通过FTD、ISE、DUO和Active Directory配置SSL VPN身份验证

目录

简介

要求

使用的组件

网络图

配置

- FTD配置。
  - 在Firepower管理中心(FMC)中集成RADIUS服务器
  - 配置远程VPN。
- ISE配置。
  - 将DUO集成为外部Radius服务器。
  - 将FTD集成为网络接入设备。
- DUO配置。
  - DUO代理安装。
  - 将DUO Proxy与ISE和DUO Cloud集成。
  - 将DUO与Active Directory集成。
  - 通过DUO云从Active Directory(AD)导出用户帐户。
  - 在Cisco DUO云中注册用户。
- 配置验证过程。

常见问题.

- 工作场景。
- 错误11353不再有外部RADIUS服务器：无法执行故障转移
- RADIUS会话不会显示在ISE实时日志中。
- 其他故障排除.

简介

本文档介绍使用思科ISE和适用于AAA的DUO安全在Firepower威胁防御中集成SSLVPN。

要求

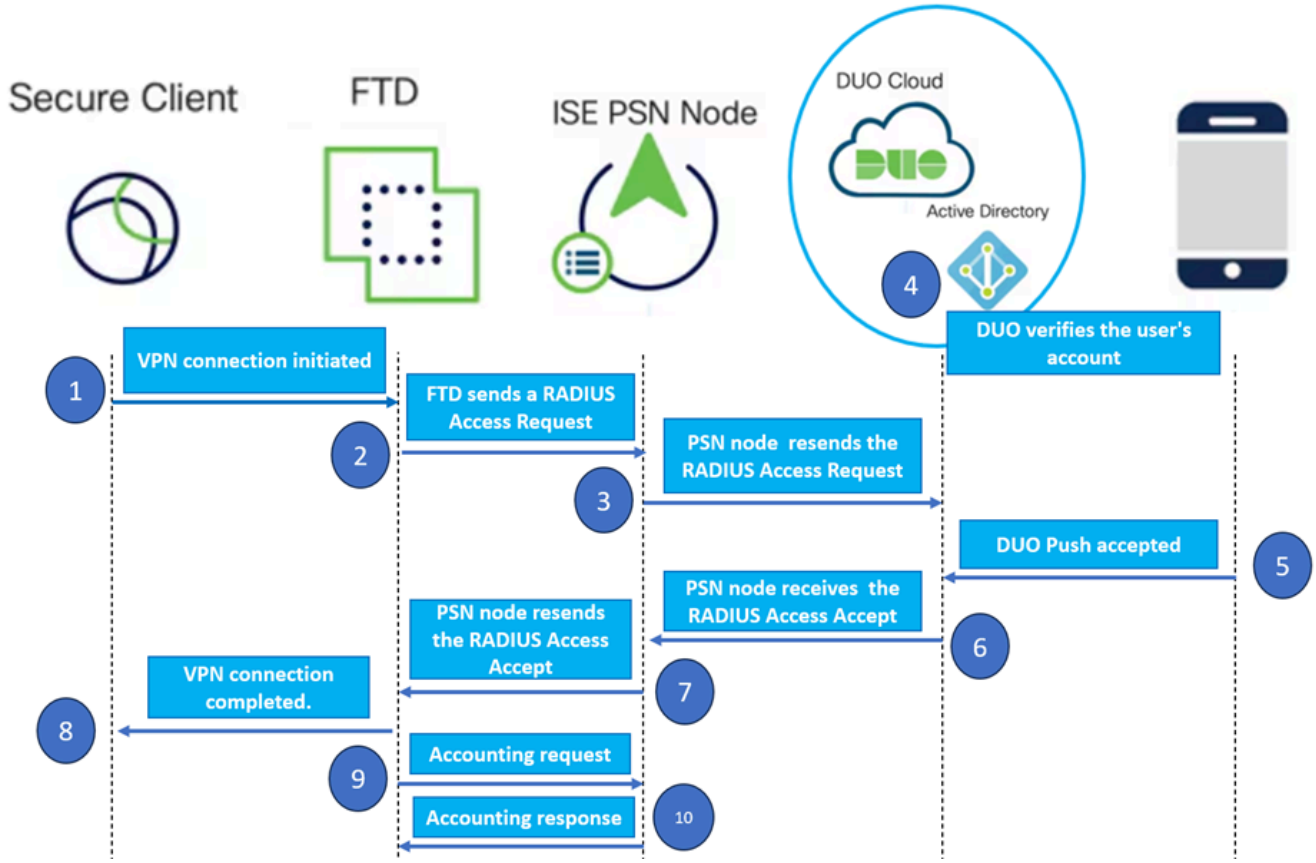
- ISE 3.0或更高版本。
- FMC 7.0或更高版本。
- FTD 7.0或更高版本。
- DUO身份验证代理。
- ISE基础版许可
- DUO Essentials许可。

使用的组件

- ISE 3.2补丁3
- FMC 7.2.5
- FTD 7.2.5
- Proxy DUO 6.3.0
- Any Connect 4.10.08029

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



拓扑。

在我们推荐的解决方案中，思科ISE是重要的RADIUS服务器代理。ISE配置为将RADIUS数据包从FTD转发到DUO身份验证代理，而不是直接评估身份验证或授权策略。

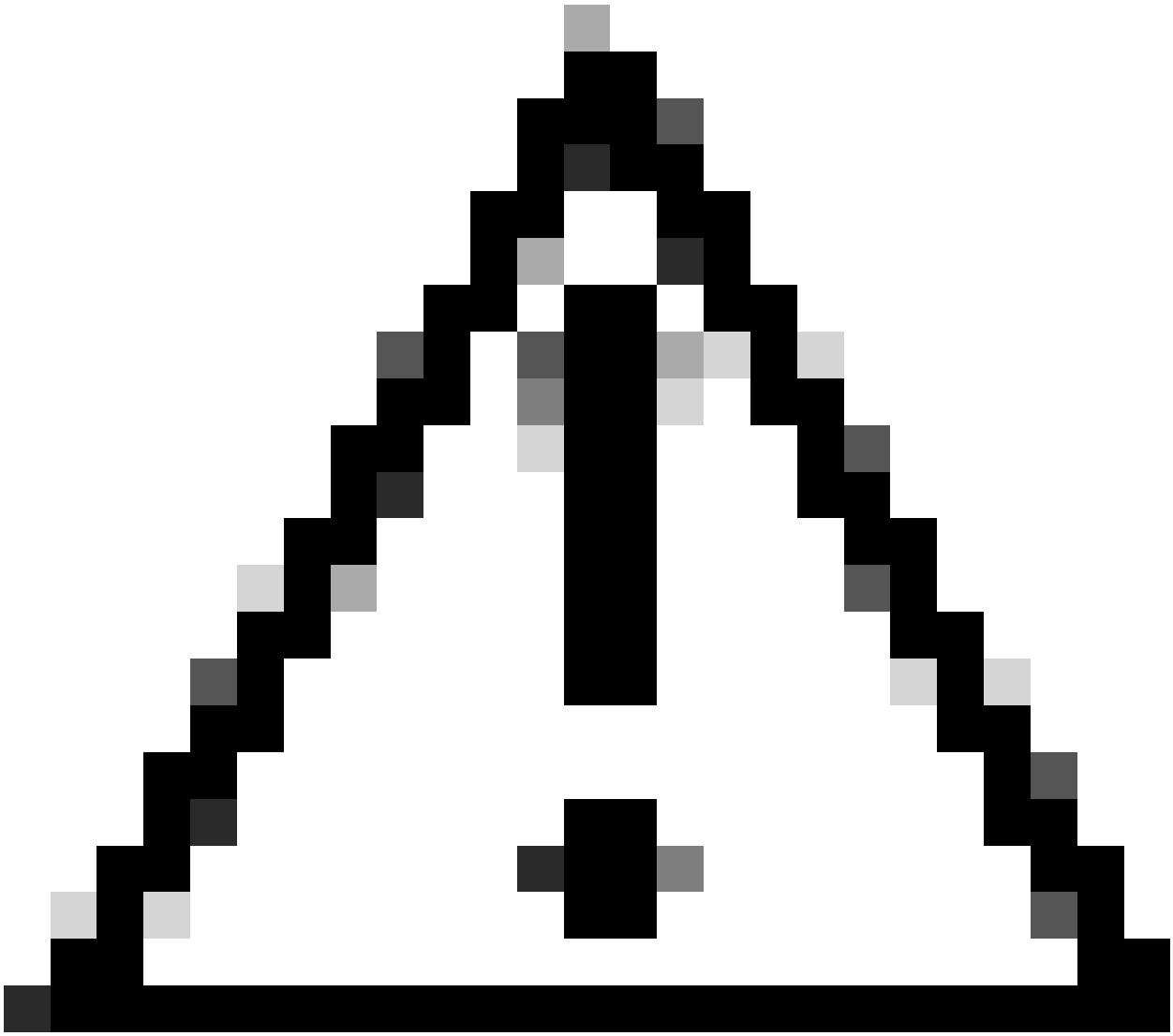
DUO身份验证代理在此身份验证流程中作为专用中间件运行。它安装在Windows服务器上，桥接Cisco ISE和DUO云之间的间隙。代理的主要功能是将身份验证请求（封装在RADIUS数据包内）传输到DUO云。DUO云最终根据双因素身份验证配置允许或拒绝网络访问。

1.用户通过输入其唯一用户名和密码启动VPN身份验证过程。

2.防火墙威胁防御(FTD)将身份验证请求发送到思科身份服务引擎(ISE)。

3.策略服务节点(PSN)将身份验证请求转发到DUO身份验证代理服务器。随后，DUO身份验证服务器通过DUO云服务验证凭证。

4. DUO Cloud根据同步数据库验证用户名和密码。



警告：DUO云和组织Active Directory之间的同步需要处于活动状态，以在DUO云中维护最新的用户数据库。

5.身份验证成功后，DUO云通过安全的加密推送通知向注册移动设备的用户启动DUO Push。然后，用户必须批准DUO Push以确认其身份并继续。

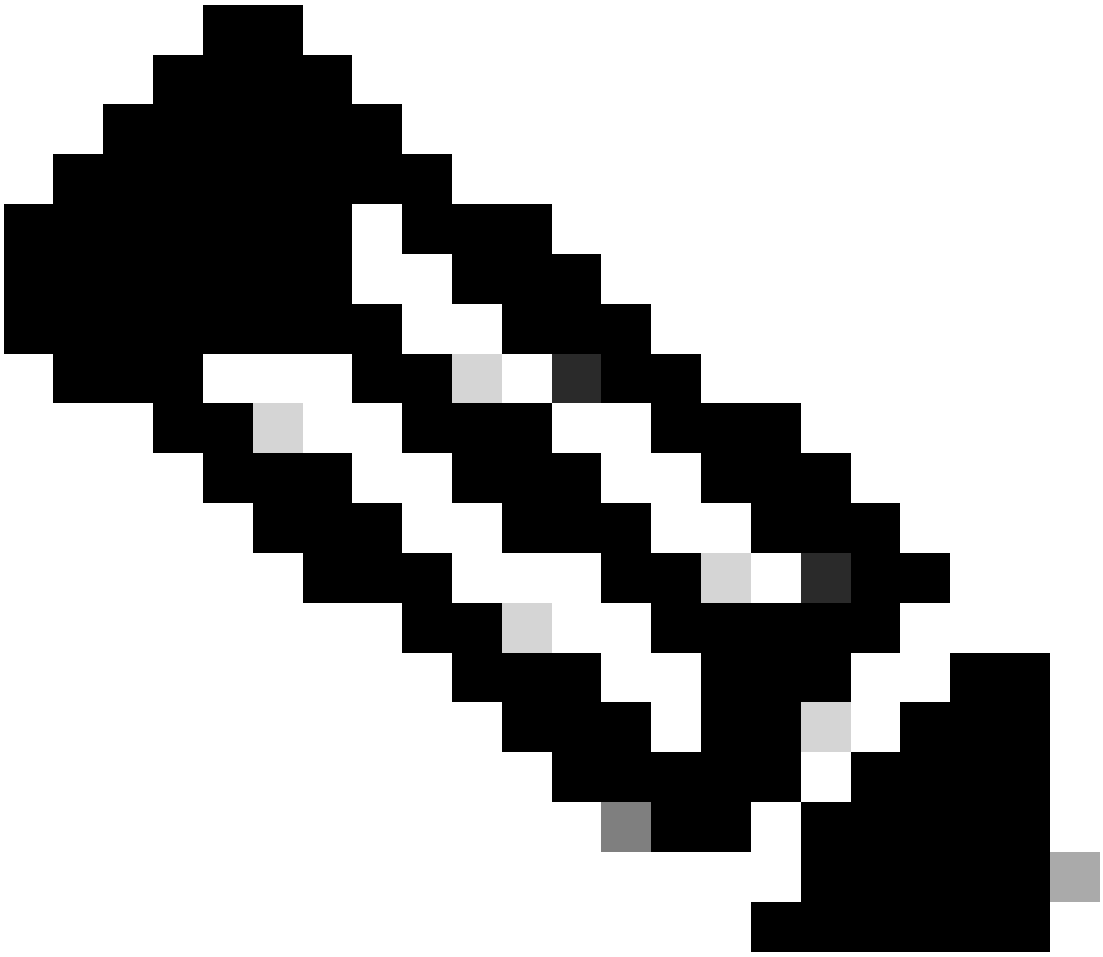
6.用户批准DUO Push后，DUO身份验证代理服务器会向PSN发送确认消息，指示用户已接受身份验证请求。

