ASA configureren: Digitaal certificaat (SSL) installeren en verlengen

Inhoud

Inleiding

In dit document wordt de installatie beschreven van een digitaal certificaat van derden dat vertrouwde op SSL is, op de ASA for Clientless VPN- en AnyConnect-verbindingen.

Achtergrondinformatie

In dit voorbeeld wordt een GoDaddy-certificaat gebruikt. In elke stap zijn de procedures met ASDM (Adaptive Security Device Manager) en via de opdrachtregelinterface opgenomen.

Voorwaarden

Vereisten

Er is toegang vereist tot een vertrouwde externe certificeringsinstantie (CA) voor certificaatinschrijving. Voorbeelden van externe CA's zijn Baltimore, Cisco, Entrust, Geotrust, G, Microsoft, RSA, Thawte en VeriSign.

Controleer voor het starten of de ASA de juiste kloktijd, datum en tijdzone heeft. Bij certificaatverificatie wordt het aanbevolen een NTP-server (Network Time Protocol) te gebruiken om de tijd op de ASA te synchroniseren. In Cisco ASA Series General Operations CLI Configuration Guide, 9.1 worden de stappen beschreven om de juiste datum en tijd in te stellen op de ASA.

Gebruikte componenten

De informatie in dit document is gebaseerd op een ASA 5500-X met softwareversie 9.4.1 en ASDM-versie 7.4(1).

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.

Configureren

Het SSL-protocol vereist dat de SSL-server de client een servercertificaat verstrekt voor serververificatie. 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. Het wordt aanbevolen vertrouwde externe CA's in te schakelen voor het verstrekken van SSL-certificaten voor de ASA.

De levenscyclus van een extern certificaat op de ASA omvat de volgende stappen:

CSR genereren

CSR-generatie is de eerste stap in de levenscyclus van elk X.509 digitaal certificaat.

Zodra het private/openbare sleutelpaar van type Rivest-Shamir-Adleman (RSA) of Elliptic Curve Digital Signature Algorithm (ECDSA) is gegenereerd, wordt een CSR (Certficate Signing Request) gemaakt (Bijlage A bevat informatie over het verschil tussen RSA en ECDSA).

Een CSR is een geformatteerd PKCS10-bericht dat de openbare sleutel en de identiteitsinformatie van de gastheer bevat die het verzoek verstuurt. PKI-gegevensformaten verklaart de verschillende certificaatformaten van toepassing op de ASA en Cisco IOS®.

> **Opmerkingen:**
> 1. Controleer met de CA op de gewenste toetsencombinatie. CA/Browser Forum heeft vastgesteld dat alle certificaten die door hun CA-leden worden gegenereerd, minimaal 2048 bits groot moeten zijn.
> 2. ASA ondersteunt momenteel geen 4096-bits sleutels (Cisco bug-ID CSCut53512) voor SSL-serververificatie. IKEv2 ondersteunt wel het gebruik van 4096-bits servercertificaten, maar alleen op de platforms ASA 5580, 5585 en 5500-X.
> 3. Gebruik de DNS-naam van de ASA in het FQDN-veld van de CSR om onvertrouwde certificaatwaarschuwingen te voorkomen en de strikte certificaatcontrole te doorlopen.

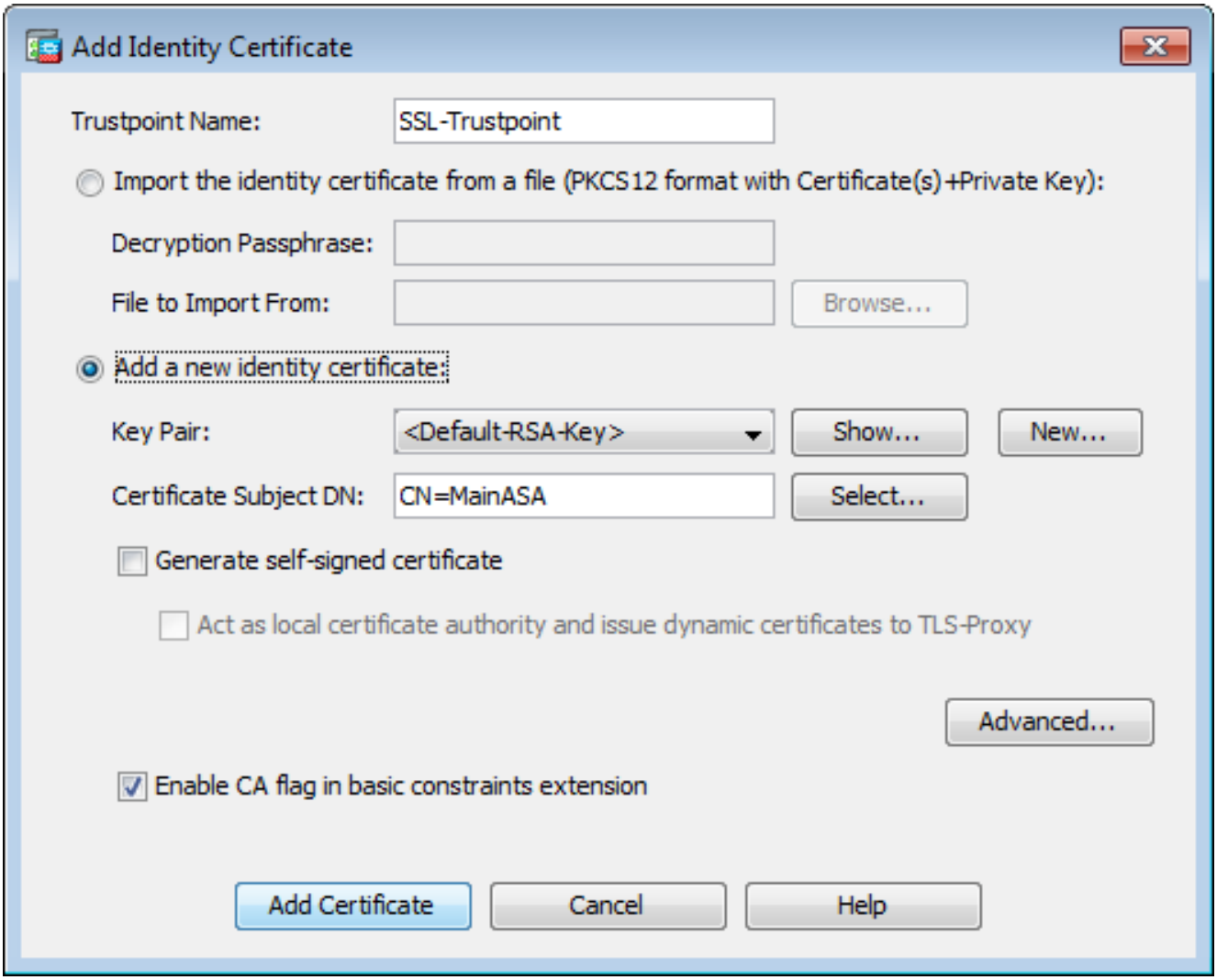
Er zijn drie methoden om MVO op te bouwen.

- Configureren met ASDM

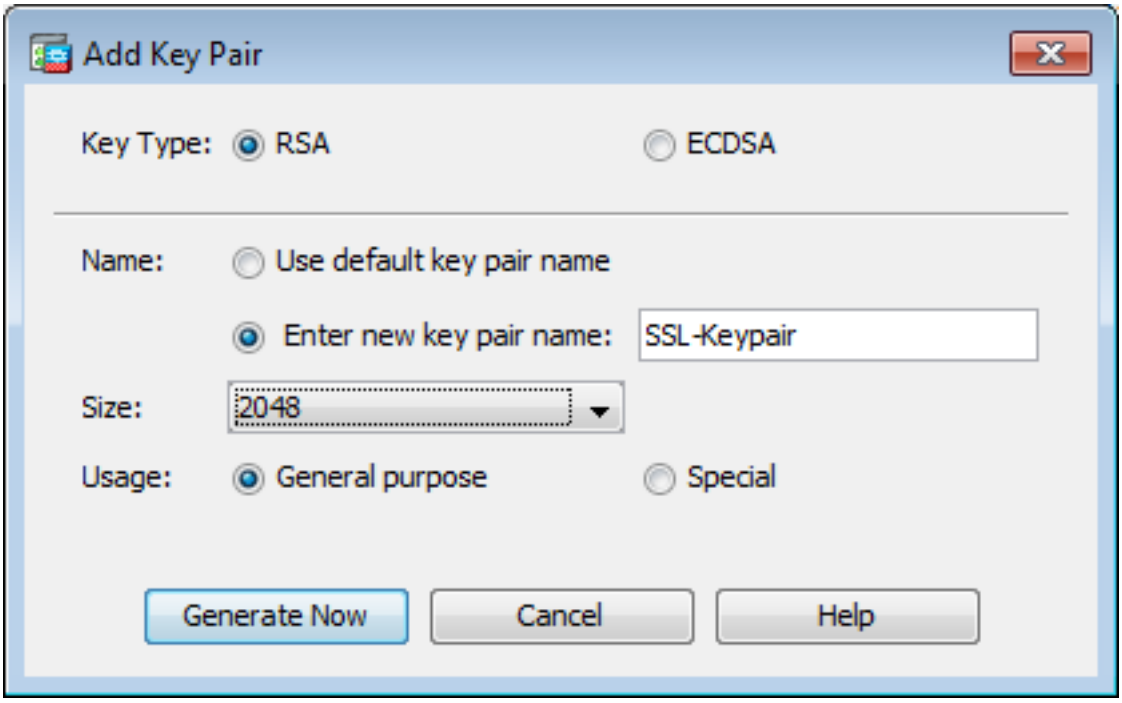
- Configureren met ASA-opdrachtregelinterface
- OpenSSL gebruiken om de CSR te genereren

1. Instellen met de ASDM

1. Navigeren in om **Configuration > Remote Access VPN > Certificate Management**, en kies **Identity Certificates**.
2. Klik **Add**.



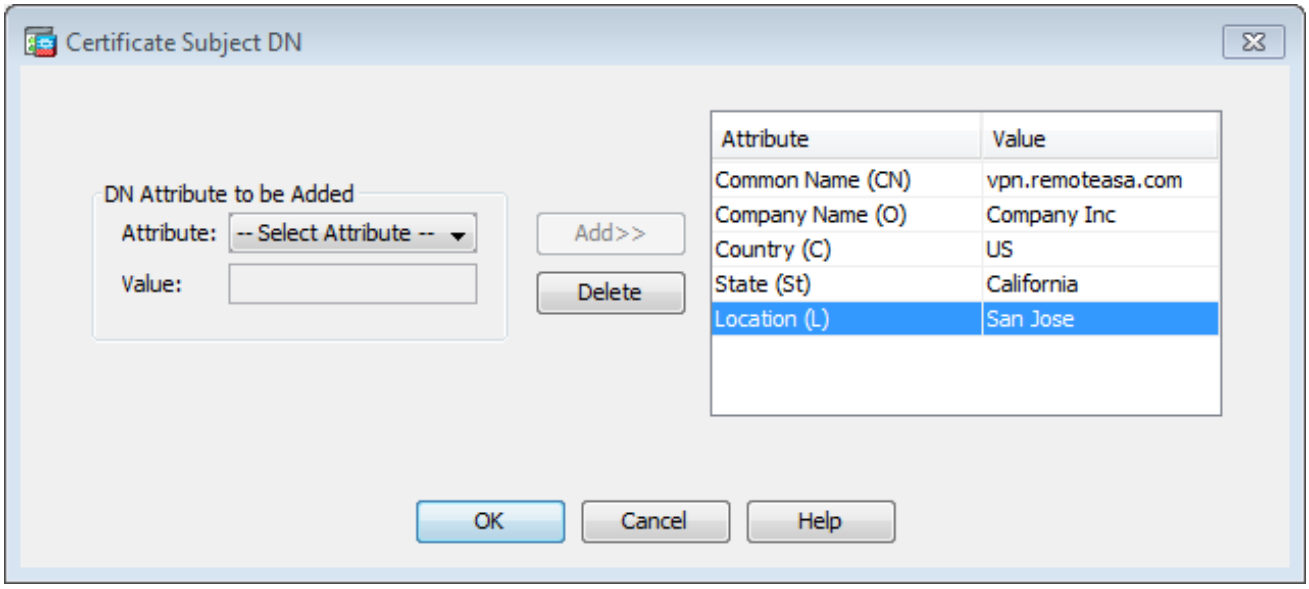
3. Defineert een naam van het trustpunt in het veld Naam van het Trustpoint.
4. Klik op het**Add a new identity certificate**radioknop.
5. Klik op voor het hoofdvenster**New**.



6. Kies het sleuteltype - RSA of ECDSA (raadpleeg Bijlage A om de verschillen te begrijpen.)
7. Klik op het**Enter new key pair name**radioknop. Identificeer de sleutelpaarnaam voor herkenningsdoeleinden.
8. Kies het**Key Size**. Kies**General Purpose for Usage** bij gebruik van RSA.
9. Klik**Generate Now**. Het sleutelpaar wordt gemaakt.
10. Om het Onderwerp van het Certificaat te definiëren DN, klik**Select**en configureren de eigenschappen die in deze tabel staan:

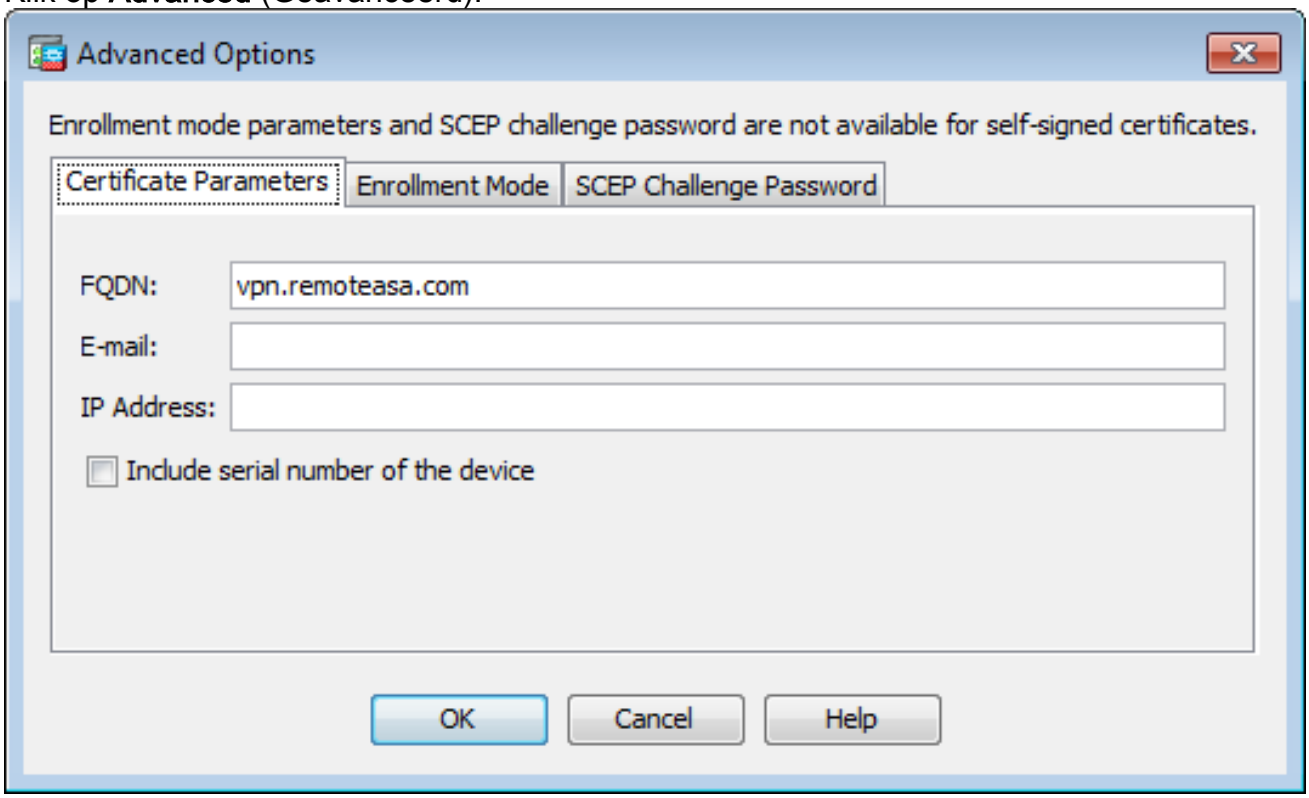
Attribute	Description
CN	FQDN (Full Qualified Domain Name) that will be used for connections to your firewall. For example, webvpn.cisco.com
OU	Department Name
O	Company Name (Avoid using Special Characters)
C	Country Code (2 Letter Code without Punctuation)
St	State (Must be spelled out completely. For example, North Carolina)
L	City
EA	Email Address

Om deze waarden te configureren kiest u een waarde uit de vervolgkeuzelijst **Eigenschappen**, voert u de waarde in en klikt u op **Toevoegen**.

