Instalar e renovar certificados no ASA gerenciado pelo ASDM

Contents

Introdução

Este documento descreve como solicitar, instalar, confiar e renovar determinados tipos de certificados no software Cisco ASA gerenciado com o ASDM.

Pré-requisitos

Requisitos

- Antes de começar, verifique se o Adaptive Security Appliance (ASA) tem a hora, a data e o fuso horário corretos. Com a autenticação de certificado, é recomendável usar um servidor Network Time Protocol (NTP) para sincronizar a hora no ASA. Consulte Informações Relacionadas para referência.
- Para solicitar um certificado que use a CSR (Certificate Signing Request, Solicitação de assinatura de certificado), é necessário ter acesso a uma CA (Certificate Authority, Autoridade de certificação) de terceiros ou interna confiável. Exemplos de fornecedores de CA de terceiros incluem, entre outros, Entrust, Geotrust, GoDaddy, Thawte e VeriSign.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASAv 9.18.1
- Para a criação de PKCS12, o OpenSSL é usado.

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.

Informações de Apoio

Os tipos de certificados que este documento aborda são:

- certificados autoassinados
- certificados assinados por uma autoridade de certificação de terceiros ou CA interna

O protocolo SSL (Secure Socket Layer), o protocolo TLS (Transport Layer Security) e o protocolo IKEv2 rfc7296 para autenticação EAP exigem que o servidor SSL/TLS/IKEv2 forneça ao cliente um certificado de servidor para que ele execute a autenticação do servidor. Para essa finalidade, é recomendável usar CAs de terceiros confiáveis para emitir certificados SSL para o ASA.

A Cisco não recomenda o uso de um certificado autoassinado, devido à possibilidade de um usuário configurar inadvertidamente um navegador para confiar em um certificado de um servidor invasor. Também há a inconveniência de os usuários responderem a um aviso de segurança quando ele se conectar ao gateway seguro.

Solicitar e Instalar um novo Certificado de Identidade com o ASDM

Um certificado pode ser solicitado de uma Autoridade de Certificação (CA) e instalado em um ASA de duas maneiras:

- Use a CSR (Certificate Signing Request, Solicitação de assinatura de certificado). Gere um par de chaves, solicite um certificado de identidade da CA com um CSR, instale o certificado de identidade assinado obtido da CA.
- Use o arquivo PKCS12 obtido de uma CA ou exportado de um dispositivo diferente. O arquivo PKCS12 contém par de chaves, certificado de identidade, certificado(s) CA.

Solicitar e instalar um novo certificado de identidade com CSR (Certificate Signing Request, Solicitação de assinatura de certificado)

Um CSR é criado no dispositivo que precisa de um certificado de identidade, use um par de chaves criado no dispositivo.

Um CSR contém:

- informações de solicitação de certificado - assunto solicitado e outros atributos, chave pública do par de chaves,
- informação de algoritmo de assinatura,
- assinatura digital de informações de solicitação de certificado, assinada com a chave privada do par de chaves.

O CSR é passado para a Autoridade de Certificação (CA), para que assine, em um formulário PKCS#10.

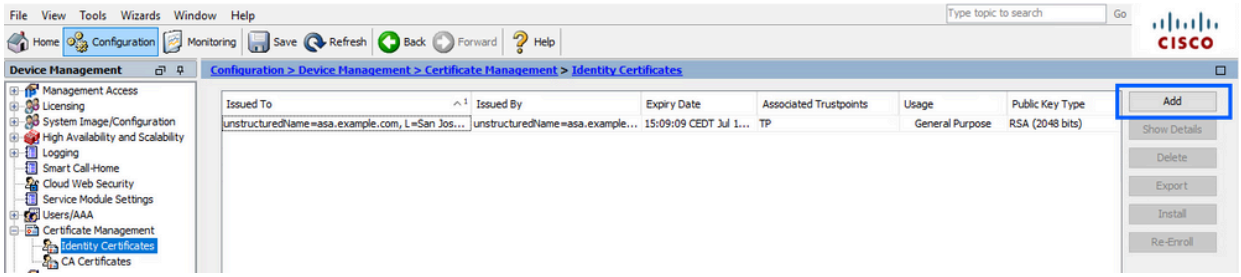
O certificado assinado é retornado da CA em um formulário PEM.

> Observação: a CA pode alterar os parâmetros FQDN e Nome do assunto definidos no ponto de confiança ao assinar o CSR e criar um Certificado de Identidade assinado.

Gerar um CSR com ASDM

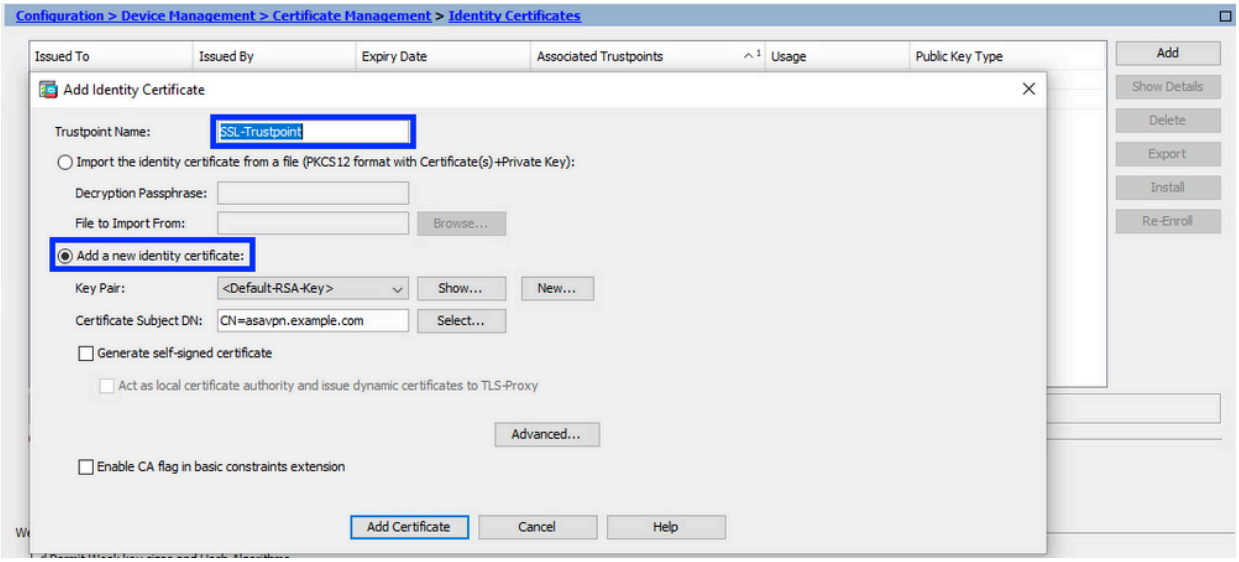
1. Criar um ponto de confiança com um nome específico

a. Navegue até Configuration > Device Management >Certificate Management > Identity Certificates.



b. Clique em Add.

c. Defina um nome de ponto confiável.



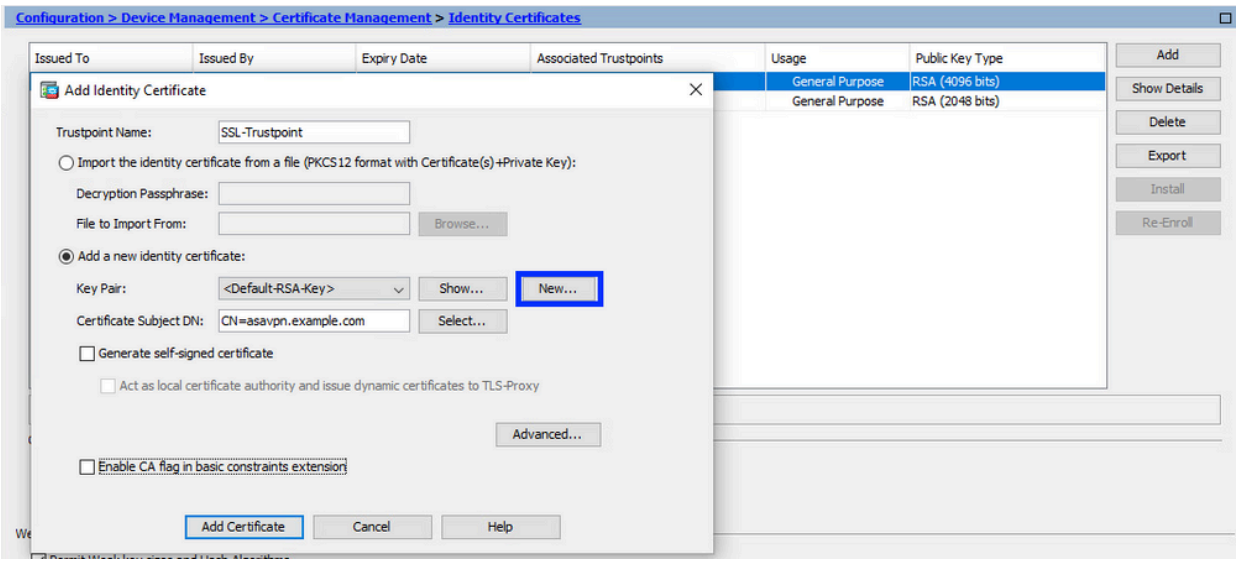
d. Clique no botão de rádio Add a new identity certificate (Adicionar um novo certificado de identidade).

2. (Opcional) Crie um novo par de chaves

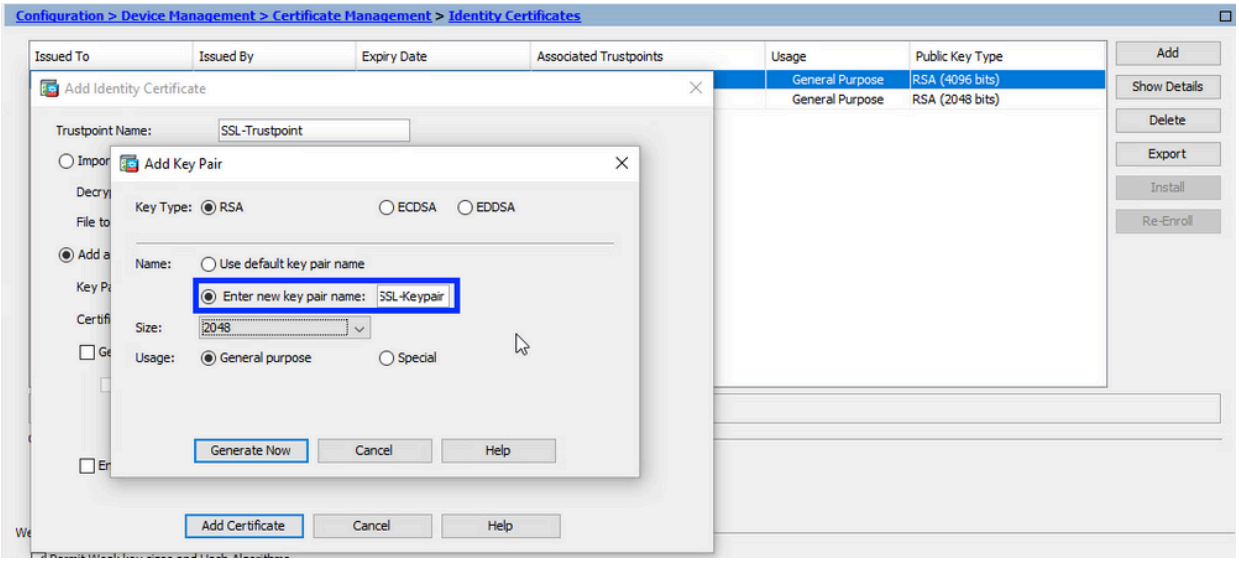
Nota: Por padrão, é usada a chave RSA com o nome Default-RSA-Key e o tamanho 2048; no entanto, recomenda-se usar um par de chaves privado/público exclusivo para cada certificado de identidade.

---

a. Clique em New para gerar um novo par de chaves.

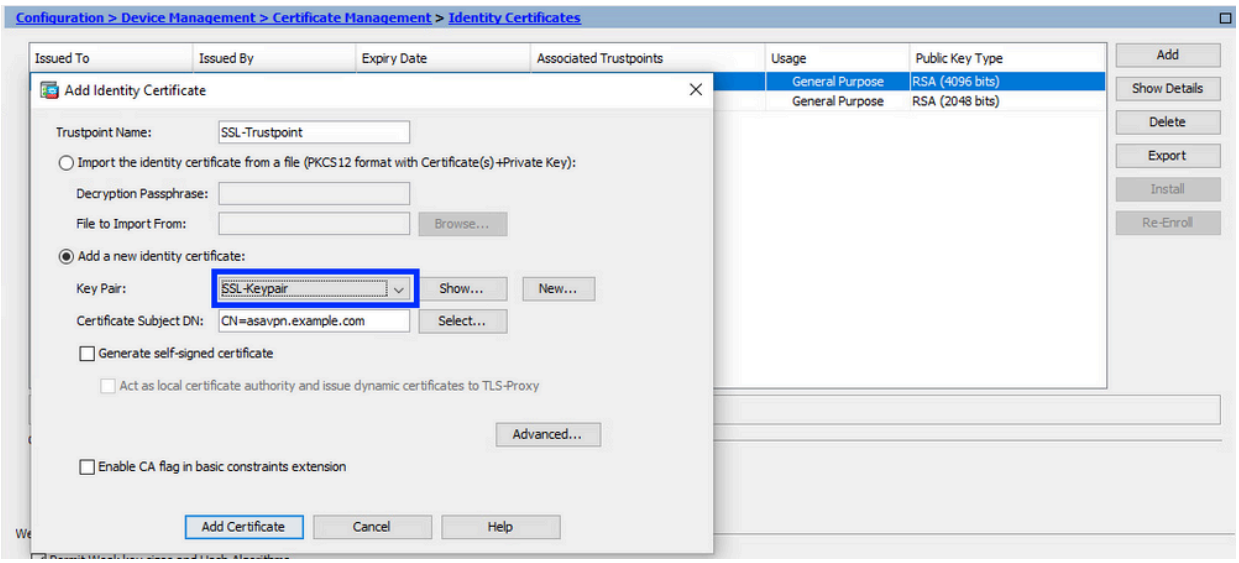


b. Escolha a opção Enter new Key Pair name e insira um nome para o novo par de chaves.
c. Escolha o tipo de chave-RSA ou ECDSA.
d. Escolha o tamanho da chave; para RSA, escolha General purpose for Usage.
e. Clique em Generate CSR (Gerar CSR). O par de chaves foi criado.



3. Escolha o nome do par de chaves

Escolha o par de chaves com o qual assinar o CSR e que será vinculado ao novo certificado.

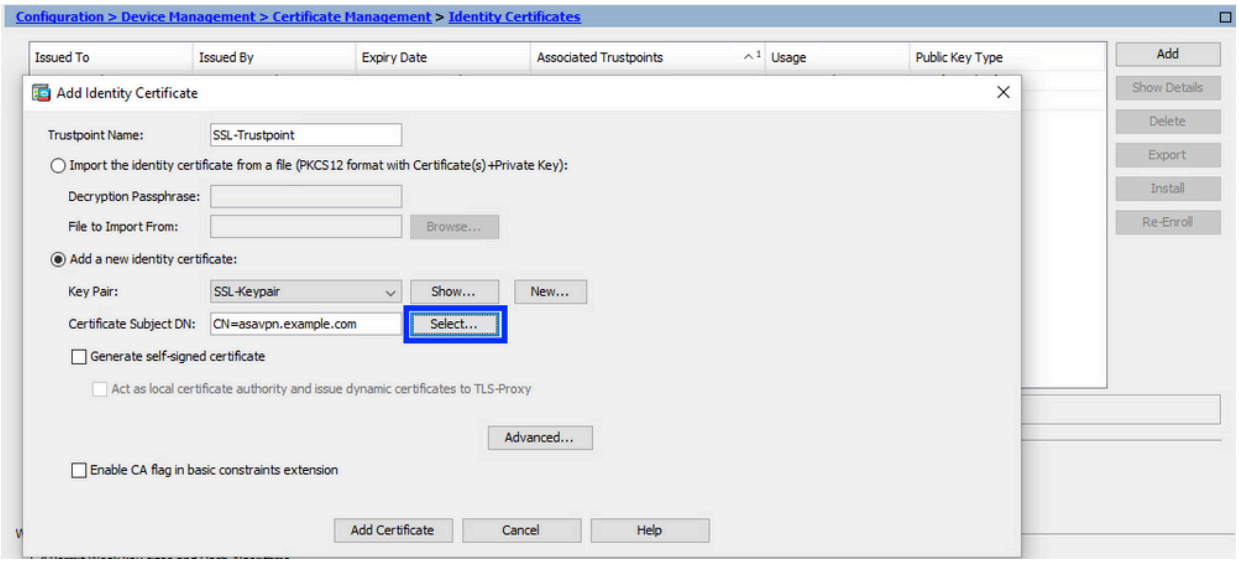


4. Configurar o assunto do certificado e o nome de domínio totalmente qualificado (FQDN)

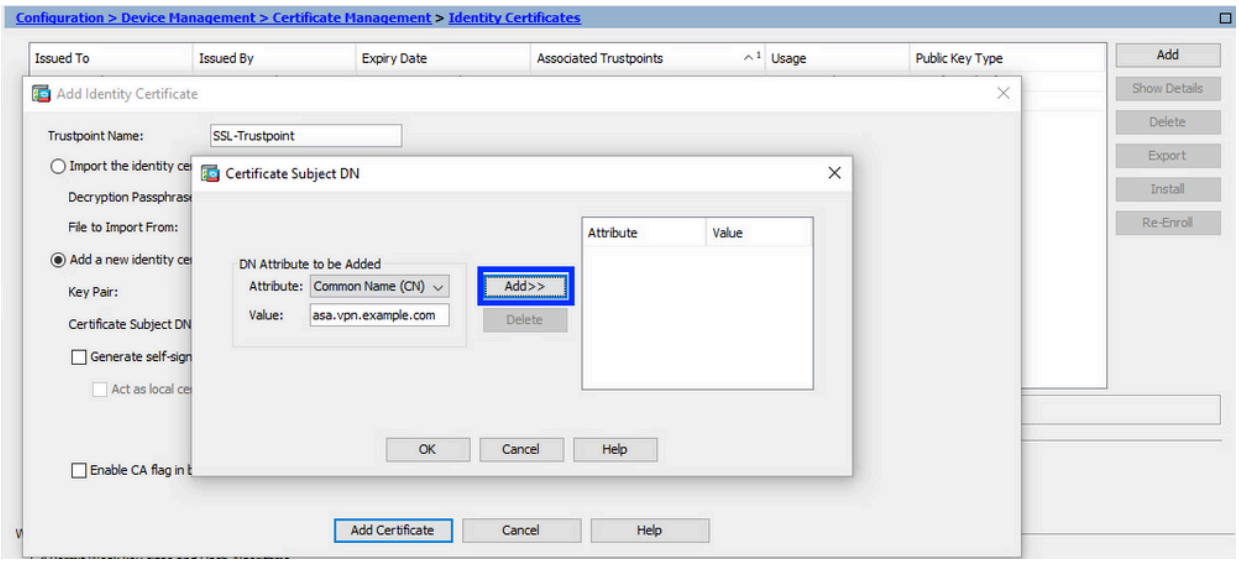
Cuidado: o parâmetro FQDN deve corresponder ao FQDN ou ao endereço IP da interface ASA para a qual o Certificado de Identidade é usado. Este parâmetro define a extensão solicitada do SAN (Nome Alternativo da Entidade) para o Certificado de Identidade. A extensão SAN é usada pelo cliente SSL/TLS/IKEv2 para verificar se o certificado corresponde ao FQDN ao qual ele se conecta.

