Certificaten installeren en verlengen op ASA die door ASDM wordt beheerd

Inhoud

Inleiding

Dit document beschrijft hoe u bepaalde typen certificaten kunt aanvragen, installeren, vertrouwen en verlengen op Cisco ASA-software die met ASDM wordt beheerd.

Voorwaarden

Vereisten

- Voordat u begint te controleren of de adaptieve security applicatie (ASA) de juiste kloktijd, datum en tijdzone heeft. Met certificaatverificatie wordt aanbevolen een NTP-server (Network Time Protocol) te gebruiken om de tijd op de ASA te synchroniseren. Controleer verwante informatie voor referentie.
- Om een certificaat aan te vragen dat gebruik maakt van certificaatondertekeningsaanvraag (CSR), moet het toegang hebben tot een vertrouwde interne of externe certificeringsinstantie (CA). Voorbeelden van CA-leveranciers van derden zijn onder meer Entrust, Geotrust, GoDaddy, Thawte en VeriSign.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASAv 9.18.1
- Voor het maken van PKCS12 wordt OpenSSL gebruikt.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Het soort certificaten dat in dit document wordt vermeld, is:

- zelfondertekende certificaten
- certificaten ondertekend door een certificeringsinstantie van een derde partij of een interne CA

De Secure Socket Layer (SSL), Transport Layer Security (TLS) en IKEv2 rfc7296 voor EAP-verificatieprotocollen schrijven voor dat de SSL/TLS/IKEv2-server de client een servercertificaat biedt waarmee de client serververificatie kan uitvoeren. Het wordt aanbevolen vertrouwde externe CA's in te schakelen voor het verstrekken van SSL-certificaten voor de ASA.

Cisco raadt het gebruik van een zelfondertekend certificaat niet aan, omdat een gebruiker daarbij per ongeluk een browser kan configureren om het certificaat van een onbetrouwbare server te vertrouwen. Bovendien moeten gebruikers dan reageren op een security waarschuwing wanneer verbinding wordt gemaakt met de beveiligde gateway.

Een nieuw identiteitscertificaat aanvragen en installeren met ASDM

Een certificaat kan worden aangevraagd bij een certificeringsinstantie (CA) en op twee manieren worden geïnstalleerd op een ASA:

- Aanvraag voor certificaatondertekening (CSR) gebruiken. Genereer een sleutelpaar, vraag een identiteitscertificaat aan bij CA met een CSR, installeer het ondertekende identiteitscertificaat dat is verkregen van de CA.
- Gebruik PKCS12-bestand dat is verkregen van een CA of dat is geëxporteerd van een ander apparaat. Het PKCS12-bestand bevat sleutelpaar, identiteitscertificaat, CA-certificaat(s).

Een nieuw identiteitscertificaat aanvragen en installeren met aanvraag voor certificaatondertekening (CSR)

Er wordt een CSR gemaakt op het apparaat dat een identiteitscertificaat nodig heeft, gebruik een sleutelpaar dat op het apparaat is gemaakt.

Een MVO bevat:

- informatie over het certificaatverzoek - aangevraagd onderwerp en andere eigenschappen, openbare sleutel van het sleutelpaar,
- informatie over handtekeningsalgoritmen;
- digitale handtekening van de informatie van het certificaatverzoek, die met de privé sleutel van het Zeer belangrijke paar wordt ondertekend.

De CSR wordt doorgegeven aan de certificeringsinstantie (CA), zodat deze deze ondertekent, in een PKCS#10-formulier.

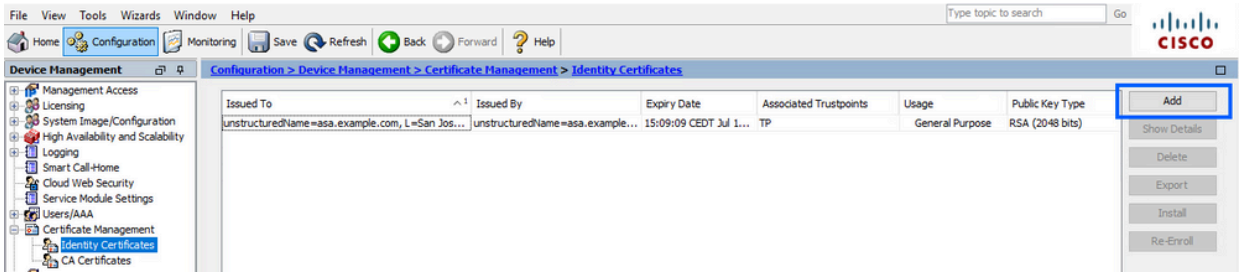
Het ondertekende certificaat wordt door CA teruggestuurd in een PEM-formulier.

> Opmerking: CA kan de FQDN- en onderwerpnaamparameters die in het Trustpoint zijn gedefinieerd, wijzigen wanneer het de CSR ondertekent en een ondertekend identiteitscertificaat aanmaakt.

Genereert een CSR met ASDM

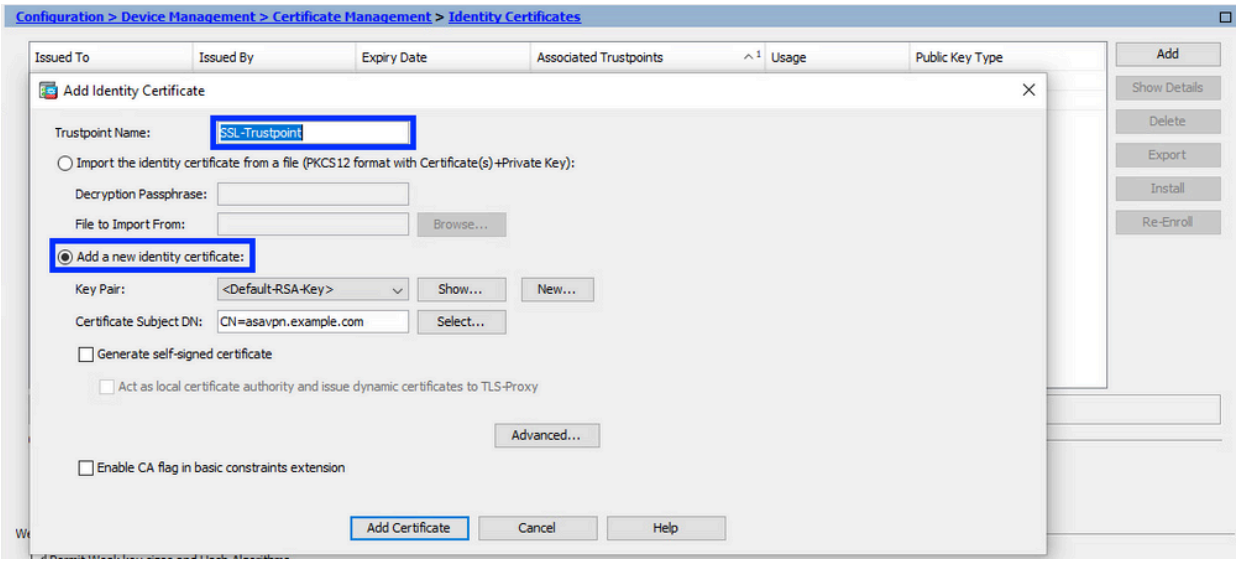
1. Een Trustpoint met een specifieke naam maken

    a. Blader naar Configuratie > Apparaatbeheer > Certificaatbeheer > Identity Certificates.



b. Klik op Add (Toevoegen).

c. Definieer een trustpoint naam.



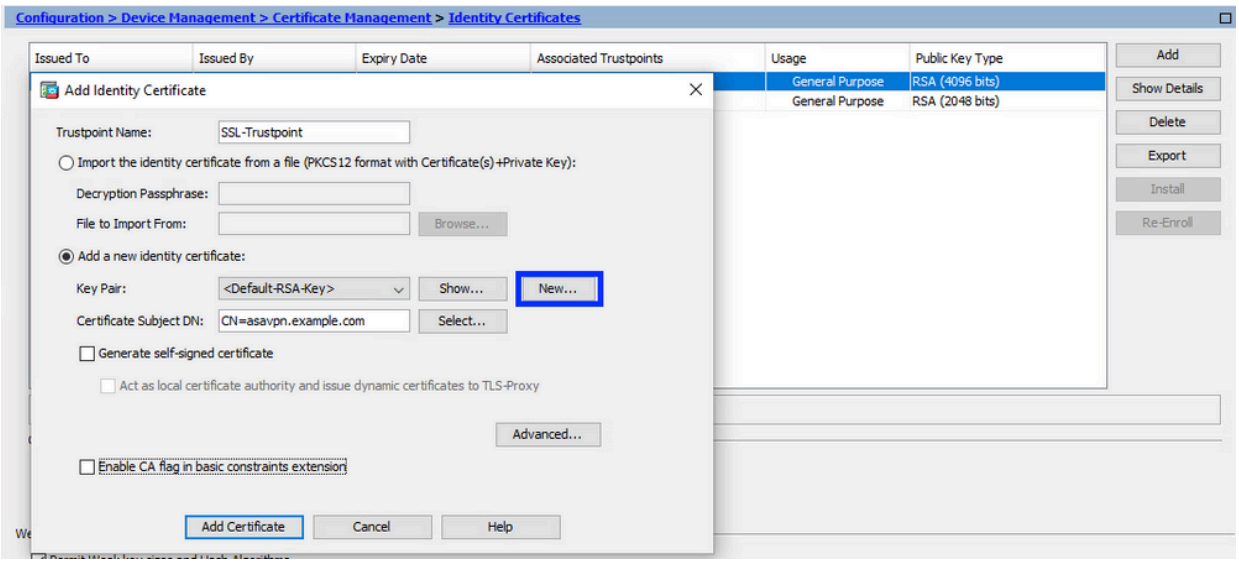
d. Klik op het keuzerondje Add a new identity certificate (Voeg een nieuw identiteitscertificaat toe).

2. (Optioneel) Maak een nieuw sleutelpaar

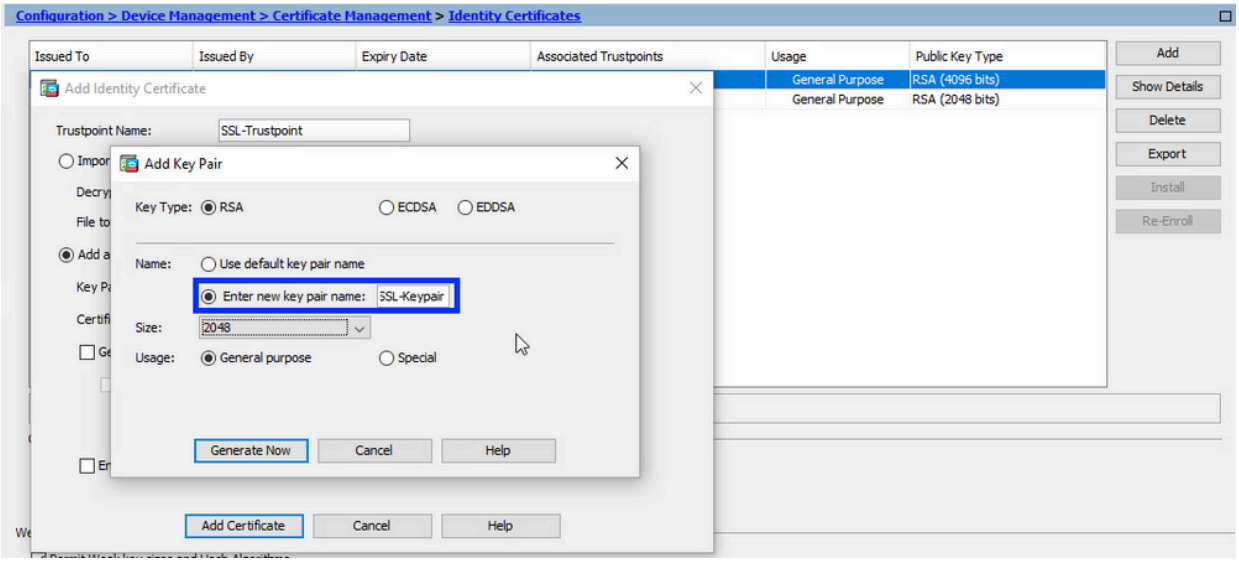
Opmerking: standaard wordt de RSA-toets met de naam Default-RSA-Key en een grootte van 2048 gebruikt. Het wordt echter aanbevolen om voor elk Identity Certificate een uniek privaat/publiek sleutelpaar te gebruiken.

---

a. Klik op Nieuw om een nieuw sleutelpaar te genereren.

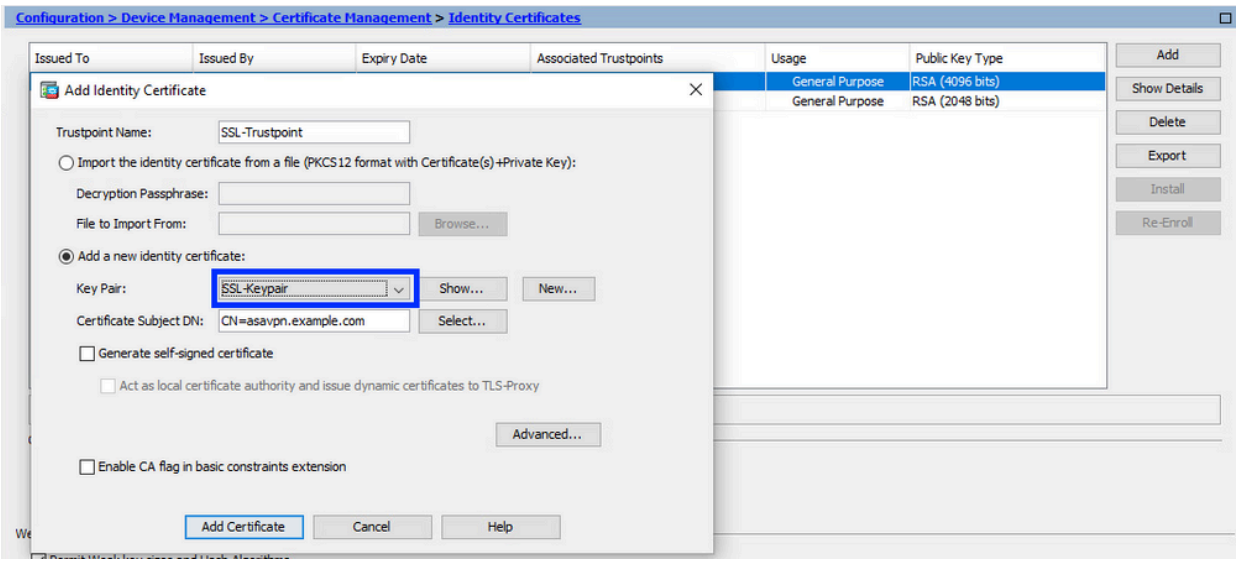


b. Kies de optie Voer een nieuwe sleutelpaarnaam in en voer een naam in voor het nieuwe sleutelpaar.
c. Selecteer RSA of ECDSA bij Key Type (Sleuteltype).
d. Kies de sleutelgrootte; voor RSA, kies algemeen doel voor gebruik.
e. Klik op Generate Now (Nu genereren). Het sleutelpaar wordt nu gecreëerd.



3. De naam van het sleutelpaar kiezen

Kies het sleutelpaar om de MVO te ondertekenen met, en te worden gebonden aan het nieuwe certificaat.

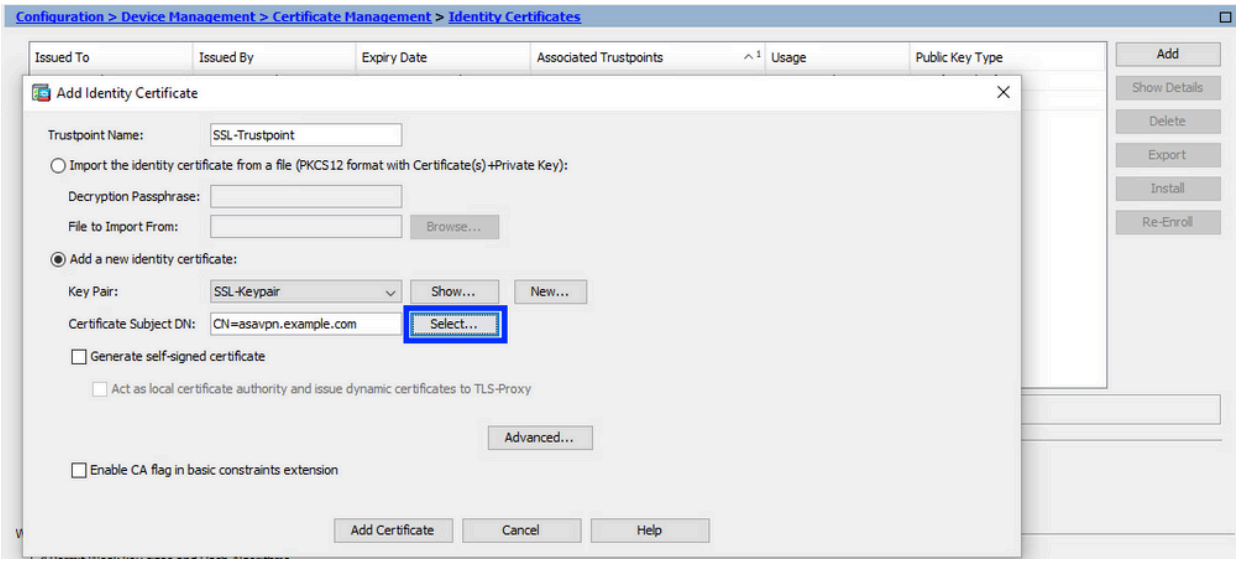


4. Configureer het certificaatonderwerp en de volledig gekwalificeerde domeinnaam (FQDN)

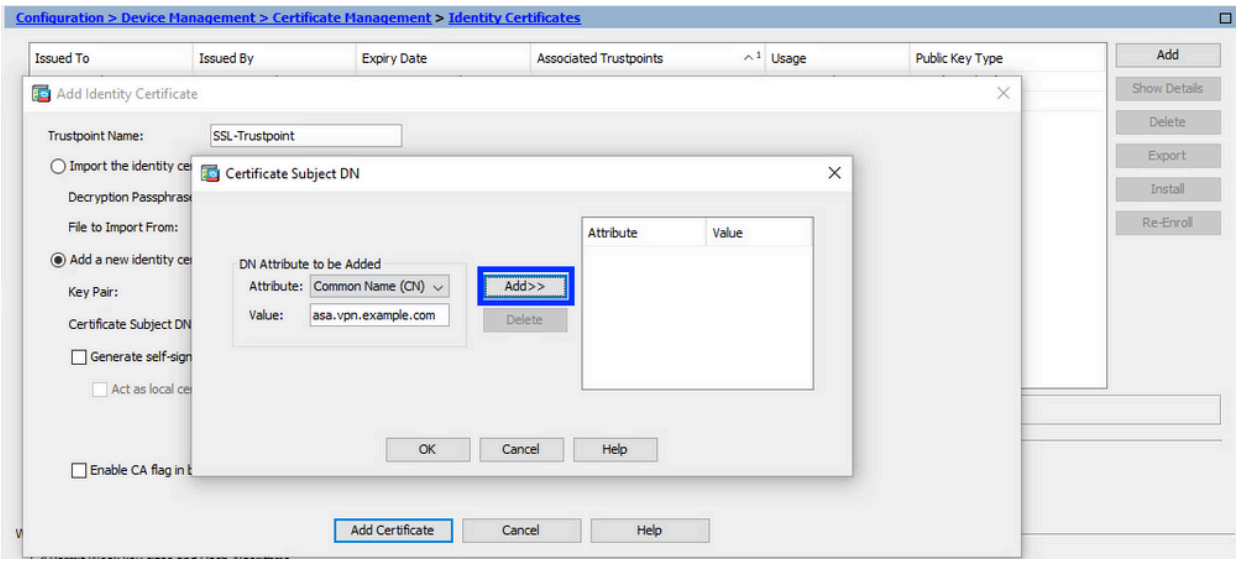
Waarschuwing: de FQDN-parameter moet overeenkomen met de FQDN of het IP-adres van de ASA-interface waarvoor het identiteitscertificaat wordt gebruikt. Deze parameter stelt de gevraagde extensie voor de alternatieve onderwerpnaam (SAN) voor het identiteitscertificaat in. De SAN-extensie wordt gebruikt door SSL/TLS/IKEv2-client om te controleren of het certificaat overeenkomt met de FQDN waarmee verbinding wordt gemaakt.

