在FTD上配置SSL AnyConnect管理VPN

目录

简介

本文档介绍如何在由思科Firepower管理中心(FMC)管理的思科Firepower威胁防御(FTD)上配置Cisco AnyConnect管理隧道。 在下面的示例中，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)。

作者：思科TAC工程师Daniel Perez Vertti Vazquez。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco AnyConnect配置文件编辑器
- 通过FMC进行SSL AnyConnect配置。
- 客户端证书身份验证

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版本6.7.0（内部版本65）

- 思科FMC版本6.7.0（内部版本65）
- 安装在Windows 10计算机上的Cisco AnyConnect 4.9.01095

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

从版本6.7开始，思科FTD支持配置AnyConnect管理隧道。此修复先前打开的增强请求CSCvs78215。

AnyConnect管理功能允许在终端完成其启动后立即创建VPN隧道。用户无需手动启动AnyConnect应用，只要其系统通电，AnyConnect VPN代理服务就会检测管理VPN功能，并使用AnyConnect管理VPN配置文件的服务器列表中定义的主机条目启动AnyConnect会话。

限制

- 仅支持客户端证书身份验证。
- Windows客户端仅支持计算机证书存储区。
- Cisco Firepower设备管理器(FDM)CSCvx90058不支持。
- Linux客户端不支持。

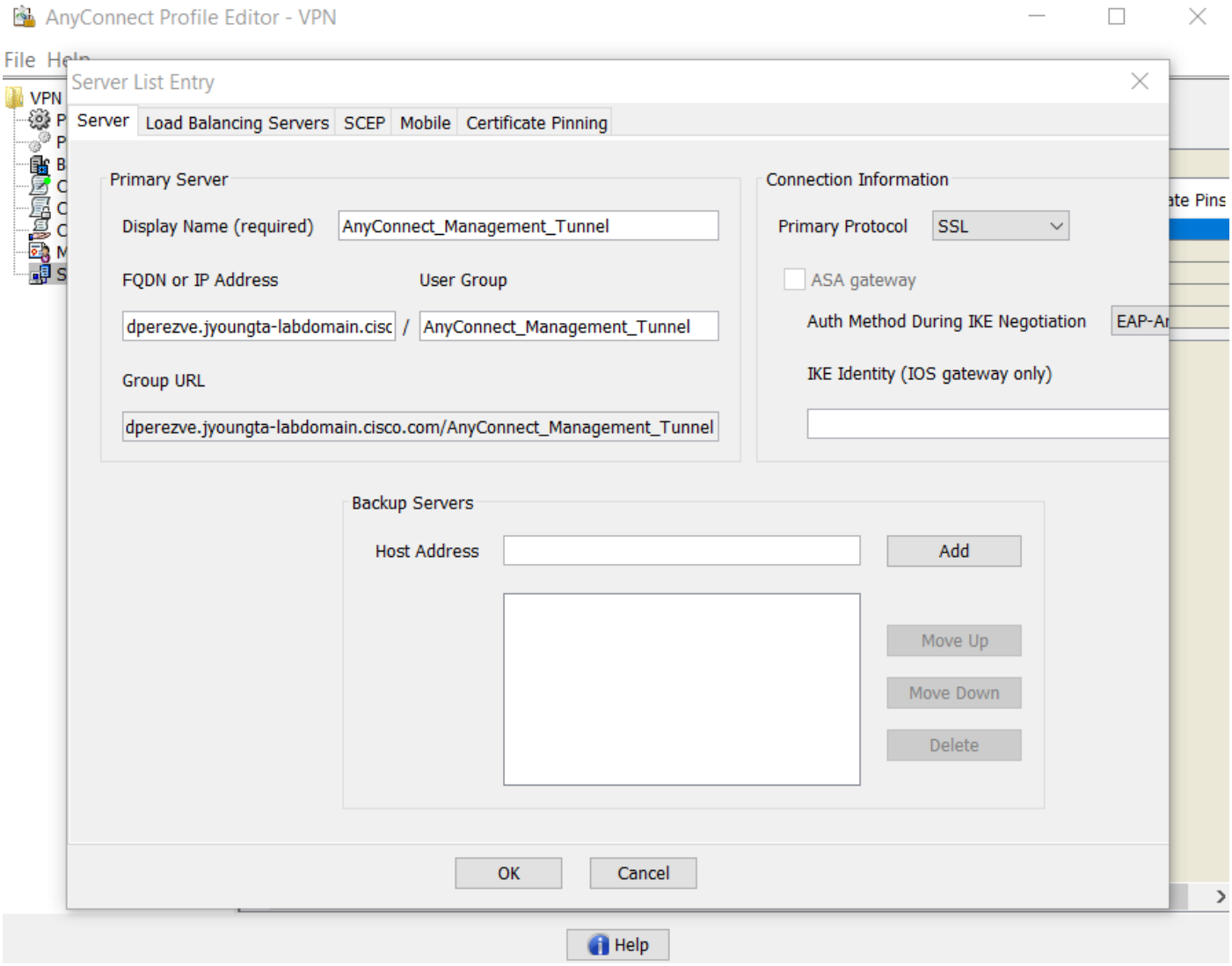
配置

配置

步骤1.创建AnyConnect管理VPN配置文件

打开AnyConnect配置文件编辑器以创建AnyConnect管理VPN配置文件。管理配置文件包含终端启动后用于建立VPN隧道的所有设置。

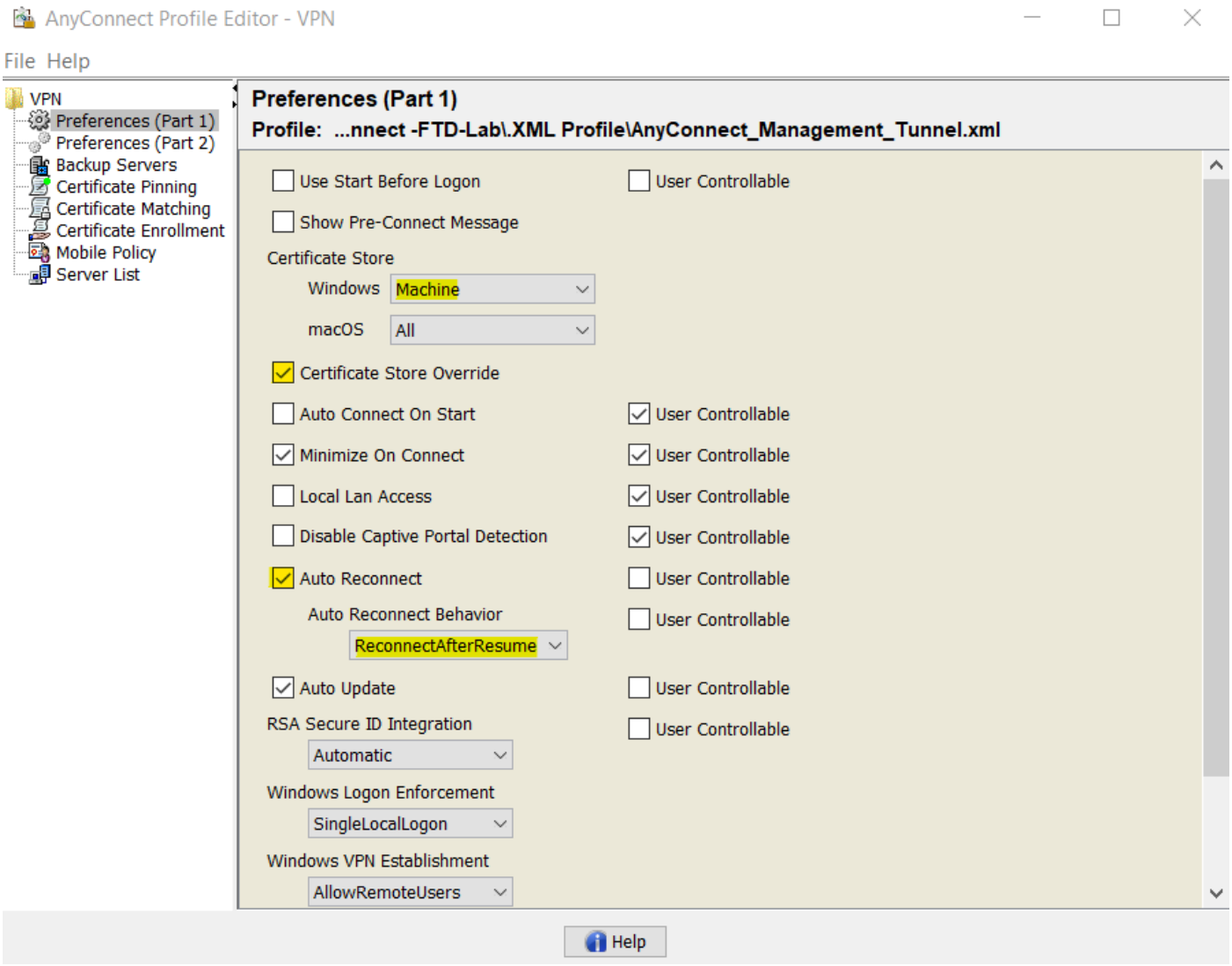
在本示例中，定义了指向完全限定域名(FQDN)dperezve.jyoungta-labdomain.cisco.com的服务器列表条目，并选择SSL作为主协议。要添加服务器列表，请导航到**服务器**列表并**选择**添加按钮，填写所需字段并保存更改。



