Certificaatinschrijving configureren met het ACME-protocol voor veilige firewallbeveiliging, beheerd door FMC

Inleiding

In dit document wordt het proces beschreven voor het inschrijven van een TLS-certificaat (Transport Layer Security) via het ACME-protocol (Automated Certificate Management Environment) op het FTD-platform (Secure Firewall Firepower Threat Defense).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over deze onderwerpen:

- Handmatige processen voor het registreren van certificaten en de basisprincipes van Secure Sockets Layer (SSL).
- Basisconcepten voor verificatie voor VPN's met externe toegang.
- Ervaring met certificaatautoriteiten (CA's).

Gebruikte componenten

- Cisco FTDv versie 10.0.0-35.
- Cisco FMC versie 10.0.0-35.
- 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 FTD voor Secure Firewall omvatten:

- Ondersteund op FTD en FMC versies 10.0.0 en hoger.
- ACME staat de uitgifte van wildcard certificaten niet toe; elk certificaatverzoek moet een precieze domeinnaam vermelden.
- Elk trustpoint dat via ACME is geregistreerd, is beperkt tot één interface, zodat certificaten die via ACME zijn verkregen, niet over meerdere interfaces kunnen worden gedeeld.
- Sleutelparen worden automatisch gegenereerd en zijn uniek voor elk certificaat dat via ACME is geregistreerd, waardoor hergebruik van sleutels wordt voorkomen en de beveiliging wordt verbeterd.

Overwegingen voor downgraden

Bij het downgraden naar een Secure Firewall FTD-versie die geen ACME-inschrijving ondersteunt (versie 7.7 of eerder):

- Alle ACME-gerelateerde trustpoint-configuraties die in versie 10.0.0 of hoger zijn geïntroduceerd, gaan verloren.
- Certificaten die zijn ingeschreven via ACME zijn nog steeds toegankelijk; hun privésleutels worden echter ontkoppeld na de eerste opslag en herstart na de downgrade.

Als een downgrade nodig is, gebruikt u de aanbevolen tijdelijke oplossing:

- Voor het downgraden exporteert u de ACME-certificaten in PKCS12-formaat.
- Verwijder voordat u de upgrade uitvoert de ACME-trustpointconfiguratie.
- Na het downgraden importeert u het PKCS12-certificaat. Het geïmporteerde trustpoint blijft geldig totdat het door de ACME afgegeven certificaat verloopt.

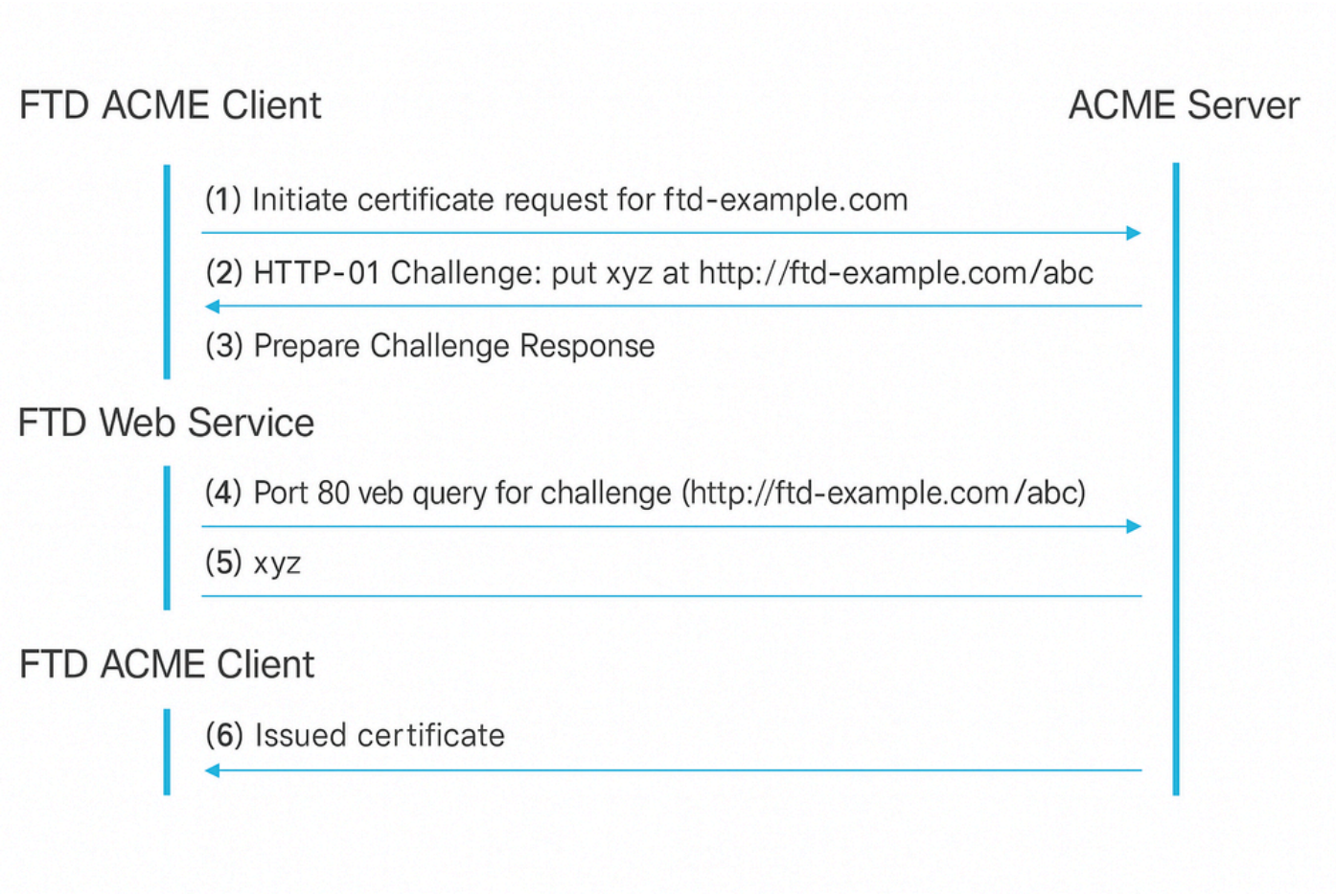
Achtergrondinformatie

Het ACME-protocol is bedoeld om het beheer van TLS-certificaten voor netwerkbeheerders te vereenvoudigen. Via ACME kunnen beheerders de taken automatiseren die gepaard gaan met het verkrijgen en vernieuwen van TLS-certificaten. Deze automatisering is vooral handig bij het werken met certificaatautoriteiten (CA's) zoals Let's Encrypt, die gratis, geautomatiseerde en openbaar toegankelijke certificaten bieden via het ACME-protocol. Deze certificaten controleren of de certificaataanvrager controle heeft over de opgegeven domeinen. De validatie vindt meestal plaats via een op HTTP gebaseerd uitdagingsproces, waarbij de aanvrager een toegewezen bestand op zijn webserver plaatst. De Certificate Authority (CA) opent vervolgens dit bestand via de HTTP-server van het domein om de domeincontrole te bevestigen. Door deze uitdaging met

succes aan te gaan, kan de CA het DV-certificaat afgeven.

Het inschrijvingsproces omvat deze stappen:

1. Certificaataanvraag initiëren: de client dient een certificaataanvraag in bij de ACME-server, met vermelding van het (de) domein(en) waarvoor het certificaat nodig is.
2. Ontvang HTTP-01 Challenge: De ACME-server reageert met een HTTP-01-uitdaging met een uniek token dat de client moet gebruiken om het eigendom van het domein te bewijzen.
3. Uitdagingsreactie voorbereiden:
    1. De client genereert een sleutelautorisatie door het token van de ACME-server te combineren met zijn accountsleutel.
    2. De client configureert zijn webserver om deze sleutelautorisatie op een specifiek URL-pad te kunnen uitvoeren.
4. ACME Server Retrieves Challenge: De ACME-server voert een HTTP GET-verzoek uit naar de opgegeven URL om de sleutelautorisatie te verkrijgen.
5. ACME Server Verifieert Eigendom: De server vergelijkt de opgehaalde sleutelautorisatie met de verwachte waarde om de controle van de client over het domein te verifiëren.
6. Uitgiftecertificaat: na succesvolle validatie geeft de ACME-server het SSL/TLS-certificaat af aan de client.



