FMCによって管理されるセキュアファイアウォール脅威対策のACMEプロトコルでの証明書登録の設定

はじめに

このドキュメントでは、Secure Firewall Firepower Threat Defense(FTD)プラットフォーム上の自動証明書管理環境(ACME)プロトコルを使用してTransport Layer Security(TLS)証明書を登録するプロセスについて説明します。

前提条件

要 件

次の項目に関する知識が推奨されます。

- 手動による証明書登録プロセスとセキュアソケットレイヤ(SSL)の基礎
- リモートアクセスVPNの基本認証の概念。
- 認証局(CA)での経験

使用するコンポーネント

- Cisco FTDvバージョン10.0.0-35
- Cisco FMCバージョン10.0.0-35
- ACMEプロトコルをサポートする認証局(CA)サーバ。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

要件および制約事項

Secure Firewall FTDでのACME登録に関する現在の前提条件と制約は次のとおりです。

- FTDおよびFMCバージョン10.0.0以降でサポートされます。
- ACMEでは、ワイルドカード証明書の発行は許可されません。各証明書要求は、正確なドメイン名を指定する必要があります。
- ACME経由で登録された各トラストポイントは、単一のインターフェイスに制限されます。そのため、ACME経由で取得した証明書を複数のインターフェイスで共有することはできません。
- キーペアは自動的に生成され、ACME経由で登録された各証明書に固有です。これにより、キーの再利用が防止され、セキュリティが強化されます。

ダウングレードの考慮事項

ACME登録をサポートしていないセキュアファイアウォールFTDバージョン（バージョン7.7以前）にダウングレードする場合：

- バージョン10.0.0以降で導入されたACME関連のトラストポイント設定はすべて失われます。
- ACME経由で登録された証明書には引き続きアクセスできますが、最初に保存した後に秘密鍵の関連付けが解除され、ダウングレード後にリブートされます。

ダウングレードが必要な場合は、推奨される回避策を使用してください。

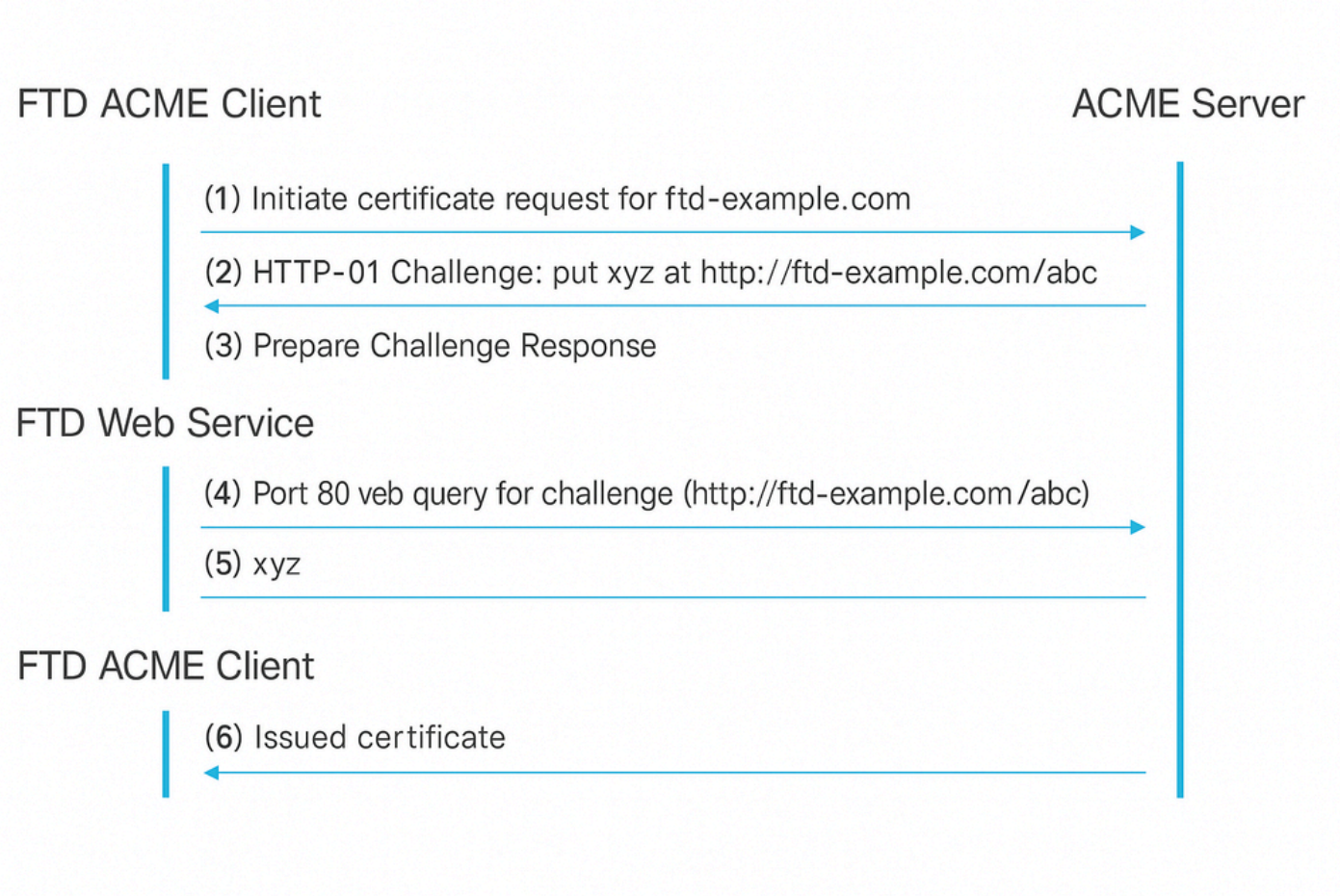
- ダウングレードする前に、ACME証明書をPKCS12形式でエクスポートしてください。
- ダウングレードする前に、ACMEトラストポイントの設定を削除してください。
- ダウングレード後、PKCS12証明書をインポートします。インポートされたトラストポイントは、ACME発行の証明書が期限切れになるまで有効です。

バックグラウンド情報

ACMEプロトコルの目的は、ネットワーク管理者向けのTLS証明書の管理を簡素化することです。ACMEを使用すると、管理者はTLS証明書の取得と更新に関連するタスクを自動化できます。この自動化は、ACMEプロトコルを介して無料で自動化された、一般にアクセス可能な証明書を提供するLet's Encryptなどの認証局(CA)と連携して作業する場合に特に役立ちます。ACMEは、ドメイン検証(DV)証明書の発行を促進します。これらの証明書は、証明書要求者が指定されたドメインを制御できることを確認します。検証は通常、HTTPベースのチャレンジプロセスを通じて行われ、申請者は指定されたファイルをWebサーバに配置します。認証局(CA)は、ドメインのHTTPサーバを介してこのファイルにアクセスし、ドメイン制御を確認します。このチャレンジに合格すると、CAはDV証明書を発行できるようになります。

登録プロセスには次の手順が含まれます。

1. 証明書要求の開始：クライアントは、証明書が必要なドメインを指定して、証明書要求をACMEサーバに送信します。
2. Receive HTTP-01 Challenge:ACMEサーバは、クライアントがドメイン所有権を証明するために使用する必要がある一意のトークンを含むHTTP-01チャレンジで応答します。
3. 課題への対応準備:
    1. クライアントは、ACMEサーバからのトークンとアカウントキーを組み合わせてキー認証を生成します。
    2. クライアントは、特定のURLパスでこのキー許可を提供するようにWebサーバを設定します。
4. ACMEサーバがチャレンジを取得：ACMEサーバは、指定されたURLに対してHTTP GET要求を実行して、キー認可を取得します。
5. ACMEサーバが所有権を確認：サーバは、取得したキー許可を期待値と比較して、ドメインに対するクライアントの制御を確認します。
6. 証明書の発行：検証が成功すると、ACMEサーバはSSL/TLS証明書をクライアントに発行します。



