Installation und Verlängerung von Zertifikaten auf von ASDM verwalteter ASA

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie bestimmte Zertifikatstypen auf der mit ASDM verwalteten Cisco ASA-Software anfordern, installieren, als vertrauenswürdig einstufen und verlängern.

Voraussetzungen

Anforderungen

- Vergewissern Sie sich vor dem Start, dass die Adaptive Security Appliance (ASA) über die richtige Uhrzeit, das richtige Datum und die richtige Zeitzone verfügt. Für die Zertifikatsauthentifizierung wird die Verwendung eines NTP-Servers (Network Time Protocol) empfohlen, um die Uhrzeit auf der ASA zu synchronisieren. Weitere Informationen finden Sie unter Zugehörige Informationen.
- Um ein Zertifikat anzufordern, das eine CSR-Anfrage (Certificate Signing Request) verwendet, muss es Zugriff auf eine vertrauenswürdige interne Zertifizierungsstelle oder eine Zertifizierungsstelle eines Drittanbieters haben. Zu den CA-Anbietern von Drittanbietern gehören u. a. Entrust, Geotrust, GoDaddy, Thawte und VeriSign.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ASA v9.18.1
- Für die PKCS12-Erstellung wird OpenSSL verwendet.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Folgende Zertifikatstypen werden in diesem Dokument adressiert:

- selbstsignierte Zertifikate
- Zertifikate, die von einer Zertifizierungsstelle oder internen Zertifizierungsstelle eines Drittanbieters unterzeichnet wurden

Die Secure Socket Layer (SSL)-, Transport Layer Security (TLS)- und IKEv2 rfc7296 für EAP-Authentifizierungsprotokolle erfordern, dass der SSL/TLS/IKEv2-Server dem Client ein Serverzertifikat für den Client bereitstellt, damit dieser die Serverauthentifizierung durchführen kann. Es wird empfohlen, vertrauenswürdige Zertifizierungsstellen von Drittanbietern zu verwenden, um SSL-Zertifikate an die ASA auszustellen.

Cisco empfiehlt die Verwendung eines selbstsignierten Zertifikats nicht, da die Möglichkeit besteht, dass ein Benutzer versehentlich einen Browser so konfigurieren kann, dass er einem Zertifikat eines nicht autorisierten Servers vertraut. Für Benutzer ist es zudem unpraktisch, auf eine Sicherheitswarnung reagieren zu müssen, wenn sie eine Verbindung mit dem sicheren Gateway herstellen.

Anfordern und Installieren eines neuen Identitätszertifikats mit ASDM

Ein Zertifikat kann von einer Zertifizierungsstelle angefordert und auf einem ASA auf zwei Arten installiert werden:

- Verwenden der Zertifikatsanforderung (CSR) Generieren Sie ein Schlüsselpaar, fordern Sie ein Identitätszertifikat von der Zertifizierungsstelle mit einem CSR an, installieren Sie das signierte Identitätszertifikat, das Sie von der Zertifizierungsstelle erhalten haben.
- Verwenden Sie eine PKCS12-Datei, die von einer CA abgerufen oder von einem anderen Gerät exportiert wurde. Die PKCS12-Datei enthält Schlüsselpaar, Identitätszertifikat, Zertifizierungsstellenzertifikat(e).

Anfordern und Installieren eines neuen Identitätszertifikats mit Zertifikatsanforderung (Certificate Signing Request, CSR)

Eine CSR-Anfrage wird auf dem Gerät erstellt, für das ein Identitätszertifikat erforderlich ist. Verwenden Sie dazu ein auf dem Gerät erstelltes Schlüsselpaar.

Ein CSR enthält:

- Informationen zur Zertifikatanforderung - angeforderter Betreff und andere Attribute, öffentlicher Schlüssel vom Schlüsselpaar,
- Informationen über den Signaturalgorithmus,
- digitale Signatur der Zertifikatanforderungsinformationen, signiert mit dem privaten Schlüssel des Schlüsselpaars.

Der CSR wird an die Zertifizierungsstelle (Certificate Authority, CA) übergeben, damit diese ihn in einem PKCS#10-Formular signiert.

Das signierte Zertifikat wird von der Zertifizierungsstelle in PEM-Form zurückgegeben.

Hinweis: Die CA kann die Parameter für den FQDN und den Antragstellernamen ändern, die

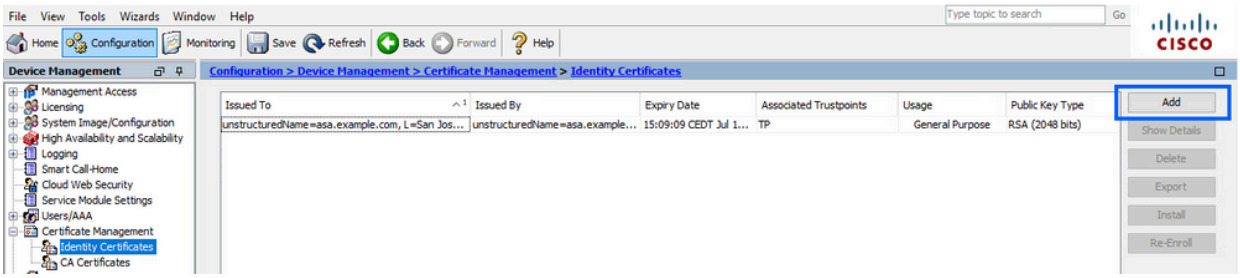
---

im Vertrauenspunkt definiert sind, wenn sie den CSR signiert und ein signiertes Identitätszertifikat erstellt.

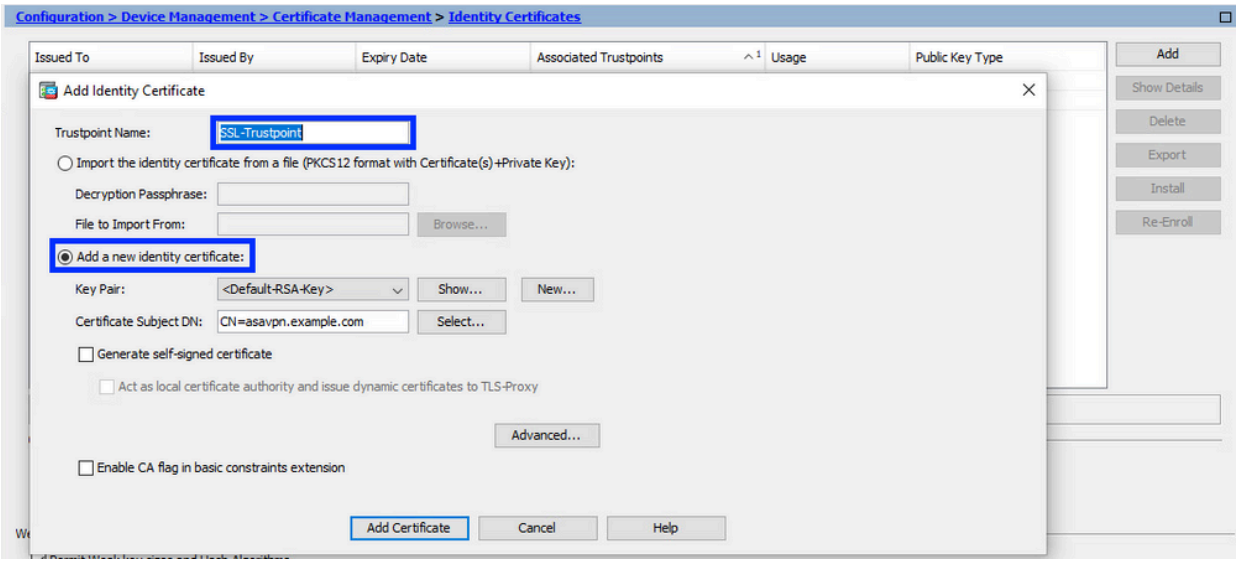
Erstellen eines CSR mit ASDM

1. Erstellen eines Vertrauenspunkts mit einem bestimmten Namen

   a. Navigieren Sie zu Konfiguration > Geräteverwaltung > Zertifikatsverwaltung > Identitätszertifikate.



   b. Klicken Sie auf Hinzufügen.
   c. Definieren Sie einen Vertrauenspunktnamen.

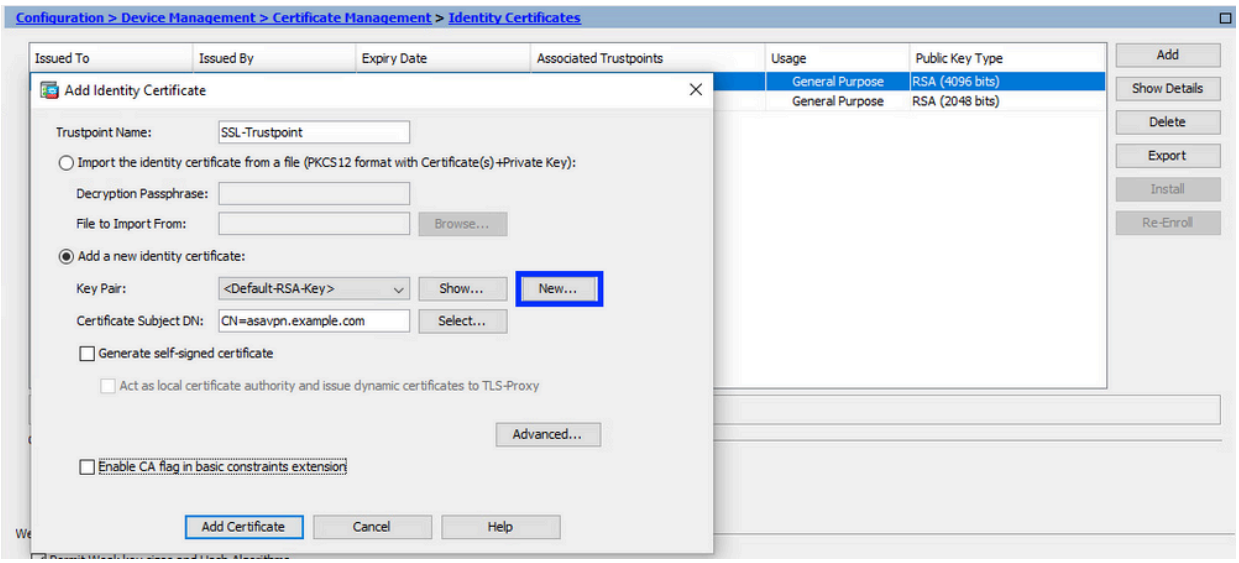


   d. Klicken Sie auf das Optionsfeld Neues Identitätszertifikat hinzufügen.

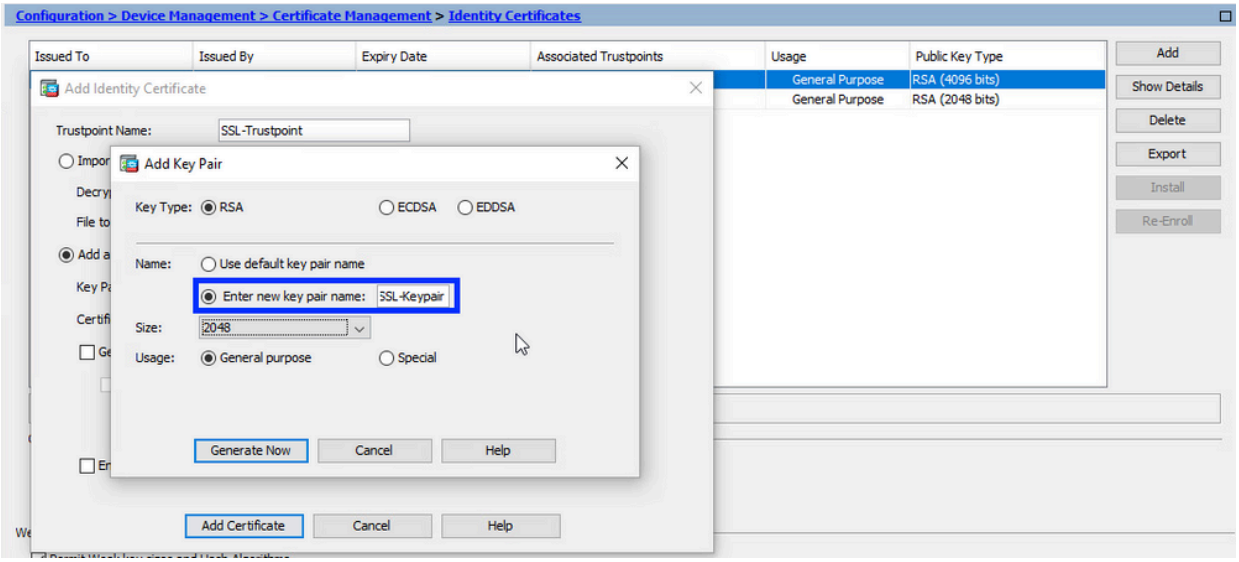
2. (Optional) Erstellen eines neuen Schlüsselpaars

> Hinweis: Standardmäßig wird der RSA-Schlüssel mit dem Namen Default-RSA-Key und einer Größe von 2048 verwendet. Es wird jedoch empfohlen, für jedes Identitätszertifikat ein eindeutiges privates/öffentliches Schlüsselpaar zu verwenden.

   a. Klicken Sie auf Neu, um ein neues Schlüsselpaar zu generieren.

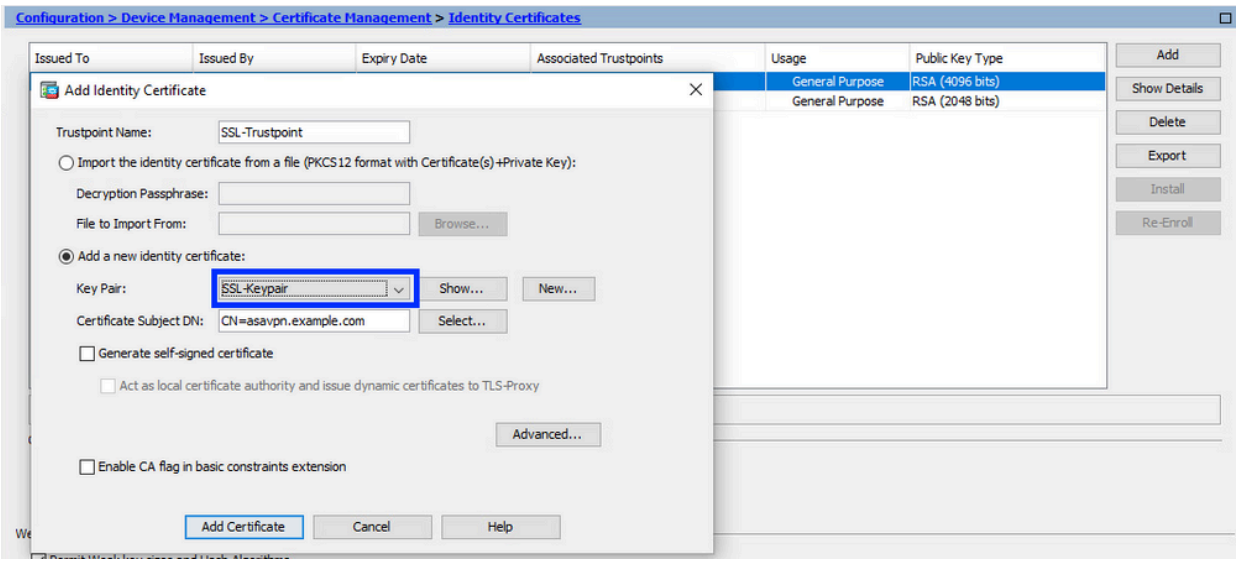


b. Wählen Sie die Option Neuen Schlüsselpaarnamen eingeben und geben Sie einen Namen für das neue Schlüsselpaar ein.
c. Wählen Sie den Schlüsseltyp aus - RSA oder ECDSA.
d. Wählen Sie die Schlüssellänge aus; für RSA wählen Sie Allgemeiner Verwendungszweck.
e. Klicken Sie auf Jetzt generieren. Das Schlüsselpaar wird nun erstellt.



3. Wählen Sie den Namen des Schlüsselpaars aus.

Wählen Sie das Schlüsselpaar aus, mit dem der CSR signiert und mit dem neuen Zertifikat verknüpft werden soll.



