Configuración de la inscripción de certificados con el protocolo ACME en un firewall seguro

Contenido

Introducción

Este documento describe el proceso para inscribir un certificado de Seguridad de la capa de transporte (TLS) mediante el protocolo del Entorno de administración automática de certificados (ACME) en Secure Firewall ASA.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

- Cisco ASAv versión 9.23.1.
- Cisco ASDM versión 7.23(1).
- Servidor de autoridad certificadora (CA) que admite el protocolo ACME.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Requisitos y limitaciones

Los requisitos y limitaciones actuales para la inscripción ACME en Secure Firewall ASA son:

- Compatible con ASA versión 9.23.1 y ASDM 7.23.1 en adelante
- No compatible con múltiples contextos
- ACME no admite la creación de certificados comodín. Cada solicitud de certificado debe especificar un nombre de dominio exacto.
- Cada punto de confianza inscrito mediante ACME está limitado a una única interfaz, lo que significa que los certificados inscritos con ACME no se pueden compartir entre varias interfaces.
- Los pares de claves se generan automáticamente y no se pueden compartir para los certificados inscritos mediante ACME. Cada certificado utiliza un par de claves único, lo que mejora la seguridad pero limita la reutilización de claves.

Consideraciones sobre downgrade

Tras la actualización a una versión que no admite la inscripción ACME en Secure Firewall ASA (9.22 o posterior):

- Se pierden todas las configuraciones de punto de confianza relacionadas con ACME nuevas en 9.23.x o posterior
- Todos los certificados inscritos mediante ACME siguen estando accesibles, pero la clave privada se desasocia después de guardar y reiniciar la versión anterior a la versión anterior

Si es necesario un downgrade, realice el siguiente procedimiento recomendado:

1. Antes de realizar la actualización a una versión anterior, asegúrese de exportar los certificados ACME en formato PKCS12.
2. Antes de realizar la actualización anterior, asegúrese de quitar la configuración de ACME trustpoint.
3. Después de la degradación, importe el certificado PKCS12. El punto de confianza resultante

seguirá siendo válido hasta que caduque el certificado emitido a través de ACME.

Antecedentes

El protocolo ACME está diseñado para simplificar la gestión de certificados TLS para los administradores de red. Con ACME, los administradores pueden automatizar los procesos relacionados con la obtención y renovación de certificados TLS. Esta automatización es especialmente beneficiosa cuando se utilizan entidades emisoras de certificados (CA) como Let's Encrypt, que ofrecen certificados gratuitos, automatizados y abiertos mediante el protocolo ACME.

ACME admite la emisión de certificados de validación de dominio (DV). Estos certificados son un tipo de certificado digital que confirma el control del titular del certificado sobre dominios especificados. El proceso de validación de los certificados de DV se lleva a cabo normalmente a través de un mecanismo de desafío basado en HTTP. En este mecanismo, el solicitante coloca un archivo específico en su servidor web, que la Autoridad de Certificación (CA) verifica accediendo al archivo a través del servidor HTTP del dominio. La superación satisfactoria de este desafío demuestra a la CA que el solicitante tiene control sobre el dominio, lo que permite la emisión del certificado de DV.

El siguiente paso es llevar a cabo el proceso de inscripción:

1. Iniciar solicitud de certificado: El cliente solicita un certificado del servidor ACME y especifica los dominios para los que se requiere el certificado.
2. Recibir desafío de HTTP-01: El servidor ACME proporciona un desafío HTTP-01 con un token único para que el cliente lo utilice para probar el control de dominio.
3. Preparación de la respuesta al desafío:
    - El cliente crea una autorización de clave combinando el token del servidor ACME con su clave de cuenta.
    - El cliente configura su servidor web para que proporcione esta autorización de clave en una ruta URL específica.
4. El servidor ACME recupera el desafío: El servidor ACME realiza una solicitud GET HTTP a la dirección URL especificada para recuperar la autorización de clave.
5. El servidor ACME verifica la propiedad: El servidor comprueba si la autorización de clave recuperada coincide con el valor esperado para confirmar el control del cliente sobre el dominio.
6. Emitir certificado: Después de la validación correcta, el servidor ACME emite el certificado SSL/TLS al cliente.

Flujo de autenticación HTTP-01 de inscripción ACME.

Las ventajas más importantes del uso del protocolo ACME para inscribir certificados TLS son:

- ACME facilita la adquisición y el mantenimiento de certificados de dominio TLS para las interfaces ASA TLS de Secure Firewall. Esta automatización reduce significativamente las tareas manuales y ayuda a mantener los certificados actualizados sin una supervisión constante.
- Con los puntos de confianza habilitados para ACME, los certificados se renuevan automáticamente cuando están a punto de caducar. Esta capacidad reduce la necesidad de intervención administrativa, lo que garantiza una seguridad ininterrumpida y evita el vencimiento inesperado de los certificados.

