Konfigurieren der Zertifikatregistrierung mithilfe des ACME-Protokolls auf der sicheren Firewall-Bedrohungsabwehr, die von FMC verwaltet wird

Einleitung

In diesem Dokument wird der Prozess zur Registrierung eines TLS-Zertifikats (Transport Layer Security) über das ACME-Protokoll (Automated Certificate Management Environment) auf der FTD-Plattform (Secure Firewall Firepower Threat Defense) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

- Manuelle Zertifikatregistrierung und Grundlagen von Secure Sockets Layer (SSL).
- Grundlegende Authentifizierungskonzepte für Remotezugriff-VPNs.
- Erfahrungen mit Zertifizierungsstellen (Certificate Authority, CA)

Verwendete Komponenten

- Cisco FTDv, Version 10.0.0-35
- Cisco FMC Version 10.0.0-35
- CA-Server (Certificate Authority), der das ACME-Protokoll unterstützt

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Anforderungen und Einschränkungen

Zu den aktuellen Voraussetzungen und Einschränkungen für die ACME-Registrierung bei Secure Firewall FTD gehören:

- Unterstützt auf FTD und FMC Versionen 10.0.0 und höher.
- ACME erlaubt keine Ausstellung von Platzhalterzertifikaten. Jede Zertifikatsanforderung muss einen präzisen Domänennamen angeben.
- Jeder über ACME registrierte Trustpoint ist auf eine Schnittstelle beschränkt, sodass über ACME erhaltene Zertifikate nicht über mehrere Schnittstellen hinweg gemeinsam genutzt werden können.
- Schlüsselpaare werden automatisch generiert und sind für jedes in ACME registrierte Zertifikat eindeutig. Dadurch wird die Wiederverwendung von Schlüsseln verhindert und die Sicherheit erhöht.

Überlegungen zur Herabstufung

Beim Downgrade auf eine FTD-Version für sichere Firewalls, die die ACME-Registrierung nicht unterstützt (Version 7.7 oder früher):

- Alle ACME-bezogenen Vertrauenspunktkonfigurationen, die in Version 10.0.0 oder höher eingeführt wurden, gehen verloren.
- Die über ACME registrierten Zertifikate sind weiterhin zugänglich. Die Verknüpfung der privaten Schlüssel wird jedoch nach dem ersten Speichern aufgehoben und nach dem Downgrade neu gestartet.

Falls ein Downgrade erforderlich ist, verwenden Sie die empfohlene Problemumgehung:

- Exportieren Sie vor dem Downgrade die ACME-Zertifikate im PKCS12-Format.
- Entfernen Sie vor dem Downgrade die ACME-Vertrauenspunktkonfiguration.
- Importieren Sie nach dem Downgrade das PKCS12-Zertifikat. Der importierte Trustpoint bleibt gültig, bis das von ACME ausgestellte Zertifikat abläuft.

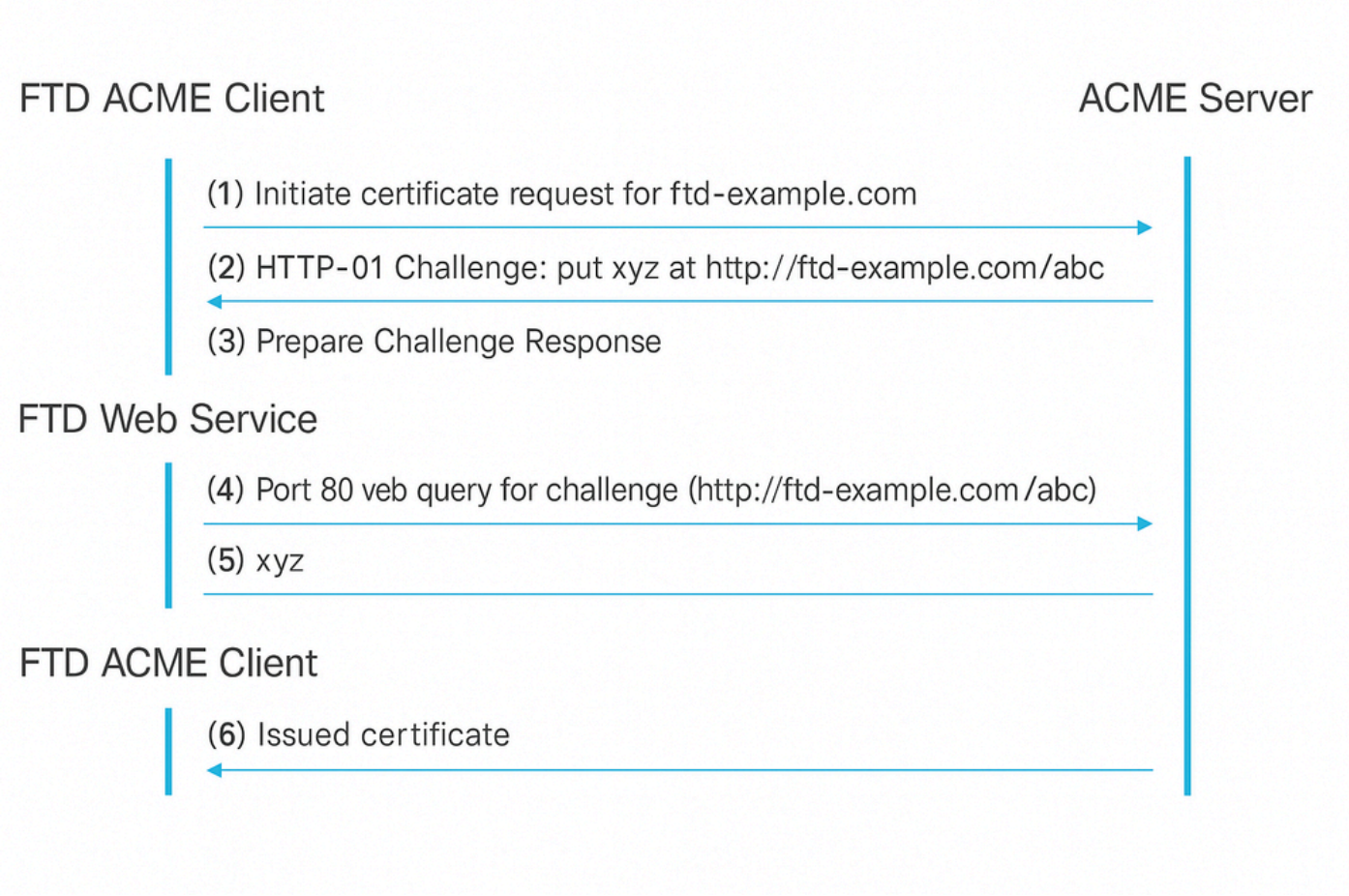
Hintergrundinformationen

Das ACME-Protokoll soll die Verwaltung von TLS-Zertifikaten für Netzwerkadministratoren vereinfachen. Mit ACME können Administratoren die Aufgaben automatisieren, die mit dem Erwerb und der Verlängerung von TLS-Zertifikaten verbunden sind. Diese Automatisierung ist besonders nützlich, wenn Sie mit Zertifizierungsstellen (Certificate Authorities, CAs) wie Let's Encrypt arbeiten, die kostenlose, automatisierte und öffentlich zugängliche Zertifikate über das ACME-Protokoll bereitstellen.ACME erleichtert die Ausstellung von Domain Validation (DV)-Zertifikaten. Mit diesen Zertifikaten wird überprüft, ob der Zertifikatanforderer die Kontrolle über die

angegebenen Domänen hat. Die Validierung erfolgt in der Regel über einen HTTP-basierten Challenge-Prozess, bei dem der Antragsteller eine bestimmte Datei auf seinem Webserver platziert. Die Zertifizierungsstelle (Certificate Authority, CA) greift dann über den HTTP-Server der Domäne auf diese Datei zu, um die Domänenkontrolle zu bestätigen. Wenn diese Prüfung erfolgreich besteht, kann die Zertifizierungsstelle das DV-Zertifikat ausstellen.

