在FMC管理的安全防火墙威胁防御上使用ACME协议配置证书注册

简介

本文档介绍在安全防火墙Firepower威胁防御(FTD)平台上通过自动证书管理环境(ACME)协议注册传输层安全(TLS)证书的过程。

先决条件

要求

思科建议您了解以下主题：

- 手动证书注册流程和安全套接字层(SSL)基础知识。
- 远程访问VPN的基本身份验证概念。
- 具有证书颁发机构(CA)的经验。

使用的组件

- Cisco FTDv版本10.0.0-35。
- Cisco FMC版本10.0.0-35。
- 支持ACME协议的证书颁发机构(CA)服务器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

要求和限制

安全防火墙FTD上ACME注册的当前必备条件和限制包括：

- 受FTD和FMC版本10.0.0及更高版本支持。
- ACME不允许颁发通配符证书；每个证书请求必须指定一个精确的域名。

- 通过ACME注册的每个信任点都限制在单个接口上，因此通过ACME获取的证书不能跨多个接口共享。
- 密钥对会自动生成，并且对于通过ACME注册的每个证书都是唯一的，从而防止密钥重复使用，增强安全性。

降级注意事项

当降级到不支持ACME注册（版本7.7或更低版本）的安全防火墙FTD版本时：

- 版本10.0.0或更高版本中引入的所有与ACME相关的信任点配置都将丢失。
- 仍可访问通过ACME注册的证书；但是，在首次保存之后，它们的私钥将取消关联，并在降级之后重新启动。

如果需要降级，请使用建议的解决方法：

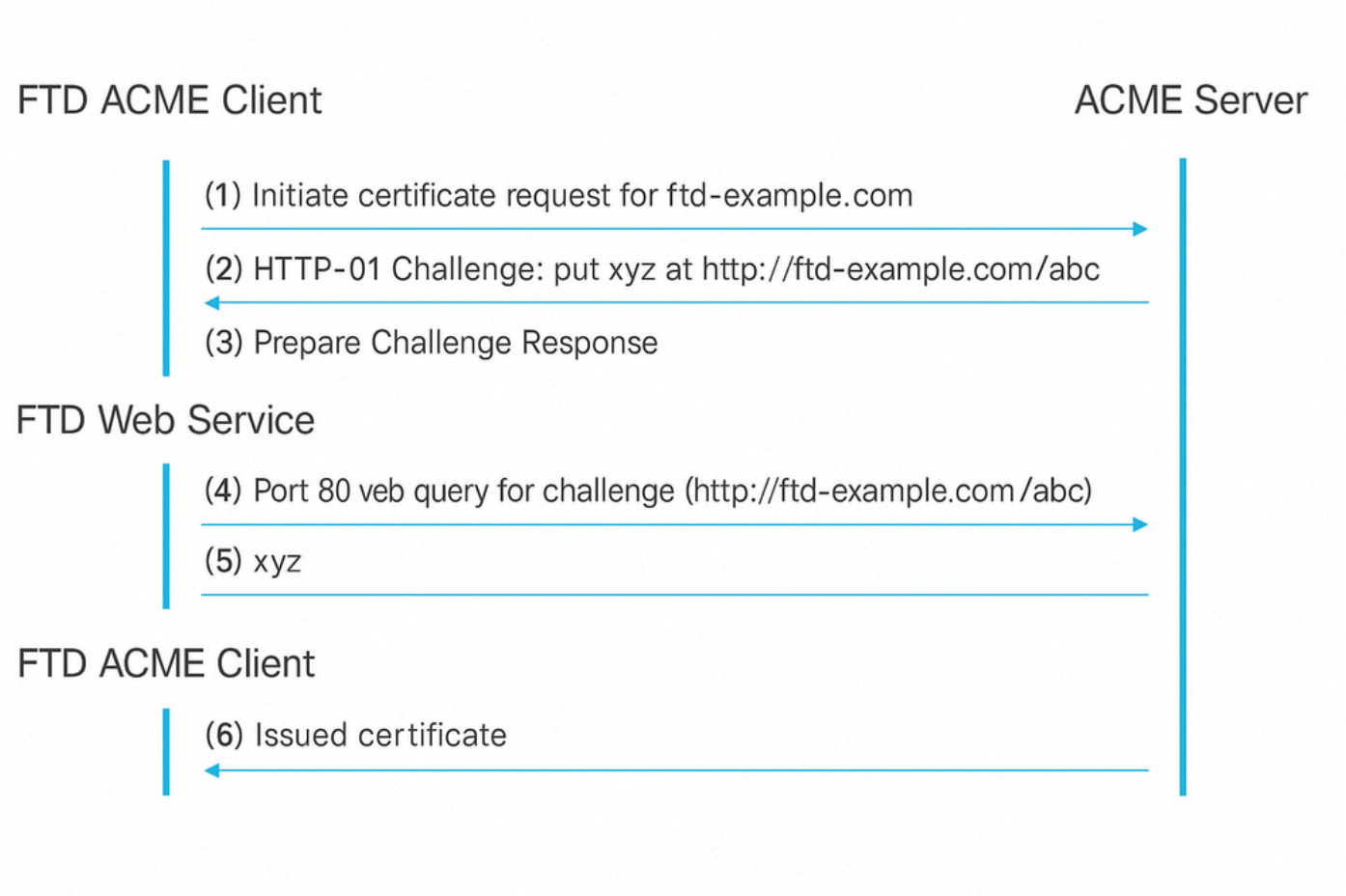
- 降级之前，以PKCS12格式导出ACME证书。
- 降级之前，请删除ACME信任点配置。
- 降级后，导入PKCS12证书。导入的信任点在ACME颁发的证书过期之前保持有效。

背景信息

ACME协议旨在简化网络管理员的TLS证书管理。通过ACME，管理员可以自动执行获取和更新TLS证书所涉及的任务。当使用证书颁发机构(CA)（如Let's Encrypt）时，这种自动化特别有用，该证书颁发机构通过ACME协议提供免费、自动且可供公众访问的证书。ACME有助于颁发域验证(DV)证书。这些证书验证证书请求者是否对指定域拥有控制权。验证通常通过基于HTTP的质询过程进行，申请人将指定文件放在其Web服务器上。然后，证书颁发机构(CA)通过域的HTTP服务器访问此文件，以确认域控制。成功传递此质询使CA能够颁发DV证书。

注册过程包括以下步骤：

1. 启动证书请求：客户端向ACME服务器提交证书请求，指定需要证书的域。
2. 接收HTTP-01质询：ACME服务器使用包含客户端必须用来证明域所有权的唯一令牌的HTTP-01质询进行响应。
3. 准备质询响应:
    1. 客户端通过将来自ACME服务器的令牌与其帐户密钥组合来生成密钥授权。
    2. 客户端将其Web服务器配置为在特定URL路径上提供此密钥授权。
4. ACME服务器检索质询：ACME服务器对提供的URL执行HTTP GET请求以获取密钥授权。
5. ACME服务器验证所有权：服务器将检索到的密钥授权与预期值进行比较，以验证客户端对域的控制。
6. 颁发证书：成功验证后，ACME服务器会向客户端颁发SSL/TLS证书。



