Configurar a inscrição de certificado com o protocolo ACME no Secure Firewall Threat Defense Gerenciado pelo FMC

Introdução

Este documento descreve o processo para registrar um certificado TLS (Transport Layer Security) através do protocolo ACME (Automated Certificate Management Environment) na plataforma FTD (Secure Firewall Firepower Threat Defense).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

- Processos manuais de registro de certificado e os fundamentos do Secure Sockets Layer (SSL).
- Conceitos básicos de autenticação para VPNs de acesso remoto.
- Experiência com autoridades de certificação (CAs).

Componentes Utilizados

- Cisco FTDv versão 10.0.0-35.
- Cisco FMC versão 10.0.0-35.
- Servidor de Autoridade de Certificação (CA) que suporta o protocolo ACME.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Requisitos e limitações

Os pré-requisitos e restrições atuais para a inscrição da ACME no FTD do Secure Firewall incluem:

- Suportado no FTD e no FMC versões 10.0.0 e posteriores.
- A ACME não permite a emissão de certificados curinga; cada solicitação de certificado deve especificar um nome de domínio preciso.
- Cada ponto confiável registrado por meio do ACME é restrito a uma única interface, portanto os certificados obtidos por meio do ACME não podem ser compartilhados em várias interfaces.
- Os pares de chaves são gerados automaticamente e são exclusivos para cada certificado registrado via ACME, evitando a reutilização de chaves e aumentando a segurança.

Considerações sobre downgrade

Ao fazer o downgrade para uma versão do FTD do Secure Firewall que não ofereça suporte à inscrição no ACME (versão 7.7 ou anterior):

- Todas as configurações de ponto confiável relacionadas ao ACME introduzidas na versão 10.0.0 ou posterior são perdidas.
- Os certificados inscritos através do ACME ainda estão acessíveis; no entanto, suas chaves privadas tornam-se desassociadas após o primeiro salvamento e reinicialização após o downgrade.

Se um downgrade for necessário, use a solução recomendada:

- Antes de fazer o downgrade, exporte os certificados ACME no formato PKCS12.
- Antes de fazer o downgrade, remova a configuração do ponto de confiança do ACME.
- Após o downgrade, importe o certificado PKCS12. O ponto confiável importado permanece válido até que o certificado emitido pelo ACME expire.

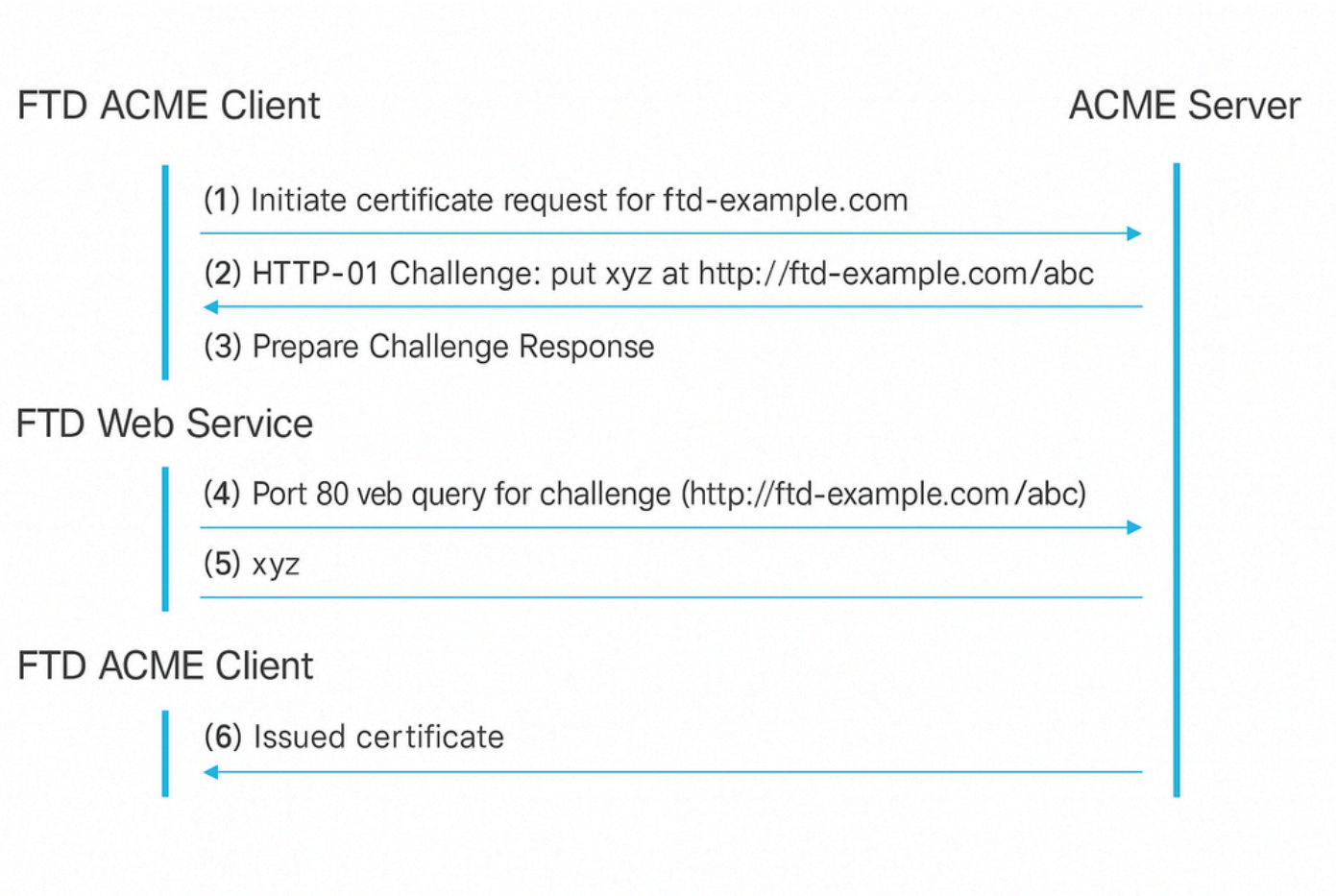
Informações de Apoio

O protocolo ACME tem como objetivo simplificar o gerenciamento de certificados TLS para administradores de rede. Através do ACME, os administradores podem automatizar as tarefas envolvidas na aquisição e renovação de certificados TLS. Essa automação é especialmente útil ao trabalhar com autoridades de certificação (CAs), como Let's Encrypt, que fornecem certificados gratuitos, automatizados e acessíveis publicamente através do protocolo ACME.O ACME facilita a emissão de certificados de validação de domínio (DV). Esses certificados verificam se o solicitante do certificado tem controle sobre os domínios especificados. A validação geralmente ocorre por meio de um processo de desafio baseado em HTTP, em que o candidato coloca um

arquivo designado em seu servidor Web. Em seguida, a CA (Certificate Authority, Autoridade de Certificação) acessa esse arquivo por meio do servidor HTTP do domínio para confirmar o controle do domínio. A aprovação bem-sucedida neste desafio permite que a CA emita o certificado de DV.

O processo de inscrição envolve estas etapas:

1. Iniciar solicitação de certificado: O cliente envia uma solicitação de certificado ao servidor ACME, especificando os domínios para os quais o certificado é necessário.
2. Receber desafio HTTP-01: O servidor ACME responde com um desafio HTTP-01 contendo um token exclusivo que o cliente deve usar para comprovar a propriedade do domínio.
3. Preparar resposta de desafio:
    1. O cliente gera uma autorização de chave combinando o token do servidor ACME com sua chave de conta.
    2. O cliente configura seu servidor Web para atender a essa autorização de chave em um caminho de URL específico.
4. O servidor ACME recupera o desafio: O servidor ACME executa uma solicitação HTTP GET ao URL fornecido para obter a autorização da chave.
5. O servidor ACME verifica a propriedade: O servidor compara a autorização da chave recuperada com o valor esperado para verificar o controle do cliente sobre o domínio.
6. Emitir certificado: Após a validação bem-sucedida, o servidor ACME emite o certificado SSL/TLS para o cliente.



