Certificaatinschrijving configureren met ACME-protocol inzake beveiligde firewall

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten
- Vereisten en beperkingen
- Overwegingen over downgrade

Achtergrondinformatie

Configureren

- Configuratie van vereisten
- ACME-inschrijving met ASDM
- ACME-inschrijving met Secure Firewall ASA CLI

Verifiëren

- Geïnstalleerd certificaat bekijken in ASA
- Syslog-evenementen

Problemen oplossen

- Opdrachten voor probleemoplossing
- Foutcode
- Reden
- Mogelijke oorzaak of oplossing

Gerelateerde informatie

Inleiding

Dit document beschrijft het proces om een TLS-certificaat (Transport Layer Security) in te schrijven met behulp van het protocol (Automated Certificate Management Environment) voor beveiligde firewall ASA.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall adaptieve security applicatie (ASA)
- Public Key Infrastructure (PKI)

Gebruikte componenten

- Cisco ASA versie 9.23.1.1
- Cisco ASDM versie 7.23(1).
- CA-server (Certificate Authority) die het ACME-protocol ondersteunt.

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.

Vereisten en beperkingen

De huidige vereisten en beperkingen voor ACME-inschrijving op Secure Firewall ASA zijn:

- Ondersteuning voor ASA versie 9.23.1 en ASDM 7.23.1 vanaf
- Niet ondersteund in meerdere context
- ACME ondersteunt het maken van wildcard certificaten niet. Elk certificaatverzoek moet een exacte domeinnaam vermelden.
- Elk trustpoint dat via ACME is ingeschreven, is beperkt tot één interface, wat betekent dat certificaten die met ACME zijn ingeschreven, niet over meerdere interfaces kunnen worden gedeeld.
- Keypairs worden automatisch gegenereerd en kunnen niet worden gedeeld voor certificaten die zijn ingeschreven via ACME. Elk certificaat gebruikt een uniek sleutelpaar, wat de beveiliging verbetert maar het hergebruik van sleutels beperkt.

Overwegingen over downgrade

Tijdens downgrading naar een versie die geen ACME-inschrijving ondersteunt op Secure Firewall ASA (9.22 en ouder):

- Alle aan ACME gerelateerde trustpoint configuraties die nieuw zijn op 9.23.x of nieuwer gaan verloren
- Alle certificaten die via ACME zijn ingeschreven, blijven toegankelijk, maar de privésleutel wordt losgekoppeld na de eerste opslag en herstart na de downgrade

Als een downgrade is vereist, voert u de volgende aanbevolen tijdelijke procedure uit:

1. Zorg ervoor dat u de ACME-certificaten in PKCS12-formaat exporteert voordat u ze degradeert.
2. Alvorens te degraderen, zorg ervoor om de configuratie van ACME te verwijderen trustpoint.
3. Voer na de downgrade het PKCS12-certificaat in. Het resulterende vertrouwenspunt blijft geldig tot het certificaat dat via ACME is afgegeven, verloopt.

Achtergrondinformatie

Het ACME-protocol is ontworpen om het beheer van TLS-certificaten voor netwerkbeheerders te stroomlijnen. Door gebruik te maken van ACME, kunnen beheerders de processen automatiseren die betrokken zijn bij het verkrijgen en verlengen van TLS-certificaten. Deze automatisering is met name nuttig bij het gebruik van certificaatautoriteiten (CA's) zoals Let's Encrypt, die gratis, geautomatiseerde en open certificaten aanbieden met behulp van het ACME-protocol.

ACME ondersteunt de afgifte van Domain Validation (DV)-certificaten. Deze certificaten zijn een type digitaal certificaat dat de controle van de certificaathouder over gespecificeerde domeinen bevestigt. Het validatieproces voor DV-certificaten wordt doorgaans uitgevoerd via een op HTTP gebaseerd provocatiemechanisme. In dit mechanisme plaatst de aanvrager een specifiek bestand op zijn webserver, dat door de certificaatautoriteit (CA) wordt geverifieerd door toegang tot het bestand te krijgen via de HTTP-server van het domein. Door deze uitdaging met succes af te ronden, toont de CA aan dat de aanvrager zeggenschap heeft over het domein, waardoor de afgifte van het DV-certificaat mogelijk wordt.

Het proces om de inschrijving te verwezenlijken is het volgende:

1. Certificaataanvraag initiëren: De client vraagt een certificaat aan bij de ACME-server en specificeert de domeinen waarvoor het certificaat is vereist.
2. Ontvang HTTP-01-uitdaging: De ACME-server biedt een HTTP-01-uitdaging met een uniek token die de client kan gebruiken om de domeincontrole te bewijzen.
3. Bereid de reactie op de uitdaging voor:
    - De client maakt een sleutelautorisatie door het token van de ACME-server te combineren met de accountsleutel.
    - De client stelt zijn webserver in om deze sleutelautorisatie op een specifiek URL-pad te ondersteunen.
4. Uitdaging voor ACME-server: De ACME server doet een HTTP GET verzoek aan de gespecificeerde URL om de sleutel autorisatie op te halen.
5. ACME Server verifieert eigendom: De server controleert of de opgehaalde sleutelautorisatie overeenkomt met de verwachte waarde om de controle van de client over het domein te bevestigen.
6. Certificaat van afgifte: Na een succesvolle validatie geeft de ACME-server het SSL/TLS-certificaat af aan de client.

