セキュアファイアウォールでのACMEプロトコルによる証明書登録の設定

内容

はじめに

このドキュメントでは、セキュアファイアウォールASAで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あることが推奨されます。

- Ciscoセキュアファイアウォール適応型セキュリティアプライアンス(ASA)
- 公開キー インフラストラクチャ（PKI）

使用するコンポーネント

- Cisco ASAvバージョン9.23.1
- Cisco ASDM バージョン 7.23(1).
- 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ました。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

セキュアファイアウォールASAでのACME登録の現在の要件と制限は次のとおりです。

- ASAバージョン9.23.1およびASDM 7.23.1以降でサポート
- マルチコンテキストではサポートされない

- ACMEでは、ワイルドカード証明書の作成はサポートされていません。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。つまり、ACMEに登録された証明書は、複数のインターフェイスで共有できません。

- キーペアは自動的に生成され、ACMEを介して登録された証明書では共有できません。各証明書は一意のキーペアを使用し、セキュリティを強化しますが、キーの再利用は制限されます。

ダウングレードの考慮事項

Secure Firewall ASA（9.22以前）でACME登録をサポートしていないバージョンにダウングレードする場合：

- 9.23.x以降で新規のACME関連トラストポイント設定はすべて失われます
- ACMEを介して登録された証明書はアクセス可能なままですが、ダウングレード後の最初の保存とリブートの後に秘密キーの関連付けが解除されます

ダウングレードが必要な場合は、次の推奨回避策を実行してください。

1. ダウングレードする前に、ACME証明書をPKCS12形式で必ずエクスポートしてください。
2. 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。
3. ダウングレード後、PKCS12証明書をインポートします。結果として生じるトラストポイントは、ACME経由で発行された証明書が期限切れになるまで有効です。

背景説明

ACMEプロトコルは、ネットワーク管理者のTLS証明書の管理を合理化するように設計されています。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プロセスを自動化できます。この自動化は、ACMEプロトコルを使用して無料で自動化されたオープンな証明書を提供

するLet's Encryptなどの認証局(CA)を利用する場合に特に役立ちます。

ACMEは、ドメイン検証(DV)証明書の発行をサポートしています。これらの証明書は、特定のドメインに対する証明書保持者の制御を確認するデジタル証明書の一種です。DV証明書の検証プロセスは通常、HTTPベースのチャレンジメカニズムを通じて実行されます。このメカニズムでは、申請者はWebサーバに特定のファイルを配置します。このファイルは、ドメインのHTTPサーバを介してファイルにアクセスすることで、認証局(CA)によって検証されます。このチャレンジを正常に完了すると、申請者がドメインを制御し、DV証明書の発行を許可していることがCAに示されます。

登録を完了するプロセスは次のとおりです。

1. 証明書要求の開始：クライアントはACMEサーバに証明書を要求し、証明書が必要なドメインを指定します。
2. Receive HTTP-01 Challenge:ACMEサーバは、ドメイン制御を証明するためにクライアントが使用する一意のトークンを使用して、HTTP-01チャレンジを提供します。
3. チャレンジ応答の準備：
    - 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作成します。
    - 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要求を行い、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、取得したキー許可がドメイン経由でクライアントの制御を確認するために期待される値と一致するかどうかを確認します。
6. 証明書の発行：検証が成功すると、ACMEサーバが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TLS証明書を登録する最も関連性の高い利点は次のとおりです。

- ACMEは、セキュアファイアウォールASA TLSインターフェイスのTLSドメイン証明書の取得とメンテナンスを容易にします。この自動化により、手作業が大幅に削減され、継続的な監視なしで証明書を最新の状態に維持できます。
- ACME対応のトラストポイントを使用すると、証明書の有効期限が近づくと自動的に更新されます。この機能により、管理者の介入が必要なくなり、中断のないセキュリティが確保され、証明書の予期しない期限切れが防止されます。