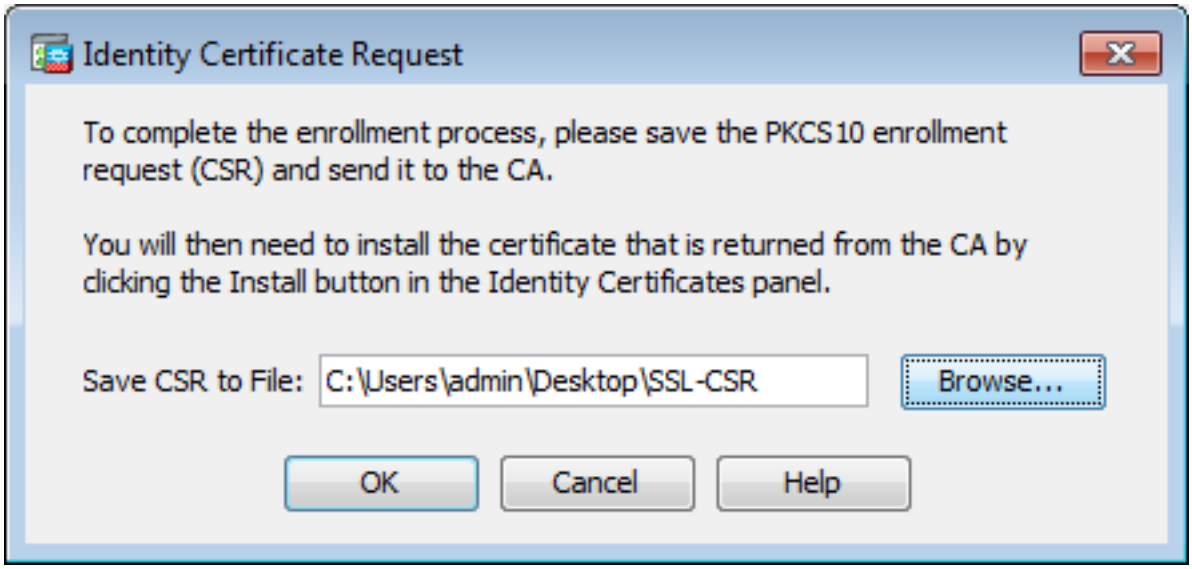


Opmerking: Sommige externe leveranciers vereisen dat bepaalde kenmerken worden opgenomen voordat een identiteitscertificaat wordt verstrekt. Neem contact op met de leverancier als u niet zeker bent van de vereiste kenmerken.

11. Klik op**OK**. Het dialoogvenster identiteitsbewijs toevoegen verschijnt met het certificaat**Subject DN** field populated.
12. Klik op **Advanced** (Geavanceerd).



13. In de**FQDN**Voer in het veld de FQDN in die wordt gebruikt om het apparaat van het internet te gebruiken. Klik**OK**.
14. Laat het keuzerondje ‘Enable CA flag in basic constraints extension’ (CA-vlag in extensie voor basisbeperkingen inschakelen) ingeschakeld. Certificaten zonder de CA-vlag kunnen dan standaard niet als CA-certificaten op de ASA worden geïnstalleerd. Via de extensie voor basisbeperkingen wordt geïdentificeerd of de houder van het certificaat een CA is en wordt de maximale diepte van geldige certificeringspaden bepaald voor dit certificaat. Schakel de optie uit om deze eis te omzeilen.
15. Klik**OK**en klik vervolgens op**Add Certificate.** Vervolgens wordt een scherm getoond met het verzoek de CSR op te slaan.



16. Klik**Browse**Selecteer een locatie waarin u de CSR wilt opslaan, en slaat u het bestand op met de .txt-extensie. **Opmerking:** Wanneer het bestand wordt opgeslagen met de extensie .txt, kan de PKCS#10-aanvraag worden geopend met een tekstverwerker (bijvoorbeeld Notepad).

2. Instellen met de ASA CLI

Het vertrouwenspunt wordt in ASDM automatisch gemaakt wanneer een CSR wordt gegenereerd of het CA-certificaat wordt geïnstalleerd. In de opdrachtregelinterface moet het vertrouwenspunt handmatig worden gemaakt.

```
! Generates 2048 bit RSA key pair with label SSL-Keypair.

MainASA(config)# crypto key generate rsa label SSL-Keypair modulus 2048

INFO: The name for the keys will be: SSL-Keypair
Keypair generation process begin. Please wait...

 ! Define trustpoint with attributes to be used on the SSL certificate

MainASA(config)# crypto ca trustpoint SSL-Trustpoint
MainASA(config-ca-trustpoint)# enrollment terminal
MainASA(config-ca-trustpoint)# fqdn vpn.remoteasa.com
MainASA(config-ca-trustpoint)# subject-name CN=vpn.remoteasa.com,O=Company Inc,C=US,
St=California,L=San Jose
MainASA(config-ca-trustpoint)# keypair SSL-Keypair
MainASA(config-ca-trustpoint)# exit

 ! Initiates certificate signing request. This is the request to be submitted via Web or
Email to the third party vendor. MainASA(config)# crypto ca enroll SSL-Trustpoint

WARNING: The certificate enrollment is configured with an fqdn
that differs from the system fqdn. If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment? [yes/no]: yes
% Start certificate enrollment ..
% The subject name in the certificate will be: subject-name CN=vpn.remoteasa.com,
O=Company Inc,C=US,St=California,L=San Jose % The fully-qualified domain name in the certificate
will be: vpn.remoteasa.com % Include the device serial number in the subject name? [yes/no]: no
```

```
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
-----BEGIN CERTIFICATE REQUEST-----
MIIDDjCCAfYCAQAwgYkxETAPBgNVBAcTCFNhbiBKb3NlMRMwEQYDVQQIEwpDYWxp
Zm9ybmlhMQswCQYDVQQGEwJVUzEUMBIGA1UEChMLQ29tcGFueSBJbmMxGjAYBgNV
BAMTEXZwbi5yZW1vdGVhc2EuY29tMSAwHgYJKoZIhvcNAQkCFhF2cG4ucmVtb3Rl
YXNhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK62Nhb9ktlK
uR3Q4TmksyuRMqJNrb9kXpvA6H200PuBfQvSF4rVnSwKOmu3c8nweEvYcdVWV6Bz
BhjXeovTVi17FlNTceaUTGikeIdXC+mw1iE7eRsynS/d4mzMWJmrvrsDNzpAW/EM
SzTca+BvqF7X2r3LU8Vsv6Oi8ylhco9Fz7bWvRWVtO3NDDbyolC9b/VgXMuBitcc
rzfUbVnm7VZDOf4jr9EXgUwXxcQidWEABlFrXrtYpFgBo9aqJmRp2YABQ1ieP4cY
3rBtgRjLcF+S9TvHG5m4v7v755meV4YqsZIXvytIOzVBihemVxaGA1oDwfkoYSFi
4CzXbFvdG6kCAwEAAaA/MD0GCSqGSIb3DQEJDjEwMC4wDgYDVR0PAQH/BAQDAgWg
MBwGA1UdEQQVMBOCEXZwbi5yZW1vdGVhc2EuY29tMA0GCSqGSIb3DQEBBQUAA4IB
AQBZuQzUXGEB0ix1yuPK0ZkRz8bPnwIqLTfxZhagmuyEhrN7N4+aQnCHj85oJane
4ztZDiCCoWTerBS4RSkKEHEspu9oohjCYuNnp5qa91SPrZNEjTWw0eRn+qKbId2J
jE6Qy4vdPCexavMLYVQxCny+gVkzPN/sFRk3EcTTVq6DxxaebpJijmiqa7gCph52
YkHXnFne1LQd41BgoLlCr9+hx74XsTHGBmI1s/9T5oAX26Ym+B2l/i/DP5BktIUA
8GvIY1/ypj9KO49fP5ap8al0qvLtYYcCcfwrCt+OojOrZ1YyJb3dFuMNRedAX37t
DuHNl2EYNpYkjVk1wI53/5w3
-----END CERTIFICATE REQUEST----- Redisplay enrollment request? [yes/no]: no

 ! Displays the PKCS#10 enrollment request to the terminal. Copy this from the terminal
to a text file to submit to the third party CA.
```

3. Gebruik OpenSSL om de CSR te genereren

OpenSSL maakt gebruik van het**openSSL config**bestand om de eigenschappen te trekken die gebruikt moeten worden in de CSR-generatie. Hierbij worden een CSR en een persoonlijke sleutel gegenereerd.

> **Voorzichtig:** Controleer dat de **Private key** die wordt gegenereerd niet met iemand anders wordt gedeeld omdat deze de integriteit van het certificaat aantast.

1. Zorg dat OpenSSL is geïnstalleerd op het systeem waarop dit proces wordt uitgevoerd. Voor Mac OSX- en GNU/Linux-gebruikers wordt dit standaard geïnstalleerd.
2. Schakel over naar een werkmap. Voor Windows: De standaardinstelling is dat de hulpprogramma's zijn geïnstalleerd in **C:\Openssl\bin**. Open een opdrachtprompt op deze locatie.Voor macOS X en Linux: Open een terminal-venster in de map die nodig is om de CSR te maken.
3. Maak een OpenSSL configuratiebestand met behulp van een teksteditor met de gegeven eigenschappen. Sla het bestand vervolgens op als **openssl.cnf** op de locatie die in de vorige stap is beschreven (Als u versie 0.9.8h en hoger hebt, is het bestand**openssl.cfg**)

```
 [req]
default_bits = 2048
default_keyfile = privatekey.key
distinguished_name = req_distinguished_name
req_extensions = req_ext

[req_distinguished_name]
commonName = Common Name (eg, YOUR name)
commonName_default = vpn.remoteasa.com

countryName = Country Name (2 letter code)
countryName_default = US

stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = California
```

```
localityName = Locality Name (eg, city)
localityName_default = San Jose

0.organizationName = Organization Name (eg, company)
0.organizationName_default = Company Inc

[req_ext]
subjectAltName = @alt_names
[alt_names]
DNS.1 = *.remoteasa.com
```

4. Genereer de CSR en de persoonlijke sleutel met de volgende opdracht: **openssl req -new -nodes -out CSR.csr -config openssl.cnf**

```
 # Sample CSR Generation:

 openssl req -new -nodes -out CSR.csr -config openssl.cnf
Generating a 2048 bit RSA private key
.....................................................................................+++
.....................................+++ writing new private key to 'privatekey.key' ---
-- You are about to be asked to enter information that will be incorporated into your
certificate request. What you are about to enter is what is called a Distinguished Name or
a DN. There are quite a few fields but you can leave some blank For some fields there will
be a default value, If you enter '.', the field will be left blank. ----- Common Name (eg,
YOUR name) [vpn.remoteasa.com]: Country Name (2 letter code) [US]: State or Province Name
(full name) [California]: Locality Name (eg, city) [San Jose]: Organization Name (eg,
company) [Company Inc]:
```

   Dien de opgeslagen CSR in bij de externe CA-leverancier. Zodra het certificaat is verstrekt, levert de CA het identiteitscertificaat en het CA-certificaat. Deze moeten op de ASA worden geïnstalleerd.

SSL-certificaat genereren bij certificeringsinstantie

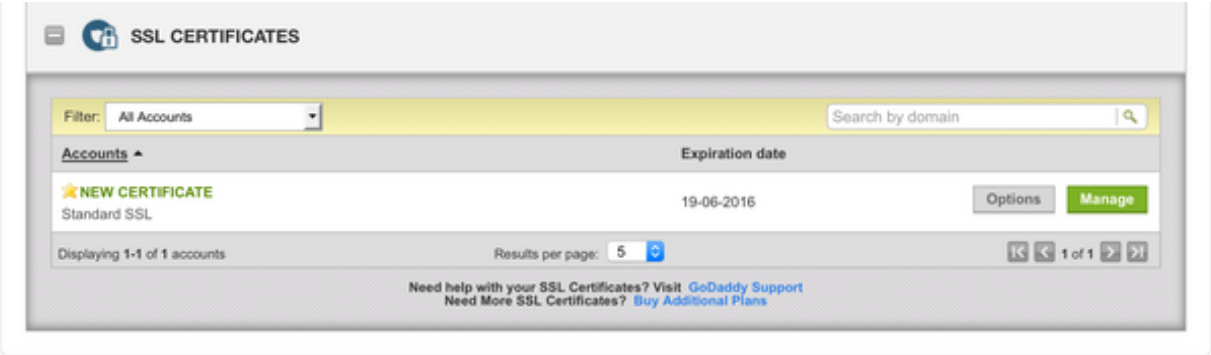
Nu moet de CSR worden ondertekend door de CA. De CA levert naast de CA-certificaatbundel een nieuw gegenereerd PEM-gecodeerd identiteitscertificaat of een PKCS12-certificaat.

Als de CSR buiten de ASA (via OpenSSL of via de CA zelf) wordt gegenereerd, is het PEM-gecodeerde Identity Certificate met het Private Key and CA-certificaat beschikbaar als afzonderlijke bestanden. In Bijlage B zijn de stappen opgenomen om deze elementen in één PKCS12-bestand (.p12 of .pfx) te bundelen.

In dit document wordt de certificeringsinstantie GoDaddy gebruikt als voorbeeld voor het verstrekken van identiteitscertificaten aan de ASA. Dit proces kan bij andere CA-verkopers verschillen.Lees zorgvuldig door de CA-documentatie voordat u verdergaat.