ACME-inschrijving voor HTTP-1001-verificatie - Flow

De meest relevante voordelen van het gebruik van het ACME-protocol om TLS-certificaten in te schrijven zijn:

- ACME vergemakkelijkt de aankoop en het onderhoud van TLS-domeincertificaten voor de Secure Firewall ASA TLS-interfaces. Deze automatisering vermindert handmatige taken aanzienlijk en helpt certificaten actueel te houden zonder constant toezicht.
- Met ACME-enabled trustpoints, vernieuwen certificaten automatisch wanneer ze bijna verlopen. Dit vermogen vermindert de noodzaak voor administratieve betrokkenheid, het verzekeren van ononderbroken veiligheid en het voorkomen van onverwachte certificaatafloop.

Configureren

Configuratie van vereisten

Zorg ervoor dat aan de volgende voorwaarden is voldaan voordat het ACME-inschrijvingsproces wordt gestart:

1. Oplosbare domeinnaam: De domeinnaam waarvoor u een certificaat aanvraagt, moet kunnen worden opgelost door de ACME-server. Dit zorgt ervoor dat de server domeineigendom kan verifiëren.
2. Secure Firewall-toegang tot ACME Server: De Secure Firewall moet de mogelijkheid hebben om de ACME-server via een van zijn interfaces te benaderen. Deze toegang hoeft niet via de interface te zijn waarvoor het certificaat wordt aangevraagd.

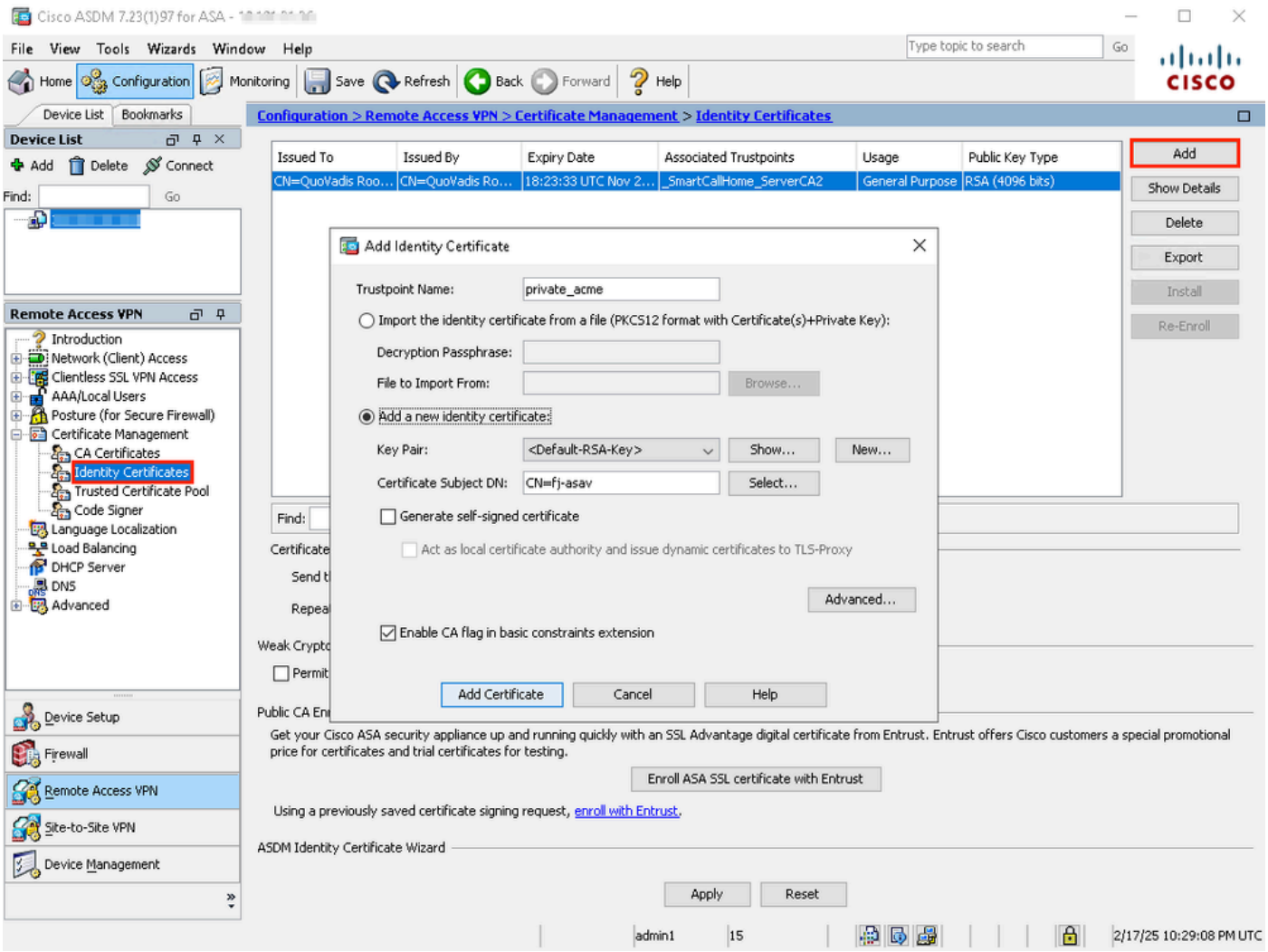
3. TCP-poort 80 beschikbaarheid: Sta TCP poort 80 toe van de ACME CA server naar de interface die correspondeert met de domeinnaam. Dit is vereist tijdens het ACME-uitwisselingsproces om de HTTP-01-uitdaging te voltooien.

Opmerking: In de periode waarin poort 80 open is, zijn alleen de ACME-provocatiegegevens toegankelijk.

