在安全防火墙上使用ACME协议配置证书注册

目录

简介

本文档介绍在安全防火墙ASA上使用自动证书管理环境(ACME)协议注册传输层安全(TLS)证书的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙自适应安全设备(ASA)
- 公用密钥基础结构 (PKI)

使用的组件

- Cisco ASAv 9.23.1版。
- Cisco ASDM 7.23(1) 版.

- 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ASA上ACME注册的当前要求和限制如下：

- 在ASA版本9.23.1和ASDM 7.23.1及以上版本上受支持
- 不支持多情景
- ACME不支持通配符证书的创建。每个证书请求必须指定一个确切的域名。
- 通过ACME注册的每个信任点都限于单个接口，这意味着通过ACME注册的证书不能跨多个接口共享。
- 密钥对是自动生成的，不能为通过ACME注册的证书共享。每个证书都使用唯一的密钥对，从而增强了安全性，但限制了密钥的重复使用。

降级注意事项

当降级到不支持安全防火墙ASA（9.22及更早版本）上的ACME注册的版本时：

- 9.23.x或更高版本的所有与ACME相关的信任点配置都将丢失
- 通过ACME注册的所有证书仍然可访问，但在首次降级后保存并重新启动后，私钥将取消关联

如果需要降级，请执行以下建议的解决步骤：

1. 在降级之前，请确保以PKCS12格式导出ACME证书。
2. 在降级之前，请确保删除ACME信任点配置。
3. 降级后，导入PKCS12证书。生成的信任点在通过ACME颁发的证书到期之前仍然有效。

背景信息

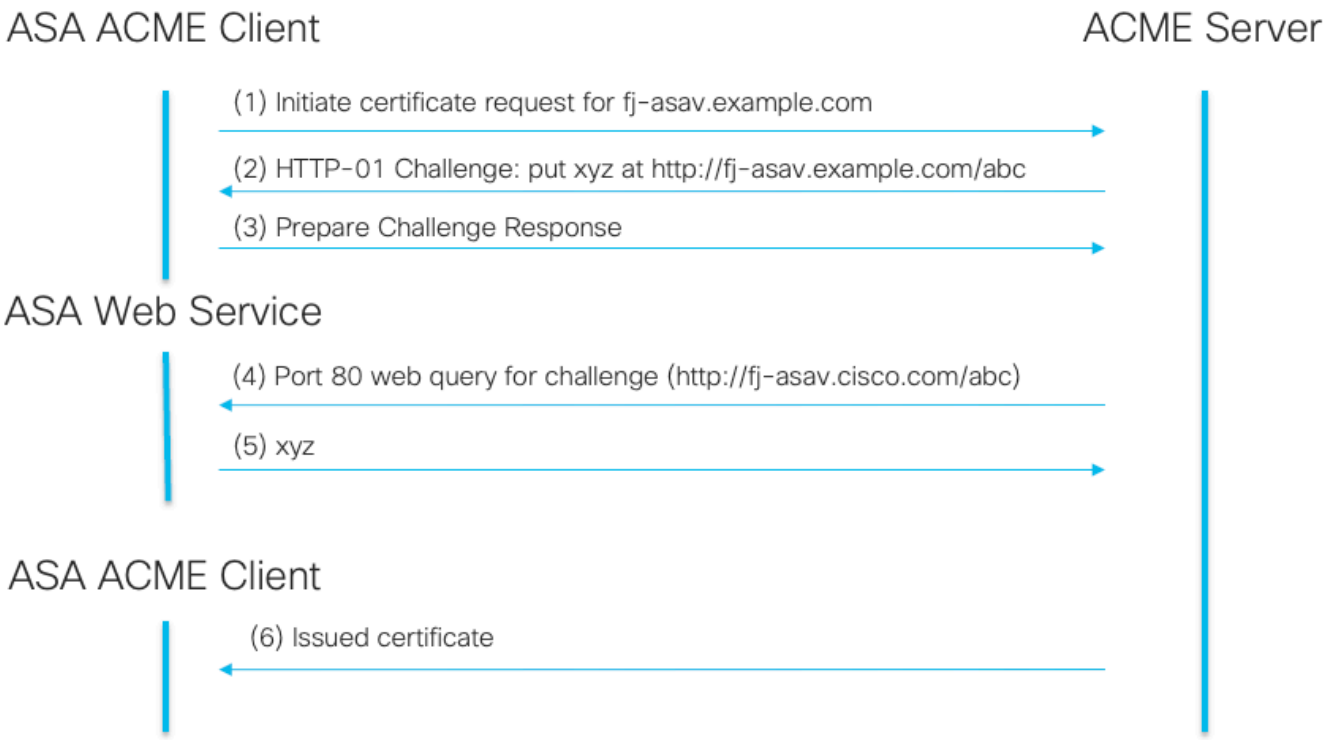
ACME协议旨在简化网络管理员的TLS证书管理。通过使用ACME，管理员可以自动执行获取和更新TLS证书所涉及的进程。当使用证书颁发机构(CA)（如Let's Encrypt）时，这种自动化尤其有益，该证书颁发机构使用ACME协议提供免费的、自动化的开放式证书。