7. PSN节点向FTD发送确认，通知用户已通过身份验证。

8. FTD收到身份验证确认信息，并建立到终端的VPN连接，同时采用适当的安全措施。

9. FTD记录成功的VPN连接的详细信息，并将记帐数据安全地传输回ISE节点，以便进行记录和审核。

10. ISE节点将会计信息记录在其日志中，确保安全存储所有记录，并可访问这些记录以供将来审计或合规性检查。



注意：

本指南中的设置利用以下网络参数：

— 主网络服务器(PNS)节点IP:10.4.23.21

— 适用于对等VPN的Firepower威胁防御(FTD)IP:10.4.23.53

- DUO身份验证代理IP:10.31.126.207

-域名：testlab.local

配置

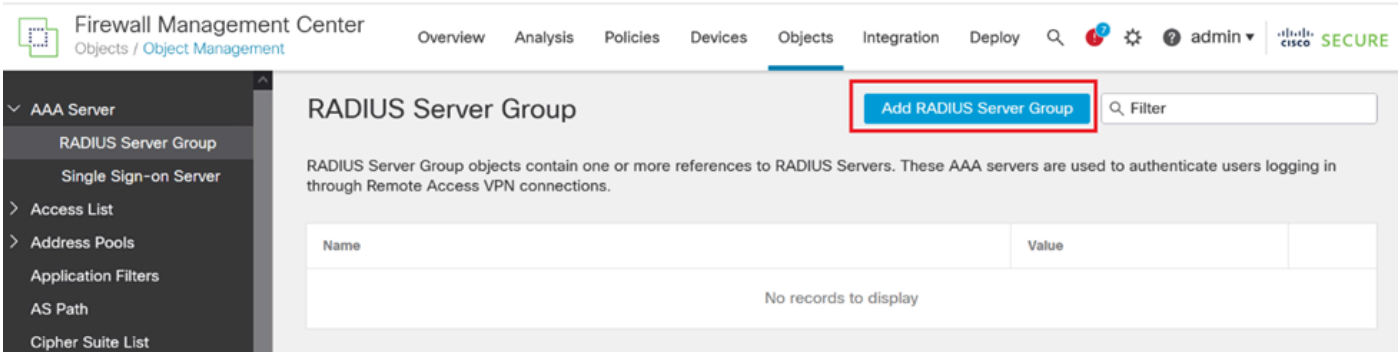
FTD配置。

在Firepower管理中心(FMC)中集成RADIUS服务器

1.通过启动Web浏览器并输入FMC IP地址打开图形用户界面(GUI)来访问FMC。

2.导航到对象菜单，选择AAA服务器，然后转到RADIUS服务器组选项。

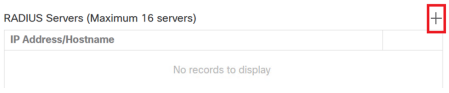
3.单击Add RADIUS Server Group按钮，为RADIUS服务器创建一个新组。



RADIUS服务器组。

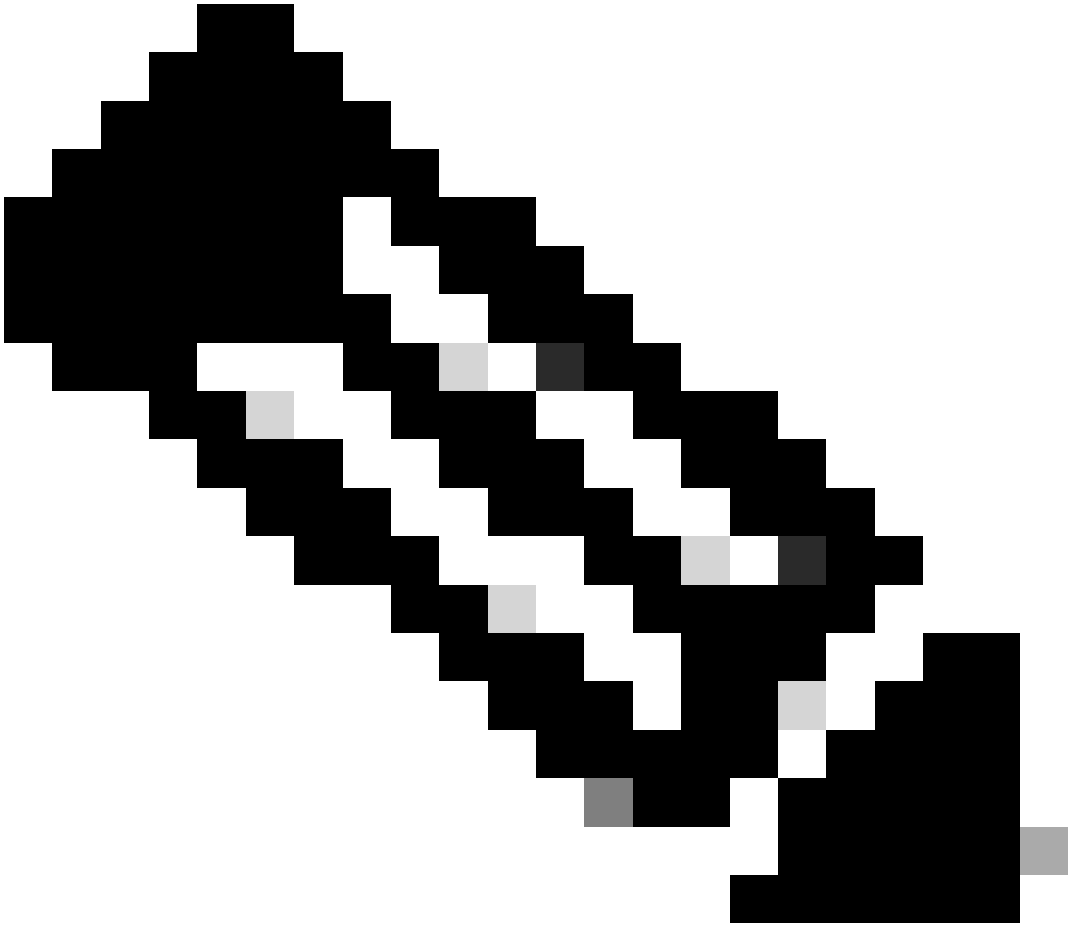
4.输入新AAA RADIUS服务器组的描述性名称，以确保在网络基础设施内进行明确的标识。

5.通过在组配置中选择适当的选项，继续添加新的RADIUS服务器。

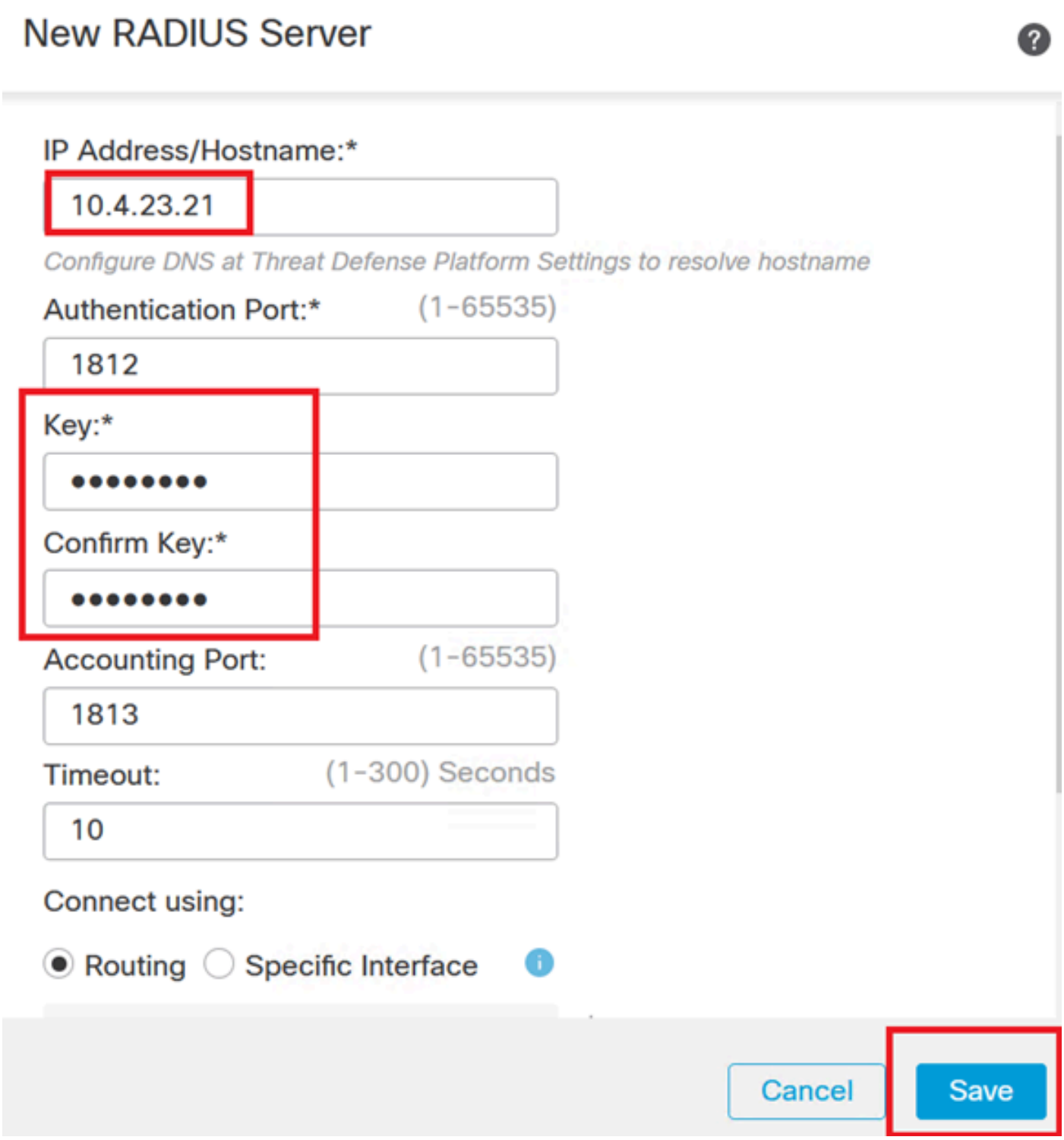


RADIUS 服务器.