Fluxo de Autenticação HTTP-01 da Inscrição ACME.

Os principais benefícios do uso do protocolo ACME para registrar certificados TLS no FTD do Secure Firewall incluem:

- Automação do gerenciamento de certificados: O ACME simplifica o processo de obtenção e manutenção de certificados de domínio TLS para interfaces TLS FTD com firewall seguro, reduzindo significativamente as tarefas administrativas manuais.
- Renovação automática de certificado: Com os pontos de confiança habilitados para ACME, os certificados são renovados automaticamente à medida que se aproximam da expiração, minimizando a necessidade de intervenção administrativa contínua.
- Garantia de segurança contínua: Essa automação garante que os certificados permaneçam válidos sem interrupções, evitando expirações inesperadas de certificados e mantendo comunicações seguras.

Essas vantagens, em conjunto, melhoram a eficiência operacional e a segurança para implantações de FTD do Secure Firewall.

Configurar

Configuração de pré-requisitos

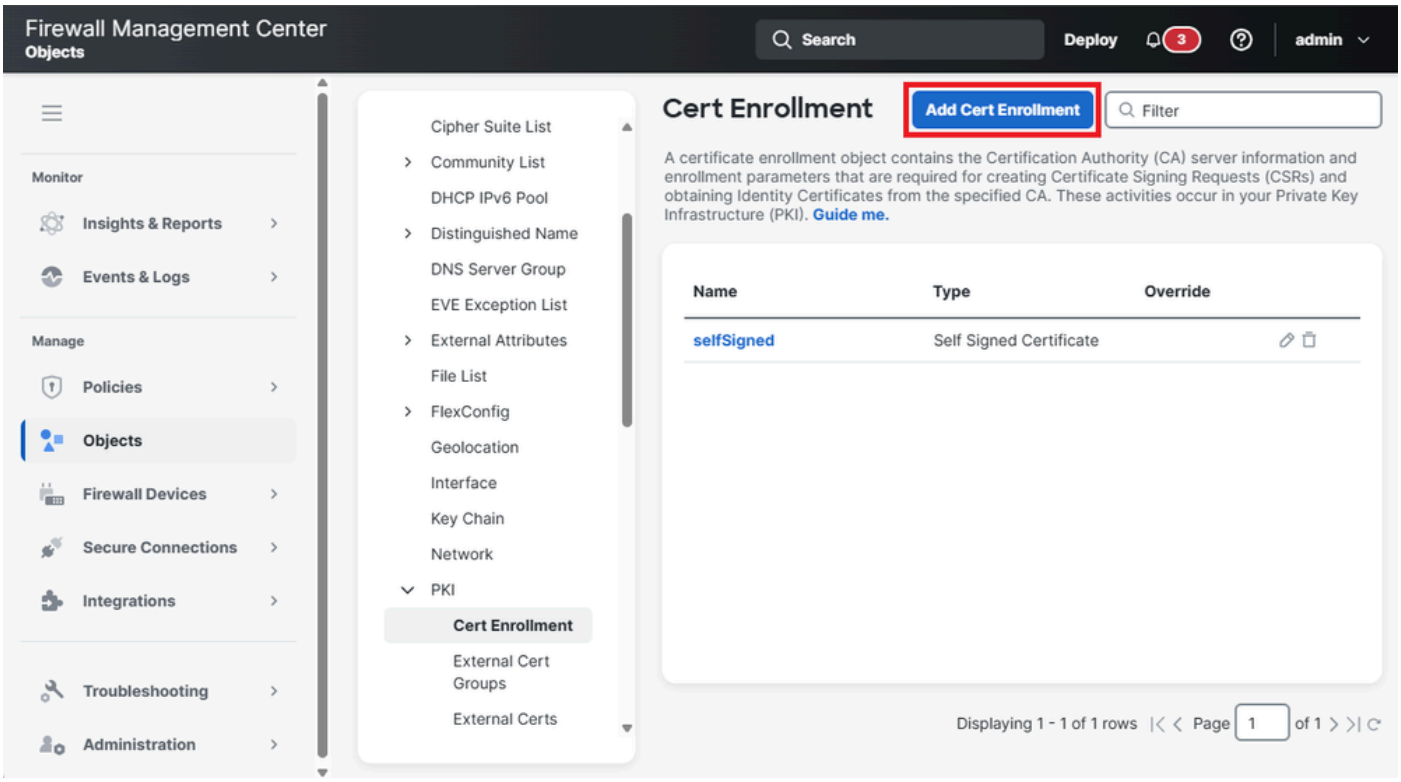
Antes de iniciar o processo de inscrição no ACME, certifique-se de que as próximas condições sejam atendidas:

1. Nome de domínio resolvível:O nome de domínio para o qual você solicita um certificado deve ser resolvível pelo servidor ACME. Isso garante que o servidor possa verificar a propriedade do domínio.
2. Acesso seguro de firewall ao servidor ACME:o firewall seguro deve ter a capacidade de acessar o servidor ACME por meio de uma de suas interfaces. Esse acesso não precisa ser feito através da interface para a qual o certificado é solicitado.
3. Disponibilidade da porta TCP 80: permita a porta TCP 80 do servidor CA ACME para a interface que corresponde ao nome do domínio. Isso é necessário durante o processo de troca do ACME para concluir o desafio HTTP-01.

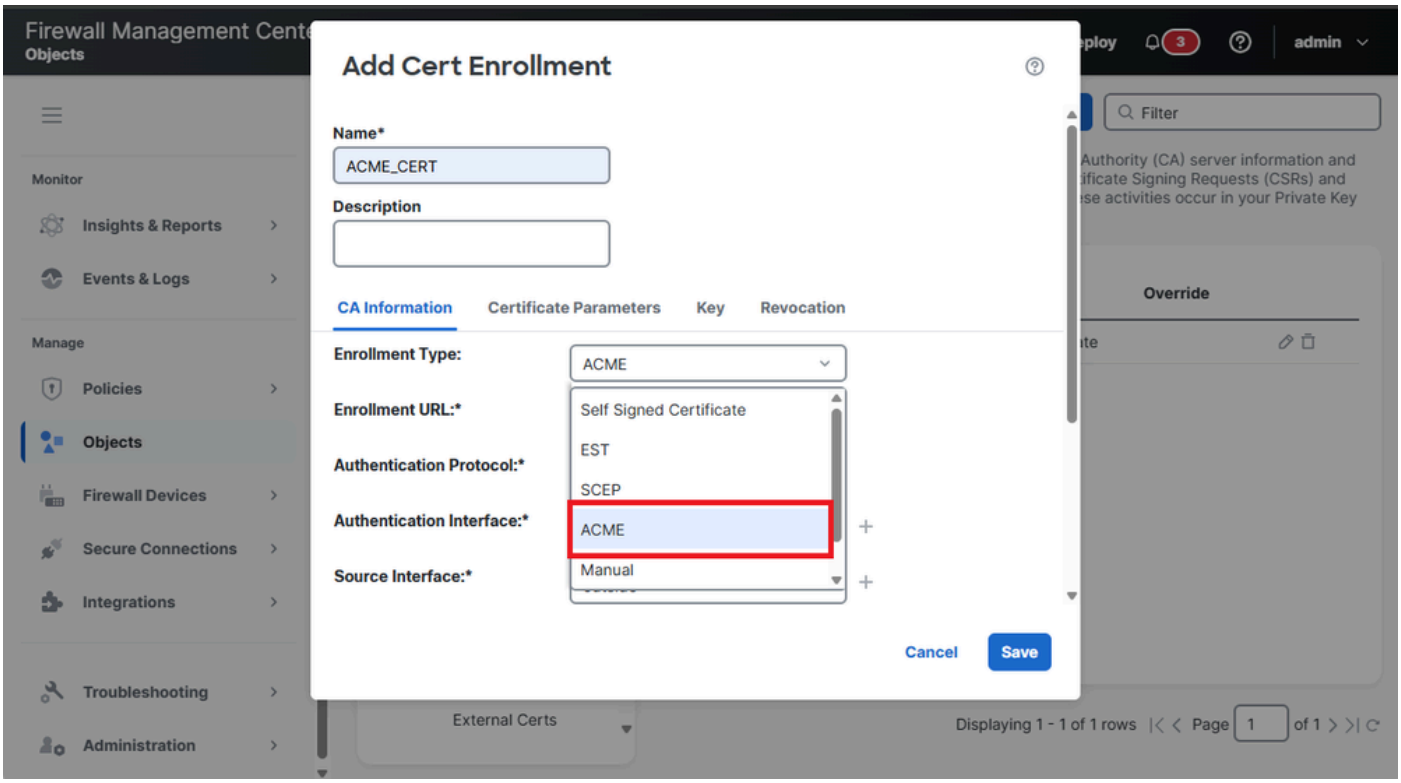
Note: Durante o período em que a porta 80 está aberta, somente os dados de desafio do ACME estão acessíveis.