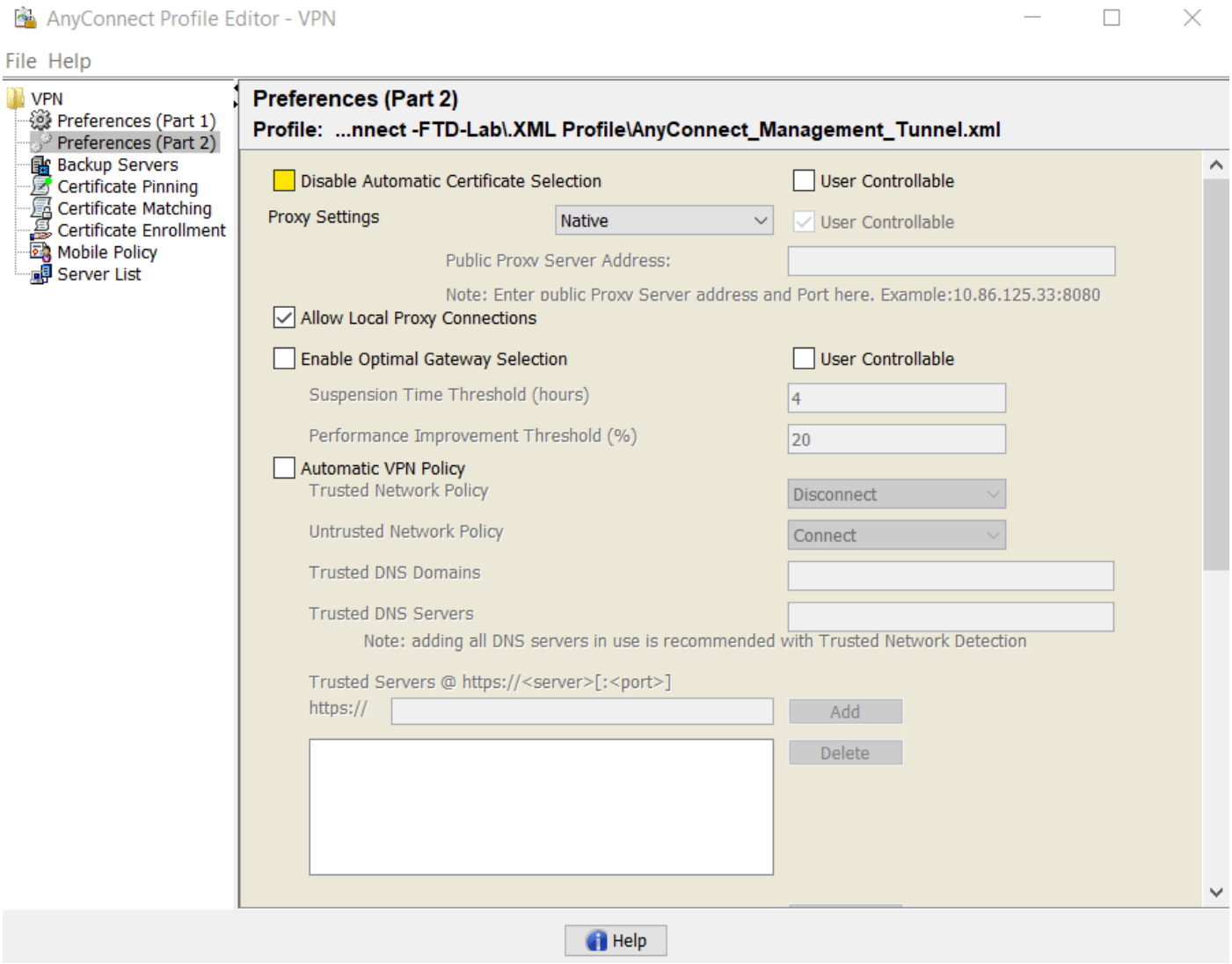
除服务器列表外，管理VPN配置文件还必须包含一些必需首选项：

- **AutomaticCertSelection**必须设置为**true**。
- **AutoReconnect**必须设置为**true**。
- **必须为**ReconnectAfterResume配置AutoReconnectBehavior。
- **自动更**新必须设置为**false**。
- **BlockUntrustedServers**必须设置为**true**。
- **必须为**MachineStore配置**CertificateStore**。
- **CertificateStoreOverride**必须设置为**true**。
- **必须将EnableAutomaticServerSelection**设置为**false**。
- **EnableScripting**必须设置为**false**。
- **RetainVPNOnLogoff**必须设置为**true**。

在AnyConnect配置文件编辑器中，导航至**“首选项（第1部分）”**并调整设置，如下所示：



然后导航至“首**选项（第2部分）”，并取**消选中“**禁用自动证书选**择”选项。



步骤2.创建AnyConnect VPN配置文件

除管理VPN配置文件外，还需要配置常规AnyConnect VPN配置文件。AnyConnect VPN配置文件用于首次连接尝试，在此会话期间从FTD下载管理VPN配置文件。