ACME Enrollment HTTP-01 Authentication Flow.

De belangrijkste voordelen van het gebruik van het ACME-protocol voor het inschrijven van TLS-certificaten op Secure Firewall FTD zijn:

- Automatisering van certificaatbeheer: ACME stroomlijnt het proces van het verkrijgen en onderhouden van TLS-domeincertificaten voor Secure Firewall FTD TLS-interfaces, waardoor handmatige administratieve taken aanzienlijk worden verminderd.
- Automatische verlenging van certificaten: met ACME-enabled trustpoints worden certificaten automatisch verlengd wanneer ze verlopen, waardoor de noodzaak voor voortdurende administratieve interventie wordt geminimaliseerd.
- Continuous Security Assurance: deze automatisering zorgt ervoor dat certificaten ononderbroken geldig blijven, voorkomt onverwachte verlopen van certificaten en zorgt voor veilige communicatie.

Deze voordelen verbeteren gezamenlijk de operationele efficiëntie en beveiliging voor FTD-implementaties van Secure Firewall.

Configureren

Configuratie van voorwaarden

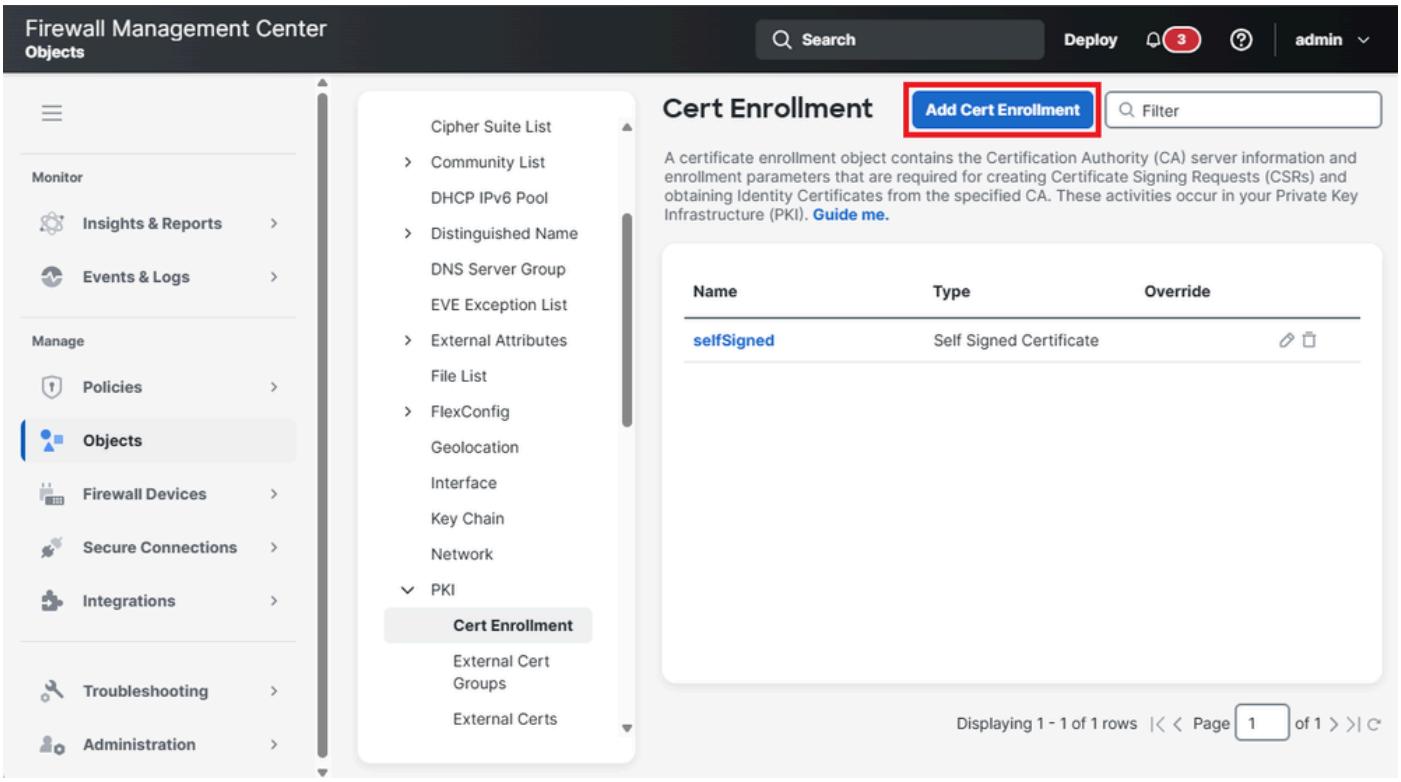
Voordat u het ACME-inschrijvingsproces start, moet u ervoor zorgen dat aan de volgende voorwaarden wordt voldaan:

1. Oplosbare domeinnaam: de domeinnaam waarvoor u een certificaat aanvraagt, moet door de ACME-server kunnen worden opgelost. Dit zorgt ervoor dat de server het eigendom van het domein kan verifiëren.
2. Veilige firewalltoegang tot de ACME-server: de beveiligde firewall moet de mogelijkheid hebben om toegang te krijgen tot de ACME-server via een van de interfaces. Deze toegang hoeft niet via de interface te gebeuren waarvoor het certificaat wordt aangevraagd.
3. Beschikbaarheid TCP-poort 80: Sta TCP-poort 80 toe van de ACME CA-server naar de interface die overeenkomt met de domeinnaam. Dit is vereist tijdens het ACME-uitwisselingsproces om de HTTP-01-uitdaging te voltooien.

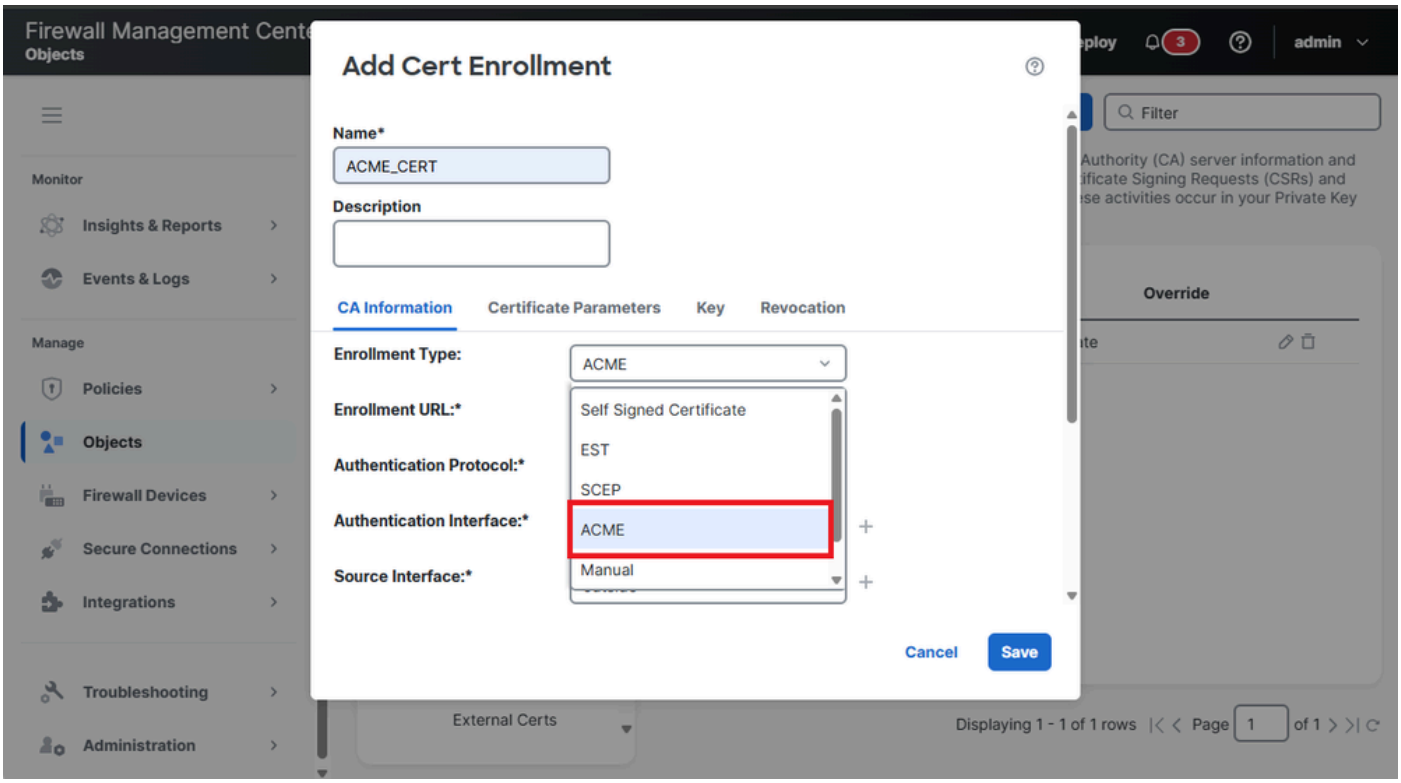
 Opmerking: tijdens de periode waarin poort 80 is geopend, zijn alleen de gegevens van de ACME-uitdaging toegankelijk.