ACME登録HTTP-01認証フロー。

ACMEプロトコルを使用してセキュアファイアウォールFTDにTLS証明書を登録する主な利点は

次のとおりです。

- 証明書管理の自動化:ACMEは、Secure Firewall FTD TLSインターフェイスのTLSドメイン証明書の取得と維持のプロセスを合理化し、手動の管理タスクを大幅に削減します。
- 証明書の自動更新:ACME対応のトラストポイントを使用すると、証明書は有効期限が近づくにつれて自動的に更新されるため、継続的な管理介入の必要性が最小限に抑えられます。
- 継続的なセキュリティ保証：この自動化により、証明書が中断されることなく有効であり続け、予期しない証明書の期限切れを防ぎ、安全な通信を維持します。

これらの利点を組み合わせることで、セキュアなファイアウォールFTD導入の運用効率とセキュリティが向上します。

設定

前提条件の設定

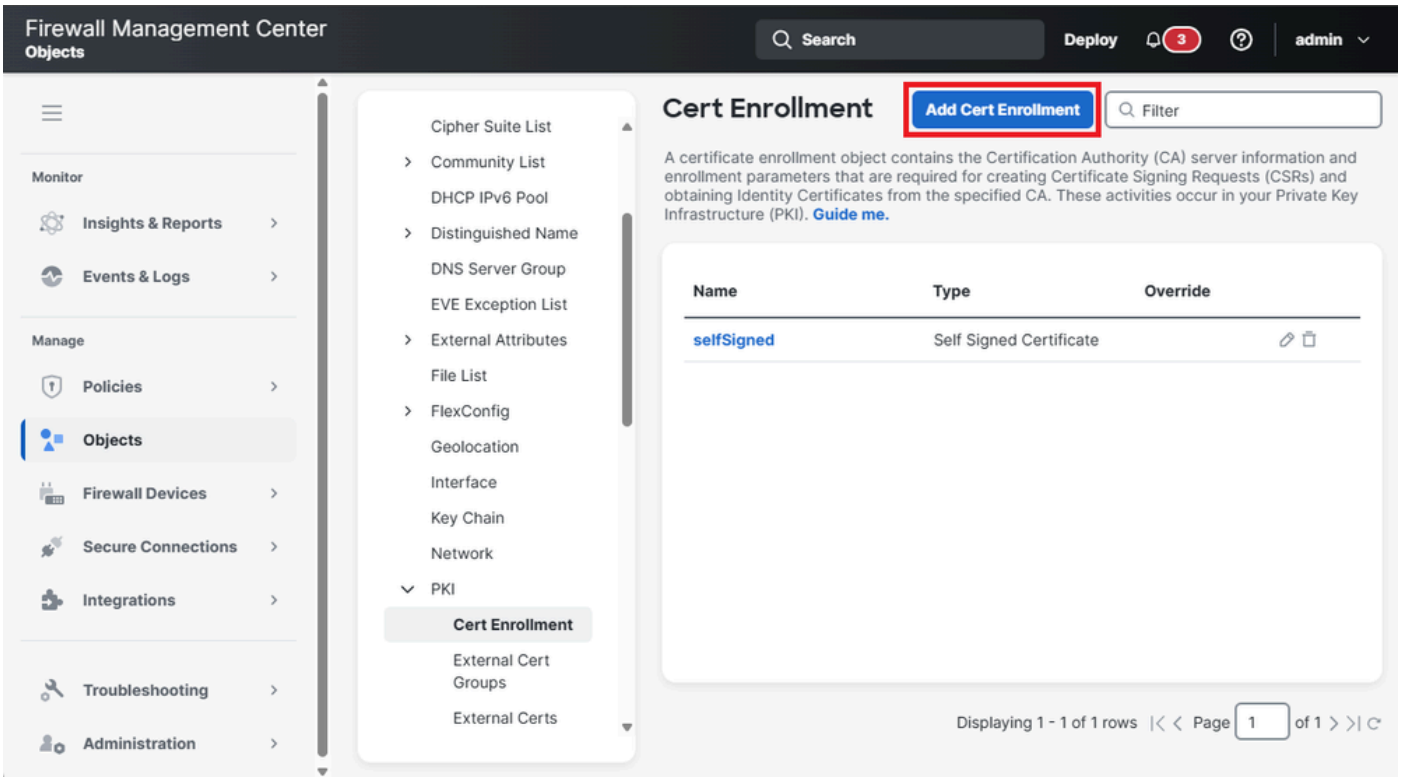
ACME登録プロセスを開始する前に、次の条件が満たされていることを確認します。

1. 解決可能なドメイン名：証明書を要求するドメイン名は、ACMEサーバで解決可能である必要があります。これにより、サーバはドメインの所有権を確認できます。
2. Secure Firewall Access to ACME Server:セキュアファイアウォールには、インターフェイスの1つを介してACMEサーバにアクセスする機能が必要です。このアクセスは、証明書が要求されるインターフェイスを経由する必要はありません。
3. TCP Port 80 Availability:ACME CAサーバからドメイン名に対応するインターフェイスへのTCPポート80の接続を許可します。これは、ACME交換プロセス中にHTTP-01チャレンジを完了するために必要です。

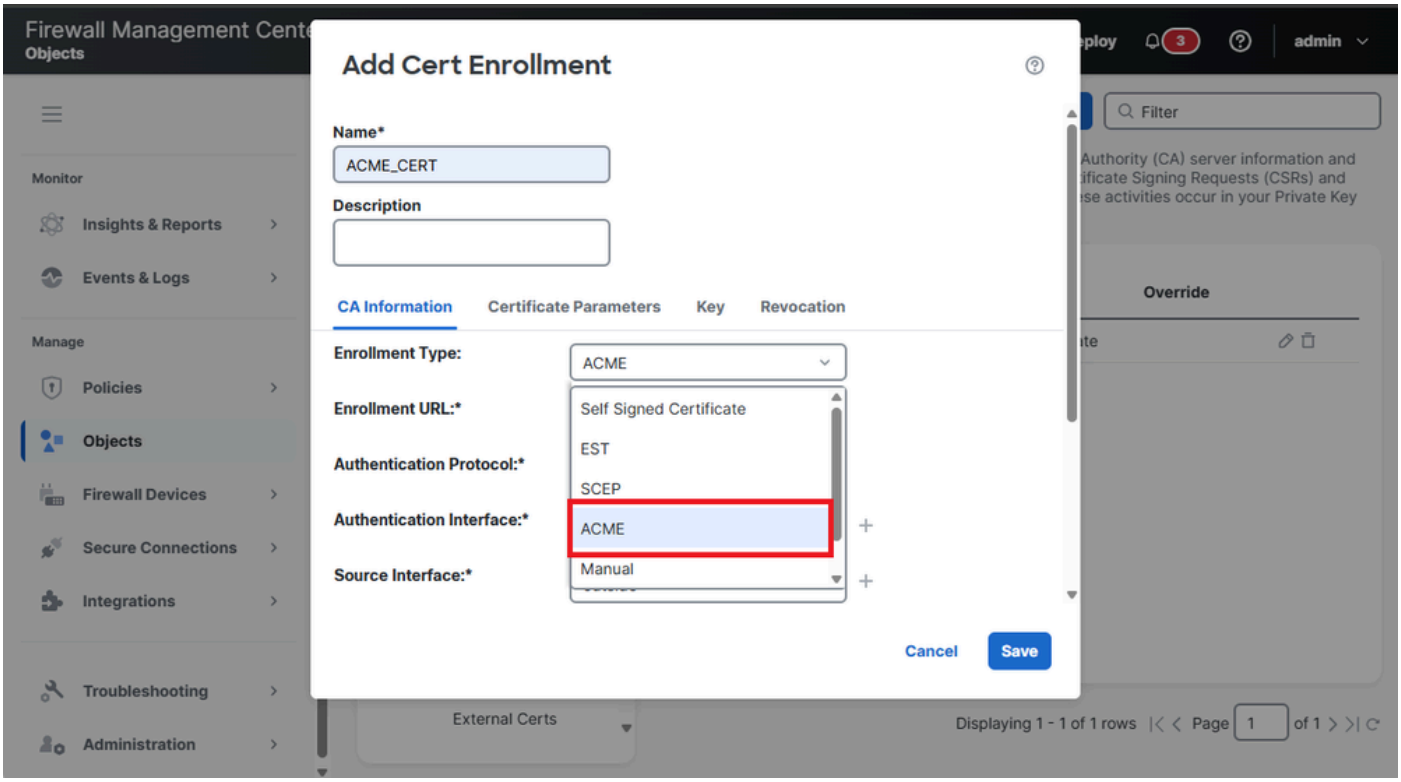
注：ポート80が開いている間は、ACMEチャレンジデータのみにアクセスできます。

