Configuración de la inscripción de certificados con el protocolo ACME en la defensa contra amenazas de firewall seguro gestionada por FMC

Introducción

En este documento se describe el proceso para inscribir un certificado de seguridad de la capa de transporte (TLS) a través del protocolo del Entorno de administración automática de certificados (ACME) en la plataforma Firepower Threat Defence (FTD) de Secure Firewall.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre estos temas:

- Procesos manuales de inscripción de certificados y los fundamentos de Secure Sockets Layer (SSL).
- Conceptos básicos de autenticación para VPN de acceso remoto.
- Experiencia con las autoridades certificadoras (CA).

Componentes Utilizados

- Cisco FTDv versión 10.0.0-35.
- Cisco FMC versión 10.0.0-35.
- 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 previos y las restricciones actuales para la inscripción ACME en Secure Firewall FTD incluyen:

- Compatible con FTD y FMC versiones 10.0.0 y posteriores.
- ACME no permite la emisión de certificados comodín; cada solicitud de certificado debe especificar un nombre de dominio preciso.
- Cada punto de confianza inscrito a través de ACME está restringido a una única interfaz, por lo que los certificados obtenidos a través de ACME no se pueden compartir entre varias interfaces.
- Los pares de claves se generan automáticamente y son exclusivos de cada certificado inscrito a través de ACME, lo que evita la reutilización de claves y mejora la seguridad.

Consideraciones sobre downgrade

Al realizar la actualización a una versión de FTD de Secure Firewall que no admita la inscripción ACME (versión 7.7 o anterior):

- Se pierden todas las configuraciones de punto de confianza relacionadas con ACME introducidas en la versión 10.0.0 o posterior.
- Todavía se puede acceder a los certificados inscritos mediante ACME; sin embargo, sus claves privadas se desasocian después de la primera operación de guardar y reiniciar después de la reversión.

Si es necesario un downgrade, utilice la solución alternativa recomendada:

- Antes de realizar la degradación, exporte los certificados ACME en formato PKCS12.
- Antes de realizar la degradación, elimine la configuración del punto de confianza ACME.
- Después de la actualización, importe el certificado PKCS12. El punto de confianza importado permanece válido hasta que caduca el certificado emitido por ACME.

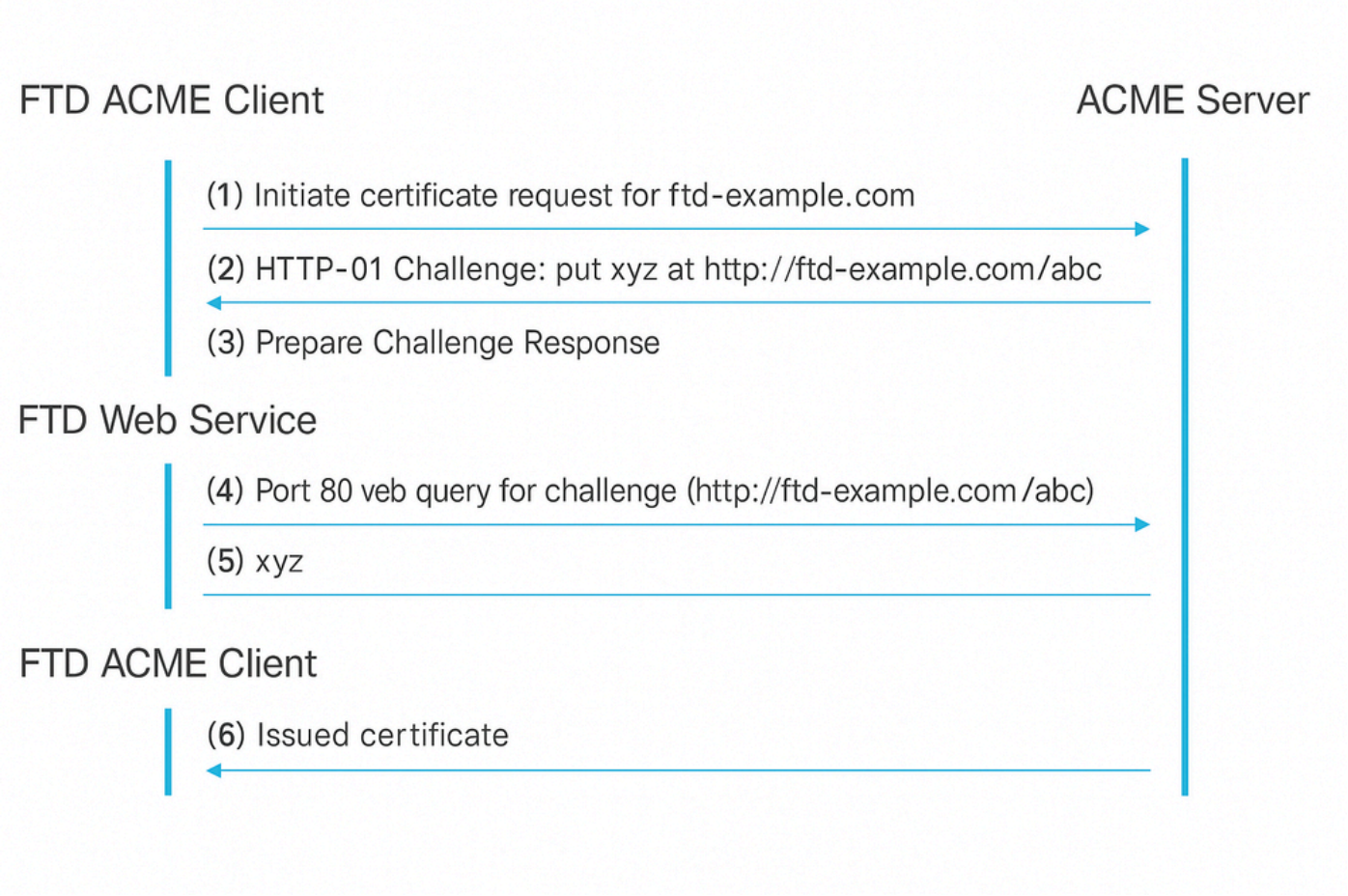
Antecedentes

El protocolo ACME tiene como objetivo simplificar la gestión de certificados TLS para los administradores de red. A través de ACME, los administradores pueden automatizar las tareas relacionadas con la adquisición y renovación de certificados TLS. Esta automatización es especialmente útil cuando se trabaja con entidades emisoras de certificados (CA) como Let's Encrypt, que proporcionan certificados gratuitos, automatizados y accesibles públicamente a

través del protocolo ACME.ACME facilita la emisión de certificados de validación de dominio (DV). Estos certificados comprueban que el solicitante del certificado tiene control sobre los dominios especificados. La validación se realiza normalmente a través de un proceso de impugnación basado en HTTP, en el que el solicitante coloca un archivo designado en su servidor web. A continuación, la Autoridad de certificación (CA) obtiene acceso a este archivo a través del servidor HTTP del dominio para confirmar el control del dominio. Si se supera correctamente este desafío, la CA podrá emitir el certificado de DV.