ACME注册HTTP-01身份验证流程。

使用ACME协议在安全防火墙FTD上注册TLS证书的主要优势包括：

- 证书管理自动化:ACME简化了获取和维护安全防火墙FTD TLS接口的TLS域证书的过程，从而显着减少了手动管理任务。
- 自动证书续订:通过启用ACME的信任点，证书在即将到期时自动更新，从而最大程度地减少持续管理干预的需要。
- 持续安全保证:此自动化可确保证书保持有效而不中断，从而防止意外证书过期并保持安全通信。

这些优势共同提高了安全防火墙FTD部署的运营效率和安全性。

配置

必备项配置

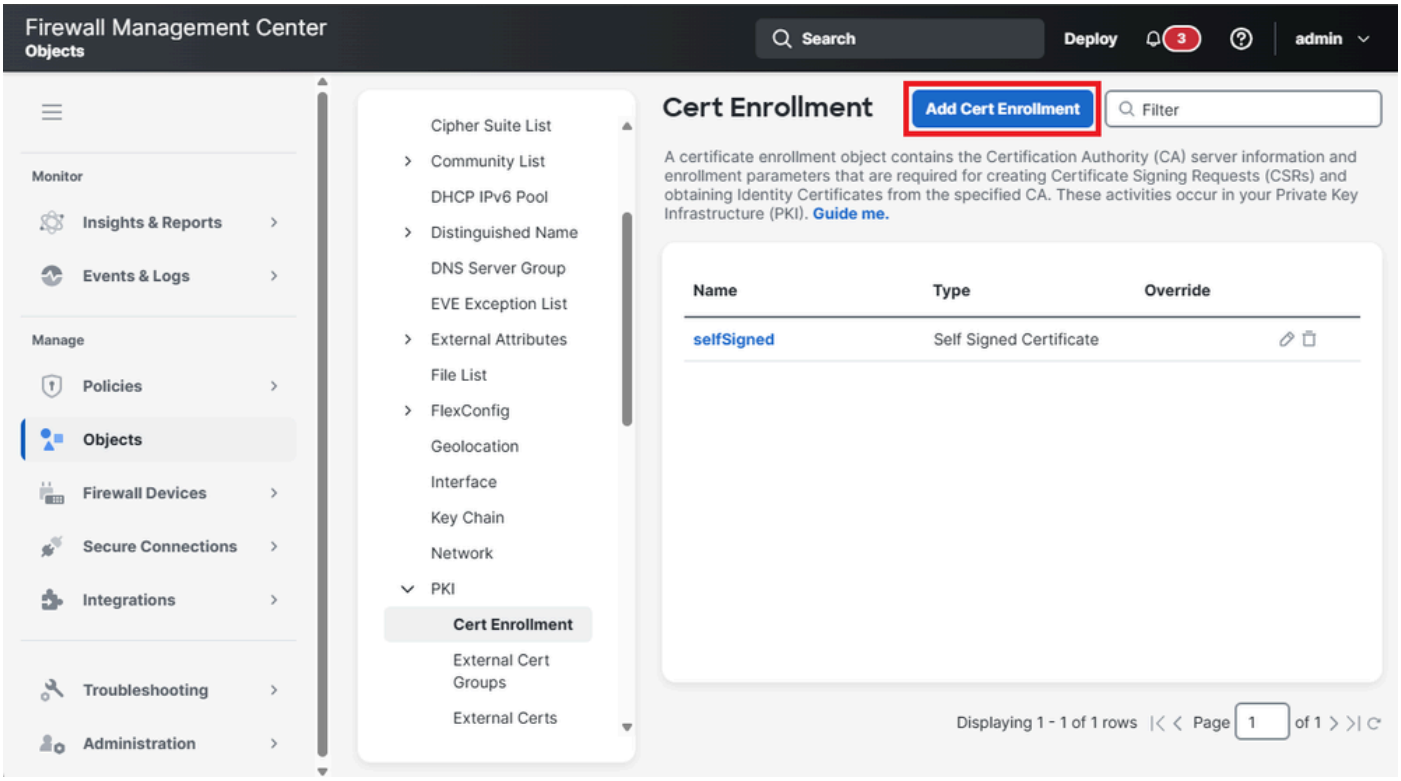
在启动ACME注册流程之前，请确保满足以下条件：

1. 可解析域名:请求证书的域名必须由ACME服务器进行解析。这可确保服务器可以验证域所有权。
2. 对ACME服务器的安全防火墙访问：安全防火墙必须能够通过其接口之一访问ACME服务器。此访问不需要通过请求证书的接口。
3. TCP端口80可用性：允许从ACME CA服务器到与域名对应的接口的TCP端口80。在ACME交换过程中，完成HTTP-01质询时需要此步骤。