ACME-inschrijving met ASDM

1. Voeg een nieuw identiteitsbewijs toe.

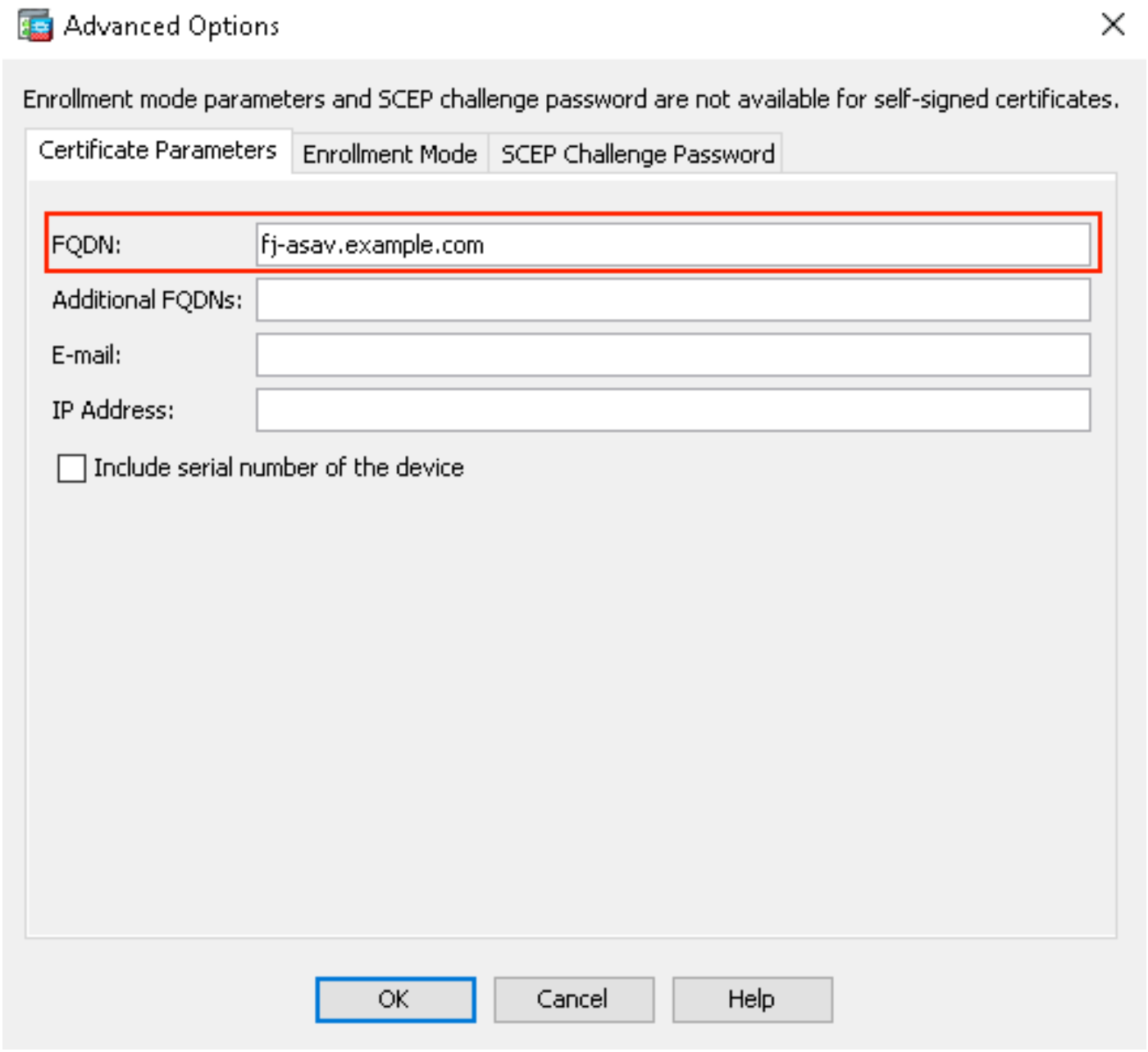
- Navigeer naar Configuration > Remote Access VPN > Certificaatbeheer > Identity Certificates.
- Klik op de knop Toevoegen en selecteer Een nieuw identiteitsbewijs toevoegen.



ASDM-identiteitscertificaat voor ACME-inschrijving.

2. Specificeer de FQDN voor het identificatiecertificaat.

- Klik op de knop Advanced.
- Specificeer onder het tabblad Certificaatparameters de FQDN die het certificaat moet hebben.