El proceso de inscripción incluye los siguientes pasos:

1. Iniciar solicitud de certificado: El cliente envía una solicitud de certificado al servidor ACME, especificando los dominios para los que se necesita el certificado.
2. Recibir desafío de HTTP-01: El servidor ACME responde con un desafío HTTP-01 que contiene un token único que el cliente debe utilizar para probar la propiedad del dominio.
3. Preparar respuesta al desafío:
    1. El cliente genera una autorización de clave al combinar el token del servidor ACME con su clave de cuenta.
    2. 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 proporcionada para obtener la autorización de clave.
5. El servidor ACME verifica la propiedad: El servidor compara la autorización de clave recuperada con el valor esperado para comprobar el control del cliente sobre el dominio.
6. Emitir certificado: Tras la validación correcta, el servidor ACME emite el certificado SSL/TLS al cliente.



Flujo de autenticación HTTP-01 de inscripción ACME.

Entre las principales ventajas de utilizar el protocolo ACME para inscribir certificados TLS en Secure Firewall FTD se incluyen:

- Automatización de la administración de certificados: ACME agiliza el proceso de obtención y mantenimiento de certificados de dominio TLS para interfaces TLS de FTD de Secure Firewall, lo que reduce significativamente las tareas administrativas manuales.
- Renovación automática de certificados: Con los puntos de confianza habilitados para ACME, los certificados se renuevan automáticamente a medida que se acerca el vencimiento, lo que minimiza la necesidad de una intervención administrativa continua.
- Garantía de seguridad continua: Esta automatización garantiza que los certificados sigan siendo válidos sin interrupción, lo que evita que caduquen de forma inesperada y mantiene comunicaciones seguras.

Estas ventajas mejoran colectivamente la eficacia operativa y la seguridad para las implementaciones de FTD de firewall seguro.

Configurar

Prerrequisitos de Configuración

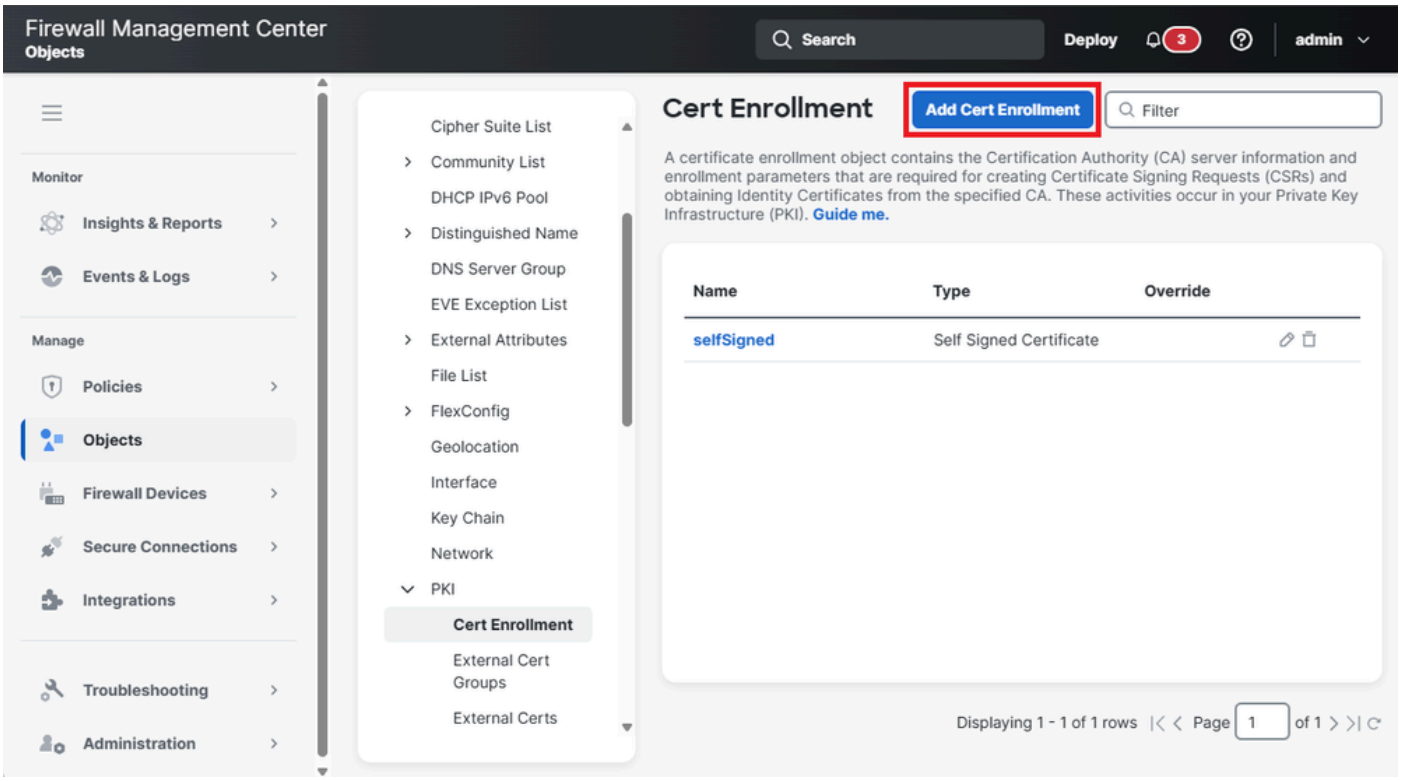
Antes de iniciar el proceso de inscripción en ACME, asegúrese de que se cumplen las siguientes condiciones:

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 de firewall seguro 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.

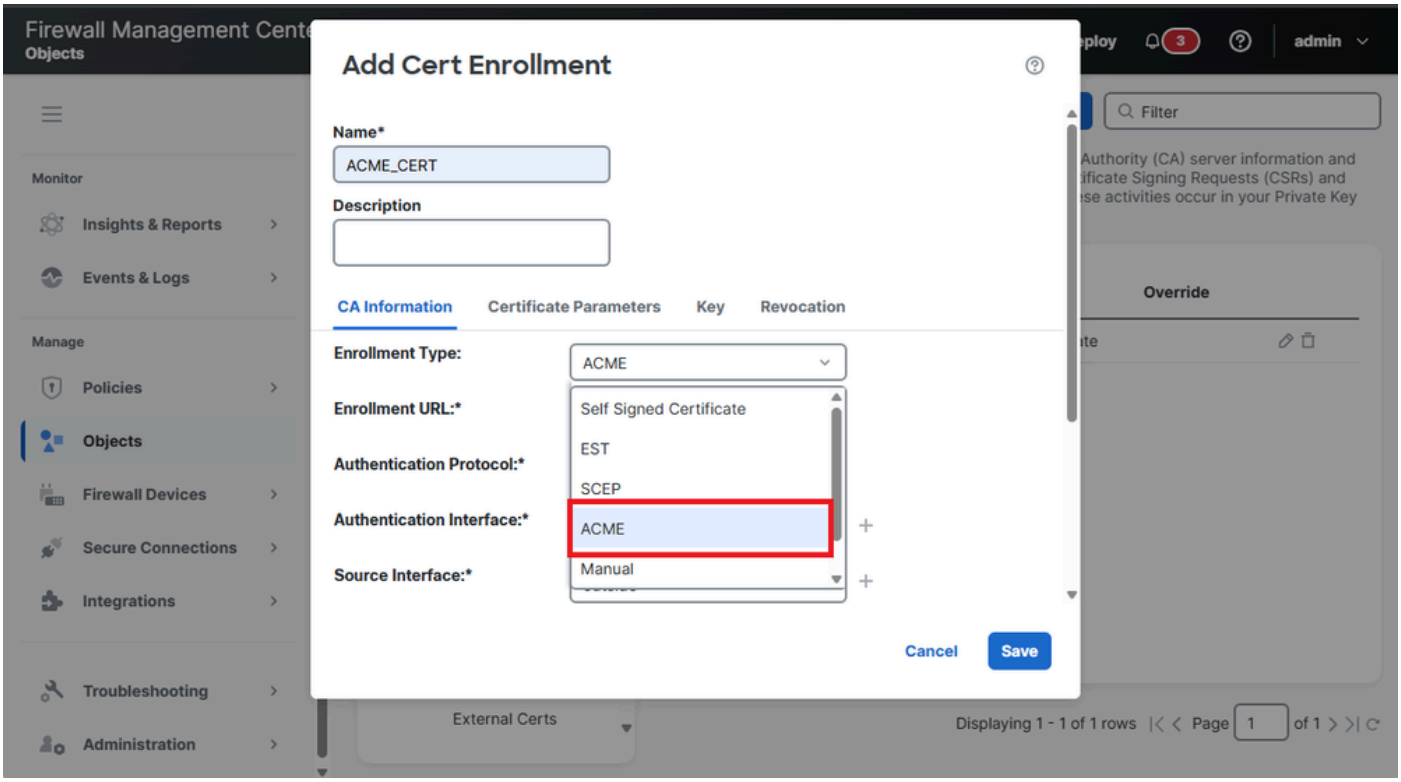
Nota: Durante el período en el que el puerto 80 está abierto, solo se puede acceder a los datos de desafío de ACME.