6.指定RADIUS服务器IP地址并输入共享密钥。

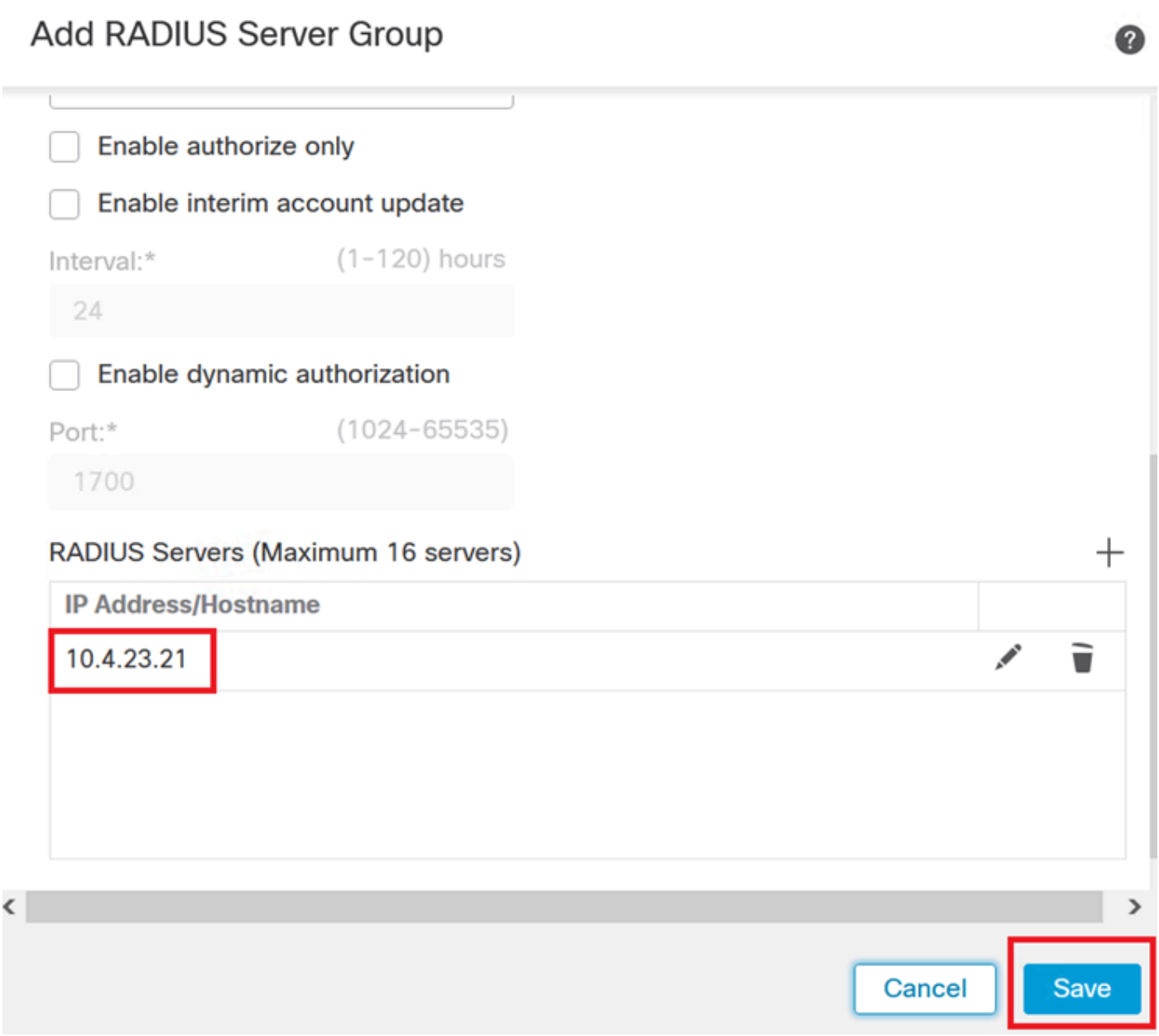


注意：必须确保此密钥与ISE服务器安全共享，才能建立成功的RADIUS连接。



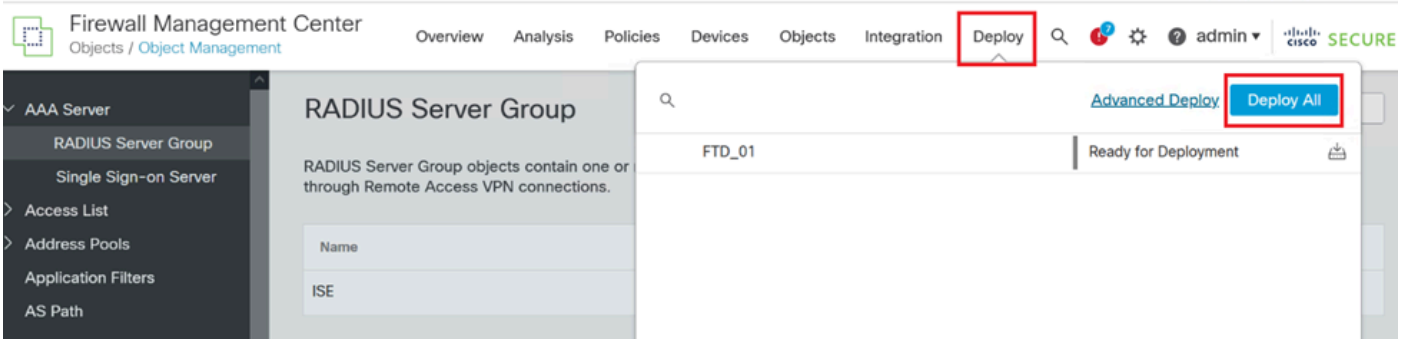
新建*RADIUS*服务器。

7.配置RADIUS服务器详细信息后，单击Save以保留RADIUS服务器组的设置。



服务器组详细信息。

8.要在网络中最终完成并实施AAA服务器配置，请导航到部署菜单，然后选择全部部署以应用设置。

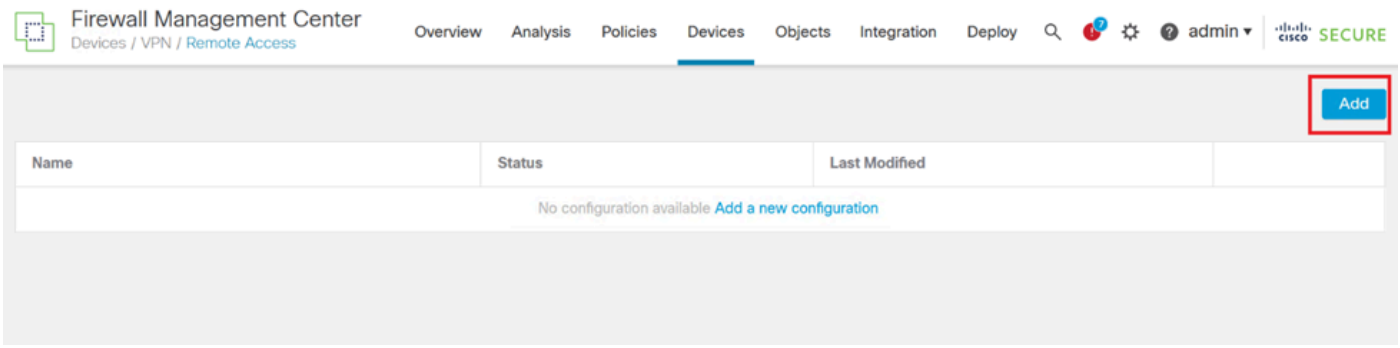


部署*AAA*服务器。

配置远程VPN。

1.在FMC GUI中导航到设备> VPN >远程访问，以开始VPN配置过程。

2.单击Add按钮以创建新的VPN连接配置文件。

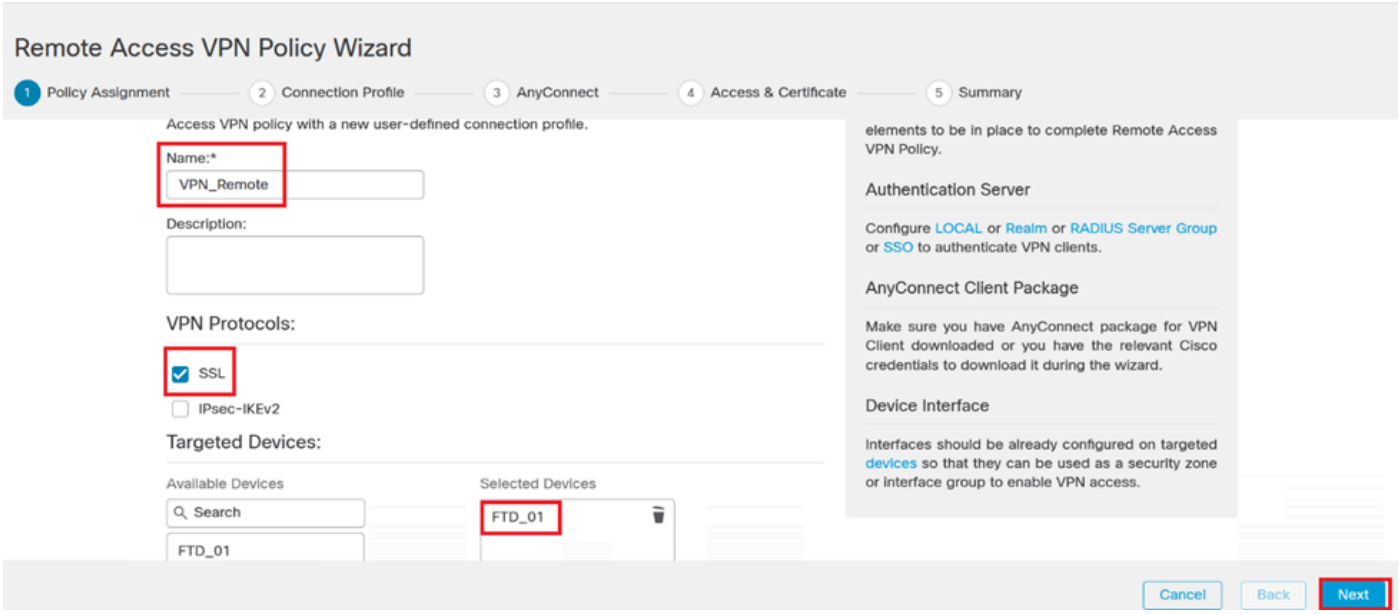


*VPN*连接配置文件。

