在FMC管理的FTD上配置安全客户端证书身份验证

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图
- 配置
  - 创建/导入用于服务器身份验证的证书
  - 添加受信任/内部CA证书
  - 配置VPN用户的地址池
  - 上传安全客户端映像
  - 创建和上传XML配置文件
- 远程访问VPN配置

验证

故障排除

简介

本文档介绍如何在Firepower威胁防御(FTD)通过证书身份验证管理的Firepower管理中心(FMC)上配置远程访问VPN。

先决条件

要求

Cisco 建议您了解以下主题：

- 手动证书注册和安全套接字层(SSL)基础知识
- FMC
- 远程访问VPN的基本身份验证知识
- 第三方证书颁发机构(CA)，如Entrust、Geotrust、GoDaddy、Thawte和VeriSign

使用的组件

本文档中的信息基于以下软件版本：

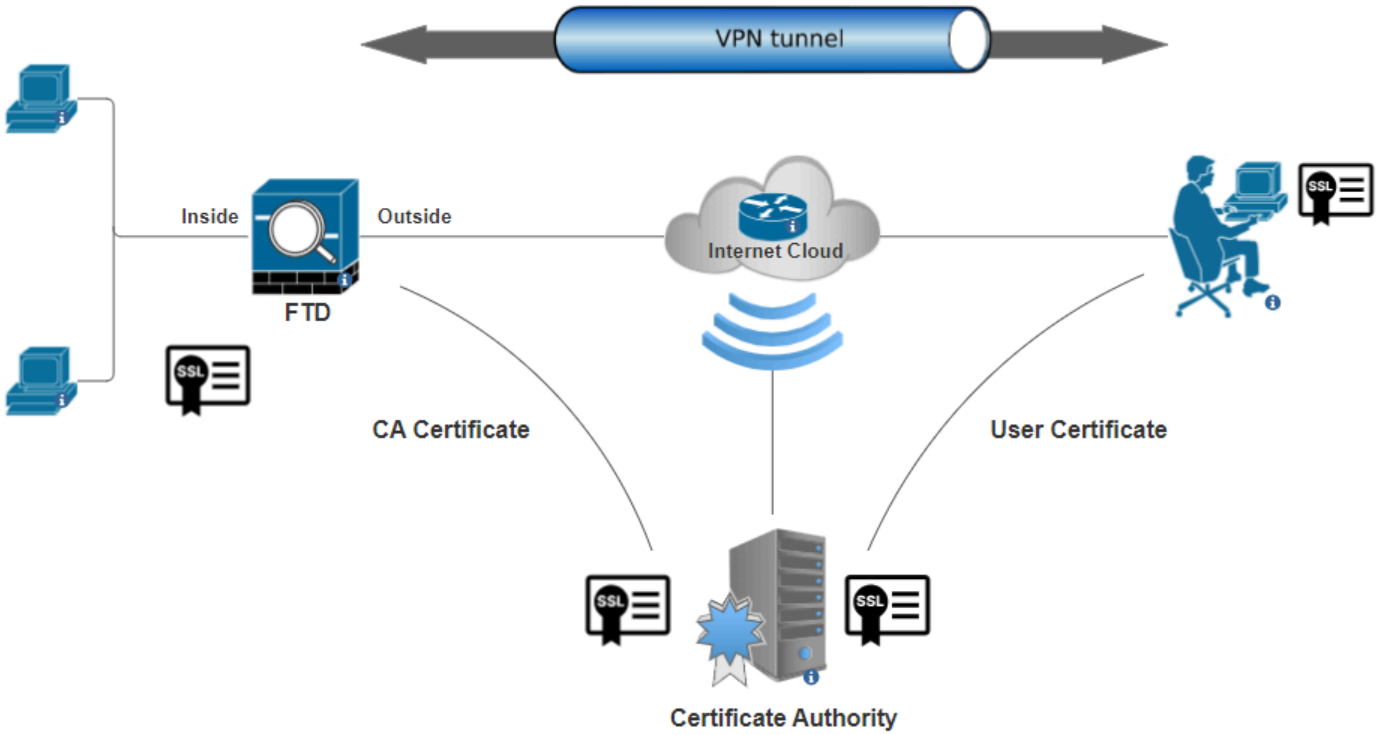
- 安全Firepower威胁防御版本7.4.1

- FMC版本7.4.1
- 安全客户端5.0.05040版