ACME証明書登録オブジェクトの作成

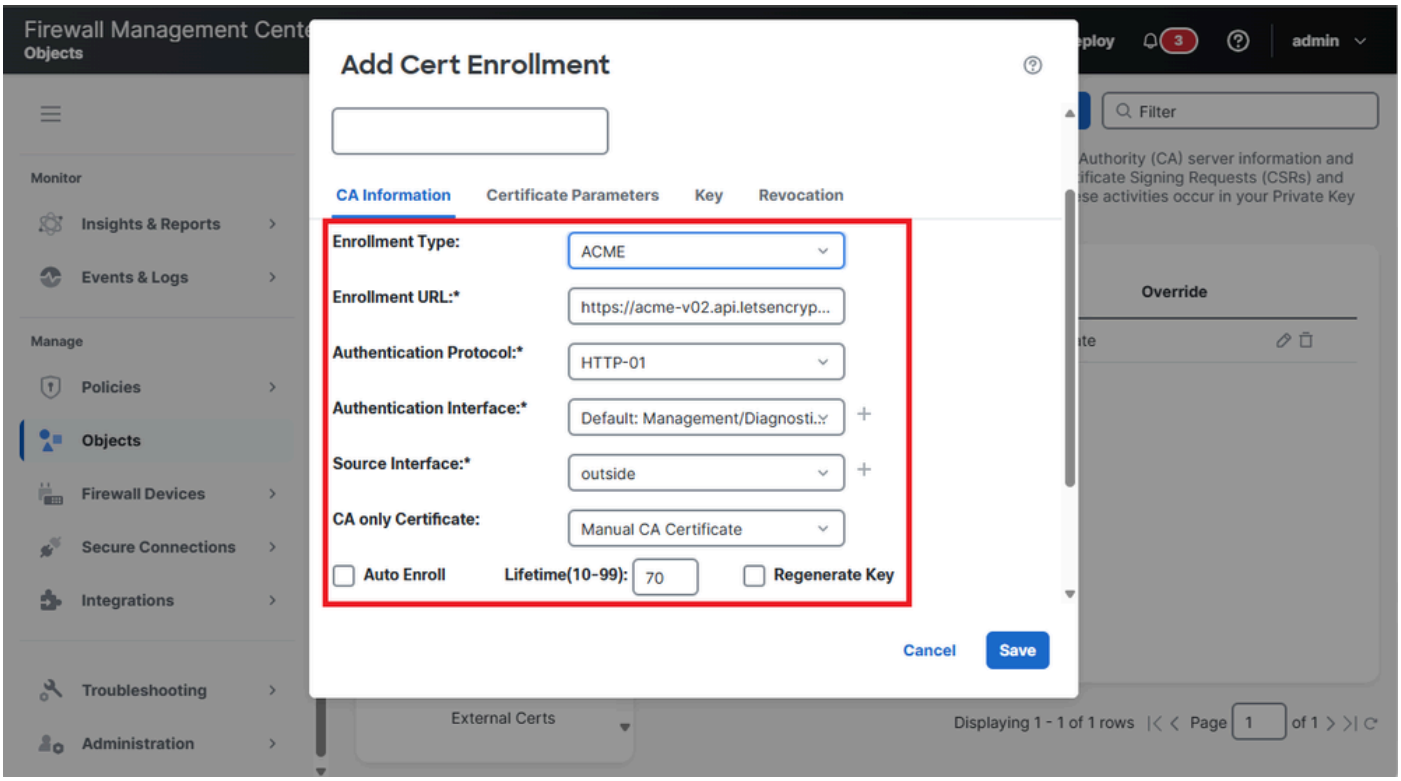
1. Objects > PKI > Cert Enrollmentの順に移動し、Add Cert Enrollmentをクリックして設定プロセスを開始します。