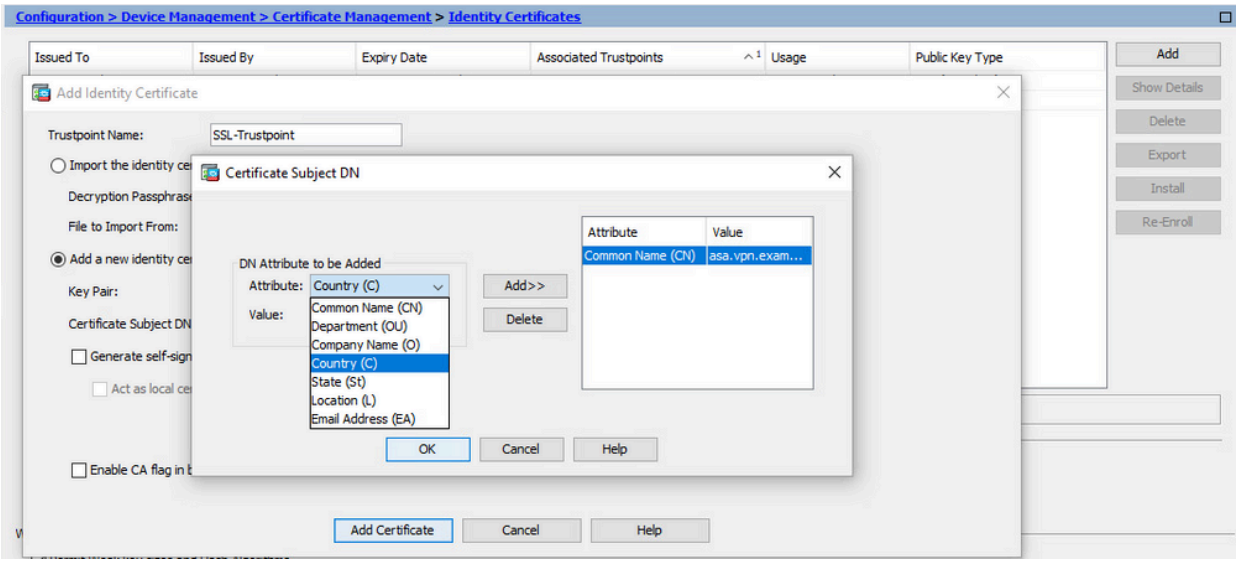
---

a. Klik op Selecteren.



b. In het venster Certificaat Onderwerp DN, vorm certificaatattributen - kies attribuut van vervolgkeuzelijst, ga de waarde in, klik op Add.



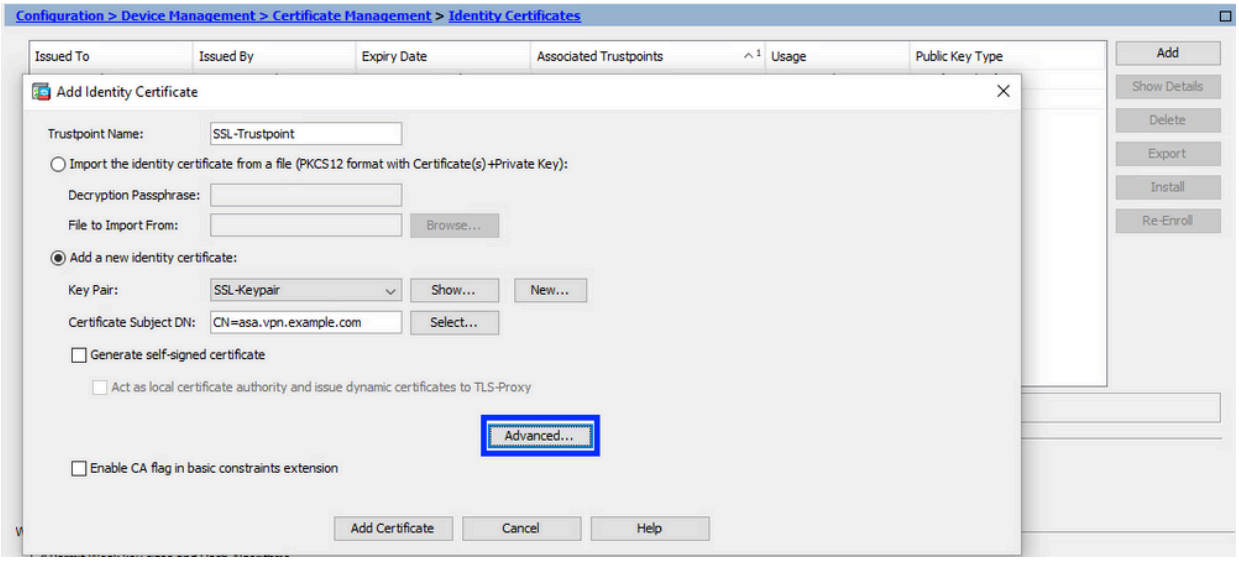


Kenmerk	Beschrijving
CN	De naam waardoor de firewall kan worden benaderd (meestal de volledig gekwalificeerde domeinnaam, bijvoorbeeld vpn.example.com).
OU	De naam van uw afdeling binnen de organisatie
O	De wettelijk geregistreerde naam van uw organisatie/bedrijf
C	Landnummer (2-lettercode zonder punctuatie)
ST	De staat waarin uw organisatie is gevestigd.
L	De stad waar uw organisatie zich bevindt.
EA	E-mailadres

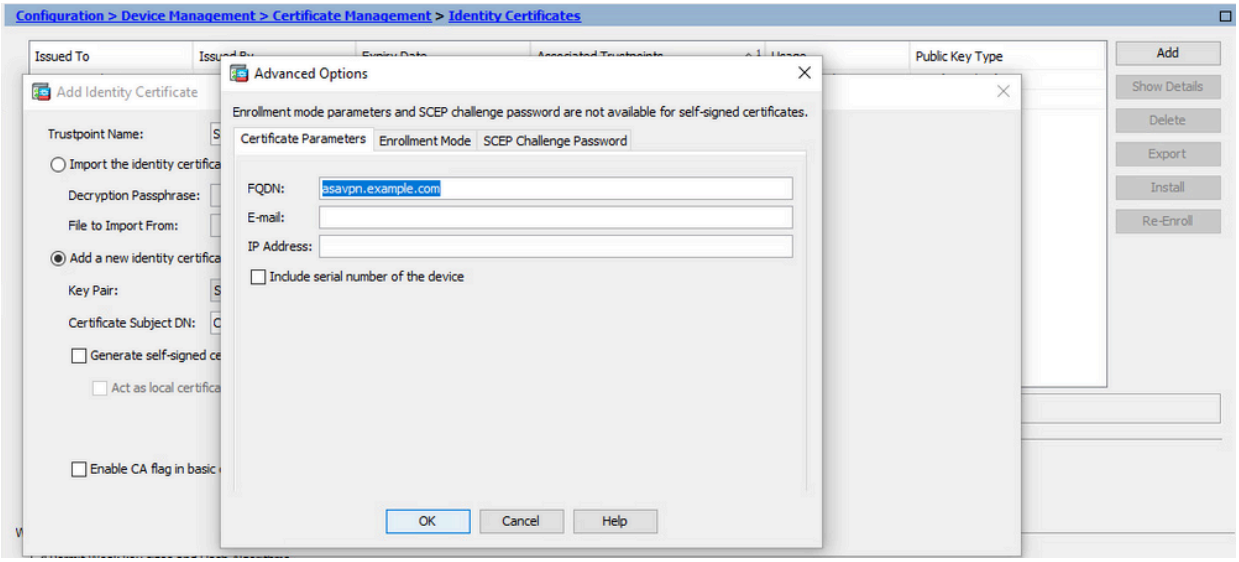
N.B.: Geen van de vorige veldwaarden kan een tekenlimiet van 64 tekens overschrijden. Een langere waarde kan problemen opleveren met de installatie van het identiteitscertificaat. Het is ook niet nodig om alle DN-kenmerken te definiëren.

Klik op OK nadat alle kenmerken zijn toegevoegd.

c. Configureer het apparaat FQDN - klik op Advanced.

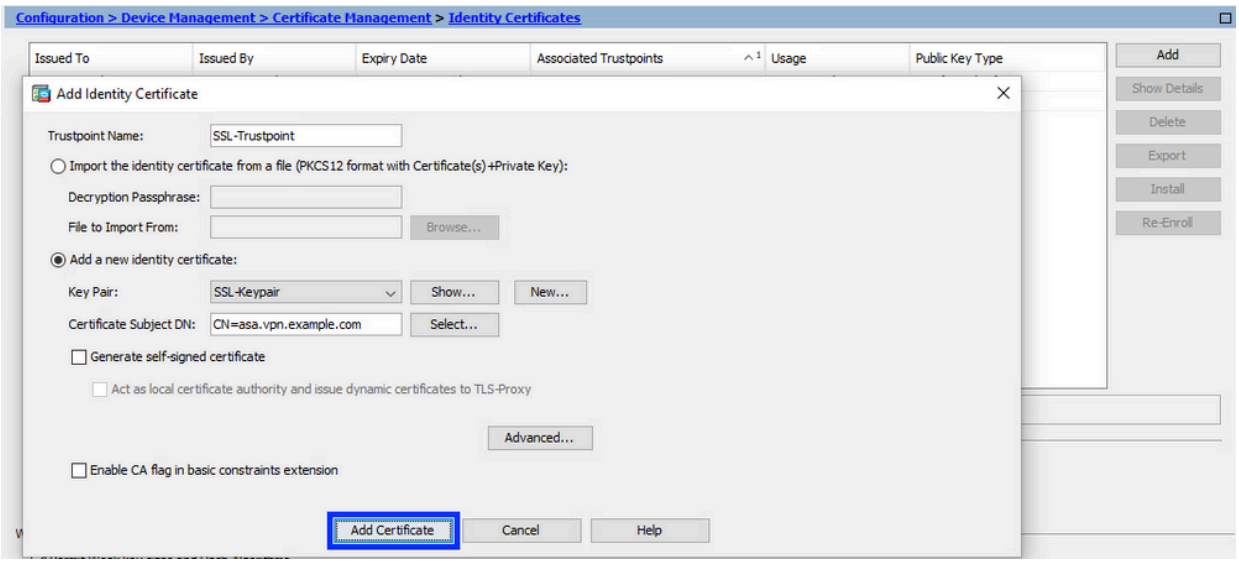


d. Voer in het veld FQDN de volledig gekwalificeerde domeinnaam in via welke het apparaat via internet toegankelijk is. Klik op OK.

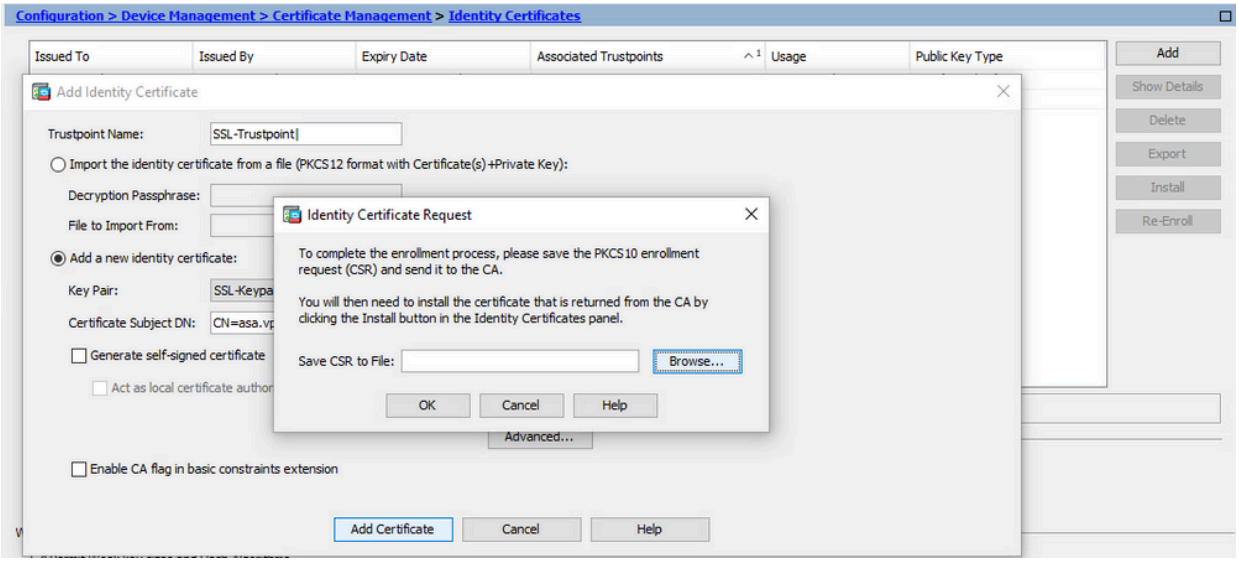


5. MVO genereren en opslaan

a. Klik op Add Certificate (Certificaat toevoegen).



b. Vervolgens wordt een scherm getoond met het verzoek de CSR op te slaan.

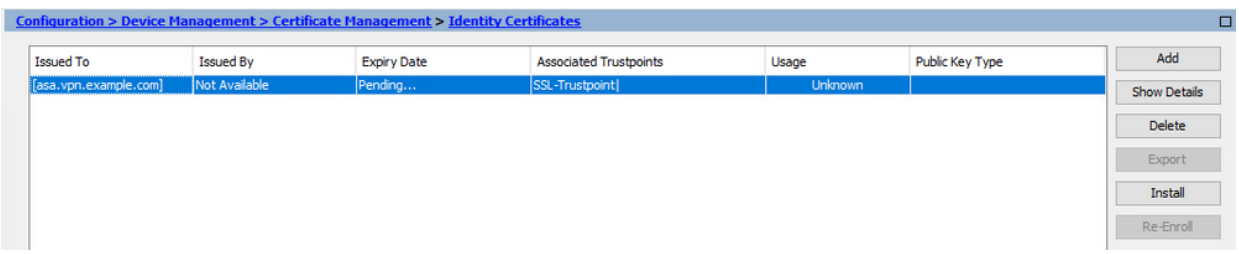


Klik op Browse (Bladeren), selecteer de locatie waar u de CSR wilt opslaan en sla het bestand op met de extensie .txt.

Opmerking: Wanneer het bestand met de extensie .txt wordt opgeslagen, kan het PKCS#10-verzoek worden geopend en bekeken met een teksteditor (zoals Kladblok).

---

c. Nu wordt het nieuwe trustpoint weergegeven in een hangende staat.

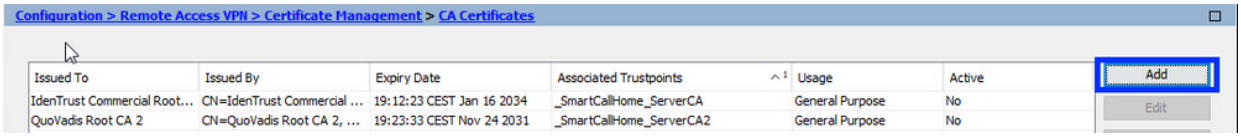


Installeer het Identity Certificate in PEM-formaat met ASDM

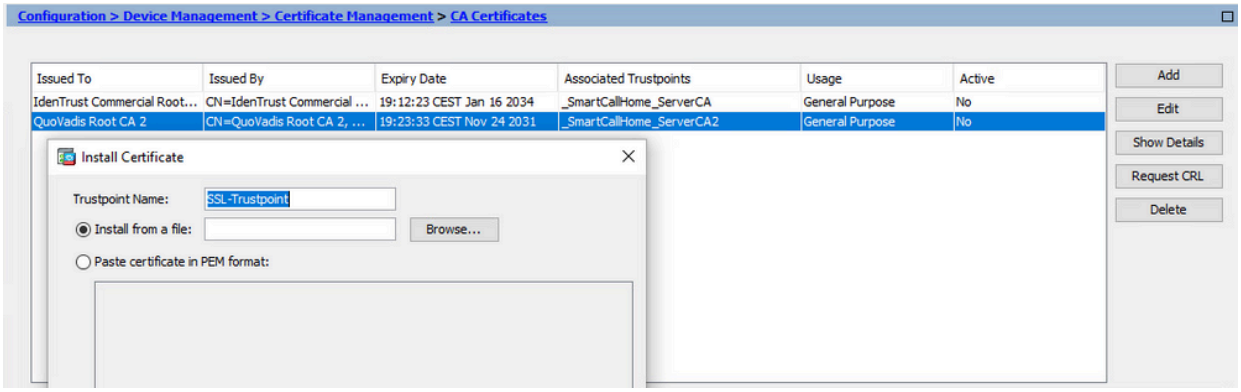
De installatiestappen gaan ervan uit dat de CA de CSR heeft ondertekend en een PEM-gecodeerd identiteitscertificaat en CA-certificaatbundel (pem, .cer, .crt) heeft geleverd.