Configurar

Prerrequisitos de Configuración

Antes de iniciar el proceso de inscripción en ACME, asegúrese de que se cumplen las siguientes condiciones:

1. Nombre de dominio resoluble: El servidor ACME debe poder resolver el nombre de dominio para el que solicita un certificado. Esto garantiza que el servidor pueda comprobar la propiedad del dominio.
2. Acceso seguro de firewall al servidor ACME: El firewall seguro debe tener la capacidad de acceder al servidor ACME a través de una de sus interfaces. No es necesario que este acceso se realice mediante la interfaz para la que se solicita el certificado.

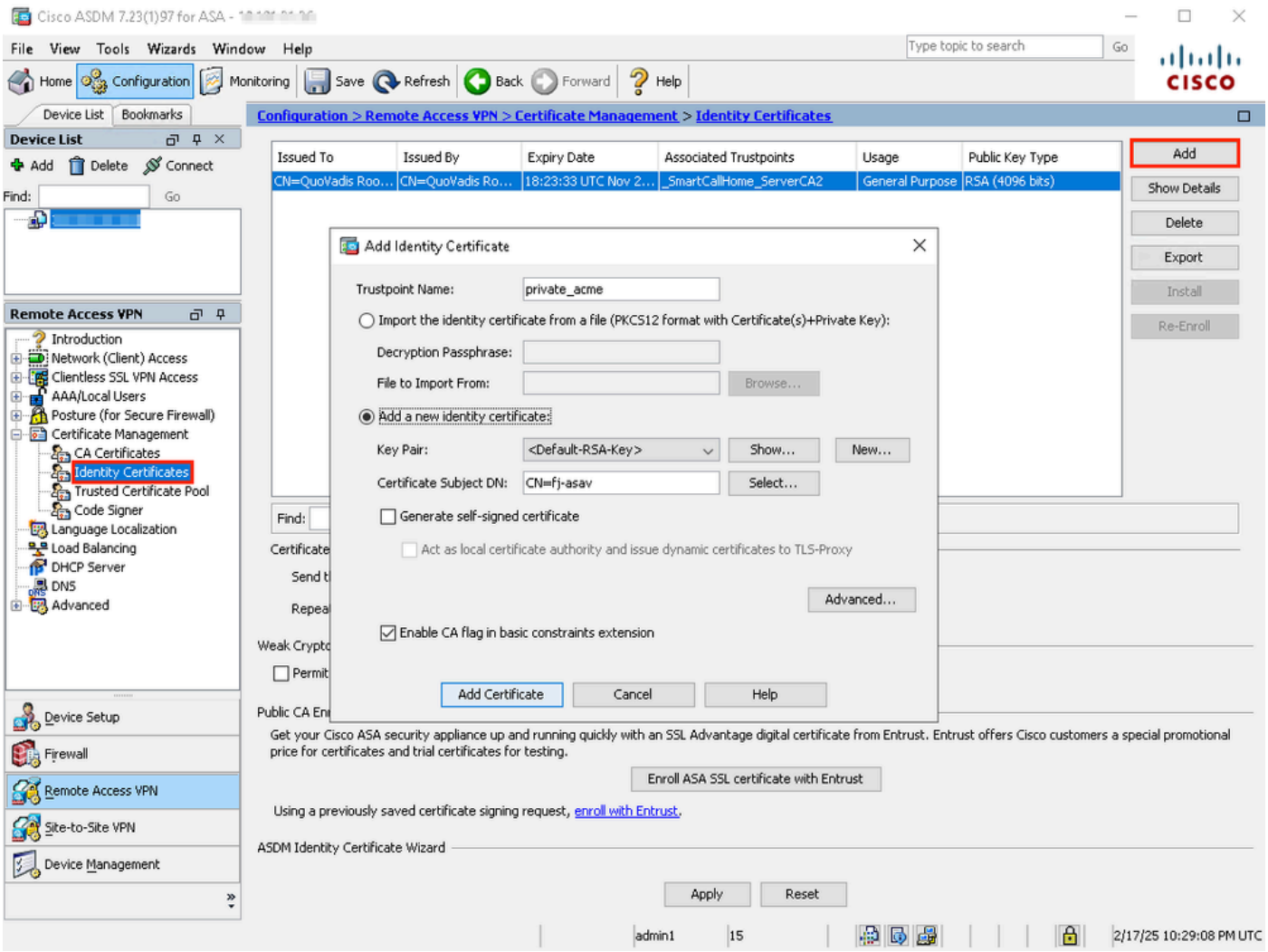
3. Disponibilidad del puerto TCP 80: Permita el puerto TCP 80 desde el servidor ACME CA a la interfaz que corresponde al nombre de dominio. Esto es necesario durante el proceso de intercambio ACME para completar el desafío HTTP-01.

Nota: Durante el período en el que el puerto 80 está abierto, solo se puede acceder a los datos de desafío de ACME.