Criação de Objeto de Registro de Certificado ACME

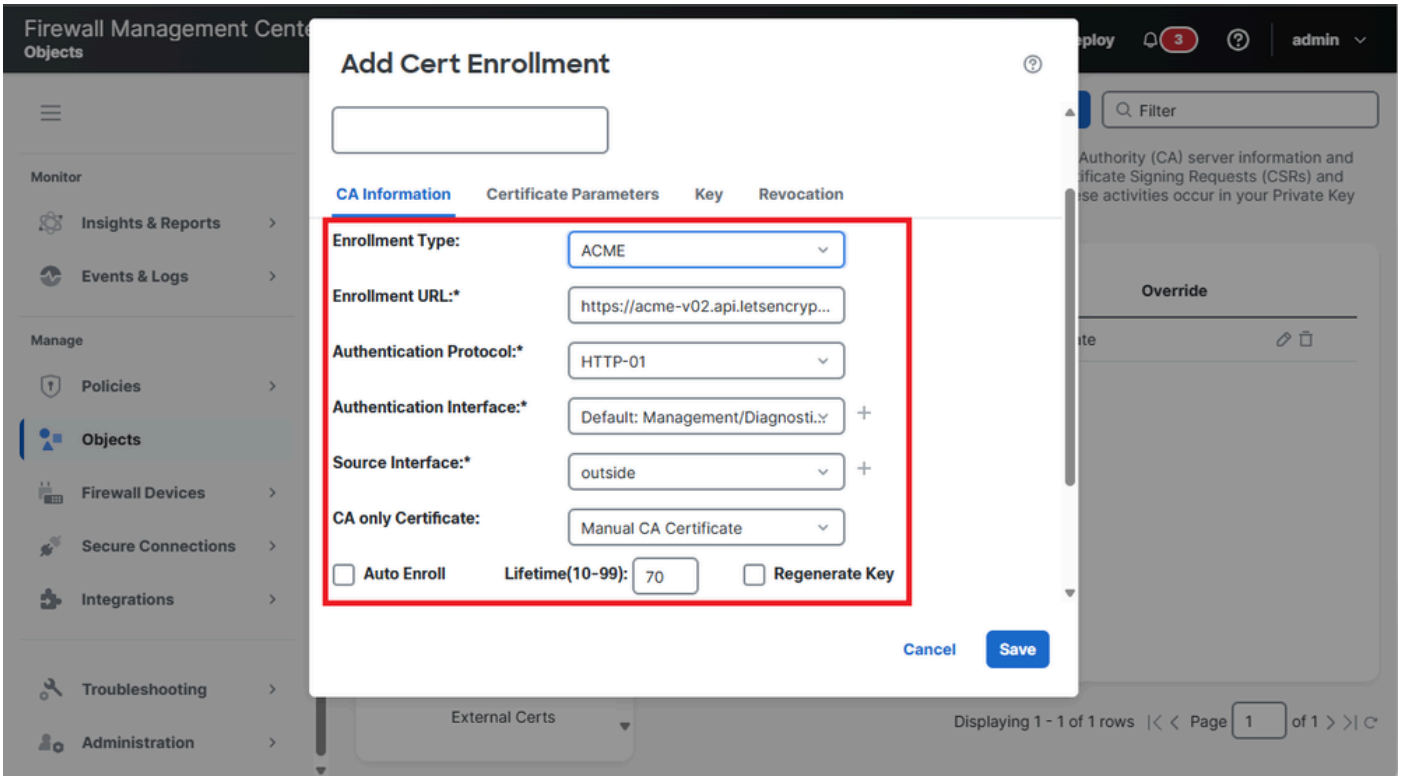
1. Navegue até Objects > PKI > Cert Enrollment e clique em Add Cert Enrollment para iniciar o processo de configuração.



2. A opção de inscrição no ACME é listada no menu suspenso juntamente com outros métodos de inscrição. Selecione ACME no menu suspenso Enrollment Type para continuar.



3. As opções para configurar parâmetros de certificado são exibidas, preencha os campos com as informações apropriadas.



- URL de inscrição: Esse é o endereço do servidor ACME (como Let's Encrypt) usado para solicitar e recuperar certificados.
- Protocolo de autenticação: Especifica o método empregado para verificar a propriedade do

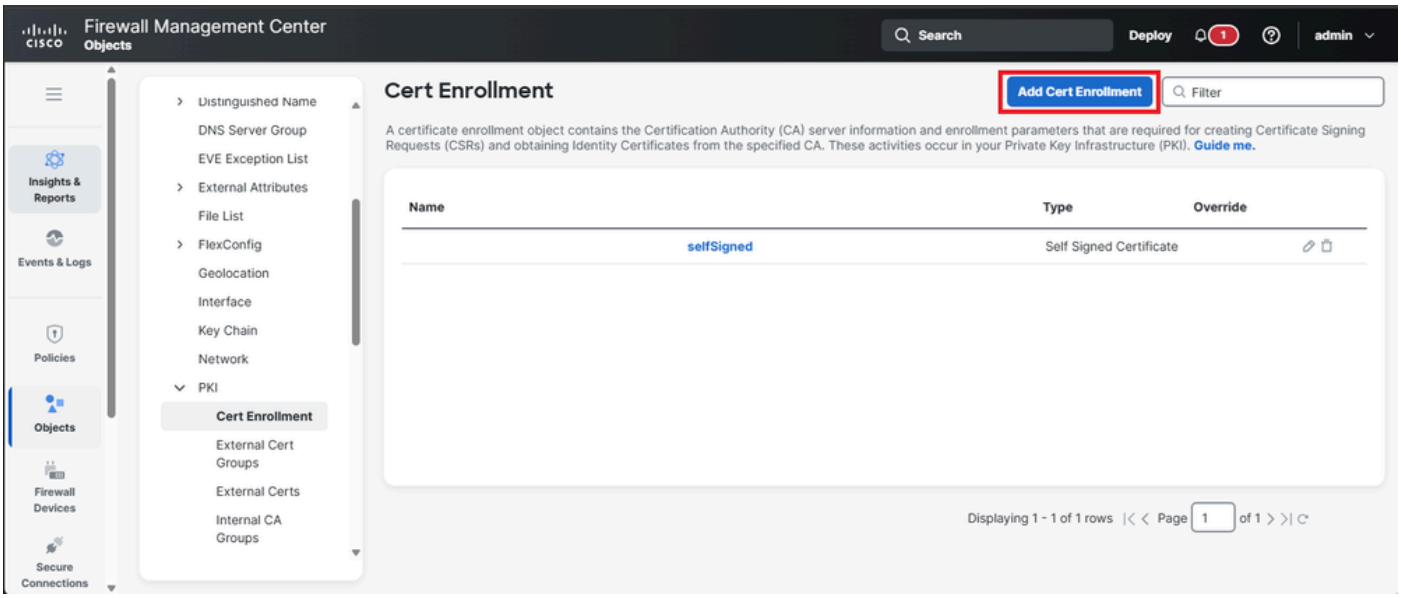
domínio. O protocolo suportado para os desafios da ACME é HTTP-01.