ACME支持颁发域验证(DV)证书。这些证书是一种数字证书，用于确认证书持有者对指定域的控制。DV证书的验证过程通常通过基于HTTP的质询机制进行。在此机制中，申请人将特定文件放在其Web服务器上，由证书颁发机构(CA)通过域的HTTP服务器访问该文件进行验证。成功完成此练习可向CA证明申请人对域拥有控制权，从而允许颁发DV证书。

完成注册的过程如下：

1. 启动证书请求：客户端向ACME服务器请求证书，并指定需要证书的域。
2. 接收HTTP-01质询：ACME服务器提供带有唯一令牌的HTTP-01质询，供客户端用于证明域控

制。
3. 准备质询响应：
    - 客户端通过将ACME服务器的令牌与其帐户密钥组合来创建密钥授权。
    - 客户端设置其Web服务器，以在特定URL路径上提供此密钥授权。
4. ACME服务器检索质询：ACME服务器向指定的URL发出HTTP GET请求以检索密钥授权。
5. ACME服务器验证所有权：服务器检查检索到的密钥授权是否与预期值匹配，以确认客户端对域的控制。
6. 颁发证书：验证成功后，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协议注册TLS证书的最相关优势包括：

- ACME有助于获取和维护安全防火墙ASA TLS接口的TLS域证书。这种自动化可显着减少手动任务，并有助于保持证书最新，而不会受到持续监督。
- 使用启用ACME的信任点，证书在接近到期时自动更新。此功能可降低管理参与需求，确保不间断安全并防止意外证书过期。

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. 可解析的域名：请求证书的域名必须由ACME服务器解析。这可确保服务器可以验证域所有权。

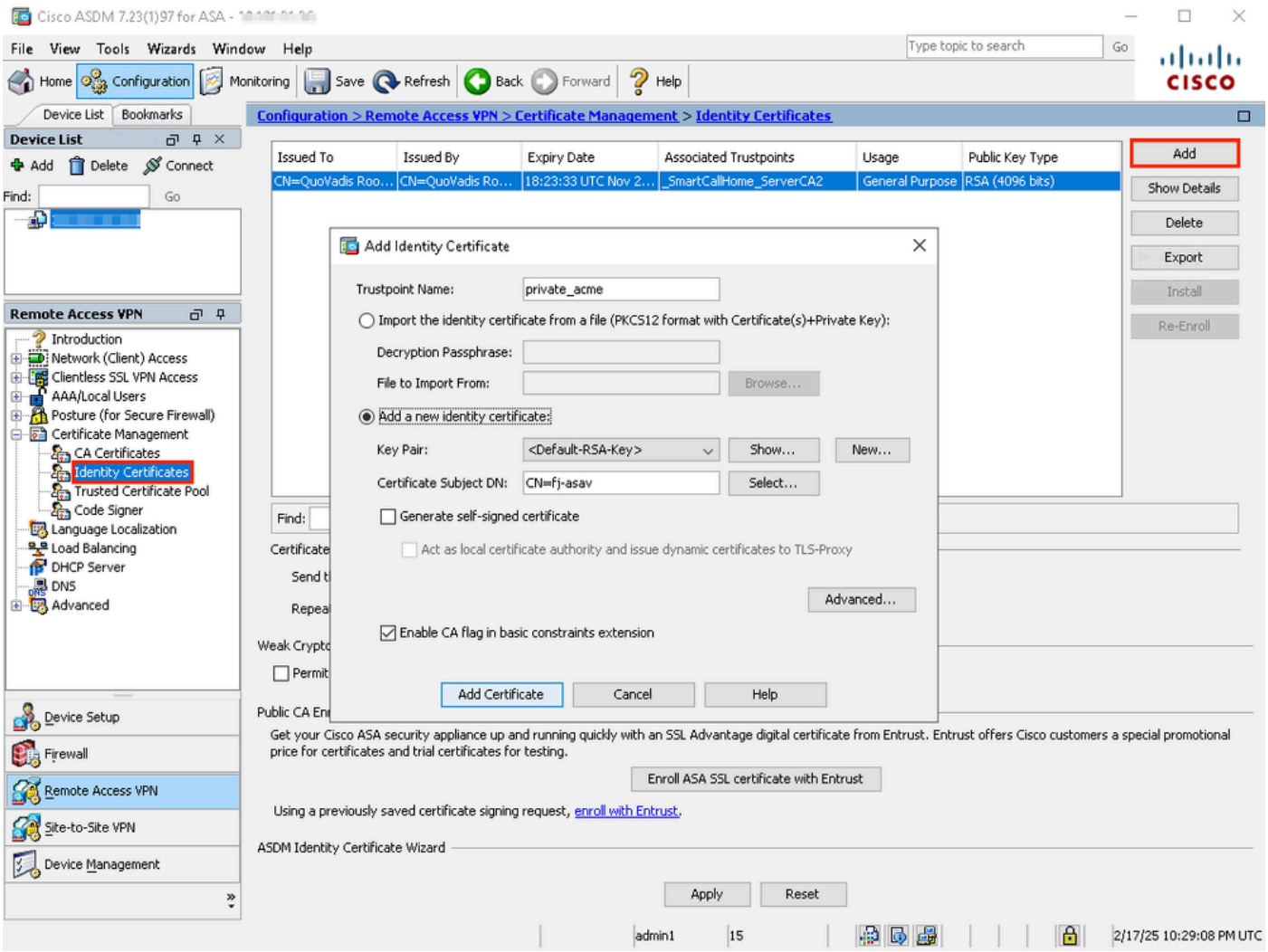
2. 对ACME服务器的安全防火墙访问：安全防火墙必须能够通过其接口之一访问ACME服务器。此访问不需要通过请求证书的接口。
3. TCP端口80可用性：允许从ACME CA服务器到与域名对应的接口的TCP端口80。在ACME交换过程中，完成HTTP-01质询时需要此步骤。