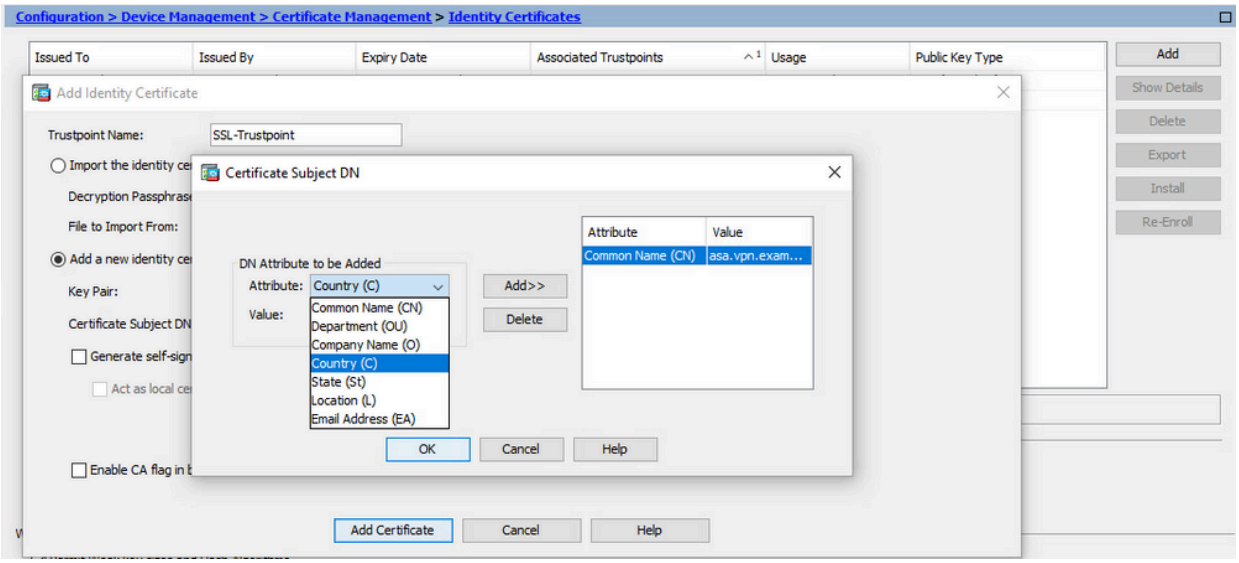
---

a. Clique em Selecionar.



b. Na janela Certificate Subject DN (DN do assunto do certificado), configure certificate attributes - escolha o atributo na lista suspensa, digite o valor e clique em Add.



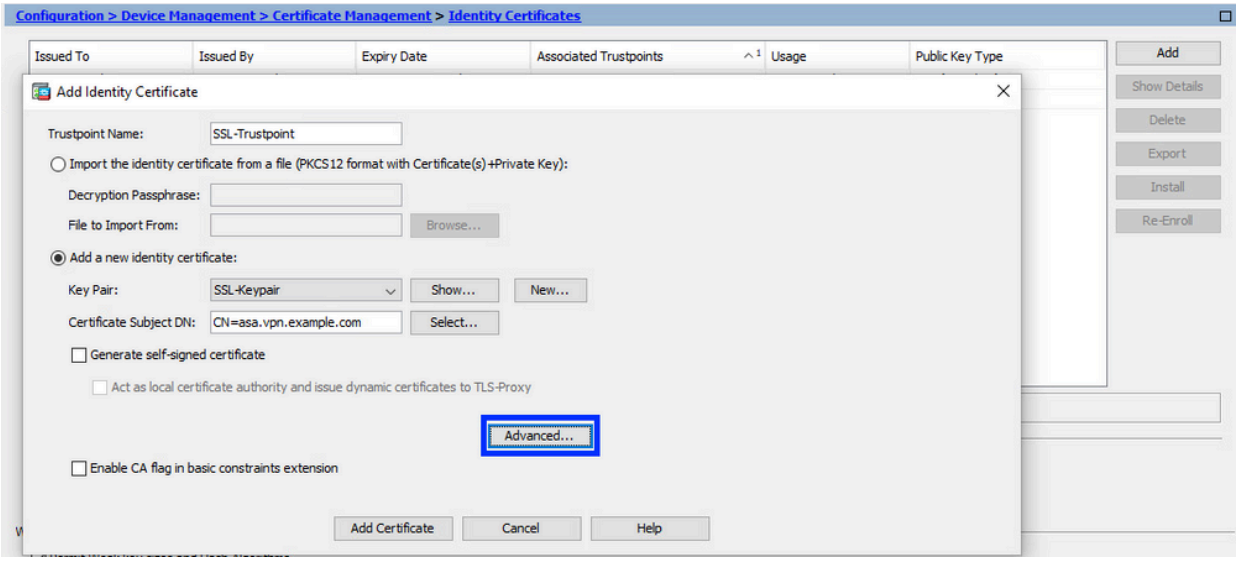


Atributo	Descrição
CN	O nome pelo qual o firewall pode ser acessado (geralmente o nome de domínio totalmente qualificado, por exemplo, vpn.example.com).
OU	O nome do seu departamento na organização
O	O nome legalmente registrado da sua organização/empresa
C	Código do país (código de 2 letras sem pontuação)
ST	O estado no qual sua organização está localizada.
I	A cidade em que sua organização está localizada.
EA	Endereço de e-mail

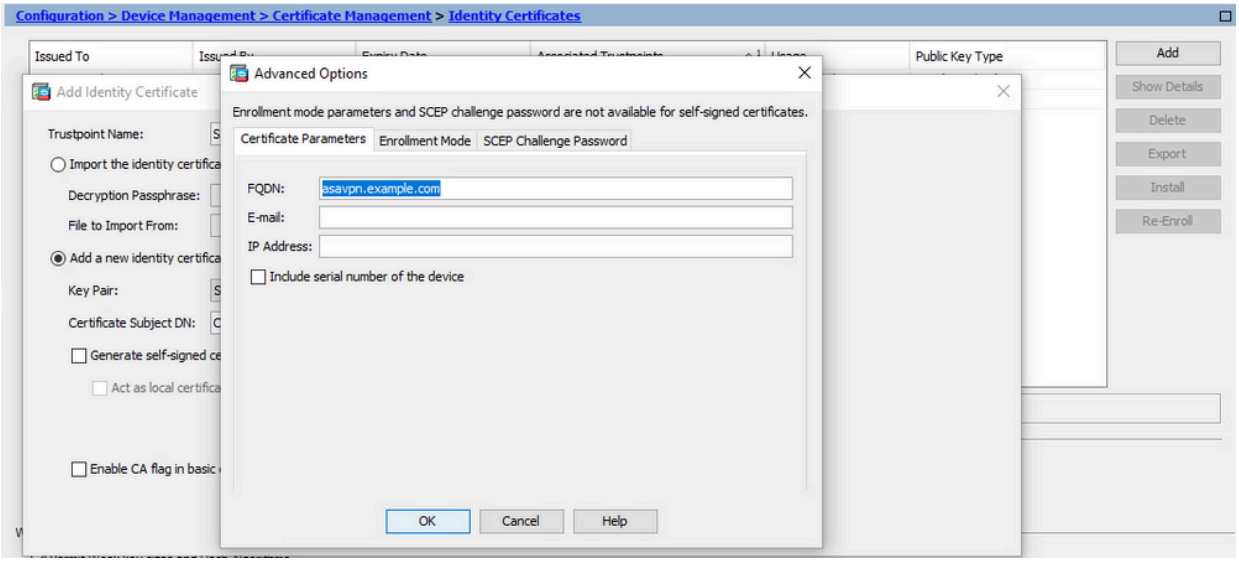
Observação: nenhum dos valores dos campos anteriores pode exceder um limite de 64 caracteres. Um valor mais longo pode causar problemas com a instalação do Certificado de Identidade. Além disso, não é necessário definir todos os atributos DN.

Clique em OK depois que todos os atributos forem adicionados.

c. Configure o FQDN do dispositivo - clique em Avançado.

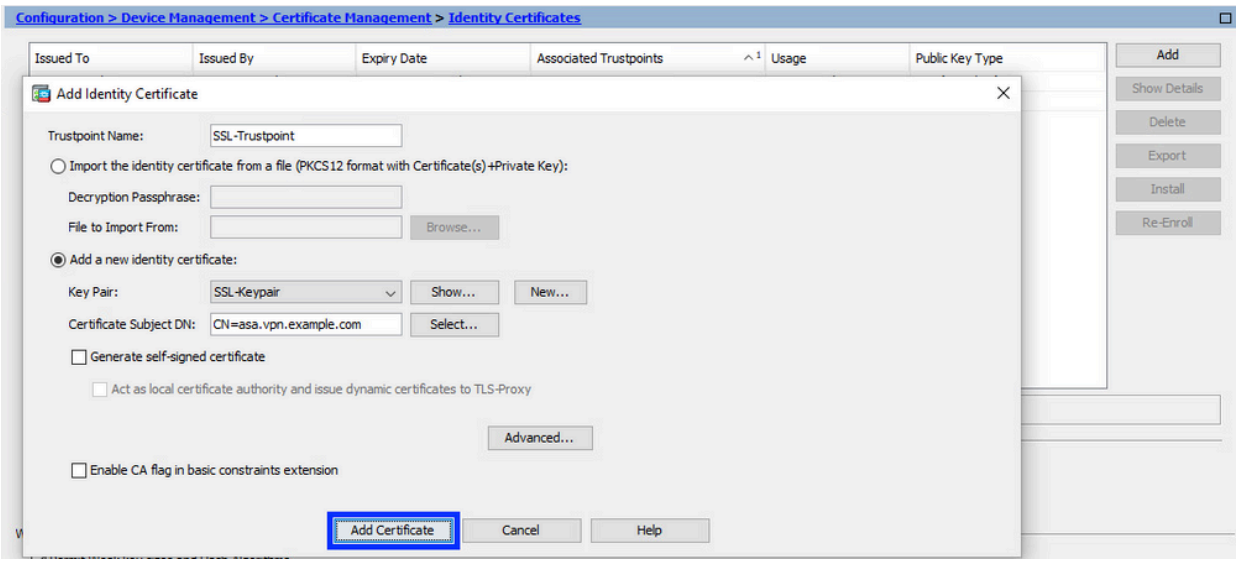


d. No campo FQDN, insira o nome de domínio totalmente qualificado pelo qual o dispositivo pode ser acessado a partir da Internet. Click OK.

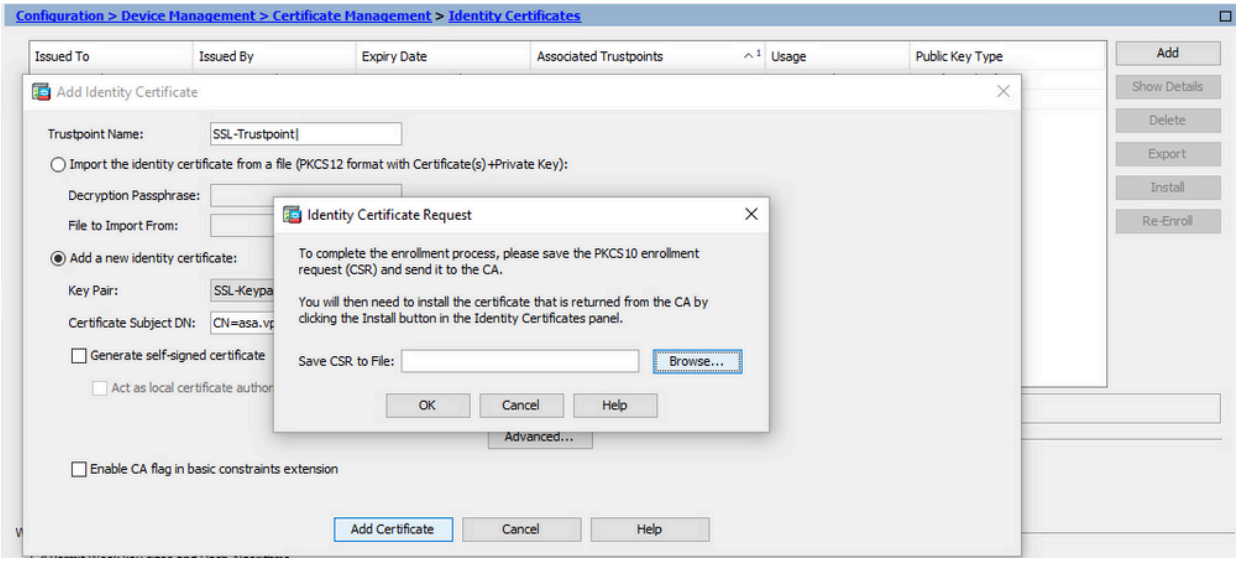


5. Gerar e salvar o CSR

a. Clique em Add Certificate (Adicionar certificado).



b. Um prompt é exibido para salvar o CSR em um arquivo na máquina local.

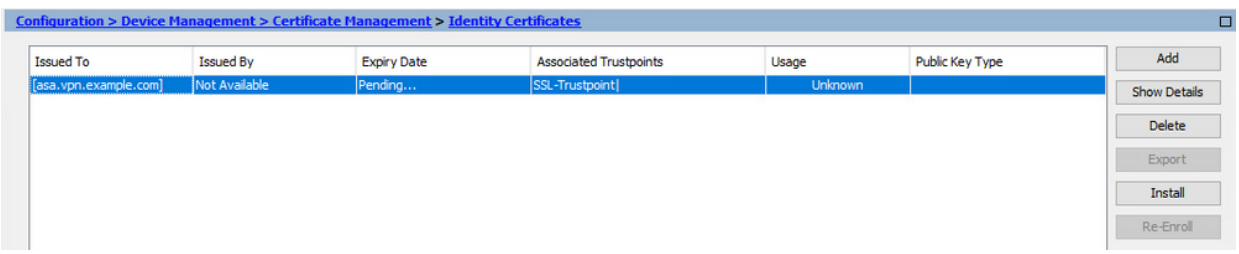


Clique em Browse (Procurar), escolha um local para salvar o CSR e salve o arquivo com a extensão .txt.

> Observação: quando o arquivo é salvo com uma extensão .txt, a solicitação PKCS#10 pode ser aberta e visualizada com um editor de texto (como o Notepad).

---

c. Agora o novo ponto confiável é exibido em um estado Pendente.

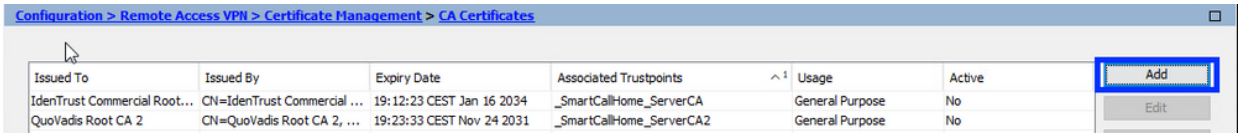


Instalar o Certificado de Identidade no formato PEM com o ASDM

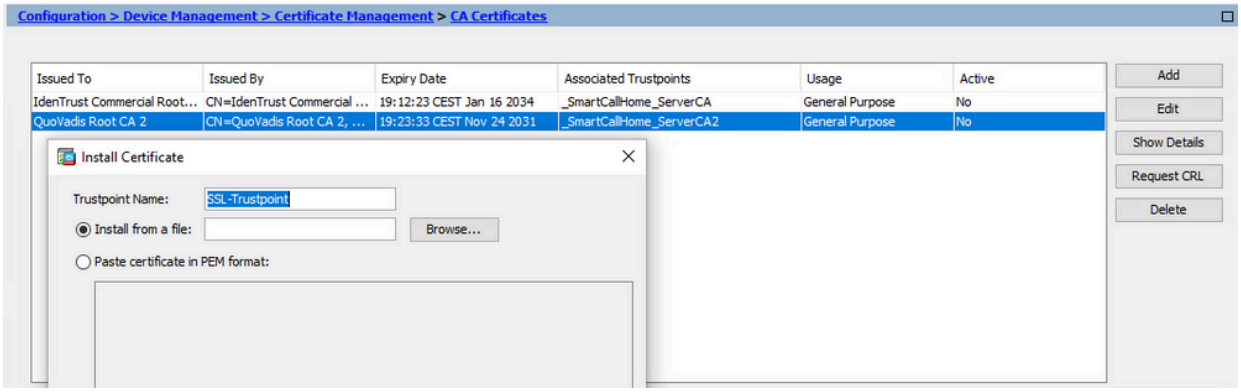
As etapas de instalação pressupõem que a CA assinou o CSR e forneceu um certificado de identidade codificado PEM (.pem, .cer, .crt) e um pacote de certificados CA.