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。

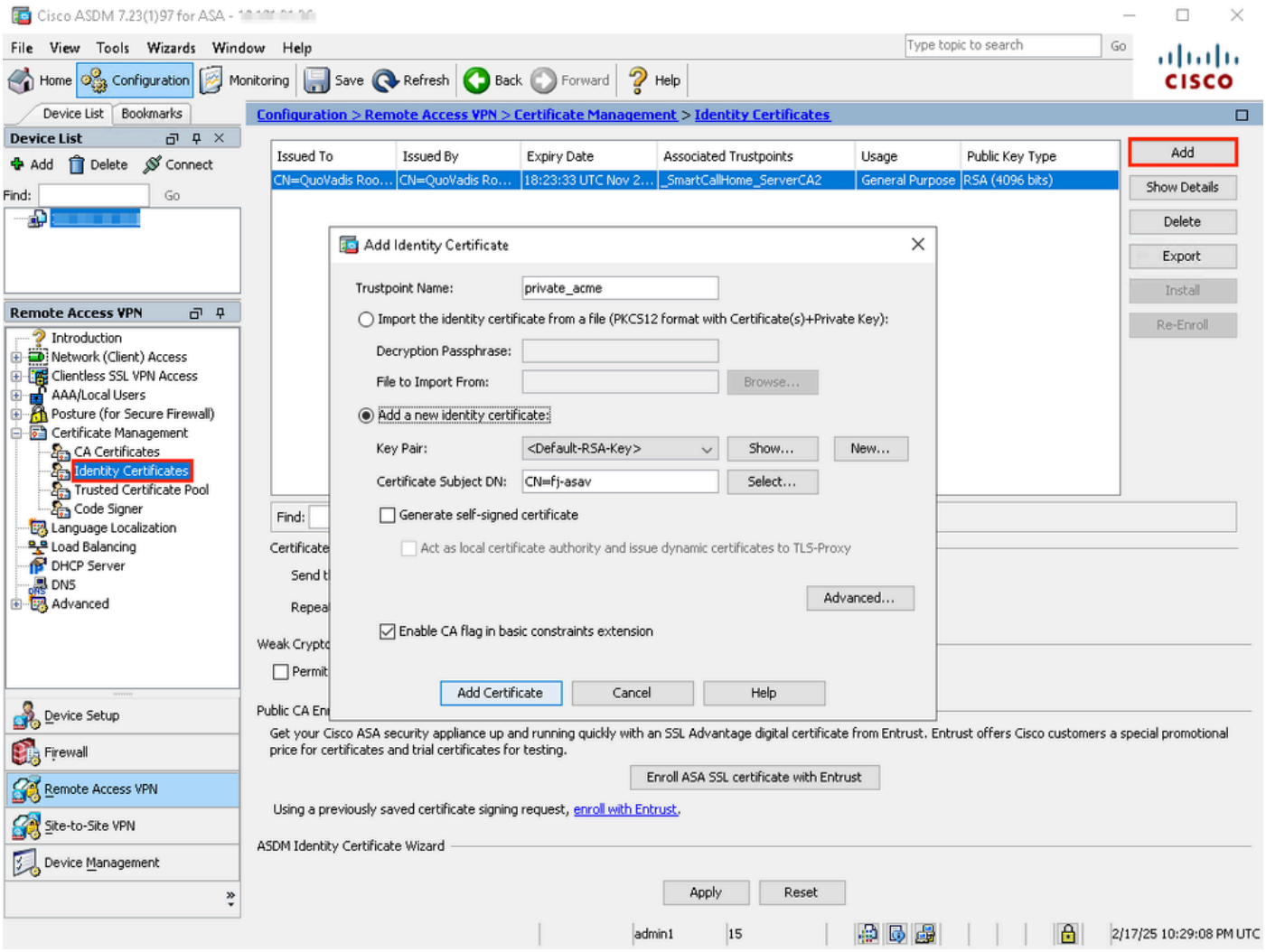
1. 解決可能なドメイン名：証明書を要求するドメイン名は、ACMEサーバで解決可能である必要があります。これにより、サーバはドメインの所有権を確認できます。
2. ACMEサーバへのセキュアなファイアウォールアクセス：セキュアファイアウォールには、インターフェイスの1つを介してACMEサーバにアクセスする機能が必要です。このアクセスは、証明書が要求されるインターフェイスを経由する必要はありません。
3. TCP Port 80 Availability:ACME CAサーバからドメイン名に対応するインターフェイスへのTCPポート80の接続を許可します。これは、ACME交換プロセス中にHTTP-01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