注意：在端口80打开期间，只有ACME质询数据可访问。

使用ASDM进行ACME注册

1.添加新的身份证书。

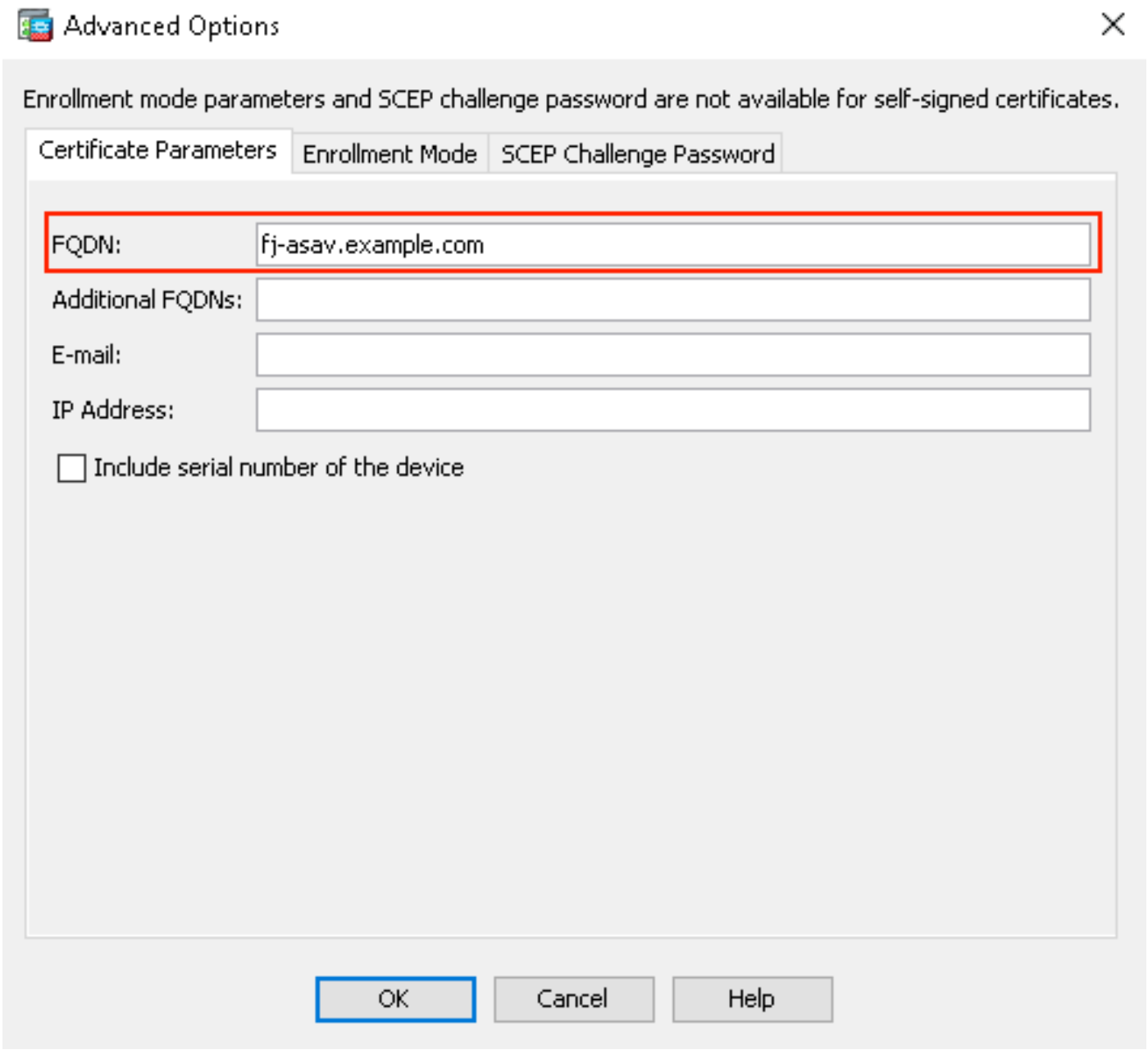
- 导航到Configuration > Remote Access VPN > Certificate Management > Identity Certificates。
- 单击Add按钮，然后选择Add a new identity certificate。