Creación de objetos de inscripción de certificados ACME

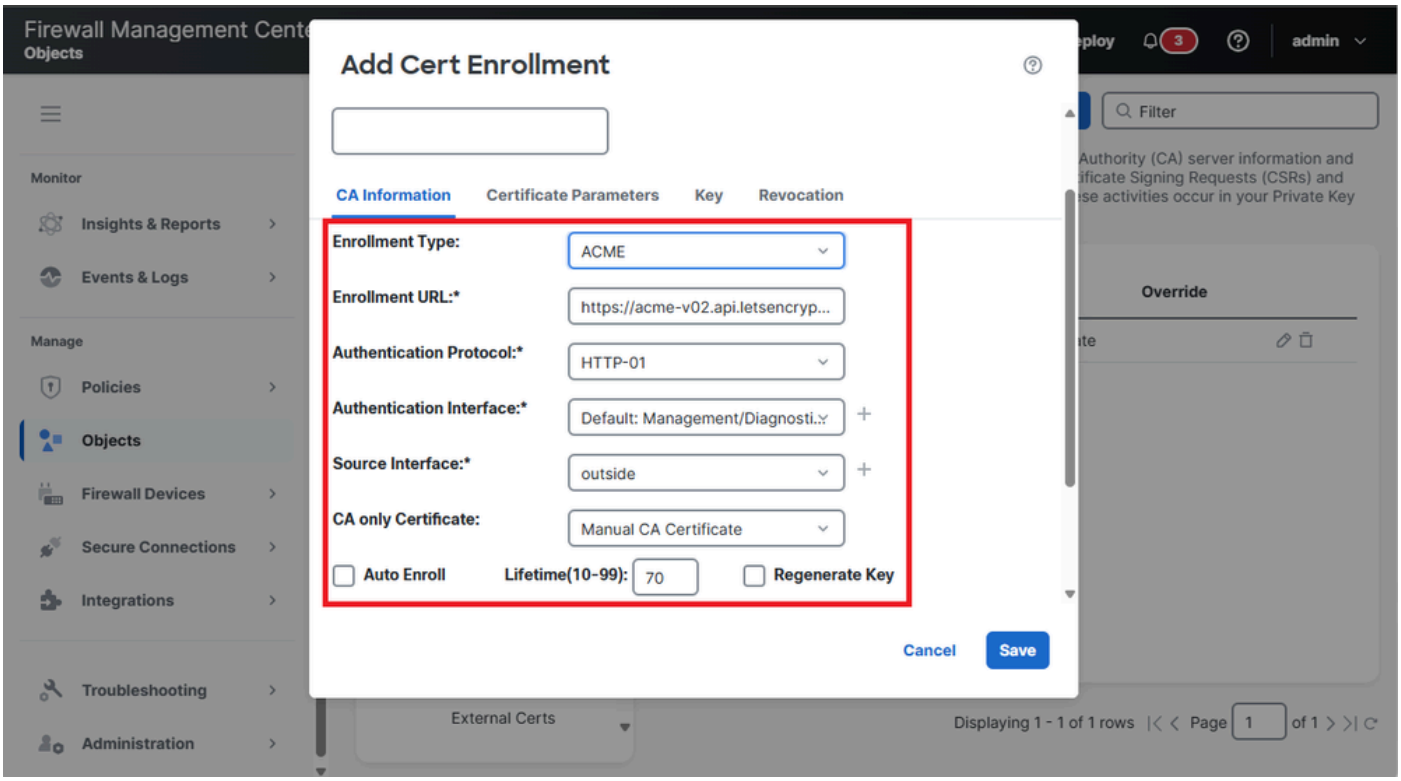
1. Navegue hasta Objetos > PKI > Inscripción de Cert y haga clic en Agregar Inscripción de Cert para comenzar el proceso de configuración.



2. La opción ACME enrollment aparece en el menú desplegable junto con otros métodos de inscripción. Seleccione ACME en el menú desplegable Tipo de inscripción para continuar.



3. Se muestran las opciones para configurar los parámetros del certificado. Complete los campos con la información correspondiente.

