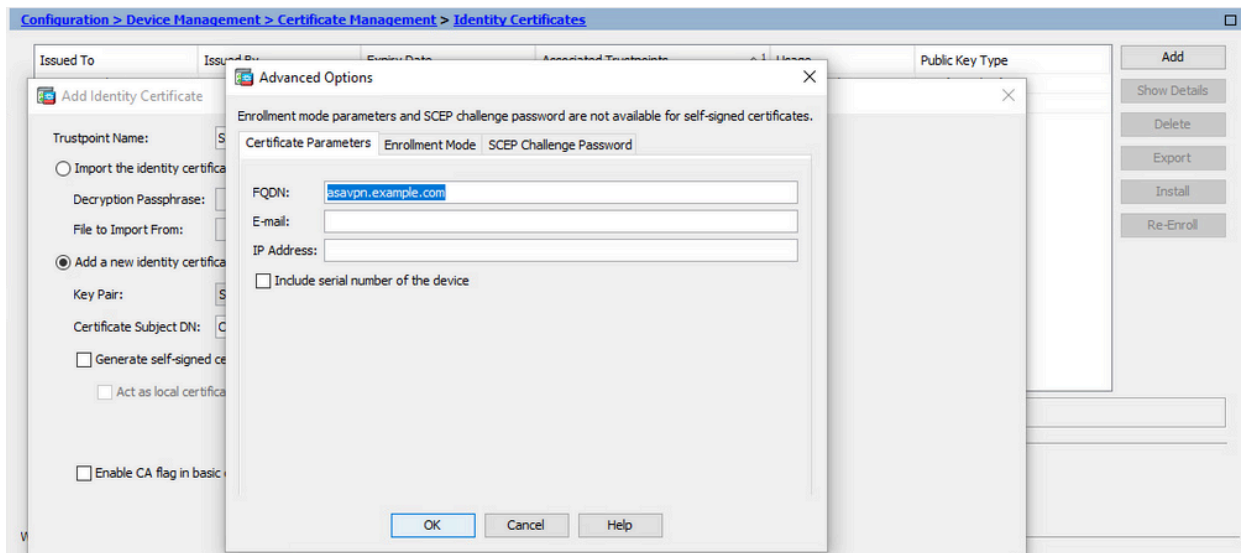
Atributo	Descripción
CN	El nombre a través del cual se puede acceder al firewall (normalmente el nombre de dominio completo, por ejemplo, vpn.example.com).
OU	El nombre de su departamento dentro de la organización
O	El nombre registrado legalmente de su organización/empresa
C	Código de país (código de 2 letras sin puntuación)
ST	El estado en el que se encuentra la organización.
L	La ciudad en la que se encuentra su organización.
EA	Dirección de correo

 Nota: ninguno de los valores de campos anteriores puede superar un límite de 64 caracteres. Un valor mayor podría causar problemas con la instalación del certificado de identidad. Además, no es necesario definir todos los atributos DN.

- Haga clic en Aceptar después de agregar todos los atributos.
 c. Configure el FQDN del dispositivo: haga clic en Advanced.

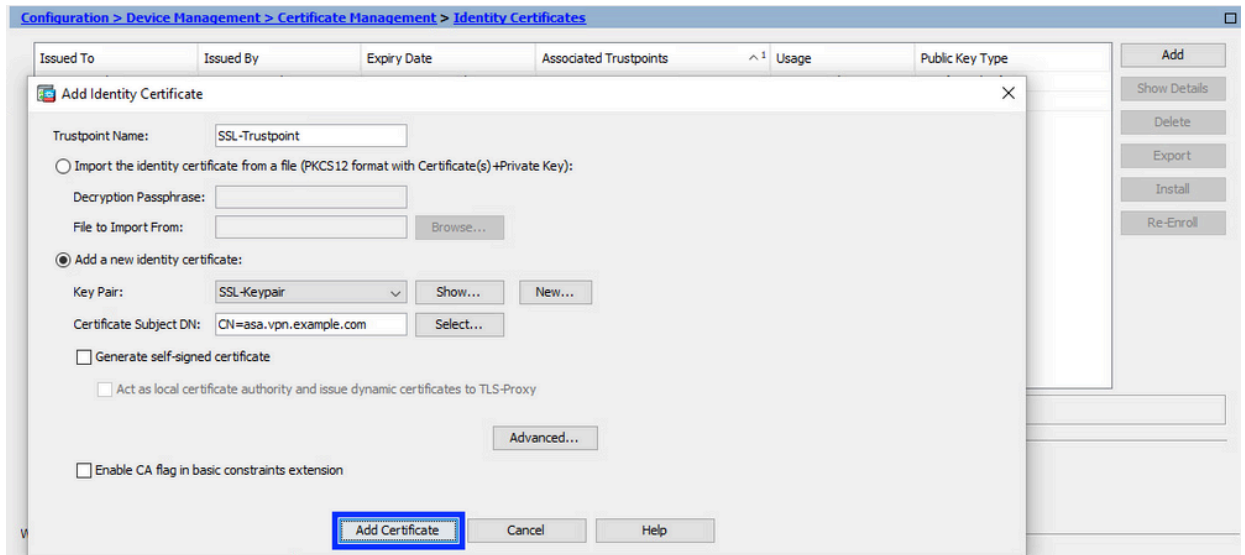


- d. En el campo FQDN, introduzca el nombre de dominio completo a través del cual se puede acceder al dispositivo desde Internet. Click OK.

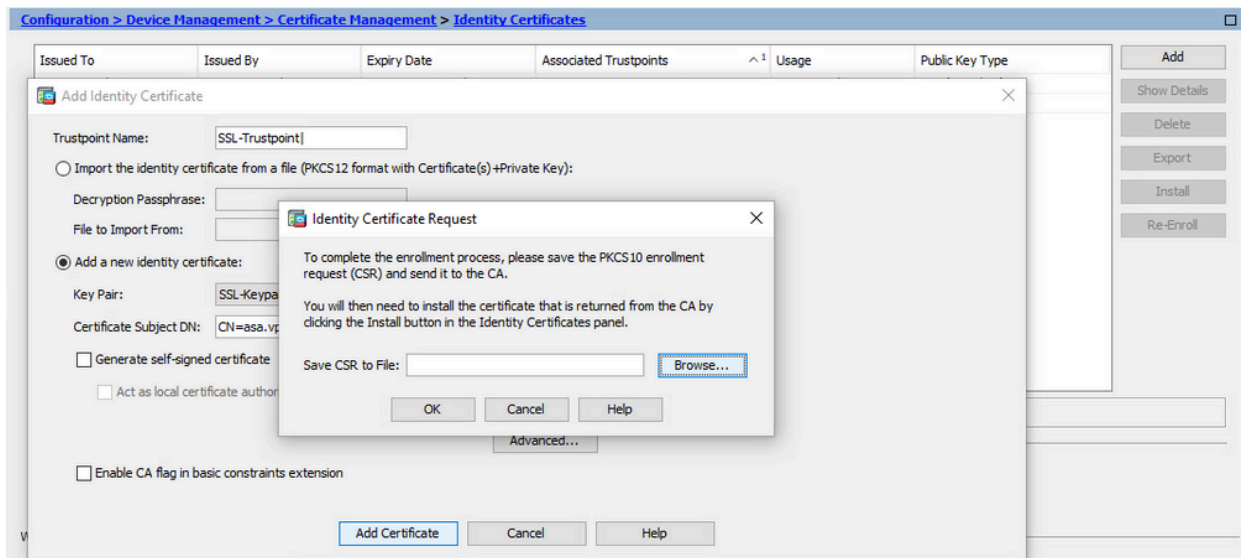


5. Generar y guardar el CSR


- a. Haga clic en Agregar certificado.



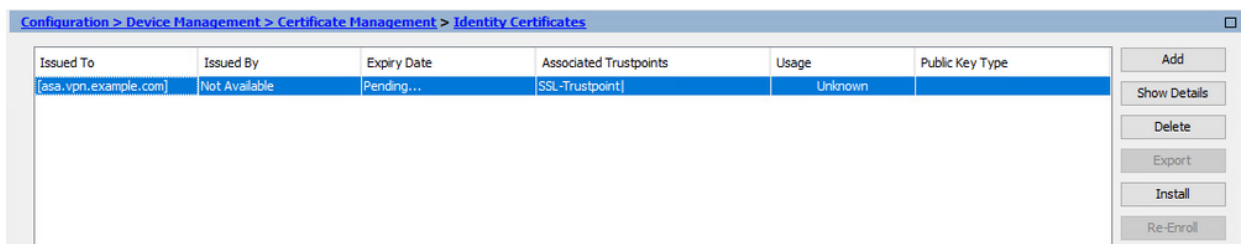
b. Se muestra un mensaje para guardar el CSR en un archivo en la máquina local.



Haga clic en Browse, elija una ubicación en la que guardar el CSR, y guarde el archivo con la extensión .txt.

 Nota: Cuando el archivo se guarda con una extensión .txt, la solicitud PKCS#10 se puede abrir y ver con un editor de texto (como el Bloc de notas).

c. Ahora el nuevo punto de confianza se muestra en un estado Pendiente.

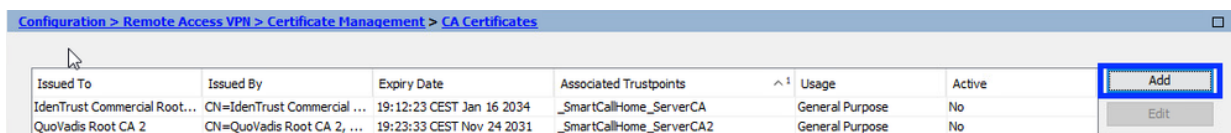


Instalación del Certificado de Identidad en formato PEM con ASDM

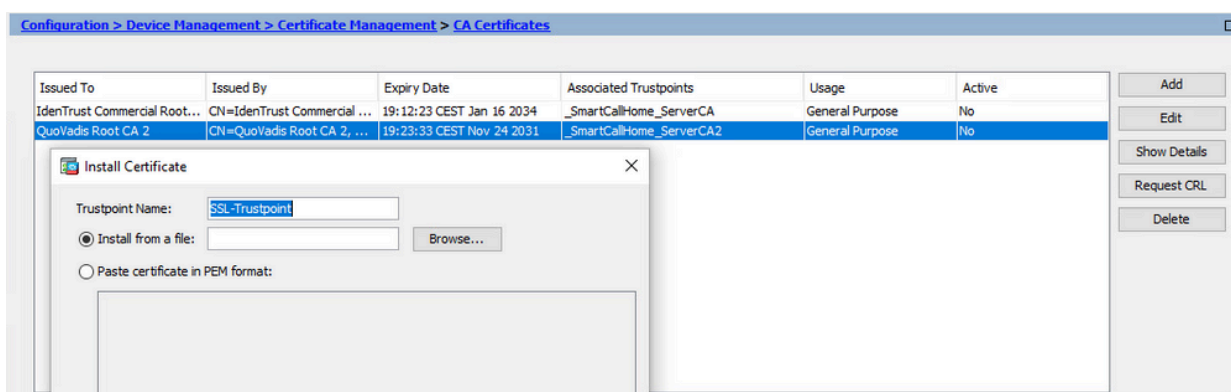
En los pasos de instalación, se supone que la CA firmó el CSR y proporcionó un paquete de certificados de CA y un certificado de identidad codificados por PEM (.pem, .cer, .crt).


1. Instalar el certificado de CA que firmó el CSR

- a. Vaya a Configuration > Device Management > Certificate Management > y elija CA Certificates. Haga clic en Add (Agregar).