Voorbeeld van genereren van SSL-certificaat bij GoDaddy

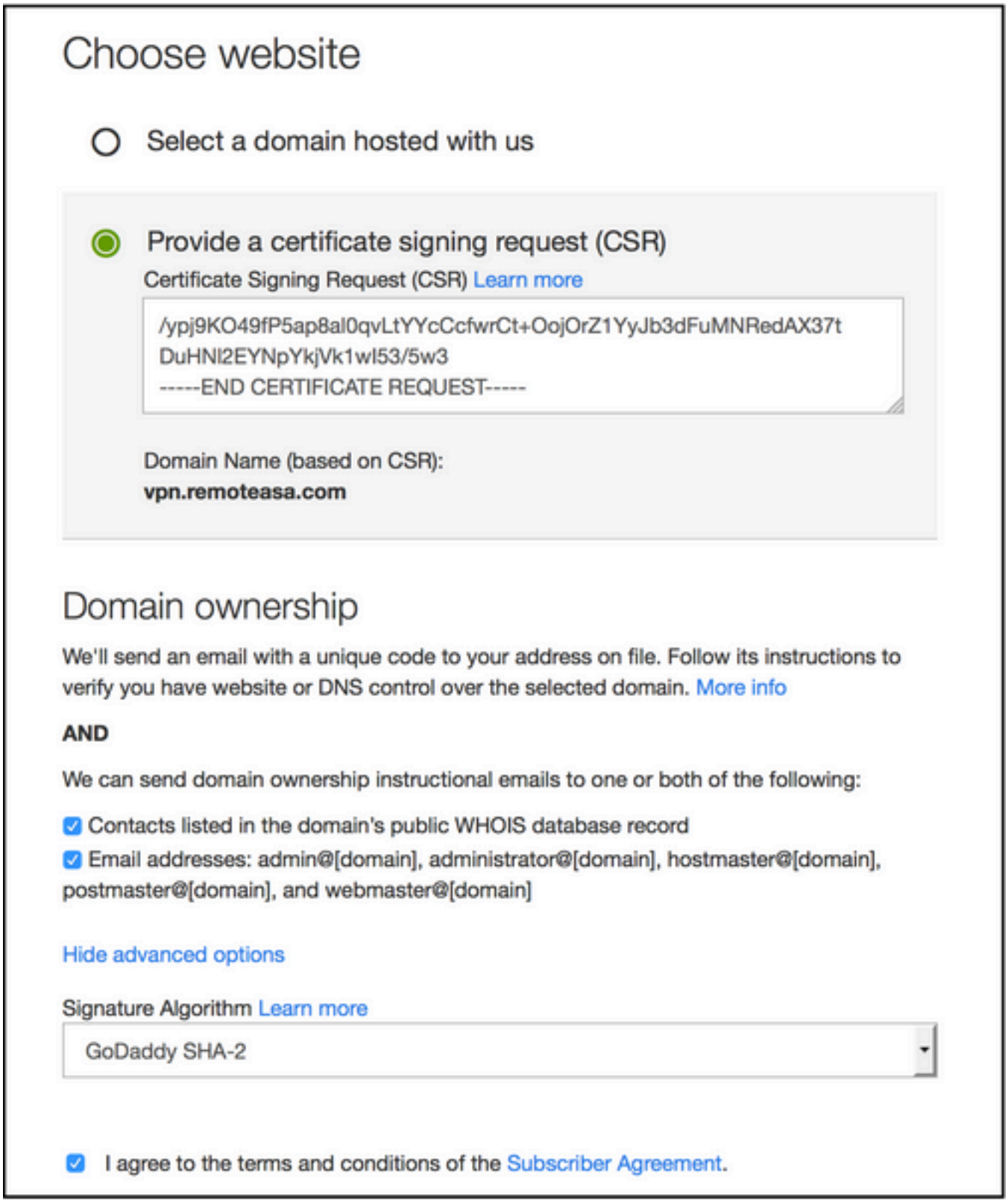
Na aanschaf en eerste installatiefase van het SSL-certificaat gaat u naar de GoDaddy-account en bekijkt u de SSL-certificaten. Daar staat nu een nieuw certificaat. Klik**Manage** om verder te gaan.



Er wordt een pagina geopend voor het maken van de CSR (zie afbeelding).

Op basis van de opgegeven CSR bepaalt de CA de domeinnaam waaraan het certificaat moet worden verstrekt.

Controleer of deze overeenkomt met de FQDN van de ASA.

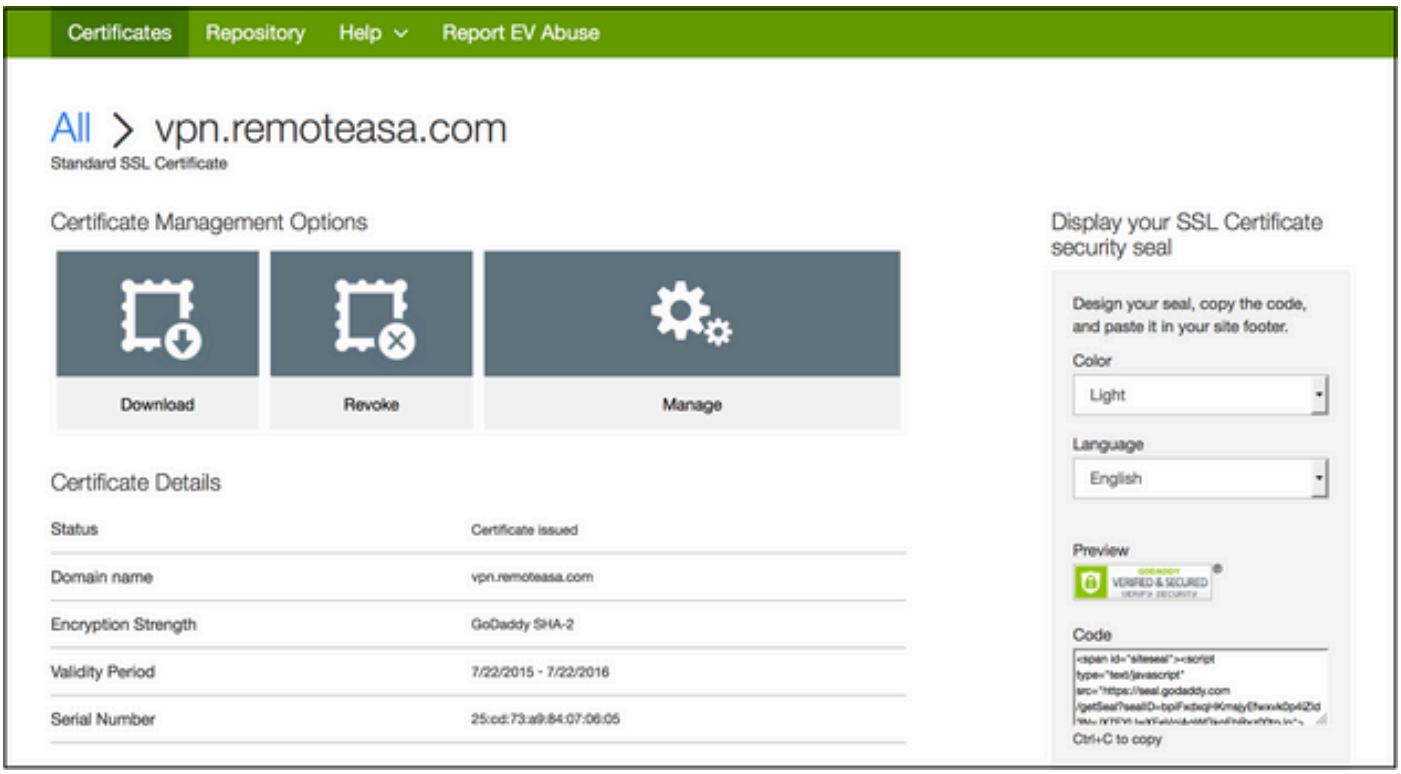


Opmerking: GoDaddy en de meeste andere CA's gebruiken SHA-2 of SHA-256 als het standaard handtekeningalgoritme voor certificaten. ASA ondersteunt het handtekeningalgoritme SHA-2 vanaf versie **8.2(5) [releases voor 8.3] en** 8.4(1) [releases na 8.3] (Cisco bug-ID CSCti30937). Kies het handtekeningalgoritme SHA-1 als een versie ouder dan 8.2(5) of 8.4(1) wordt gebruikt.

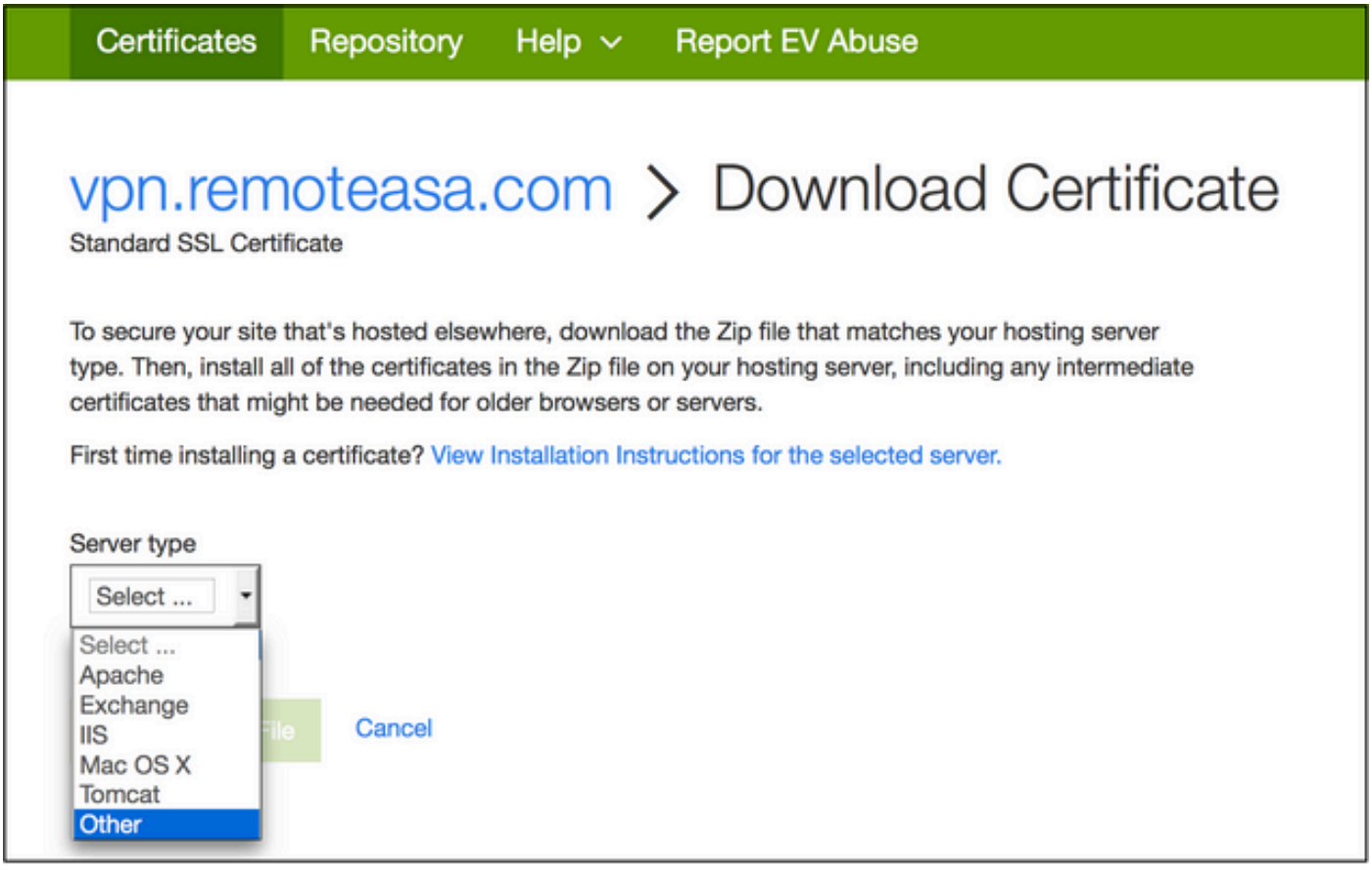
Zodra de aanvraag is ingediend, controleert GoDaddy de aanvraag voordat het certificaat wordt verstrekt.

Nadat de certificaataanvraag is gevalideerd, verstrekt GoDaddy het certificaat aan de account.

Het certificaat kan dan worden gedownload en op de ASA worden geïnstalleerd. Klik**Download** op de pagina om verder te gaan.



Kies**Other** als het servertype en het zip-pakket van het certificaat downloaden.



Het zip-bestand bevat het identiteitscertificaat en de GoDaddy-certificaatketenbundels als twee afzonderlijke crt-bestanden. Ga naar SSL certificatie installatie om deze certificaten op de ASA te

installeren.

SSL-certificaat installeren op de ASA

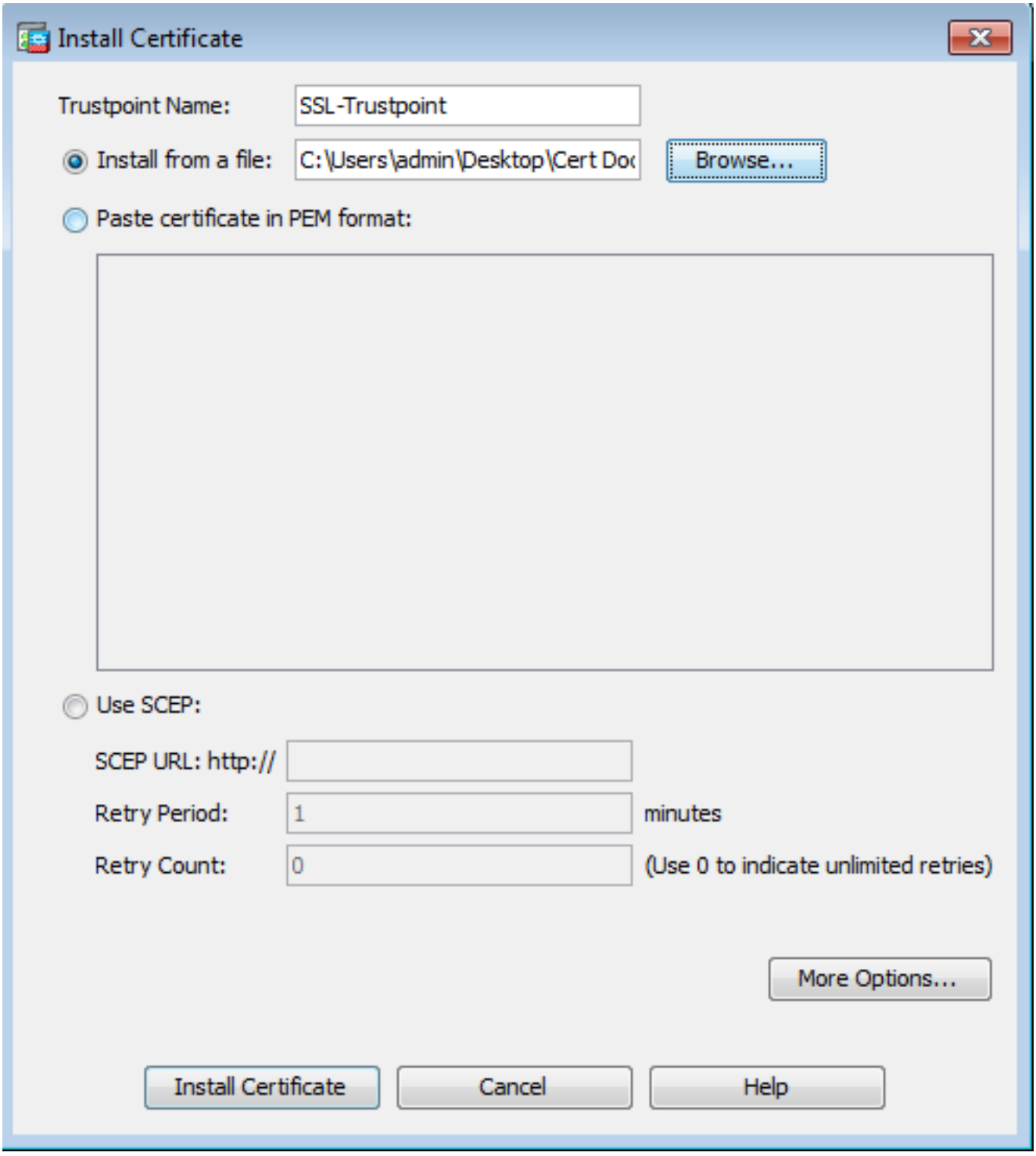
Het SSL-certificaat kan via de ASDM of de opdrachtregelinterface op twee manieren worden geïnstalleerd op de ASA:

1. Importeer het CA- en identiteitscertificaat afzonderlijk in PEM-opmaak.
2. Importeer het PKCS12-bestand (base64-gecodeerd voor de opdrachtregelinterface) met gebundeld identiteitscertificaat, CA-certificaat en persoonlijke sleutel. **Opmerking:** Als de CA een CA-certificaatketen levert, moet u alleen het directe CA-tussencertificaat in de hiërarchie installeren op het vertrouwenspunt dat wordt gebruikt om de CSR te genereren. Het basis-CA-certificaat en enige andere CA-tussencertificaten kunnen op nieuwe vertrouwenspunten worden geïnstalleerd.