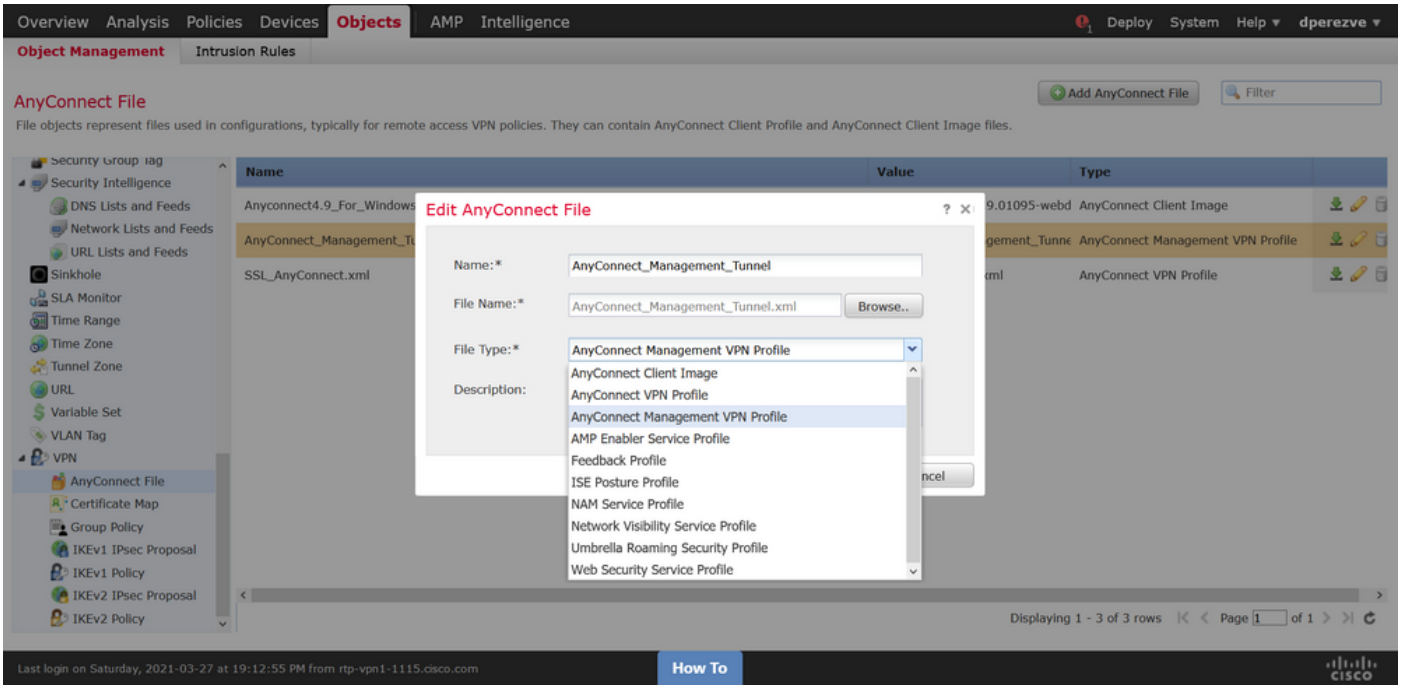
使用AnyConnect配置文件编辑器创建AnyConnect VPN配置文件。在这种情况下，两个文件都包含相同的设置，因此可以遵循相同的步骤。

步骤3.将AnyConnect管理VPN配置文件和AnyConnect VPN配置文件上传到FMC

创建配置文件后，下一步是将其作为AnyConnect文件对象上传到FMC。

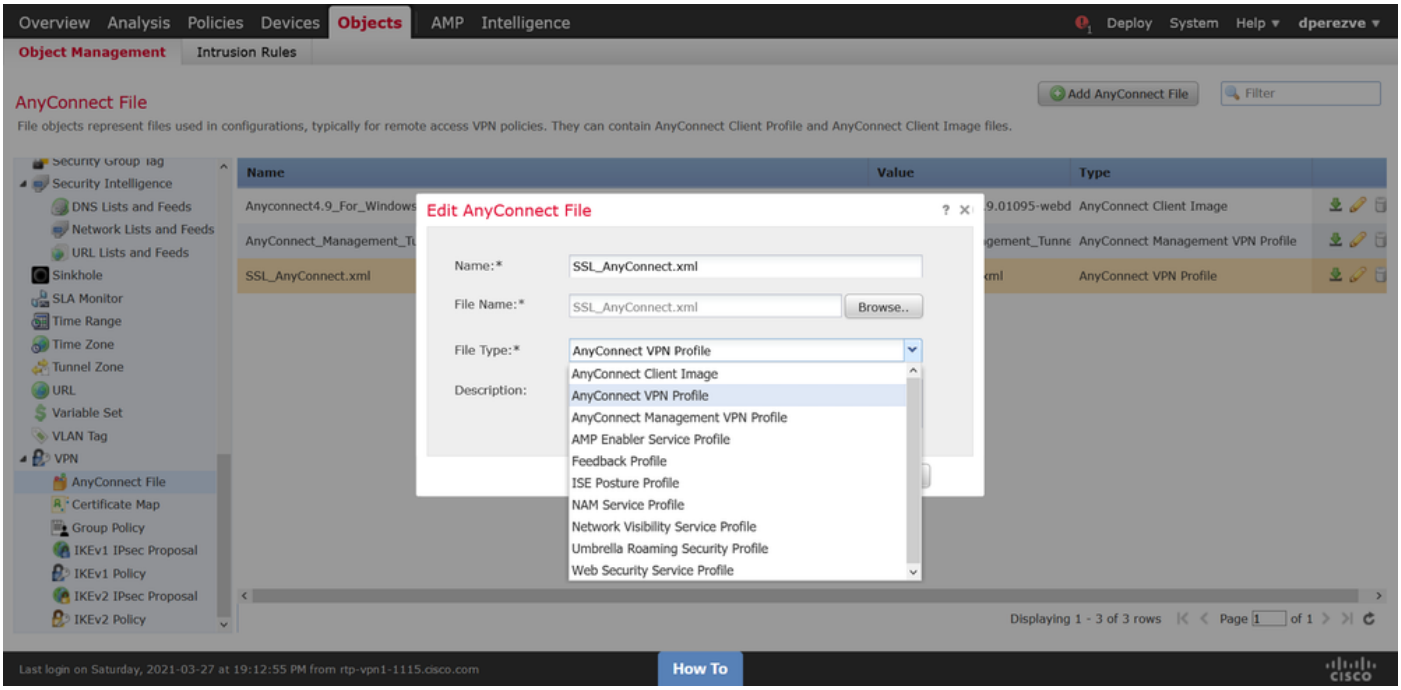
要将新的AnyConnect Management VPN配置文件上传到FMC，请导航到**Objects > Object Management**，然后从目录中选择**VPN** 选项，然后选择**Add AnyConnect File**按钮。

