在FTD上配置使用本地身份验证的SSL安全客户端

目录

简介

本文档介绍如何在Cisco FMC管理的Cisco FTD上配置采用本地身份验证的Cisco安全客户端（包括Anyconnect）。

先决条件

要求

Cisco 建议您了解以下主题：

- 通过Firepower管理中心(FMC)配置SSL安全客户端
- 通过FMC配置Firepower对象
- Firepower上的SSL证书

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Firepower威胁防御(FTD) 7.0.0版（内部版本94）
- Cisco FMC版本7.0.0（内部版本94）
- 思科安全移动客户端4.10.01075

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。

背景信息

在本示例中，安全套接字层(SSL)用于在FTD和Windows 10客户端之间创建虚拟专用网络(VPN)。

从版本7.0.0开始，由FMC管理的FTD支持思科安全客户端的本地身份验证。这可以定义为主要身份验证方法，或作为主要方法发生故障时的回退。在本示例中，本地身份验证配置为主要身份验证。

在此软件版本之前，FTD上的思科安全客户端本地身份验证仅在Cisco Firepower设备管理器(FDM)上可用。

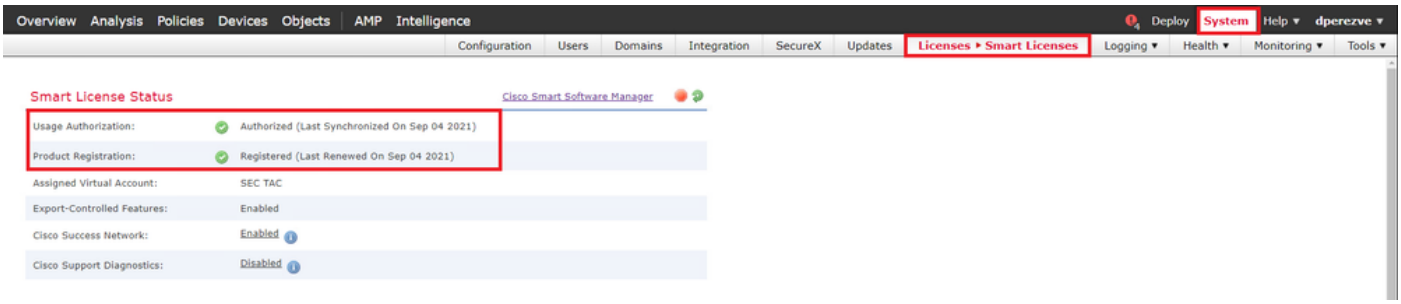
配置

配置

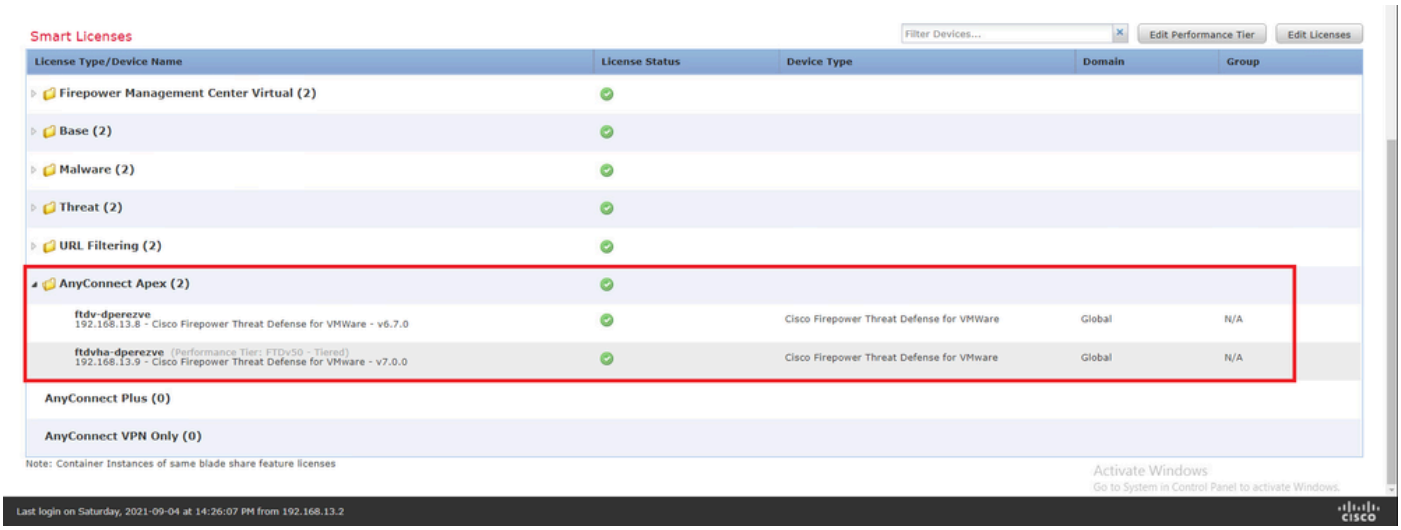
步骤1:验证许可

在配置思科安全客户端之前，必须注册FMC并符合智能许可门户的规定。如果FTD没有有效的Plus、Apex或仅VPN许可证，则无法部署思科安全客户端。

导航到系统>许可证>智能许可证，确保FMC已注册并符合智能许可门户的规定：



在同一页上向下滚动。在智能许可证图表的底部，您可以看到不同类型的可用思科安全客户端(AnyConnect)许可证和已订购的每台设备。确保手头的FTD按以下任何类别进行注册：