3.输入VPN的唯一描述性名称，以帮助在网络设置中识别它。

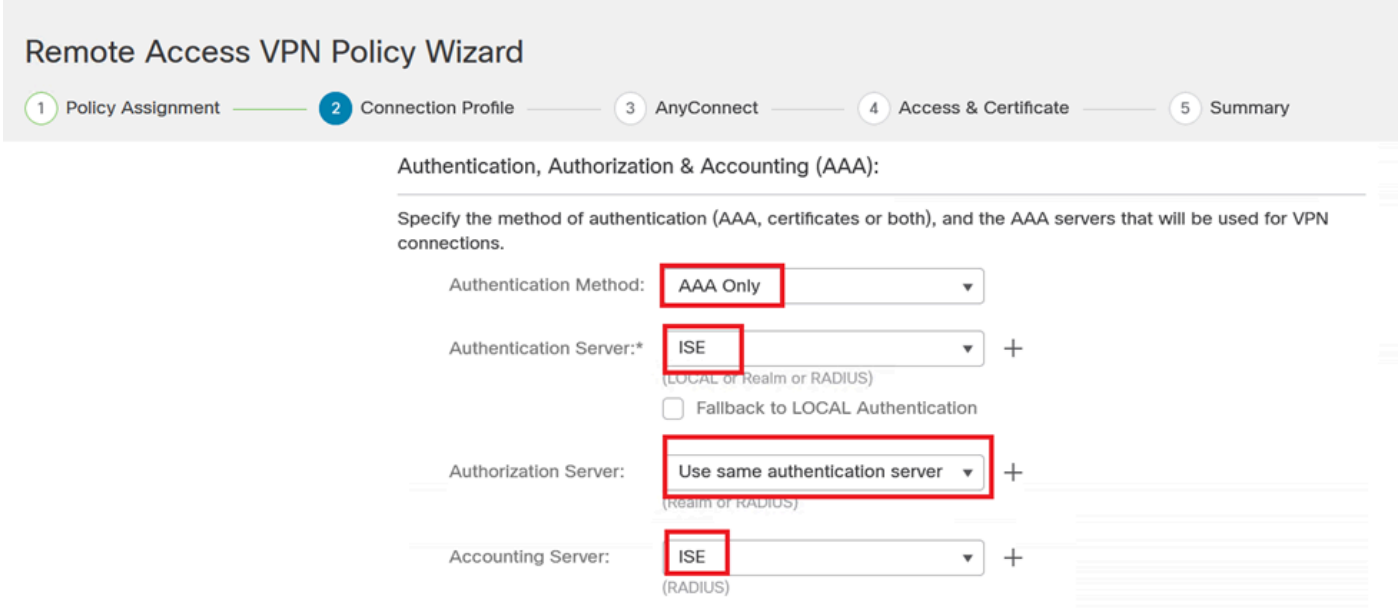
4.选择SSL选项以确保使用SSL VPN协议的安全连接。

5.从设备列表中选择特定的FTD设备。



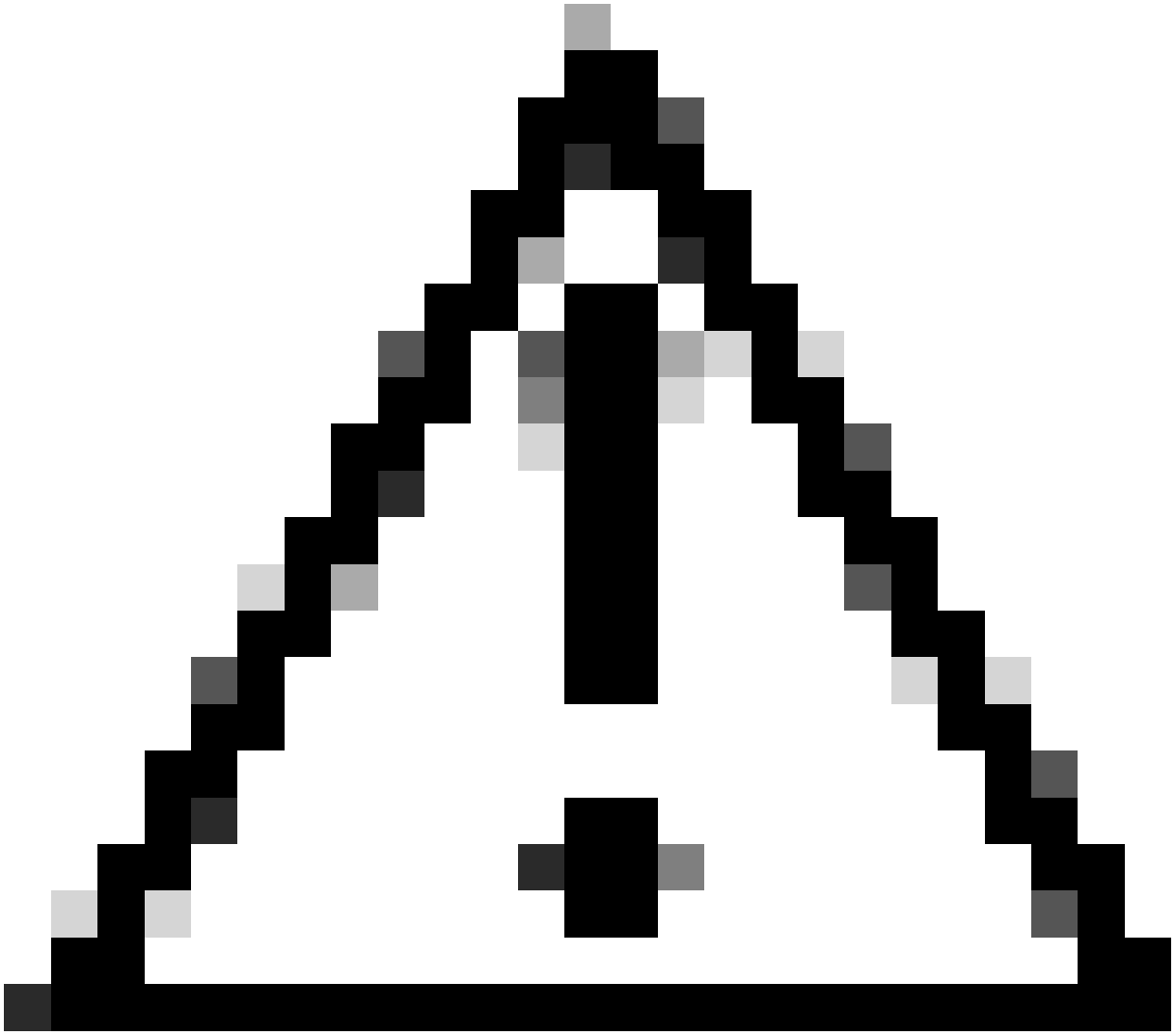
*VPN*设置。

6.将AAA方法配置为在身份验证设置中使用PSN节点。

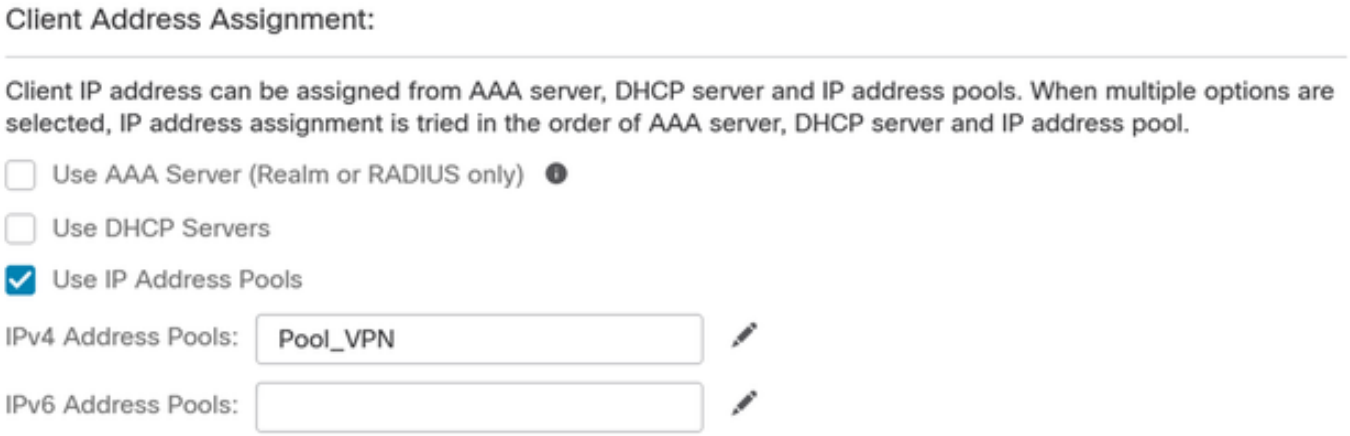


连接配置文件。

7.为VPN设置动态IP地址分配。

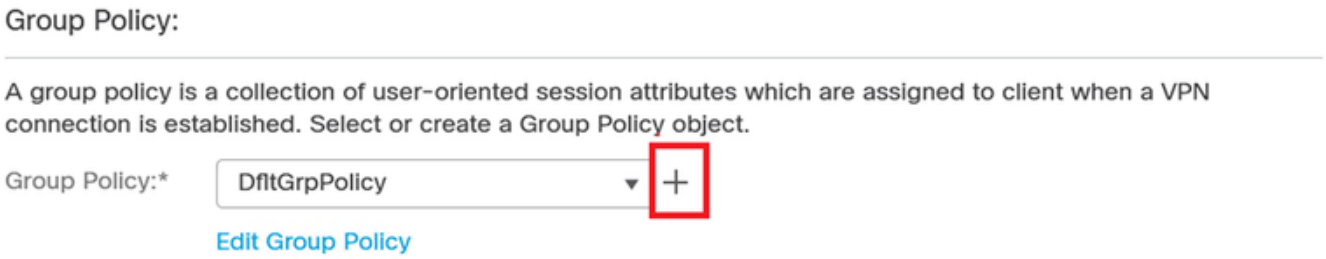


警告：例如，已选择DHCP VPN池。



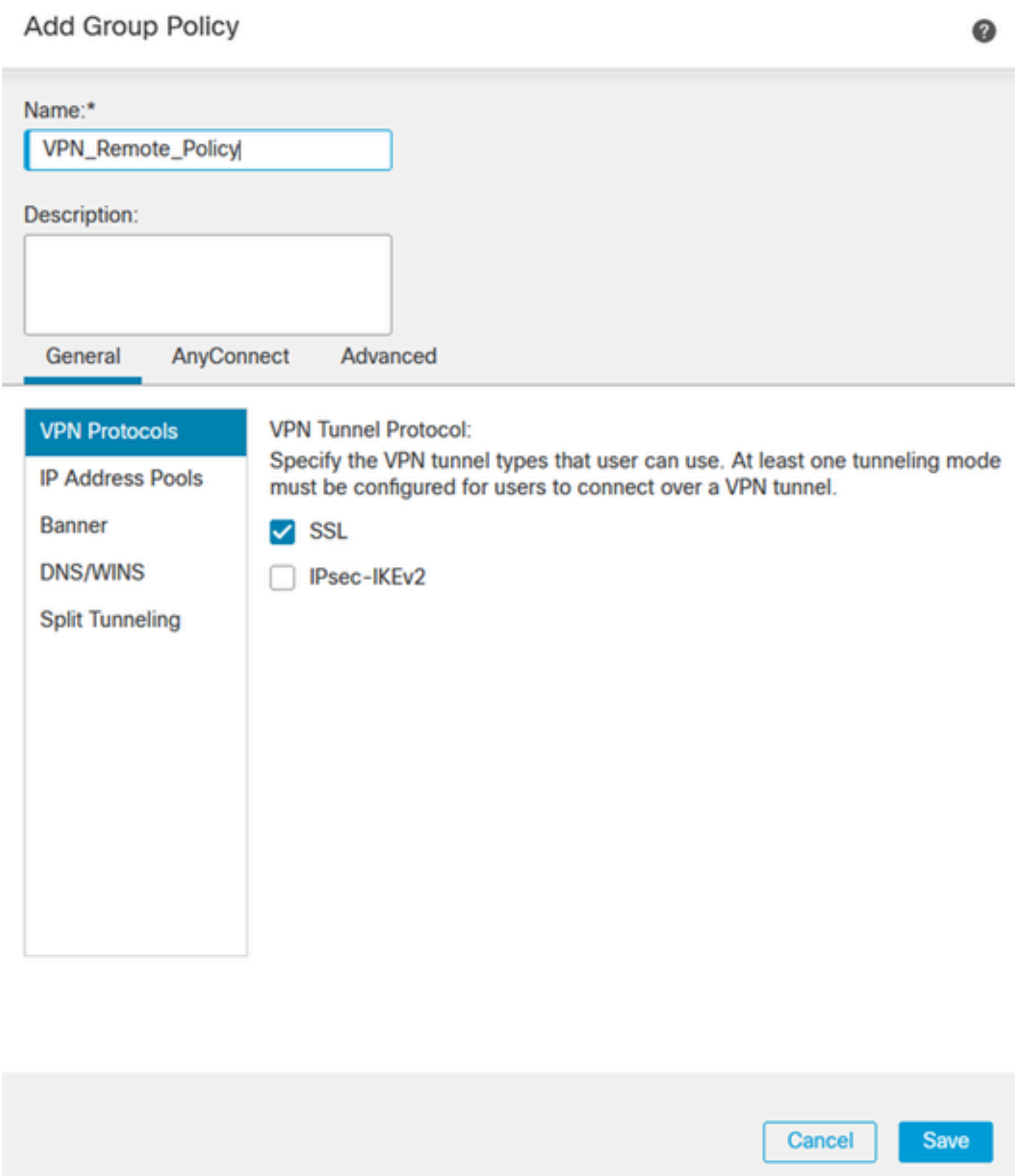
IP Address Pool.

8.继续创建新的组策略。



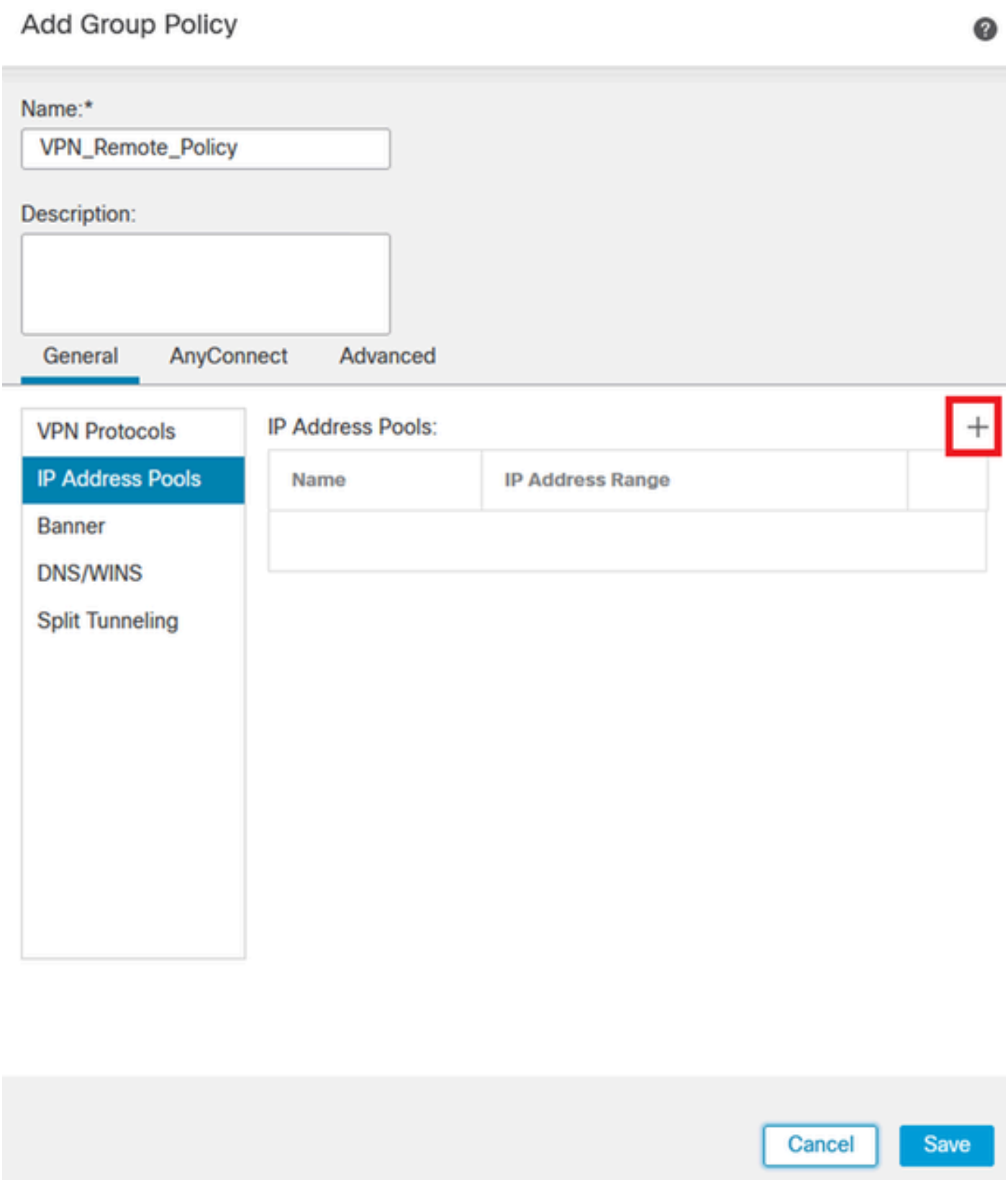
组策略.