为文件提供名称，选择AnyConnect Management VPN Profile**作为文**件类型并保存对象。

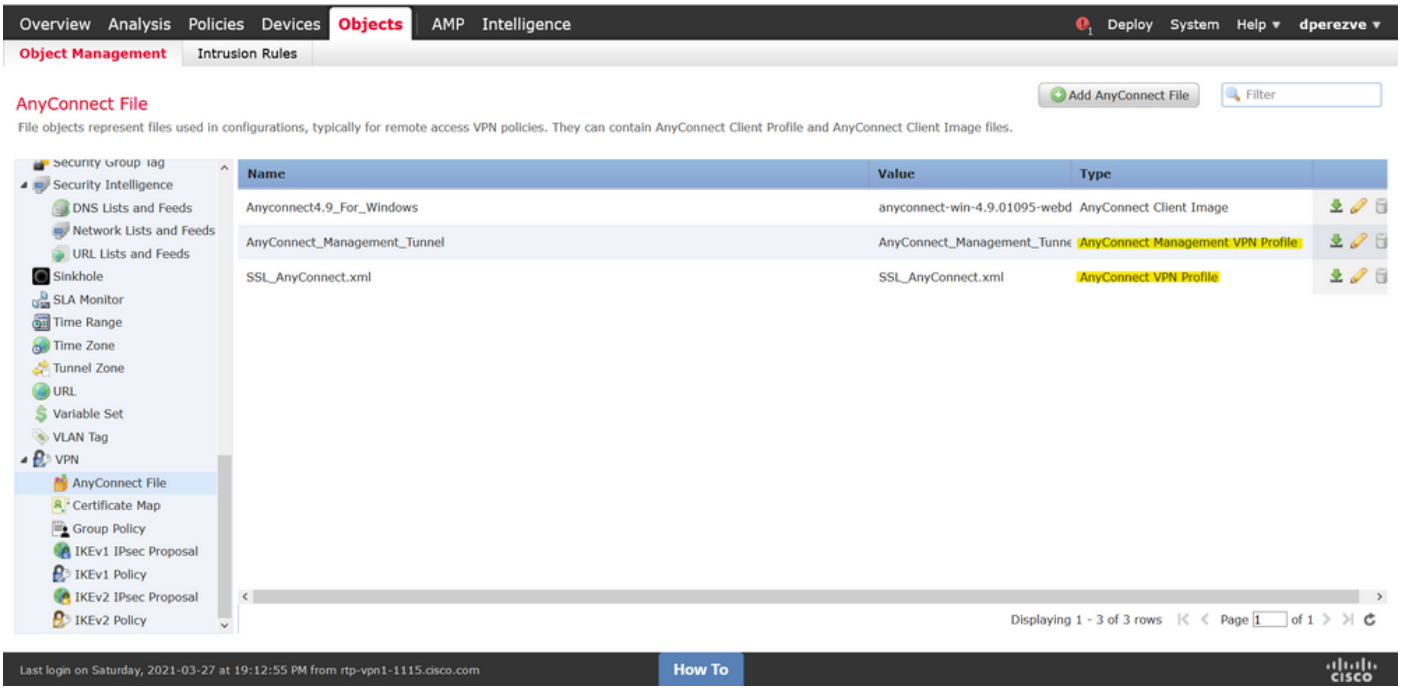


现在，要上传AnyConnect VPN配置文件，请再次导航到**Objects > Object Management**，然后从目录中选择**VPN**选项，然后选择**Add AnyConnect File**按钮。

为文件提供名称，但此时选择**AnyConnect VPN Profile**作为文件类型并保存新对象。



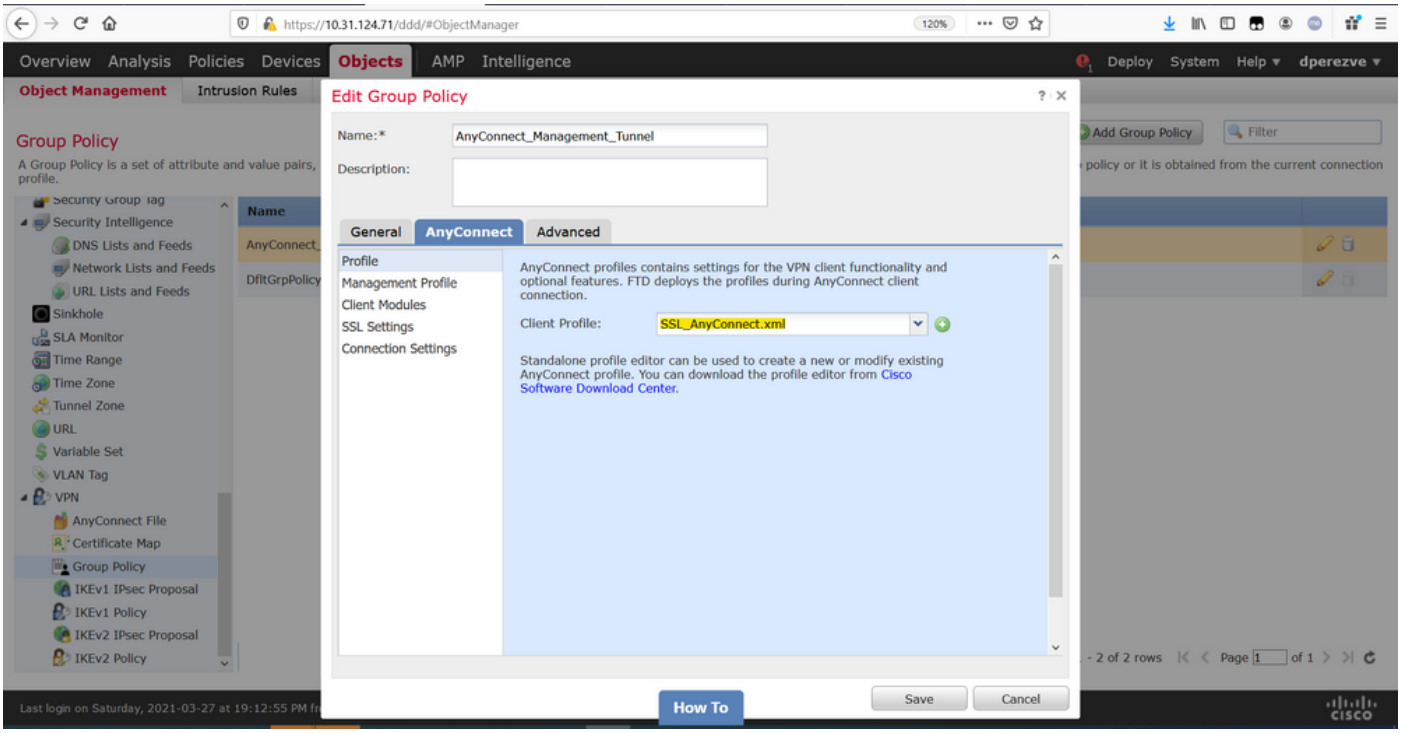
必须将配置文件添加到对象列表并分别标记为**AnyConnect Management VPN Profile和**AnyConnect VPN配**置文件**。