Der Registrierungsprozess umfasst folgende Schritte:

1. Zertifikatanforderung initiieren: Der Client sendet eine Zertifikatanforderung an den ACME-Server und gibt dabei die Domäne(n) an, für die das Zertifikat benötigt wird.
2. HTTP-01-Anforderung empfangen: Der ACME-Server antwortet mit einer HTTP-01-Herausforderung, die ein eindeutiges Token enthält, das der Client verwenden muss, um den Domänenbesitz nachzuweisen.
3. Vorbereitung der Antwort auf die Herausforderung:
    1. Der Client generiert eine Schlüsselautorisierung, indem er das Token vom ACME-Server mit seinem Kontoschlüssel kombiniert.
    2. Der Client konfiguriert seinen Webserver so, dass er diese Schlüsselautorisierung über einen bestimmten URL-Pfad bereitstellt.
4. ACME Server ruft Herausforderung ab: Der ACME-Server führt eine HTTP GET-Anforderung an die bereitgestellte URL aus, um die Schlüsselautorisierung zu erhalten.
5. ACME Server verifiziert Besitz: Der Server vergleicht die abgerufene Schlüsselautorisierung mit dem erwarteten Wert, um die Kontrolle des Clients über die Domäne zu überprüfen.
6. Ausstellungszertifikat: Nach erfolgreicher Validierung gibt der ACME-Server das SSL/TLS-Zertifikat an den Client aus.



ACME-Registrierung HTTP-01-Authentifizierungsablauf.

Die wichtigsten Vorteile der Verwendung des ACME-Protokolls für die Registrierung von TLS-Zertifikaten bei Secure Firewall FTD sind:

- Automatisierung der Zertifikatsverwaltung: ACME rationalisiert den Prozess des Erwerbs und der Verwaltung von TLS-Domänenzertifikaten für sichere FTD-TLS-Firewall-Schnittstellen und reduziert dadurch den manuellen Verwaltungsaufwand erheblich.
- Automatische Zertifikatsverlängerung: Bei ACME-fähigen Vertrauenspunkten werden die Zertifikate nach ihrem Ablauf automatisch erneuert, sodass laufender Verwaltungsaufwand minimiert wird.
- Kontinuierliche Sicherheitsgarantie: Durch diese Automatisierung wird sichergestellt, dass Zertifikate unterbrechungsfrei gültig bleiben, unerwartete Zertifikatabläufe verhindert werden und eine sichere Kommunikation gewährleistet ist.

Zusammen steigern diese Vorteile die Betriebseffizienz und die Sicherheit bei FTD-Bereitstellungen mit sicheren Firewalls.

Konfigurieren

Konfiguration der Voraussetzungen

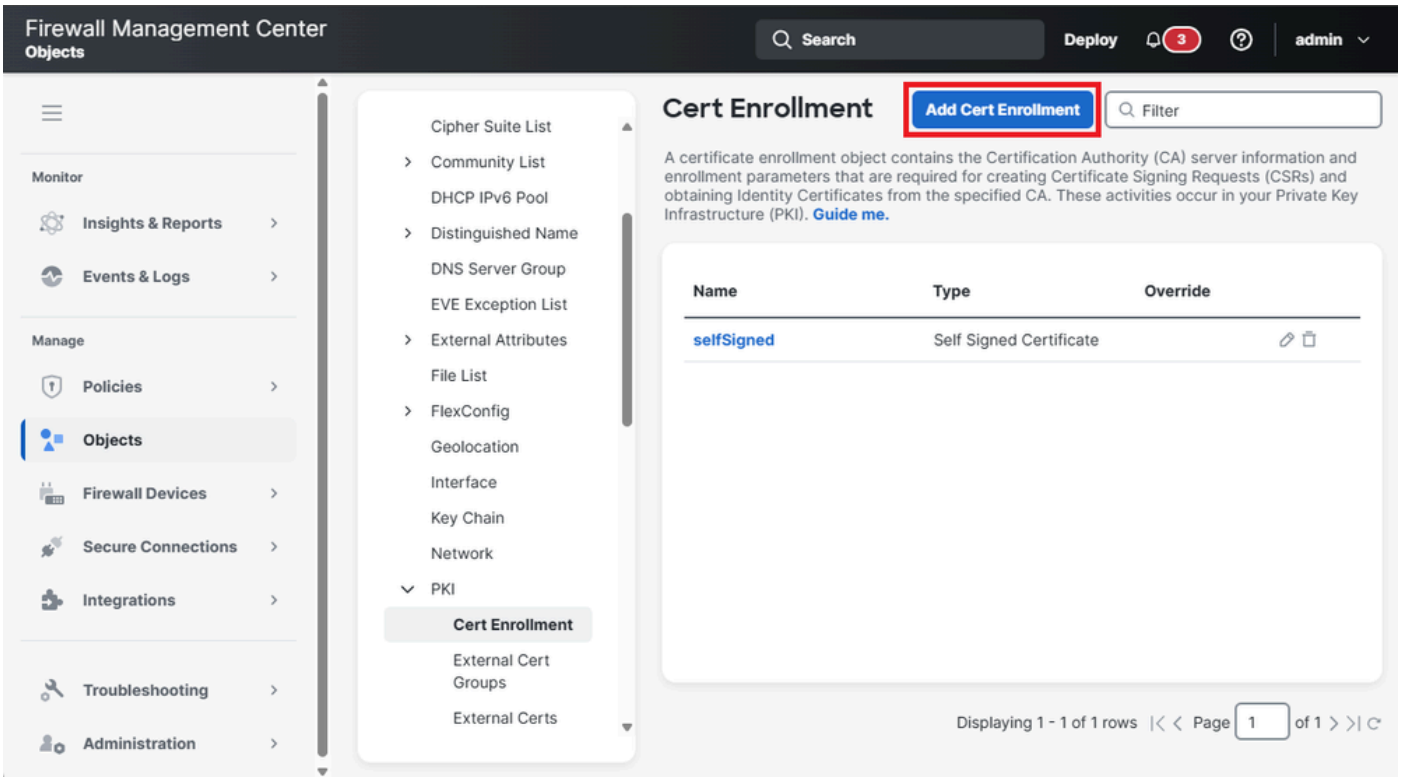
Bevor Sie den ACME-Registrierungsprozess einleiten, stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

1. Auflösbarer Domänenname: Der Domänenname, für den Sie ein Zertifikat anfordern, muss vom ACME-Server auflösbar sein. Dadurch wird sichergestellt, dass der Server das Domäneneigentum überprüfen kann.
2. Sicherer Firewallzugriff auf den ACME-Server: Die sichere Firewall muss über eine der Schnittstellen des ACME-Servers auf diesen zugreifen können. Dieser Zugriff muss nicht über die Schnittstelle erfolgen, für die das Zertifikat angefordert wird.
3. Verfügbarkeit von TCP-Port 80: Erlaubt TCP-Port 80 vom ACME CA-Server zu der Schnittstelle, die dem Domänennamen entspricht. Dies ist während des ACME-Austauschprozesses erforderlich, um die HTTP-01-Herausforderung abzuschließen.