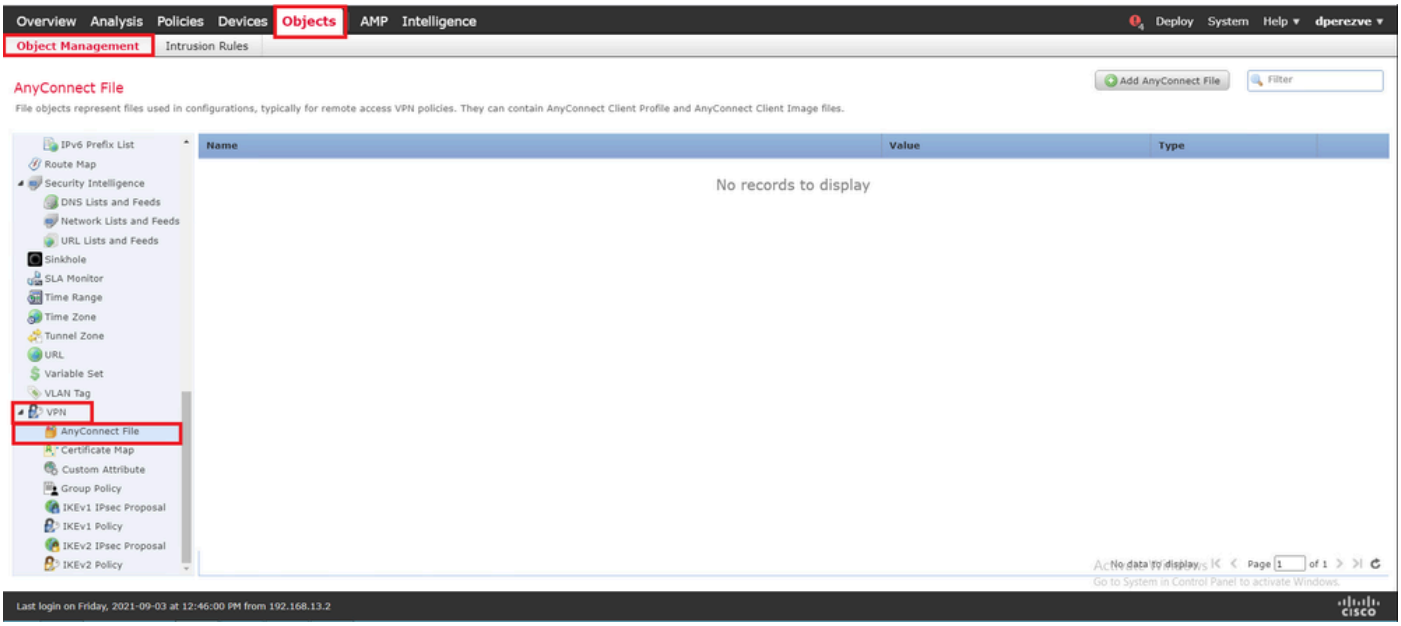


第二步：将思科安全客户端软件包上传到FMC

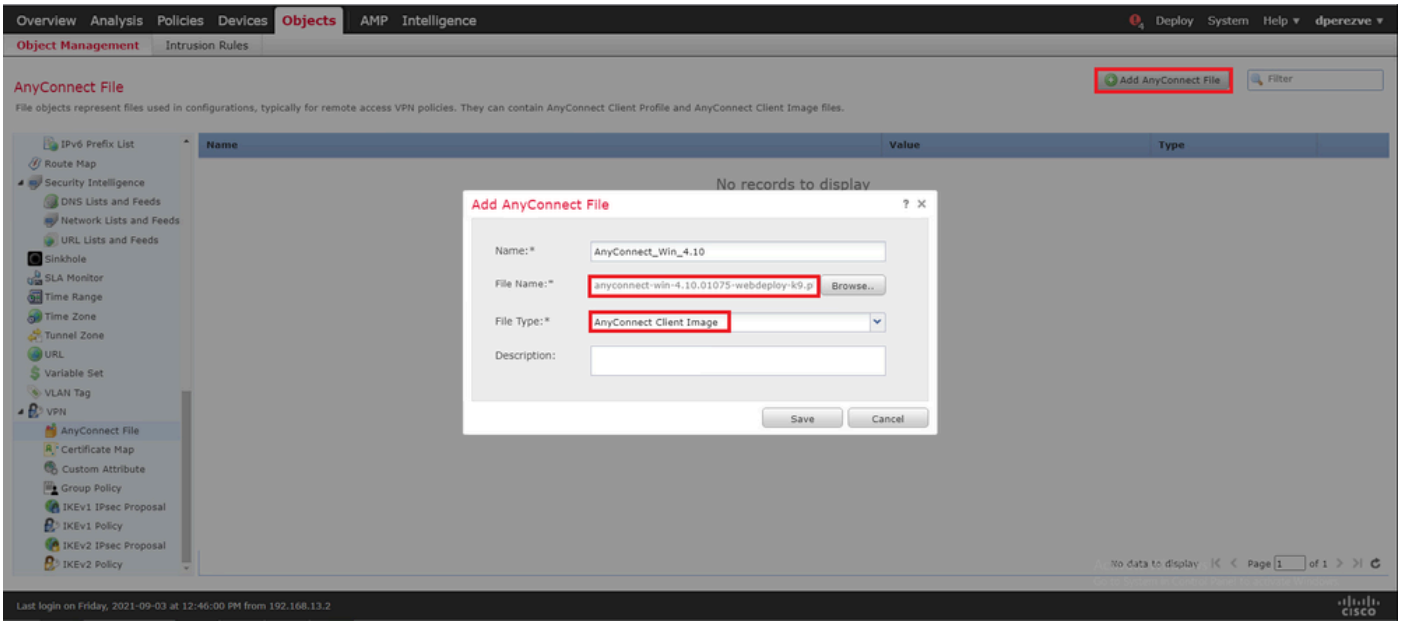
从cisco.com下载适用于Windows的思科安全客户端(AnyConnect)前端部署软件包：

Application Programming Interface [API] (Windows) anyconnect-win-4.10.01075-vpnapi.zip Advisories	21-May-2021	141.72 MB
AnyConnect Headend Deployment Package (Windows) anyconnect-win-4.10.01075-webdeploy-k9.pkg Advisories	21-May-2021	77.81 MB
AnyConnect Pre-Deployment Package (Windows 10 ARM64) - includes individual MSI files anyconnect-win-arm64-4.10.01075-predeploy-k9.zip Advisories	21-May-2021	34.78 MB
AnyConnect Headend Deployment Package (Windows 10 ARM64) anyconnect-win-arm64-4.10.01075-webdeploy-k9.pkg Advisories	21-May-2021	44.76 MB
Profile Editor (Windows) tools-anyconnect-win-4.10.01075-profileeditor-k9.msi Advisories	21-May-2021	10.90 MB
AnyConnect Installer Transforms (Windows) tools-anyconnect-win-4.10.01075-transforms.zip Advisories	21-May-2021	0.05 MB

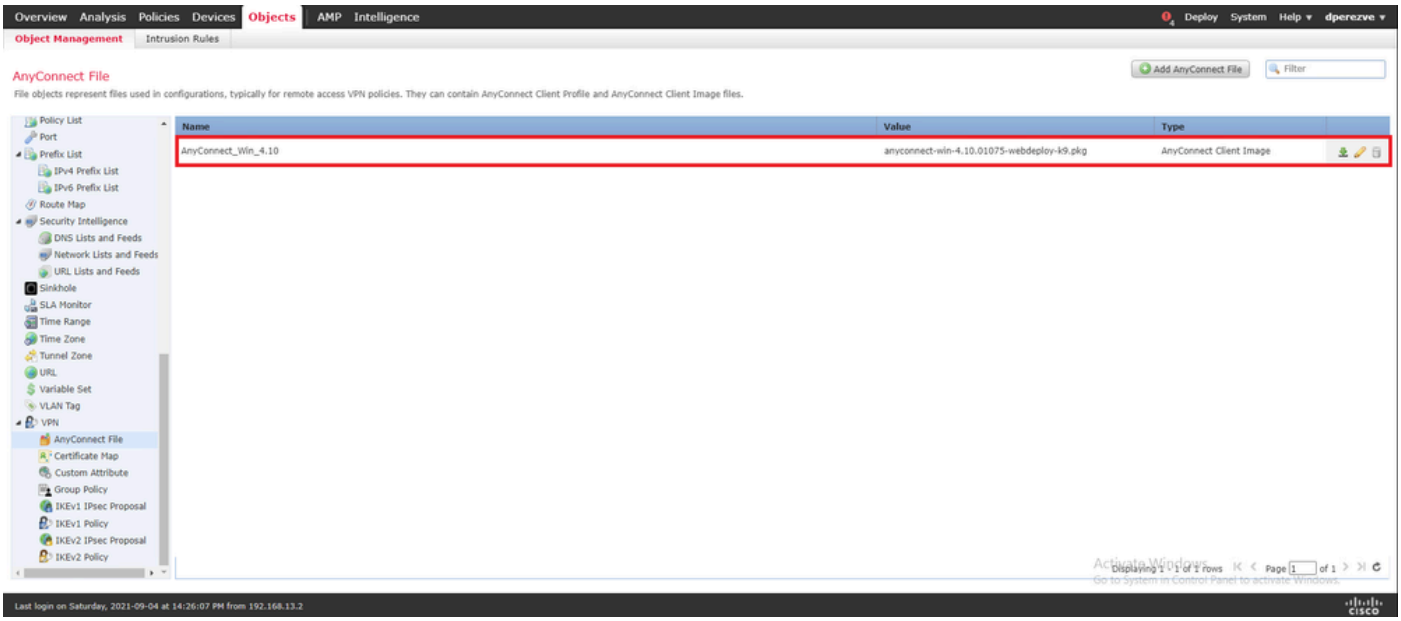
要上传Cisco安全客户端映像，请导航到对象>对象管理，在目录中的VPN类别下选择Cisco安全客户端文件：



选择Add AnyConnect File按钮。在Add AnyConnect Secure Client File窗口中，为对象指定名称，然后选择Browse...以选择Cisco Secure Client软件包。最后，在下拉菜单中选择AnyConnect Client Image作为文件类型：