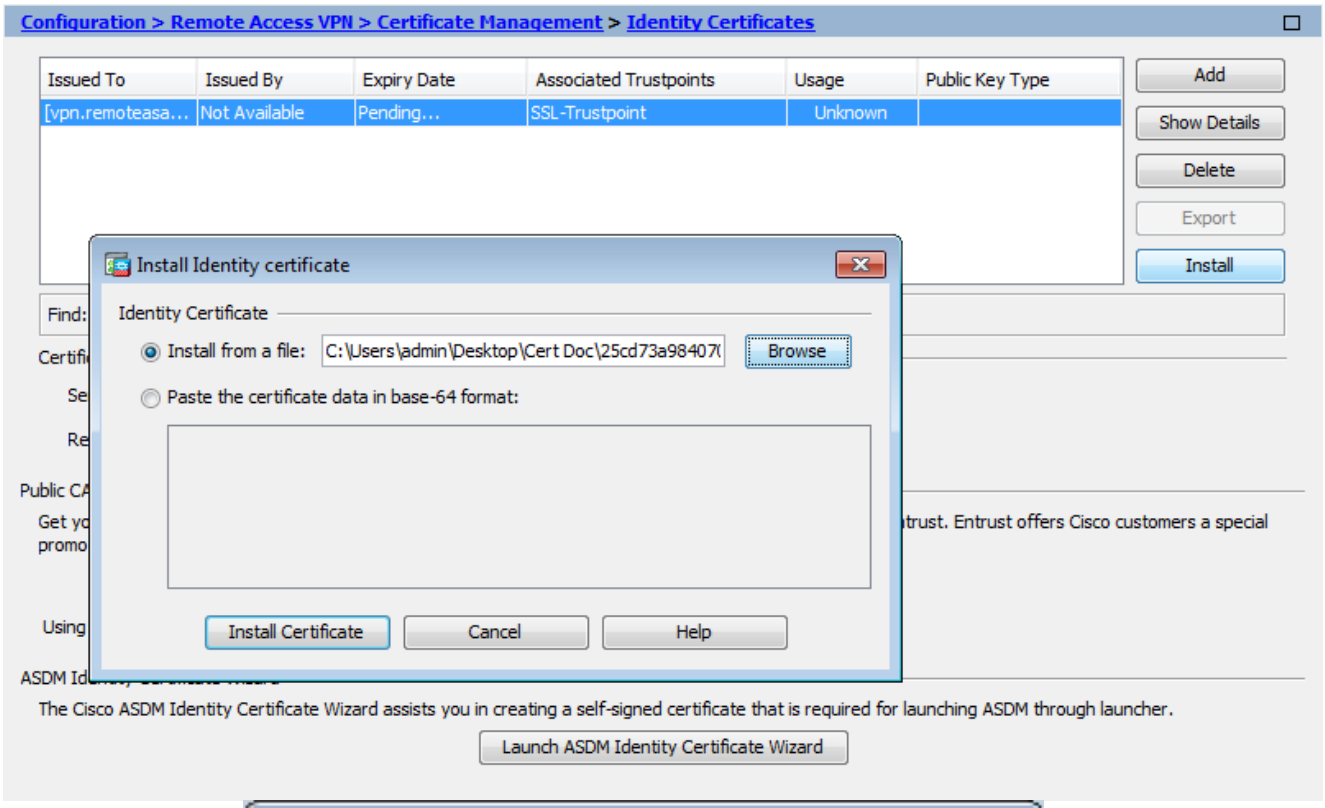
1.1 Identiteitscertificaat in PEM-opmaak installeren met ASDM

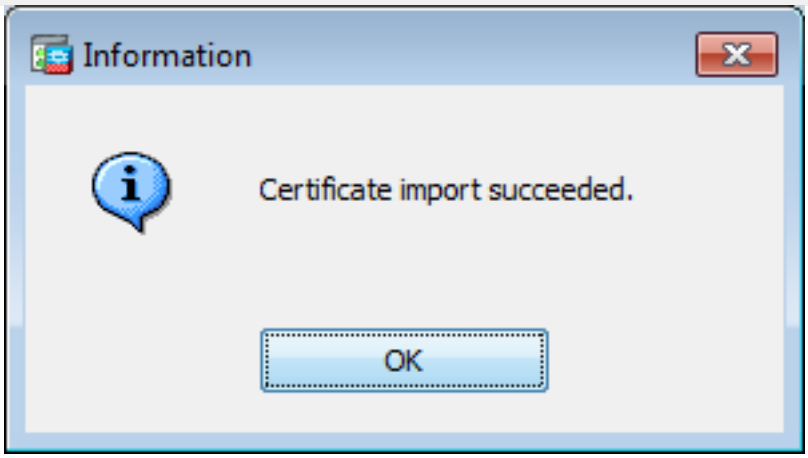
Bij de onderstaande installatiestappen wordt ervan uitgegaan dat de CA een bundel met een PEM-gecodeerd (.pem, .cer, .crt) identiteitscertificaat en CA-certificaat levert.

1. Navigeren in om **Configuration > Remote Access VPN > Certificate Management**en kies CA-certificaten.
2. Open het PEM-gecodeerde certificaat in een tekstverwerker, kopieer het base64-gecodeerde CA-certificaat van de externe leverancier en plak dit in het tekstveld.

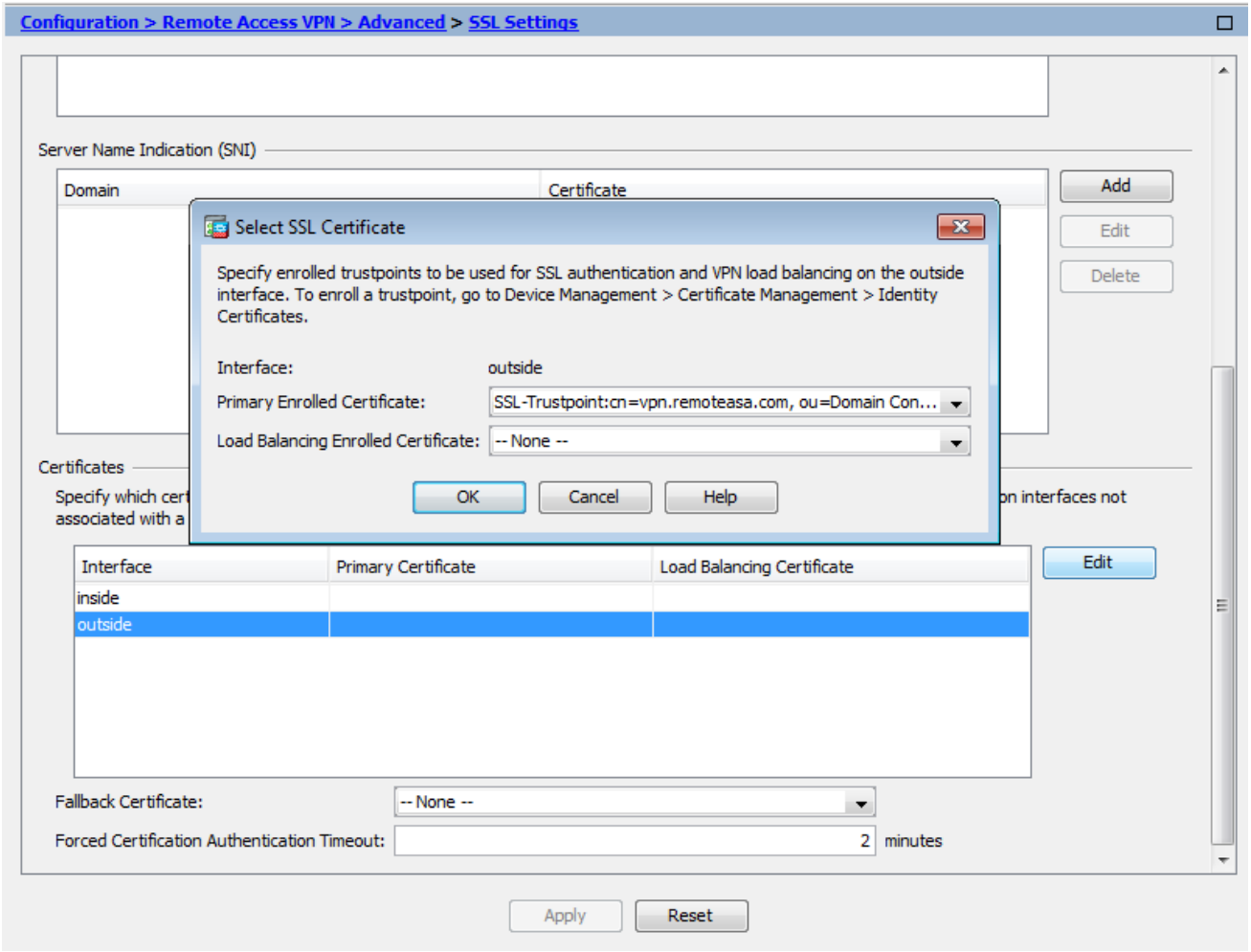


3. Klik op **Install Certificate** (Certificaat installeren).
4. Navigeren in om**Configuration > Remote Access VPN > Certificate Management**, en kies identiteitsbewijzen.
5. Selecteer het eerder gemaakte identiteitscertificaat. Klik **Install**.
6. Klik op de optie**Install from a file** radioknop en kies het PEM-gecodeerde identiteitsbewijs of, open het PEM-gecodeerde certificaat in een teksteditor en kopieer en plak het basiscertificaat 64 dat door de derde verkoper in het tekstveld wordt verstrekt.





7. Klik **Add Certificate**.
8. Navigeren in om **Configuration > Remote Access VPN > Advanced > SSL Settings**.
9. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.
10. Klik **Edit**.
11. Selecteer in de vervolgkeuzelijst Certificaat en het nieuwe geïnstalleerde certificaat.



12. Klikok.
13. Klik**Apply**. Het nieuwe certificaat wordt nu gebruikt voor alle WebVPN sessies die op de gespecificeerde interface eindigen.

1.2. Installatie van een PEM-certificaat bij de CLI

```
MainASA(config)# crypto ca authenticate SSL-Trustpoint

Enter the base 64 encoded CA certificate. End with the word"quit"on a line by itself

-----BEGIN CERTIFICATE----- MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh
MB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE
YWRkeSBDbGFzcyAyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTA0MDYyOTE3
MDYyMFoXDTM0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRo
ZSBHbyBEYWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3Mg
MiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTCCASAwDQYJKoZIhvcNAQEBBQADggEN
ADCCAQgCggEBAN6d1+pXGEmhW+vXX0iG6r7d/+TvZxz0ZWizV3GgXne77ZtJ6XCA
PVYYYwhv2vLM0D9/AlQiVBDYsoHUwHU9S3/Hd8M+eKsaA7Ugay9qK7HFiH7Eux6w
wdhFJ2+qN1j3hybX2C32qRe3H3I2TqYXP2WYktsqbl2i/ojgC95/5Y0V4evLOtXi
EqITLdiOr18SPaAIBQi2XKVlOARFmR6jYGB0xUGlcmIbYsUfb18aQr4CUWWoriMY
avx4A6lNf4DD+qta/KFApMoZFv6yyO9ecw3ud72a9nmYvLEHZ6IVDd2gWMZEewo+
YihfukEHU1jPEX44dMX4/7VpkI+EdOqXG68CAQOjgcAwgb0wHQYDVR0OBBYEFNLE
sNKR1EwRcbNhyz2h/t2oatTjMIGNBgNVHSMEgYUwgYKAFNLEsNKR1EwRcbNhyz2h
/t2oatTjoWekZTBjMQswCQYDVQQGEwJVUzEhMB8GA1UEChMYVGhlIEdvIERhZGR5
IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBEYWRkeSBDbGFzcyAyIENlcnRpZmlj
YXRpb24gQXV0aG9yaXR5ggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQAD
ggEBADJL87LKPpH8EsahB4yOd6AzBhRckB4Y9wimPQoZ+YeAEW5p5JYXMP80kWNy
OO7MHAGjHZQopDH2esRU1/blMVgDoszOYtuURXO1v0XJJLXVggKtI3lpjbi2Tc7P
TMozI+gciKqdi0FuFskg5YmezTvacPd+mSYgFFQlq25zheabIZ0KbIIOqPjCDPoQ
```

```
HmyW74cNxA9hi63ugyuV+I6ShHI56yDqg+2DzZduCLzrTia2cyvk0/ZM/iZx4mER
dEr/VxqHD3VILs9RaRegAhJhldXRQLIQTO7ErBBDpqWeCtWVYpoNz4iCxTIM5Cuf ReYNnyicsbkqWletNw+vHX/bvZ8= --
---END CERTIFICATE----- quit INFO: Certificate has the following attributes: Fingerprint:
96c25031 bc0dc35c fba72373 1e1b4140 Do you accept this certificate? [yes/no]: yes Trustpoint
'SSL-Trustpoint' is a subordinate CA and holds a non self-signed certificate. Trustpoint CA
certificate accepted. % Certificate successfully imported
```

!!! - Installing Next-level SubCA in the PKI hierarchy.
!!! - Create a separate trustpoint to install the next subCA certificate (if present)
in the hierarchy leading up to the Root CA (including the Root CA certificate)

```
MainASA(config)#crypto ca trustpoint SSL-Trustpoint-1
MainASA(config-ca-trustpoint)#enrollment terminal
MainASA(config-ca-trustpoint)#exit
MainASA(config)#
MainASA(config)# crypto ca authenticate SSL-Trustpoint-1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself


-----BEGIN CERTIFICATE-----
MIIEfTCCA2WgAwIBAgIDG+cVMA0GCSqGSIb3DQEBCwUAMGMxCzAJBgNVBAYTAlVT
MSEwHwYDVQQKExhUaGUgR28gRGFkZHkgR3JvdXAsIEluYy4xMTAvBgNVBAsTKEdv
IERhZGR5IENsYXNzIDIgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQwMTAx
MDcwMDAwWhcNMzEwNTMwMDcwMDAwWjCBgzELMAkGA1UEBhMCVVMxEDAOBgNVBAgT
B0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNVBAoTEUdvRGFkZHku
Y29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb290IENlcnRpZmljYXRlIEF1
dGhvcml0eSAtIEcyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv3Fi
CPH6WTT3G8kYo/eASVjpIoMTpsUgQwE7hPHmhUmfJ+r2hBtOoLTbcJjHMgGxBT4H
Tu70+k8vWTAi56sZVmvigAf88xZ1gDlRe+X5NbZ0TqmNghPktj+pA4P6or6KFWp/
3gvDthkUBcrqw6gElDtGfDIN8wBmIsiNaW02jBEYt9OyHGC0OPoCjM7T3UYH3go+
6118yHz7sCtTpJJiaVElBWEaRIGMLKlDliPfrDqBmg4pxRyp6V0etp6eMAo5zvGI
gPtLXcwy7IViQyU0AlYnAZG0O3AqP26x6JyIAX2f1PnbU21gnb8s51iruF9G/M7E
GwM8CetJMVxpRrPgRwIDAQABo4IBFzCCARMwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFDqahQcQZyi27/a9BUFuIMGU2g/eMB8GA1Ud
IwQYMBaAFNLEsNKR1EwRcbNhyz2h/t2oatTjMDQGCCsGAQUFBwEBBCgwJjAkBggr
BgEFBQcwAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMDIGA1UdHwQrMCkwJ6Al
oCOGIWh0dHA6Ly9jcmwuZ29kYWRkeS5jb20vZ2Ryb290LmNybDBGBgNVHSAEPzA9
MDsGBFUdIAAwMzAxBggrBgEFBQcCARYlaHR0cHM6Ly9jZXJ0cy5nb2RhZGR5LmNv
bS9yZXBvc2l0b3J5LzANBgkqhkiG9w0BAQsFAAOCAQEAWQtTvZKGEacke+1bMc8d
H2xwxbhuvk679r6XUOEwf7ooXGKUwuN+M/f7QnaF25UcjCJYdQkMiGVnOQoWCcWg
OJekxSOTP7QYpgEGRJHjp2kntFolfzq3Ms3dhP8qOCkzpN1nsoX+oYggHFCJyNwq
9kIDN0zmiN/VryTyscPfzLXs4Jlet0lUIDyUGAzHHFIYSaRt4bNYC8nY7NmuHDKO
KHAN4v6mF56ED71XcLNa6R+ghlO773z/aQvgSMO3kwvIClTErF0UZzdsyqUvMQg3
qm5vjLyb4lddJIGvl5echK1srDdMZvNhkREg5L4wn3qkKQmw4TRfZHcYQFHfjDCm
rw==
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint:     81528b89 e165204a 75ad85e8 c388cd68
Do you accept this certificate? [yes/no]: yes

Trustpoint 'SSL-Trustpoint-1' is a subordinate CA and holds a non self-signed certificate.

Trustpoint CA certificate accepted.

% Certificate successfully imported
BGL-G-17-ASA5500-8(config)#
```