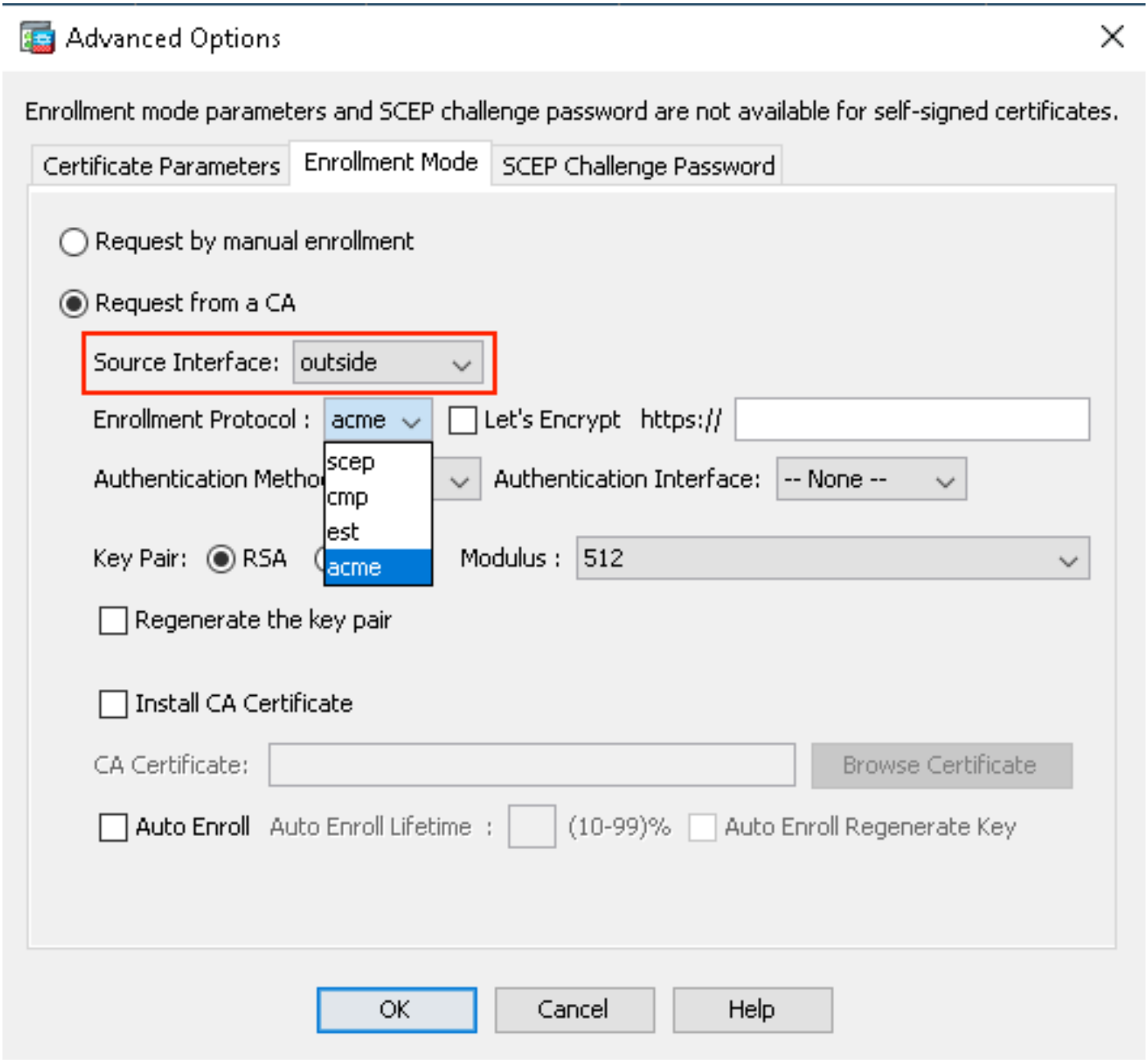


ACME-inschrijving voor ASDM FQDN.

3. Selecteer ACME als inschrijvingsprotocol.

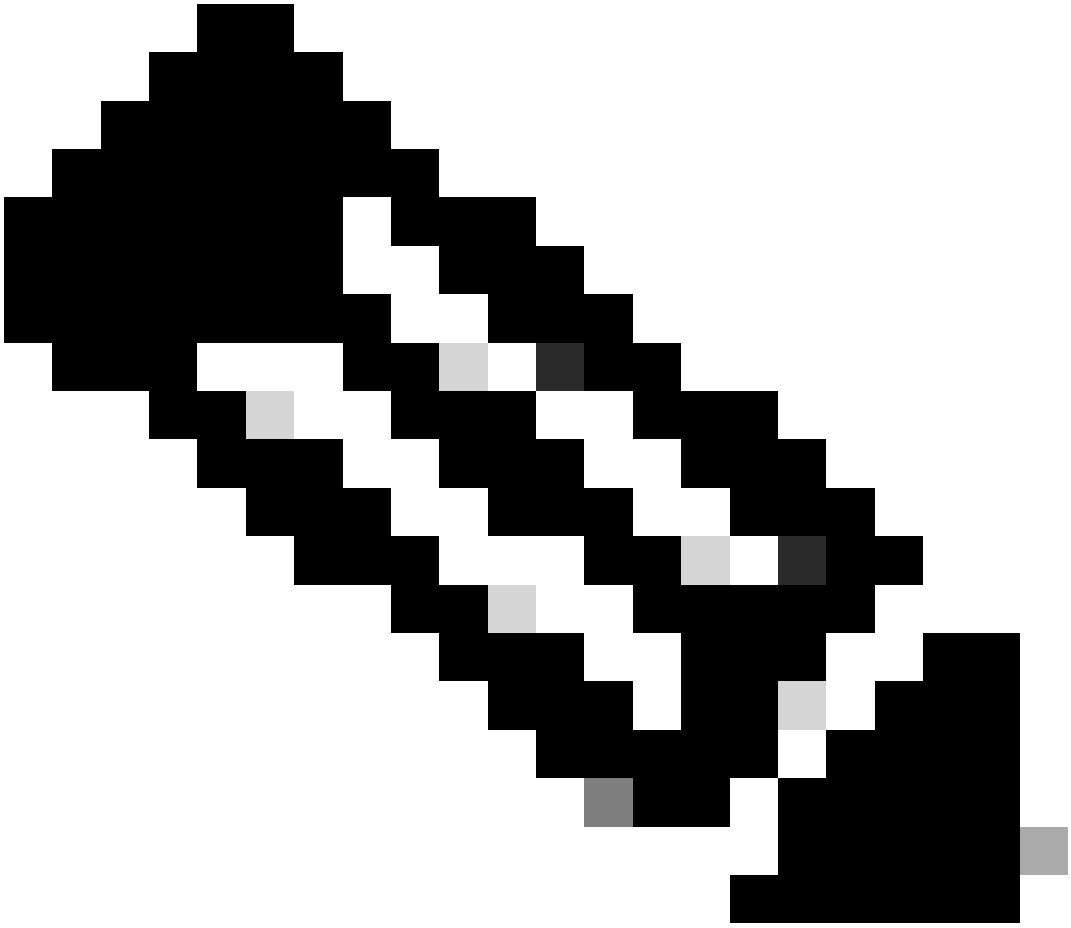
- Selecteer onder het tabblad Inschrijfmodus de optie Aanvragen bij CA-optie.