选择Save按钮。必须将对象添加到对象列表：



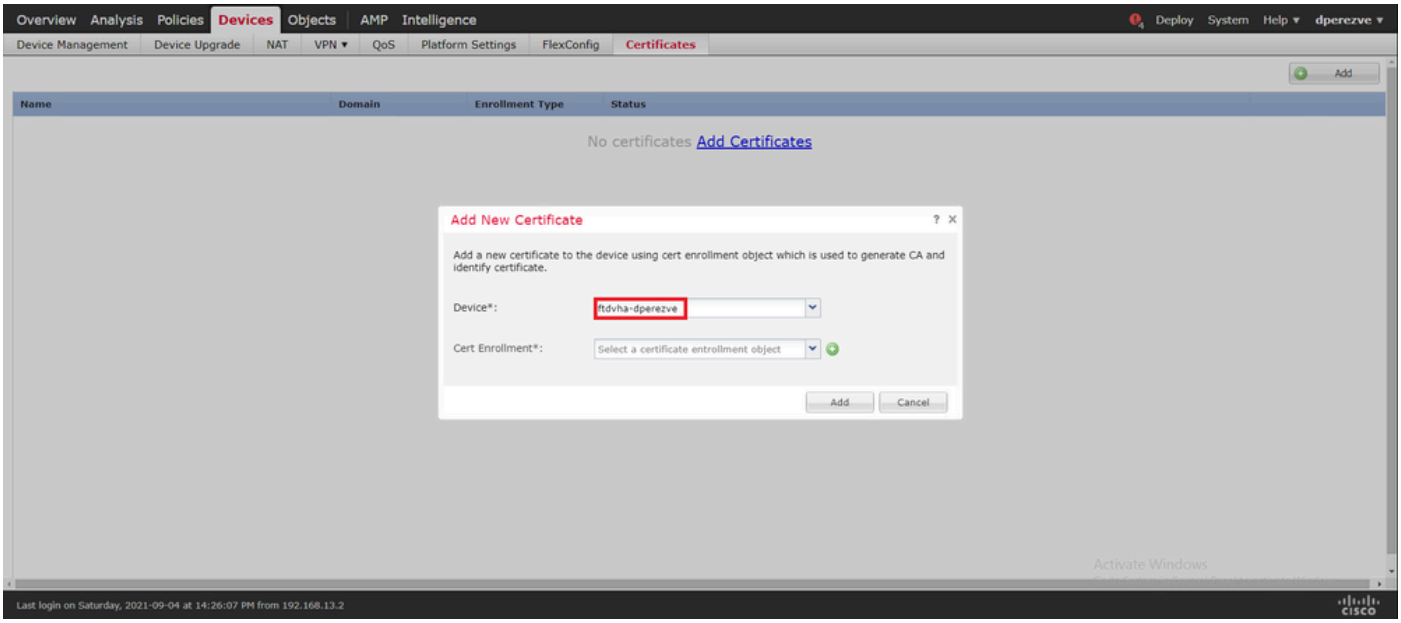
第三步：生成自签名证书

SSL思科安全客户端(AnyConnect)要求在VPN头端和客户端之间的SSL握手中使用一个有效证书。

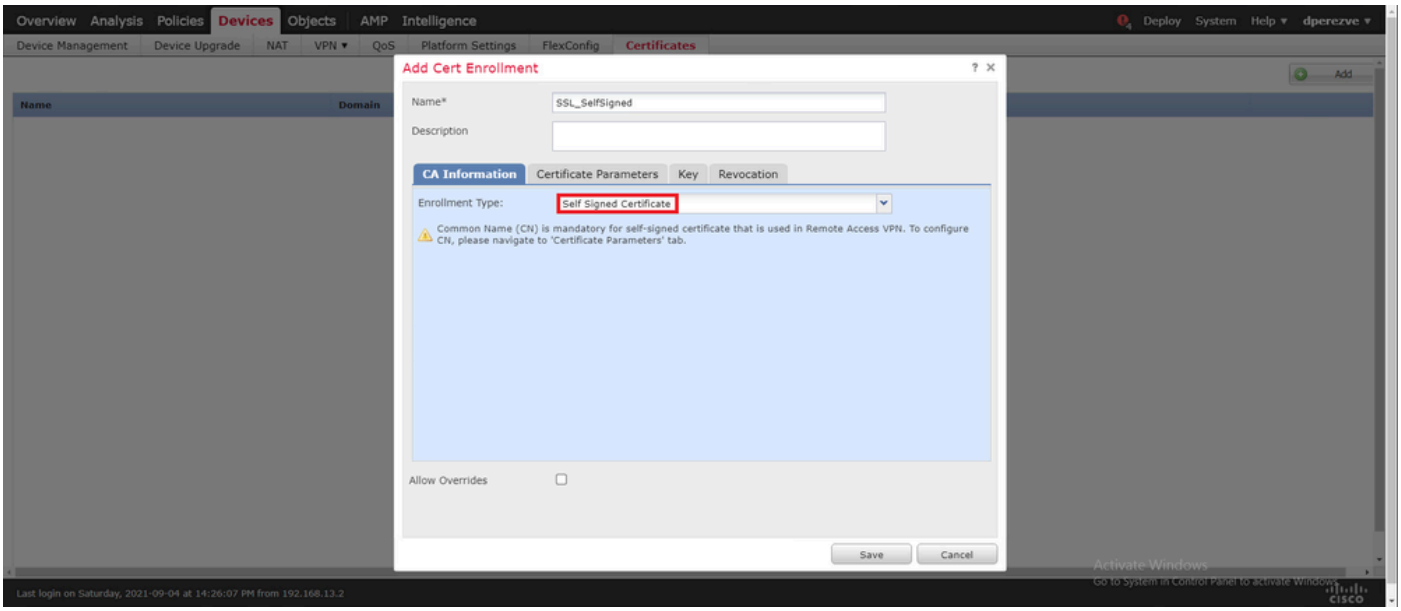
注意：在本示例中，将为此生成自签名证书。此外，除了自签名证书之外，还可以上传由内部证书颁发机构(CA)或公认CA签名的证书。

要创建自签名证书，请导航到设备>证书。

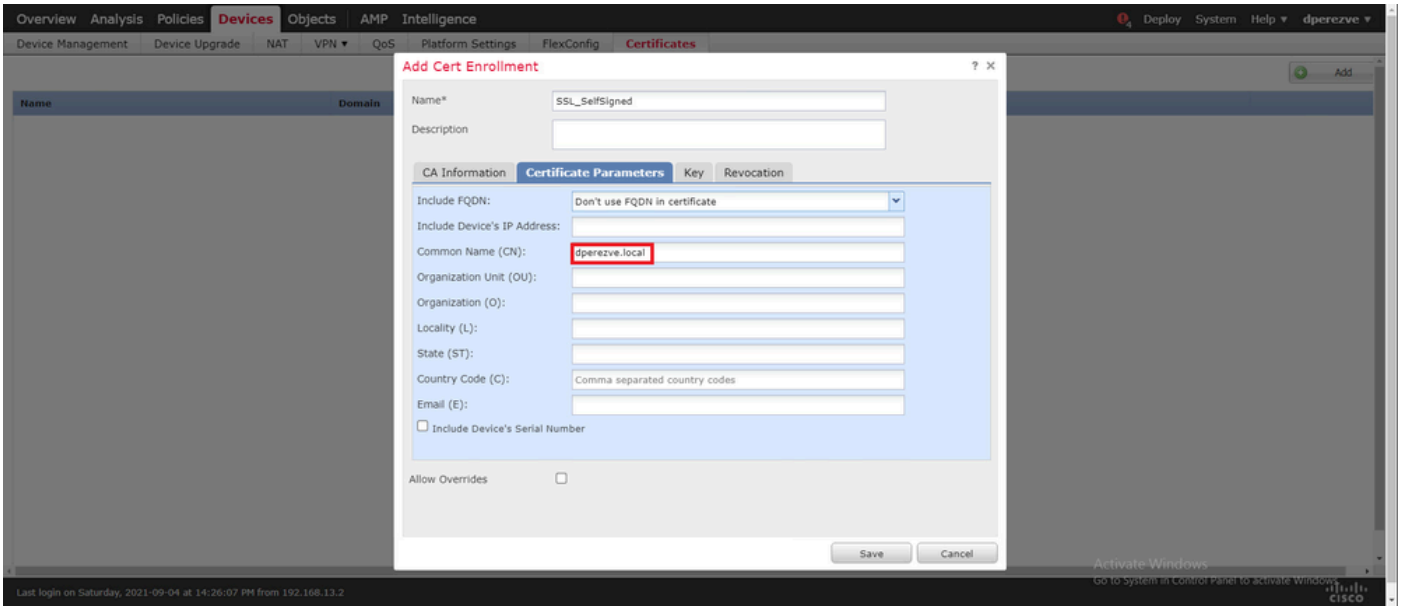
选择Add按钮。然后选择Add New Certificate窗口的Device下拉菜单中列出的FTD。



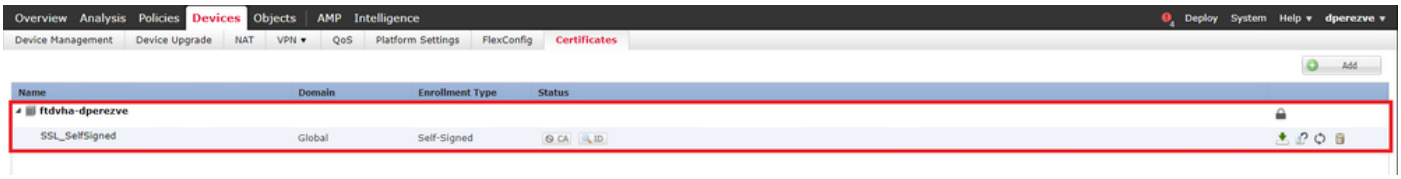
选择Add Cert Enrollment按钮（绿色+符号）以创建新的注册对象。现在，在Add Cert Enrollment窗口中，为对象分配一个名称，并在Enrollment Type下拉菜单中选择Self Signed Certificate。