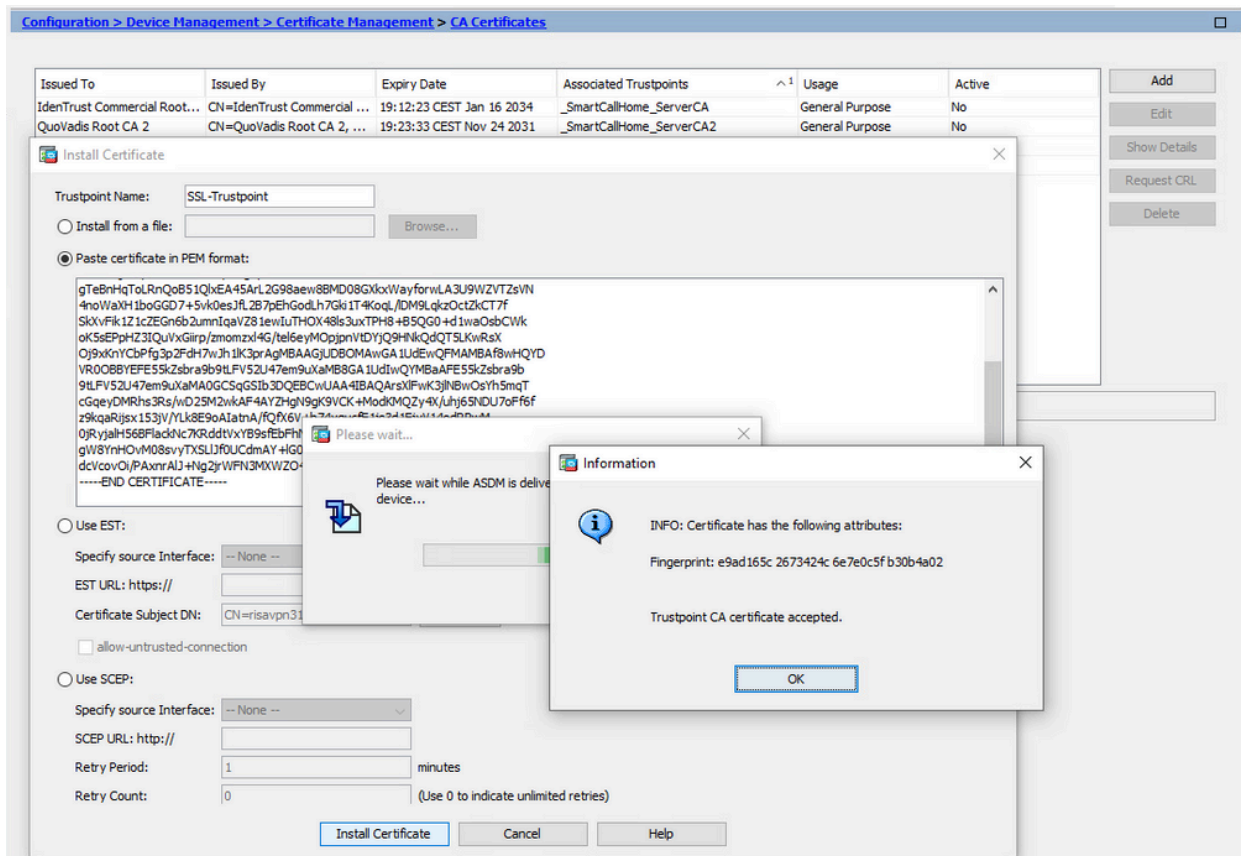


- b. Introduzca el nombre del punto de confianza y seleccione Install From File (Instalar desde archivo), haga clic en el botón Browse (Examinar) y seleccione el certificado intermedio. También puede pegar el certificado de CA codificado PEM de un archivo de texto en el campo de texto.



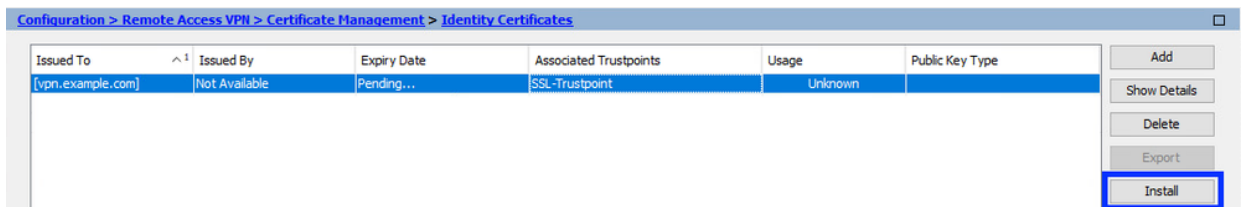
 Nota: instale el certificado de CA que firmó el CSR. Utilice el mismo nombre de punto de confianza que el certificado de identidad. Los otros certificados de CA superiores en la jerarquía PKI se pueden instalar en puntos de confianza independientes.


- c. Haga clic en Install Certificate.



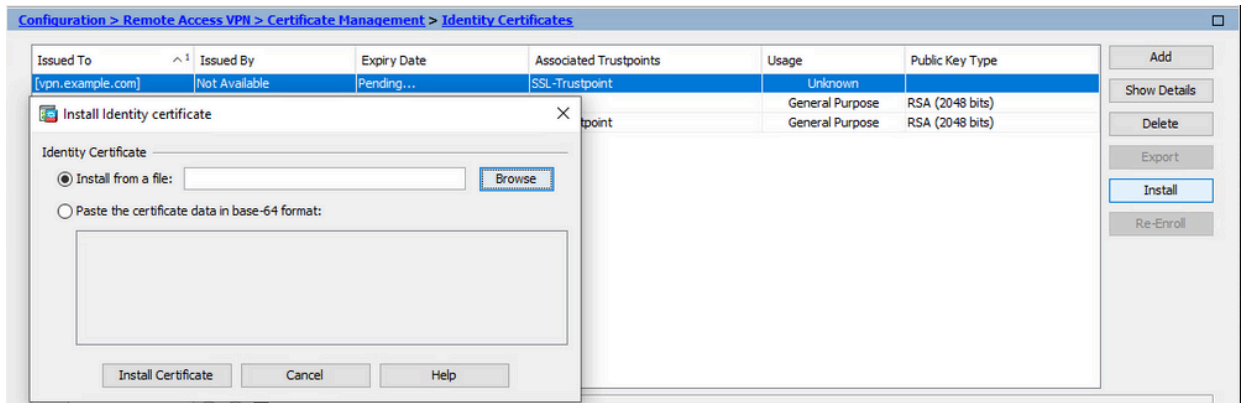
2. Instalar certificado de identidad


- a. Elija el certificado de identidad creado anteriormente durante la generación de CSR. Haga clic en Instale.



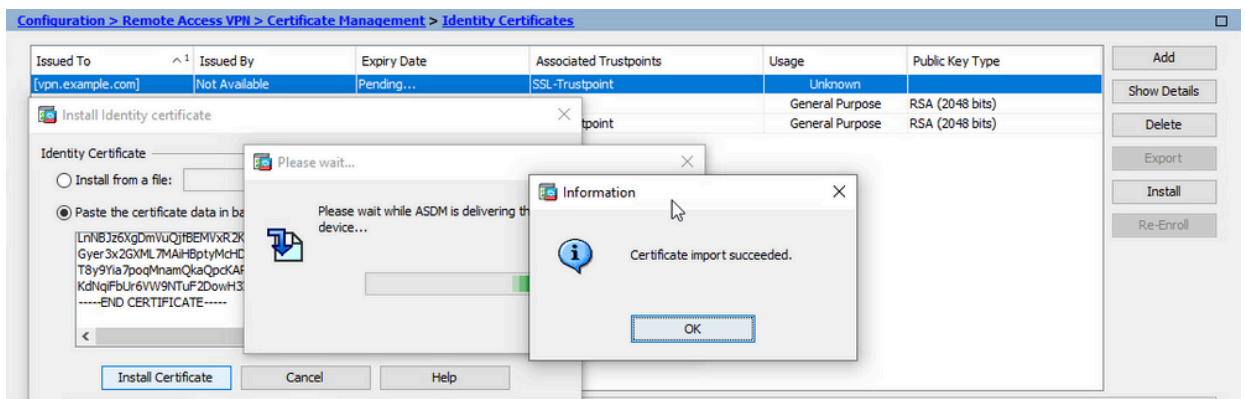
 Nota: El certificado de identidad puede tener el campo Emitido por como No disponible y el campo Fecha de vencimiento como Pendiente.

- b. Elija un archivo que contenga el certificado de identidad con codificación PEM recibido de la CA, o abra el certificado con codificación PEM en un editor de texto y copie y pegue el certificado de identidad proporcionado por la CA en el campo de texto.



 Nota: el certificado de identidad puede tener el formato .pem, .cer o .crt para su instalación.

c. Haga clic en Install Certificate.



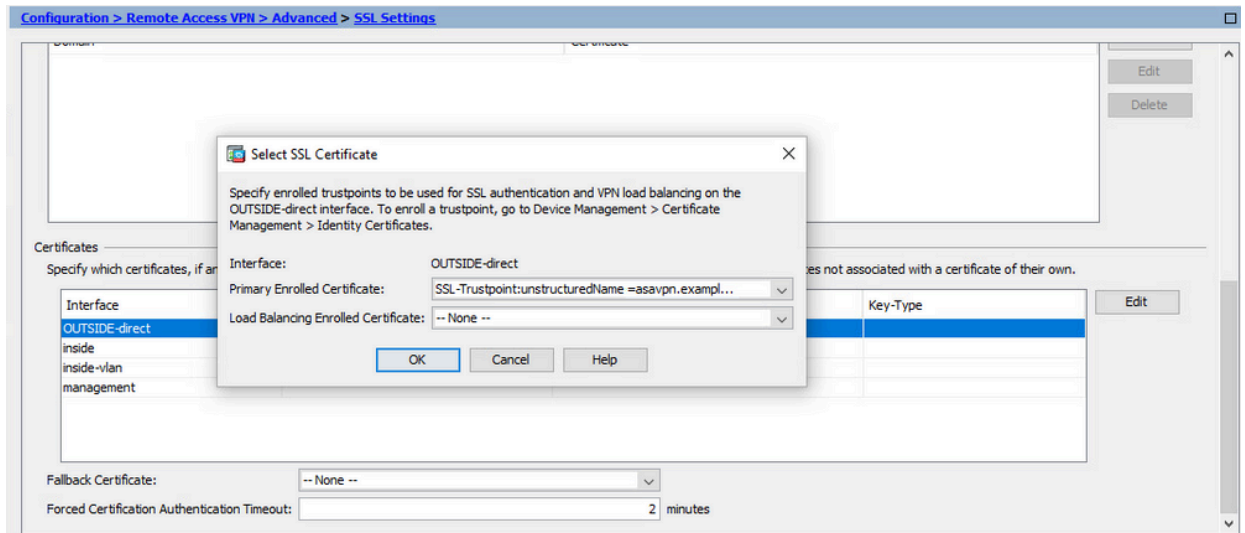
3. Enlace del Nuevo Certificado a la Interfaz con ASDM

El ASA debe configurarse para utilizar el nuevo certificado de identidad para las sesiones WebVPN que terminan en la interfaz especificada.

- a. Vaya a Configuration > Remote Access VPN > Advanced > SSL Settings.
- b. En Certificados, elija la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.

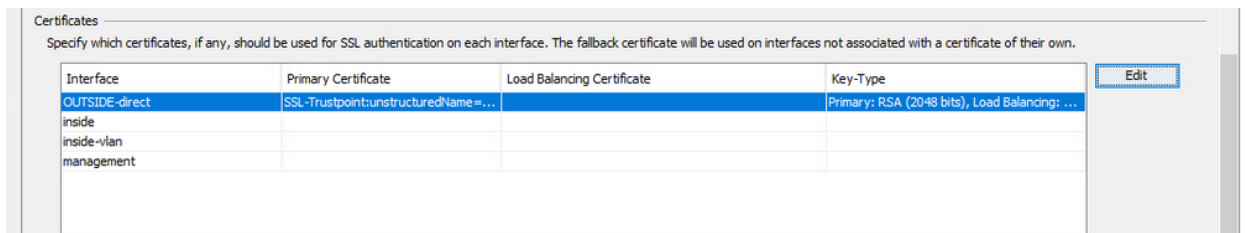
Haga clic en Editar.

- c. En la lista desplegable Certificado, seleccione el certificado recién instalado.



d. Click OK.

e. Haga clic en Apply (Aplicar).



Ahora el nuevo certificado de identidad está en uso.

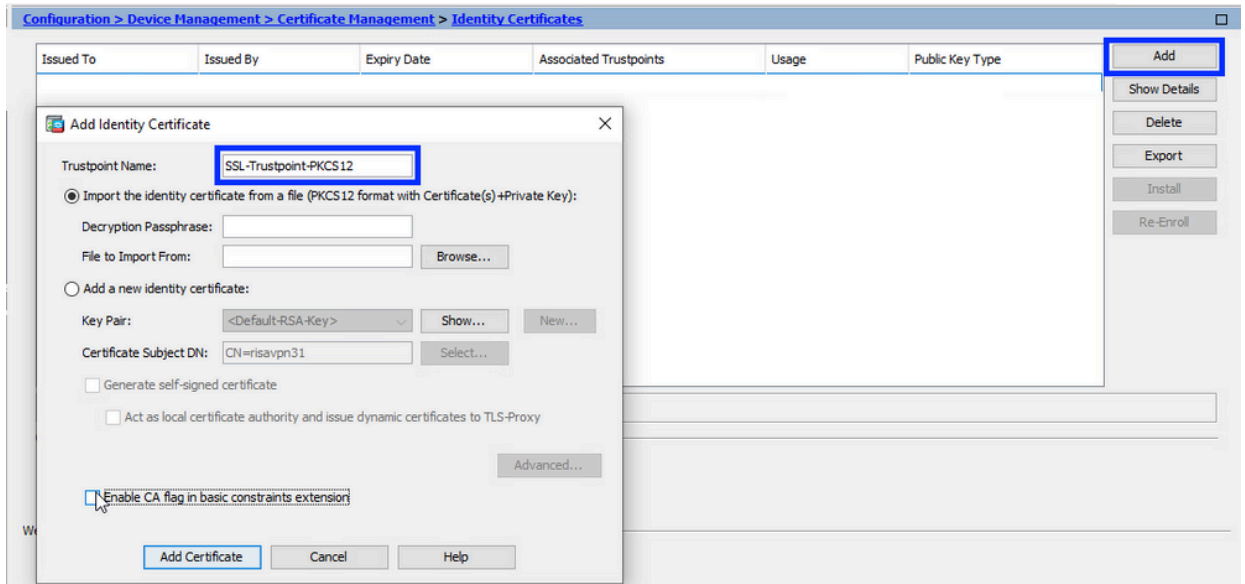
Instalación de un Certificado de Identidad Recibido en Formato PKCS12 con ASDM

El archivo PKCS12 (formato .p12 o .pfx) contiene el certificado de identidad, el par de claves y los certificados de CA. Es creado por la CA, por ejemplo, en el caso de un certificado comodín, o exportado desde un dispositivo diferente. Es un archivo binario, no se puede ver con el editor de texto.

