# Configure Certificate Enrollment with ACME Protocol on Secure Firewall

## Contents

## Introduction

This document describes the process to enroll a Transport Layer Security (TLS) certificate using the Automated Certificate Management Environment (ACME) protocol on Secure Firewall ASA.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Firewall Adaptative Security Appliance (ASA)
- Public Key Infrastructure (PKI)

### Components Used

- Cisco ASAv version 9.23.1.
- Cisco ASDM version 7.23(1).
- Certificate Authority (CA) server that supports ACME protocol.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

### Requirements and Limitations

The current requirements and limitations for ACME enrollment on Secure Firewall ASA are:

- Supported on ASA version 9.23.1 and ASDM 7.23.1 onwards
- Not supported in multiple context

- ACME does not support the creation of wildcard certificates. Each certificate request must specify an exact domain name.

- Each trustpoint enrolled via ACME is limited to a single interface, meaning certificates enrolled with ACME cannot be shared across multiple interfaces.

- Keypairs are automatically generated and cannot be shared for certificates enrolled through ACME. Each certificate uses a unique keypair, enhancing security but limiting key reuse.

### Downgrade Considerations

Upon downgrade to a version that does not support ACME enrollment on Secure Firewall ASA (9.22 and older):

- All ACME related trustpoint configurations new to 9.23.x or newer are lost
- Any certificates enrolled via ACME remain accessible, but the private key are disassociated after the first post-downgrade save and reboot

If a downgrade is needed, perform the next recommended workaround procedure:

1. Before downgrade, ensure to export the ACME certificates in PKCS12 format.
2. Before downgrade, ensure to remove the ACME trustpoint configuration.
3. After downgrade, import the PKCS12 certificate. The resulting trustpoint is still valid until the certificate issued via ACME expires.

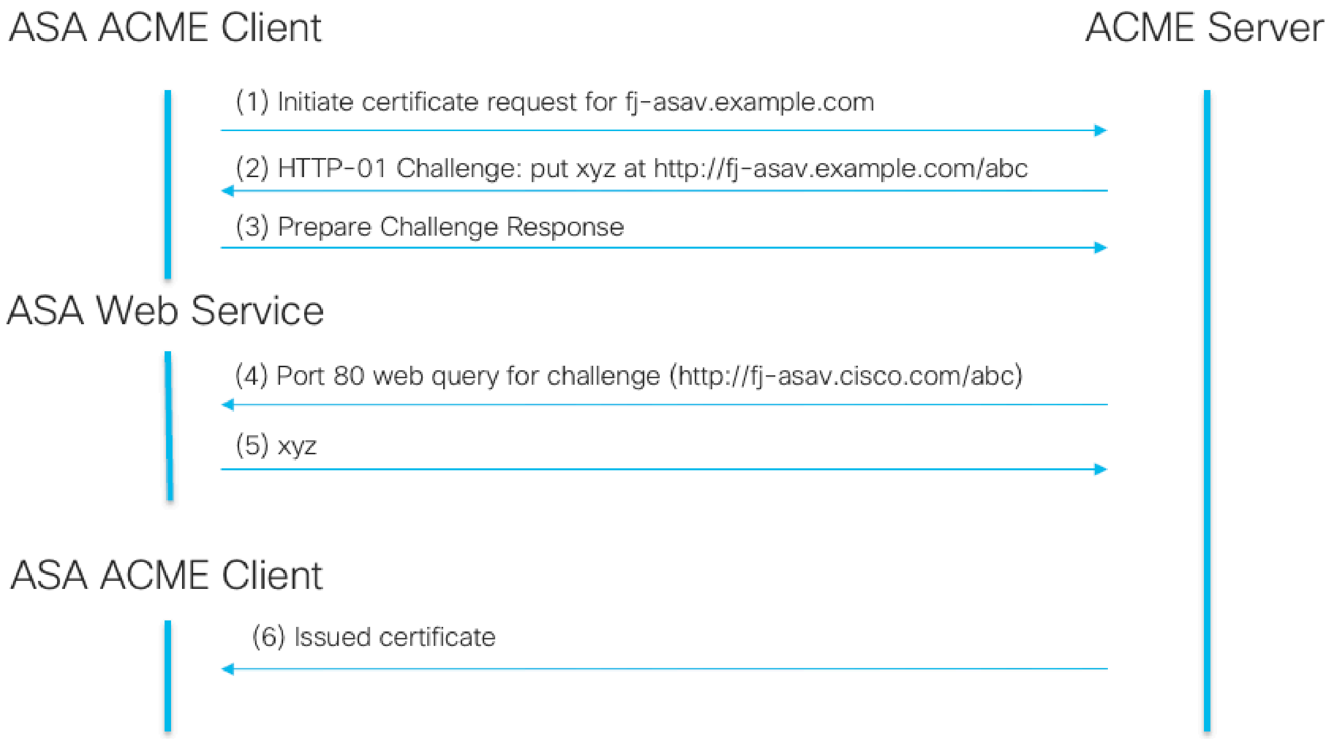
## Background Information

The ACME protocol is designed to streamline the management of TLS certificates for network administrators. By using ACME, administrators can automate the processes involved in obtaining and renewing TLS certificates. This automation is particularly beneficial when utilizing certificate authorities (CAs) like Let's Encrypt, which offer free, automated, and open certificates using the ACME protocol.