ACME Certificate Enrollment Object maken

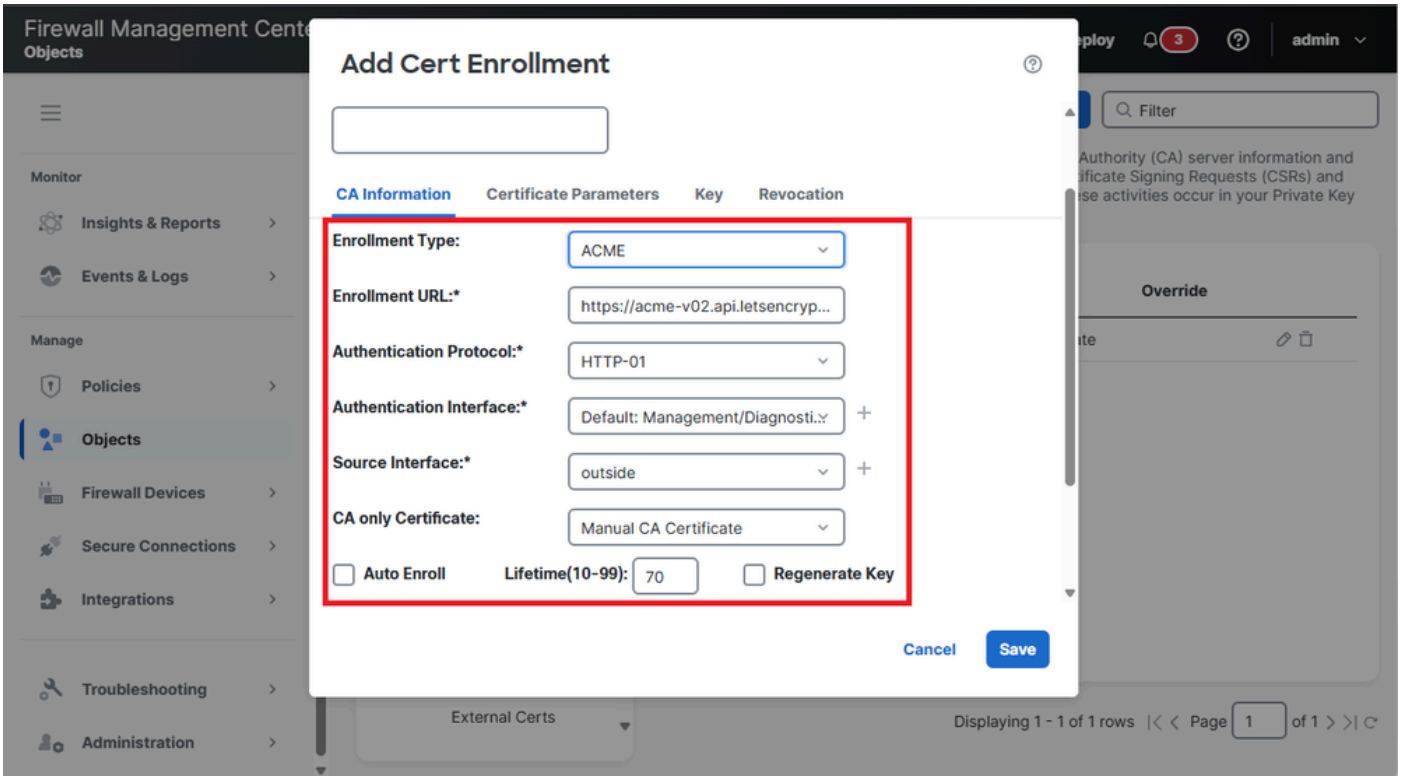
1. Navigeer naar Objecten > PKI > Cert Enrollment en klik op Cert Enrollment toevoegen om het configuratieproces te starten.



2. De optie voor ACME-inschrijving wordt samen met andere inschrijvingsmethoden in het vervolgkeuzemenu weergegeven. Selecteer ACME in de keuzelijst Inschrijvingstype om door te gaan.



3. De opties voor het configureren van certificaatparameters worden weergegeven. Vul de velden met de juiste informatie in.



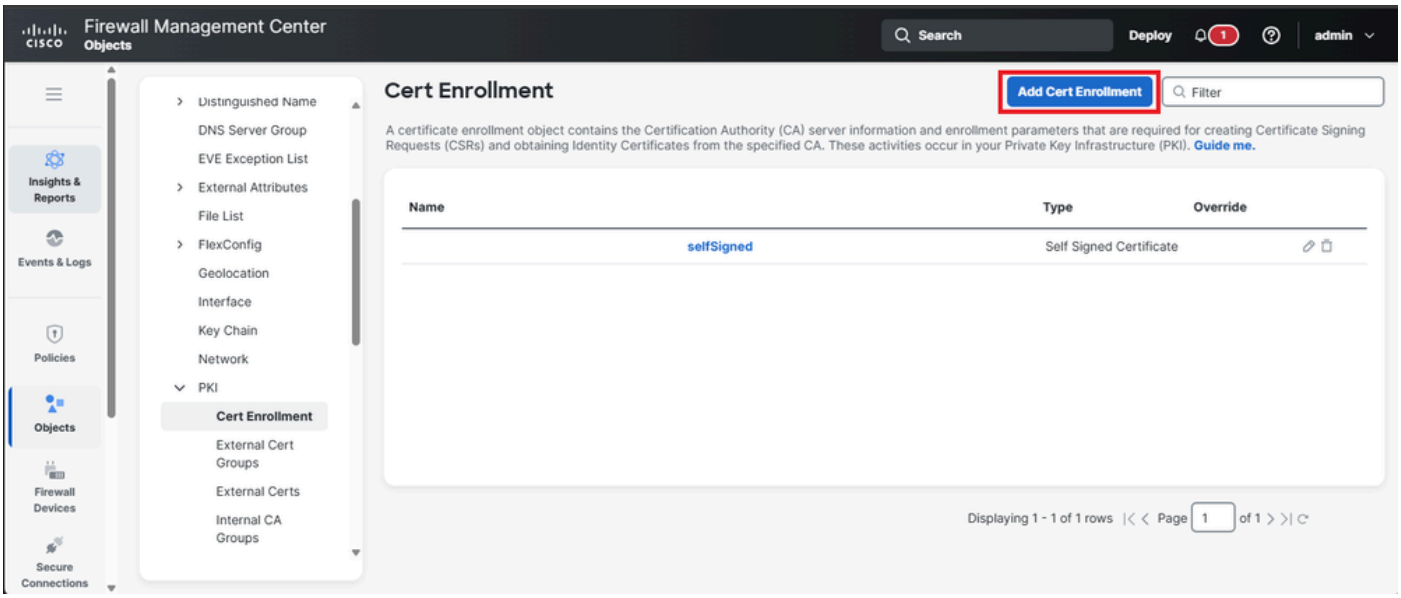
- Inschrijving-URL: Dit is het adres van de ACME-server (zoals Let's Encrypt) die wordt gebruikt om certificaten aan te vragen en op te halen.
- Verificatieprotocol: Hiermee wordt de methode opgegeven die wordt gebruikt om het

