在SCC上使用内部托管FMC配置通用ZTNA的安全访问

目录

简介

先决条件

- 要求
- 使用的组件
- 网络图

后台信息

- 支持的设备
- 限制

配置

- 检查FMC版本
- 检查FTD版本
- 验证FTD许可证
- 检查平台设置和DNS配置是否正确
- 在CDO上创建安全云控制租户
- 确保配置了SCC防火墙常规设置
- 验证您的安全访问租户和安全控制防火墙管理基础集成
- 生成防火墙威胁防御(FTD)CA签名证书
- 内置防火墙管理中心到安全云控制
- 在FTD上注册通用零信任网络访问(uZTNA)设置
- 使用uZTNA注册客户端
  - 安全访问配置
  - 客户端配置

验证

相关信息

简介

本文档介绍如何使用安全访问和由内部虚拟FMC管理的虚拟FTD配置通用ZTNA。

先决条件

- 需要使用7.7.10或更高软件版本部署防火墙管理中心(FMC)和防火墙威胁防御(FTD)。
- 防火墙威胁防御(FTD)必须由防火墙管理中心(FMC)管理
- 防火墙威胁防御(FTD)必须使用加密（强加密必须启用导出功能）、安全控制所需的IPS和威胁许可证进行许可
- 防火墙威胁防御(FTD)的基本配置必须从防火墙管理中心(FMC)执行，例如接口、路由等。

- 需要从FMC在设备上应用DNS配置才能解析应用的FQDN
- Cisco安全客户端版本必须为5.1.10或更高版本
- 安全云控制调配给已启用防火墙和安全访问微应用和UZTNA功能标志的客户

要求

- 所有安全防火墙管理中心(FMC)(包括cdFMC和防火墙威胁防御(FTD)设备)都必须运行软件版本7.7.10或更高版本。
- 防火墙威胁防御(FTD)必须由防火墙管理中心管理；不支持本地管理器防火墙防御管理器(FDM)
- 所有防火墙威胁防御(FTD)设备必须配置为路由模式；不支持透明模式。
- 不支持集群设备。
- 支持高可用性(HA)设备；它们显示为一个实体。
- 安全客户端5.1.10版或更高版本

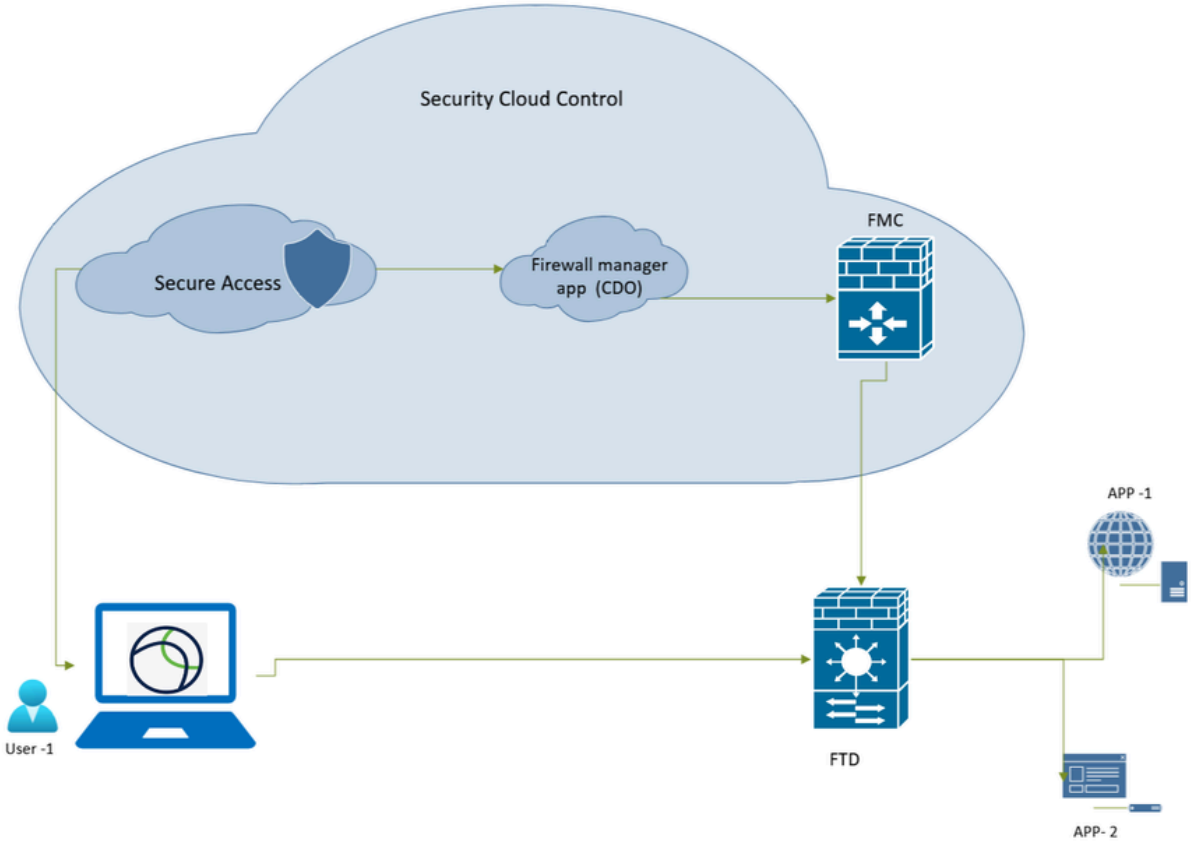
使用的组件

本文档中的信息基于

- 安全云控制(SCC)
- 安全防火墙管理中心(FMC)版本7.7.10
- 安全防火墙威胁防御(FTD)虚拟 — 100版本7.7.10
- 用于Windows的安全客户端5.1.10版
- 安全访问

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。

网络图



安全访问 — 网络拓扑

后台信息

支持的设备

支持的安全防火墙威胁防御模式：

- FPR 1150
- 3105、310、3120、3130、3140法郎
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- 虚拟防火墙威胁防御(FTD)，最少16个CPU核心

限制

- 对象共享
- 不支持IPv6。
- 仅支持全局VRF。
- 通用的ZTNA策略不会在到设备的站点到站点隧道流量上实施。
- 不支持集群设备。
- 不支持在4K和9K firepower系列上部署为容器的FTD

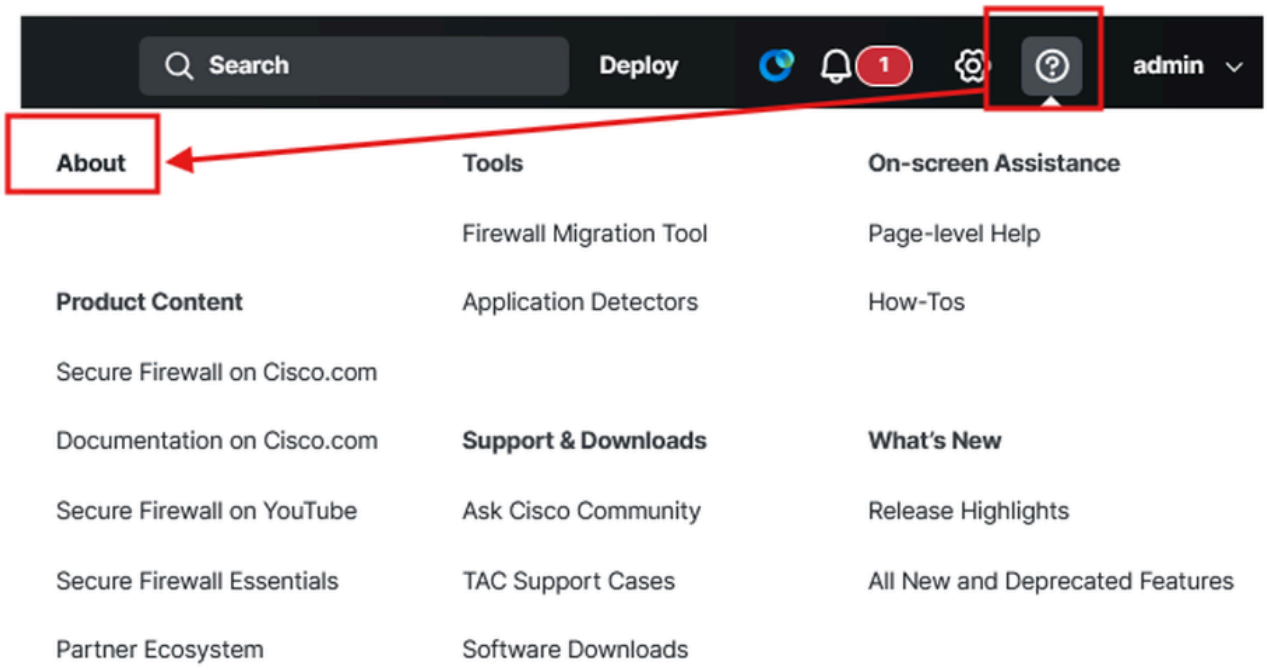
- 通用ZTNA会话不支持巨型帧

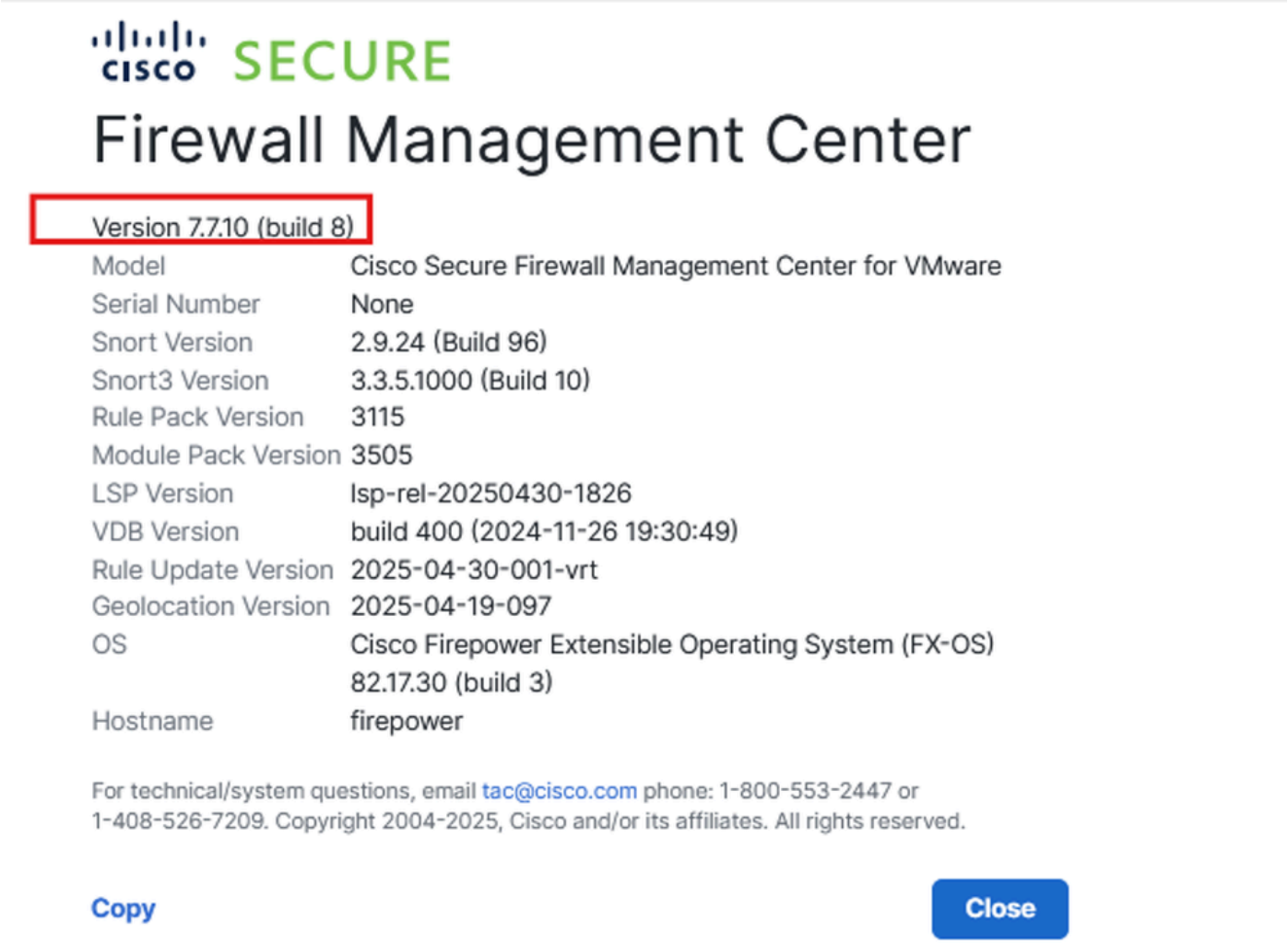
配置

检查FMC版本

验证在通用ZTNA（可以是7.7.10或更高版本）的受支持软件版本上运行的防火墙管理中心和防火墙FTD:

- 点击?（右上角），然后点击 About



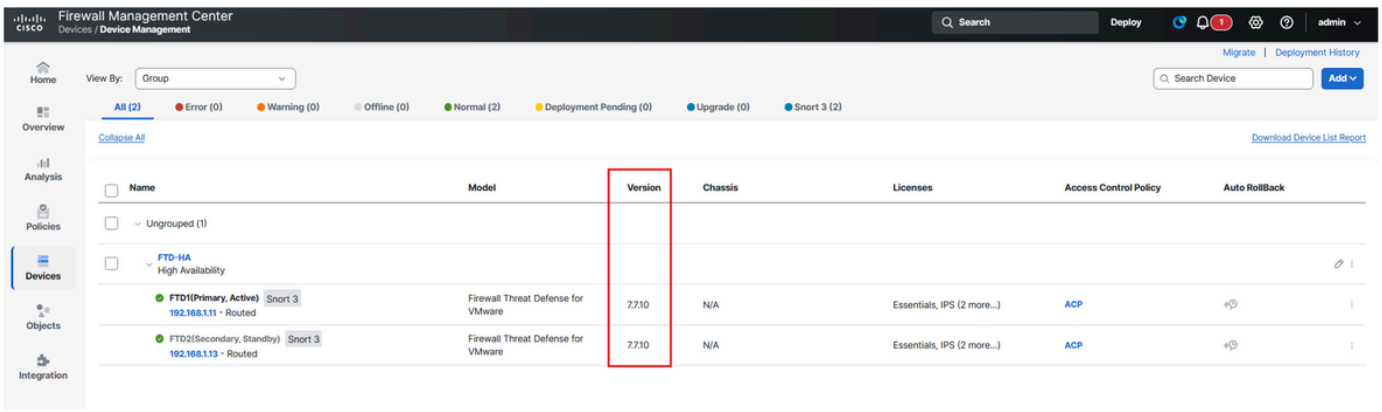


安全防火墙管理中心 — 软件版本

检查FTD版本

导航至FMC UI:

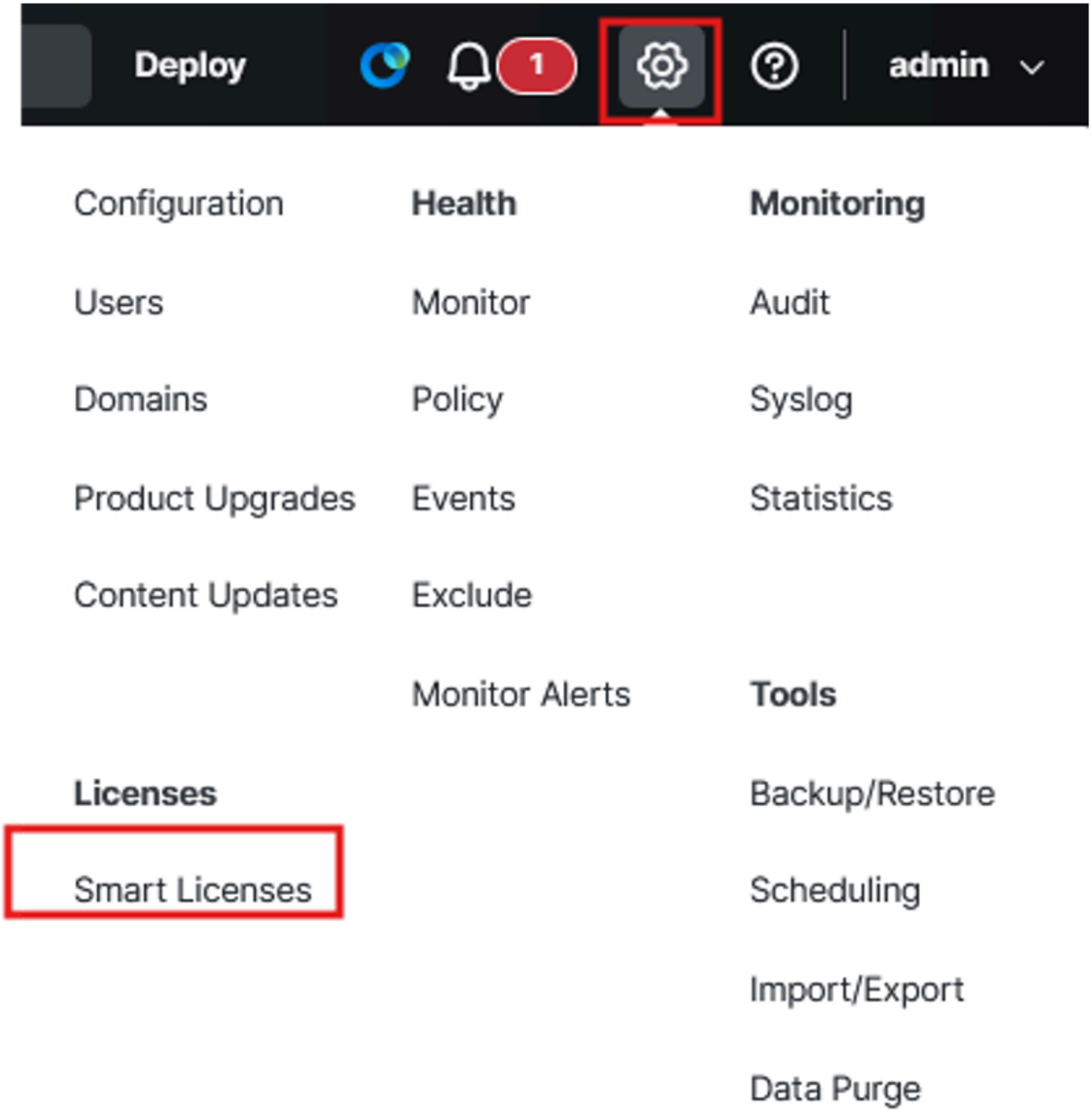
- 点击Devices> Device Management

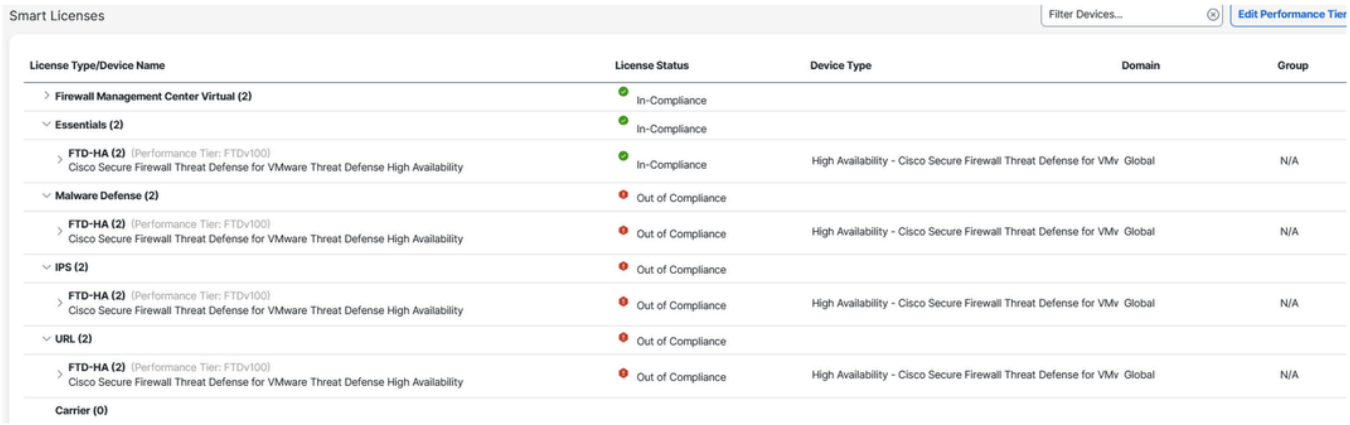


安全防火墙威胁防御 — 软件版本

验证FTD许可证

- 单击Setting Icon> Licenses > Smart Licenses





安全防火墙威胁防御 — 智能许可证

检查平台设置和DNS配置是否正确

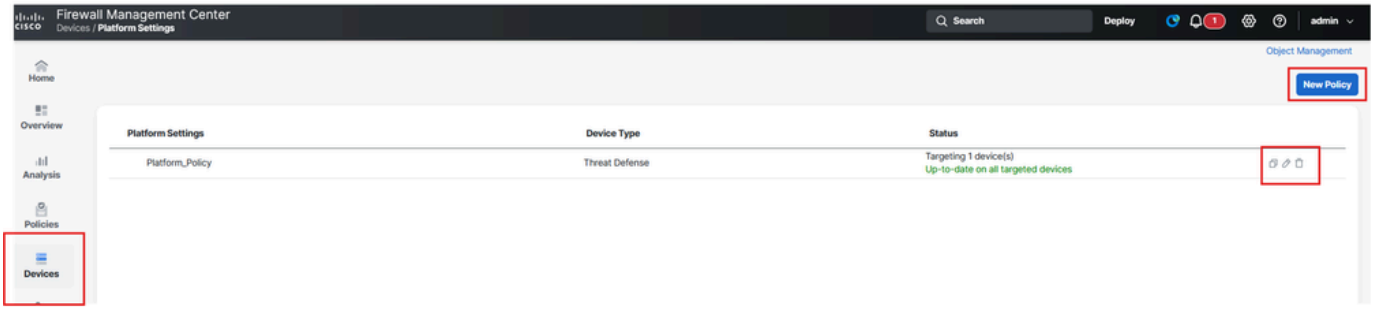
通过CLI登录到FTD:

- 运行命令以验证是否配置了DNS:

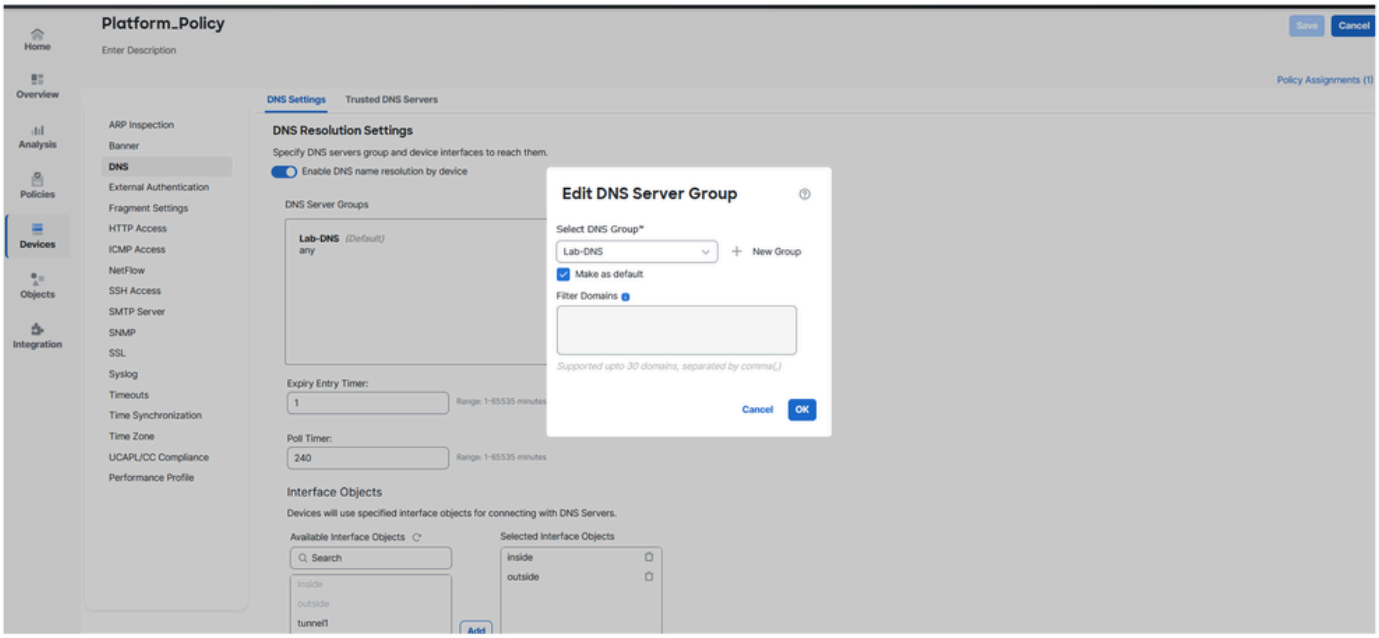
```
show run dns
```

在FMC中：

- 点击DevicesPlatform Settings > ，编辑或创建新策略



安全防火墙威胁防御 — 平台策略



安全防火墙威胁防御 — DNS配置

通过FTD cli验证您可以ping私有资源IP地址和FQDN（如果要使用其FQDN访问PR）。

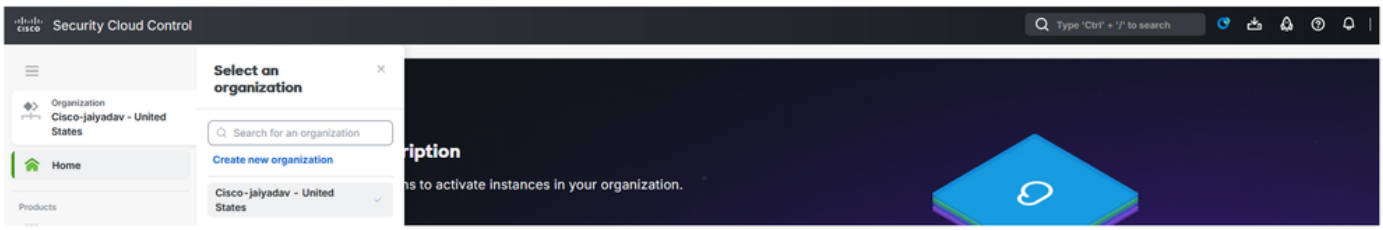
```
dns-group Lab-DNS
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

在CDO上创建安全云控制租户

注意：如果已配置SCC租户，则不必创建新租户。

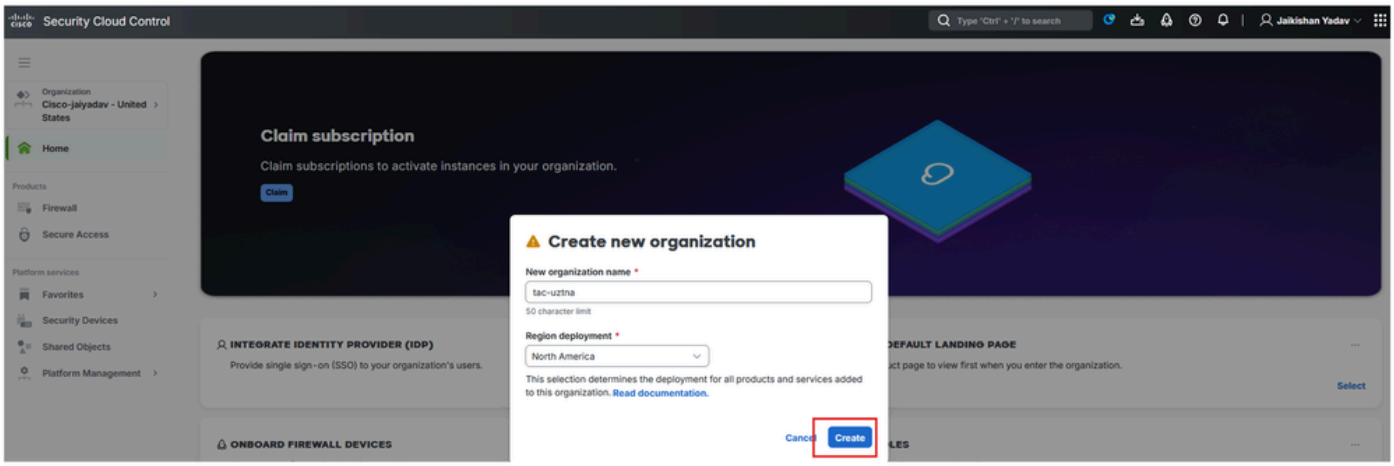
导航到[安全云控制：]

- 点击Organization> Create new organization



安全云控制 — 组织

- 点击 Create



安全云控制 — 组织创建

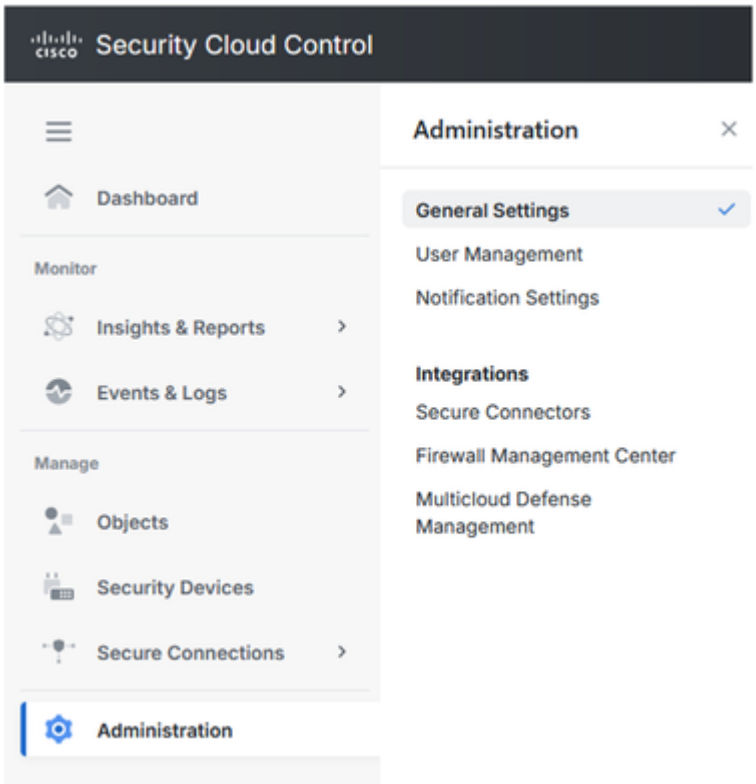
创建SCC租户后，收集租户信息以启用防火墙和安全访问微应用以及启用uZTNA。

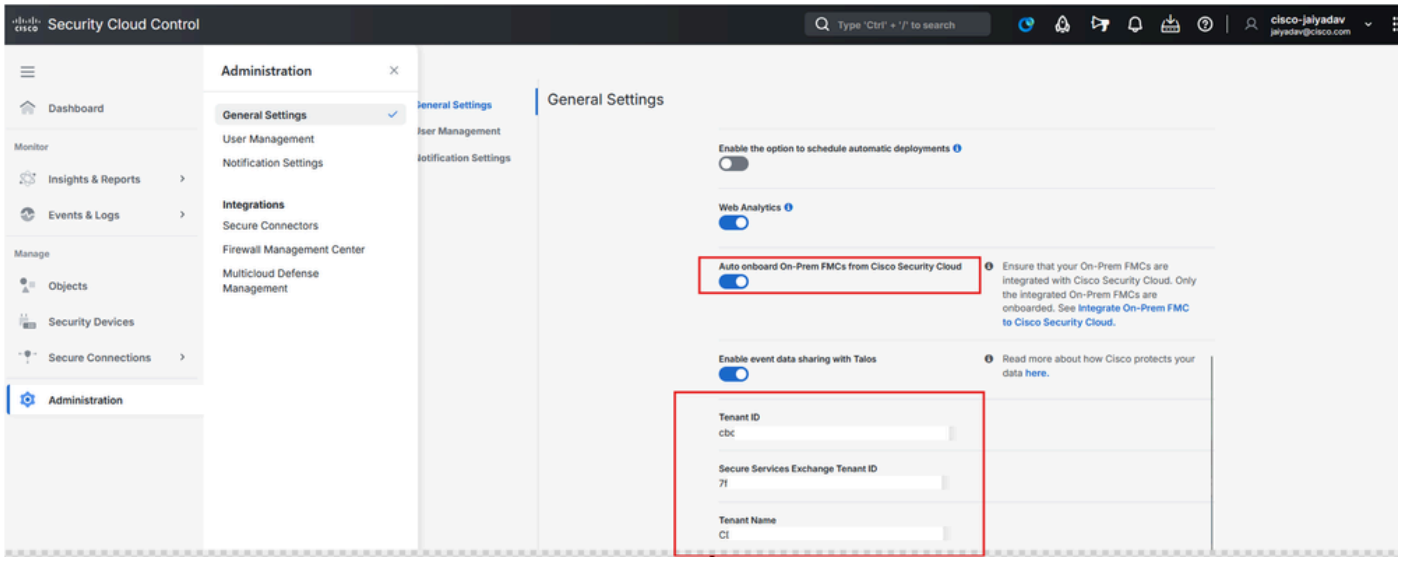
确保配置了SCC防火墙常规设置

导航到CDO/SCC:

- 点击Administration> General Settings
- 确保选项Auto onboard On-Prem FMCs from Cisco Security Cloud“已启用”。

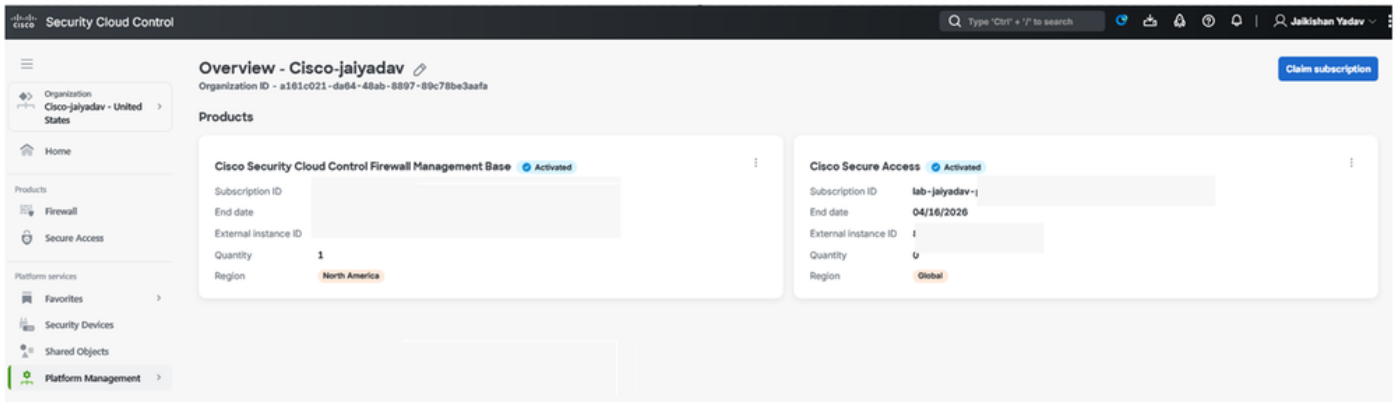
注意：Secure Access 尝试访问Secure Access MicroApp的用户必须具有和管Security Cloud Control理角色。





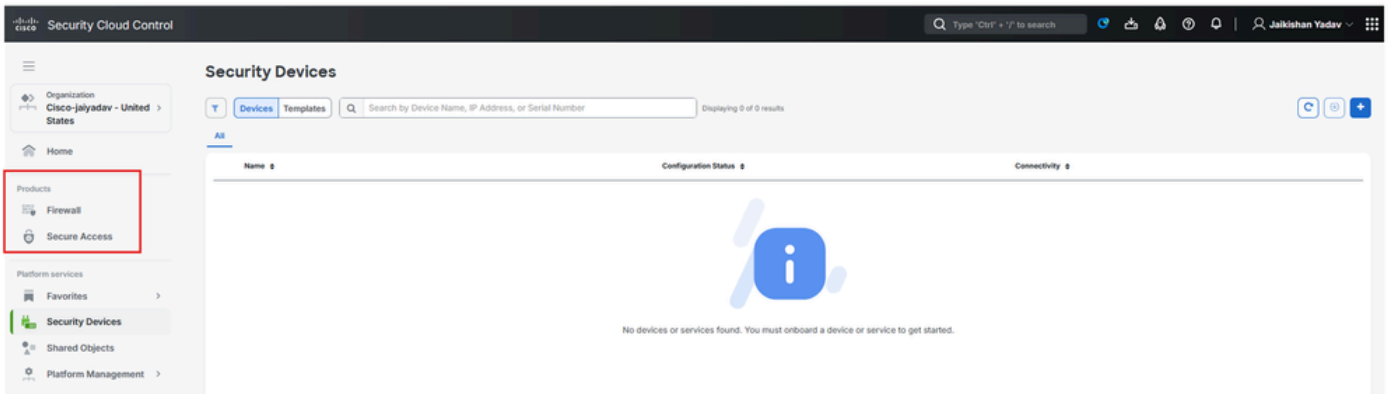
安全云控制 — 组织详细信息

验证您的安全访问租户和安全控制防火墙管理基础集成



安全云控制 — 安全访问激活

完成在CDO上创建安全云控制租户和在CDO上创建安全云控制租户的步骤后，您可以在SCC控制面板上查看防火墙和安全访问微应用：



安全云控制 — 微应用

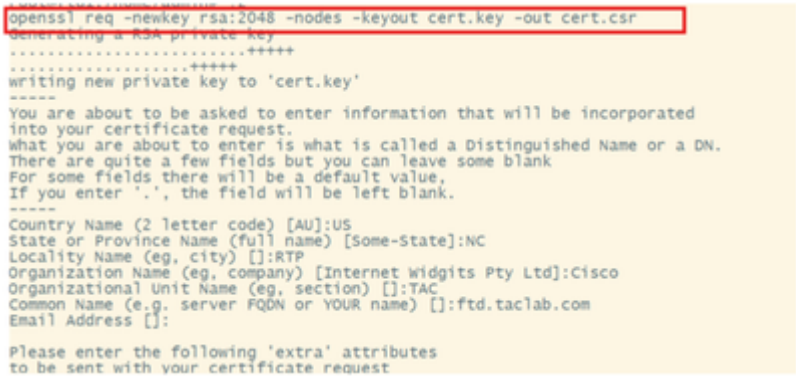
生成防火墙威胁防御(FTD)CA签名证书

注意：您还可以使用FTD自签名证书FTD证书（请参阅生成自签名内部和内部CA证书部分）。 证书必须采用PKCS12格式，并且必须存在于受信任根CA下的用户计算机存储中。

要在build openssl功能中使用FTD生成CA签名证书，请执行以下操作：

- 导航至FTD
- 运行命expert令
- 使用openssl生成CSR和密钥
  - OpenSSL命令：