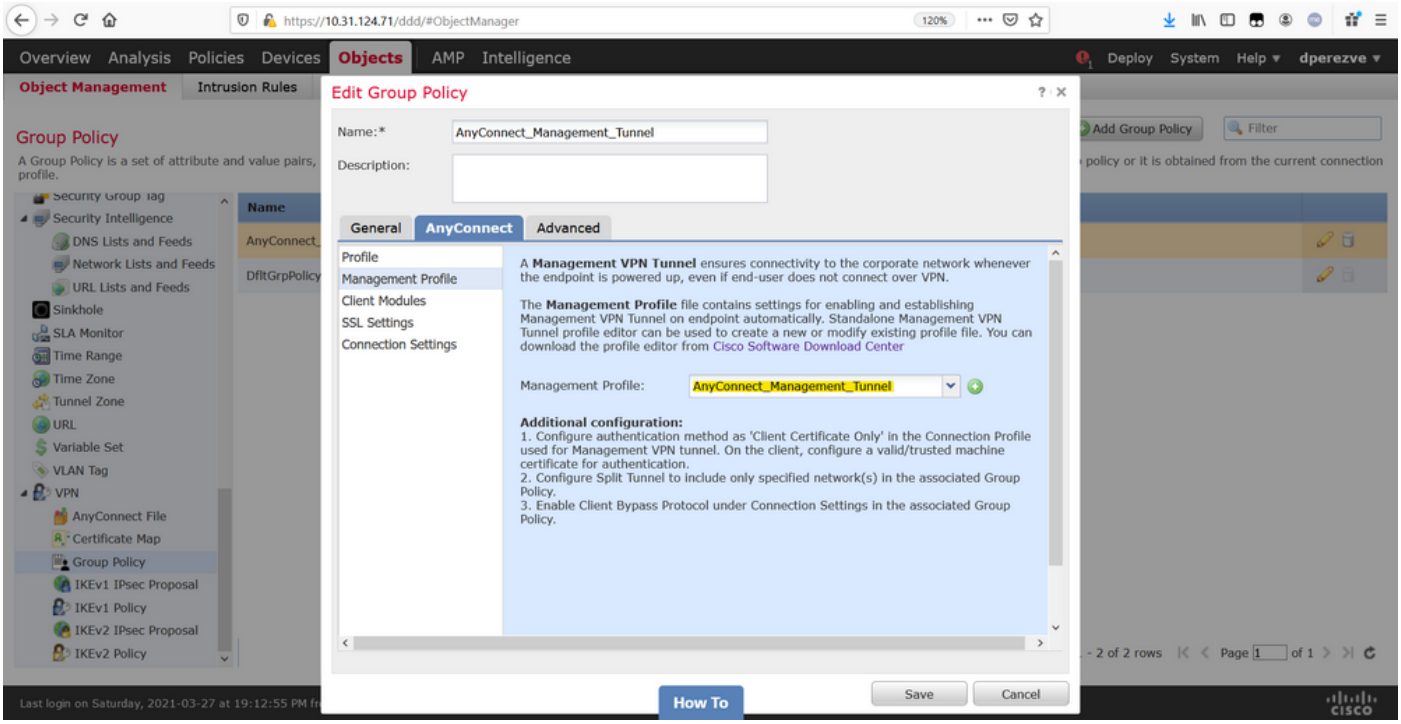
步骤4.创建组策略

要创建新组策略，请导航到**Objects > Object Management**并从目录中选择**VPN**选项，然后选择**Group Policy**并单击**Add Group Policy**按钮。

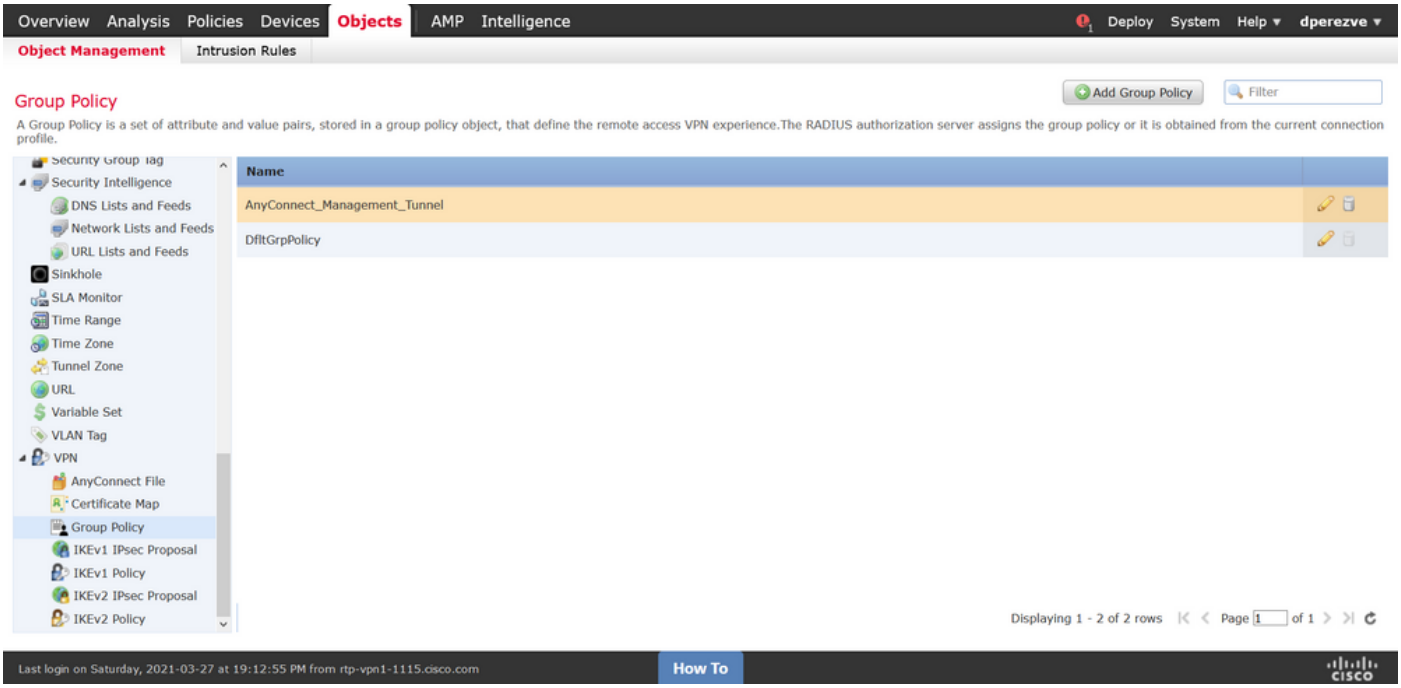
打开“**添加组策**略”窗口后，指定名称，定义AnyConnect池并打开“AnyConnect”**选项**卡。导航至**Profile**，并在Client Profile下拉菜单中选择表示常规AnyConnect VPN Profile**的对**象。



然后导航至**Management Profile选**项卡，并在Management Profile下拉菜单中选择包含**Management VPN Profile**的对象。



