ASA 8.x: Verleng en Installeer het SSL-certificaat met ASDM

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Procedure](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Hoe SSL-certificaten van de ene ASA naar de andere kopiëren](#)
[Gerelateerde informatie](#)

Inleiding

De procedure in dit document is een voorbeeld en kan als richtlijn worden gebruikt bij elke certificatenverkoper of uw eigen basiscertificeringsserver. Soms worden er speciale certificaateparameter-vereisten vereist door uw certificaathouder, maar dit document is bedoeld om de algemene stappen te leveren die vereist zijn om een SSL-certificaat te vernieuwen en het op een ASA te installeren die software 8.0 gebruikt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Deze procedure heeft betrekking op ASA versie 8.x met ASDM versie 6.0(2) of hoger.

De procedure in dit document is gebaseerd op een geldige configuratie met een certificaat dat is geïnstalleerd en gebruikt voor SSL VPN-toegang. Deze procedure heeft geen invloed op uw netwerk zolang het huidige certificaat niet wordt verwijderd. Deze procedure is een stap-voor-stap proces voor het uitgeven van een nieuw CSR voor een huidig certificaat met het zelfde wortelcertificaat dat de originele wortel CA verstrekte.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Als uw netwerk live is, moet u de potentiële impact van elke opdracht

begrijpen.

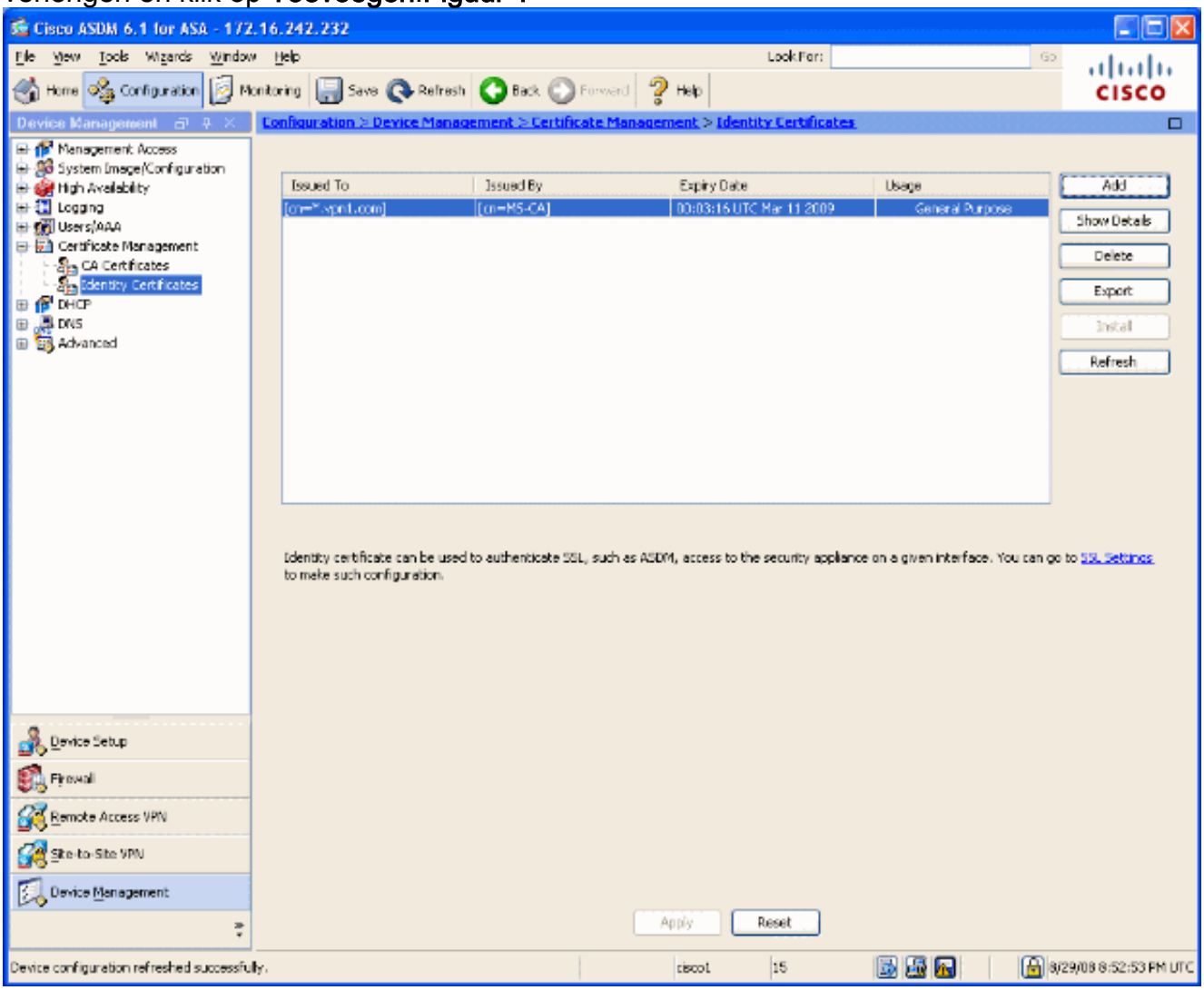
Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