Inscripción en ACME con ASDM

1. Agregue un nuevo certificado de identidad.

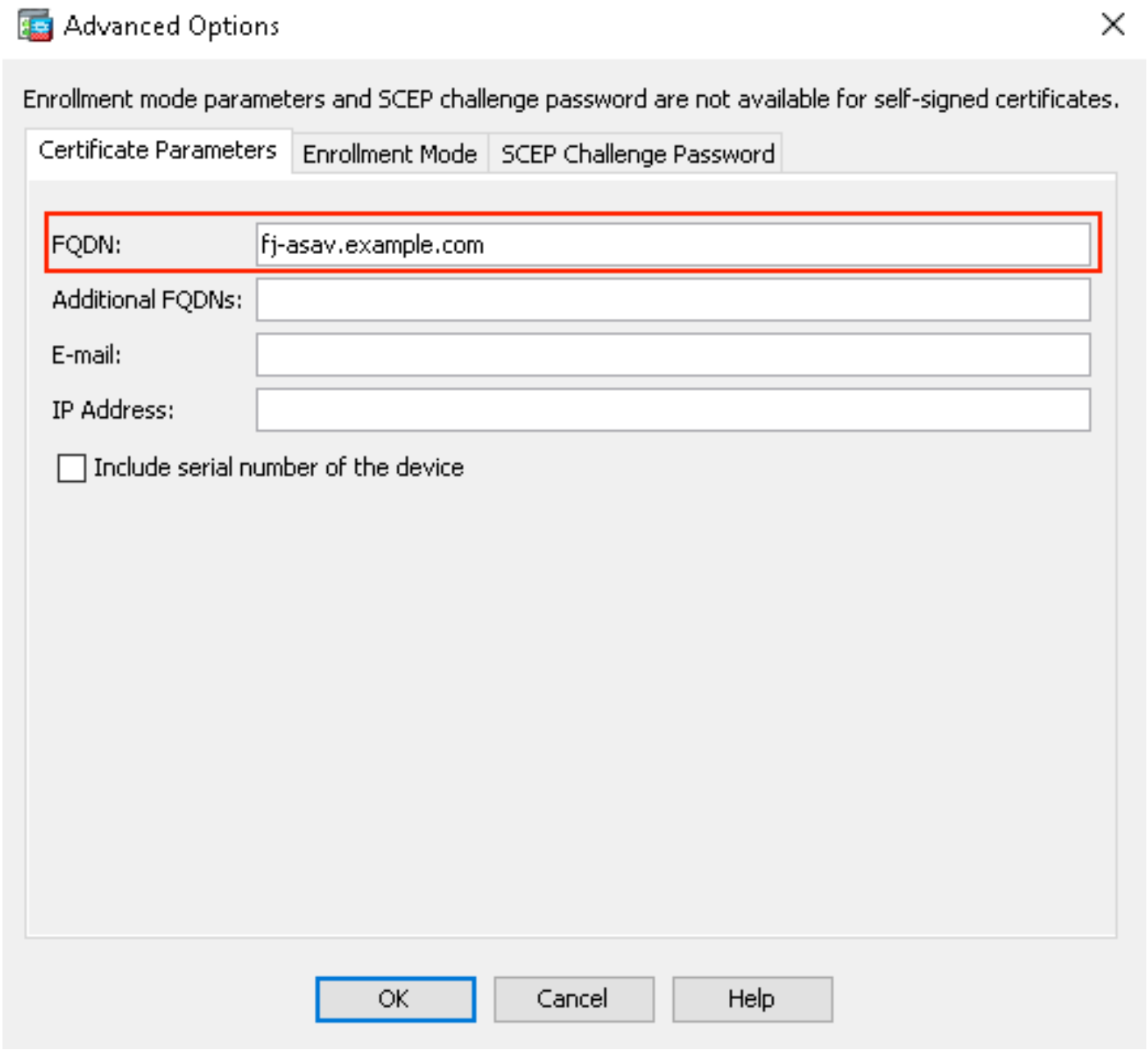
- Vaya a Configuration > Remote Access VPN > Certificate Management > Identity Certificates.
- Haga clic en el botón Add y seleccione Add a new identity certificate.



Certificado de identidad ASDM de inscripción ACME.