eigendom van het domein te verifiëren. Het ondersteunde protocol voor ACME-uitdagingen is HTTP-01.
- Authenticatie-interface: de netwerkinterface op het FTD-apparaat dat de HTTP-01-uitdaging ontvangt van de ACME-server.
- Alleen CA-certificaat: er moet een certificaat van een certificeringsinstantie (CA) worden gekozen om de ACME-server te vertrouwen.

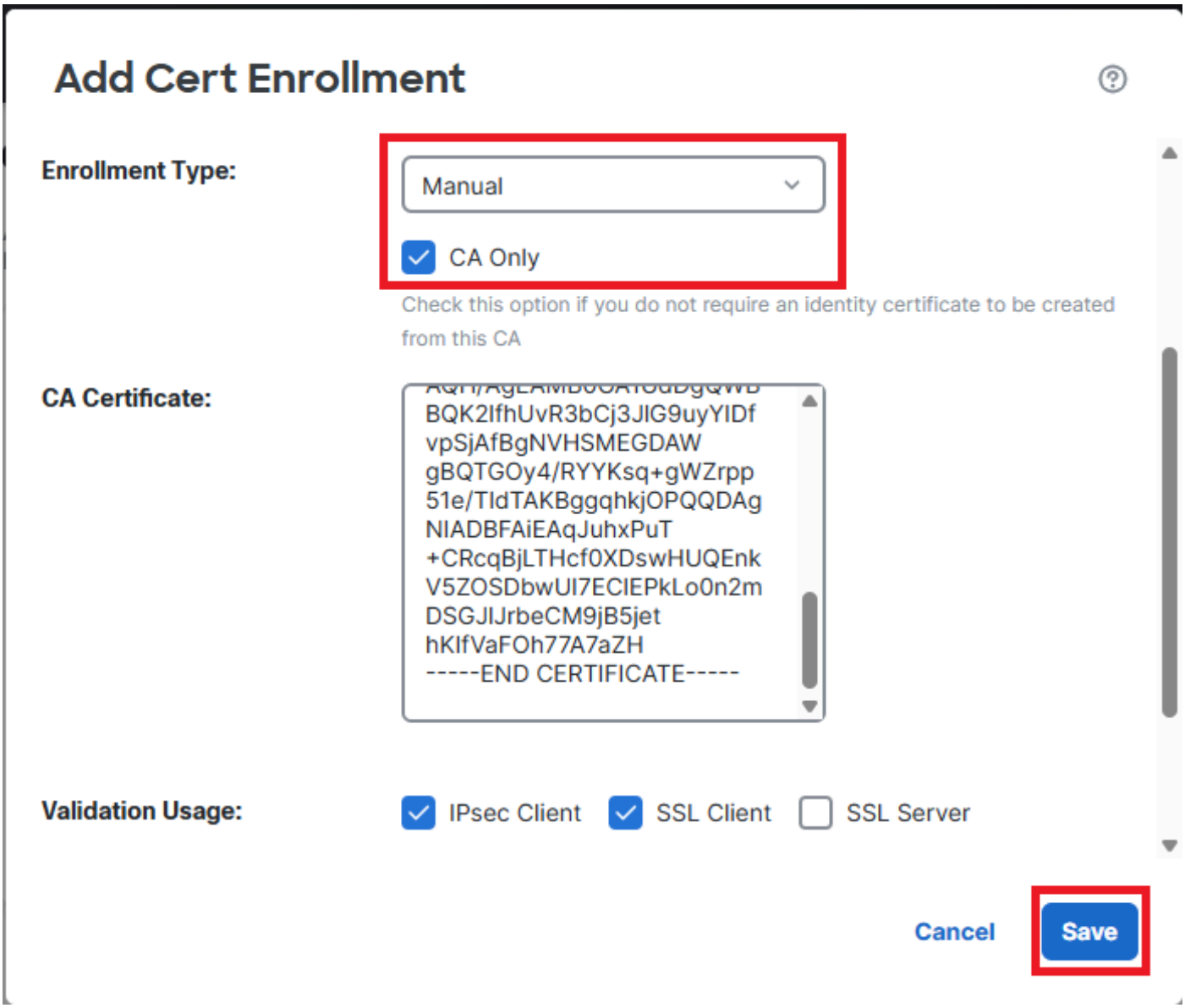
Opmerking: standaard wordt verwezen naar de openbare Let's Encrypt-service-URL: https://acme-v02.api.letsencrypt.org/directory.

---

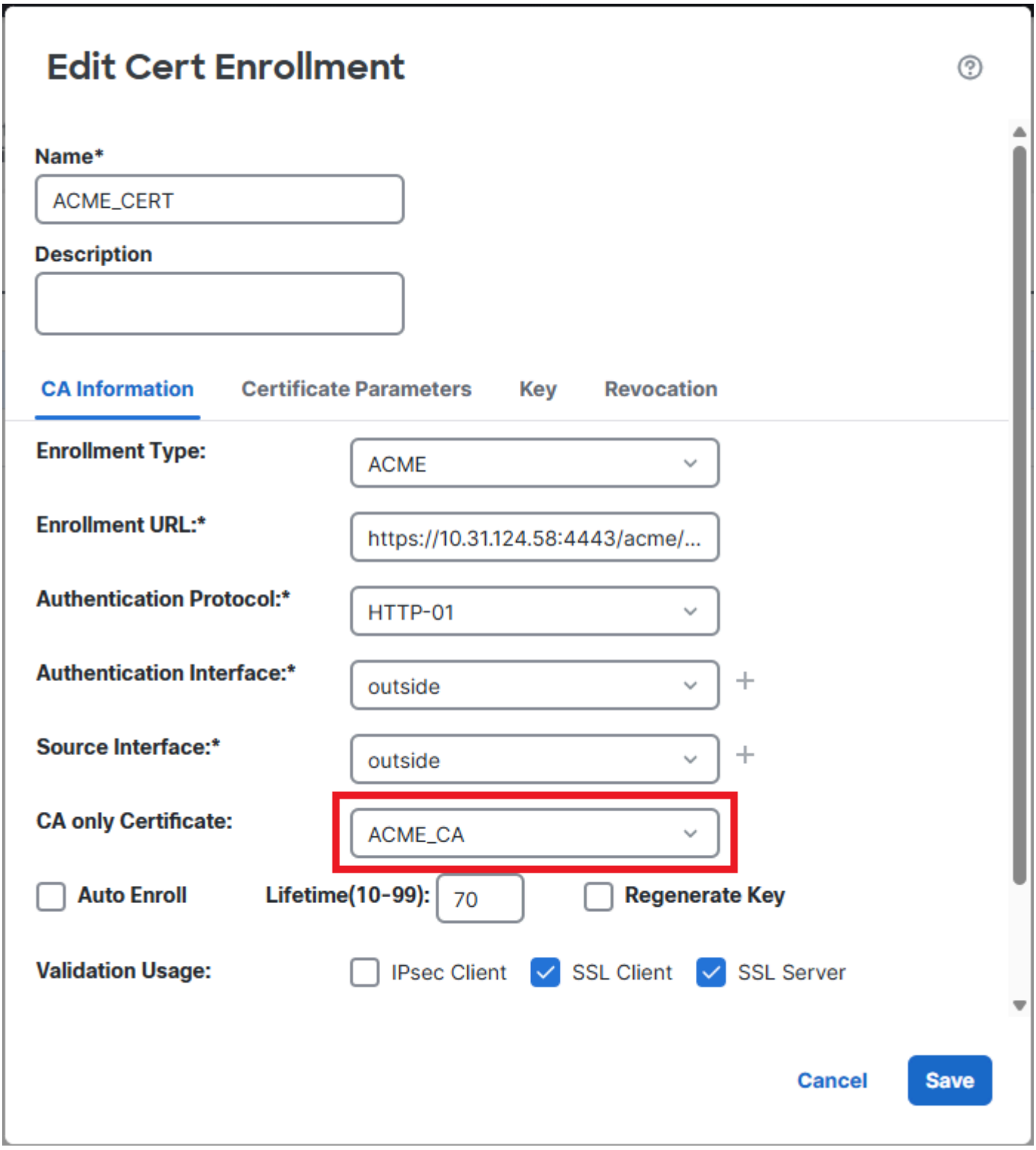
4. Als u een ACME-server gebruikt die niet goed bekend is, moet u het CA-certificaat van de ACME-server toevoegen. Navigeer naar Objecten > Cert Enrollment en klik op de knop Cert Enrollment toevoegen.