ACME注册ASDM身份证书。

2.指定身份证书的FQDN。

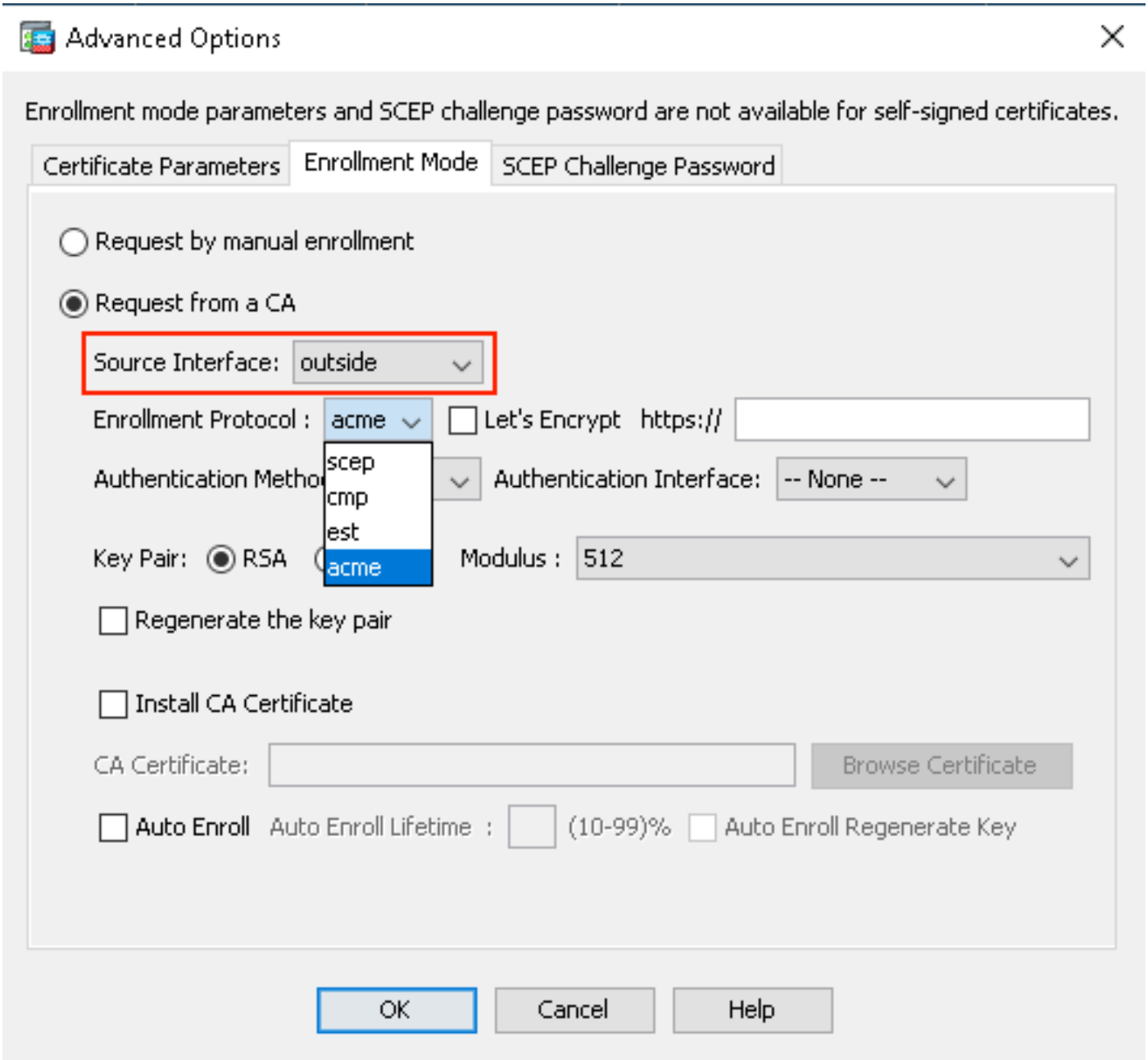
- 单击Advanced按钮。
- 在Certificate Parameters选项卡下，指定证书必须具有的FQDN。