- Interface de autenticação: A interface de rede no dispositivo FTD que recebe o desafio HTTP-01 do servidor ACME.
- Certificado Somente CA: É necessário escolher um certificado de uma CA (Autoridade de Certificação) para confiar no servidor ACME.

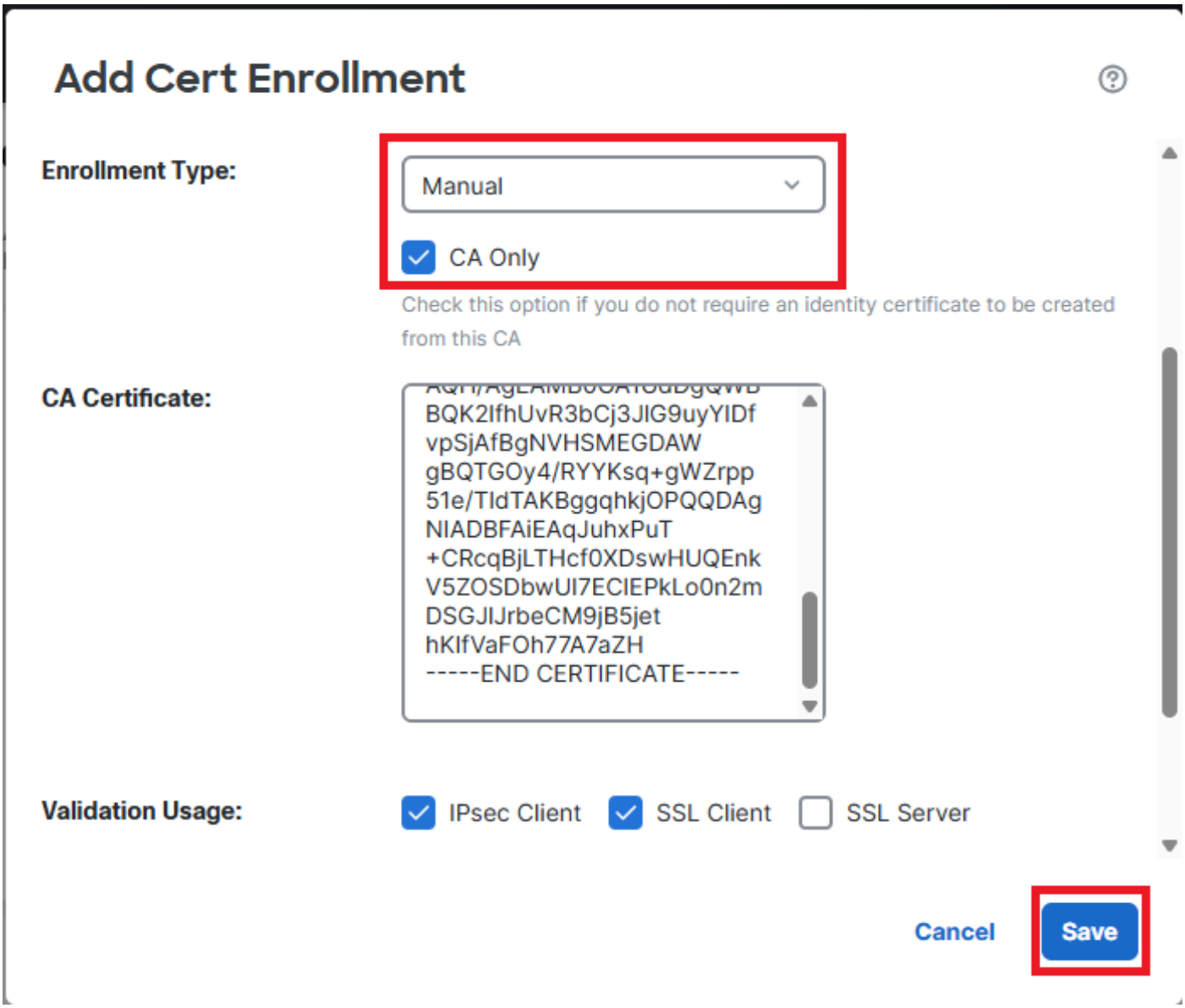
Note: Por padrão, ele aponta para a URL do serviço Let's Encrypt pública: https://acme-v02.api.letsencrypt.org/directory.

---

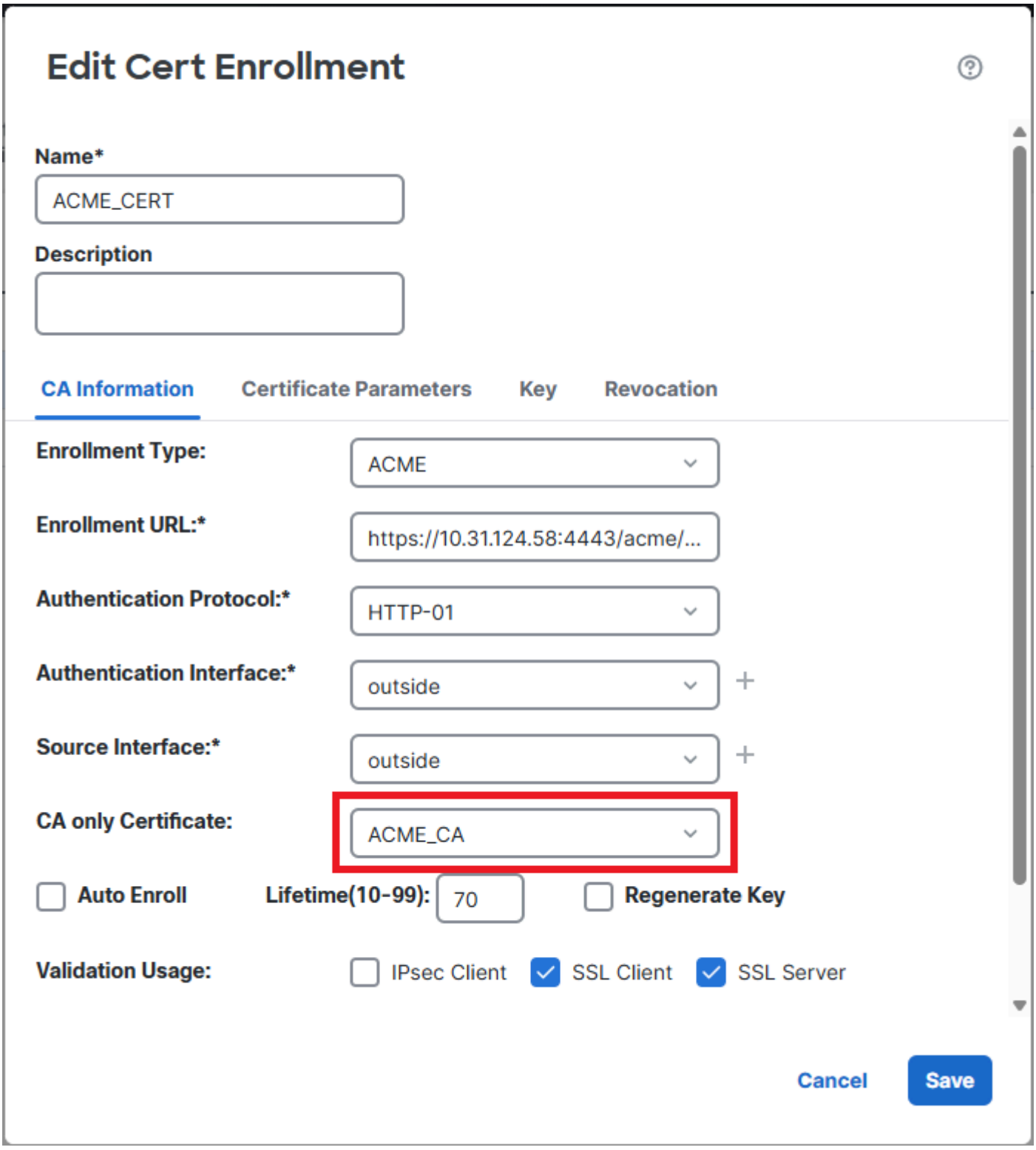
4. Se estiver usando um servidor ACME que não seja bem conhecido, você precisará adicionar o Certificado CA do servidor ACME. Navegue até Objects > Cert Enrollment e clique no botão Add Cert Enrollment.