9.在组策略设置中，确保已选择SSL协议。



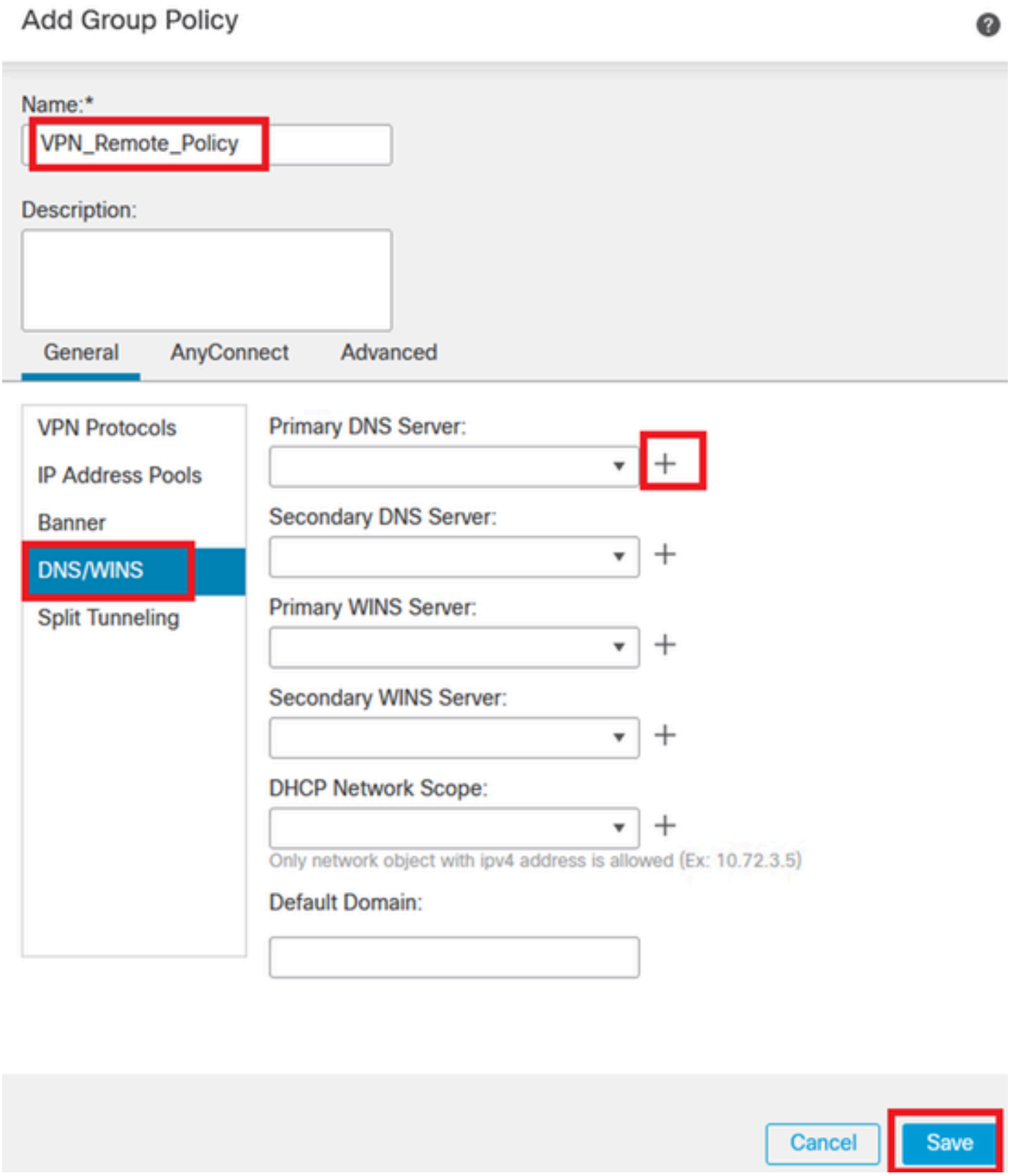
VPN协议。

10.创建新的VPN池或选择现有VPN池，以定义可用于VPN客户端的IP地址范围。

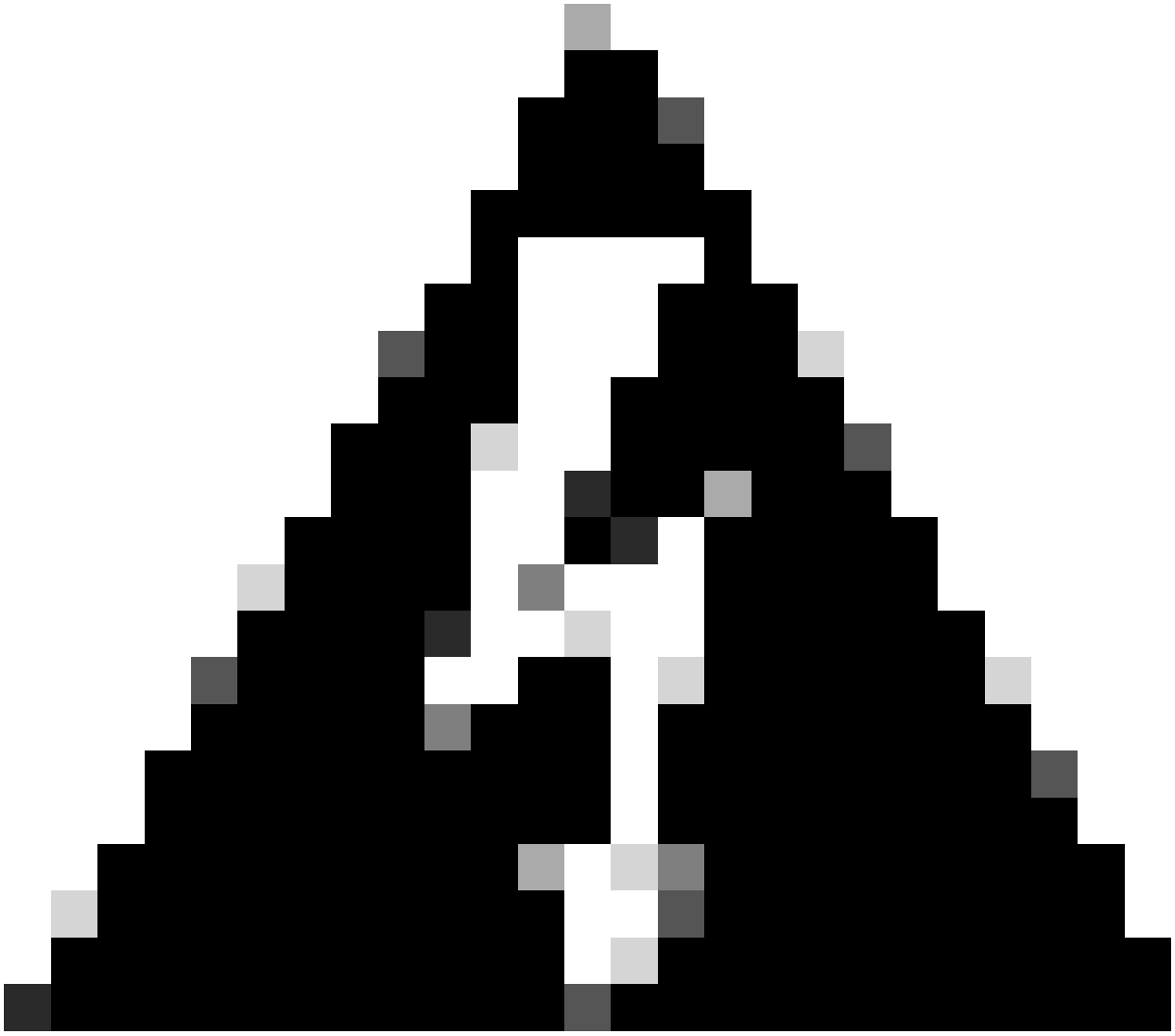


池*VPN*。

11.指定VPN连接的DNS服务器详细信息。

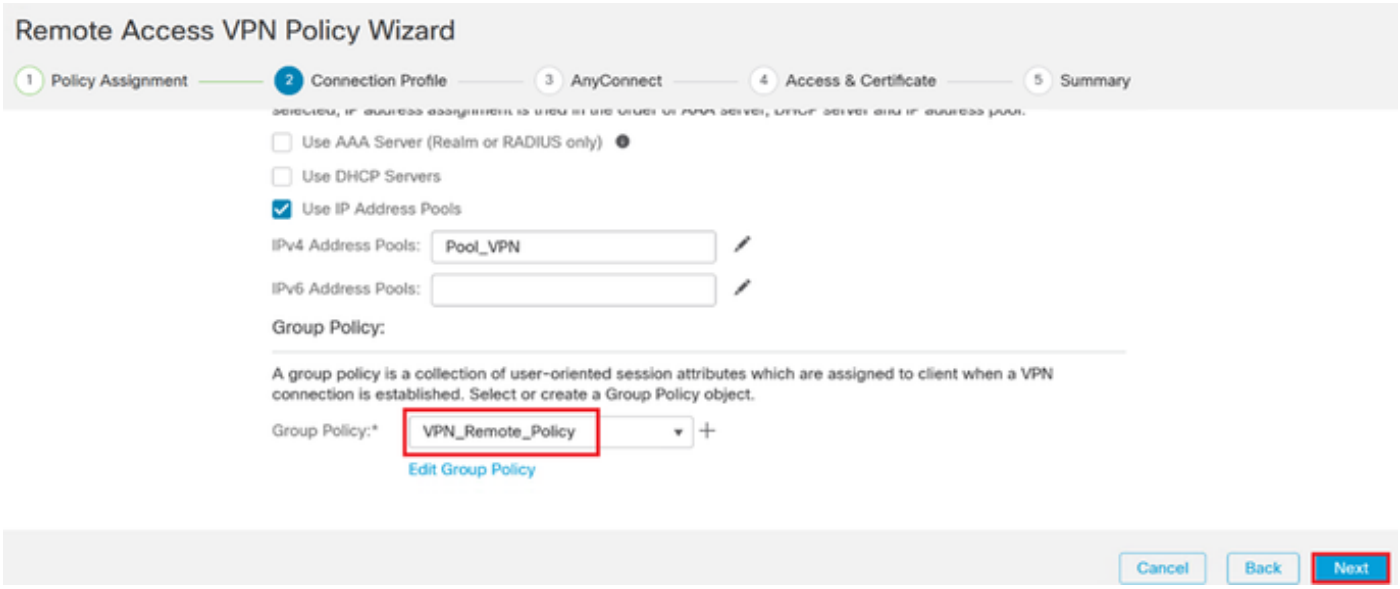

Add Group Policy
Name:*
VPN_Remote_Policy
Description:
General
AnyConnect
Advanced
VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling
Primary DNS Server:
Secondary DNS Server:
Primary WINS Server:
Secondary WINS Server:
DHCP Network Scope:
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)
Default Domain:
Cancel
Save

*DNS*设置。



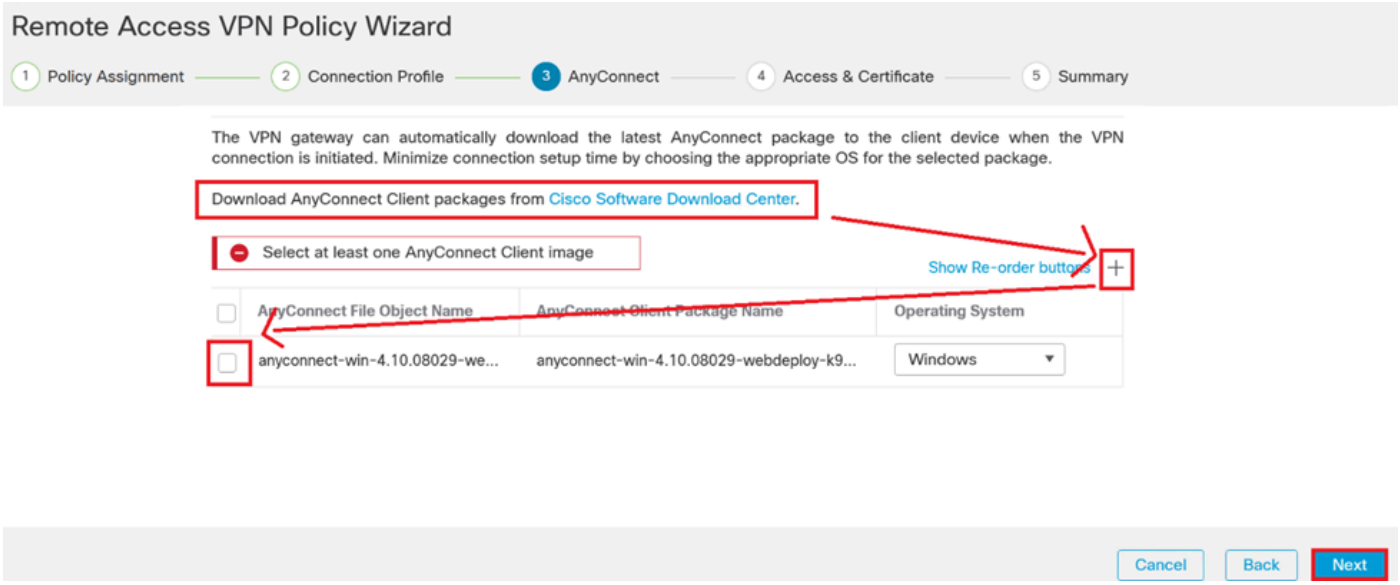
警告：请注意，Banner、Split Tunneling、AnyConnect和Advanced选项等其他功能被视为此配置的可选功能。

12.配置必要的详细信息后，单击下一步继续下一步的设置。



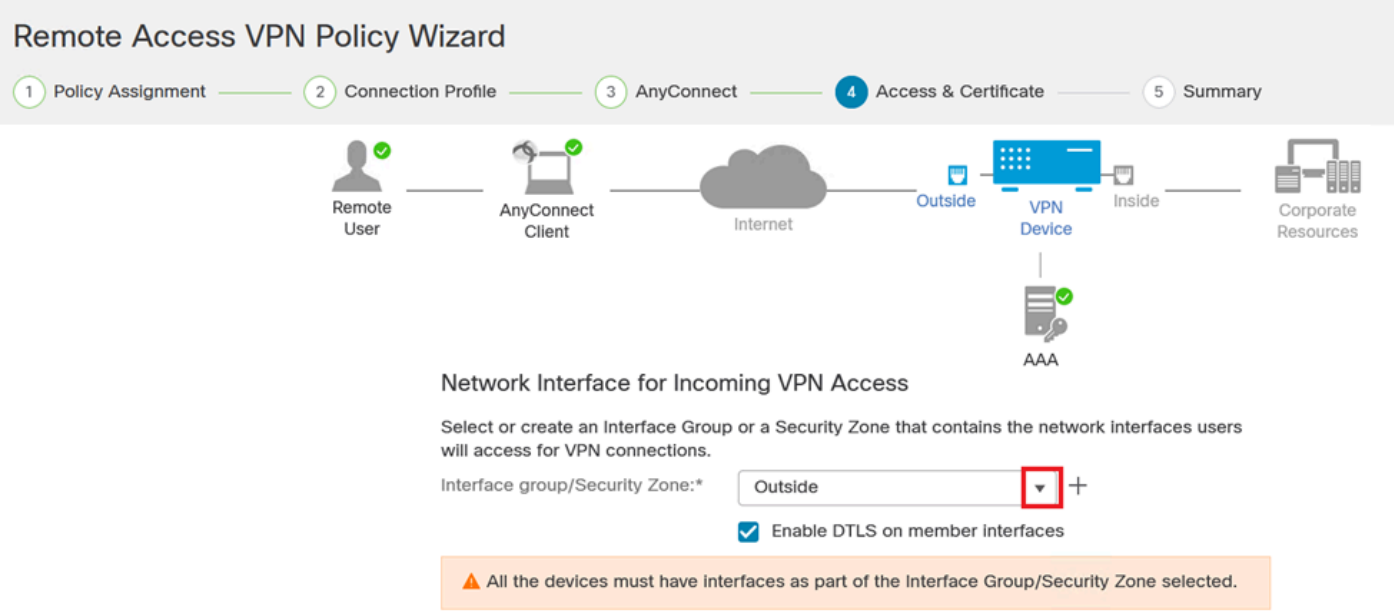
组策略.

