

在FTD上配置使用本地身份验证的SSL安全客户端

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[配置](#)

[步骤1:验证许可](#)

[第二步：将思科安全客户端软件包上传到FMC](#)

[第三步：生成自签名证书](#)

[第四步：在FMC上创建本地领域](#)

[第五步：配置SSL Cisco安全客户端](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何在Cisco FMC管理的Cisco FTD上配置思科安全客户端（包括Anyconnect）和本地身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 通过Firepower管理中心(FMC)进行SSL安全客户端配置
- 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)版本7.0.0 (内部版本94)
- 思科FMC 7.0.0版 (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，或定义为主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。

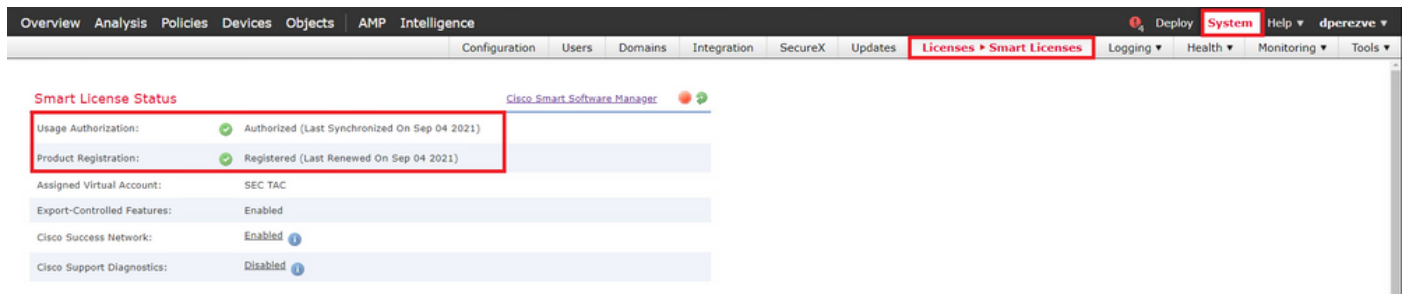
配置

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要求。如果FTD没有有效的Plus、Apex或仅VPN许可证，则无法部署Cisco安全客户端。

导航到System > Licenses > Smart Licenses，以验证FMC已注册且符合智能许可门户的要求。



在同一页面上向下滚动，在Smart Licenses图表底部，您可以看到不同类型的可用思科安全客户端(AnyConnect)许可证以及每个许可证所订用的设备。验证手头的FTD是否已按以下任何类别进行注册。

Smart Licenses

Filter Devices... Edit Performance Tier Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	✓			
Base (2)	✓			
Malware (2)	✓			
Threat (2)	✓			
URL Filtering (2)	✓			
AnyConnect Apex (2)	✓			
ftdv-dperezve 192.168.13.8 - Cisco Firepower Threat Defense for VMWare - v6.7.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
ftdvh-dperezve (Performance Tier: FTDv50 - Tiered) 192.168.13.9 - Cisco Firepower Threat Defense for VMWare - v7.0.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

Note: Container Instances of same blade share feature licenses

Activate Windows
Go to System in Control Panel to activate Windows.

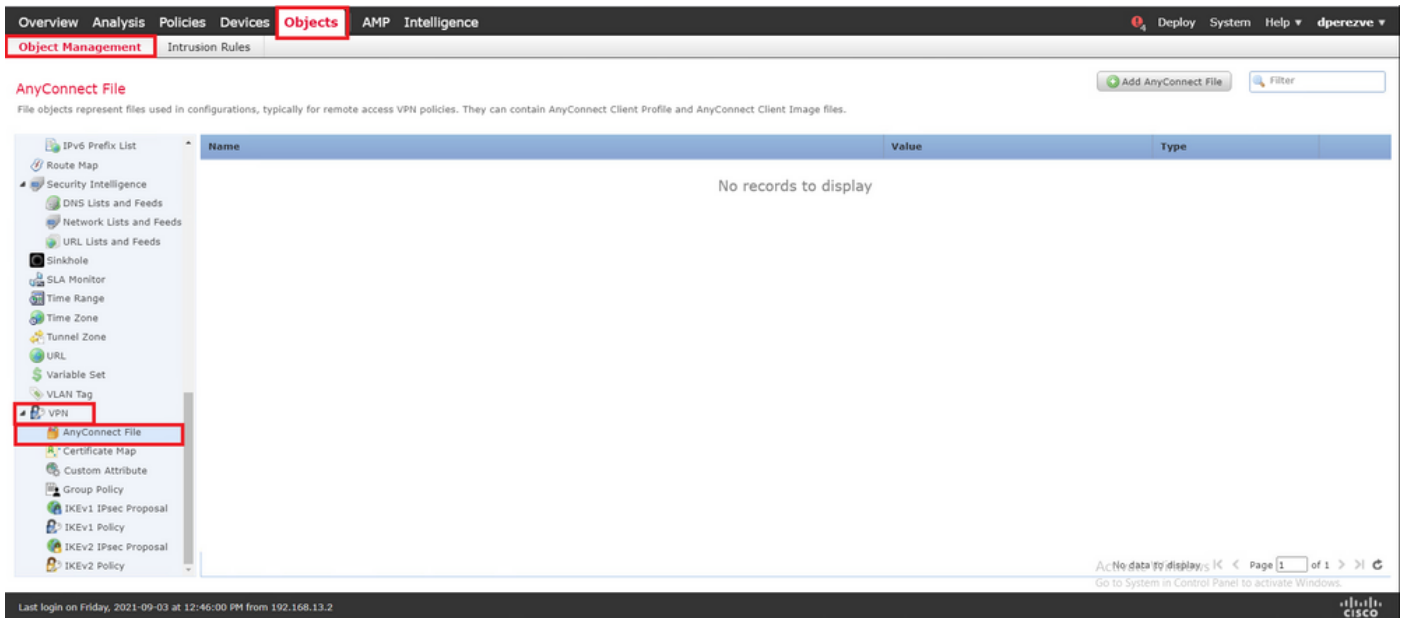
Last login on Saturday, 2021-09-04 at 14:26:07 PM from 192.168.13.2