2. ACME登録オプションが、他の登録方法とともにドロップダウンメニューに表示されます。Enrollment Typeドロップダウンから**ACME**を選択して続行します。



3. 証明書パラメータの構成オプションが表示されます。フィールドに適切な情報を入力します。

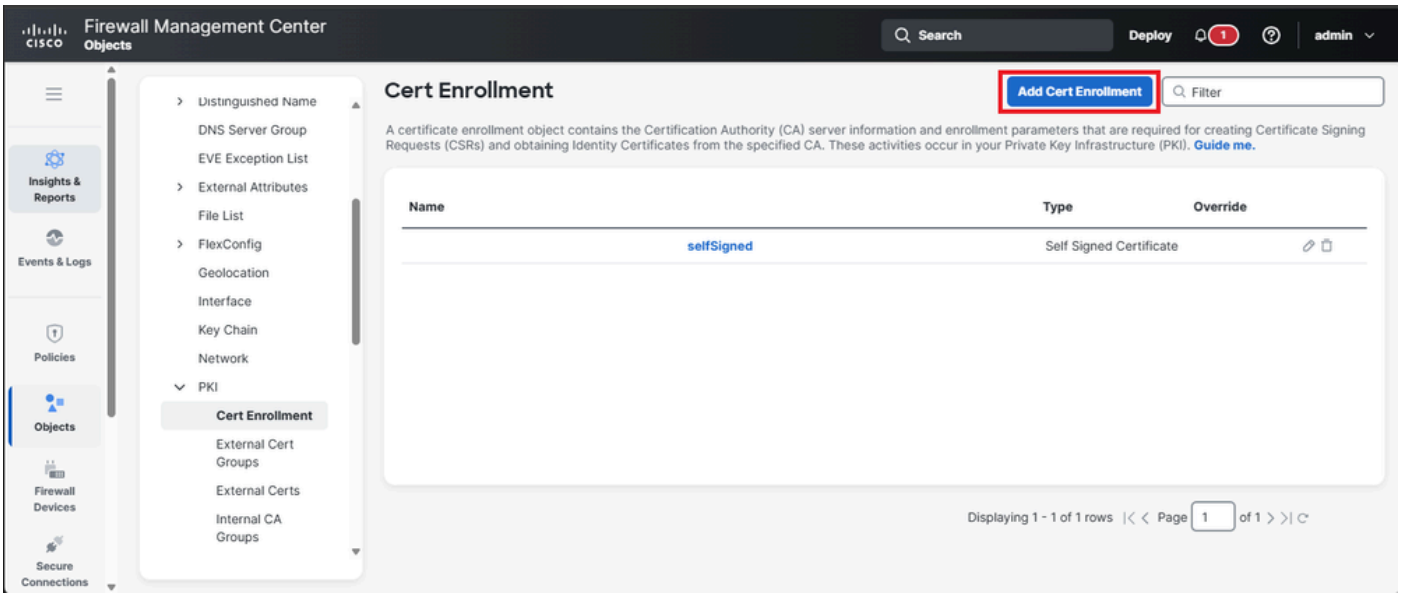


- Enrollment URL：証明書の要求と取得に使用するACMEサーバのアドレス(Let's Encryptなど)。
- 認証プロトコル：ドメインの所有権を確認するために使用する方法を指定します。ACMEの課題でサポートされるプロトコルはHTTP-01です。
- 認証インターフェイス:ACMEサーバからHTTP-01チャレンジを受信するFTDデバイスのネットワークインターフェイスです。
- CAのみの証明書:ACMEサーバを信頼するための認証局(CA)からの証明書を選択する必要があります。

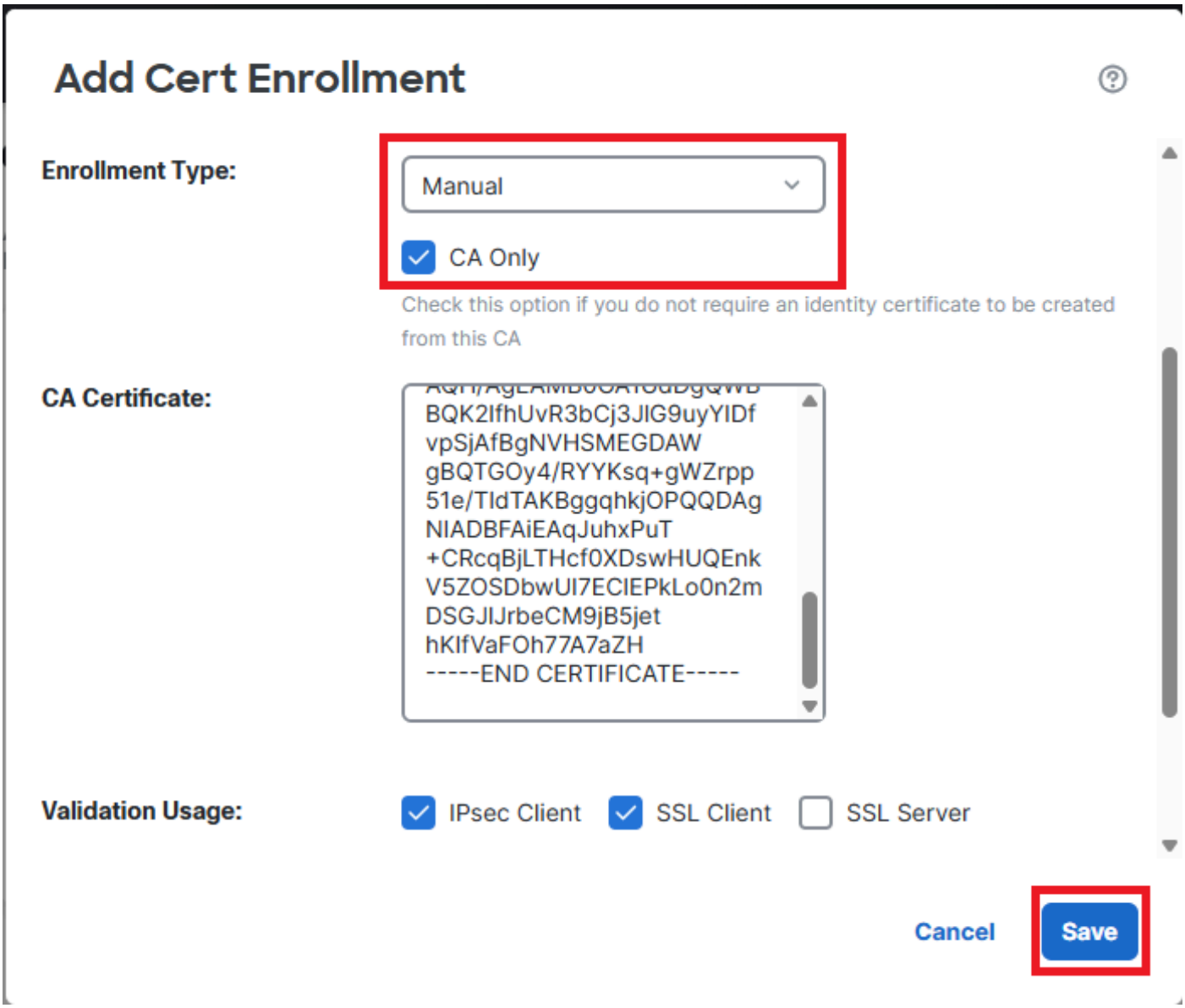
注：デフォルトでは、パブリックのLet's EncryptサービスURL(https://acme-v02.api.letsencrypt.org/directory)を指します。

---

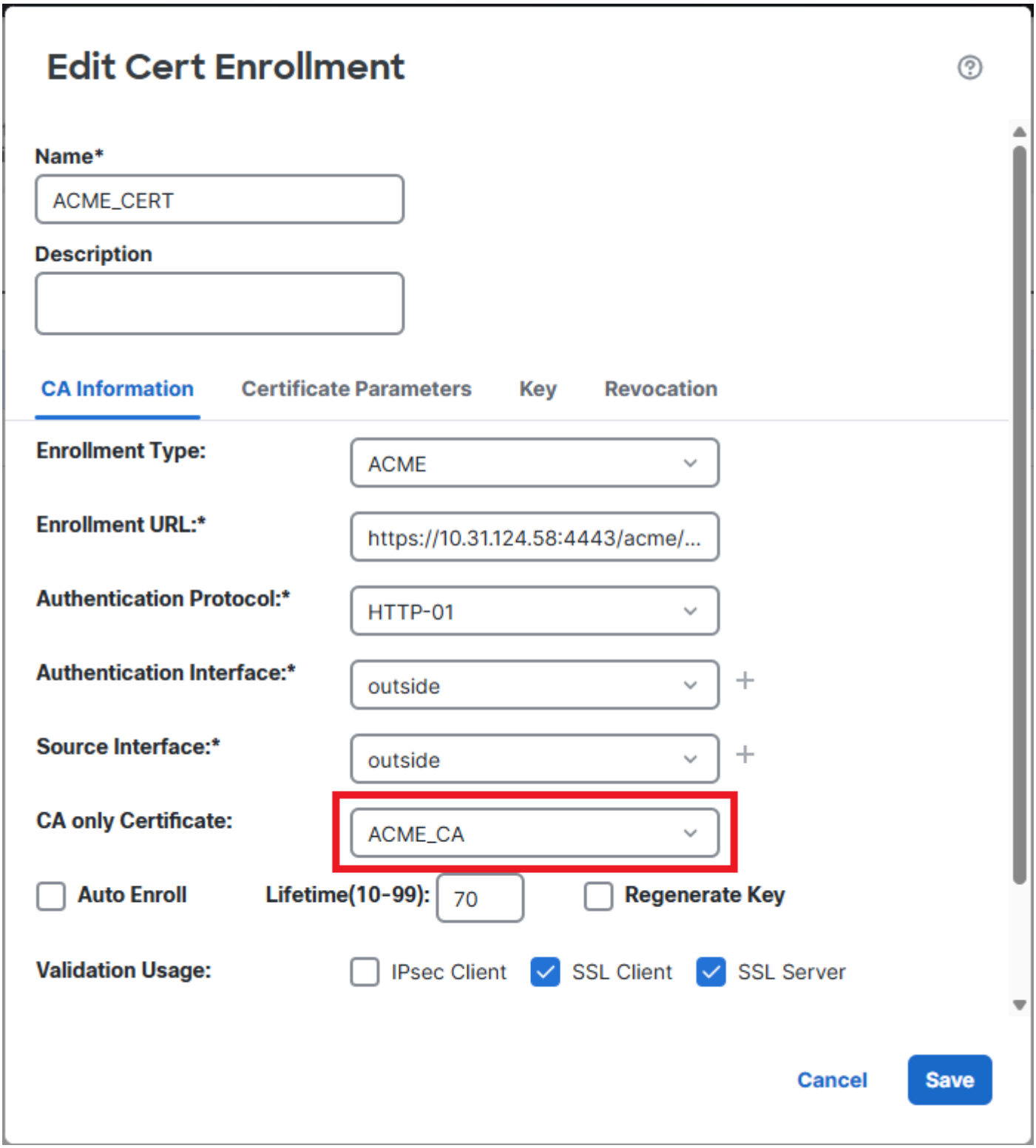
4. よく知られていないACMEサーバを使用している場合、ACMEサーバのCA証明書を追加する必要があります。Objects > Cert Enrollmentの順に移動し、Add Cert Enrollmentボタンをクリックします。