ASDMへのACME登録

1. 新しいID証明書を追加します。

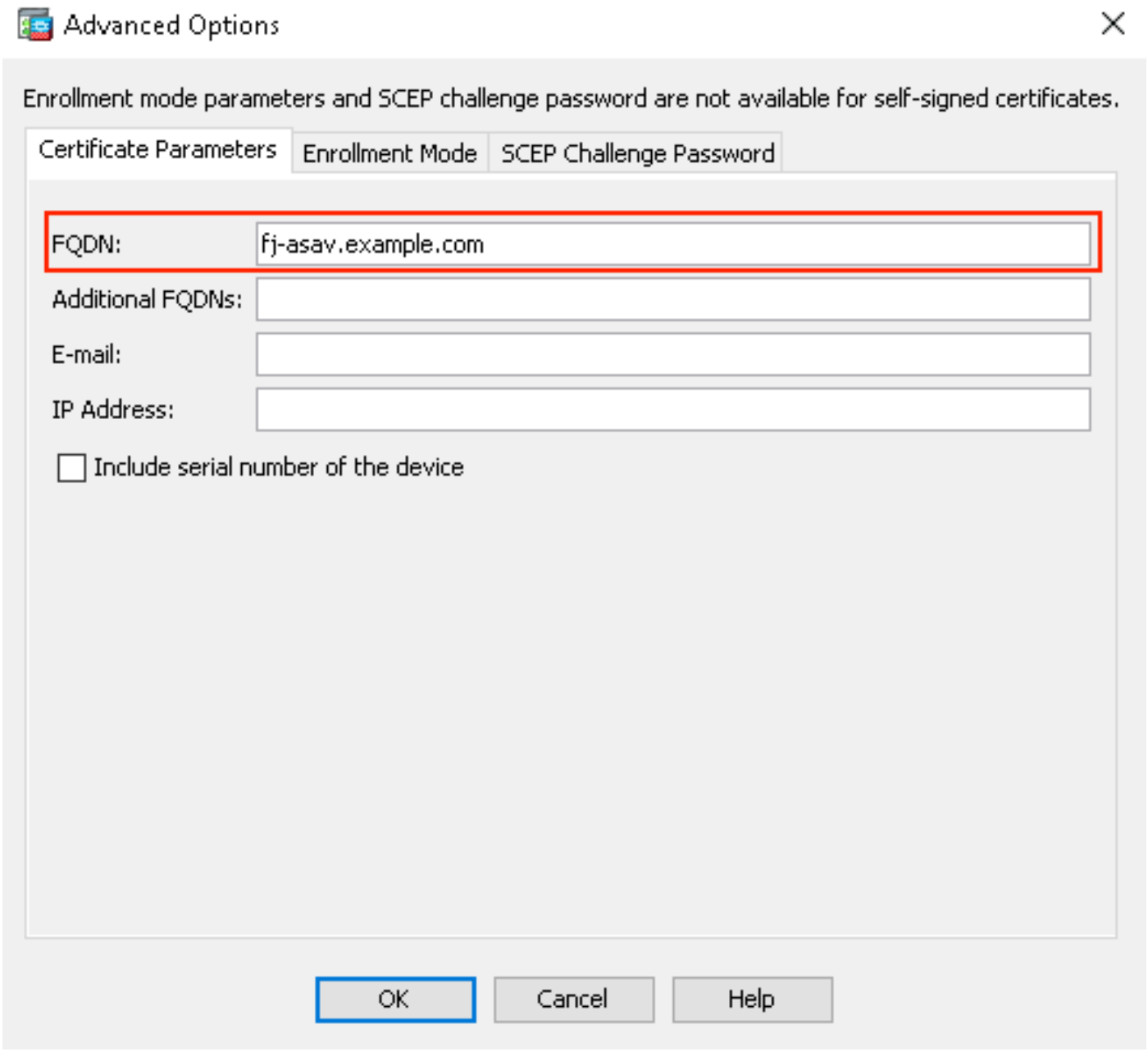
- Configuration > Remote Access VPN > Certificate Management > Identity Certificatesの順に移動します。
- Addボタンをクリックし、Add a new identity certificateを選択します。