最后，对于自签名证书，必须具有公用名(CN)。导航到证书参数选项卡以定义CN：

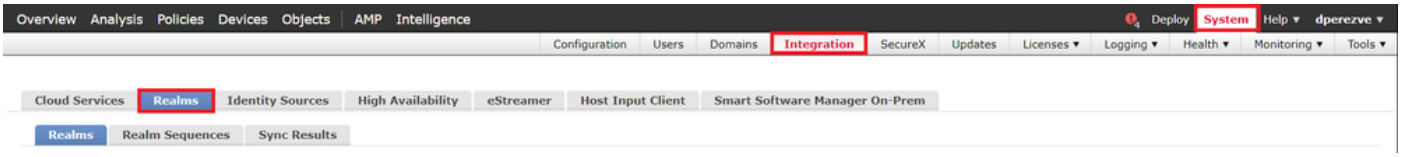


单击Save和Add按钮。几秒钟后，新证书必须添加到证书列表：

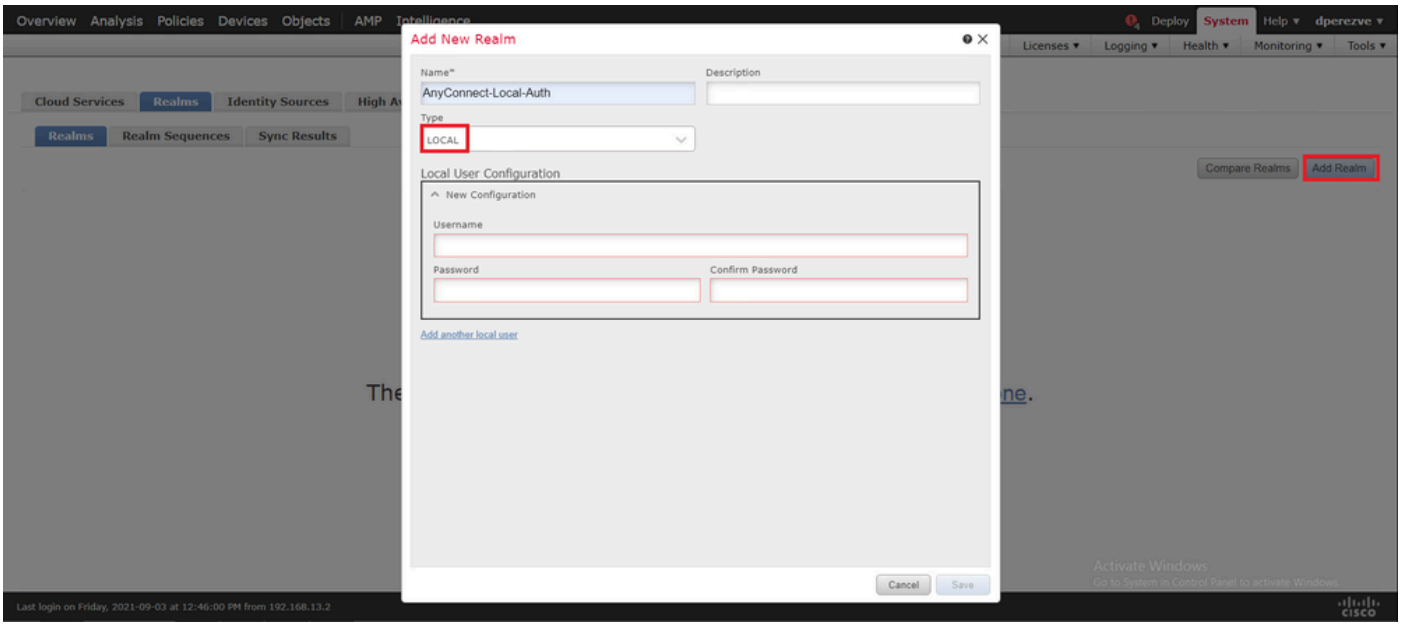


第四步：在FMC上创建本地领域

本地用户数据库和各自的口令存储在本地领域中。要创建本地领域，请导航到系统>集成>领域：

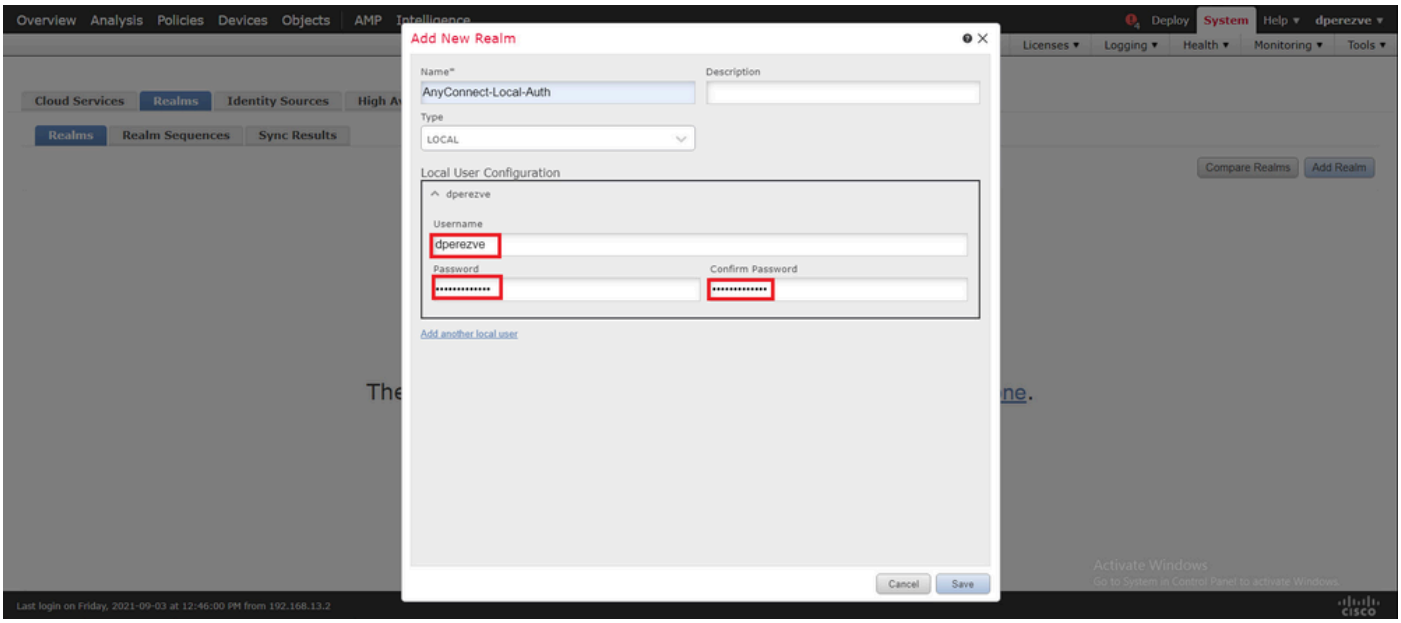


选择Add Realm按钮。在添加新领域窗口中，在类型下拉菜单中分配一个名称并选择本地选项：

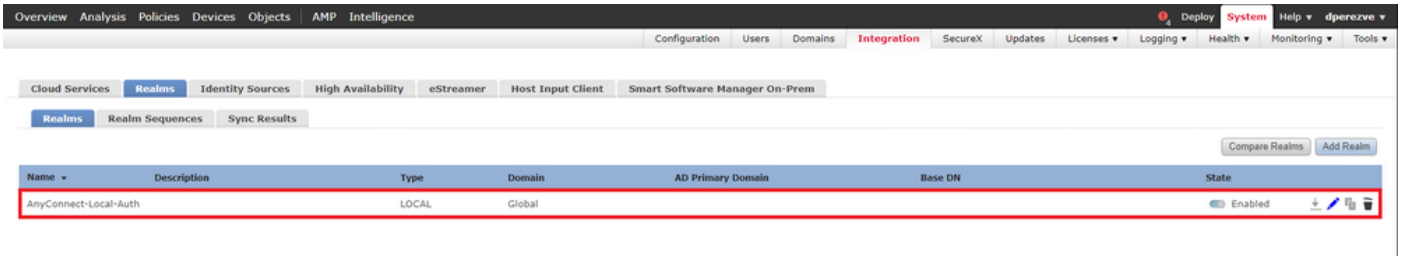


用户帐户和密码在Local User Configuration部分创建。

