配置证书身份验证&DUO SAML身份验证

目录

简介

本文档介绍实施基于证书的身份验证和双重SAML身份验证的示例。

先决条件

本指南中使用的工具和设备包括：

- 思科Firepower威胁防御(FTD)
- Firepower Management Center (FMC)
- 内部证书颁发机构(CA)
- Cisco DUO Premier帐户
- Cisco DUO身份验证代理
- 思科安全客户端(CSC)

要求

Cisco 建议您了解以下主题：

- 基本VPN、
- SSL/TLS
- 公钥基础设施

- 使用FMC的经验
- 思科安全客户端
- FTD代码7.2.0或更高版本
- Cisco DUO身份验证代理

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTD(7.3.1)
- 思科FMC(7.3.1)
- 思科安全客户端(5.0.02075)
- 思科DUO身份验证代理(6.0.1)
- Mac OS(13.4.1)
- Active Directory

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。

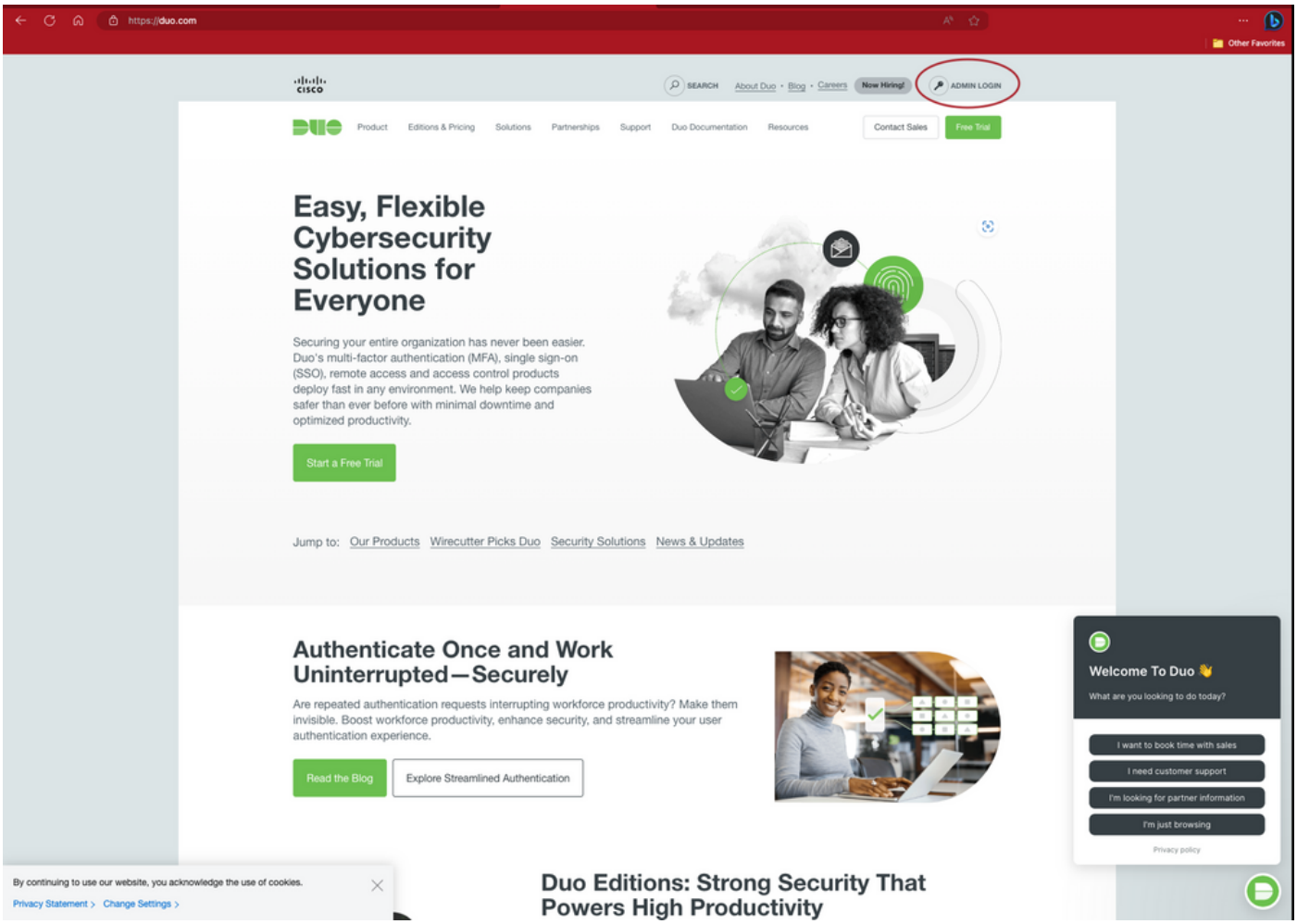
在DUO上配置步骤

本节介绍配置Cisco DUO单点登录(SSO)的步骤。开始之前，请确保实施身份验证代理。

警告：如果尚未实施身份验证代理，此链接带有此任务的指南。DUO Authentication Proxy Guide

创建应用保护策略

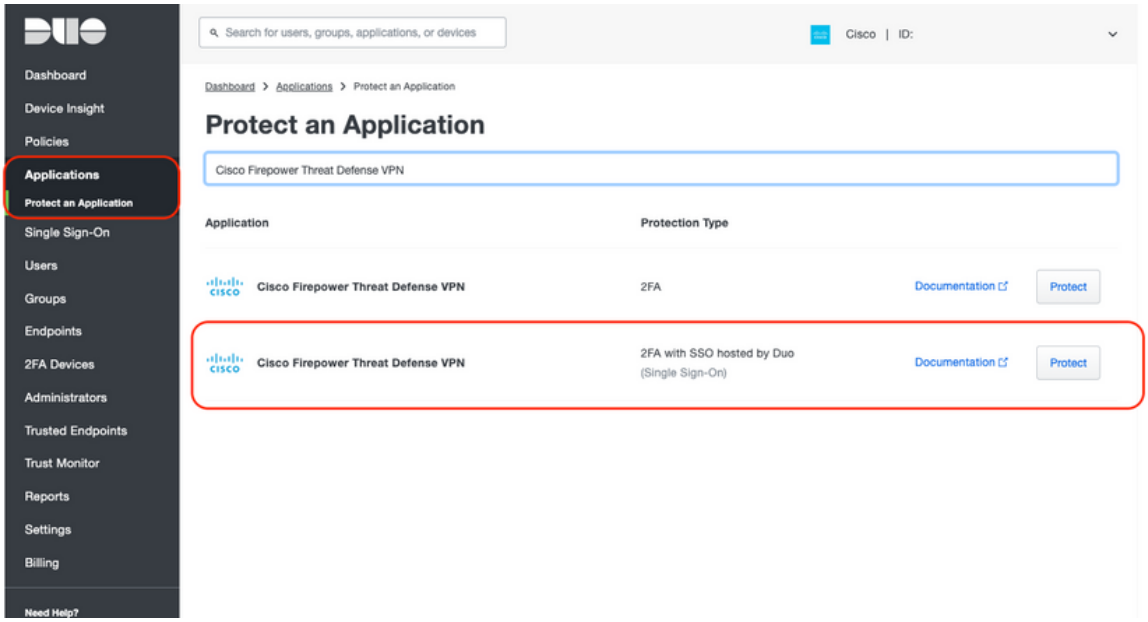
步骤1.通过此链接Cisco Duo，登录到管理面板



Cisco DUO主页