1. Instalar o certificado de autoridade de certificação que assinou o CSR

   a. Navegue até Configuration > Device Management >Certificate Management > e escolha CA Certificates. Clique em Add.



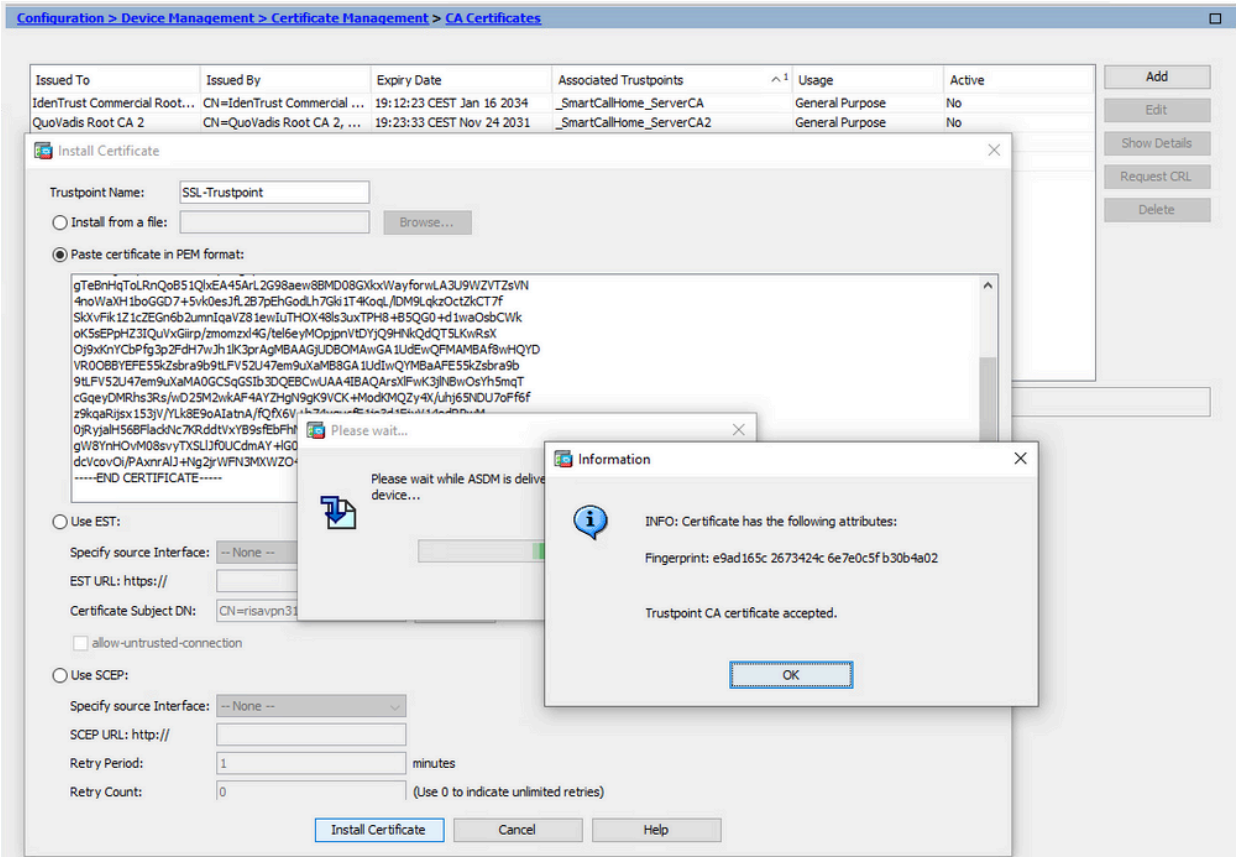
   b. Insira o nome do ponto de confiança e selecione Instalar do arquivo, clique no botão Procurar e selecione o certificado intermediário. Como alternativa, cole o certificado CA codificado PEM de um arquivo de texto no campo de texto.



Observação: instale o certificado CA que assinou o CSR e use o mesmo nome de Ponto de Confiança do Certificado de Identidade. Os outros certificados CA mais altos na hierarquia PKI podem ser instalados em Pontos Confiáveis separados.

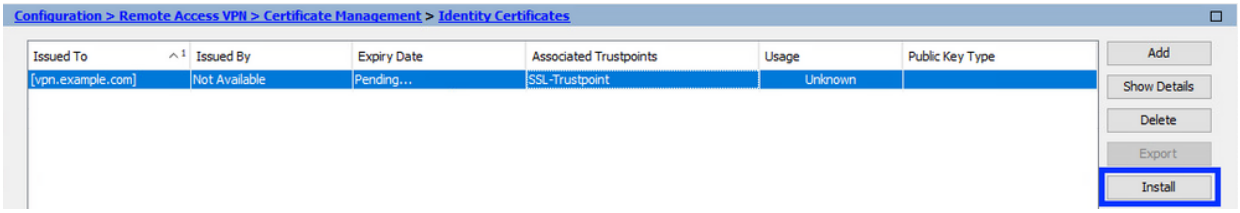
---

   c. Clique em Install certificate (Instalar certificado).



2. Instalar certificado de identidade

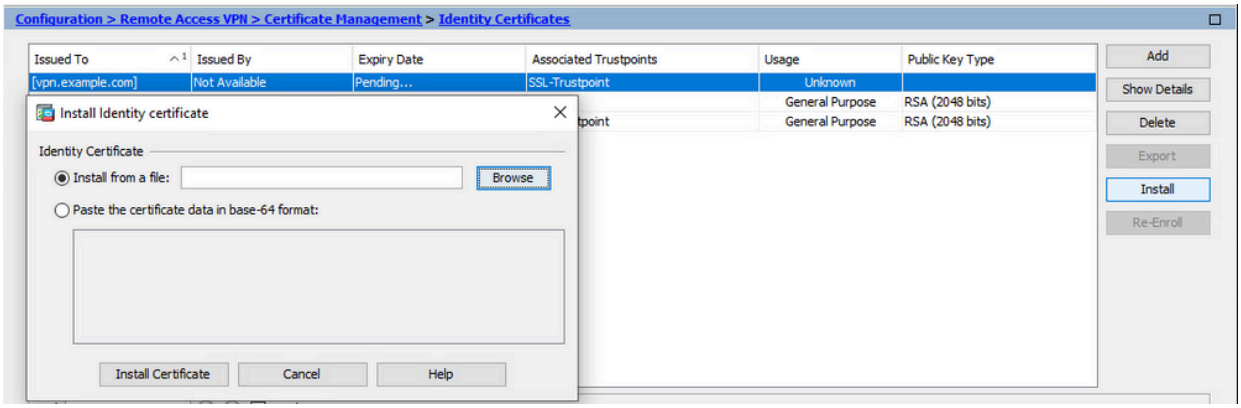
a. Escolha o Certificado de Identidade criado anteriormente durante a geração do CSR. Clique em Instalar.



Observação: o certificado de identidade pode ter o campo Emitido por como Não disponível e o campo Data de expiração como Pendente.

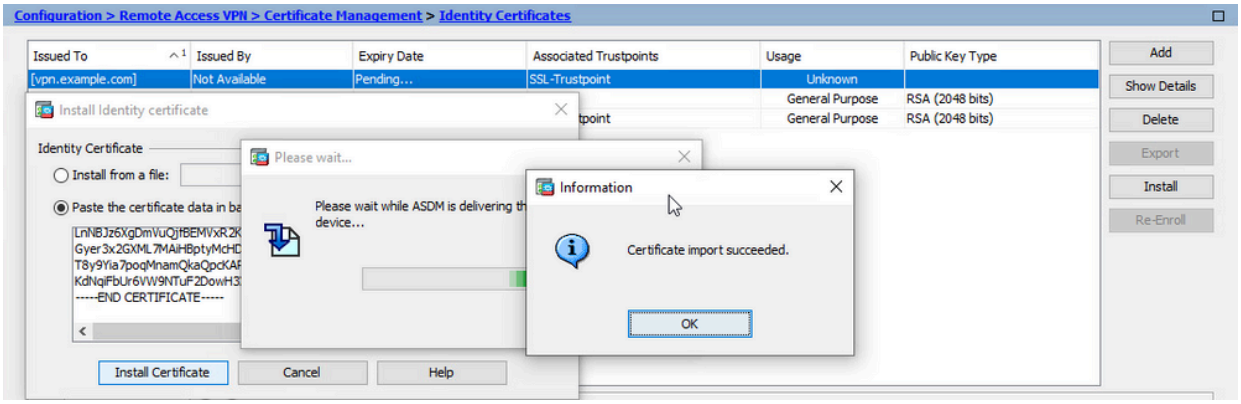
---

b. Escolha um arquivo que contenha o Certificado de Identidade codificado PEM recebido da CA ou abra o certificado codificado PEM em um editor de texto e copie e cole o Certificado de Identidade fornecido pela CA no campo de texto.



Observação: o certificado de identidade pode estar no formato .pem, .cer, .crt para instalar.

c. Clique em Install certificate (Instalar certificado).



3. Vincular o Novo Certificado à Interface com o ASDM

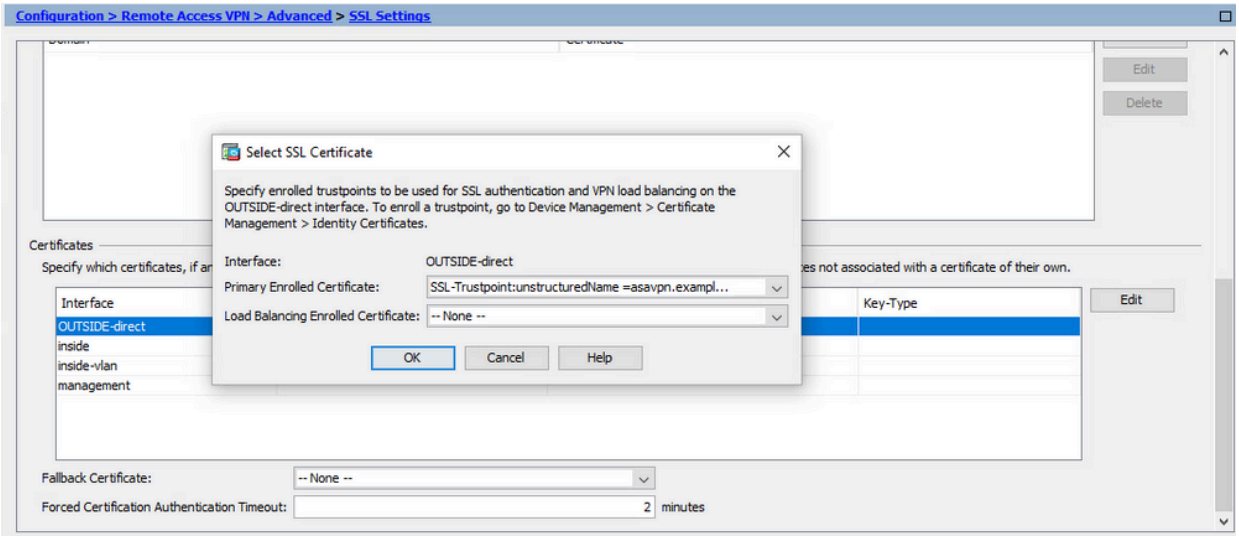
O ASA precisa ser configurado para usar o novo Certificado de Identidade para sessões WebVPN que terminam na interface especificada.

a. Navegue até Configuration > Remote Access VPN > Advanced > SSL Settings (Configuração > VPN de acesso remoto > Avançado > Configurações SSL).

b. Em certificados, escolha a interface usada para encerrar sessões de WebVPN. Neste exemplo, a interface externa é usada.

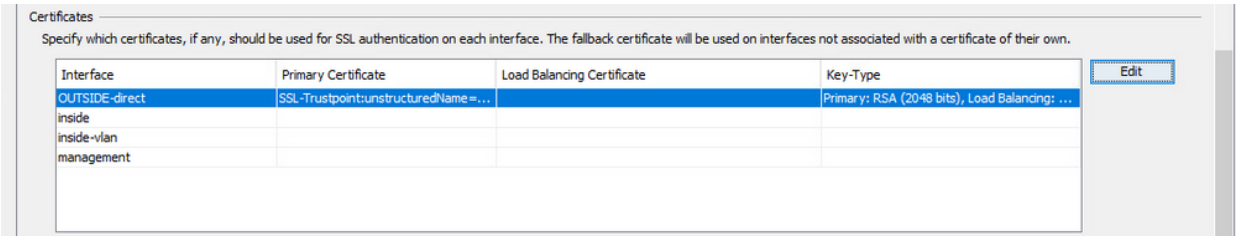
Clique em Editar.

c. Na lista suspensa Certificate (Certificado), escolha o certificado recém-instalado.



d. Click OK.

e. Clique em Apply.



Agora o novo Certificado de Identidade está em uso.

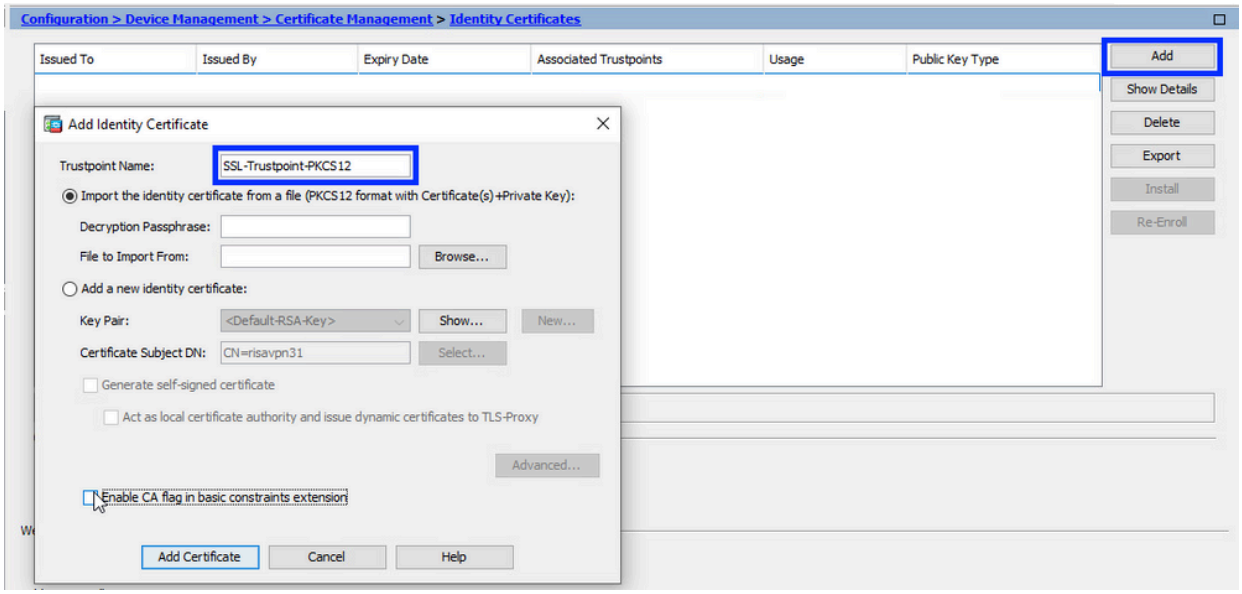
Instalar um certificado de identidade recebido no formato PKCS12 com ASDM

O arquivo PKCS12 (formato .p12 ou .pfx) contém certificado de identidade, par de chaves e certificado(s) de autoridade de certificação. Ele é criado pela CA, por exemplo, no caso de um certificado curinga, ou exportado de um dispositivo diferente. É um arquivo binário, não pode ser exibido com o editor de texto.

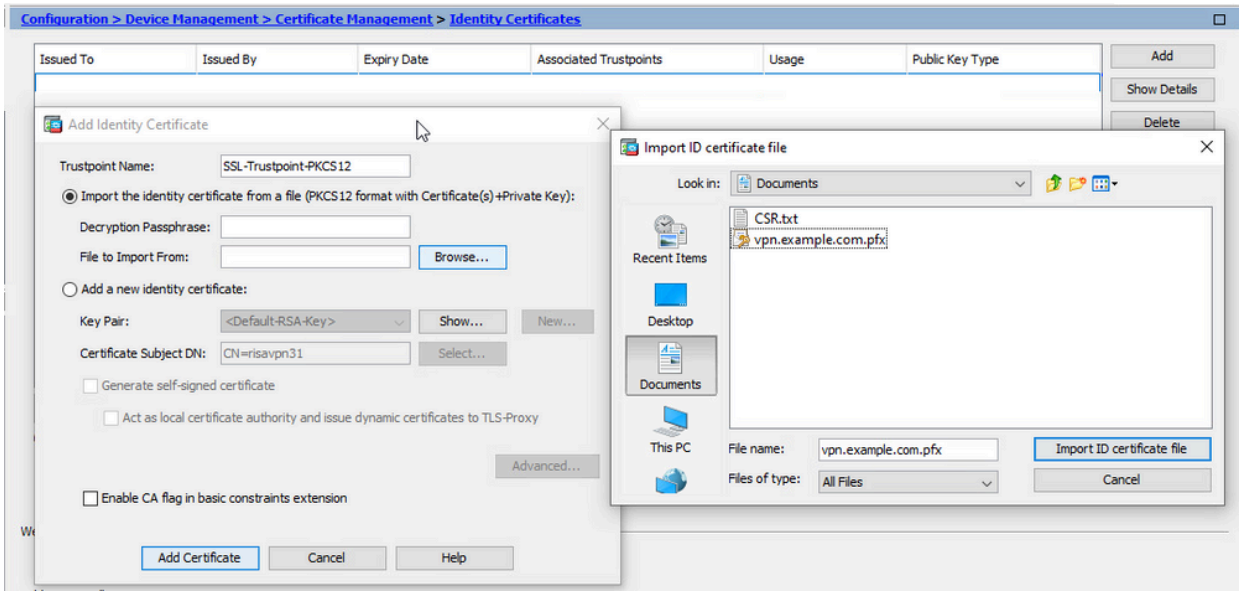
1. Instalar os certificados de identidade e CA de um arquivo PKCS12

O Certificado de identidade, o(s) certificado(s) de CA e o par de chaves precisam ser agrupados em um único arquivo PKCS12.