- Specificeer de broninterface en selecteer Cam als inschrijvingsprotocol.

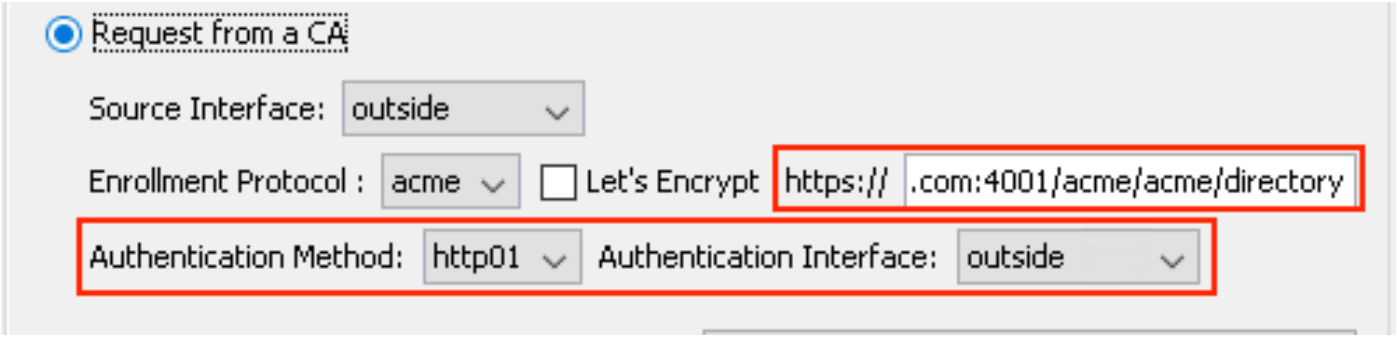


ACME-inschrijvingsprotocol voor ASDM Nacme. keuze

4. Selecteer Let's Encrypt for your certificate to be signed by Let's Encrypt public CA. Anders specificeert u de URL van uw interne CA die het ACME-inschrijvingsprotocol ondersteunt. Specificeer bovendien de verificatieinterface.



Opmerking: Wanneer het selectievakje Let's Encrypt is ingeschakeld, wordt de server-URL automatisch ingevuld.



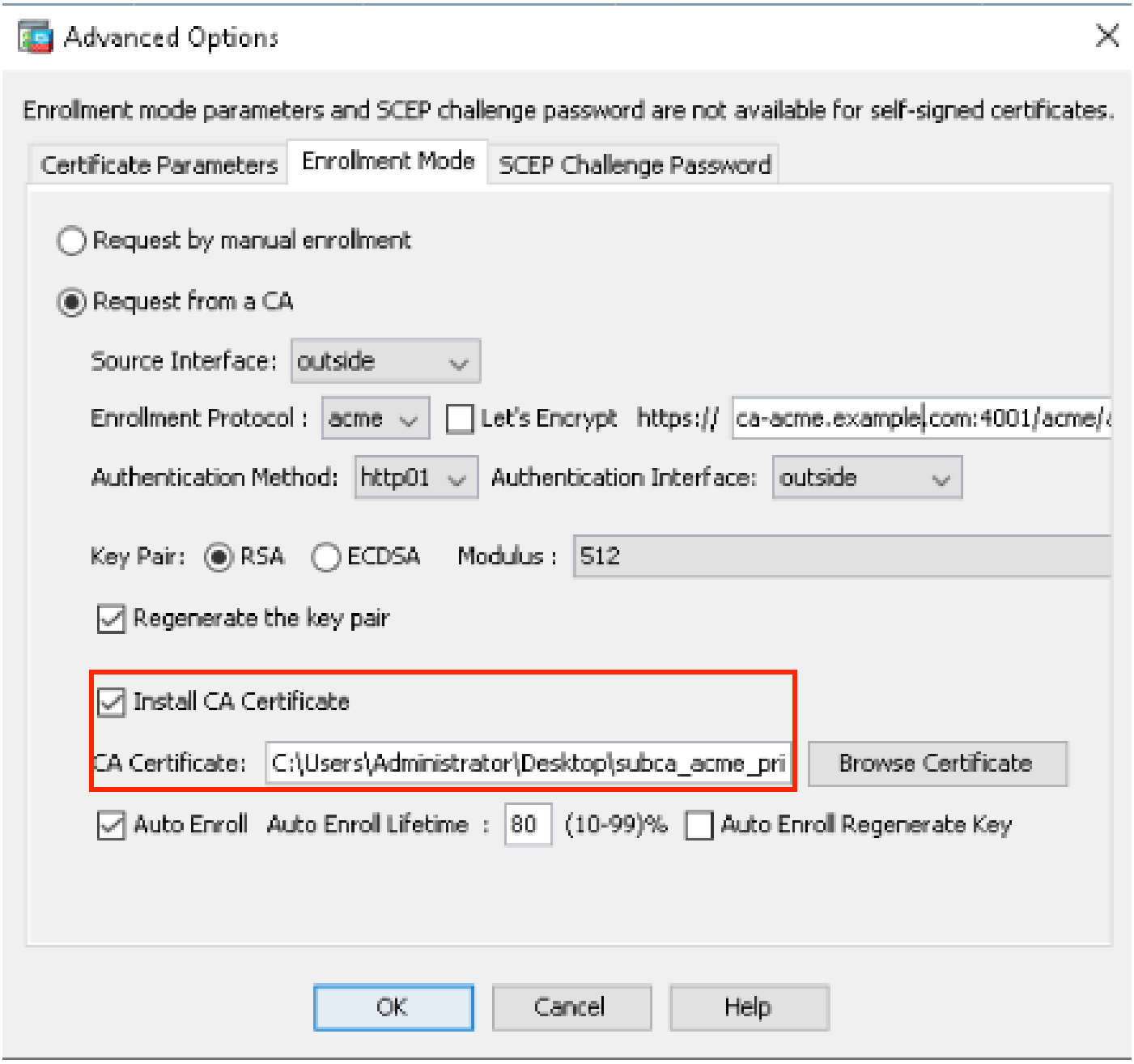
ASDM-verificatiemethode voor ACME-inschrijving.