- 作为CA服务器的Microsoft Windows Server 2019

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。

配置

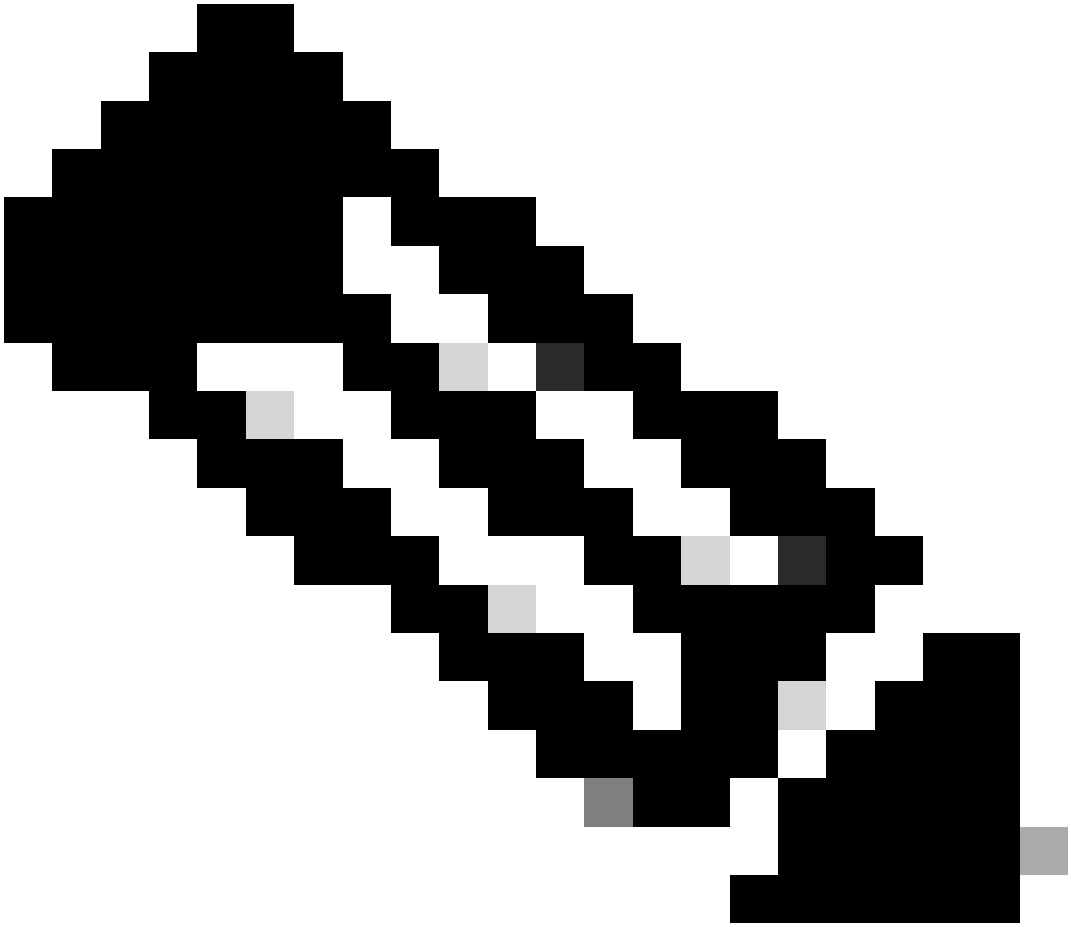
网络图



网络图

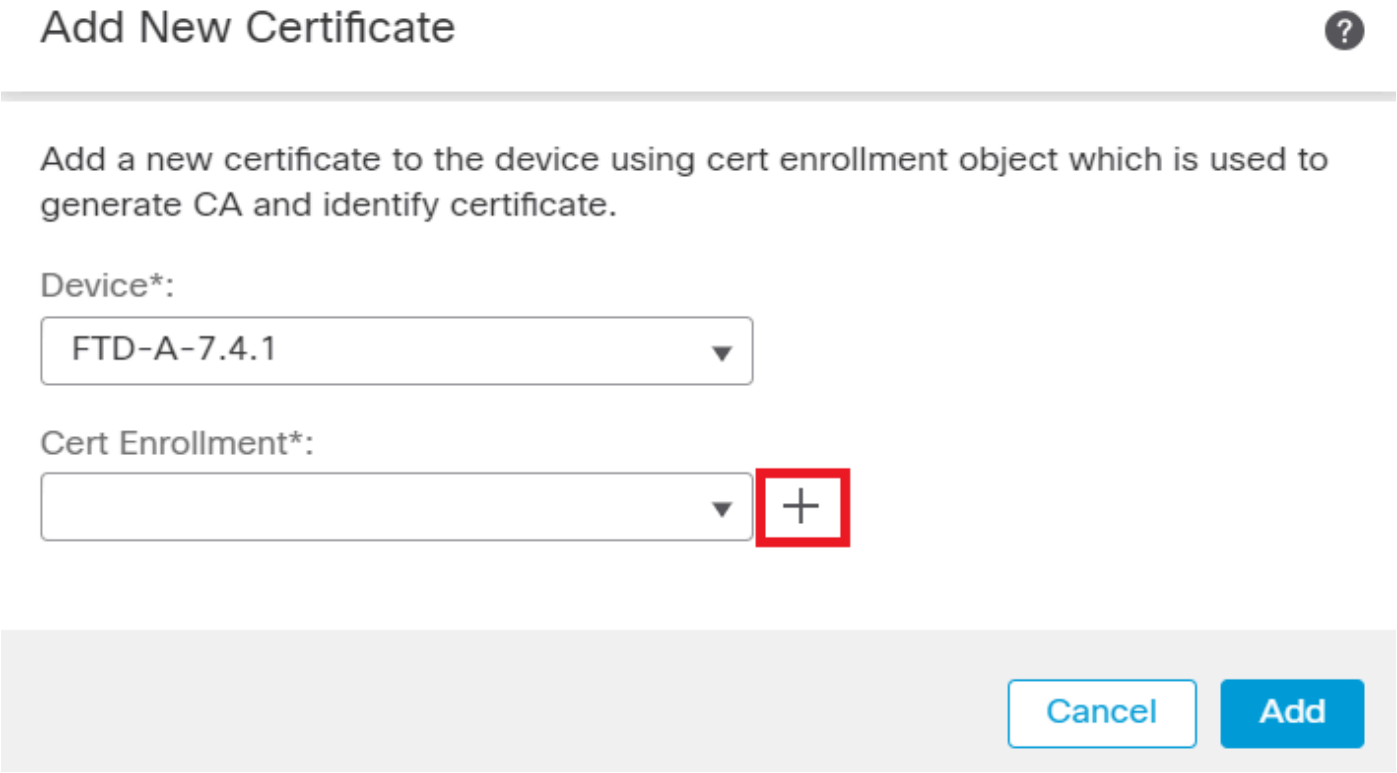
配置

创建/导入用于服务器身份验证的证书



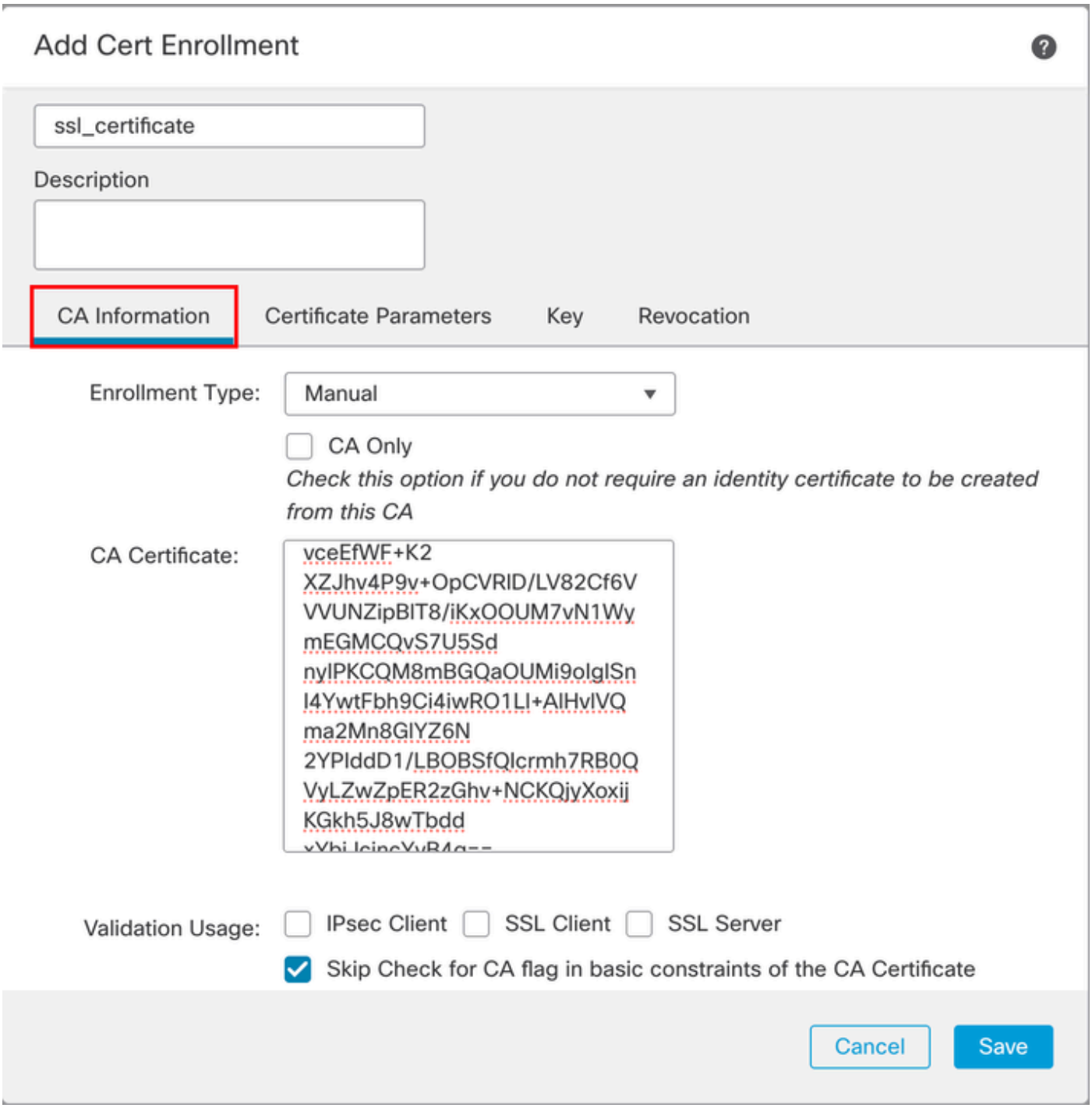
注意：在FMC上，需要证书颁发机构(CA)证书，然后才能生成CSR。如果从外部源（OpenSSL或第三方）生成CSR，手动方法将失败，并且必须使用PKCS12证书格式。

步骤1.导航到Devices > Certificates并点击Add。选择Device，然后单击Cert Enrollment下的加号(+)。



添加证书注册

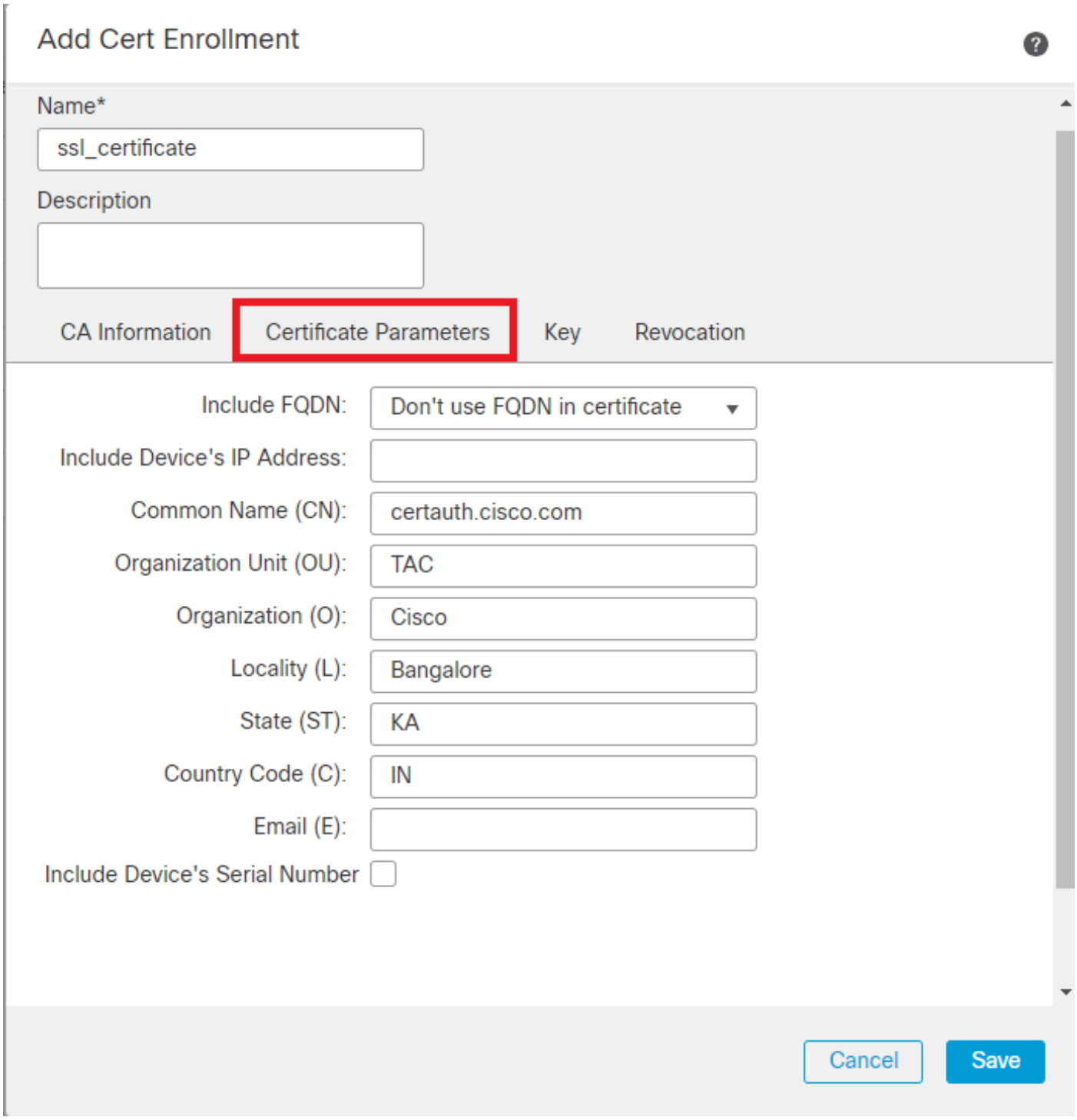
第2步：在CA Information下，选择注册类型Manual，然后粘贴用于签署CSR的CA证书。