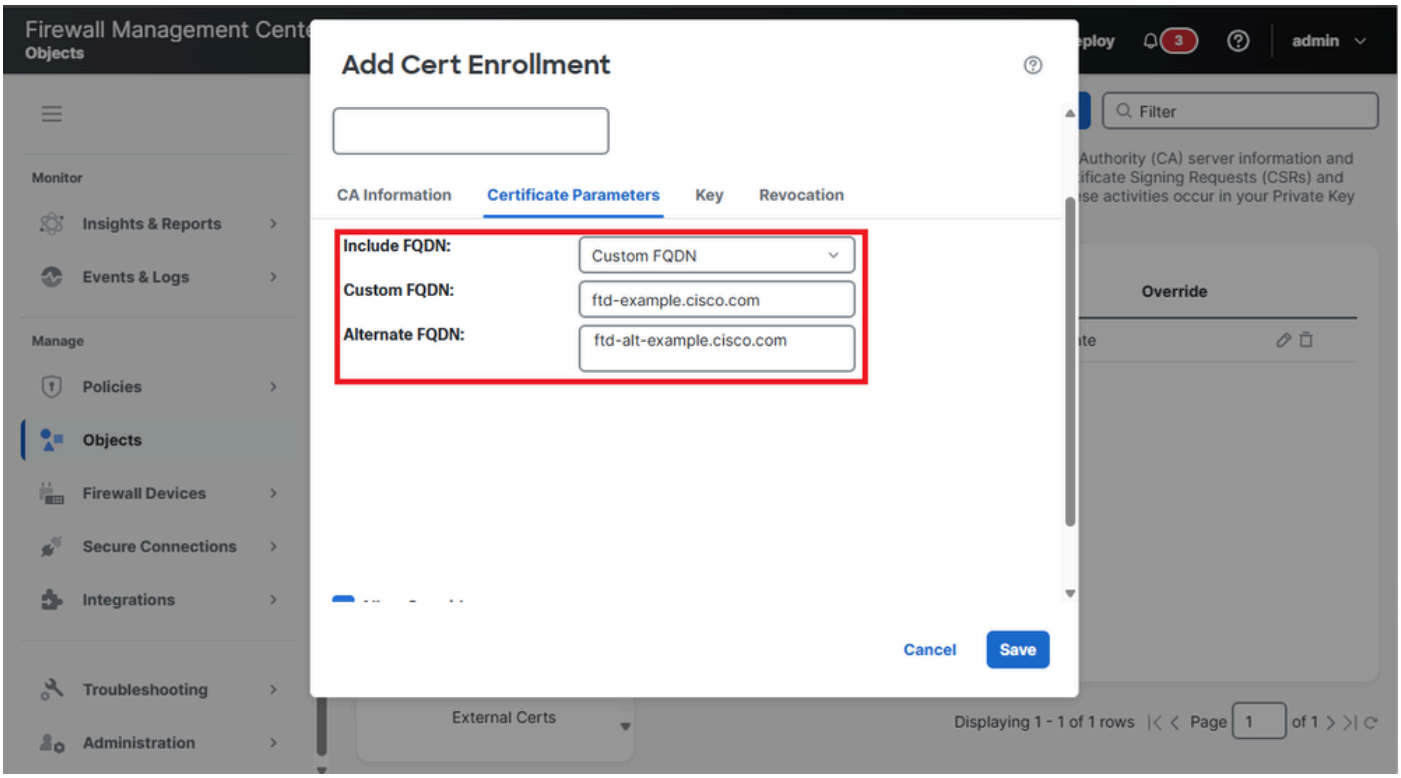
- Noem het trustpoint en selecteer het inschrijvingstype als handleiding. Controleer vervolgens de optie Alleen CA. Plak ten slotte het CA-certificaat van de ACME-server en klik op Opslaan.



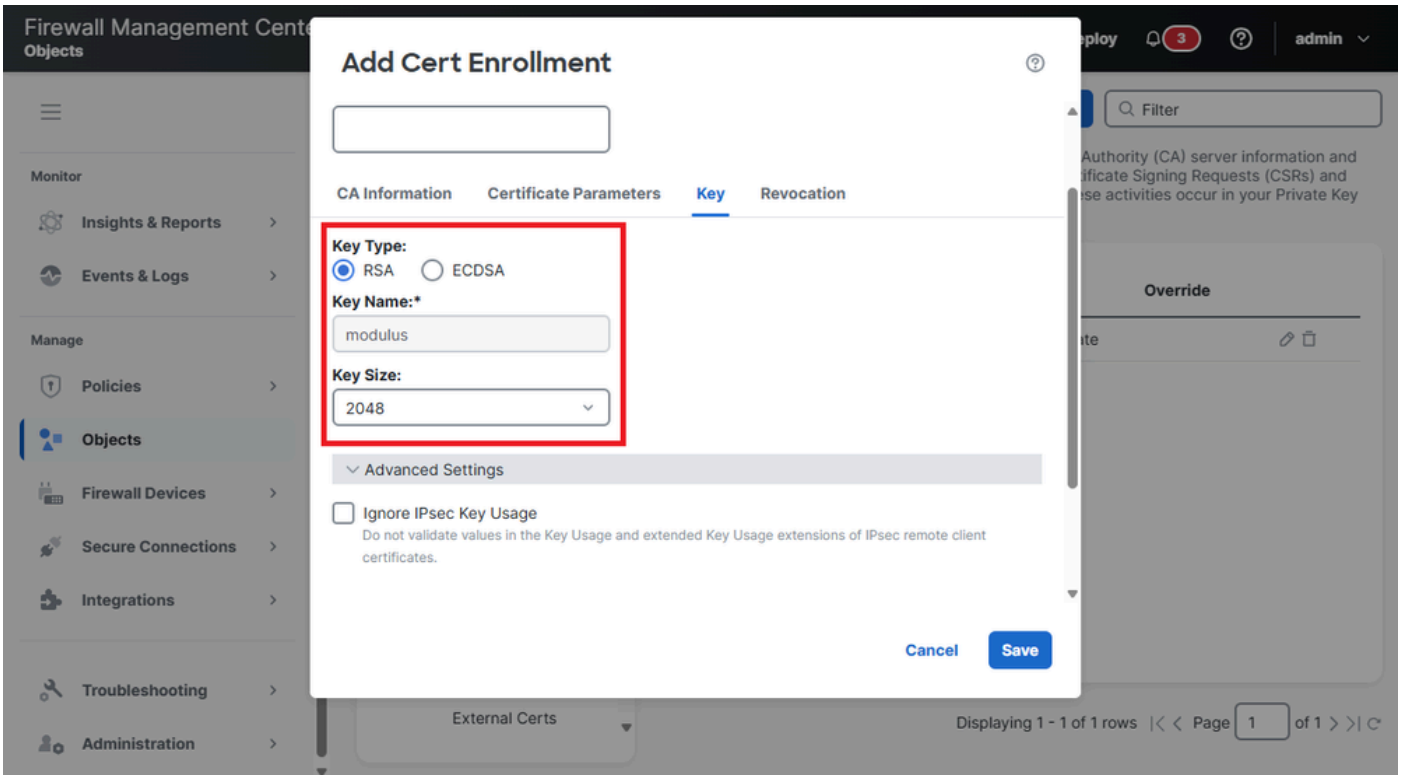
- Selecteer ten slotte het vertrouwenspunt van de ACME CA-server in de sectie CA Only Certificate.