5. Installeer het CA-certificaat.

Als de optie CA-certificaat installeren is ingeschakeld, moet u het certificaat uploaden van de directe CA die uw certificaat afgeeft.

Opmerking: Als het CA-certificaat al bestaat op de Secure Firewall, hetzij van een vorige installatie of binnen de trustpool, is het niet nodig deze optie te controleren. Schakel het selectievakje CA-certificaat installeren niet in.

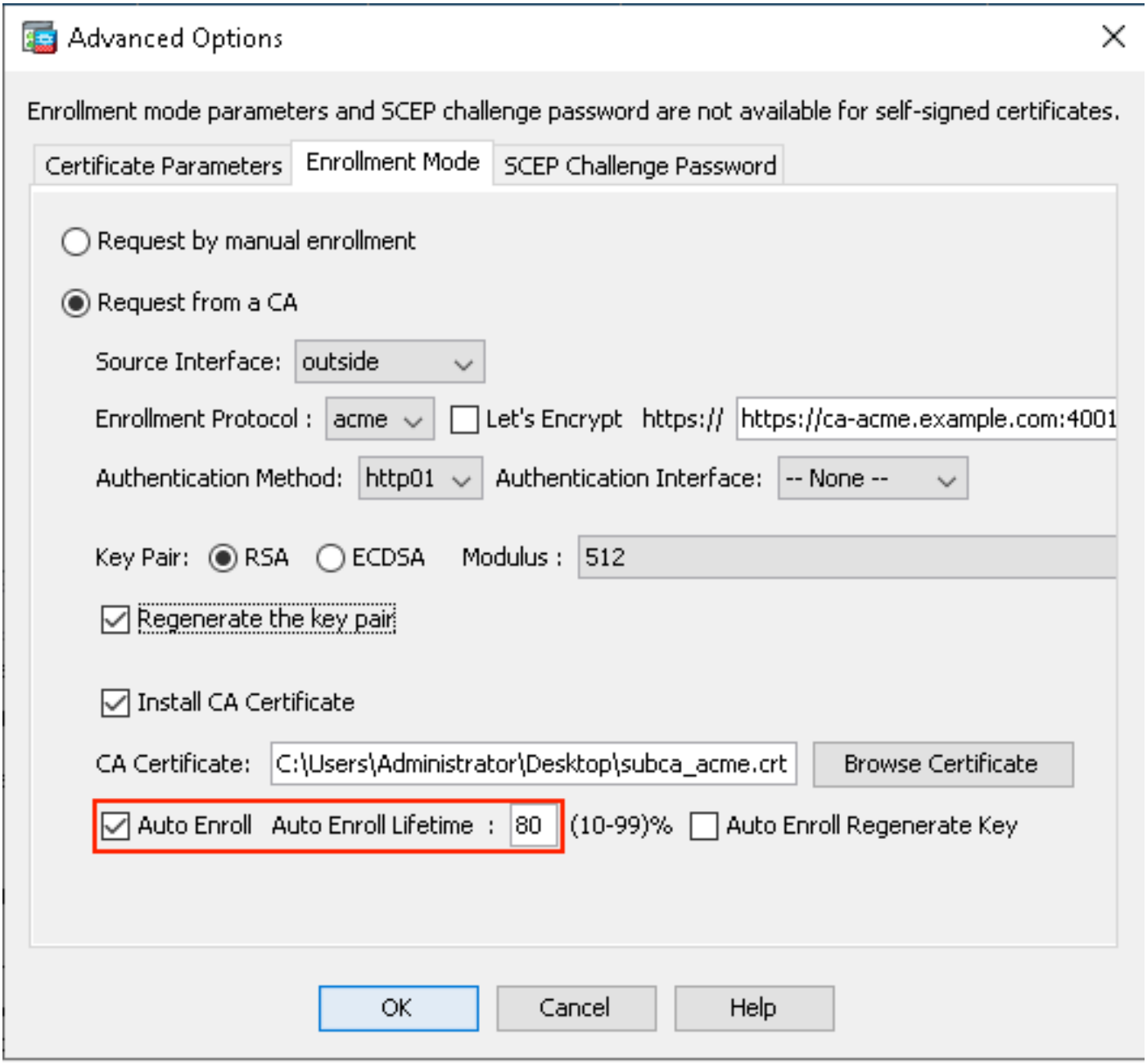
Opmerking: Wanneer u de optie Let's Encrypt selecteert, laat het aanvinkvakje Install CA Certificate onaangevinkt, aangezien de basiscertificaten van CA voor Let's Encrypt al zijn opgenomen in de Secure Firewall trustpool.



6. (Optioneel) Auto Enroll inschakelen voor het identiteitscertificaat.

Schakel het aanvinkvakje Auto Enroll in en specificeer het percentage voor de levensduur van de Auto Enroll.