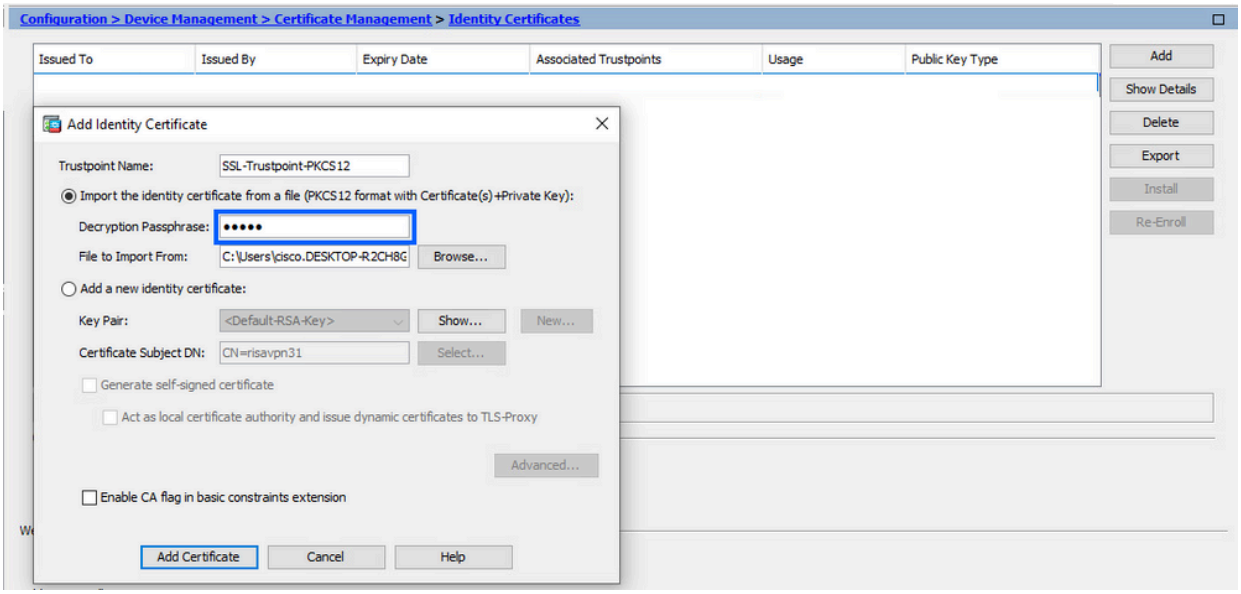
a. Navegue até Configuration > Device Management > Certificate Management e escolha Identity Certificates.
b. Clique em Add.
c. Especifique um nome de Trustpoint.



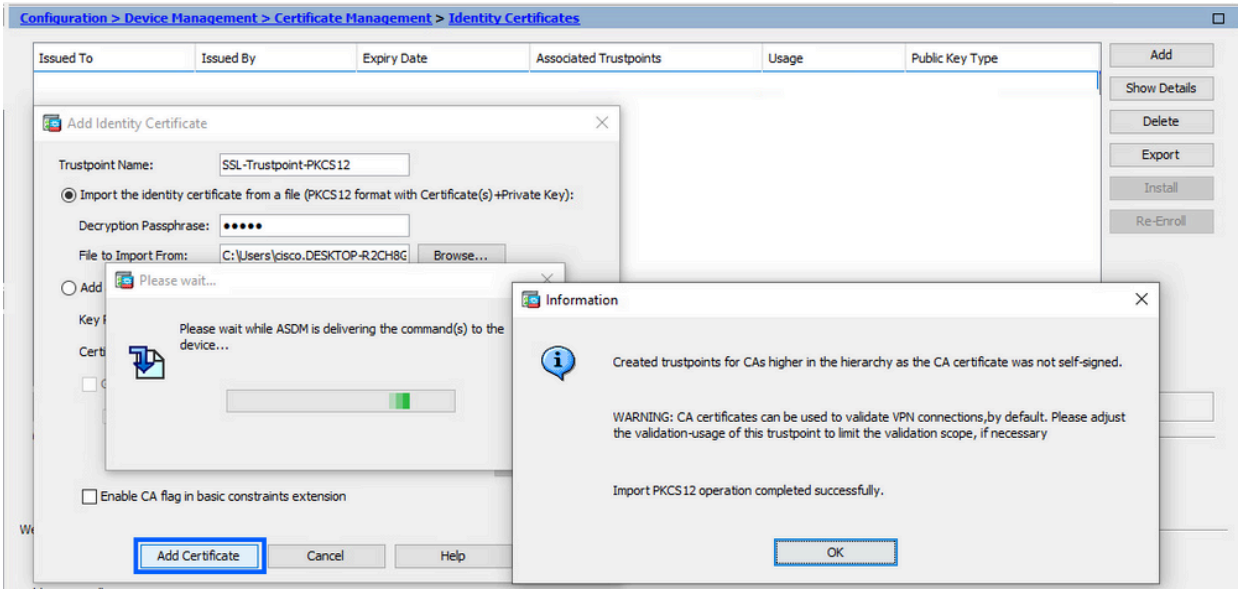
d. Clique no botão de rádio Import the identity certificate from a file (Importar o certificado de identidade de um arquivo).



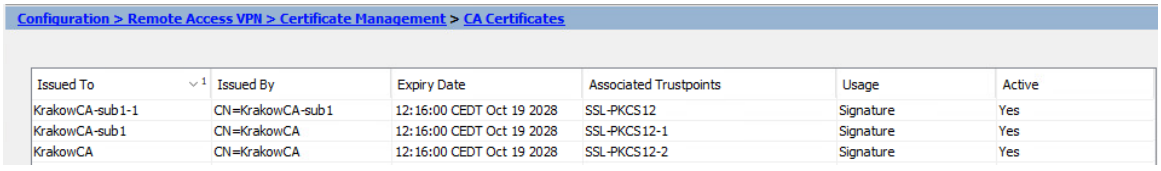
e. Insira a senha usada para criar o arquivo PKCS12.



f. Clique em Add Certificate (Adicionar certificado).



Observação: quando você importa um PKCS12 com uma cadeia de certificados CA, o ASDM cria automaticamente os pontos de confiança da CA de upstream com nomes com sufixo -number adicionado.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. Vincular o Novo Certificado à Interface com o ASDM

O ASA precisa ser configurado para usar o novo Certificado de Identidade para sessões WebVPN que terminam na interface especificada.

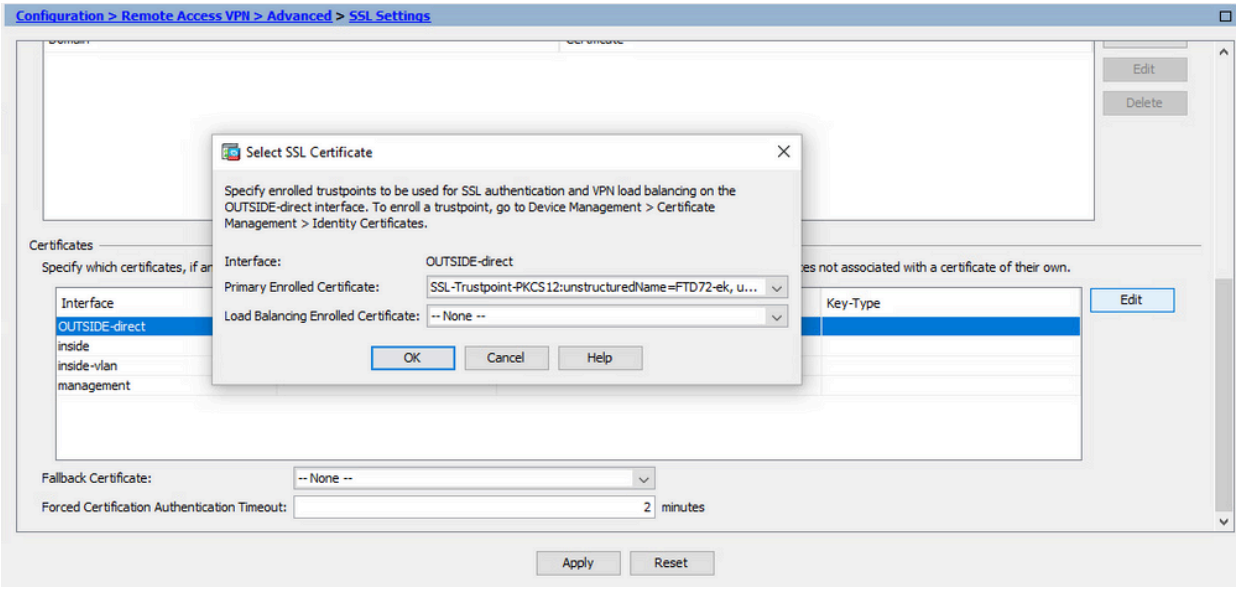
a. Navegue até Configuration > Remote Access VPN > Advanced > SSL Settings

(Configuração > VPN de acesso remoto > Avançado > Configurações SSL).

b. Em Certificates (Certificados), selecione a interface usada para encerrar sessões de WebVPN. Neste exemplo, a interface externa é usada.

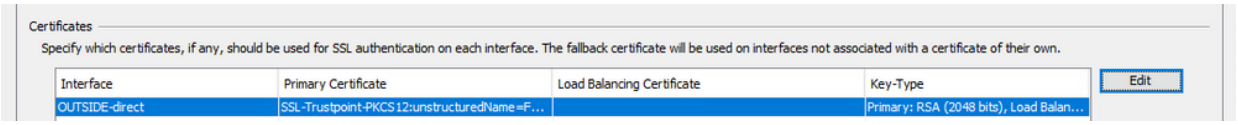
Clique em Editar.

c. Na lista suspensa Certificate (Certificado), escolha o certificado recém-instalado.



d. Click OK.

e. Clique em Apply.



Agora o novo Certificado de Identidade está em uso.

Renovação de certificado

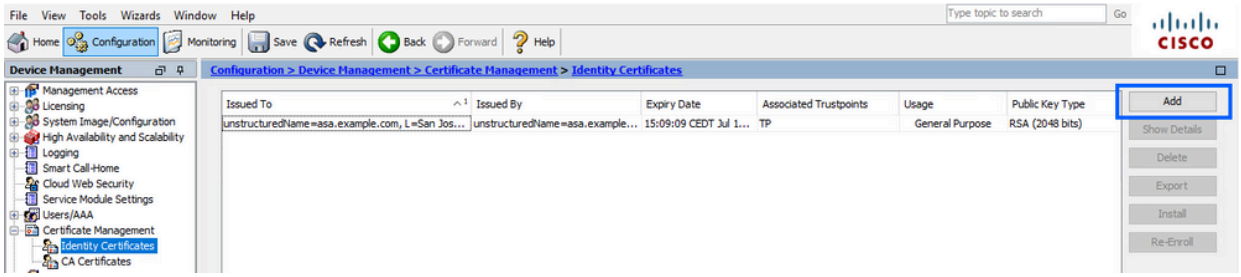
Renove um certificado registrado com CSR (Certificate Signing Request, solicitação de assinatura de certificado) com ASDM

A renovação de certificado registrado CSR requer a criação e a inscrição de um novo ponto de confiança. Ele precisa ter um nome diferente (por exemplo, nome antigo com sufixo de ano de inscrição). Ele pode usar os mesmos parâmetros e Par de chaves que o certificado antigo, ou pode usar diferentes.

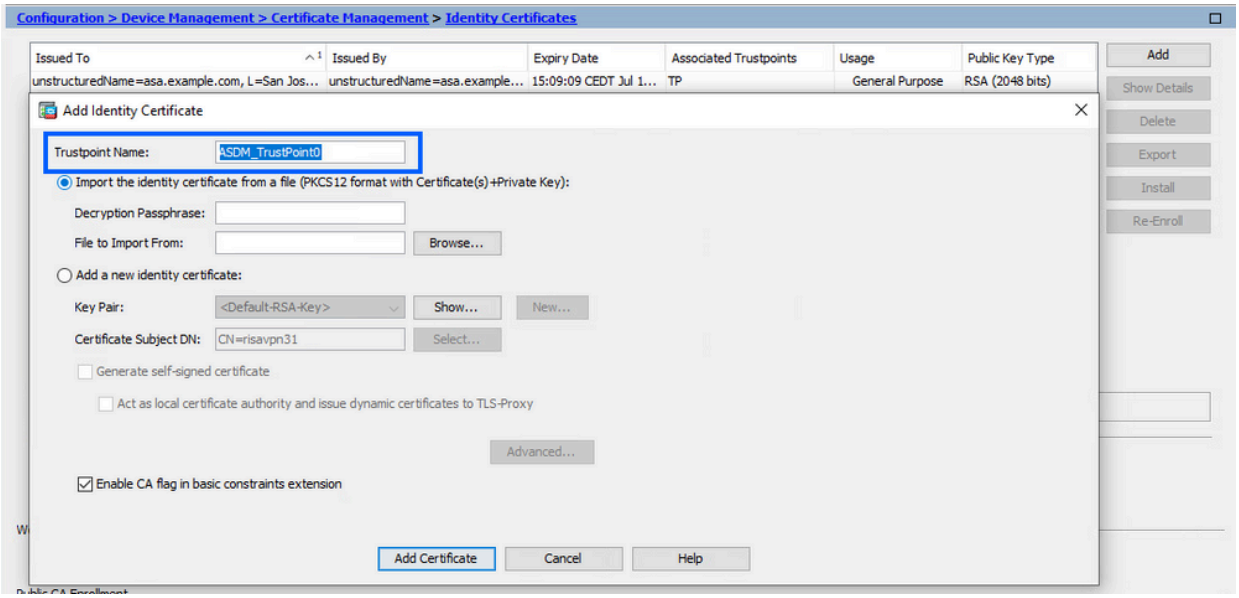
Gerar um CSR com ASDM

1. Crie um Novo Ponto de Confiança com um Nome Específico.

a. Navegue até Configuration > Device Management >Certificate Management > Identity Certificates.



b. Clique em Add.
c. Defina um nome de ponto confiável.



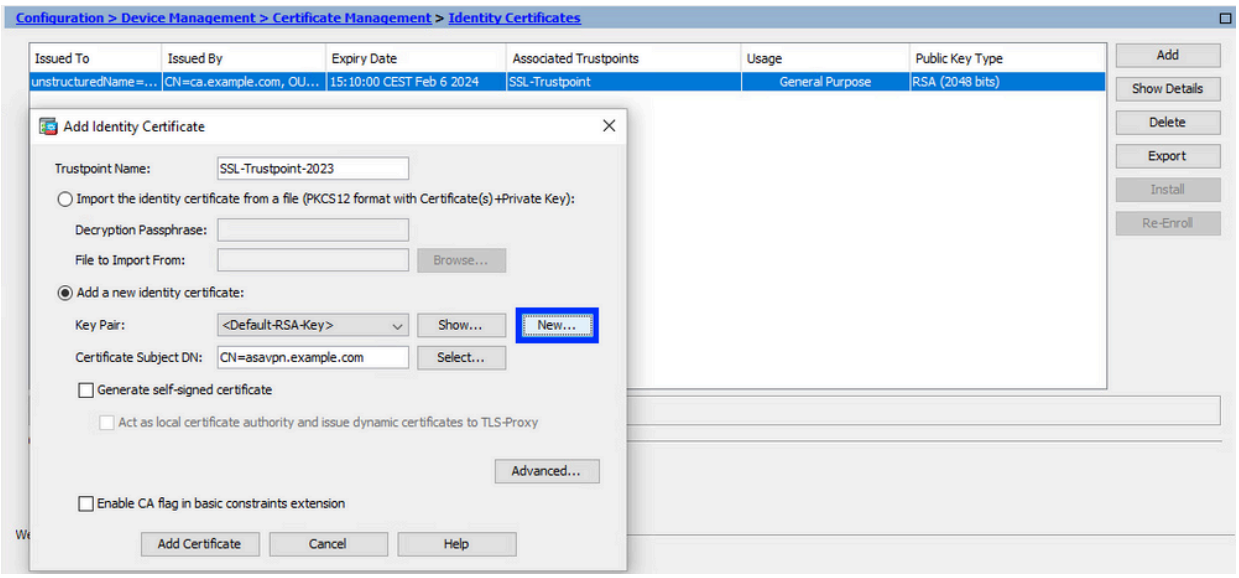
d. Clique no botão de rádio Add a new identity certificate (Adicionar um novo certificado de identidade).