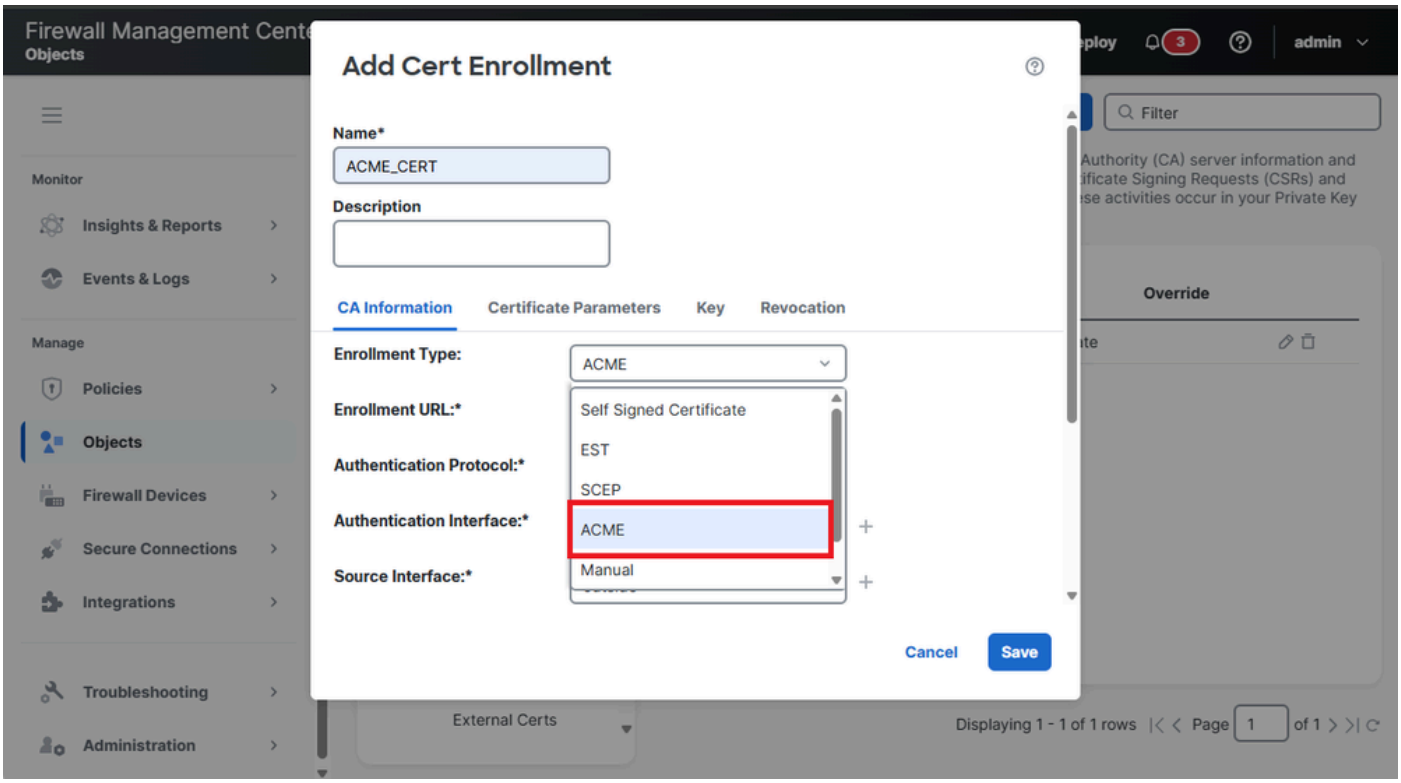
注意：在端口80打开期间，只有ACME质询数据可访问。

ACME证书注册对象创建

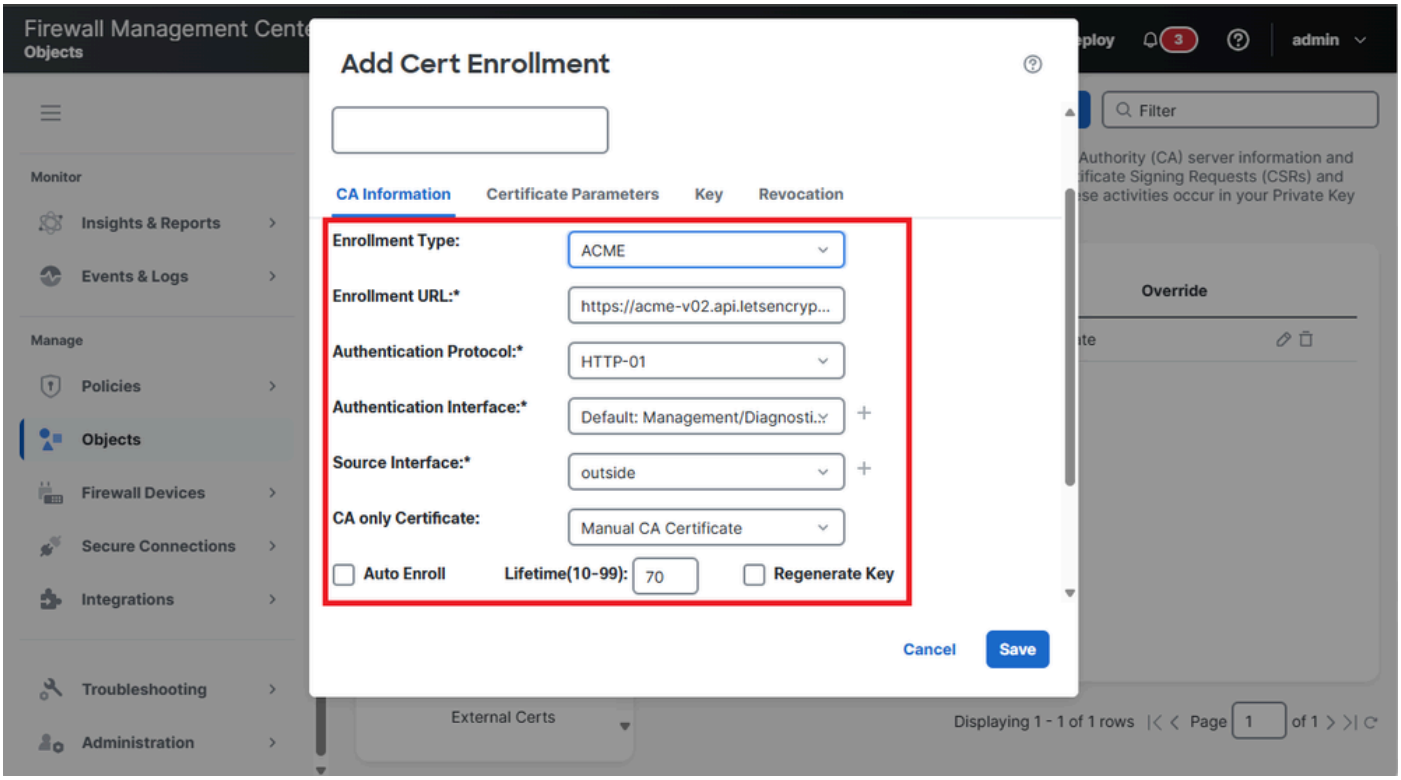
1.导航到对象> PKI >证书注册，然后单击添加证书注册开始配置过程。



2.下拉菜单中列出了ACME enrollment选项以及其他注册方法。从Enrollment Type下拉列表中选择ACME以继续。



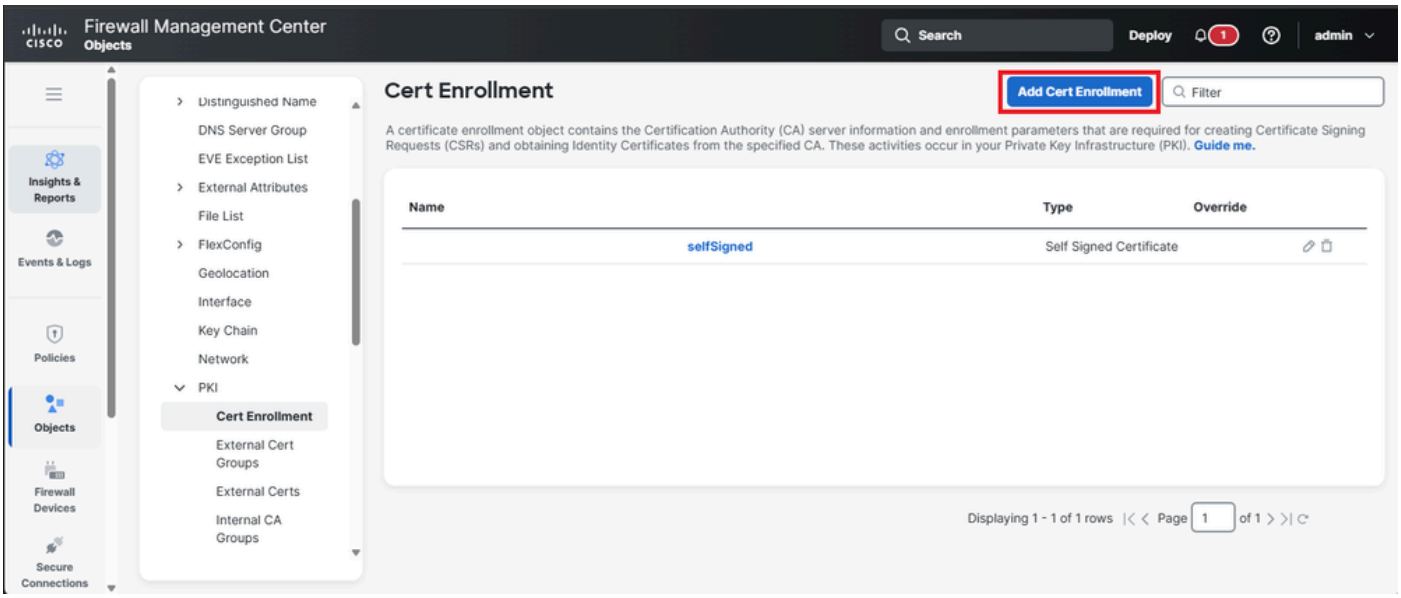
3.显示配置证书参数的选项，使用适当信息填写字段。



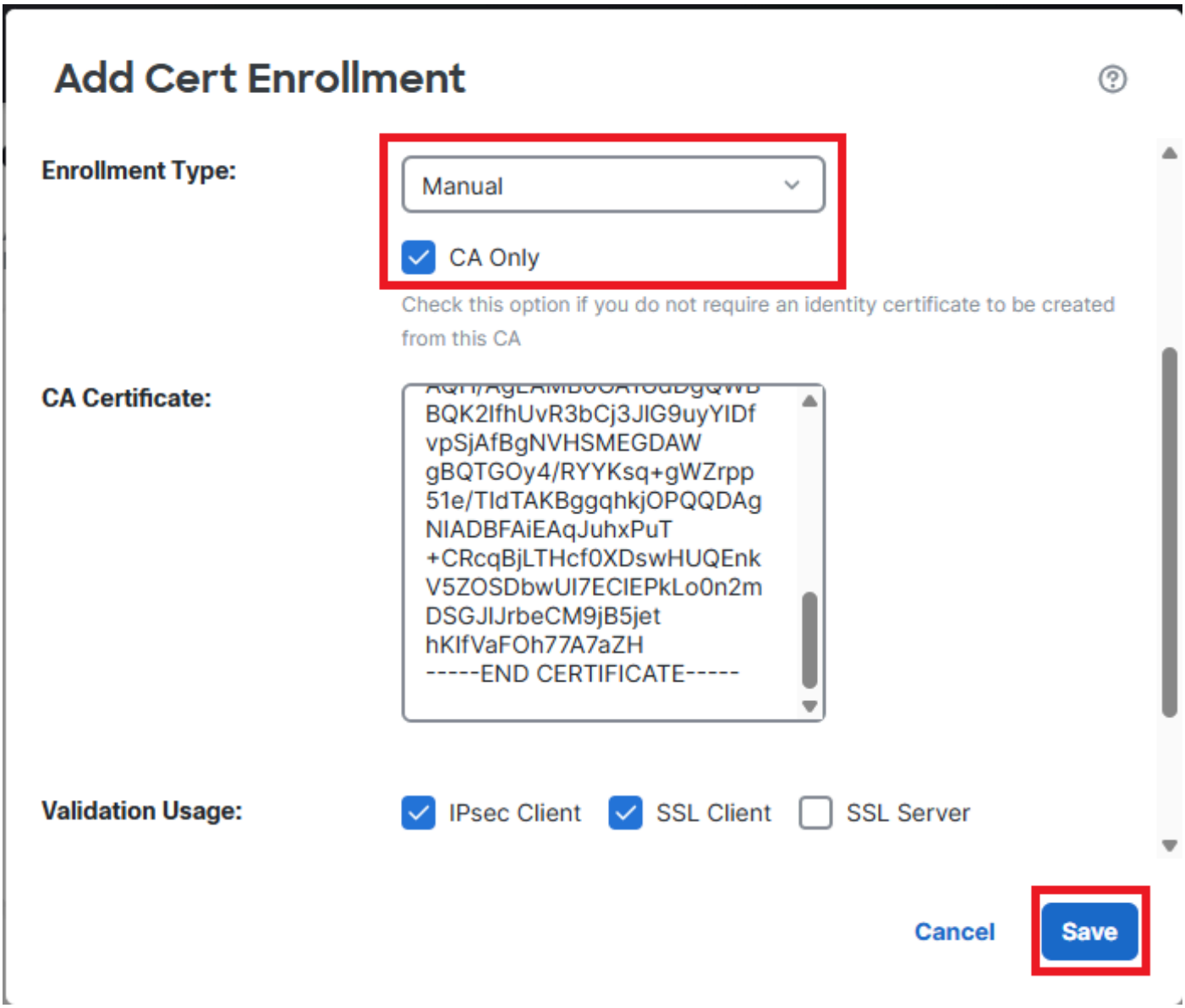