ACME登録ASDM ID証明書。

2. ID証明書のFQDNを指定します。

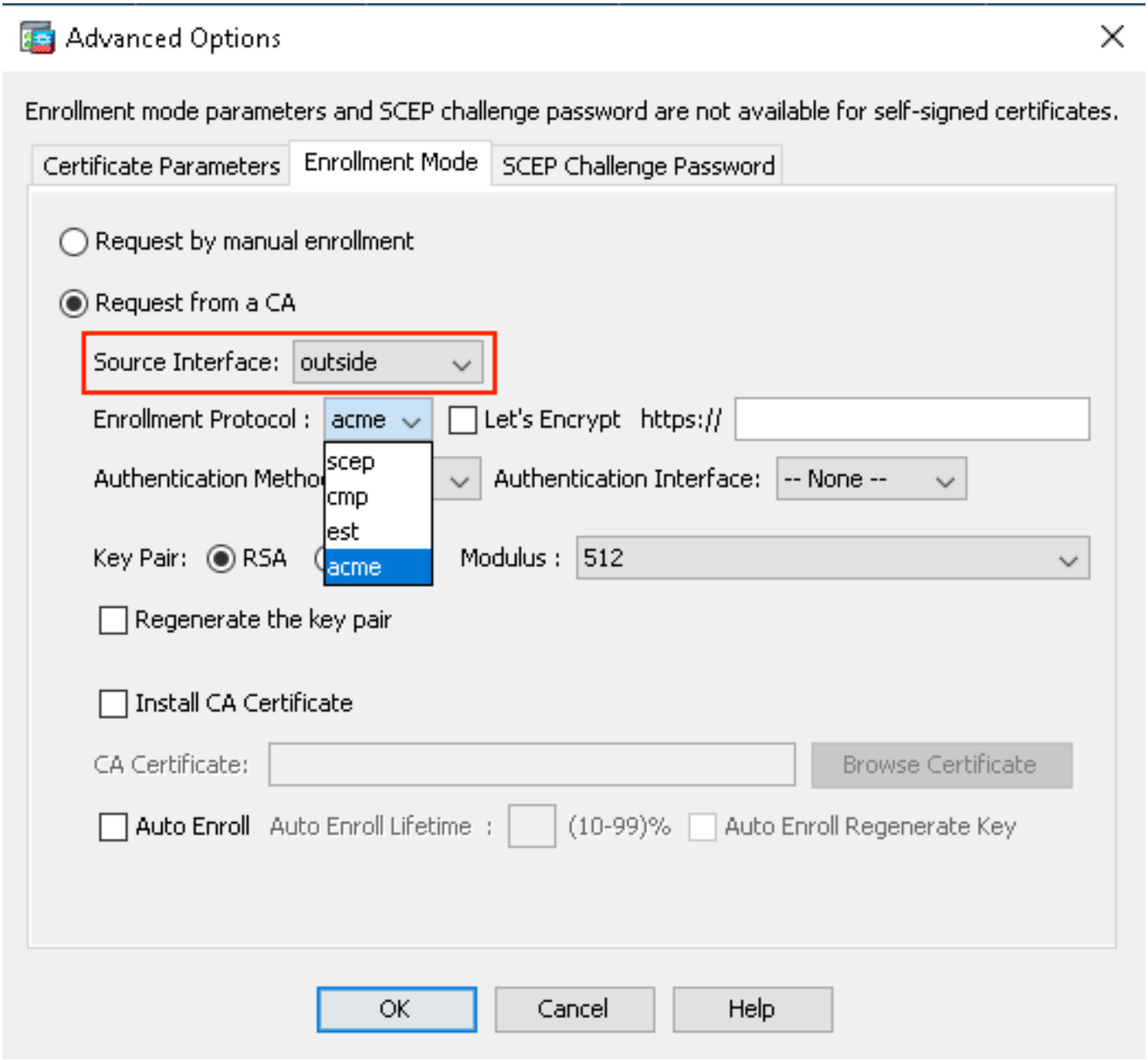
- Advancedボタンをクリックします。
- Certificate Parametersタブで、証明書に必要なFQDNを指定します。