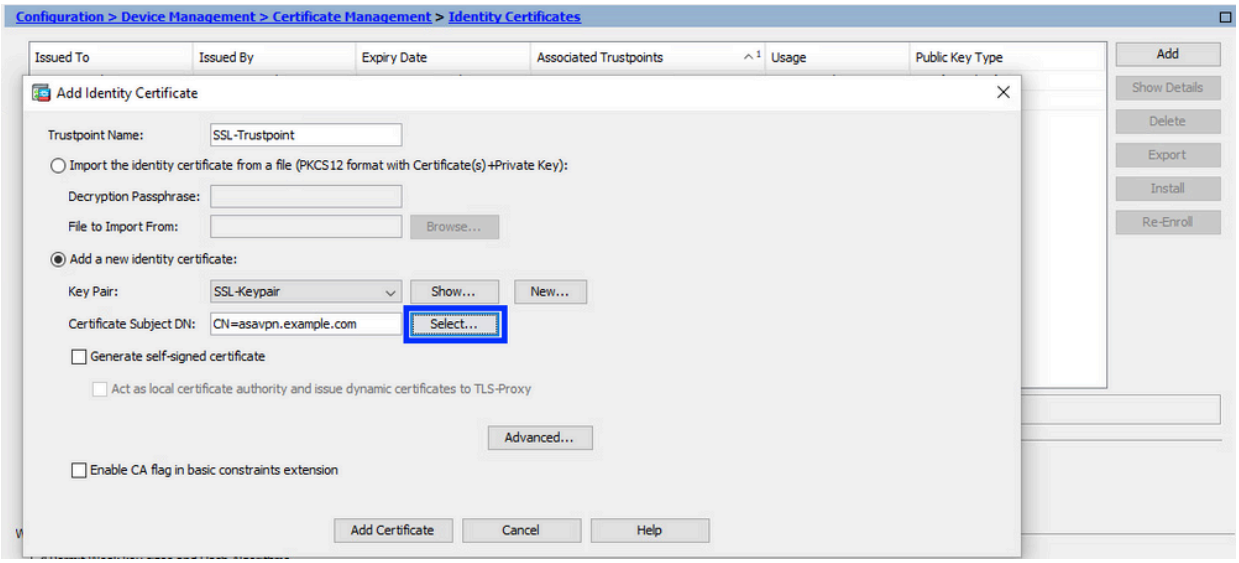
4. Zertifikatantragsteller und vollständig qualifizierter Domänenname (FQDN) konfigurieren

---

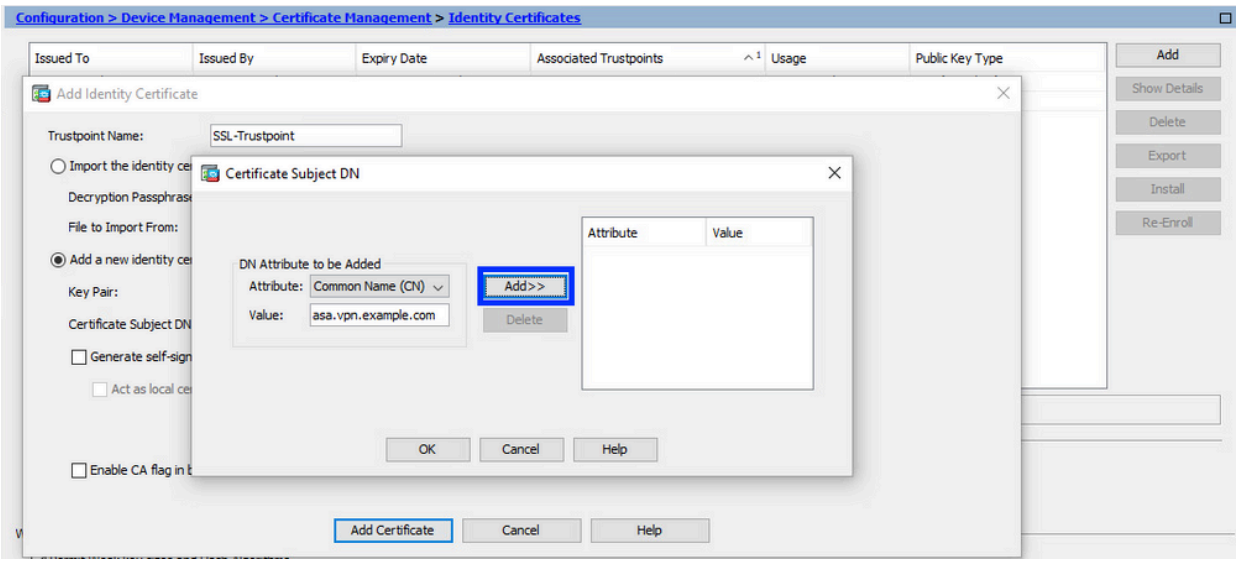
Achtung: Der FQDN-Parameter muss mit dem FQDN oder der IP-Adresse der ASA-Schnittstelle übereinstimmen, für die das Identitätszertifikat verwendet wird. Dieser Parameter legt die angeforderte SAN-Erweiterung (Subject Alternative Name) für das Identitätszertifikat fest. Die SAN-Erweiterung wird vom SSL/TLS/IKEv2-Client verwendet, um zu überprüfen, ob das Zertifikat mit dem FQDN übereinstimmt, mit dem es verbunden wird.

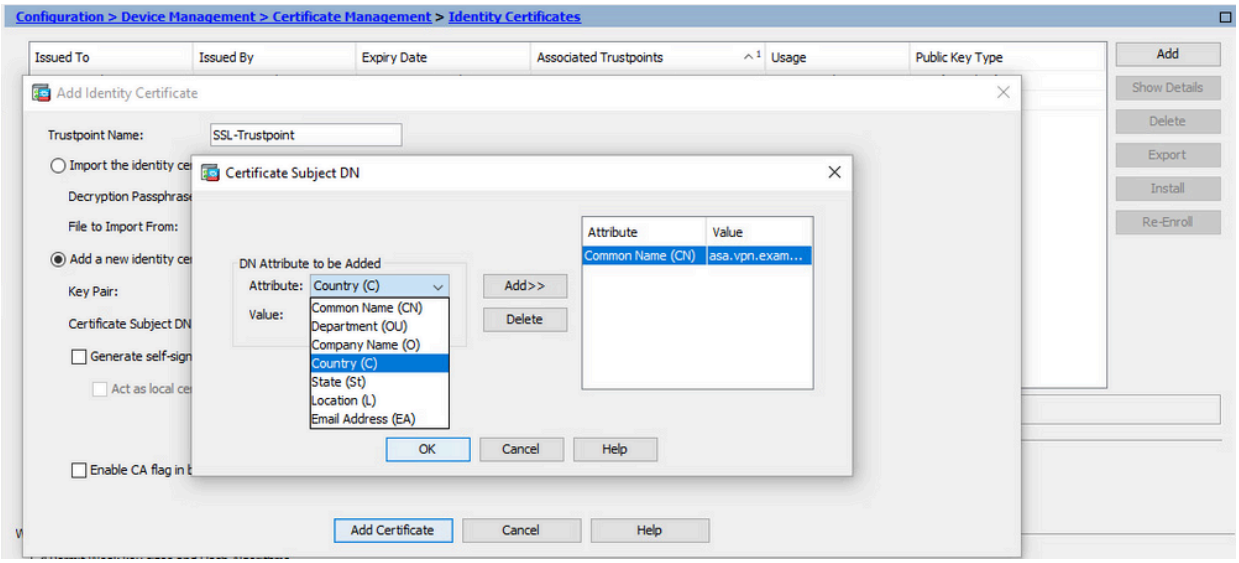
---

a. Klicken Sie auf Auswählen.



b. Konfigurieren Sie im Fenster Zertifikatantragsteller-DN Zertifikatattribute. Wählen Sie ein Attribut aus der Dropdown-Liste aus, geben Sie den Wert ein, und klicken Sie auf Hinzufügen.



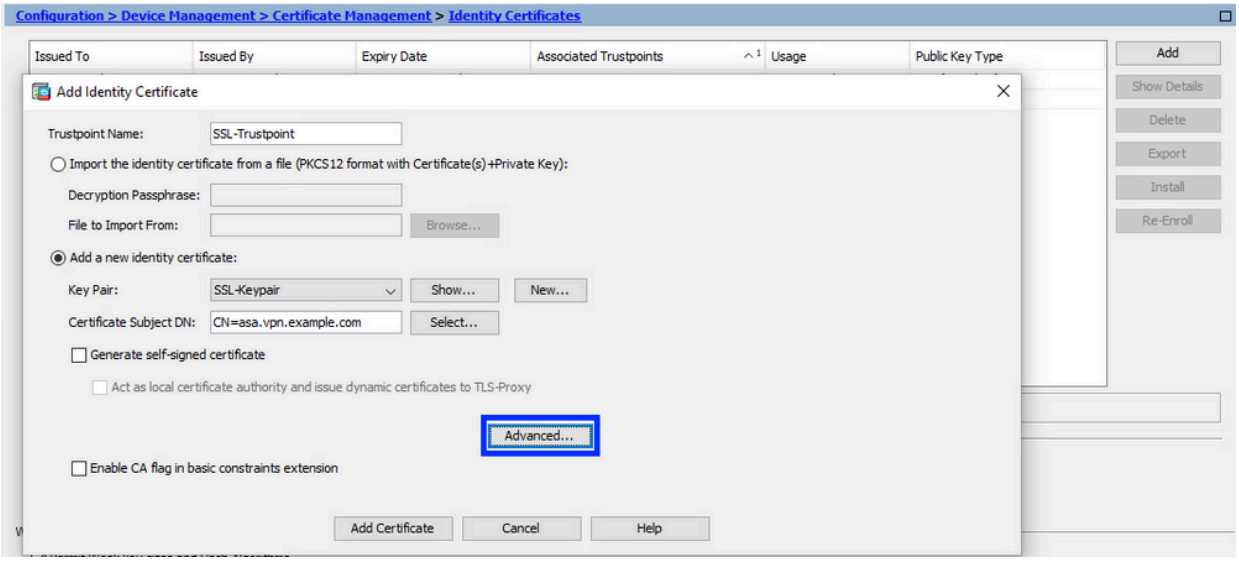


Attribut	Beschreibung
KN	Der Name, über den auf die Firewall zugegriffen werden kann (normalerweise der vollqualifizierte Domänenname, z. B. vpn.example.com).
OU	Der Name Ihrer Abteilung innerhalb der Organisation.
O	Der gesetzlich registrierte Name Ihrer Organisation/Ihres Unternehmens
C	Landesvorwahl (Code aus 2 Buchstaben ohne Interpunktion)
ST	Der Status, in dem sich Ihre Organisation befindet.
L	Die Stadt, in der Ihre Organisation ansässig ist.
EA	Email-Adresse

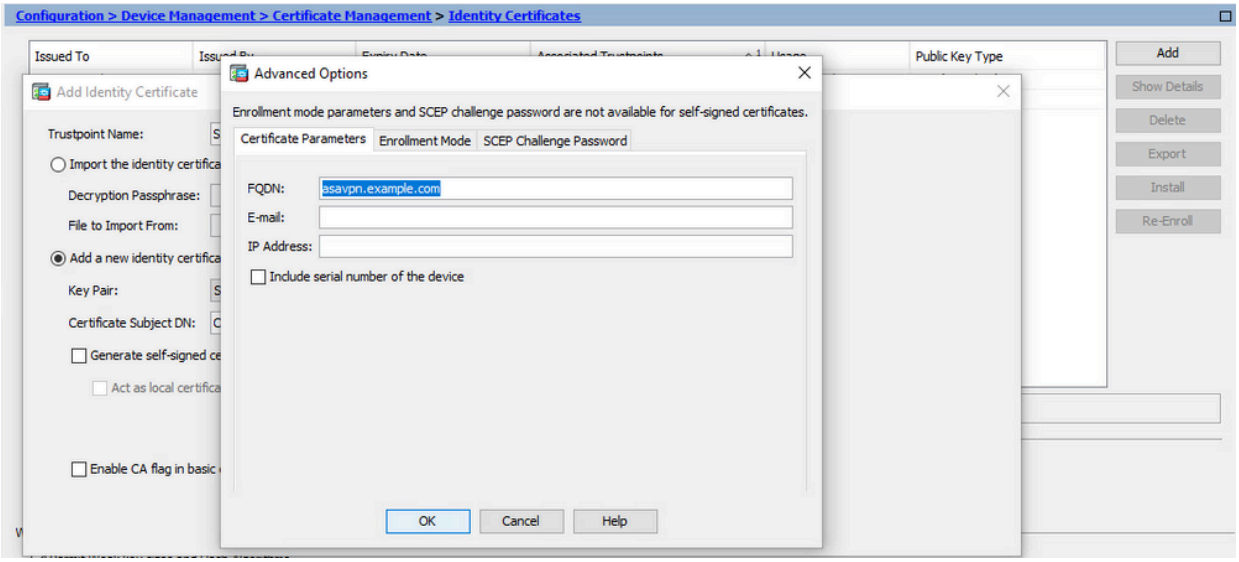
Hinweis: Keiner der vorherigen Feldwerte darf mehr als 64 Zeichen enthalten. Ein größerer Wert kann zu Problemen bei der Installation des Identitätszertifikats führen. Außerdem müssen nicht alle DN-Attribute definiert werden.

Klicken Sie nach Hinzufügen aller Attribute auf OK.

c. Konfigurieren Sie den FQDN des Geräts: Klicken Sie auf Erweitert.

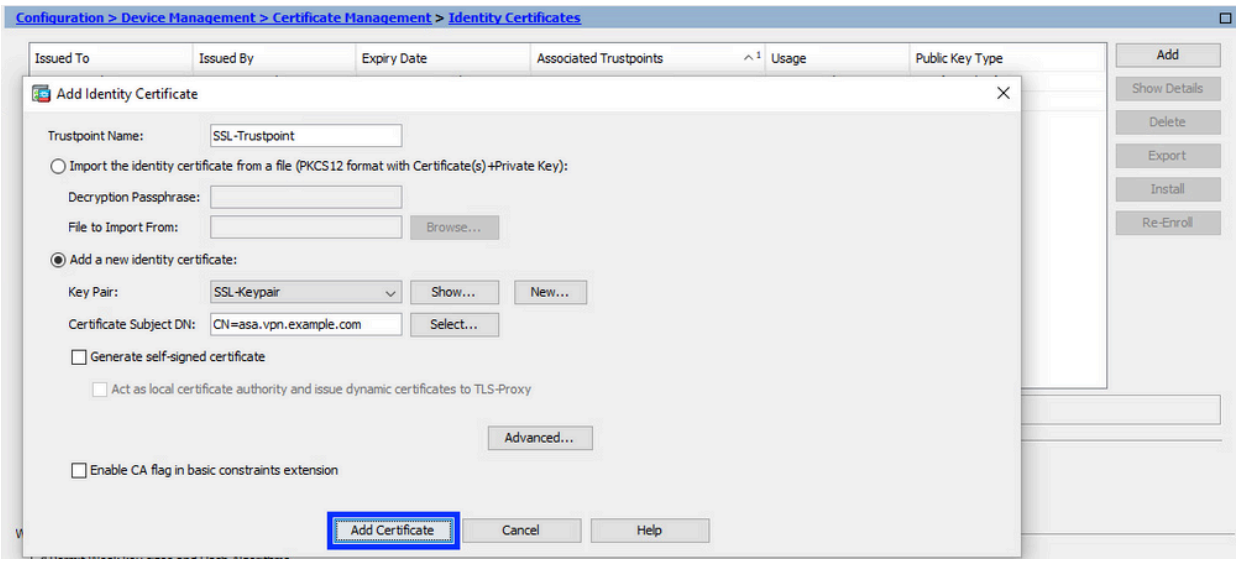


d. Geben Sie im Feld FQDN den vollqualifizierten Domänennamen ein, über den das Gerät vom Internet aus erreichbar ist. Klicken Sie auf OK.

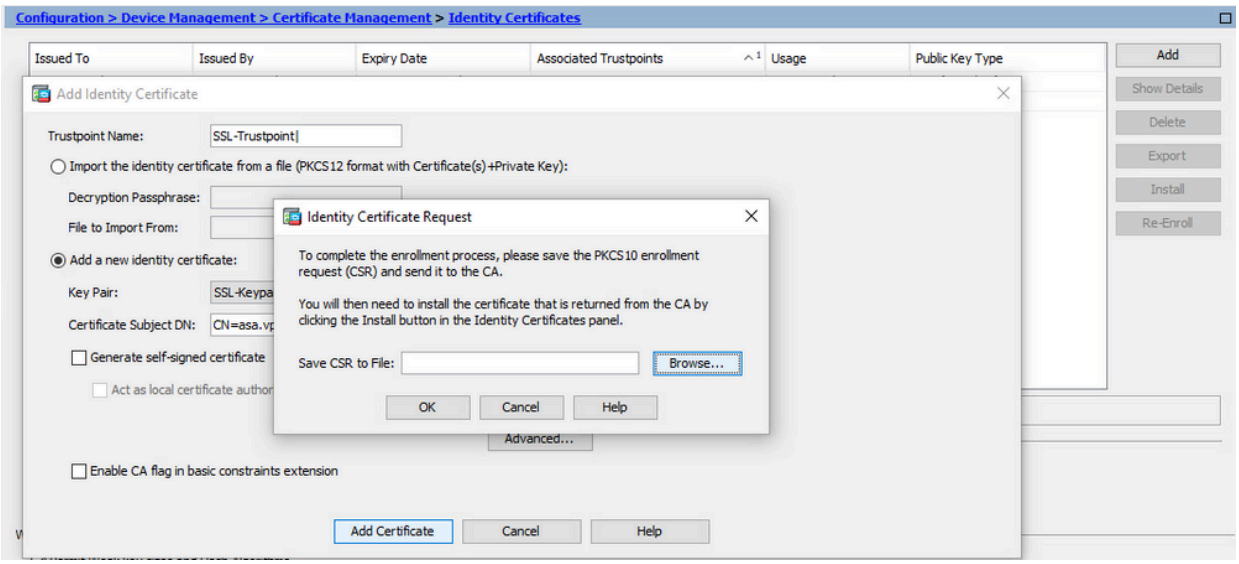


5. Erstellen und Speichern der CSR-Anfrage

a. Klicken Sie auf Zertifikat hinzufügen.



b. Es wird eine Aufforderung angezeigt, den CSR in einer Datei auf dem lokalen Computer zu speichern.

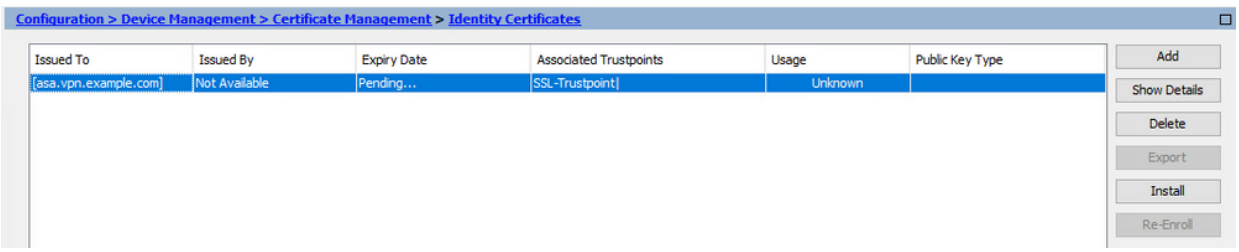


Klicken Sie auf Durchsuchen, wählen Sie einen Speicherort für die CSR-Datei aus, und speichern Sie die Datei mit der Erweiterung .txt.

Hinweis: Wenn die Datei mit der Erweiterung .txt gespeichert wird, kann die PKCS#10-Anforderung geöffnet und mit einem Texteditor (z. B. Editor) angezeigt werden.

---

c. Jetzt wird der neue Vertrauenspunkt im Status Ausstehend angezeigt.

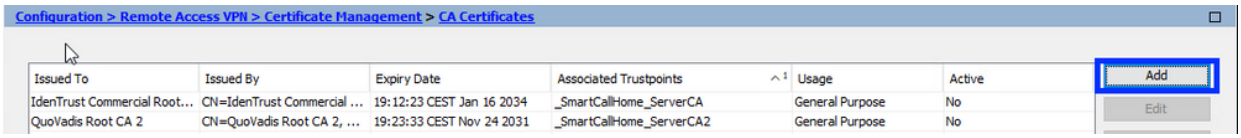


Installieren des Identitätszertifikats im PEM-Format mit ASDM

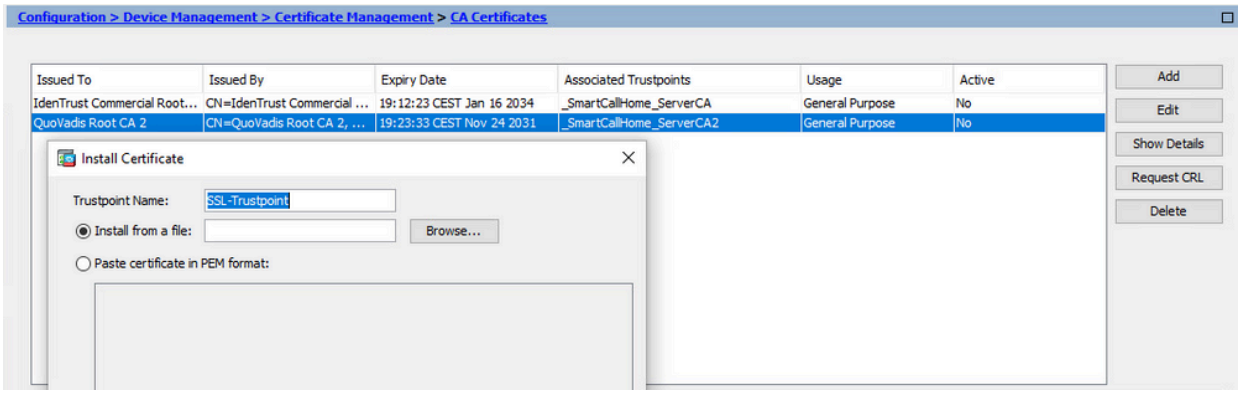
Bei den Installationsschritten wird davon ausgegangen, dass die Zertifizierungsstelle den CSR signiert und ein PEM-codiertes Identitätszertifikat- und Zertifizierungsstellen-Zertifikatpaket (.pem, .cer, .crt) bereitgestellt hat.