ACME注册ASDM FQDN。

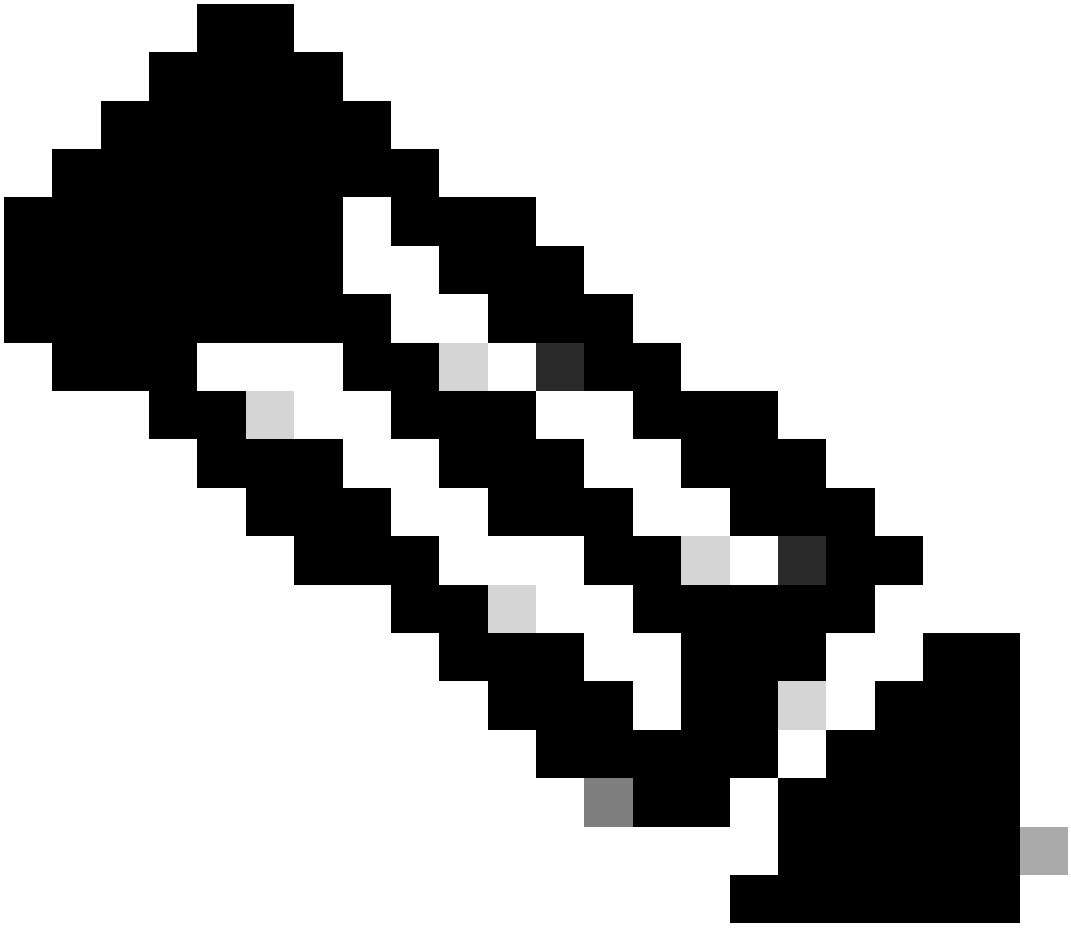
3.选择ACME作为注册协议。

- 在Enrollment Mode选项卡下，选择Request from CA 选项。
- 指定Source Interface并选择acme作为Enrollment Protocol。

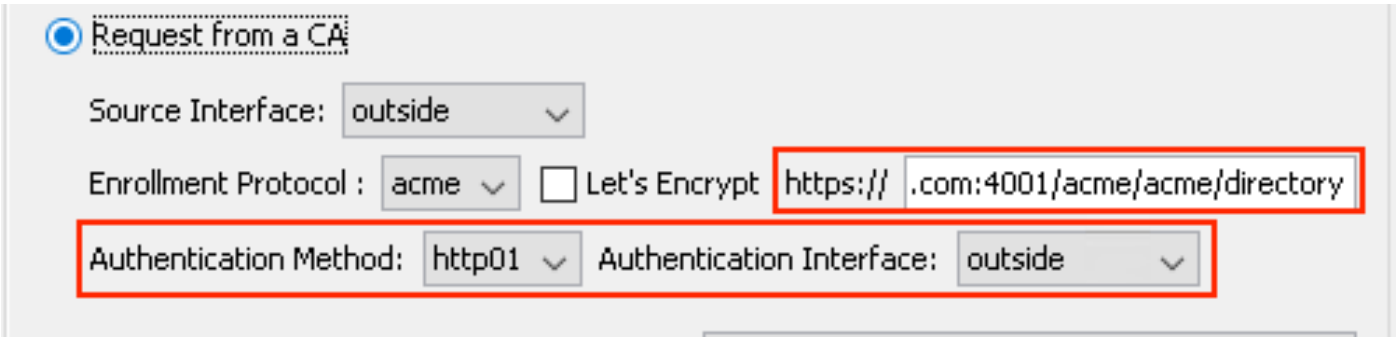


ACME注册ASDM acme协议。选择

4.选择Let's Encrypt，以便证书由Let's Encrypt公共CA签名。否则，请指定支持ACME注册协议的内部CA的URL。此外，指定Authentication Interface。