ACME登録ASDM FQDN。

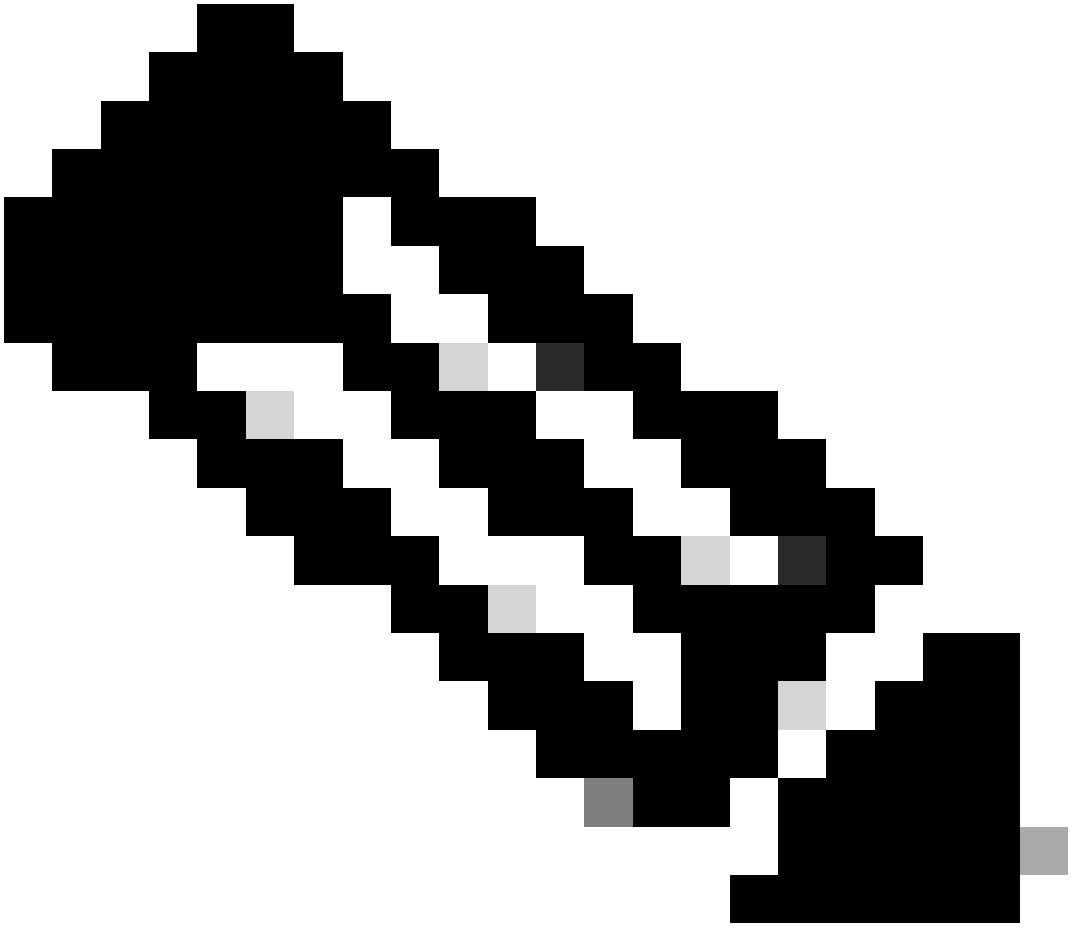
3. 登録プロトコルとしてACMEを選択します。

- Enrollment ModeタブでRequest from CAオプションを選択します。
- 発信元インターフェイスを指定し、登録プロトコルとしてacmeを選択します。

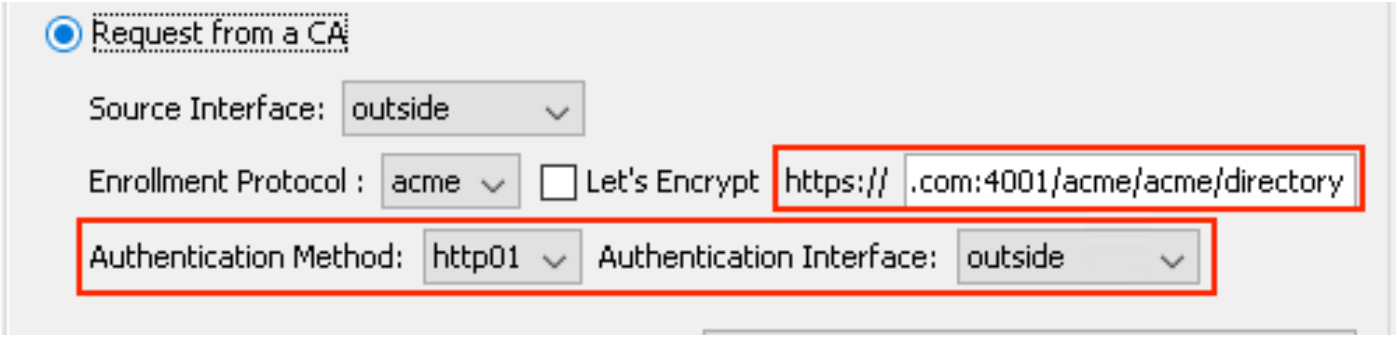


ACME登録ASDM acmeプロトコル。選択

4.「パブリックCAを暗号化しましょう」で署名する証明書に対して、「暗号化しましょう」を選択します。それ以外の場合は、ACME登録プロトコルをサポートする内部CAのURLを指定します。さらに、認証インターフェイスを指定します。