1. CA-certificaat installeren dat de CSR heeft ondertekend

   a. Navigeer naar Configuration > Device Management >Certificate Management > en kies CA-certificaten. Klik op Add (Toevoegen).



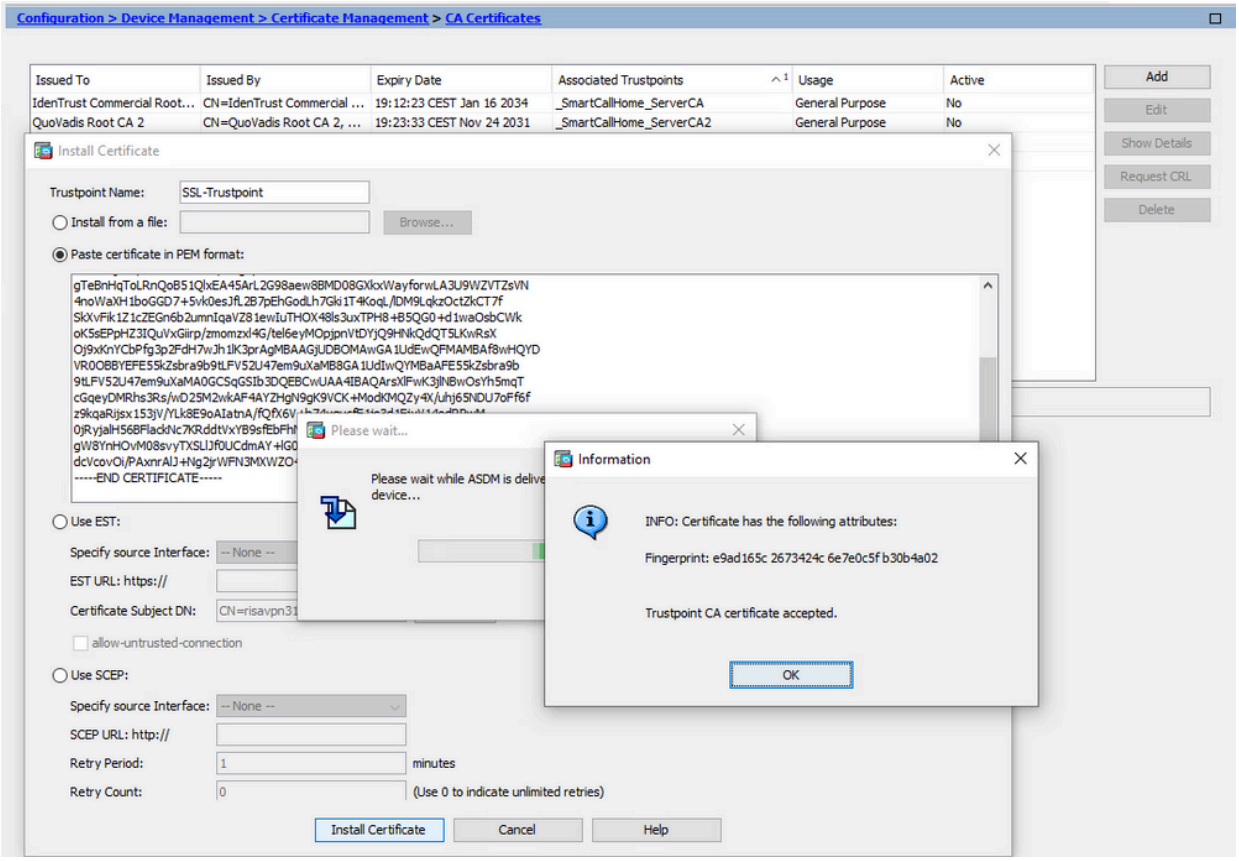
   b. Voer de naam van het Trustpoint in en selecteer Installeren uit bestand, klik op de knop Bladeren en selecteer het tussenliggende certificaat. U kunt ook het PEM-gecodeerde CA-certificaat vanuit een tekstbestand in het tekstveld plakken.



Opmerking: Installeer het CA-certificaat dat de CSR heeft ondertekend en gebruik dezelfde naam als het Identity Certificate. De andere CA-certificaten hoger in de PKI-hiërarchie kunnen in afzonderlijke Trust Points worden geïnstalleerd.

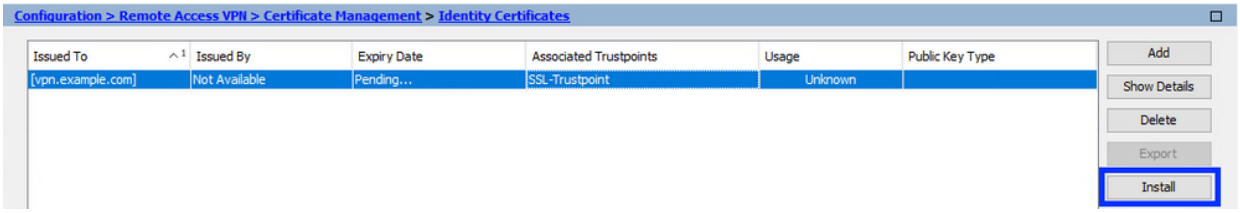
---

   c. Klik op Install Certificate (Certificaat installeren).



2. Installeer het identiteitscertificaat

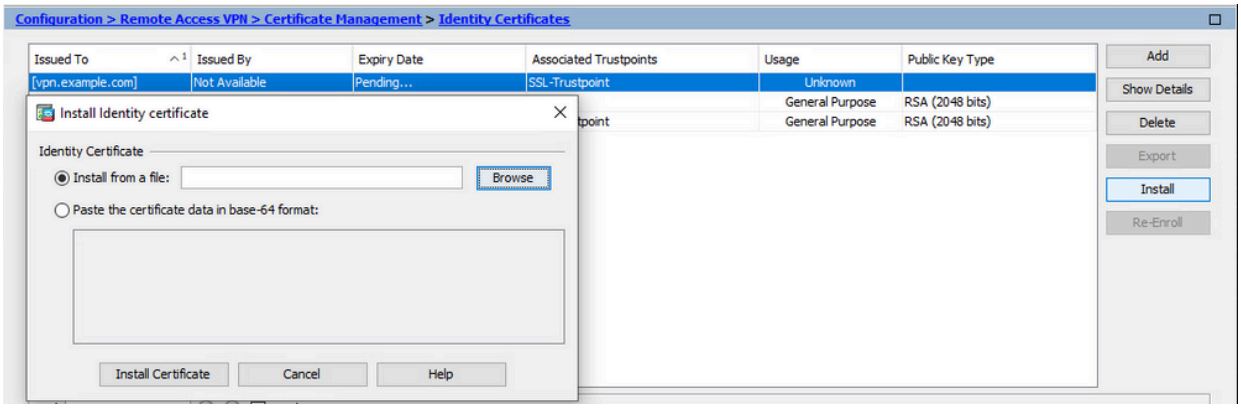
   a. Kies het identiteitscertificaat dat eerder tijdens de MVO-generatie is gemaakt. Klik op Install (Installeren).



Opmerking: het identiteitscertificaat kan per veld zijn afgegeven als niet beschikbaar en het veld Vervaldatum als hangend.

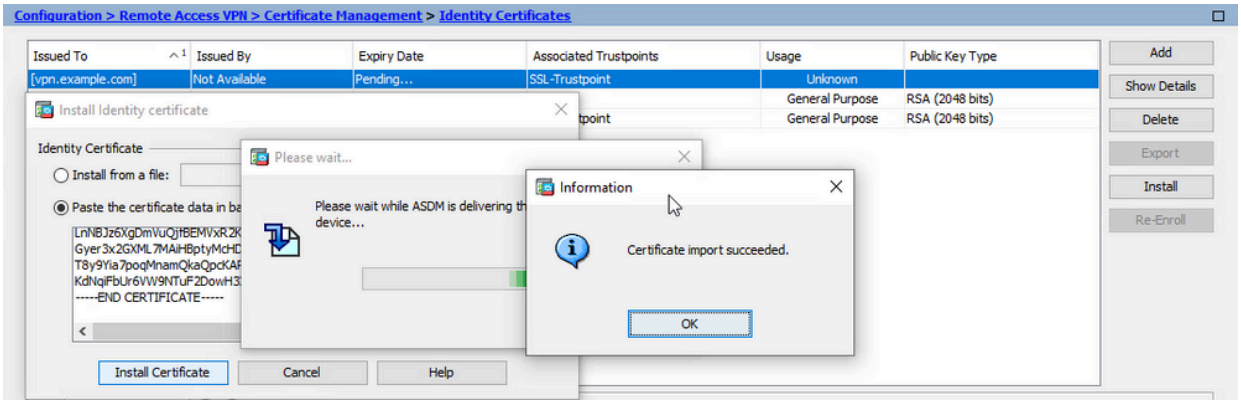
---

   b. Kies een bestand dat het PEM-gecodeerde identiteitscertificaat bevat dat u van de CA hebt ontvangen, of open het PEM-gecodeerde certificaat in een teksteditor en kopieer en plak het door de CA verstrekte identiteitscertificaat in het tekstveld.



Opmerking: identiteitscertificaat kan worden geïnstalleerd in .pem, .cer, .crt formaat.

c. Klik op Install Certificate (Certificaat installeren).



3. Bind het nieuwe certificaat aan Interface met ASDM

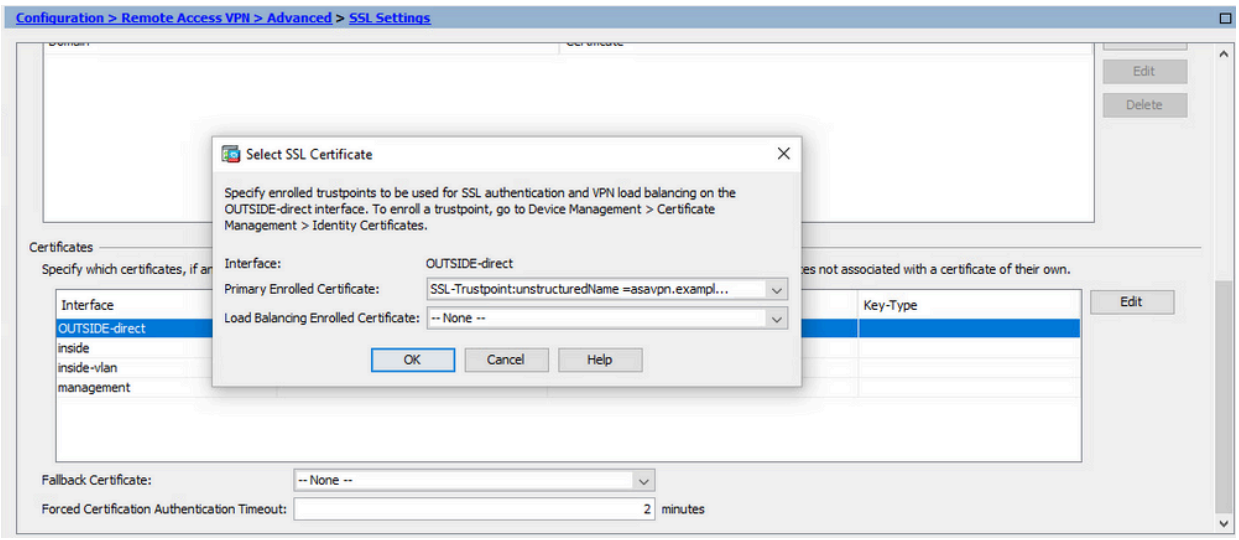
ASA moet worden geconfigureerd om het nieuwe identiteitscertificaat te gebruiken voor WebVPN-sessies die eindigen op de gespecificeerde interface.

a. Ga naar Configuration > Remote Access VPN > Advanced > SSL Settings (Configuratie > VPN voor externe toegang > Geavanceerd > SSL-instellingen).

b. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.

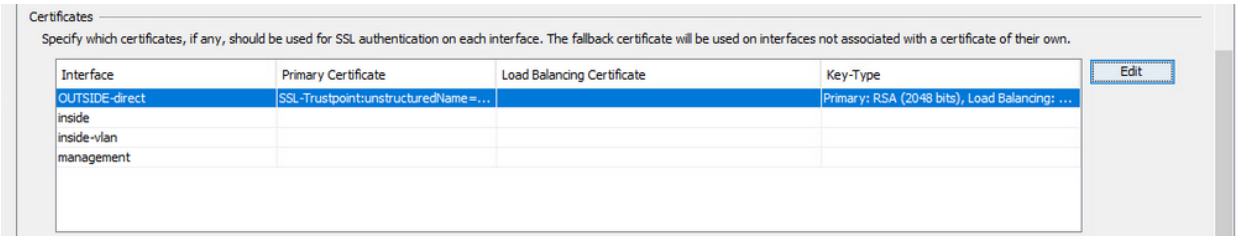
Klik op Edit (Bewerken).

c. Kies in de vervolgkeuzelijst Certificate (Certificaat) het nieuw geïnstalleerde certificaat.



d. Klik op OK.

e. Klik op Apply (Toepassen).



Nu wordt het nieuwe identiteitsbewijs gebruikt.

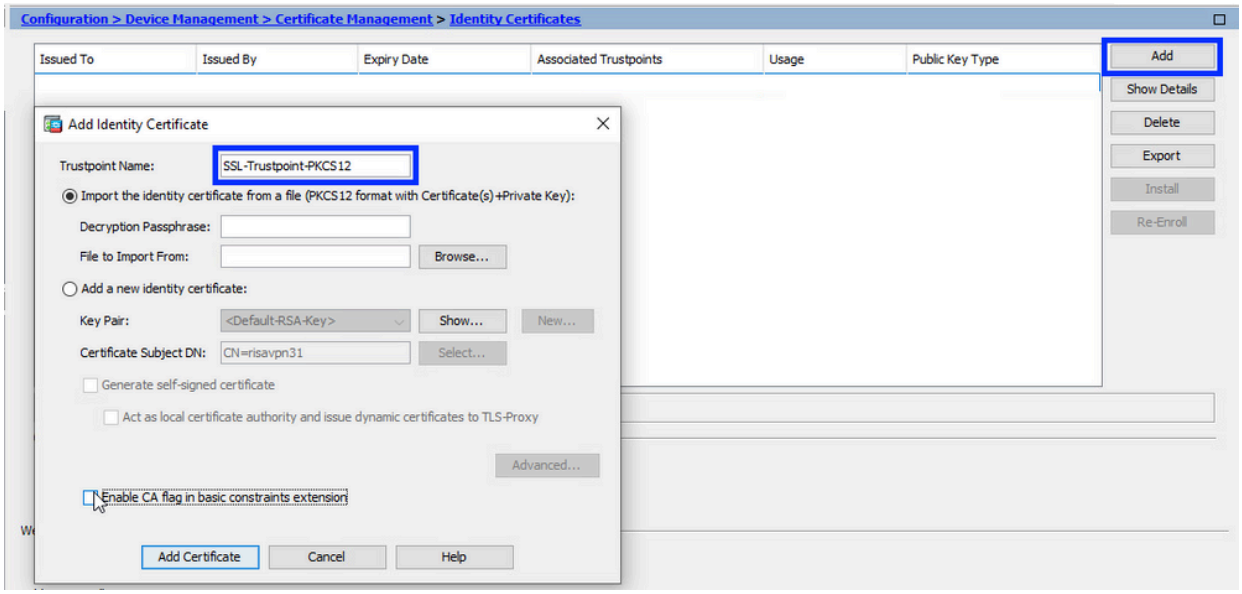
Installeer een Identity Certificate dat is ontvangen in PKCS 12-formaat met ASDM

Het PKCS12-bestand (.p12- of .pfx-formaat) bevat identiteitsbewijs, sleutelpaar en CA-certificaat(en). Het wordt gemaakt door de CA, bijvoorbeeld in het geval van wildcard certificaat, of geëxporteerd van een ander apparaat. Het is een binair bestand, kan niet worden bekeken met teksteditor.

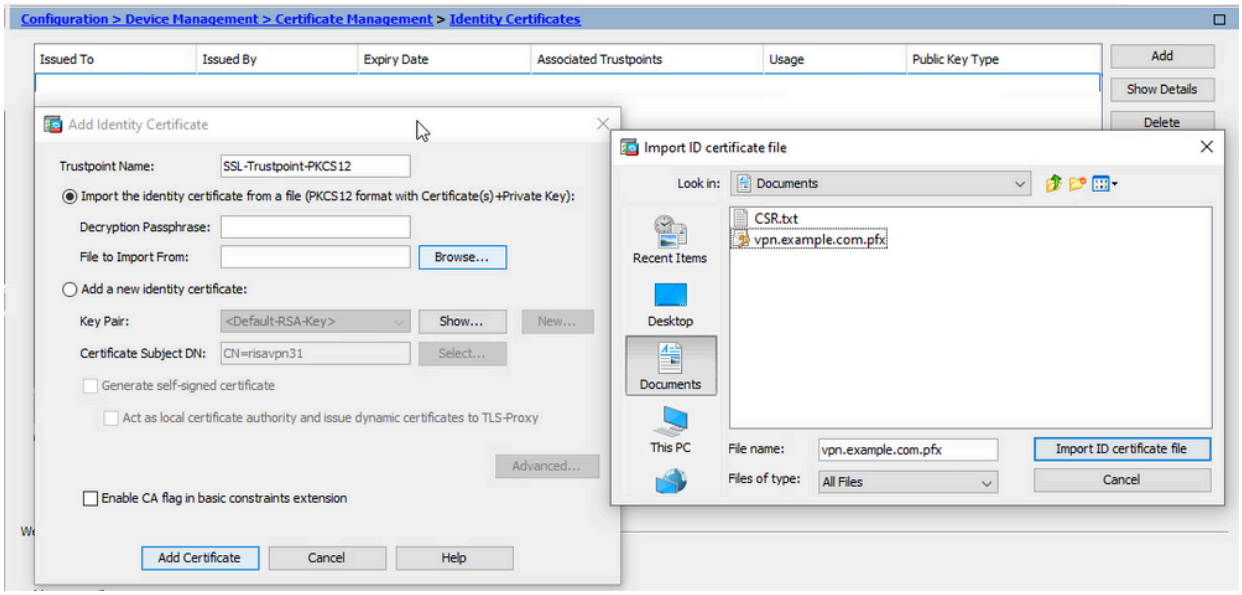
1. Installeer de Identity en CA-certificaten uit een PKCS12-bestand

Het identiteitsbewijs, CA-certificaat(en) en sleutelpaar moeten worden gebundeld in één PKCS12-bestand.