```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
```



证书签名请求

- 复制CSR并获取CA签名证书
- 使用FTD CA签名证书和密钥并将证书转换为PKCS12格式
  - OpenSSL命令：

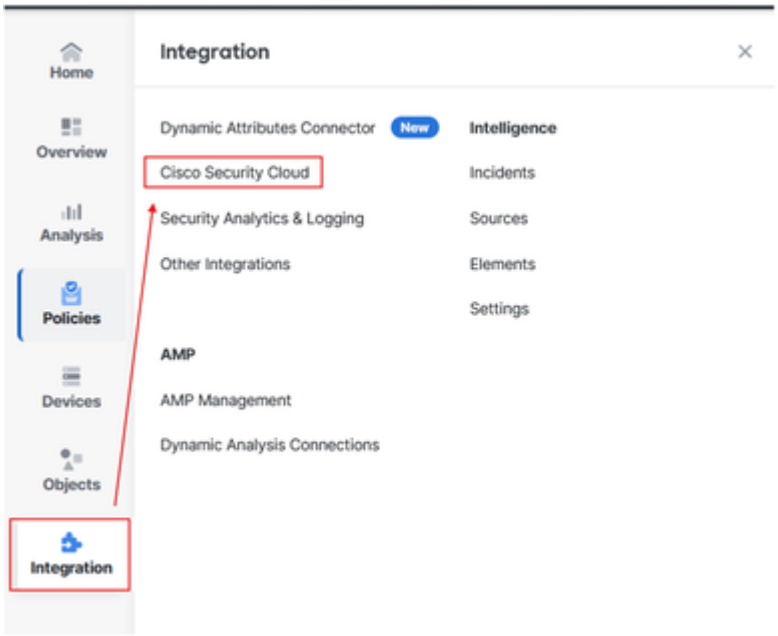
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- 使用SCP或其他工具导出证书。

内置防火墙管理中心到安全云控制

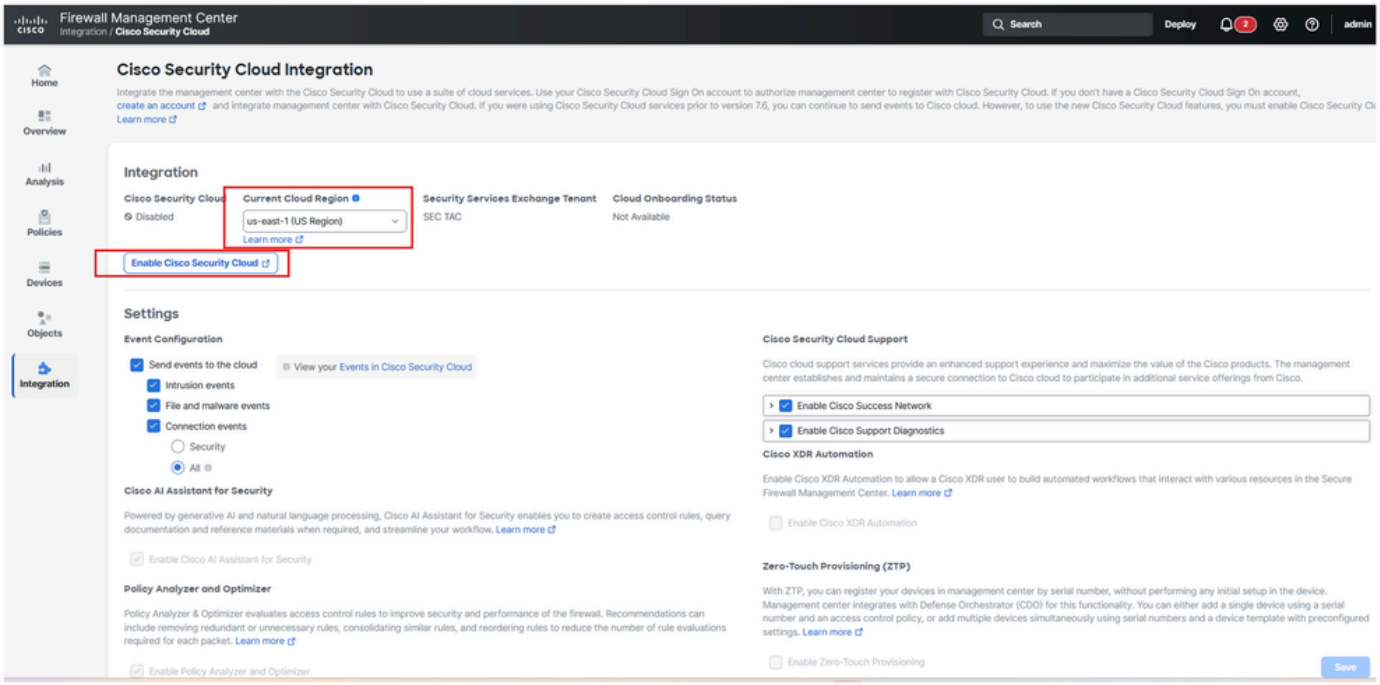
导航至FMC:

- 点击Integration> Cisco Security Cloud



防火墙管理中心与SCC集成

- 选择云区域，然后点击 Enable Cisco Security Cloud

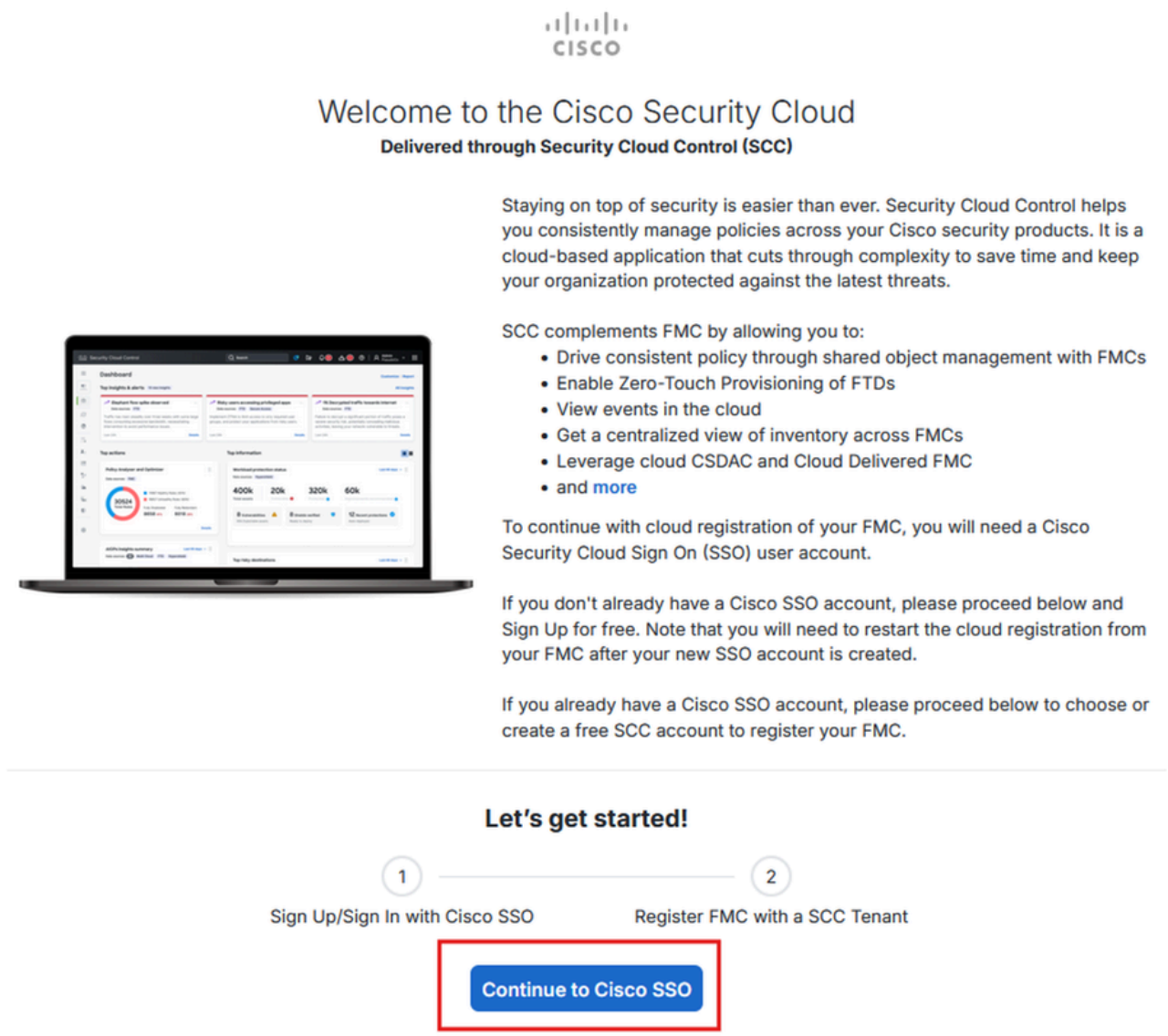


防火墙管理中心自注册到SCC

它将在新选项卡上打开一个新的浏览器选项卡：

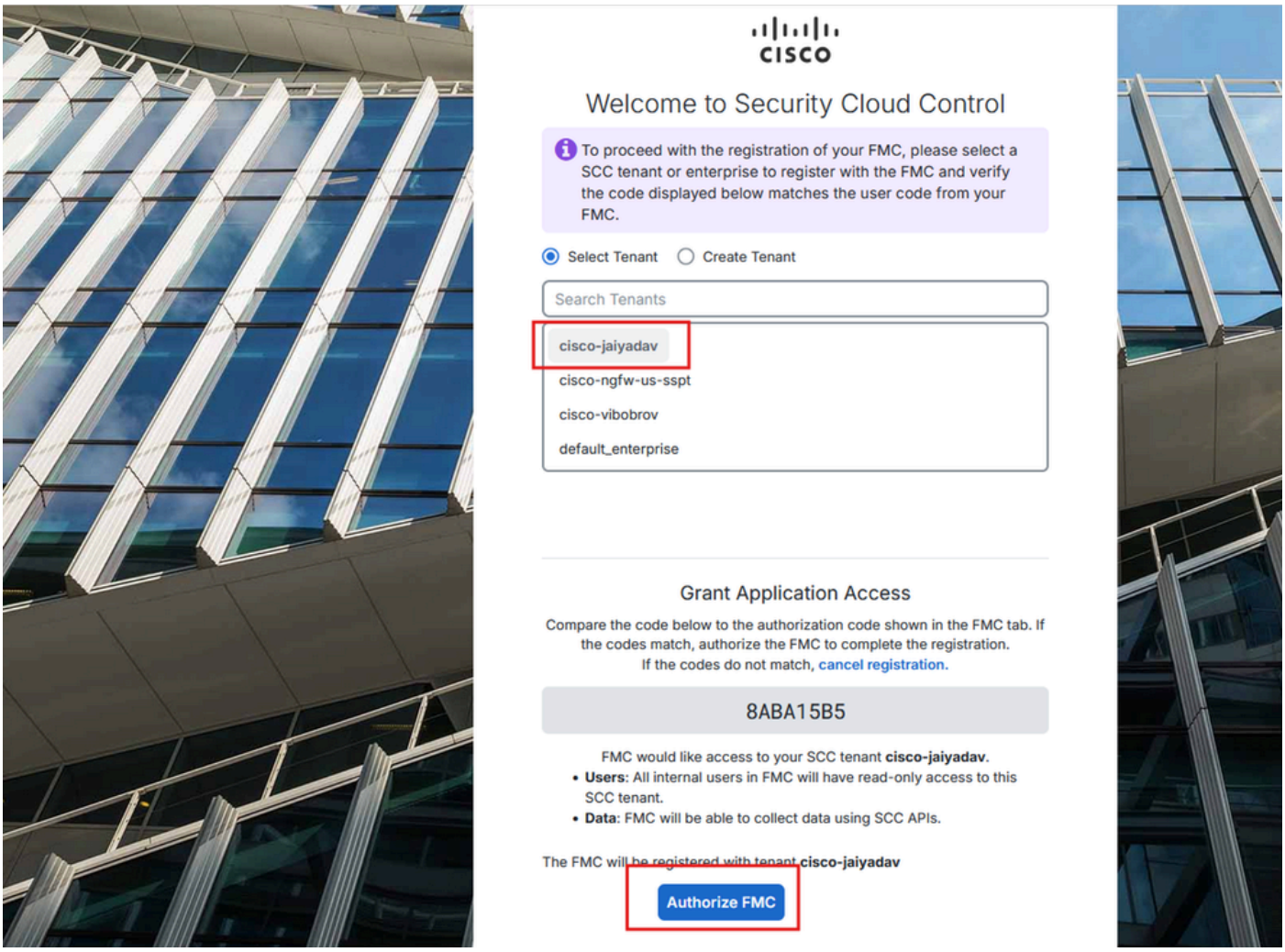