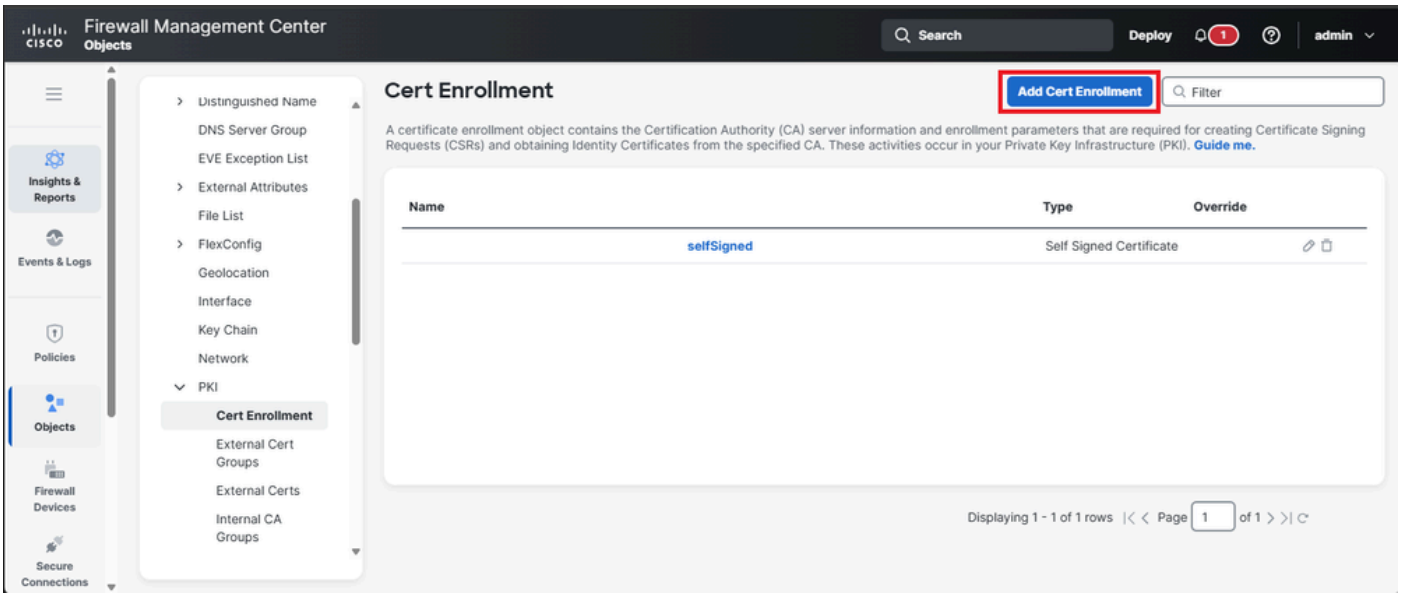


- URL de inscripción: Se trata de la dirección del servidor ACME (como Let's Encrypt) utilizado para solicitar y recuperar certificados.
- Protocolo de autenticación: Especifica el método empleado para comprobar la propiedad del dominio. El protocolo admitido para los retos de ACME es HTTP-01.
- Interfaz de autenticación: La interfaz de red en el dispositivo FTD que recibe el desafío HTTP-01 del servidor ACME.
- Certificado solo de CA: Se debe elegir un certificado de una autoridad de certificación (CA) para confiar en el servidor ACME.

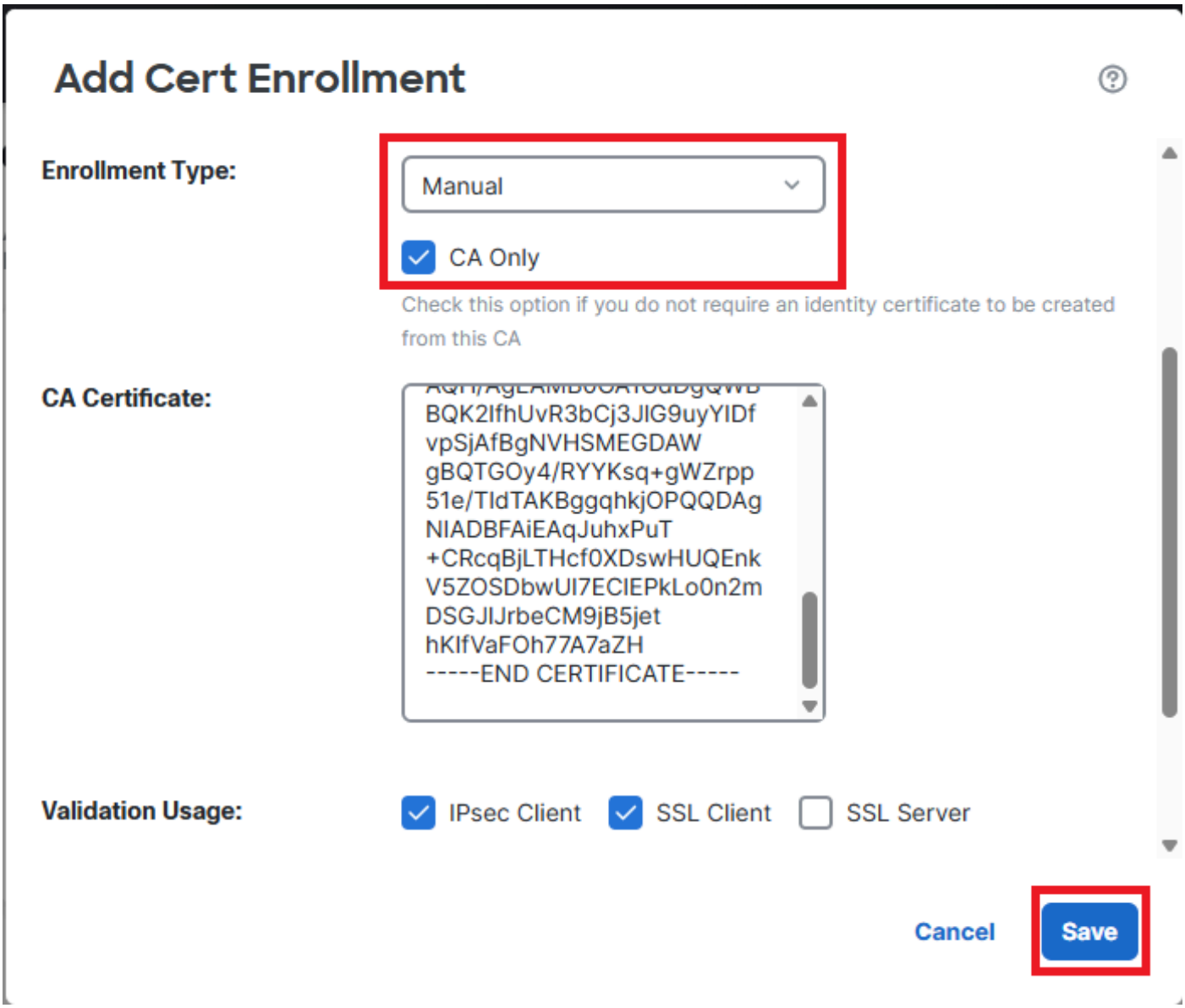
Nota: De forma predeterminada, apunta a la URL pública del servicio Let's Encrypt: https://acme-v02.api.letsencrypt.org/directory.

---

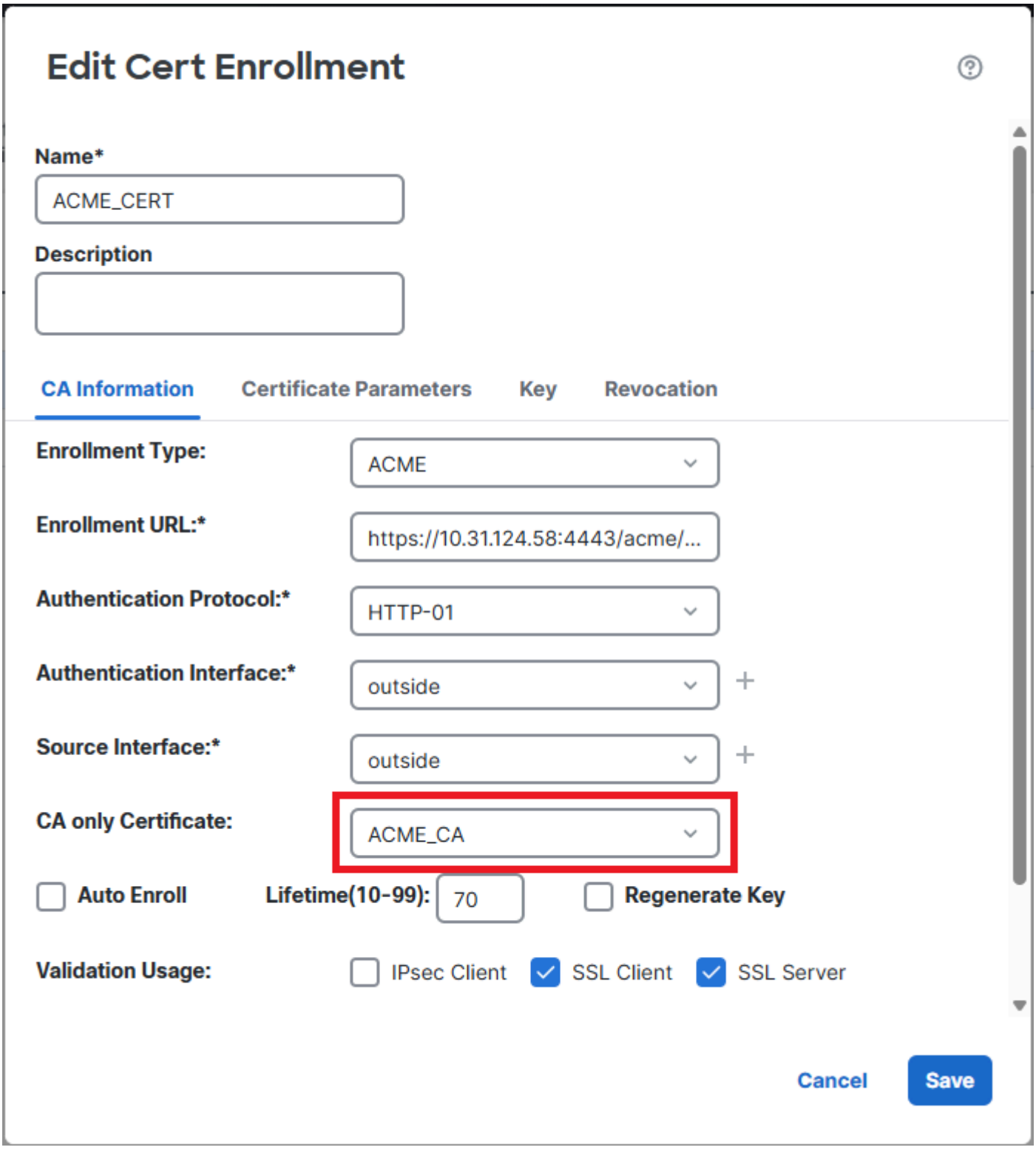
4. Si utiliza un servidor ACME que no es muy conocido, debe agregar el certificado de CA del servidor ACME. Navegue hasta Objetos > Inscripción de certificados y haga clic en el botón Agregar inscripción de certificados.