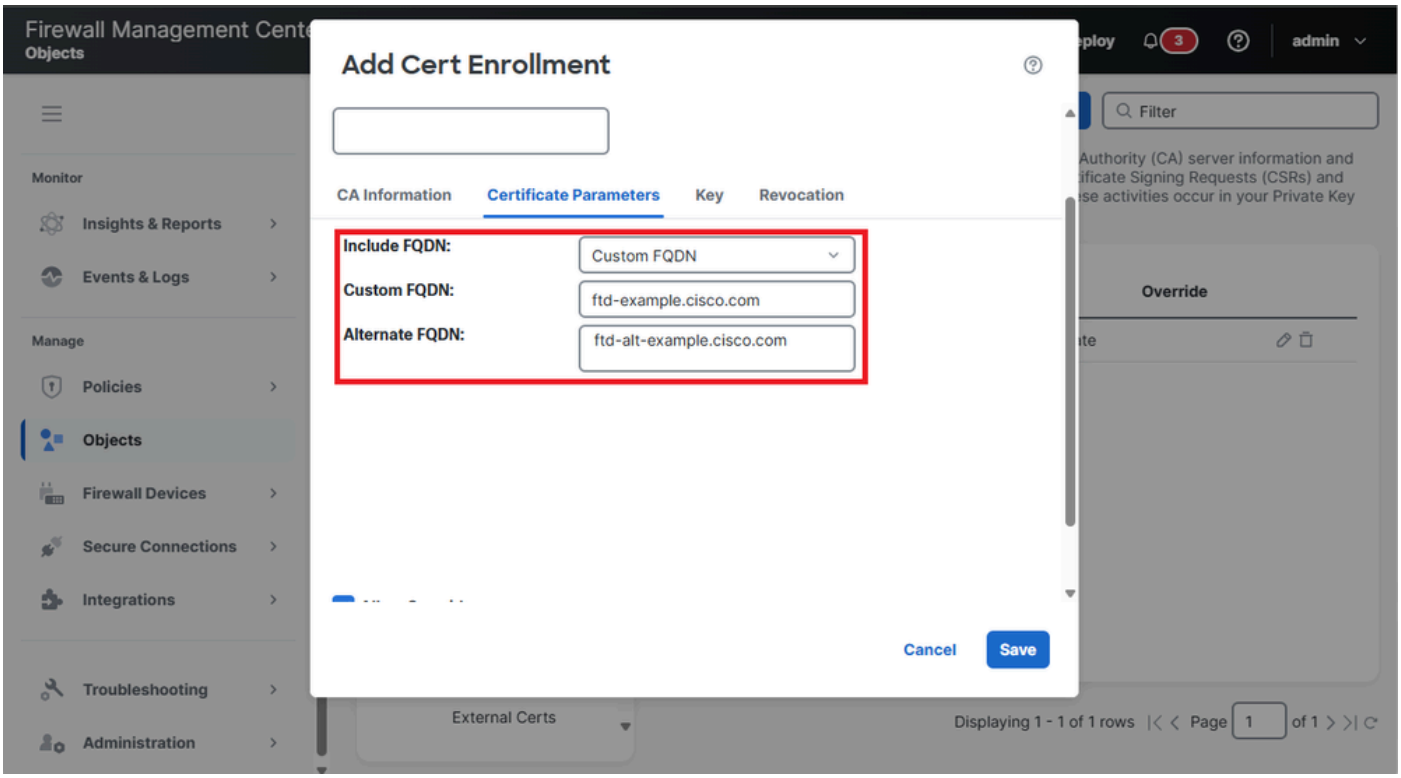
- トラストポイントに名前を付け、登録タイプとしてManualを選択します。次に、CA Onlyオプションにチェックマークを付けます。最後に、ACMEサーバのCA証明書を貼り付け、Saveをクリックします。



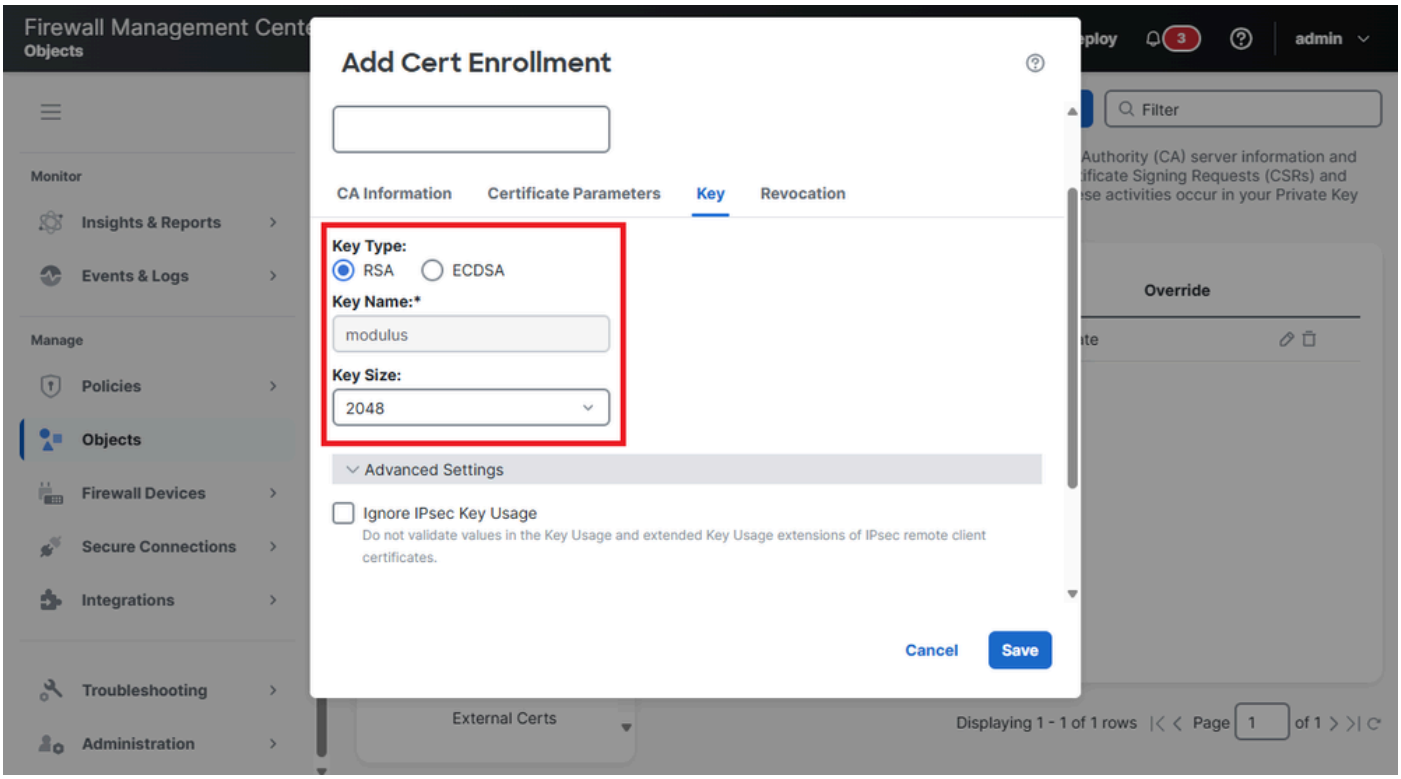
- 最後に、CA Only Certificateセクションで ACME CAサーバのトラストポイントを選択します。