2. (Opcional) Crie um novo par de chaves

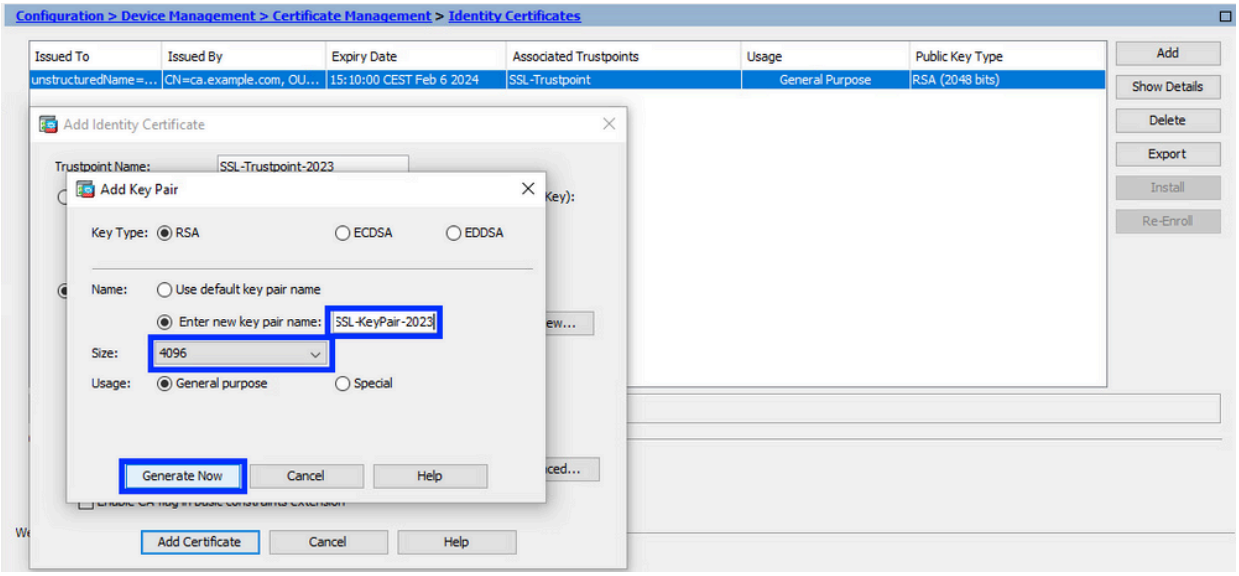
Nota: Por padrão, é usada a chave RSA com o nome Default-RSA-Key e o tamanho 2048; no entanto, recomenda-se usar um par de chaves privado/público exclusivo para cada certificado de identidade.

---

a. Clique em New para gerar um novo par de chaves.

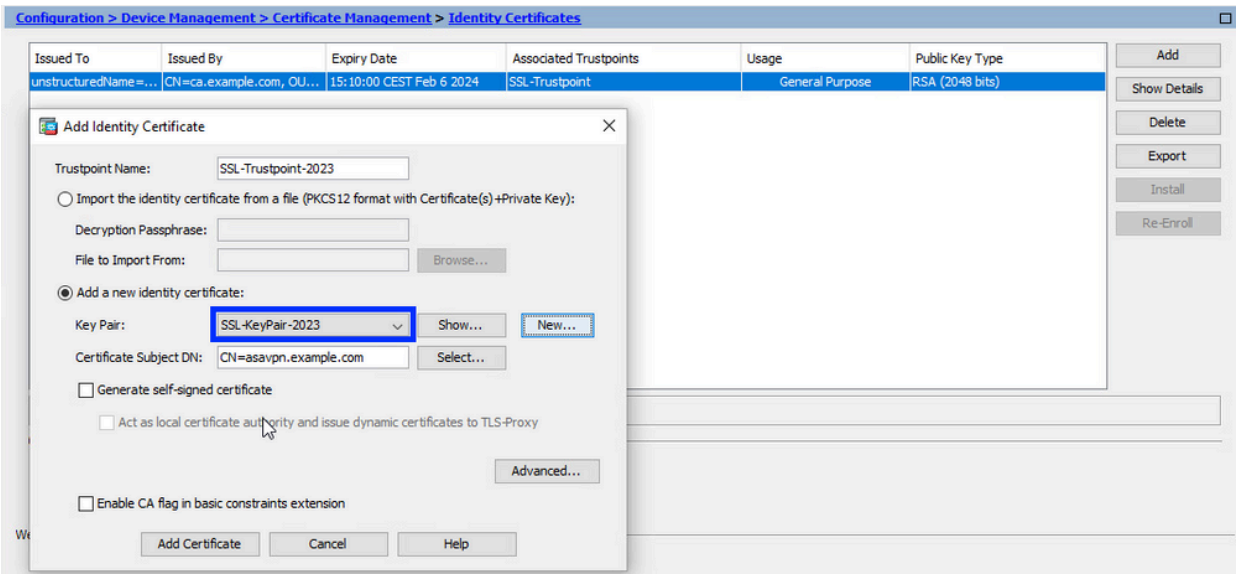


b. Escolha a opção Enter new Key Pair name e insira um nome para o novo par de chaves.
c. Escolha o tipo de chave-RSA ou ECDSA.
d. Escolha o tamanho da chave; para RSA, escolha Uso geral.
e. Clique em Generate CSR (Gerar CSR). O par de chaves foi criado.



3. Selecione o nome do par de chaves

Escolha o par de chaves com o qual assinar o CSR e que será vinculado ao novo certificado.



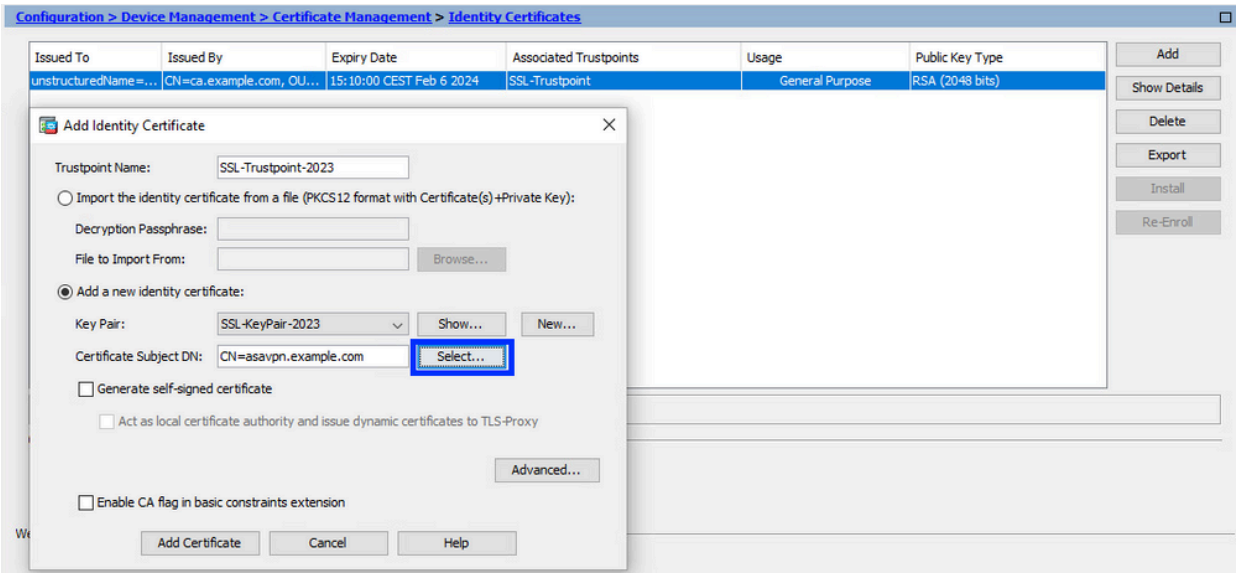
4. Configurar o assunto do certificado e o nome de domínio totalmente qualificado (FQDN)

Cuidado: o parâmetro FQDN deve corresponder ao FQDN ou ao endereço IP da interface ASA para a qual o certificado é usado. Esse parâmetro define o SAN (Nome Alternativo da Entidade) do certificado. O campo SAN é usado pelo cliente SSL/TLS/IKEv2 para verificar se o certificado corresponde ao FQDN ao qual ele se conecta.

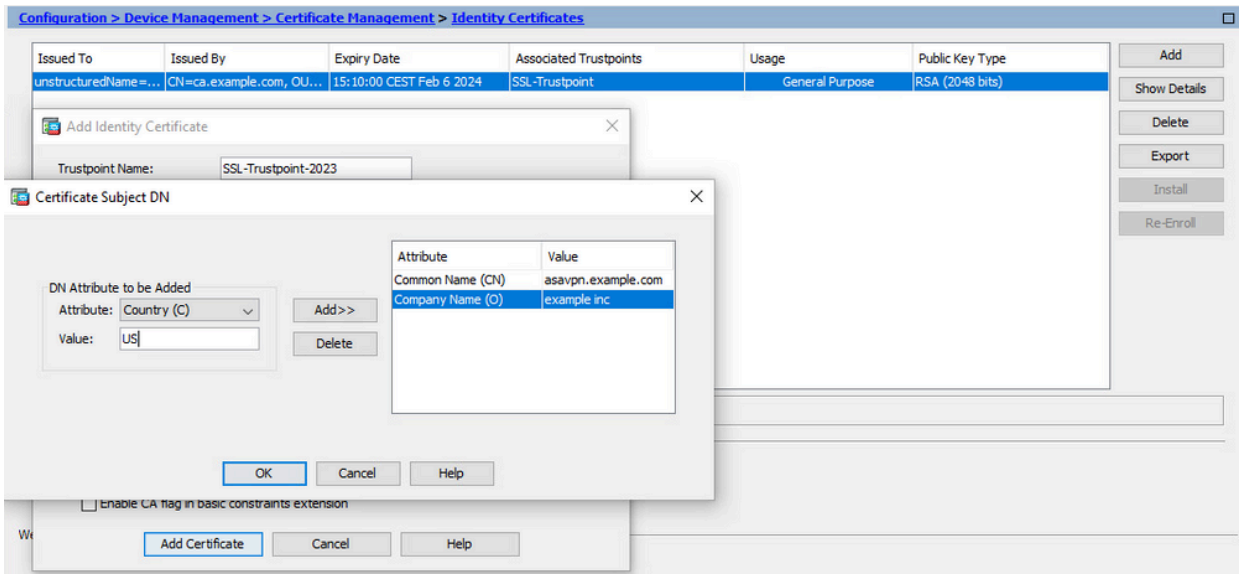
Observação: a CA pode alterar os parâmetros FQDN e Nome do assunto definidos no ponto de confiança ao assinar o CSR e criar um Certificado de Identidade assinado.

---

a. Clique em Selecionar.



b. Na janela Certificate Subject DN (DN do assunto do certificado), configure certificate attributes - selecione o atributo na lista suspensa, digite o valor e clique em Add.

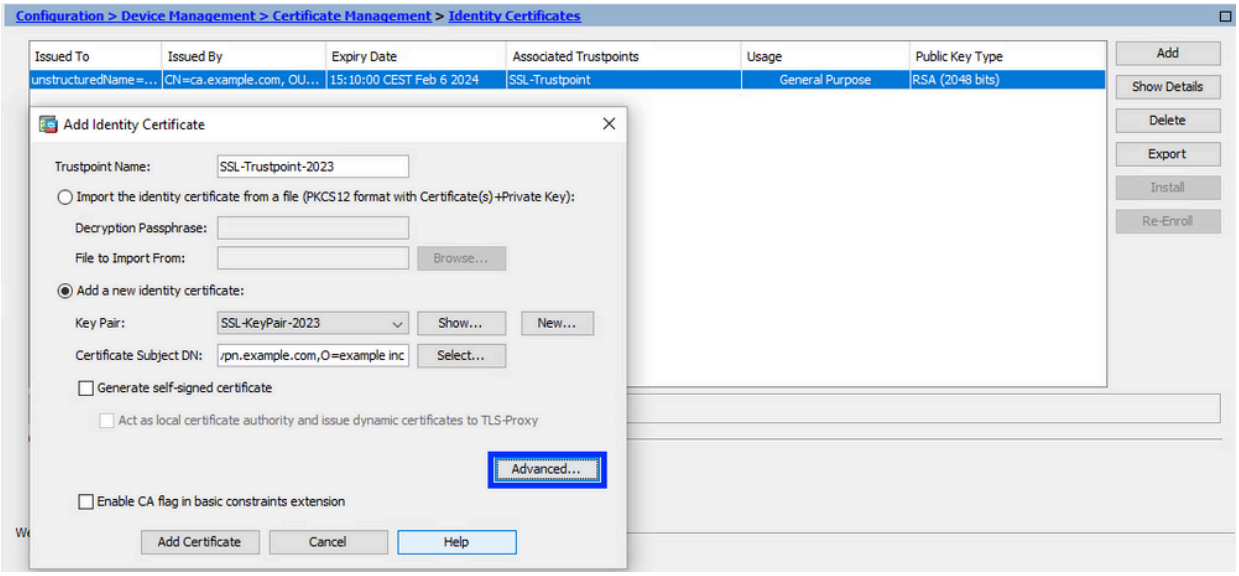


Atributo	Descrição
CN	O nome pelo qual o firewall pode ser acessado (geralmente o nome de domínio totalmente qualificado, por exemplo, vpn.example.com).
OU	O nome do seu departamento na organização
O	O nome legalmente registrado da sua organização/empresa
C	Código do país (código de 2 letras sem pontuação)
ST	O estado no qual sua organização está localizada.
I	A cidade em que sua organização está localizada.
EA	Endereço de e-mail

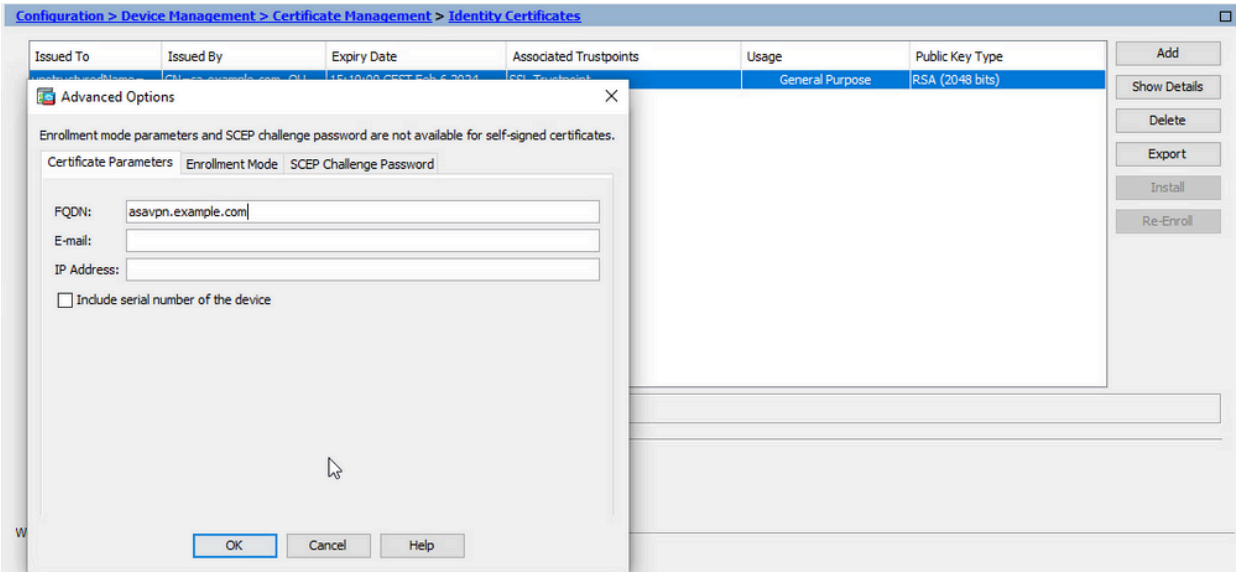
Observação: nenhum dos campos anteriores pode exceder um limite de 64 caracteres. Um valor mais longo pode causar problemas com a instalação do Certificado de Identidade. Além disso, não é necessário definir todos os atributos DN.

Clique em OK depois que todos os atributos forem adicionados.

c. Para configurar o FQDN do dispositivo, clique em Avançado.

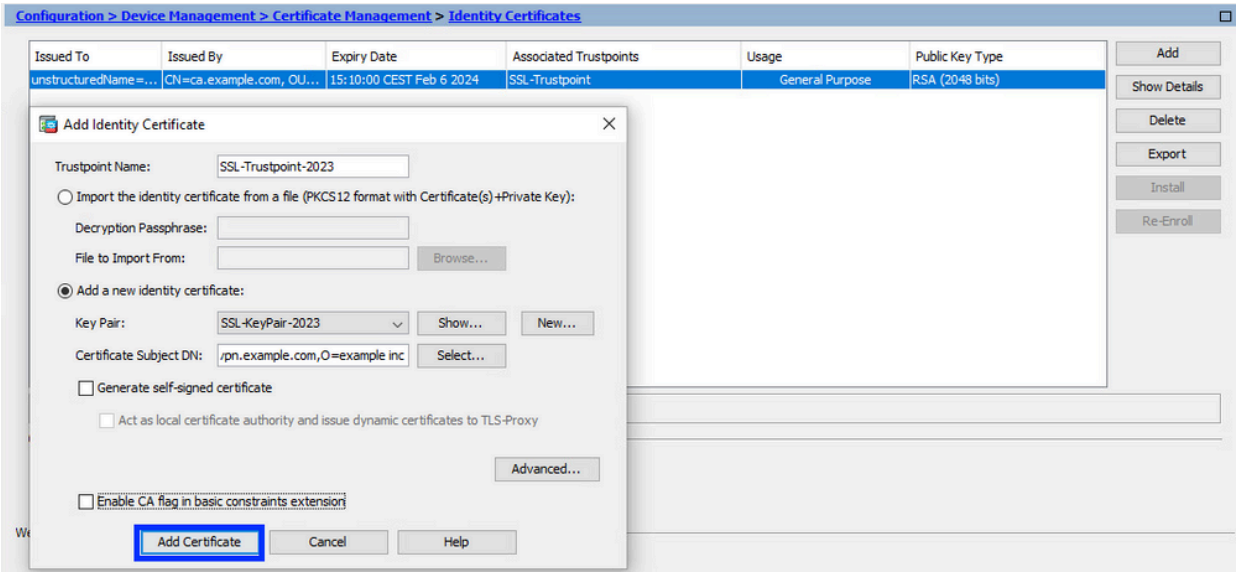


d. No campo FQDN, insira o nome de domínio totalmente qualificado pelo qual o dispositivo pode ser acessado a partir da Internet. Click OK.