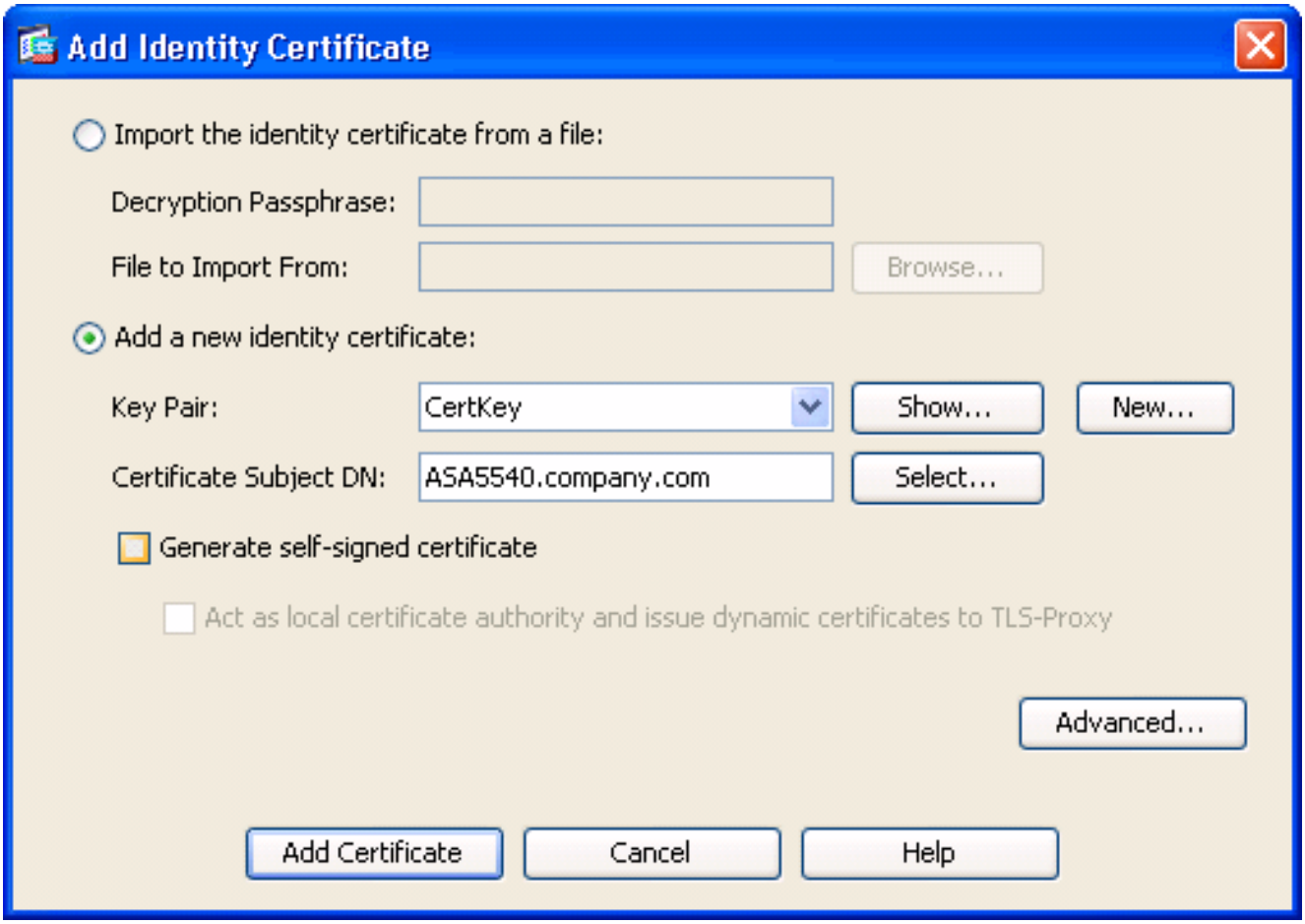
Procedure

Voer de volgende stappen uit:

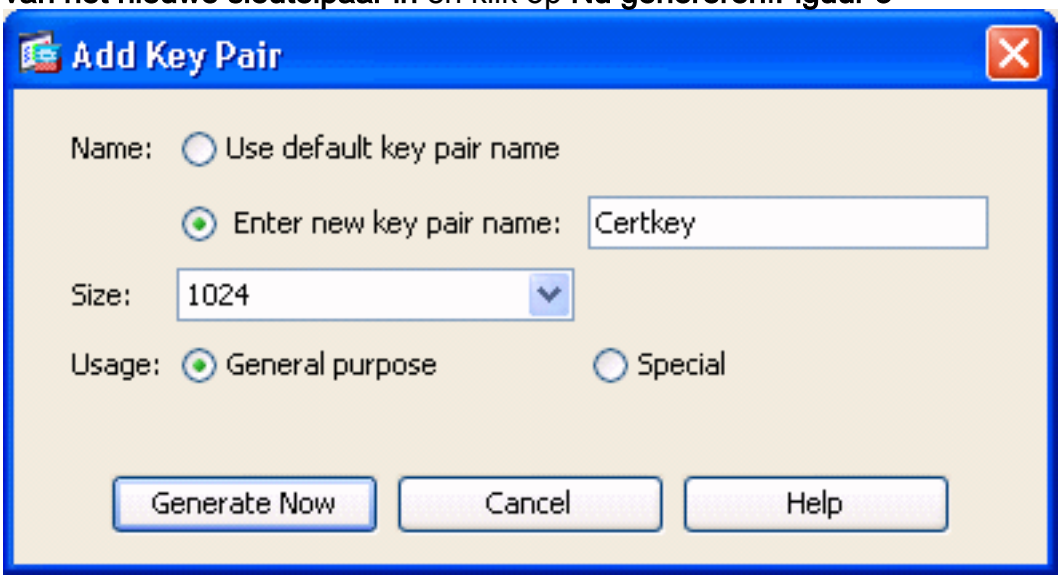
1. Selecteer het certificaat dat u onder Configuratie > Apparaatbeheer > Identity Certificaten wilt verlengen en klik op **Toevoegen**.**Figuur 1**



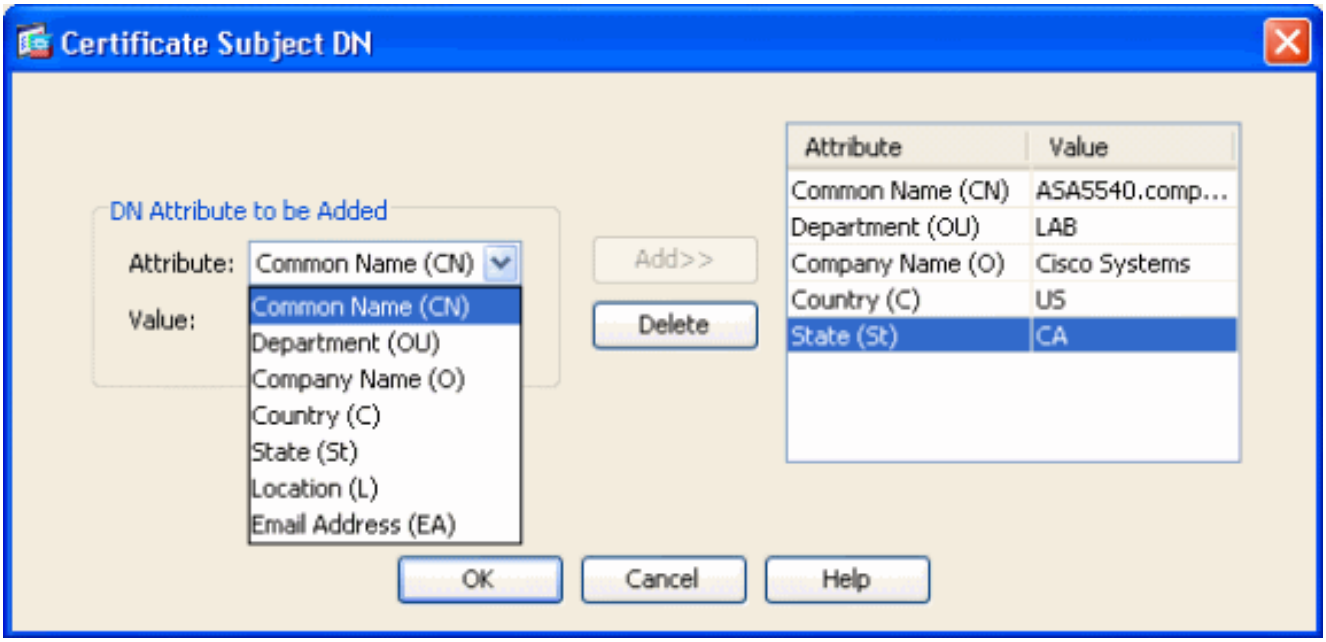
2. Selecteer onder Add Identity Certificate (identiteitsbewijs) de radioknop **Add a new Identity Certificate** en kies uw sleutelpaar in het vervolgkeuzemenu.**Opmerking:** het is niet aanbevolen om <Default-RSA-Key> te gebruiken, omdat als u de SSH-toets regenereert, u het certificaat ongeldig maakt. Als u geen RSA-toets hebt, moet u stappen a en b voltooien. Ga verder met Stap 3.**Figuur 2**



(Optioneel) Voltooi deze stappen als u nog geen RSA-toets hebt ingesteld en anders naar Stap 3 overslaat.Klik op **Nieuw...**.Voer de naam van het sleutelpaar in het veld **Nieuwe naam van het nieuwe sleutelpaar in** en klik op **Nu genereren**.**Figuur 3**