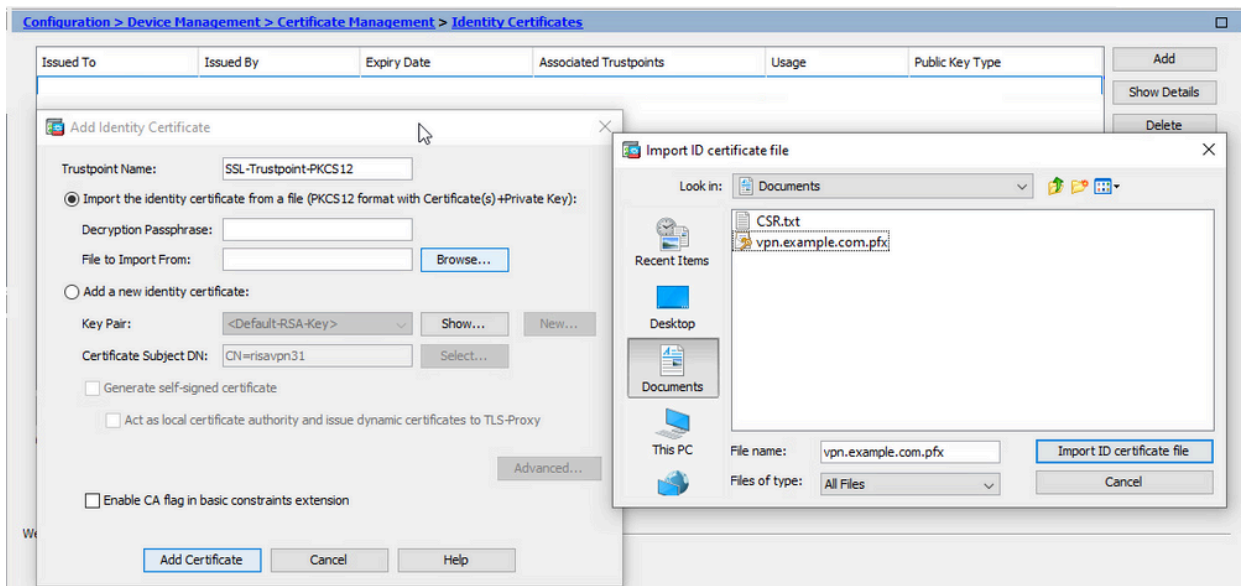
1. Instalar la identidad y los certificados de CA desde un archivo PKCS12

El certificado de identidad, los certificados de CA y el par de claves deben incluirse en un único archivo PKCS12.

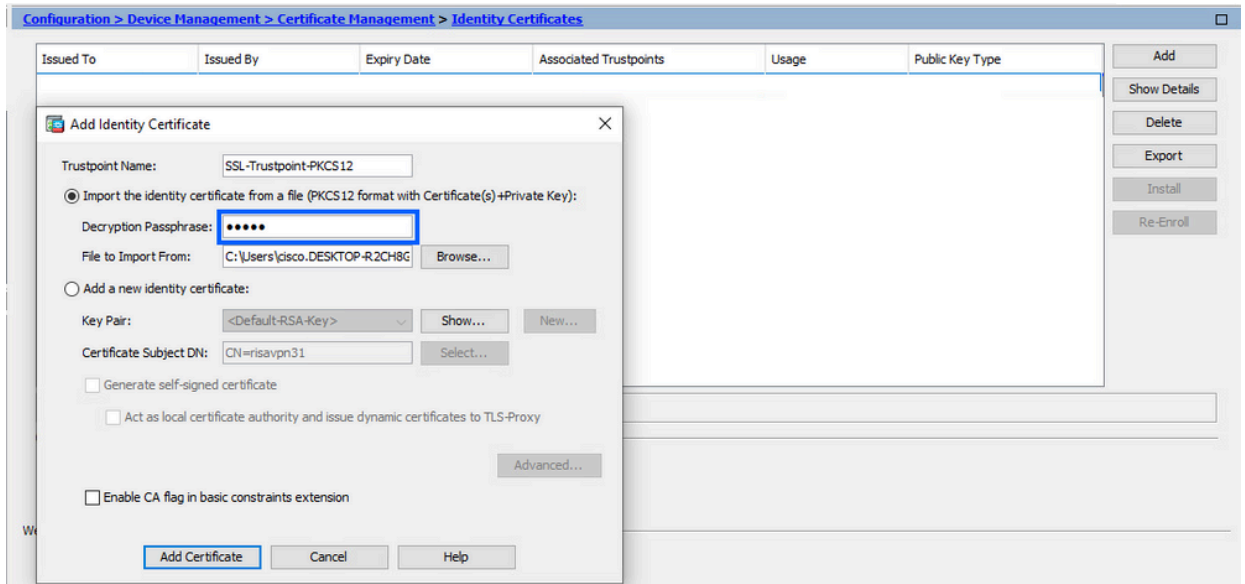
- Navegue hasta Configuration > Device Management > Certificate Management, y elija Identity Certificates.
- Haga clic en Add (Agregar).
- Especifique un nombre de punto de confianza.



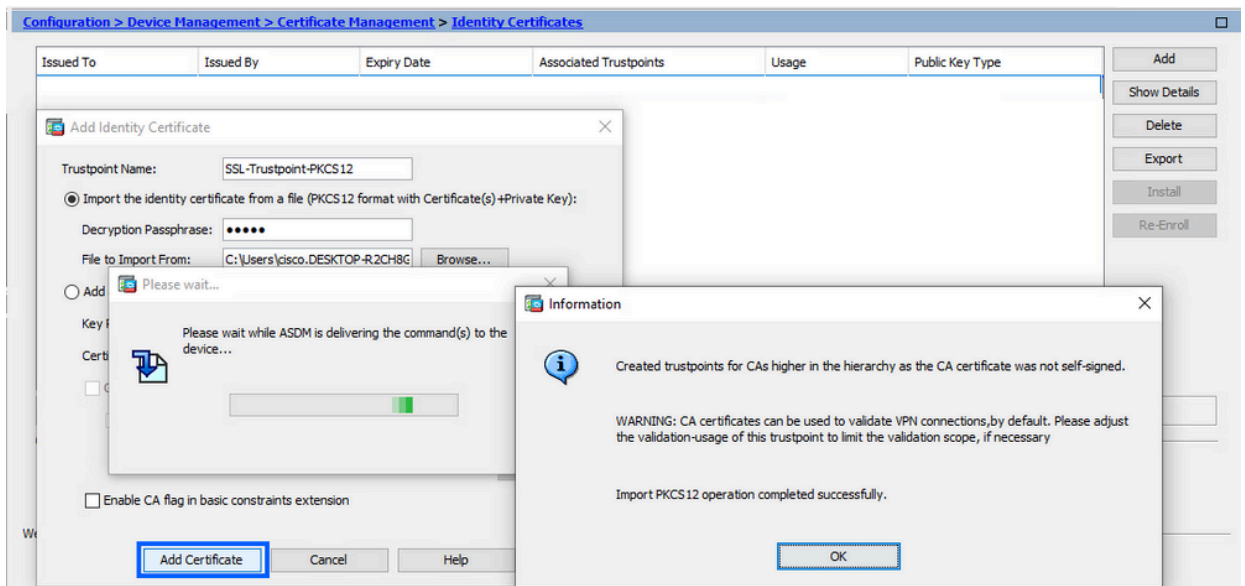
d. Haga clic en el botón de opción Import The Identity Certificate from a File .




e. Introduzca la frase de paso utilizada para crear el archivo PKCS12.



f. Haga clic en Agregar certificado.



 Nota: Al importar un PKCS12 con la cadena de certificados de CA, el ASDM crea automáticamente los puntos de confianza de CA ascendentes con nombres con el sufijo -number agregado.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub 1-1	CN=KrakowCA-sub 1	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12	Signature	Yes
KrakowCA-sub 1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12-2	Signature	Yes

2. Enlace del Nuevo Certificado a la Interfaz con ASDM

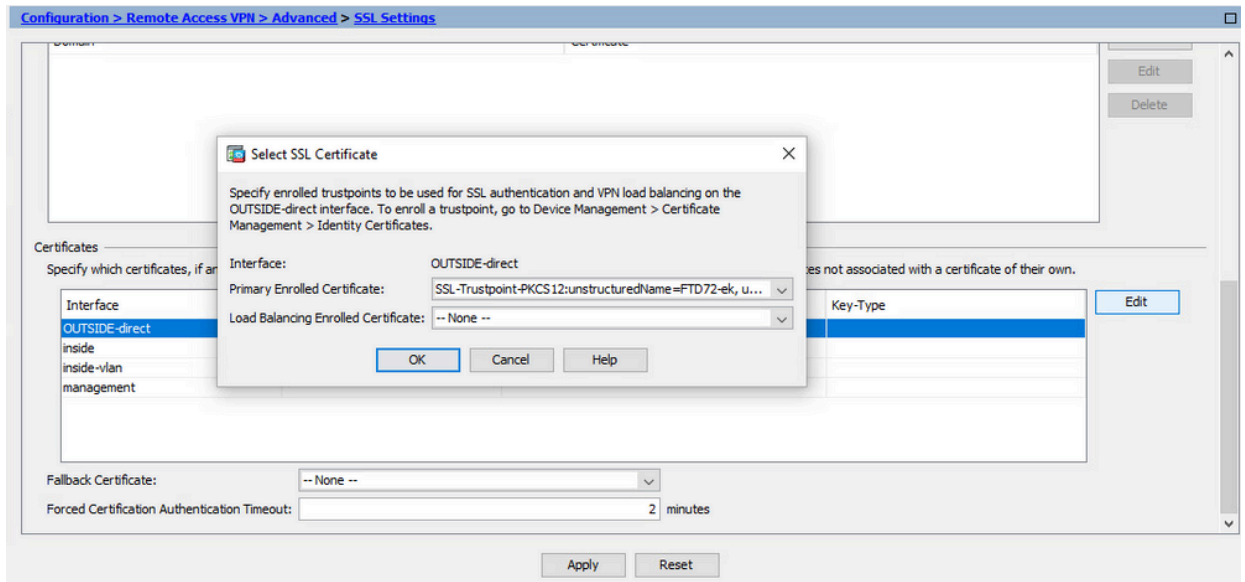
El ASA debe configurarse para utilizar el nuevo certificado de identidad para las sesiones WebVPN que terminan en la interfaz especificada.

a. Vaya a Configuration > Remote Access VPN > Advanced > SSL Settings.

- b. En Certificados, seleccione la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.

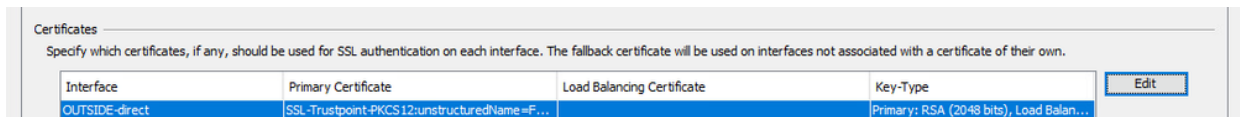
Haga clic en Editar.

- c. En la lista desplegable Certificado, seleccione el certificado recién instalado.



- d. Click OK.

- e. Haga clic en Apply (Aplicar).



Ahora el nuevo certificado de identidad está en uso.