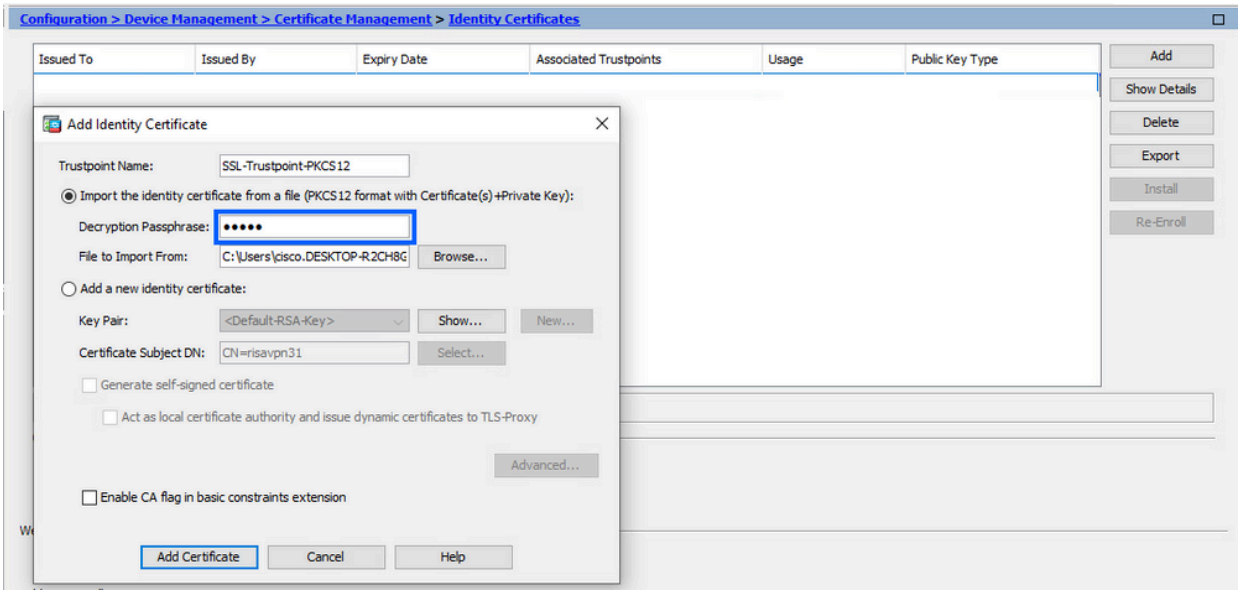
a. Navigeer naar Configuratie > Apparaatbeheer > Certificaatbeheer en kies Identity Certificates.
b. Klik op Add (Toevoegen).
c. Geef een naam op bij Trustpoint Name (Naam van vertrouwenspunt).



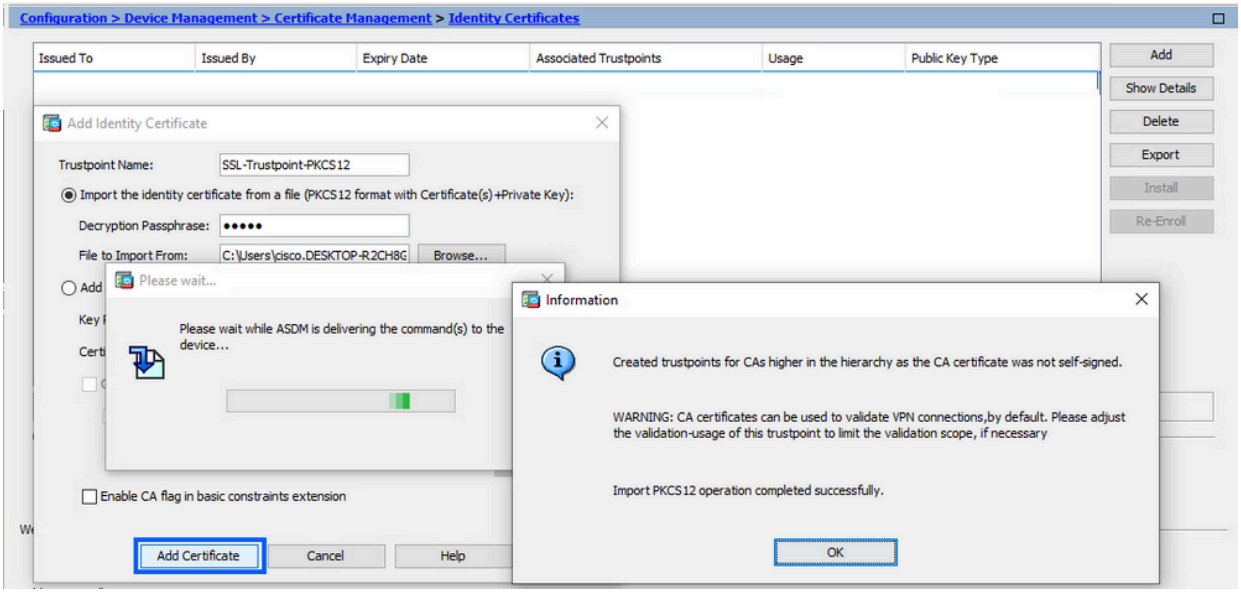
d. Klik op het keuzerondje Import the identity certificate from a file (Identiteitscertificaat importeren uit een bestand).



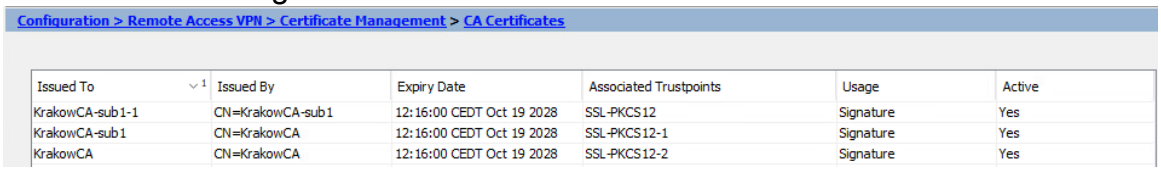
e. Geef bij Decryption Passphrase (Wachtwoord voor ontsleuteling) het wachtwoord op dat is gebruikt om het PKCS12-bestand te maken.



f. Klik op Add Certificate (Certificaat toevoegen).



Opmerking: Wanneer u een PKCS12 met CA-certificatenketen importeert, creëert de ASDM automatisch de upstream CA-trustpoints met namen met een -nummer-achtervoegsel.



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. Bind het nieuwe certificaat aan Interface met ASDM

ASA moet worden geconfigureerd om het nieuwe identiteitscertificaat te gebruiken voor WebVPN-sessies die eindigen op de gespecificeerde interface.

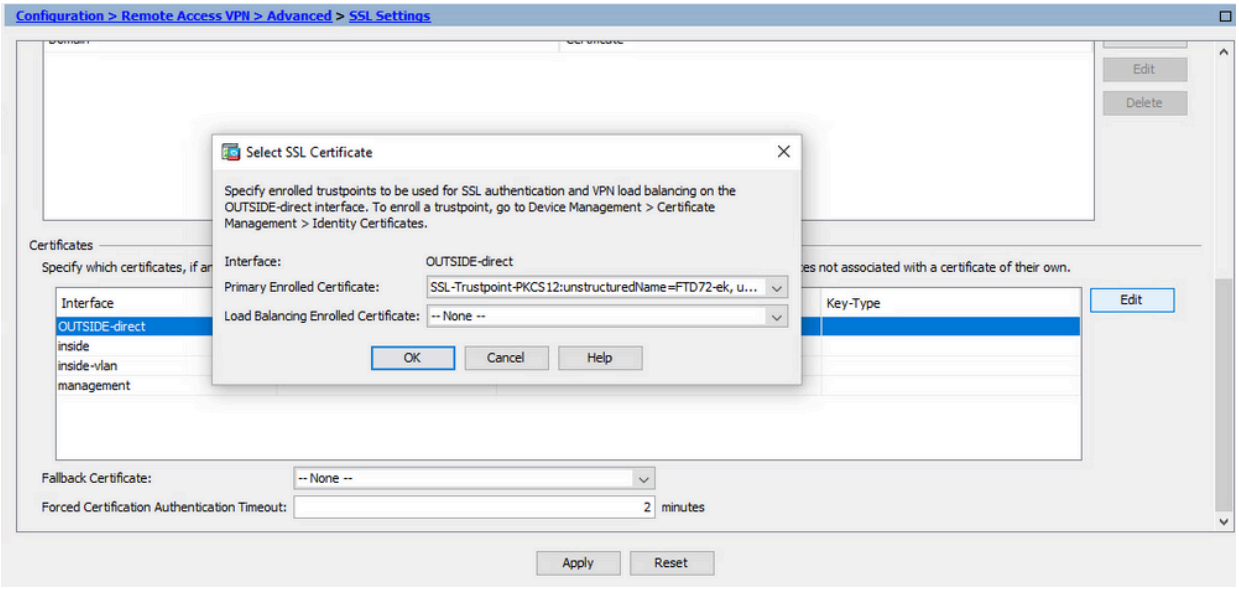
a. Ga naar Configuration > Remote Access VPN > Advanced > SSL Settings

(Configuratie > VPN voor externe toegang > Geavanceerd > SSL-instellingen).

b. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.

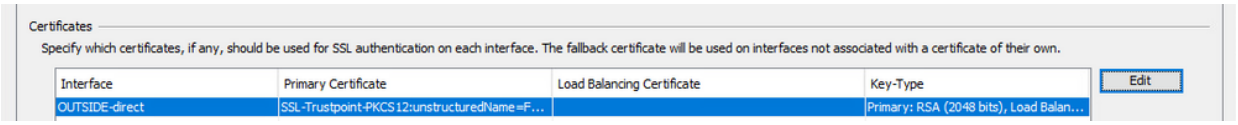
Klik op Edit (Bewerken).

c. Kies in de vervolgkeuzelijst Certificate (Certificaat) het nieuw geïnstalleerde certificaat.



d. Klik op OK.

e. Klik op Apply (Toepassen).



Nu wordt het nieuwe identiteitsbewijs gebruikt.

Certificaat-verlenging

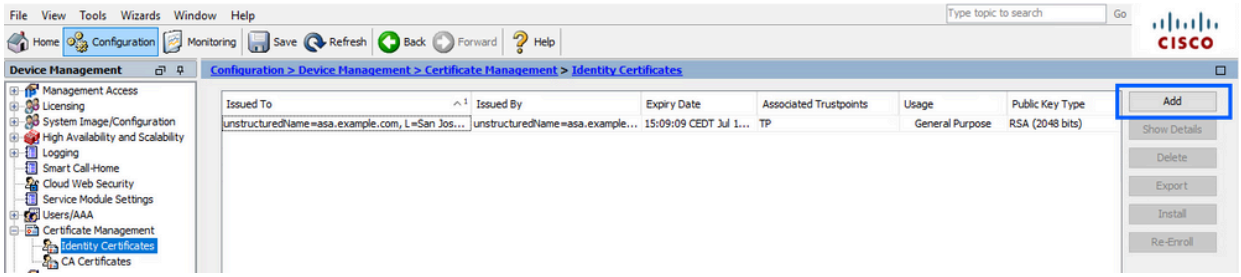
Verleng een certificaat dat is ingeschreven met aanvraag voor certificaatondertekening (CSR) met ASDM

Certificaatverlenging van CSR-ingeschreven certificaat vereist om een nieuw Trustpoint te creëren en in te schrijven. Het moet een andere naam hebben (bijvoorbeeld oude naam met jaarachtervoegsel inschrijven). Het kan dezelfde parameters en sleutelpaar gebruiken als het oude certificaat, of verschillende.

Genereert een CSR met ASDM

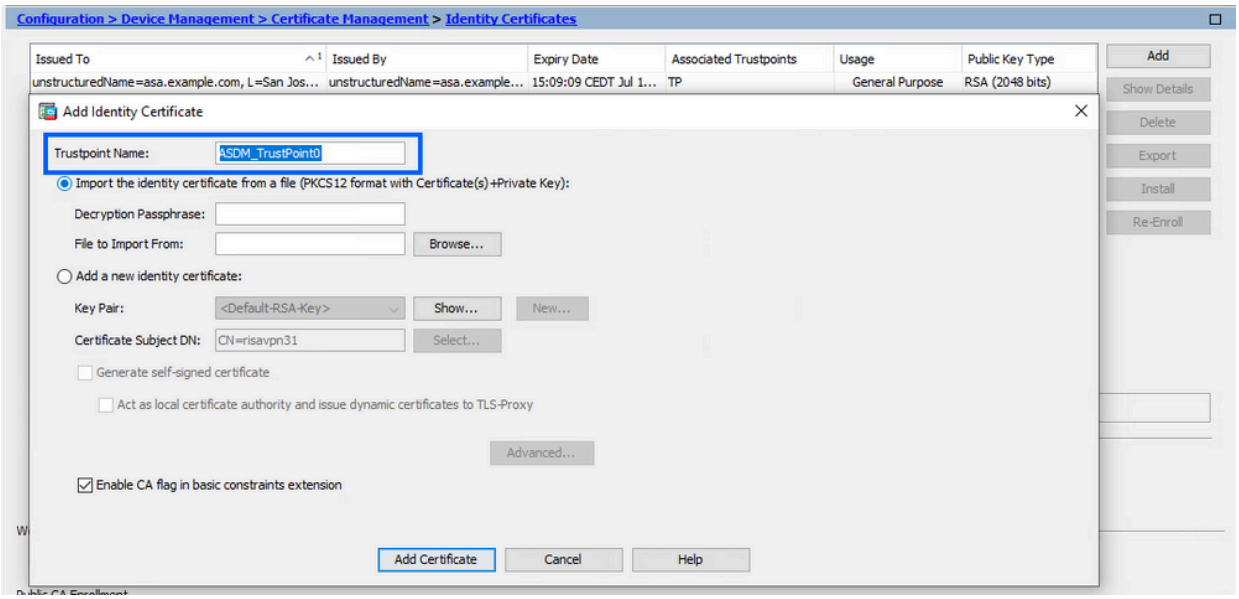
1. Maak een nieuw Trustpoint met een specifieke naam.

a. Blader naar Configuratie > Apparaatbeheer > Certificaatbeheer > Identity Certificates.



b. Klik op Add (Toevoegen).

c. Definieer een trustpoint naam.



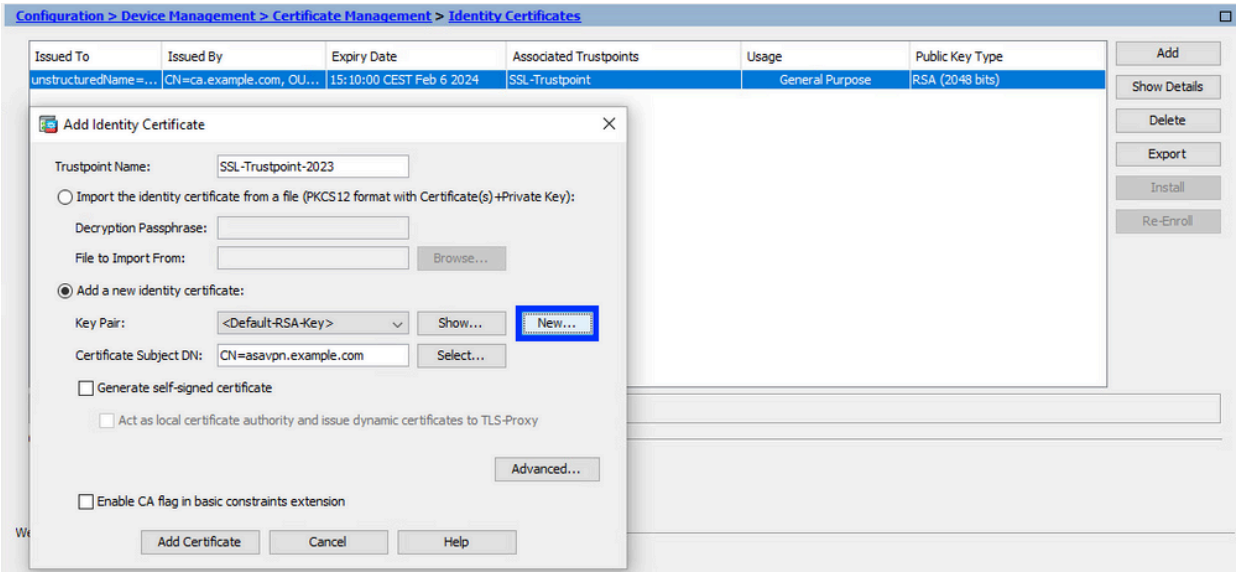
d. Klik op het keuzerondje Add a new identity certificate (Voeg een nieuw identiteitscertificaat toe).