1. Installieren des Zertifizierungsstellenzertifikats, das den CSR signiert hat

   a. Navigieren Sie zu Configuration > Device Management > Certificate Management >, und wählen Sie CA Certificates aus. Klicken Sie auf Hinzufügen.



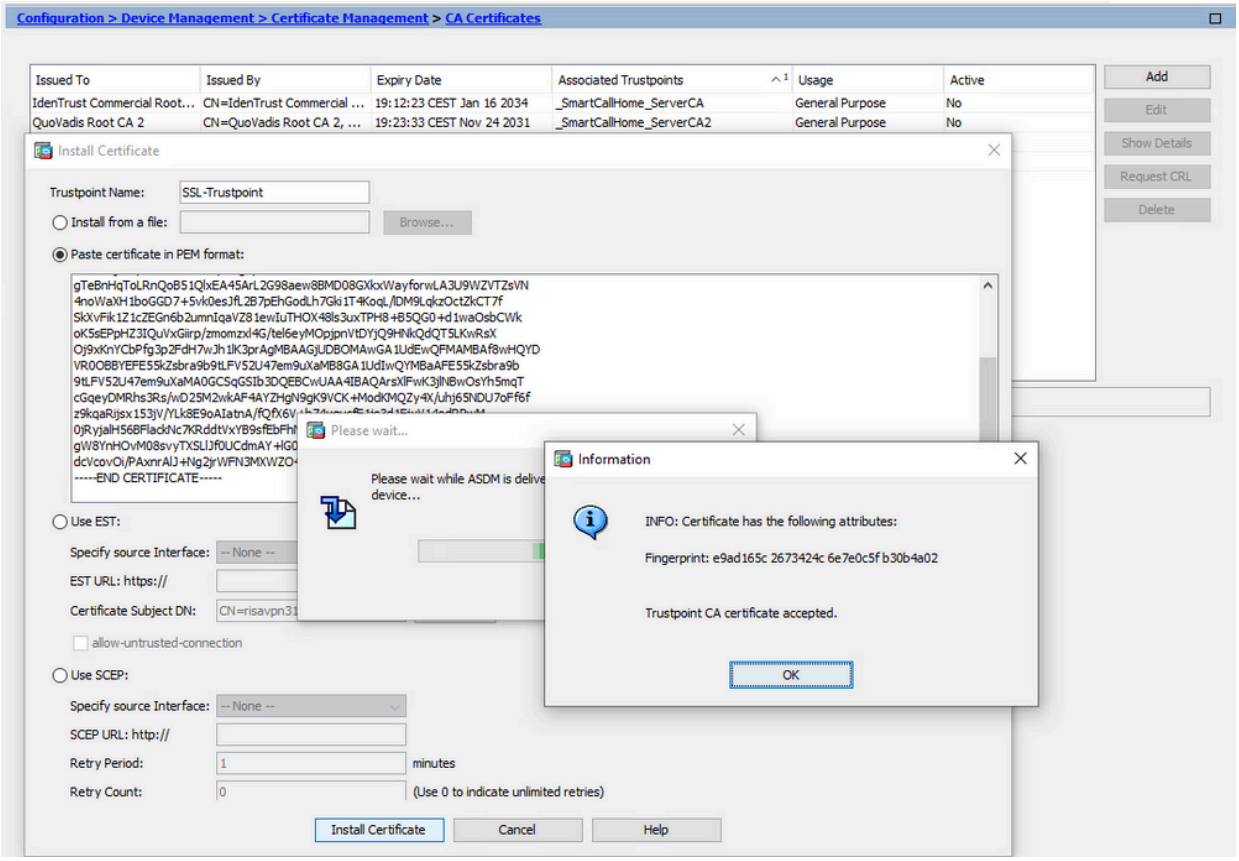
   b. Geben Sie den Namen des Vertrauenspunkts ein, wählen Sie Install From File (Von Datei installieren) aus, klicken Sie auf Browse (Durchsuchen), und wählen Sie das Zwischenzertifikat aus. Sie können auch das PEM-codierte CA-Zertifikat aus einer Textdatei in das Textfeld einfügen.



Hinweis: Installieren Sie das Zertifizierungsstellenzertifikat, das den CSR signiert hat, und verwenden Sie den gleichen Namen für den Vertrauenspunkt wie das Identitätszertifikat. Die anderen Zertifizierungsstellenzertifikate weiter oben in der PKI-Hierarchie können in separaten Vertrauenspunkten installiert werden.

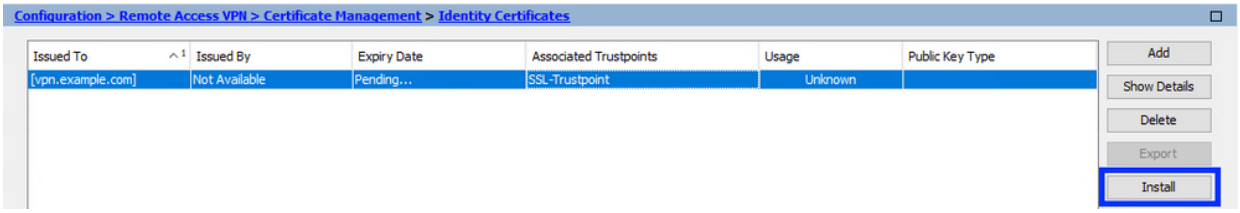
---

   c. Klicken Sie auf Zertifikat installieren.



2. Identitätszertifikat installieren

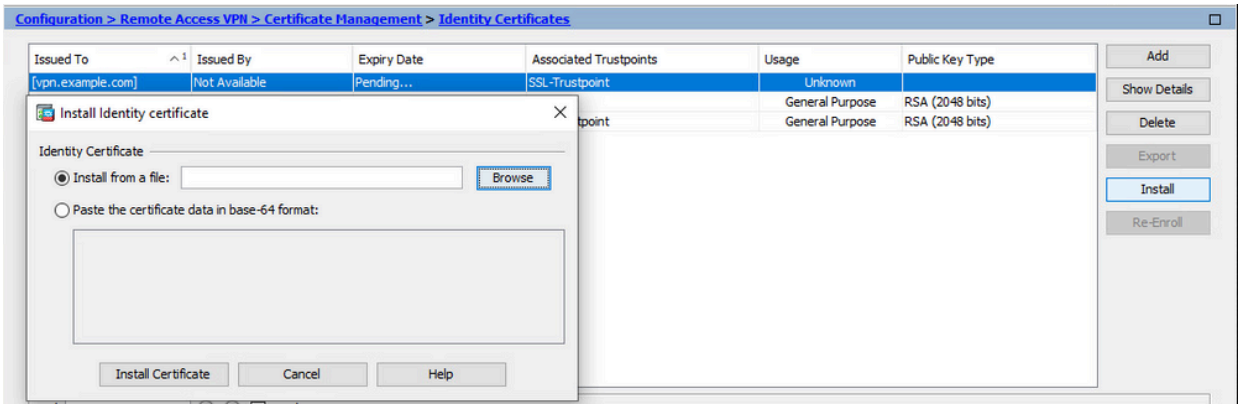
a. Wählen Sie das Identitätszertifikat aus, das zuvor während der CSR-Generierung erstellt wurde. Klicken Sie auf Install (Installieren).



Hinweis: Das Identitätszertifikat kann im Feld "Ausgestellt von" den Wert "Nicht verfügbar" und im Feld "Ablaufdatum" den Wert "Ausstehend" aufweisen. (Möglicherweise auf Englisch).

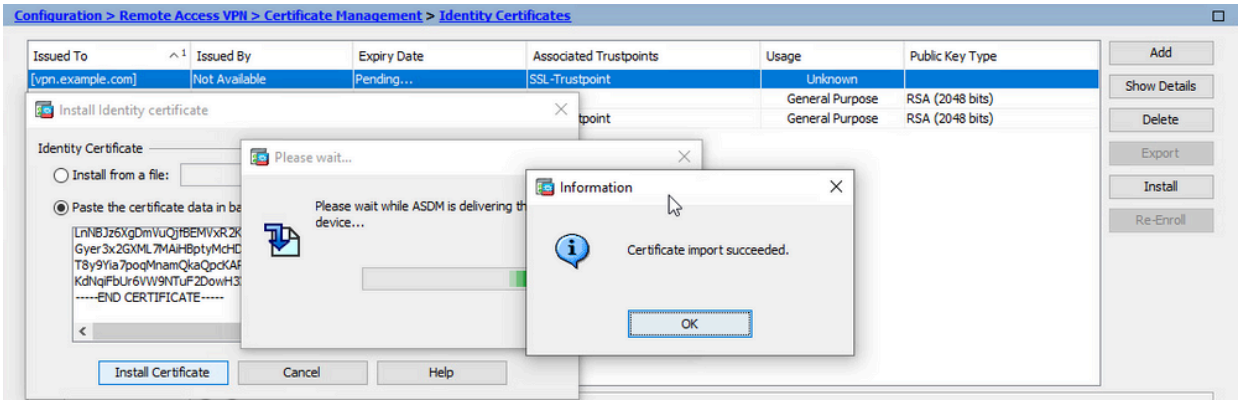
---

b. Wählen Sie eine Datei aus, die das von der Zertifizierungsstelle empfangene PEM-codierte Identitätszertifikat enthält, oder öffnen Sie das PEM-codierte Zertifikat in einem Texteditor, und kopieren Sie das von der Zertifizierungsstelle bereitgestellte Identitätszertifikat, und fügen Sie es in das Textfeld ein.



Hinweis: Identitätszertifikate können im Format .pem, .cer oder .crt installiert werden.

c. Klicken Sie auf Zertifikat installieren.



3. Anbinden des neuen Zertifikats an eine ASDM-Schnittstelle

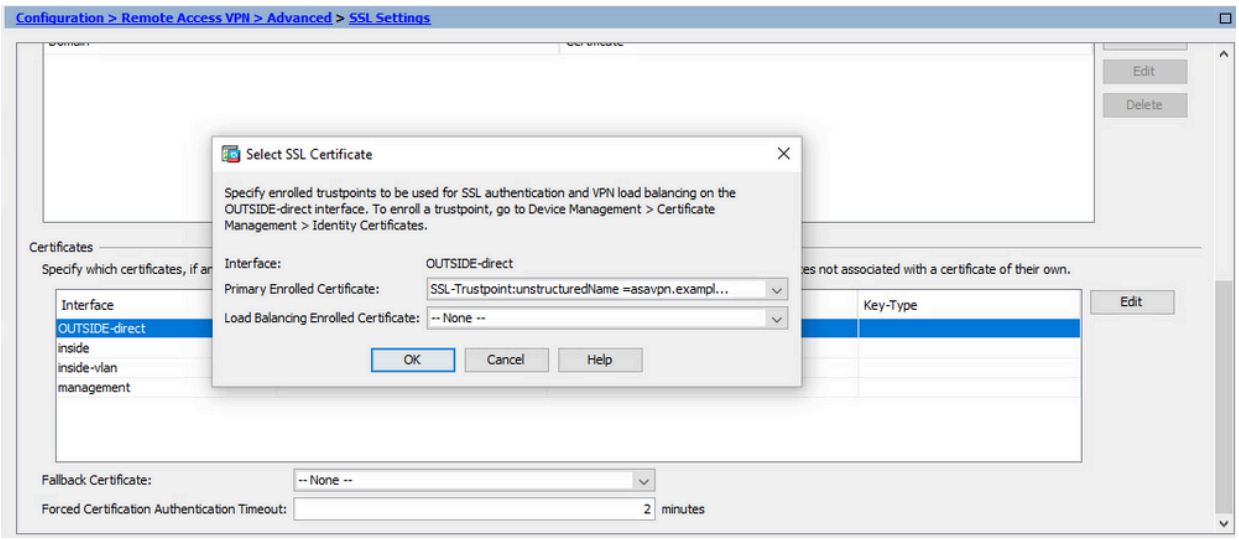
Die ASA muss so konfiguriert werden, dass das neue Identitätszertifikat für WebVPN-Sitzungen verwendet wird, die auf der angegebenen Schnittstelle enden.

a. Navigieren Sie zu Configuration > Remote Access VPN > Advanced > SSL Settings.

b. Wählen Sie unter Certificates (Zertifikate) die Schnittstelle aus, die zum Beenden von WebVPN-Sitzungen verwendet wird. In diesem Beispiel wird die externe Schnittstelle verwendet.

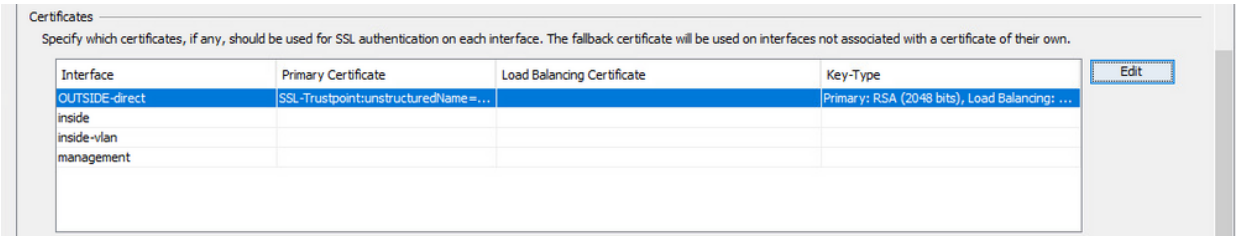
Klicken Sie auf Bearbeiten.

c. Wählen Sie in der Dropdown-Liste Zertifikat (Certificate) das neu installierte Zertifikat aus.



d. Klicken Sie auf OK.

e. Klicken Sie auf Apply (Anwenden).



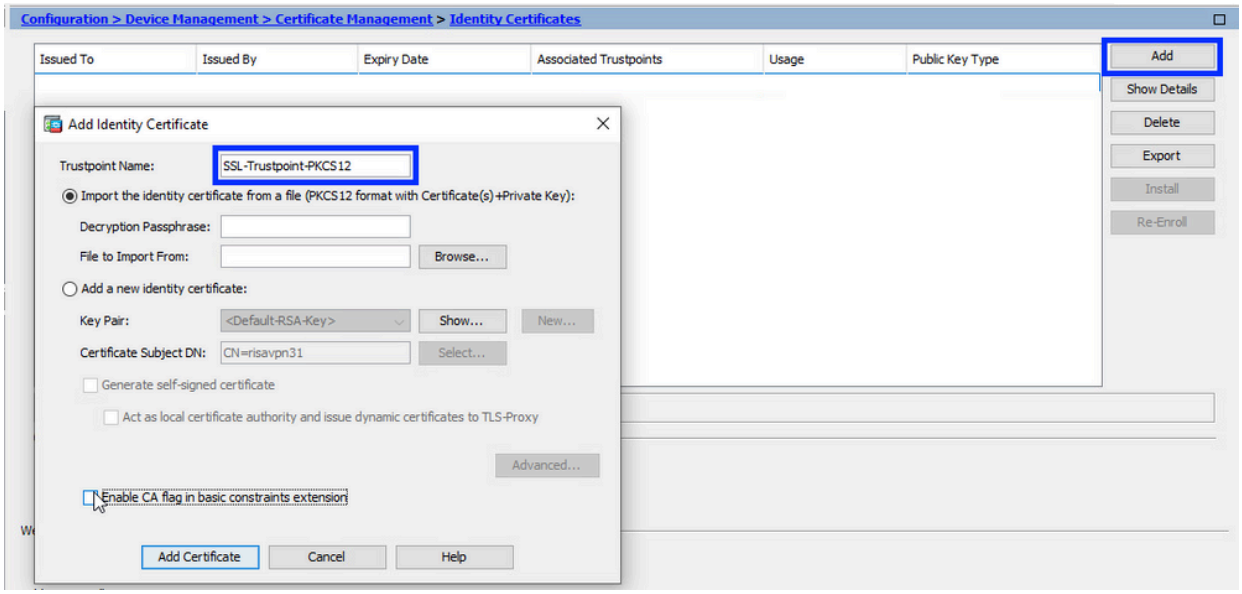
Jetzt wird das neue Identitätszertifikat verwendet.

Installieren eines im PKCS12-Format empfangenen Identitätszertifikats mit ASDM

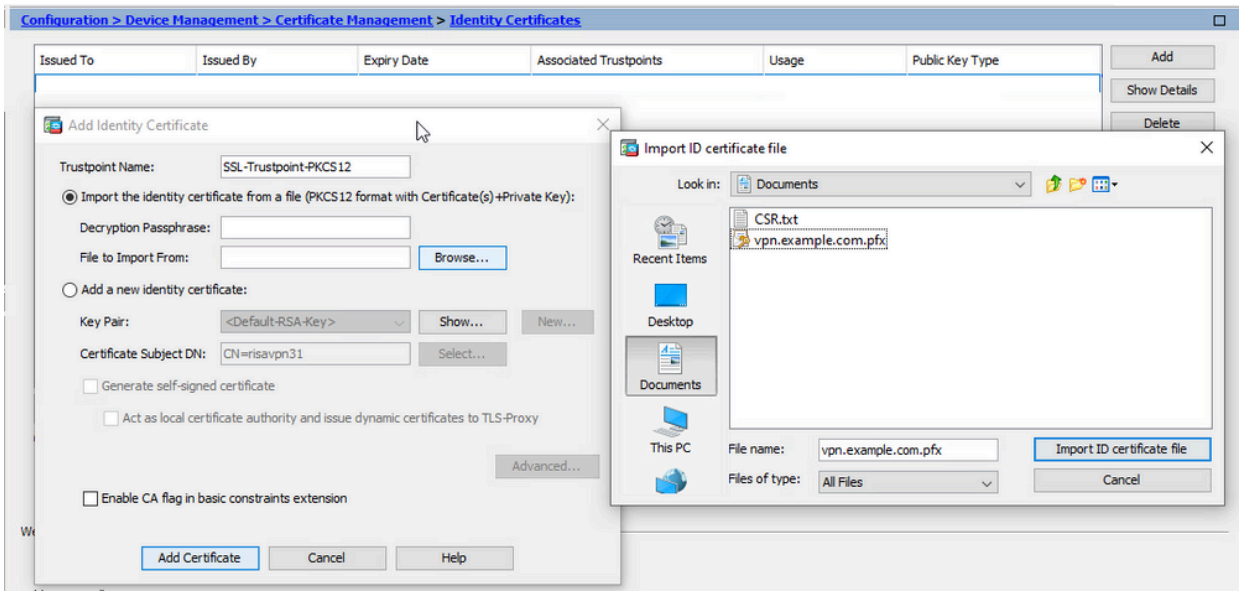
Die PKCS12-Datei (im .p12- oder .pfx-Format) enthält Identitätszertifikat, Schlüsselpaar und Zertifizierungsstellenzertifikat(e). Er wird von der Zertifizierungsstelle erstellt, z. B. im Falle eines Platzhalterzertifikats, oder von einem anderen Gerät exportiert. Es handelt sich um eine Binärdatei, die nicht mit einem Texteditor angezeigt werden kann.