注意：选中Let's Encrypt复选框后，将自动填充服务器URL。



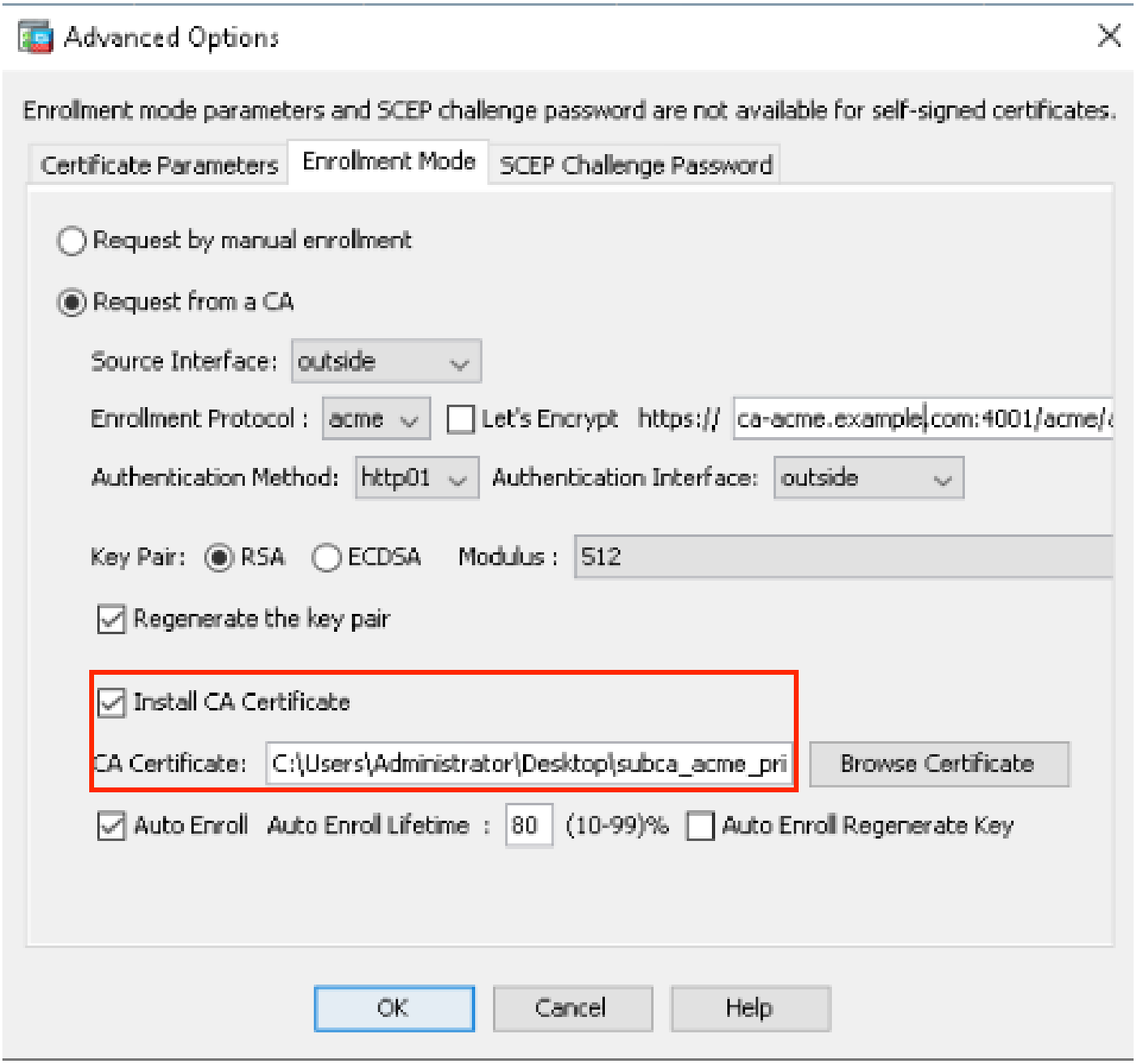
ACME注册ASDM身份验证方法。

5.安装CA证书。

如果选中安装CA证书选项，则必须上传颁发证书的即时CA的证书。

注意：如果CA证书已存在于安全防火墙上（来自以前的安装或位于信任池中），则无需选中此选项。取消选中Install CA Certificate复选框。

注意：选择Let's Encrypt选项时，请取消选中Install CA Certificate复选框，因为Let's Encrypt的根CA证书已包含在安全防火墙信任池中。