ACME supports the issuance of Domain Validation (DV) certificates. These certificates are a type of digital certificate that confirms the control of the certificate holder over specified domains. The validation process for DV certificates is typically conducted through an HTTP-based challenge mechanism. In this mechanism, the applicant places a specific file on their web server, which the Certificate Authority (CA) verifies by accessing the file through the HTTP server of the domain. Successfully completing this challenge demonstrates to the CA that the applicant has control over the domain, allowing the issuance of the DV certificate.

The process to accomplish the enrollment are the next:

1. **Initiate Certificate Request:** The client requests a certificate from the ACME server and specifies the domain(s) for which the certificate is required.
2. **Receive HTTP-01 Challenge:** The ACME server provides an HTTP-01 challenge with a unique token for the client to use to prove domain control.
3. **Prepare Challenge Response:**
   - The client creates a key authorization by combining the token from the ACME server with its account key.
   - The client sets up its web server to serve this key authorization at a specific URL path.
4. **ACME Server Retrieves Challenge:** The ACME server makes an HTTP GET request to the specified URL to retrieve the key authorization.
5. **ACME Server Verifies Ownership:** The server checks if the retrieved key authorization matches the expected value to confirm the control of the client over the domain.
6. **Issue Certificate:** After successful validation, the ACME server issues the SSL/TLS certificate to the client.


ASA ACME Client
ACME Server
(1) Initiate certificate request for fj-asav.example.com
(2) HTTP-01 Challenge: put xyz at http://fj-asav.example.com/abc
(3) Prepare Challenge Response
ASA Web Service
(4) Port 80 web query for challenge (http://fj-asav.cisco.com/abc)
(5) xyz
ASA ACME Client
(6) Issued certificate

*ACME Enrollment HTTP-01 Authentication Flow.*

The most relevant benefits of using ACME protocol to enroll TLS certificates are:

- ACME facilitates the acquisition and maintenance of TLS domain certificates for the Secure Firewall ASA TLS interfaces. This automation significantly reduces manual tasks and helps keep certificates current without constant oversight.
- With ACME-enabled trustpoints, certificates automatically renew as they near expiration. This capability reduces the need for administrative involvement, ensuring uninterrupted security and preventing unexpected certificate expiration.

# Configure

## Prerequisites Configuration

Before initiating the ACME enrollment process, ensure the next conditions are met:

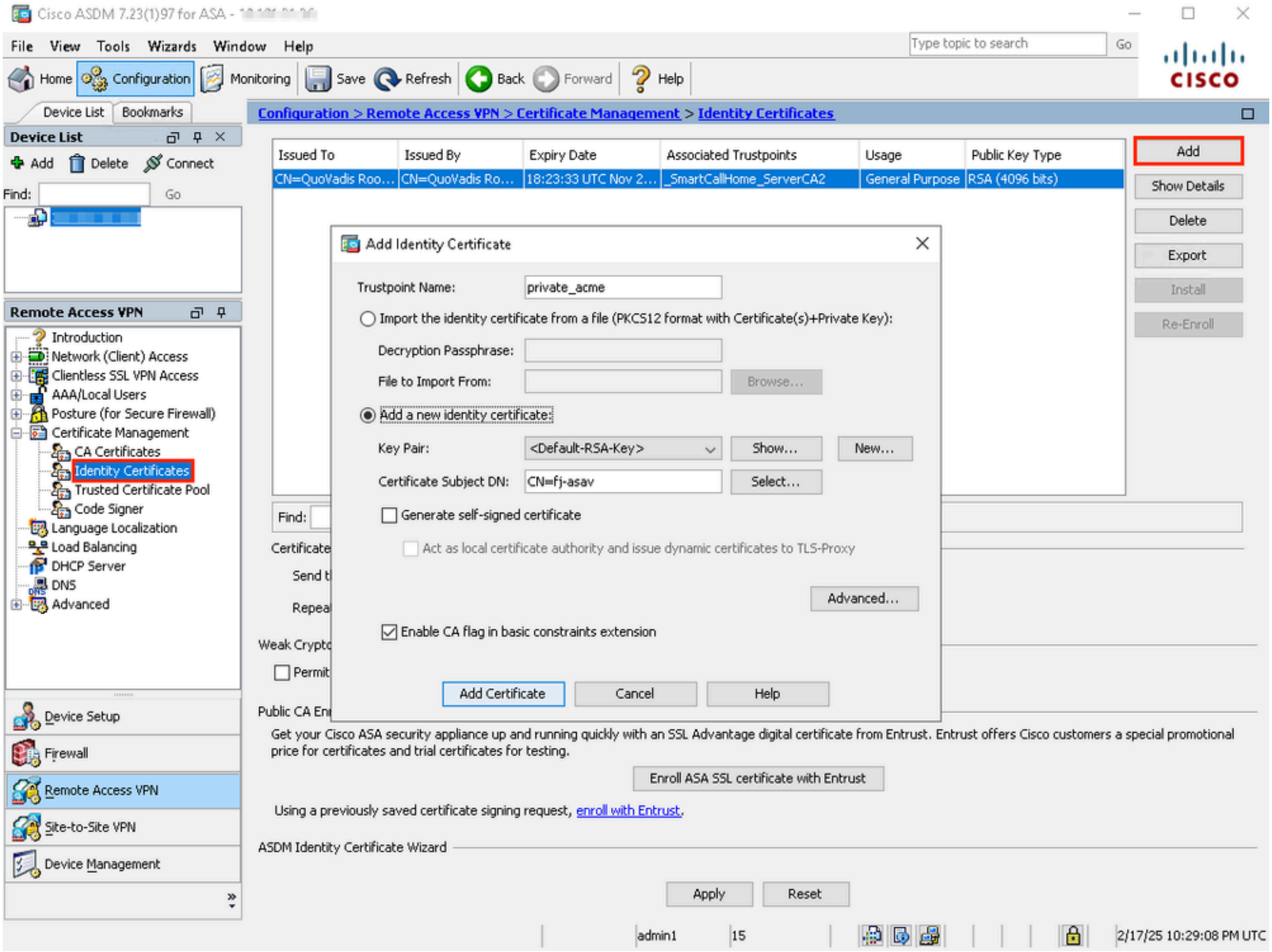
1. **Resolvable Domain Name:** The domain name for which you request a certificate must be resolvable by the ACME server. This ensures that the server can verify domain ownership.
2. **Secure Firewall Access to ACME Server:** The Secure Firewall must have the capability to access the ACME server through one of its interfaces. This access does not need to be via the interface for which the certificate is requested.
3. **TCP Port 80 Availability:** Allow TCP port 80 from the ACME CA server to the interface that corresponds to the domain name. This is required during the ACME exchange process to complete the HTTP-01 challenge.

**Note**: During the period when port 80 is open, only the ACME challenge data is accessible.

## ACME Enrollment with ASDM

1. Add a new Identity Certificate.

- Navigate to **Configuration > Remote Access VPN > Certificate Management > Identity Certificates**.
- Click the **Add** button and select **Add a new identity certificate**.



| Issued To | Issued By | Expiry Date | Associated Trustpoints | Usage | Public Key Type |
|---|---|---|---|---|---|
| CN=QuoVadis Roo... | CN=QuoVadis Ro... | 18:23:33 UTC Nov 2... | _SmartCallHome_ServerCA2 | General Purpose | RSA (4096 bits) |

Add Identity Certificate

Trustpoint Name: private_acme

○ Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):

Decryption Passphrase:

File to Import From: Browse...

● Add a new identity certificate:

Key Pair: <Default-RSA-Key> Show... New...

Certificate Subject DN: CN=fj-asav Select...

□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Advanced...