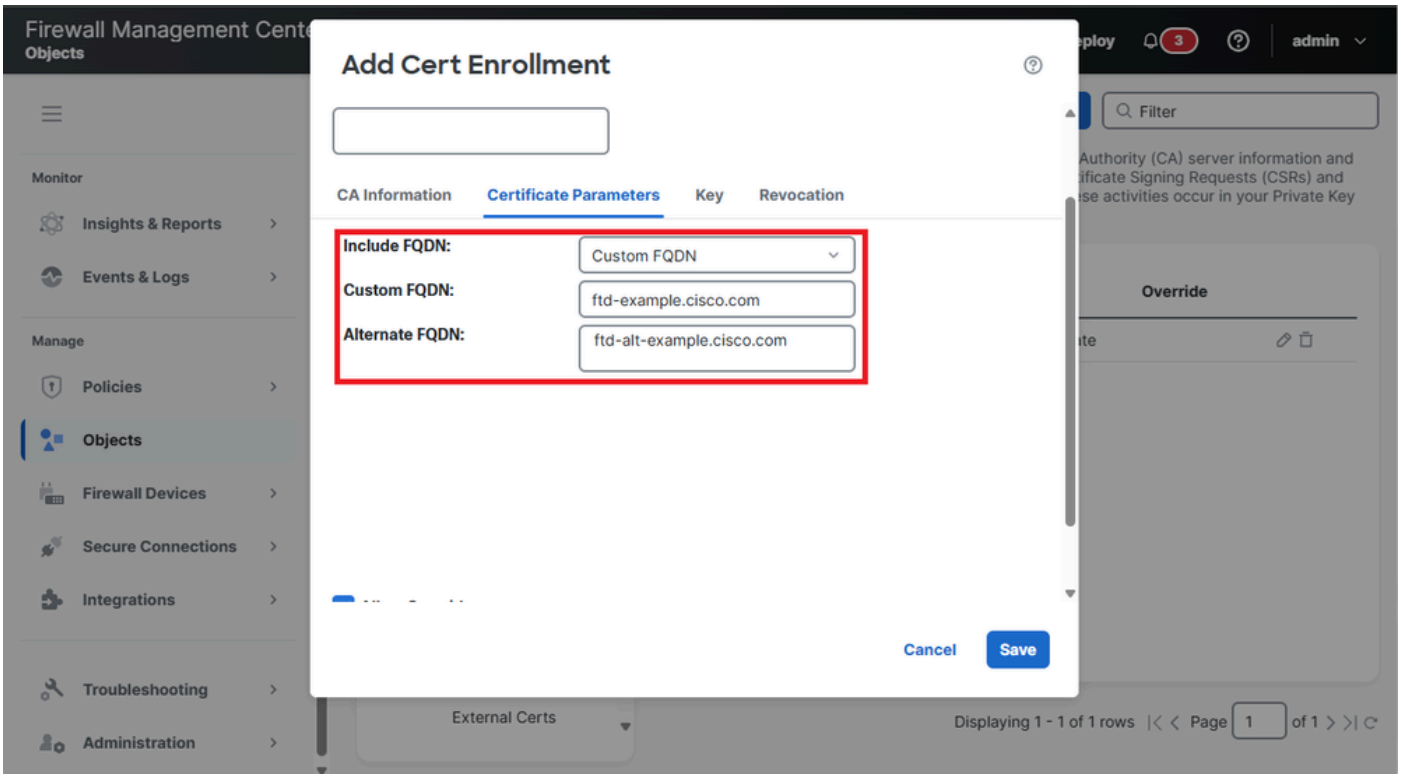
- Nomeie o ponto confiável e selecione o Tipo de inscrição como Manual. Em seguida, marque a opção CA Only. Finalmente, cole o certificado CA do servidor ACME e clique em Salvar.



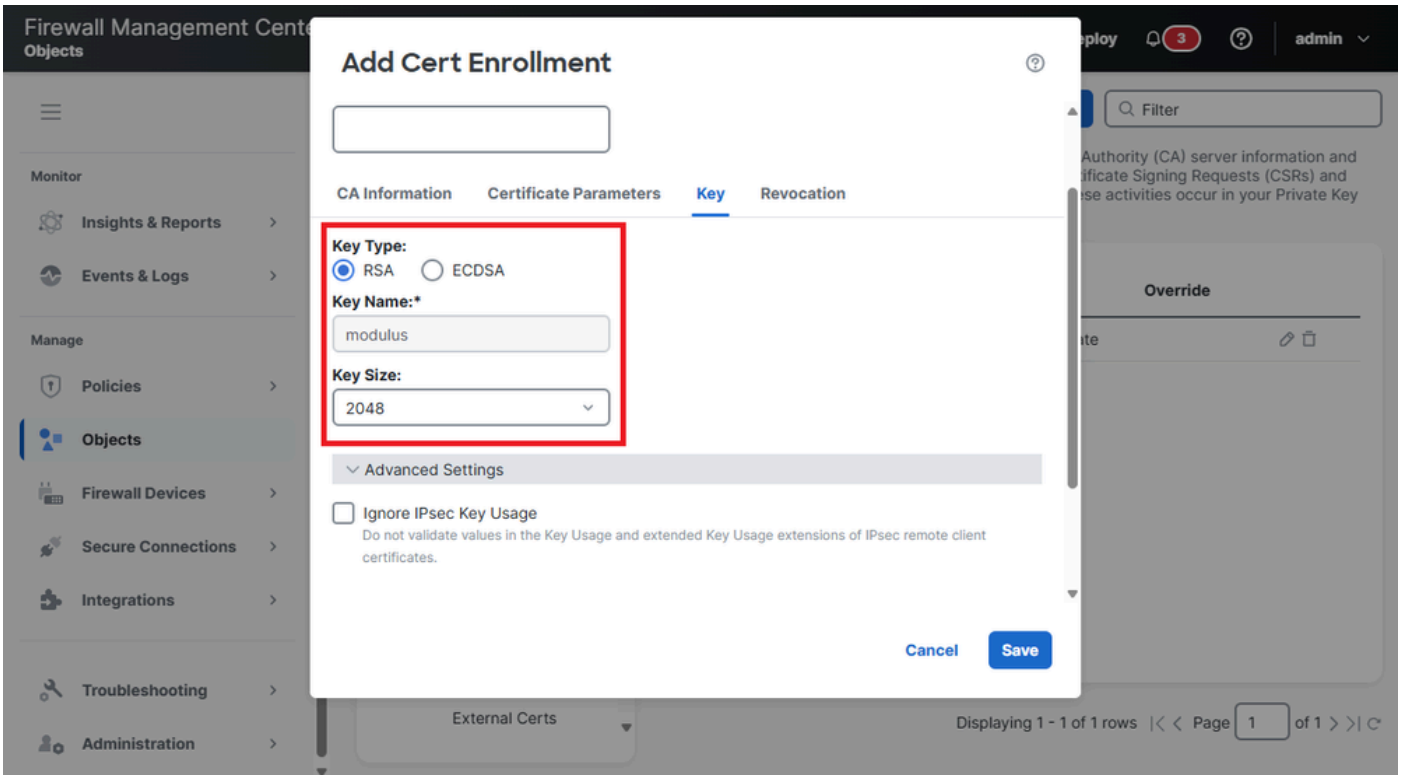
- Por fim, selecione o ponto de confiança do servidor de CA ACME na seção CA Only Certificate.