1. Installieren der Identitäts- und Zertifizierungsstellenzertifikate aus einer PKCS12-Datei

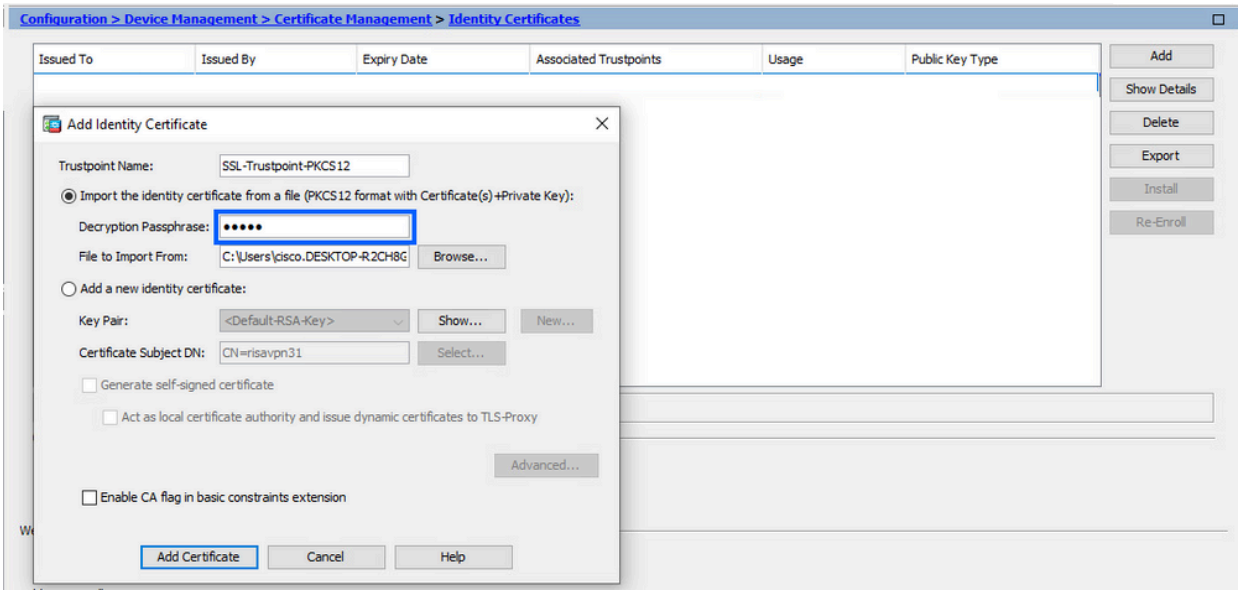
   Identitätszertifikat, Zertifizierungsstellenzertifikat(e) und Schlüsselpaar müssen in einer einzigen PKCS12-Datei gebündelt werden.
   a. Navigieren Sie zu Configuration > Device Management > Certificate Management, und wählen Sie Identity Certificates aus.
   b. Klicken Sie auf Hinzufügen.
   c. Geben Sie einen Vertrauenspunktnamen an.



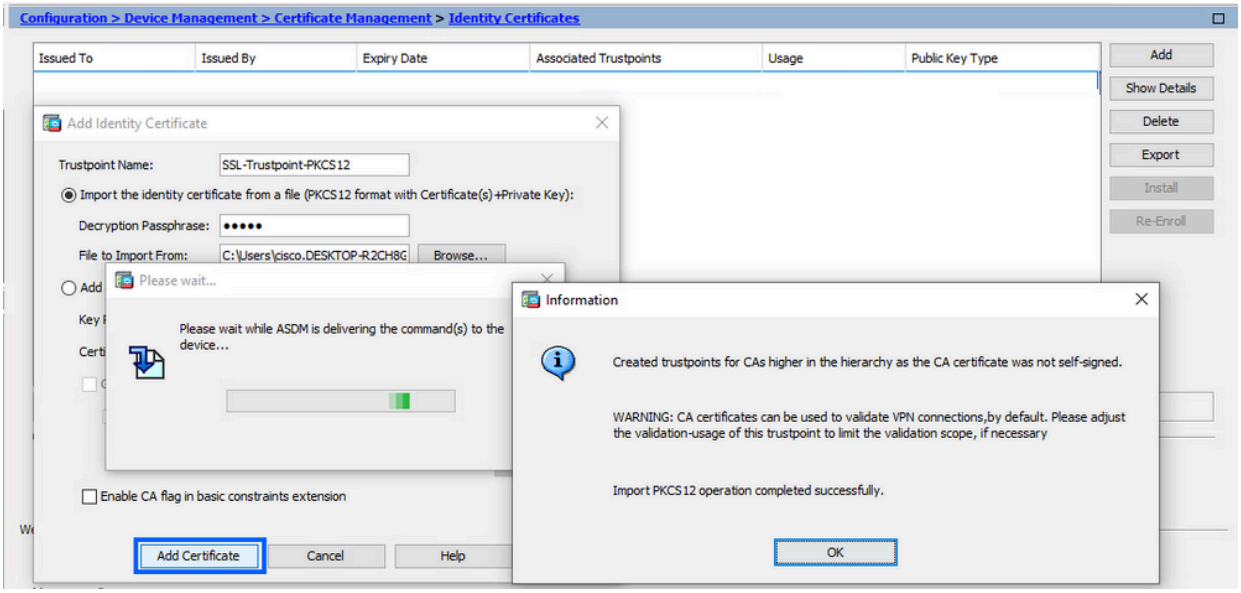
d. Klicken Sie auf das Optionsfeld Identitätszertifikat aus einer Datei importieren.



e. Geben Sie die Passphrase ein, die zum Erstellen der PKCS12-Datei verwendet wird.



f. Klicken Sie auf Zertifikat hinzufügen.



Hinweis: Wenn Sie eine PKCS12 mit Zertifizierungsstellen-Zertifikatkette importieren, erstellt der ASDM die Upstream-Zertifizierungsstellen-Vertrauenspunkte automatisch mit Namen mit dem Suffix "-Nummer".

Configuration > Remote Access VPN > Certificate Management > CA Certificates

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. Anbinden des neuen Zertifikats an eine ASDM-Schnittstelle

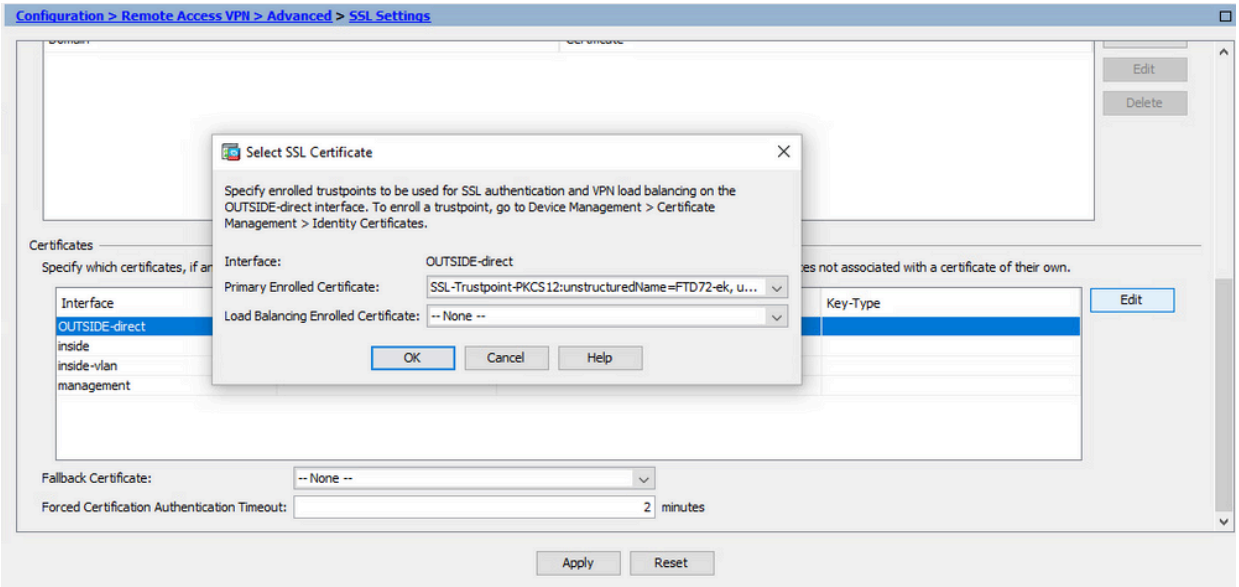
Die ASA muss so konfiguriert werden, dass das neue Identitätszertifikat für WebVPN-Sitzungen verwendet wird, die auf der angegebenen Schnittstelle enden.

a. Navigieren Sie zu Configuration > Remote Access VPN > Advanced > SSL Settings.

b. Wählen Sie unter Zertifikate die Schnittstelle aus, die zum Beenden von WebVPN-Sitzungen verwendet wird. In diesem Beispiel wird die externe Schnittstelle verwendet.

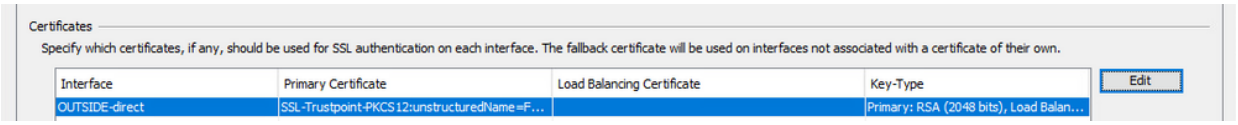
   Klicken Sie auf Bearbeiten.

c. Wählen Sie in der Dropdown-Liste Zertifikat (Certificate) das neu installierte Zertifikat aus.



d. Klicken Sie auf OK.

e. Klicken Sie auf Apply (Anwenden).



Jetzt wird das neue Identitätszertifikat verwendet.

Erneuerung des Zertifikats

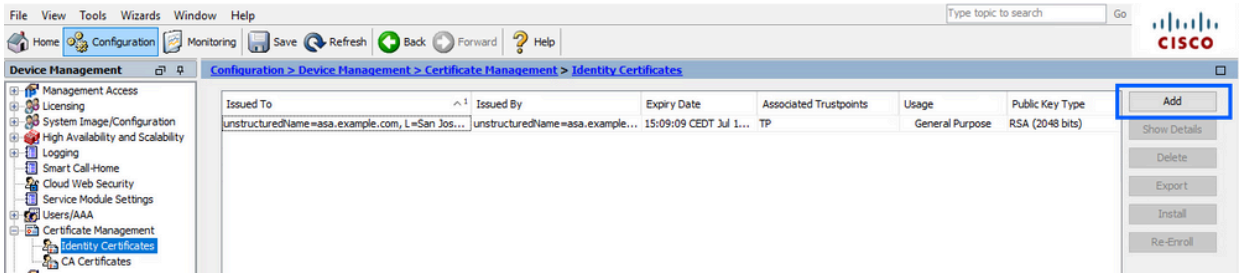
Erneuern eines Zertifikats, das für eine Zertifikatsanforderung (Certificate Signing Request, CSR) beim ASDM registriert ist

Für die Zertifikaterneuerung eines im CSR registrierten Zertifikats muss ein neuer Trustpoint erstellt und registriert werden. Sie muss einen anderen Namen haben (z. B. den alten Namen mit dem Suffix für das Registrierungsjahr). Es können die gleichen Parameter und das Schlüsselpaar wie das alte Zertifikat verwendet werden, oder es können verschiedene verwendet werden.

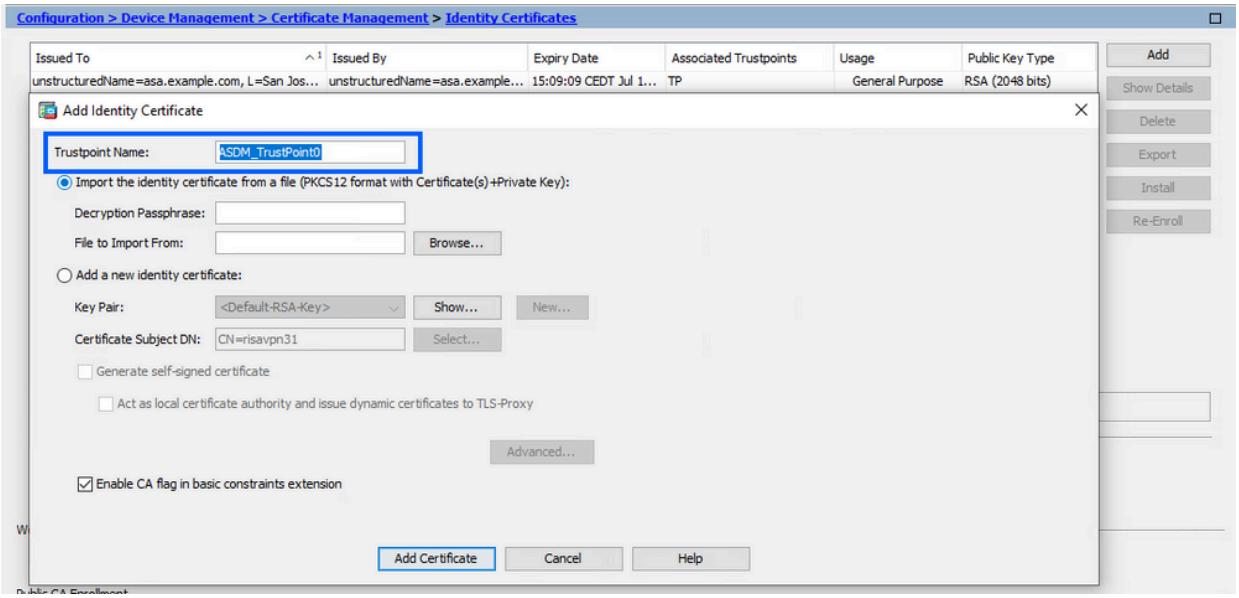
Erstellen eines CSR mit ASDM

1. Erstellen Sie einen neuen Vertrauenspunkt mit einem bestimmten Namen.

a. Navigieren Sie zu Konfiguration > Geräteverwaltung > Zertifikatsverwaltung > Identitätszertifikate.



b. Klicken Sie auf Hinzufügen.
c. Definieren Sie einen Vertrauenspunktnamen.



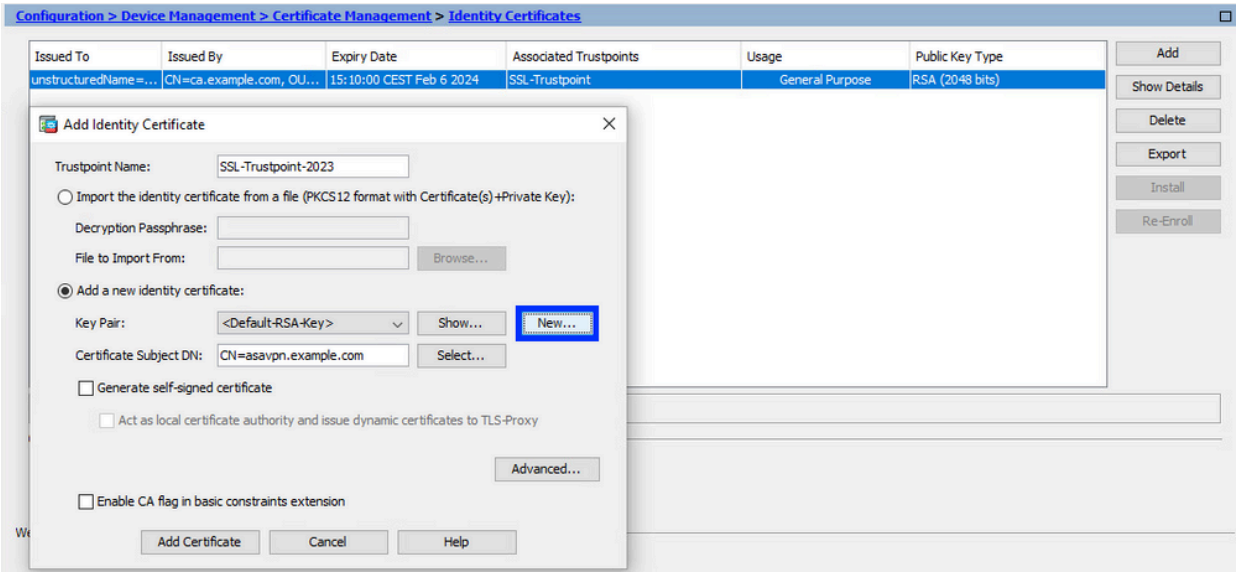
d. Klicken Sie auf das Optionsfeld Neues Identitätszertifikat hinzufügen.