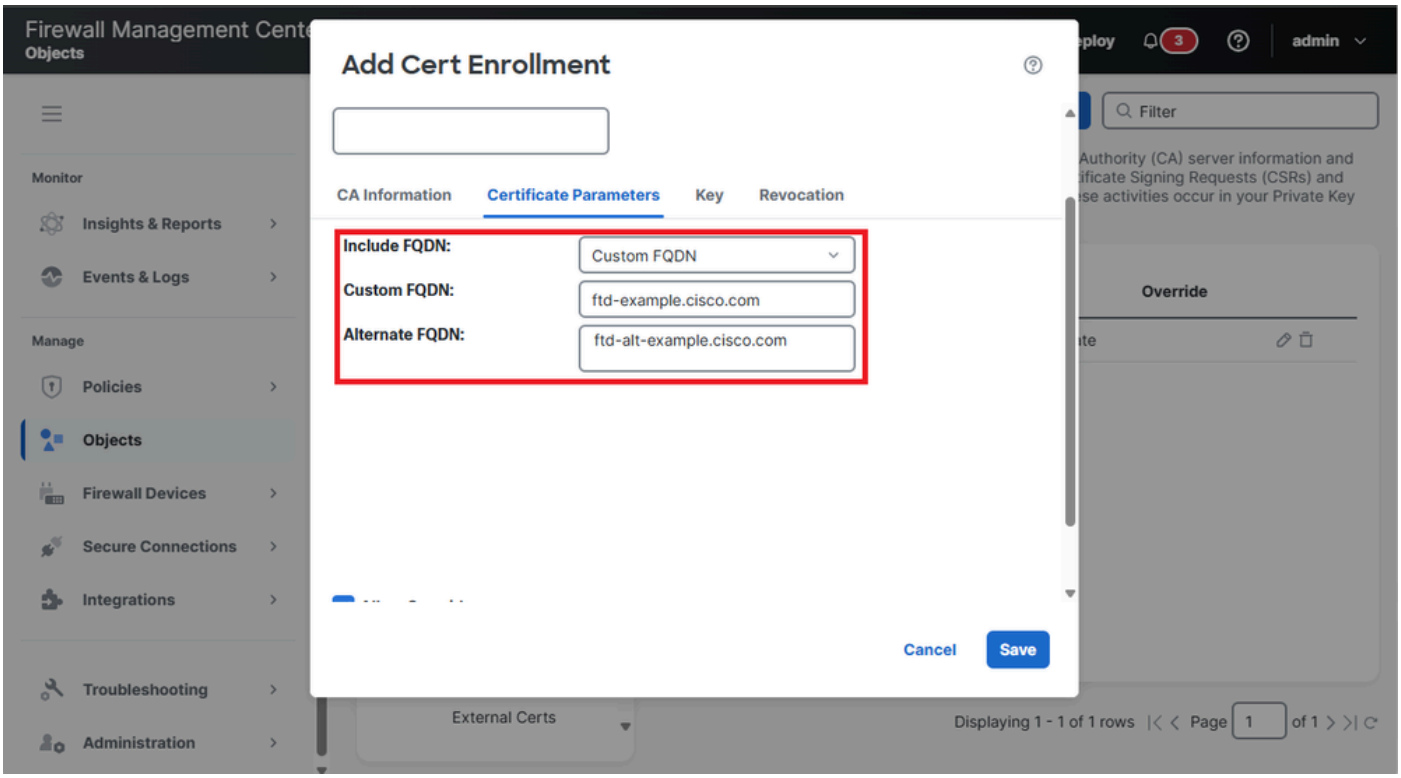
- Dé un nombre al punto de confianza y seleccione el Tipo de inscripción como Manual. A continuación, marque la opción CA Only. Por último, pegue el certificado de CA del servidor ACME y haga clic en Guardar.