第二步：将思科安全客户端软件包上传到FMC

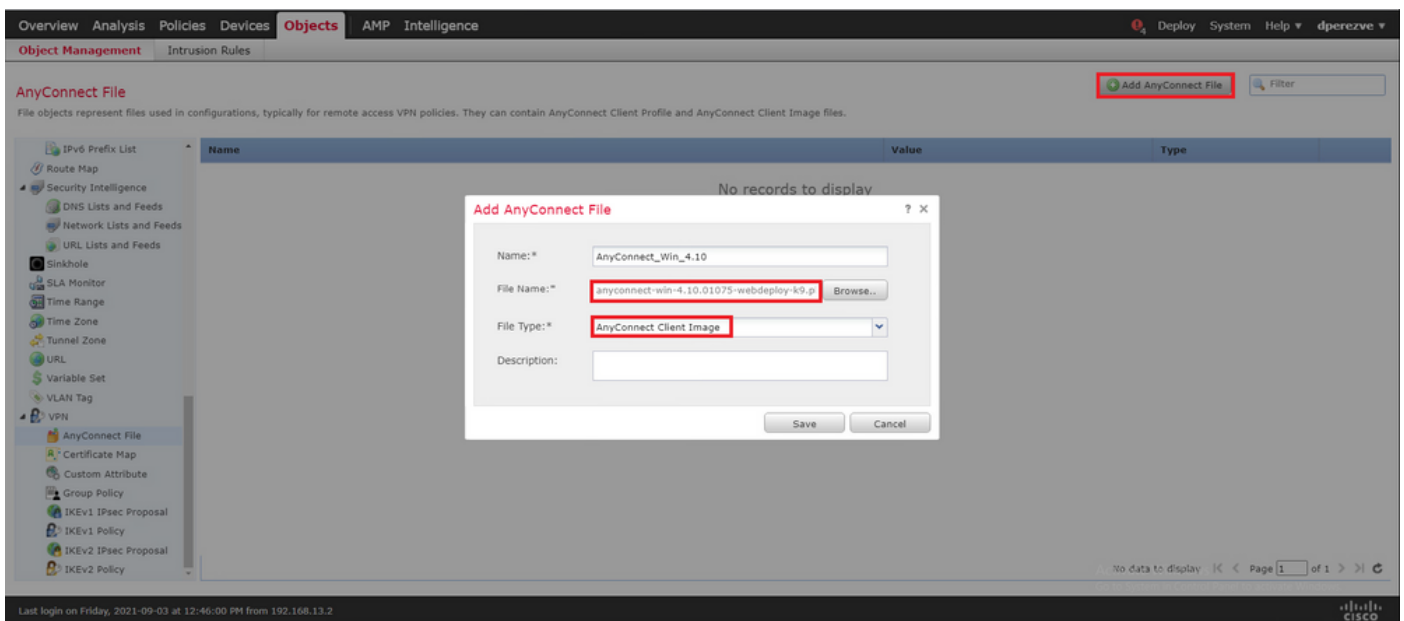
从 cisco.com 下载适用于Windows的Cisco安全客户端(AnyConnect)头端部署包。

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

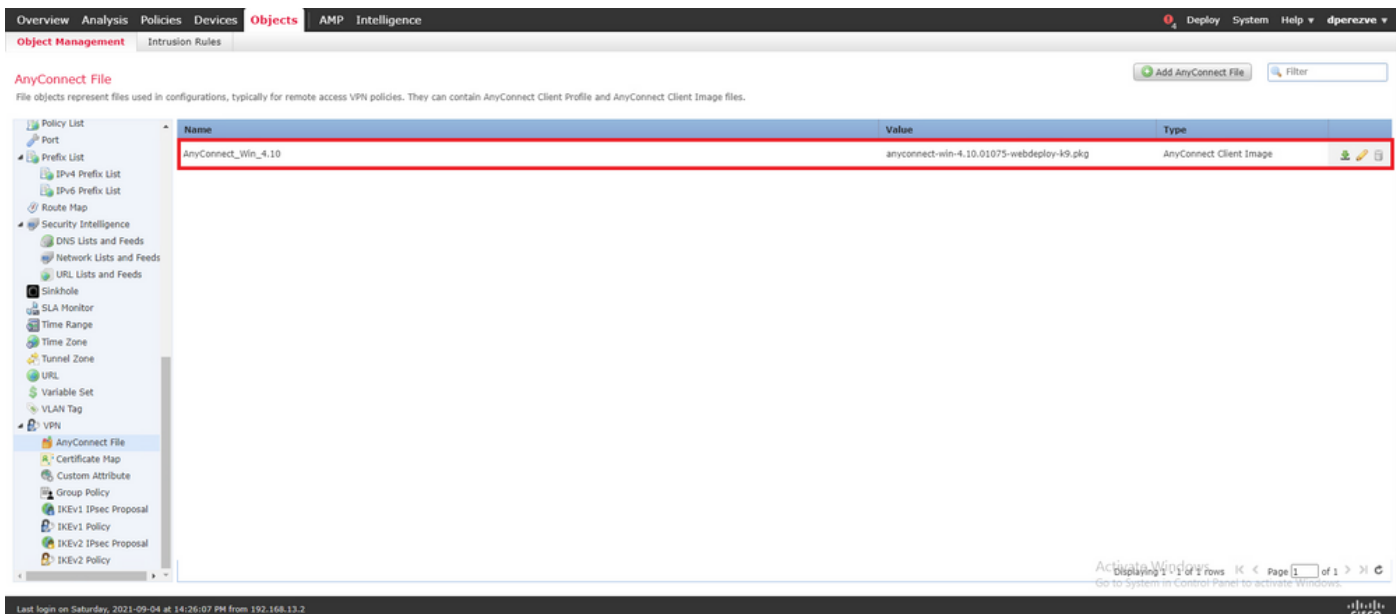
要上传Cisco Secure Client映像，请导航到Objects > Object Management，然后在目录的VPN类别下选择Cisco Secure Client File。



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，并最终选择AnyConnect Client Image 作为下拉菜单中的文件类型。




选择Save按钮。必须将对象添加到对象列表中。



第三步：生成自签名证书

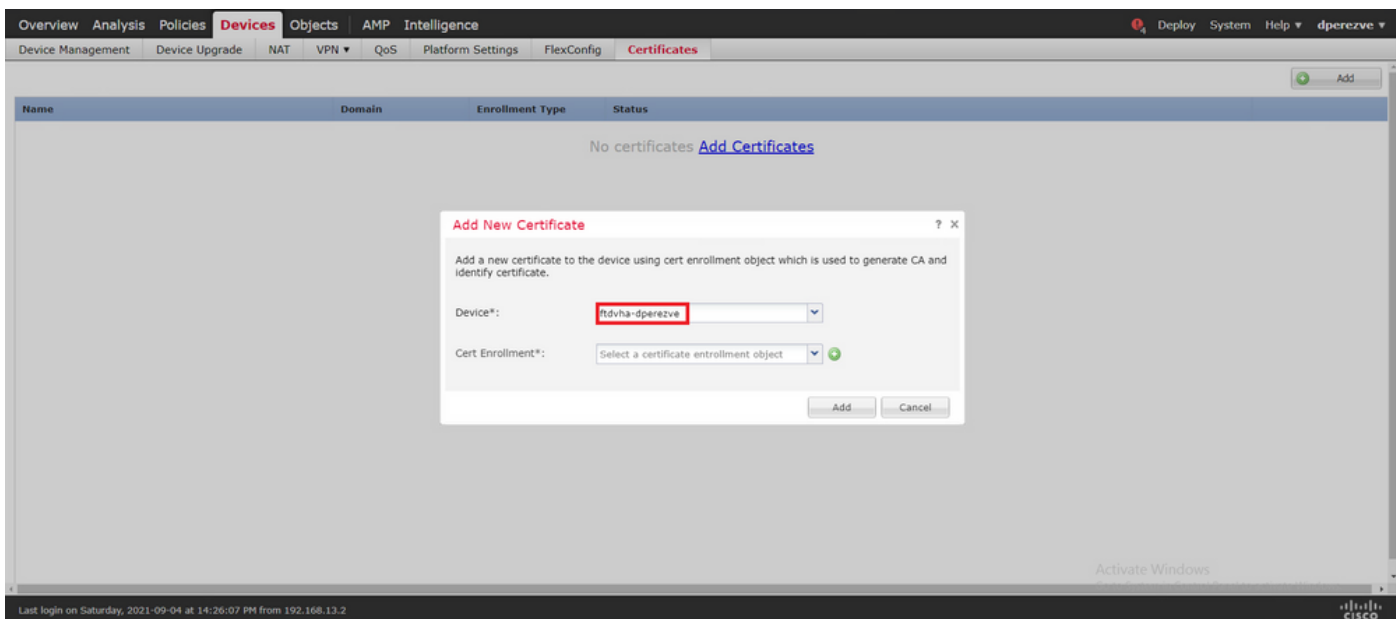
SSL思科安全客户端(AnyConnect)要求在VPN头端和客户端之间的SSL握手中使用一个有效证书。