2. (Optional) Erstellen eines neuen Schlüsselpaars

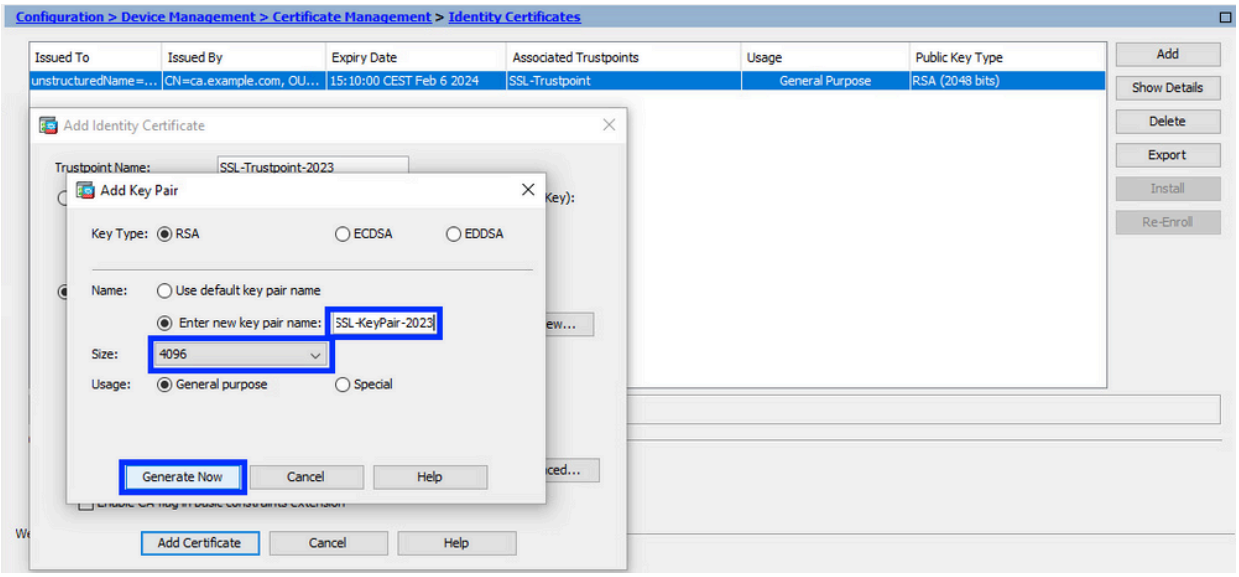
Hinweis: Standardmäßig wird der RSA-Schlüssel mit dem Namen Default-RSA-Key und einer Größe von 2048 verwendet. Es wird jedoch empfohlen, für jedes Identitätszertifikat ein eindeutiges privates/öffentliches Schlüsselpaar zu verwenden.

---

a. Klicken Sie auf Neu, um ein neues Schlüsselpaar zu generieren.

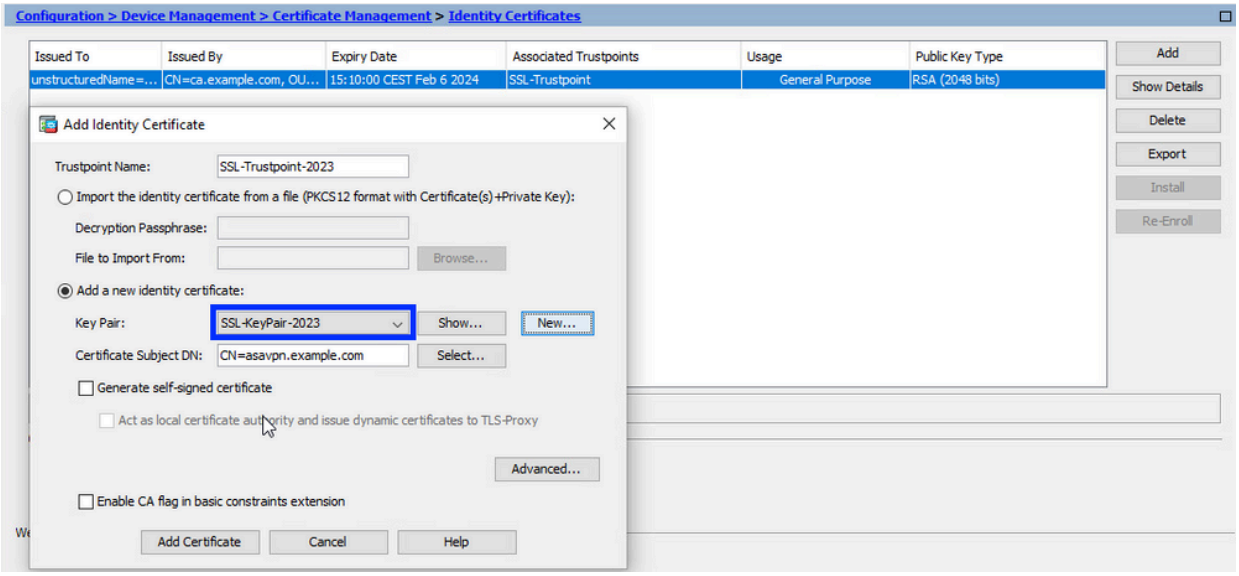


b. Wählen Sie die Option Neuen Schlüsselpaarnamen eingeben aus, und geben Sie einen Namen für das neue Schlüsselpaar ein.
c. Wählen Sie den Schlüsseltyp aus - RSA oder ECDSA.
d. Wählen Sie die Schlüssellänge aus. Wählen Sie für RSA "Allgemeiner Verwendungszweck" aus.
e. Klicken Sie auf Jetzt generieren. Das Schlüsselpaar wird nun erstellt.



3. Wählen Sie den Namen des Schlüsselpaars aus.

Wählen Sie das Schlüsselpaar aus, mit dem der CSR signiert und mit dem neuen Zertifikat verknüpft werden soll.



4. Zertifikatantragsteller und vollständig qualifizierter Domänenname (FQDN) konfigurieren

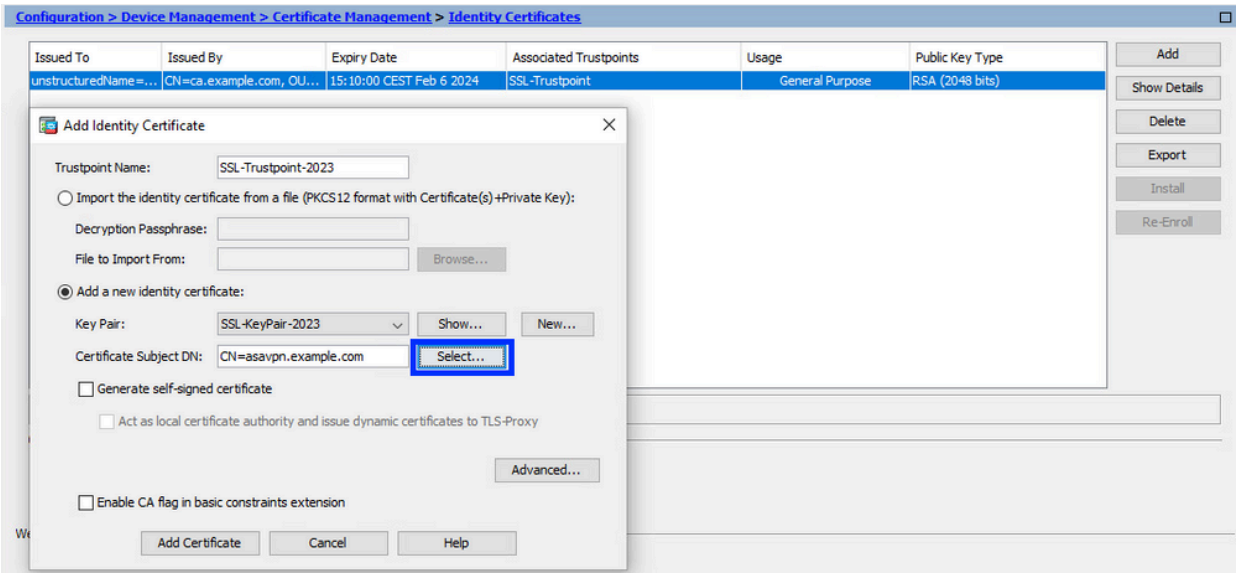
---

Achtung: Der FQDN-Parameter muss mit dem FQDN oder der IP-Adresse der ASA-Schnittstelle übereinstimmen, für die das Zertifikat verwendet wird. Dieser Parameter legt den alternativen Antragstellernamen (SAN) für das Zertifikat fest. Das SAN-Feld wird vom SSL/TLS/IKEv2-Client verwendet, um zu überprüfen, ob das Zertifikat mit dem FQDN übereinstimmt, mit dem die Verbindung hergestellt wird.

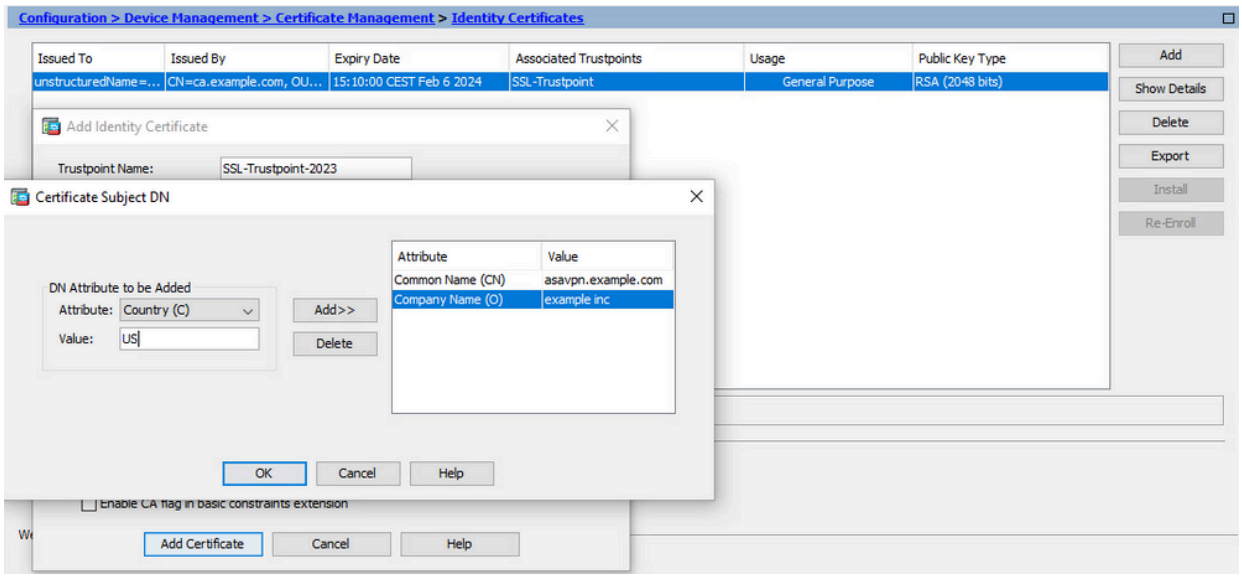
Hinweis: Die CA kann die im Vertrauenspunkt definierten Parameter FQDN und Subject Name (Antragstellername) ändern, wenn sie den CSR signiert und ein signiertes Identitätszertifikat erstellt.

---

a. Klicken Sie auf Auswählen.



b. Konfigurieren Sie im Fenster Zertifikatantragsteller-DN Zertifikatattribute - Wählen Sie ein Attribut aus der Dropdown-Liste aus, geben Sie den Wert ein, und klicken Sie auf Hinzufügen.

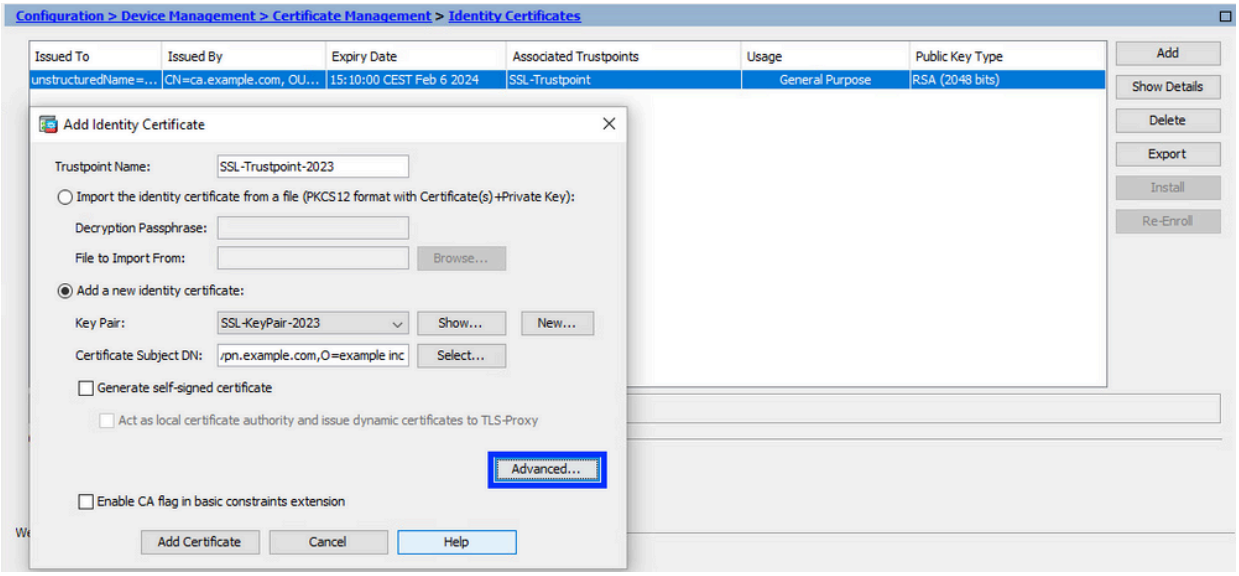


Attribut	Beschreibung
KN	Der Name, über den auf die Firewall zugegriffen werden kann (normalerweise der vollqualifizierte Domänenname, z. B. vpn.example.com).
OU	Der Name Ihrer Abteilung innerhalb der Organisation.
O	Der gesetzlich registrierte Name Ihrer Organisation/Ihres Unternehmens
C	Landesvorwahl (Code aus 2 Buchstaben ohne Interpunktion)
ST	Der Status, in dem sich Ihre Organisation befindet.
L	Die Stadt, in der Ihre Organisation ansässig ist.
EA	Email-Adresse

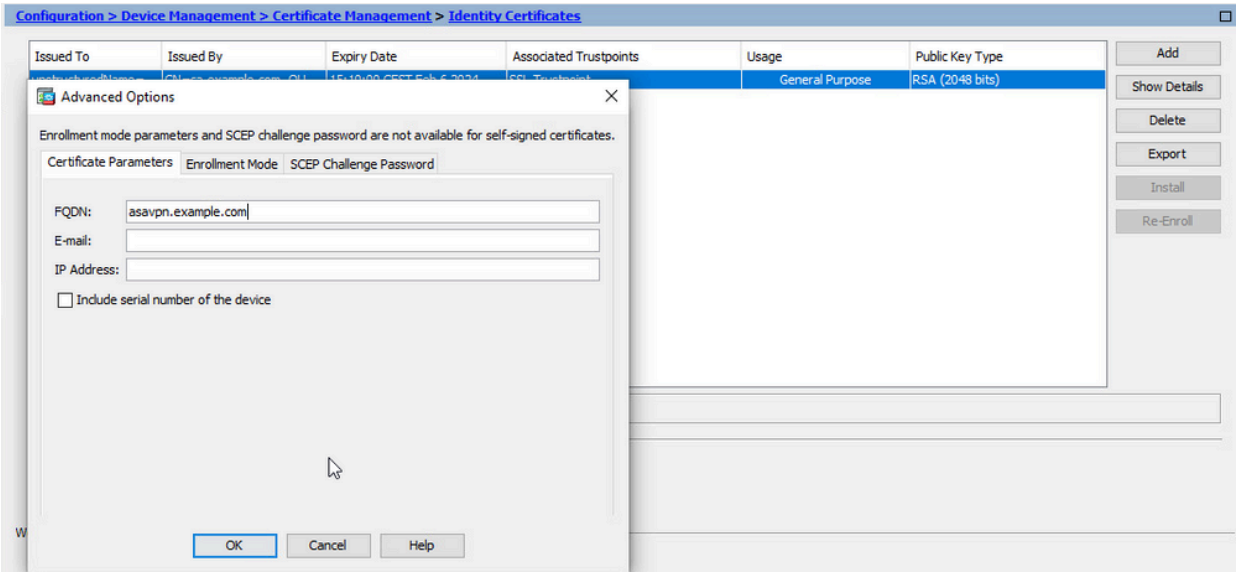
Hinweis: Keines der vorherigen Felder darf mehr als 64 Zeichen enthalten. Ein größerer Wert kann zu Problemen bei der Installation des Identitätszertifikats führen. Außerdem müssen nicht alle DN-Attribute definiert werden.

Klicken Sie nach Hinzufügen aller Attribute auf OK.

c. Um den FQDN des Geräts zu konfigurieren, klicken Sie auf Advanced (Erweitert).

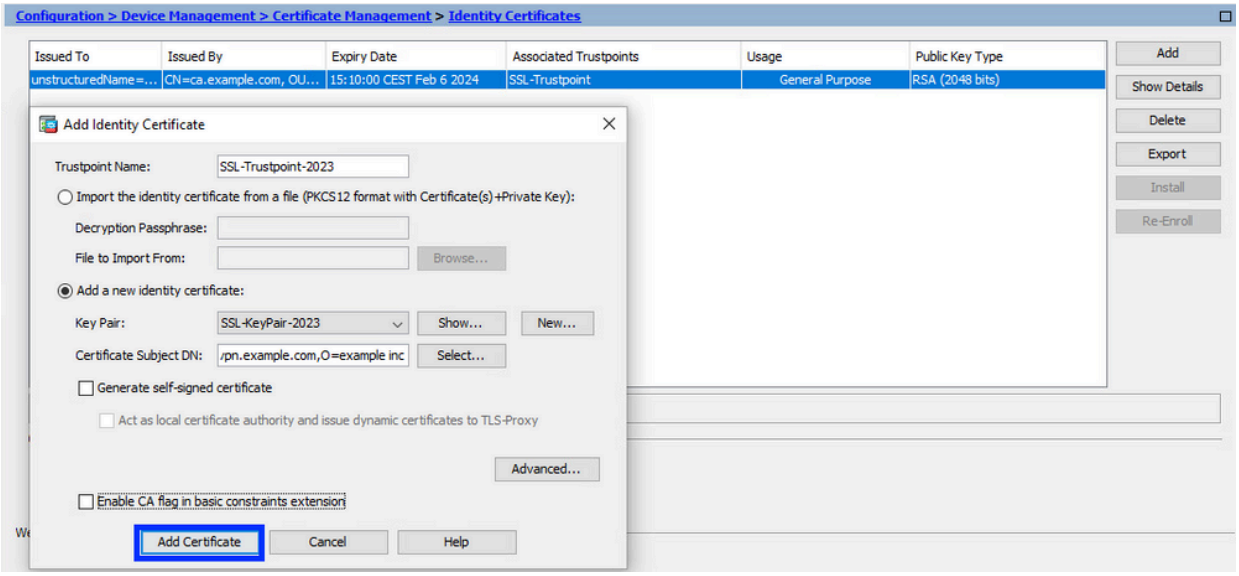


d. Geben Sie im Feld FQDN den vollqualifizierten Domänennamen ein, über den das Gerät vom Internet aus erreichbar ist. Klicken Sie auf OK.