- 点击 Continue to Cisco SSO

注意：确保您从SCC注销，并且没有打开任何其他选项卡。



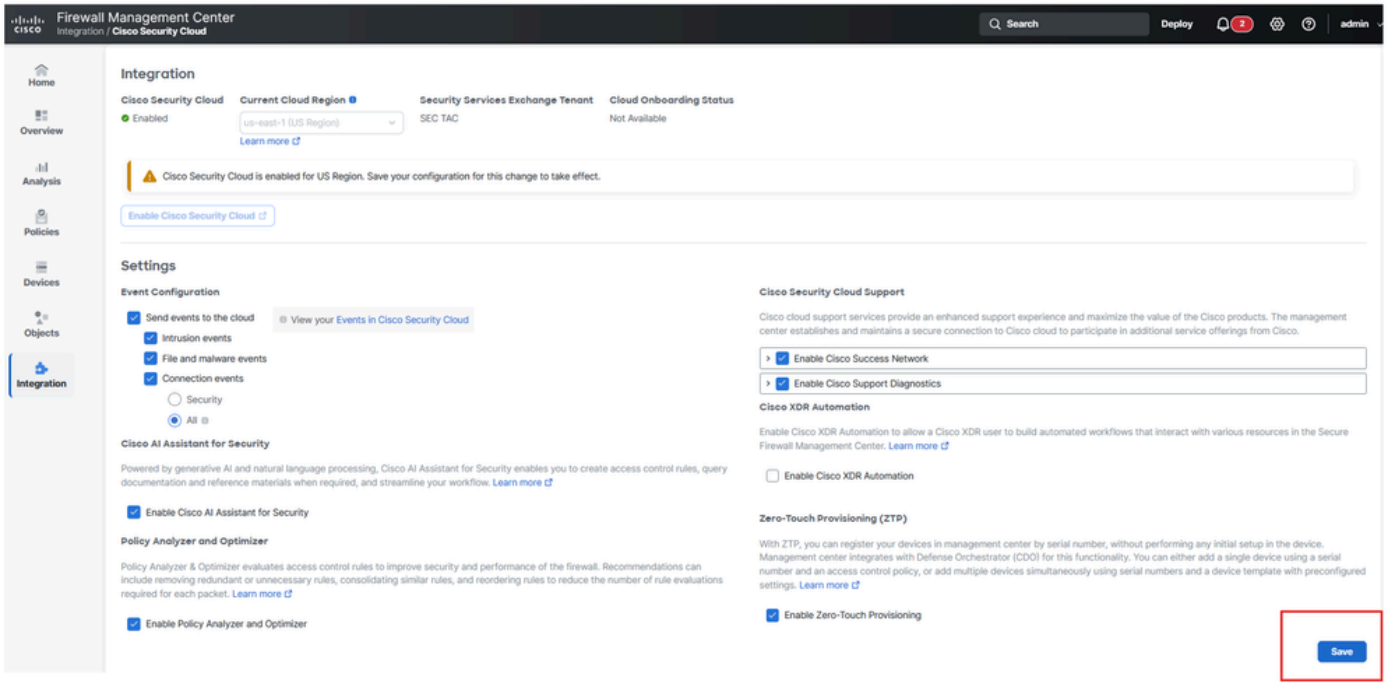
防火墙管理中心自注册到SCC

- 选择您的SCC租户并点击 Authorize FMC



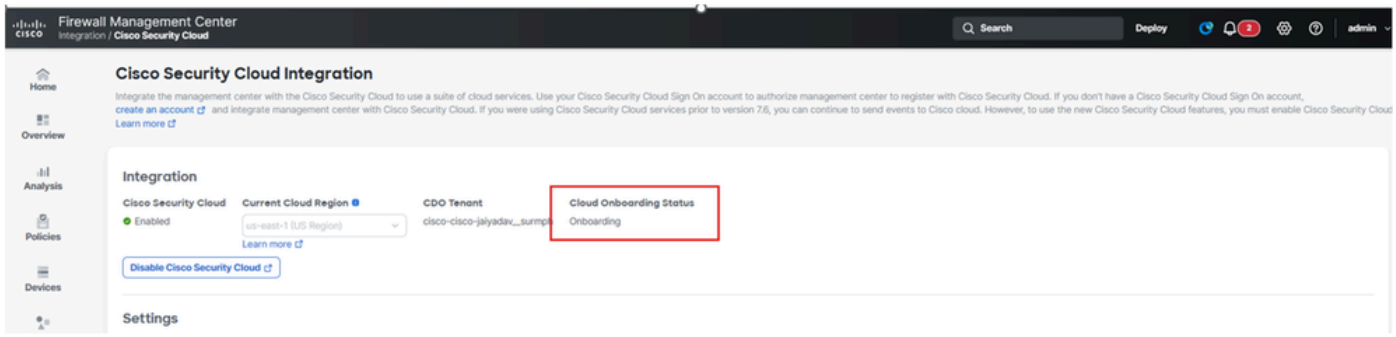
防火墙管理中心自注册到SCC

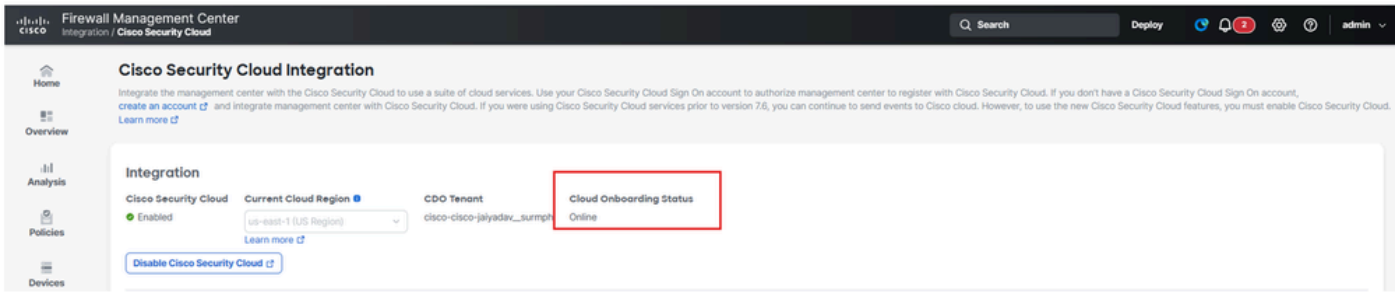
- 点击 Save



防火墙管理中心自注册到SCC

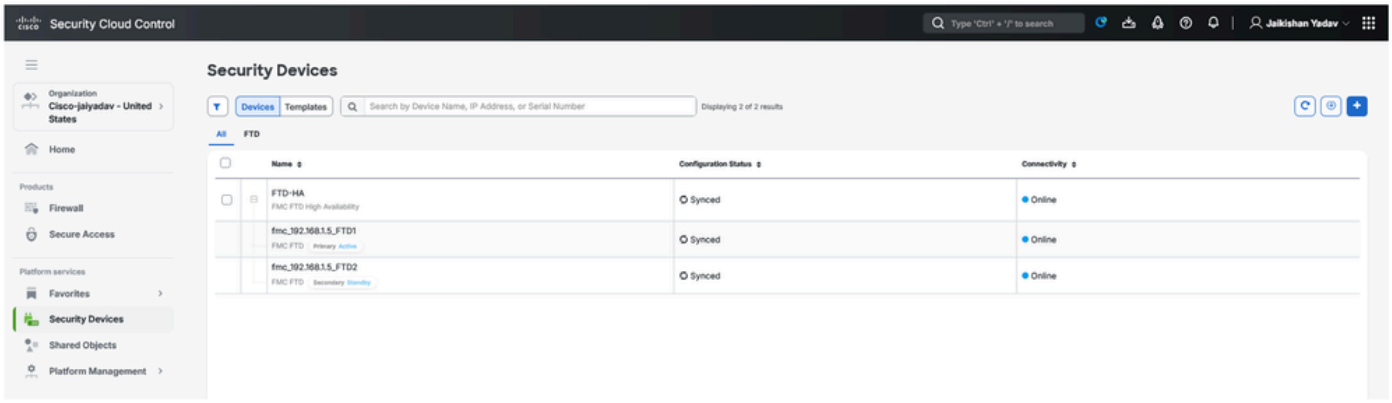
的状态必Cloud Onboarding Status须从更改为**Not Available**Onboarding ，然Online。





防火墙管理中心自注册状态

- 导航到SCC，并检查>下的FTD状Platform Services态 Security Devices

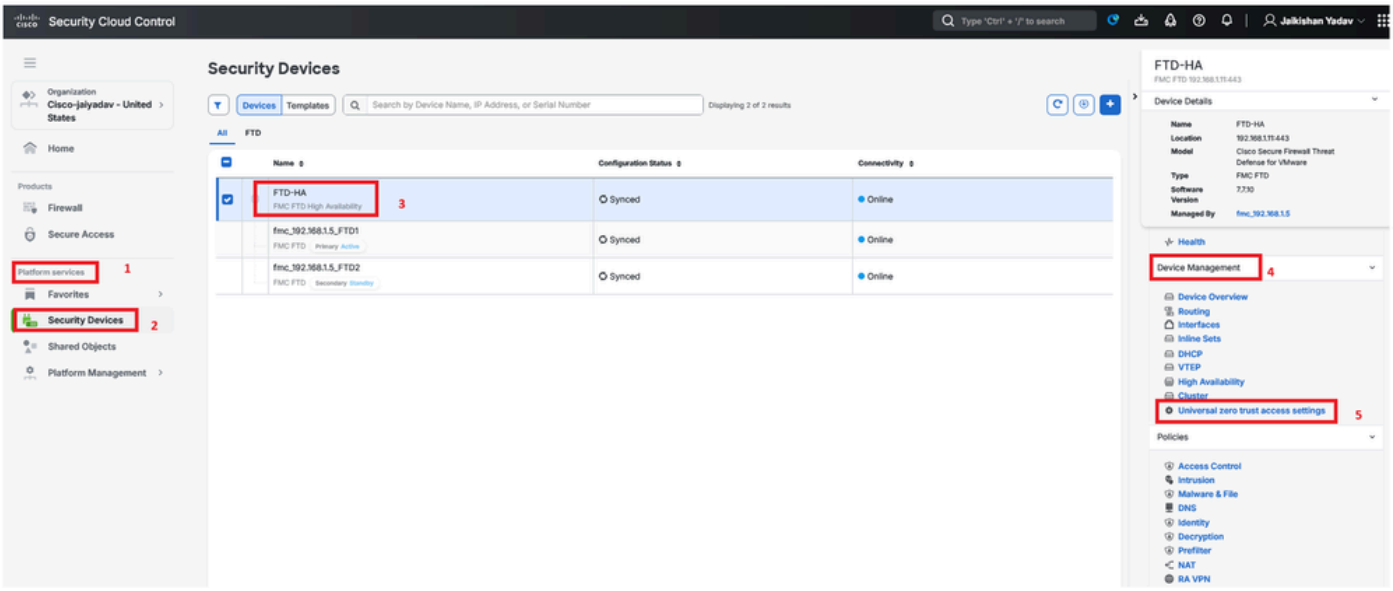


SCC上的安全防火墙威胁防御状态