添加CA信息

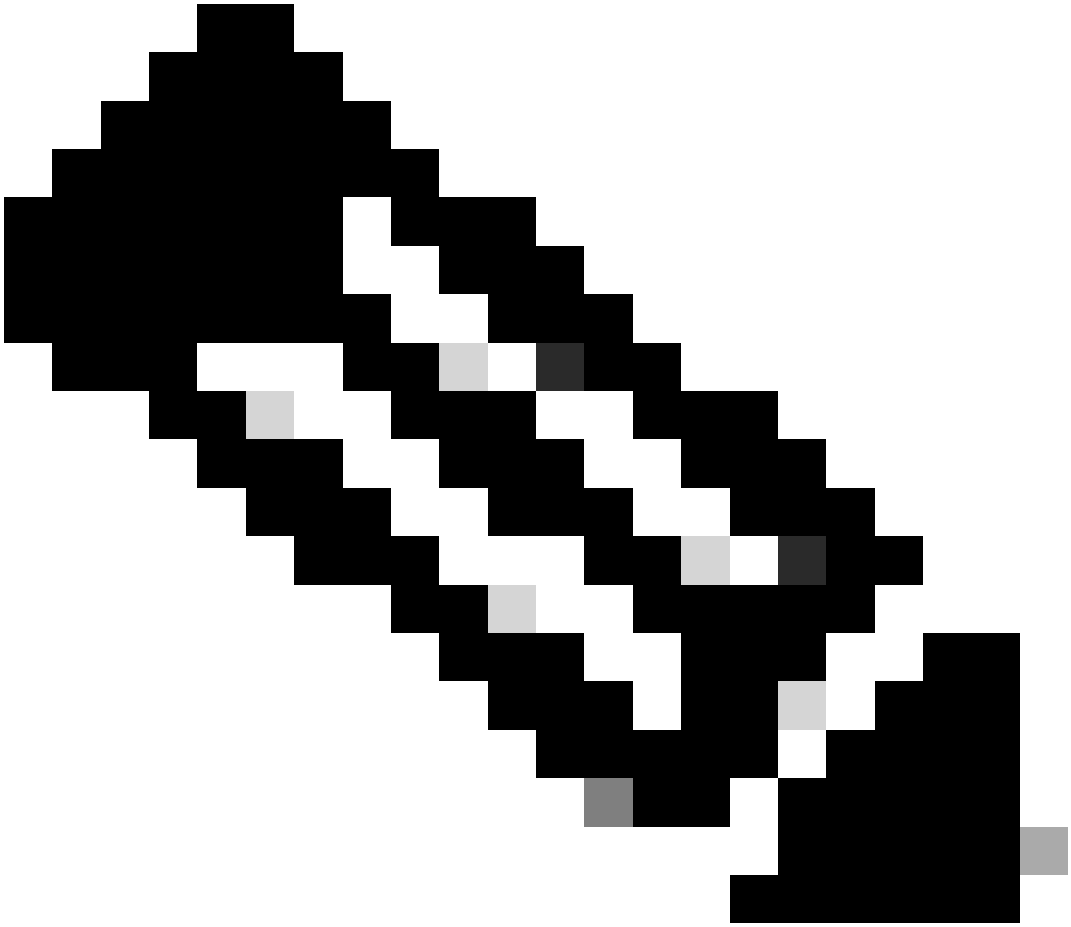
步骤3.选择 Skip Check for CA flag in basic constraints of the CA Certificate as shown in the earlier image.