5. Navigeer naar Certificaatparameters, selecteer de optie Aangepaste FQDN in het vak Inclusief FQDN en vul de velden Aangepaste FQDN en Alternatieve FQDN in met de primaire FQDN en eventuele alternatieve domeinnamen die in het certificaat moeten worden opgenomen.



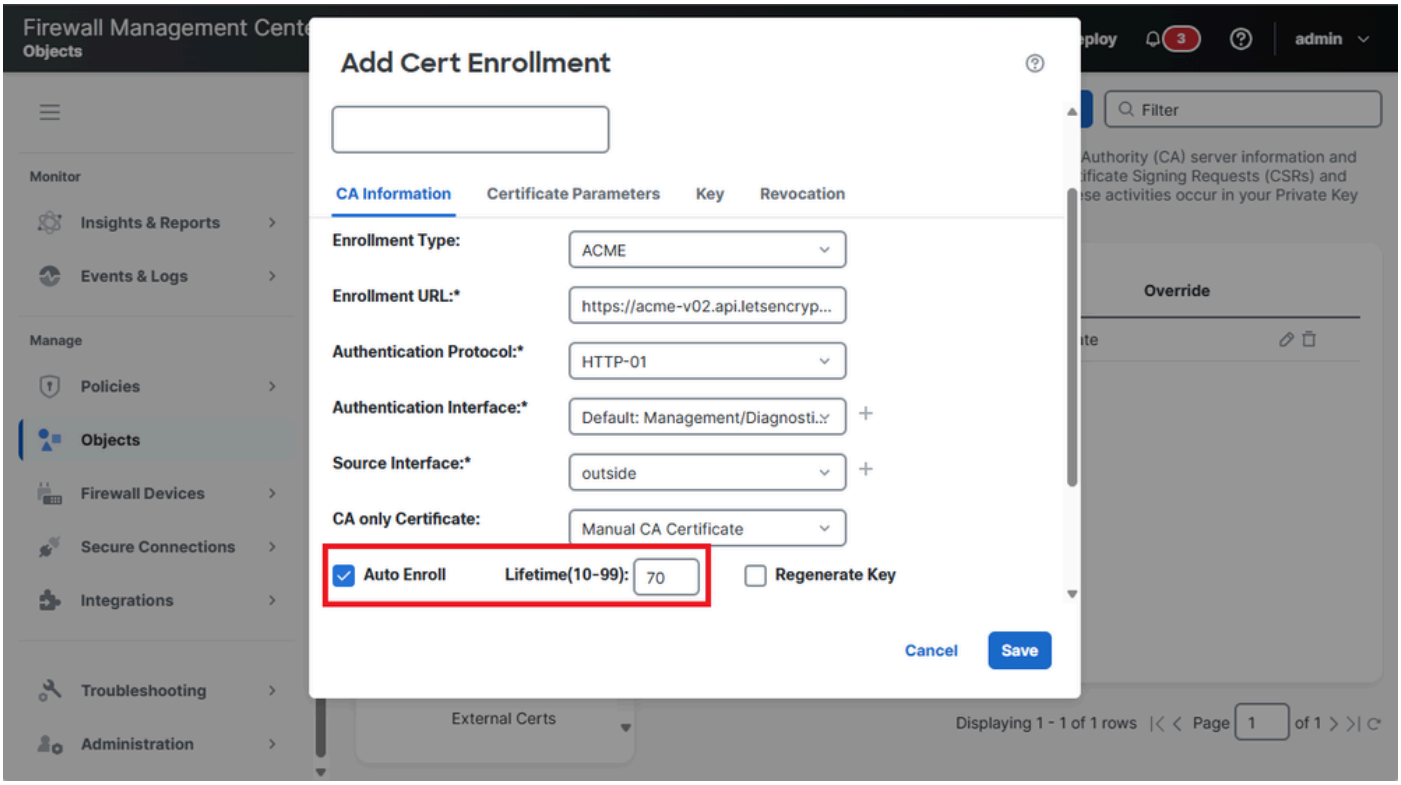
6. Navigeer naar Sleutel om de instellingen voor Sleuteltype en Sleutelgrootte te wijzigen.



7. (Optioneel) Automatische inschrijving voor het identiteitscertificaat inschakelen.

Schakel het selectievakje Automatisch inschrijven in en geef het percentage op voor de levensduur van Automatisch inschrijven.

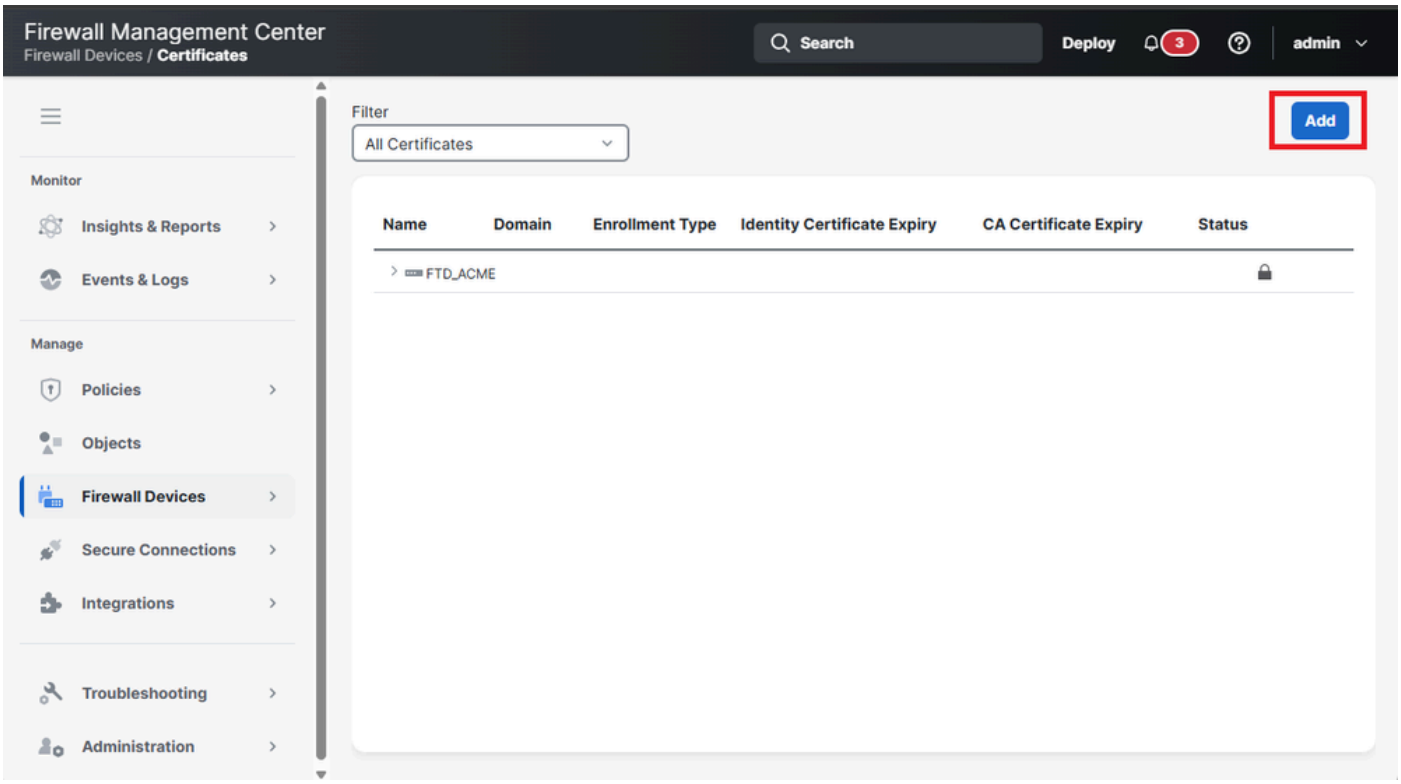
Deze functie zorgt ervoor dat het certificaat automatisch wordt verlengd voordat het verloopt. Het percentage bepaalt hoe ver voor het verstrijken van het certificaat het verlengingsproces begint. Bijvoorbeeld, als ingesteld op 80%, begint het verlengingsproces wanneer het certificaat 80% van de geldigheidsperiode heeft bereikt.