- 注册 URL:这是用于请求和检索证书的ACME服务器(如Let's Encrypt)的地址。
- 验证协议：这指定用于验证域所有权的方法。ACME质询支持的协议是HTTP-01。
- 身份验证接口：FTD设备上接收来自ACME服务器的HTTP-01质询的网络接口。
- 仅CA证书:必须选择来自证书颁发机构(CA)的证书以信任ACME服务器。

注意：默认情况下，它指向公共Let's Encrypt服务URL:https://acme-v02.api.letsencrypt.org/directory。

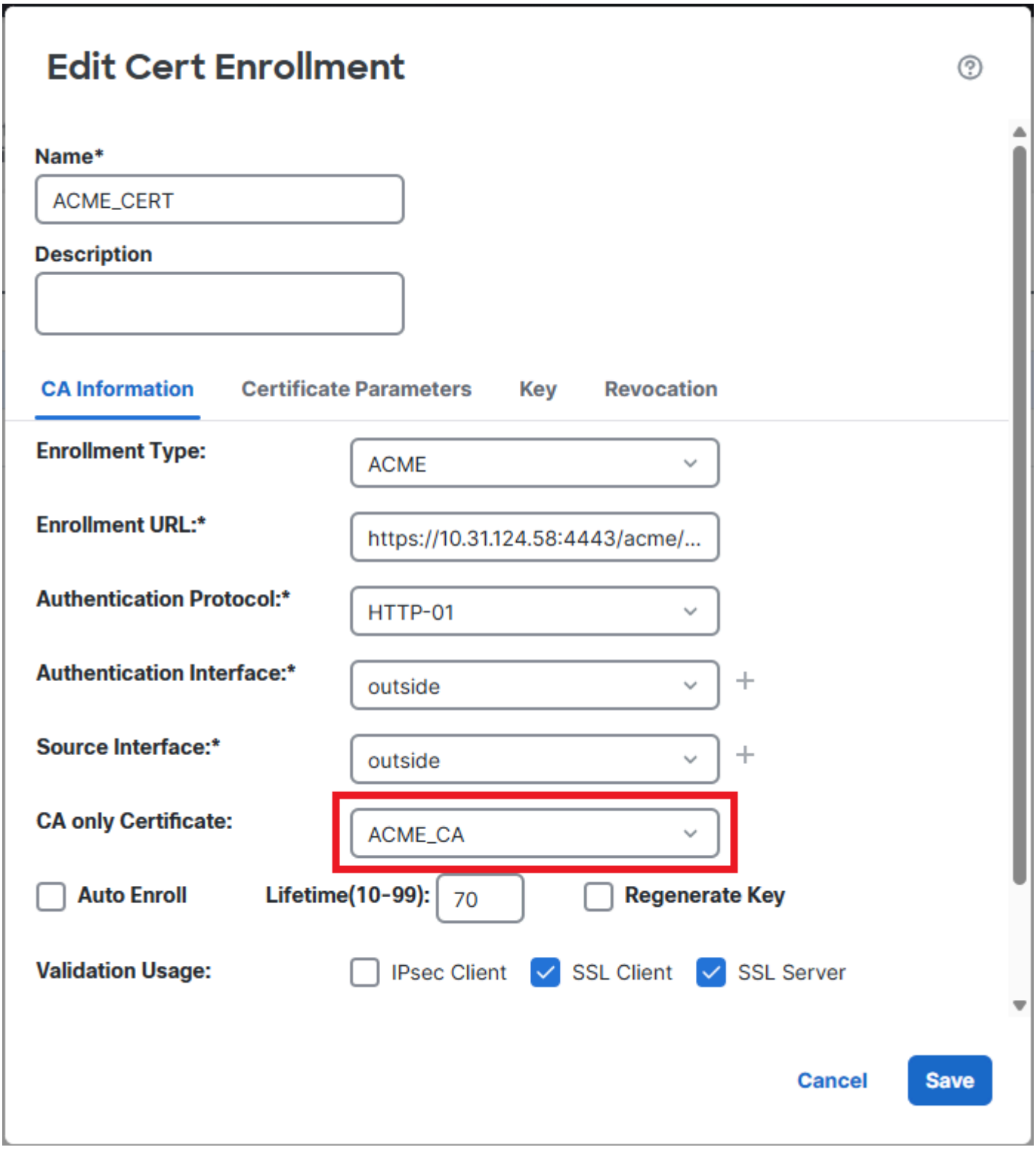
4.如果您使用的是未知的ACME服务器，则需要添加ACME服务器的CA证书。导航到对象>证书注册，然后单击添加证书注册按钮。