步骤4.在Certificate Parameters下，填写主题名称详细信息。

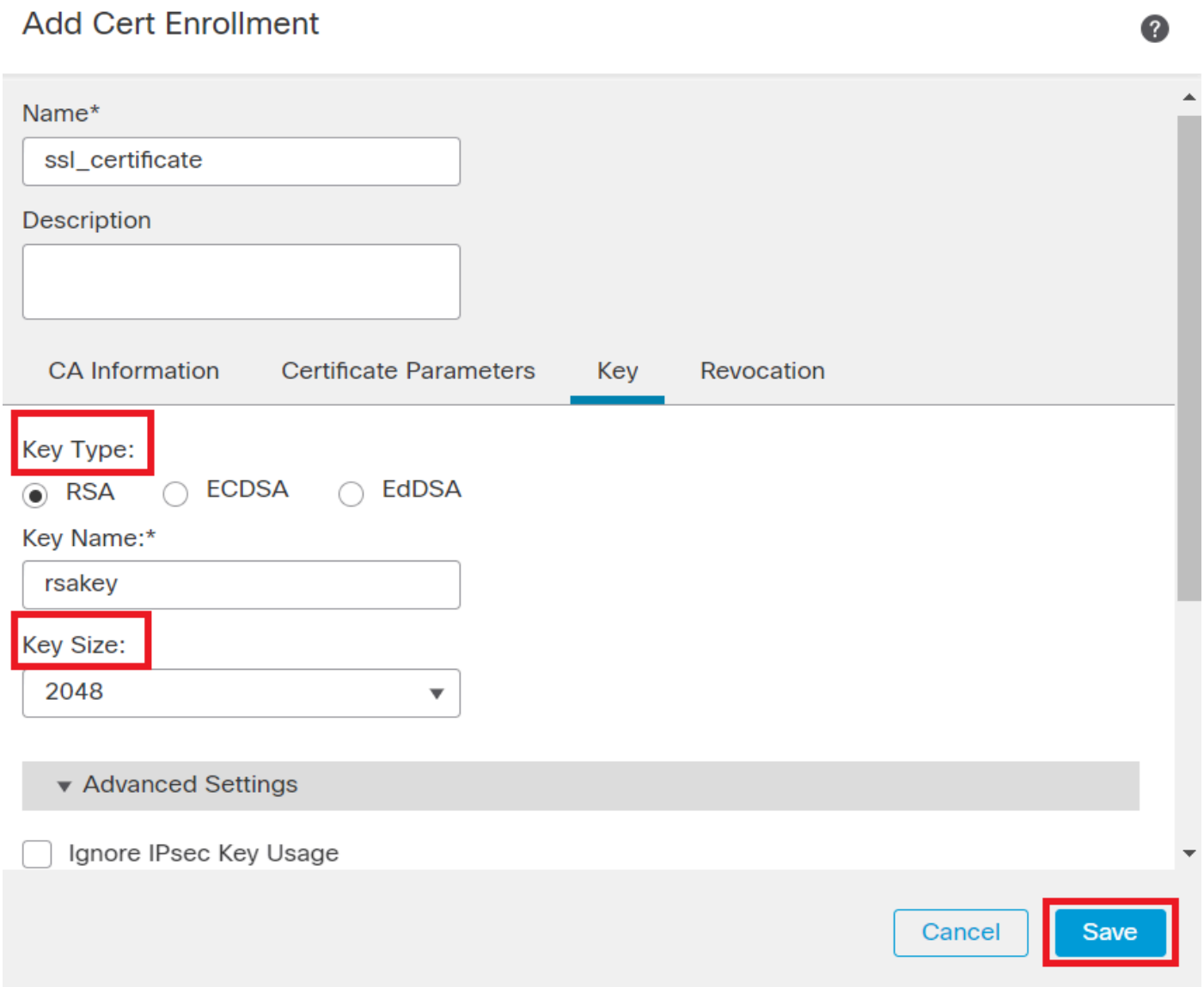


添加证书参数

步骤5.在Key下,选择密钥类型为RSA并带有密钥名称和大小。单击Save。

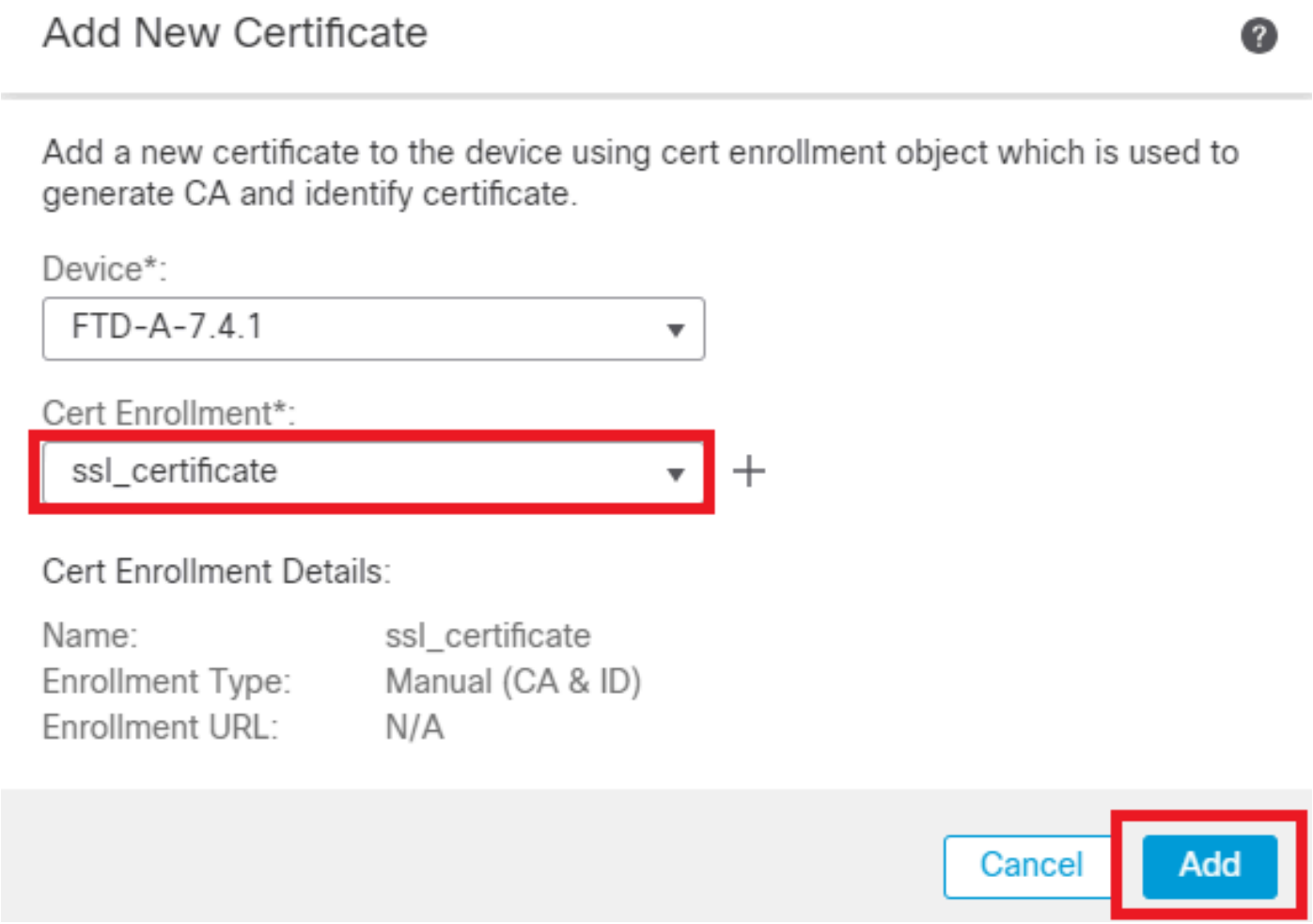


注意：对于RSA密钥类型，最小密钥大小为2048位。



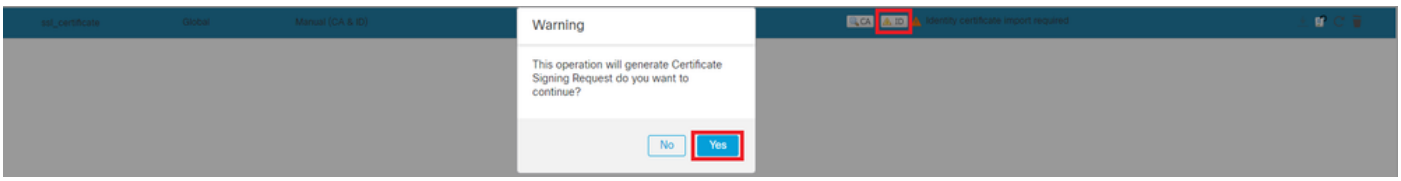
添加RSA密钥

步骤6.在Cert Enrollment下，从刚创建的下拉列表中选择信任点，然后点击Add。



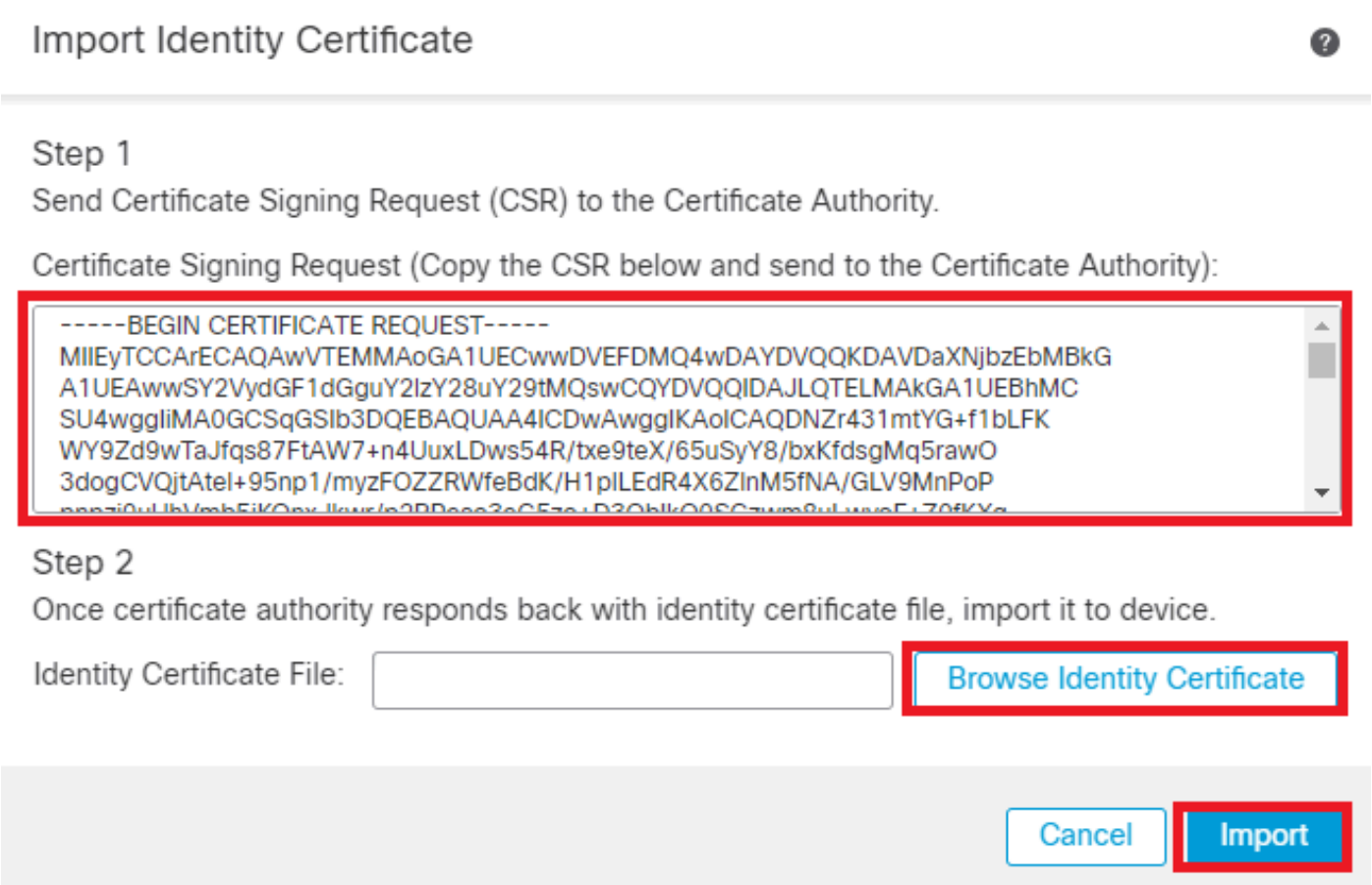
添加新证书

步骤7.单击ID，然后单击Yes“进一步的提示”以生成CSR。

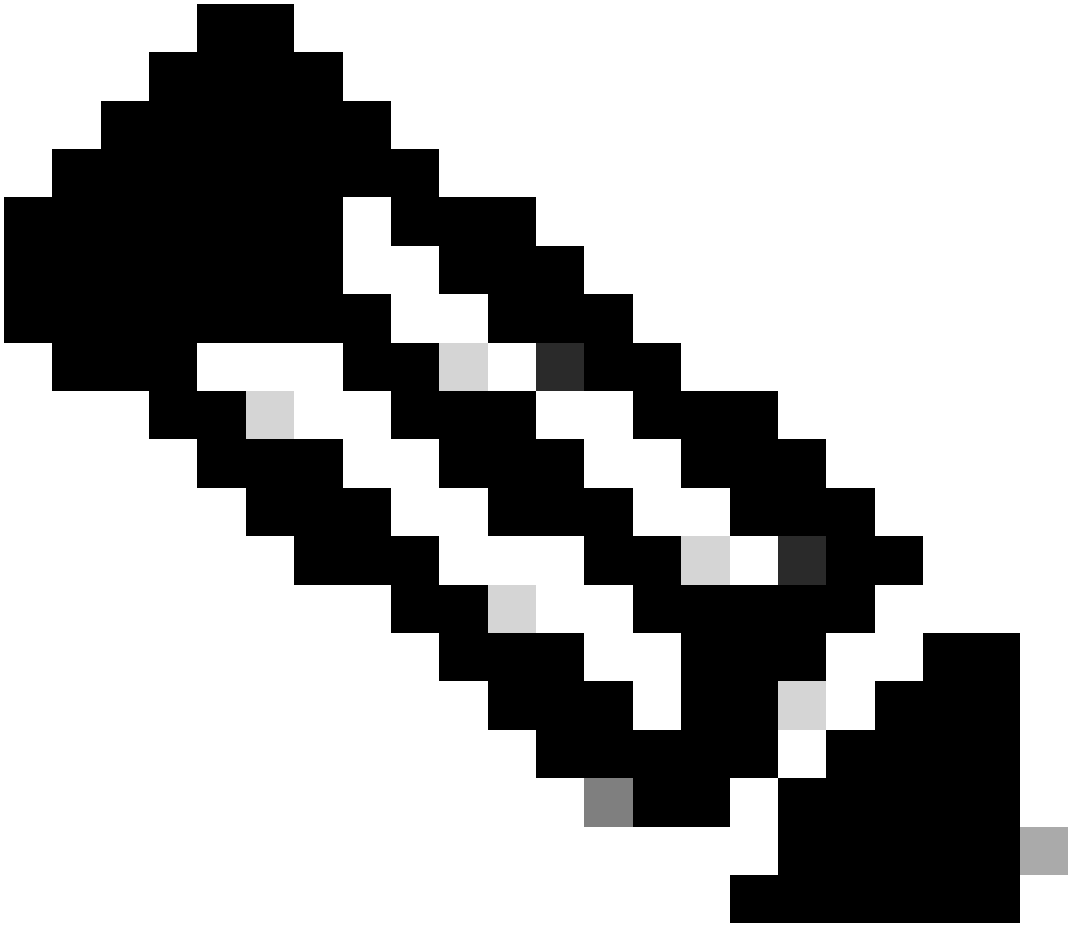


生成 CSR

步骤8.复制CSR并由证书颁发机构签名。一旦身份证书由CA颁发，通过点击并点击Browse Identity Certificate导入身份证Import。


Import Identity Certificate
Step 1
Send Certificate Signing Request (CSR) to the Certificate Authority.
Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):