2. (Optioneel) Maak een nieuw sleutelpaar

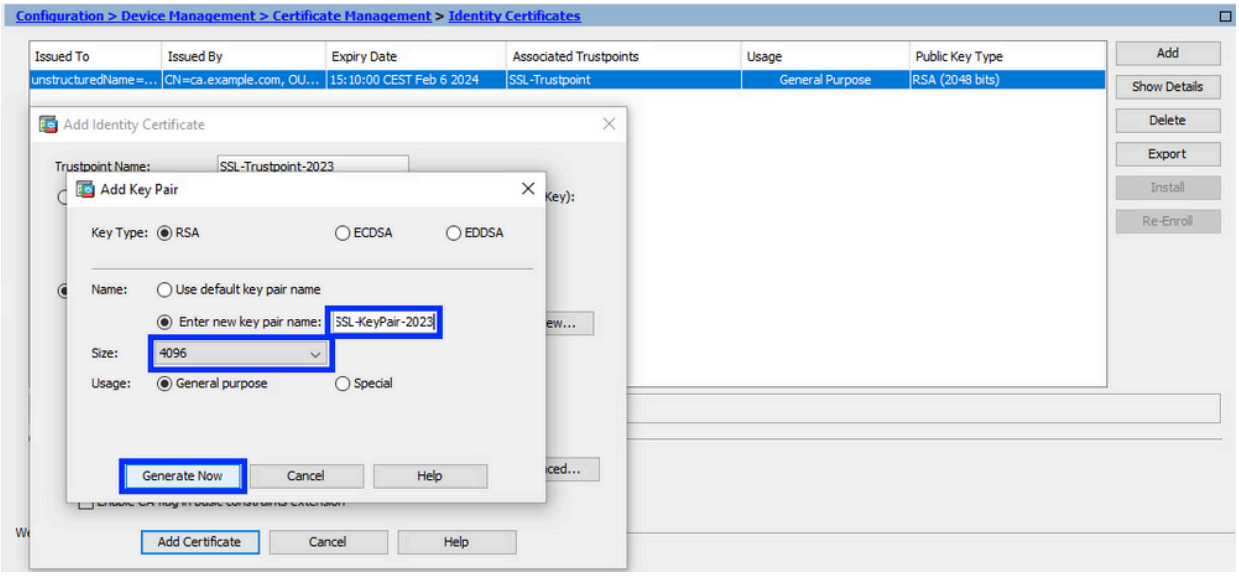
Opmerking: standaard wordt de RSA-toets met de naam Default-RSA-Key en een grootte van 2048 gebruikt. Het wordt echter aanbevolen om voor elk Identity Certificate een uniek privaat/publiek sleutelpaar te gebruiken.

---

a. Klik op Nieuw om een nieuw sleutelpaar te genereren.

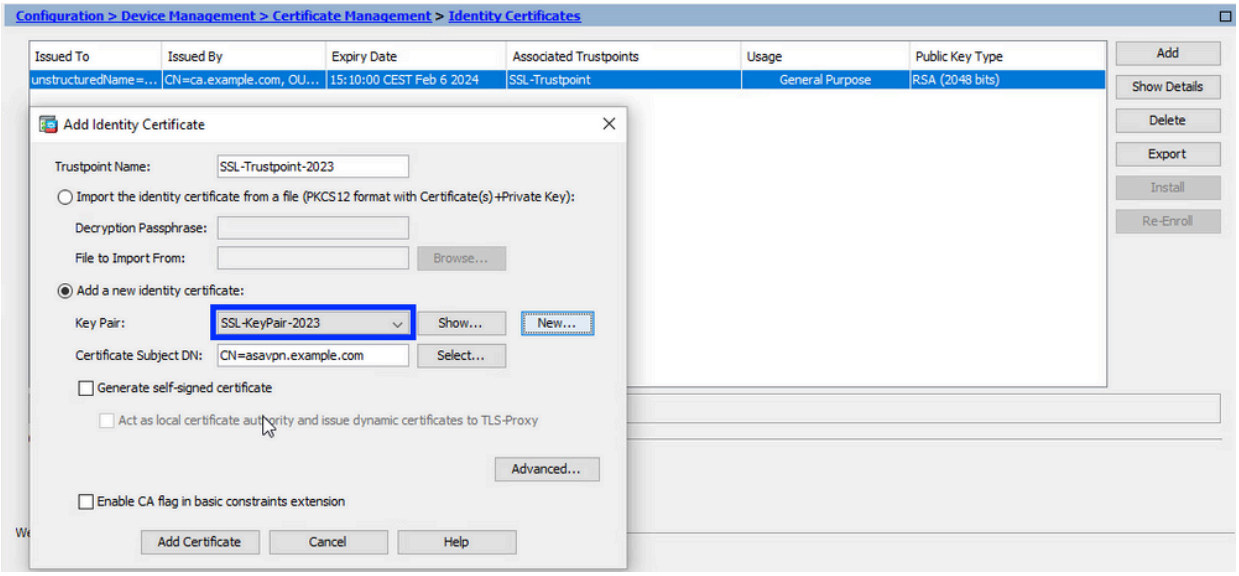


b. Kies de optie Voer een nieuwe naam in voor het sleutelpaar en voer een naam in voor het nieuwe sleutelpaar.
c. Selecteer RSA of ECDSA bij Key Type (Sleuteltype).
d. Kies de sleutelgrootte; voor RSA, kies algemeen doel voor Gebruik.
e. Klik op Generate Now (Nu genereren). Het sleutelpaar wordt nu gecreëerd.



3. Selecteer de naam van het sleutelpaar

Kies het sleutelpaar om de MVO te ondertekenen met, en te worden gebonden aan het nieuwe certificaat.



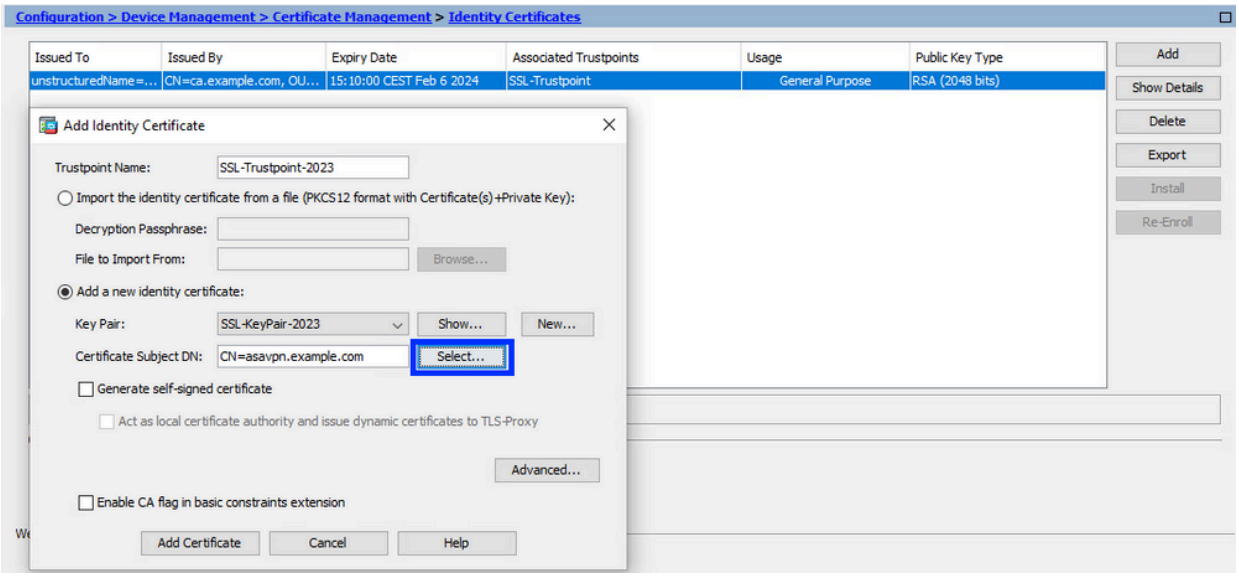
4. Configureer het certificaatonderwerp en de volledig gekwalificeerde domeinnaam (FQDN)

Waarschuwing: de FQDN-parameter moet overeenkomen met de FQDN of het IP-adres van de ASA-interface waarvoor het certificaat wordt gebruikt. Deze parameter stelt de alternatieve onderwerpnaam (SAN) voor het certificaat in. Het SAN-veld wordt gebruikt door SSL/TLS/IKEv2-client om te controleren of het certificaat overeenkomt met de FQDN waarmee verbinding is gemaakt.

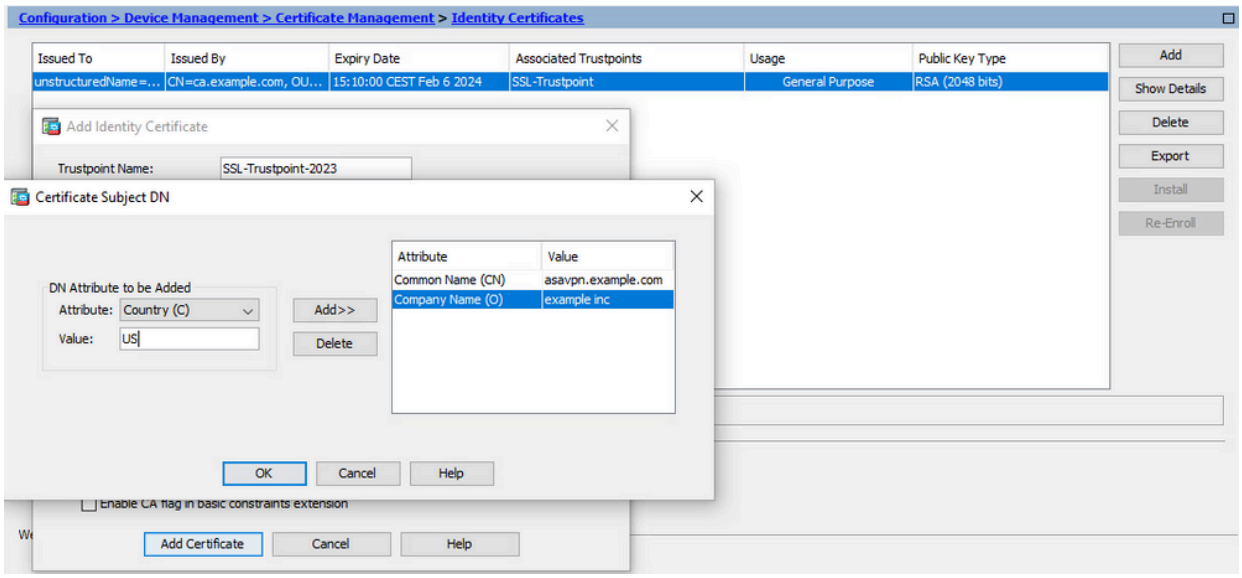
Opmerking: CA kan de FQDN- en onderwerpnamen die in het trustpoint zijn gedefinieerd, wijzigen wanneer het de CSR ondertekent en een ondertekend identiteitscertificaat aanmaakt.

---

a. Klik op Selecteren.



b. Configureer in het venster CertificaatonderwerpDN de certificaatkenmerken - selecteer attribuut uit de vervolgkeuzelijst, voer de waarde in en klik op Toevoegen.

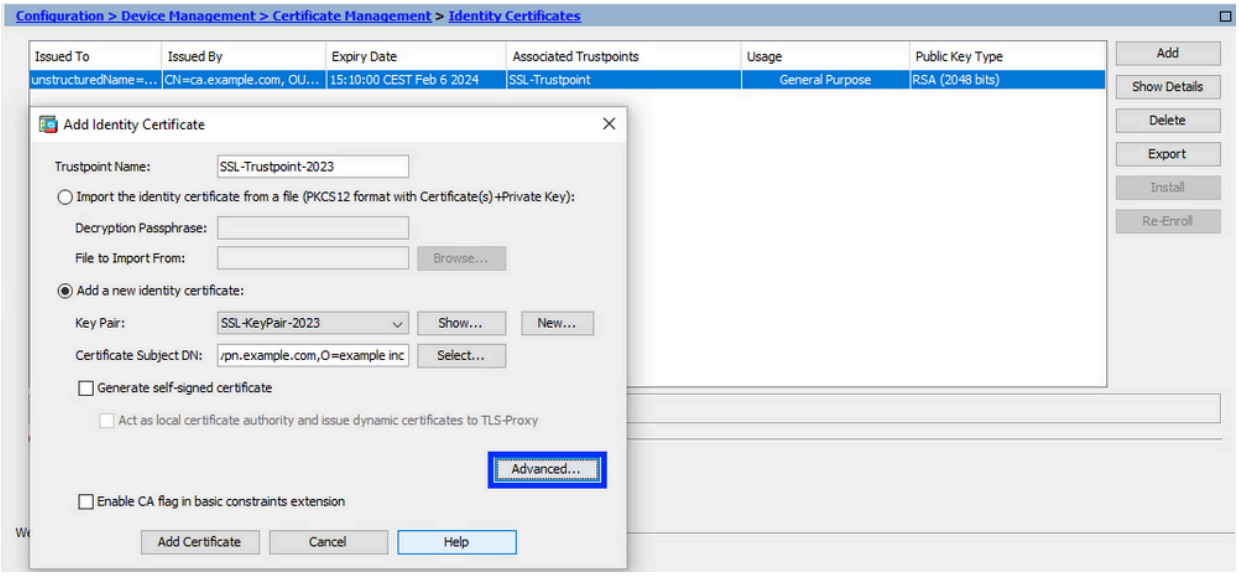


Kenmerk	Beschrijving
CN	De naam waardoor de firewall kan worden benaderd (meestal de volledig gekwalificeerde domeinnaam, bijvoorbeeld vpn.example.com).
OU	De naam van uw afdeling binnen de organisatie
O	De wettelijk geregistreerde naam van uw organisatie/bedrijf
C	Landnummer (2-lettercode zonder punctuatie)
ST	De staat waarin uw organisatie is gevestigd.
L	De stad waar uw organisatie zich bevindt.
EA	E-mailadres

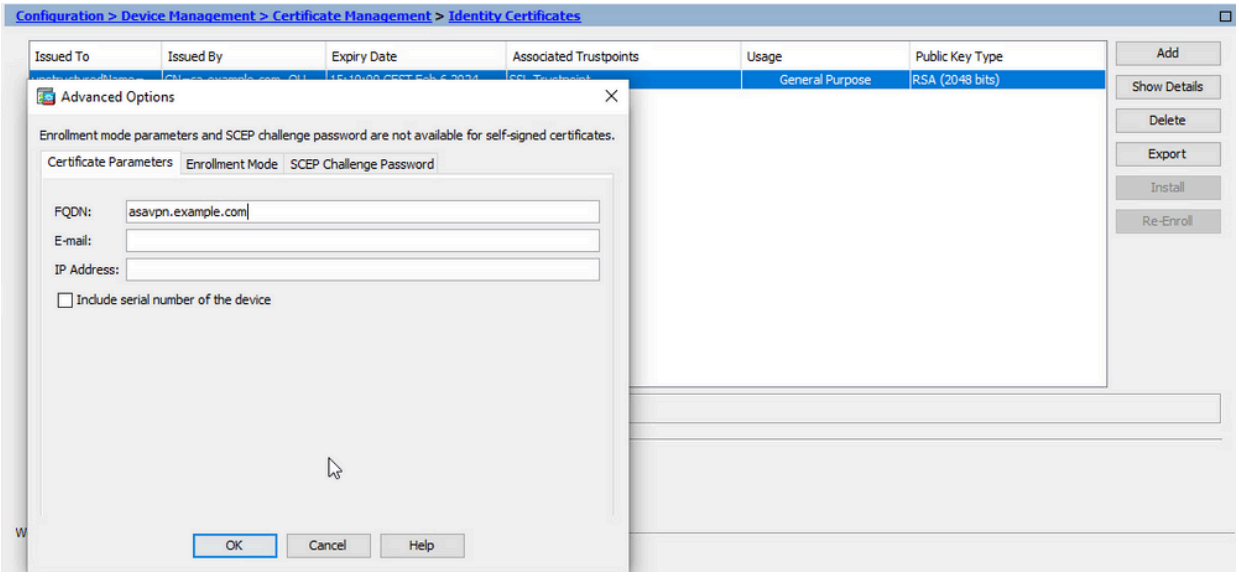
N.B.: Geen van de vorige velden kan een waarde van 64 tekens overschrijden. Een langere waarde kan problemen opleveren met de installatie van het identiteitscertificaat. Het is ook niet nodig om alle DN-kenmerken te definiëren.

Klik op OK nadat alle kenmerken zijn toegevoegd.

c. Om apparaat FQDN te configureren klikt u op Geavanceerd.

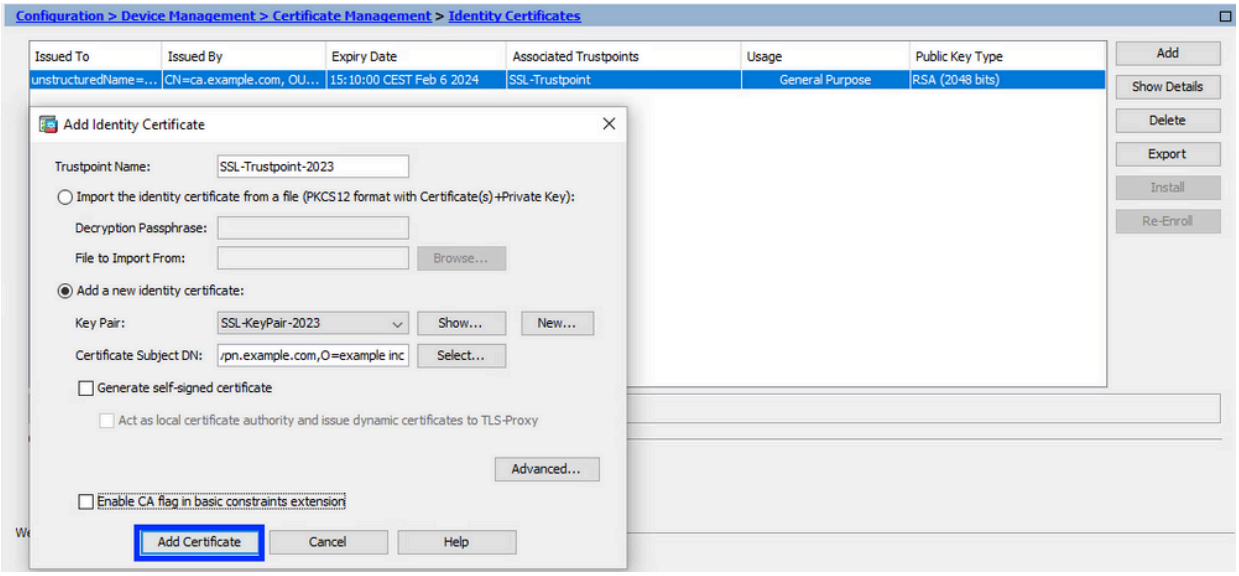


d. Voer in het veld FQDN de volledig gekwalificeerde domeinnaam in via welke het apparaat via internet toegankelijk is. Klik op OK.