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

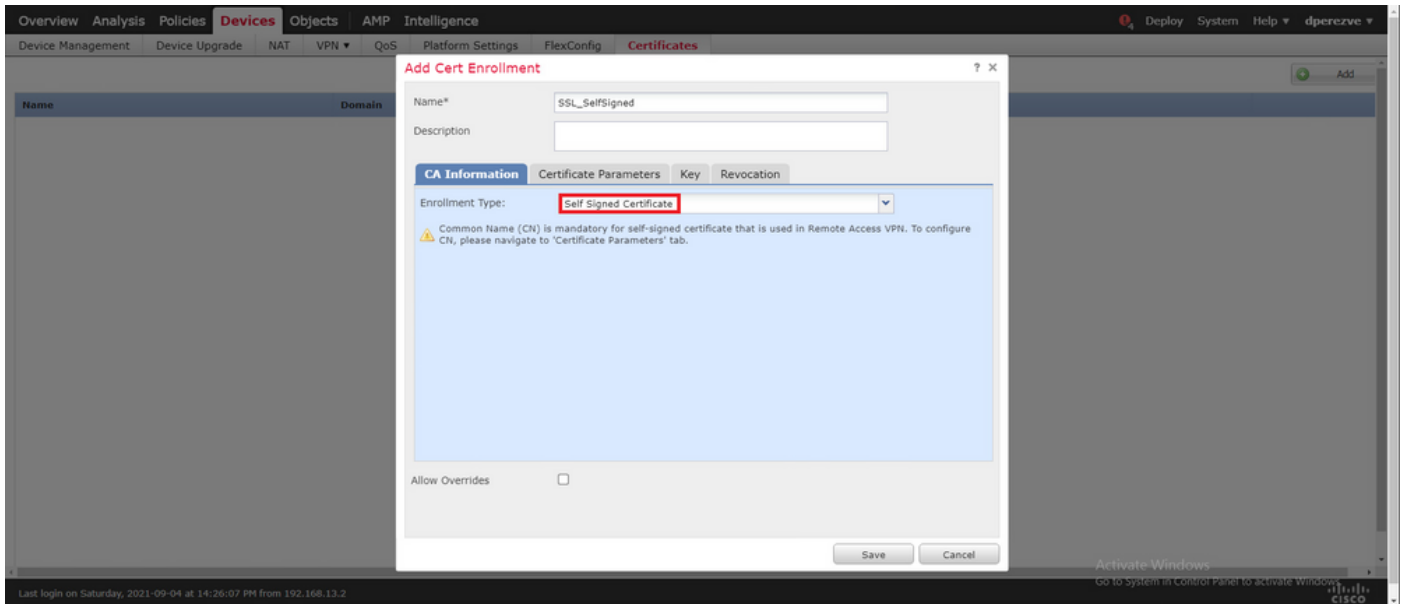
要创建自签名证书，请导航到设备>证书。



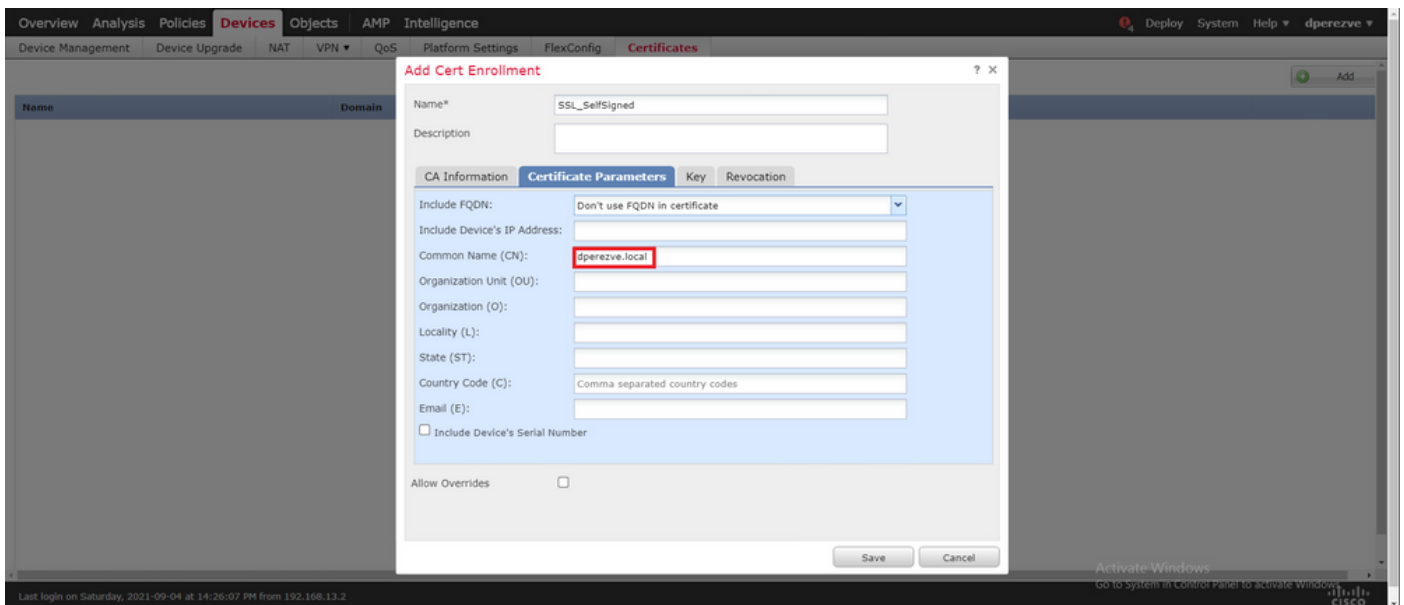
选择Add按钮。然后，在添加新证书窗口的设备下拉菜单中选择手头的FTD。



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，必须使用公用名(CN)。导航到证书参数选项卡以定义CN。