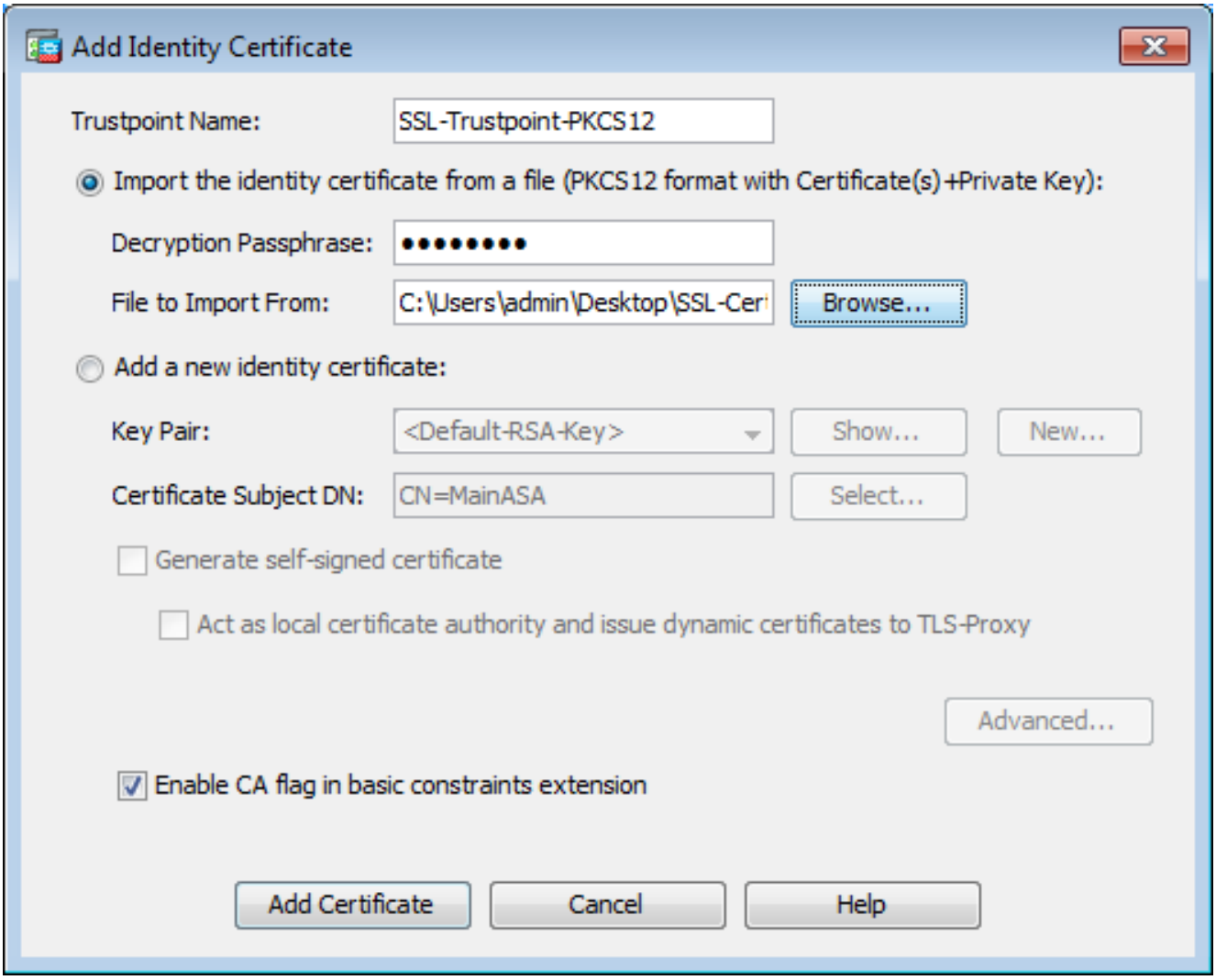
!!! - Similarly create additional trustpoints (of the name "SSL-Trustpoint-n",
where n is number thats incremented for every level in the PKI hierarchy) to
import the CA certificates leading up to the Root CA certificate.

```
!!! - Importing identity certificate (import it in the first trustpoint that was
created namely "SSL-Trustpoint") MainASA(config)# crypto ca import SSL-Trustpoint certificate
WARNING: The certificate enrollment is configured with an fqdn that differs from the system
fqdn. If this certificate will be used for VPN authentication this may cause connection
problems. Would you like to continue with this enrollment? [yes/no]: yes % The fully-qualified
domain name in the certificate will be: vpn.remoteasa.com Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself ----BEGIN CERTIFICATE-----
MIIFRjCCBC6gAwIBAgIIJc1zqYQHBgUwDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNV
BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMRow
GAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UECxMkaHR0cDovL2NlcnRz
LmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQDEypHbyBEYWRkeSBTZWN1
cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMTUwNzIyMTIwNDM4WhcN
MTYwNzIyMTIwNDM4WjA/MSEwHwYDVQQLExhEb21haW4gQ29udHJvbCBWYWxpZGF0
ZWQxGjAYBgNVBAMTEXZwbi5yZW1vdGVhc2EuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEArrY2Fv2S2Uq5HdDhOaSzK5Eyok2tv2Rem8DofbTQ+4F9
C9IXitWdLAo6a7dzyfB4S9hx1VZXoHMGGNd6i9NWLXsWU1Nx5pRMaKR4h1cL6bDW
ITt5GzKdL93ibMxYmau+uwM3OkBb8QxLNNxr4G+oXtfavctTxWy/o6LzKWFyj0XP
tta9FZW07c0MNvKiUL1v9WBcy4GK1xyvN9RtWebtVkM5/iOv0ReBTBfFxCJ1YQAG
UWteu1ikWAGj1qomZGnZgAFDWJ4/hxjesG2BGMtwX5L1O8cbmbi/u/vnmZ5Xhiqx <snip>
CCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHkuY29tL3JlcG9z
aXRvcnkvMHYGCCsGAQUFBwEBBGowaDAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
Z29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydGlmaWNhdGVzLmdv
ZGFkZHkuY29tL3JlcG9zaXRvcnkvZ2RpZzIuY3J0MB8GA1UdIwQYMBaAFEDCvSeO
zDSDMKIz1/tss/C0LIDOMEYGA1UdEQQ/MD2CEXZwbi5yZW1vdGVhc2EuY29tghV3
d3cudnBuLnJlbW90ZWFzYS5jb22CEXZwbi5yZW1vdGVhc2EuY29tMB0GA1UdDgQW
BBT7en7YS3PH+s4z+wTRlpHr2tSzejANBgkqhkiG9w0BAQsFAAOCAQEAO9H8TLNx
2Y0rYdI6gS8n4imaSYg9Ni/9Nb6mote3J2LELG9HY9m/zUCR5yVktra9azdrNUAN
1hjBJ7kKQScLC4sZLONdqG1uTP5rbWR0yikF5wSzgyMWd03kOR+vM8q6T57vRst5
69vzBUuJc5bSu1IjyfPP19z1l+B2eBwUFbVfXLnd9bTfiG9mSmC+4V63TXFxt1Oq
xkGNys3GgYuCUy6yRP2cAUV1lc2tYtaxoCL8yo72YUDDgZ3a4PyO1EvC1FOaUtgv
6QNEOYwmbJkyumdPUwko6wGOC0WLumzv5gHnhil68HYSZ/4XIlp3B9Y8yfG5pwbn 7puhazH+xgQRdg== -----END
CERTIFICATE----- quit INFO: Certificate successfully imported ! Apply the newly installed SSL
certificate to the interface accepting SSL connections MainASA(config)# ssl trust-point SSL-
Trustpoint outside
```

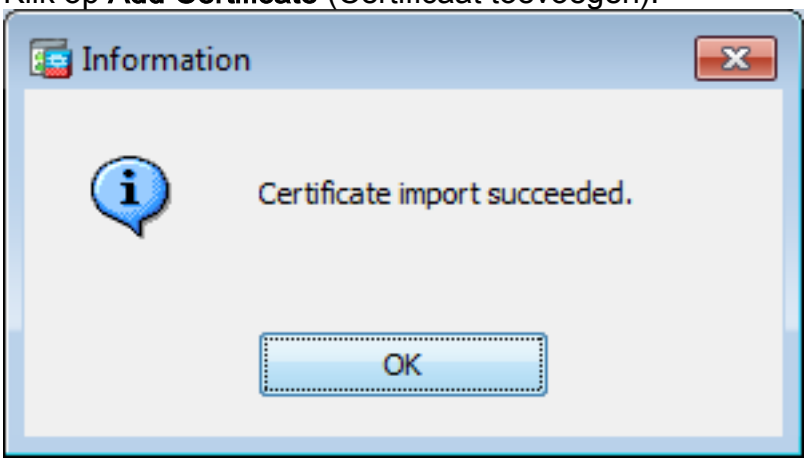
2.1 PKCS12-certificaat installeren met ASDM

In die gevallen waar de CSR niet op de ASA wordt gegenereerd, zoals bij een wildcard-certificaat of wanneer een UC-certificaat wordt gegenereerd, kunnen een identiteitscertificaat en de persoonlijke sleutel worden ontvangen als afzonderlijke bestanden of als gebundeld PKCS12-bestand (.p12 of .pfx). Voer de volgende stappen uit om dit type certificaat te installeren.

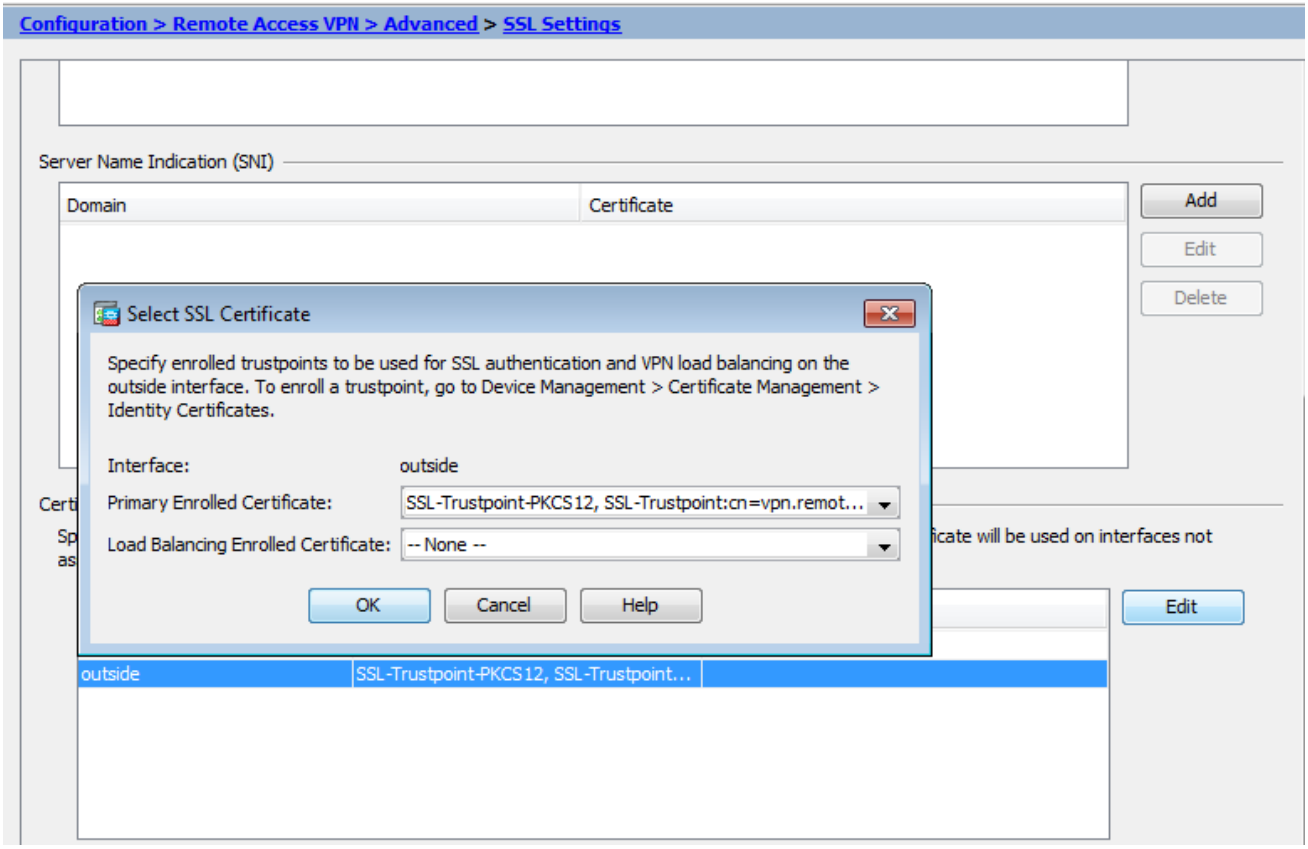
1. Het identiteitsbewijs, bundel het CA-certificaat en de privé-toets in één PKCS12-bestand. In Bijlage B zijn de stappen hiertoe met OpenSSL opgenomen. Als deze al door de CA zijn gebundeld, gaat u verder met de volgende stap.
2. Navigeren in om**Configuration > Remote Access VPN > Certificate Management,** en kies **Identity Certificates.**
3. Klik**Add**.
4. Geef een naam op bij Trustpoint Name (Naam van vertrouwenspunt).
5. Klik op het **Import the identity certificate from a file**radioknop.
6. Geef bij Decryption Passphrase (Wachtwoord voor ontsleuteling) het wachtwoord op dat is gebruikt om het PKCS12-bestand te maken. Blader naar het PKCS12-bestand en selecteer dit. Voer het wachtwoord voor het certificaat in.



7. Klik op **Add Certificate** (Certificaat toevoegen).



8. Navigeren in om**Configuration > Remote Access VPN > Advanced**, en kies **SSL Settings.**
9. Selecteer onder Certificates (Certificaten) de interface waarop WebVPN-sessies moeten eindigen. In dit voorbeeld wordt de buiteninterface gebruikt.
10. Klik**Edit**.
11. Kies in de vervolgkeuzelijst Certificate (Certificaat) het nieuw geïnstalleerde certificaat.



12. Klik**OK**.
13. Klik**Apply**. Het nieuwe certificaat wordt nu gebruikt voor alle WebVPN sessies die op de gespecificeerde interface eindigen.