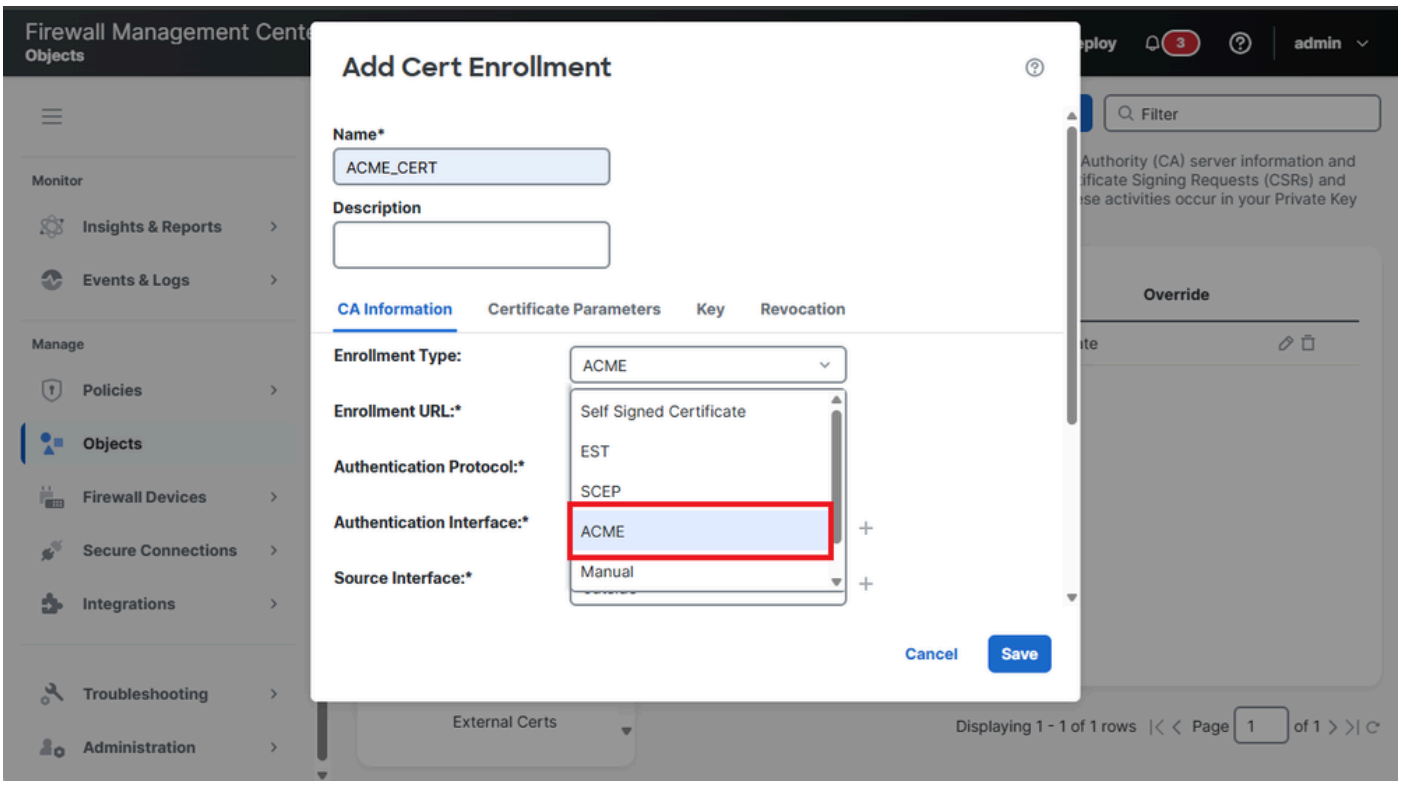
Anmerkung: Während des Zeitraums, in dem Port 80 geöffnet ist, ist nur auf die ACME-Abfragedaten zugegriffen werden können.

Erstellung des ACME-Zertifikatregistrierungsobjekts

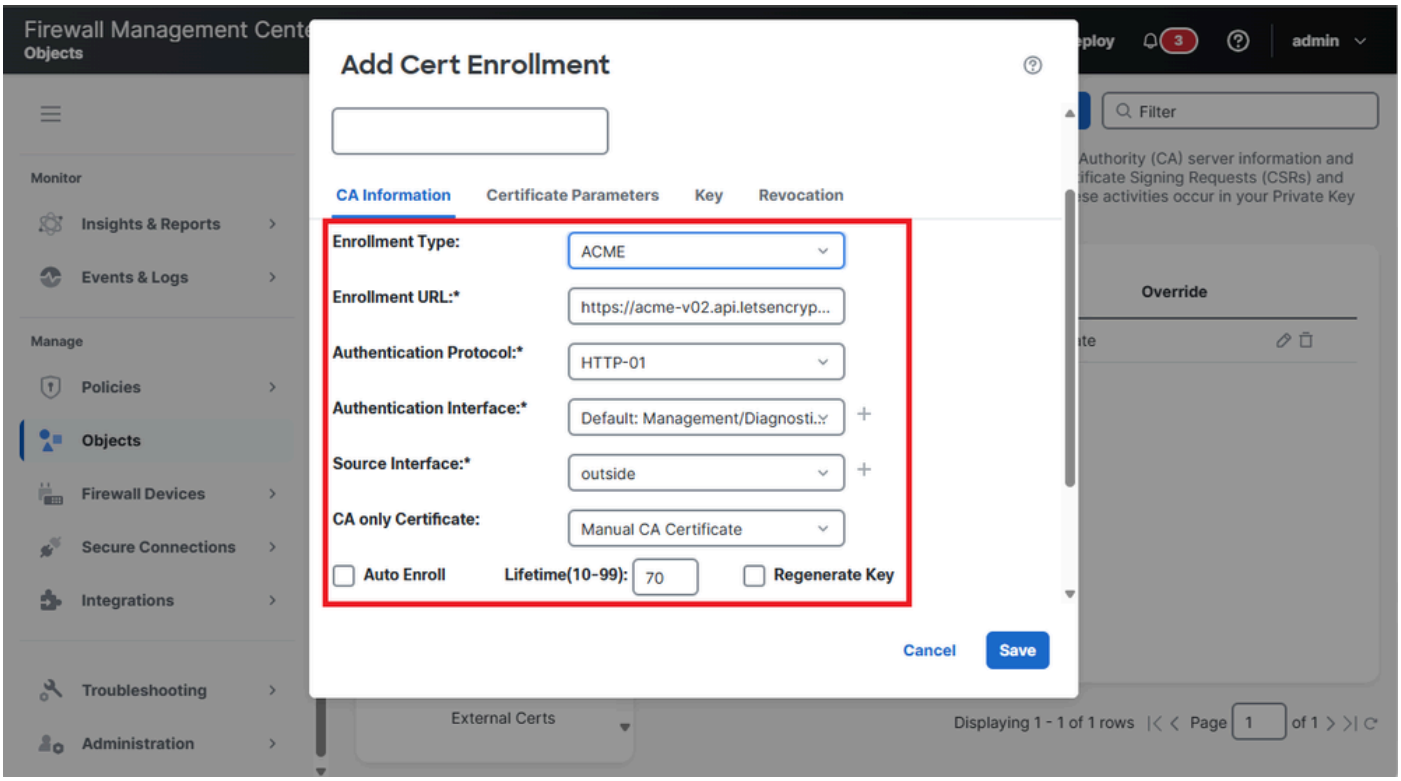
1. Navigieren Sie zu Objekte > PKI > Zertifikatregistrierung, und klicken Sie auf Zertifikatregistrierung hinzufügen, um den Konfigurationsprozess zu starten.



2. Die ACME-Registrierungsoption wird zusammen mit anderen Registrierungsmethoden im Dropdown-Menü aufgeführt. Wählen Sie ACME aus dem Dropdown-Menü Anmeldungstyp aus, um fortzufahren.



3. Die Optionen zum Konfigurieren der Zertifikatparameter werden angezeigt. Füllen Sie die Felder mit den entsprechenden Informationen aus.