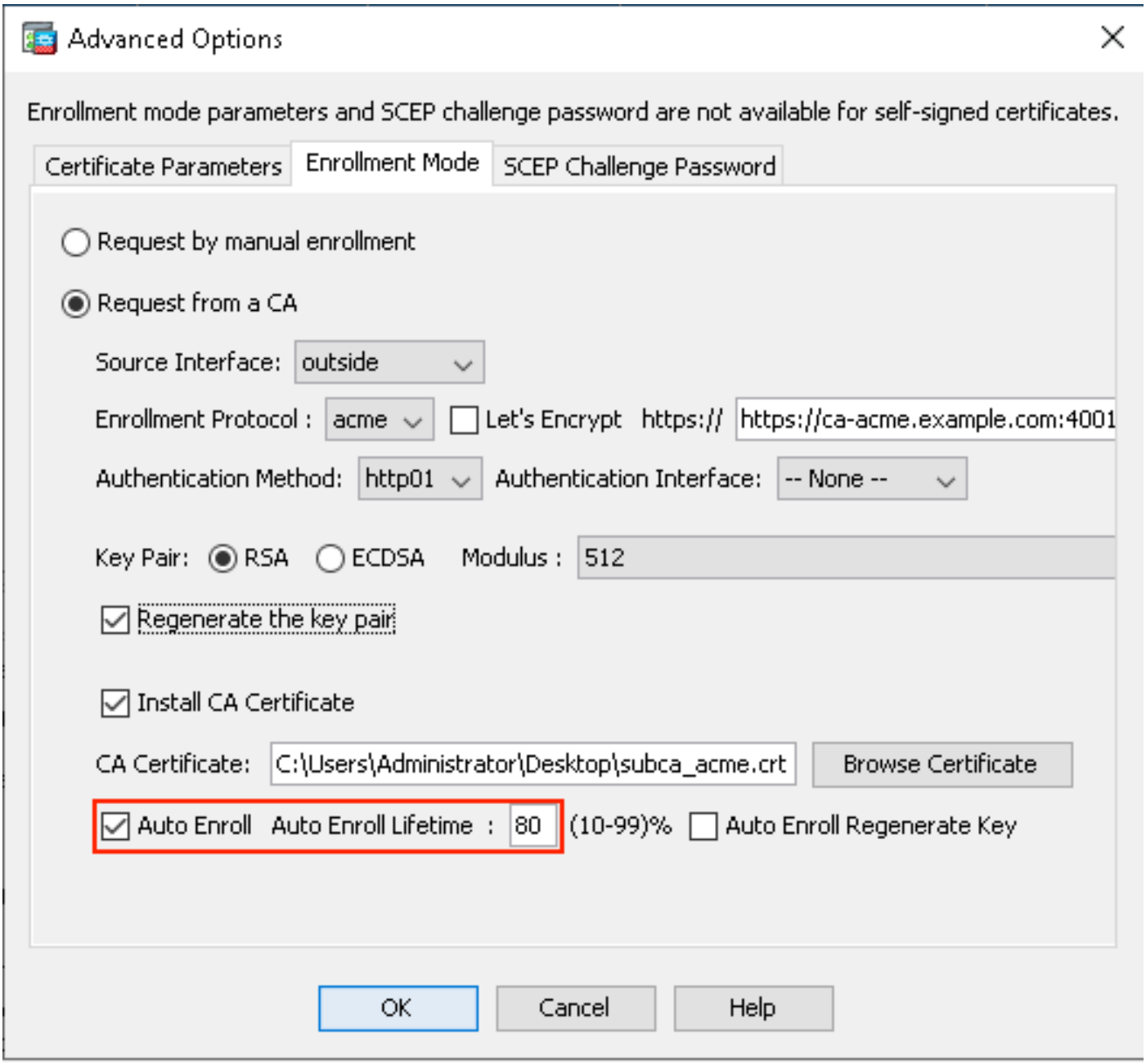


ACME注册ASDM CA安装。

6.（可选）为身份证书启用自动注册。

选中Auto Enroll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。



ACME注册ASDM自动注册。

7.单击OK和Save配置。

使用安全防火墙ASA CLI的ACME注册

1.创建新信任点。

创建信任点并指定acme作为注册协议。

<#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.选择用于验证域控制的身份验证的HTTP-01方法。