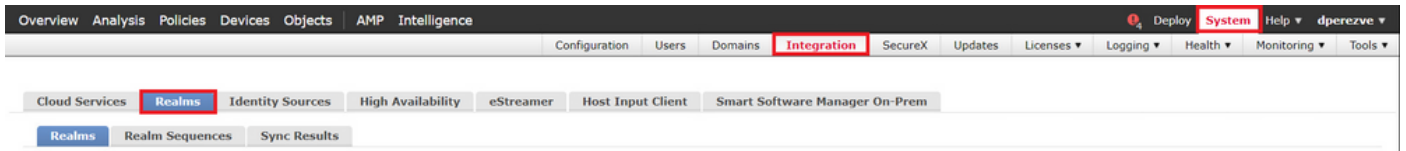


选择Save和Add按钮。几秒钟后，必须将新证书添加到证书列表中。

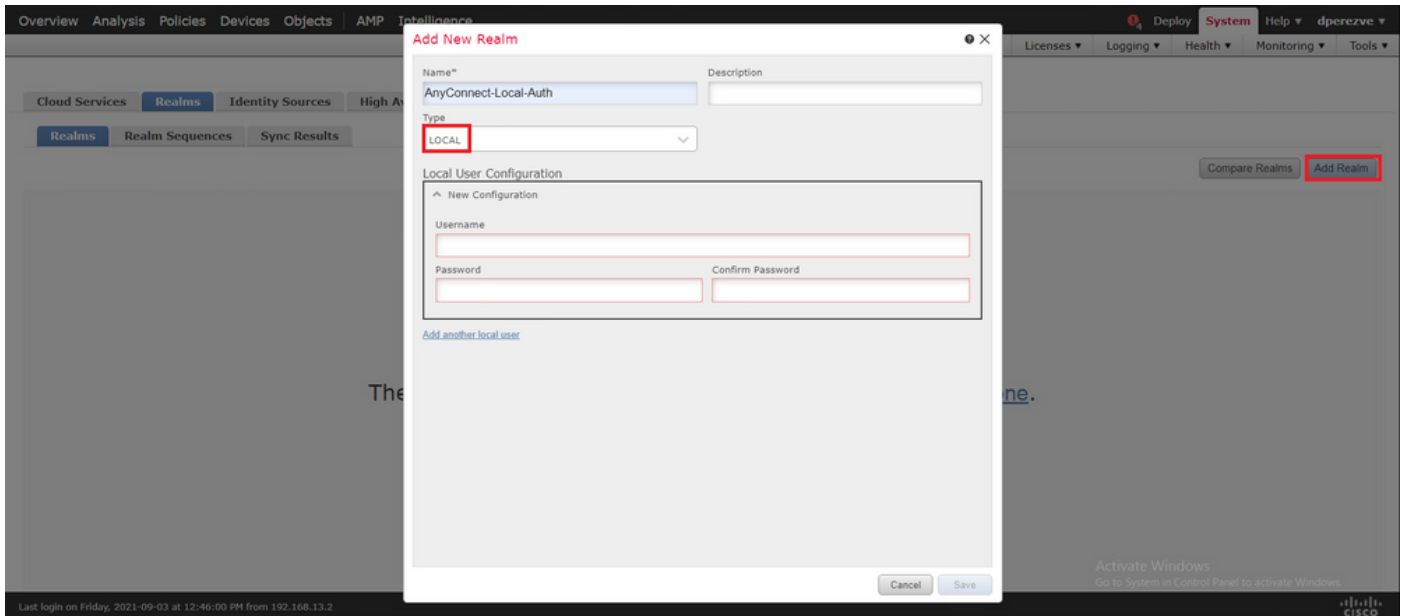


第四步：在FMC上创建本地领域


本地用户数据库和各自的密码存储在本地领域中。要创建本地领域，请导航到System > Integration > Realms。

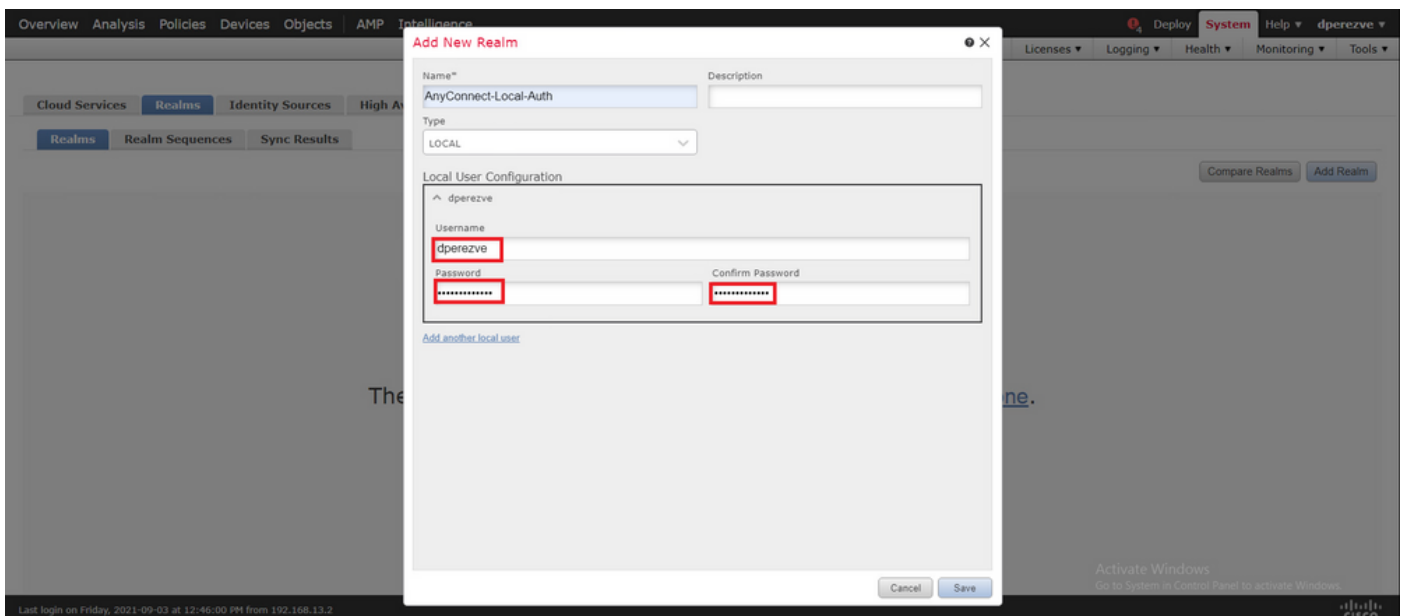


选择Add Realm按钮。在添加新领域窗口中，分配名称并在类型下拉菜单中选择LOCAL选项。

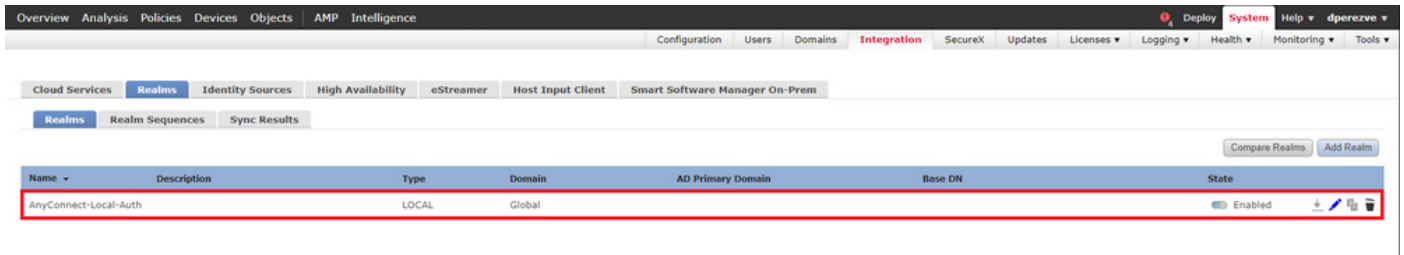


用户帐户和密码在Local User Configuration部分创建。

 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。

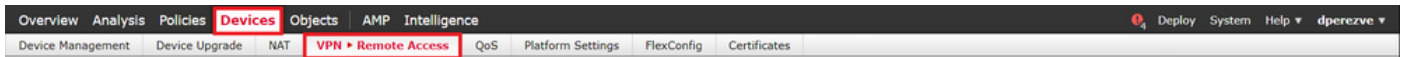