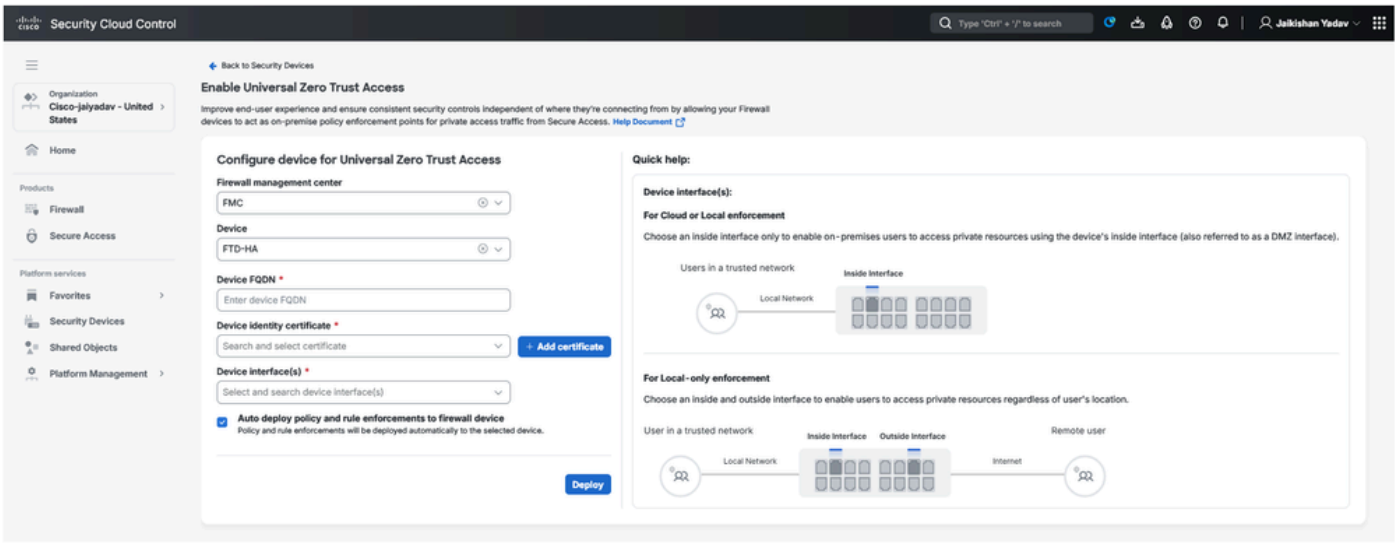
在FTD上注册通用零信任网络访问(uZTNA)设置

导航至SCC:

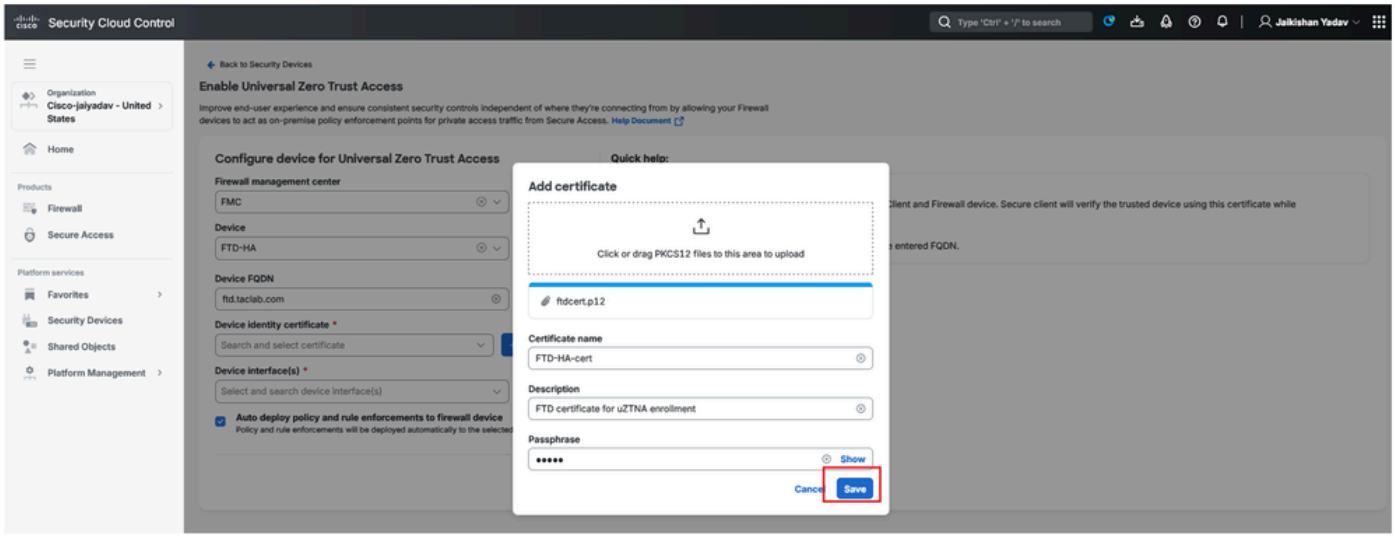
- 点击Platform Services>**Security Devices** > **FTD** > **Device Management** > Universal Zero Trust Network Access



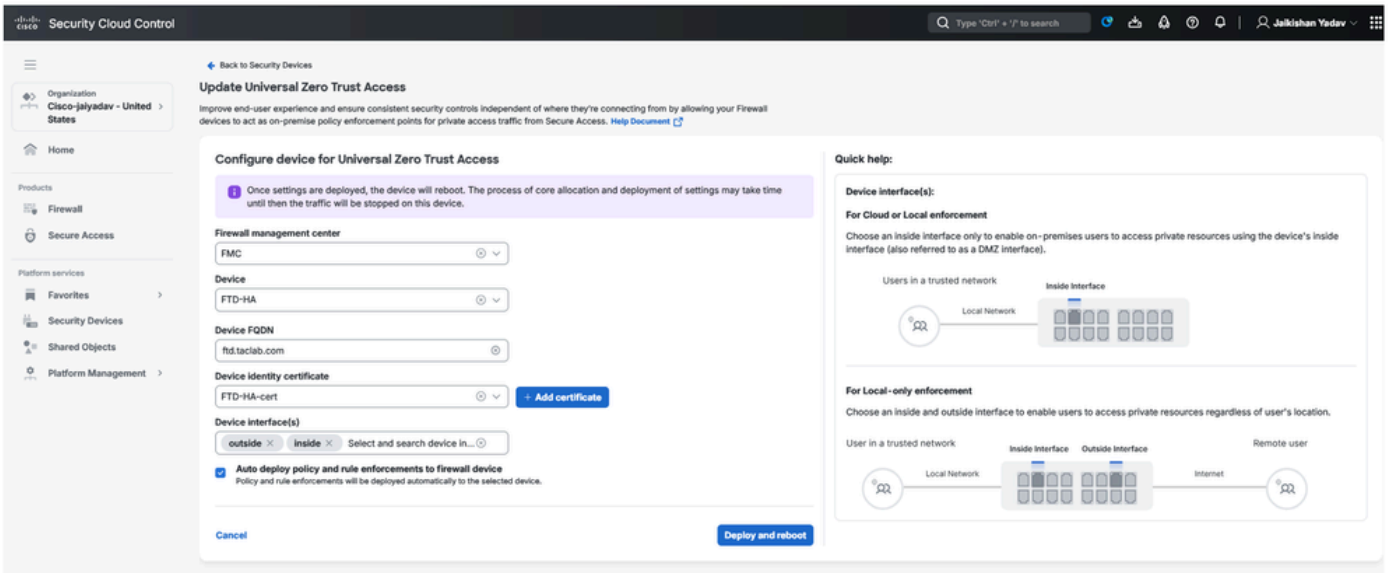
- 填写信息并上传在步骤[生成防火墙威胁防御(FTD)CA签名证书中生成的FTD证书]



安全防火墙威胁防御 — 通用ZTNA配置



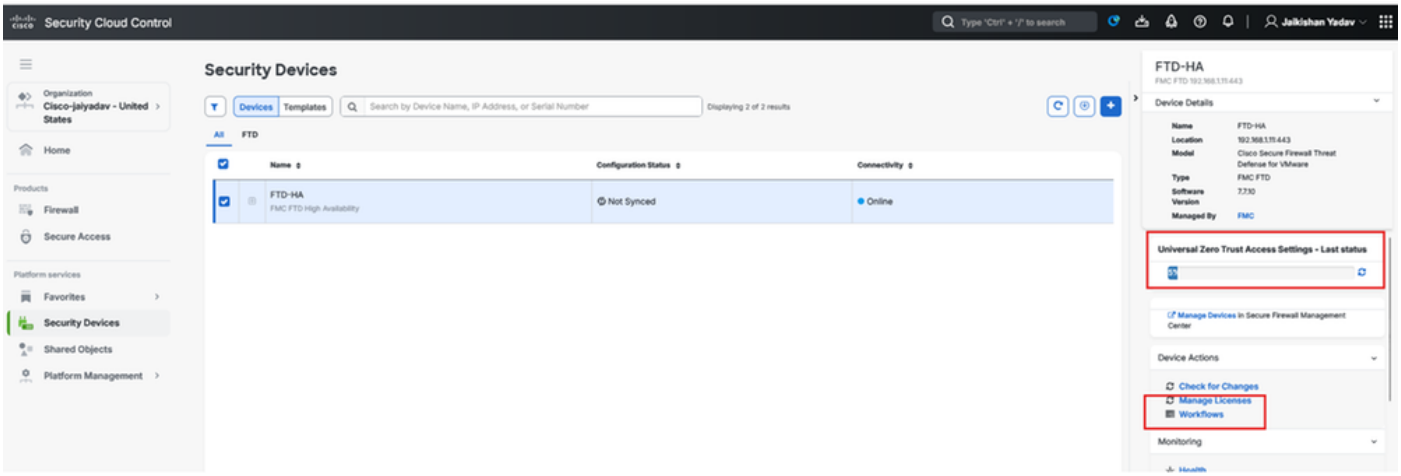
安全防火墙威胁防御 — 通用ZTNA配置



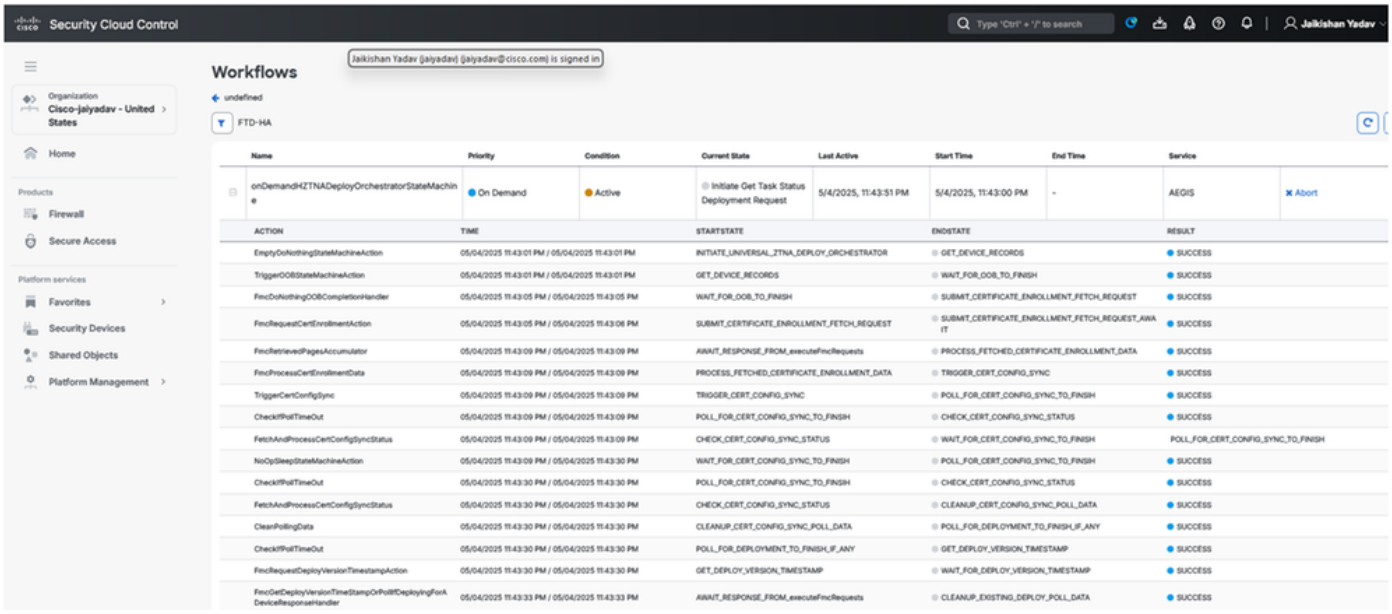
安全防火墙威胁防御 — 通用ZTNA配置

注意：当您在FTD HA上启用uZTNA时，它将部署更改并同时重新启动两个防火墙威胁防御(FTD)设备。确保安排适当的维护窗口。