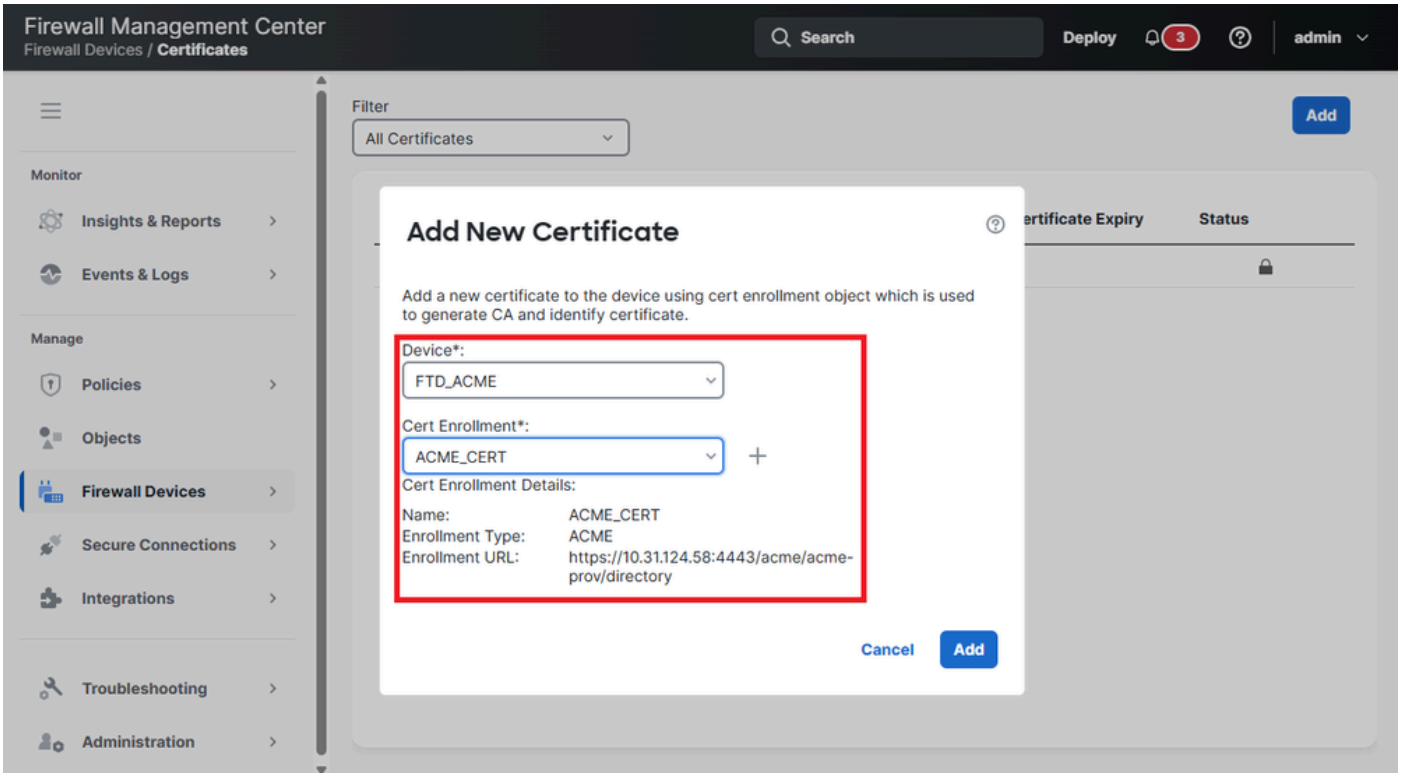
8. Klik op Opslaan.

Inschrijving voor ACME-certificaat op het apparaat

1.Navigeer naar Firewallapparaten > Certificaten en klik op de knop Toevoegen om een nieuw certificaat in te schrijven.



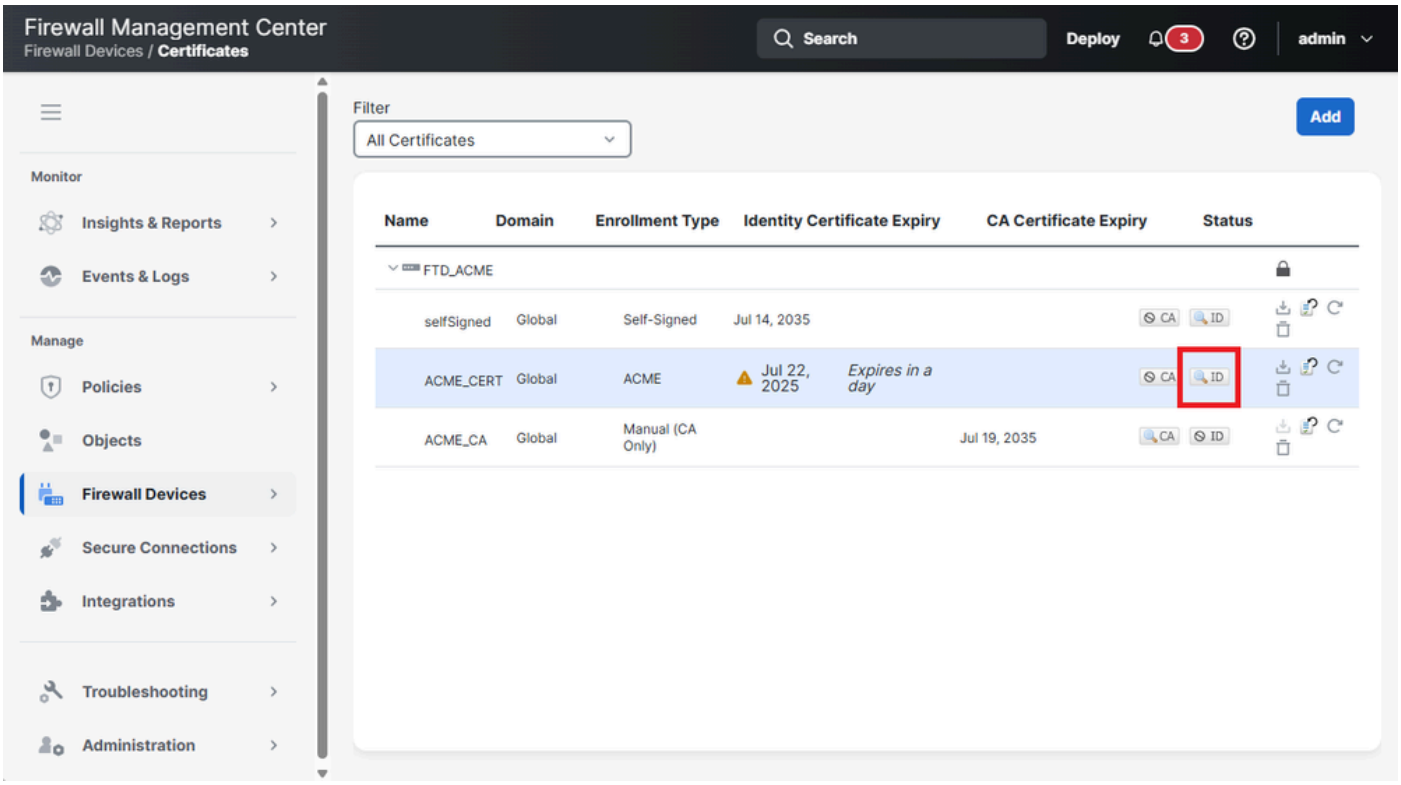
2. Selecteer het FTD-apparaat in de vervolgkeuzelijst Apparaat en het certificaatobject dat eerder is gemaakt in Cert Enrollment.