Renovación de certificados

Renovación de un certificado inscrito con solicitud de firma de certificado (CSR) con ASDM

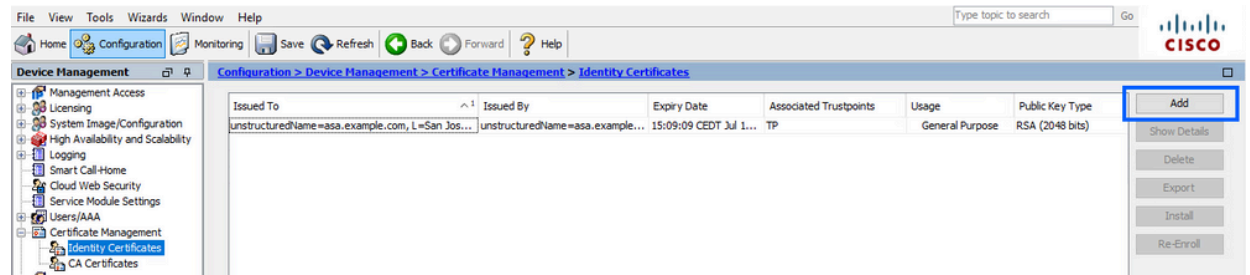
La renovación del certificado CSR inscrito requiere crear e inscribir un nuevo punto de confianza. Debe tener un nombre diferente (por ejemplo, nombre antiguo con sufijo de año de inscripción). Puede utilizar los mismos parámetros y par de claves que el certificado anterior, o puede utilizar otros diferentes.

Generación de un CSR con ASDM

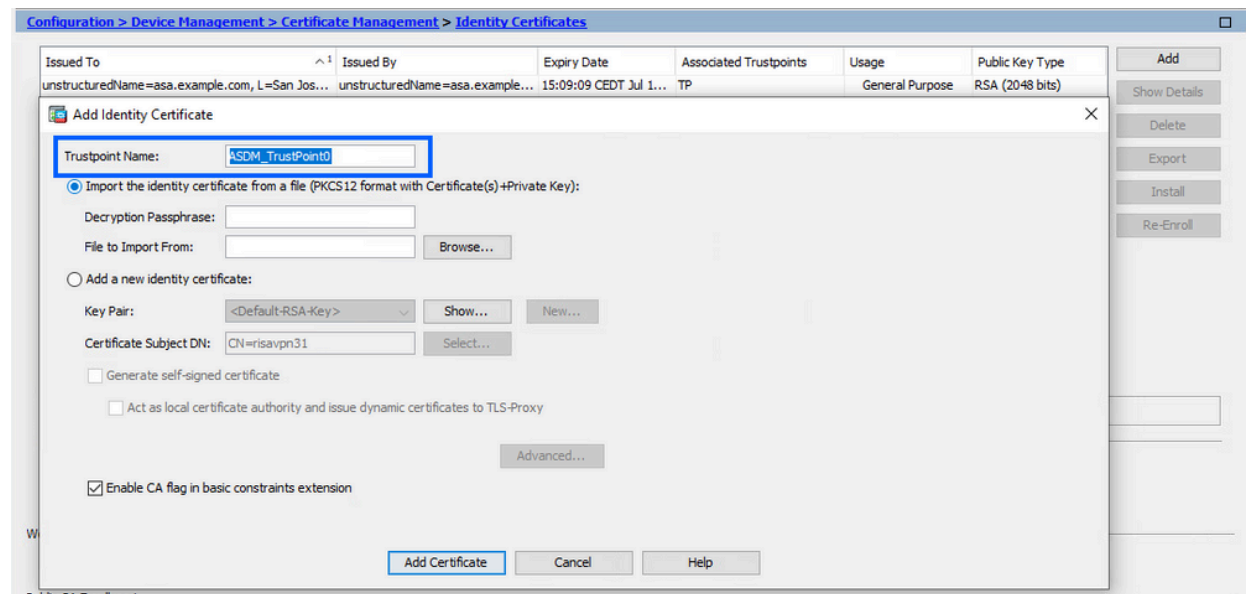
1. Cree un nuevo punto de confianza con un nombre específico.

- a. Vaya a Configuración > Administración de dispositivos > Administración de certificados

> Certificados de identidad.




- b. Haga clic en Add (Agregar).
- c. Defina un nombre de punto de confianza.

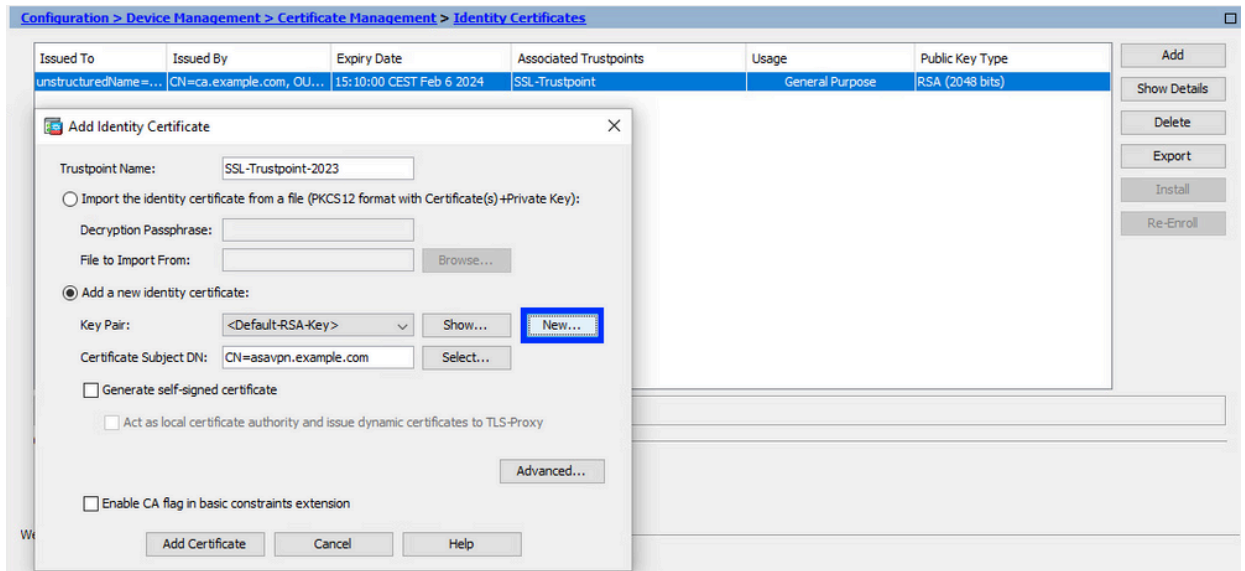


- d. Haga clic en el botón de opción Add a New Identity Certificate .

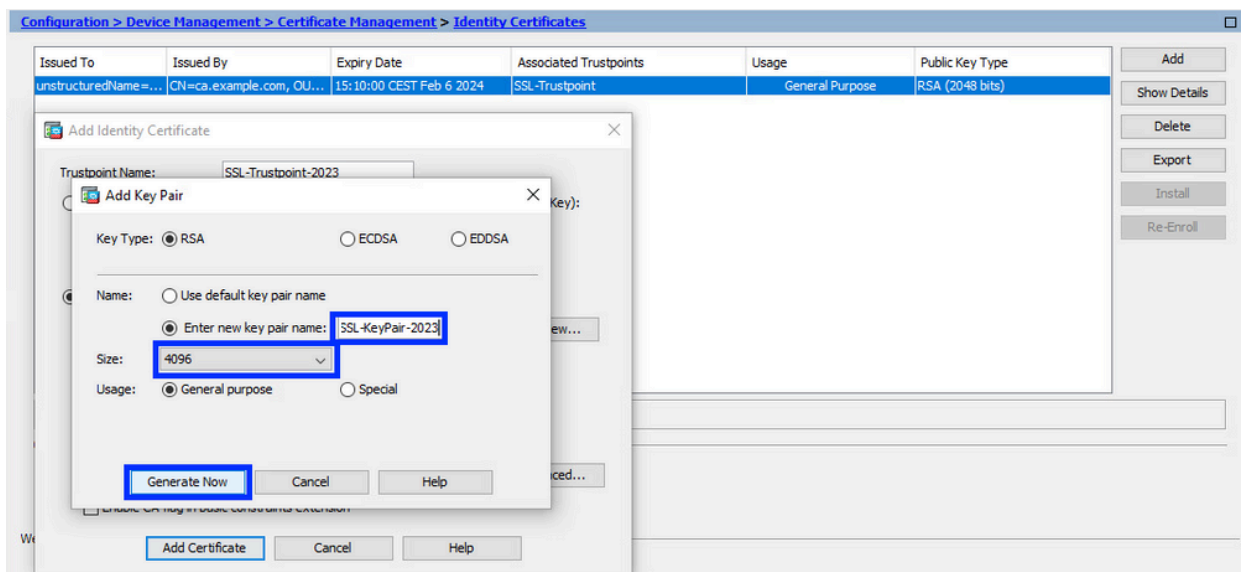
2. (Opcional) Creación de un nuevo par de claves

 Nota: De forma predeterminada, se utiliza la clave RSA con el nombre Default-RSA-Key y un tamaño de 2048; sin embargo, se recomienda utilizar un par de claves privada/pública único para cada certificado de identidad.

- a. Haga clic en Nuevo para generar un nuevo par de claves.

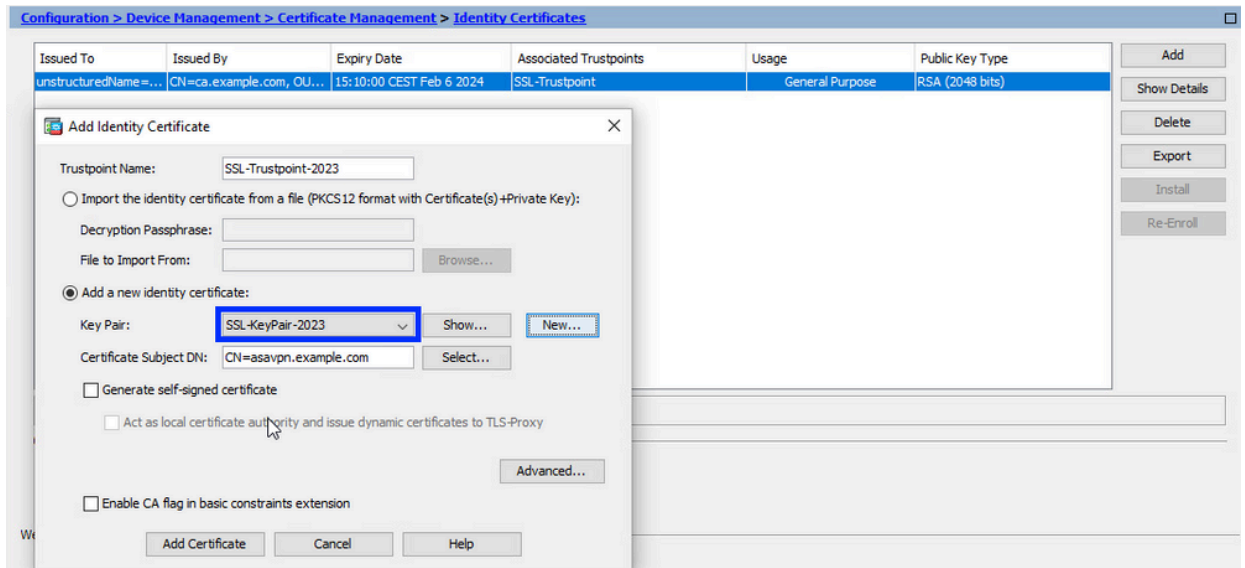


- b. Elija la opción Enter new Key Pair name e ingrese un nombre para el nuevo Key Pair.
- c. Elija el tipo de clave: RSA o ECDSA.
- d. Elija el tamaño de clave; para RSA, elija Propósito general para Uso.
- e. Haga clic en Generar ahora. Ya se ha creado el par de claves.



3. Seleccione el nombre del par de claves

Elija el par de claves con el que firmar el CSR y al que se vinculará con el nuevo certificado.