- 点击Workflow，检查日志

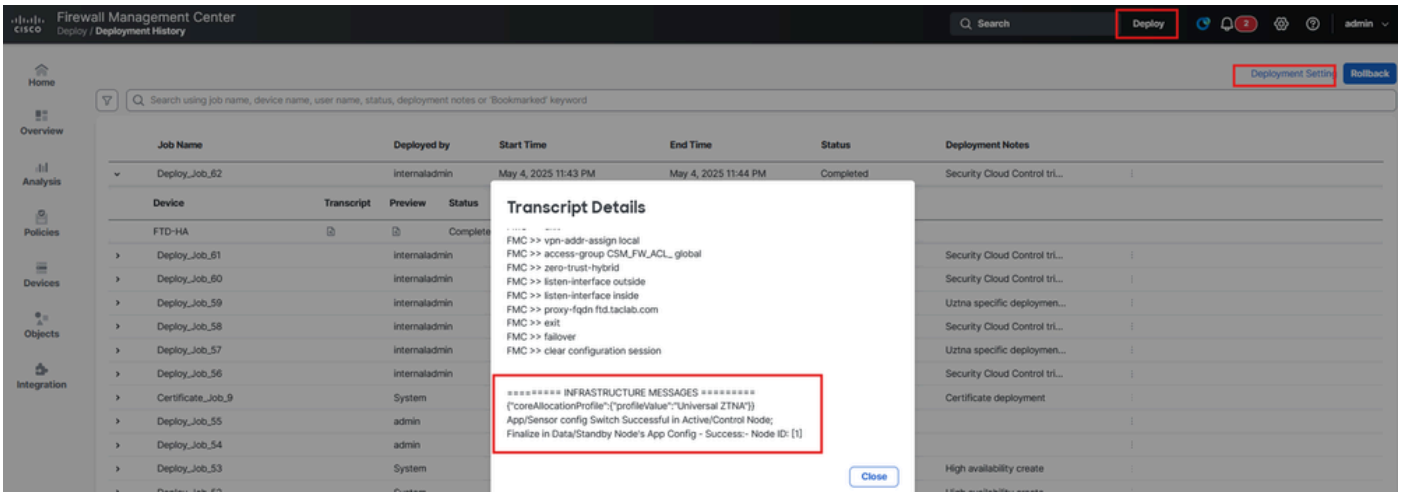


安全防火墙威胁防御 — 通用ZTNA配置状态



安全云控制工作流程

在Transcript Details下，您可以查看Policy Deployment Status和更改 FMC.



安全防火墙管理中心 — 策略部署状态

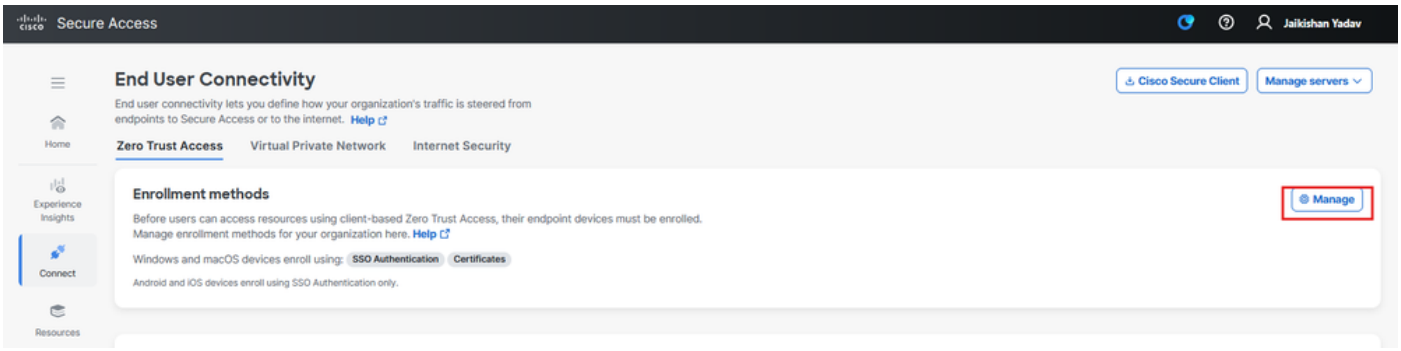
使用uZTNA注册客户端

安全访问配置

注意：您可以使用SSO或基于证书的ZTA注册。接下来是基于证书的ZTA注册的步骤

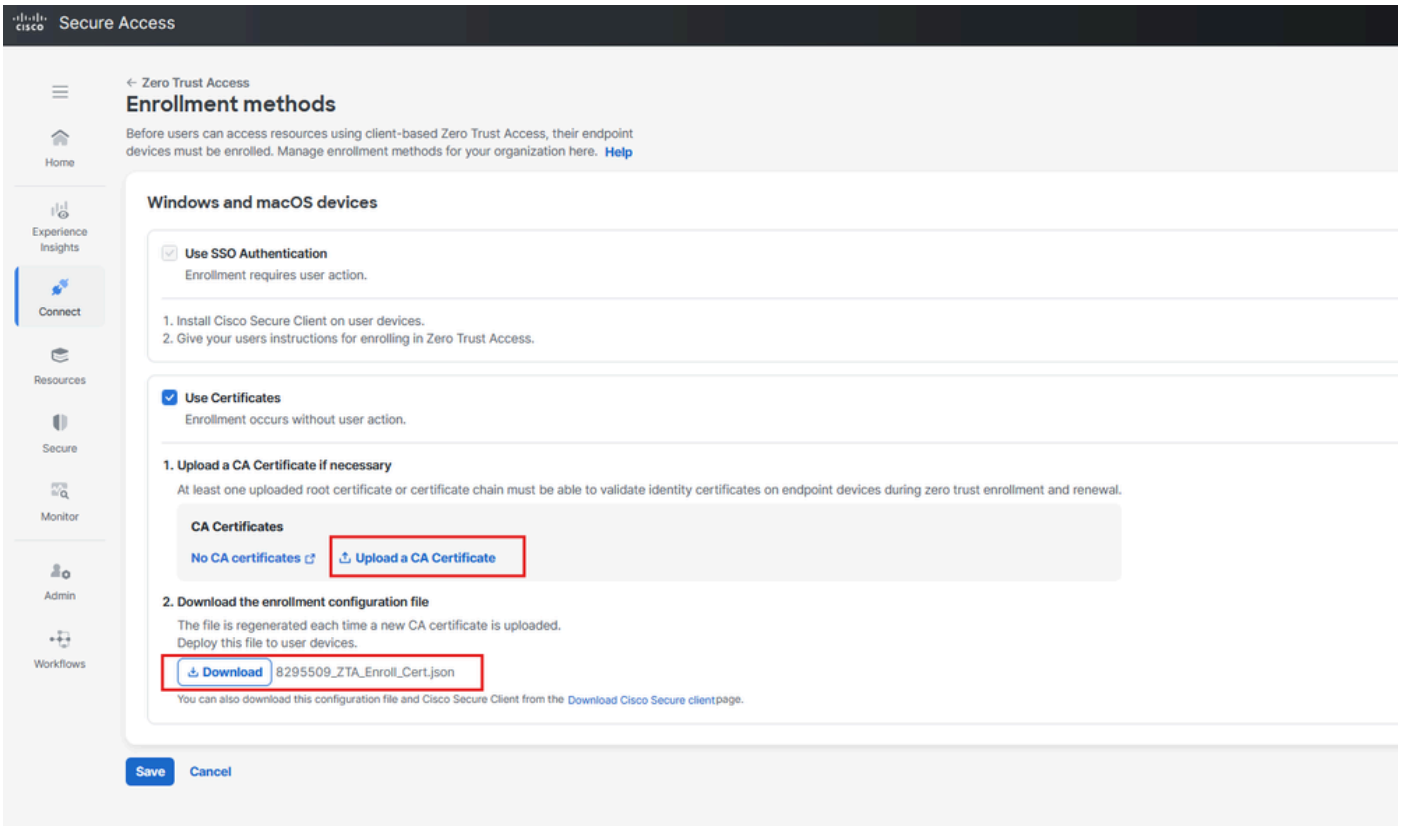
导航到安全访问控制面板:

- 点击**Connect> End User Connectivity>** Zero Trust Access
- 点击 Manage



安全访问 — ZTA证书注册

- 上传根CA证书并下载注册配置文件

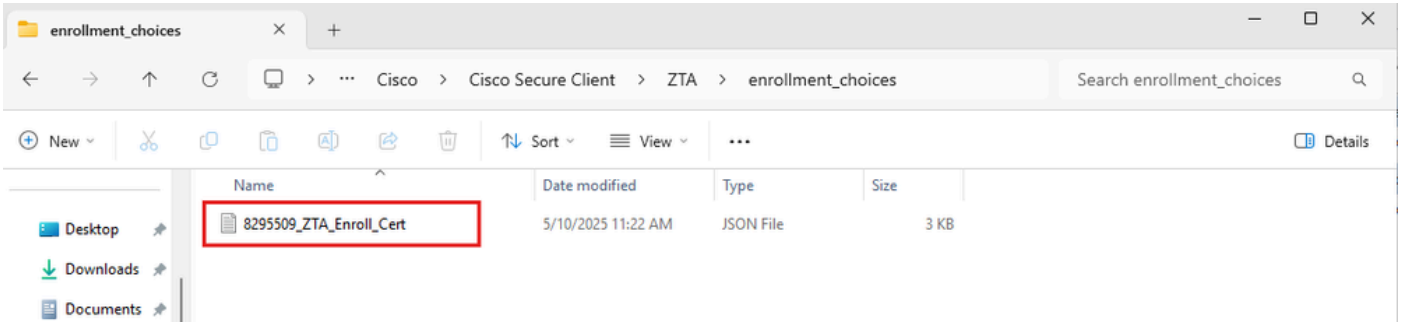


安全访问 — ZTA证书注册

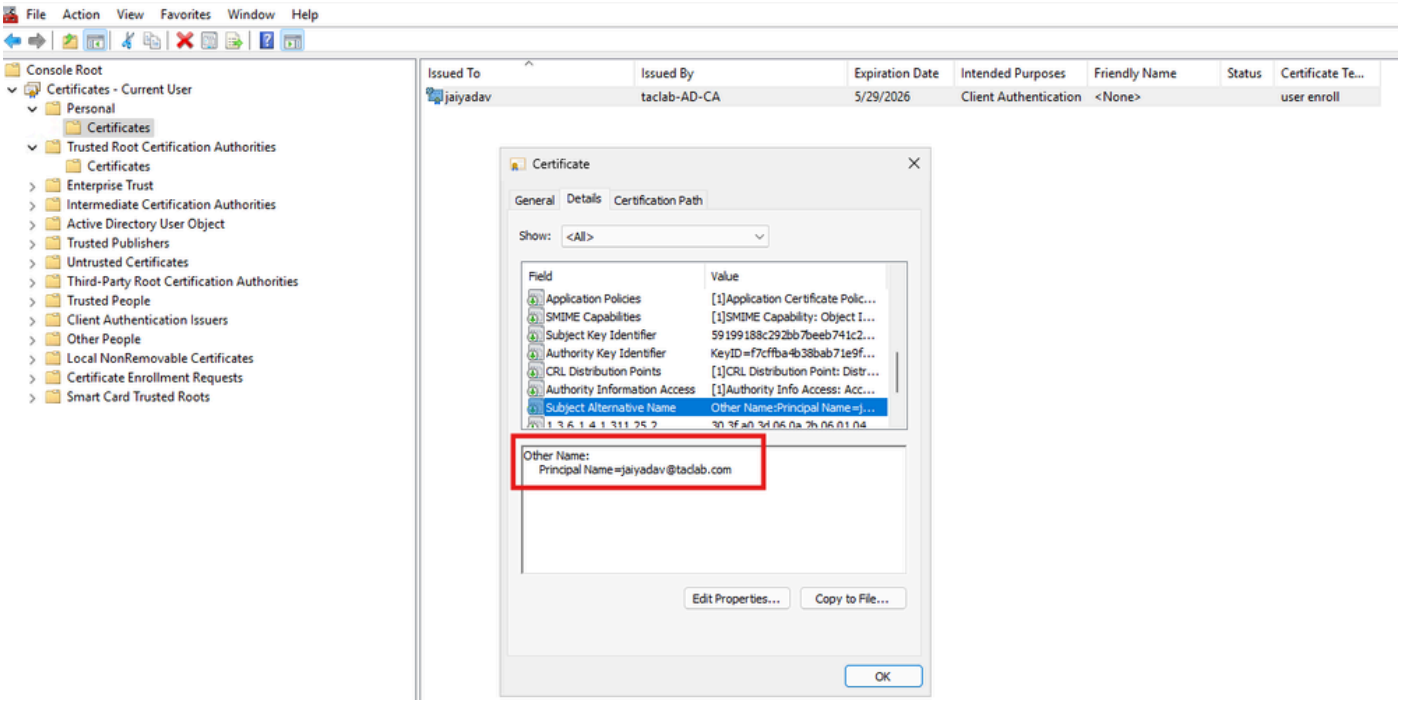