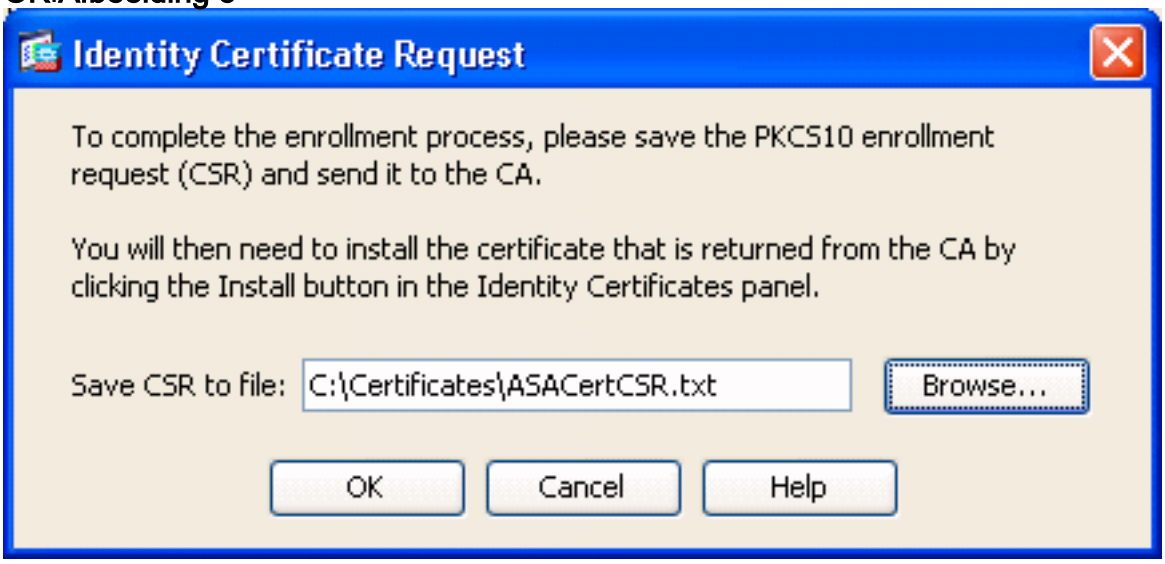
3. Klik op **Selecteren**.
4. Voer de juiste certificeringseigenschappen in zoals in afbeelding 4. Klik na voltooiing op **OK**. Klik vervolgens op **Certificaat toevoegen**.**Figuur 4**



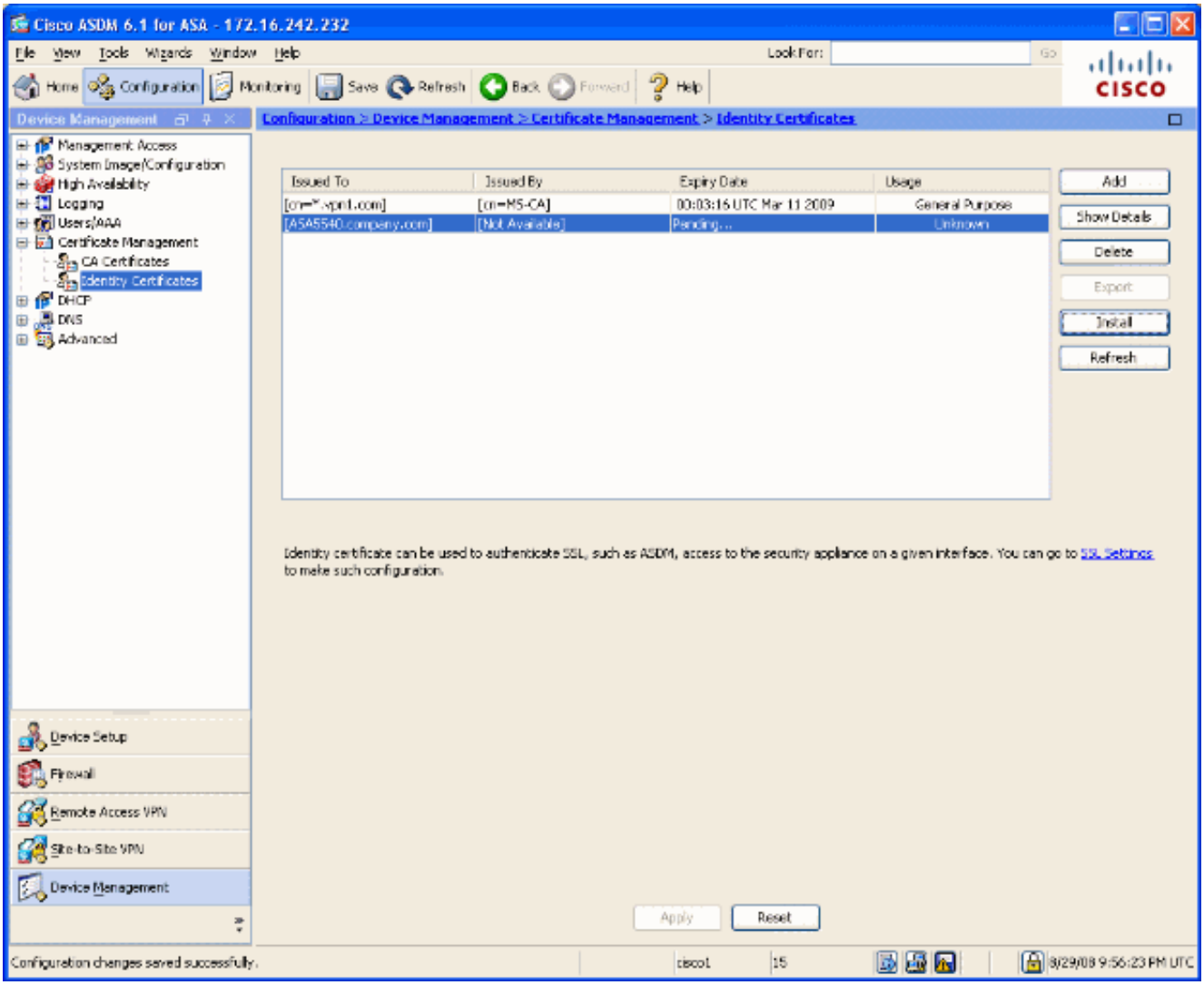
CLI-uitvoer:

```
crypto ca trustpoint ASDM_TrustPoint0
        keypair CertKey
        id-usage ssl-ipsec
        fqdn 5540-uwe
        subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA
        enrollment terminal
 crypto ca enroll ASDM_TrustPoint0
```