2.2 PKCS12-certificaat installeren met opdrachtregelinterface

```
  MainASA(config)# crypto ca trustpoint SSL-Trustpoint-PKCS12
MainASA(config-ca-trustpoint)# enrollment terminal
MainASA(config-ca-trustpoint)# exit

MainASA(config)# crypto ca import SSL-Trustpoint-PKCS12 pkcs12 cisco123

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
-----BEGIN PKCS12-----
MIISNwIBAzCCEfEGCSqGSIb3DQEHAaCCEeIEghHeMIIR2jCCEdYGCSqGSIb3DQEH
BqCCEccwghHDAgEAMIIRvAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIWO3D
hDti/uECAQGAghGQ9ospee/qtIbVZh2T8/Z+5dxRPBcStDTqyKy7q3+9ram5AZdG
Ce9n5UCckqT4WcTjs7XZtCrUrt/LkNbmGDVhwGBmYWiOS7npgaUq0eoqiJRK+Yc7
LN0nbho6I5WfL56/JiceAMlXDLr/IqqLg2QAApGdN+F5vANsHse2GsAATewBDLt7
Jy+SKfoNvvIw9QvzCiUzMjYZBANmBdMCQ13H+YQTHitT3vn2/iCDlzRSuXcqypEV
q5e3heiOO75lE8TDLWmO3PMvwIZqi8yzWesjcTt1Kd4FoJBZpB70/v9LntoIUOY7
kIQM8fHb4ga8BYfbgRmG6mkMmO1STtbSvlvTa19WTmdQdTyCa+G5PkrryRsy3Ww1
lkGFMhImmrnNADF7HmzbyslVohQZ7h09iVQY9krJogoXHjmQYxG9brf0oEwxSJDa
mGDhhESh+s/WuFSV9Z9kiTXpJNZxpTASoWBQrrwmO5v8ZwbjbVNJ7sVdbwpUl6d+
NNFGR7LTqO8hpupeeJnY9eJc2yYqeAXWXQ5kLOZo6/gBEdGtEaZBgCFK9JZ3bl3A
xqxGifanWPnLYG611NKuNjTgbjhnEEYI2uZzU0qxnlKa8zyXw+lzrKuJscDbkAPZ
wKtw8K+p4OzXVHhuANo6MDvffNRY1KQDtyK1inoPH5ksVSE5awkVam4+HTcqEUfa
16LMana+4QRgSetJhU0LtSMaQfRJGkha4JLq2t+JrCAPz2osARlTsBOjQBNq6YNj
0uB+gGk2Gl8Q5Nln6K1fz0XBFZLWEDBLsaBRO5MAnE7wWtO0+4awGYqVdmIF1lkf
XIRKAiQEr1pZ6BVPuvsCNJxaaUHzufhYI2ZAckasKBZOT8/7YK3fnAaGoBCz4cHa
o2EEQhq2aYb6YTv0+wtLEWGHzsbGZEM/u54XmsXAI7g28LGJYdfWi509KyV+Ac1V
KzHqXZMM2BbUQCNcTF5JIMiW+r62k42FdahfaQb0vJsIe/IwkAKG7y6DIQFs0hwg
ZlPXiDbNr1k4e8L4gqupMKWg853PY+oY22rLDC7bul1CKtixIYBCvbn7dAYsI4GQ
```

l6xXhNu3+iye0HgbUQQCfTU/mBrA0ZO+bpKjWOCfqNBuYnZ6kUEdCI7GFLH9QqtM
K7YinFLoHwTWbi3MsmqVv+Z4ttVWy7XmikoO2nMynJMP6/CNV8OMxMKdC2qm+c1j
s4QlKcAmFsQmNp/7SIP1wnvOc6JbUmC1O520U/r8ftTzn8C7WL62W79cLK4HOr7J
sNsZnOz0JOZ/xdZT+cLTCtVevKJOQMK3vMsiOuy52FkuF3HnfrmBqDkbR7yZxELG
RCEL0EDdbp8VP0+IhNlyz1q7975SscdxFSL0TvjnHGFWd14ndoqN+bLhWbdPjQWV
l3W2NCI95tmHDLGgp3P0OlS+RjdCEGGMg+9cpgBfFC1JocuTDIEcUbJBY8QRUNiS
/ubyUagdzUKt1ecfb9hMLP65ZNQ93VIw/NJKbIm7b4P/1Zp/lFP5eq7LkQPAxE4/
bQ4mHcnwrs+JGFkN19B8hJmmGoowH3p4IEvwZy7CThB3E1ejw5R4enqmrgvHqpQe
B7odN1OFLAHdo1G5BsHExluNEsEb4OQ0pmKXidDB5B001bJsr748fZ6L/LGx8Al3
<snip>
ijDqxyfQXY4zSytljSMwMtYA9hG5I79Sg7pnME1E9xq1DOoRGg8vgxlwiciKtLxp
LL0ReDY31KRYv00vW0gf+tE7lST/3TKZvh0sQ/BE0V3kHnwldejMFH+dvyAA9Y1E
c8O+tdafBFX4B/HP46E6heP6ZSt0xAfRW1/JF4ljNvUNVO9VtVfR2FTyWpzZFY8A
GG5XPIA80WF6wKEPFHIcN8scY+Vot8kXxG96hwt2Cm5NQ2OnVzxUZQbpKsjs/2jC
3HVFe3UJFBsY9UxTLcPXYBSIG+VeqkI8hWZp6clTfNDLY2ELDylQzp1mBg2FujZa
YuE0avjCJzBzZUG2umtS5mHQnwPF+XkOujEyhGMauhGxHp4nghSzrUZrBeuL9lUF
2mbpsOcgZkzxMS/rjdNXjCmPFloRBvKkZSlxHFrE/5ZopAhn4i7YtHQNrz9U4RjQ
xo9cUuaJ+LNmvzE8Yg3epAMYZ16UNGQQkVQ6ME4BcjRONzW8BYgTq4+pmT1ZNq1P
X87CXCPtYRpHF57eSo+tHDINCgfqYXD6e/7r2ngfiCeUeNDZ4aVl2XxvZDaUlBPP
Tx5fMARqx/Z8BdDyBJDVBjdsxmQau9HLkhPvdfGlZIWdTe13CzKqXA5Ppmpjt4q9
GnCpC53m76x9Su4ZDw6aUdBcgCTMvfaqJC9gzObee2Wz+aRRwzSxu6tEWVZolPEM
v0AA7po3vPeklgOnLRAwEoTTn4SdgNLWeRoxqZgkw1FC1GrotxF1so7uA+z0aMeU
lw73reonsNdZvRAcVX3Y6UNFdyt70Ixvo1H4VLzWm0K/oP62C9/eqqMwZ8zoCMPt
ENna7T+7Os66SCbMmXCHwyhO0tygNKZFFw/AATFyjqPMWPAxGuPNOrnB6uYCn0Hk
1BU7tF143RNIZaQQEH3XnaPvUuAA4C0FCoE3h+/tVjtfNKDvFmb6ZLZHYQmUYpyS
uhdFEpoDrJH1VmI2Tik/iqYWaZ+oDqXPHQXnJhw25h9ombR4qnD+FCfwFCGtPFON
o3QffZ53C95n5jPHVMyUrOxDdpwnvzCQPdj6yQm564TwLAmiz7uDlpqJZJe5QxHD
nolv+4MdGSfVtBq+ykFoVCaamqeaq6sKgvAVujLXXEs4KEmIgcPqATVRG49ElndI
LO1DEQyKhVoDGebAuVRBjzwAm/qxWxxFv3hrbCjpHCwEYms4Wgt/vKKRFsuWJNZf
efHldwlltkd5dKwSvDocPT/7mSLtLJa94c6AfgxXy9zO+FTLDQwzxga7xC2krAN1
yHxR2KHN5YeRL+KDzu+u6dYoKAz+YAgwlW6KbeavALSuH4EYqcvg8hUEhp/ySiSc
RDhuygxEovIMGfES4FP5V52lPyDhM3Dqwhn0vuYUmYnX8EXURkay44iwwI5HhqYJ
lptWyYo8Bdr4WNwt5xqszGzYR6mmGeAIin7bDunsF1uBHWYF4dyKlz1tsdRNMYqQ
+W5q+QjVdrjldWv/bMFOaqEjxeNWBRqjzcff3BxMnwvVxtgqxFvRh+DZxiJoiBG+
yx7x8np2AQ1r0METSSxbnZzfnKZKVvBVMkIC6Jsmt2WEVTQvoFJ8em+nemOWgTi/
hHSBzjE7RhAucnHuifOCXOgvR1SDDqyCQbiduc1QjXN0svA8Fqbea9WEH5khOPv3
pbtsL4gsfl2pv8diBQkVQgiZDi8Wb++7PR6ttiY65kVwrdsoNl1/qq+xWOd3tB4/
zoH9LEMgTy9Sz7myWrB9EOOZ8BIjL1M8oMigEYrTDOc3KbyW1S9dd7QAxiuOBaX1
8J8q1OydvTBzmqcjeSsFH4/1NHn5VnfOZnNpui4uhpOXBG+K2zJUJXm6dq1AHBlE
KQFsFZpNNyave0Kk8JzQnLAPd7OUU/IksyOCGQozGBH+HSzVp1RDjrrbC342rkBj
wnI+j+/1JdWBmHdJMZCfoMZFLSI9ZBqFirdii1/NRu6jh76TQor5TnNjxIyNREJC
FE5FZnMFvhM900LaiUZff8WWCOfeRDMttLXb1nuxPFl+lRk+LNlPLVptWgcxzfsr
JXrGiwjxybBB9oCOrACq8fGAtEs8WRxJyDH3Jjmn9i/Gl6J1mMCUF//LxAH2WQx8
Ld/qS5OM2iFCffDQjxAj0K6DEN5pUebBv1Em5SOHXvyq5nxgUh4/y84CWaKjw0MQ
5tbbLMlnc7ALIJ9LxZ97YiXSTyeM6oBXBFx6RpklkDv05mlBghSpVQiMcQ2ORIkh
UVVNbSHOl9S3cb5wqxaWqAKBqb4h1uLGVbYWZf2mzLZ8U5U5ioiqoMBqNZbzTXpO
EqEFuatTllQvCRbcKS3xou4MAixcYUxKwEhbZA/6hd10XSBJwe7jKBV9M6wliKab
UfoJCGTAf3sY68lqrMPrbBt0eeWf1C02Sd9Mn+V/jvnil7mxYFFUpruRq3r1LeqP
J5camfTtHwyL8N3Q/Zwp+zQeWZiLA8a/iAVu/hYLR1bpF2WCK0lOtJqkvVmrLVLz
maZZjbJeOft5cP/lRxbKlS6Gd5dFTEKDE15c6gWUX8RKZP6Q7iaE5hnGmQjm8Ljl
kXwF+ivoxOQ8a+Gg1bVTROc7tqW9e9/ewisV1mwvEB6Ny7TDS1oPUDHM84pY6dqi
1+Oio07Ked4BySwNlYy9yaJtBTZSCstfP+ApLidN7pSBvvXf1aHmeNbkPOZJ+c+t
fGpUdL6V2UTXfCsOPHTC0ezA15sOHwCuPchrDIj/eGUwMS3NfS25XgcMuvnLqGVO
RzcRzlZIg8G0oLYwOCuzoY0D/m9010O1ahePyA9tmVB7HRRbytLdaW7gYeEikoCv
7qtBqJFF17ntWJ3EpQHZUcVClbHIKqjNqRbDCY7so4AlIW7kSEUGWMIUDhprE8Ks
NpnvPH2i9JrYrTeROyUI0tL/7SATd2P0a2lxz/zUWekeqd0bmVCsAgQNbB2XkrR3
XS0B52ol+63e8KDqS2zL2TZd3daDFidHlB8QB26tfbfOAcaObJH5/dWP8ddo8UYo
Y3JqTl0malxSJhaMHmQdZIQp49utW3TcjqGllYS4HEmcqtHud0ShaUysC6239jlQ
KlFWrwXTlBC5vnq5IcOMqx5zyNbfxXz28969cWoMCyU6+kRw0TyF6kF7EEv6XWca
XLEwABx+tKRUKHJ673SyDMu96KMV3yZN+RtKbCjqCPVTP/3ZeIp7nCMUcj5sW9HI
N34yeI/0RCLyeGsOEiBLkucikC32LI9ik5HvImVTELQ0Uz3ceFqU/PkasjJUve6S
/n/1ZVUHbUk71xKR2bWZgECl7fIel7wlrbjpF3Wbk+Er0kfYcsNRHxeTDpKPSt9s
u/UsyQJiyNARG4X3iYQlsTce/06Ycyri6GcLHAu58B02nj4CxolCplABZ2N79HtN
/7Kh5L0pS9MwsDCHuUI8KFrTsET7TB1tIU99FdB19L64sl/shYAHbccvVWU50Wht

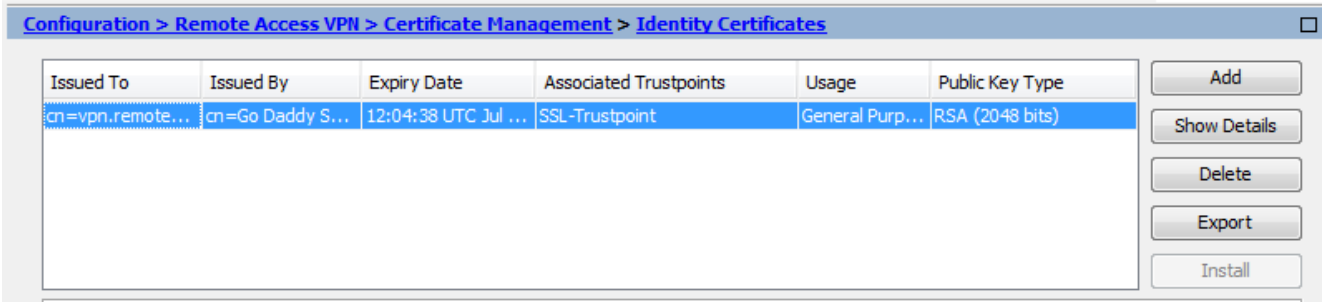
```
PdLoaErrX81Tof41IxbSZbI8grUC4KfG2sdPLJKu3HVTeQ8LfllbBLxfs8ZBS+Oc
v8rHlQ012kY6LsFGLehJ+/yJ/uvXORiv0ESp4EhFpFfkp+o+YcFeLUUPd+jzb62K
HfSCCbLpCKyEay80dyWkHfgylqxmb9ud0oMO50aFJyqR0NjNt6pcxBRY2A6AJR5S
IIC26YNwbh0GjF9qL2FiUqnNH/7GTqPnd2qmsB6FTIwSBT6d854qN7PRt+ZXgdtQ
OjcYt1r9qpWDZpNFK8EzizwKiAYTsiEh2pzPt6YUpksRb6CXTkIzoG+KLsv2m3b8
OHyZ9a8z81/gnxrZlls5SCTfOSU70pHWh8VAYKVHHK+MWgQr0m/2ocV32dkRBLMy
2R6P4WfHyI/+9de1x3PtIuOiv2knpxHv2fKM6sQw45F7XkmwHxjq1YRJ6vIwPTAh
MAkGBSsOAwIaBQAEFFTRETzpisHKZR+Kmen68VrTwpV7BBSQi0IesQ4n4E/bSVsd
qJSzcwh0hgICBAA=
-----END PKCS12-----
quit
INFO: Import PKCS12 operation completed successfully

!!! Link the SSL trustpoint to the appropriate interface MainASA(config)# ssl trust-point SSL-
Trustpoint-PKCS12 outside
```

Verifiëren

Voer de volgende stappen uit om geslaagde installatie van het certificaat van de externe leverancier en gebruik voor SSLVPN-verbindingen te verifiëren.

Geïnstalleerde certificaten bekijken via ASDM

1. Navigeren in om**Configuration > Remote Access VPN > Certificate Management,**en kies **Identity Certificates.**
2. Het door de derde verkoper afgegeven identiteitsbewijs verschijnt.