-----BEGIN CERTIFICATE REQUEST-----
MIIEyTCCArECAQAwVTEMMAoGA1UECwwDVEFDMQ4wDAYDVQQKDAVDaXNjbzEbMBkG
A1UEAwwSY2VydGF1dGguY2lzY28uY29tMQswCQYDVQQIDAJLQTELMAkGA1UEBhMC
SU4wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDNZr431mtYG+f1bLFK
WY9Zd9wTaJfqs87FtAW7+n4UuxLDws54R/txe9teX/65uSyY8/bxKfdsgMq5rawO
3dogCVQjtAtel+95np1/myzFOZZRWfeBdK/H1plLEdR4X6ZlnM5fNA/GLV9MnPoP
Step 2
Once certificate authority responds back with identity certificate file, import it to device.
Identity Certificate File:
Browse Identity Certificate
Cancel
Import

导入ID证书



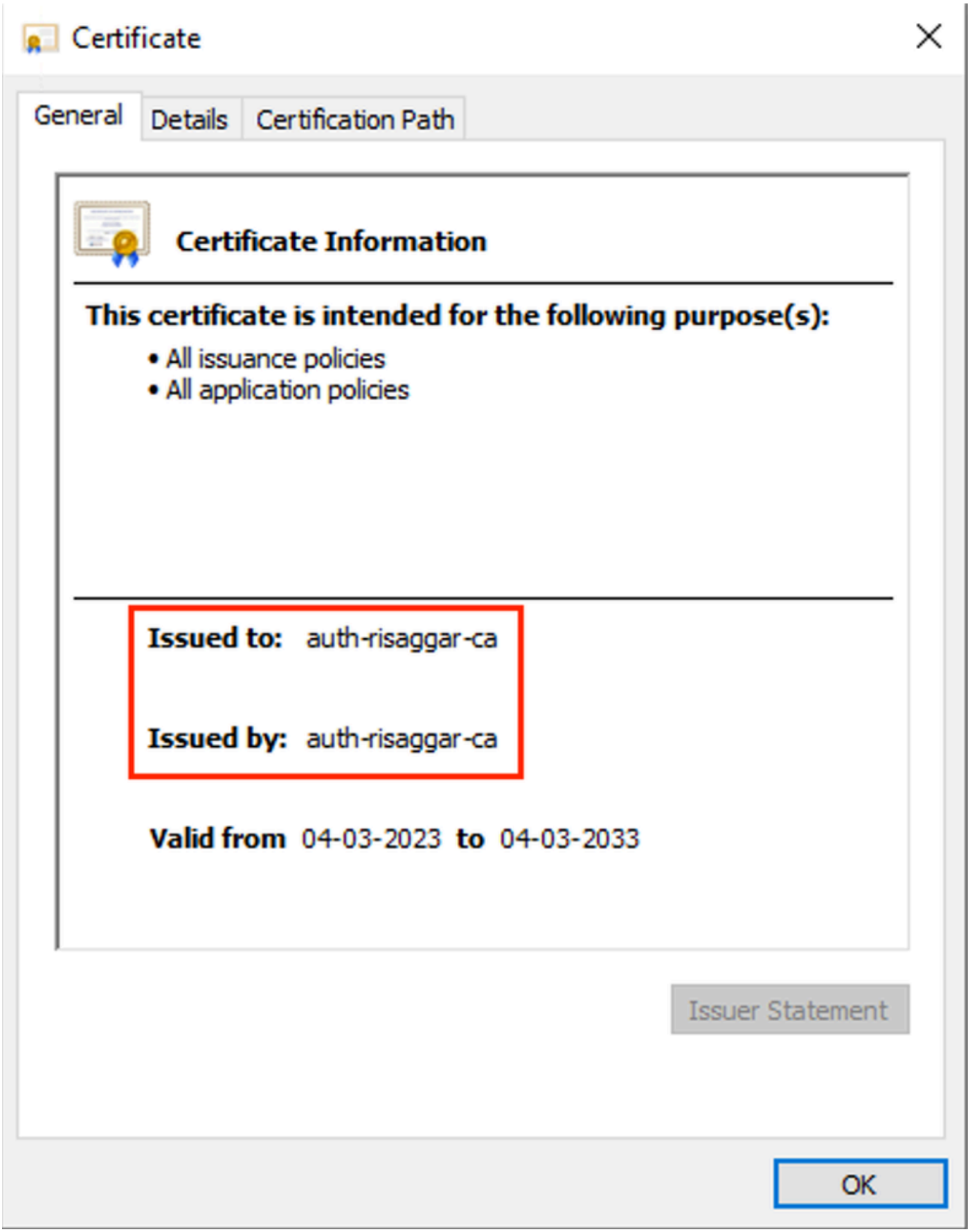
注意：如果ID证书的颁发需要时间，您可以稍后重复步骤7。这将生成相同的CSR，您可以导入ID证书。