2. Especifique el FQDN para el certificado de identidad.

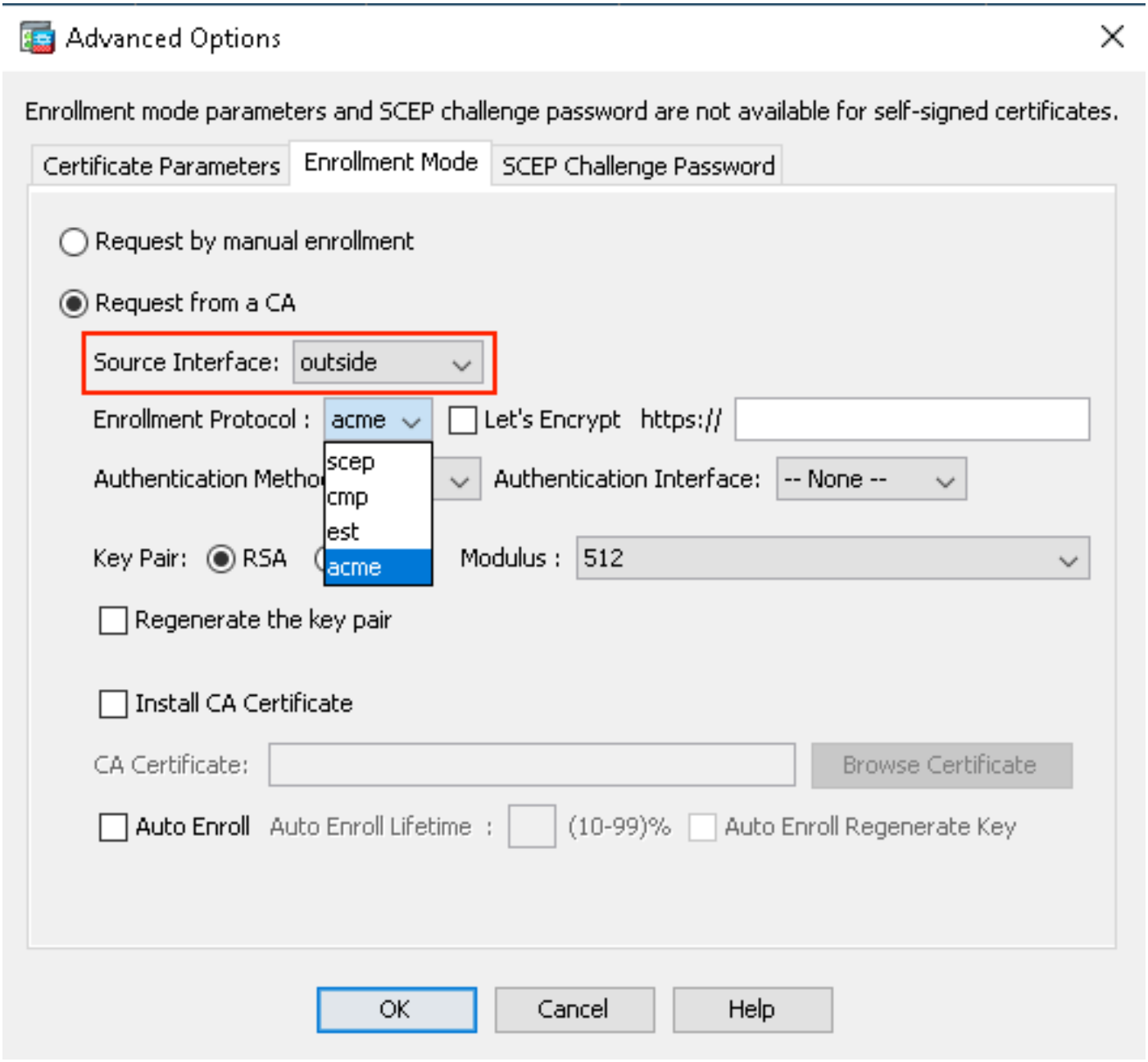
- Haga clic en el botón Advanced.
- En la pestaña Parámetros de certificado, especifique el FQDN que debe tener el certificado.



FQDN de ASDM de inscripción ACME.

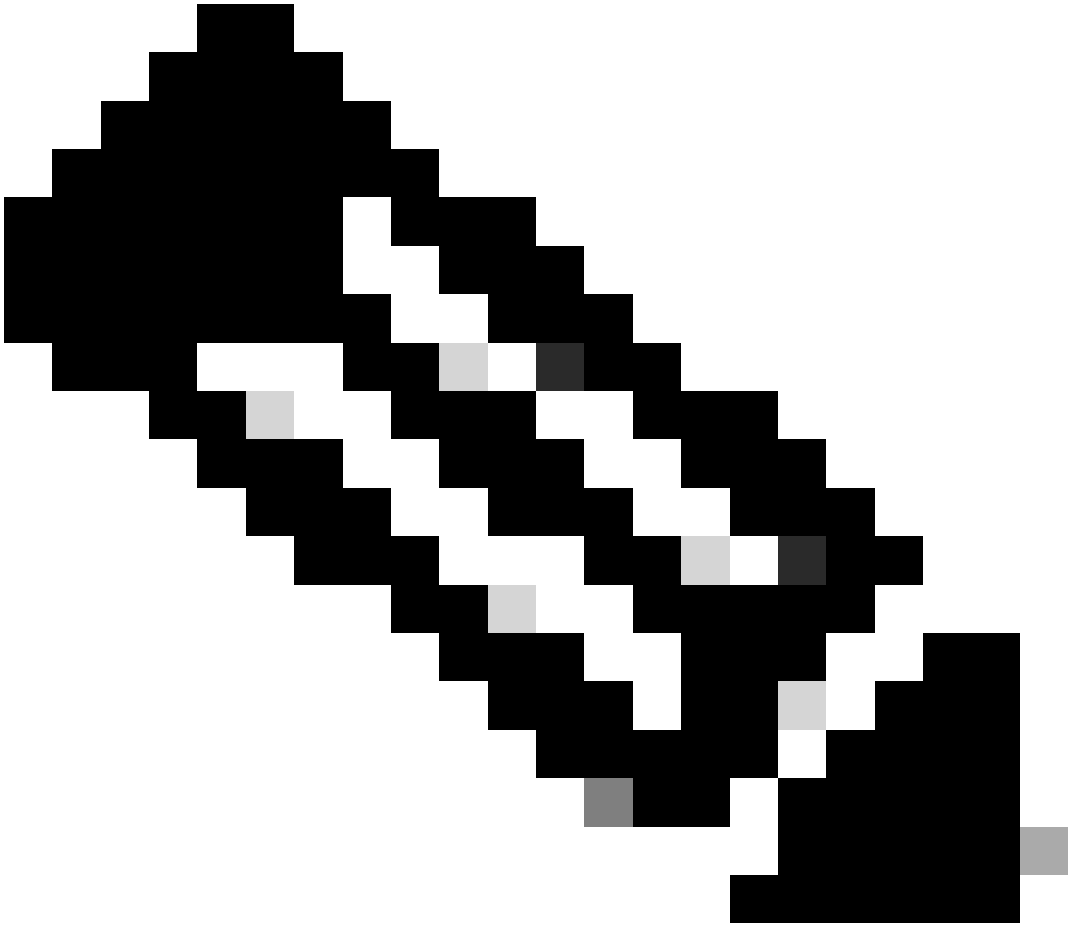
3. Seleccione ACME como protocolo de inscripción.