13.为VPN用户选择适当的AnyConnect软件包。如果所需的包没有列出，您可以选择在此阶段添加所需的包。



软件包安装。

14.选择要启用VPN Remote功能的FTD设备上的网络接口。



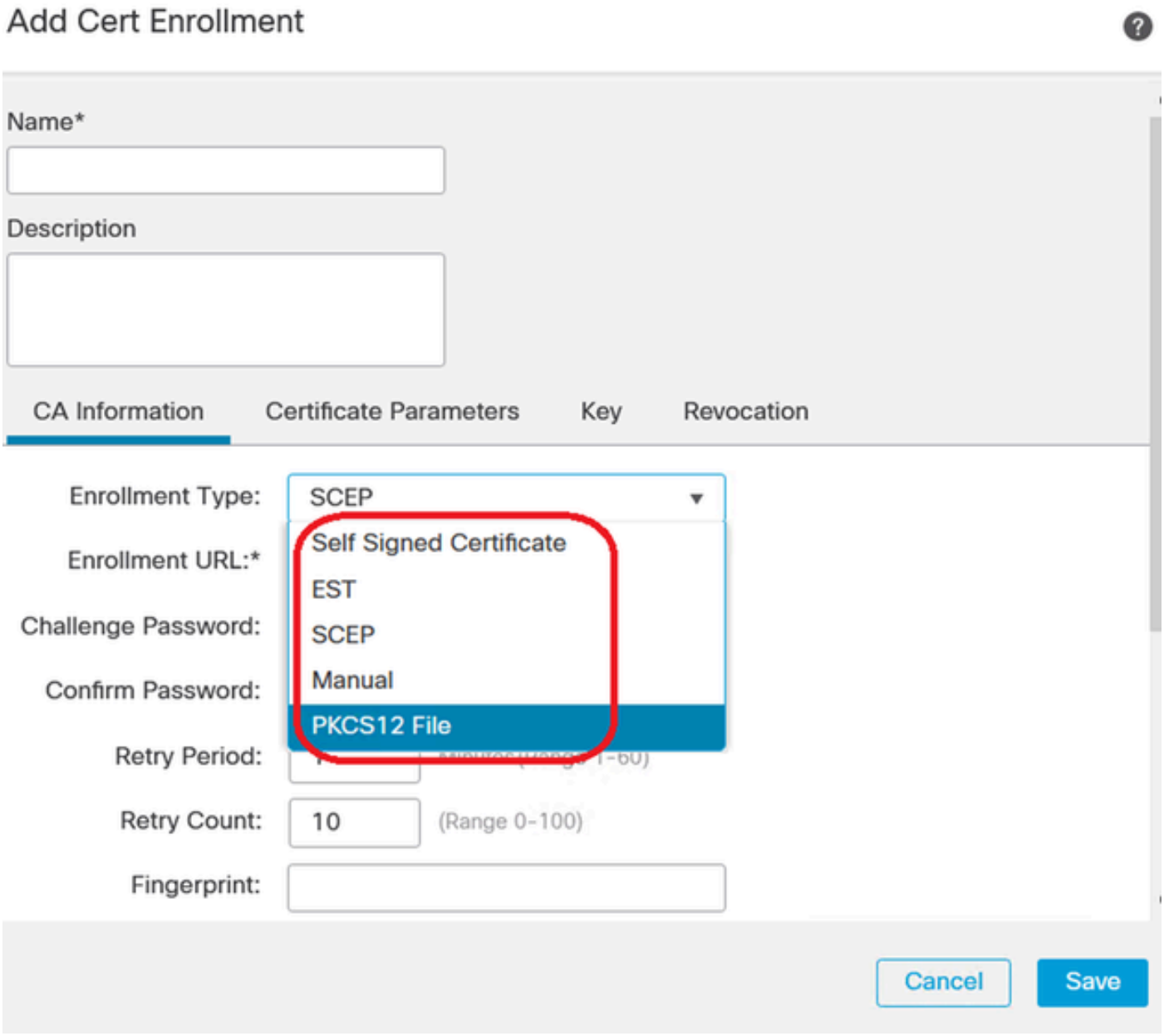
VPN接口

15.通过选择一种可用方法创建证书并在防火墙上安装证书，建立证书注册流程，这对安全VPN连接至关重要。

警告：例如，在本指南中选择了自签名证书。

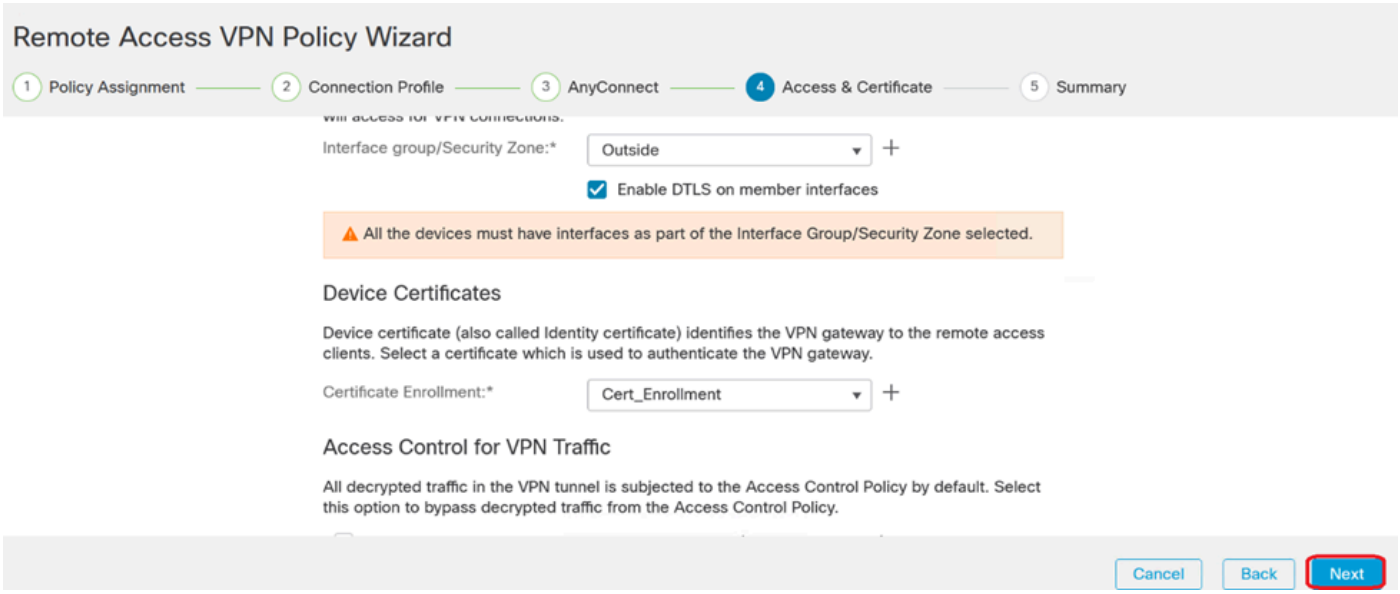


设备证书。



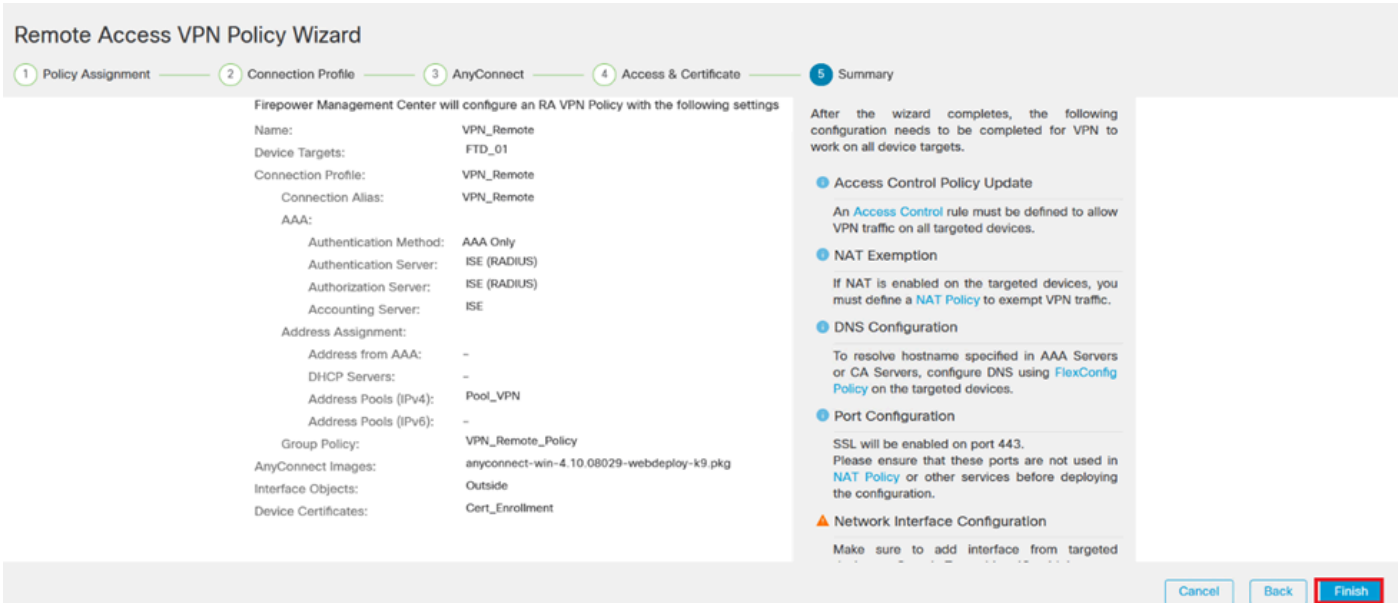
证书注册。

16.配置证书注册后，单击Next。



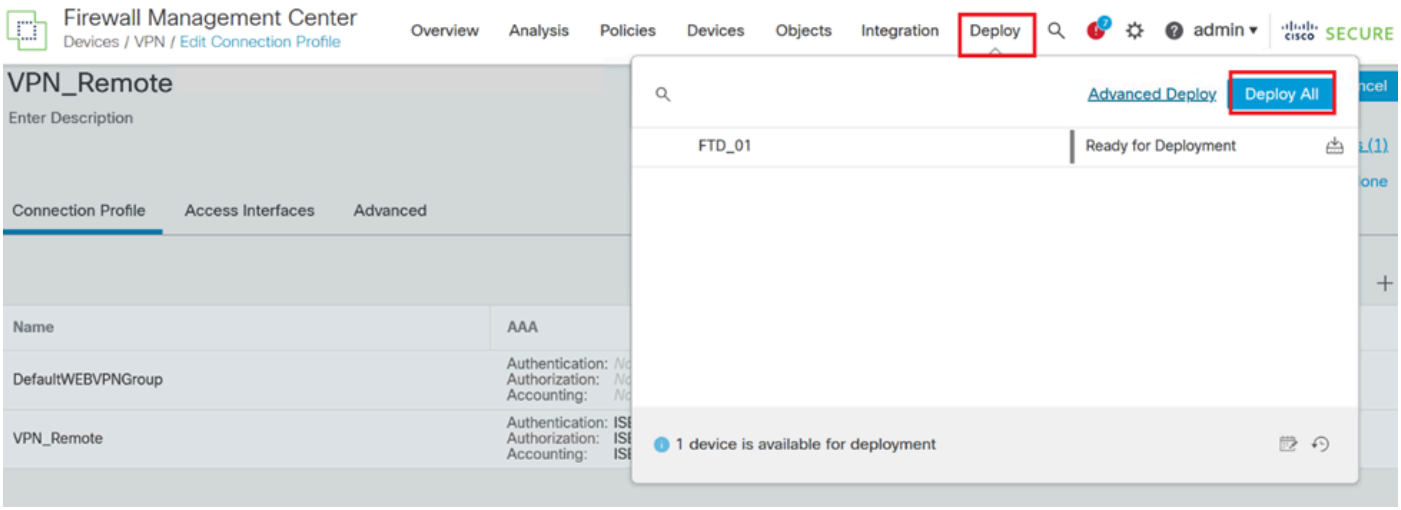
访问和服务摘要

17.检查所有配置的摘要，确保配置准确并反映您预期的设置。



*VPN*设置摘要。

18.要应用和激活VPN远程访问配置，请导航到部署>全部部署，然后对所选的FTD设备执行部署。



部署*VPN*设置。

ISE配置。

将DUO集成为外部Radius服务器。

1.在Cisco ISE管理界面中导航到Administration > Network Resources > External RADIUS Servers。