Deze eigenschap zorgt ervoor dat het certificaat automatisch wordt verlengd alvorens het verloopt. Het percentage bepaalt hoe lang vóór het verstrijken van het certificaat het vernieuwingsproces begint. Als dit bijvoorbeeld is ingesteld op 80%, start het vernieuwingsproces als het certificaat 80% van de geldigheidsperiode heeft bereikt.



ACME-inschrijving voor ASDM Auto Enroll.

7. Klik op OK en sla de configuratie op.

ACME-inschrijving met Secure Firewall ASA CLI

1. Maak een nieuw Trustpoint.

Maak een trustpoint en specificeer de naam van het inschrijvingsprotocol.

<#root>

```
asav(config)# crypto ca trustpoint private_acme
asav(config-ca-trustpoint)# enrollment protocol ?

crypto-ca-trustpoint mode commands/options:

acme Automatic Certificate Management Environment

  cmp Certificate Management Protocol Version 2
  est Enrollment over Secure Transport
  scep Simple Certificate Enrollment Protocol
```

2. Selecteer de HTTP-01 methode voor verificatie om de domeincontrole te verifiëren.

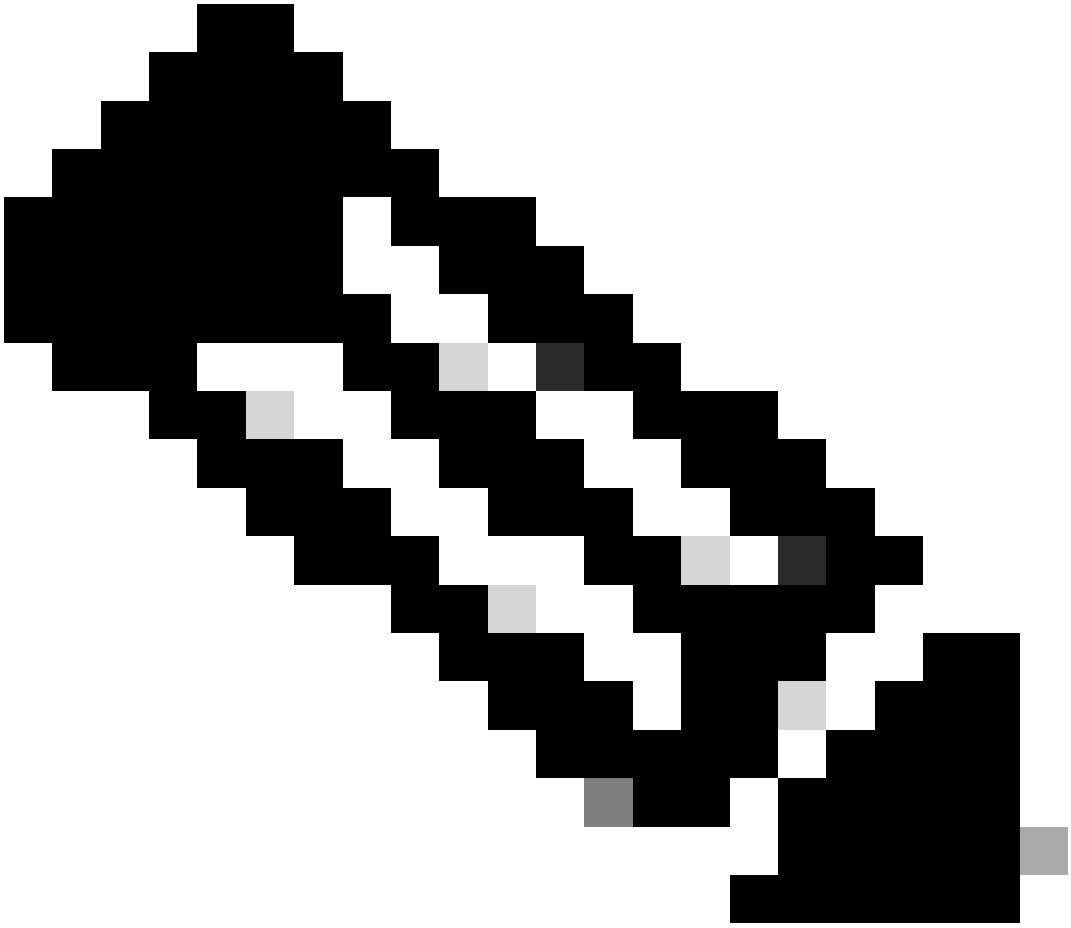
```
asav(config-ca-trustpoint)# enrollment protocol acme authentication ?

crypto-ca-trustpoint mode commands/options:
http01 Use the HTTP-01 method, which opens port 80 on the specified
interface
```

3. Selecteer Let's Encrypt als ACME CA. Als u een andere CA gebruikt die ACME-protocol ondersteunt, dient u de juiste URL in te vullen.

```
asav(config-ca-trustpoint)# enrollment protocol acme url ?

crypto-ca-trustpoint mode commands/options:
LINE < 477 char URL
LetsEncrypt Use the Let's Encrypt CA
```



Opmerking: Wanneer LetEncrypt-trefwoord is geconfigureerd, is de URL van de Let's Encrypt server automatisch ingevuld.