5. Navegue até Parâmetros do Certificado, selecione a opção FQDN Personalizado na caixa Incluir FQDN e preencha os campos FQDN Personalizado e FQDN Alternativo com o FQDN primário e quaisquer nomes de domínio alternativos a serem incluídos no certificado.



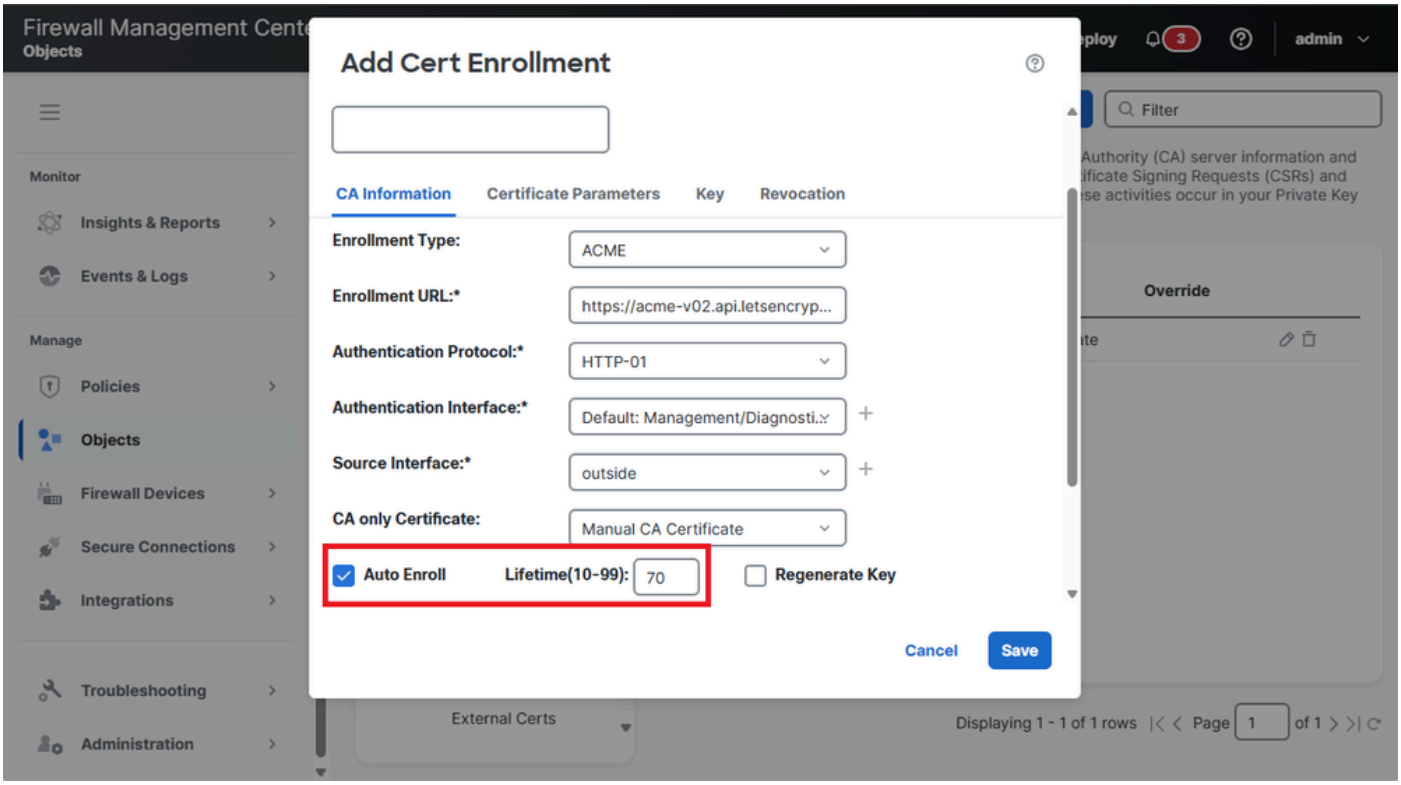
6. Navegue até Chave para modificar as configurações Tipo de Chave e Tamanho da Chave .



7. (Opcional) Ative a Inscrição Automática para o Certificado de Identidade.

Marque a caixa de seleçãoInscrição Automática e especifique o percentual para oTempo de Vida da Inscrição Automática.