添加受信任/内部CA证书

步骤1.导航至Devices > Certificates，然后点Add击。

选择Device，然后单击Cert Enrollment下的加号(+)。

此处，auth-risaggar-ca用于颁发身份/用户证书。

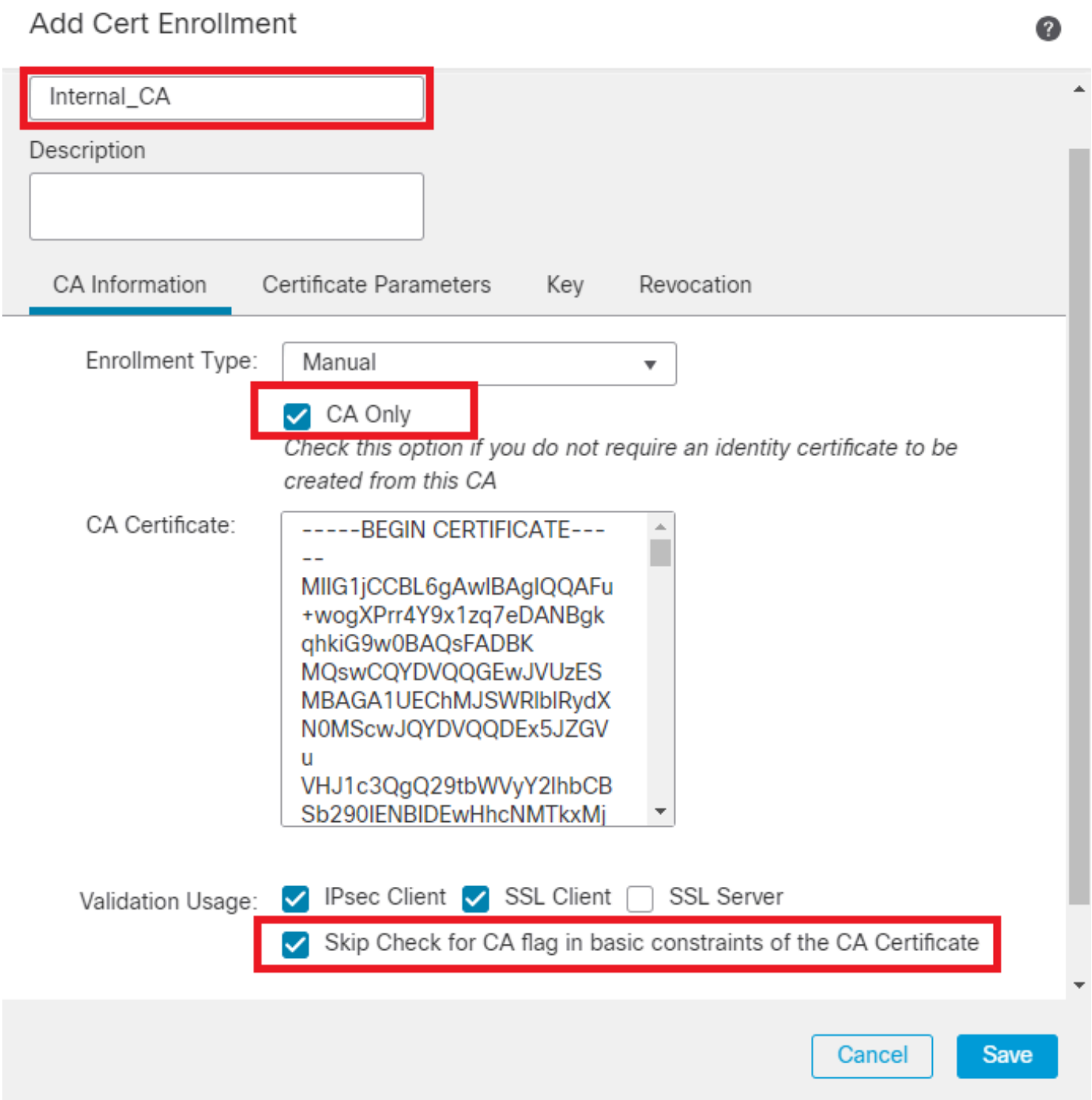


auth-risaggar-ca

步骤2.输入信任点名称，然后Manual选择作为注册类CA information型。

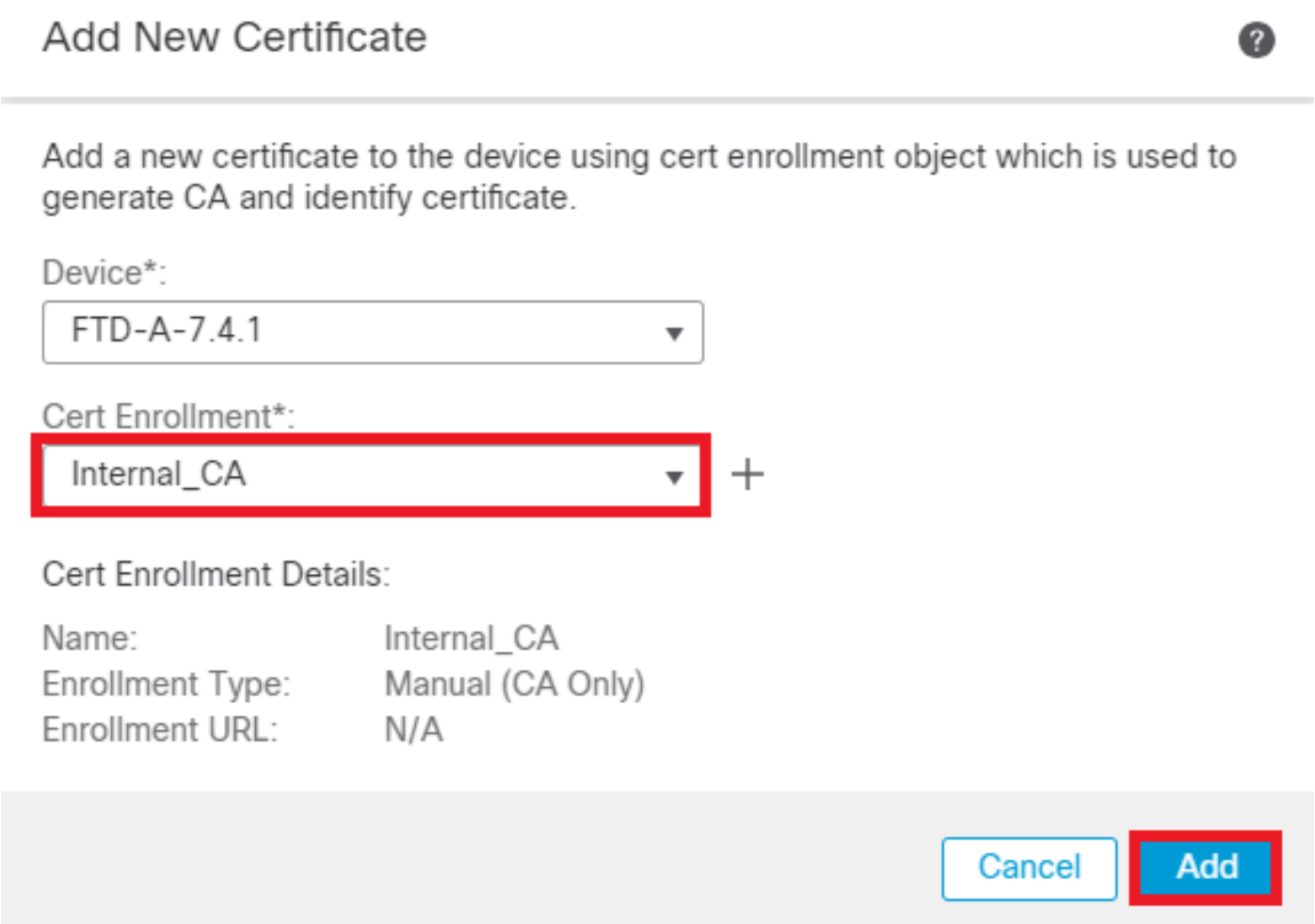
步骤3.检查CA Only并粘贴受CA信任的/内部CA证书的PEM格式。

步骤4.选中**Skip Check for CA flag in basic constraints of the CA Certificate**并单击Save。