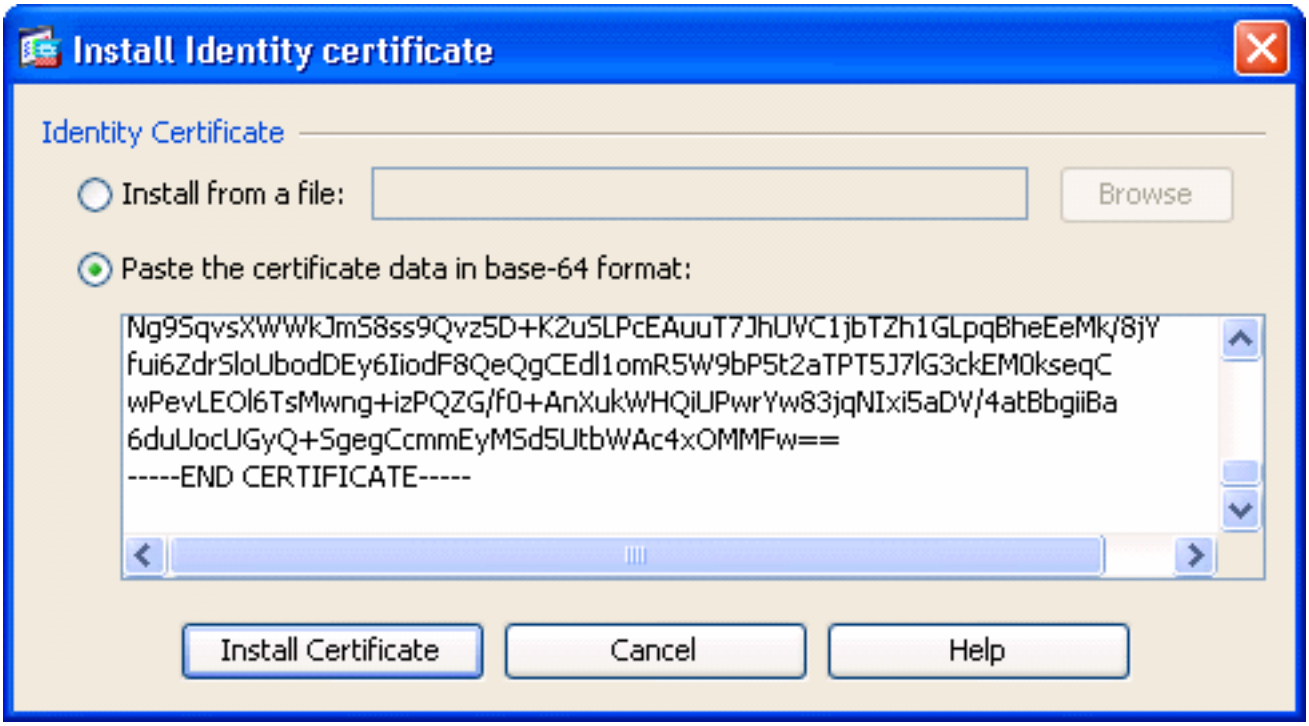
5. Sla in het dialoogvenster **Identity certificaataanvraag** op (CSR) in een tekstbestand en klik op **OK**.**Afbeelding 5**



6. (Optioneel) Controleer in ASDM of de CSR in behandeling is, zoals in afbeelding 6.**Figuur 6**