2.单击Add按钮配置新的外部RADIUS服务器。

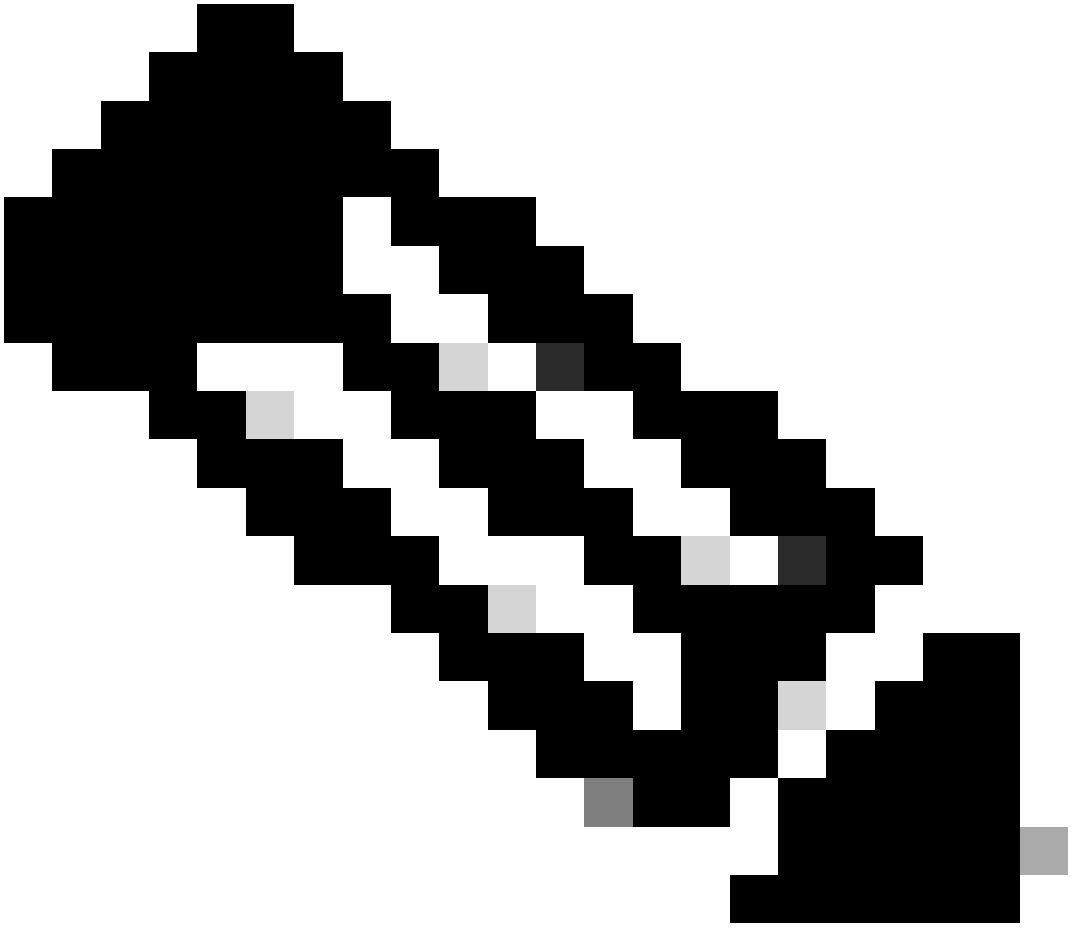


外部Radius服务器

3.输入代理DUO服务器的名称。

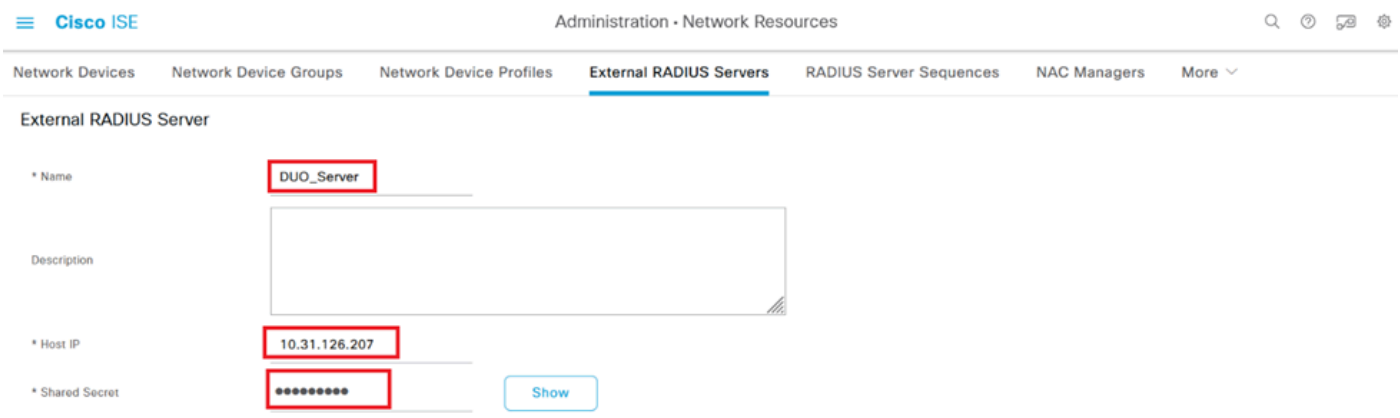
4.输入代理DUO服务器的正确IP地址，以确保ISE和DUO服务器之间正确通信。

5.设置共享密钥。



注意：必须将此共享密钥配置到代理DUO服务器才能成功建立RADIUS连接。

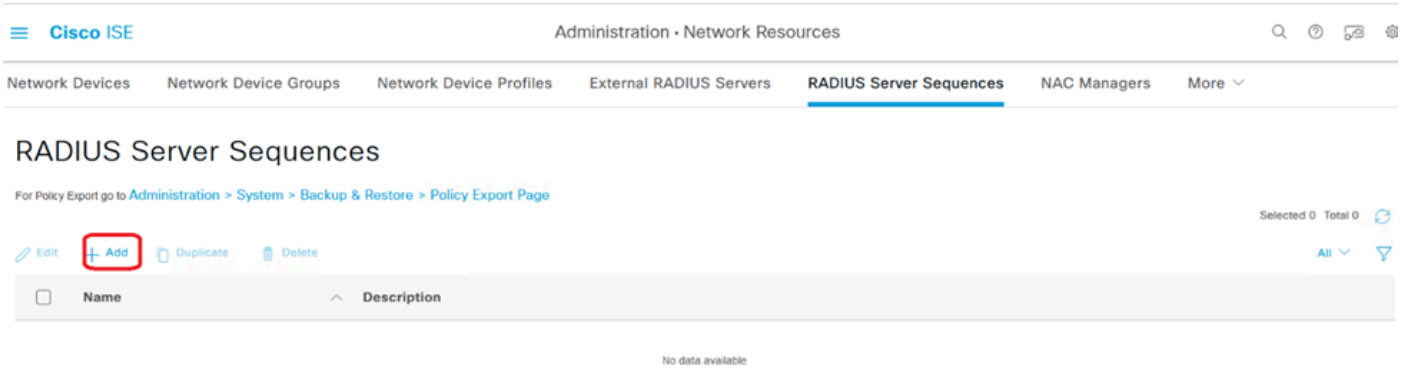
6.正确输入所有详细信息后，单击**Submit**保存新的Proxy DUO Server配置。