步骤2.导航到控制面板>应用>保护应用。

在搜索栏中，输入“Cisco Firepower Threat Defense VPN”，然后选择“Protect”。



保护应用屏幕截图

选择仅具有保护类型“2FA with SSO hosted by Duo”的选项。

步骤 3：在元数据下复制此URL信息。

- 标识提供程序实体ID
- SSO URL
- 注销URL

要复制的信息示例

注意：屏幕截图中已省略了这些链接。

第4步：选择“下载证书”以下载“下载”下的身份提供程序证书。

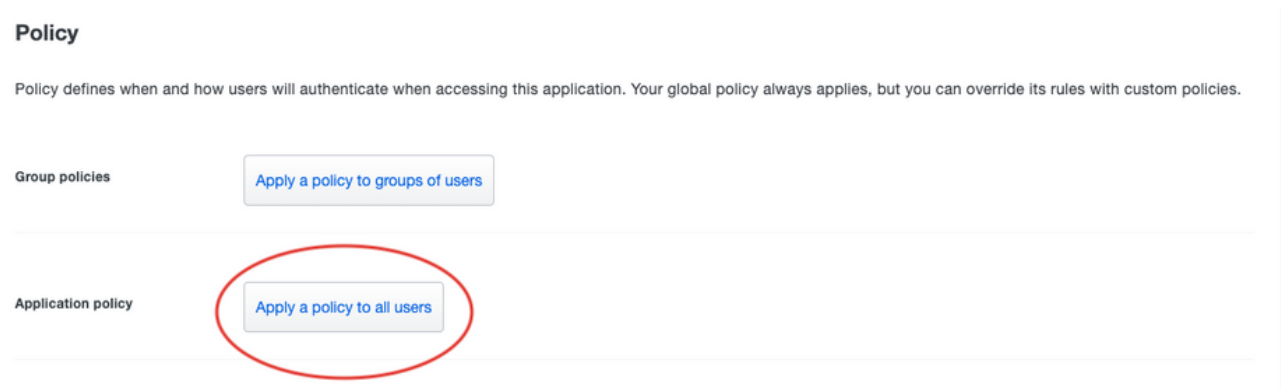
步骤5.填写服务提供商信息

Cisco Firepower基础URL — 用于访问FTD的FQDN

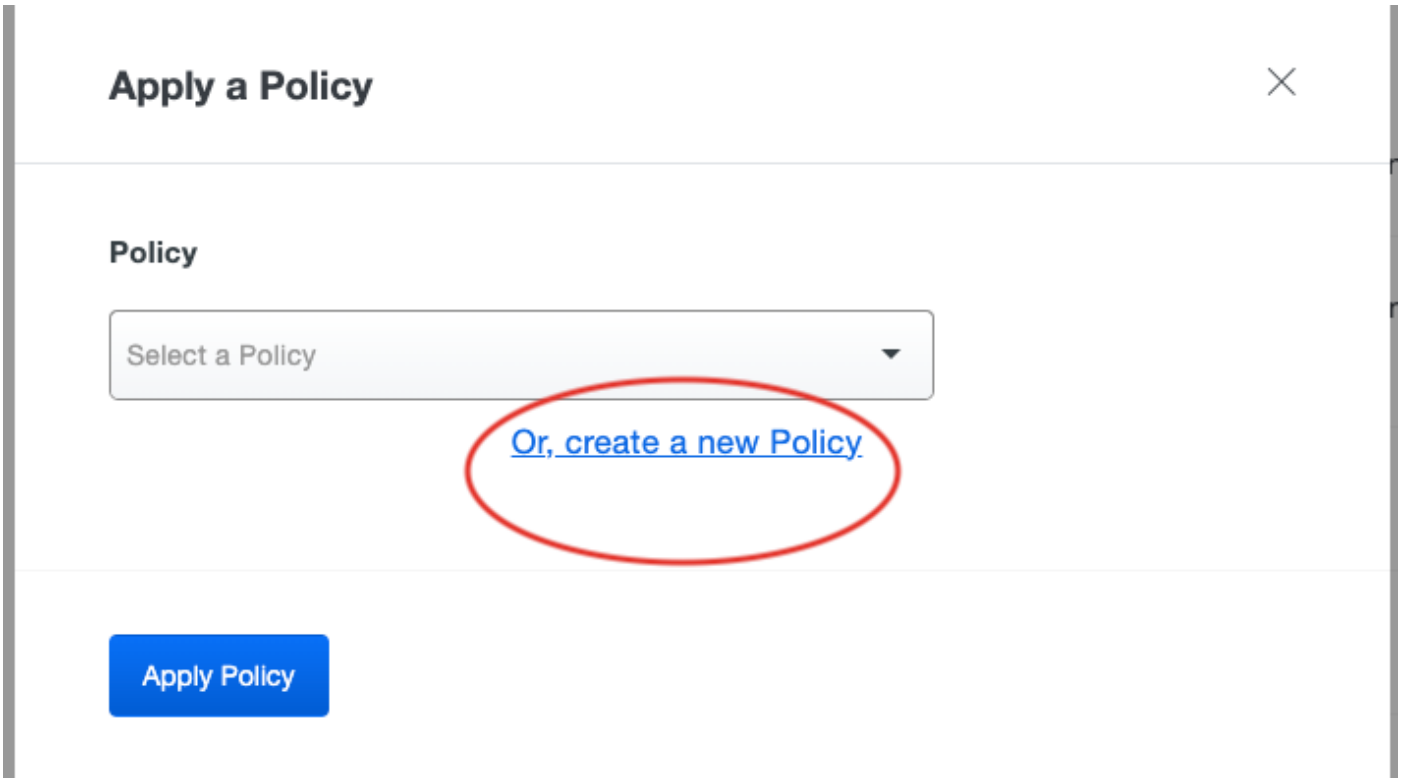
连接配置文件名称 — 隧道组名称

创建应用策略

步骤 1：要在Policy 下创建Application Policy，请选择“Apply a policy to all users”，然后选择“Or，create a new Policy”，如图所示。

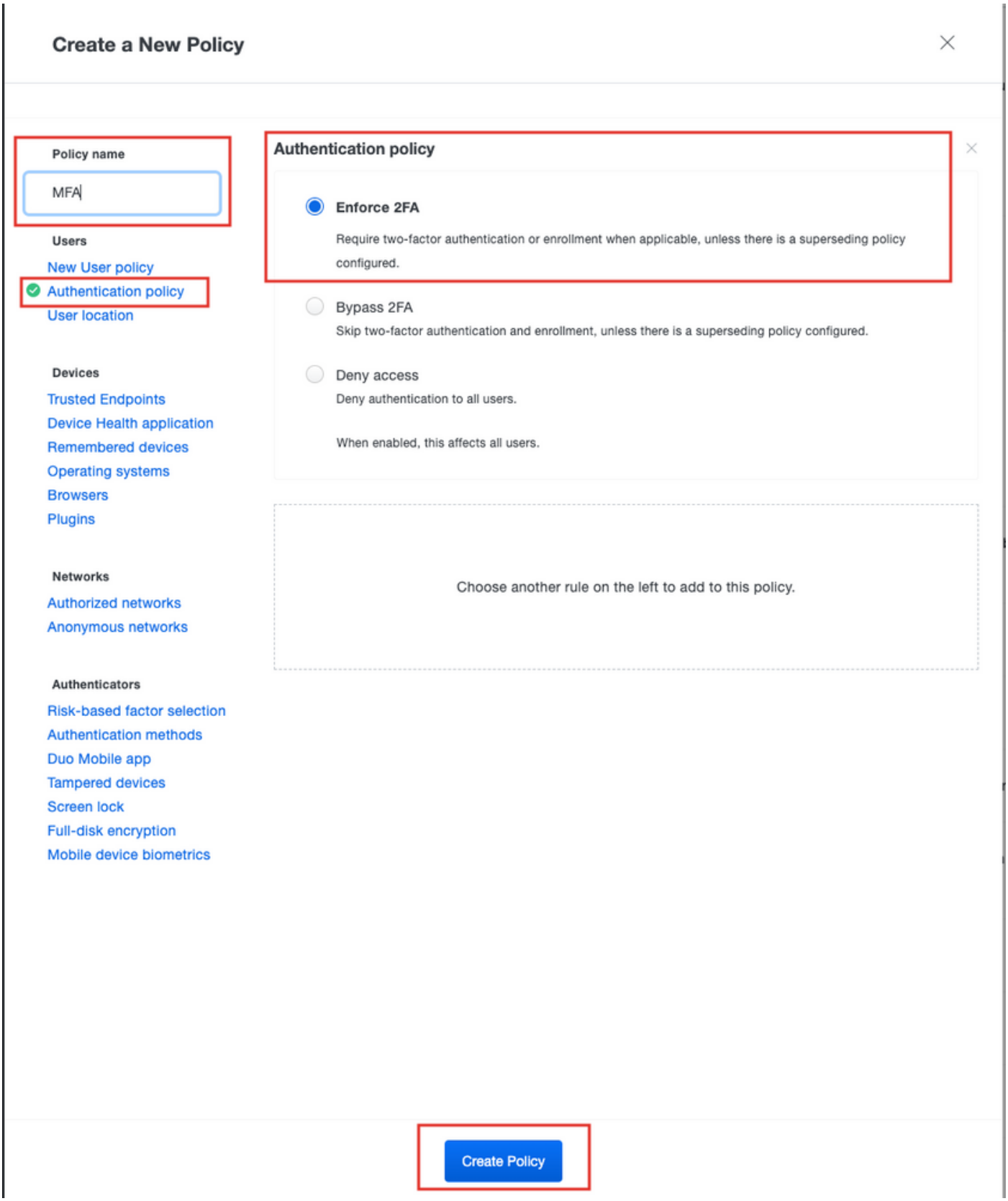


创建应用策略示例



创建应用策略示例

步骤2.在Policy name下，输入所需的名称，在Users下选择“Authentication policy”，然后选择“实施2FA。”然后使用“创建策略”进行保存。



创建应用策略示例

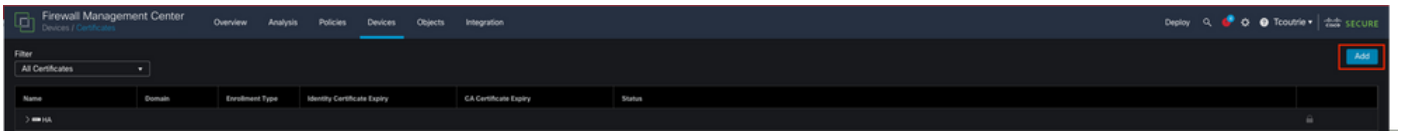
步骤3.在下一个窗口中使用“Apply Policy”应用策略。然后滚动到页面底部并选择“Save”完成DUO配置