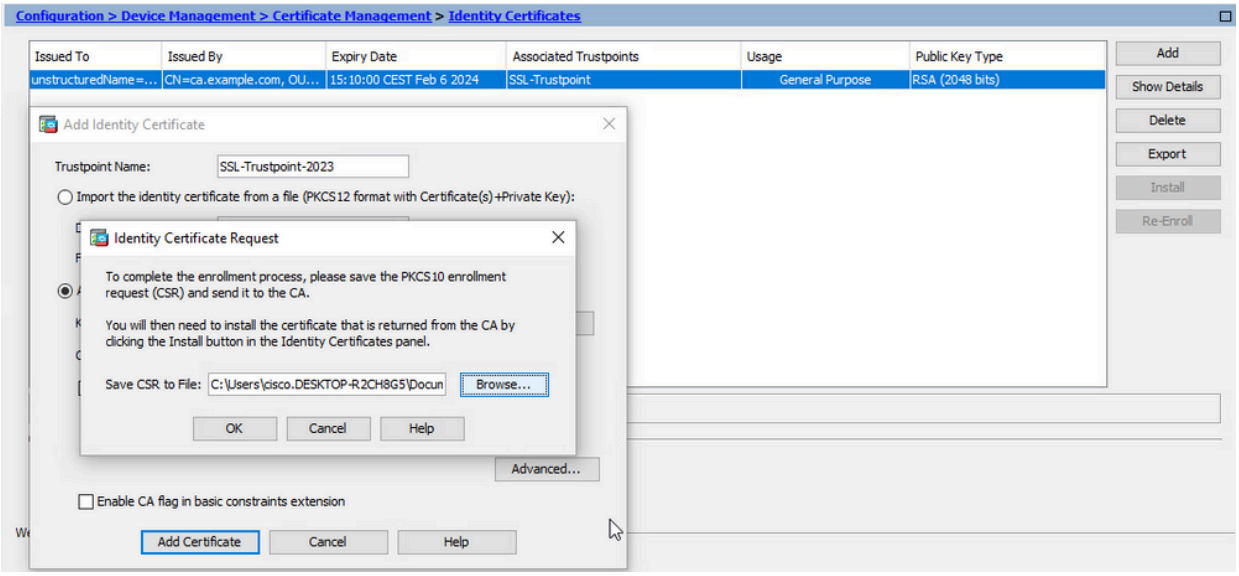


5. MVO genereren en opslaan

a. Klik op Add Certificate (Certificaat toevoegen).



b. Vervolgens wordt een scherm getoond met het verzoek de CSR op te slaan.

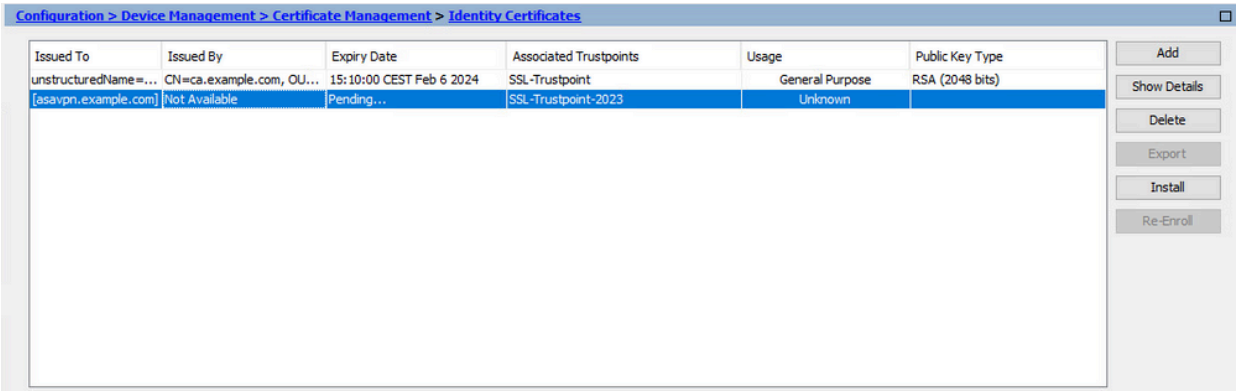


Klik op Bladeren. Kies een locatie waar u de CSR wilt opslaan en sla het bestand op met de extensie .txt.

> Opmerking: Wanneer het bestand met de extensie .txt wordt opgeslagen, kan het PKCS#10-verzoek worden geopend en bekeken met een teksteditor (zoals Kladblok).

---

c. Nu wordt het nieuwe trustpoint weergegeven in een hangende staat.



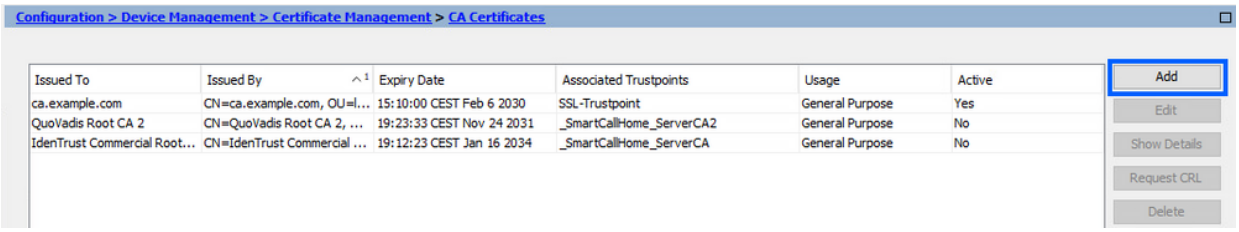
Installeer het identiteitscertificaat in PEM-formaat met ASDM

De installatiestappen gaan ervan uit dat de CA de CSR heeft ondertekend en een PEM-gecodeerd pakket (.pem, .cer, .crt) heeft geleverd met een nieuw identiteitscertificaat en CA-certificaatbundel.

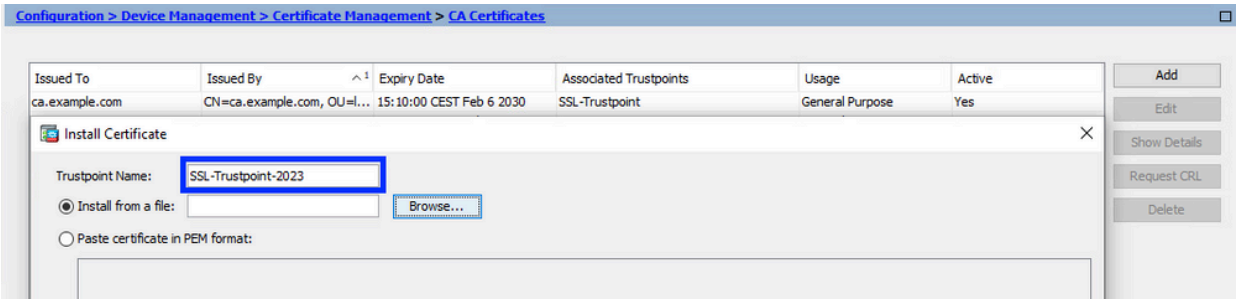
1. CA-certificaat installeren dat de CSR heeft ondertekend

   Het CA-certificaat dat het Identity Certificate heeft ondertekend, kan worden geïnstalleerd in het Trustpoint dat voor Identity Certificate is gecreëerd. Als het Identity Certificate is ondertekend door een bemiddelende CA, kan dit CA-certificaat worden geïnstalleerd in het Identity Certificate Trustpoint. Alle CA-certificaten stroomopwaarts in de hiërarchie kunnen worden geïnstalleerd in afzonderlijke CA Trustpoints.

   a. Navigeer naar Configuration > Device Management >Certificate Management > en kies CA-certificaten. Klik op Add (Toevoegen).



   b. Voer de naam van Trustpoint in en kies Installeren uit bestand, klik op Bladeren knop en kies het tussenliggende certificaat. U kunt ook het PEM-gecodeerde CA-certificaat vanuit een tekstbestand in het tekstveld plakken.

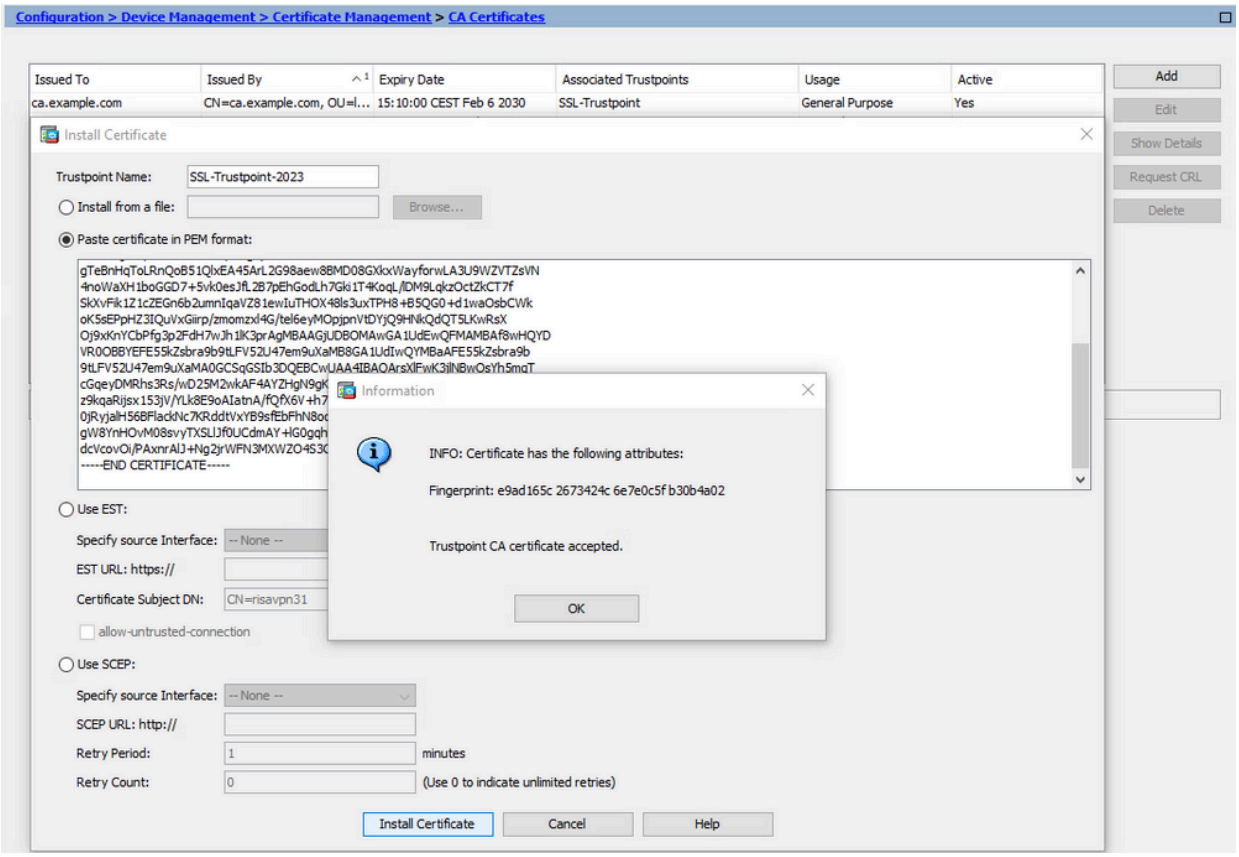


Opmerking: Installeer het tussentijdse certificaat met dezelfde vertrouwenspuntnaam als de vertrouwenspuntnaam van het identiteitsbewijs,

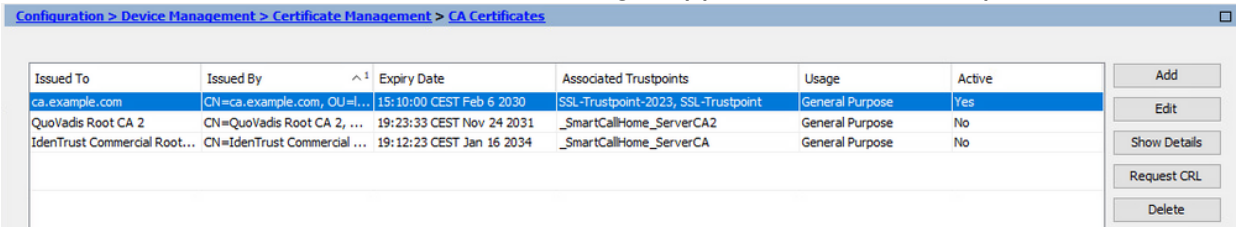
---

indien het identiteitsbewijs is ondertekend door een tussenliggend CA-certificaat.

c. Klik op Install Certificate (Certificaat installeren).

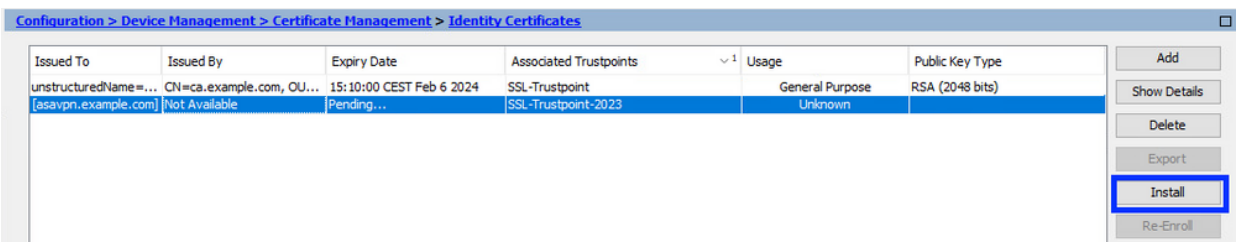


In het voorbeeld wordt het nieuwe certificaat ondertekend met hetzelfde CA-certificaat als het oude. Hetzelfde CA-certificaat is nu gekoppeld aan twee Trustpoints.



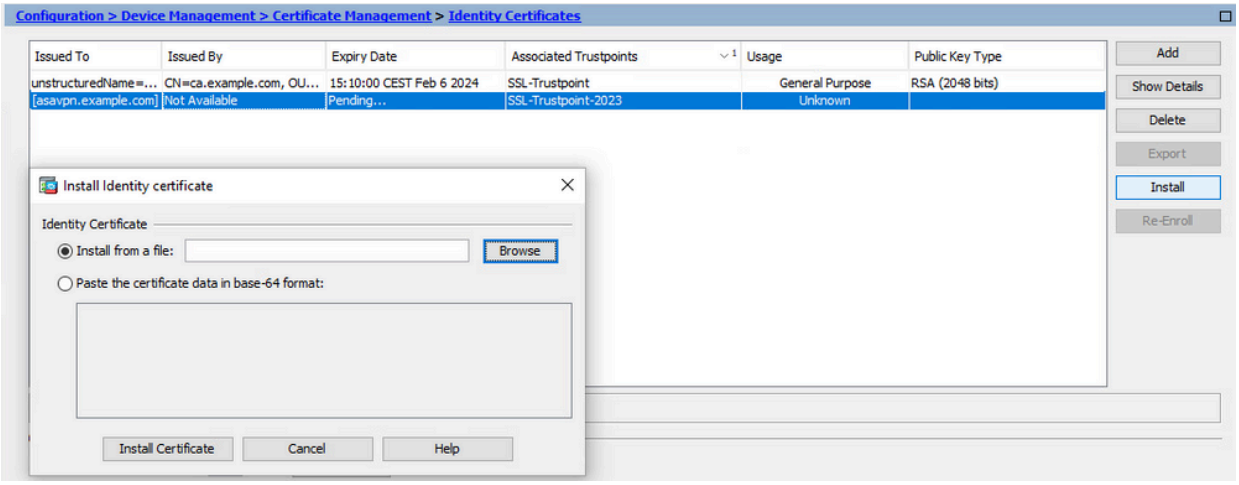
2. Installeer het identiteitscertificaat

a. Kies het identiteitscertificaat dat eerder met de MVO-generatie is gemaakt. Klik op Install (Installeren).



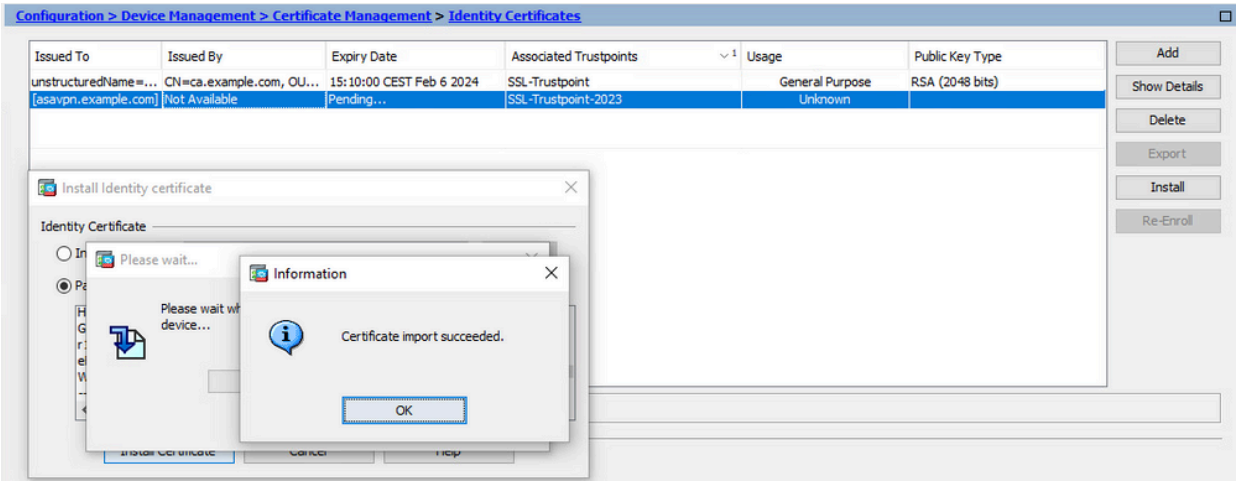
Opmerking: het identiteitscertificaat kan per veld zijn afgegeven als niet beschikbaar, en het veld Vervaldatum als hangend.

b. Kies een bestand dat het PEM-gecodeerde identiteitscertificaat bevat dat u van de CA hebt ontvangen, of open het PEM-gecodeerde certificaat in een teksteditor en kopieer en plak het door de CA verstrekte identiteitscertificaat naar het tekstveld.