4. Definieer het RSA-sleutelpaar, de volledig gekwalificeerde domeinnaam (FQDN) en de onderwerpnaam voor het certificaat.

```
crypto ca trustpoint private_acme
 enrollment interface outside
 enrollment protocol acme authentication http01 outside
 enrollment protocol acme url https://ca-acme.example.com:4001/acme/acme/directory
 fqdn fj-asav.cisco.com
 subject-name CN=fj-asav.example.com
 keypair rsa modulus 4096
 auto-enroll 80 regenerate
 crl configure
```

5. Verifieer het trustpoint.

> Opmerking: Als de CA al bestaat op de beveiligde firewall of bij het gebruik van Let's Encrypt, kan deze stap worden overgeslagen.

```
asav(config)# crypto ca authenticate private_acme
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIBwzCCAWqgAwIBAgIQedxaTDOJ1G6tLgAGti6tizAKBggqhkjOPQQDAjAsMRAw
DgYDVQQKEwdjYS1hY21lMRgwFgYDVQQDEw9jYS1hY21lIFJvb3QgQOEwHhcNMjQx
[truncated]
ADBEAiB7S4YZfnOK82K2yz5F5CzMe2t98LCpLRzoPJXMo7um1AIgH+K8EZMLstLN
AJQoplycJENo5D7kUmVrwUBBjREqv9I=
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: 40000000 40000000 40000000 40000000
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

6. Schrijf het certificaat in.

```
asav(config)# crypto ca enroll private_acme
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=fj-asav.cisco.com

% The fully-qualified domain name in the certificate will be: fj-asav.example.com

% Include the device serial number in the subject name? [yes/no]: no

Request certificate from CA? [yes/no]: yes
```

Verifiëren

Geïnstalleerd certificaat bekijken in ASA

Bevestig dat het certificaat is ingeschreven en controleer de vernieuwingsdatum.

```
asav# show crypto ca certificates private_acme
```

```
CA Certificate
Status: Available
Certificate Serial Number: 79d000000000000000000008b
Certificate Usage: General Purpose
Public Key Type: ECDSA (256 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Root CA
O=ca-acme
Subject Name:
CN=ca-acme Intermediate CA
O=ca-acme
Validity Date:
start date: 23:20:19 UTC Nov 26 2024
end date: 23:20:19 UTC Nov 24 2034
Storage: config
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: 8c8200000000000000000000000000000000000077
SHA1 PublicKeyInfo hash: 974c0000000000000000000000000000000009e1

Certificate
Status: Available
Certificate Serial Number: 666000000000000000000000000000be
Certificate Usage: General Purpose
Public Key Type: RSA (4096 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Intermediate CA
O=ca-acme
Subject Name:
CN=fj-asav.example.com
Validity Date:
start date: 20:51:00 UTC Feb 14 2025
end date: 20:52:00 UTC Feb 15 2025
renew date: 16:03:48 UTC Feb 15 2025
Storage: immediate
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: e6e000000000000000000000000000000000089a
SHA1 PublicKeyInfo hash: 5e300000000000000000000000000000000009f
```

Syslog-evenementen

Er zijn nieuwe systemen in de Secure Firewall om gebeurtenissen met betrekking tot de certificaatinschrijving op te nemen met behulp van het ACME-protocol:

- 717067: Hier vindt u informatie over het moment waarop de inschrijving van het ACME-certificaat begint

```
%ASA-5-717067: Starting ACME certificate enrollment for the trustpoint <private_acme> with CA <ca-acme.
```

- 717068: Hier vindt u informatie over wanneer de inschrijving van een ACME-certificaat is geslaagd

```
%ASA-5-717068: ACME Certificate enrollment succeeded for trustpoint <private_acme> with CA <ca-acme.exa
```

- 717069: Hier vindt u informatie over wanneer ACME-inschrijving mislukt

```
%ASA-3-717069: ACME Certificate enrollment failed for trustpoint <private_acme>
```

- 717070: Biedt informatie over het sleutelpaar voor certificaatinschrijving of certificaatverlenging

```
%ASA-5-717070: Keypair <Auto.private_acme> in the trustpoint <private_acme> is regenerated for <manual>
```

Problemen oplossen

Als een ACME-certificaatinschrijving mislukt, overweegt u de volgende stappen om het probleem te identificeren en op te lossen:

- Controleer de verbinding met de server: Bevestig dat de Secure Firewall netwerkverbinding met de ACME-server heeft. Controleer of er geen netwerkproblemen of firewallregels zijn die de communicatie blokkeren.
- Zorg ervoor dat de Secure Firewall Domain Name kan worden opgelost: Controleer of de domeinnaam die in de Secure Firewall is ingesteld, kan worden opgelost door de ACME-server. Deze verificatie is cruciaal voor de server om het verzoek te valideren.
- Domeineigendom bevestigen: Controleer of alle domeinnamen die in het trustpoint zijn opgegeven, eigendom zijn van de Secure Firewall. Dit zorgt ervoor dat de ACME-server domeineigendom kan valideren.

Opdrachten voor probleemoplossing

Verzamel de uitvoer van de volgende debug-opdrachten voor aanvullende informatie:

- debug crypto ca.com <1-25>
- debug crypto ca <1-14>

Vaak voorkomende ACME-inschrijvingsfouten:

Foutcode	Reden	Mogelijke oorzaak of oplossing
7	Kan geen verbinding maken met de server	Server is bereikbaar, maar ACME-service is niet actief.
28	Kan geen verbinding maken met de server	Server is niet bereikbaar. Controleer de basisnetwerktoegang tot de ACME-server.
60	Kan servercertificaat niet valideren	Zorg ervoor dat root of emittent CA aanwezig is in een trustpoint of in de trustpool.
124	ACME-verwerkingstijd	Zorg ervoor dat alle gevraagde FQDN's zijn opgelost in de interface die is geconfigureerd voor HTTP-01-verificatie. Controleer of de geconfigureerde ACME URL juist is.

Gerelateerde informatie

Voor extra hulp kunt u contact opnemen met TAC. Een geldig ondersteuningscontract is vereist: Cisco's wereldwijde contactgegevens voor ondersteuning.
U kunt hier ook de Cisco VPN-community bezoeken.

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.