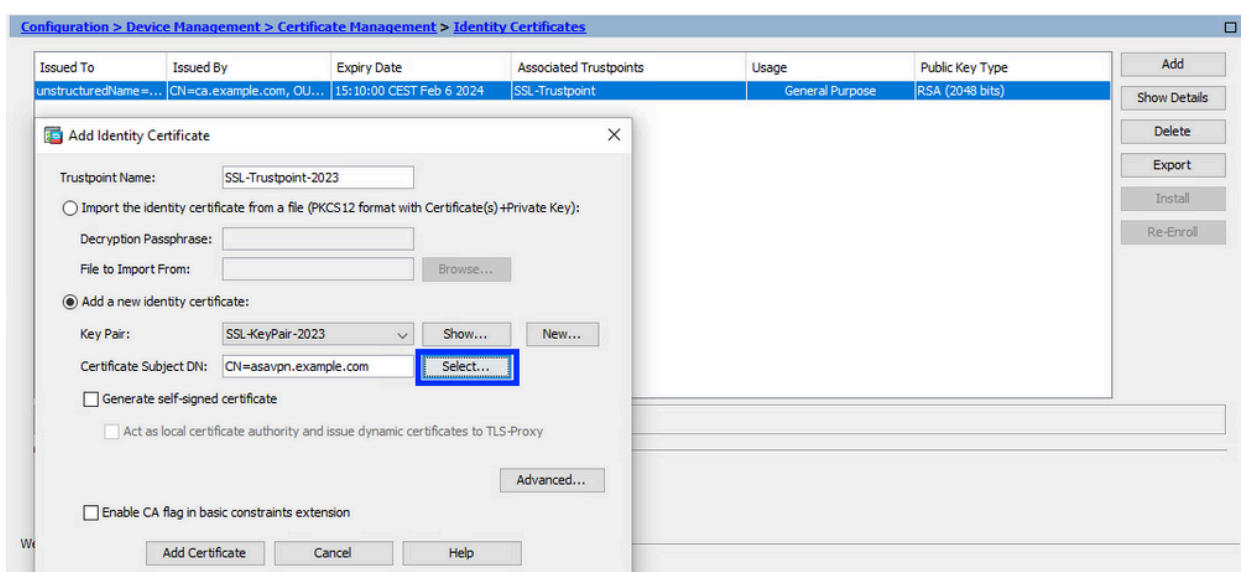


4. Configure el asunto del certificado y el nombre de dominio completamente calificado (FQDN)

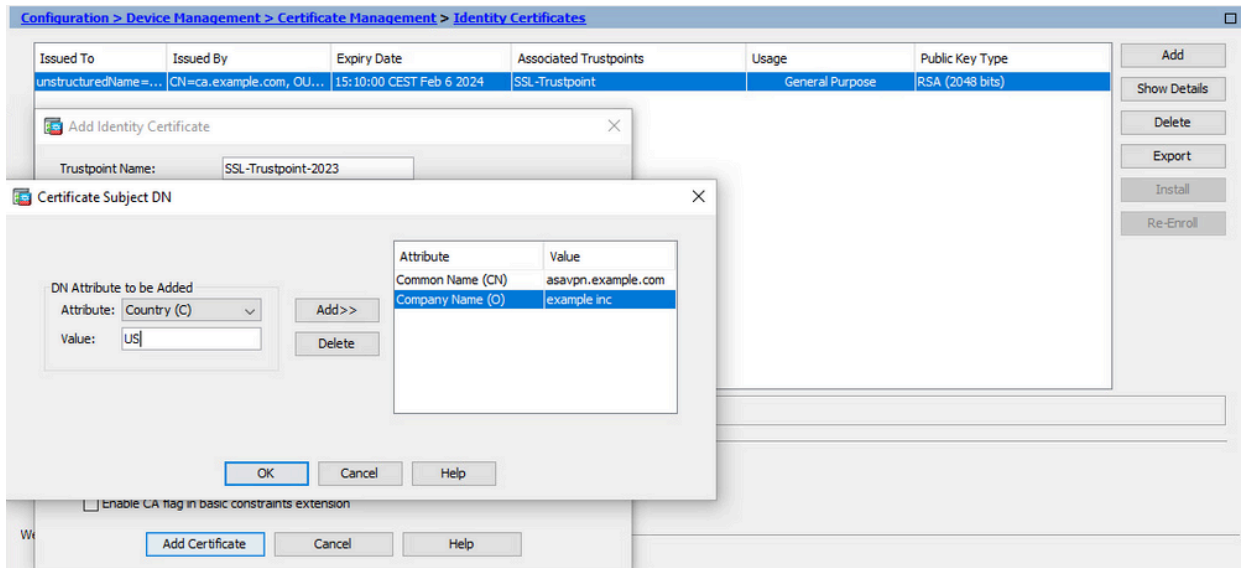
⚠️ Precaución: el parámetro FQDN debe coincidir con el FQDN o la dirección IP de la interfaz ASA para la que se utiliza el certificado. Este parámetro establece el nombre alternativo del sujeto (SAN) para el certificado. El campo SAN es utilizado por el cliente SSL/TLS/IKEv2 para verificar si el certificado coincide con el FQDN al que se conecta.

✍️ Nota: CA puede modificar los parámetros FQDN y nombre de sujeto definidos en el punto de confianza cuando firma el CSR y crea un certificado de identidad firmado.


a. Haga clic en Seleccionar.



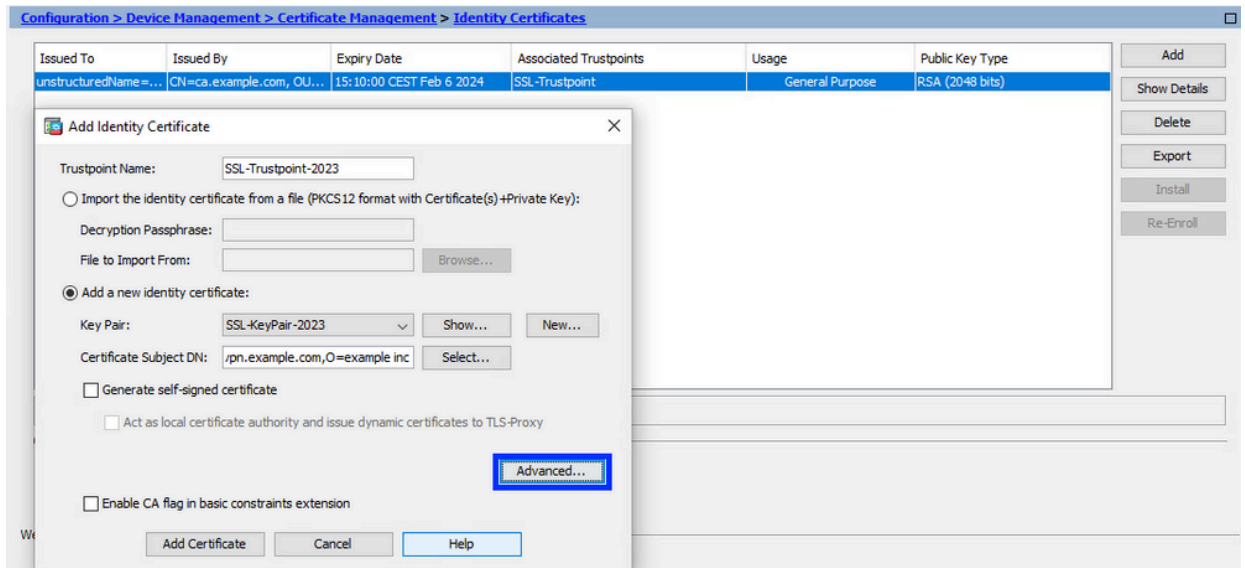
b. En la ventana Certificate Subject DN, configure certificate attributes - select attribute from drop-down list, ingrese el valor, haga clic en Add.



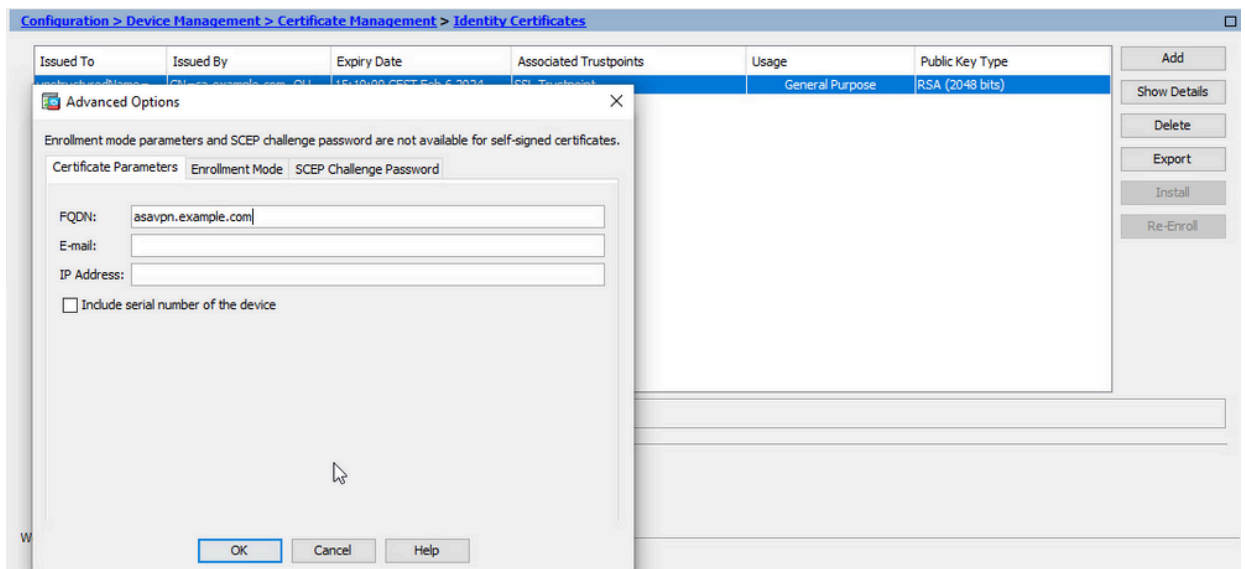
Atributo	Descripción
CN	El nombre a través del cual se puede acceder al firewall (normalmente el nombre de dominio completo, por ejemplo, vpn.example.com).
OU	El nombre de su departamento dentro de la organización
O	El nombre registrado legalmente de su organización/empresa
C	Código de país (código de 2 letras sin puntuación)
ST	El estado en el que se encuentra la organización.
L	La ciudad en la que se encuentra su organización.
EA	Dirección de correo

 Nota: ninguno de los campos anteriores puede superar un límite de 64 caracteres. Un valor mayor podría causar problemas con la instalación del certificado de identidad. Además, no es necesario definir todos los atributos DN.

- Haga clic en Aceptar después de agregar todos los atributos.
- c. Para configurar el FQDN del dispositivo, haga clic en Advanced.

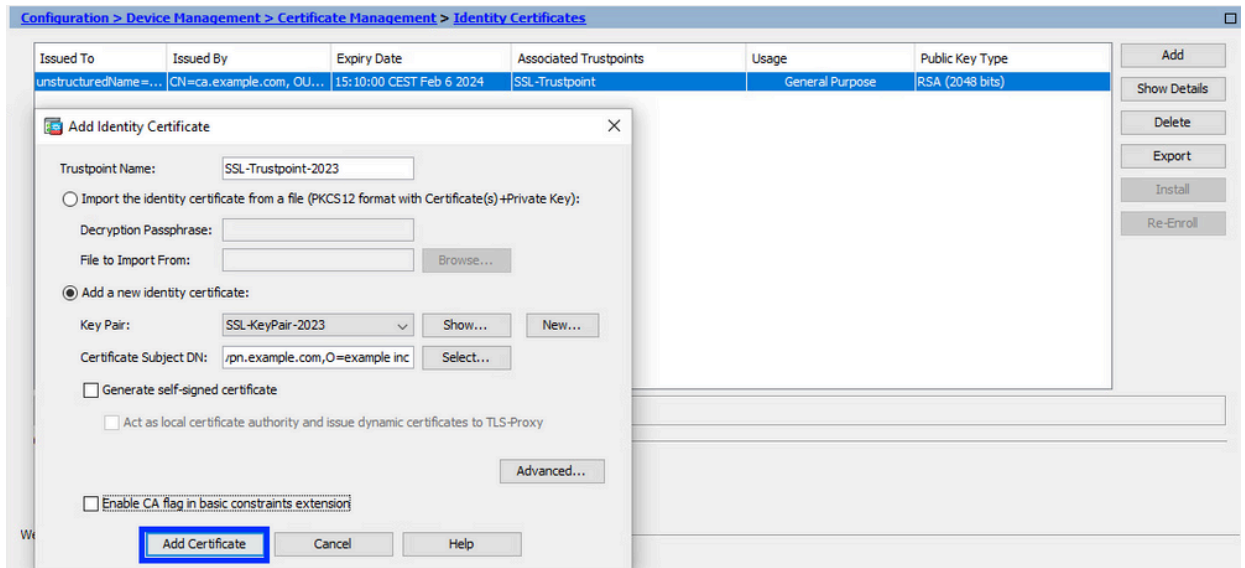


- d. En el campo FQDN, introduzca el nombre de dominio completo a través del cual se puede acceder al dispositivo desde Internet. Click OK.