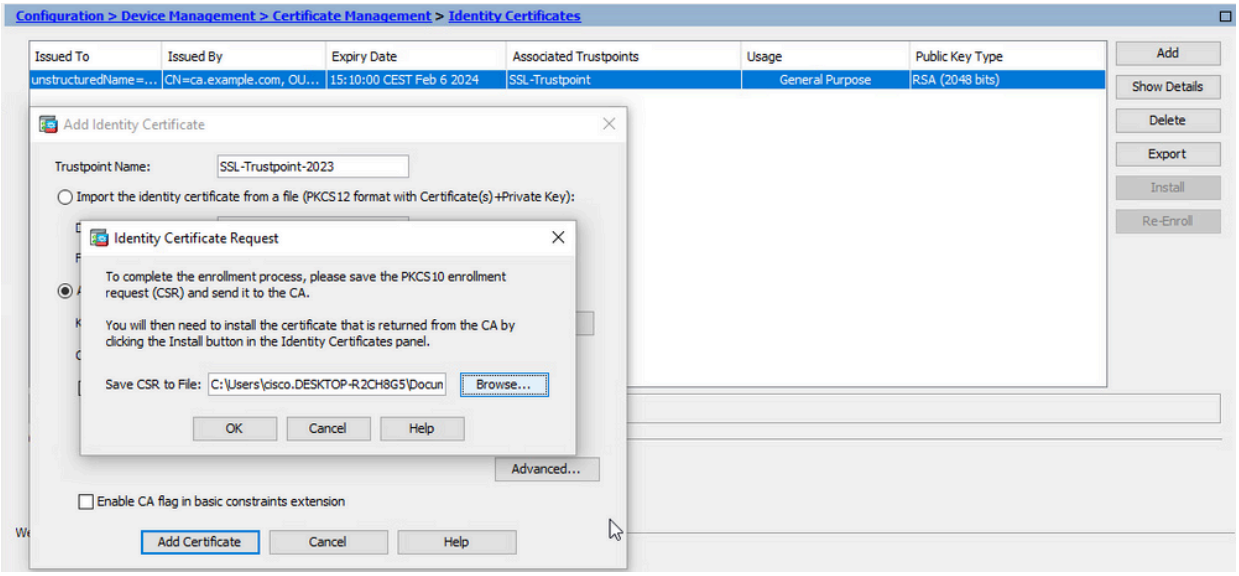


5. Gerar e salvar o CSR

a. Clique em Add Certificate (Adicionar certificado).



b. Um prompt é exibido para salvar o CSR em um arquivo na máquina local.

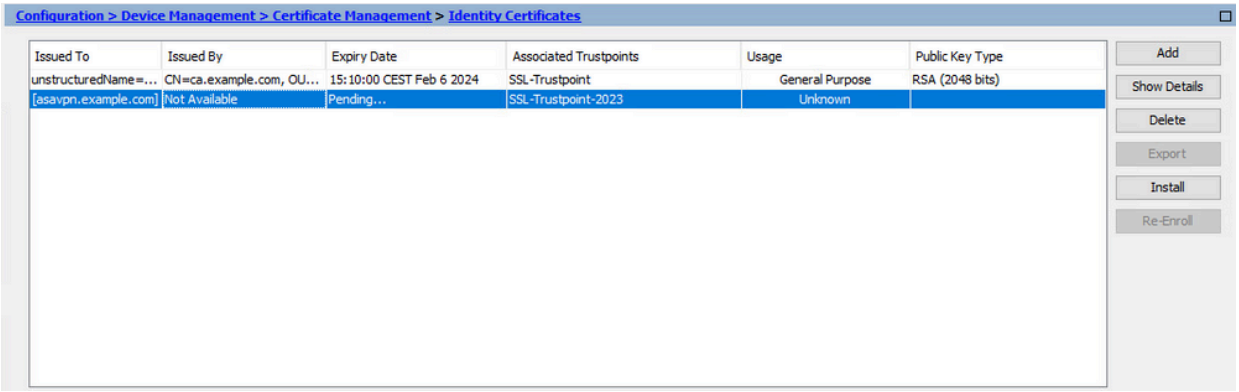


Clique em Procurar. Escolha um local para salvar o CSR e salve o arquivo com a extensão .txt.

> Observação: quando o arquivo é salvo com uma extensão .txt, a solicitação PKCS#10 pode ser aberta e visualizada com um editor de texto (como o Notepad).

---

c. Agora o novo ponto confiável é exibido em um estado Pendente.



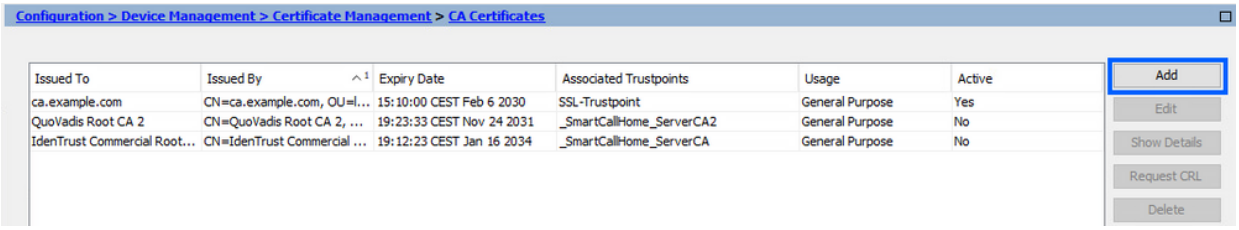
Instalar o Certificado de Identidade no Formato PEM com o ASDM

As etapas de instalação pressupõem que a CA assinou o CSR e forneceu um novo certificado de identidade e um pacote de certificado de CA codificados em PEM (.pem, .cer, .crt).

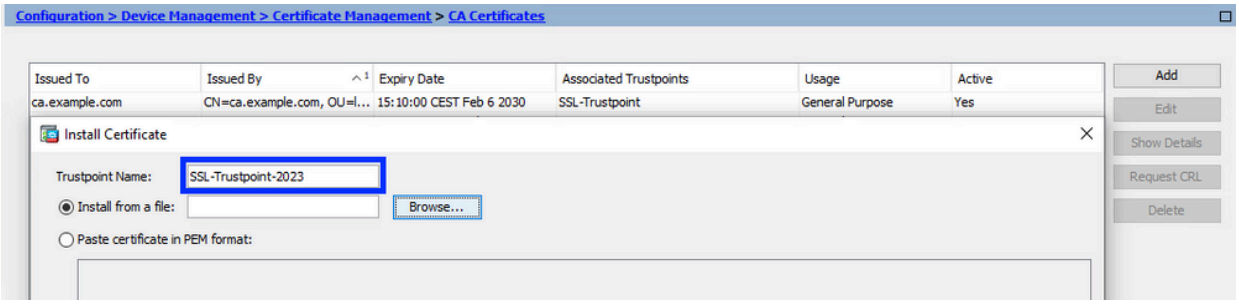
1. Instalar o certificado de autoridade de certificação que assinou o CSR

   O certificado CA que assinou o Certificado de Identidade pode ser instalado no Ponto de Confiança criado para o Certificado de Identidade. Se o Certificado de Identidade for assinado por uma autoridade de certificação intermediária, esse certificado de autoridade de certificação poderá ser instalado no Ponto de Confiança do Certificado de Identidade. Todos os certificados de autoridade de certificação upstream na hierarquia podem ser instalados em pontos confiáveis de autoridade de certificação separados.

   a. Navegue até Configuration > Device Management >Certificate Management > e escolha CA Certificates. Clique em Add.



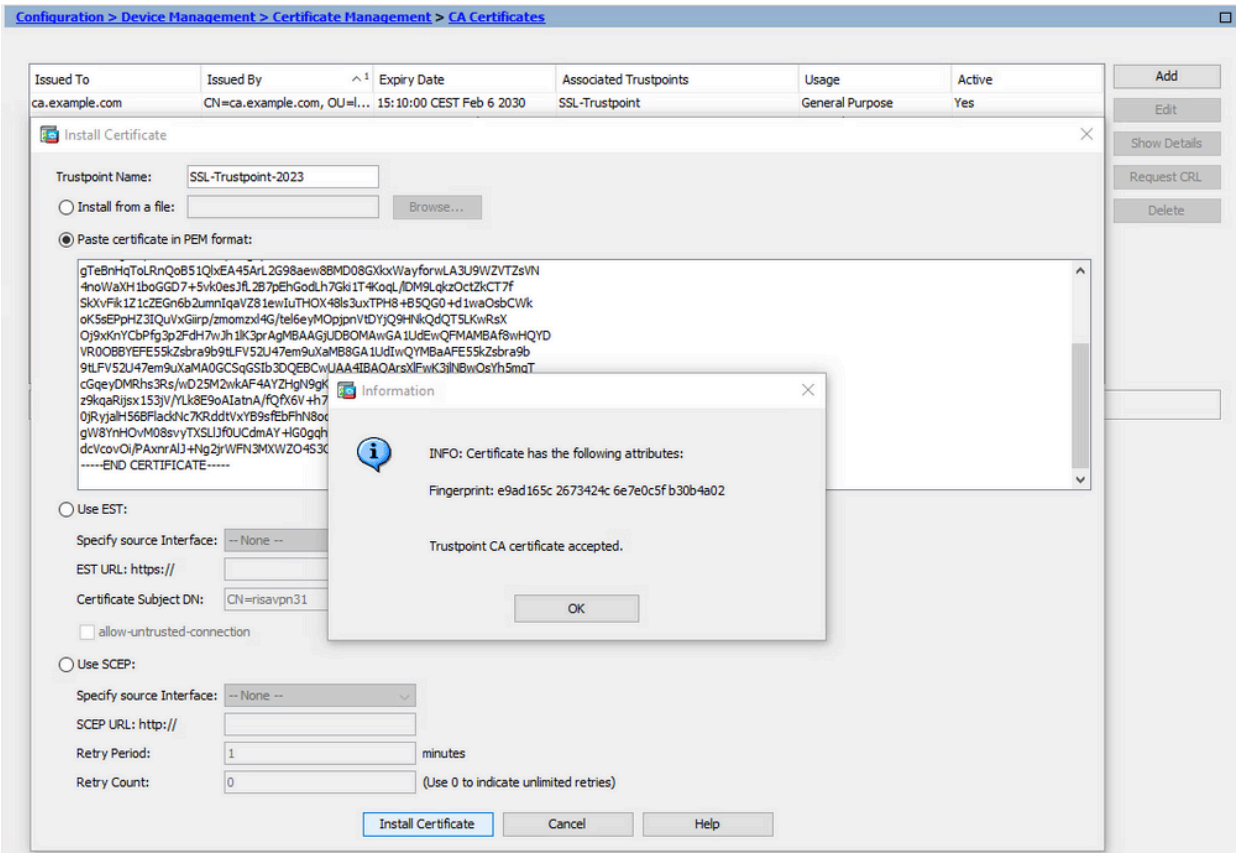
   b. Insira o nome do ponto de confiança e escolha Instalar do arquivo, clique no botão Procurar e escolha o certificado intermediário. Como alternativa, cole o certificado CA codificado PEM de um arquivo de texto no campo de texto.



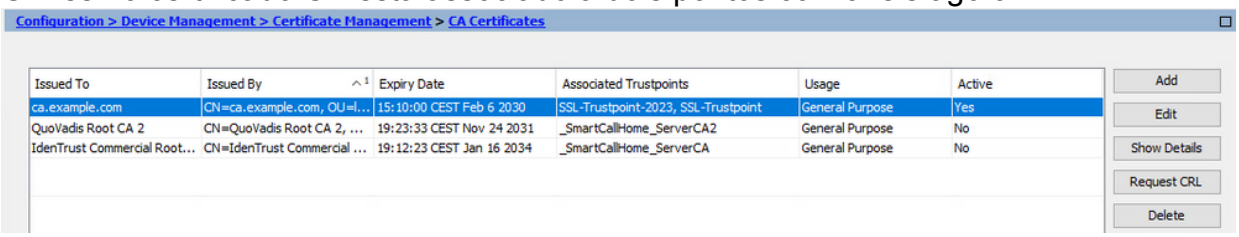
Observação: instale o certificado intermediário com o mesmo nome de ponto de

confiança que o nome de ponto de confiança do Certificado de Identidade, se o Certificado de Identidade for assinado pelo certificado de CA intermediário.

c. Clique em Install certificate (Instalar certificado).

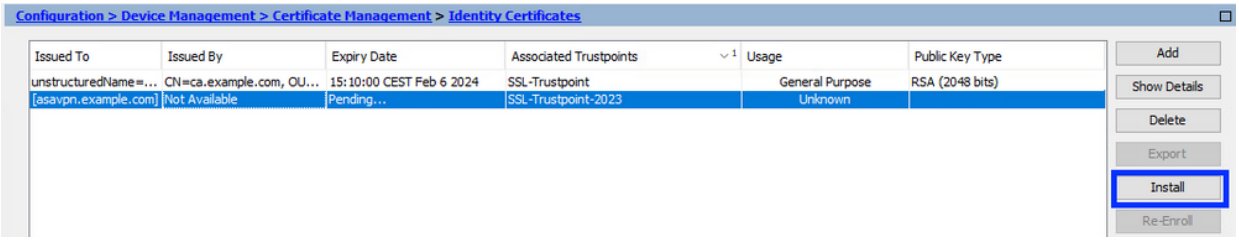


No exemplo, o novo certificado é assinado com o mesmo certificado CA que o antigo. O mesmo certificado CA está associado a dois pontos confiáveis agora.



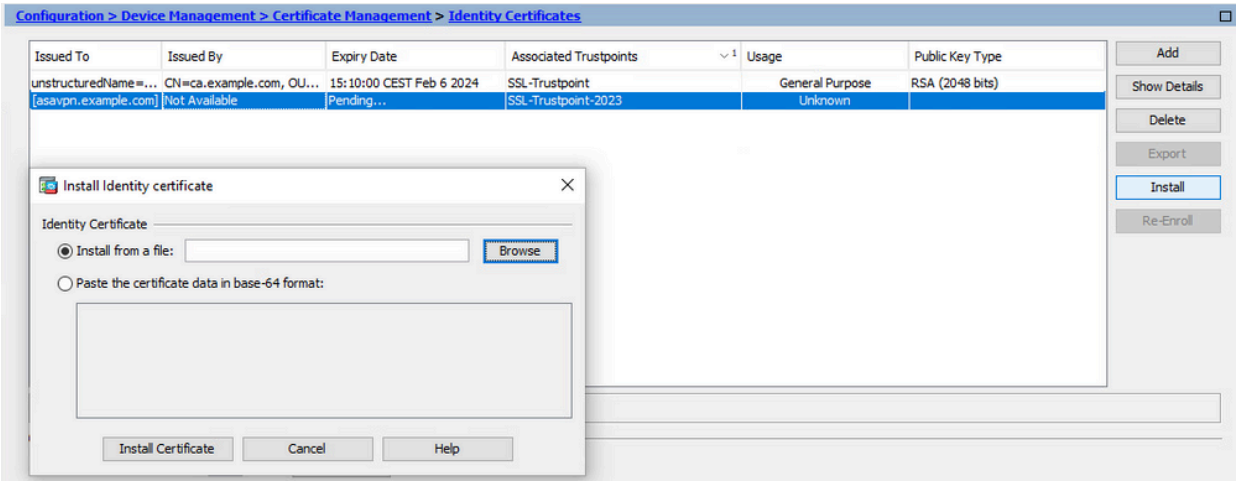
2. Instalar certificado de identidade

a. Escolha o Certificado de Identidade criado anteriormente com a geração de CSR. Clique em Instalar.



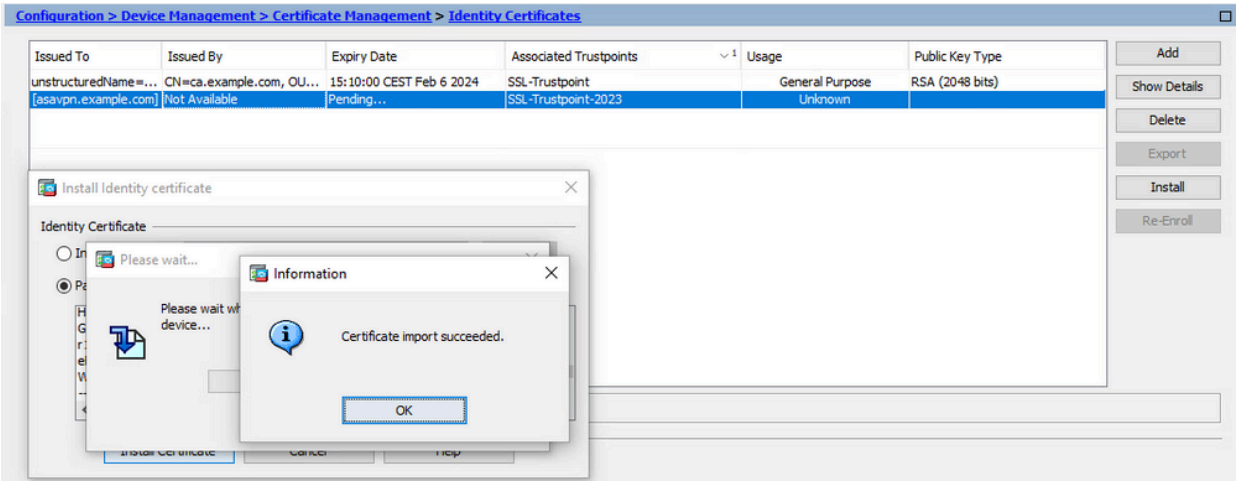
Observação: o certificado de identidade pode ter o campo Emitido por como Não disponível, e o campo Data de expiração como Pendente.

b. Escolha um arquivo que contenha o Certificado de Identidade codificado PEM recebido da CA ou abra o certificado codificado PEM em um editor de texto e copie e cole o Certificado de Identidade fornecido pela CA no campo de texto.