5. Certificate Parametersに移動し、Include FQDNボックスでCustom FQDNオプションを選択し、Custom FQDNおよびAlternate FQDNフィールドに証明書に含めるプライマリFQDNと代替ドメイン名を入力します。



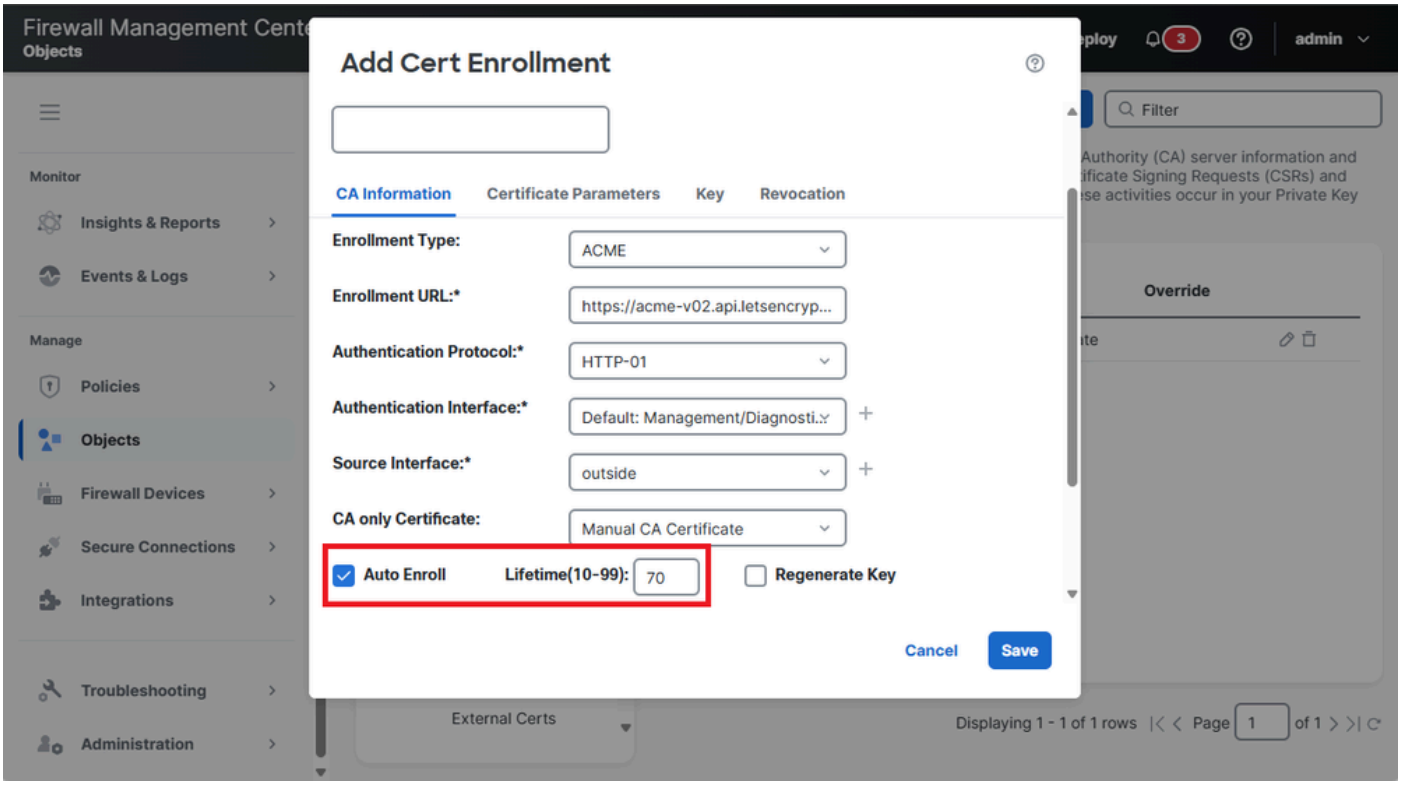
6. Keyに移動して、Key TypeとKey Sizeの設定を変更します。



7.（オプション）ID証明書の自動登録を有効にします。

Auto Enrollsチェックボックスをオンにして、Auto Enroll Lifetimeのパーセンテージを指定します。

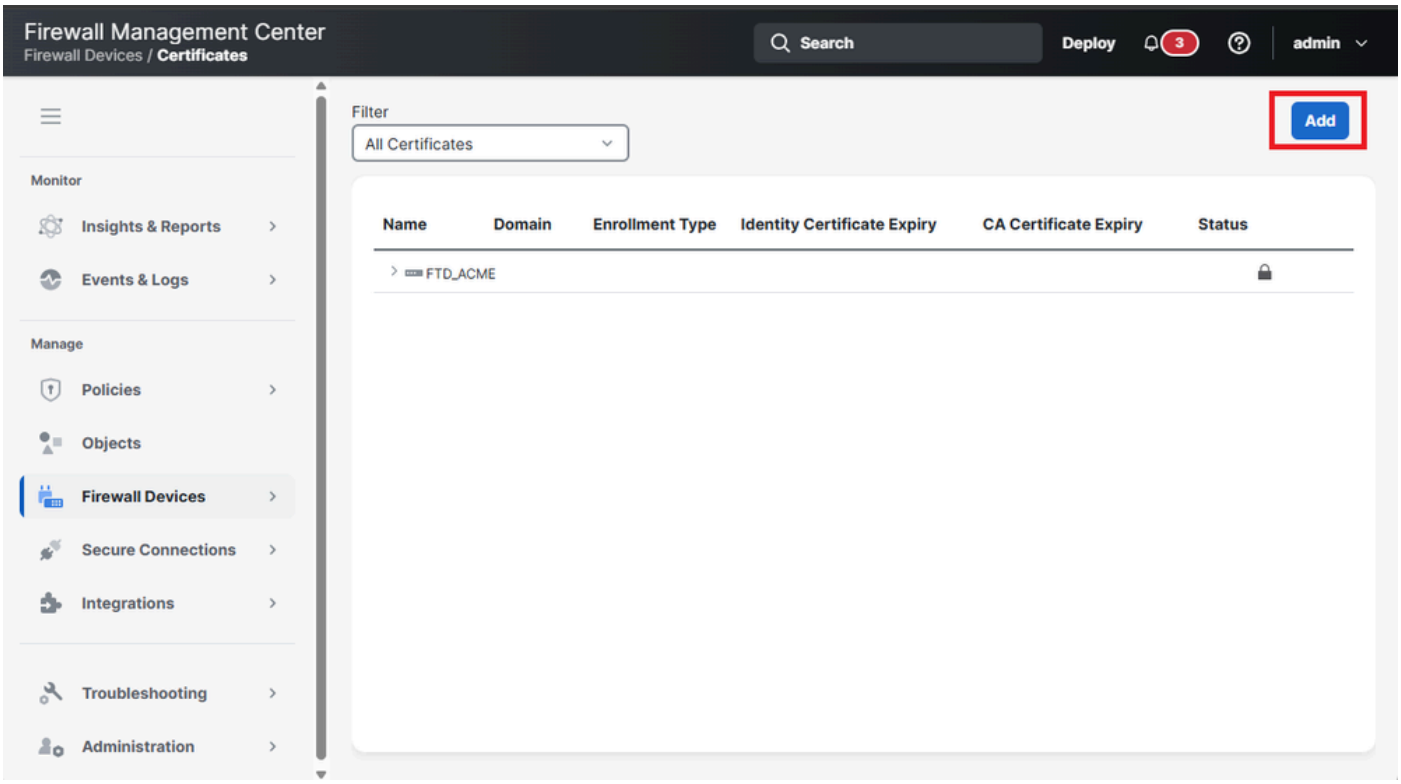
この機能により、証明書が期限切れになる前に自動的に更新されます。この割合によって、証明書の有効期限が切れる前に更新プロセスが開始される程度が決まります。たとえば、80 %に設定すると、証明書が有効期間の80 %に達したときに更新プロセスが開始されます。