- 点击 Save

客户端配置

将注册配置文件复制到 C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices

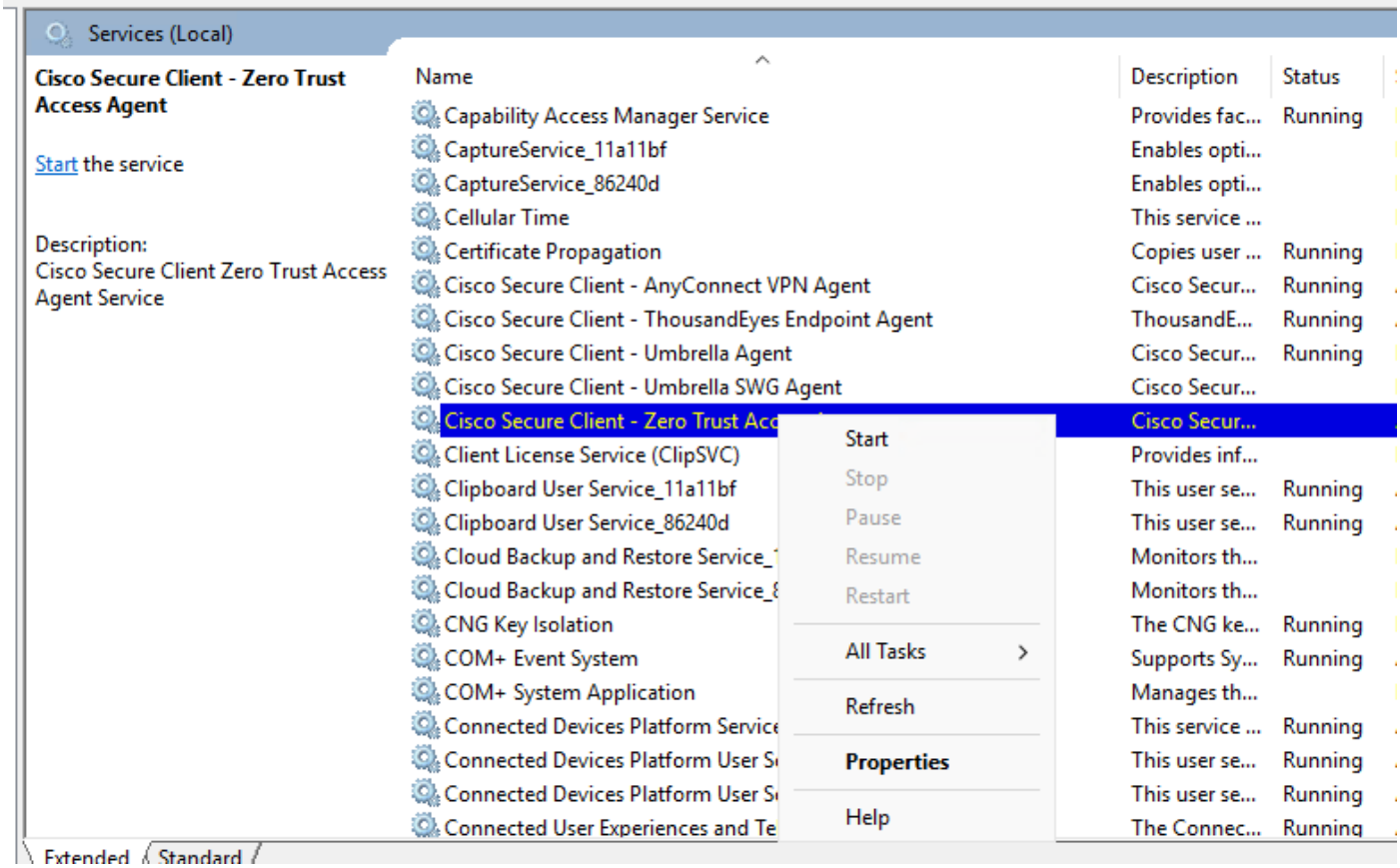


- 创建客户端证书，该证书必须在SAN中具有UPN



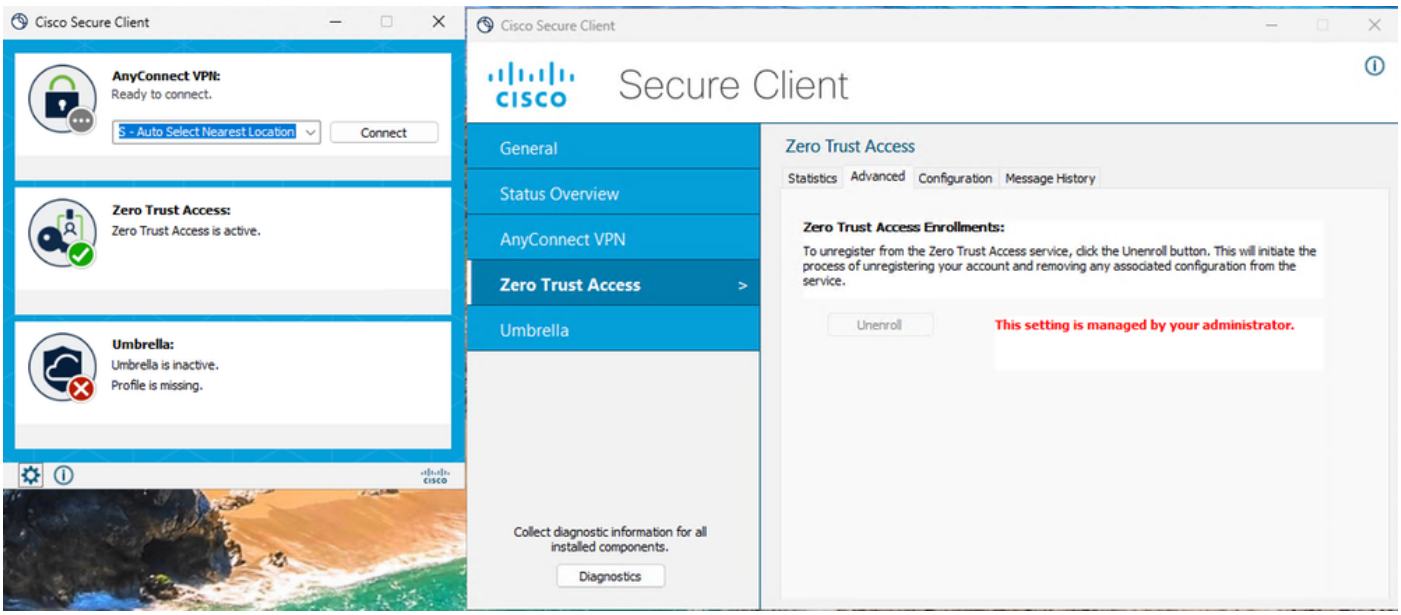
证书安装

- **启动/重新启动** Cisco Secure Client - Zero Trust Access Agent



Windows服务

- 验证ZTA模块状态



安全访问 — ZTA证书注册状态

验证

使用下一命令验证防火墙威胁防御(FTD)上的uZTNA配置：

```
show allocate-core profile
show running-config universal-zero-trust
```

相关信息

- 思科技术支持和下载
- 思科安全访问帮助中心
- Cisco SASE设计指南

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）。