> 注意：密码必须至少包含一个大写字母、一个小写字母、一个数字和一个特殊字符。

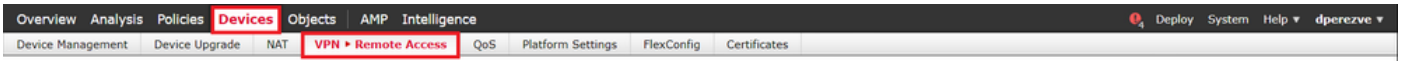


保存更改，然后点击添加领域以向现有领域列表中添加新领域。

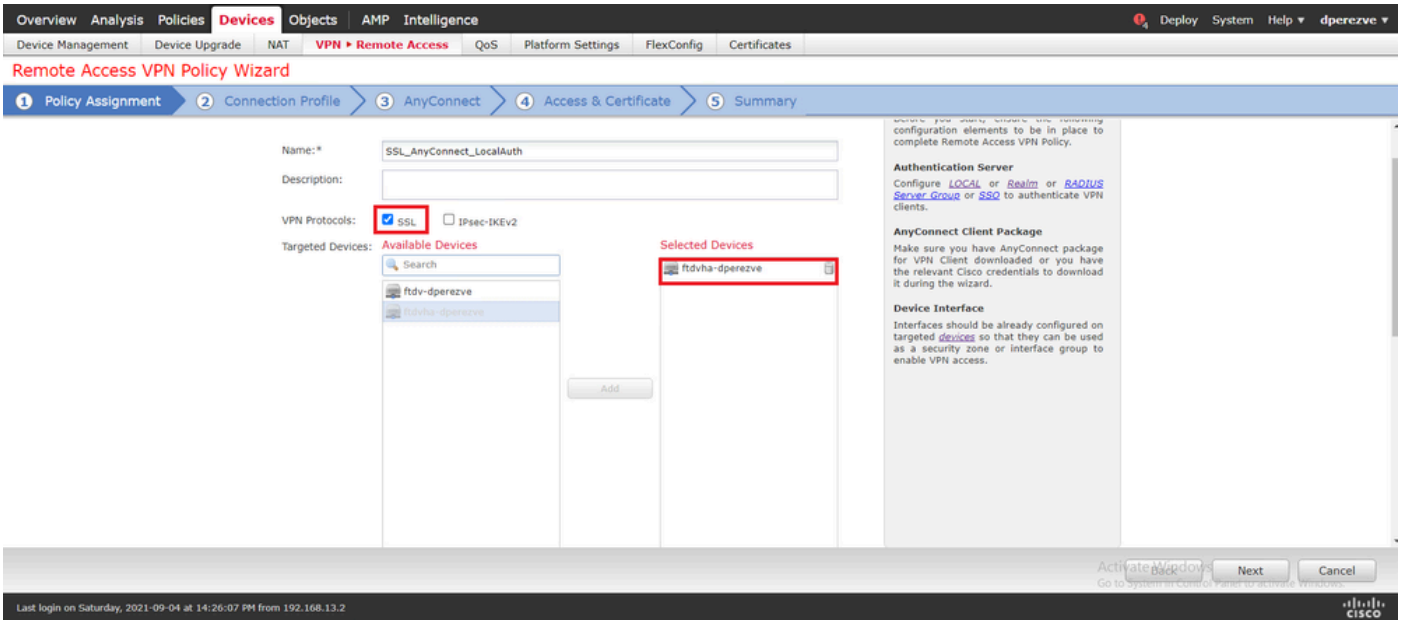


第五步：配置SSL Cisco安全客户端

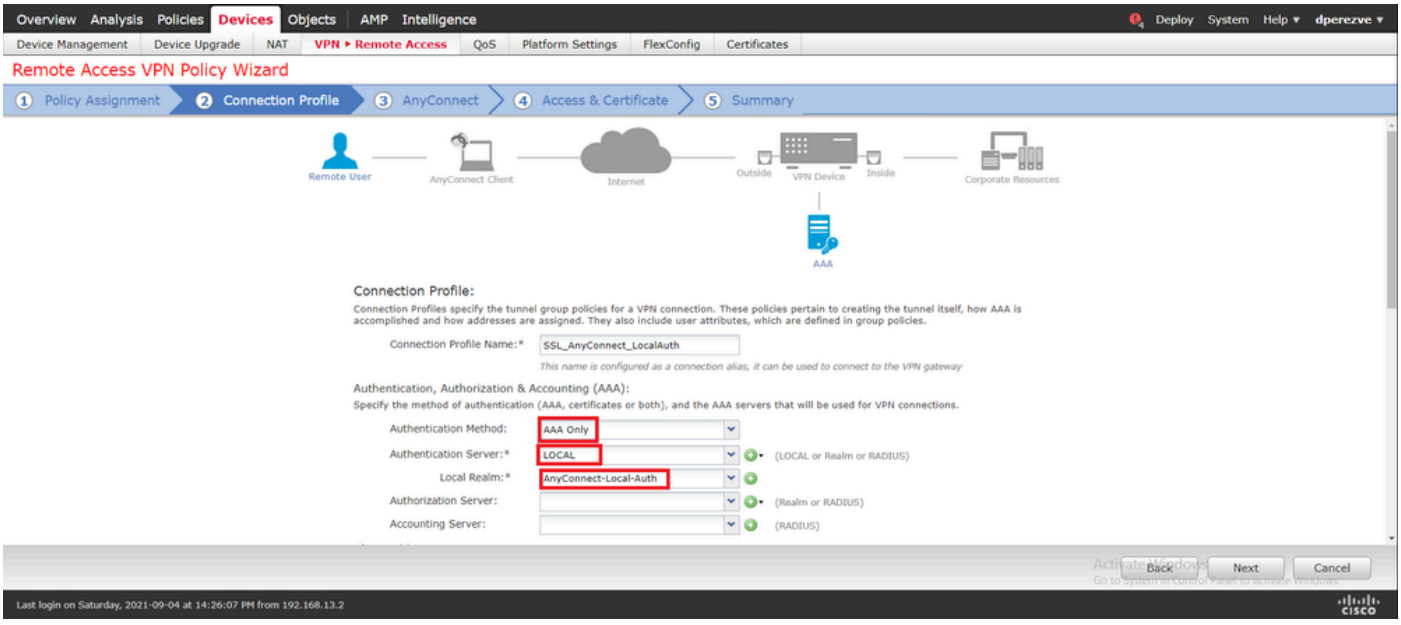
要配置SSL Cisco安全客户端，请导航到Devices > VPN > Remote Access：



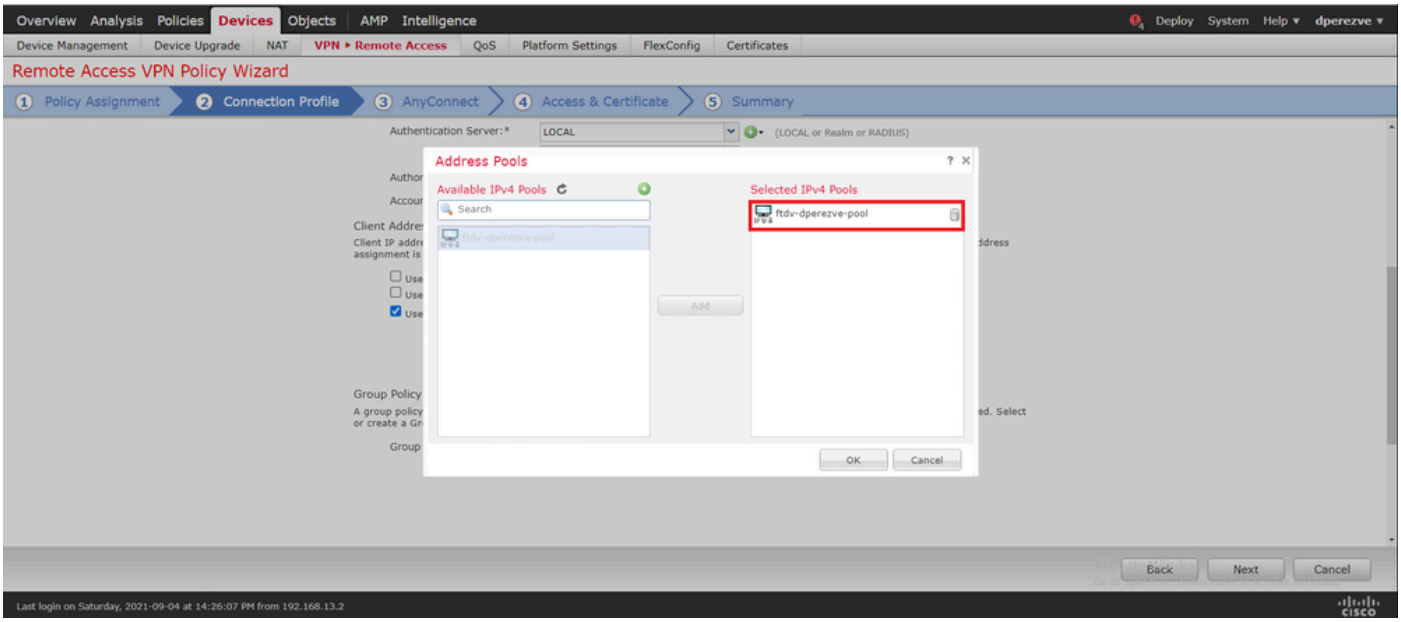
单击Add按钮以创建新的VPN策略。定义连接配置文件的名称，选中SSL复选框，然后选择作为目标设备列出的FTD。必须在远程访问VPN策略向导的策略分配部分中配置所有内容：