FMC的配置步骤

将身份证书部署到FTD

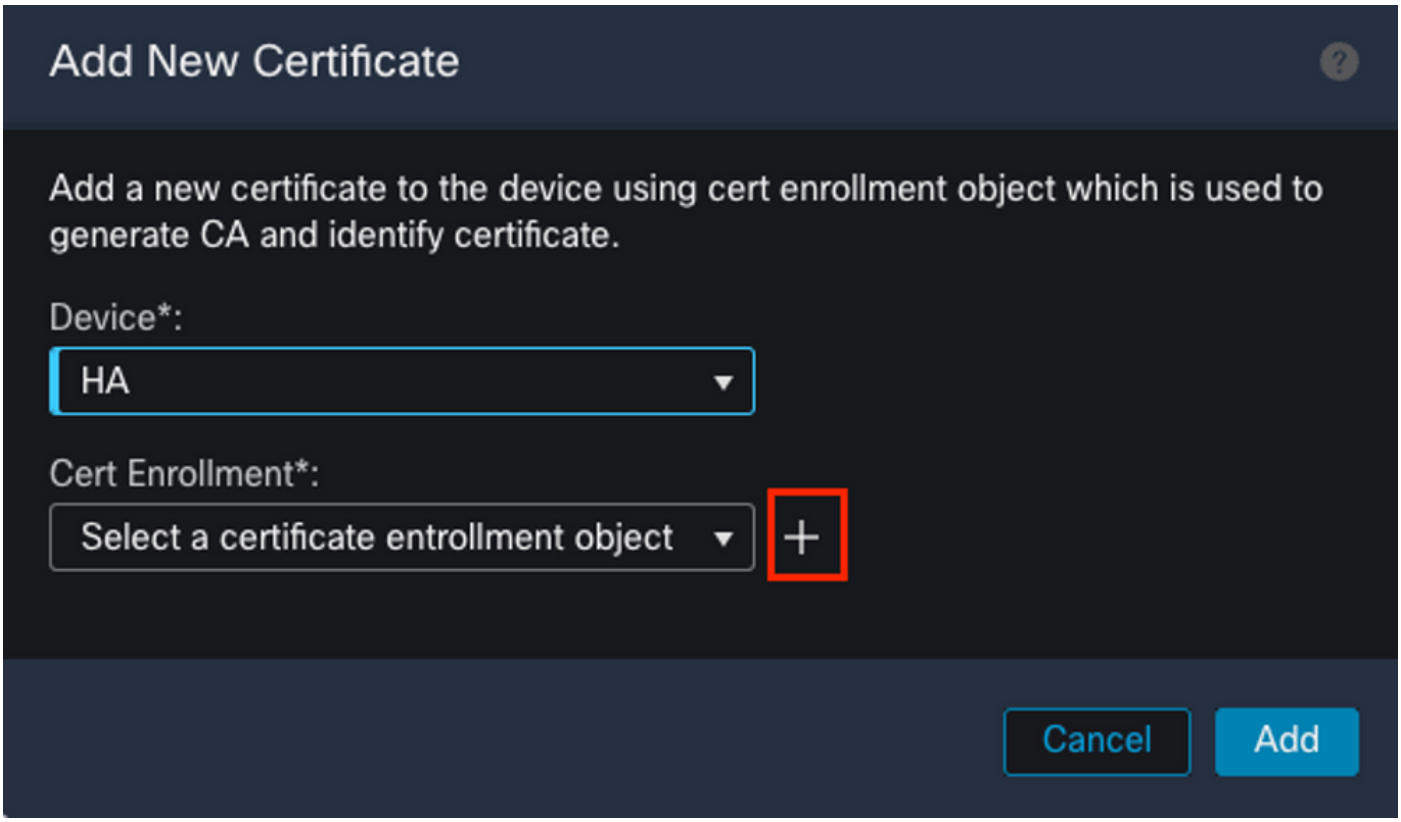
本节介绍如何配置身份证书并将其部署到FTD中所需的证书身份验证。开始之前，请确保部署所有配置。

第1步：导航到设备(Devices)>证书(Certificates)，然后选择添加(Add)，如图所示。



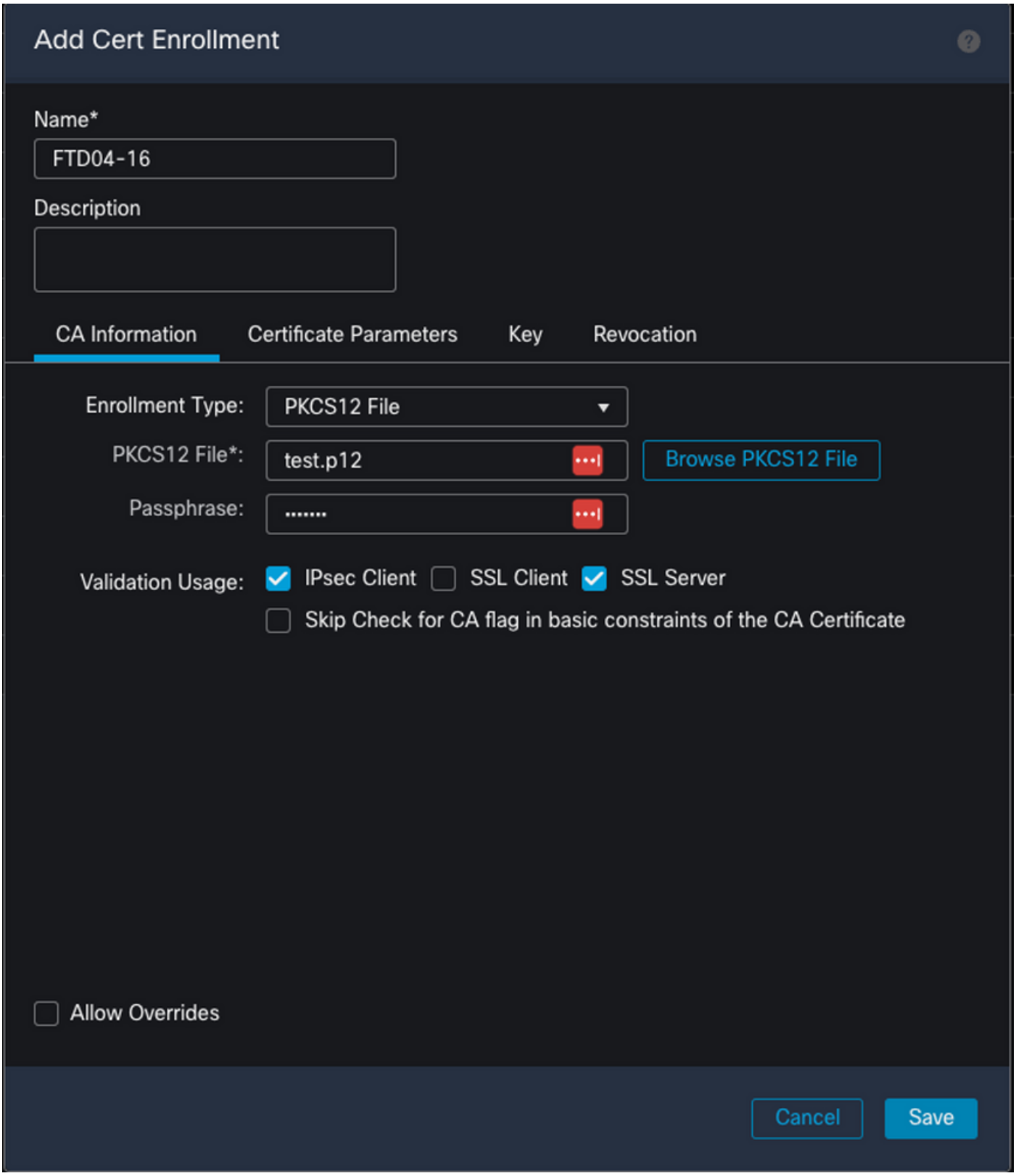
设备/证书的截图

步骤 2：从devices下拉列表中选择FTD设备。单击+图标可添加新的证书注册方法。



添加新证书的截图

第3步：选择通过“Enrollment Type”在环境中获取证书的首选方法，如图所示。



新证书注册页面的截图

提示：可用选项包括：自签名证书 — 本地生成新证书，SCEP — 使用简单证书注册协议从CA获取证书，手动 — 手动安装根和身份证书，PKCS12 — 上传带根、身份和私钥的加密证书捆绑包。