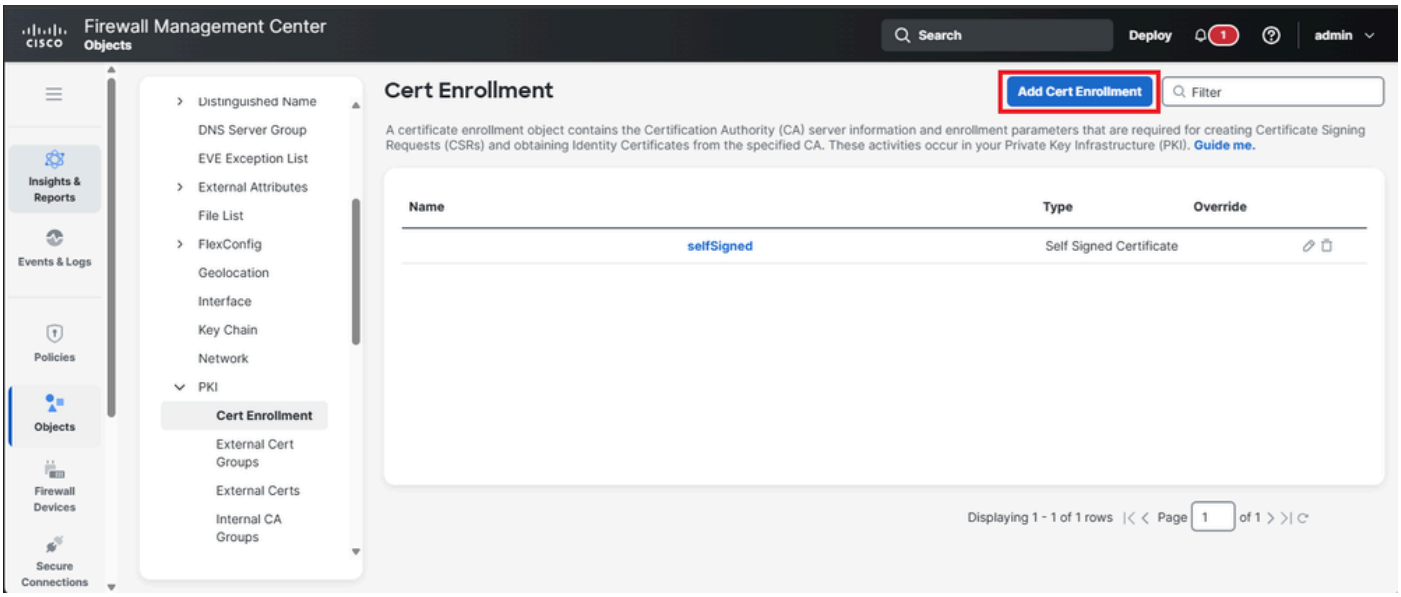


- Anmeldungs-URL: Dies ist die Adresse des ACME-Servers (wie Let’s Encrypt), der zum Anfordern und Abrufen von Zertifikaten verwendet wird.
- Authentifizierungsprotokoll: Gibt die Methode an, mit der das Domäneneigentum überprüft wird. Das unterstützte Protokoll für ACME-Herausforderungen ist HTTP-01.
- Authentifizierungsschnittstelle: Die Netzwerkschnittstelle des FTD-Geräts, das die HTTP-01-Anforderung vom ACME-Server empfängt.
- Zertifikat nur für Zertifizierungsstelle: Es muss ein Zertifikat von einer Zertifizierungsstelle (Certificate Authority, CA) ausgewählt werden, das dem ACME-Server vertrauen soll.

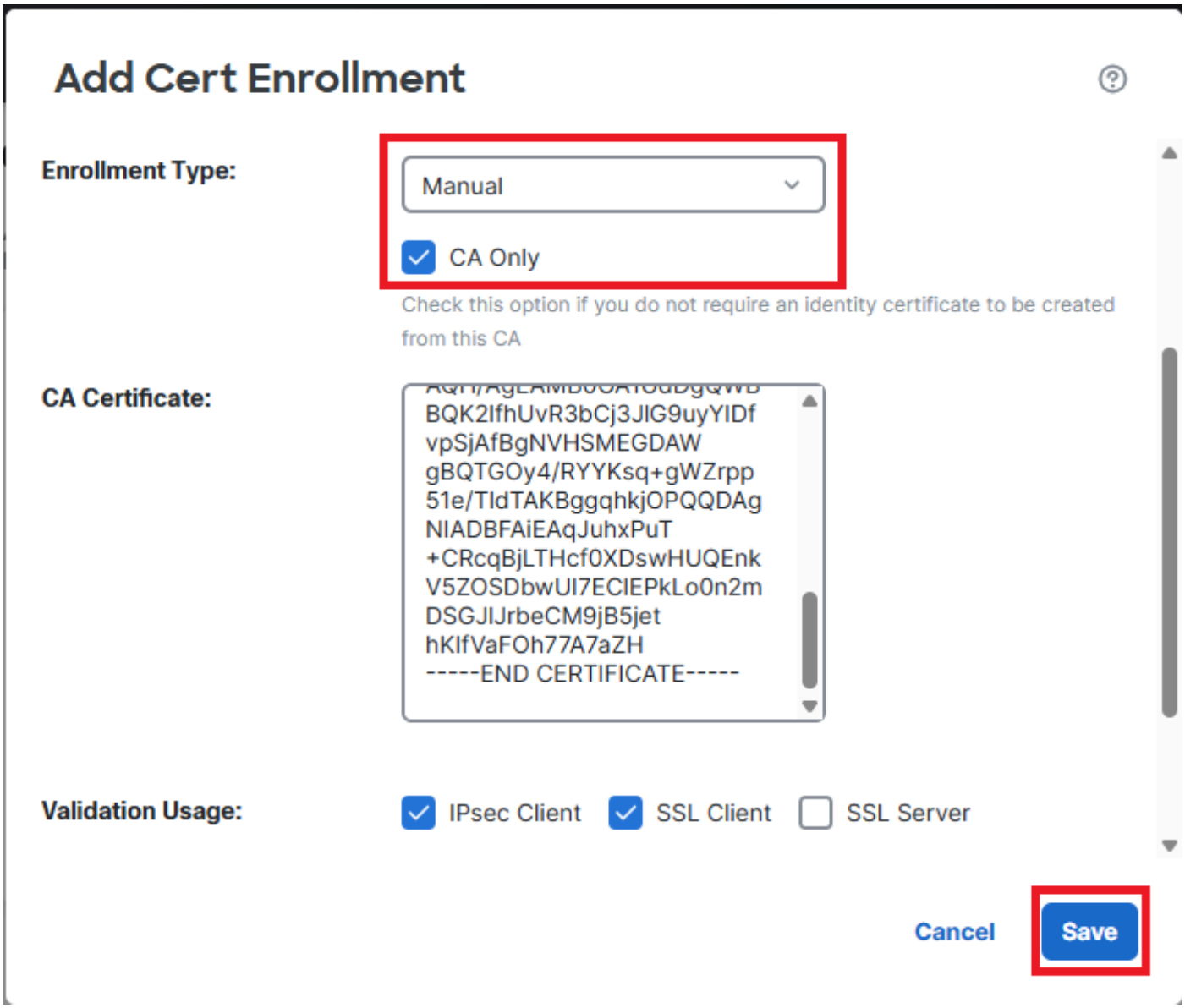
Anmerkung: Standardmäßig verweist er auf die öffentliche Let's Encrypt-Service-URL: https://acme-v02.api.letsencrypt.org/directory