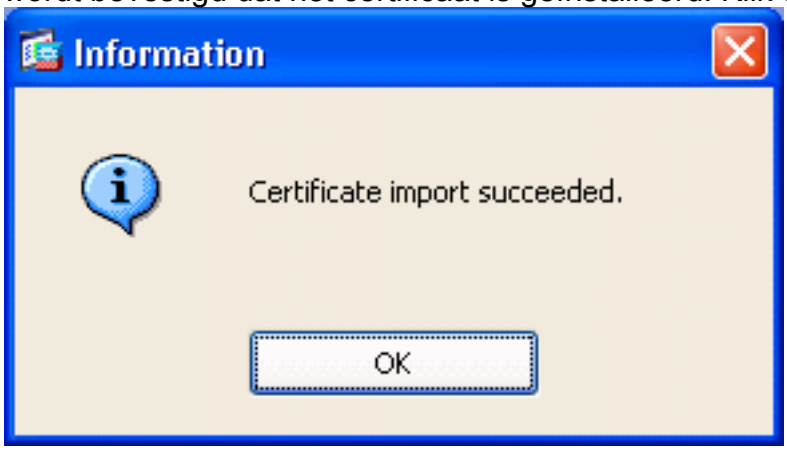
7. Dien het certificaatverzoek in bij de certificaatbeheerder, die het certificaat op de server afgeeft. Dit kan via een web interface, e-mail of rechtstreeks naar de root CA server worden verzonden voor het uitgeven van certificaten.
8. Voltooi deze stappen om het hernieuwde certificaat te installeren.Selecteer het hangende certificaatverzoek onder Configuration > Apparaatbeheer > Identity Certificaten, zoals in afbeelding 6, en klik op **Install**.Selecteer in het venster Installeer Identity Certificate de **certificaatgegevens in het** radioknop **van de** basis-64**-indeling** en klik op **Installeer**.**N.B.:** Als het certificaat ook wordt afgegeven in een .cer-bestand in plaats van in een tekstbestand of een e-mail, kunt u ook **Installeer uit een bestand** selecteren, naar het juiste bestand op uw pc bladeren, op **Installeer ID-certificaatbestand** klikken en vervolgens op **Installeer**.**Figuur 7**



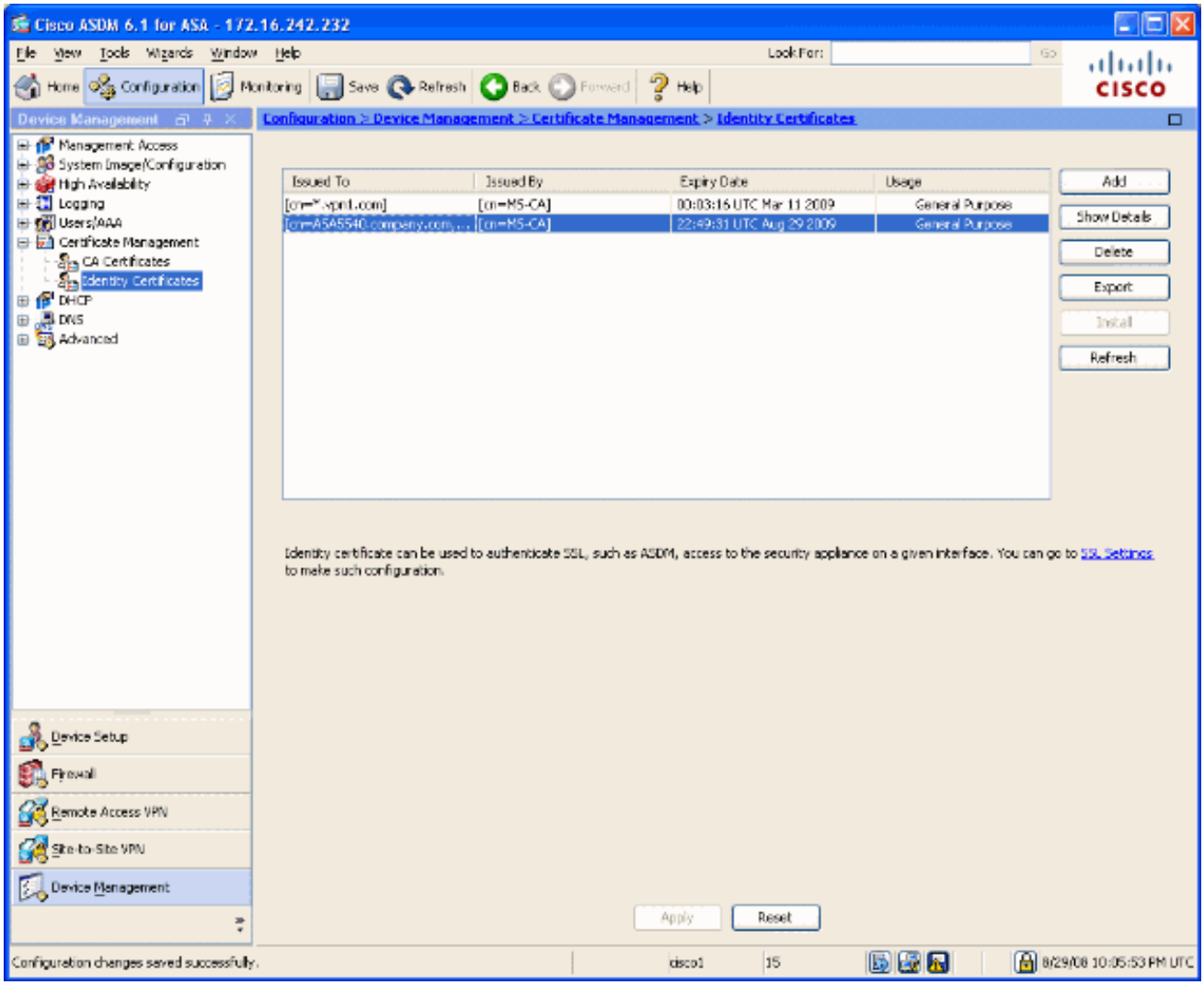
CLI-uitvoer:

```
crypto ca import ASDM_TrustPoint0 certificate
WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ
!--- output truncated wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit
```