☑ Enable CA flag in basic constraints extension

Add Certificate Cancel Help

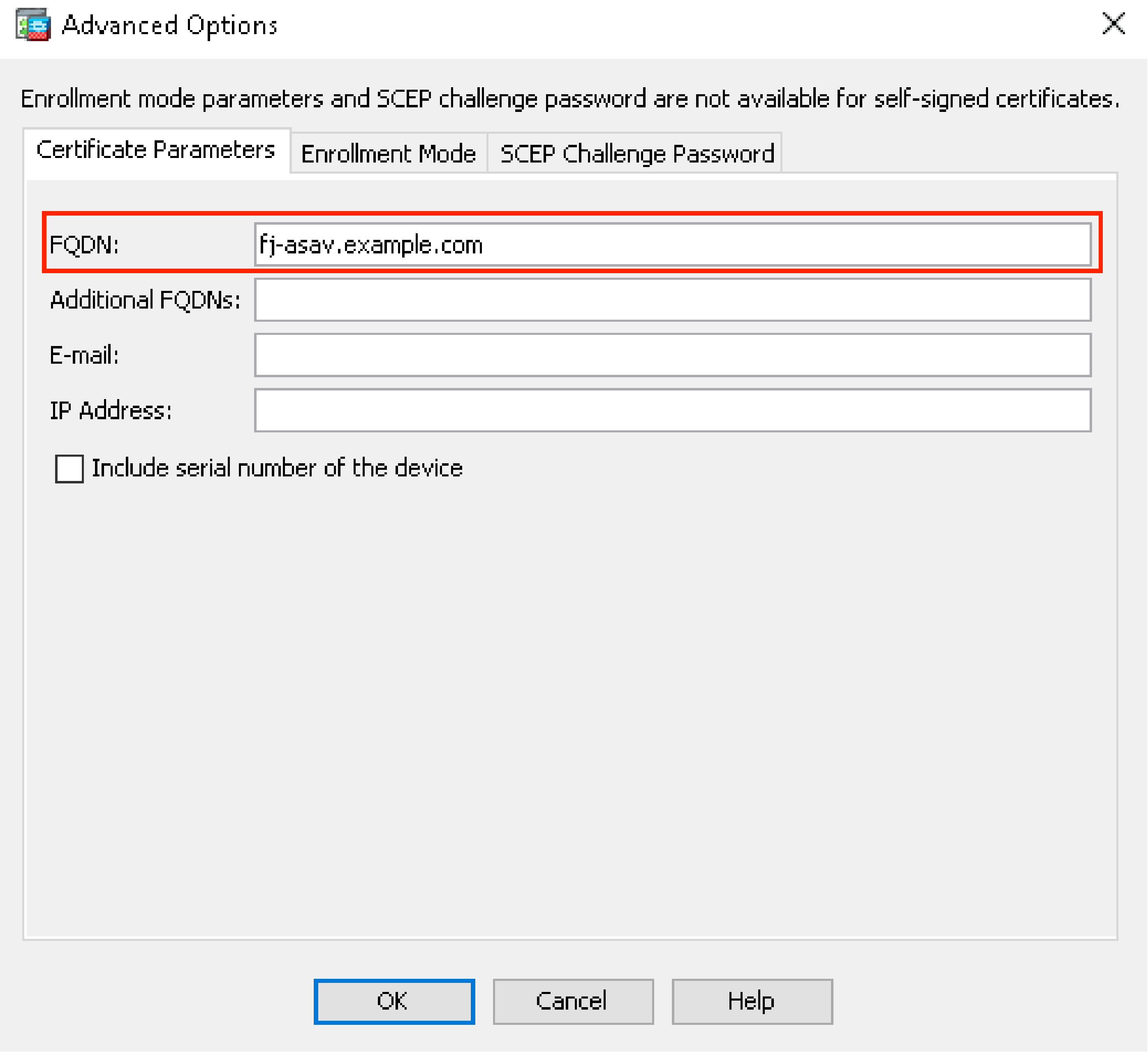
Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

Using a previously saved certificate signing request, enroll with Entrust.

*ACME Enrollment ASDM Identity Certificate.*

2. Specify the FQDN for the Idenity Certificate.

- Click the **Advanced** button.
- Under the **Certificate Parameters** tab, specify the **FQDN** that the certificate must have.



Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

FQDN: fj-asav.example.com

Additional FQDNs:

E-mail:

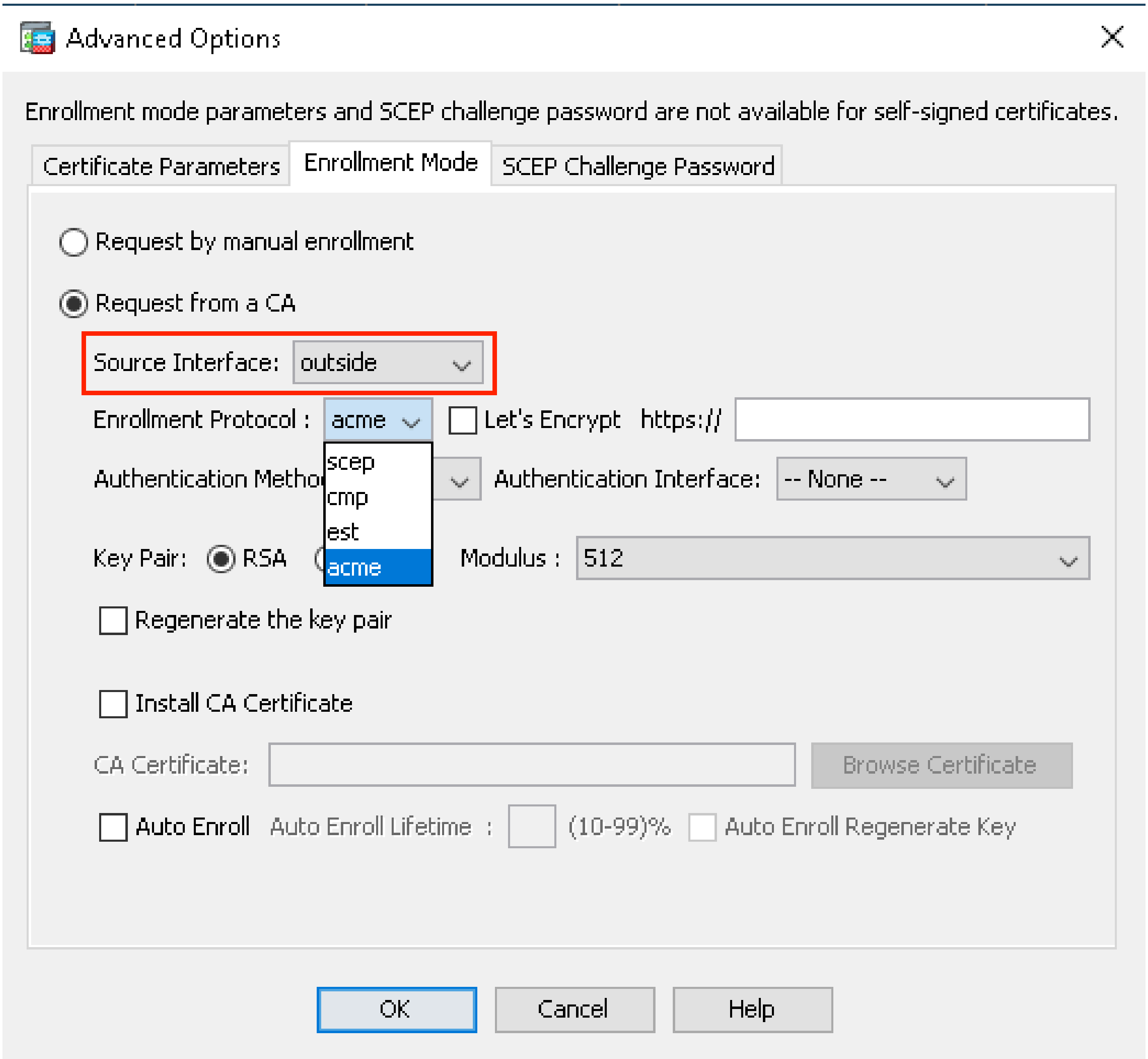
IP Address:

□ Include serial number of the device

*ACME Enrollement ASDM FQDN.*

3. Select ACME as the enrollment protocol.

- Under the **Enrollment Mode** tab, select **Request from CA** option.
- Specify the **Source Interface** and select **acme** as the **Enrollment Protocol**.



Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

○ Request by manual enrollment

● Request from a CA

Source Interface: outside

Enrollment Protocol : acme □ Let's Encrypt https://

Authentication Metho Authentication Interface: -- None --

Key Pair: ● RSA Modulus : 512

□ Regenerate the key pair

□ Install CA Certificate

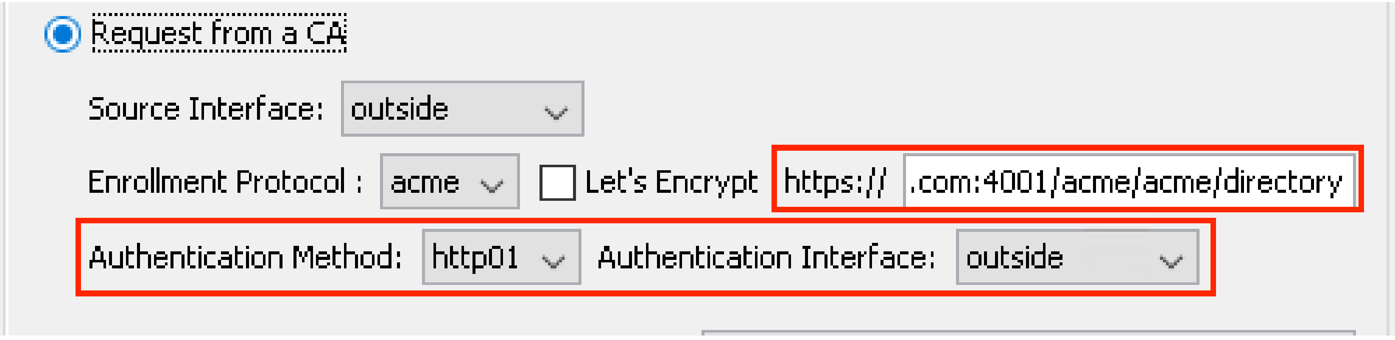
CA Certificate:

□ Auto Enroll Auto Enroll Lifetime : (10-99)% □ Auto Enroll Regenerate Key

*ACME Enrollment ASDM acme protocol. selection*

4. Select **Let's Encrypt** for your certificate to be signed by Let's Encrypt public CA. Otherwise, specify the URL of your internal CA that supports ACME enrollment protocol. Additionally, specify the **Authentication Interface**.