必须将保存更改和新领域添加到现有领域列表。

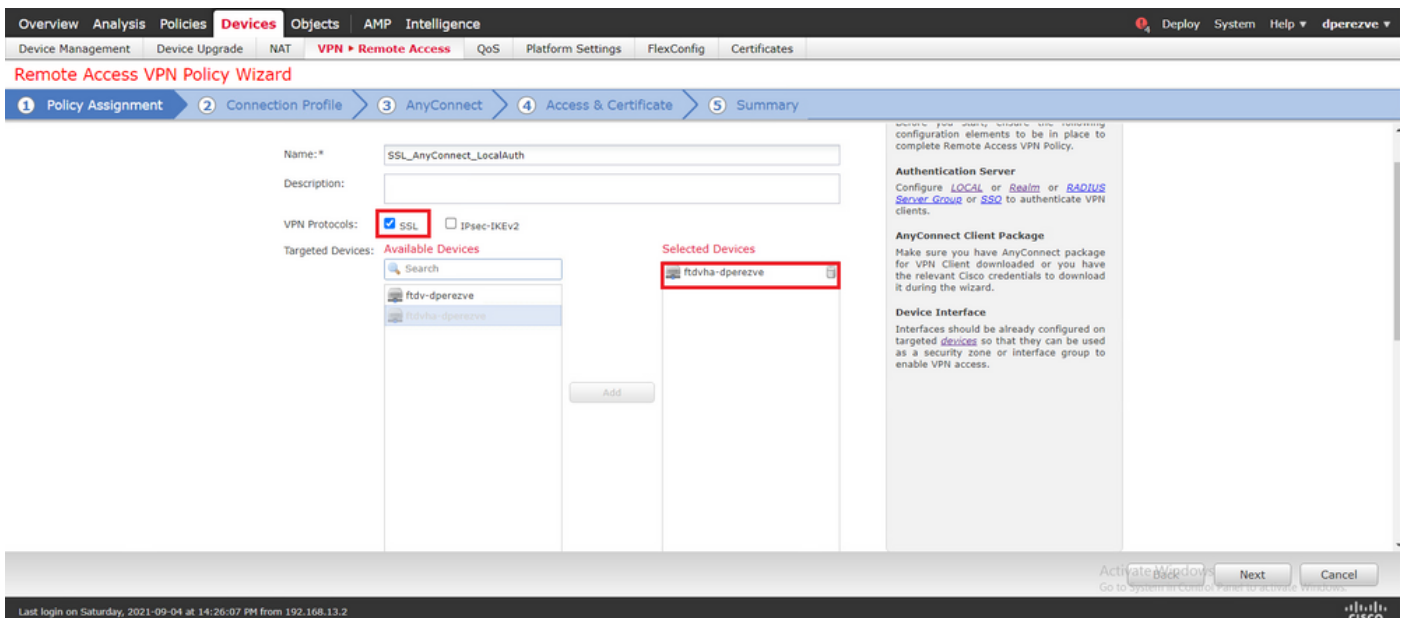


第五步：配置SSL Cisco安全客户端

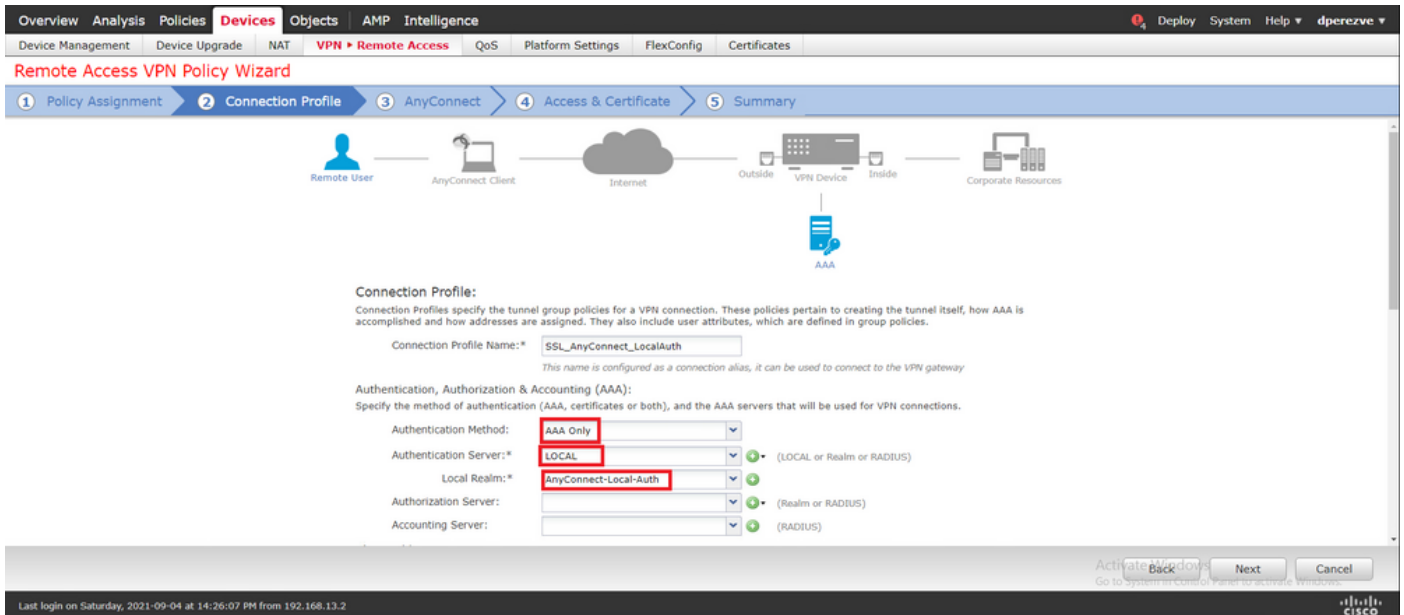
要配置SSL Cisco安全客户端，请导航到设备> VPN >远程访问。



选择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，然后选择手边的FTD作为目标设备。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。

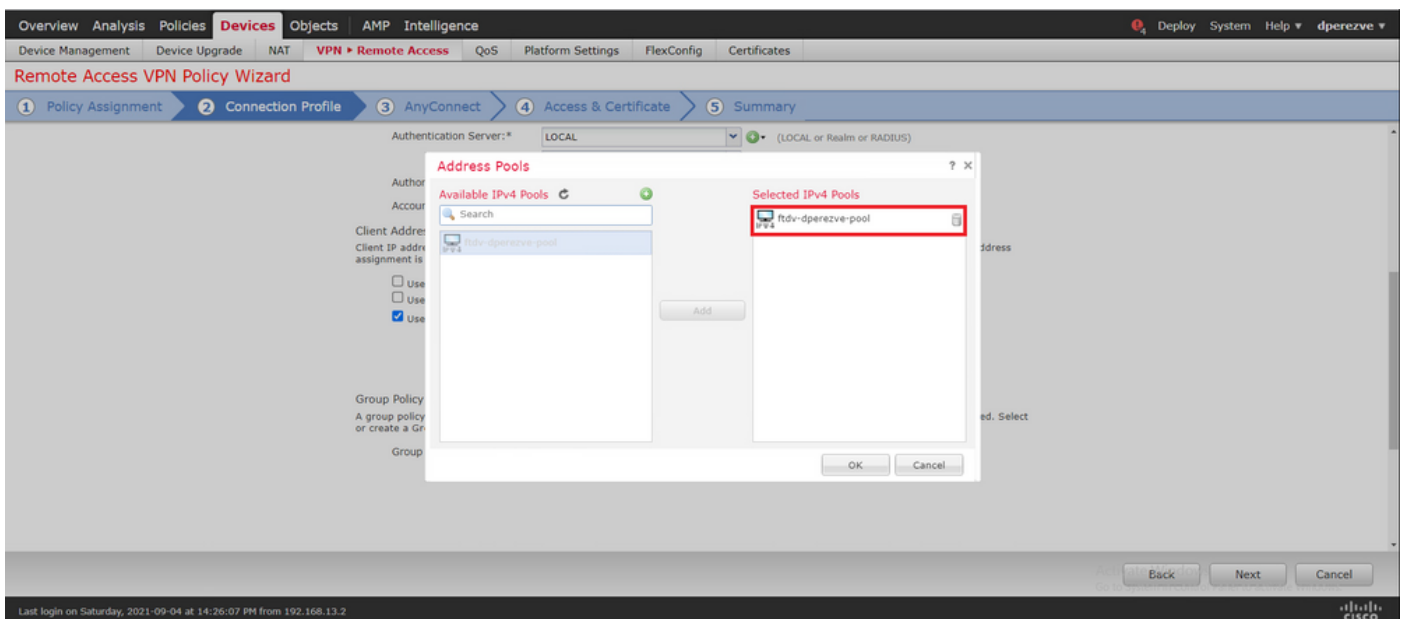


选择Next以转到Connection Profile配置。定义连接配置文件的名称，然后选择AAA Only作为身份验证方法。然后，在Authentication Server下拉菜单中，选择LOCAL，最后，在Local Realm下拉菜单中选择步骤4中创建的本地领域。