- En la pestaña Modo de inscripción, seleccione la opción Solicitar desde CA.
- Especifique la Interfaz de Origen y seleccione acme como el Protocolo de Inscripción.

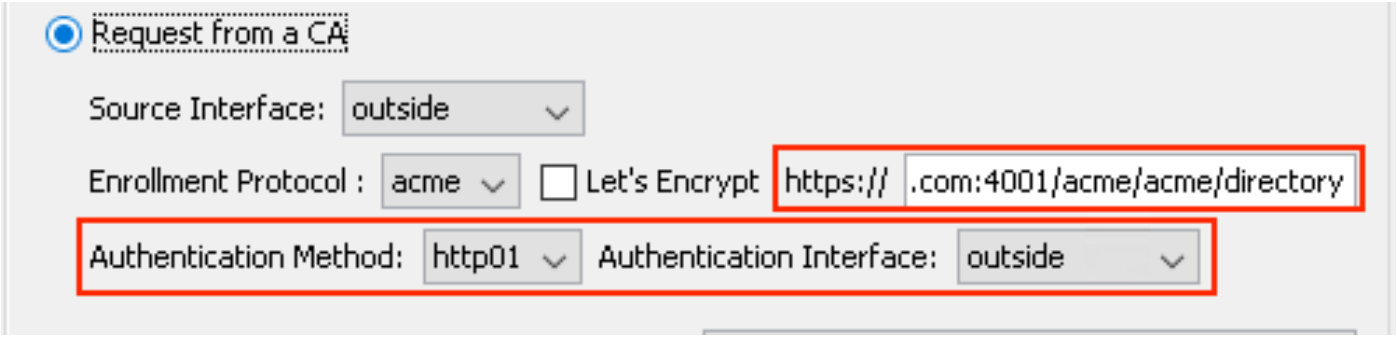


Protocolo ACME ASDM de suscripción ACME. selección

4. Seleccione Let's Encrypt para que su certificado esté firmado por Let's Encrypt public CA. De lo contrario, especifique la dirección URL de la CA interna que admite el protocolo de inscripción ACME. Además, especifique la Interfaz de autenticación.



Nota: Cuando se selecciona la casilla de verificación Let's Encrypt, la URL del servidor se rellena automáticamente.