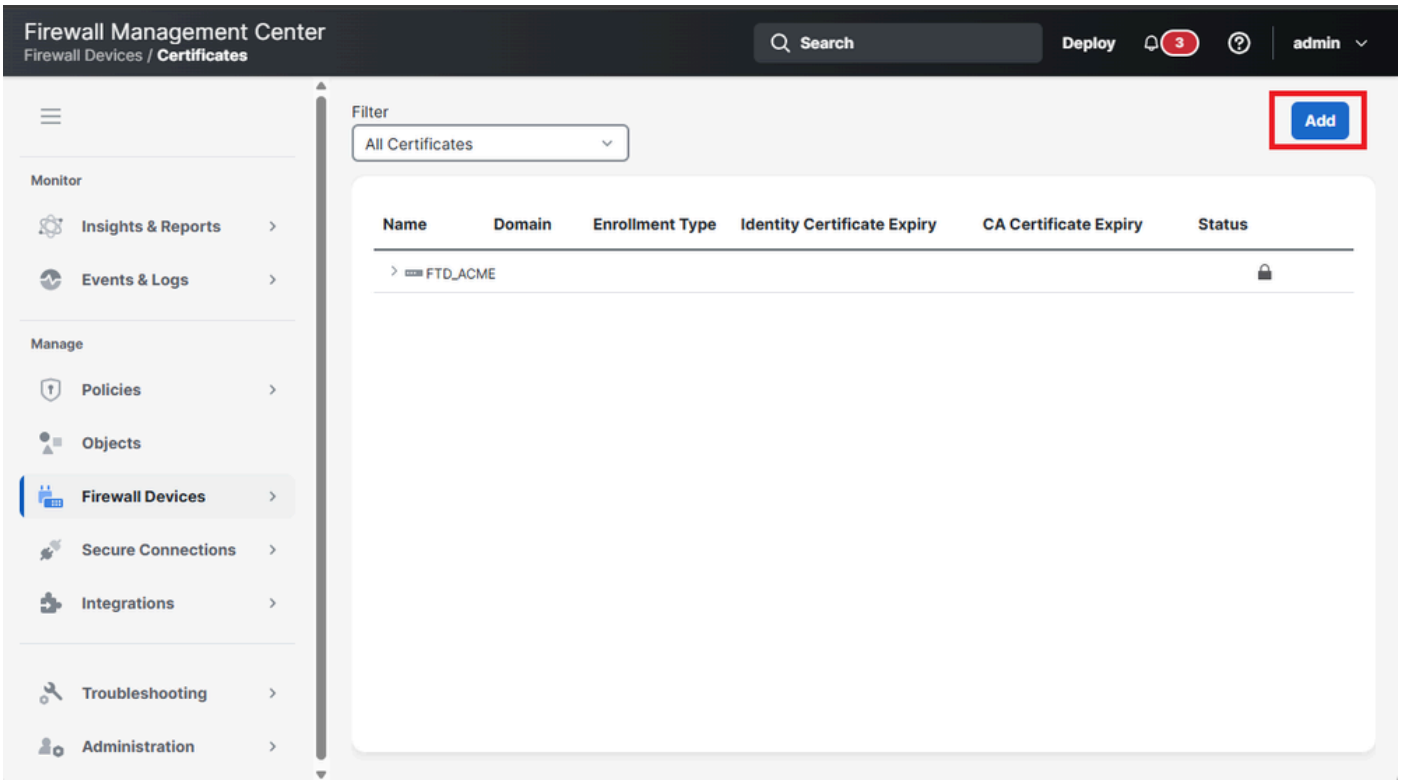
Este recurso garante que o certificado seja renovado automaticamente antes de expirar. A porcentagem determina com que antecedência da expiração do certificado o processo de renovação começa. Por exemplo, se definido como 80%, o processo de renovação começa quando o certificado atinge 80% de seu período de validade.



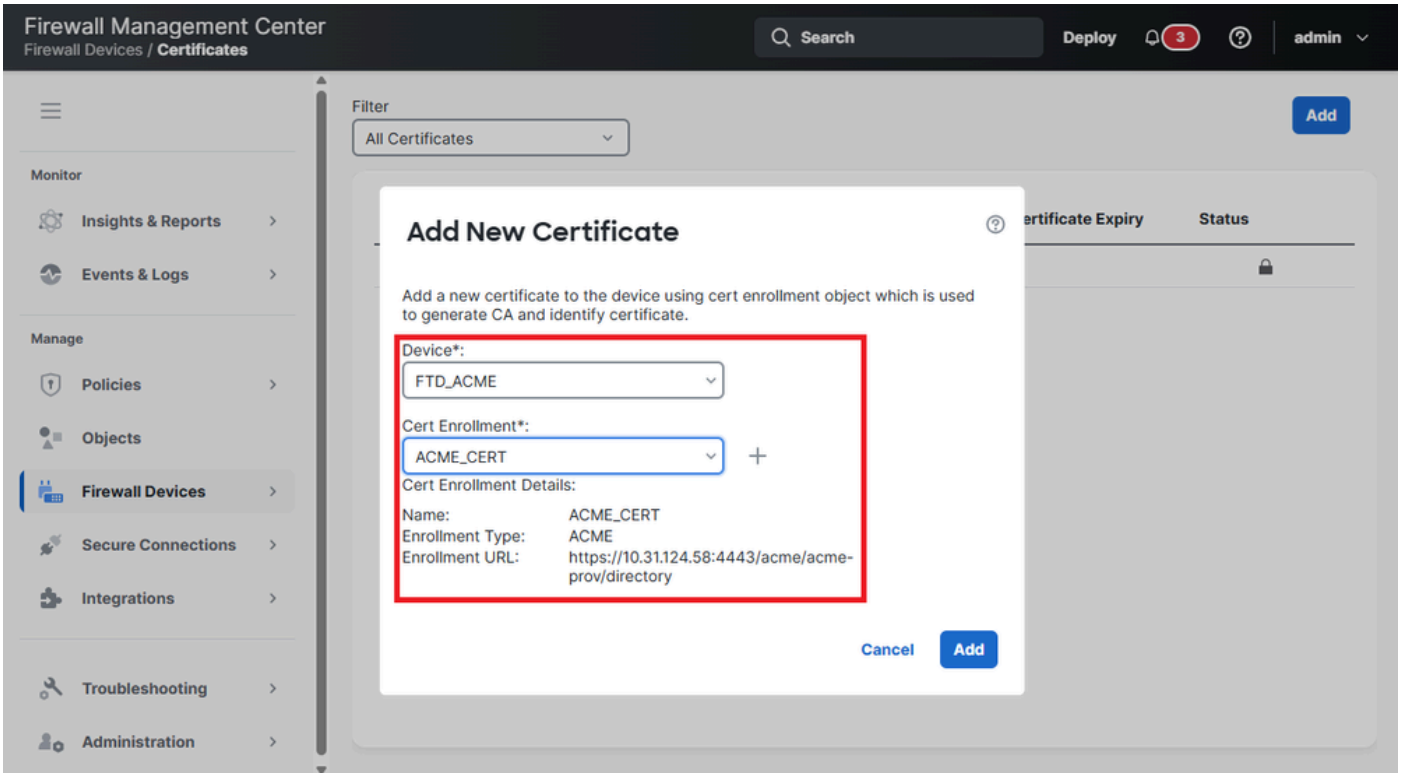
8. Clique em Salvar.

Registro de certificado ACME no dispositivo

1.Navegue até Dispositivos de firewall > Certificados e clique no botão Adicionar para registrar um novo certificado.