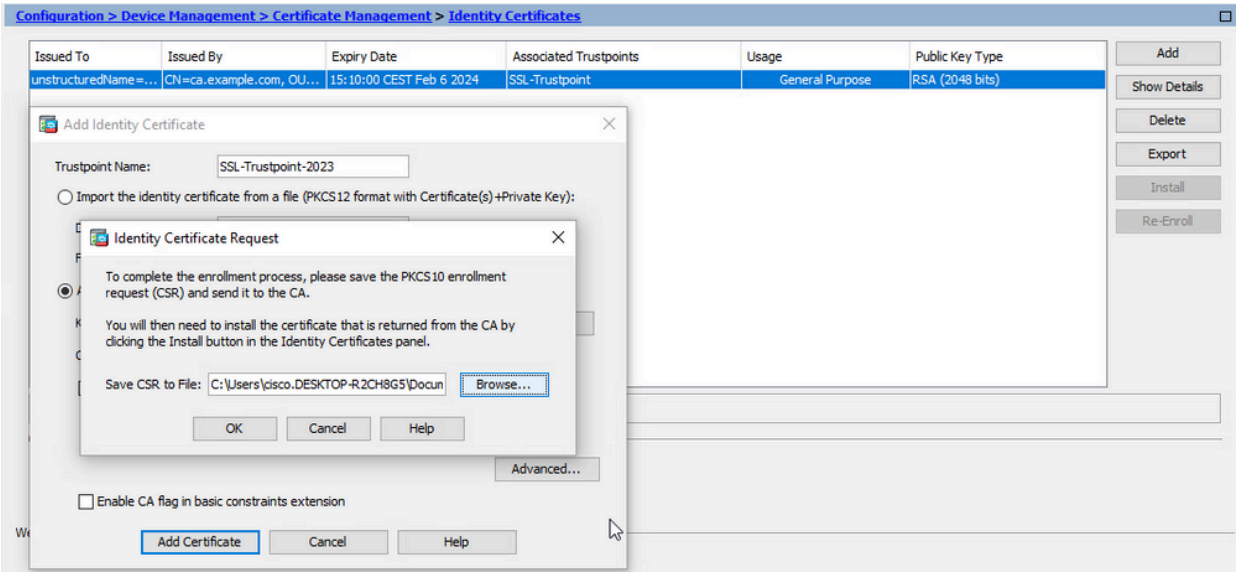


5. Erstellen und Speichern der CSR-Anfrage

a. Klicken Sie auf Zertifikat hinzufügen.



b. Es wird eine Aufforderung angezeigt, den CSR in einer Datei auf dem lokalen Computer zu speichern.

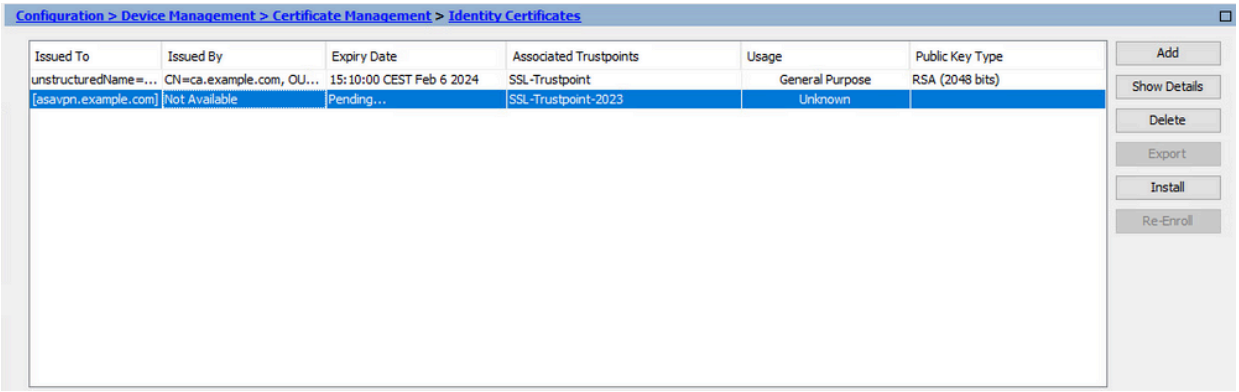


Klicken Sie auf Durchsuchen. Wählen Sie einen Speicherort für die CSR-Datei aus, und speichern Sie die Datei mit der Erweiterung .txt.

Hinweis: Wenn die Datei mit der Erweiterung .txt gespeichert wird, kann die PKCS#10-Anforderung geöffnet und mit einem Texteditor (z. B. Editor) angezeigt werden.

---

c. Jetzt wird der neue Vertrauenspunkt im Status Ausstehend angezeigt.

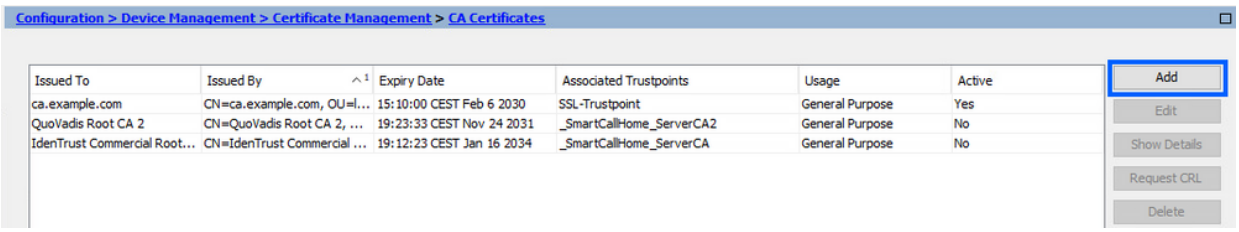


Installieren des Identitätszertifikats im PEM-Format mit ASDM

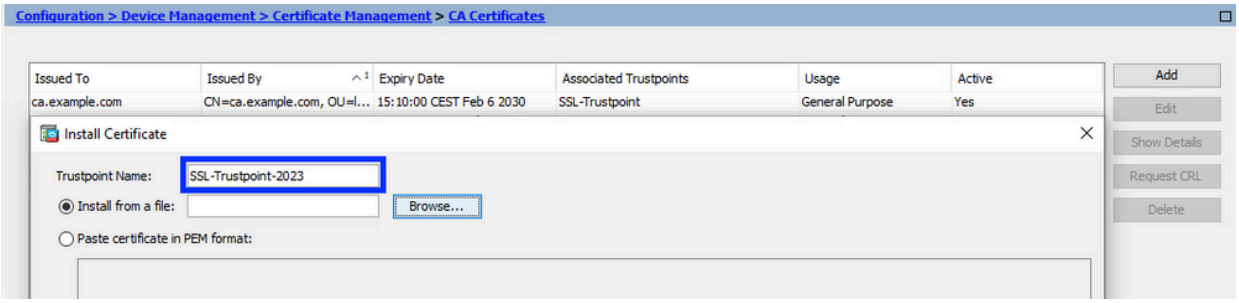
Bei den Installationsschritten wird davon ausgegangen, dass die Zertifizierungsstelle den CSR signiert und ein PEM-codiertes (.pem, .cer, .crt) neues Identitätszertifikat- und Zertifizierungsstellen-Zertifikatpaket bereitgestellt hat.

1. Installieren des Zertifizierungsstellenzertifikats, das den CSR signiert hat

   Das Zertifizierungsstellenzertifikat, das das Identitätszertifikat signiert hat, kann in dem für das Identitätszertifikat erstellten Vertrauenspunkt installiert werden. Wenn das Identitätszertifikat von einer zwischengeschalteten Zertifizierungsstelle signiert wird, kann dieses Zertifizierungsstellenzertifikat im Vertrauenspunkt für das Identitätszertifikat installiert werden. Alle in der Hierarchie vorgelagerten Zertifizierungsstellenzertifikate können in separaten Zertifizierungsstellen-Vertrauenspunkten installiert werden.
   a. Navigieren Sie zu Configuration > Device Management > Certificate Management >, und wählen Sie CA Certificates aus. Klicken Sie auf Hinzufügen.

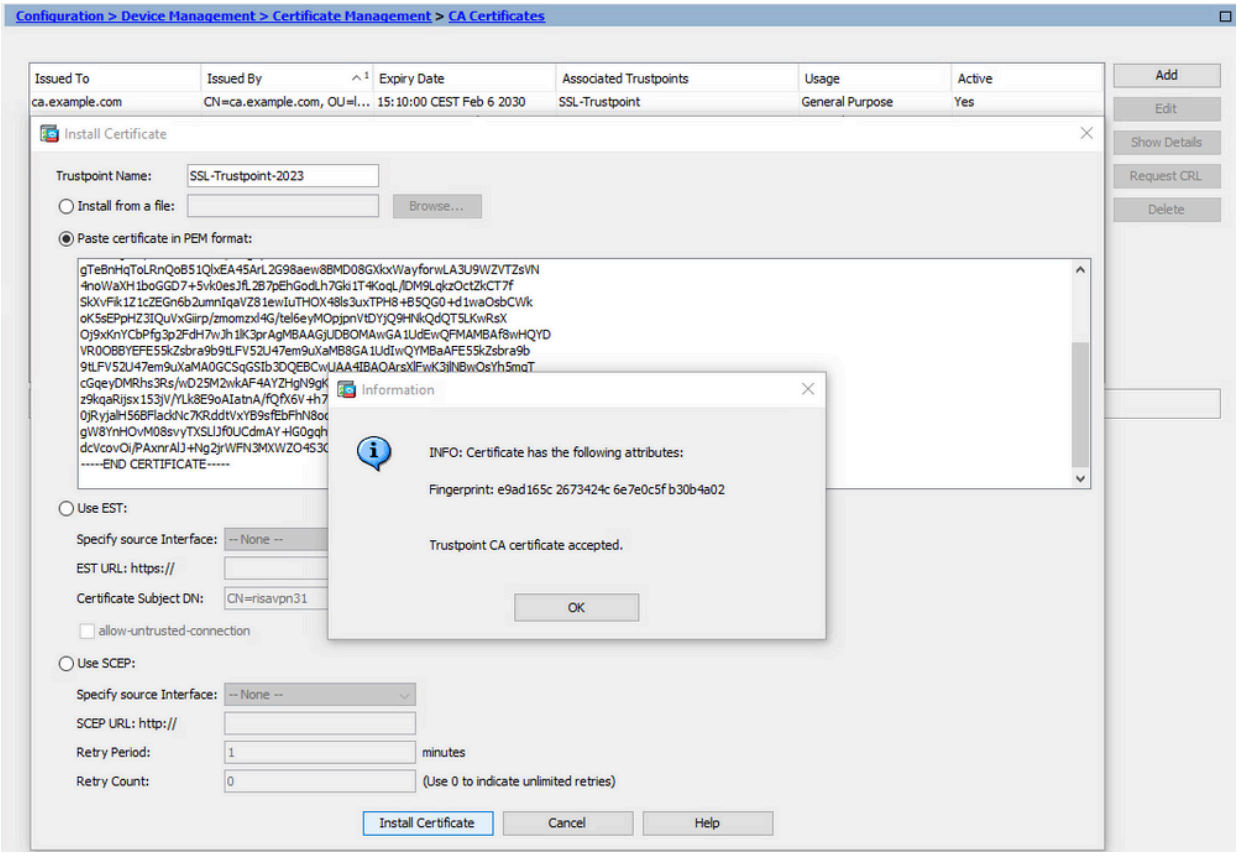


   b. Geben Sie den Namen des Vertrauenspunkts ein, und wählen Sie Install From File (Von Datei installieren), klicken Sie auf Browse (Durchsuchen), und wählen Sie das zwischengeschaltete Zertifikat aus. Sie können auch das PEM-codierte CA-Zertifikat aus einer Textdatei in das Textfeld einfügen.

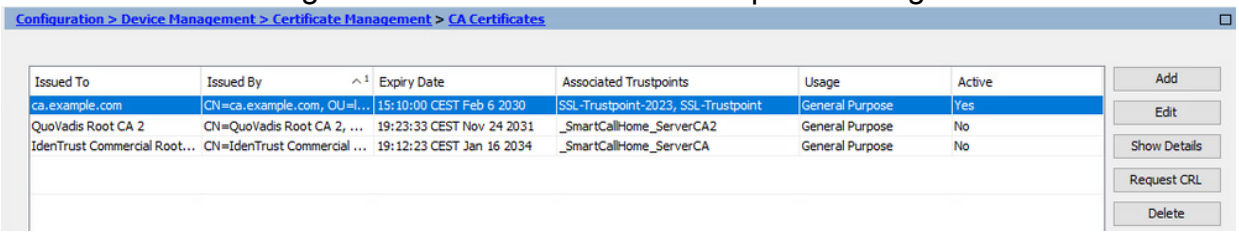


> Hinweis: Installieren Sie das Zwischenzertifikat mit demselben Vertrauenspunktnamen wie den Namen des Vertrauenspunkts des Identitätszertifikats, wenn das Identitätszertifikat vom Zwischenzertifikat signiert wird.

c. Klicken Sie auf Zertifikat installieren.

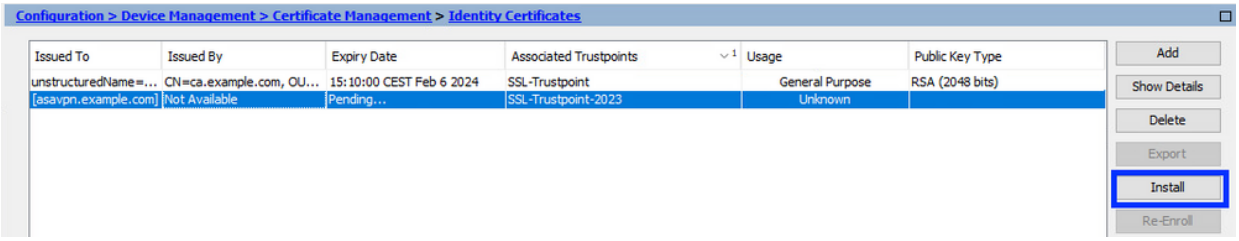


Im Beispiel wird das neue Zertifikat mit demselben CA-Zertifikat signiert wie das alte. Dieselbe Zertifizierungsstelle ist nun zwei Vertrauenspunkten zugeordnet.



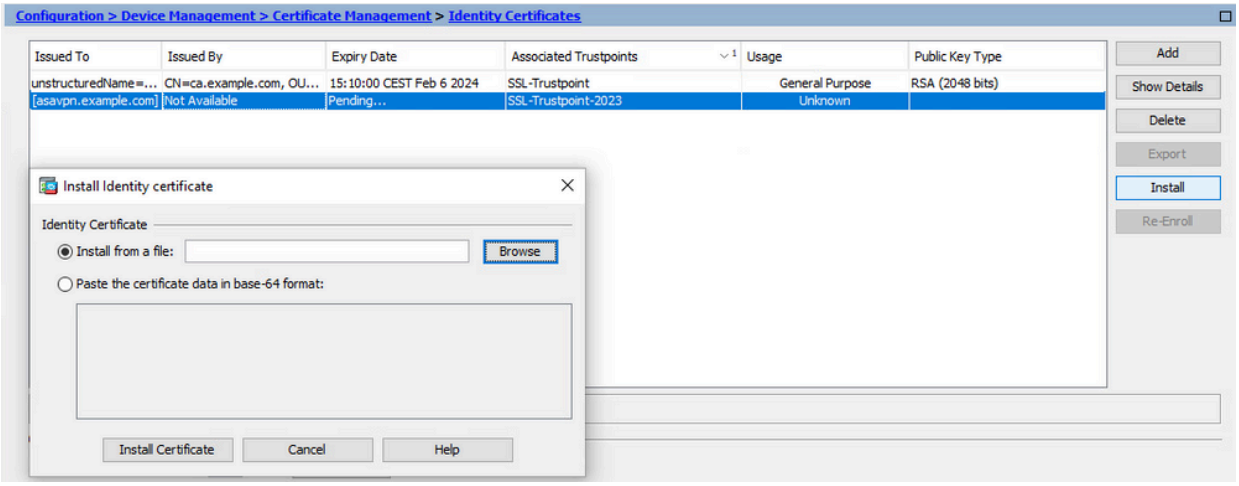
2. Identitätszertifikat installieren

a. Wählen Sie das Identitätszertifikat aus, das zuvor mit der CSR-Generierung erstellt wurde. Klicken Sie auf Install (Installieren).



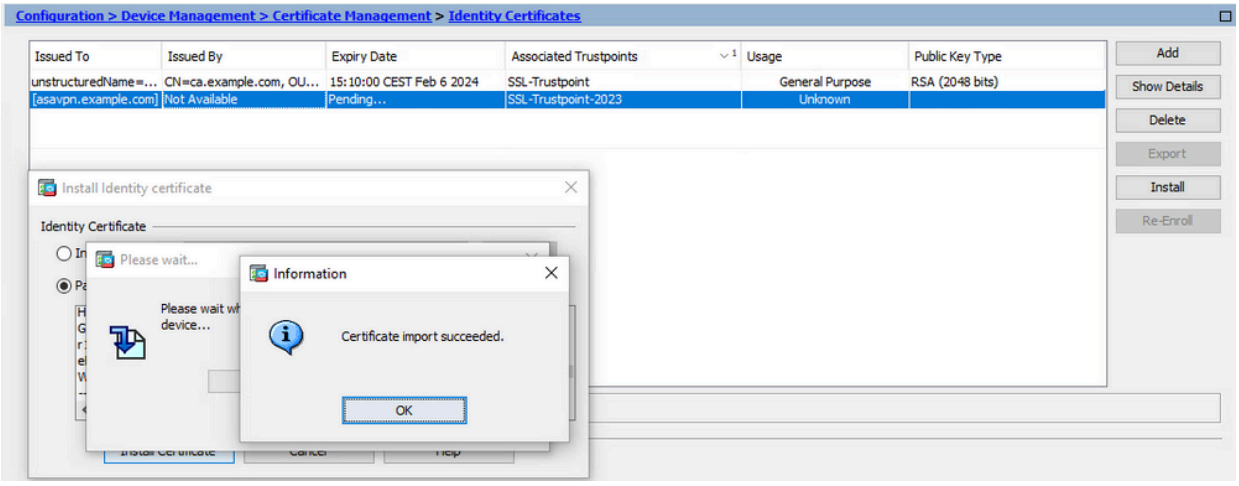
> Hinweis: Das Identitätszertifikat kann im Feld Ausgestellt von als Nicht verfügbar und im Feld Ablaufdatum als Ausstehend angezeigt werden.

b. Wählen Sie eine Datei aus, die das von der Zertifizierungsstelle empfangene PEM-codierte Identitätszertifikat enthält, oder öffnen Sie das PEM-codierte Zertifikat in einem Texteditor, und kopieren Sie das von der Zertifizierungsstelle bereitgestellte Identitätszertifikat, und fügen Sie es in das Textfeld ein.