---

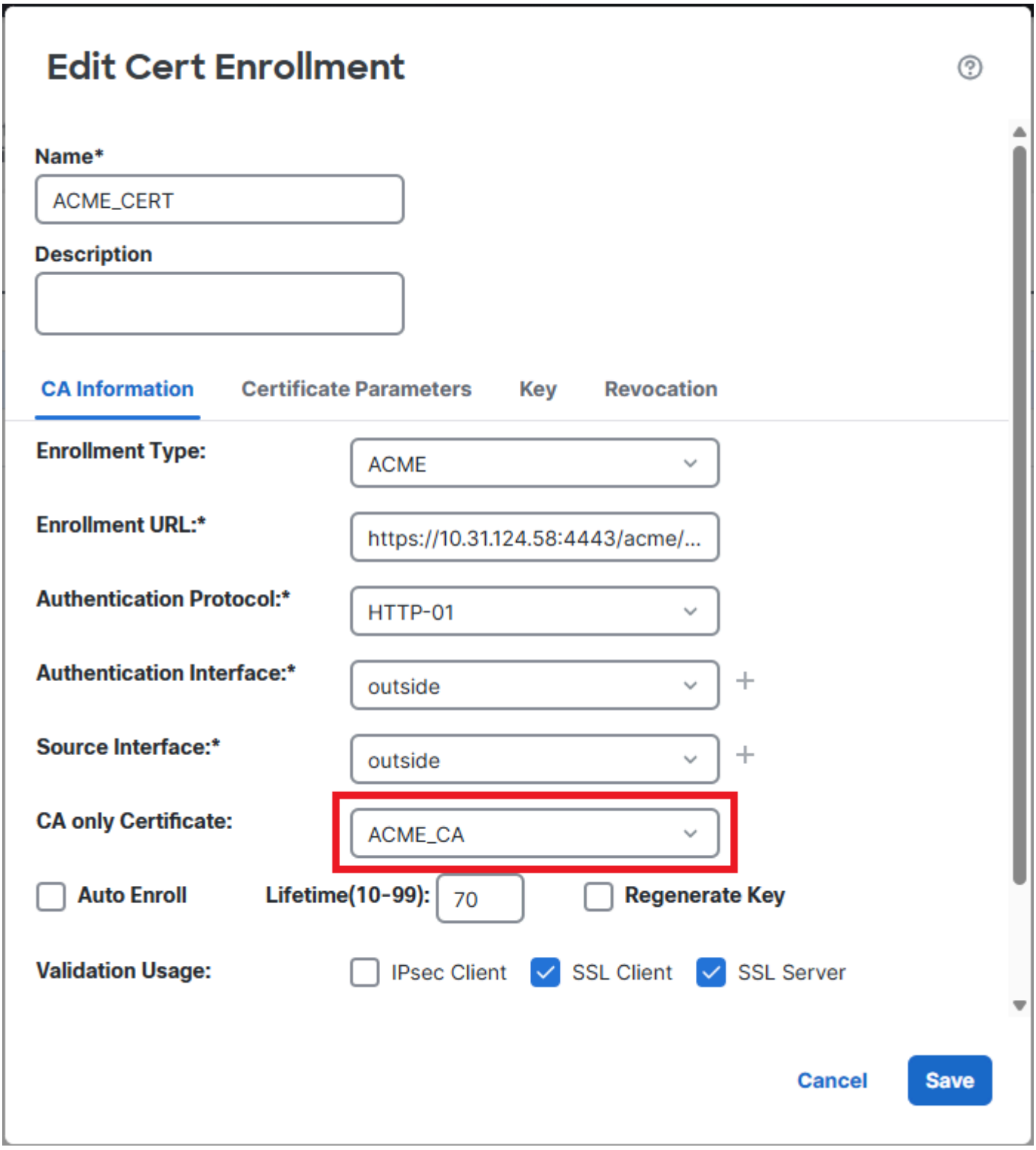
4. Wenn Sie einen unbekannten ACME-Server verwenden, müssen Sie das Zertifizierungsstellenzertifikat des ACME-Servers hinzufügen. Navigieren Sie zu Objekte > Zertifikatregistrierung, und klicken Sie auf die Schaltfläche Zertifikatregistrierung hinzufügen.



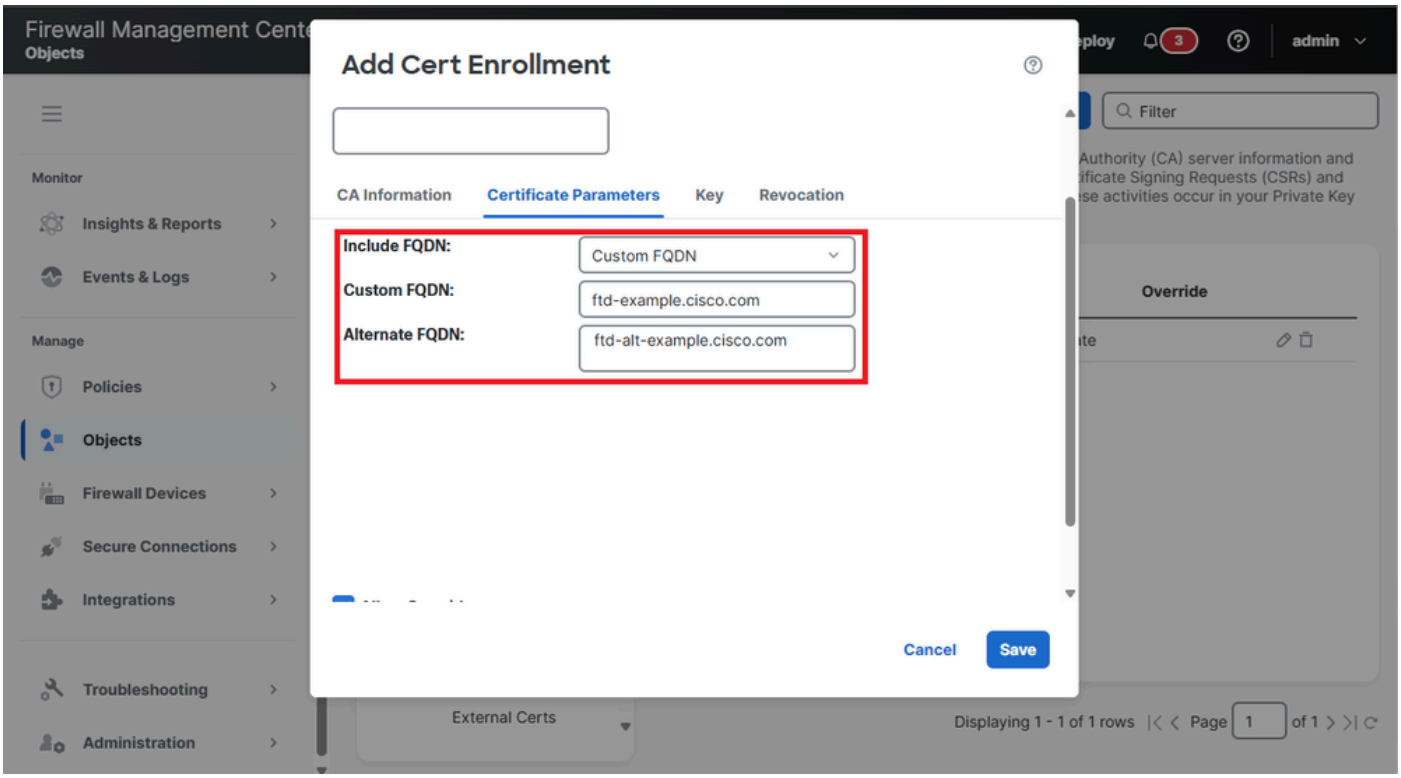
- Geben Sie dem Vertrauenspunkt einen Namen, und wählen Sie den Anmeldungstyp als Manuell aus. Aktivieren Sie dann die Option Nur CA. Fügen Sie nun das CA-Zertifikat des ACME-Servers ein, und klicken Sie auf Speichern.



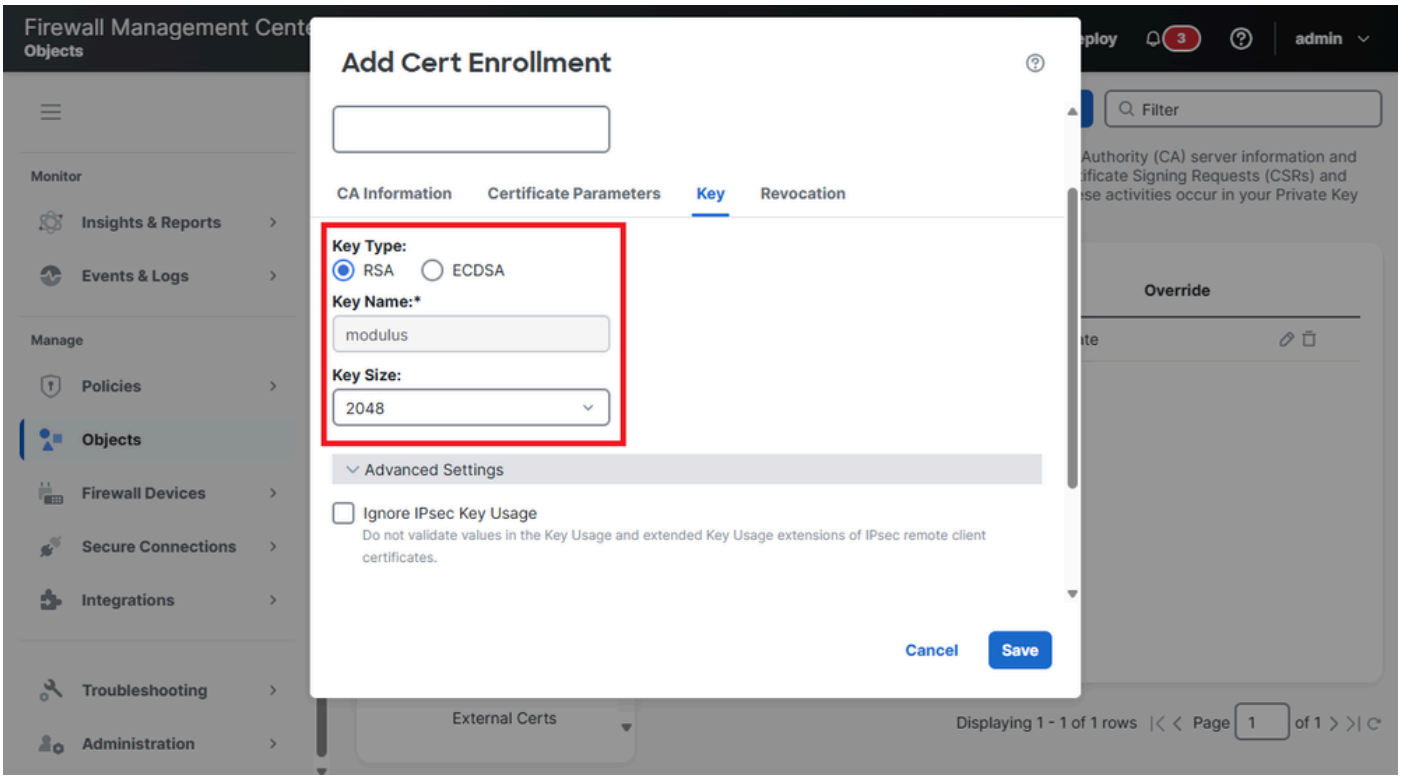
- Wählen Sie anschließend im Abschnitt "CA Only Certificate" (Nur CA-Zertifikat) den Vertrauenspunkt des ACME-Zertifizierungsstellenservers aus.