将IDP证书部署到FTD

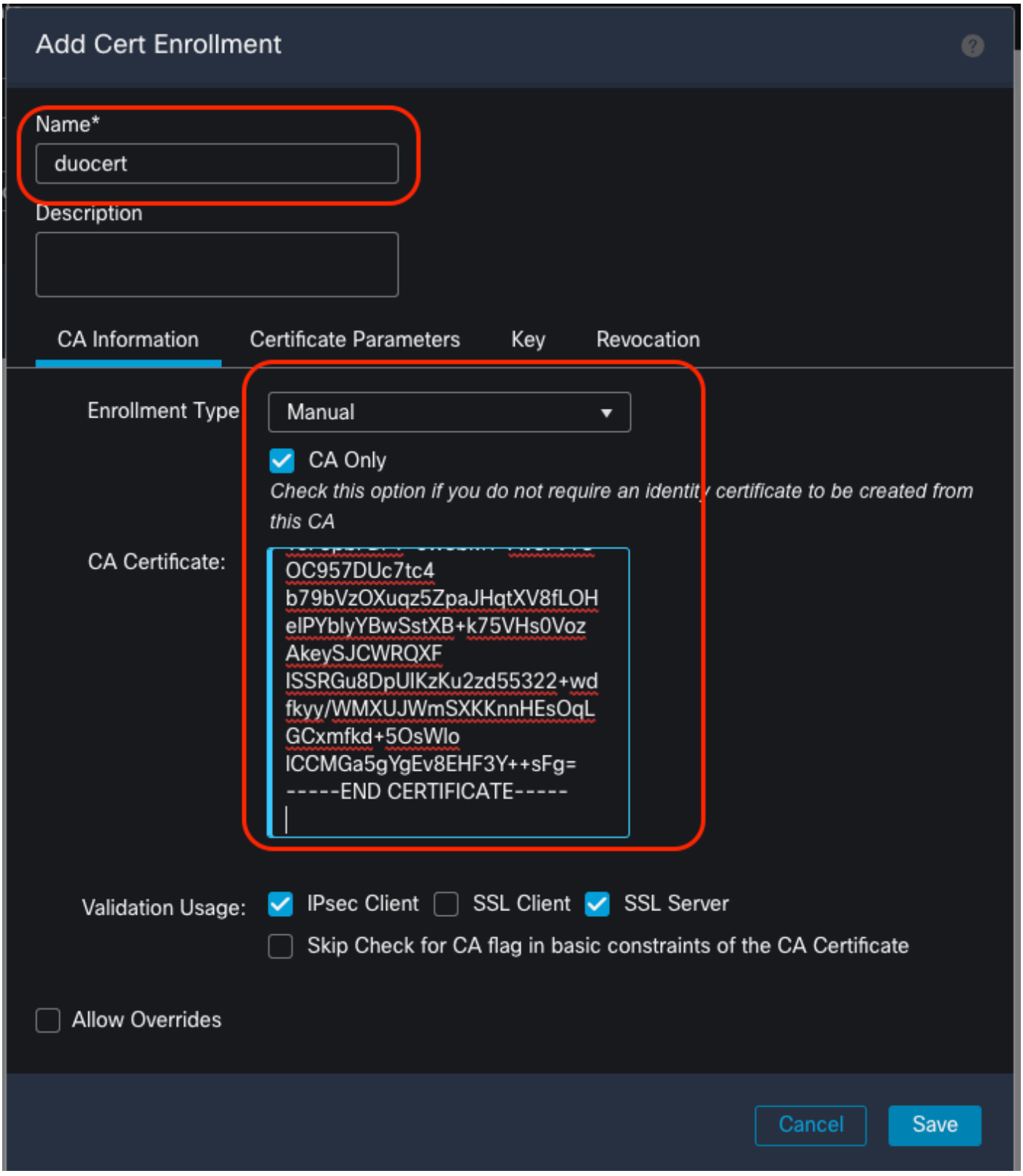
本节介绍如何配置并将IDP证书部署到FTD。开始之前，请确保部署所有配置。

步骤 1：导航到Devices > Certificate，然后选择Add。

步骤 2：从devices下拉列表中选择FTD设备。单击+图标可添加新的证书注册方法。

第3步：在“添加证书注册”窗口中，输入所需的信息（如图所示），然后“保存”（如图所示）。

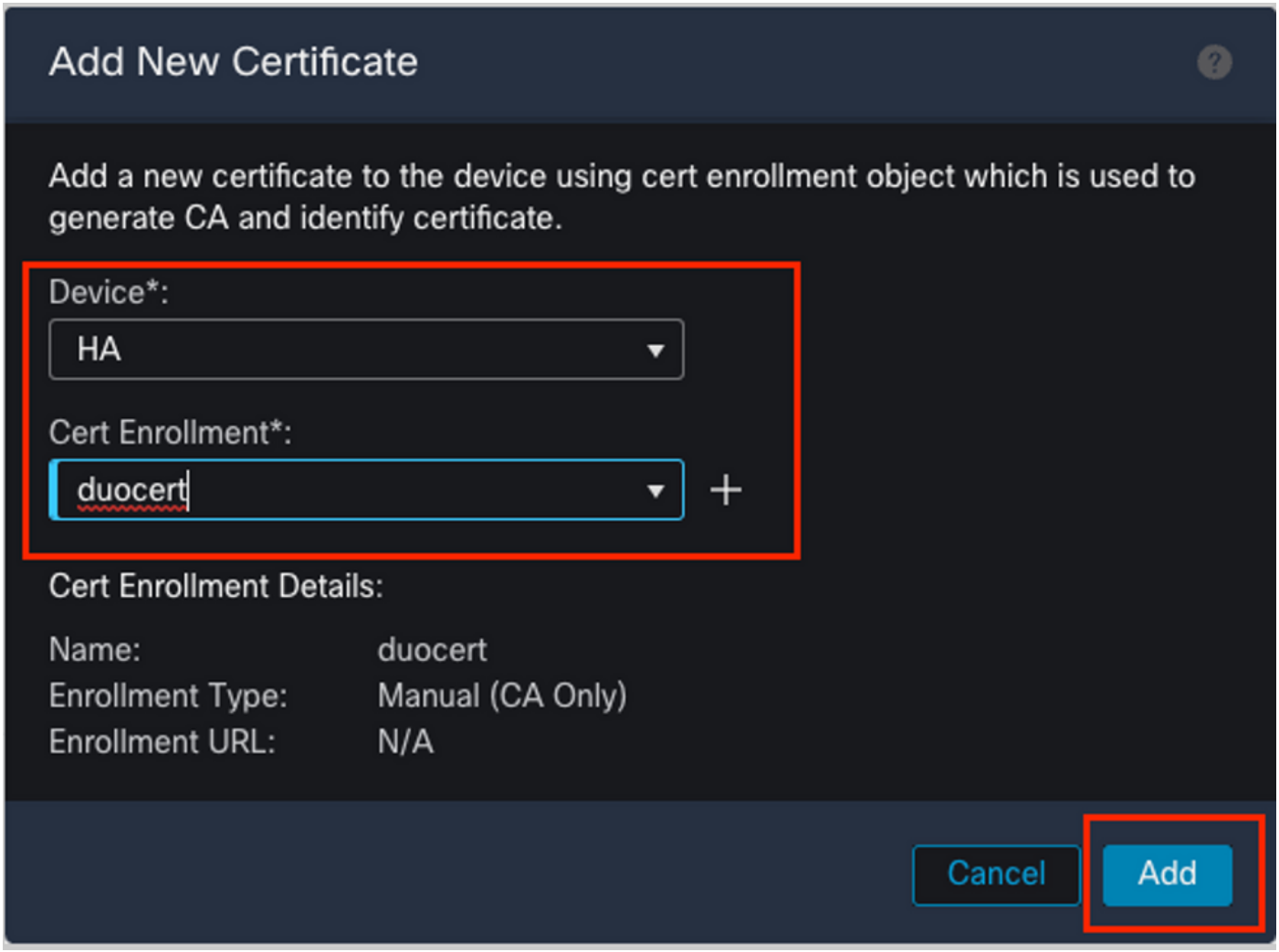
- 名称：对象的名称
- 注册类型:手动
- 复选框已启用:仅CA
- CA 证书:证书的PEM格式