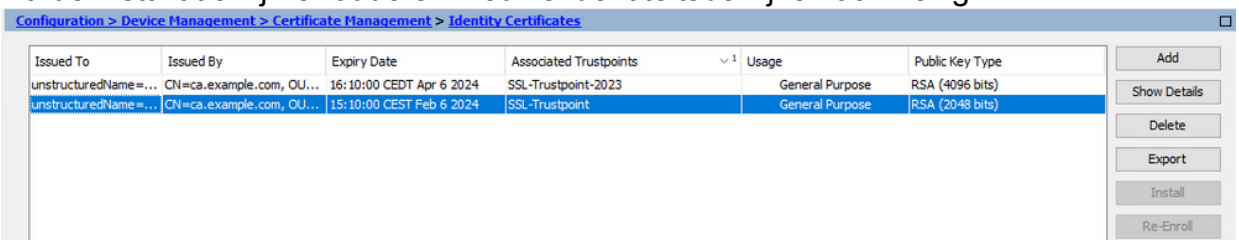


Opmerking: identiteitscertificaat kan worden geïnstalleerd in .pem, .cer, .crt formaat.

c. Klik op Install Certificate (Certificaat installeren).



Na de installatie zijn er oude en nieuwe identiteitsbewijzen aanwezig.



3. Bind het nieuwe certificaat aan Interface met ASDM

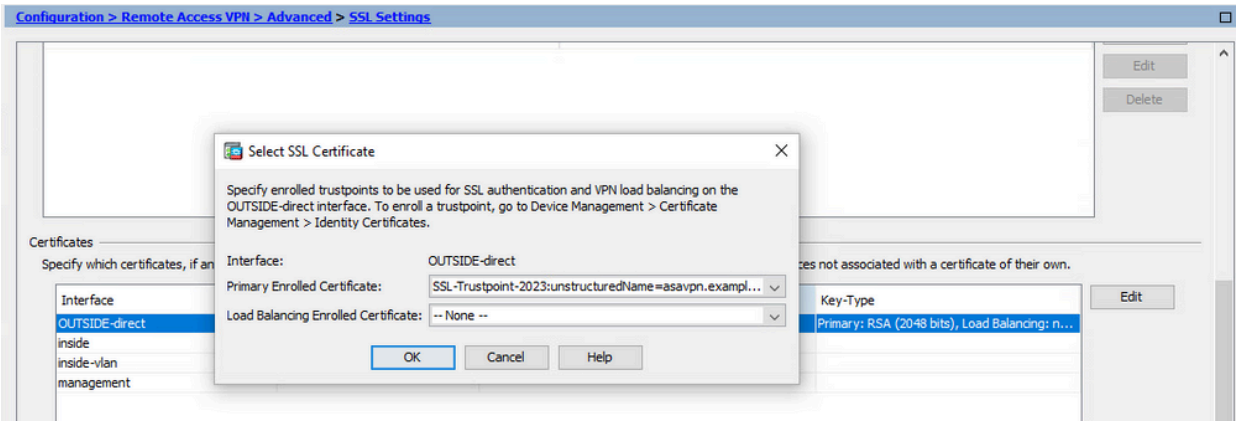
ASA moet worden geconfigureerd om het nieuwe identiteitscertificaat te gebruiken voor WebVPN-sessies die eindigen op de gespecificeerde interface.

a. Ga naar Configuration > Remote Access VPN > Advanced > SSL Settings (Configuratie > VPN voor externe toegang > Geavanceerd > SSL-instellingen).

b. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.

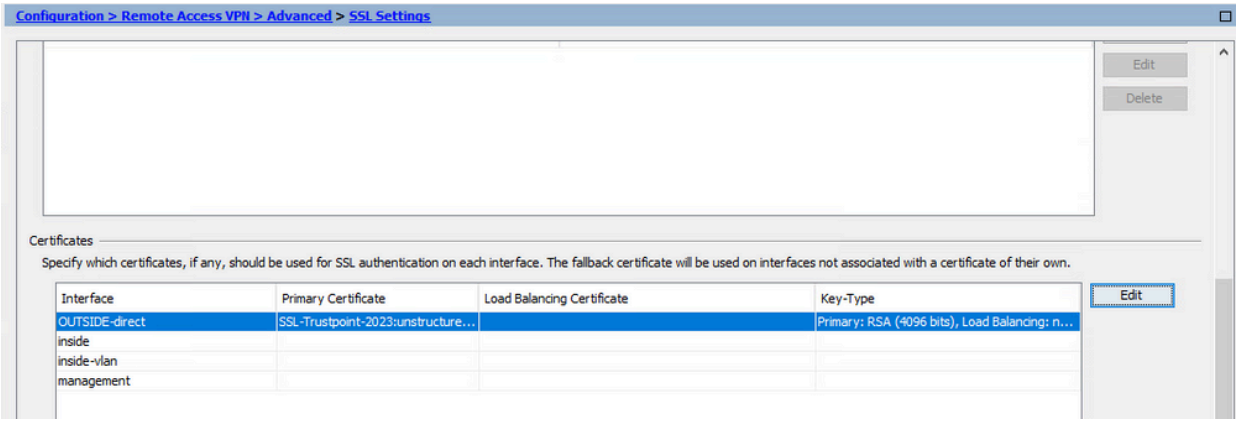
   Klik op Edit (Bewerken).

c. Kies in de vervolgkeuzelijst Certificate (Certificaat) het nieuw geïnstalleerde certificaat.



d. Klik op OK.

e. Klik op Apply (Toepassen). Nu wordt het nieuwe identiteitsbewijs gebruikt.



Verleng een certificaat dat is ingeschreven voor PKCS 12-bestand met ASDM

Certificaat verlenging van PKCS12 ingeschreven certificaat vereist om een nieuw Trustpoint te maken en in te schrijven. Het moet een andere naam hebben (bijvoorbeeld oude naam met jaarachtervoegsel inschrijven).

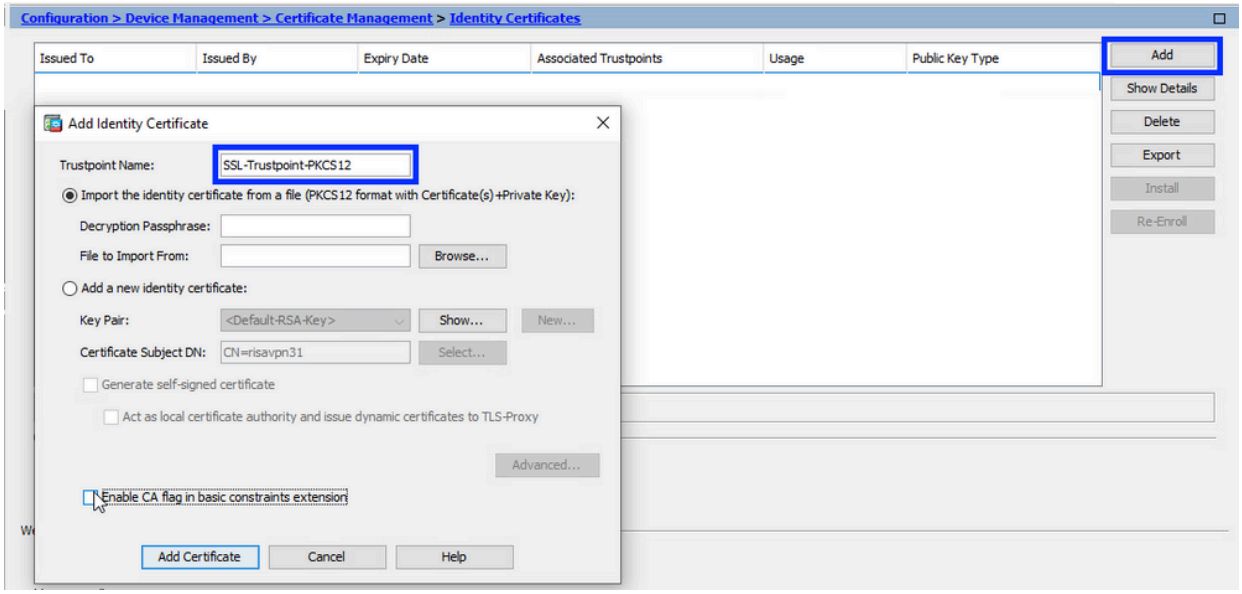
Het PKCS12-bestand (.p12- of .pfx-formaat) bevat identiteitsbewijs, sleutelpaar en CA-certificaat(en). Het wordt gemaakt door de CA, bijvoorbeeld in het geval van wildcard certificaat, of

geëxporteerd van een ander apparaat. Het is een binair bestand en kan niet worden weergegeven met de teksteditor.

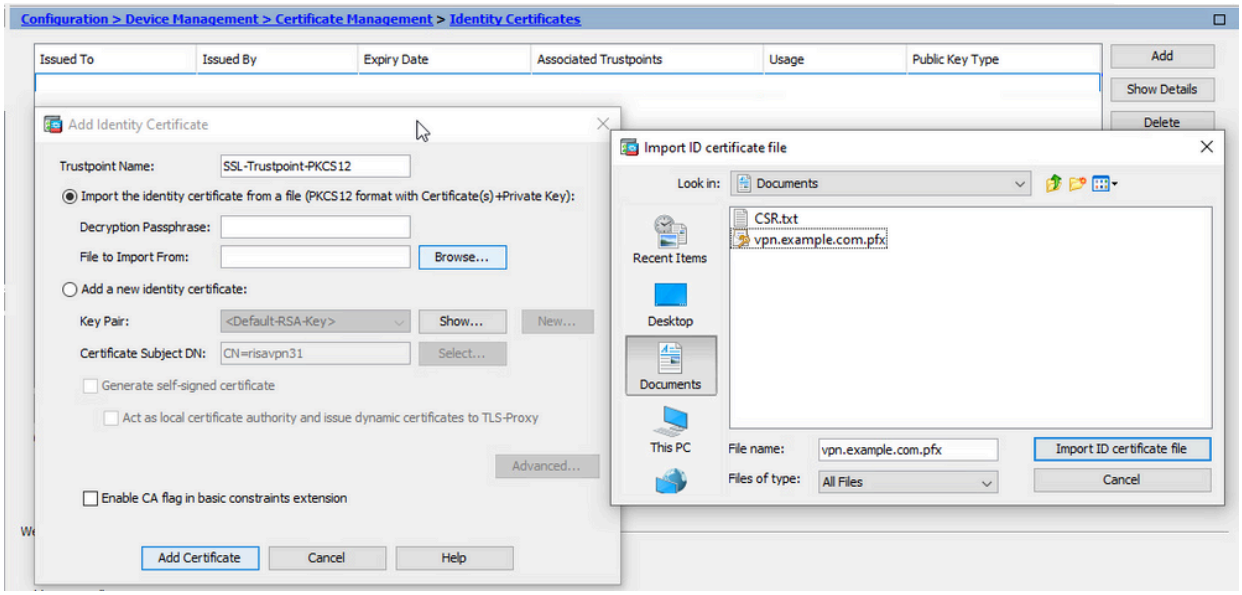
1. Installeer het vernieuwde identiteitscertificaat en CA-certificaten uit een PKCS12-bestand

   Het identiteitsbewijs, CA-certificaat(en) en sleutelpaar moeten worden gebundeld in één PKCS12-bestand.

   a. Navigeer naar Configuratie > Apparaatbeheer > Certificaatbeheer en kies Identity Certificates.
   b. Klik op Add (Toevoegen).
   c. Geef een nieuwe Trustpoint naam op.

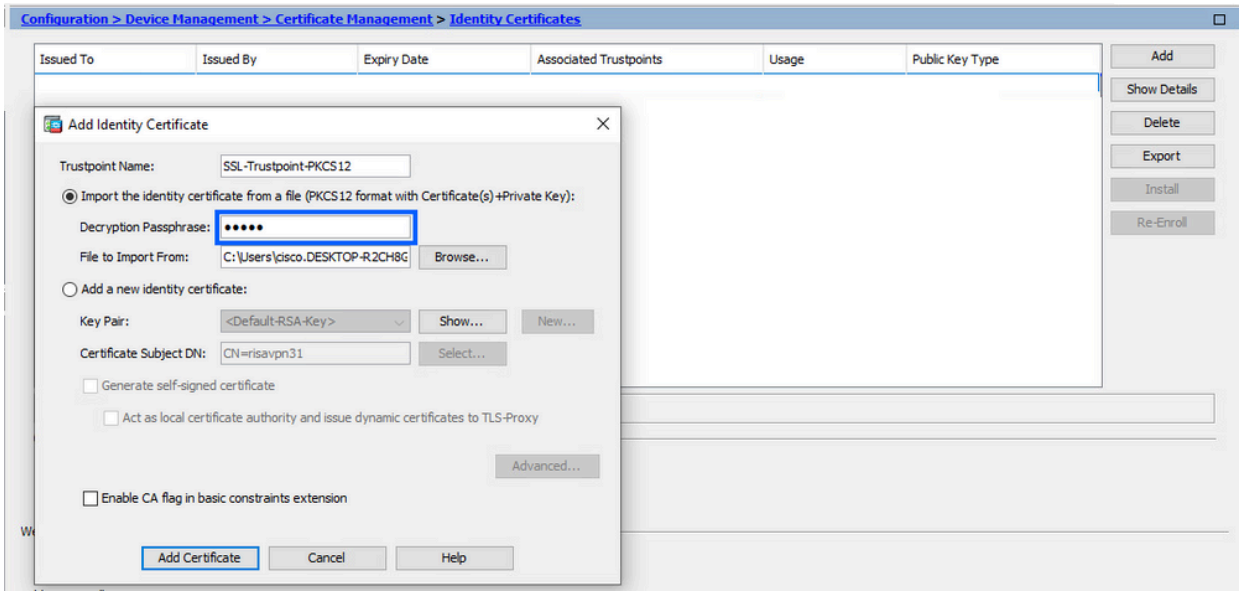


   d. Klik op het keuzerondje Import the identity certificate from a file (Identiteitscertificaat importeren uit een bestand).

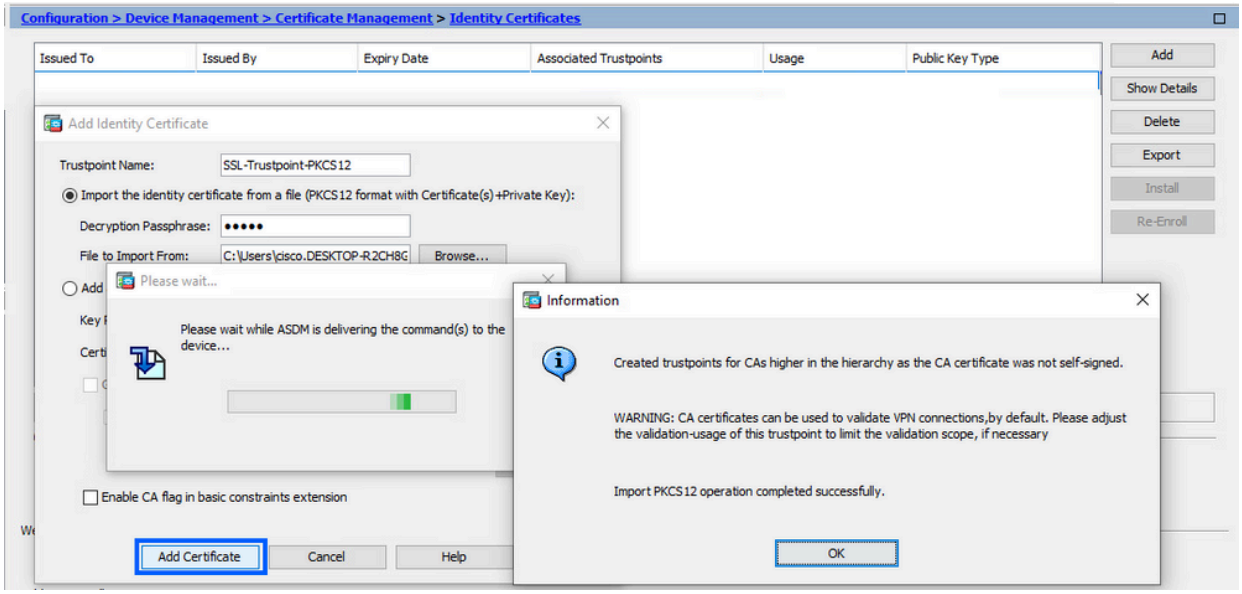


   e. Geef bij Decryption Passphrase (Wachtwoord voor ontsleuteling) het wachtwoord op

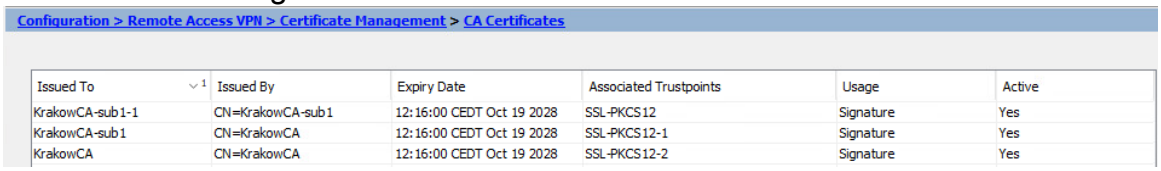
dat is gebruikt om het PKCS12-bestand te maken.



f. Klik op Add Certificate (Certificaat toevoegen).



Opmerking: Wanneer een PKCS12 met CAs-certificaatketen wordt geïmporteerd, creëert de ASDM automatisch de upstream CAs trustpoints met namen met een -nummer achtervoegsel.