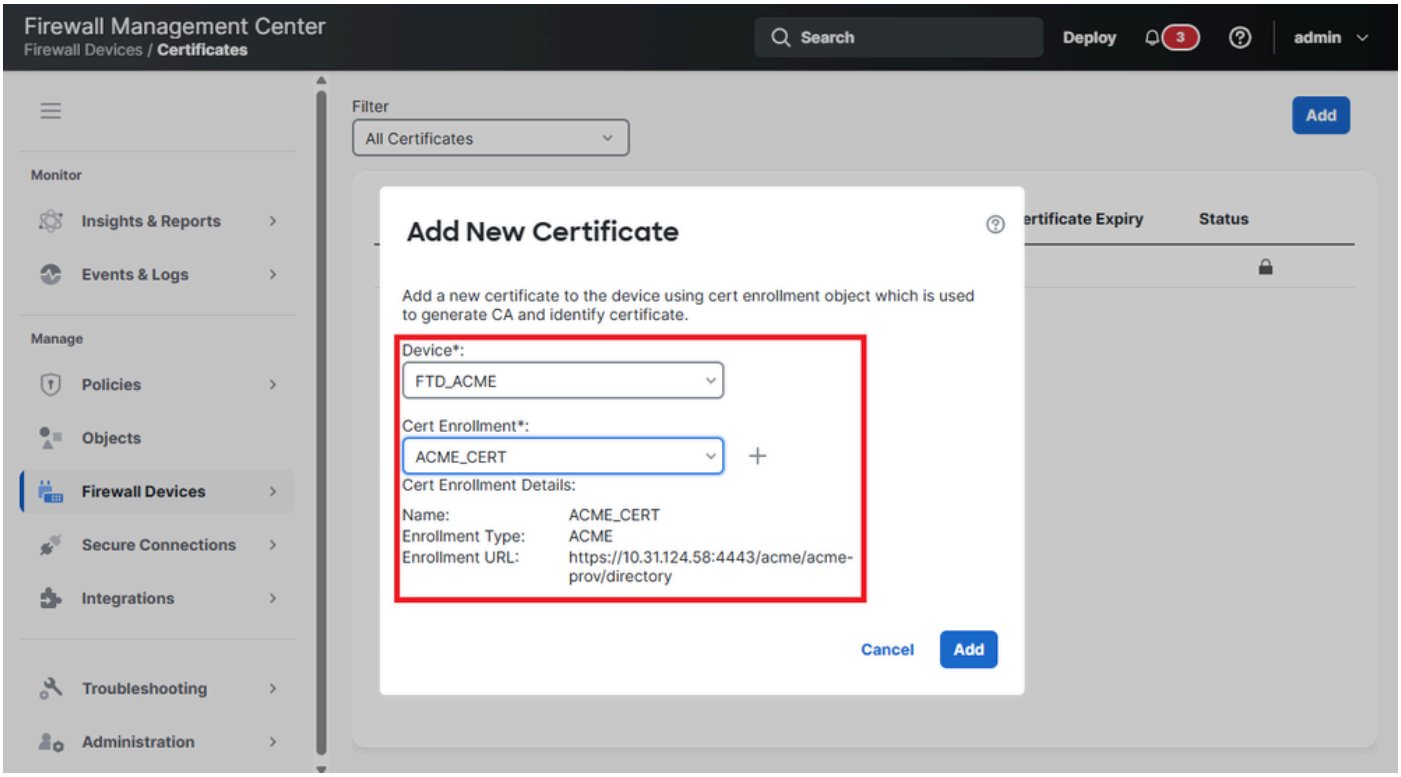
8. 「保存」をクリックします。

デバイスでのACME証明書の登録

1.Firewall Devices > Certificatesの順に移動し、Addボタンをクリックして新しい証明書を登録します。

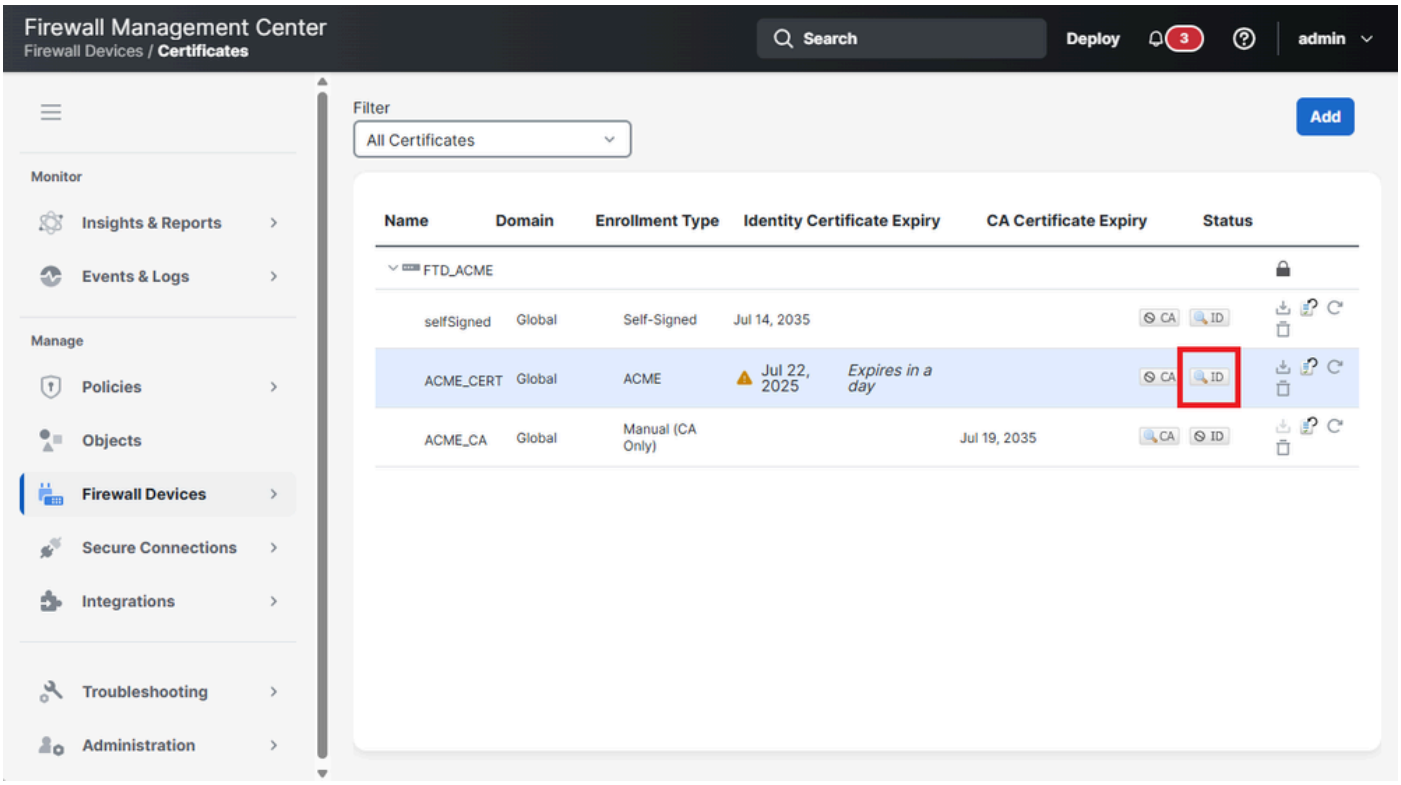


2. Deviceドロップダウンリストから FTDデバイスを選択し、証明書オブジェクトは前にCert Enrollmentで作成されています。

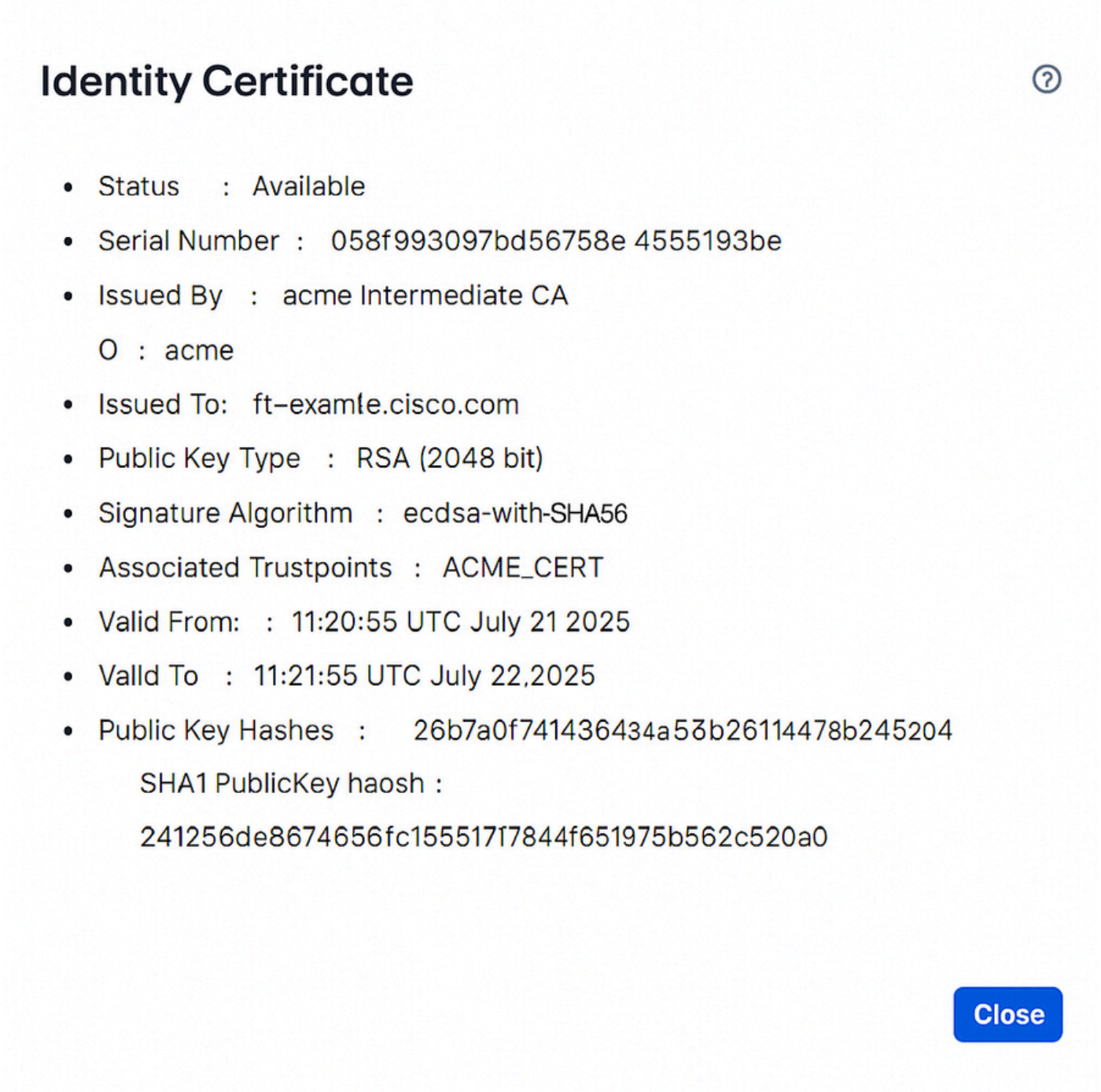


3. Addをクリックします。

4. デプロイが完了すると、ステータス列にID証明書ボタンが表示されます。



5. IDボタンをクリックして、ID証明書情報を検証します。



確認

FTDでインストールされた証明書を表示

コマンドshow crypto ca certificates <Trust Point Name>を使用して、証明書が登録されていることを確認します。

```
<#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 イベント

ACMEプロトコルを使用して証明書の登録に関連するイベントをキャプチャする、セキュアファイアウォールFTDの新しいsyslogがあります。

- 717067:ACME証明書登録が開始されるタイミングに関する情報を提供します。

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

- 717068:ACME証明書の登録が正常に行われた時点に関する情報を提供します。

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

- 717069:ACME登録が失敗した場合の情報を提供します。

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

- 717070：証明書の登録または証明書の更新に使用するキーペアに関する情報を提供します。

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

トラブルシュート

ACME証明書の登録が失敗した場合は、次の手順を検討して問題を特定し、解決します。

- サーバへの接続を確認します。セキュアファイアウォールにACMEサーバへのネットワーク接続があることを確認します。通信をブロックしているネットワークの問題やファイアウォール規則がないことを確認します。
- Secure Firewallのドメイン名が解決可能であることを確認します。Secure Firewall FTDに設定されているドメイン名が、ACMEサーバで解決可能であることを確認します。この検証は、サーバが要求を検証するために重要です。
- ドメイン所有権の確認：トラストポイントで指定されたすべてのドメイン名が、Secure Firewall FTDによって所有されていることを確認します。これにより、ACMEサーバはドメインの所有権を検証できます。

トラブルシューティングのためのコマンド

詳細については、次のdebugコマンドの出力を収集します。

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。