5. Navigieren Sie zu Zertifikatsparametern, wählen Sie die Option Benutzerdefinierter FQDN im Feld FQDN einschließen, und füllen Sie die Felder Benutzerdefinierter FQDN und Alternativer FQDN mit dem primären FQDN und allen alternativen Domänennamen aus, die in das Zertifikat aufgenommen werden sollen.



6. Navigieren Sie zu Schlüssel, um die Einstellungen für Schlüsseltyp und Schlüsselgröße zu ändern.

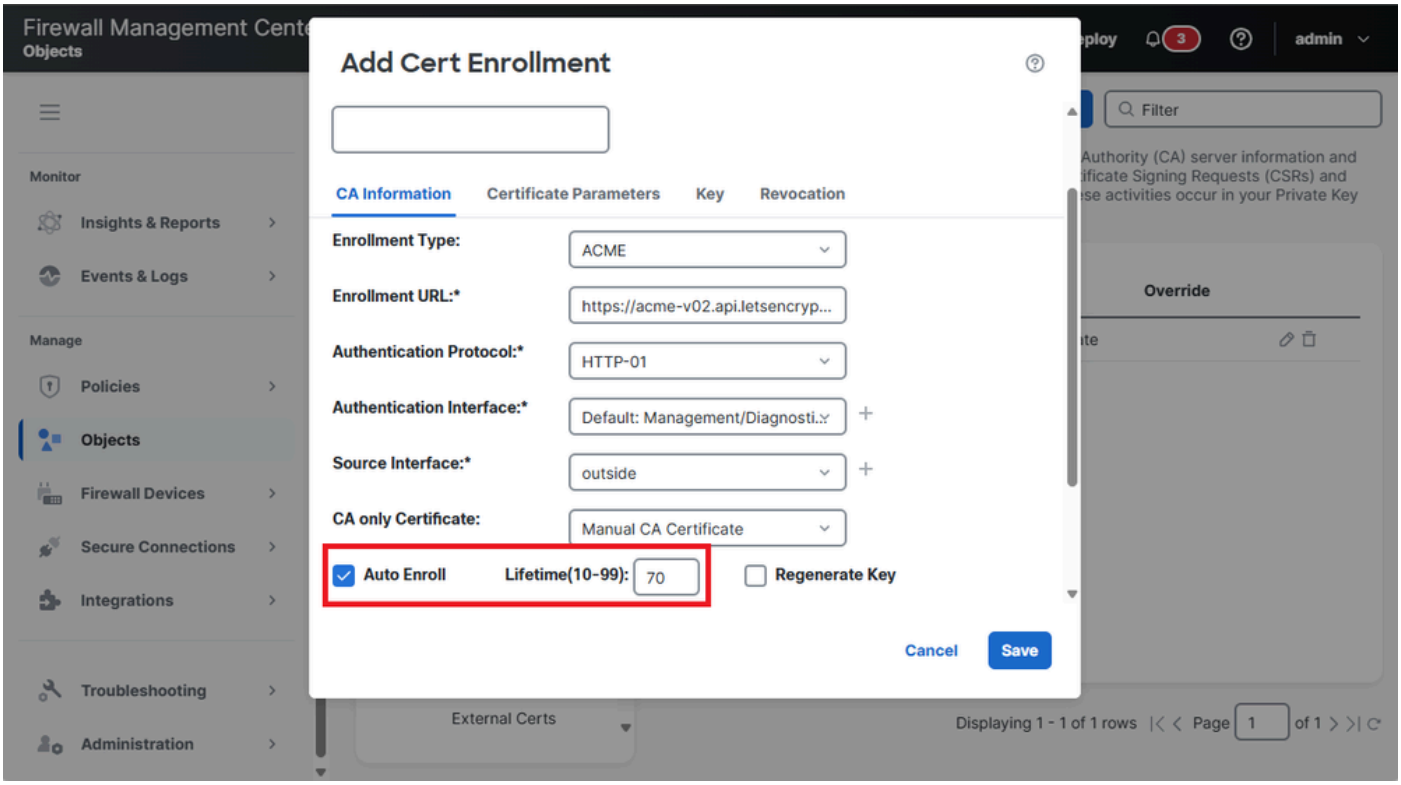


7. (Optional) Aktivieren Sie die automatische Registrierung für das Identitätszertifikat.

Aktivieren Sie das Kontrollkästchen Automatische Anmeldung, und geben Sie den Prozentsatz für

die Lebensdauer der automatischen Anmeldung an.