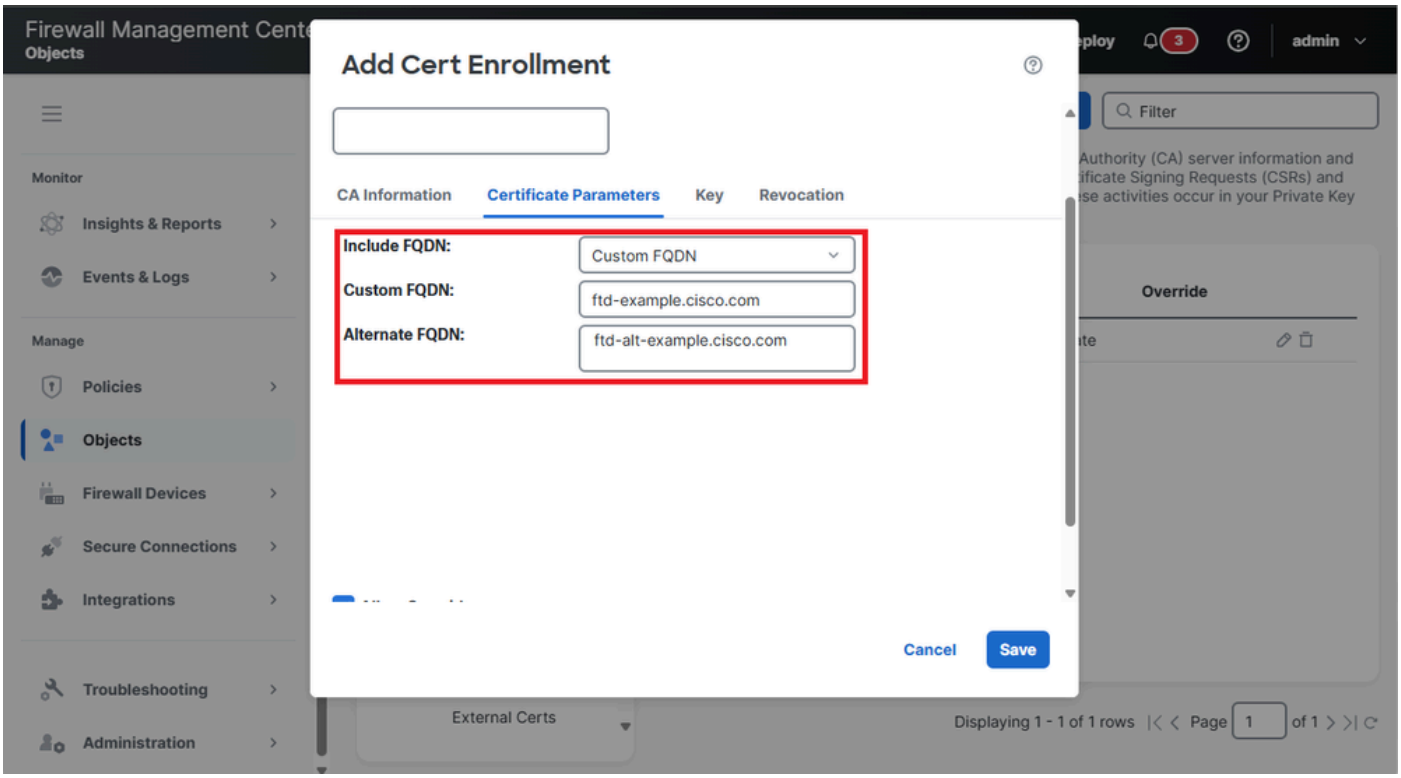
- 将信任点命名为，然后选择Enrollment Type作为Manual。然后，选中选项CA Only。最后，粘贴ACME服务器的CA证书，然后单击Save。



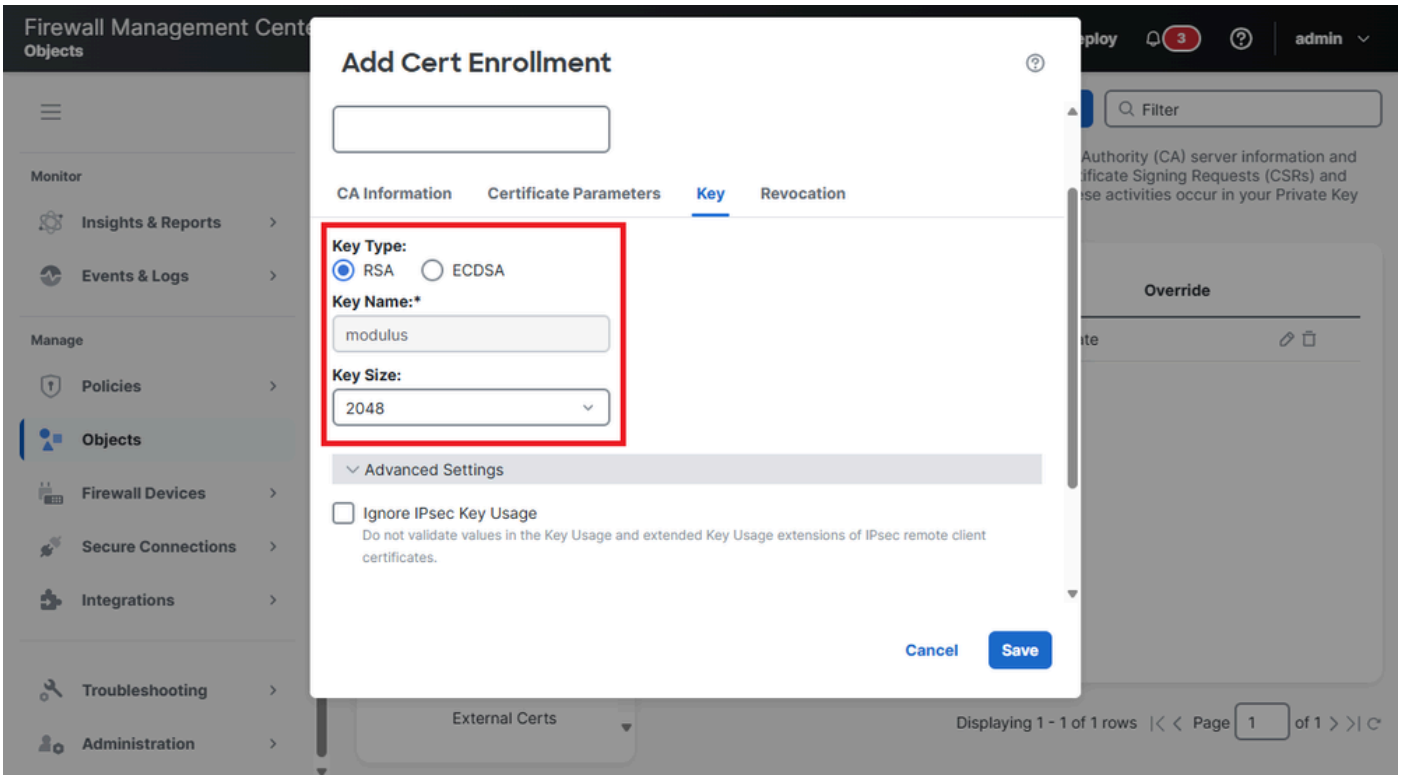
- 最后，在CA Only Certificate部分中选择ACME CA服务器的信任点。