**Note**: When the **Let's Encrypt** checkbox is selected, the server URL is auto-populated.



● Request from a CA

Source Interface: outside

Enrollment Protocol : acme □ Let's Encrypt https:// .com:4001/acme/acme/directory

Authentication Method: http01 Authentication Interface: outside

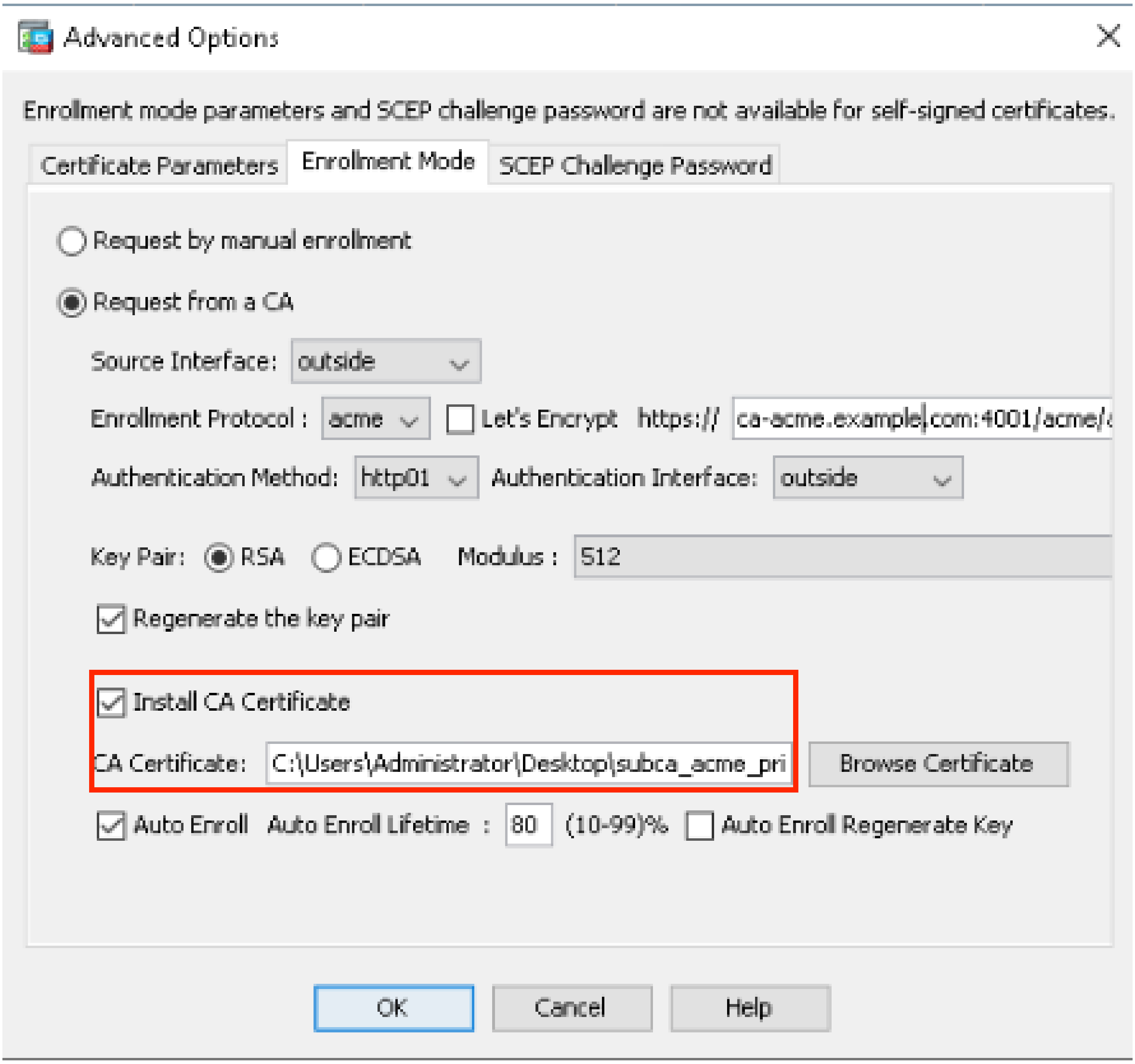
*ACME Enrollment ASDM Authenticaiton Method.*

5. Install CA Certificate.

If the **Install CA Certificate** option is checked, you must upload the certificate of the immediate CA that issues your certificate.