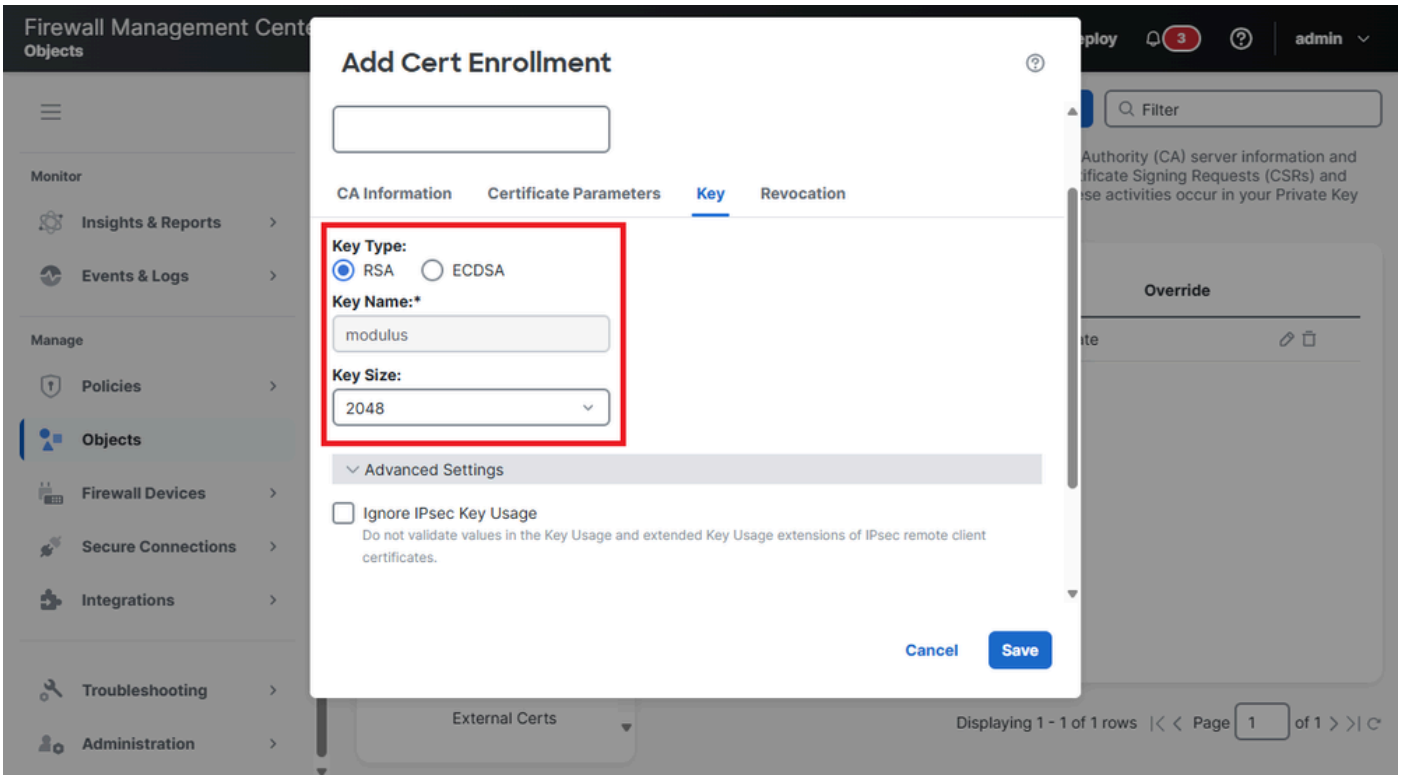
- Por último, seleccione el punto de confianza del servidor ACME CA en la sección Certificado sólo CA.



5. Navegue hasta Parámetros de certificado, seleccione la opción FQDN personalizado en el cuadro Incluir FQDN y rellene los campos FQDN personalizado y FQDN alternativo con el FQDN principal y cualquier nombre de dominio alternativo que se incluya en el certificado.



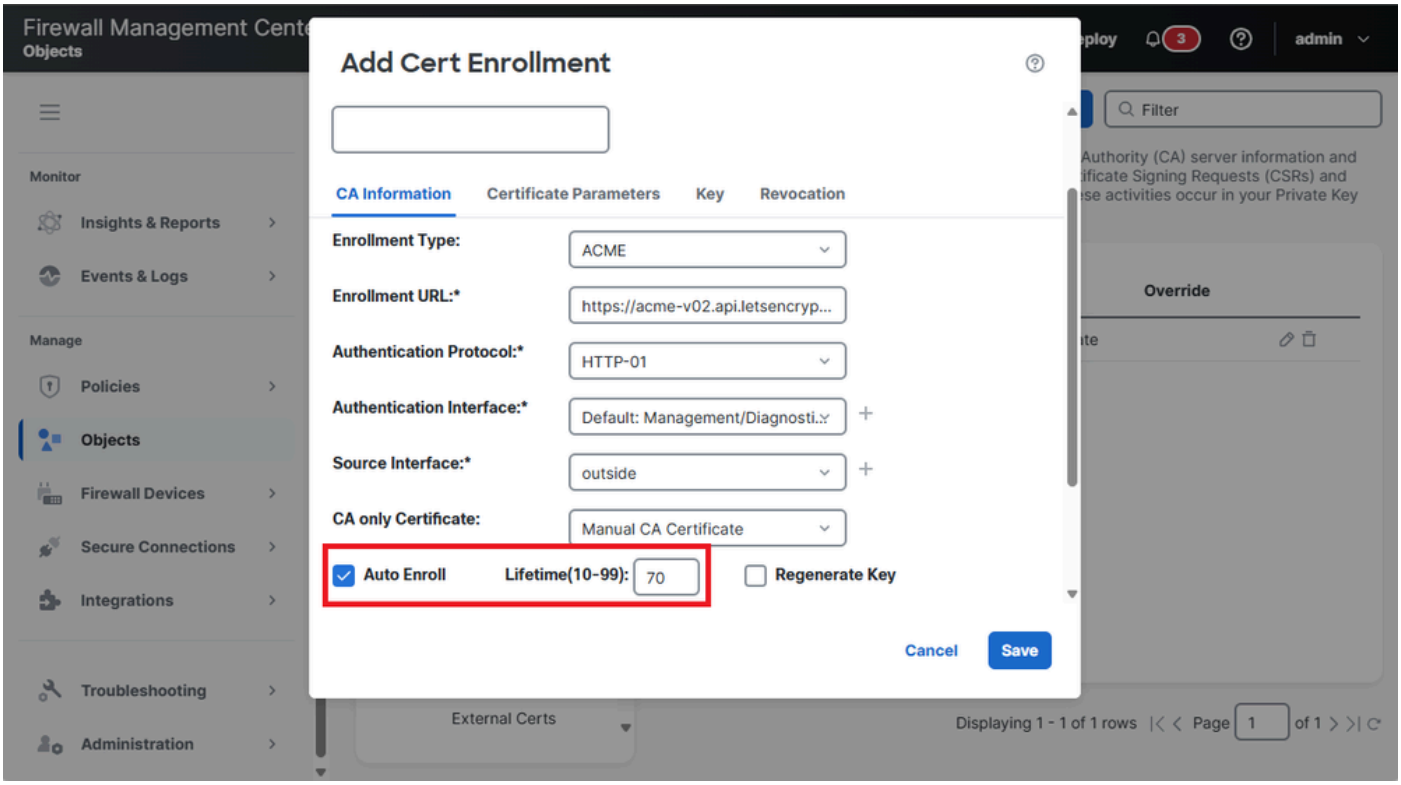
6. Acceda a Clave para modificar los parámetros Tipo de Clave y Tamaño de Clave.



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

Marque la casilla de verificaciónInscripción automática y especifique el porcentaje para la duración de la inscripción automática.