5.导航至“证书参数”(Certificate Parameters)，在包括FQDN(Include FQDN)框中选择自定义FQDN(Custom FQDN)选项，并填写自定义FQDN和备用FQDN字段，其中包含主要FQDN和要包含在证书中的任何备用域名。



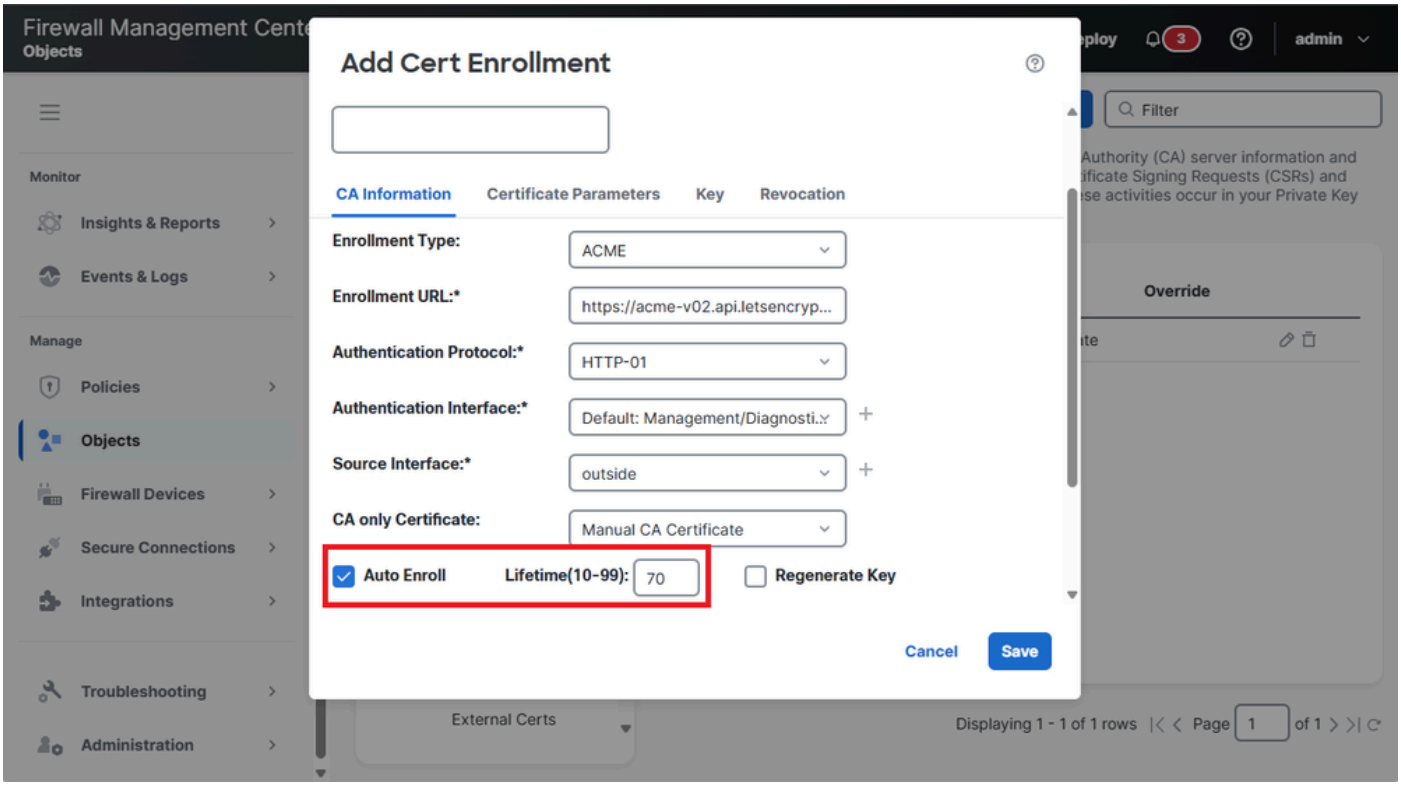
6.定位至密钥，以修改密钥类型和密钥大小设置。



7.（可选）为身份证书启用Auto Enroll。

选中Auto Enrollment复选框并指定Auto Enroll Lifetime的百分比。

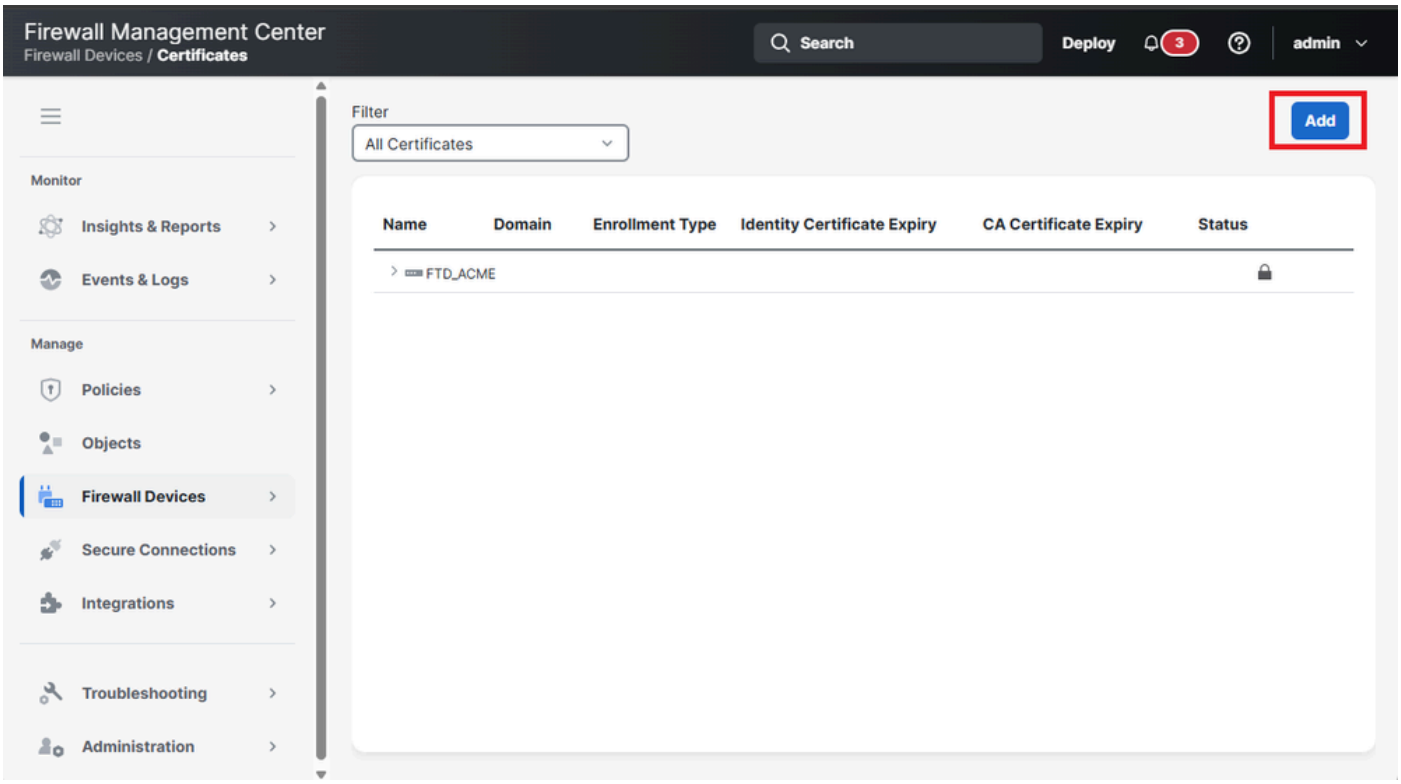
此功能可确保证书在到期之前自动续订。该百分比确定证书到期前续订流程开始的时间。例如，如果设置为80%，则当证书达到其有效期的80%时，续订过程开始。