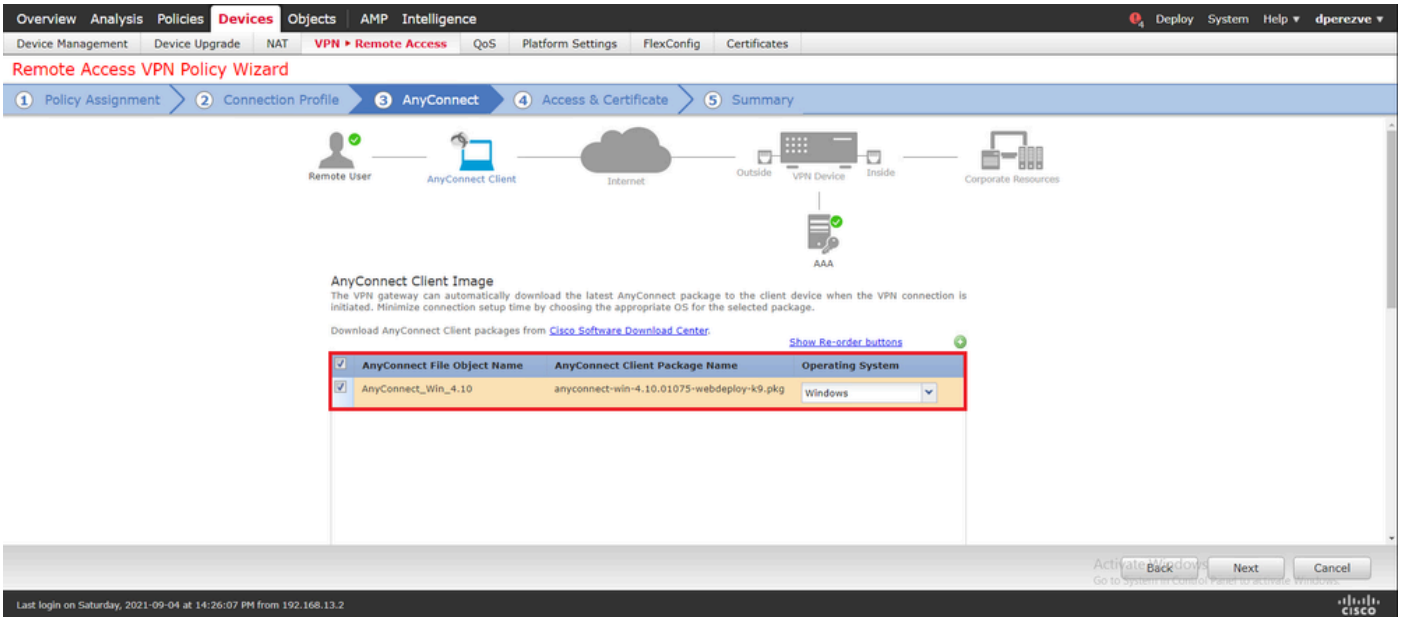
选择Next 转到连接配置文件配置。定义连接配置文件的名称并选择AAA Only作为身份验证方法。然后，在Authentication Server下拉菜单中，选择LOCAL，最后，在Local Realm下拉菜单中选择步骤4中创建的本地领域：



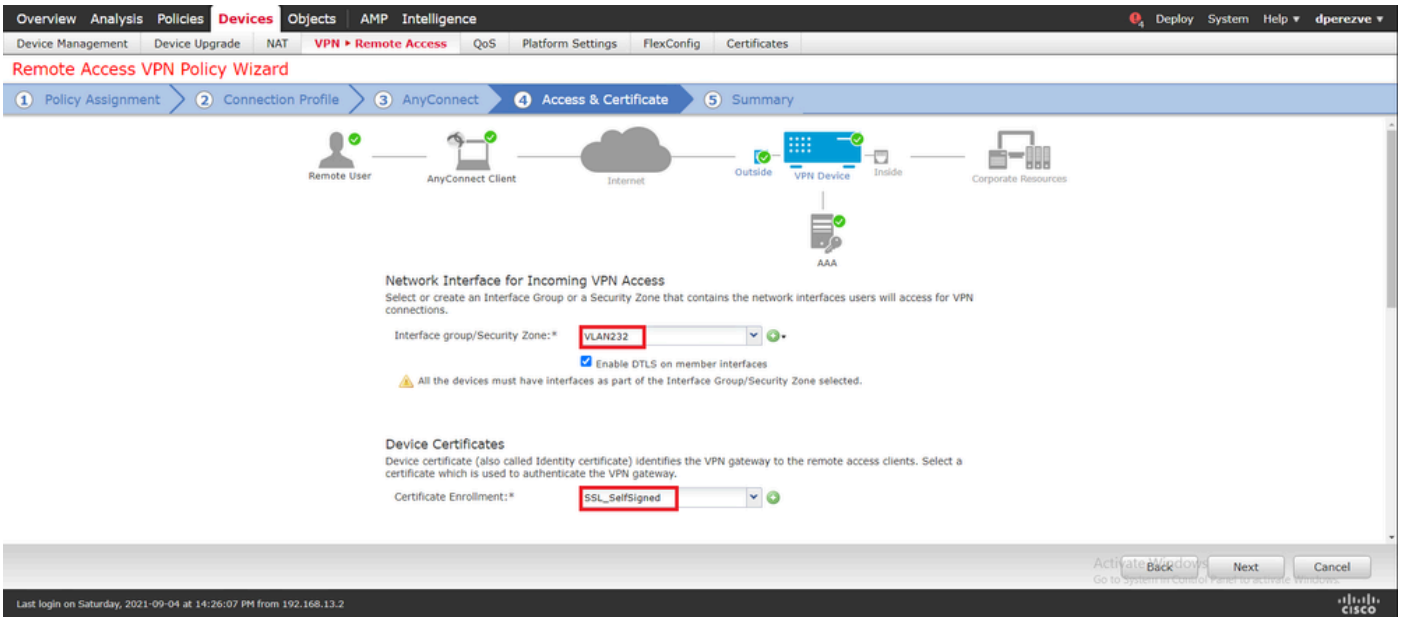
在同一页上向下滚动，然后单击IPv4地址池部分中的铅笔图标以定义Cisco安全客户端使用的IP池：