**Note**: If the CA certificate already exists on the Secure Firewall, either from a previous installation or within the trustpool, there is no need to check this option. Leave the **Install CA Certificate** checkbox unchecked.

**Note:** When you select the **Let's Encrypt** option, leave the **Install CA Certificate** checkbox unchecked, as the root CA certificates for Let's Encrypt are already included in the Secure Firewall trustpool.



Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

○ Request by manual enrollment

● Request from a CA

Source Interface: outside

Enrollment Protocol : acme □ Let's Encrypt https:// ca-acme.example.com:4001/acme/

Authentication Method: http01 Authentication Interface: outside

Key Pair: ● RSA ○ ECDSA Modulus : 512

☑ Regenerate the key pair

☑ Install CA Certificate

CA Certificate: C:\Users\Administrator\Desktop\subca_acme_pri

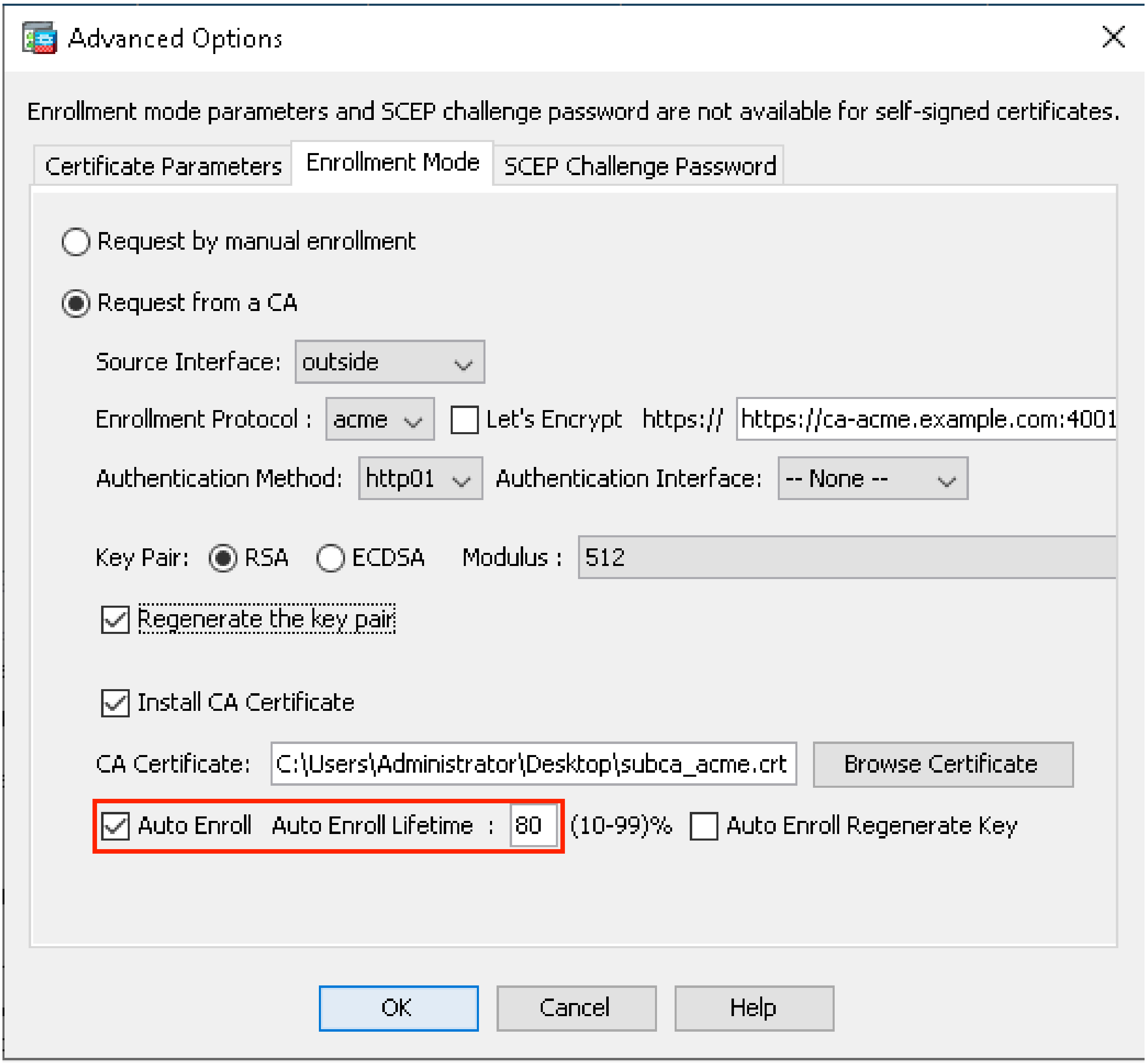
☑ Auto Enroll Auto Enroll Lifetime : 80 (10-99)% □ Auto Enroll Regenerate Key

*ACME Enrollment ASDM CA Installation.*

6. (Optional) Enable Auto Enroll for the Identity Certificate.