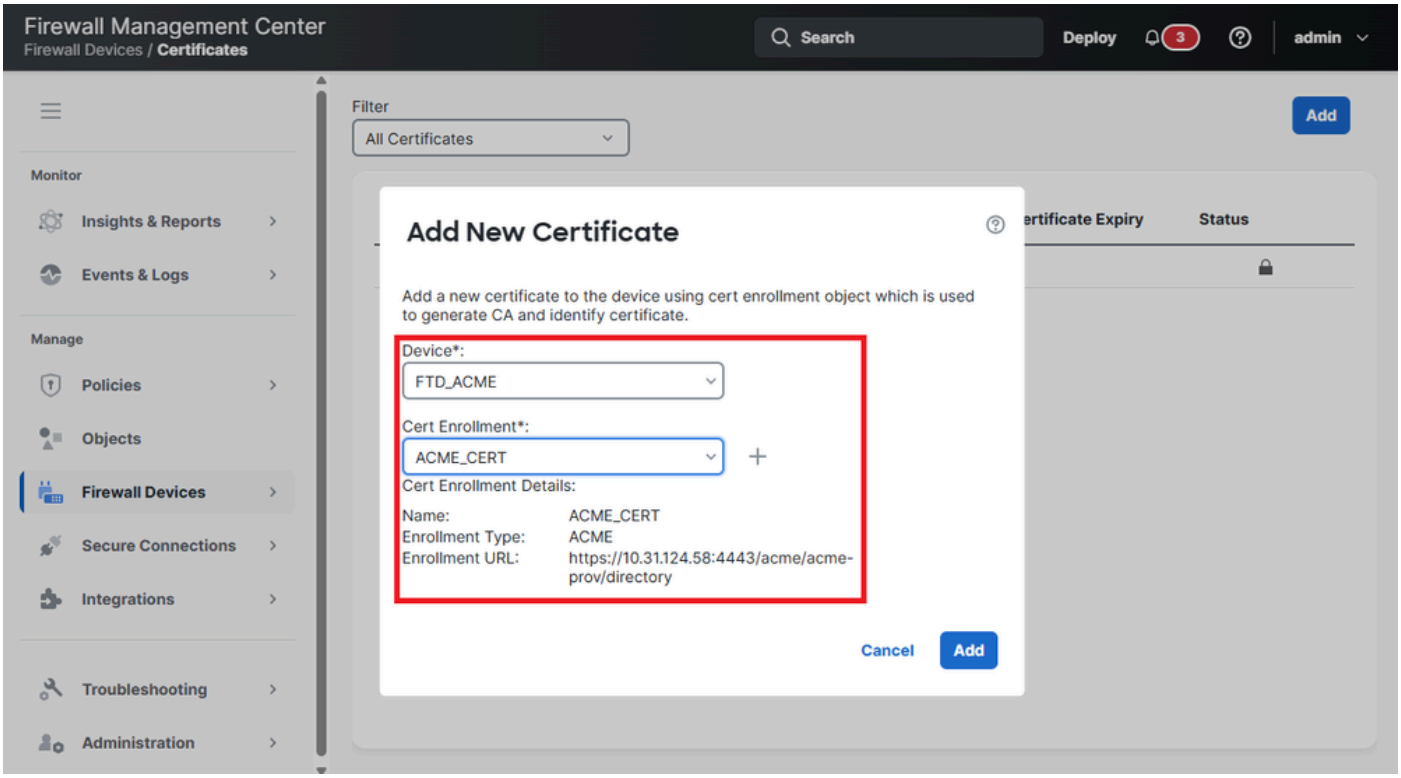
8.单击保存。

设备上的ACME证书注册

1.导航到Firewall Devices > Certificates，然后单击Add按钮注册新证书。

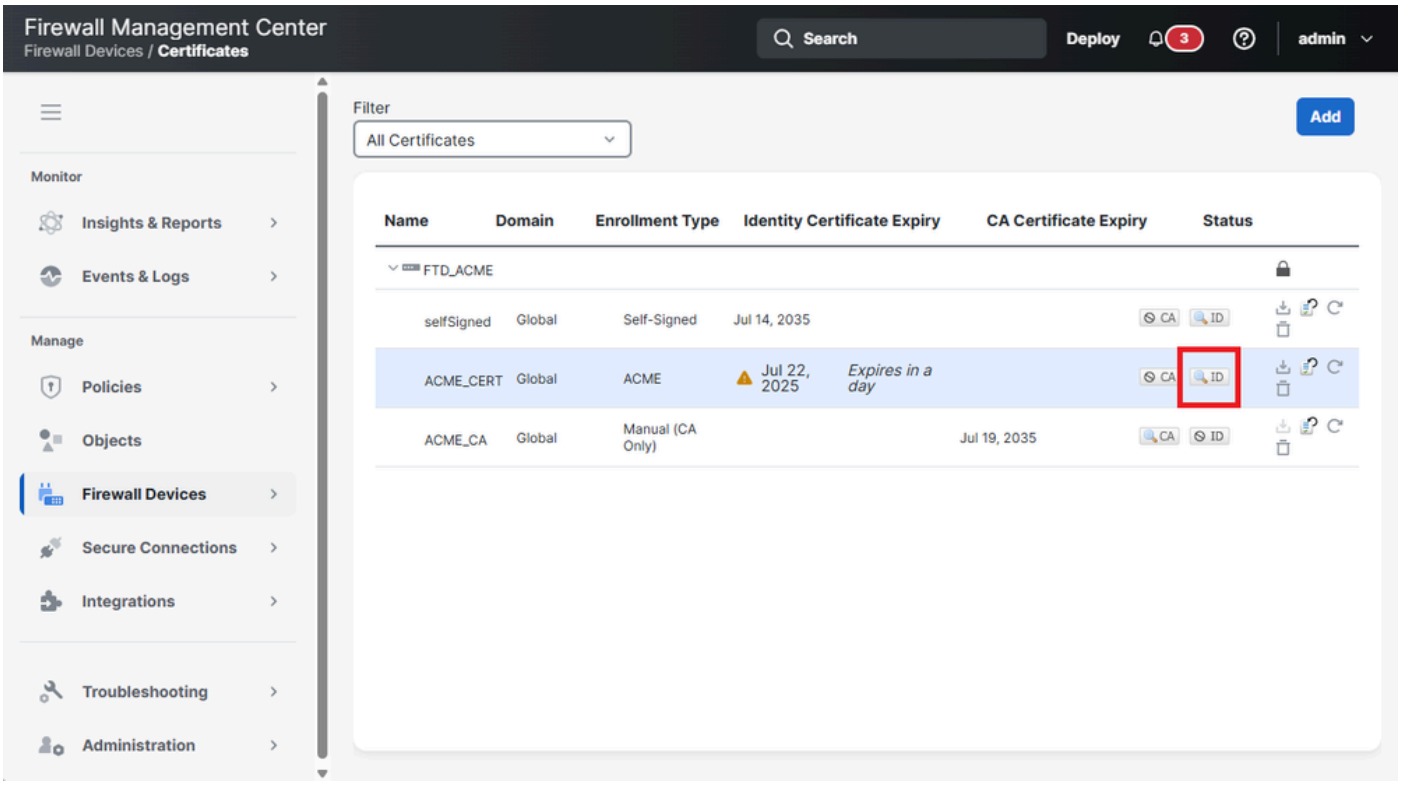


2.从Device下拉列表中选择FTD设备，以及以前在Cert Enrollment中创建的证书对象。

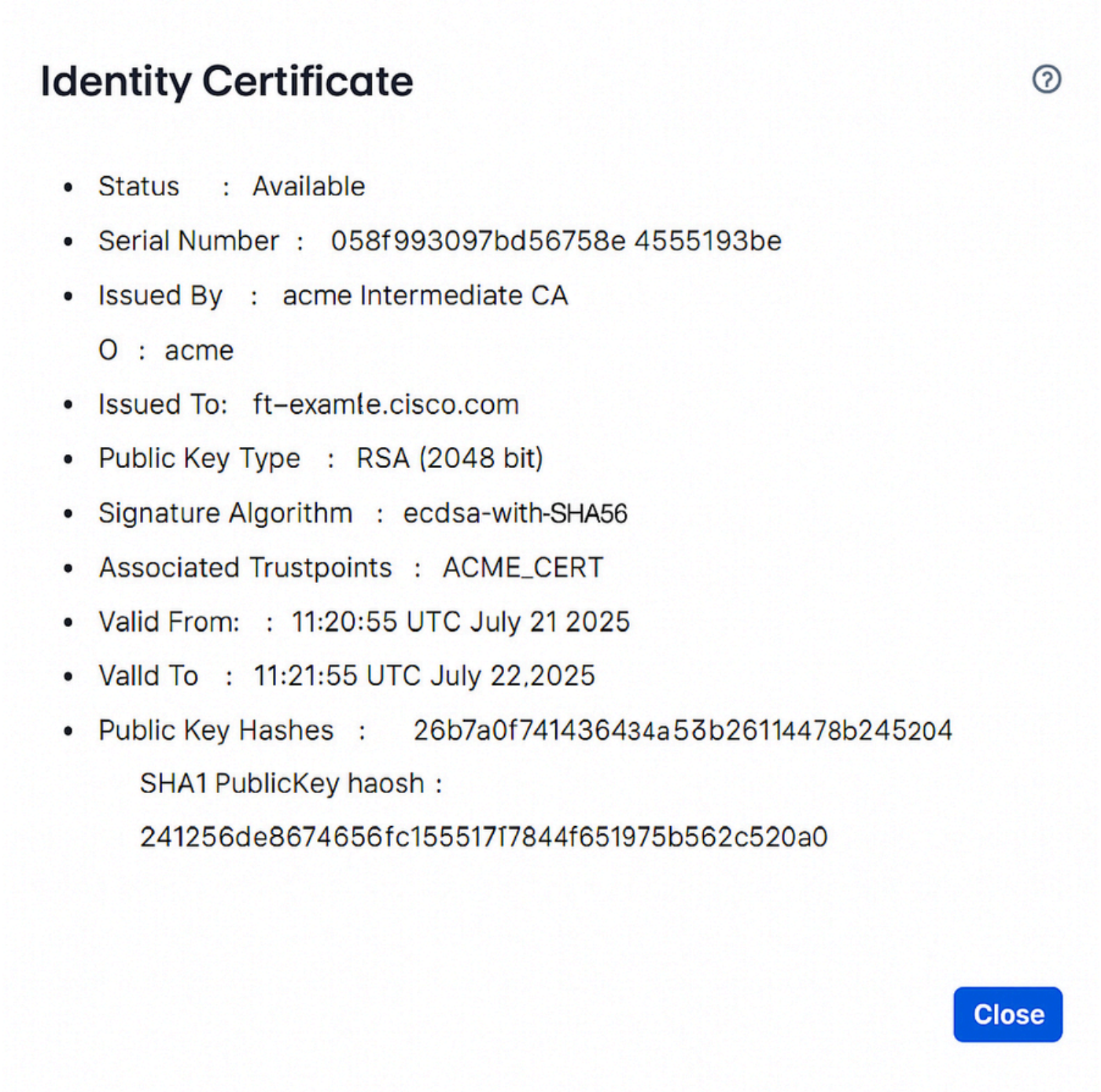


3.单击Add。

4.部署完成后，状态列将显示ID证书按钮。



5.单击ID按钮验证ID证书信息。



验证

查看FTD中安装的证书

使用命令确认已注册证书。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
```

系统日志事件

安全防火墙FTD中有新的系统日志，用于捕获使用ACME协议的证书注册相关事件：

- 717067：提供ACME证书注册何时启动的信息。

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

- 717068：提供ACME证书注册何时成功的信息。

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

- 717069：提供ACME注册失败时的相关信息。

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

- 717070：提供与证书注册或证书续订的密钥对相关的信息。

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

故障排除

如果ACME证书注册失败，请考虑以下步骤来识别和解决问题：

- 检查与服务器的连接：确认安全防火墙与ACME服务器具有网络连接。确认没有网络问题或防火墙规则阻止通信。
- 确保安全防火墙域名可解析：确保安全防火墙FTD上配置的域名可由ACME服务器解析。此验证对于服务器验证请求至关重要。
- 确认域所有权：验证信任点中指定的所有域名是否归安全防火墙FTD所有。这可确保ACME服务器可以验证域所有权。

故障排除命令

有关其他信息，请收集下一个debug命令的输出：

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。