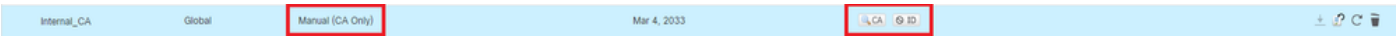
添加信任点

步骤5.在Cert Enrollment下，从刚创建的下拉列表中选择信任点，然后点击Add。



添加内部CA

步骤6.前面添加的证书显示如下：

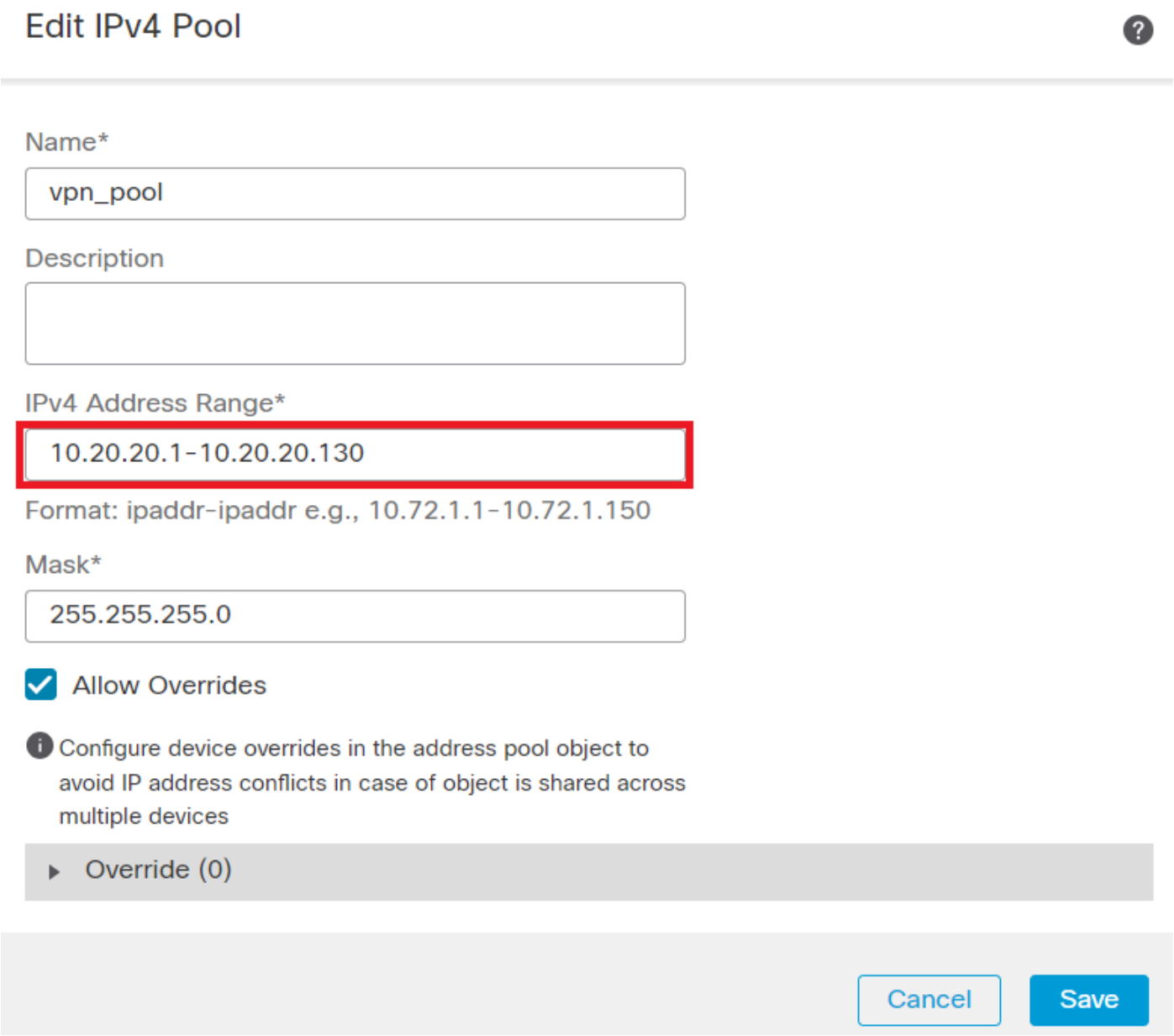


已添加证书

配置VPN用户的地址池

步骤1.导航至Objects > Object Management > Address Pools > IPv4 Pools。

步骤2.输入名称和带掩码的IPv4地址范围。



添加IPv4池

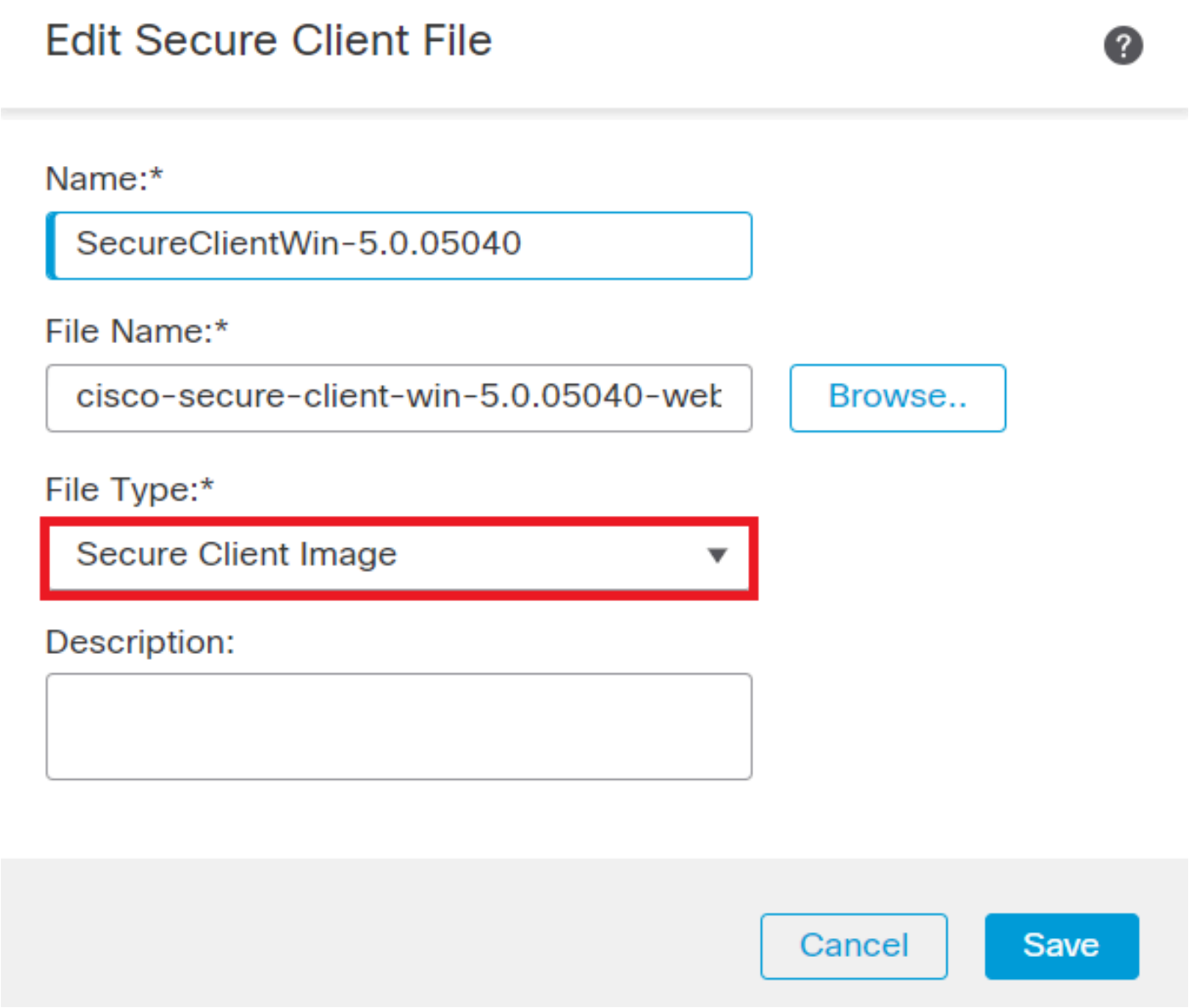
上传安全客户端映像

步骤1.从思科软件站点按操作系统下载webdeploy安全客户端映像。

步骤2.导航至Objects > Object Management > VPN > Secure Client File > Add Secure Client File。