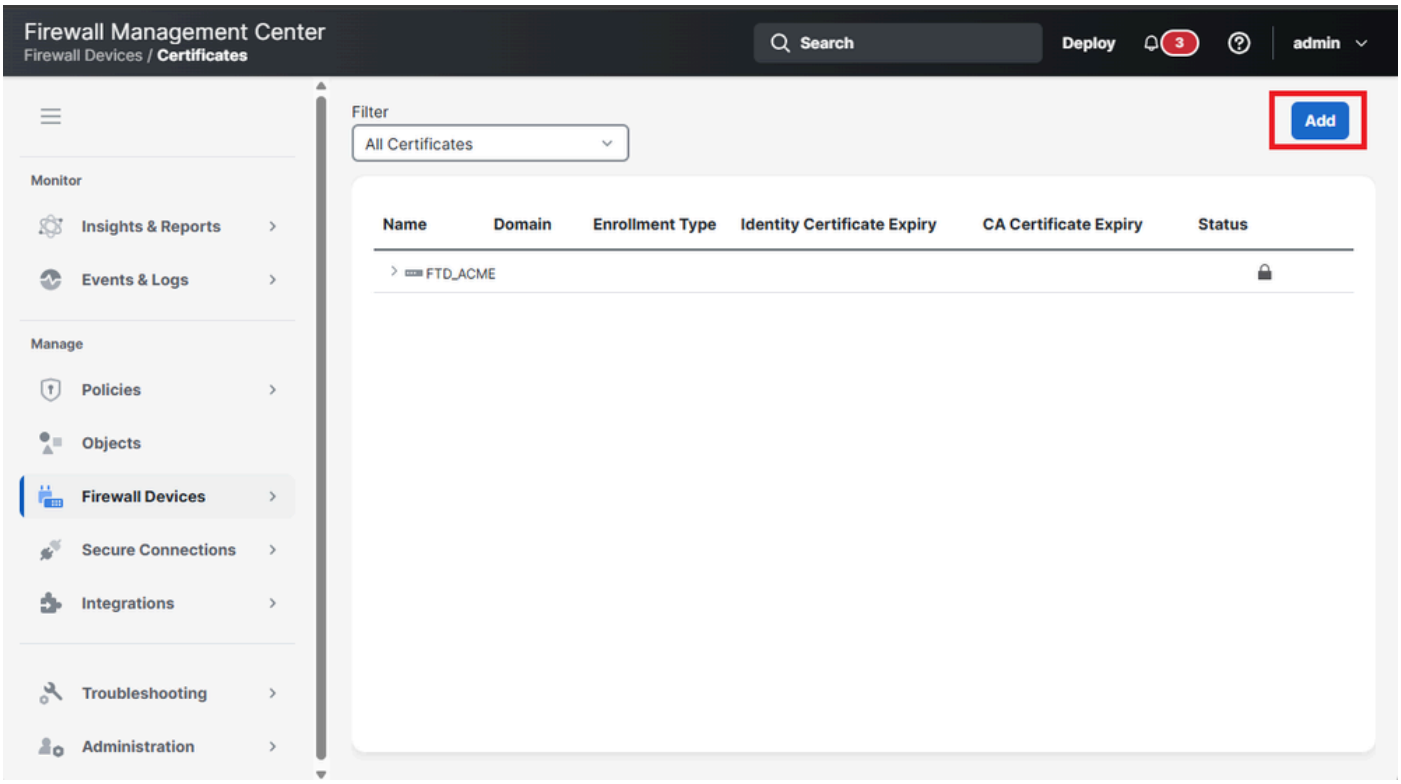
Mit dieser Funktion wird sichergestellt, dass das Zertifikat vor Ablauf automatisch erneuert wird. Der Prozentsatz bestimmt, wie weit der Verlängerungsprozess vor Ablauf des Zertifikats beginnt. Wenn Sie beispielsweise einen Wert von 80 % festlegen, beginnt der Verlängerungsprozess, wenn das Zertifikat 80 % seiner Gültigkeitsdauer erreicht hat.



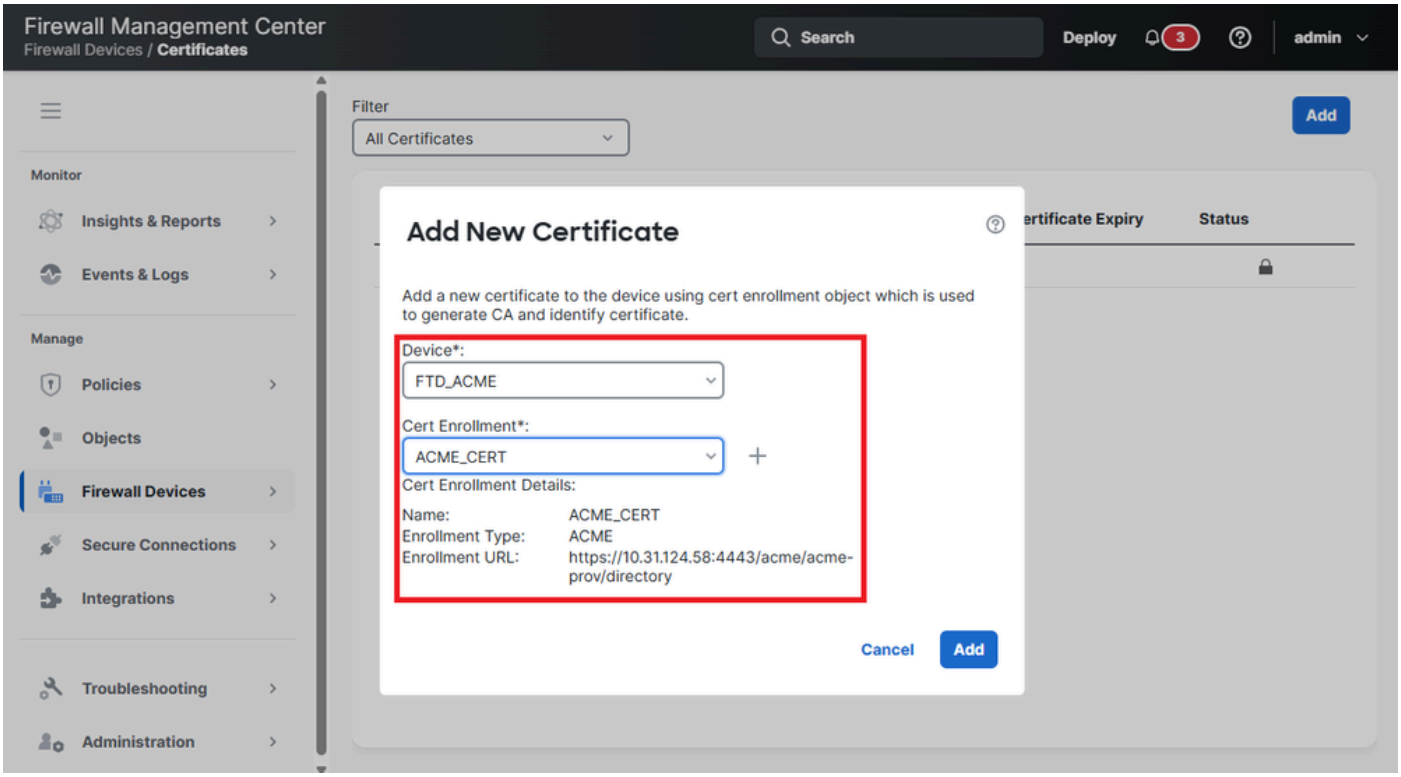
8. Klicken Sie auf Speichern.

ACME-Zertifikatregistrierung auf dem Gerät

1. Navigieren Sie zu Firewall Devices > Certificates (Firewall-Geräte > Zertifikate), und klicken Sie auf die Schaltfläche Add (Hinzufügen), um ein neues Zertifikat zu registrieren.



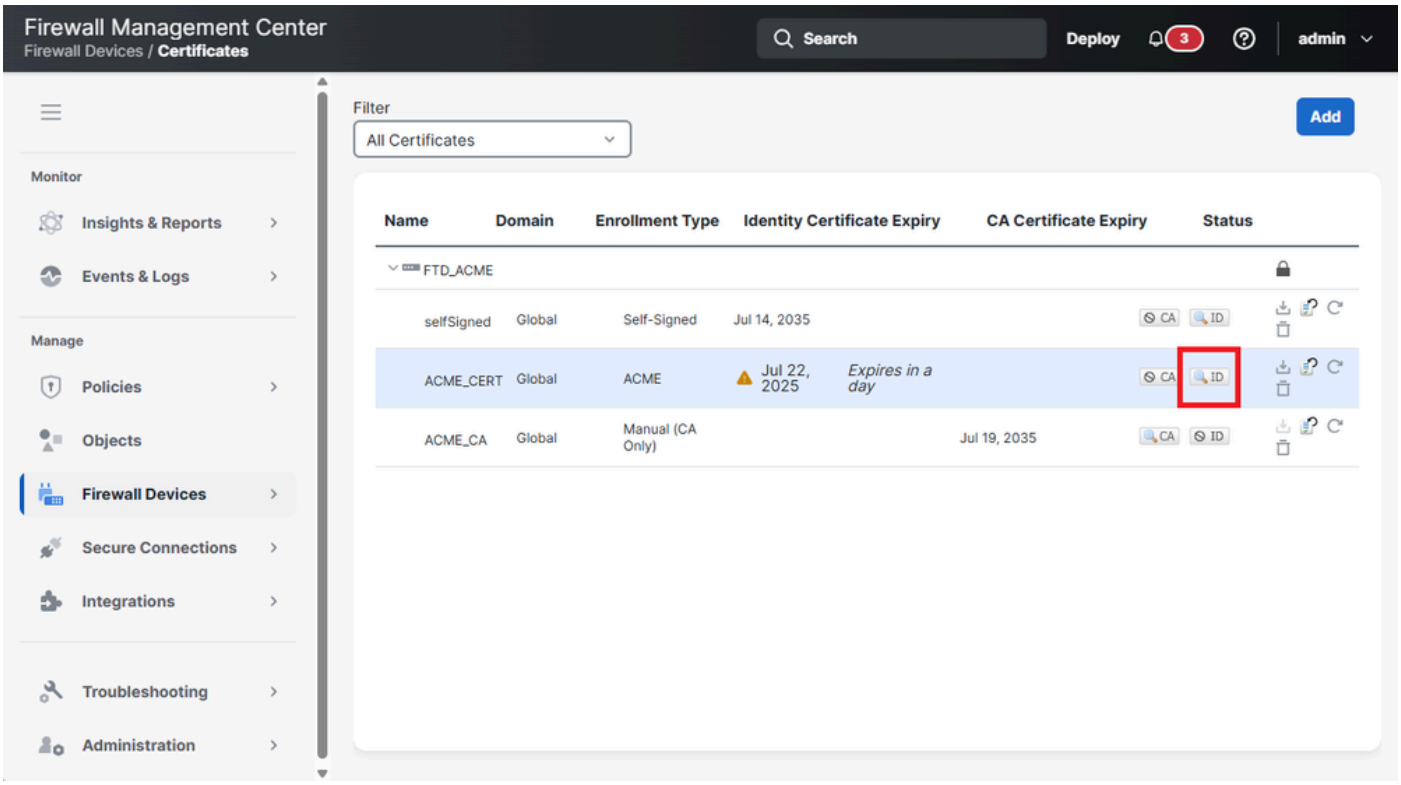
2. Wählen Sie das FTD-Gerät aus der Dropdown-Liste Gerät und das zuvor unter Zertifikatregistrierung erstellte Zertifikatobjekt aus.