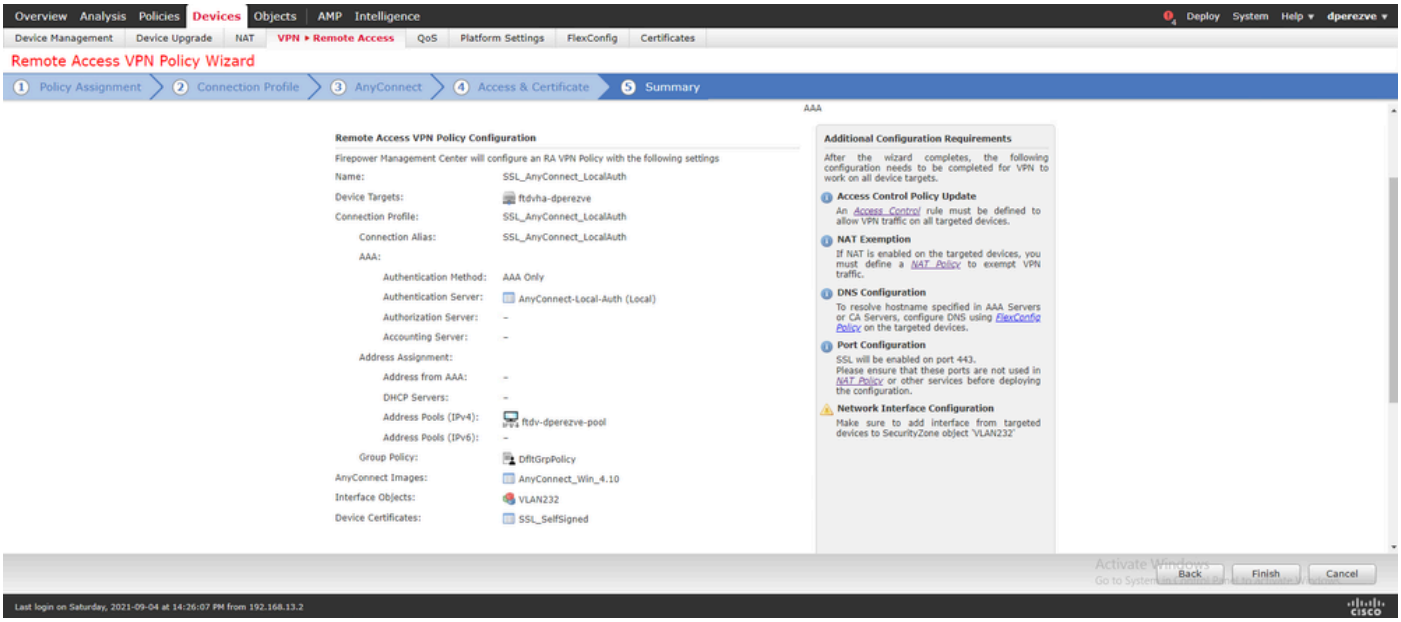
点击下一步，转到AnyConnect部分。现在，请选择在步骤2中上传的Cisco Secure Client映像：



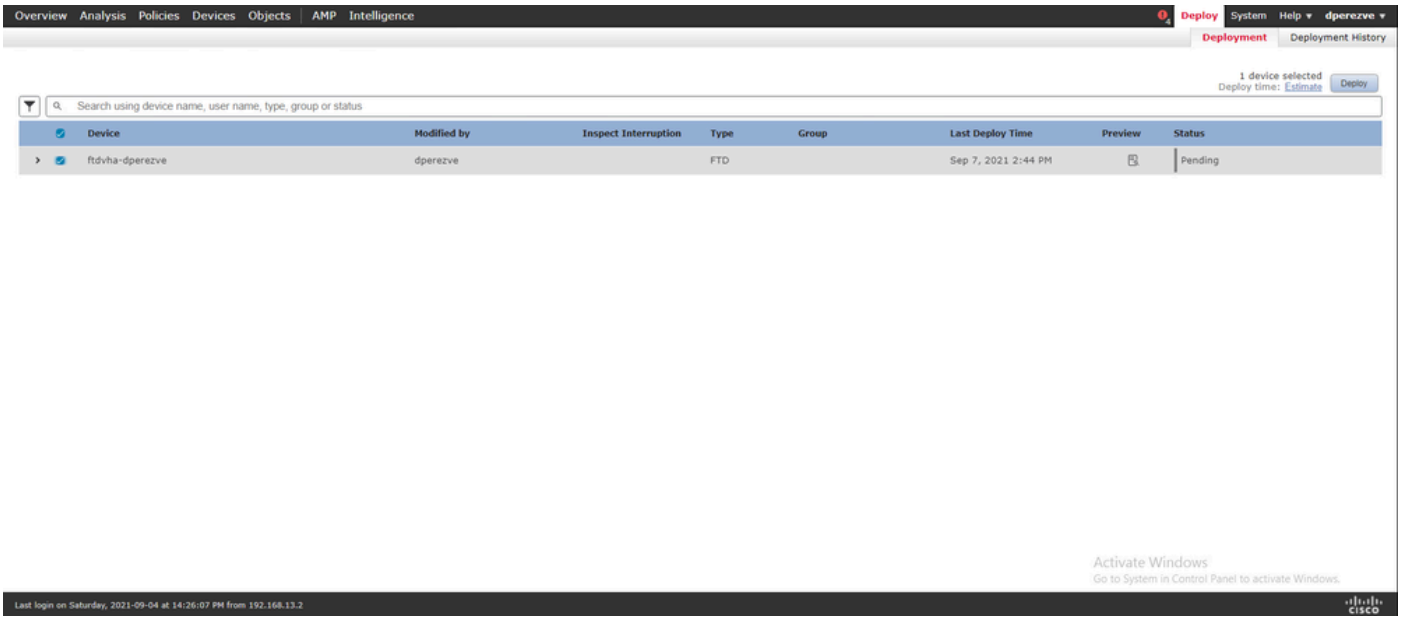
单击Next 转到Access & Certificate 部分。在Interface group/Security Zone下拉菜单中，选择需要启用Cisco安全客户端(AnyConnect)的接口。然后，在Certificate Enrollment下拉菜单中，选择在第3步中创建的证书：