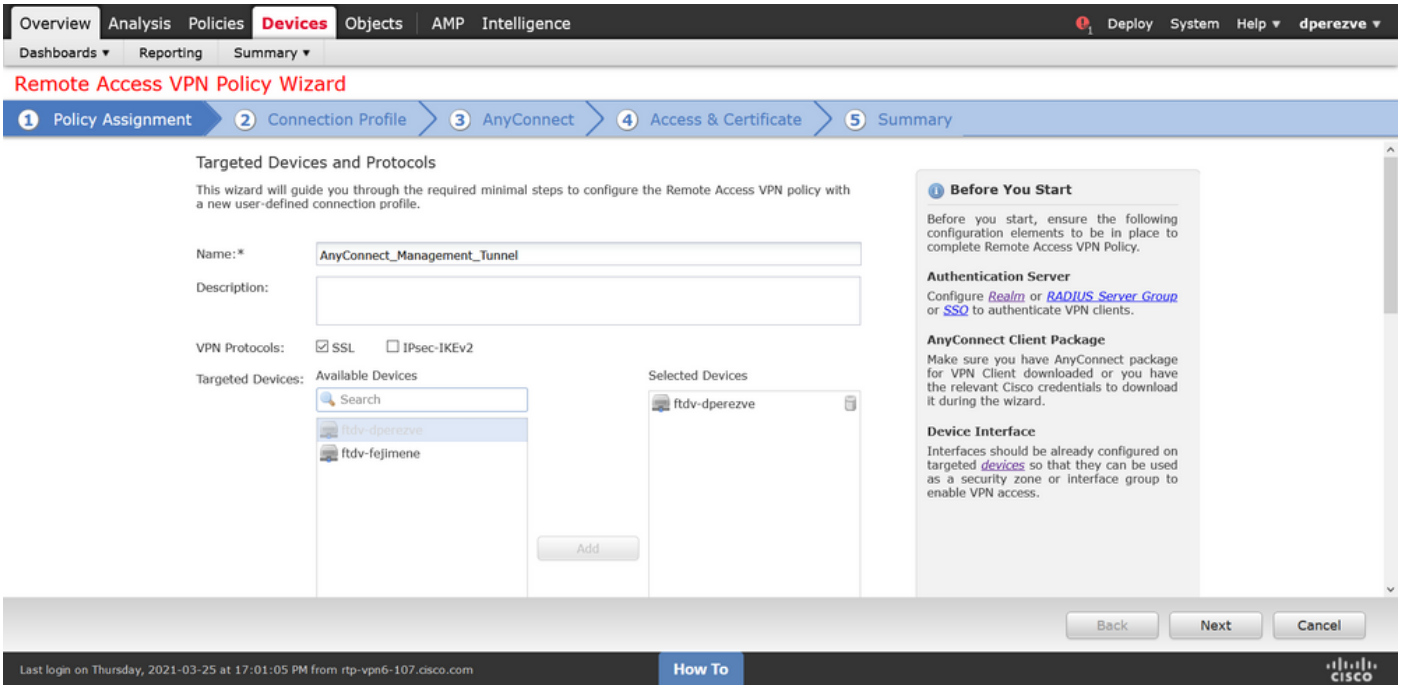
保存更改以将新对象添加到现有组策略。



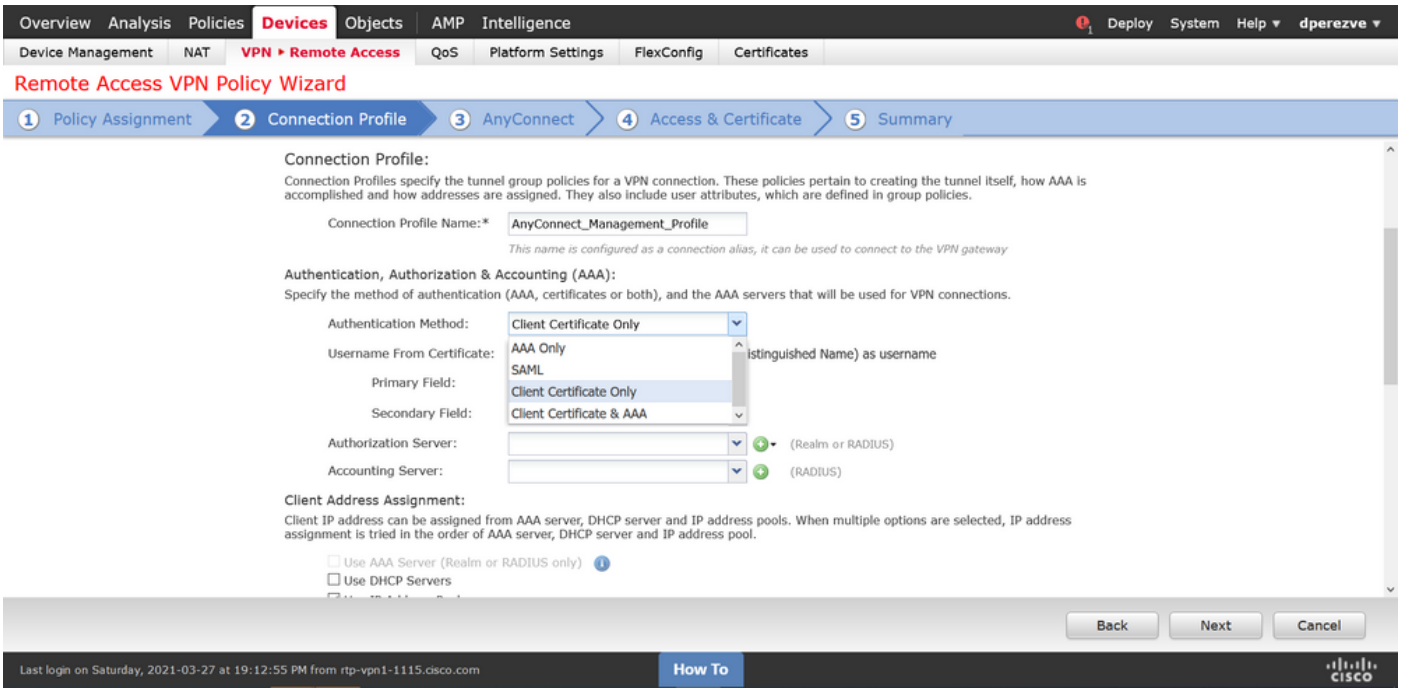
步骤5.创建新的AnyConnect配置

在FMC中配置SSL AnyConnect由4个不同步骤组成。要配置AnyConnect，请导航**到Devices > VPN > Remote Access**，然后选择**Add**按钮。这必须打开“**远程访问VPN策略向导**”。

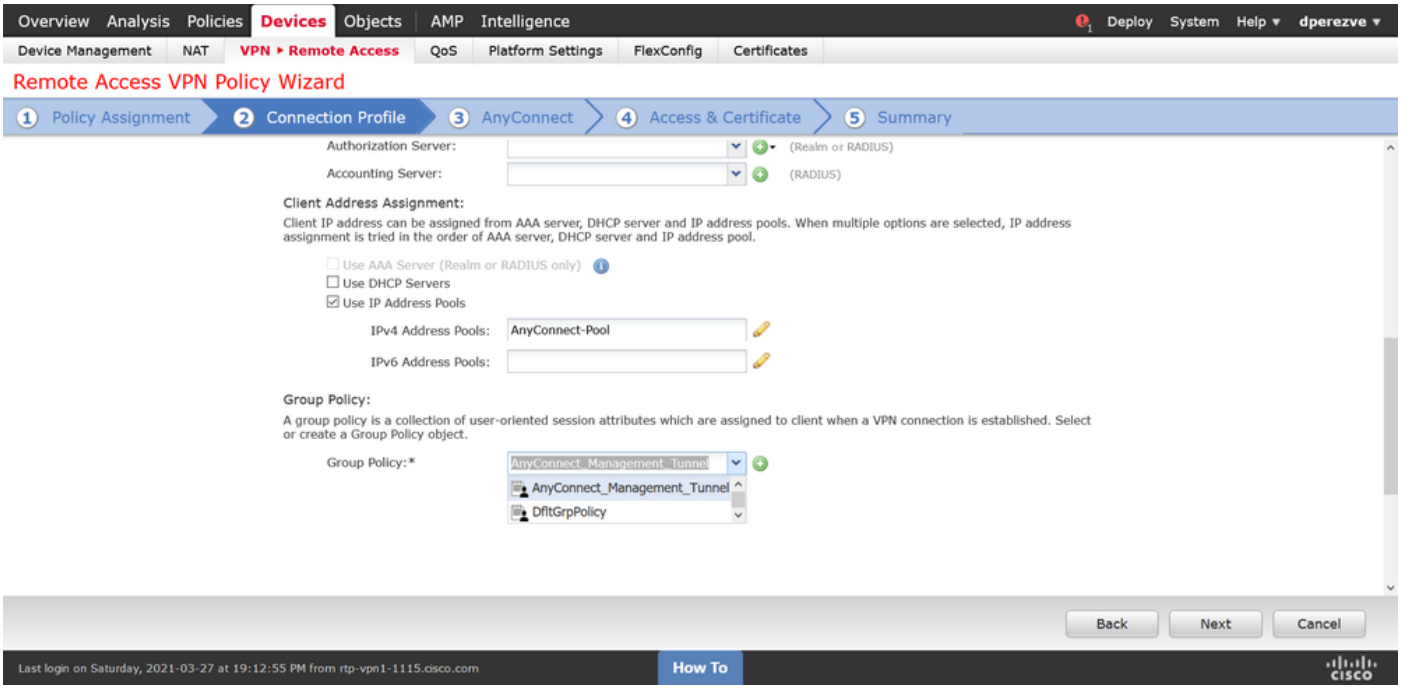
在**Policy Assigment** 选项卡上，选择手边的FTD设备，定义连接配置文件的名称并选中SSL复选框。