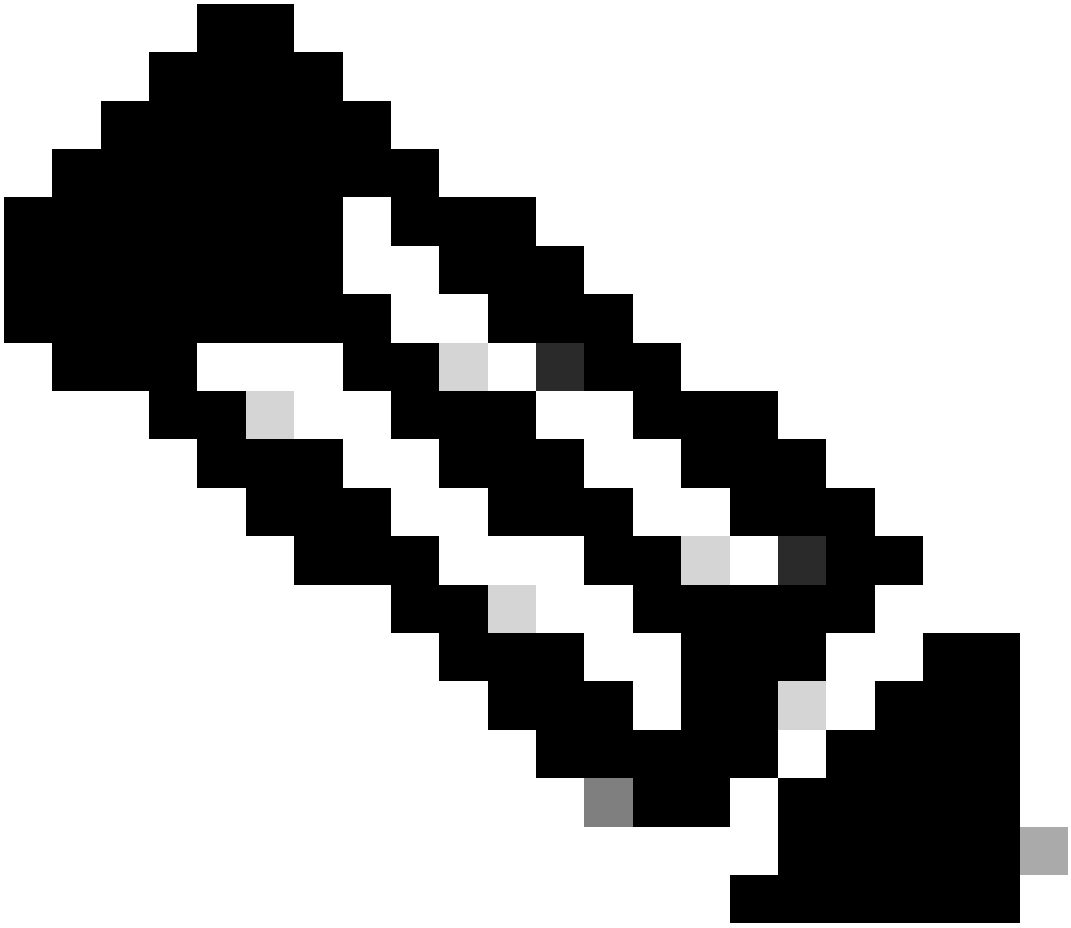
```
asav(config-ca-trustpoint)# enrollment protocol acme authentication ?

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

3.选择“让我们加密作为ACME CA”。如果使用支持ACME协议的另一个CA，请提供相应的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
```



注意：配置LetEncrypt关键字时，将自动填充Let's Encrypt服务器URL。

4.定义RSA密钥对、完全限定域名(FQDN)和证书的使用者名称。

```
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.验证信任点。

> 注意：如果CA已存在于安全防火墙上或者使用Let's Encrypt时，可跳过此步骤。

```
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-----
MIIBwzCCAWqgAwIBAgIQedxaTD0J1G6tLgAGti6tizAKBggqhkjOPQQDAjAsMRAw
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.注册证书。

```
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
```

验证

查看ASA中安装的证书

确认证书已注册并验证续订日期。

```
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: 8c820000000000000000000000000000000000077
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
```

系统日志事件

安全防火墙中有新的系统日志，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

```
%ASA-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

```
%ASA-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

```
%ASA-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

```
%ASA-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>

常见ACME注册错误：

错误代码	原因	可能的原因或补救措施
7	无法连接到服务器	服务器可访问，但ACME服务未运行。
28	无法连接到服务器	无法访问服务器。

		检查对ACME服务器的基本网络访问。
60	无法验证服务器证书	确保根或颁发者CA存在于信任点或信任池中。
124	ACME处理超时	确保所有请求的FQDN都解析到为HTTP-01身份验证配置的接口。 确保配置的ACME URL正确。

相关信息

如需更多帮助，请联系TAC。需要有效的支持合同：思科全球支持联系方式.
您还可以在此处访问Cisco VPN社区。

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）。