创建证书注册对象的示例

⚠ 警告：如果需要，可以使用“CA证书基本限制中的CA跳过检查”标志。请谨慎使用此选项。

步骤 4：在“Cert Enrollment*：”下选择新创建的证书注册对象，然后选择“Add”，如图所示。



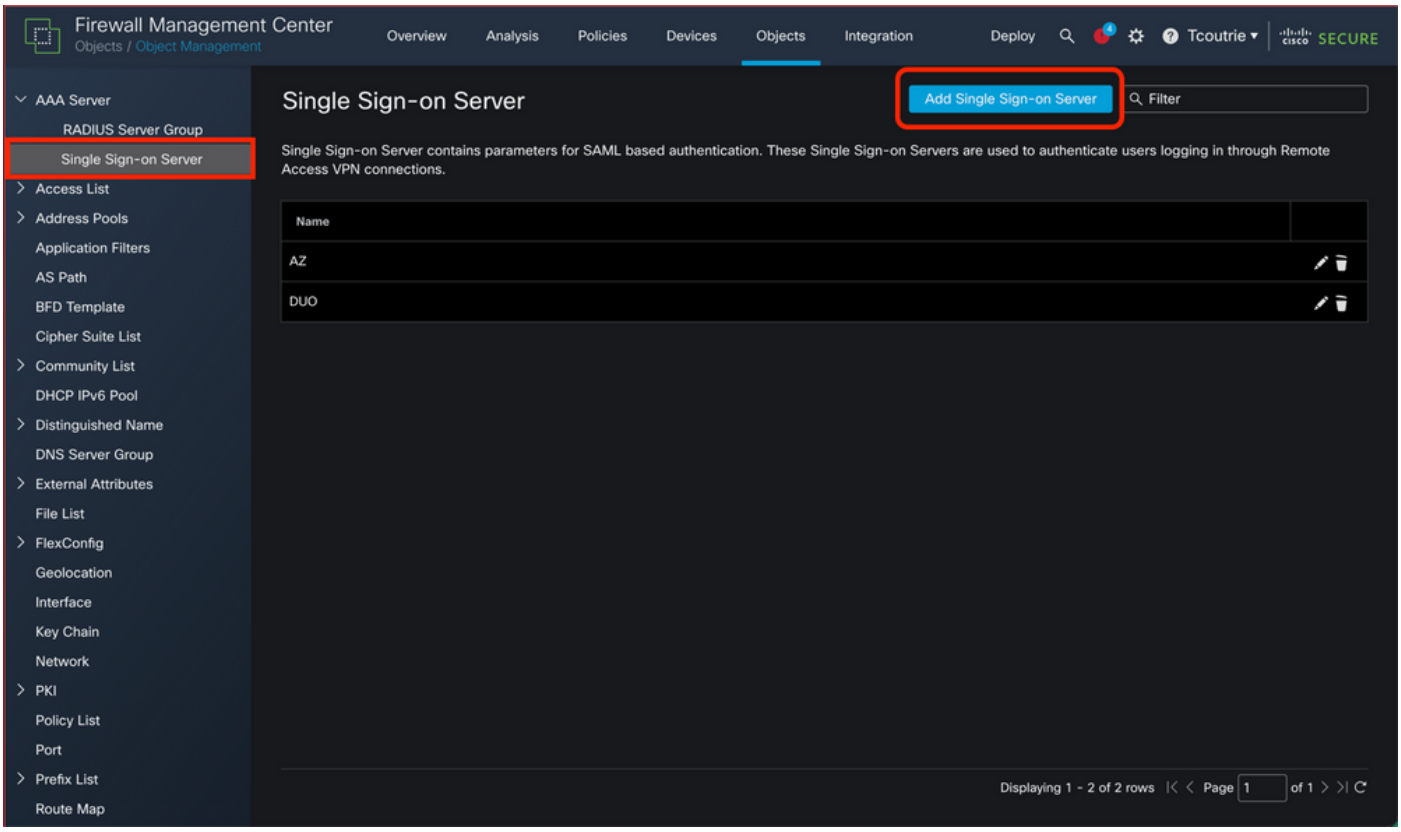
已添加的证书注册对象和设备的截图

注意：添加证书后，立即部署。

创建SAML SSO对象

本节介绍通过FMC配置SAML SSO的步骤。开始之前，请确保部署所有配置。

第1步：导航到对象(Objects)> AAA服务器(AAA Server)>单点登录服务器(Single Sign-on Server)，然后选择“添加单点登录服务器”(Add Single Sign-on Server)。

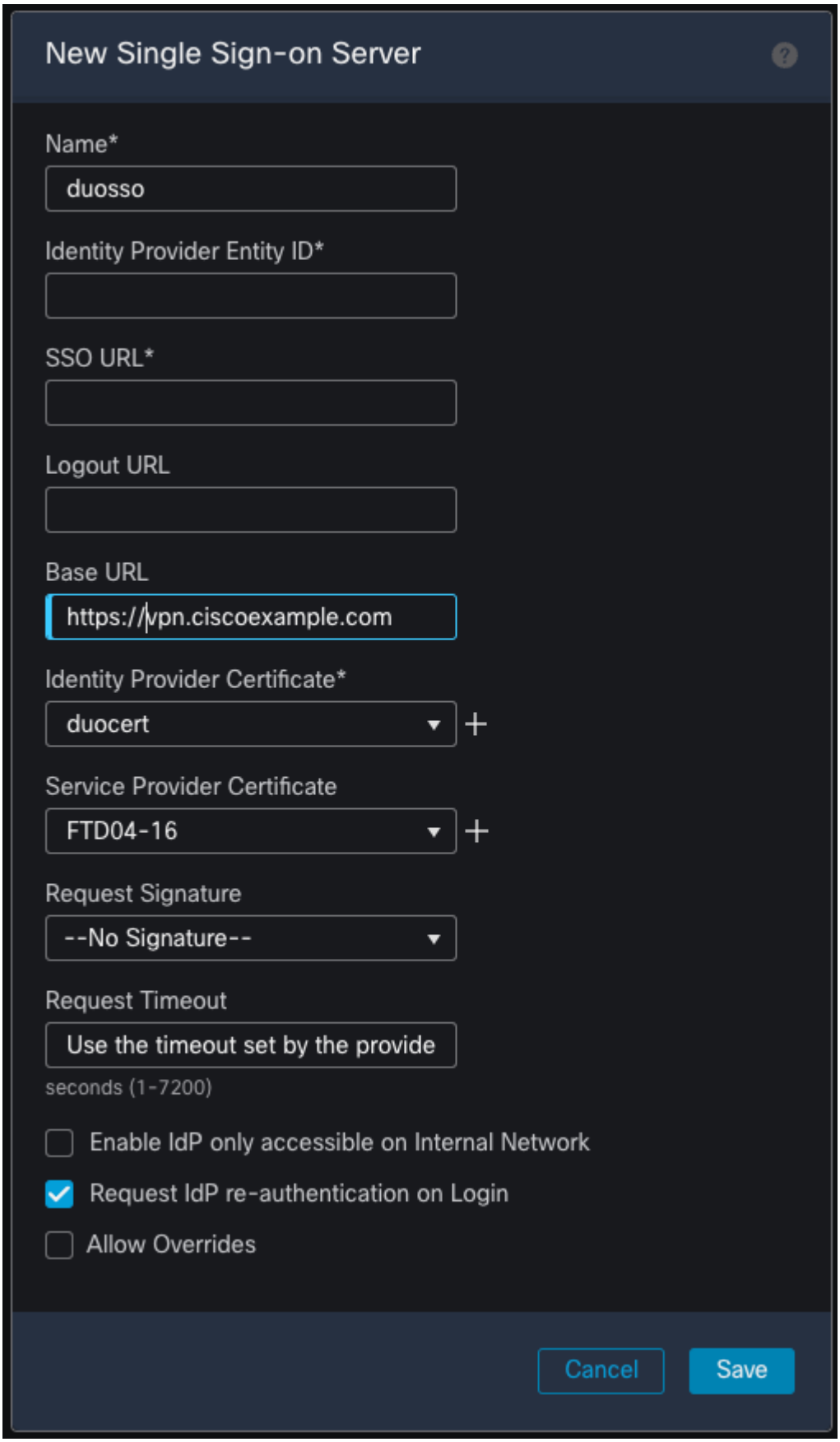


创建新SSO对象的示例

步骤2.从“创建应用保护策略”输入所需信息

". 要在完成之后继续，请选择“保存”。

- 姓名*:对象的名称
- 身份提供程序实体ID*:第3步中的实体ID
- SSO URL*:从步骤3复制的登录URL
- 注销URL:从步骤3复制的注销URL
- 基本URL:使用与步骤5中的“Cisco Firepower基础URL”相同的FQDN
- 身份提供程序证书*:已部署的IDP证书
- 服务提供商证书:FTD外部接口上的证书