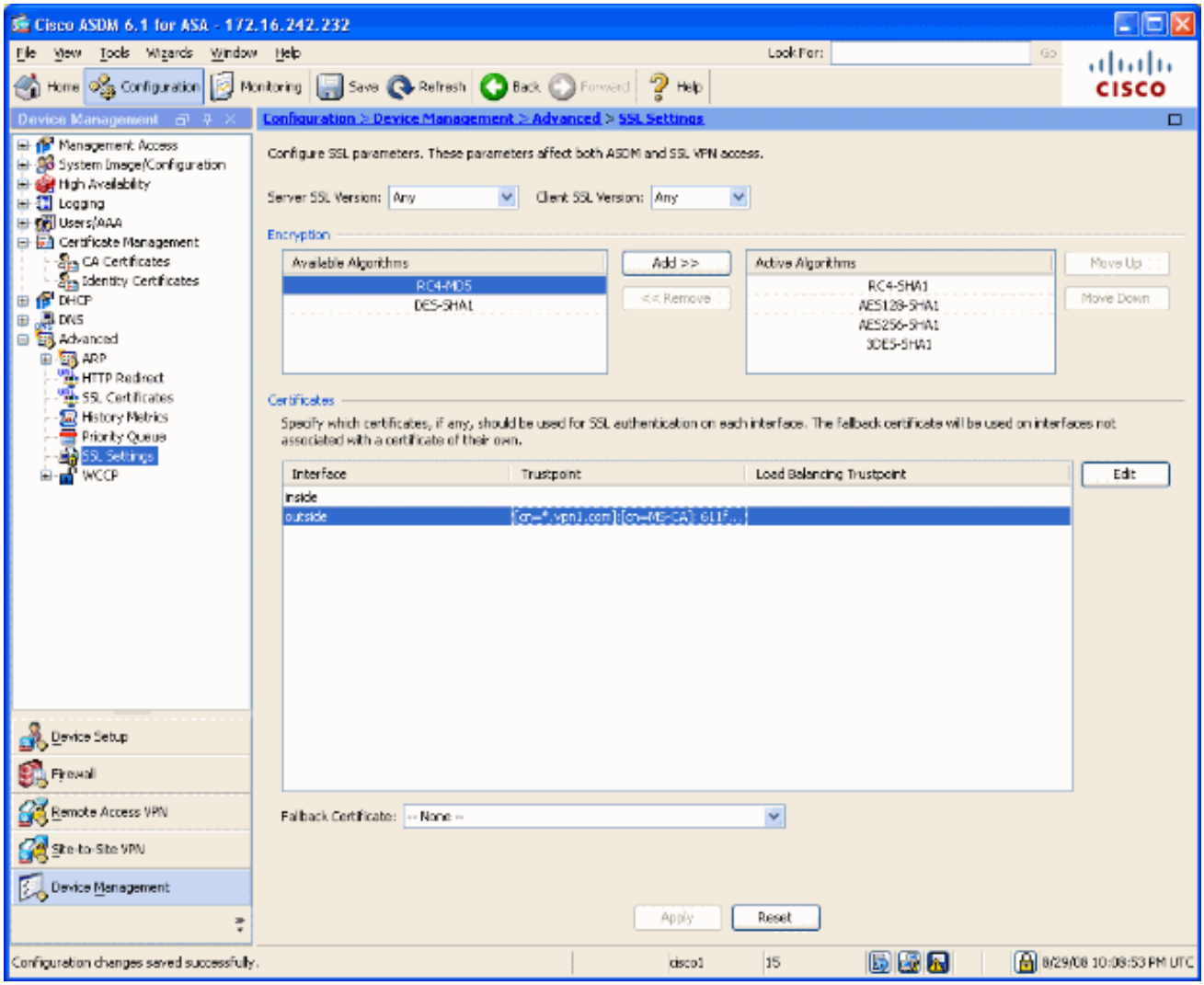
9. Het venster verschijnt waarin wordt bevestigd dat het certificaat is geïnstalleerd. Klik op "OK" om dit te bevestigen.**Figuur 8**