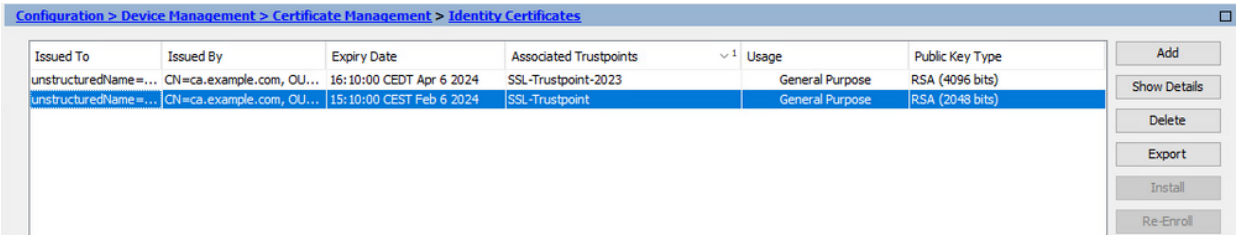


> Hinweis: Identitätszertifikate können im Format .pem, .cer oder .crt installiert werden.

c. Klicken Sie auf Zertifikat installieren.



Nach der Installation sind alte und neue Identitätszertifikate vorhanden.



3. Anbinden des neuen Zertifikats an eine ASDM-Schnittstelle

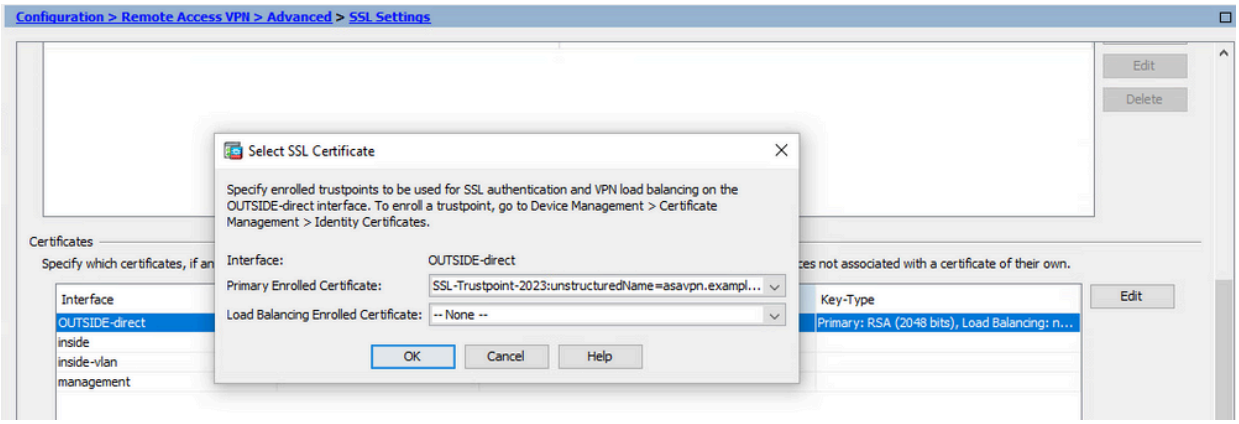
   Die ASA muss so konfiguriert werden, dass das neue Identitätszertifikat für WebVPN-Sitzungen verwendet wird, die auf der angegebenen Schnittstelle enden.

   a. Navigieren Sie zu Configuration > Remote Access VPN > Advanced > SSL Settings.

   b. Wählen Sie unter Certificates (Zertifikate) die Schnittstelle aus, die zum Beenden von WebVPN-Sitzungen verwendet wird. In diesem Beispiel wird die externe Schnittstelle verwendet.

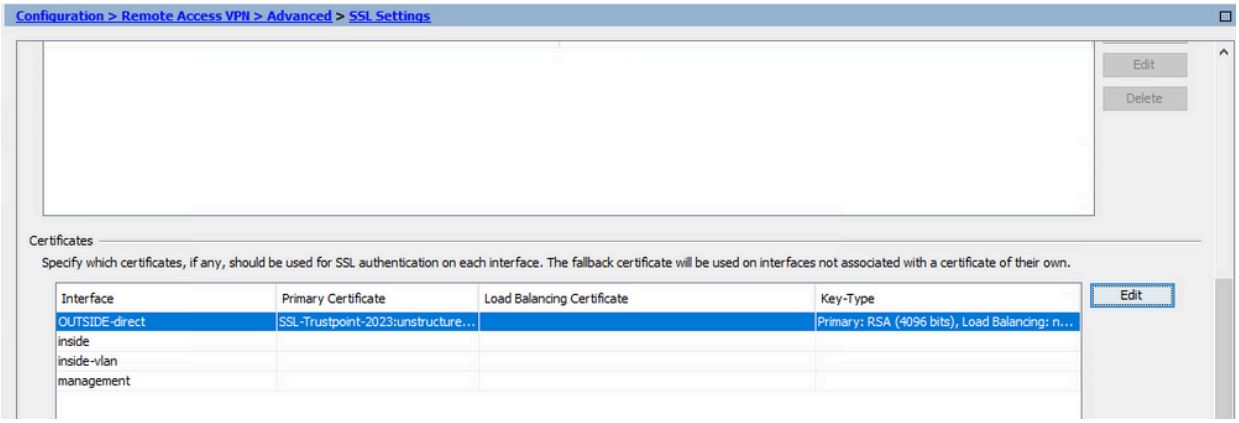
      Klicken Sie auf Bearbeiten.

   c. Wählen Sie in der Dropdown-Liste Zertifikat (Certificate) das neu installierte Zertifikat aus.



   d. Klicken Sie auf OK.

   e. Klicken Sie auf Apply (Anwenden). Jetzt wird das neue Identitätszertifikat verwendet.



Erneuern eines Zertifikats, das bei einer PKCS12-Datei bei ASDM registriert ist

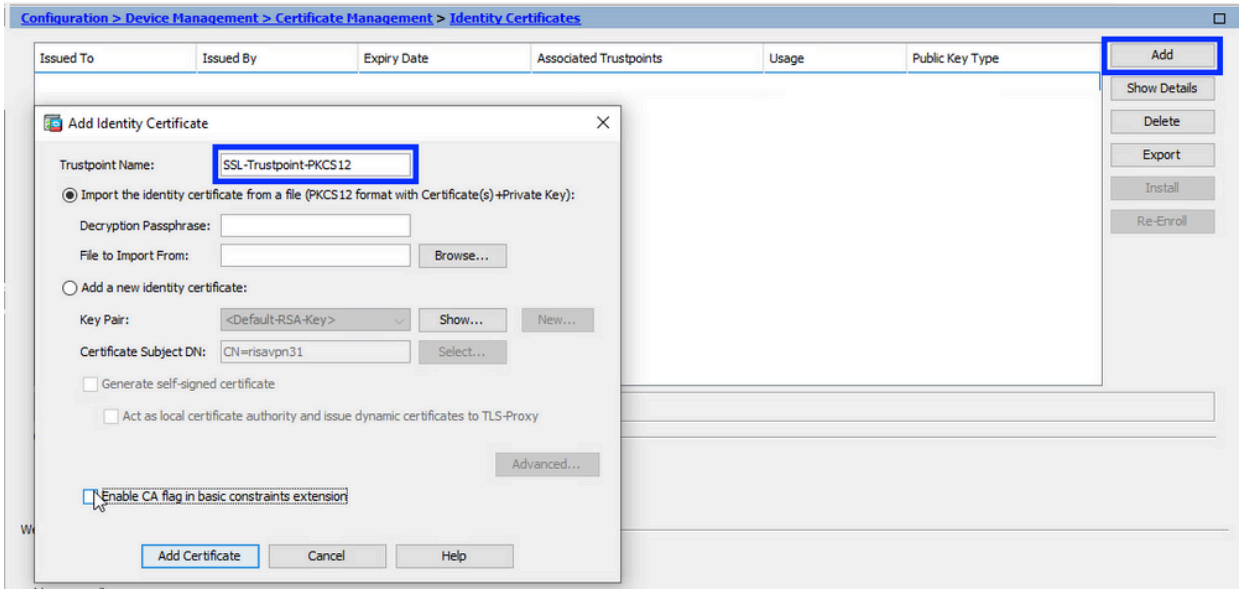
Für die Zertifikatverlängerung eines für PKCS12 registrierten Zertifikats muss ein neuer Vertrauenspunkt erstellt und registriert werden. Sie muss einen anderen Namen haben (z. B. den alten Namen mit dem Suffix für das Registrierungsjahr).

Die PKCS12-Datei (im .p12- oder .pfx-Format) enthält Identitätszertifikat, Schlüsselpaar und Zertifizierungsstellenzertifikat(e). Sie wird von der Zertifizierungsstelle erstellt, z. B. bei einem Platzhalterzertifikat, oder von einem anderen Gerät exportiert. Es handelt sich um eine Binärdatei, die nicht mit einem Texteditor angezeigt werden kann.

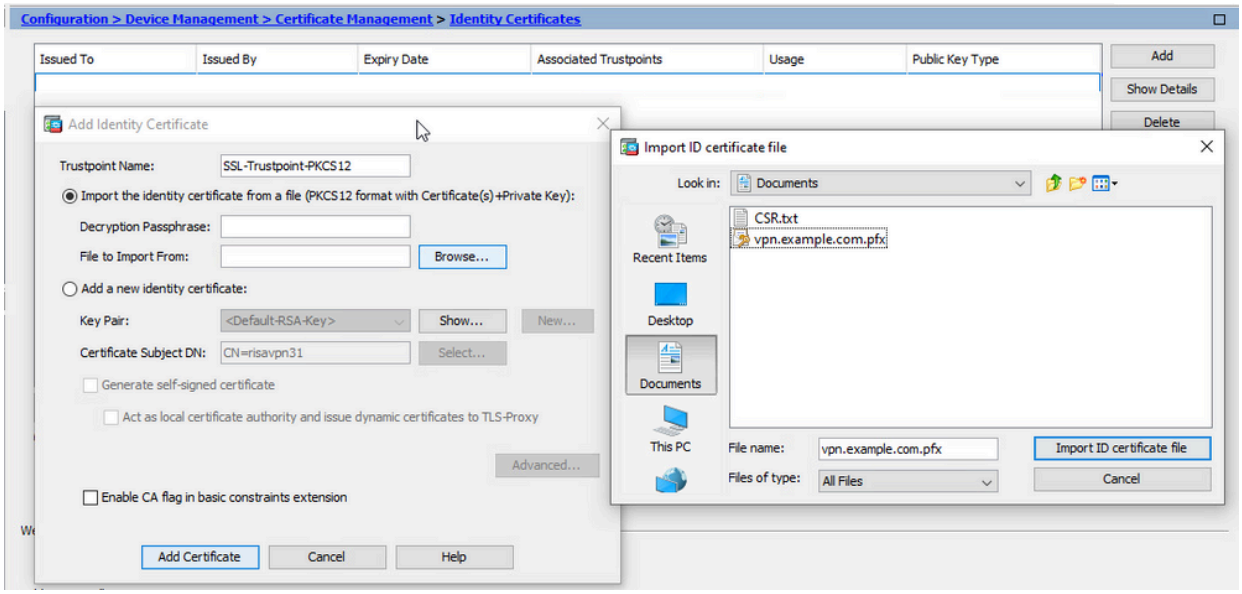
1. Installieren des verlängerten Identitätszertifikats und der Zertifizierungsstellenzertifikate aus einer PKCS12-Datei

   Identitätszertifikat, Zertifizierungsstellenzertifikat(e) und Schlüsselpaar müssen in einer einzigen PKCS12-Datei gebündelt werden.

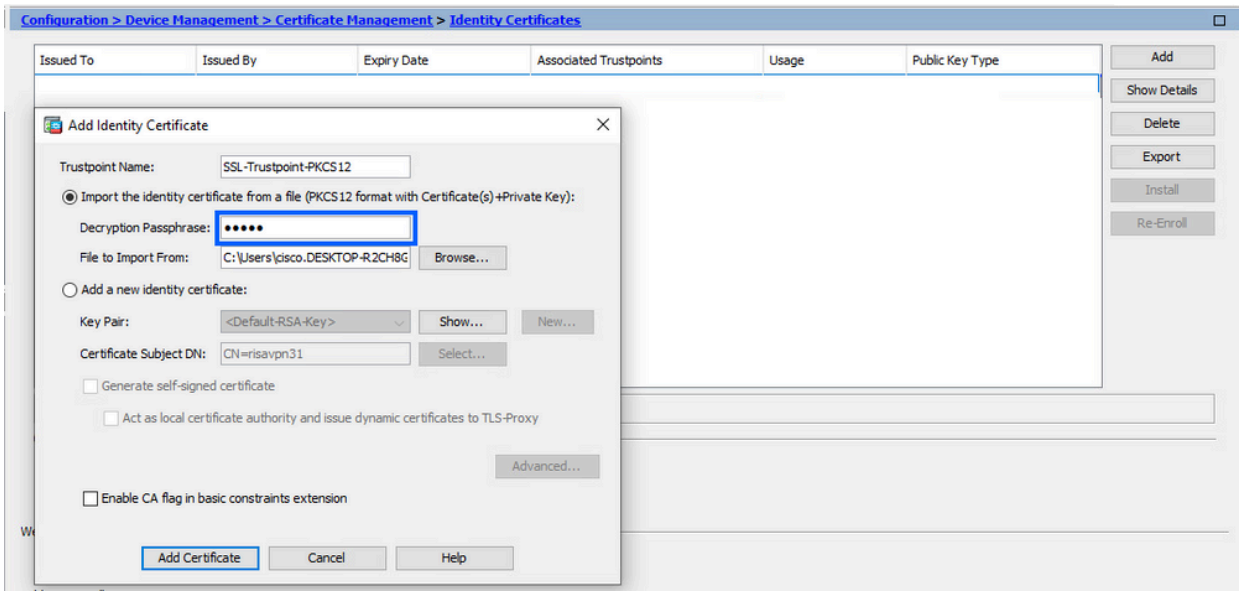
   a. Navigieren Sie zu Configuration > Device Management > Certificate Management, und wählen Sie Identity Certificates aus.
   b. Klicken Sie auf Hinzufügen.
   c. Geben Sie einen neuen Vertrauenspunktnamen an.



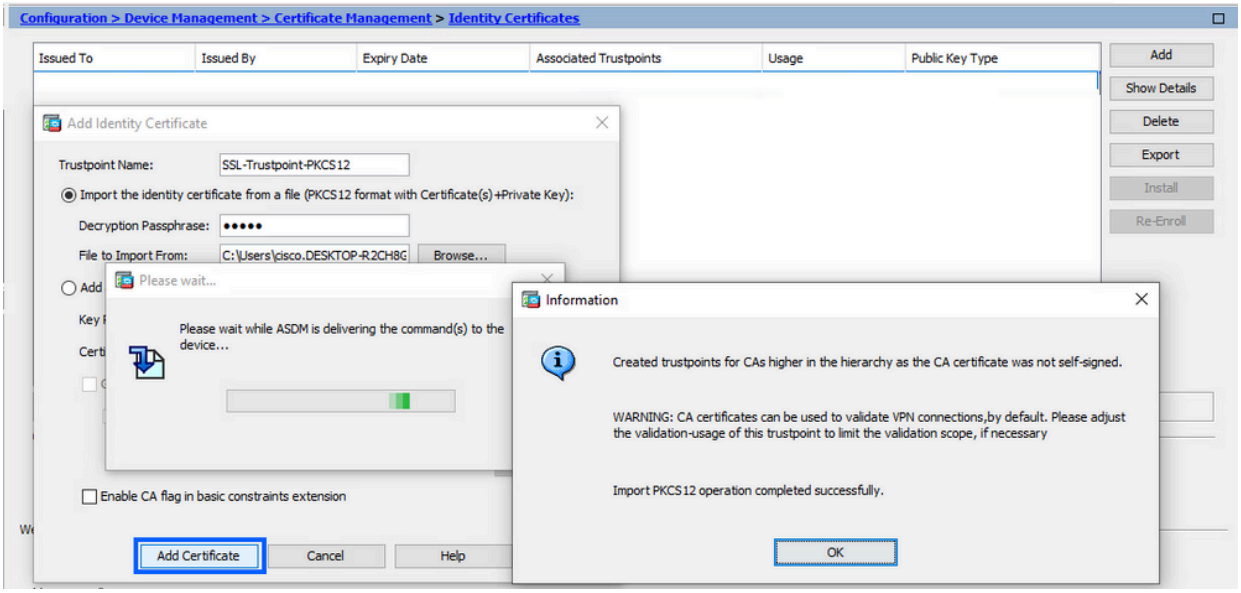
   d. Klicken Sie auf das Optionsfeld Identitätszertifikat aus einer Datei importieren.



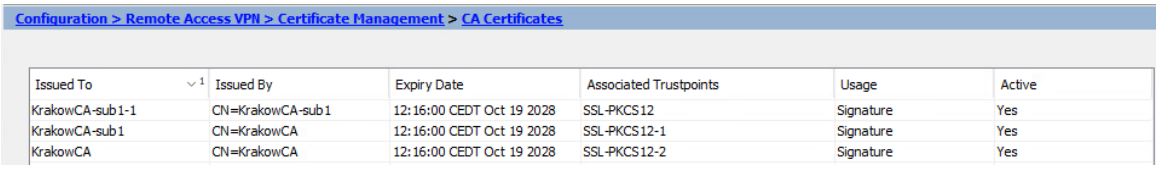
e. Geben Sie die Passphrase ein, die zum Erstellen der PKCS12-Datei verwendet wird.



f. Klicken Sie auf Zertifikat hinzufügen.



Hinweis: Wenn eine PKCS12 mit CAs-Zertifikatkette importiert wird, erstellt der ASDM die Trustpoints der Upstream-CAs automatisch mit Namen mit dem Suffix "-Nummer".