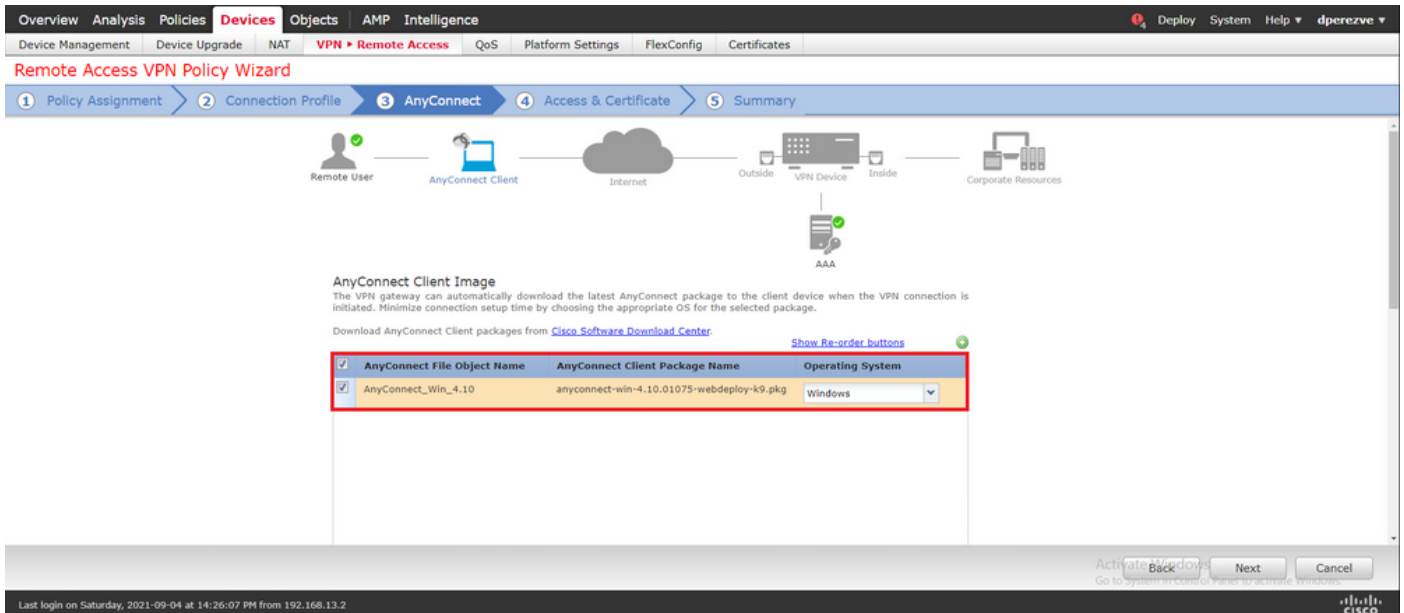


在同一页上向下滚动，然后在IPv4地址池部分中选择铅笔图标，以定义Cisco安全客户端使用的IP池

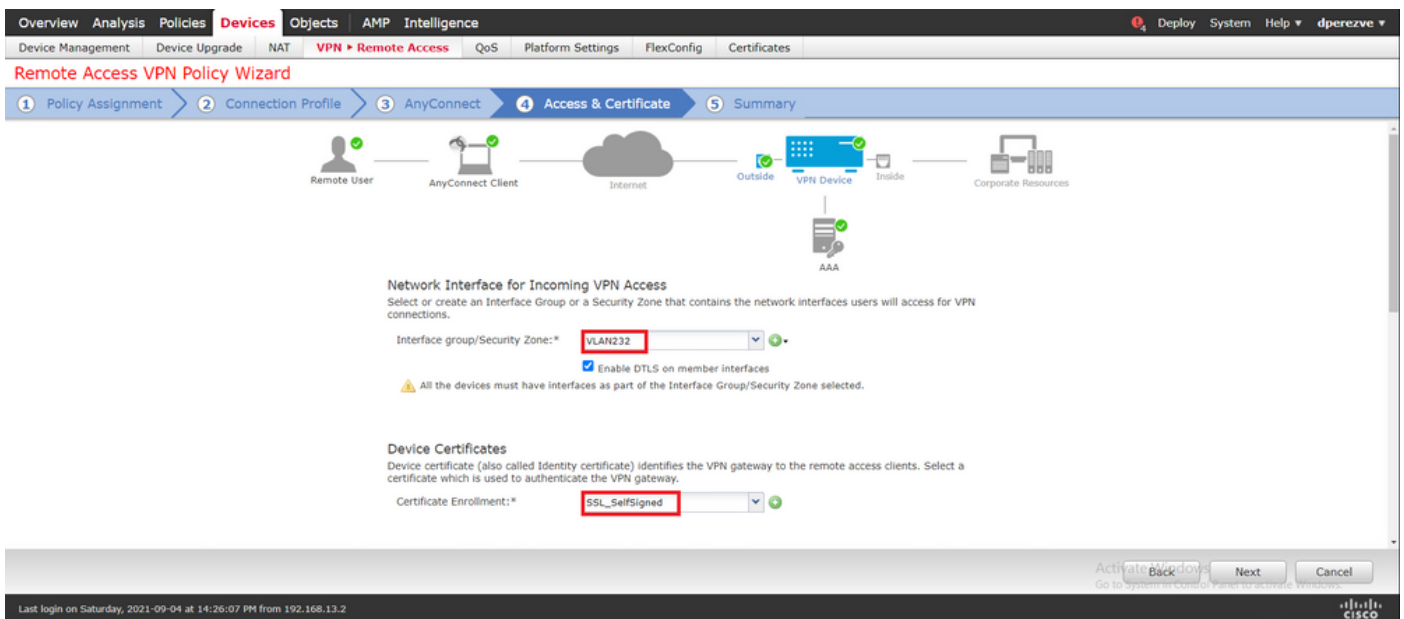
o



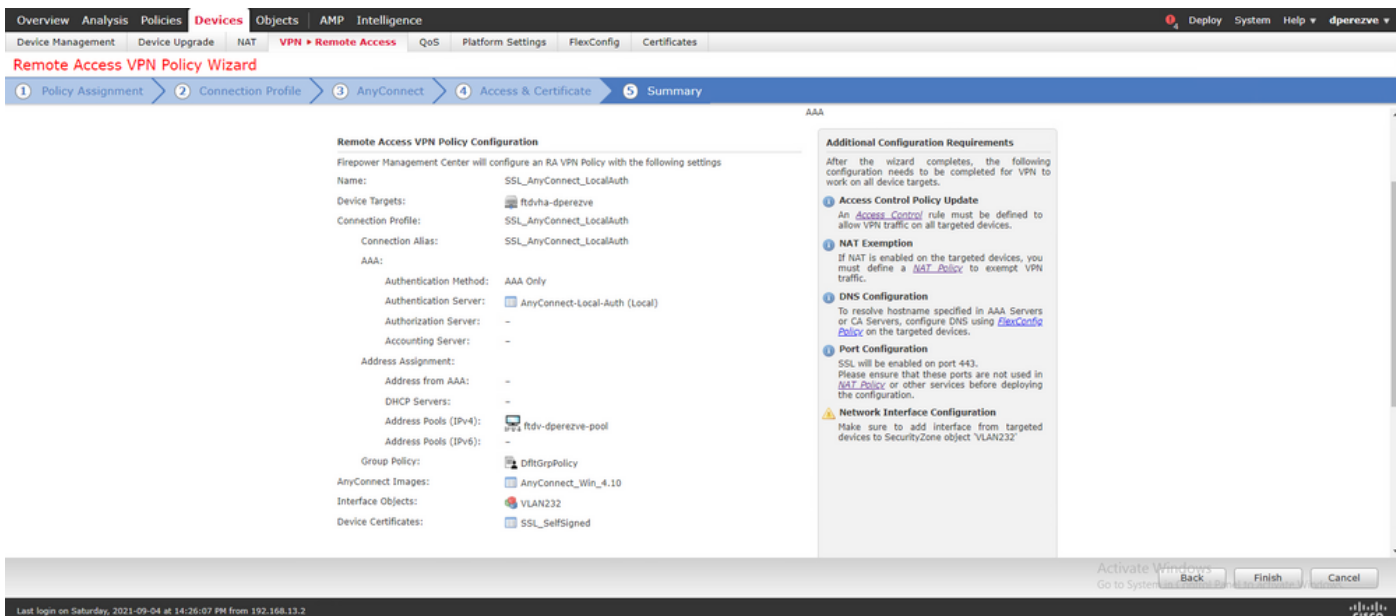
选择Next以转到AnyConnect部分。现在，请选择步骤2中上传的Cisco安全客户端映像。