注:「Let's Encrypt」チェックボックスをオンにすると、サーバのURLが自動的に入力されます。



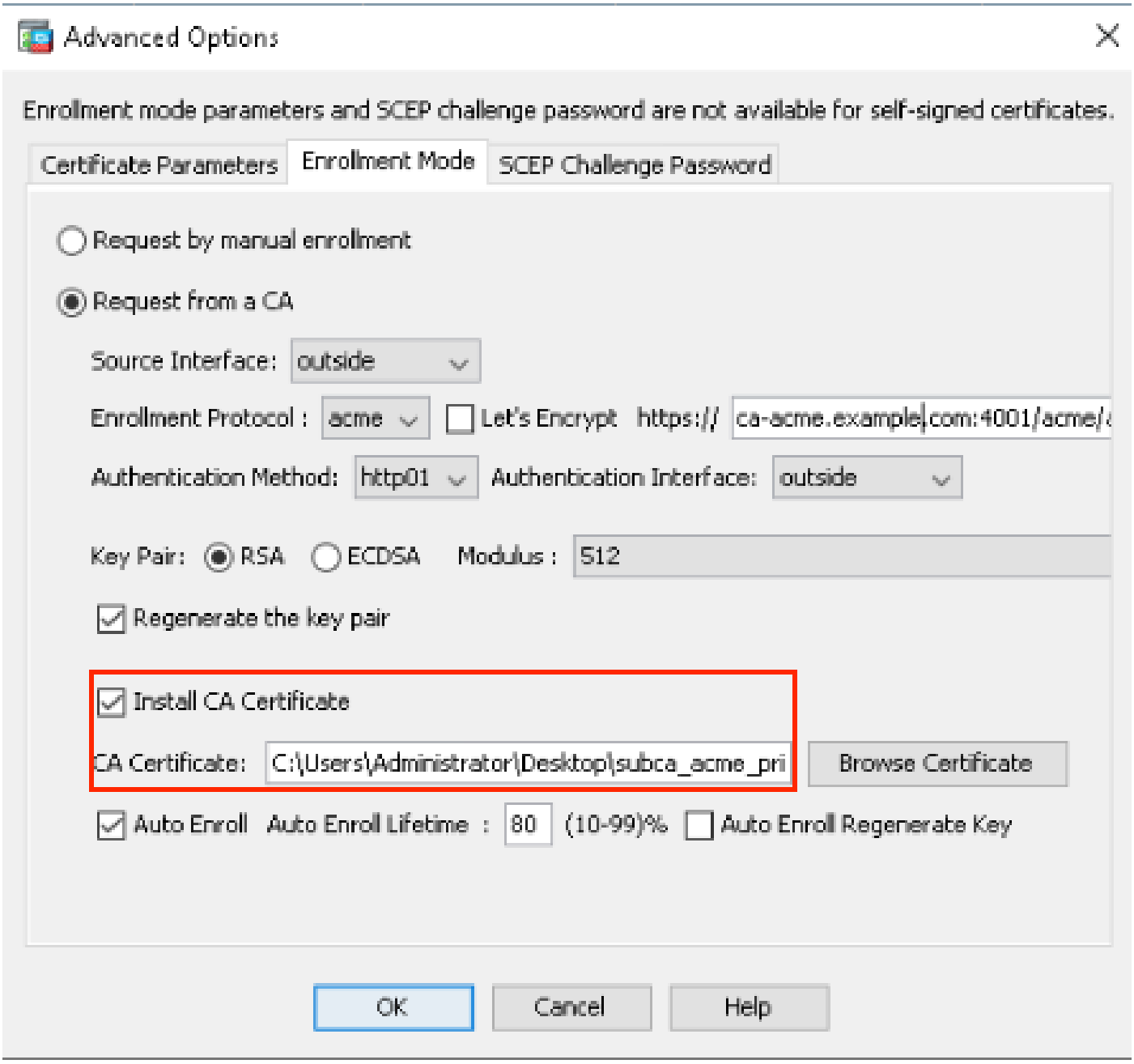
ACME登録ASDM認証方式。

5. CA証明書をインストールします。

Install CA Certificateオプションにチェックマークを入れている場合は、証明書を発行する直近のCAの証明書をアップロードする必要があります。

注:CA証明書が以前のインストールまたはトラストプール内のセキュアファイアウォールにすでに存在している場合は、このオプションをチェックする必要はありません。Install CA Certificateチェックボックスにチェックマークを付けないままにします。

注：Let's EncryptのルートCA証明書はSecure Firewall信頼プールにすでに含まれているため、Let's Encryptオプションを選択する際は、Install CA Certificateチェックボックスのチェックマークを外したままにしておきます。