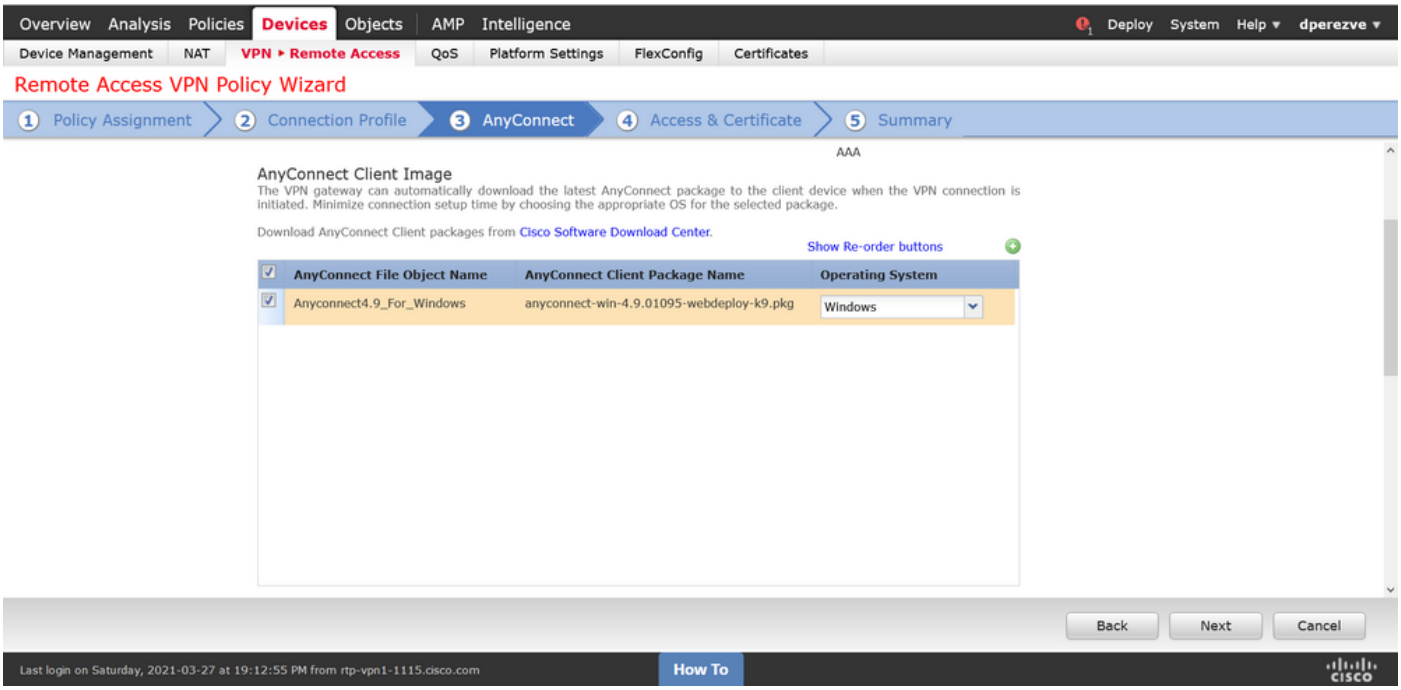
在连**接配置文件**上，**选择Client Certificate Only**作为身份验证方法。这是该功能支持的唯一身份验证。



然后在Group Policy下拉列表中选择在步骤3中创**建的Group Policy**对象。



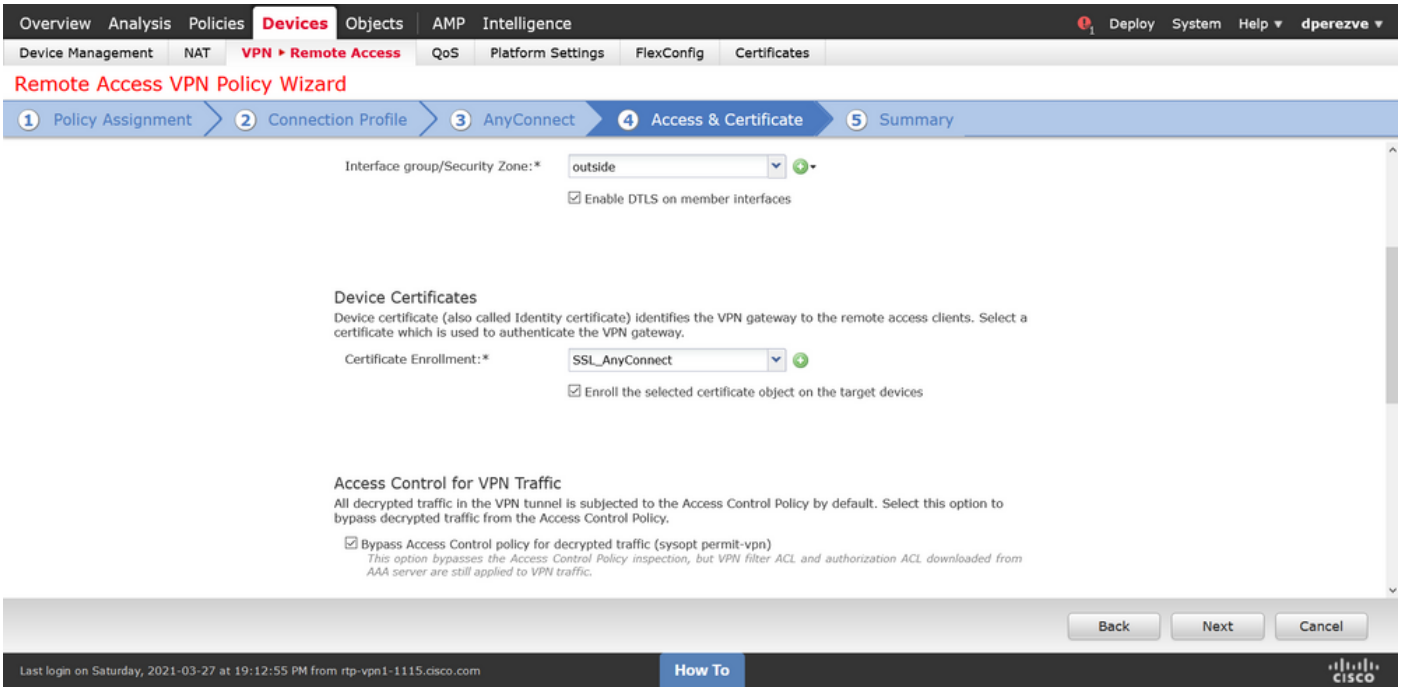
在AnyConnect选项卡上，根据终端上的操作系统(OS)选择AnyConnect File Object。