Geïnstalleerde certificaten bekijken via opdrachtregelinterface

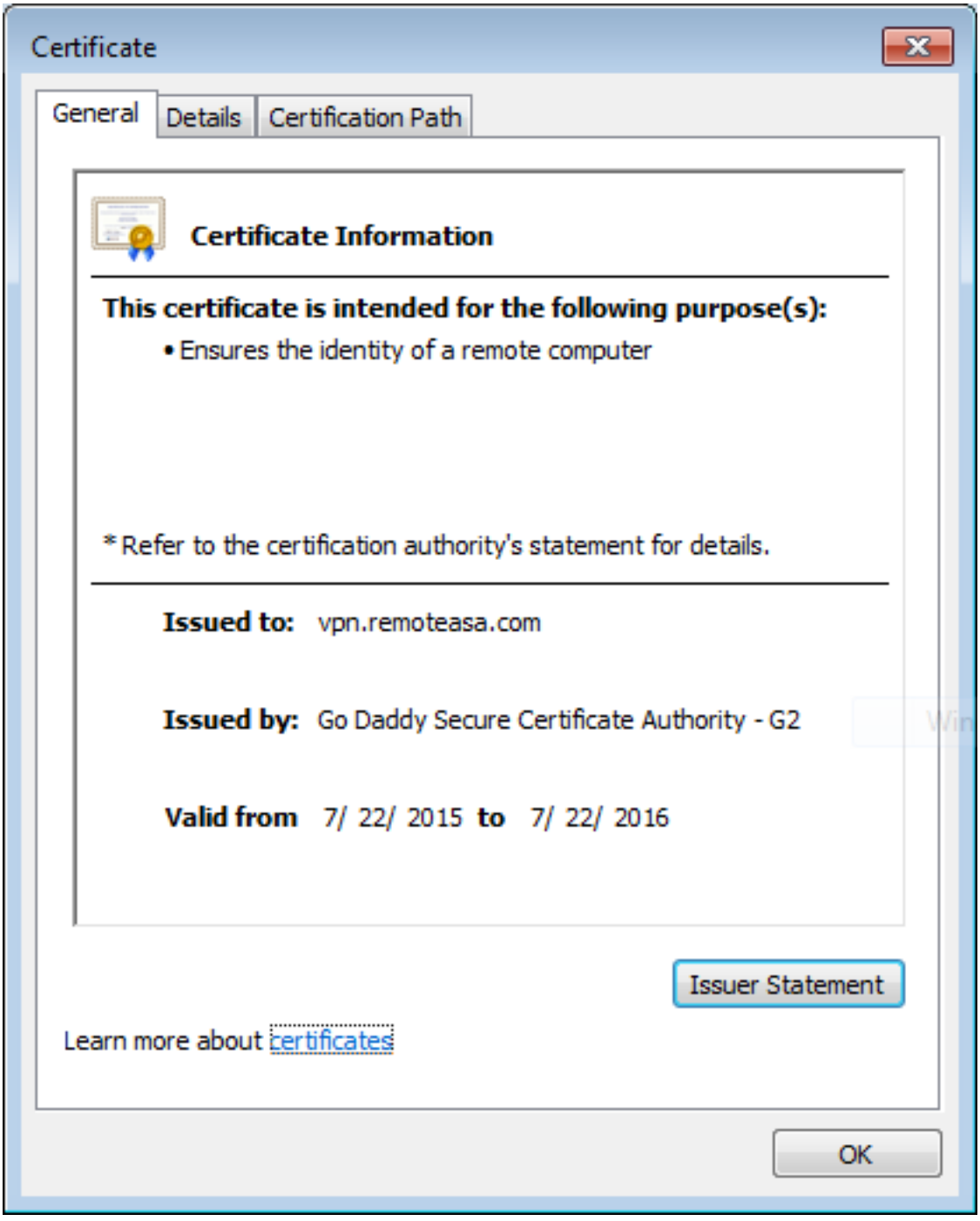
```
 MainASA(config)# show crypto ca certificate

Certificate
  Status: Available
  Certificate Serial Number: 25cd73a984070605
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject Name:
    cn=vpn.remoteasa.com
    ou=Domain Control Validated
  OCSP AIA:
    URL: http://ocsp.godaddy.com/
```

```
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdig2s1-96.crl
  Validity Date:
    start date: 12:04:38 UTC Jul 22 2015
    end   date: 12:04:38 UTC Jul 22 2016
  Associated Trustpoints: SSL-Trustpoint

CA Certificate
  Status: Available
  Certificate Serial Number: 07
  Certificate Usage: General Purpose
  Public Key Type: RSA (2048 bits)
  Signature Algorithm: SHA256 with RSA Encryption
  Issuer Name:
    cn=Go Daddy Root Certificate Authority - G2
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  Subject Name:
    cn=Go Daddy Secure Certificate Authority - G2
    ou=http://certs.godaddy.com/repository/
    o=GoDaddy.com\, Inc.
    l=Scottsdale
    st=Arizona
    c=US
  OCSP AIA:
    URL: http://ocsp.godaddy.com/
  CRL Distribution Points:
    [1]  http://crl.godaddy.com/gdroot-g2.crl
  Validity Date:
    start date: 07:00:00 UTC May 3 2011
    end   date: 07:00:00 UTC May 3 2031
  Associated Trustpoints: SSL-Trustpoint

CA Certificate
 Status: Available
 Certificate Serial Number: 1be715
 Certificate Usage: General Purpose
 Public Key Type: RSA (2048 bits)
 Signature Algorithm: SHA256 with RSA Encryption
 Issuer Name:
   ou=Go Daddy Class 2 Certification Authority
   o=The Go Daddy Group\, Inc.
   c=US
 Subject Name:
   cn=Go Daddy Root Certificate Authority - G2
   o=GoDaddy.com\, Inc.
   l=Scottsdale
   st=Arizona
   c=US
 OCSP AIA:
   URL: http://ocsp.godaddy.com/
 CRL Distribution Points:
   [1]  http://crl.godaddy.com/gdroot.crl
 Validity Date:
   start date: 07:00:00 UTC Jan 1 2014
   end   date: 07:00:00 UTC May 30 2031
 Associated Trustpoints: SSL-Trustpoint-1

...(and the rest of the Sub CA certificates till the Root CA)
```

Geïnstalleerde certificaten voor WebVPN verifiëren via een webbrowser

Controleer dat WebVPN het nieuwe certificaat gebruikt.

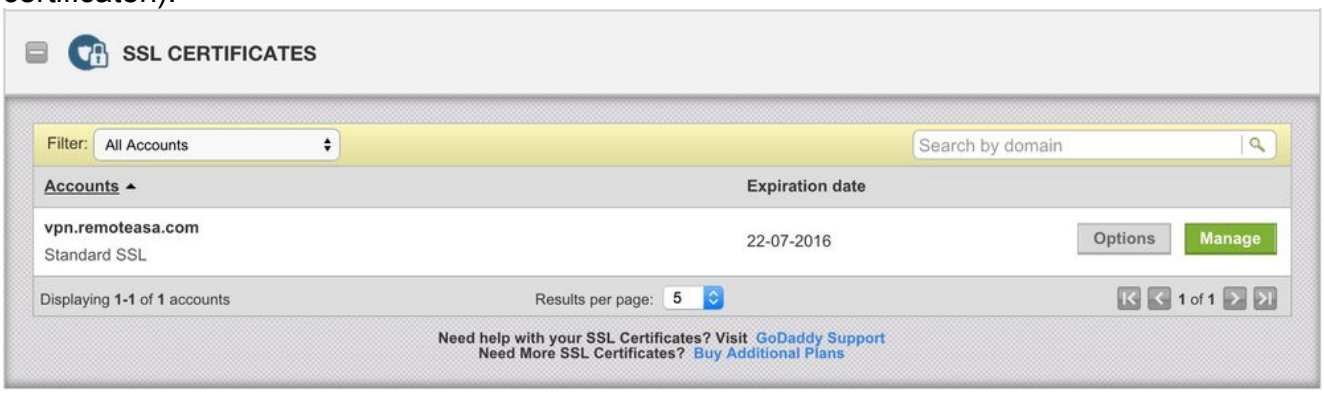
1. Maak via een webbrowser verbinding met de WebVPN-interface. Gebruik https:// en de FQDN om het certificaat op te vragen (bijvoorbeeld https://vpn.remoteasa.com).
2. Dubbelklik op het slotpictogram dat rechtsonder in het WebVPN-aanmeldingspagina staat. De informatie van het geïnstalleerde certificaat wordt getoond.
3. Bekijk de inhoud om te controleren of dit certificaat overeenkomt met het certificaat dat door de externe leverancier is verstrekt.



SSL-certificaat verlengen op de ASA

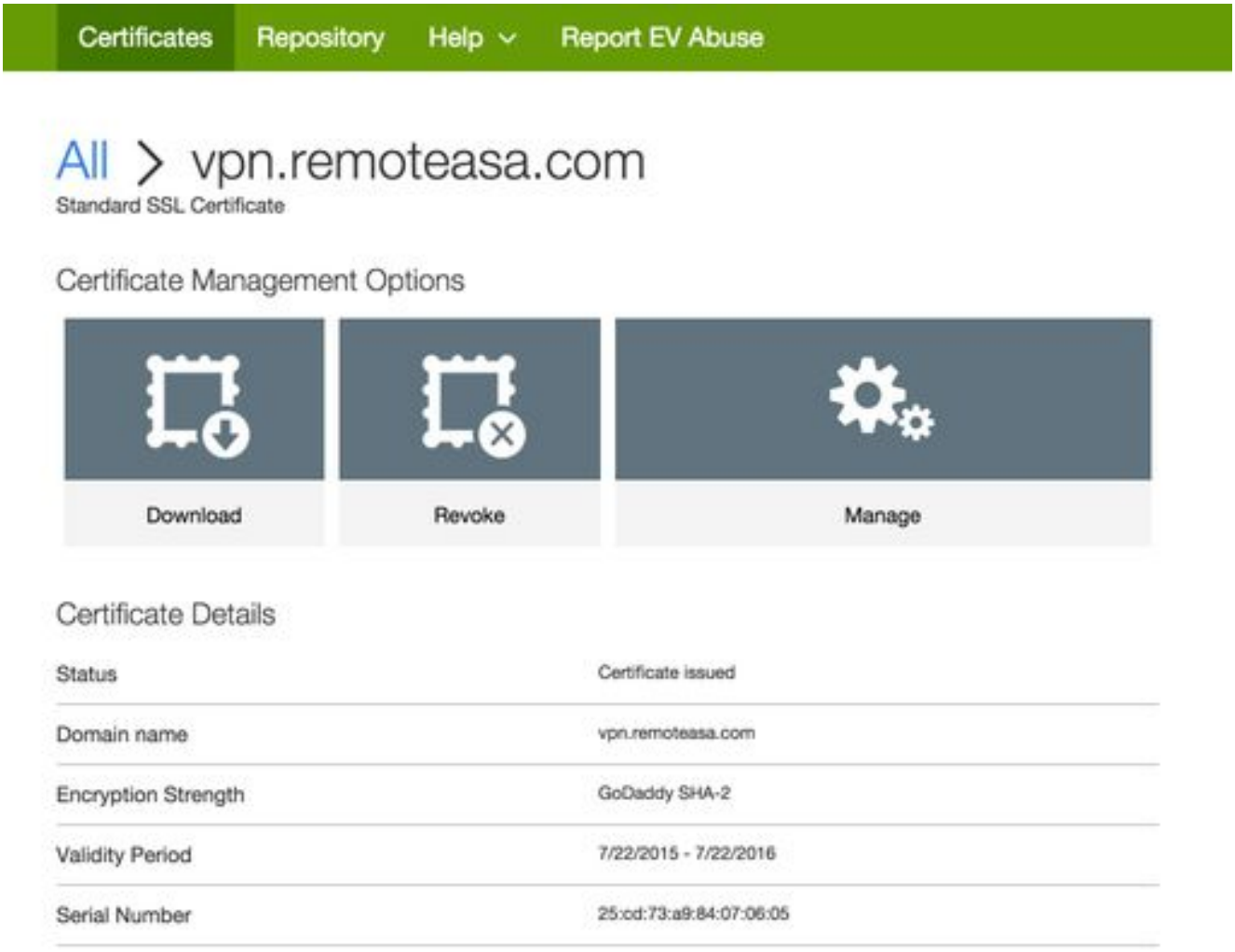
1. Regenereer de CSR op de ASA, met OpenSSL of op de CA met dezelfde kenmerken als het oude certificaat. Voer de stappen bij CSR genereren uit.
2. Dien de CSR in bij de CA en genereer een nieuw identiteitscertificaat in PEM-opmaak (.pem, .cer, .crt) samen met het CA-certificaat. In het geval van een PKCS12-certificaat zal er ook

sprake zijn van een nieuwe persoonlijke sleutel. In het geval van GoDaddy CA kan het certificaat opnieuw worden versleuteld met een nieuwe gegenereerde CSR.Ga naar GoDaddy en klik op **Manage** (Beheren) bij SSL Certificates (SSL-certificaten).

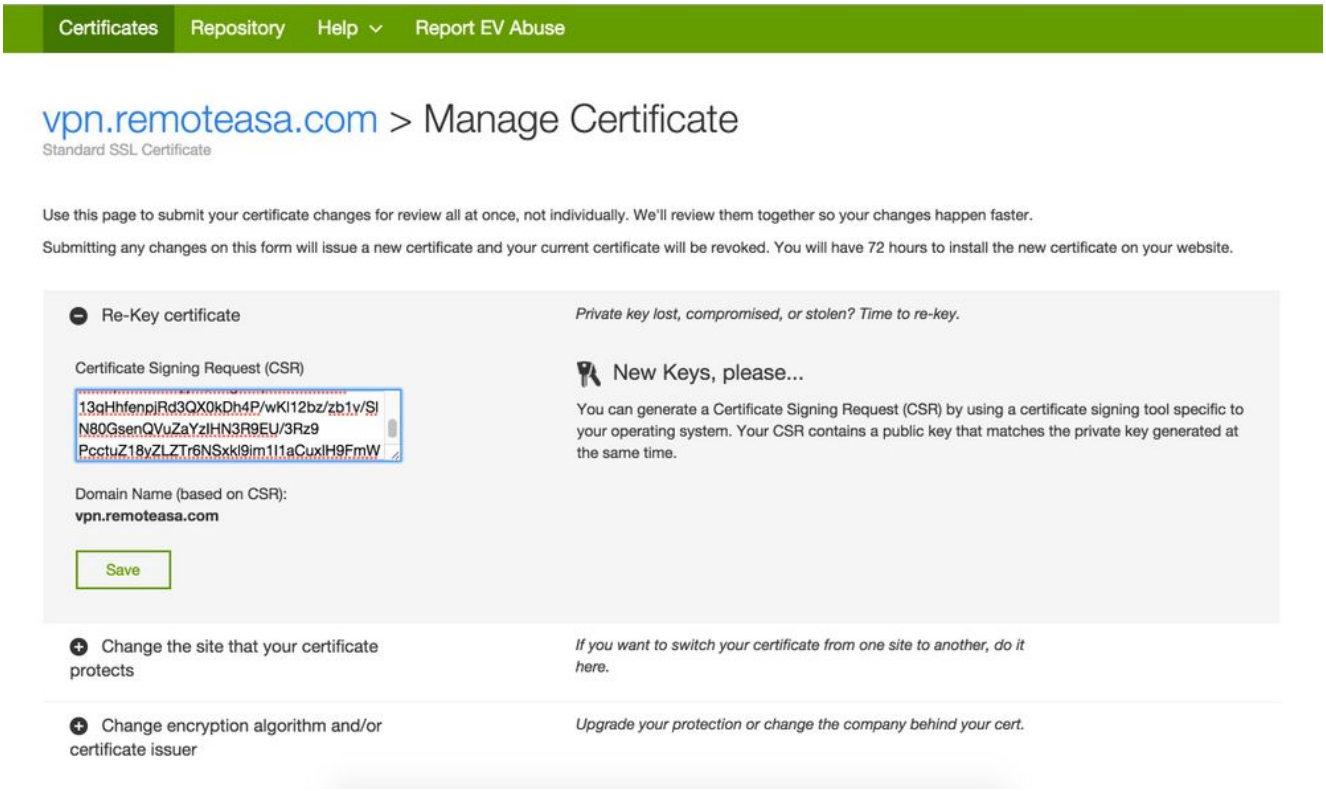


Klik op **View Status (Status weergeven) voor de vereiste domeinnaam.**

Klik op **Bewerken** om opties te geven om het certificaat opnieuw te selecteren.



Vouw de optie **Re-Key certificate (Certificaat opnieuw versleutelen) uit en voeg de nieuwe CSR**
toe.