10. Zorg ervoor dat uw nieuwe certificaat onder Identity Services Engine verschijnt.**Afbeelding 9**



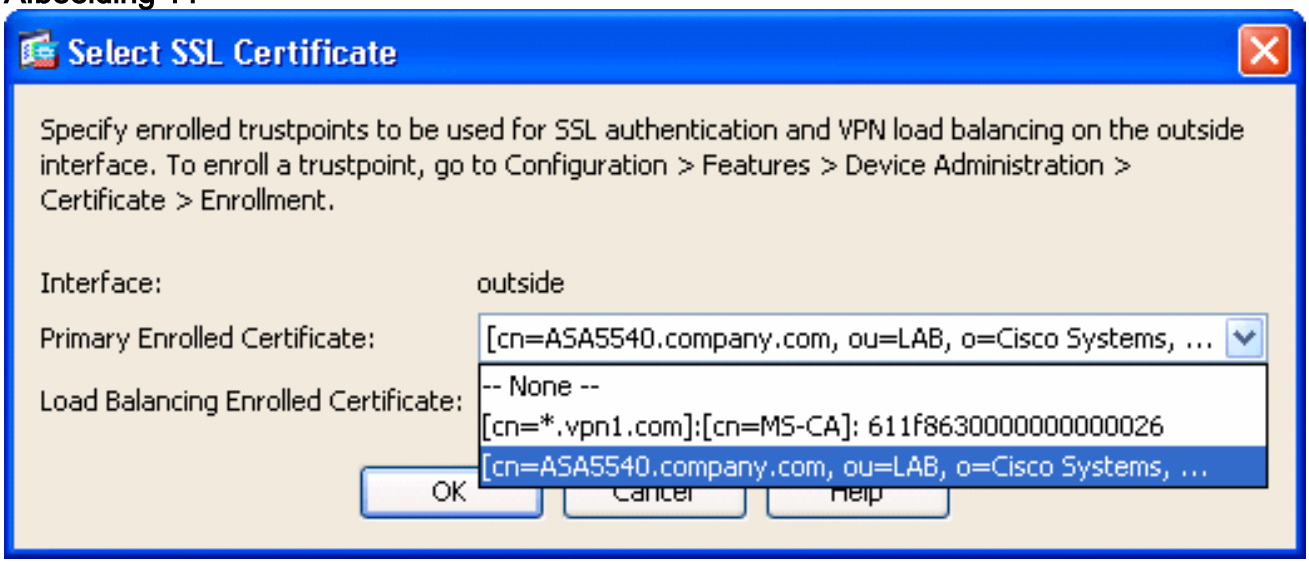
11. Voltooi deze stappen om het nieuwe certificaat aan de interface te binden:Kies **Configuratie > Apparaatbeheer > Geavanceerd > SSL-instellingen**, zoals in afbeelding 10.Selecteer uw interface onder Certificaten en klik op **Bewerken**.**Afbeelding 10**



12. Kies uw nieuwe certificaat in het vervolgkeuzemenu, klik op **OK** en klik op **Toepassen**.

```
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point ASDM_TrustPoint0 outside
```

Afbeelding 11



13. Bewaar uw configuratie in ofwel ASDM ofwel in de CLI.

Verifiëren

U kunt de CLI-interface gebruiken om te controleren of het nieuwe certificaat correct in de ASA is geïnstalleerd, zoals in deze voorbeelduitvoer wordt weergegeven:

```
ASA(config)#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 61bf707b000000000027
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Issuer Name:
    cn=MS-CA
  Subject Name:
    cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems st=CA c=US CRL
Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-
base1\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008 end date:
22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate Status:
Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage:
Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---
'old' certificate CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006
end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available
Certificate Serial Number: 611f8630000000000026 Certificate Usage: General Purpose Public Key
Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points:
[1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\CertEnroll\MS-CA.crl
Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009
Associated Trustpoints: test ASA(config)#
```

Problemen oplossen

(Optioneel) Controleer op de CLI of het juiste certificaat op de interface wordt toegepast:

```
ASA(config)#show running-config ssl
ssl trust-point ASDM_TrustPoint0 outside
!--- Shows that the correct trustpoint is tied to the outside interface that terminates SSL VPN.
ASA(config)#
```

Hoe SSL-certificaten van de ene ASA naar de andere kopiëren

Dit kan als je exportbare sleutels had gegenereerd. U moet het certificaat exporteren naar een PKCS-bestand. Dit houdt in dat alle bijbehorende sleutels moeten worden geëxporteerd.

Gebruik deze opdracht om uw certificaat via CLI te exporteren:

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

Opmerking: Wachtwoord - gebruikt om het bestand pkcs12 te beschermen.

Gebruik deze opdracht om uw certificaat te importeren via CLI:

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

N.B.: Dit wachtwoord dient hetzelfde te zijn als bij het exporteren van het bestand.

Dit kan ook via ASDM worden gedaan voor een ASA failover-paar. Volg deze stappen om dit uit te voeren:

1. Meld u aan bij de primaire ASA via ASDM en kies **Gereedschappen—> Back-upconfiguratie**.
2. U kunt back-ups maken van alles of alleen van de certificaten.
3. Open ASDM in de standby-modus en kies **Gereedschappen —> Herstel de configuratie**.

Gerelateerde informatie

- Ondersteuning van Cisco-pagina voor adaptieve security applicatie (ASA)
- ASA 8.x Installeer Verkrakers van 3 partijen handmatig voor gebruik met WebVPN-configuratievoorbeeld
- Technische ondersteuning en documentatie – Cisco Systems