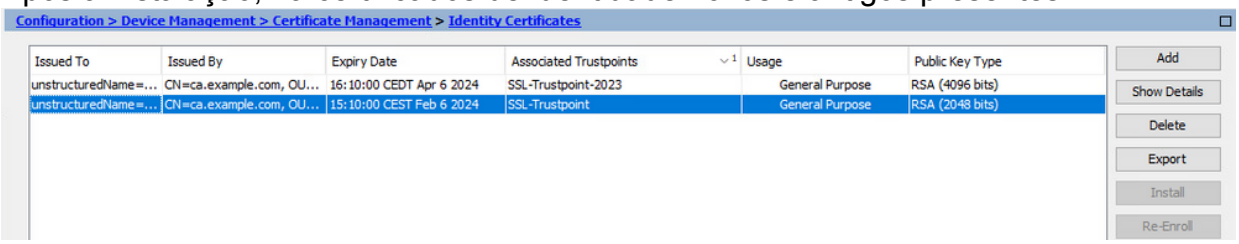


Observação: o certificado de identidade pode estar no formato .pem, .cer, .crt para instalar.

c. Clique em Install certificate (Instalar certificado).



Após a instalação, há certificados de identidade novos e antigos presentes.



3. Vincular o Novo Certificado à Interface com o ASDM

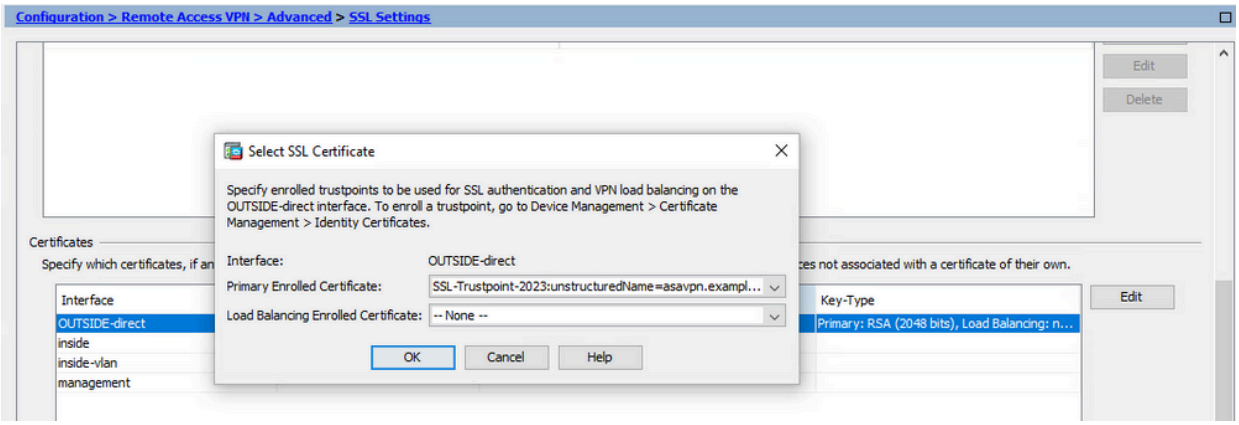
O ASA precisa ser configurado para usar o novo Certificado de Identidade para sessões WebVPN que terminam na interface especificada.

a. Navegue até Configuration > Remote Access VPN > Advanced > SSL Settings (Configuração > VPN de acesso remoto > Avançado > Configurações SSL).

b. Em certificados, escolha a interface usada para encerrar sessões de WebVPN. Neste exemplo, a interface externa é usada.

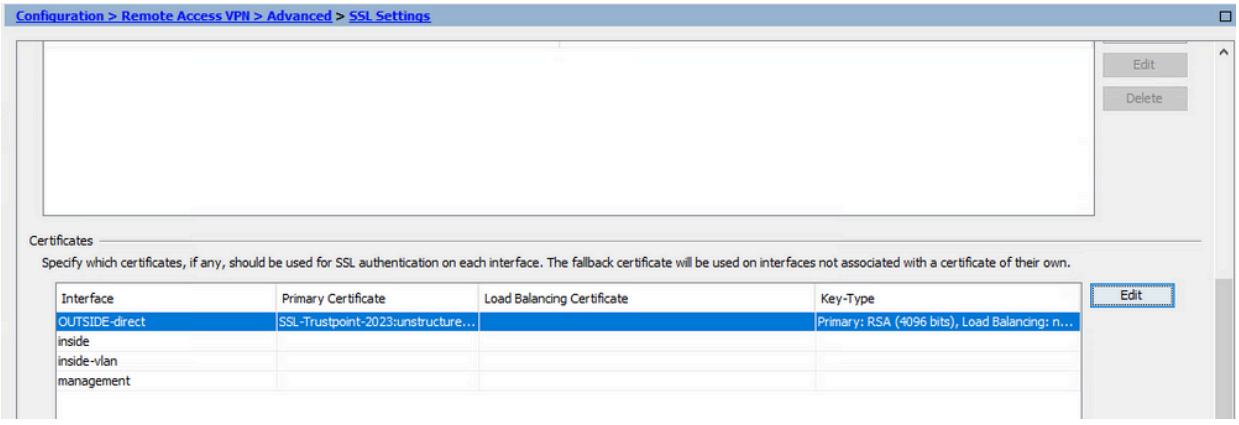
   Clique em Editar.

c. Na lista suspensa Certificate (Certificado), escolha o certificado recém-instalado.



d. Click OK.

e. Clique em Apply. Agora o novo Certificado de Identidade está em uso.



Renove um certificado registrado com o arquivo PKCS12 com ASDM

A renovação de certificado registrado no PKCS12 requer a criação e a inscrição de um novo ponto confiável. Ele precisa ter um nome diferente (por exemplo, nome antigo com sufixo de ano de inscrição).

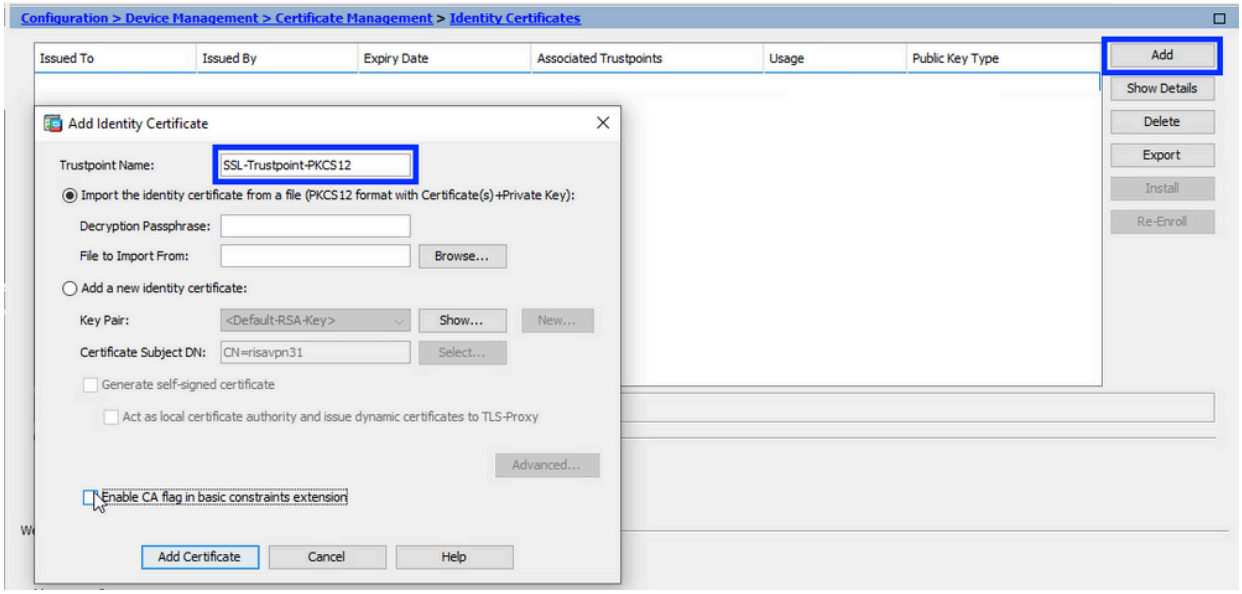
O arquivo PKCS12 (formato .p12 ou .pfx) contém certificado de identidade, par de chaves e certificado(s) de autoridade de certificação. Ele é criado pela CA, por exemplo, no caso de um

certificado curinga, ou exportado de um dispositivo diferente. É um arquivo binário e não pode ser exibido com o editor de texto.

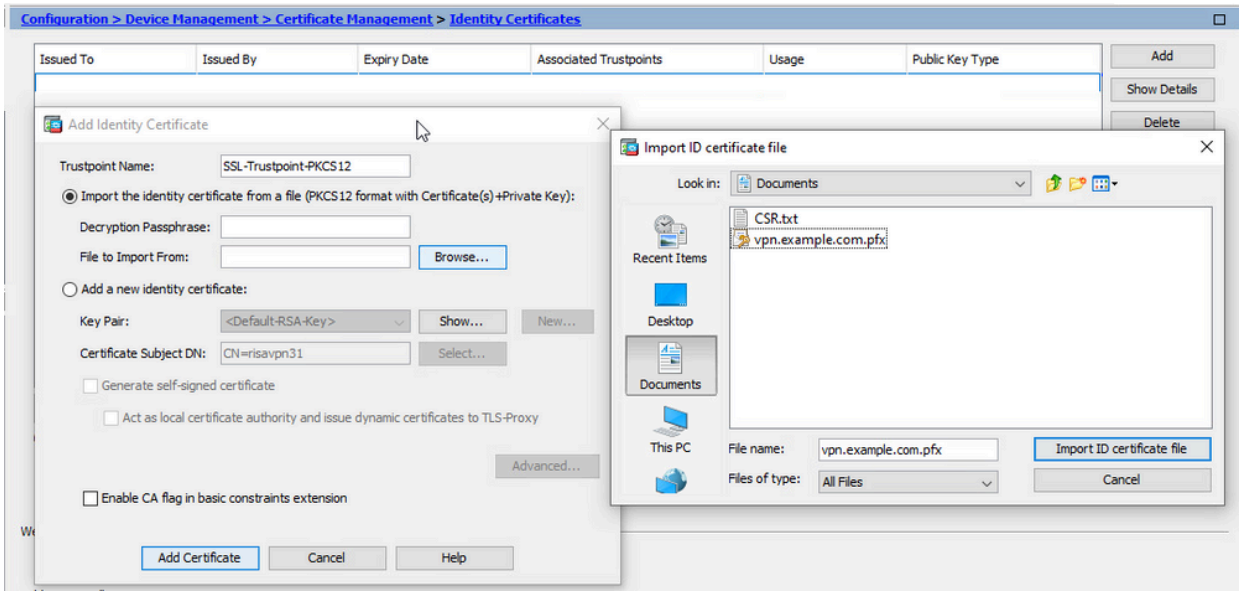
1. Instalar o certificado de identidade renovado e os certificados CA de um arquivo PKCS12

   O Certificado de identidade, o(s) certificado(s) de CA e o par de chaves precisam ser agrupados em um único arquivo PKCS12.

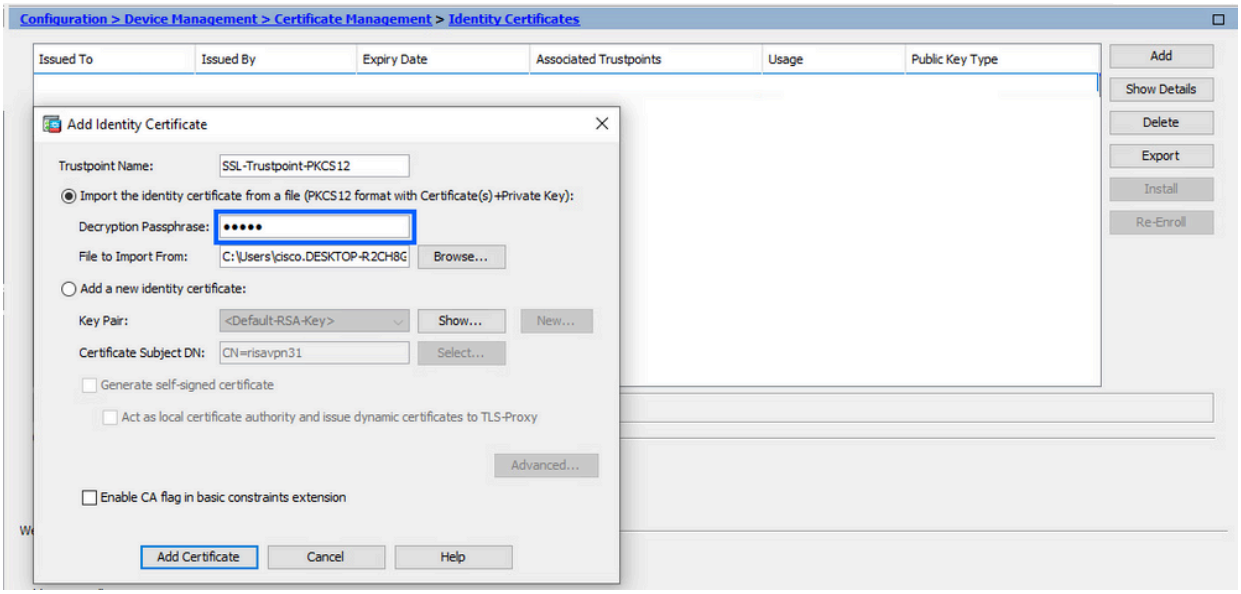
   a. Navegue até Configuration > Device Management > Certificate Management e escolha Identity Certificates.
   b. Clique em Add.
   c. Especifique um novo nome de Ponto de Confiabilidade.



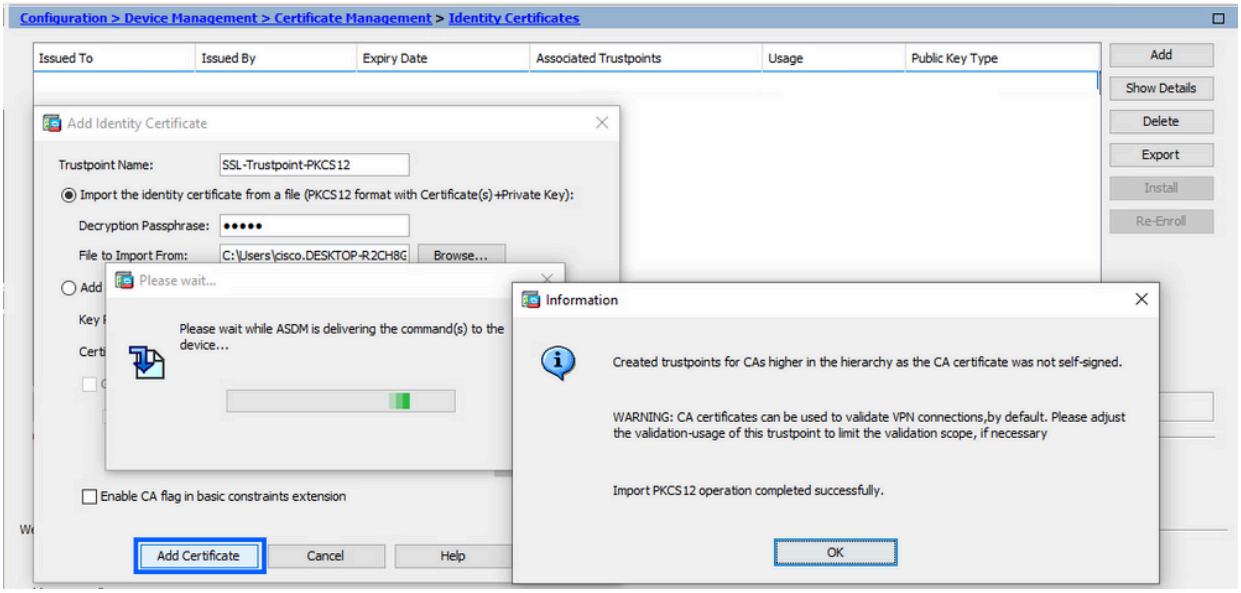
   d. Clique no botão de rádio Import the identity certificate from a file (Importar o certificado de identidade de um arquivo).



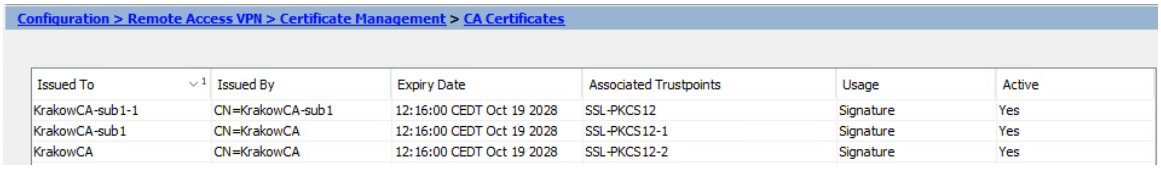
   e. Insira a senha usada para criar o arquivo PKCS12.



f. Clique em Add Certificate (Adicionar certificado).