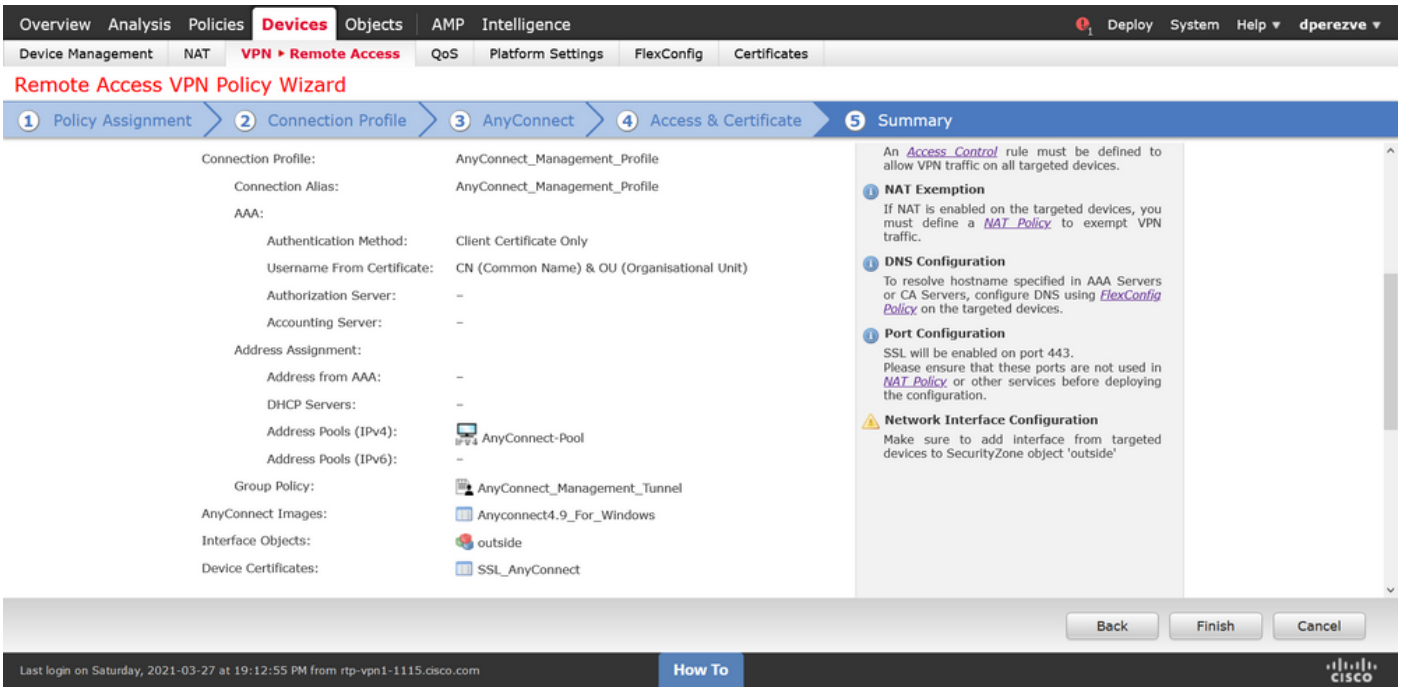
在Access & Certificate上，指定FTD必须使用的证书，以探测Windows客户端的身份。

注意：由于用户在使用管理VPN功能时不应与AnyConnect应用交互，因此证书需要完全受信任，并且不得打印任何警告消息。

注意：为防止证书验证错误，证书的使用者名称中包含的公用名称(CN)字段必须与XML配置文件服务器列表中定义的FQDN匹配（步骤1和步骤2）。



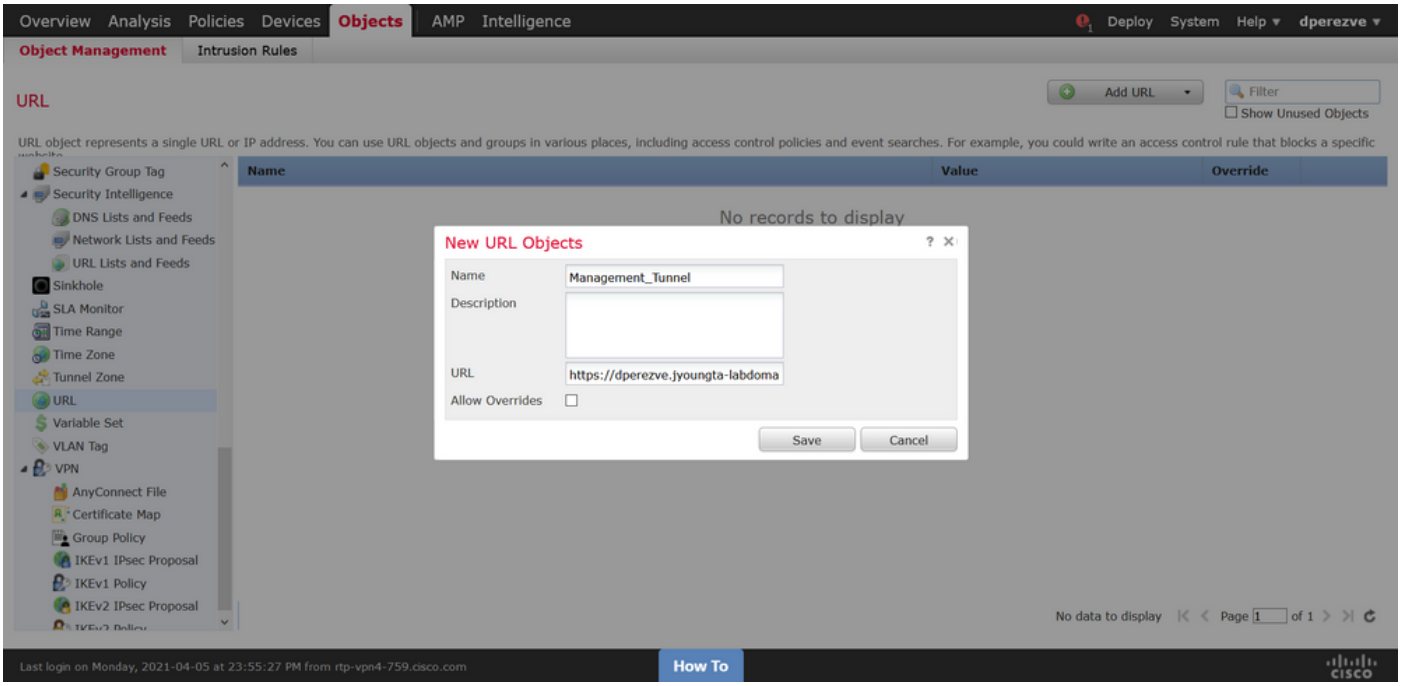
最后，在“摘**要**”选项卡上选**择“完**成”按钮以添加新的AnyConnect配置。



步骤6.创建URL对象

导航至**对象>对象管**理，**然后从**目录中选择URL。然后在“**添加URL**”下**拉菜单中**选择“添加对象”。

为对象提供名称，并使用在管理VPN配置文件服务器列表中指定的相同FQDN/用户组定义URL（步骤2）。 在本例中，URL必须为dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel。



保存更改以将对象添加到对象列表。

步骤7.定义URL别名

要启用AnyConnect配置中的URL别名，请导航至**Devices > VPN > Remote Access**，然后单击铅笔图标进行编辑。

然后，在“连接配置文件”选项卡上，选择现有配置，导航至“别名”，单击“添加”按钮并在“URL别名”下拉**菜单中选**择“URL对象”。确保选**中“**已启用”复选框。

保存更改并将配置部署到FTD。

验证

部署完成后，需要与AnyConnect VPN配置文件进行第一个手动AnyConnect连接。在此连接期间，管理VPN配置文件从FTD下载并存储在**C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**中。此时，必须通过管理VPN配置文件启动后续连接，无需任何用户交互。

故障排除

对于证书验证错误：

- 确保FTD上已安装证书颁发机构(CA)的根证书。
- 确保在Windows计算机存储上安装由同一CA签名的身份证书。
- 确保CN字段包含在证书中，并且与在URL别名中定义的管理VPN配置文件和FQDN的服务器列表中定义的FQDN相同。

对于管理隧道未启动：

- 确保已下载管理VPN配置文件并将其存储在**C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun中**。
- 确保管理VPN配置文件的名称**为VpnMgmtTunProfile.xml**。

有关连接问题，请收集DART捆绑包并联系Cisco TAC以进一步研究。