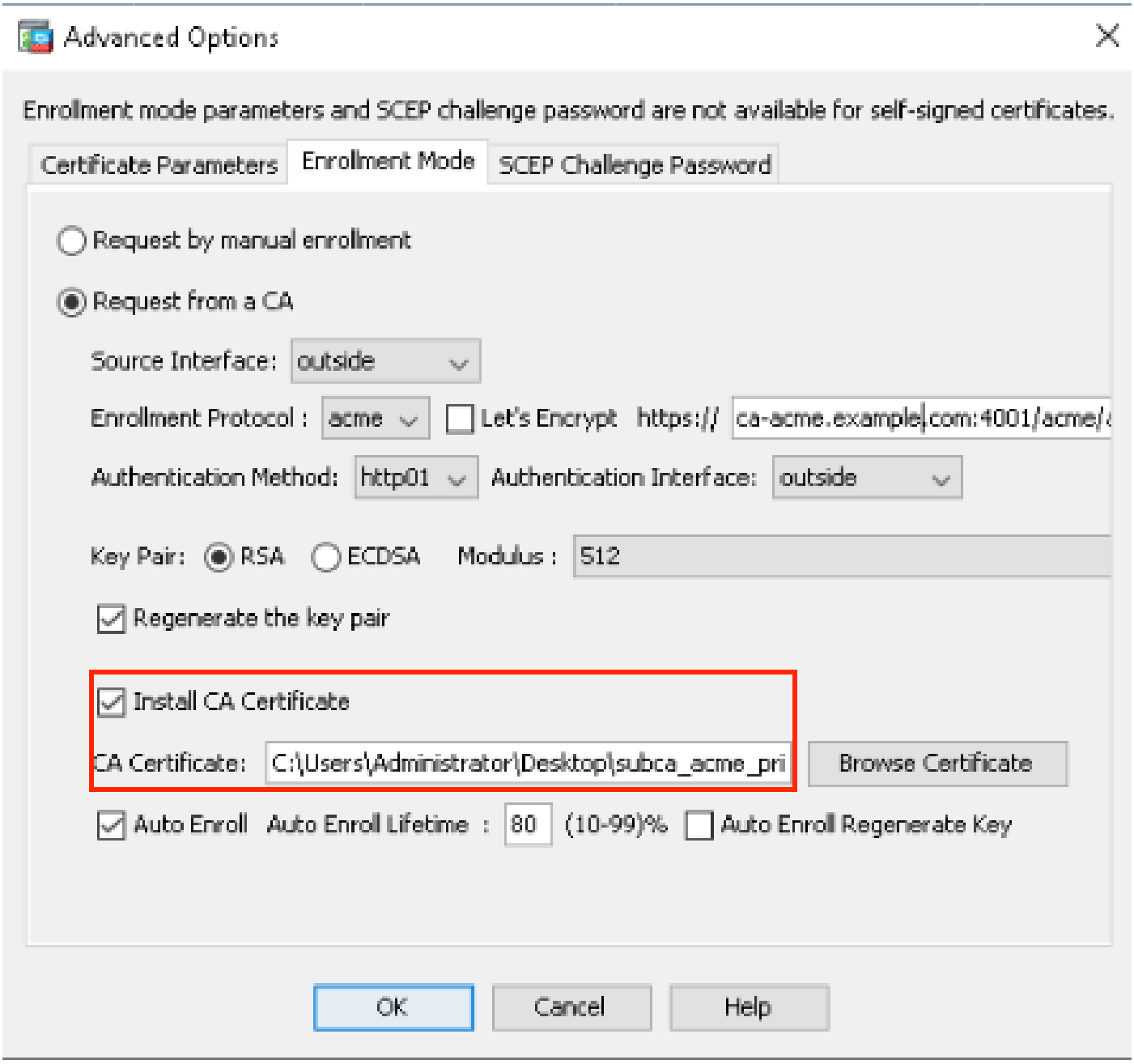
Método de autenticación ASDM de inscripción ACME.

5. Instale el certificado de la CA.

Si la opción Install CA Certificate está marcada, debe cargar el certificado de la CA inmediata que emite su certificado.

Nota: Si el certificado de la CA ya existe en Secure Firewall, ya sea desde una instalación anterior o dentro del grupo de confianza, no es necesario marcar esta opción. No marque la casilla de verificación Install CA Certificate.