Observação: quando uma cadeia de certificados PKCS12 com CAs é importada, o ASDM cria automaticamente pontos de confiança de CAs upstream com nomes com sufixo -number adicionado.



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Active
KrakowCA-sub1-1	CN=KrakowCA-sub1	12:16:00 CEDT Oct 19 2028	SSL-PKCS12	Signature	Yes
KrakowCA-sub1	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-1	Signature	Yes
KrakowCA	CN=KrakowCA	12:16:00 CEDT Oct 19 2028	SSL-PKCS12-2	Signature	Yes

2. Vincular o Novo Certificado à Interface com o ASDM

O ASA precisa ser configurado para usar o novo Certificado de Identidade para sessões WebVPN que terminam na interface especificada.

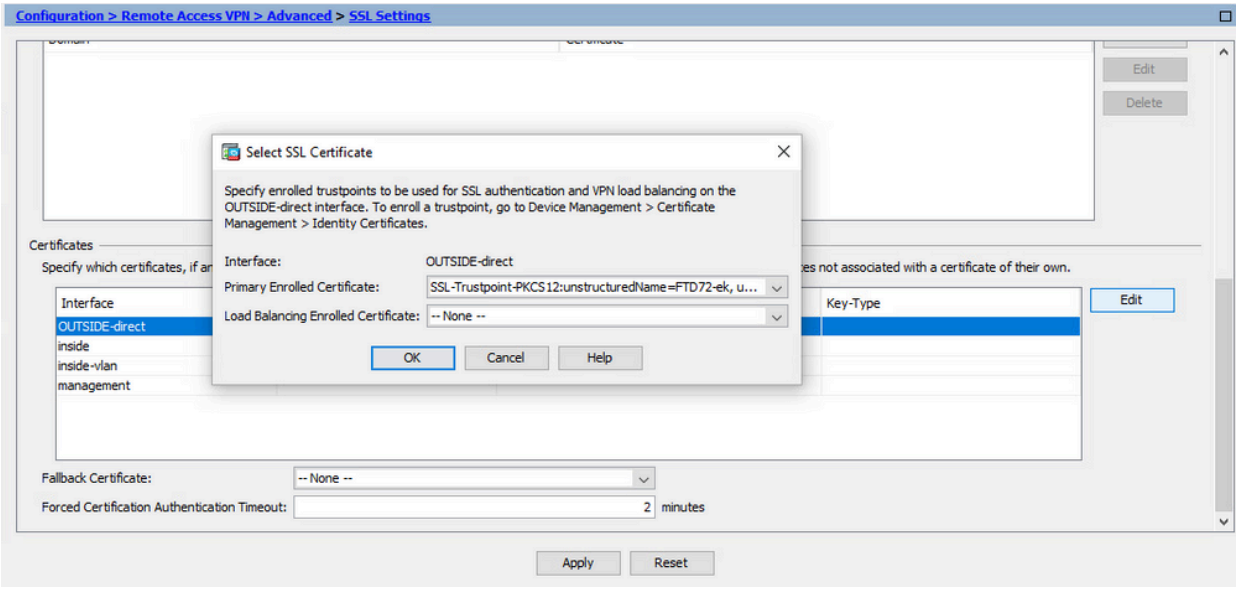
a. Navegue até Configuration > Remote Access VPN > Advanced > SSL Settings

(Configuração > VPN de acesso remoto > Avançado > Configurações SSL).

b. Em certificados, escolha a interface usada para encerrar sessões de WebVPN. Neste exemplo, a interface externa é usada.

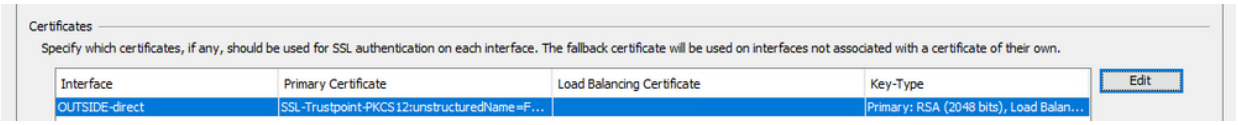
Clique em Editar.

c. Na lista suspensa Certificate (Certificado), escolha o certificado recém-instalado.



d. Click OK.

e. Clique em Apply.



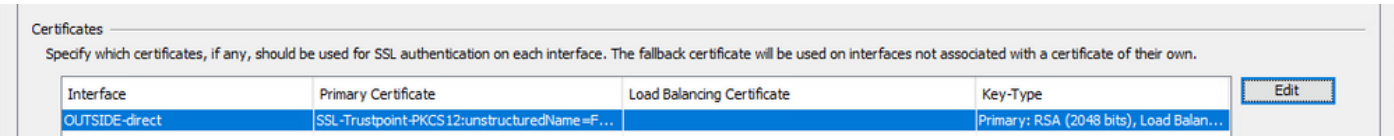
Agora o novo Certificado de Identidade está em uso.

Verificar

Use estas etapas para verificar se a instalação do Certificado de fornecedor de terceiros foi bem-sucedida e o uso para conexões VPN SSL.

Exibir certificados instalados via ASDM

1. Navegue até Configuration > Remote Access VPN > Certificate Management (Configuração > Acesso remoto > Gerenciamento) e escolha Identity Certificates (Certificados de identidade).
2. O Certificado de Identidade emitido pelo fornecedor terceirizado pode ser exibido.



Troubleshooting

Este comando de depuração deve ser coletado na CLI em caso de falha na instalação do certificado SSL.

- debug crypto ca 14

Perguntas mais freqüentes

P.O que é um PKCS12?
R.Na criptografia, o PKCS12 define um formato de arquivo criado para armazenar muitos objetos de criptografia como um único arquivo. É comumente usado para agrupar uma chave privada com seu certificado X.509 ou para agrupar todos os membros de uma cadeia de confiança.

P.O que é CSR?
R.Nos sistemas de infraestrutura de chave pública (PKI), um pedido de assinatura de certificado (também CSR ou pedido de certificação) é uma mensagem enviada de um requerente a uma autoridade de registro da infraestrutura de chave pública para solicitar um certificado de identidade digital. Ele geralmente contém a chave pública para a qual o certificado pode ser emitido, informações que são usadas para identificar o certificado assinado (como um nome de domínio no Assunto) e proteção de integridade (por exemplo, uma assinatura digital).

P.Onde está a senha do PKCS12?
R.Quando os certificados e os pares de chaves são exportados para um arquivo PKCS12, a senha é fornecida no comando export. Para importar um arquivo pkcs12, a senha precisa ser entregue pelo proprietário do servidor da autoridade de certificação ou pela pessoa que exportou o PKCS12 de outro dispositivo.

P.Qual é a diferença entre a raiz e a identidade?
R.Na criptografia e na segurança do computador, um certificado raiz é um certificado de chave pública que identifica uma autoridade de certificação raiz (CA). Os certificados raiz são autoassinados (e é possível que um certificado tenha vários caminhos confiáveis, digamos que o certificado tenha sido emitido por uma raiz que foi assinada) e formam a base de uma infraestrutura de chave pública (PKI) baseada em X.509. Um certificado de chave pública, também conhecido como certificado digital ou certificado de identidade, é um documento eletrônico usado para provar a propriedade de uma chave pública. O certificado inclui informações sobre a chave, informações sobre a identidade do seu proprietário (denominada entidade) e a assinatura digital de uma entidade que verificou o conteúdo do certificado (denominada emitente). Se a assinatura for válida e o software que examina o certificado confiar no emissor, ele poderá usar essa chave para se comunicar com segurança com o requerente do certificado.

P.Instalei o certificado, por que ele não funciona?
R.Isso pode ser devido a muitas razões, por exemplo:

1. O certificado e o ponto confiável estão configurados, mas não foram vinculados ao processo que deve usá-los. Por exemplo, o ponto confiável a ser usado não está vinculado à interface externa que termina os clientes Anyconnect.

2. Um arquivo PKCS12 está instalado, mas apresenta erros devido à ausência do certificado intermediário CA no arquivo PKCS12. Os clientes que têm o certificado intermediário de autoridade de certificação como confiável, mas não têm o certificado raiz de autoridade de certificação como confiável, não podem verificar toda a cadeia de certificados e relatar o certificado de identidade do servidor como não confiável.

3. Um certificado preenchido com atributos incorretos pode causar falha na instalação ou erros no lado do cliente. Por exemplo, determinados atributos podem ser codificados com o formato incorreto. Outro motivo é que o Certificado de Identidade não tem o SAN (Nome Alternativo da Entidade) ou o nome de domínio usado para acessar o servidor não está presente como uma SAN.

P. A instalação de um novo certificado requer uma janela de manutenção ou causa tempo de inatividade?
R. A instalação de um novo certificado (identidade ou CA) não é intrusiva e não deve causar tempo de inatividade ou exigir uma janela de manutenção. Permitir que um novo certificado seja usado para um serviço que existe é uma alteração e pode exigir uma janela de solicitação/manutenção de alteração.

P.A adição ou alteração de um certificado pode desconectar os usuários conectados?
R.Não, os usuários que estão conectados no momento permanecem conectados. O certificado é usado no estabelecimento da conexão. Quando os usuários se reconectarem, o novo certificado será usado.

P.Como posso criar um CSR com um curinga? Ou um nome alternativo para o assunto (SAN)?
R.Atualmente, o ASA/FTD não pode criar um CSR com curinga; no entanto, esse processo pode ser feito com o OpenSSL. Para gerar a chave CSR e ID, você pode executar os comandos:

```
openssl genrsa -out id.key 2048

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

Quando um ponto confiável é configurado com o atributo Fully Qualified Domain Name (FQDN), o CSR criado pelo ASA/FTD contém a SAN com esse valor. Mais atributos de SAN podem ser adicionados pela CA quando ela assina o CSR, ou o CSR pode ser criado com o OpenSSL

P.A substituição de certificado entra em vigor imediatamente?

R. O novo certificado de identidade do servidor é usado somente para as novas conexões. O novo certificado está pronto para ser usado imediatamente após a alteração, mas é usado com novas conexões.

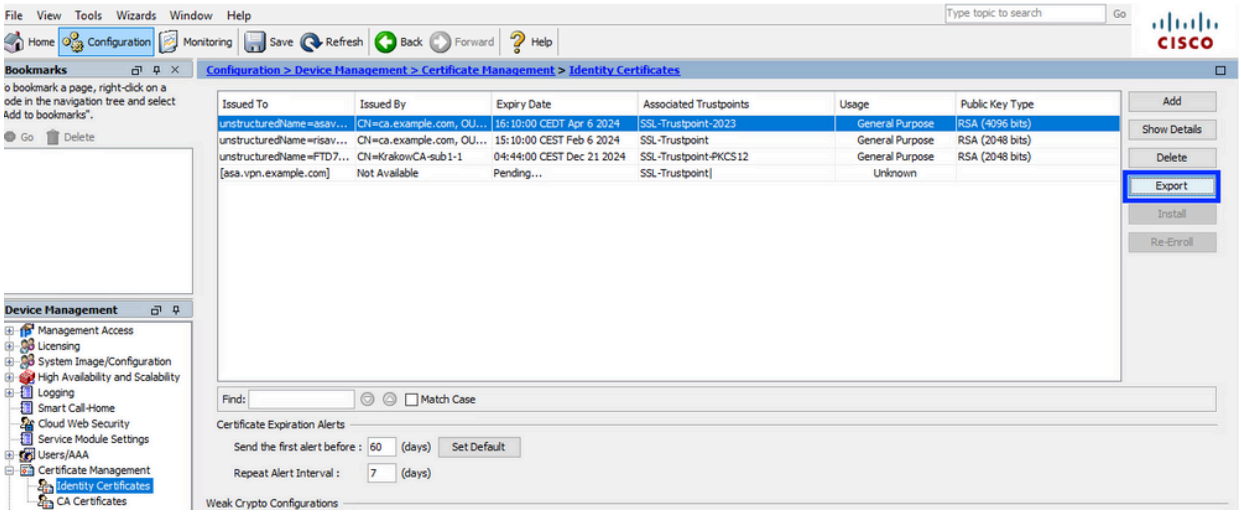
P.Como posso verificar se a instalação funcionou?
R.O comando CLI a ser verificado: show crypto ca cert <nome_do_ponto_de_confiança>

P.Como gerar PKCS12 a partir do Certificado de identidade, certificado CA e chave privada?
R. O PKCS12 pode ser criado com OpenSSL, com o comando:
openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

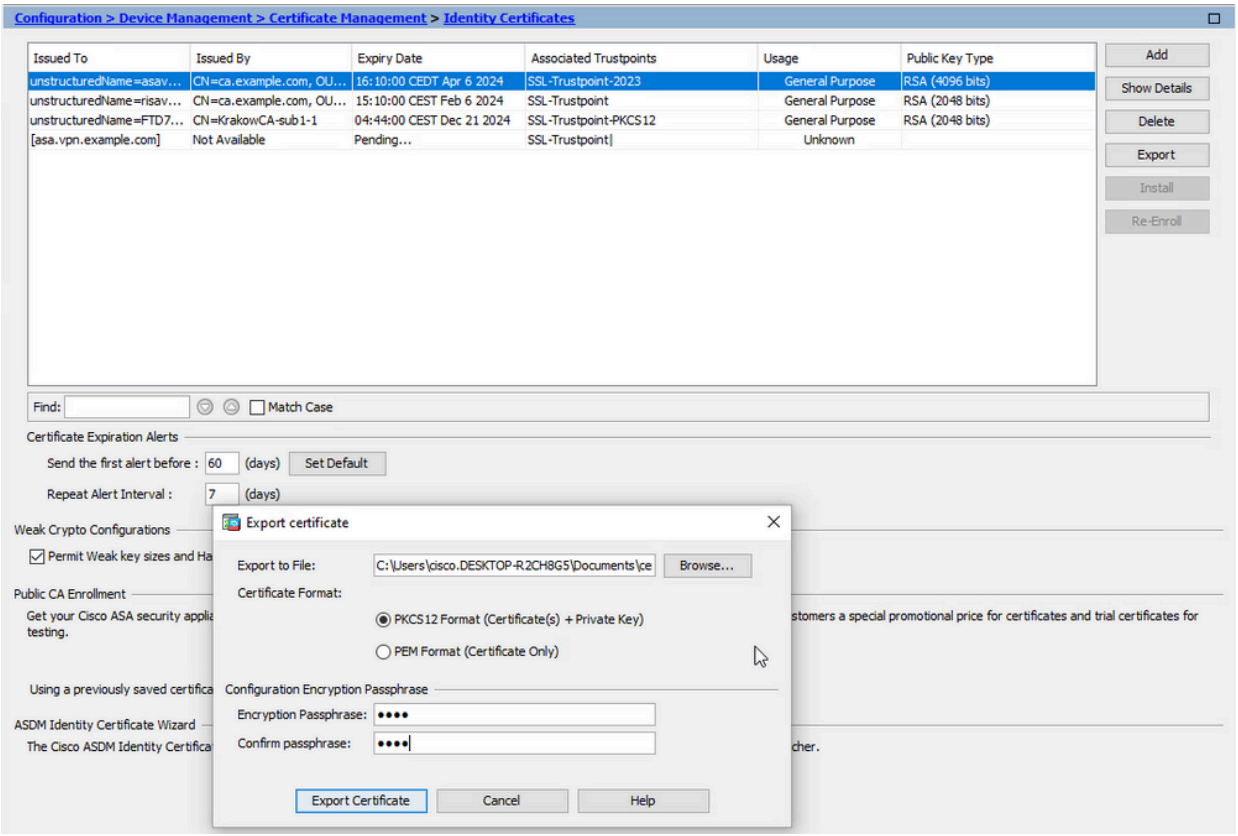
P. Como exportar um certificado para instalá-lo em um novo ASA?
A.

- Com CLI: use o comando: crypto ca export <nome_do_ponto_de_confiança> pkcs12 <senha>
- Com ASDM:

a. Navegue para Configuration > Device Management > Certificate Management > Identity Certificates e escolha o Identity Certificate. Clique em Exportar.



b. Escolha para onde exportar o arquivo, especifique a senha de exportação e clique em Export Certificate.



O certificado exportado pode estar no disco do computador. Por favor, anote a senha em um lugar seguro, o arquivo é inútil sem ele.

P.Se as chaves ECDSA forem usadas, o processo de geração de certificado SSL será diferente?
R.A única diferença na configuração é a etapa de geração do par de chaves, onde um par de chaves ECDSA pode ser gerado em vez de um par de chaves RSA. O restante do endereço permanece o mesmo.

P.É sempre necessário gerar um novo par de chaves?
R.A etapa de geração do par de chaves é opcional. O par de chaves existente pode ser usado ou, no caso de PKCS12, o par de chaves é importado com o certificado. Consulte a seção Selecionar o Nome do Par de Chaves para o respectivo tipo de inscrição/reinscrição.

P.É seguro gerar um novo par de chaves para um novo certificado de identidade?
R.O processo é seguro desde que um novo nome de par de chaves seja usado. Nesse caso, os antigos Pares de Chave não são alterados.

P.É necessário gerar a chave novamente quando um firewall é substituído (como RMA)?
R.O novo firewall por design não tem Pares de chaves presentes no firewall antigo.
O backup da configuração atual não contém os Pares de Chaves.
O backup completo feito com o ASDM pode conter os Pares de Chaves.
Os certificados de identidade podem ser exportados de um ASA com ASDM ou CLI, antes de falhar.

No caso do par de failover, os certificados e os pares de chaves são sincronizados com uma unidade em espera com o comando write standby. No caso de um nó do par de failover ser substituído, é suficiente configurar o failover básico e enviar a configuração para o novo dispositivo.
Caso um par de chaves seja perdido com o dispositivo e não haja backup, um novo certificado precisa ser assinado com o par de chaves presente no novo dispositivo.

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.