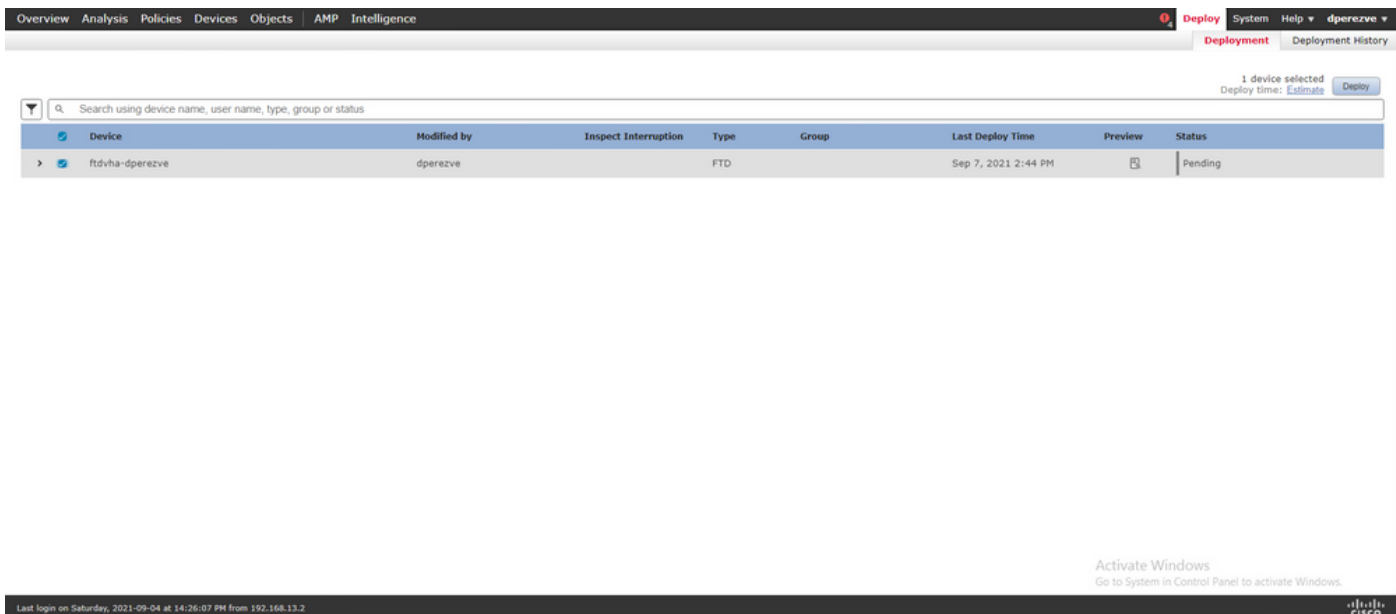
选择Next以转到Access & Certificate部分。在Interface group/Security Zone下拉菜单中，选择需要启用Cisco安全客户端(AnyConnect)的接口。然后，在Certificate Enrollment下拉菜单中，选择在第3步中创建的证书。