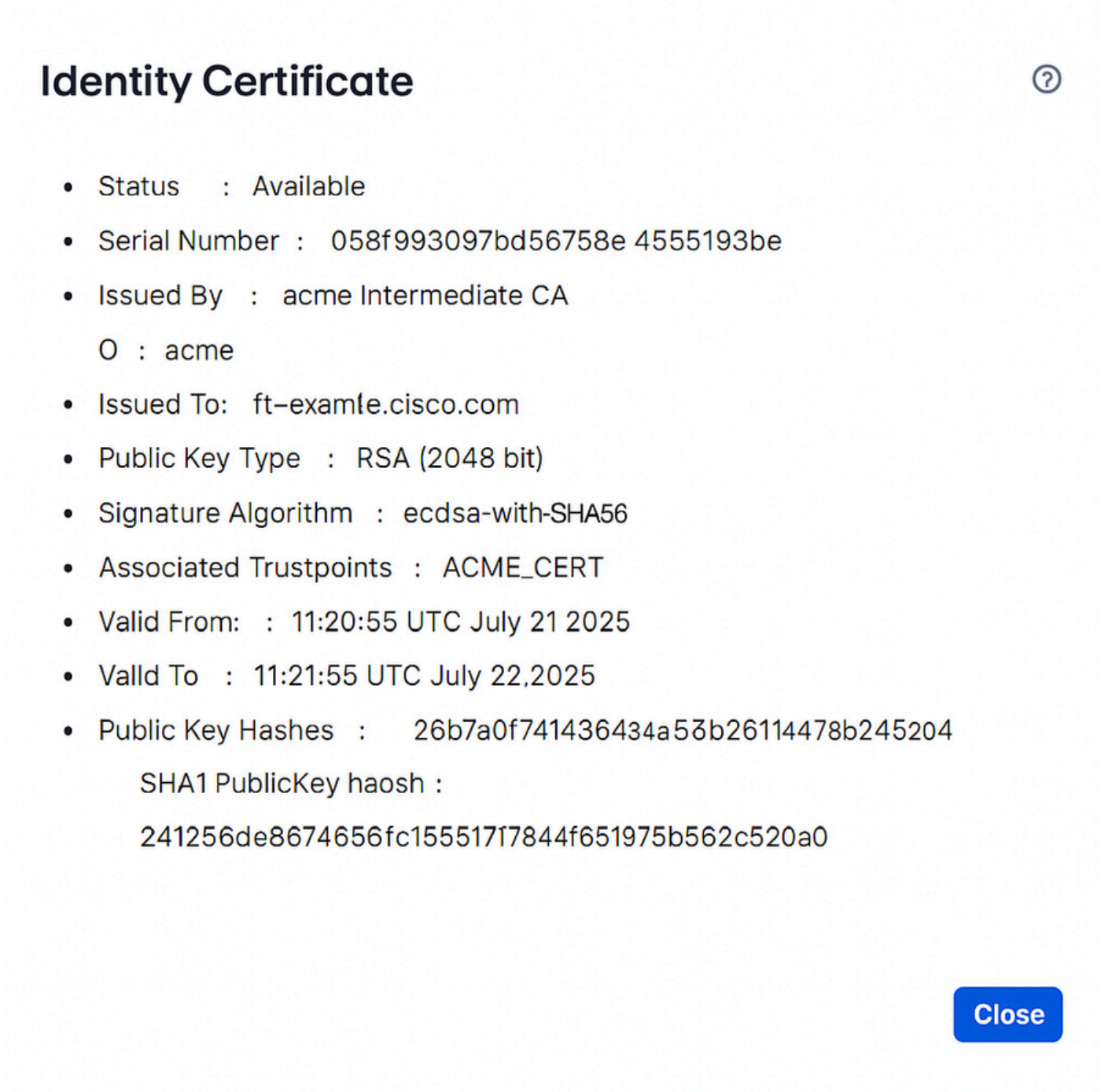
3. Klicken Sie auf Hinzufügen.

4. Nach Abschluss der Bereitstellung wird in der Statusspalte die Schaltfläche ID-Zertifikat

angezeigt.



5. Validieren Sie die ID-Zertifikatinformationen, indem Sie auf die Schaltfläche ID klicken.



Überprüfung

Installiertes Zertifikat in FTD anzeigen

Vergewissern Sie sich, dass das Zertifikat mit dem Befehl.show crypto ca Certificates <Name des Vertrauenspunkts> registriert ist.

<#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-Ereignisse

Die FTD der sicheren Firewall enthält neue Syslogs zur Erfassung von Ereignissen, die mit der Zertifikatsregistrierung unter Verwendung des ACME-Protokolls zusammenhängen:

- 717067: Enthält Informationen zum Zeitpunkt des Beginns der ACME-Zertifikatregistrierung.

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

- 717068: Stellt Informationen zum Zeitpunkt der erfolgreichen ACME-Zertifikatregistrierung bereit.

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

- 717069: Enthält Informationen über den Fall, dass die ACME-Registrierung fehlschlägt.

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

- 717070: Stellt Informationen bereit, die sich auf das Tastenpaar für die Zertifikatregistrierung oder die Zertifikatverlängerung beziehen.

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

Fehlerbehebung

Wenn die Registrierung eines ACME-Zertifikats fehlschlägt, überlegen Sie sich die nächsten Schritte zur Identifizierung und Behebung des Problems:

- Verbindung zum Server überprüfen:Bestätigen Sie, dass die sichere Firewall über eine Netzwerkverbindung zum ACME-Server verfügt. Stellen Sie sicher, dass keine Netzwerkprobleme auftreten oder die Kommunikation durch Firewall-Regeln blockiert wird.
- Stellen Sie sicher, dass der Secure Firewall-Domänenname auflösbar ist:Stellen Sie sicher, dass der auf der Secure Firewall FTD konfigurierte Domänenname vom ACME-Server auflösbar ist. Diese Verifizierung ist für den Server zur Validierung der Anfrage von entscheidender Bedeutung.
- Domänenbesitz bestätigen:Überprüfen Sie, ob alle im Vertrauenspunkt angegebenen Domänennamen der FTD der sicheren Firewall gehören. Dadurch wird sichergestellt, dass der ACME-Server das Domäneneigentum überprüfen kann.

Befehle zur Fehlerbehebung

Sammeln Sie für weitere Informationen die Ausgabe der nächsten Debugbefehle:

- debug crypto ca acme <1-255>
- debug crypto ca <1-14>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.