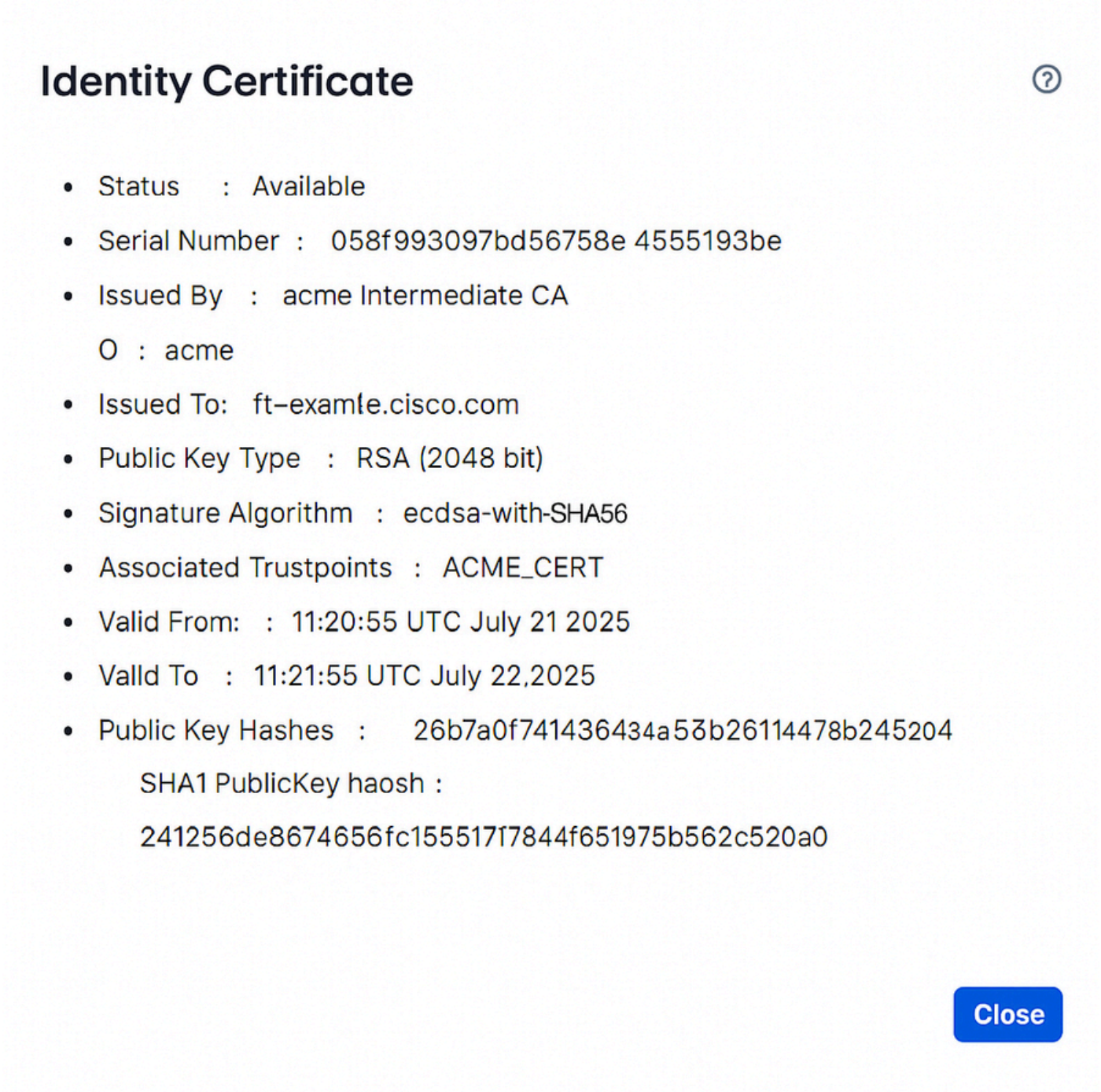
3. Klik op Toevoegen.

4. Zodra de implementatie is voltooid, wordt in de kolom Status de knop ID-certificaat

weergegeven.



5. Valideer de certificaatgegevens door op de knop ID te klikken.



Verifiëren

Geïnstalleerd certificaat bekijken in FTD

Bevestig dat het certificaat is geregistreerd met de opdracht.show crypto ca certificates <Trust Point Name>.

<#root>

```
firepower#
```

show crypto ca certificates

ACME_CERT

```
Certificate
Status: Available
Certificate Serial Number: 058f993097bd56758e44554194a953be
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=acme Intermediate CA
O=acme
Subject Name:
CN=ftd-example.cisco.com
Validity Date:
start date: 11:20:55 UTC Jul 21 2025
end date: 11:21:55 UTC Jul 22 2025
Storage: immediate
Associated Trustpoints: ACME_CERT
Public Key Hashes:
SHA1 PublicKey hash: 26b7a0f7414364a45b246114478bb74f432520c4
SHA1 PublicKeyInfo hash: 24125d6e8674566c1551784f651975b562c520a
```

Syslog-evenementen

Er zijn nieuwe syslogs in de Secure Firewall FTD om gebeurtenissen met betrekking tot de certificaatinschrijving vast te leggen met behulp van het ACME-protocol:

- 717067: geeft informatie over wanneer de inschrijving voor het ACME-certificaat begint.

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

- 717068: geeft informatie over wanneer de inschrijving voor het ACME-certificaat succesvol is.

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

- 717069: geeft informatie over wanneer ACME-inschrijving mislukt.

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

- 717070: biedt informatie over het sleutelpaar voor certificaatinschrijving of certificaatvernieuwing.

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

Problemen oplossen

Als een inschrijving voor een ACME-certificaat mislukt, overweeg dan de volgende stappen om het probleem te identificeren en op te lossen:

- Connectiviteit met de server controleren: Bevestig dat de Secure Firewall netwerkconnectiviteit heeft met de ACME-server. Controleer of er geen netwerkproblemen of firewallregels zijn die de communicatie blokkeren.
- Zorg ervoor dat de Secure Firewall-domeinnaam oplosbaar is: zorg ervoor dat de domeinnaam die op de Secure Firewall FTD is geconfigureerd, oplosbaar is 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 FTD voor beveiligde firewall. Dit zorgt ervoor dat de ACME-server domeineigendom kan valideren.

Opdrachten voor probleemoplossing

Verzamel voor meer informatie de uitvoer van de volgende foutopsporingsopdrachten:

- Debug Crypto Cacme <1-255>
- Debug Crypto CA <1-14>

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.