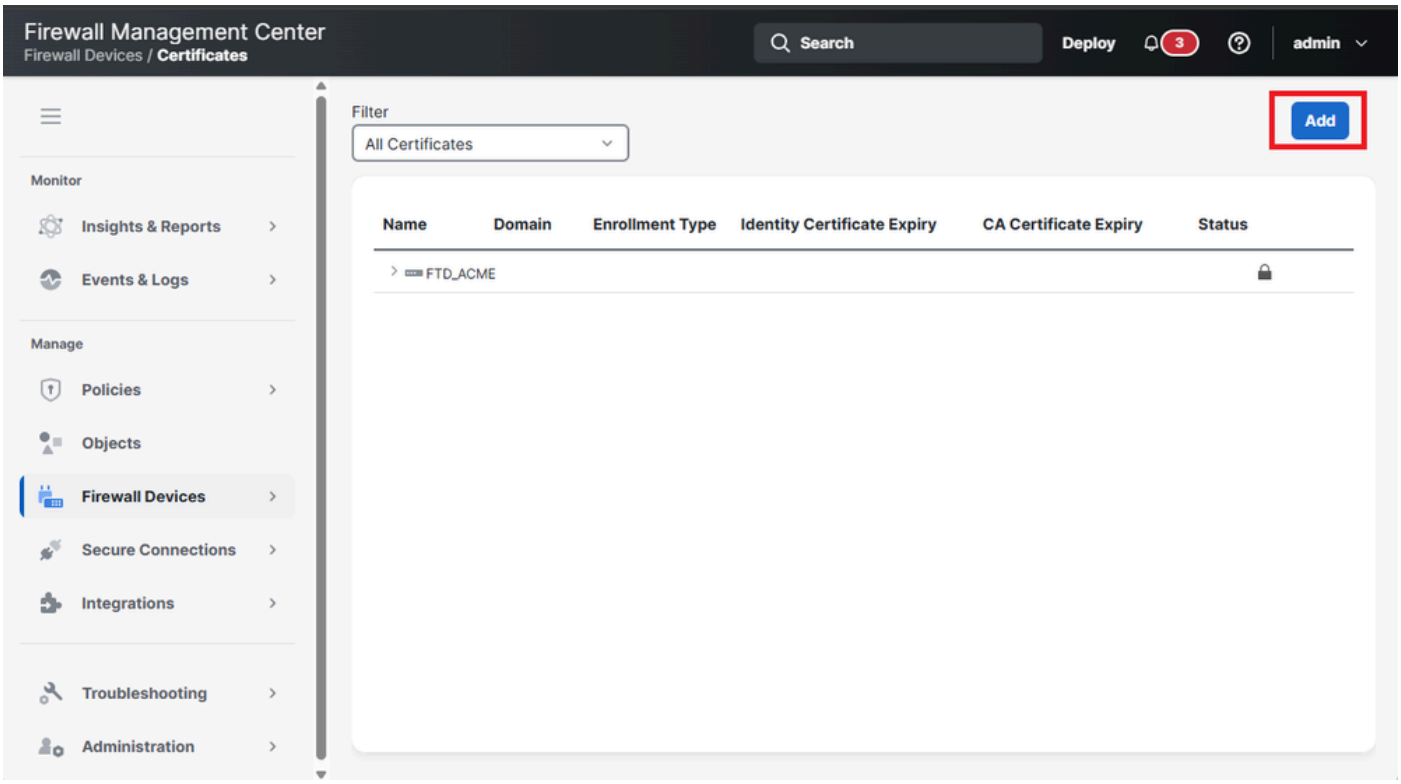
Esta función garantiza que el certificado se renueva automáticamente antes de que caduque. El porcentaje determina con cuánta antelación a la expiración del certificado comienza el proceso de renovación. Por ejemplo, si se establece en 80%, el proceso de renovación comienza cuando el certificado alcanza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



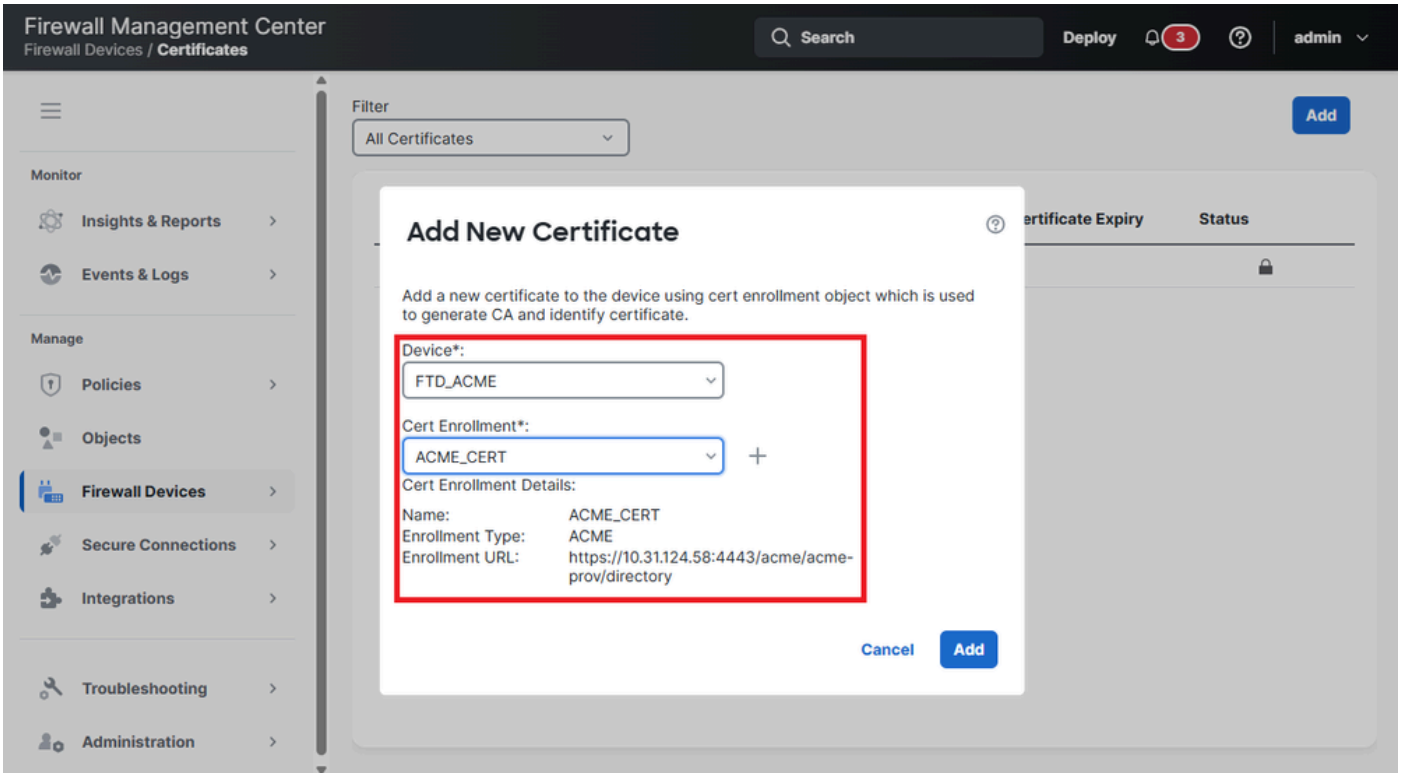
8. Haga clic en Guardar.