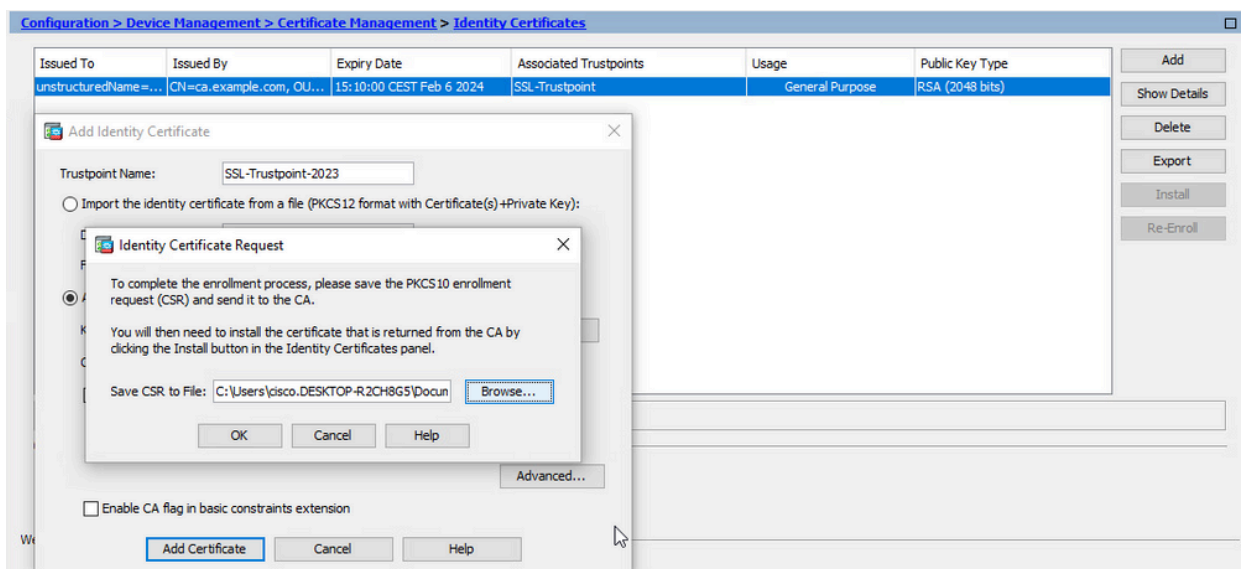


5. Generar y guardar el CSR


- a. Haga clic en Agregar certificado.



b. Se muestra un mensaje para guardar el CSR en un archivo en la máquina local.



Haga clic en Examinar. Elija una ubicación en la que guardar el CSR y guarde el archivo con la extensión .txt.

 Nota: Cuando el archivo se guarda con una extensión .txt, la solicitud PKCS#10 se puede abrir y ver con un editor de texto (como el Bloc de notas).

c. Ahora el nuevo punto de confianza se muestra en un estado Pendiente.

Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU=...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[ssavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	

Buttons: Add, Show Details, Delete, Export, Install, Re-Enroll

Instalación del Certificado de Identidad en Formato PEM con ASDM

En los pasos de instalación se supone que la CA firmó el CSR y proporcionó un nuevo paquete de certificados de identidad y certificados de CA codificado por PEM (.pem, .cer, .crt).

1. Instalar el certificado de CA que firmó el CSR

El certificado de CA que firmó el certificado de identidad se puede instalar en el punto de confianza creado para el certificado de identidad. Si el certificado de identidad está firmado por una CA intermedia, este certificado de CA se puede instalar en el punto de confianza del certificado de identidad. Todos los certificados de CA ascendentes de la jerarquía se pueden instalar en puntos de confianza de CA independientes.

- a. Vaya a Configuración > Administración de dispositivos > Administración de certificados > y elija Certificados de CA. Haga clic en Add (Agregar).

Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes
QuoVadis Root CA 2	CN=QuoVadis Root CA 2, ...	19:23:33 CEST Nov 24 2031	_SmartCallHome_ServerCA2	General Purpose	No
IdenTrust Commercial Root...	CN=IdenTrust Commercial ...	19:12:23 CEST Jan 16 2034	_SmartCallHome_ServerCA	General Purpose	No

Buttons: Add, Edit, Show Details, Request CRL, Delete

- b. Ingrese el nombre de Trustpoint y elija Install From File, haga clic en el botón Browse y elija el certificado intermedio. También puede pegar el certificado de CA codificado PEM de un archivo de texto en el campo de texto.

Configuration > Device Management > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
ca.example.com	CN=ca.example.com, OU=...	15:10:00 CEST Feb 6 2030	SSL-Trustpoint	General Purpose	Yes


Install Certificate dialog:

Trustpoint Name:

Install from a file:

Paste certificate in PEM format:

Buttons: Add, Edit, Show Details, Request CRL, Delete

 Nota: instale el certificado intermedio con el mismo nombre de punto de confianza que el nombre de punto de confianza del certificado de identidad, si el



Nota: El certificado de identidad puede tener el campo Emitido por como No disponible y el campo Fecha de vencimiento como Pendiente.

- b. Elija un archivo que contenga el certificado de identidad con codificación PEM recibido de la CA, o abra el certificado con codificación PEM en un editor de texto, y copie y pegue el certificado de identidad proporcionado por la CA en el campo de texto.

The screenshot shows the 'Identity Certificates' configuration page. A table lists existing certificates. The 'Install Identity Certificate' dialog box is open, showing the 'Install from a file' option selected. The dialog has fields for 'Identity Certificate', 'Install Certificate', 'Cancel', and 'Help' buttons.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)
[asavpn.example.com]	Not Available	Pending...	SSL-Trustpoint-2023	Unknown	



Nota: el certificado de identidad puede tener el formato .pem, .cer o .crt para su instalación.

- c. Haga clic en Install Certificate.

The screenshot shows the 'Identity Certificates' configuration page with the 'Install Identity Certificate' dialog box open. An 'Information' dialog box is displayed over it, stating 'Certificate import succeeded.' There are also 'Please wait...' dialog boxes visible in the background.

Después de la instalación, hay certificados de identidad nuevos y antiguos presentes.

The screenshot shows the 'Identity Certificates' configuration page after installation. The table now contains two certificates, one with an expiry date of April 6, 2024, and another with an expiry date of February 6, 2024.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
unstructuredName=...	CN=ca.example.com, OU...	16:10:00 CEDT Apr 6 2024	SSL-Trustpoint-2023	General Purpose	RSA (4096 bits)
unstructuredName=...	CN=ca.example.com, OU...	15:10:00 CEST Feb 6 2024	SSL-Trustpoint	General Purpose	RSA (2048 bits)

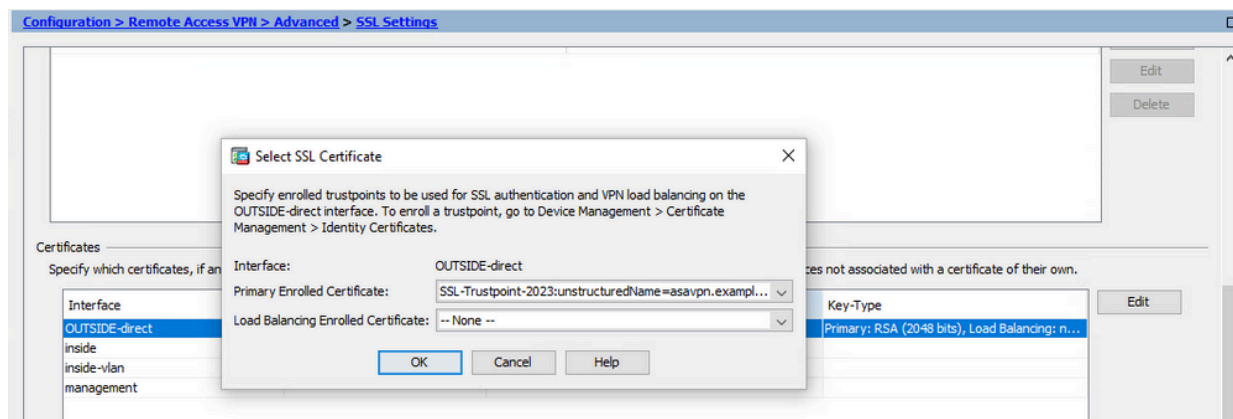
3. Enlace del Nuevo Certificado a la Interfaz con ASDM

El ASA debe configurarse para utilizar el nuevo certificado de identidad para las sesiones WebVPN que terminan en la interfaz especificada.

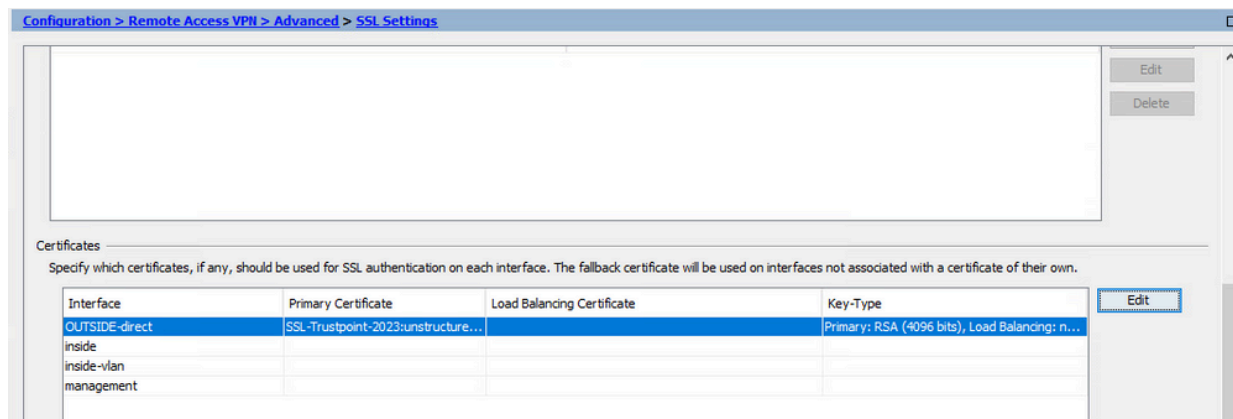
- a. Vaya a Configuration > Remote Access VPN > Advanced > SSL Settings.
- b. En Certificados, elija la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.

Haga clic en Editar.

- c. En la lista desplegable Certificado, elija el certificado recién instalado.



- d. Click OK.
- e. Haga clic en Apply (Aplicar). Ahora el nuevo certificado de identidad está en uso.



Renovación de un Certificado Inscrito con el Archivo PKCS12 con ASDM

La renovación del certificado PKCS12 inscrito requiere crear e inscribir un nuevo punto de confianza. Debe tener un nombre diferente (por ejemplo, nombre antiguo con sufijo de año de inscripción).

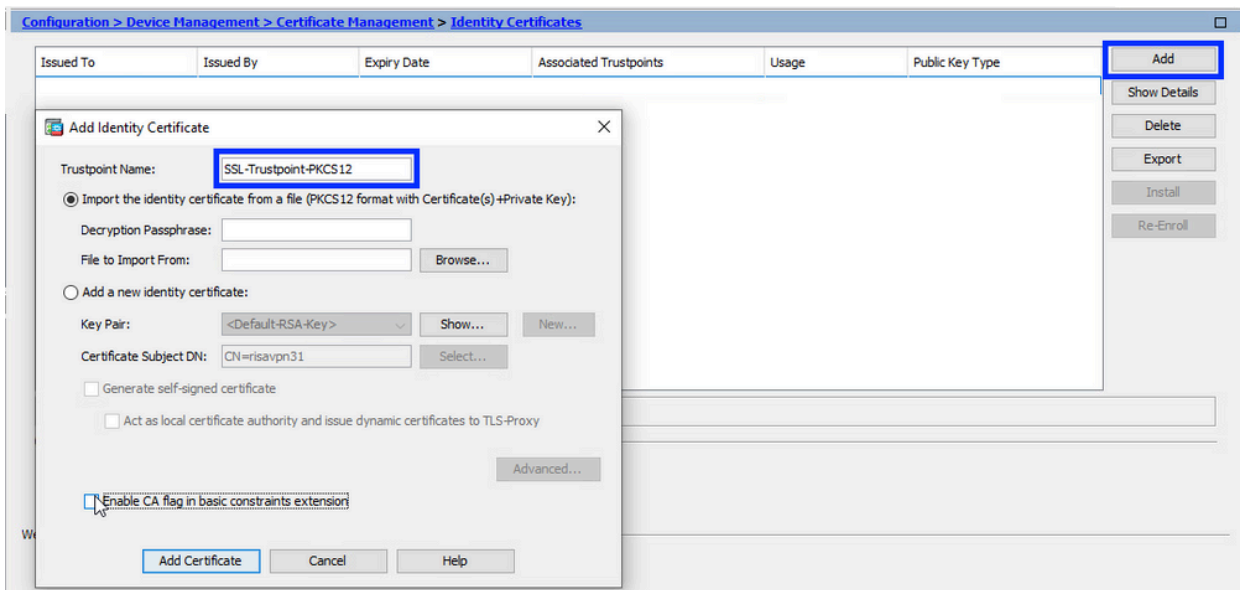
El archivo PKCS12 (formato .p12 o .pfx) contiene el certificado de identidad, el par de claves y los certificados de CA. Es creado por la CA, por ejemplo, en el caso de un certificado comodín, o exportado desde un dispositivo diferente. Es un archivo binario y no se puede ver con el editor de

texto.