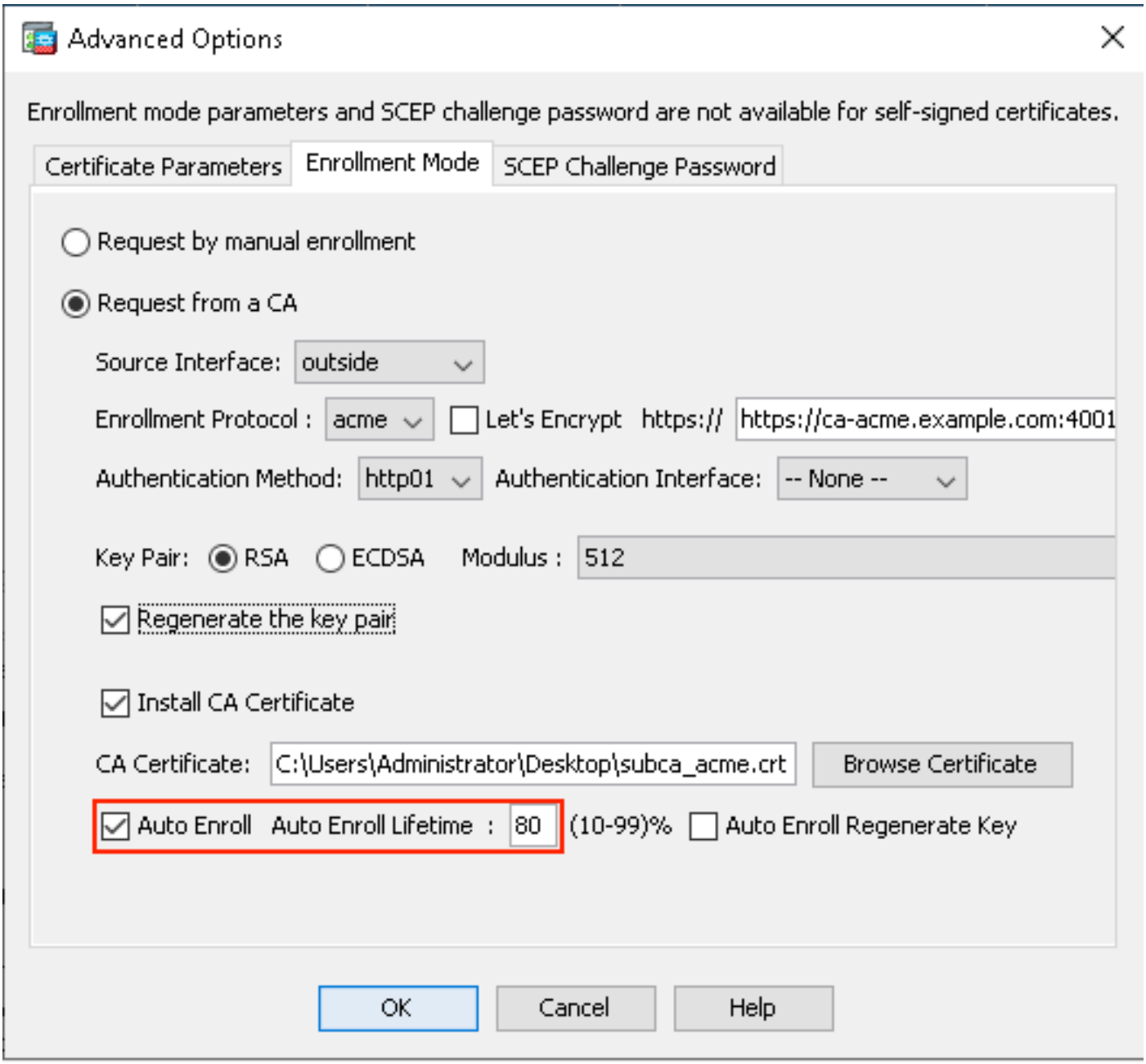


ACME登録ASDM CAのインストール。

6.（オプション）ID証明書の自動登録を有効にします。

Auto Enrollチェックボックスをオンにして、Auto Enroll Lifetimeに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。



ACME登録ASDM自動登録。

7. OKをクリックし、設定を保存します。

セキュアファイアウォールASA CLIを使用したACME登録

1. 新しいトラストポイントを作成します。

トラストポイントを作成し、登録プロトコルとしてacmeを指定します。

<#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. ドメイン制御を確認するための認証にHTTP-01方式を選択します。