Inscripción de certificados ACME en el dispositivo

1. Navegue hasta Firewall Devices > Certificates y haga clic en el botón Add para inscribir un nuevo certificado.

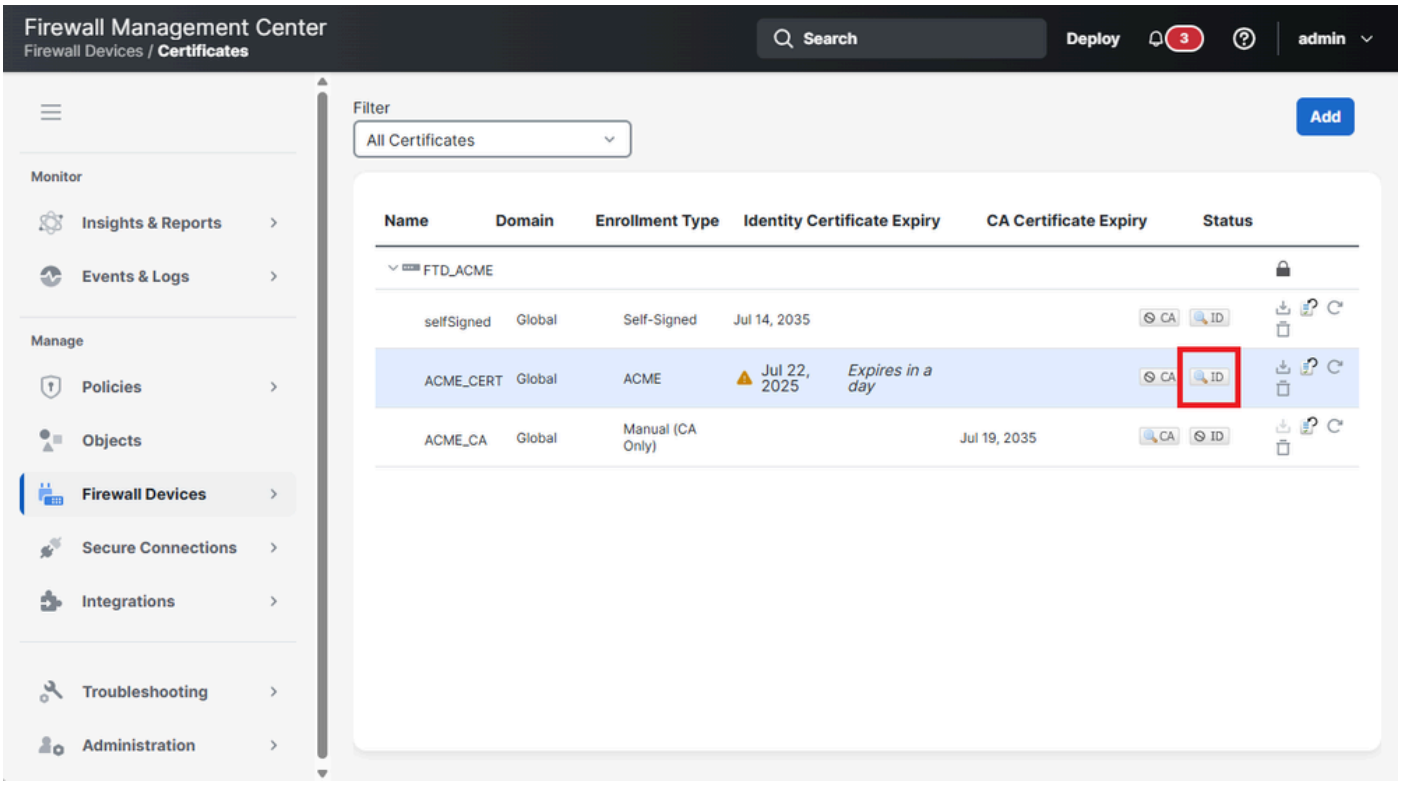


2. Seleccione el dispositivo FTD de la lista desplegable Dispositivo y el objeto de certificado creado anteriormente en Inscripción de Certificados.

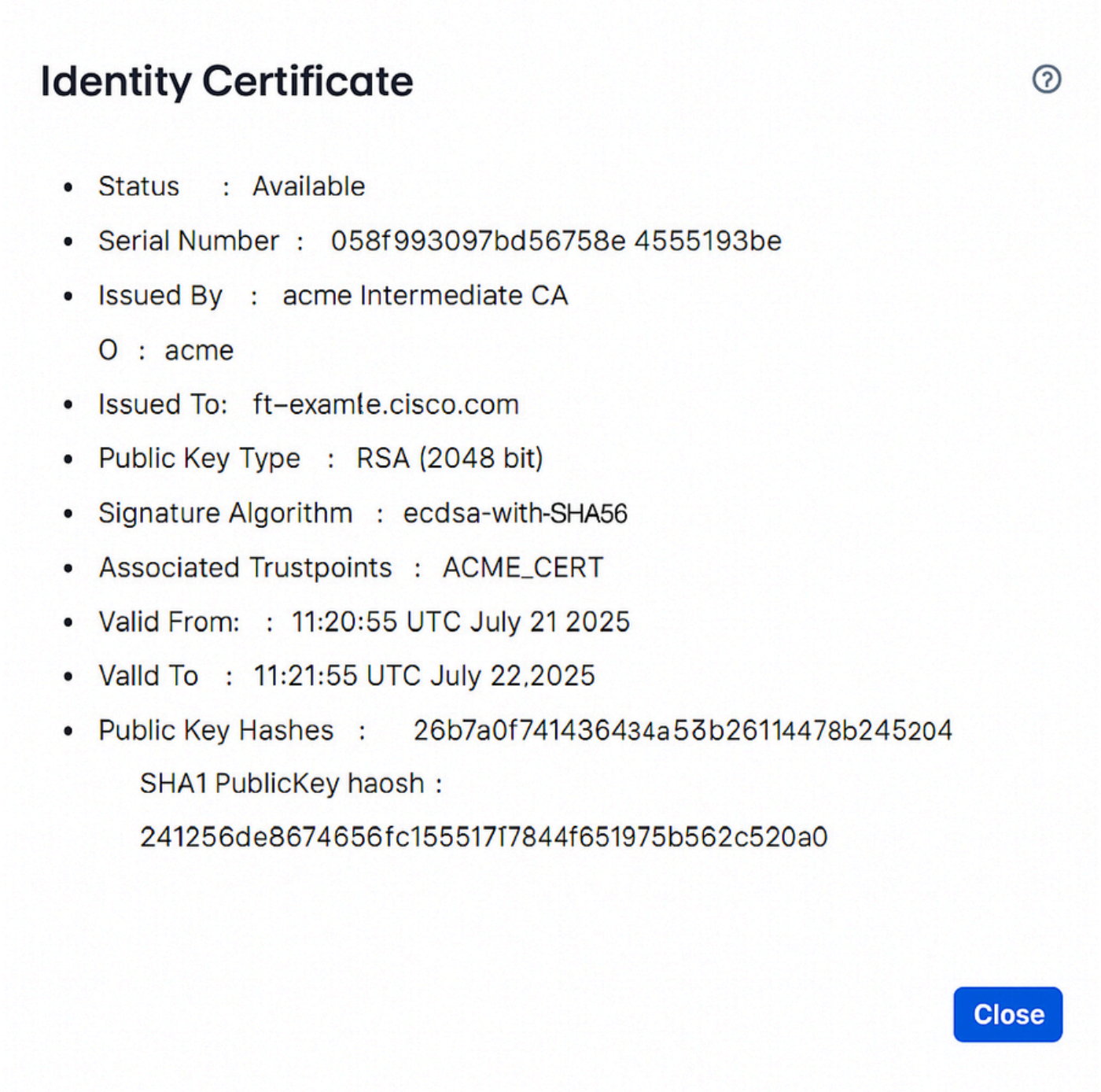


3. Haga clic en Agregar.

4. Una vez finalizado el despliegue, la columna de estado muestra el botón Certificado de ID.



5. Valide la información del certificado de ID haciendo clic en el botón ID.



Verificación

Ver certificado instalado en FTD

Confirme que el certificado esté inscrito con el comando.show crypto ca certificates <Trust Point Name>.

<#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
```

Eventos de Syslog

Hay nuevos registros del sistema en el FTD de 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.

```
%FTD-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.

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

- 717069: Proporciona información sobre cuándo falla la inscripción ACME.

```
%FTD-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.

```
%FTD-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 tiene 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 firewall seguro se puede resolver:asegúrese de que el nombre de dominio configurado en el FTD de firewall seguro se puede resolver 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 del FTD 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>

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).