步骤3.输入名称，然后从磁盘中选择Secure Client文件。

步骤4.选择文件类型作为Secure Client Image，然后单Save击。



添加安全客户端映像

创建和上传XML配置文件

步骤1.从思科软件站点下载Profile Editor并安装安全客户端。

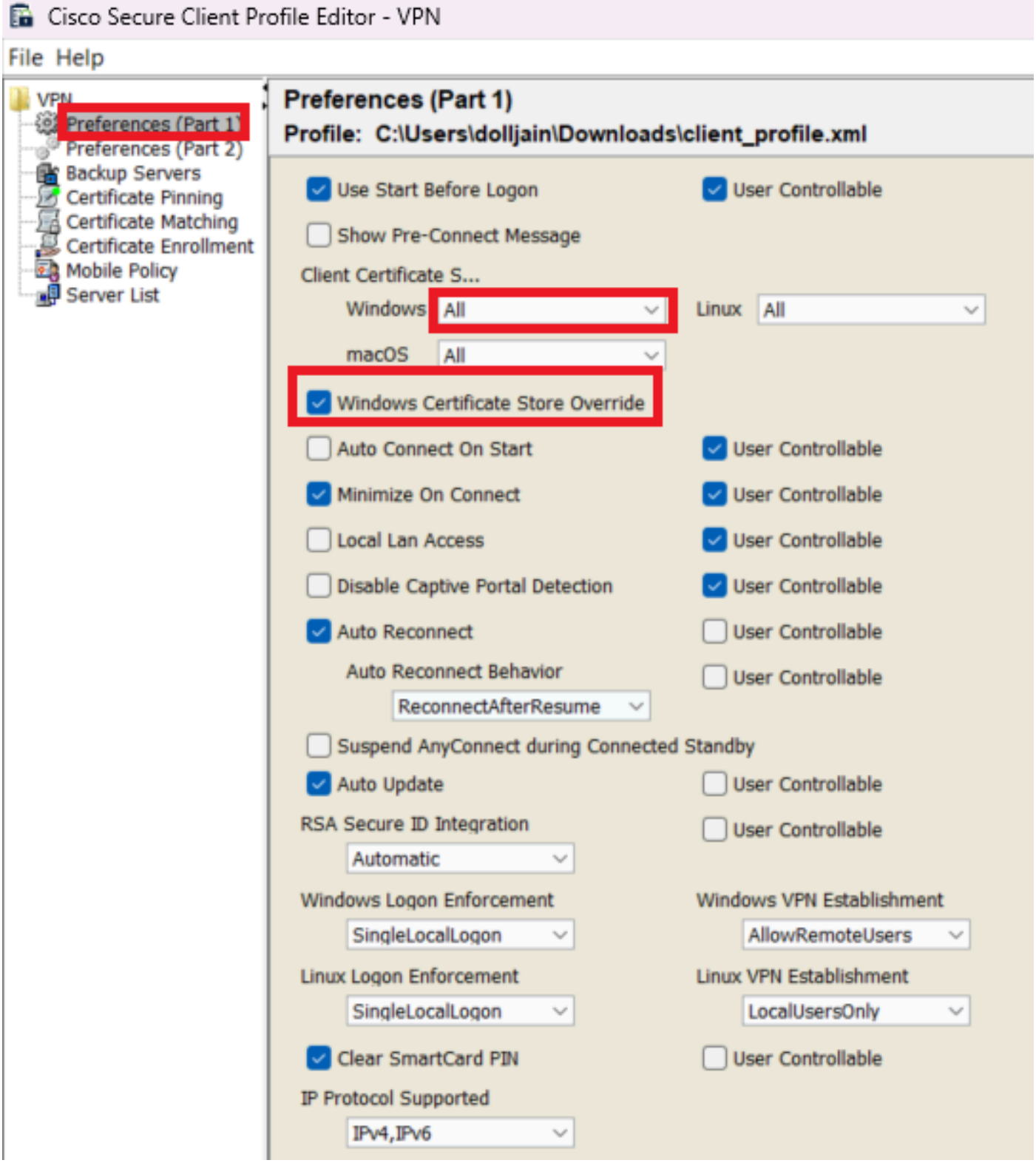
步骤2.创建新配置文件并从AllClient Certificate Selection下拉列表中选择。它主要控制Secure Client可以使用哪些证书存储区来存储和读取证书。

另外两个可用选项是：

1. 计算机 — 安全客户端仅限于Windows本地计算机证书存储区上的证书查找。
2. 用户 — 安全客户端仅限于在本地Windows用户证书存储区上查找证书。

将“证书存储区覆盖”(Certificate Store Override)设置为True。

这允许管理员指示安全客户端使用Windows计算机（本地系统）证书存储中的证书进行客户端证书身份验证。证书存储区覆盖仅适用于SSL，默认情况下，连接由UI进程发起。使用IPSec/IKEv2时，安全客户端配置文件中的此功能不适用。



添加首选项（第1部分）

步骤3.（可选）取消选中Disable Automatic Certificate Selection，因为它会避免提示用户选择身份验证证书。

Cisco Secure Client Profile Editor - VPN

File Help

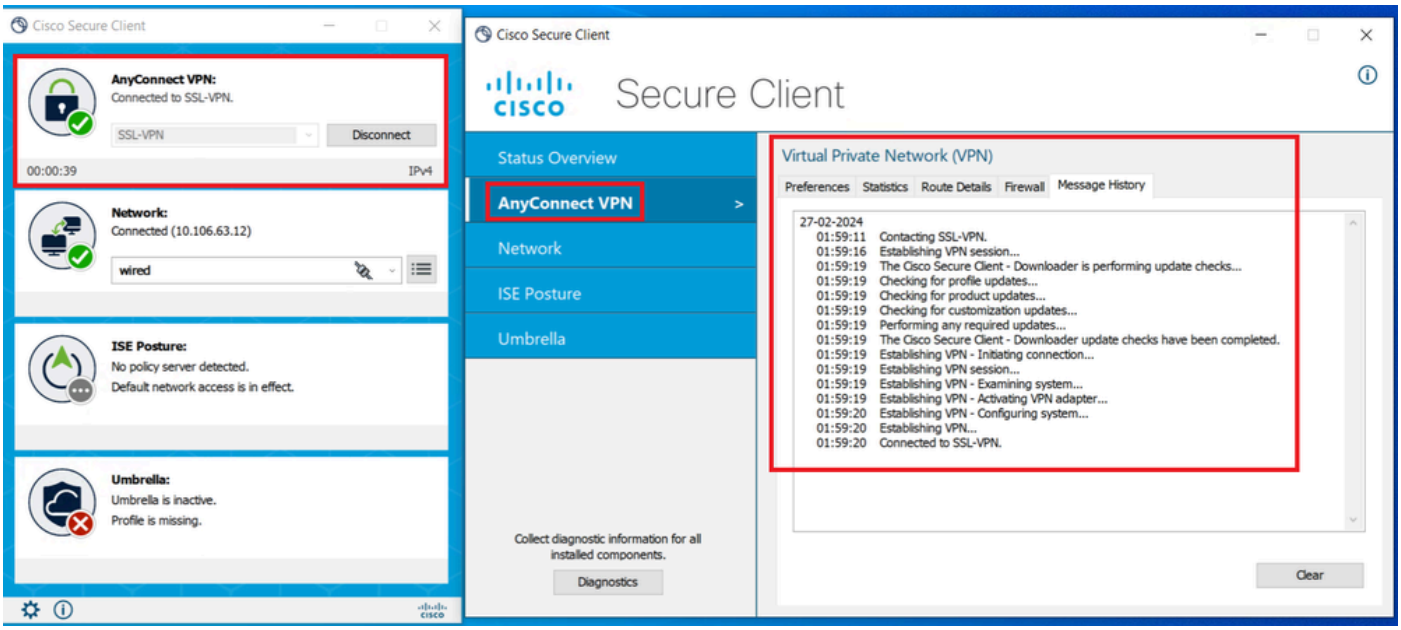
VPN
- Preferences (Part 1)
- Preferences (Part 2)
- Backup Servers
- Certificate Pinning
- Certificate Matching
- Certificate Enrollment
- Mobile Policy
- Server List

Preferences (Part 2)

Profile: C:\Users\dolljain\Downloads\client_profile.xml

- [ ] Disable Automatic Certificate Selection — [ ] User Controllable
- Proxy Settings: Native — [x] User Controllable
- Public Proxy Server Address:
- Note: Enter public Proxy Server address and Port here. Example:10.86.125.33:8080
- [x] Allow Local Proxy Connections
- [ ] Enable Optimal Gateway Selection — [ ] User Controllable
- Suspension Time Threshold (hours): 4
- Performance Improvement Threshold (%): 20
- [ ] Automatic VPN Policy
- Trusted Network Policy: Disconnect
- Untrusted Network Policy: Connect
- [ ] Bypass connect upon VPN session timeout
- Trusted DNS Domains
- Trusted DNS Servers
- Note: adding all DNS servers in use is recommended with Trusted Network Detection
- Trusted Servers @ https://<server>[:<port>]
- https://
- Add
- Delete
- Certificate Hash:
- Set
- [ ] Disable interfaces without trusted server connectivity while in truste...
- [ ] Always On — (More Information)
- [ ] Allow VPN Disconnect
- Allow access to the following hosts with VPN disconn...
- Connect Failure Policy: Closed
- [ ] Allow Captive Portal Remediation
- Remediation Timeout (min.): 5
- [ ] Apply Last VPN Local Resource Rules
- [ ] Captive Portal Remediation Browser Failover
- [x] Allow Manual Host Input
- PPP Exclusion: Disable — [ ] User Controllable
- PPP Exclusion Server IP — [ ] User Controllable
- [ ] Enable Scripting — [ ] User Controllable
- [ ] Terminate Script On Next Event — [ ] Enable Post SBL On Connect Script
- [ ] Retain VPN on Logoff
- User Enforcement: Same User Only
- Authentication Timeout (seconds): 30

添加首选项（第2部分）



成功的安全客户端连接

3.运行show vpn-sessiondb anyconnect，以便确认已使用的隧道组下活动用户的连接详细信息。

```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dolljain.cisco.com     Index        : 8
Assigned IP  : 10.20.20.1             Public IP    : 72.163.X.X
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256
Bytes Tx     : 14402                  Bytes Rx     : 9652
Group Policy : DfltGrpPolicy          Tunnel Group : RAVPN-CertAuth
Login Time   : 08:32:22 UTC Mon Mar 18 2024
Duration     : 0h:03m:59s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0ac5de050000800065f7fc16
Security Grp : none                   Tunnel Zone  : 0
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

1.可以从FTD的诊断CLI运行调试：

```
debug crypto ca 14
debug webvpn anyconnect 255
debug crypto ike-common 255
```

2.有关常见问题，请参阅本指南。

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）。