最后，单击Next查看Cisco安全客户端配置的摘要：

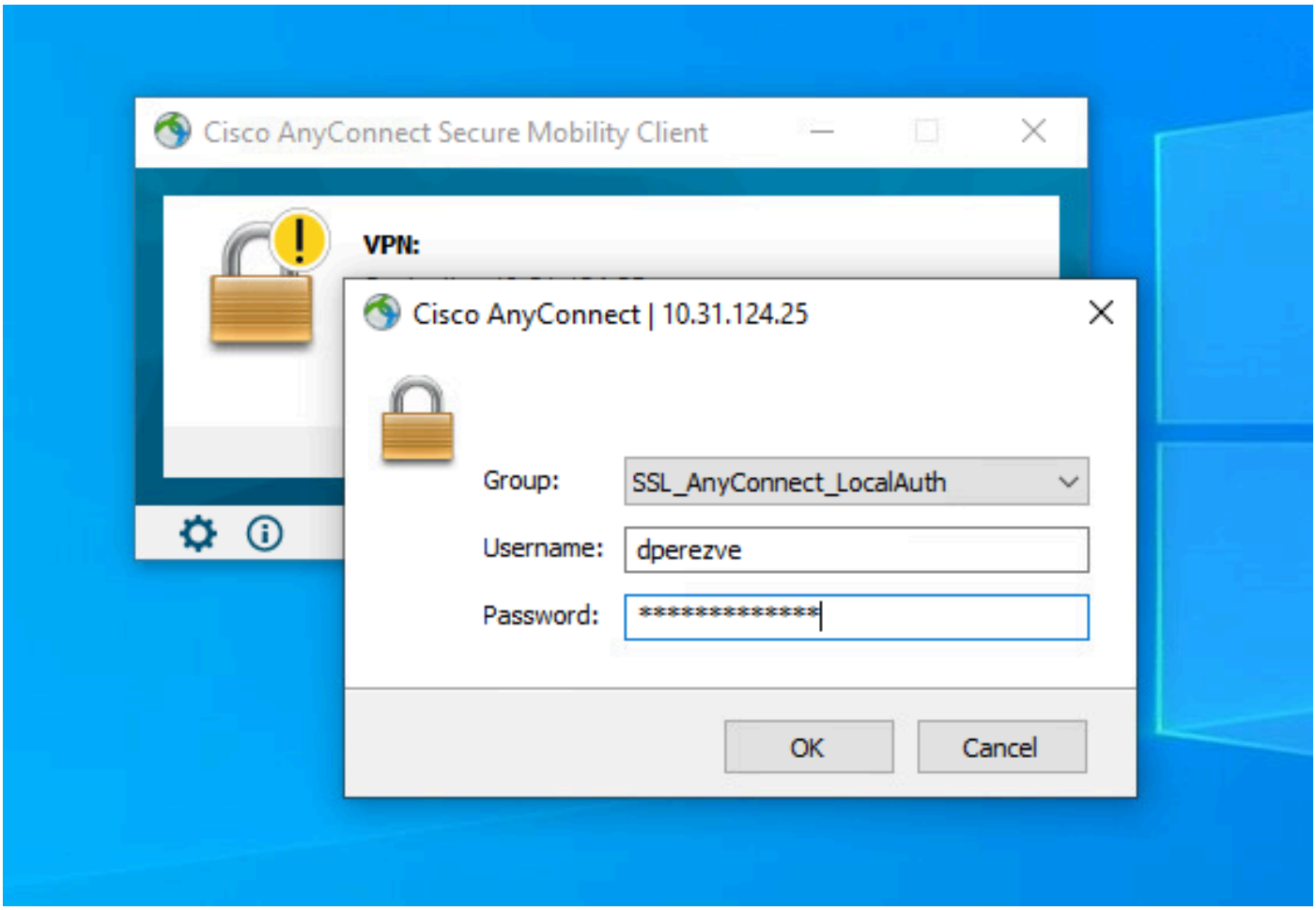


如果所有设置均正确，请单击Finish并将更改部署到FTD。

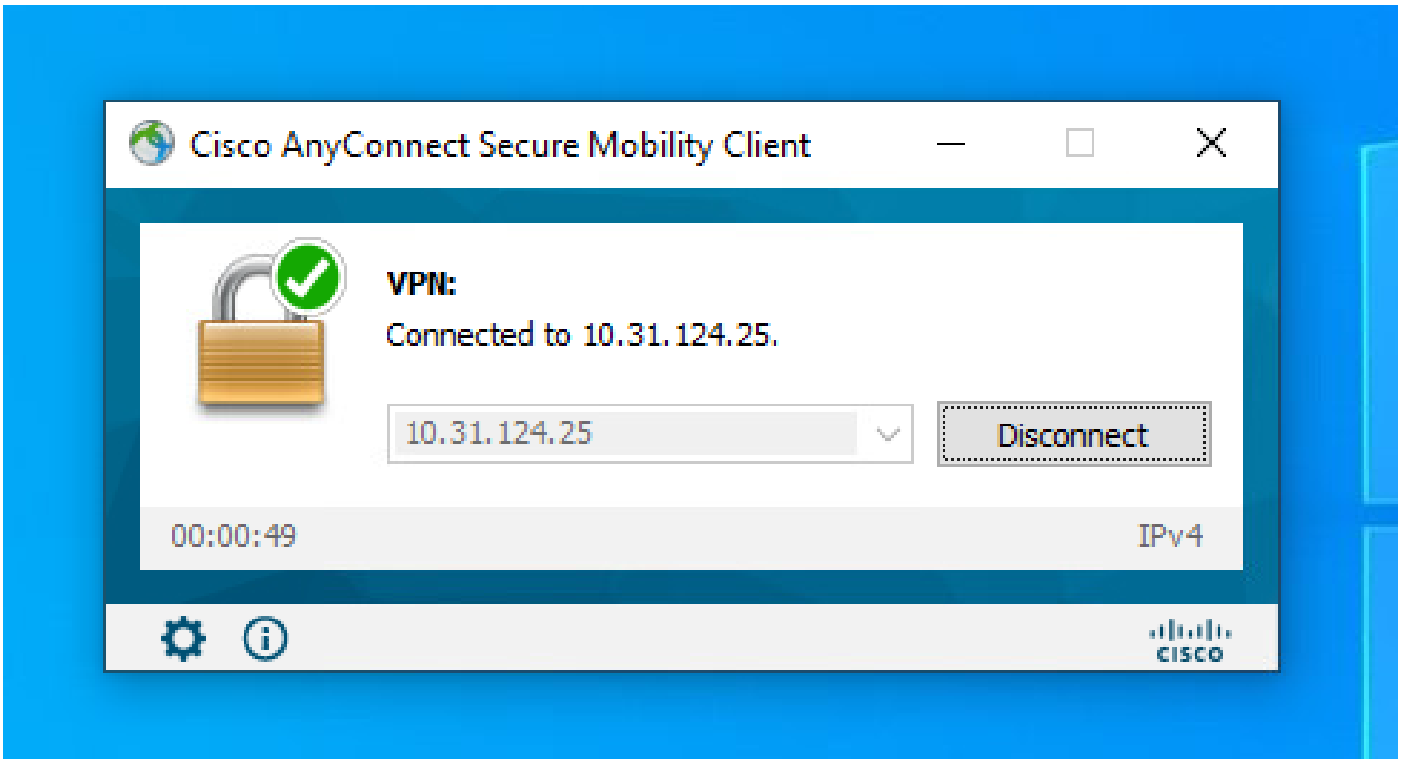


验证

部署成功后，启动Cisco AnyConnect安全移动客户端从Windows客户端到FTD的连接。身份验证提示中使用的用户名和密码必须与步骤4中创建的用户名和密码相同：



凭证通过FTD批准后，Cisco AnyConnect安全移动客户端应用必须显示连接状态：



从FTD中，可以运行show vpn-sessiondb anyconnect命令以显示防火墙上当前处于活动状态的Cisco安全客户端会话：

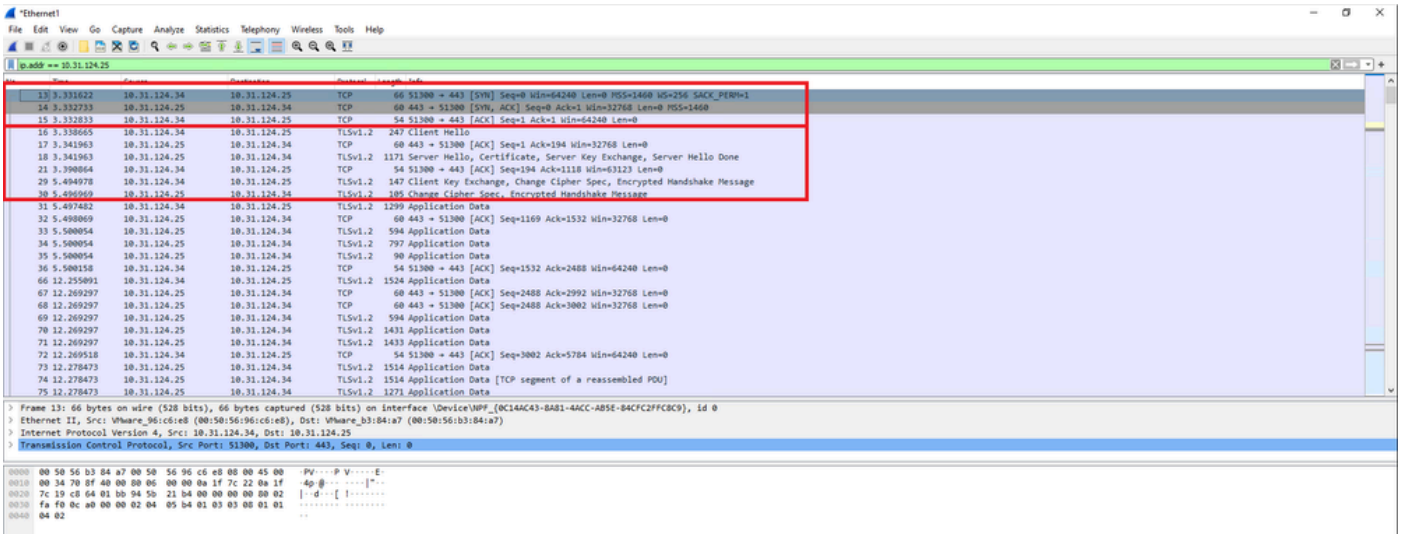
```
firepower# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : dperezve               Index        : 8
Assigned IP  : 172.16.13.1            Public IP    : 10.31.124.34
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
Bytes Tx     : 15756                  Bytes Rx     : 14606
Group Policy : DfltGrpPolicy
Tunnel Group : SSL_AnyConnect_LocalAuth
Login Time   : 21:42:33 UTC Tue Sep 7 2021
Duration     : 0h:00m:30s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 00000000000080006137dcc9
Security Grp : none                   Tunnel Zone  : 0
```

故障排除

对FTD运行debug webvpn anyconnect 255命令，以查看FTD上的SSL连接流：

```
firepower# debug webvpn anyconnect 255
```

除Cisco安全客户端调试外，还可以使用TCP数据包捕获来观察连接流。这是成功连接的示例，Windows客户端和FTD之间定期完成三次握手，然后是用来同意密码的SSL握手。



在协议握手之后，FTD必须使用本地领域存储的信息验证凭证。

收集DART捆绑包，并联系思科TAC进行进一步研究。

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）。