新SSO对象的示例。

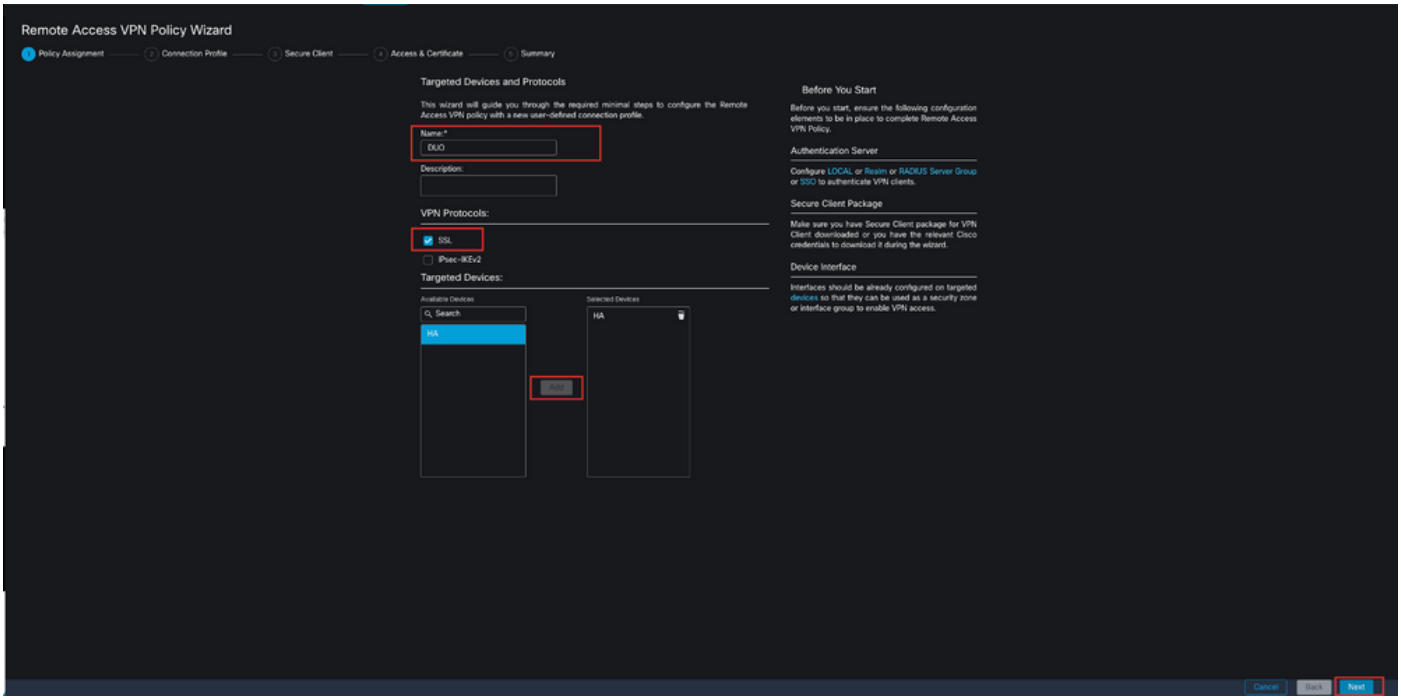
注意：屏幕截图中已省略了实体ID、SSO URL和注销URL链接

创建远程访问虚拟专用网络(RAVPN)配置

本节介绍使用向导配置RAVPN的步骤。

步骤1.导航到设备>远程访问，选择“添加”。

步骤2.在向导中，输入新RAVPN策略向导的名称，在VPN协议：添加目标设备下选择SSL，如图所示。完成后，选择“下一步”。



RAVPN向导的第1步

步骤2.对于连接配置文件，设置选项（如下所示）：完成后选择“下一步”。

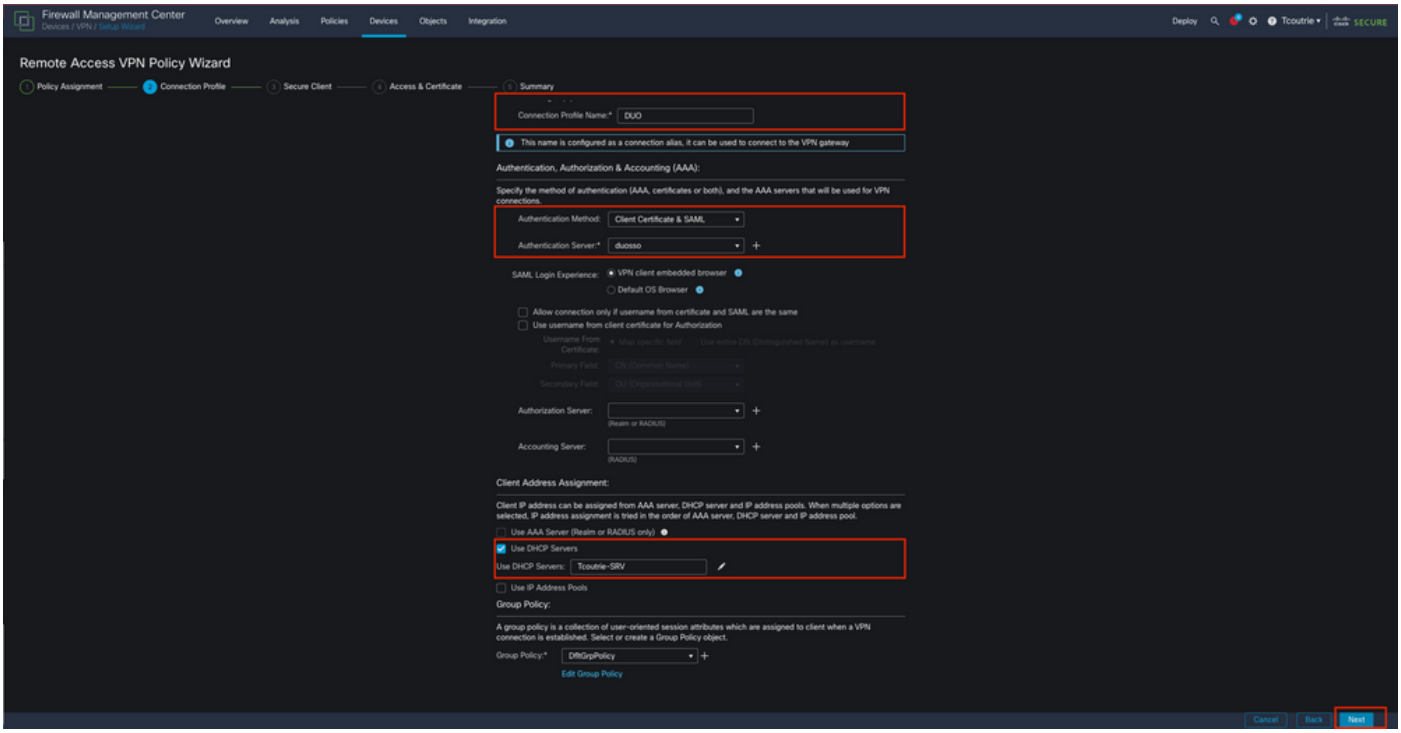
- 连接配置文件名称： 使用创建应用保护策略的第5步中的隧道组名称。

身份验证、授权和记帐(AAA):

- 认证方法: 客户端证书和SAML
- 身份验证服务器:*选择在“创建SAML SSO对象”期间创建的SSO对象。

客户端地址分配：

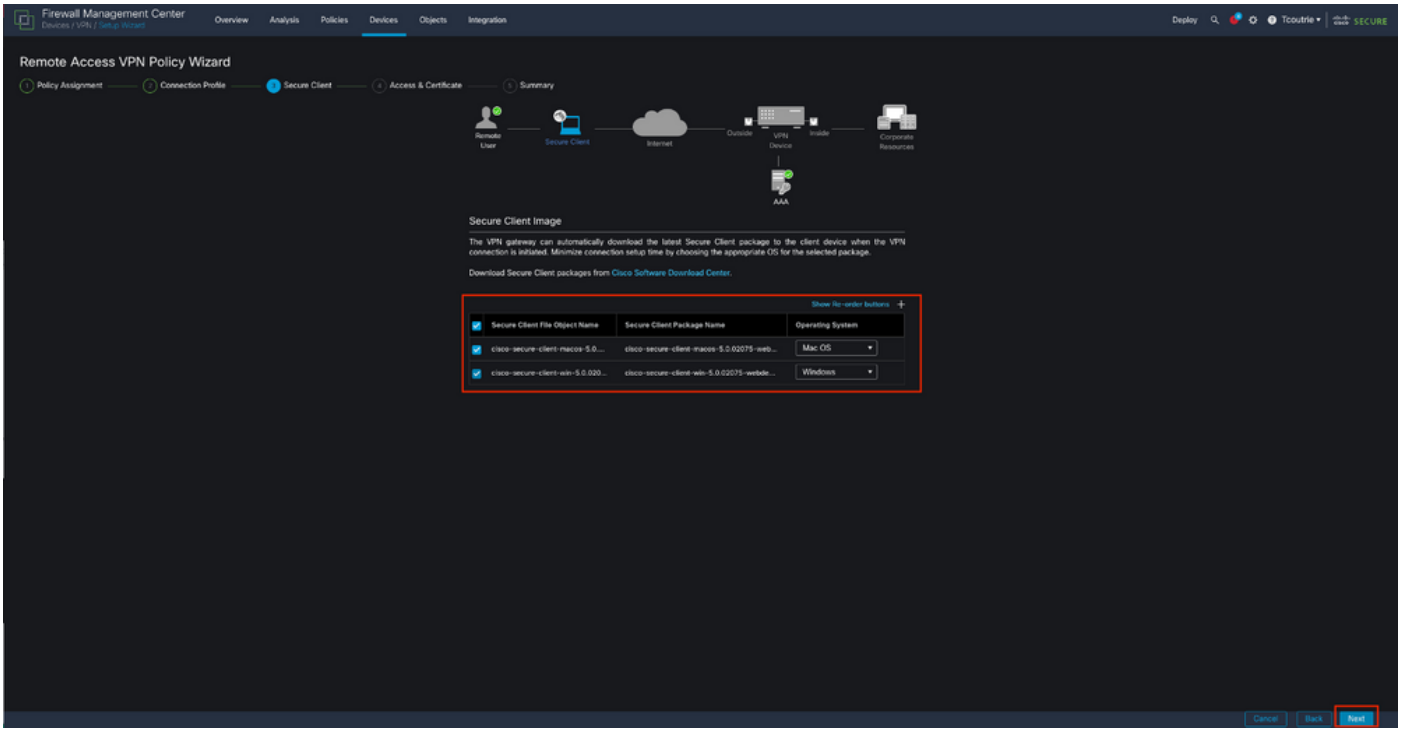
- 使用AAA服务器（仅限领域或RADIUS）— Radius或LDAP
- 使用DHCP服务器 — DHCP服务器
- 使用IP地址池- FTD上的本地池