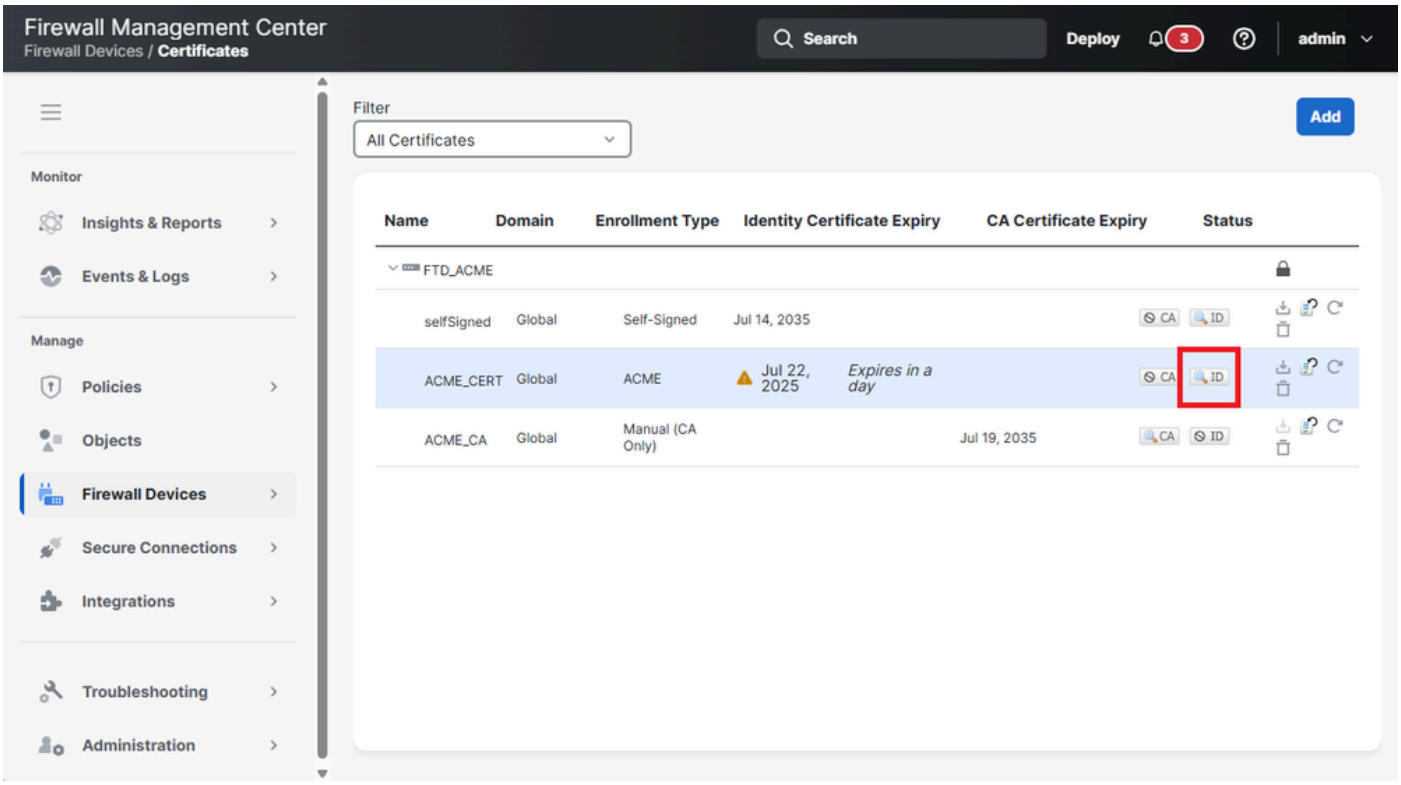
2. Selecione o dispositivo FTD na lista suspensa Dispositivo e o objeto de certificado criado anteriormente no Registro de Certificado.



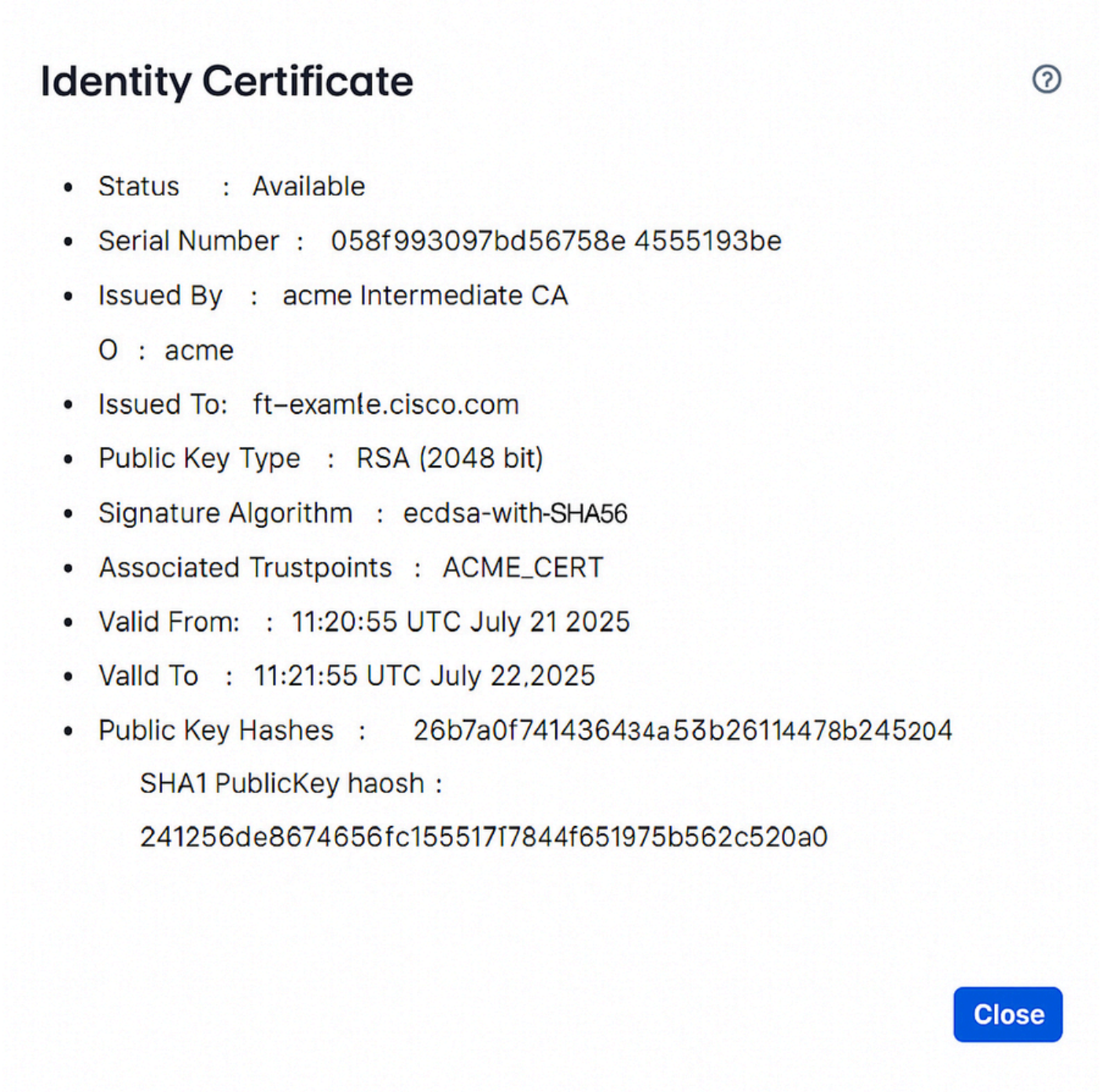
3. Clique em Adicionar.

4. Quando a implantação estiver concluída, a coluna de status exibirá o botão do certificado de

ID.



5. Valide as informações do certificado de ID clicando no botão ID.



Verificar

Exibir Certificado Instalado no FTD

Confirme se o certificado está registrado com o comando.show crypto ca certificates <Nome do ponto de confiança>.

<#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

Há novos syslogs no FTD do Secure Firewall para capturar eventos relacionados à inscrição de certificado usando o protocolo ACME:

- 717067 : Fornece informações sobre quando o registro do certificado ACME é iniciado.

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

- 717068 : Fornece informações sobre quando o registro do certificado ACME é bem-sucedido.

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

- 717069 : Fornece informações sobre quando a inscrição no ACME falha.

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

- 717070 : Fornece Informações relacionadas ao par de chaves para registro ou renovação de certificado.

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

Troubleshooting

Se uma inscrição de certificado ACME falhar, considere as próximas etapas para identificar e resolver o problema:

- Verifique a conectividade com o servidor:confirme se o Firewall Seguro tem conectividade de rede com o servidor ACME. Verifique se não há problemas de rede ou regras de firewall bloqueando a comunicação.
- Verifique se o Nome de domínio do firewall seguro pode ser resolvido:Verifique se o nome de domínio configurado no FTD do firewall seguro pode ser resolvido pelo servidor ACME. Essa verificação é crucial para que o servidor valide a solicitação.
- Confirmar propriedade de domínio:verifique se todos os nomes de domínio especificados no ponto de confiança pertencem ao FTD do Firewall seguro. Isso garante que o servidor ACME possa validar a propriedade do domínio.

Comandos de solução de problemas

Para obter informações adicionais, colete a saída dos próximos comandos de depuração:

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.