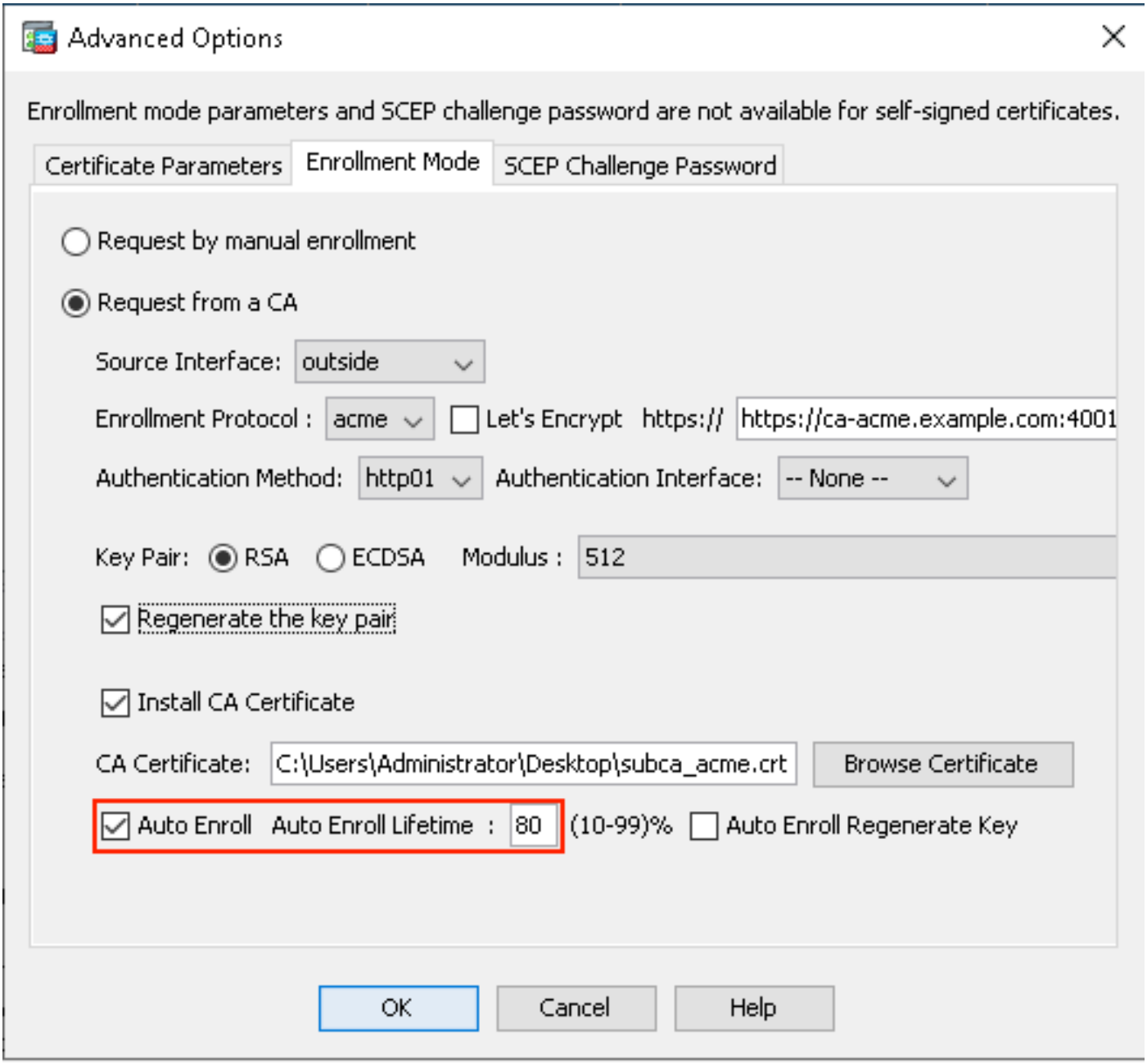
Nota: Cuando seleccione la opción Let's Encrypt, deje sin marcar la casilla de verificación Install CA Certificate, ya que los certificados de CA raíz para Let's Encrypt ya están incluidos en el grupo de confianza de Secure Firewall.



6. (Opcional) Active la inscripción automática para el certificado de identidad.

Marque la casilla de verificación Auto Enroll y especifique el porcentaje para la duración de la inscripción automática.

Esta función garantiza que el certificado se renueva automáticamente antes de que caduque. El porcentaje determina con cuánta antelación a la expiración del certificado comienza el proceso de renovación. Por ejemplo, si se establece en 80%, el proceso de renovación comienza cuando el certificado alcanza el 80% de su período de validez.



Inscripción ACME Inscripción automática ASDM.

7. Haga clic en Aceptar y en Guardar la configuración.

Inscripción en ACME con Secure Firewall ASA CLI

1. Cree un nuevo punto de confianza.

Cree un punto de confianza y especifique acme como protocolo de inscripción.

<#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. Seleccione el método HTTP-01 de autenticación para verificar el control de dominio.