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. Anbinden des neuen Zertifikats an eine ASDM-Schnittstelle

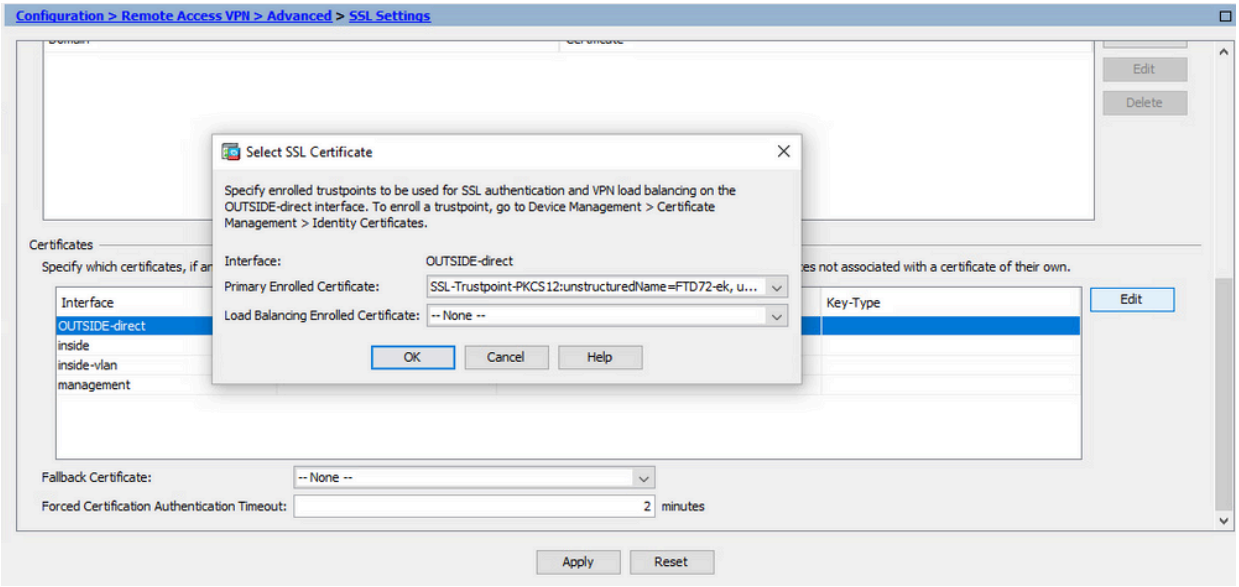
Die ASA muss so konfiguriert werden, dass das neue Identitätszertifikat für WebVPN-Sitzungen verwendet wird, die auf der angegebenen Schnittstelle enden.

a. Navigieren Sie zu Configuration > Remote Access VPN > Advanced > SSL Settings.

b. Wählen Sie unter Certificates (Zertifikate) die Schnittstelle aus, die zum Beenden von WebVPN-Sitzungen verwendet wird. In diesem Beispiel wird die externe Schnittstelle verwendet.

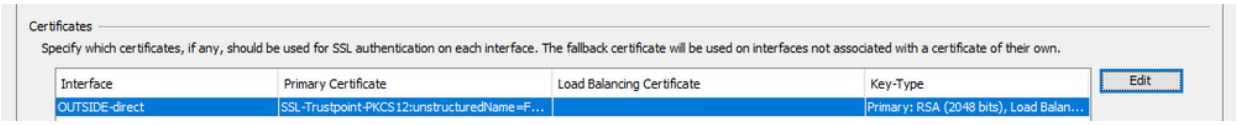
Klicken Sie auf Bearbeiten.

c. Wählen Sie in der Dropdown-Liste Zertifikat (Certificate) das neu installierte Zertifikat aus.



d. Klicken Sie auf OK.

e. Klicken Sie auf Apply (Anwenden).



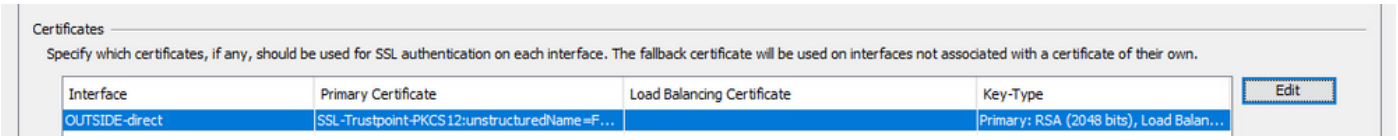
Jetzt wird das neue Identitätszertifikat verwendet.

Überprüfung

Verwenden Sie diese Schritte, um die erfolgreiche Installation des Drittanbieter-Zertifikats zu überprüfen und für SSL VPN-Verbindungen zu verwenden.

Anzeigen installierter Zertifikate über ASDM

1. Navigieren Sie zu Configuration > Remote Access VPN > Certificate Management, und wählen Sie Identity Certificates aus.
2. Das vom Drittanbieter ausgestellte Identitätszertifikat kann angezeigt werden.



Fehlerbehebung

Dieser Debug-Befehl wird in der CLI gesammelt, wenn bei der Installation des SSL-Zertifikats ein Fehler auftritt.

- debug crypto ca 14

Häufig gestellte Fragen

F.Was ist ein PKCS12?
A.In der Verschlüsselung definiert PKCS12 ein Archivdateiformat, das zum Speichern vieler Kryptografieobjekte als eine einzige Datei erstellt wurde. Es wird häufig verwendet, um einen privaten Schlüssel mit seinem X.509-Zertifikat zu bündeln oder um alle Mitglieder einer Vertrauenskette zu bündeln.

F.Was ist eine CSR?
A.In Public Key Infrastructure (PKI)-Systemen ist eine Zertifikatsunterzeichnungsanforderung (auch CSR oder Zertifizierungsanforderung) eine Nachricht, die von einem Antragsteller an eine Registrierungsbehörde der Public Key-Infrastruktur gesendet wird, um ein digitales Identitätszertifikat zu beantragen. Es enthält in der Regel den öffentlichen Schlüssel, für den das Zertifikat ausgestellt werden kann, Informationen zur Identifizierung des signierten Zertifikats (z. B. einen Domänennamen im Betreff) und Integritätsschutz (z. B. eine digitale Signatur).

F.Wo ist das Kennwort des PKCS12?
A.Wenn Zertifikate und Schlüsselpaare in eine PKCS12-Datei exportiert werden, wird das Kennwort im Exportbefehl angegeben. Um eine pkcs12-Datei zu importieren, muss das Kennwort vom Besitzer des Zertifizierungsstellenservers oder von der Person übermittelt werden, die die PKCS12-Datei von einem anderen Gerät exportiert hat.

F.Was ist der Unterschied zwischen der Root und der Identität?
A.In Kryptografie und Computersicherheit ist ein Stammzertifikat ein Public-Key-Zertifikat, das eine Stammzertifizierungsstelle (Certificate Authority, CA) identifiziert. Stammzertifikate sind selbstsigniert (und ein Zertifikat kann über mehrere vertrauenswürdige Pfade verfügen, z. B. wenn das Zertifikat von einem Stamm ausgestellt wurde, der kreuzsigniert wurde) und bilden die Grundlage einer X.509-basierten Public Key Infrastructure (PKI). Ein Public-Key-Zertifikat, auch als digitales Zertifikat oder Identitätszertifikat bezeichnet, ist ein elektronisches Dokument, mit dem der Besitz eines öffentlichen Schlüssels nachgewiesen wird. Das Zertifikat enthält Informationen über den Schlüssel, Informationen über die Identität seines Besitzers (als Antragsteller bezeichnet) und die digitale Signatur einer Stelle, die den Inhalt des Zertifikats überprüft hat (als Aussteller bezeichnet). Wenn die Signatur gültig ist und die Software, die das Zertifikat prüft, dem Aussteller vertraut, kann sie diesen Schlüssel verwenden, um sicher mit dem Antragsteller des Zertifikats zu kommunizieren.

Q.I installierte das Zertifikat, warum es nicht funktioniert?
A.Dies kann auf viele Gründe zurückzuführen sein, zum Beispiel:

1. Das Zertifikat und der Vertrauenspunkt sind konfiguriert, wurden jedoch nicht an den Prozess gebunden, der es verwenden soll. Der zu verwendende Trustpoint ist beispielsweise nicht an die externe Schnittstelle gebunden, die AnyConnect-Clients terminiert.

2. Eine PKCS12-Datei ist installiert, es werden jedoch Fehler ausgegeben, da in der PKCS12-Datei ein Zertifikat der zwischengeschalteten Zertifizierungsstelle fehlt. Die Clients, bei denen das Zwischenzertifikat der Zertifizierungsstelle vertrauenswürdig ist, das Stammzertifikat der

Zertifizierungsstelle jedoch nicht vertrauenswürdig ist, können nicht die gesamte Zertifikatkette überprüfen und das Serveridentitätszertifikat als nicht vertrauenswürdig melden.

3. Ein mit falschen Attributen gefülltes Zertifikat kann zu Installationsfehlern oder clientseitigen Fehlern führen. Bestimmte Attribute können beispielsweise in einem falschen Format codiert werden. Ein weiterer Grund besteht darin, dass im Identitätszertifikat der alternative Antragstellername (SAN) fehlt oder der Domänenname, der für den Zugriff auf den Server verwendet wird, nicht als SAN vorhanden ist.

F. Ist für die Installation eines neuen Zertifikats ein Wartungsfenster erforderlich oder treten Ausfallzeiten auf?
A. Die Installation eines neuen Zertifikats (Identität oder CA) ist nicht störend und sollte keine Ausfallzeiten verursachen oder ein Wartungsfenster erfordern. Um die Verwendung eines neuen Zertifikats für einen bereits vorhandenen Dienst zu aktivieren, ist eine Änderung erforderlich, die u. U. ein Fenster für den Änderungsantrag bzw. die Wartung erfordert.

F. Kann durch Hinzufügen oder Ändern eines Zertifikats die Verbindung zu den verbundenen Benutzern getrennt werden?
A.Nein, die Benutzer, die aktuell verbunden sind, bleiben in Verbindung. Das Zertifikat wird beim Verbindungsaufbau verwendet. Sobald die Benutzer die Verbindung wieder herstellen, wird das neue Zertifikat verwendet.

F.Wie kann ich eine CSR-Anfrage mit einem Platzhalter erstellen? Oder einen alternativen Antragstellernamen (SAN)?
A.Derzeit kann ASA/FTD keinen CSR mit Platzhalter erstellen. Dieser Vorgang kann jedoch mit OpenSSL durchgeführt werden. Um den CSR- und ID-Schlüssel zu generieren, können Sie die folgenden Befehle ausführen:

```
openssl genrsa -out id.key 2048

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

Wenn ein Vertrauenspunkt mit dem FQDN-Attribut (Fully Qualified Domain Name) konfiguriert ist, enthält der von ASA/FTD erstellte CSR das SAN mit diesem Wert. Weitere SAN-Attribute können von der CA hinzugefügt werden, wenn sie den CSR signiert, oder der CSR kann mit OpenSSL erstellt werden

F.Wird der Zertifikatersatz sofort wirksam?

A. Das neue Serveridentitätszertifikat wird nur für die neuen Verbindungen verwendet. Das neue Zertifikat ist sofort nach der Änderung einsatzbereit, wird aber tatsächlich mit neuen Verbindungen verwendet.

F.Wie kann ich überprüfen, ob die Installation funktioniert hat?
A.Der CLI-Befehl zur Überprüfung: show crypto ca cert <trustpointname>

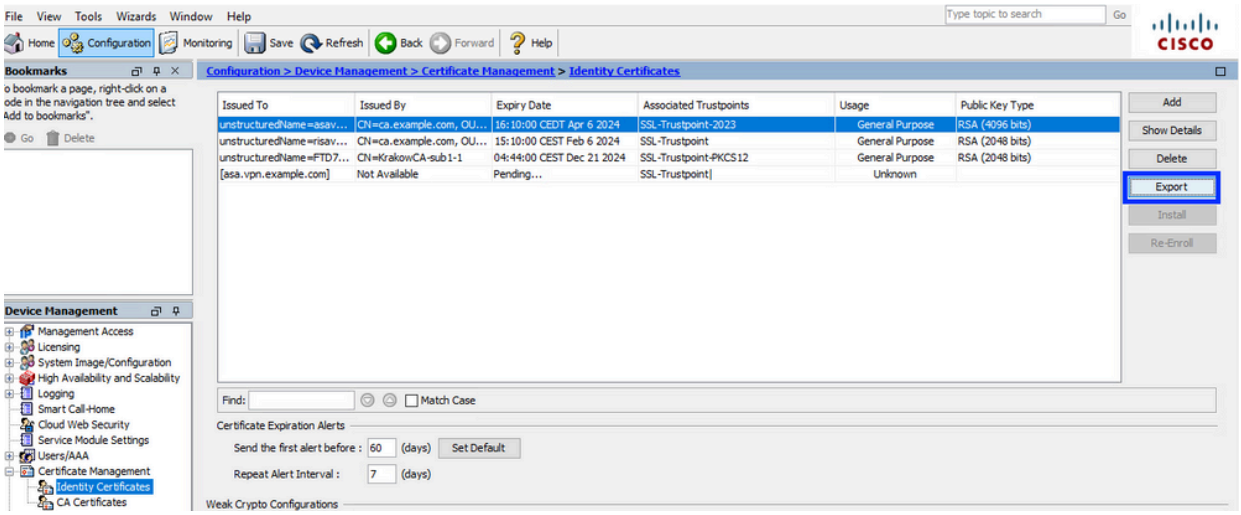
F.Wie wird PKCS12 aus dem Identitätszertifikat, dem Zertifizierungsstellenzertifikat und dem privaten Schlüssel generiert?
A. PKCS12 kann mit OpenSSL mit dem folgenden Befehl erstellt werden:

openssl pkcs12 -export -out p12.pfx -inkey id.key -in id.crt -certfile ca.crt

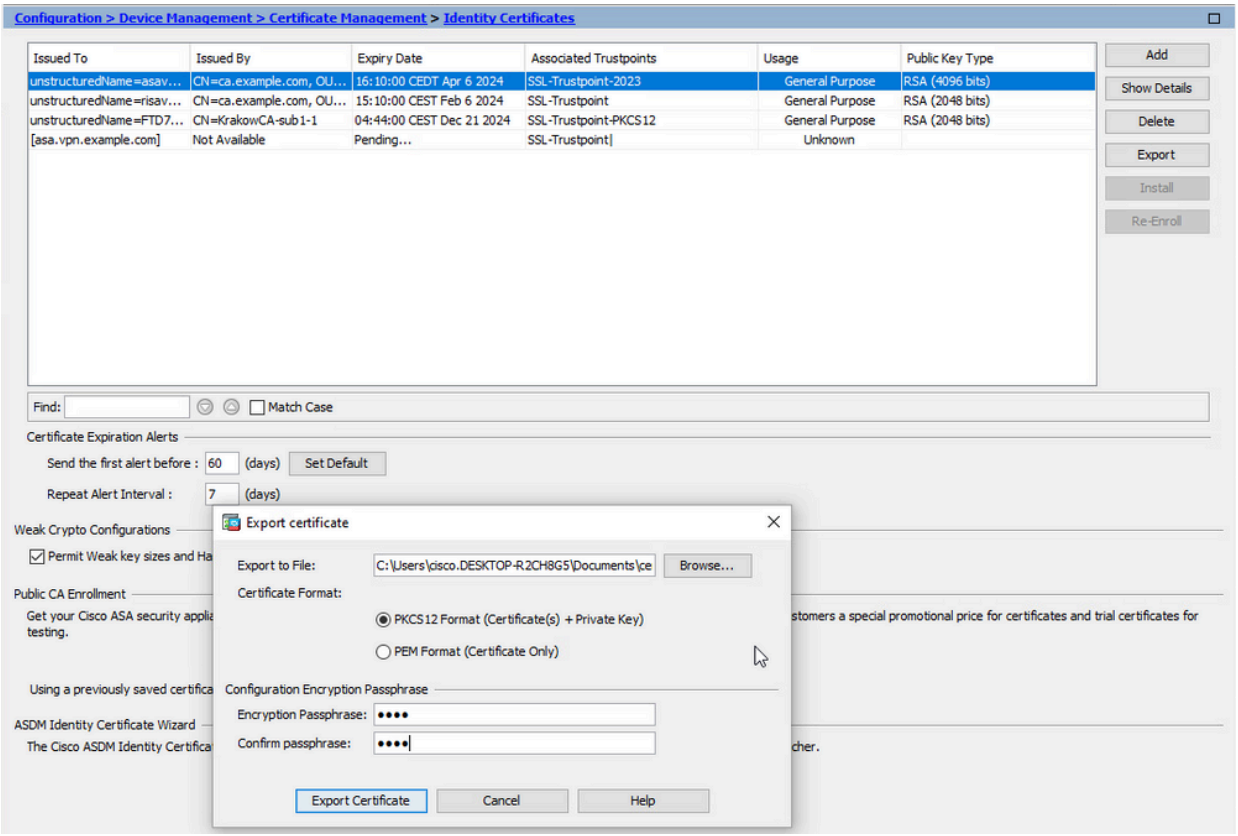
Frage: Wie exportiere ich ein Zertifikat, um es in einer neuen ASA zu installieren?
Antwort:

- Mit CLI: Verwenden Sie den Befehl crypto ca export <trustpointname> pkcs12 <Kennwort>
- Mit ASDM:

a. Navigieren Sie zu Configuration > Device Management > Certificate Management > Identity Certificates, und wählen Sie das Identity Certificate aus. Klicken Sie auf Exportieren.



b. Wählen Sie aus, wohin die Datei exportiert werden soll, geben Sie das Exportkennwort an, und klicken Sie auf Zertifikat exportieren.



Das exportierte Zertifikat kann sich auf dem Datenträger befinden. Bitte beachten Sie die Passphrase an einem sicheren Ort, da die Datei ohne sie nutzlos ist.

F.Wenn ECDSA-Schlüssel verwendet werden, unterscheidet sich der Prozess zur Erstellung von SSL-Zertifikaten?
A.Der einzige Konfigurationsunterschied besteht im Schritt zur Generierung eines Tastenpaars, bei dem anstelle eines RSA-Tastenpaars ein ECDSA-Tastenpaar generiert werden kann. Die übrigen Schritte bleiben gleich.

F.Muss immer ein neues Schlüsselpaar generiert werden?
A.Der Schritt zum Generieren von Schlüsselpaaren ist optional. Vorhandenes Schlüsselpaar kann verwendet werden, oder im Fall von PKCS12 wird das Schlüsselpaar mit dem Zertifikat importiert. Informationen zur jeweiligen Anmeldungs-/Erneuerungsart finden Sie im Abschnitt Wählen Sie den Key-Pair-Namen aus.

F.Ist es sicher, ein neues Schlüsselpaar für ein neues Identitätszertifikat zu generieren?
A.Der Prozess ist sicher, solange ein neuer Schlüsselpaarname verwendet wird. In diesem Fall werden die alten Schlüsselpaare nicht geändert.

Frage: Muss der Schlüssel erneut generiert werden, wenn eine Firewall ersetzt wird (z. B. RMA)?
A.Die neue Firewall enthält keine Schlüsselpaare auf der alten Firewall.
Die Sicherung der aktuellen Konfiguration enthält nicht die Schlüsselpaare.
Die vollständige Sicherung mit ASDM kann die Schlüsselpaare enthalten.

Die Identitätszertifikate können von einer ASA mit ASDM oder CLI exportiert werden, bevor sie fehlschlagen.
Bei einem Failover-Paar werden die Zertifikate und Schlüsselpaare mit einem Write-Standby-Befehl mit einer Standby-Einheit synchronisiert. Wenn ein Knoten des Failover-Paars ersetzt wird, reicht es aus, das grundlegende Failover zu konfigurieren und die Konfiguration auf das neue Gerät zu übertragen.
Wenn ein Schlüsselpaar mit dem Gerät verloren geht und es keine Sicherung gibt, muss ein neues Zertifikat signiert werden, wobei das Schlüsselpaar auf dem neuen Gerät vorhanden ist.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.