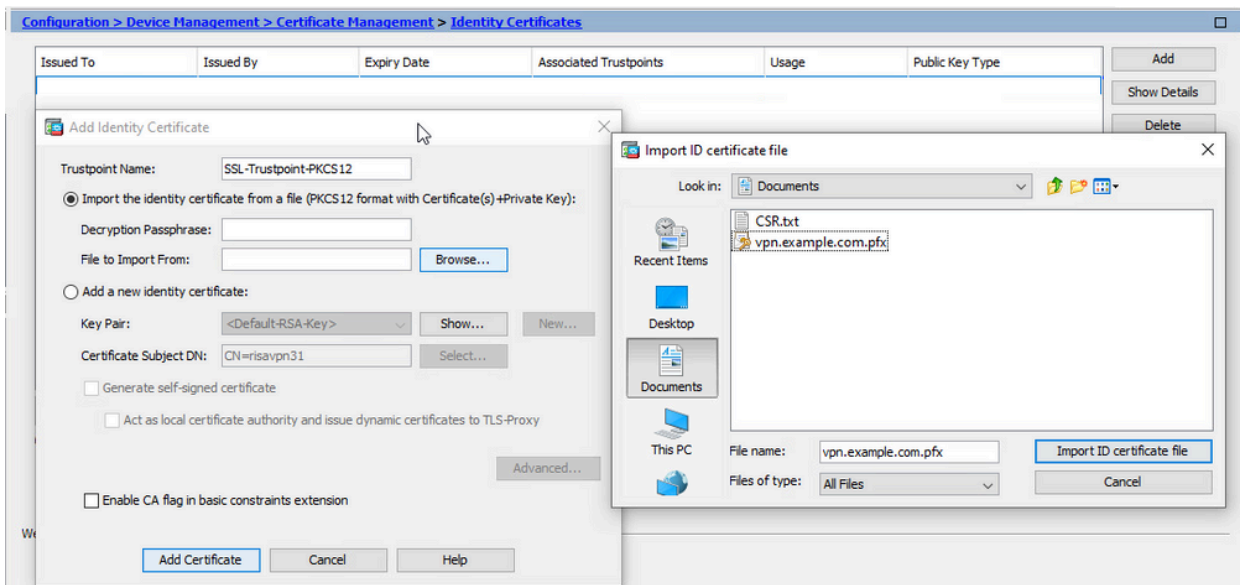
1. Instalación del certificado de identidad renovado y los certificados de CA desde un archivo PKCS12

El certificado de identidad, los certificados de CA y el par de claves deben incluirse en un único archivo PKCS12.

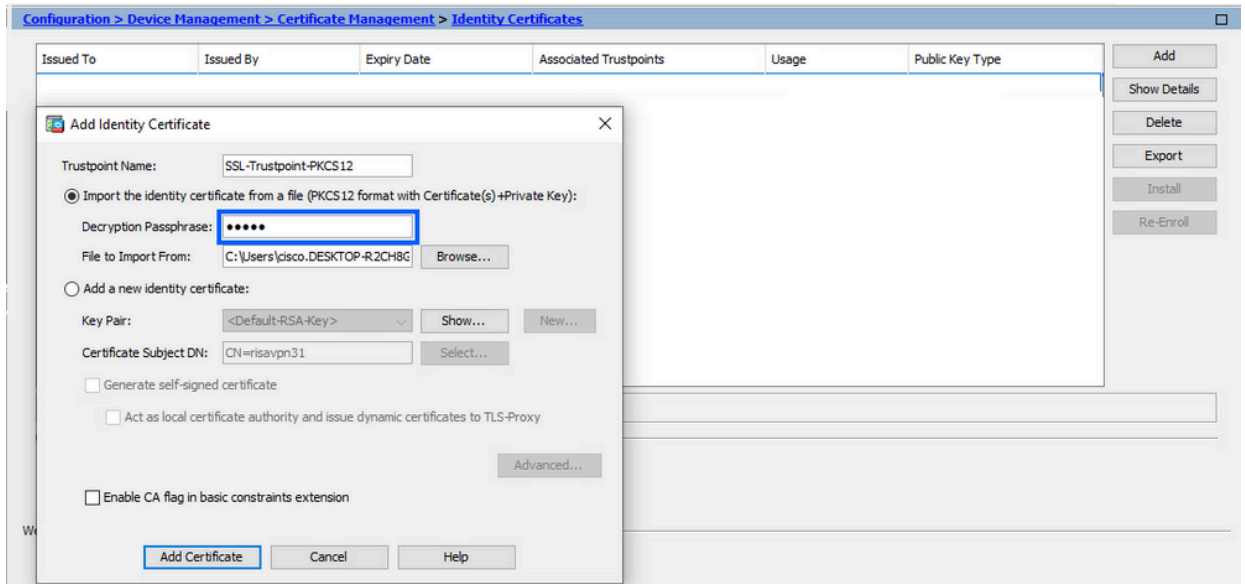
- Navegue hasta Configuration > Device Management > Certificate Management, y elija Identity Certificates.
- Haga clic en Add (Agregar).
- Especifique un nuevo nombre de Trustpoint.



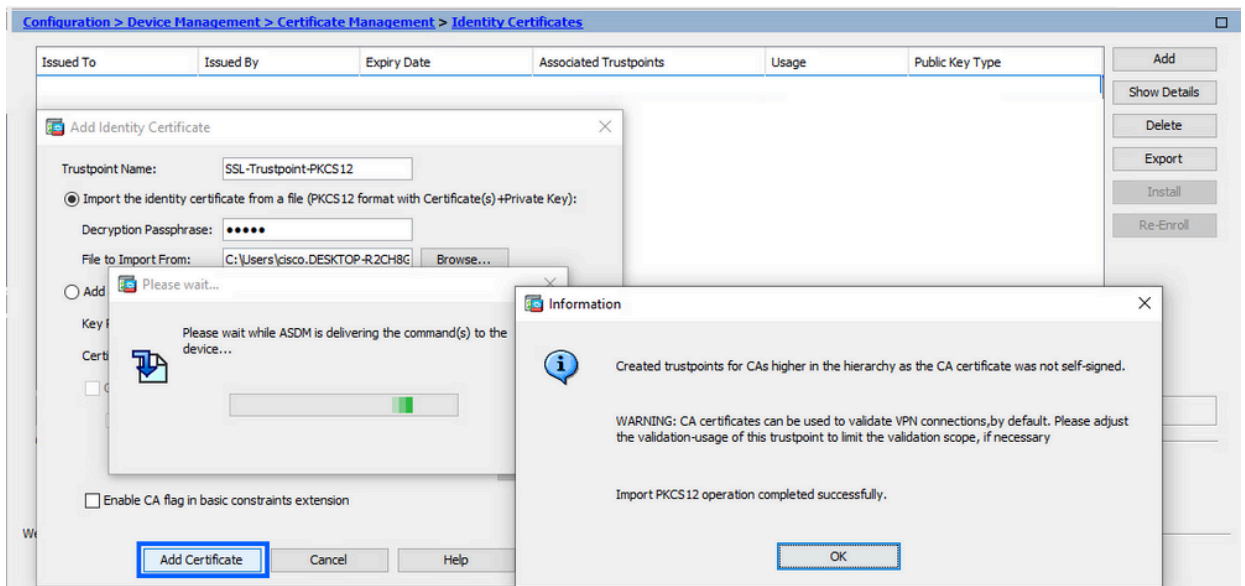
- Haga clic en el botón de opción Import The Identity Certificate from a File .




- Introduzca la frase de paso utilizada para crear el archivo PKCS12.



f. Haga clic en Agregar certificado.



 Nota: Cuando se importa una cadena PKCS12 con certificados de CA, el ASDM crea los puntos de confianza de CA ascendentes automáticamente con nombres con el sufijo -numero agregado.

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub 1-1	CN=KrakowCA-sub 1	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12	Signature	Yes
KrakowCA-sub 1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS 12-2	Signature	Yes

2. Enlace del Nuevo Certificado a la Interfaz con ASDM

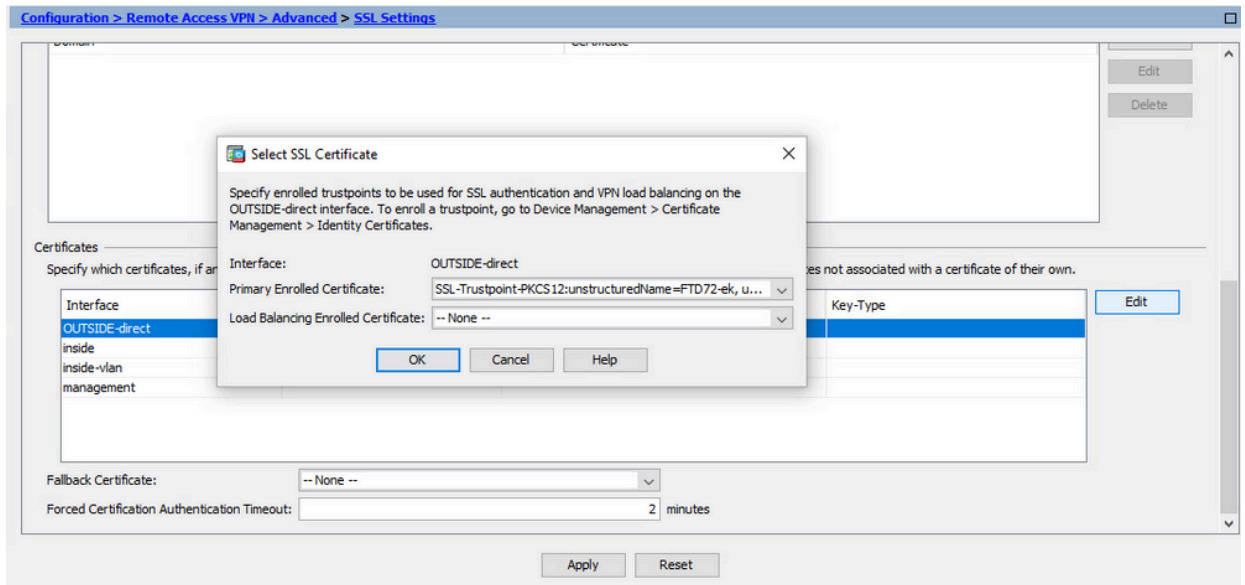
El ASA debe configurarse para utilizar el nuevo certificado de identidad para las sesiones WebVPN que terminan en la interfaz especificada.

a. Vaya a Configuration > Remote Access VPN > Advanced > SSL Settings.

b. En Certificados, elija la interfaz que se utiliza para terminar las sesiones WebVPN. En este ejemplo, se utiliza la interfaz externa.

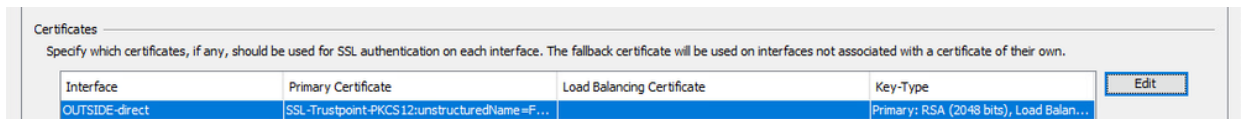
Haga clic en Editar.

c. En la lista desplegable Certificado, seleccione el certificado recién instalado.



d. Click OK.

e. Haga clic en Apply (Aplicar).



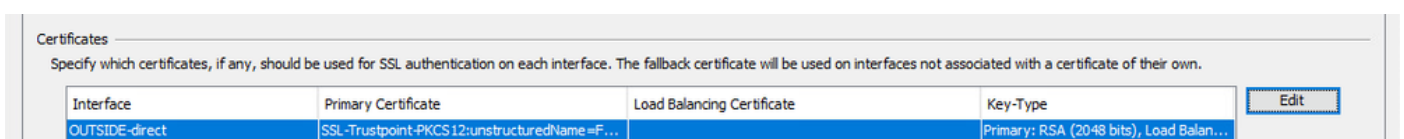
Ahora el nuevo certificado de identidad está en uso.

Verificación

Siga estos pasos para verificar la correcta instalación del certificado de proveedor de terceros y su uso para conexiones VPN SSL.

Ver certificados instalados mediante ASDM

1. Navegue hasta Configuration > Remote Access VPN > Certificate Management, y elija Identity Certificates.
2. Puede aparecer el certificado de identidad emitido por el proveedor externo.



Troubleshoot

Este comando de depuración se debe recolectar en la CLI en caso de una falla en la Instalación del Certificado SSL.