最后，选择Next以查看Cisco安全客户端配置的摘要。

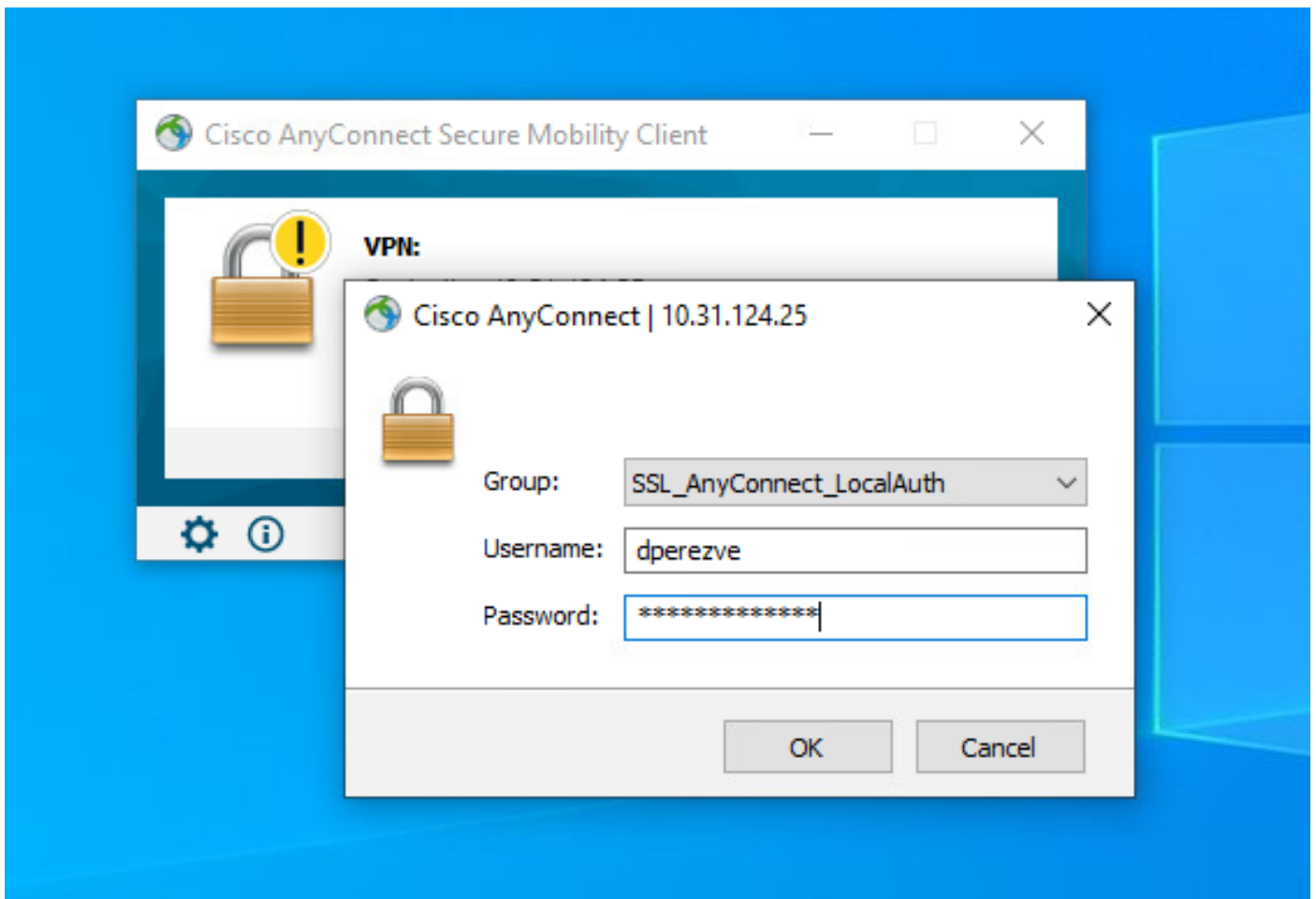


如果所有设置都正确，请选择Finish并将更改部署到FTD。

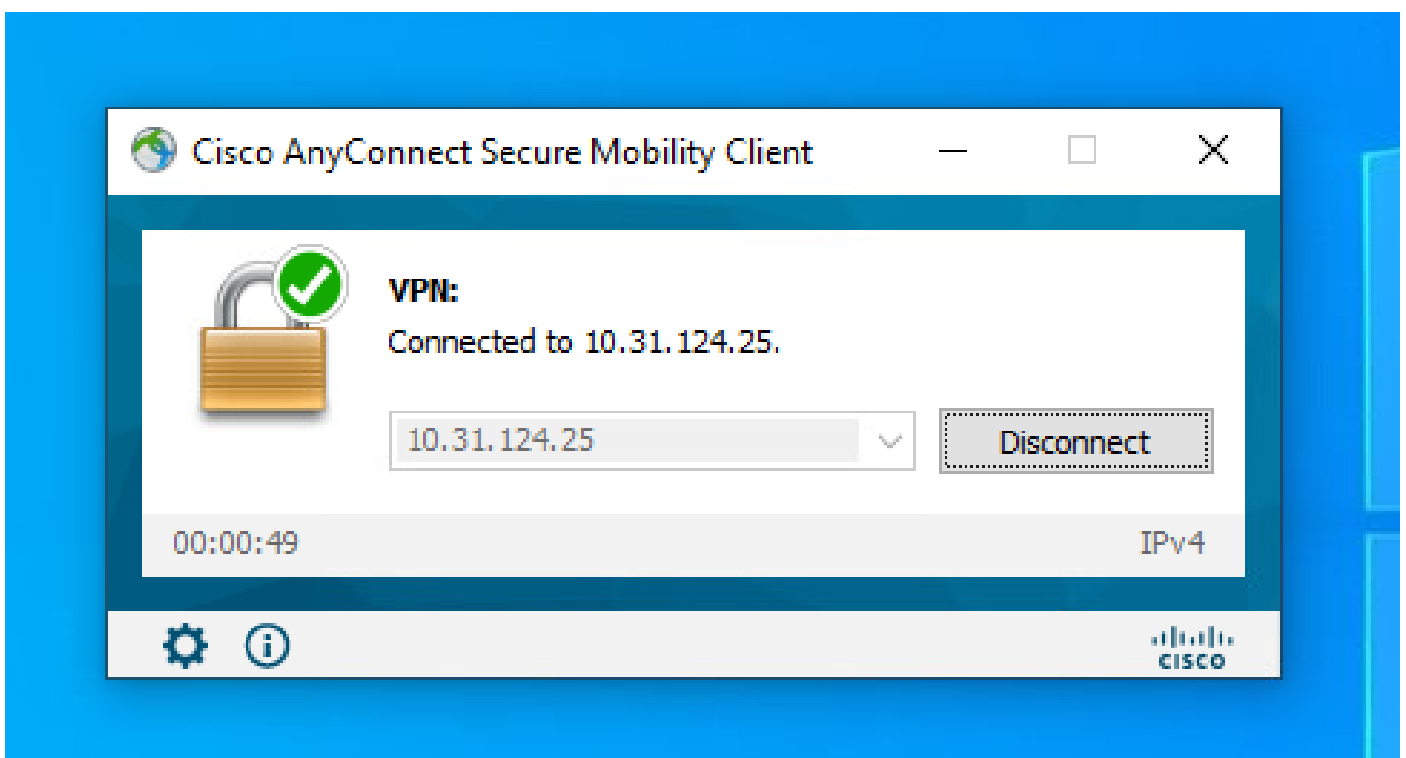


验证

部署成功后，启动从Windows客户端到FTD的Cisco AnyConnect安全移动客户端连接。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。



FTD批准凭证后，Cisco AnyConnect安全移动客户端应用必须显示已连接状态。



在FTD中，您可以运行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

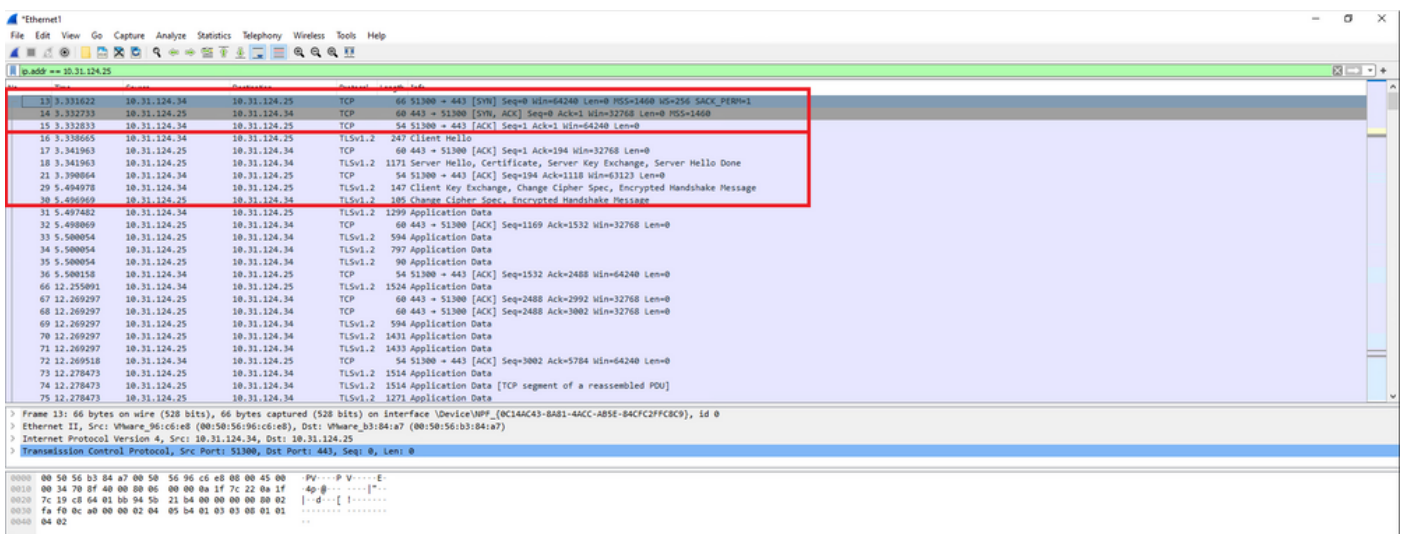
```
Username      : dperezve          Index       : 8
Assigned IP   : 172.16.13.1      Public IP   : 10.31.124.34
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
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  : 00000000000080006137dccc9
Security Grp  : none           Tunnel Zone : 0
```

故障排除

在FTD上运行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，还可以通过TCP数据包捕获观察连接流。这是一个成功连接的示例，Windows客户端和FTD之间定期完成三次握手，然后是用于约定密码的SSL握手。



协议握手后，FTD必须使用存储在本地领域中的信息验证凭证。

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）。