RAVPN向导的第2步

提示：本实验使用DHCP服务器。

步骤3.选择“+”上传要部署的Cisco安全客户端的Web部署映像。然后选中要部署的CSC映像的复选框。如图所示.完成后选择“Next”。

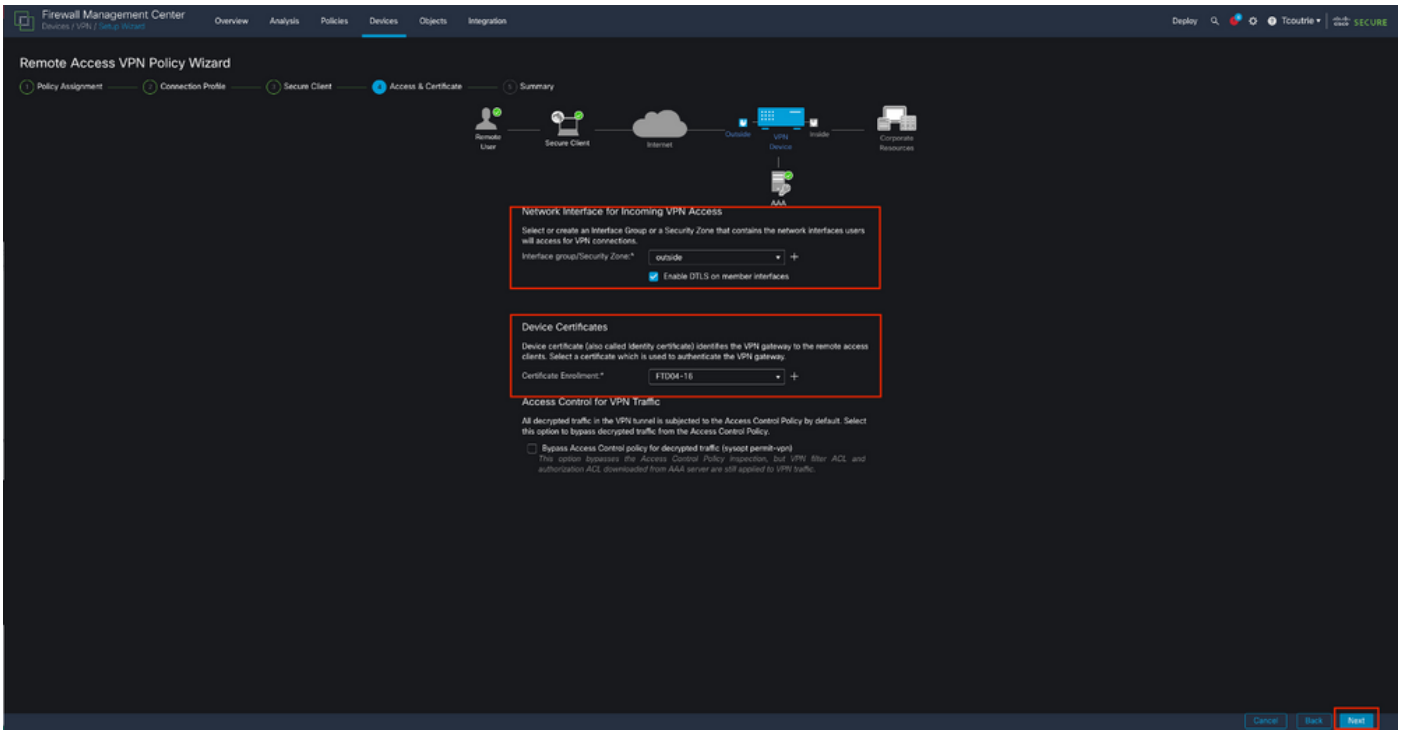


第3步RAVPN向导

步骤4.设置这些对象（如图所示）：完成后，选择“下一步”。

接口组/安全区域：*:外部接口

"证书注册：*":在本指南的“将身份证书部署到FTD”部分期间创建的身份证书

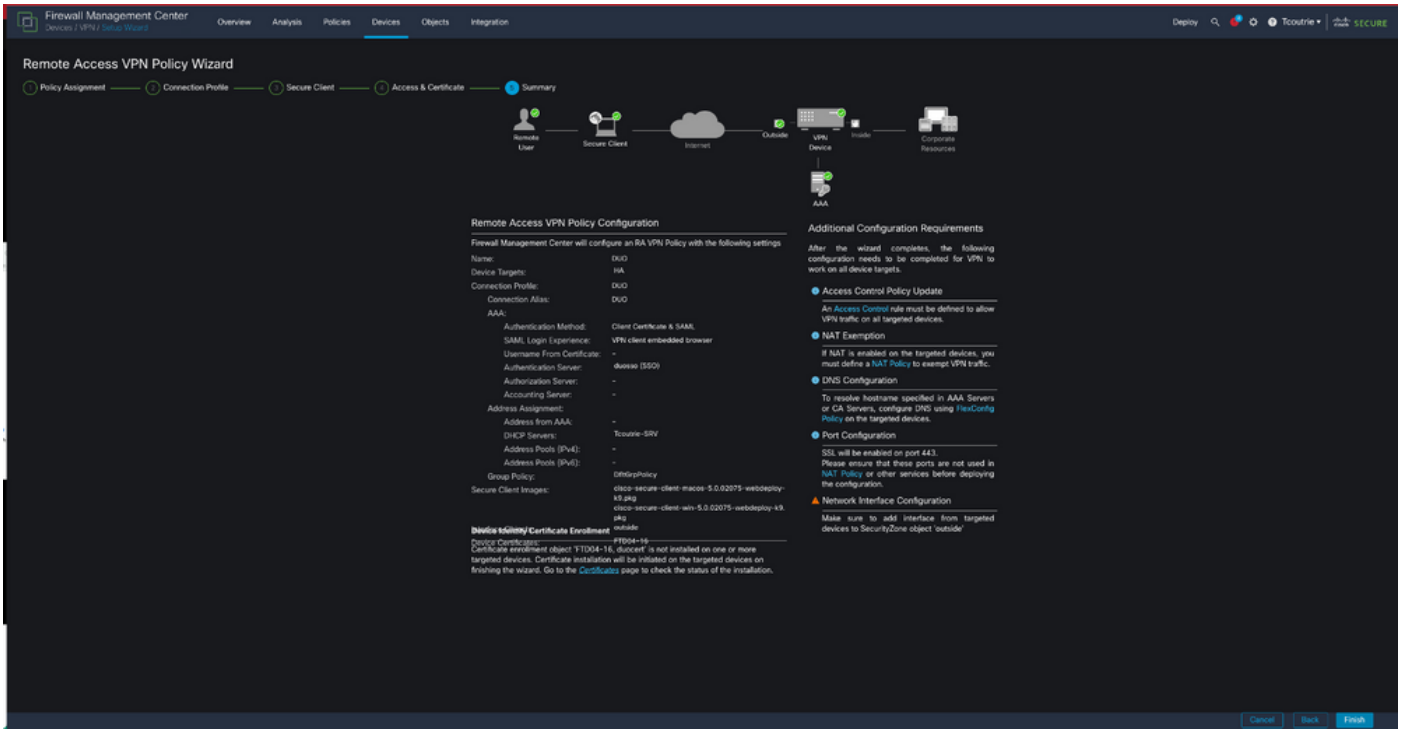


RAVPN向导的第4步

提示：如果尚未创建，请选择“+”添加新的证书注册对象。

步骤6.总结

检验所有信息。如果一切正确，请继续“完成”。



“摘要”页面

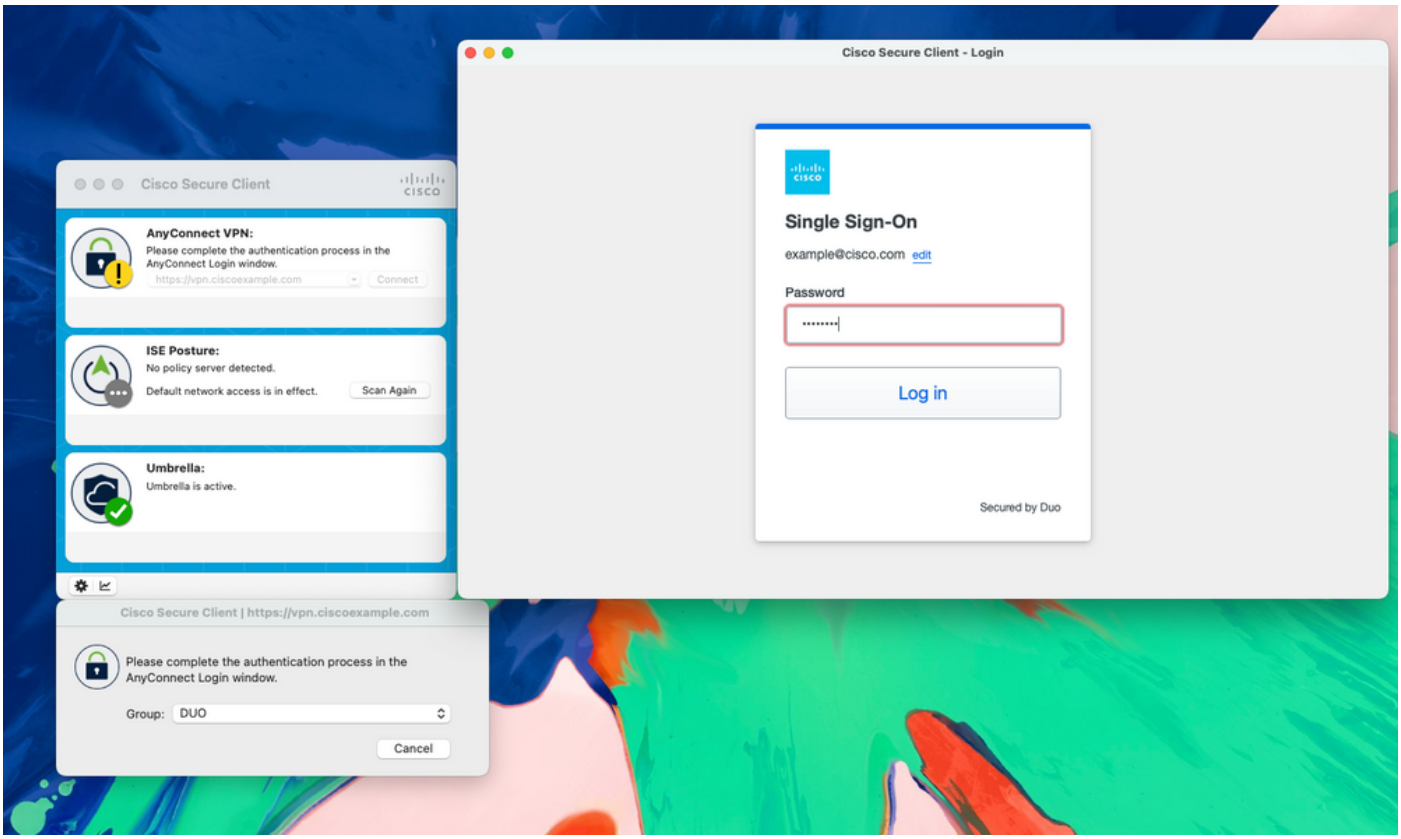
步骤7.部署新添加的配置。

验证

本节介绍如何验证连接尝试是否成功。

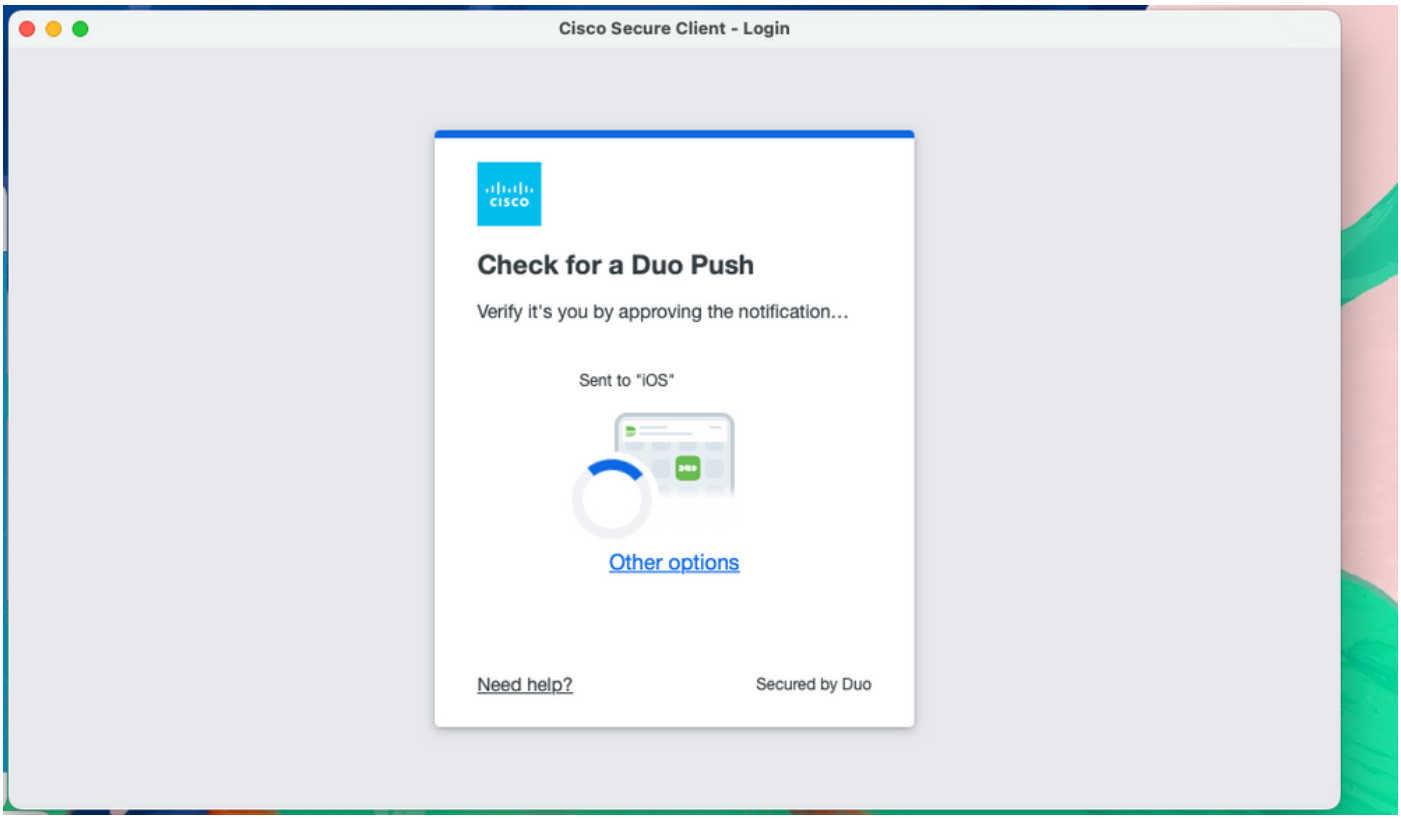
打开Cisco Secure Client并输入FTD的FQDN并连接。

在SSO页面上输入凭证。



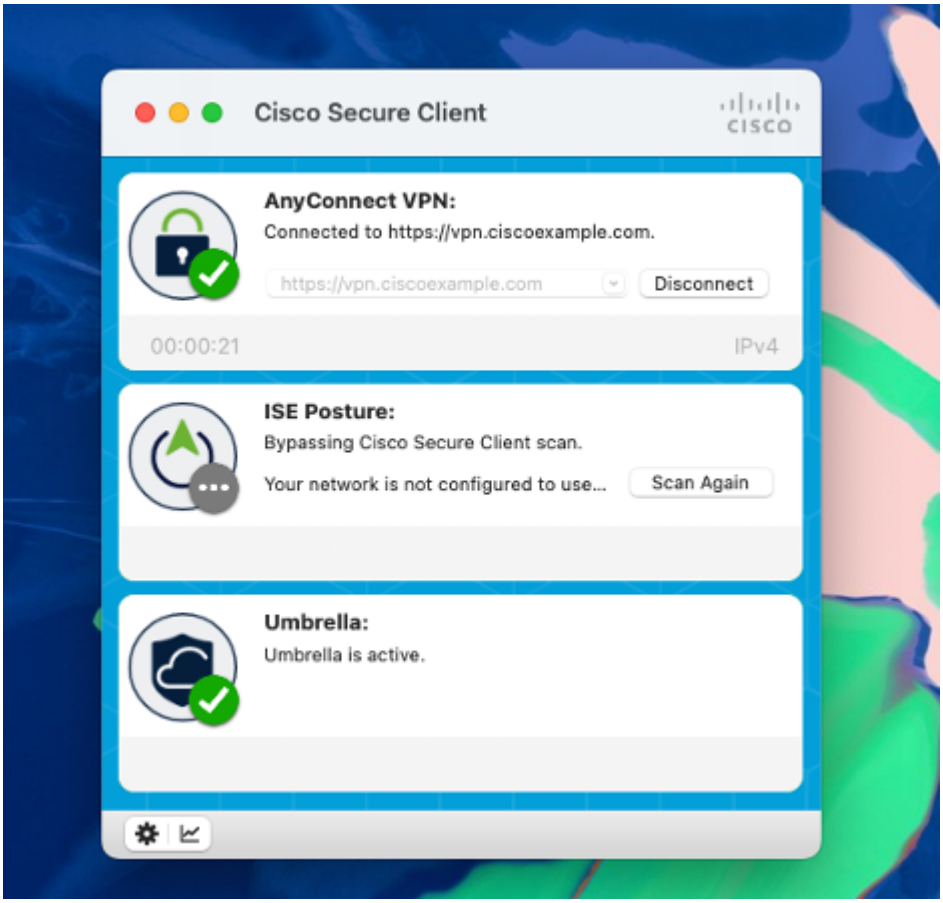
通过Cisco安全客户端的SSO页面

接受DUO推入注册设备。



DUO推送

连接成功。



已连接到FTD

使用以下命令验证FTD上的连接：show vpn-sessiondb detail anyconnect

```
tcoutrie-ftd2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     :                       Index        : 1916
Assigned IP  :                       Public IP    :
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-128  DTLS-Tunnel:
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SH
Bytes Tx     : 390964                Bytes Rx     : 124114
Pkts Tx      : 1216                  Pkts Rx      : 1223
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy :                       Tunnel Group :
Login Time   : 23:54:41 UTC Tue Jul 18 2023
Duration     : 0h:11m:28s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                   VLAN         : none
Audt Sess ID : 0a7aa95d0077c00064b72641
Security Grp : none                  Tunnel Zone  : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
  Tunnel ID    : 1916.1
  Public IP    :
  Encryption   : none                  Hashing      : none
  TCP Src Port : 53859                 TCP Dst Port : 443
  Auth Mode    : Certificate and SAML
  Idle Time Out: 30 Minutes            Idle TO Left : 18 Minutes
  Client OS    : mac-intel
```

输出示例中省略了一些信息

故障排除

这些是在实施后可能出现的问题。

问题 1:证书身份验证失败。

确保根证书安装在FTD上；

使用以下调试：

debug crypto ca 14

debug aaa shim 128

debug aaa common 128

问题 2:SAML故障

可以启用这些调试以进行故障排除：

debug aaa shim 128

debug aaa common 128

debug webvpn anyconnect 128

debug webvpn saml 255

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）。