- debug crypto ca 14

Preguntas Frecuentes

P. ¿Qué es un PKCS12?

R. En criptografía, PKCS12 define un formato de archivo de almacenamiento creado para almacenar muchos objetos criptográficos como un único archivo. Se suele utilizar para agrupar una clave privada con su certificado X.509 o para agrupar todos los miembros de una cadena de confianza.

P. ¿Qué es una CSR?

R. En los sistemas de infraestructura de clave pública (PKI), una solicitud de firma de certificado (también CSR o solicitud de certificación) es un mensaje enviado por un solicitante a una autoridad de registro de la infraestructura de clave pública para solicitar un Certificado de identidad digital. Normalmente contiene la clave pública para la que se puede emitir el certificado, información que se utiliza para identificar el certificado firmado (como un nombre de dominio en Asunto) y protección de la integridad (por ejemplo, una firma digital).

P. ¿Dónde está la contraseña del PKCS12?

A. Cuando los certificados y los pares de claves se exportan a un archivo PKCS12, la contraseña se proporciona en el comando export. Para importar un archivo pkcs12, el propietario del servidor de la CA o la persona que exportó el PKCS12 desde otro dispositivo debe proporcionar la contraseña.

P. ¿Cuál es la diferencia entre la raíz y la identidad?

R. En criptografía y seguridad del equipo, un certificado raíz es un certificado de clave pública que identifica una entidad emisora de certificados (CA) raíz. Los certificados raíz son autofirmados (y es posible que un certificado tenga varias rutas de confianza, por ejemplo, si el certificado fue emitido por una raíz que tenía una firma cruzada) y constituyen la base de una infraestructura de clave pública (PKI) basada en X.509. Un certificado de clave pública, también conocido como certificado digital o certificado de identidad, es un documento electrónico utilizado para probar la propiedad de una clave pública. El certificado incluye información sobre la clave, información sobre la identidad de su propietario (denominado el sujeto) y la firma digital de una entidad que ha verificado el contenido del certificado (denominada el emisor). Si la firma es válida y el software que examina el certificado confía en el emisor, puede utilizar esa clave para comunicarse de forma segura con el sujeto del certificado.

P. Instalé el certificado, ¿por qué no funciona?

R. Esto podría deberse a muchas razones, por ejemplo:

1. El certificado y el punto de confianza están configurados, pero no se han enlazado al proceso

que los utiliza. Por ejemplo, el punto de confianza que se va a utilizar no está enlazado a la interfaz externa que termina con los clientes de Anyconnect.

2. Hay instalado un archivo PKCS12, pero se producen errores debido a que falta el certificado de CA intermedio en el archivo PKCS12. Los clientes que tienen el certificado de la CA intermedia como de confianza, pero no tienen el certificado de la CA raíz como de confianza, no pueden verificar toda la cadena de certificados y notificar que el certificado de identidad del servidor no es de confianza.

3. Un certificado con atributos incorrectos puede provocar un error en la instalación o errores en el cliente. Por ejemplo, algunos atributos se codifican con un formato incorrecto. Otro motivo es que falta el nombre alternativo del sujeto (SAN) en el certificado de identidad o el nombre de dominio utilizado para acceder al servidor no está presente como SAN.

P. ¿La instalación de un nuevo certificado requiere un período de mantenimiento o provoca tiempo de inactividad?

R. La instalación de un nuevo certificado (identidad o CA) no es intrusiva y no causa tiempo de inactividad ni requiere una ventana de mantenimiento. Habilitar el uso de un nuevo certificado para un servicio existente es un cambio y requiere una ventana de solicitud de cambio/mantenimiento.

P. ¿Añadir o cambiar un certificado puede desconectar a los usuarios conectados?

R.No, los usuarios conectados actualmente permanecen conectados. El certificado se utiliza en el establecimiento de conexión. Una vez que los usuarios se vuelven a conectar, se utiliza el nuevo certificado.

P. ¿Cómo puedo crear un CSR con un comodín? ¿O un nombre alternativo del sujeto (SAN)?

R.Actualmente, el ASA/FTD no puede crear un CSR con comodín; sin embargo, este proceso se puede realizar con OpenSSL. Para generar la clave CSR e ID, puede ejecutar los comandos:

```
openssl genrsa -out id.key 2048
```

```
openssl req -out id.csr -key id.key -new
```

Cuando un punto de confianza se configura con el atributo de nombre de dominio completo (FQDN), la CSR creada por ASA/FTD contiene la SAN con ese valor. La CA puede agregar más atributos SAN cuando firma el CSR, o bien el CSR puede crearse con OpenSSL

P. ¿La sustitución de certificados tiene efecto inmediatamente?

R. El nuevo certificado de identidad del servidor se utiliza solamente para las nuevas conexiones. El nuevo certificado está listo para usarse inmediatamente después del cambio, pero en realidad se usa con nuevas conexiones.

P. ¿Cómo puedo comprobar si la instalación ha funcionado?

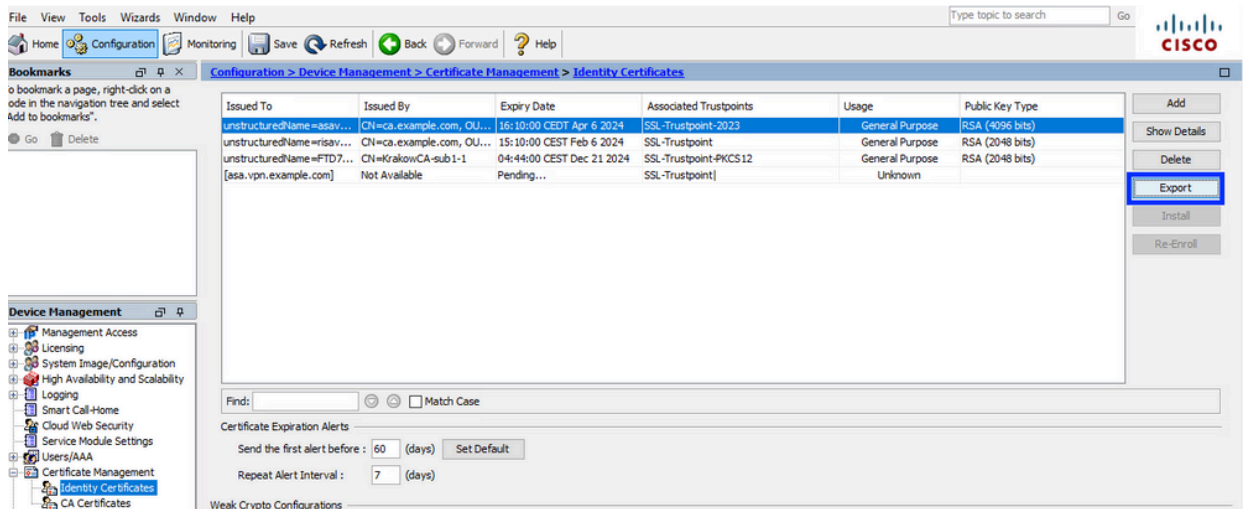
A.El comando CLI para verificar: show crypto ca cert <trustpointname>

P. ¿Cómo generar PKCS12 a partir del certificado de identidad, el certificado de CA y la clave privada?

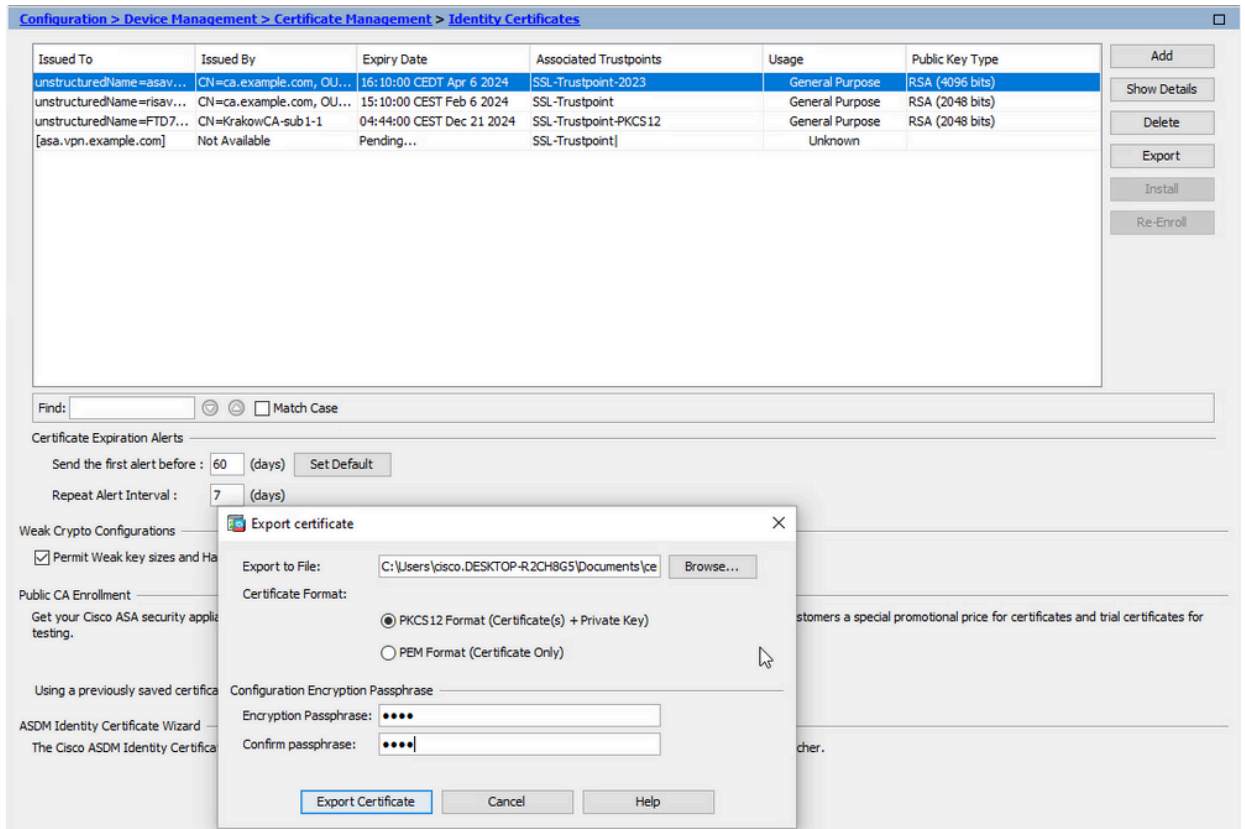
A. PKCS12 se puede crear con OpenSSL, con el comando:
openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

P. ¿Cómo exportar un certificado para instalarlo en un nuevo ASA?

- A.
- Con CLI: utilice el comando: crypto ca export <trustpointname> pkcs12 <password>
 - Con ASDM:
 - a. Navegue hasta Configuration > Device Management > Certificate Management > Identity Certificates y elija el Identity Certificate. Haga clic en Exportar.



b. Elija dónde exportar el archivo, especifique la contraseña de exportación y haga clic en Exportar certificado.



El certificado exportado puede estar en el disco del equipo. Tome nota de la frase de paso en un lugar seguro, el archivo es inútil sin él.

P. Si se utilizan claves ECDSA, ¿es diferente el proceso de generación de certificados SSL?
 A. La única diferencia en la configuración es el paso de generación de par de claves, donde se puede generar un par de claves ECDSA en lugar de un par de claves RSA. El resto de los pasos siguen siendo los mismos.

P. ¿Siempre es necesario generar un nuevo par de claves?
 R. El paso de generación del par de claves es opcional. Se puede utilizar un par de claves existente o, en el caso de PKCS12, el par de claves se importa con el certificado. Consulte la sección Select the Key Pair Name (Seleccione el nombre del par de claves) para ver el tipo de inscripción o reinscripción correspondiente.

P. ¿Es seguro generar un nuevo par de claves para un nuevo certificado de identidad?
 R. El proceso es seguro siempre que se utilice un nuevo nombre de par de claves. En tal caso, los pares de claves antiguos no se cambian.

P. ¿Es necesario volver a generar la clave cuando se sustituye un firewall (como RMA)?
 R. El nuevo firewall por diseño no tiene pares de claves presentes en el firewall antiguo. La copia de seguridad de la configuración en ejecución no contiene los pares de claves. La copia de seguridad completa realizada con ASDM puede contener los pares de claves. Los certificados de identidad se pueden exportar desde un ASA con ASDM o CLI antes de que

falle.

En el caso de un par de failover, los certificados y los pares de claves se sincronizan con una unidad standby con el comando `write standby`. En caso de que se reemplace un nodo de par de failover, es suficiente configurar el failover básico e insertar la configuración en el nuevo dispositivo.

En caso de que se pierda un par de claves con el dispositivo y no haya una copia de seguridad, se debe firmar un nuevo certificado con el par de claves presente en el nuevo dispositivo.

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).