Sla op en ga verder met de volgende stap. GoDaddy zal een nieuw certificaat verstrekken op

basis van de ingediende CSR.
3. Installeer het nieuwe certificaat op een nieuw vertrouwenspunt zoals getoond bij de sectie ‘SSL-certificaat installeren op de ASA’.

Veelgestelde vragen

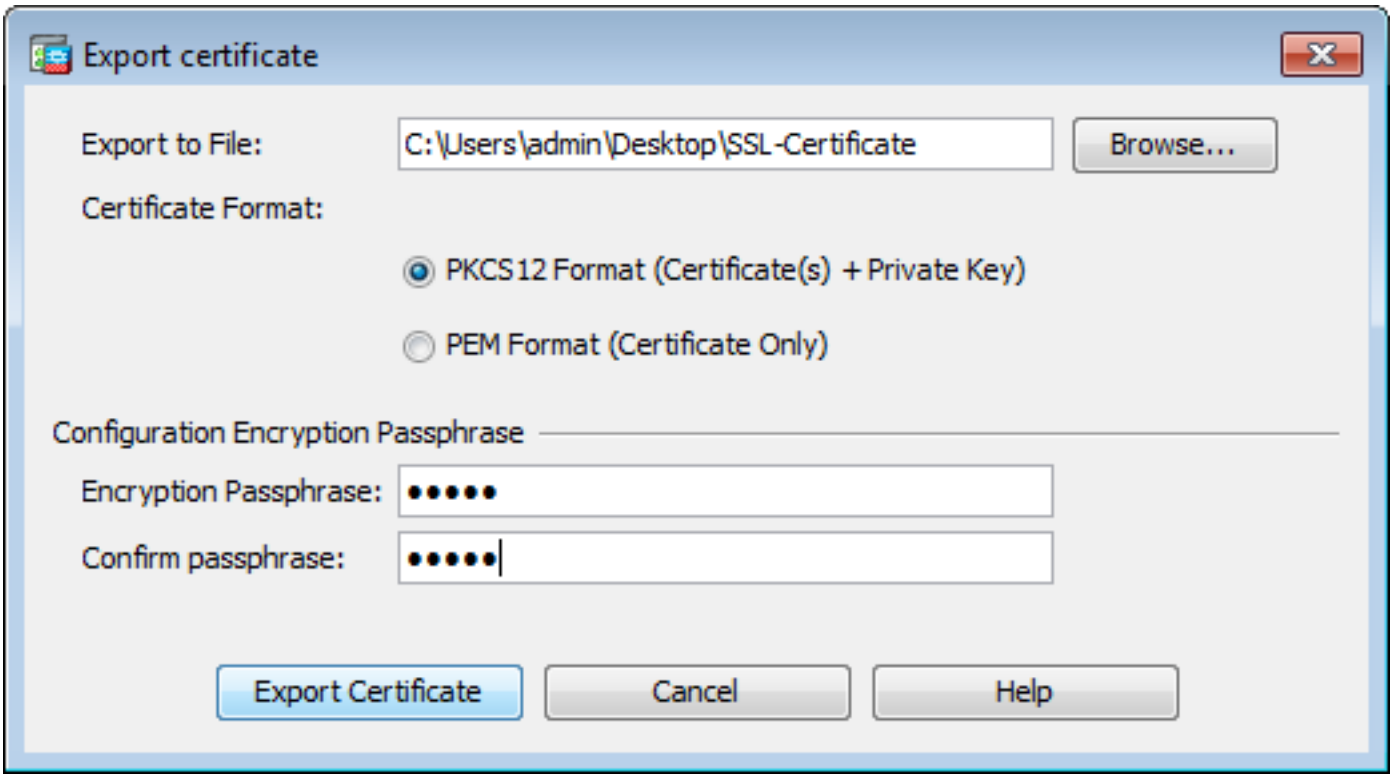
1. Wat is de beste manier om identiteitsbewijzen van de ene ASA naar de andere over te dragen?

Exporteer het certificaat samen met de sleutels naar een PKCS12-bestand.

Gebruik de volgende opdracht om het certificaat via de opdrachtregelinterface te exporteren vanaf de oorspronkelijke ASA:

```
ASA(config)#crypto ca export
```

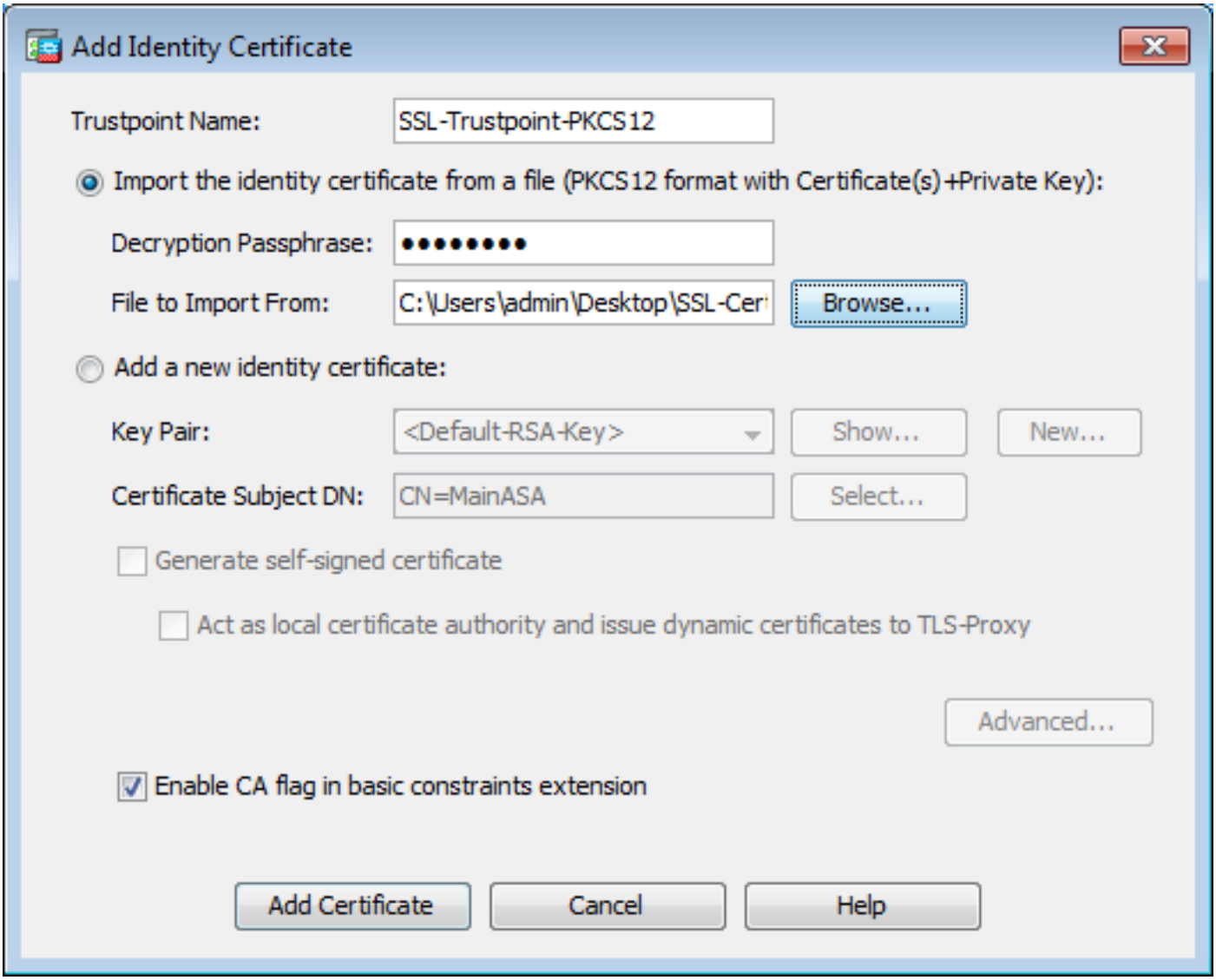
Overeenkomstige ASDM-configuratie:



Gebruik deze opdracht om het certificaat via de opdrachtregelinterface te importeren op de doel-ASA:

```
ASA(config)#crypto ca import
```

Overeenkomstige ASDM-configuratie:



Dit is ook mogelijk met de functie Backup/Restore (Back-up maken/terugzetten) op ASDM door de volgende stappen uit te voeren:

1. Meld u aan bij de ASA via ASDM en kies**Tools > Backup Configuration.**
2. Maak een back-up van de gehele configuratie of alleen van de identiteitscertificaten.
3. Open de ASDM-modus en kies in de keuze**Tools > Restore Configuration.**

2. Hoe kan ik SSL-certificaten genereren voor gebruik op ASA's met VPN-taakverdeling?

Er zijn meerdere methoden die kunnen worden toegepast om ASA's in te stellen met SSL-certificaten voor een omgeving met VPN-taakverdeling.

1. Gebruik een enkel UCC (Unified Communications Certificate voor meerdere domeinen) met de taakverdelings-FQDN als DN en elke ASA-FQDN als afzonderlijke SAN (Subject Alternative Name, alternatieve naam voor onderwerp). Er zijn meerdere bekende CA's, zoals GoDaddy, Entrust en Comodo, die dergelijke certificaten ondersteunen. Wanneer u deze methode selecteert, moet u er rekening mee houden dat de ASA momenteel het maken van

een CSR met meerdere SAN-velden niet ondersteunt. Dit is vastgelegd in Cisco bug-ID CSCso70867. In dit geval zijn er twee opties voor het genereren van de CSR: Via de opdrachtregelinterface of ASDM. Wanneer de CSR wordt ingediend bij de CA moet u de SAN's op de CA-portal toevoegen.Gebruik OpenSSL om de CSR te genereren en de meerdere SAN's in het openssl.cnf-bestand op te nemen.Zodra de CSR is ingediend bij de CA en het certificaat is gegenereerd, importeert u dit PEM-certificaat naar de ASA die de CSR heeft gegenereerd. Is dit certificaat eenmaal uitgevoerd en importeer het in PKCS12-formaat op de andere ASA-lidstaten.

2. Gebruik een wildcard-certificaat. Dit is een minder veilige en flexibele methode in vergelijking met het gebruik van een UC-certificaat. Als de CA geen UC-certificaten ondersteunt, wordt er een CSR gegenereerd via de CA of met OpenSSL waar de FQDN zich in de vorm van *.domain.com bevindt. Zodra de CSR is ingediend bij de CA en het certificaat is gegenereerd, importeert u het PKCS12-certificaat naar alle ASA's in het cluster.
3. Gebruik een afzonderlijk certificaat voor elke lid-ASA en voor de taakverdelings-FQDN. Dit is de minst effectieve oplossing. De certificaten voor elke afzonderlijke ASA kunnen worden gemaakt zoals in dit document wordt getoond. Het certificaat voor de taakverdelings-FQDN van VPN wordt op de ene ASA gemaakt en als een PKCS12-certificaat geëxporteerd en geïmporteerd op de andere ASA's.

3. Moeten de certificaten van de primaire ASA naar de secundaire ASA worden gekopieerd in een ASA failover-paar?

Het is niet nodig om de certificaten van de primaire ASA te kopiëren naar de secundaire ASA, omdat de certificaten worden gesynchroniseerd tussen de ASA's wanneer stateful failover is geconfigureerd. Als bij eerste installatie of failover de certificaten niet zichtbaar zijn op het stand-byapparaat, gebruikt u de opdracht **write standby om synchronisatie af te dwingen.**

4. Als ECDSA-toetsen worden gebruikt, is het SSL-certificeringsproces dan anders?

Het enige verschil is de stap voor het genereren van het sleutelpaar, waarbij een ECDSA-sleutelpaar wordt gegenereerd in plaats van een RSA-sleutelpaar. De overige stappen zijn gelijk. De CLI-opdracht voor het genereren van de ECDSA-toetsen wordt hier weergegeven:

```
 MainASA(config)# cry key generate ecdsa label SSL-Keypair elliptic-curve 256
INFO: The name for the keys will be: SSL-Keypair
Keypair generation process begin. Please wait...
```

Problemen oplossen

Opdrachten voor troubleshooting

De volgende foutopsporingsopdrachten moeten worden opgegeven via de opdrachtregelinterface als installatie van een SSL-certificaat mislukt:

debug crypto ca 255

debug crypto ca messages 255

debug crypto ca transactions 255

Veelvoorkomende problemen

Waarschuwing over niet-vertrouwd certificaat bij gebruik van een geldig SSL-certificaat van derden op de buiteninterface van ASA met versie 9.4(1) en hoger.

Oplossing: Dit probleem treedt op wanneer een RSA-sleutelpaar wordt gebruikt met het certificaat. Bij ASA-versies vanaf 9.4(1) worden alle ECDSA- en RSA-coderingen standaard ingeschakeld. De krachtigste codering (doorgaans ECDSA) wordt gebruikt voor onderhandeling. In dat geval wordt op de ASA een zelf-ondertekend certificaat gebruikt in plaats van het momenteel geconfigureerde RSA-gebaseerde certificaat. Er wordt gewerkt aan een verbetering om het gedrag te wijzigen wanneer een RSA-gebaseerd certificaat op een interface is geïnstalleerd. Dit is vastgelegd in Cisco bug-ID CSCuu02848.

Aanbevolen actie: Schakel ECDSA-coderingen uit met de volgende CLI-opdrachten:

```
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:
DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"
```

Of, met de ASDM, navigeer naar**Configuration > Remote Access VPN > Advanced**, en kies**SSL Settings**. Selecteer bij Encryption (Versleuteling) coderingsversie **tlsv1.2 en bewerk deze met de aangepaste tekenreeks AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5**

Bijlage

Bijlage A: ECDSA of RSA

Het ECDSA-algoritme is onderdeel van ECC (cryptografie met behulp van elliptische krommen) en maakt gebruik van een vergelijking van een elliptische kromme om een openbare sleutel te genereren. Het RSA-algoritme gebruikt het product van twee priemgetallen plus een kleiner getal om de openbare sleutel te genereren. Dit betekent dat met ECDSA hetzelfde niveau van security kan worden bereikt als met RSA, maar met kleinere sleutels. Hierdoor wordt de berekeningstijd verkort en worden de verbindingstijden verlengd voor sites die ECDSA-certificaten gebruiken.

In het document Next Generation Cryptography and the ASA (Next-generation cryptografie en de ASA) is diepgaandere informatie opgenomen.

Bijlage B: OpenSSL gebruiken om een PKCS12-certificaat te genereren op basis van een identiteitscertificaat, CA-certificaat en persoonlijke sleutel

1. Controleer dat OpenSSL op het systeem is geïnstalleerd waarop dit proces is uitgevoerd. Bij macOS X en GNU/Linux is dit standaard geïnstalleerd.
2. Schakel over naar een werkmap. Voor Windows: De hulpprogramma's worden standaard geïnstalleerd in C:\Openssl\bin. Open een opdrachtprompt op deze locatie.Voor macOS X en Linux: Open een terminal-venster in de map die nodig is om het PKCS12-certificaat te maken.
3. Sla de persoonlijke sleutel (privateKey.key), het identiteitscertificaat (certificate.crt) en de basis-CA-certificaatketen (CACert.crt) op in de map die is aangegeven in de vorige stap. Bundel de persoonlijke sleutel, het identiteitscertificaat en de basis-CA-certificaatketen in een PKCS12-bestand. Voer een wachtwoord in om uw PKCS12-certificaat te beschermen.

```
strong> openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in
certificate.crt -certfile CACert.crt
```

4. Converteer het PKCS12-certificaat dat is gegenereerd naar een Base64-gecodeerd certificaat:
   `openssl base64 -in certificate.pfx -out certificate.p12`

Importeer vervolgens het certificaat dat in de laatste stap is gegenereerd voor gebruik met SSL.

Gerelateerde informatie

- Configuratiehandleiding ASA 9.x – digitale certificaten configureren
- Een digitaal certificaat verkrijgen van een Microsoft Windows-certificeringsinstantie met ASDM op een ASA
- **Technische ondersteuning en documentatie – Cisco Systems**