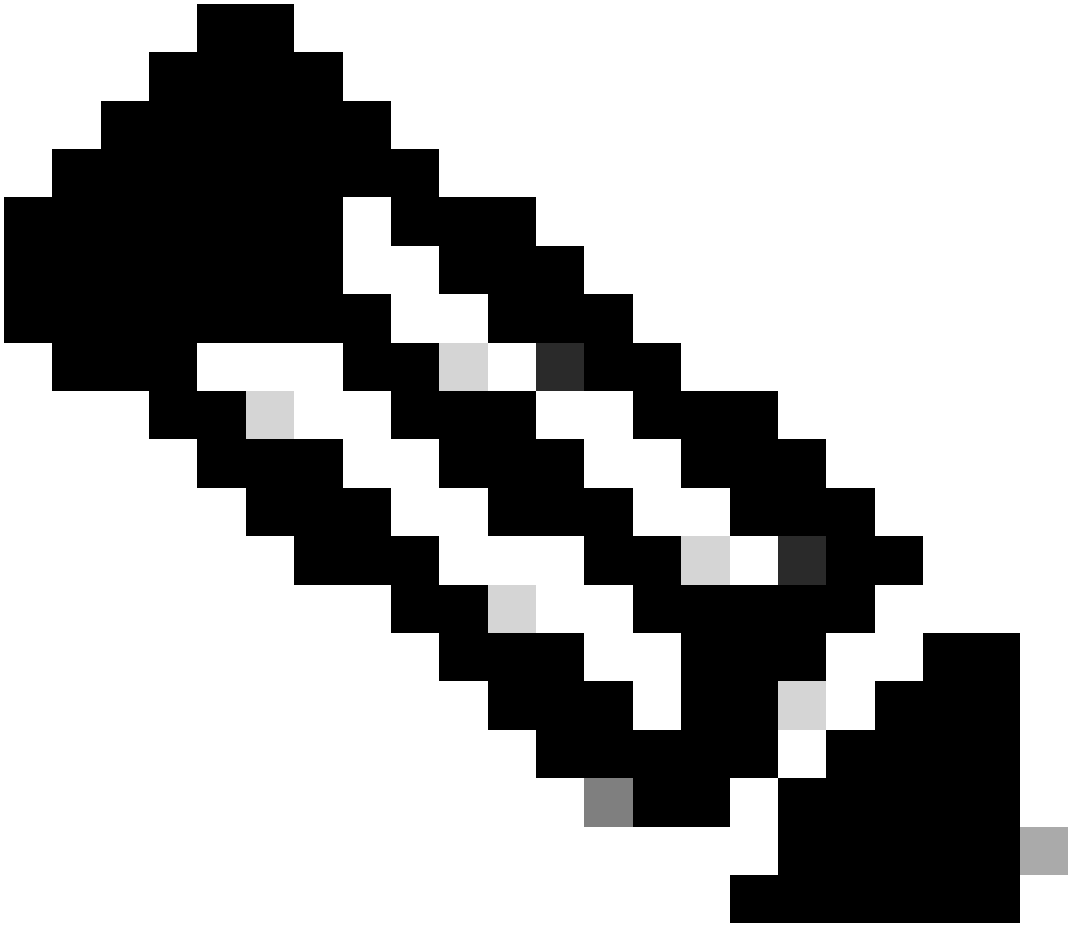
```
asav(config-ca-trustpoint)# enrollment protocol acme authentication ?

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

3. ACME CAとしてLet's Encryptを選択します。ACMEプロトコルをサポートする別のCAを使用する場合は、適切なURLを指定します。

```
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
```



注：LetsEncryptキーワードを設定すると、Let's EncryptサーバURLが自動的に入力されます。

4. RSAキーペア、完全修飾ドメイン名(FQDN)、および証明書のサブジェクト名を定義します。

```
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. トラストポイントを認証します。

注:CAがセキュアファイアウォールにすでに存在する場合、またはLet's Encryptを使用している場合は、この手順はスキップできます。

```
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. 証明書を登録します。

```
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
```

確認

ASAにインストールされた証明書の表示

証明書が登録されていることと、更新日を確認します。

```
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 イベント

ACMEプロトコルを使用して証明書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

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

- 717068:ACME証明書登録が成功した時点に関する情報を提供します。

```
%ASA-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。

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

- 717070：証明書登録または証明書の更新のキーペアに関する情報を提供します。

```
%ASA-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する：セキュアファイアウォールがACMEサーバにネットワーク接続されてい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セキュアファイアウォール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>

一般的なACME登録エラー：

エラー コード	原因	考えられる原因または修復
7	サーバに接続できません	サーバは到達可能ですが、ACMEサービスが実行されていません。
28	サーバに接続できません	サーバに到達できません。 ACMEサーバへの基本的なネットワークアクセスを確認します。
60	サーバー証明書を検証できません	ルートCAまたは発行者CAがトラストポイントまたはトラストプールにあることを確認します。
124	ACME処理タイムアウト	要求されたすべてのFQDNが、HTTP-01認証用に設定されたインターフェイスに解決されることを確認します。 設定されているACME URLが正しいことを確認します。

関連情報

詳細については、TACにお問い合わせください。有効なサポート契約が必要です。シスコワールドワイドサポートの連絡先です。
Cisco VPN コミュニティには、ここからアクセスすることもできます。

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。