Check the **Auto Enroll** checkbox and specify the percentage for the **Auto Enroll Lifetime**.

This feature ensures that the certificate is renewed automatically before it expires. The percentage determines how far in advance of the expiration of the certificate the renewal process begins. For example, if set to 80%, the renewal process starts when the certificate has reached 80% of its validity period.



Enrollment mode parameters and SCEP challenge password are not available for self-signed certificates.

○ Request by manual enrollment

● Request from a CA

Source Interface: outside

Enrollment Protocol : acme □ Let's Encrypt https:// https://ca-acme.example.com:4001

Authentication Method: http01 Authentication Interface: -- None --

Key Pair: ● RSA ○ ECDSA Modulus : 512

☑ Regenerate the key pair

☑ Install CA Certificate

CA Certificate: C:\Users\Administrator\Desktop\subca_acme.crt

☑ Auto Enroll Auto Enroll Lifetime : 80 (10-99)% □ Auto Enroll Regenerate Key

*ACME Enrollment ASDM Auto Enroll.*

7. Click **OK** and **Save** the configuration.

## ACME Enrollment with Secure Firewall ASA CLI

1. Create a new Trustpoint.

Create a trustpoint and specify **acme** as the enrollment protocol.

<#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. Select the HTTP-01 method for authentication to verify domain control.

```
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. Select Let's Encrypt as the ACME CA. If using another CA that supports ACME protocol, provide the appropriate URL.

```
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
```

**Note**: When **LetsEncrypt** keyword is configured, the Let's Encrypt server URL is auto-populated.

4. Define the RSA keypair, the Fully Qualified Domain Name (FQDN), and the Subject Name for the certificate.

```
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. Authenticate the trustpoint.

**Note**: If the CA already exists on the secure firewall or when using Let's Encrypt, this step can be skipped.

```
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
DgYDVQQKEwdjYS1hY21lMRgwFgYDVQQDEw9jYS1hY21lIFJvb3QgQ0EwHhcNMjQx
[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. Enroll the certificate.

```
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
```

# Verify

## View Installed Certificate in ASA

Confirm the certificate is enrolled and verify the renewal date.

```
asav# show crypto ca certificates private_acme
CA Certificate
Status: Available
Certificate Serial Number: 79d0000000000000000000008b
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: 8c82000000000000000000000000000000000077
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: e6e00000000000000000000000000000000089a
SHA1 PublicKeyInfo hash: 5e3000000000000000000000000000000000009f
```

## Syslog events

There are new syslogs in the Secure Firewall to capture events related to the certificate enrollment using ACME protocol:

- **717067**: Provides information of when ACME certificate enrollment starts

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

- **717068**: Provides information of when ACME certificate enrollment is successful

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

- **717069**: Provides information of when ACME enrollment fails

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

- **717070**: Provides Information related the keypair for certificate enrollment or certificate renewal

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

# Troubleshoot

If an ACME certificate enrollment fails, consider the next steps to identify and resolve the issue:

- **Check connectivity to the server:** Confirm that the Secure Firewall has network connectivity to the ACME server. Verify that there are no network issues or firewall rules blocking communication.
- **Ensure the Secure Firewall Domain Name is resolvable:** Make sure the domain name configured on the Secure Firewall is resolvable by the ACME server. This verification is crucial for the server to validate the request.
- **Confirm Domain Ownership:** Verify that all domain names specified in the trustpoint are owned by the Secure Firewall. This ensures that the ACME server can validate domain ownership.

## Troubleshoot commands

For additional information, collect the output of the next debug commands:

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

Common ACME Enrollment errors:

| Error code | Reason | Possible Cause or Remediation |
|---|---|---|
| 7 | Unable to connect to the server | Server is reachable but ACME service not running. |
| 28 | Unable to connect to the server | Server is not reachable.<br>Check basic network access to ACME server. |

| | | |
|---|---|---|
| 60 | Unable to validate server certificate | Make sure root or issuer CA is present in a trustpoint or in the trustpool. |
| 124 | ACME processing timeout | Make sure all requested FQDNs resolve to the interface configured for HTTP-01 authentication.<br>Make sure the configured ACME URL is correct. |

## Related Information

For additional assistance, please contact TAC. A valid support contract is required: Cisco Worldwide Support Contacts.
You can also visit the Cisco VPN Community here.