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. Bind het nieuwe certificaat aan Interface met ASDM

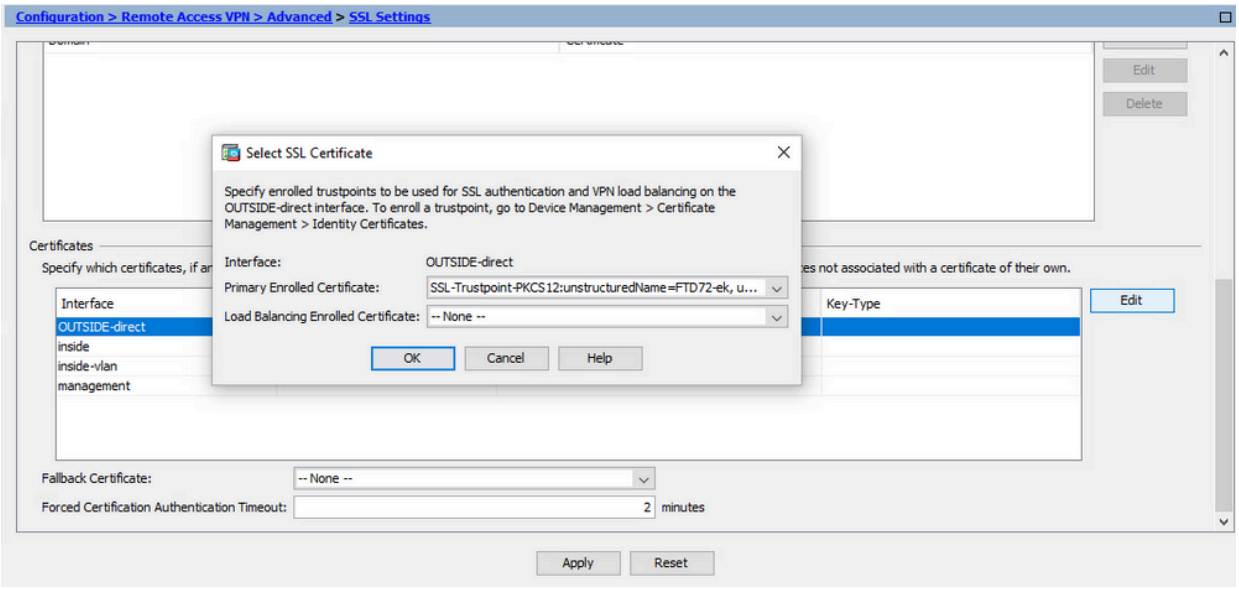
ASA moet worden geconfigureerd om het nieuwe identiteitscertificaat te gebruiken voor WebVPN-sessies die eindigen op de gespecificeerde interface.

a. Ga naar Configuration > Remote Access VPN > Advanced > SSL Settings (Configuratie > VPN voor externe toegang > Geavanceerd > SSL-instellingen).

b. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.

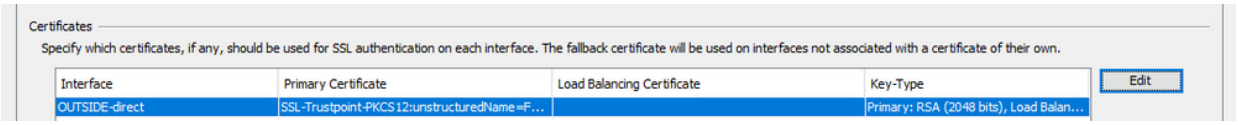
Klik op Edit (Bewerken).

c. Kies in de vervolgkeuzelijst Certificate (Certificaat) het nieuw geïnstalleerde certificaat.



d. Klik op OK.

e. Klik op Apply (Toepassen).



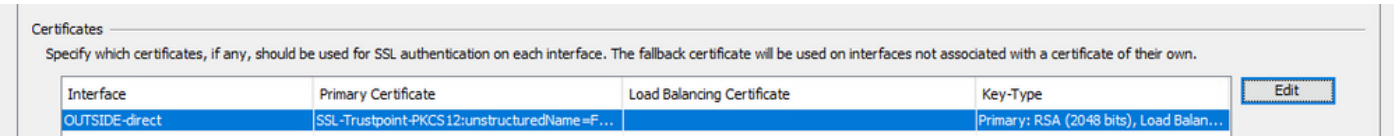
Nu wordt het nieuwe identiteitsbewijs gebruikt.

Verifiëren

Gebruik deze stappen om te controleren of de installatie van het leverancierscertificaat van een derde succesvol is en of u SSL VPN-verbindingen gebruikt.

Geïnstalleerde certificaten bekijken via ASDM

1. Ga naar Configuration > Remote Access VPN > Certificate Management (Configuratie > VPN voor externe toegang > Certificaatbeheer) en selecteer Identity Certificates (Identiteitscertificaten).
2. Het door de derde partij afgegeven identiteitsbewijs kan worden weergegeven.



Problemen oplossen

Deze debug-opdracht moet worden verzameld op de CLI in het geval van een fout bij de installatie van een SSL-certificaat.

- debug crypto ca 14

Veelgestelde vragen

Q.Wat is een PKCS12?
A.In cryptografie, definieert PKCS12 een archiefbestandsindeling die gemaakt is om vele cryptografische objecten als één bestand op te slaan. Het wordt algemeen gebruikt om een privé sleutel met zijn X.509 certificaat te bundelen of alle leden van een ketting van vertrouwen te bundelen.

V.Wat is een MVO?
A. In PKI-systemen (public key infrastructure) is een verzoek om een certificaat te ondertekenen (ook CSR of certificeringsverzoek) een bericht dat door een aanvrager wordt verzonden naar een registratieautoriteit van de openbare sleutelinfrastructuur om een digitaal identiteitscertificaat aan te vragen. Het bevat gewoonlijk de openbare sleutel waarvoor het certificaat kan worden afgegeven, informatie die wordt gebruikt om het ondertekende certificaat te identificeren (zoals een domeinnaam in Onderwerp) en integriteitsbescherming (bijvoorbeeld een digitale handtekening).

Q.Waar is het wachtwoord van de PKCS12?
A.Wanneer certificaten en sleutelparen naar een PKCS12-bestand worden geëxporteerd, wordt het wachtwoord gegeven in de opdracht Exporteren. Voor het importeren van een pkcs12-bestand moet het wachtwoord worden geleverd door de eigenaar van de CA-server of de persoon die de PKCS12 heeft geëxporteerd van een ander apparaat.

Q.Wat is het verschil tussen de wortel en de identiteit?
A. In cryptografie en computerbeveiliging is een basiscertificaat een publiek sleutelcertificaat dat een basiscertificeringsinstantie (CA) identificeert. De certificaten van de wortel zijn zelf-ondertekend (en het is mogelijk voor een certificaat om meerdere vertrouwenswegen te hebben, zeg als het certificaat door een wortel werd uitgegeven die) werd dwars-ondertekend en de basis van een op X.509-gebaseerde openbare zeer belangrijke infrastructuur (PKI) vormde. Een public key certificate, ook wel bekend als een digital certificate of Identity Certificate, is een elektronisch document dat gebruikt wordt om het eigendom van een publieke sleutel te bewijzen. Het certificaat bevat informatie over de sleutel, informatie over de identiteit van de eigenaar (het onderwerp genoemd), en de digitale handtekening van een entiteit die de inhoud van het certificaat heeft geverifieerd (de emittent genoemd). Als de handtekening geldig is, en de software die het

certificaat onderzoekt de emittent vertrouwt, dan kan het die sleutel gebruiken om veilig met het onderwerp van het certificaat te communiceren.

Q.I installeerde de cert, waarom het niet werkt?
A.Dit kan te wijten zijn aan vele redenen, bijvoorbeeld:

1. Het certificaat en trustpoint worden geconfigureerd, maar zijn niet gebonden aan het proces dat het moet gebruiken. Bijvoorbeeld, het te gebruiken trustpoint is niet gebonden aan de buiteninterface die AnyConnect-clients beëindigt.

2. Er wordt een PKCS12-bestand geïnstalleerd, maar dit bevat fouten als gevolg van het ontbreken van een tussentijds CA-certificaat in het PKCS12-bestand. De klanten die het tussenliggende CA-certificaat als betrouwbaar hebben, maar geen basiscertificaat van CA als betrouwbaar hebben, kunnen de gehele certificaatketen niet verifiëren en het server Identity Certificate niet als betrouwbaar rapporteren.

3. Een certificaat met onjuiste kenmerken kan installatiefouten of fouten aan de clientzijde veroorzaken. Bepaalde eigenschappen kunnen bijvoorbeeld met een verkeerd formaat worden gecodeerd. Een andere reden is dat het Identity Certificate ontbreekt. Alternatieve naam (SAN) ontbreekt, of dat de domeinnaam die gebruikt wordt om toegang te krijgen tot de server niet aanwezig is als SAN.

Q. Vereist een installatie van een nieuwe cert een onderhoudsvenster of veroorzaakt onderbreking?
A. De installatie van een nieuw certificaat (identiteit of CA) is niet opdringerig en zou geen onderbreking moeten veroorzaken of een onderhoudsvenster vereisen. Om een nieuw certificaat te kunnen gebruiken voor een service die bestaat, is een wijziging en vereist mogelijk een venster voor wijzigingsaanvraag/onderhoud.

Q.Kan het toevoegen of veranderen van een certificaat de verbonden gebruikers loskoppelen?
A.No, de gebruikers die op dit moment verbonden zijn blijven verbonden. Het certificaat wordt gebruikt in de verbindingsinrichting. Wanneer de gebruikers opnieuw verbinding hebben gemaakt, wordt het nieuwe certificaat gebruikt.

Q.Hoe kan ik een MVO met een vervanging creëren? Of een alternatieve onderwerpnaam (SAN)?
A. Op dit moment kan de ASA/FTD geen CSR maken met wildcard; dit proces kan echter worden uitgevoerd met OpenSSL. U kunt de opdrachten uitvoeren om de CSR- en ID-toets te genereren:

```
openssl genrsa - out id.key 2048

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

Wanneer een trustpoint is geconfigureerd met het FQDN-kenmerk (Fully Qualified Domain Name), bevat de door ASA/FTD gemaakte CSR de SAN met die waarde. Meer SAN-kenmerken kunnen door de CA worden toegevoegd wanneer deze de CSR ondertekent, of de CSR kan worden gemaakt met OpenSSL

Q.Worden certificaten onmiddellijk vervangen?

A. Het nieuwe server Identity Certificate wordt alleen gebruikt voor de nieuwe verbindingen. Het nieuwe certificaat is gereed om onmiddellijk na de wijziging gebruikt te worden, maar wordt daadwerkelijk gebruikt met nieuwe verbindingen.

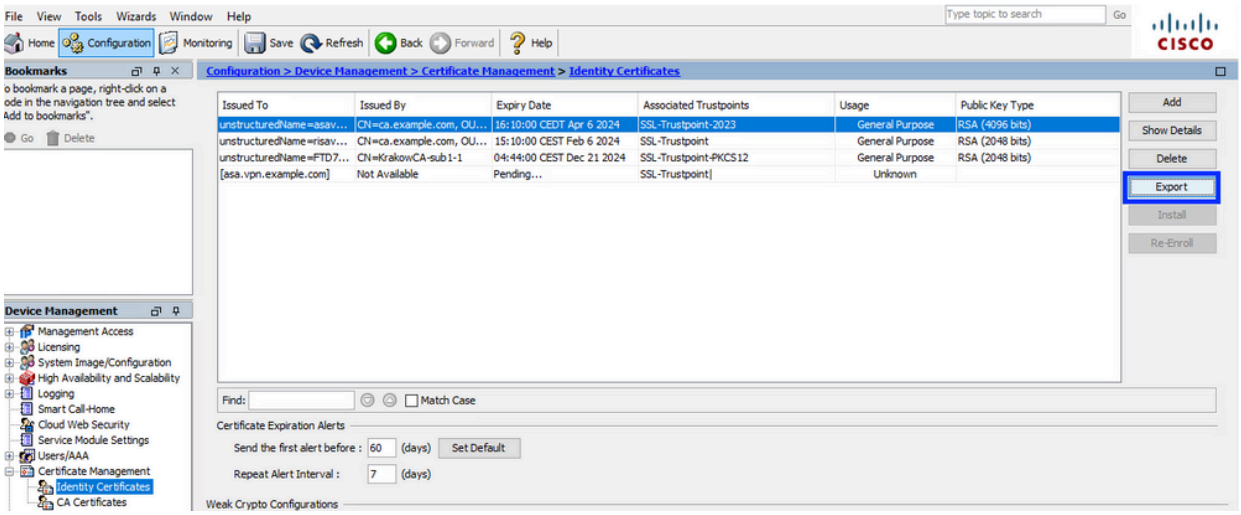
V.Hoe kan ik controleren of de installatie werkte?
A.De CLI opdracht te verifiëren: toon crypto ca cert <trustpointname>

Q.Hoe te om PKCS12 van het Certificaat van de Identiteit, het certificaat van CA, en privé sleutel te produceren?
A. PKCS12 kan worden gemaakt met OpenSSL, met de opdracht:
openssl pkcs12 -export -p12.pfx -inkey id.key -in id.crt -certfile ca.crt

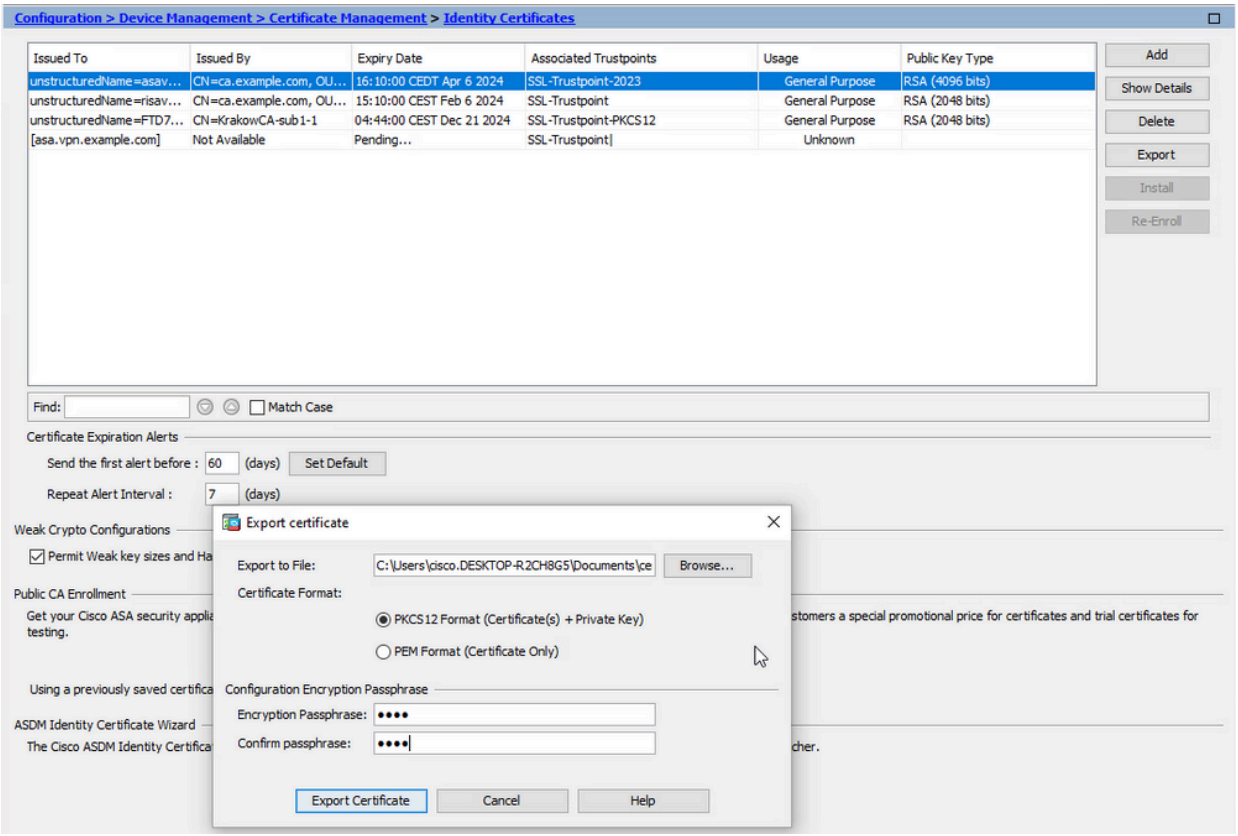
Q. Hoe een certificaat uit te voeren om het in een nieuwe ASA te installeren?
A.

- Met CLI: gebruik de opdracht: crypto kan <trustpointname> pkcs12 <password> exporteren
- Met ASDM:

a. Blader naar Configuratie > Apparaatbeheer > Certificaatbeheer > Identiteitscertificaten en kies het Identity Certificate. Klik op Exporteren.



b. Kies waar u het bestand wilt exporteren, geef het exportwachtwoord op en klik op Certificaat exporteren.



Het geëxporteerde certificaat kan op de computerschijf worden geplaatst. Let op het wachtwoord op een veilige plaats, het bestand is zonder het nutteloos.

Q.Als de sleutels ECDSA worden gebruikt, is het SSL proces van de certificaatgeneratie verschillend?
A.Het enige verschil in configuratie is de keypair generatiestap, waar een ECDSA keypair kan worden gegenereerd in plaats van een RSA keypair. De overige stappen zijn gelijk.

Q.Is het altijd vereist om een nieuw Zeer belangrijk paar te produceren?
A. De stap voor het genereren van het sleutelpaar is optioneel. Bestaand sleutelpaar kan worden gebruikt, of in het geval van PKCS12 wordt het sleutelpaar geïmporteerd met het certificaat. Zie de sectie Selecteer de Key pair Name voor het respectieve inschrijvings-/herinschrijvingstype.

Q.Is het veilig om een nieuw sleutelpaar te genereren voor een nieuw identiteitscertificaat?
A.Het proces is veilig zolang een nieuwe naam van het Zeer belangrijke paar wordt gebruikt. In een dergelijk geval worden de oude Key Pairs niet gewijzigd.

Q.Is het vereist om sleutel opnieuw te produceren wanneer een firewall (zoals RMA) wordt vervangen?
A.De nieuwe firewall door ontwerp heeft geen Key Paren aanwezig op de oude firewall.
De back-up van de actieve configuratie bevat niet de sleutelparen.
De volledige back-up met ASDM kan de sleutelparen bevatten.
De Identity Certificates kunnen worden geëxporteerd van een ASA met ASDM of CLI voordat deze

faalt.
In het geval van een failover-paar worden de certificaten en sleutelparen gesynchroniseerd naar een stand-by-eenheid met de opdracht schrijfstand-by. In het geval van één knooppunt van failover-paar wordt vervangen is het voldoende om de basisfailover te configureren en de configuratie naar het nieuwe apparaat te duwen.
Als een sleutelpaar verloren gaat met het apparaat en er geen back-up is, moet een nieuw certificaat worden ondertekend met sleutelpaar aanwezig op het nieuwe apparaat.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.