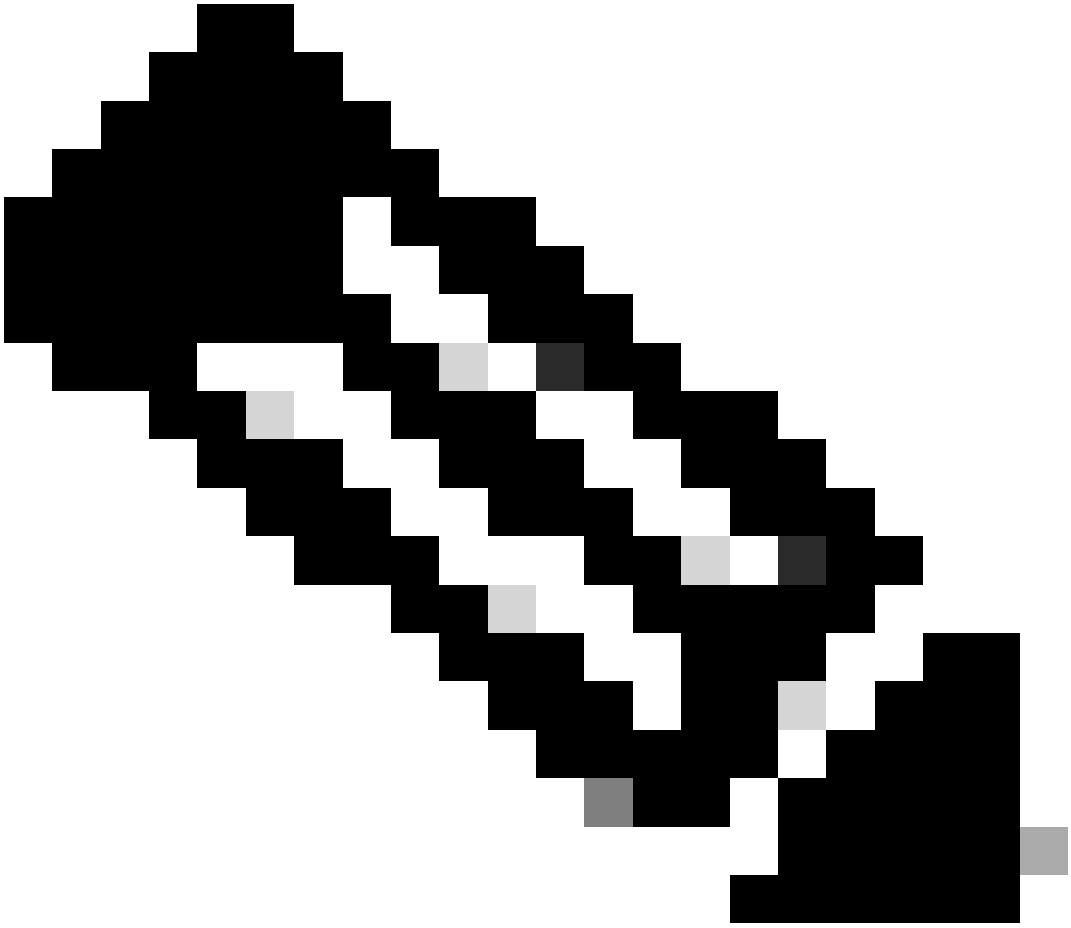
```
asav(config-ca-trustpoint)# enrollment protocol acme authentication ?

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

3. Seleccione Let's Encrypt (Cifrar) como CA ACME. Si utiliza otra CA que admita el protocolo ACME, proporcione la dirección URL adecuada.

```
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
```



Nota: Cuando se configura la palabra clave LetEncrypt, la URL del servidor Let's Encrypt se rellena automáticamente.

4. Defina el par de claves RSA, el nombre de dominio completo (FQDN) y el nombre de asunto del certificado.

```
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. Autentique el punto de confianza.

Nota: Si la CA ya existe en el firewall seguro o al utilizar Let's Encrypt, este paso se puede omitir.

```
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. Inscriba el certificado.

```
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
```

Verificación

Ver certificado instalado en ASA

Confirme que el certificado está inscrito y verifique la fecha de renovación.

```
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: e6e000000000000000000000000000000089a
SHA1 PublicKeyInfo hash: 5e300000000000000000000000000000009f
```

Eventos de Syslog

Hay nuevos registros del sistema en Secure Firewall para capturar eventos relacionados con la inscripción de certificados mediante el protocolo ACME:

- 717067: Proporciona información sobre cuándo se inicia la inscripción de certificados ACME

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

- 717068: Proporciona información sobre cuándo se realiza correctamente la inscripción de certificados ACME

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

- 717069: Proporciona información sobre cuándo falla la inscripción ACME

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

- 717070: Proporciona información relacionada con el par de claves para la inscripción o renovación de certificados

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

Troubleshoot

Si se produce un error en la inscripción de un certificado ACME, considere los siguientes pasos para identificar y resolver el problema:

- Compruebe la conectividad con el servidor: Confirme que Secure Firewall tenga conectividad de red con el servidor ACME. Compruebe que no haya problemas de red ni reglas de firewall que bloqueen la comunicación.
- Asegúrese de que el nombre de dominio de Secure Firewall se pueda resolver: Asegúrese de que el nombre de dominio configurado en Secure Firewall puede resolverse mediante el servidor ACME. Esta verificación es crucial para que el servidor valide la solicitud.
- Confirmar propiedad del dominio: Compruebe que todos los nombres de dominio especificados en el punto de confianza son propiedad de Secure Firewall. Esto garantiza que el servidor ACME puede validar la propiedad del dominio.

Comandos para Troubleshooting

Para obtener información adicional, recopile el resultado de los siguientes comandos debug:

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

Errores comunes de inscripción ACME:

Código de error	Motivo	Posible causa o remediación
7	No se puede conectar con el servidor	El servidor es accesible pero el servicio ACME no se está ejecutando.
28	No se puede conectar con el servidor	El servidor no es accesible. Compruebe el acceso de red básico al servidor ACME.
60	No se puede validar el certificado del servidor	Asegúrese de que la CA raíz o del emisor esté presente en un punto de confianza o en el grupo de confianza.
124	Tiempo de espera de procesamiento ACME	Asegúrese de que todos los FQDN solicitados se resuelven en la interfaz configurada para la autenticación HTTP-01. Asegúrese de que la URL de ACME configurada es correcta.

Información Relacionada

Para obtener ayuda adicional, póngase en contacto con el TAC. Se necesita un contrato de soporte válido: Contactos de soporte a nivel mundial de Cisco.
También puede visitar la Comunidad VPN de Cisco aquí.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).