外部*RADIUS*服务器

7.转到管理> RADIUS服务器序列。

8.单击Add以创建新的RADIUS服务器序列。

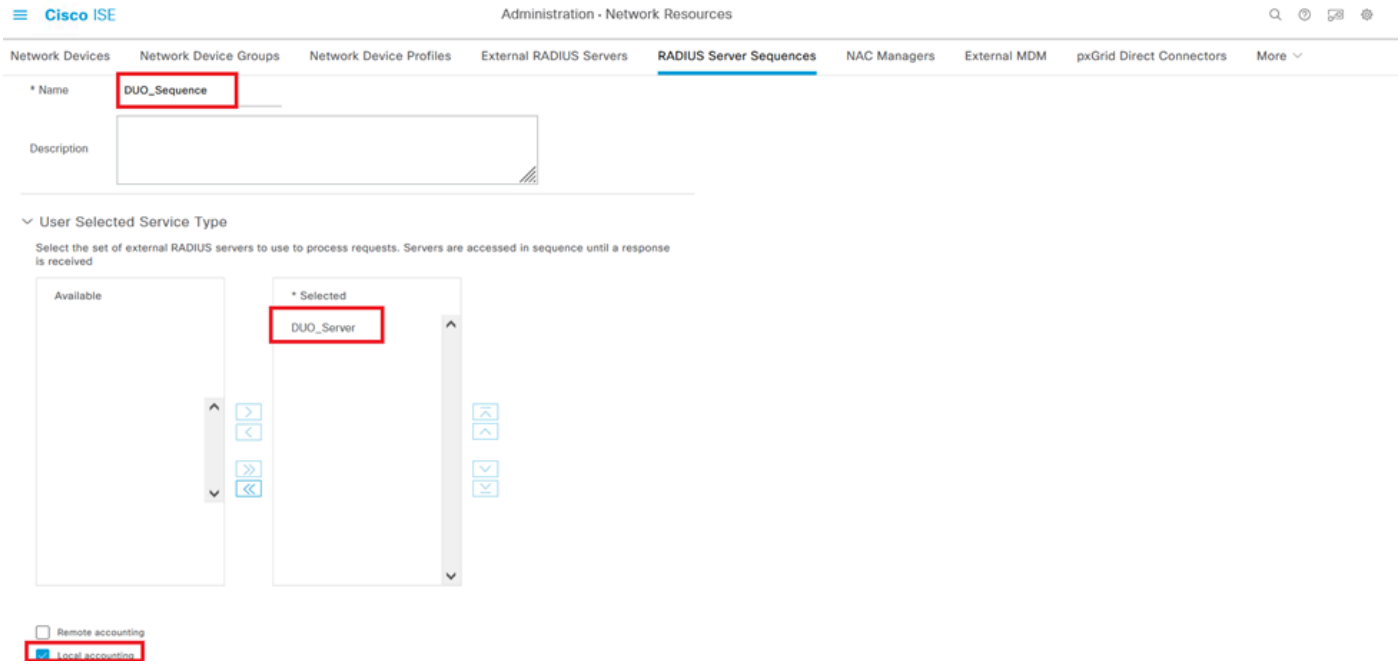


*RADIUS*服务器序列

9.为RADIUS服务器序列提供不同的名称，以便轻松识别。

10.找到以前配置的DUO RADIUS服务器(在本指南中称为DUO_Server)，并将其移至右侧的选定列表，以将其包含在序列中。

11.单击Submit完成并保存RADIUS Server Sequence配置。

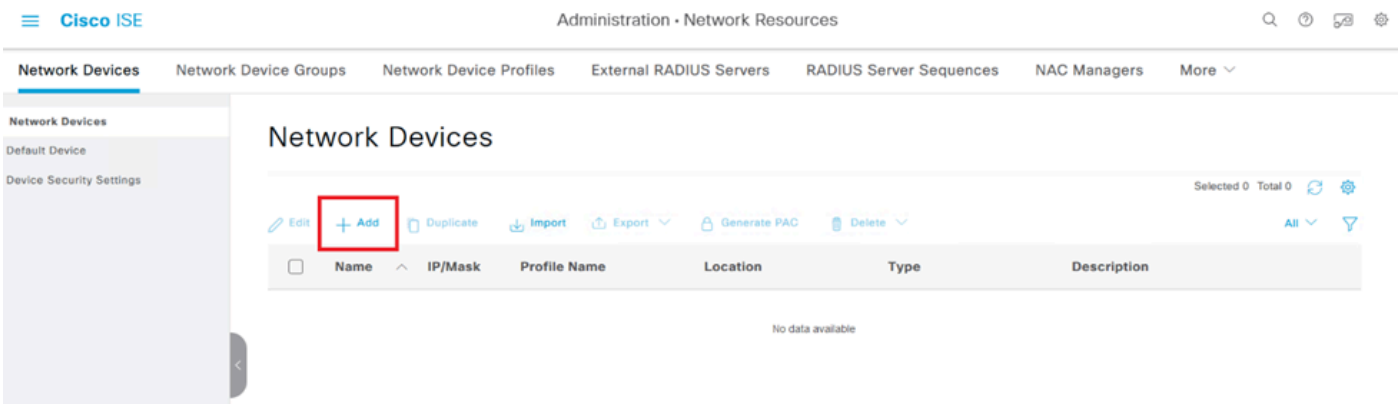


Radius服务器序列配置。

将FTD集成为网络接入设备。

1.导航到系统接口中的管理部分，并从该部分选择网络资源，以访问网络设备的配置区域。

2.进入网络资源部分后，找到并点击添加按钮以启动添加新网络接入设备的过程。



网络接入设备。

3.在提供的字段中，输入网络接入设备名称以标识网络中的设备。

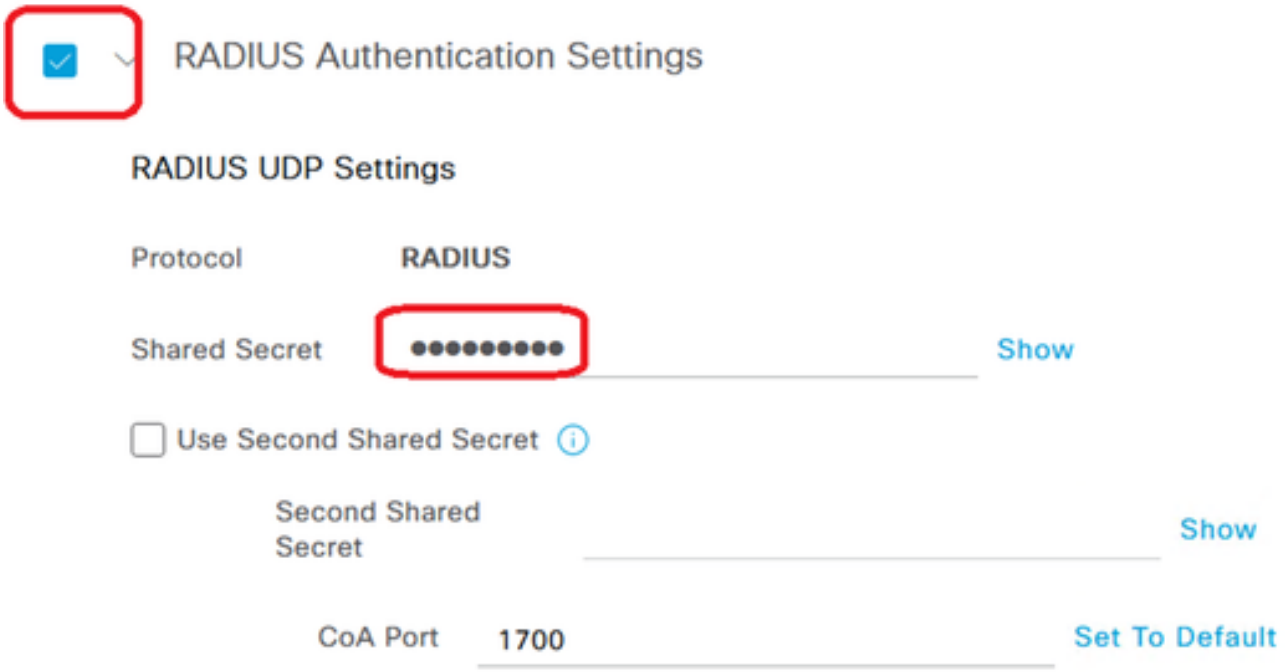
4.继续指定FTD（Firepower威胁防御）设备的IP地址。

5.输入之前在FMC（Firepower管理中心）设置期间建立的密钥。此密钥对于设备之间的安全通信至关重要。

6.单击Submit（提交）按钮完成此流程。



添加FTD作为NAD。



RADIUS设置

DUO配置。

DUO代理安装。

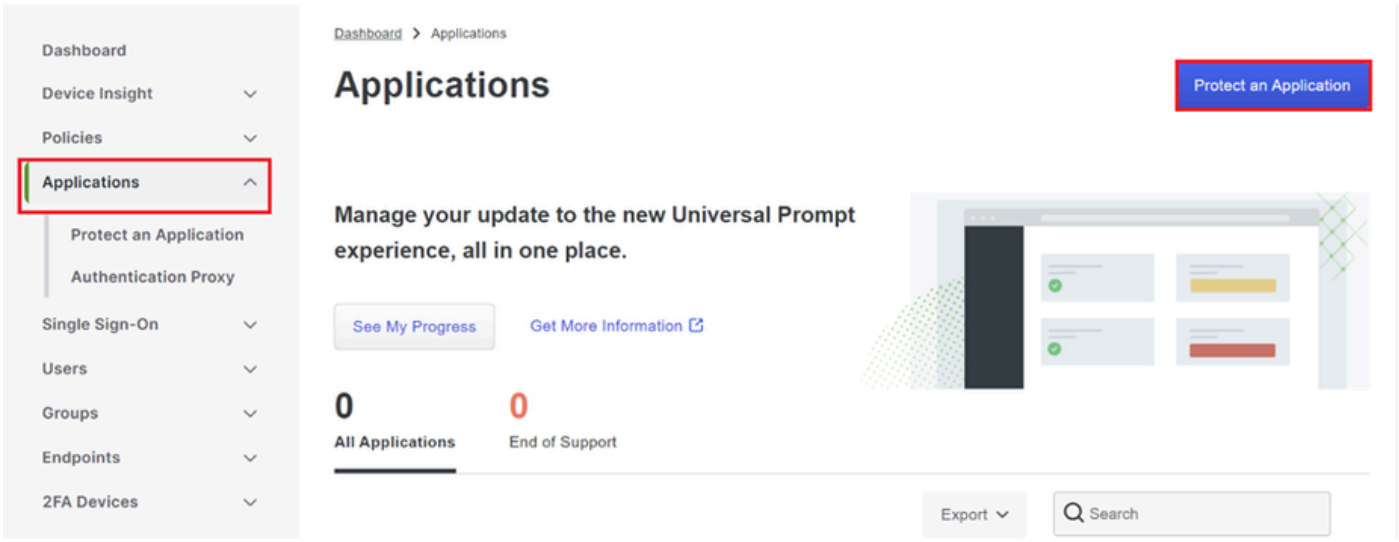
单击下一链接，访问DUO代理下载和安装指南:

https://duo.com/docs/authproxy-reference

将DUO Proxy与ISE和DUO Cloud集成。

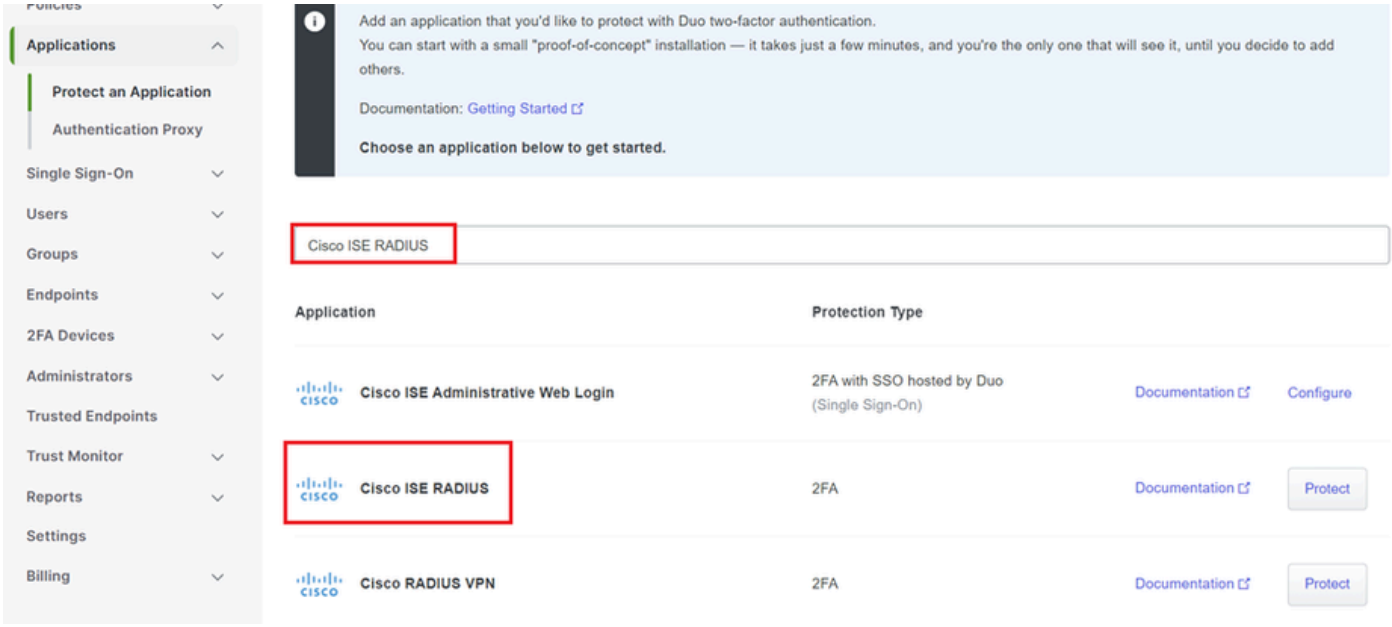
1.使用您的凭证登录DUO安全网站https://duo.com/。

2.定位至应用部分，然后选择保护应用程序以继续。



DUO应用程序

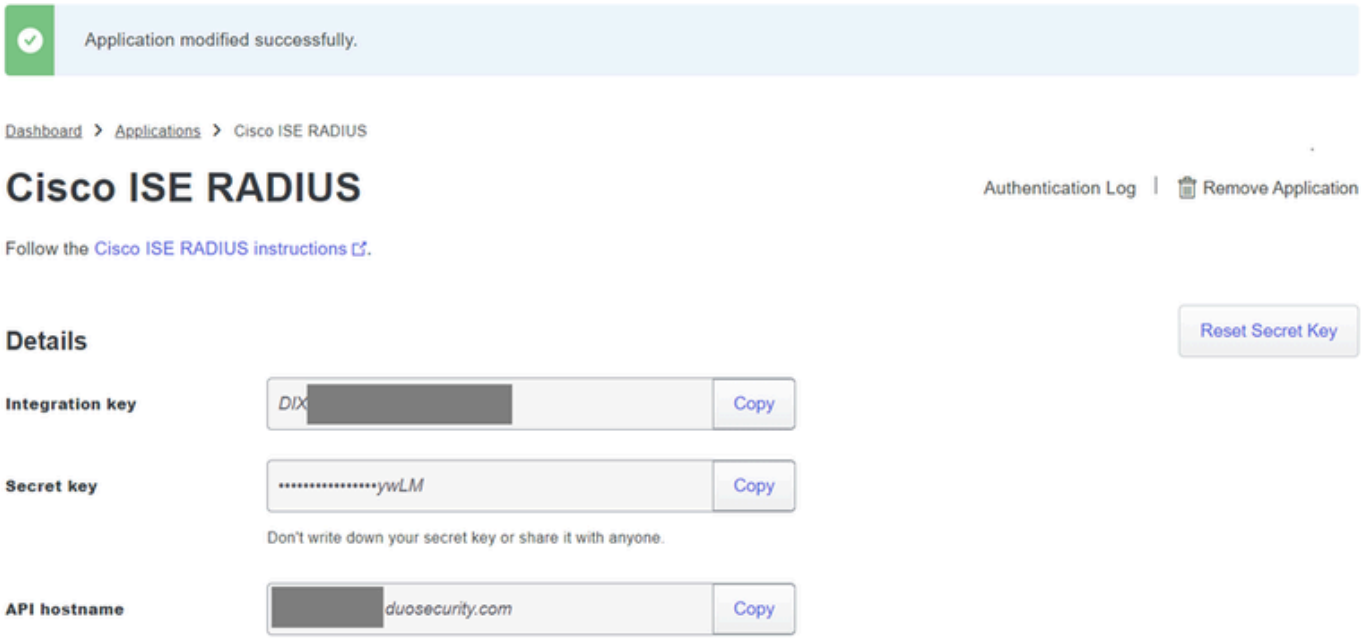
3.在列表中搜索“Cisco ISE RADIUS”选项，然后单击Protect将其添加到您的应用。



ISE RADIUS选项

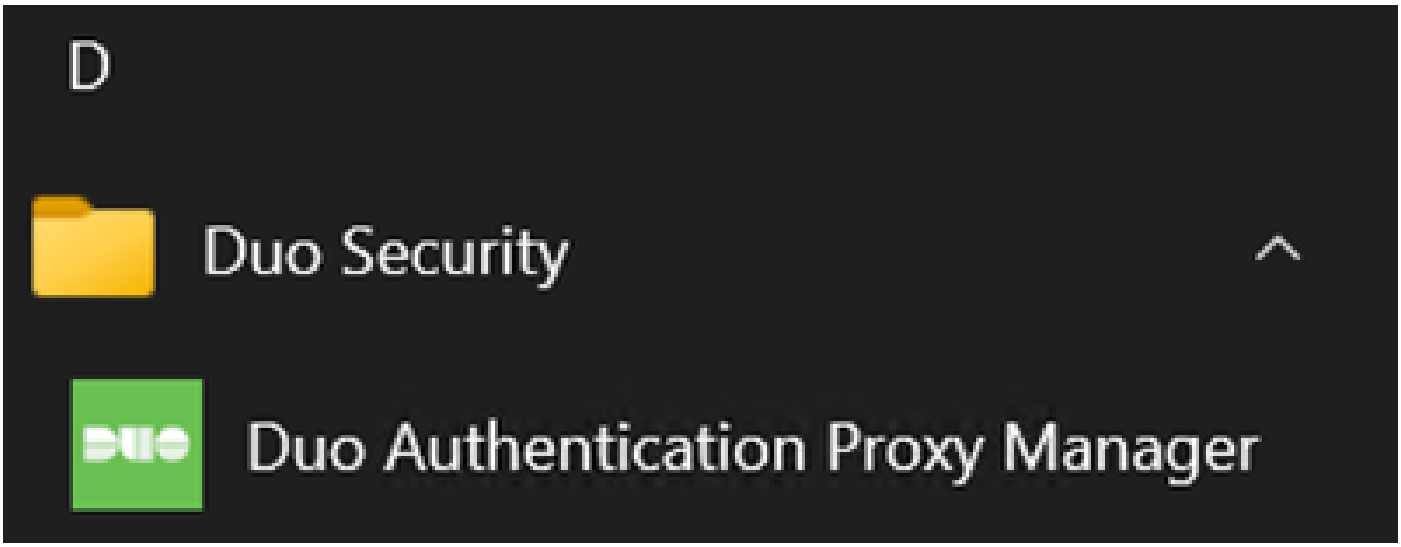
4.成功添加后，您将看到DUO应用程序的详细信息。向下滚动并单击Save。

5.复制提供的集成密钥、密钥和API主机名；这些对于即将采取的步骤至关重要。



ISE服务器详细信息

6.在系统上启动DUO Proxy Manager以继续设置。



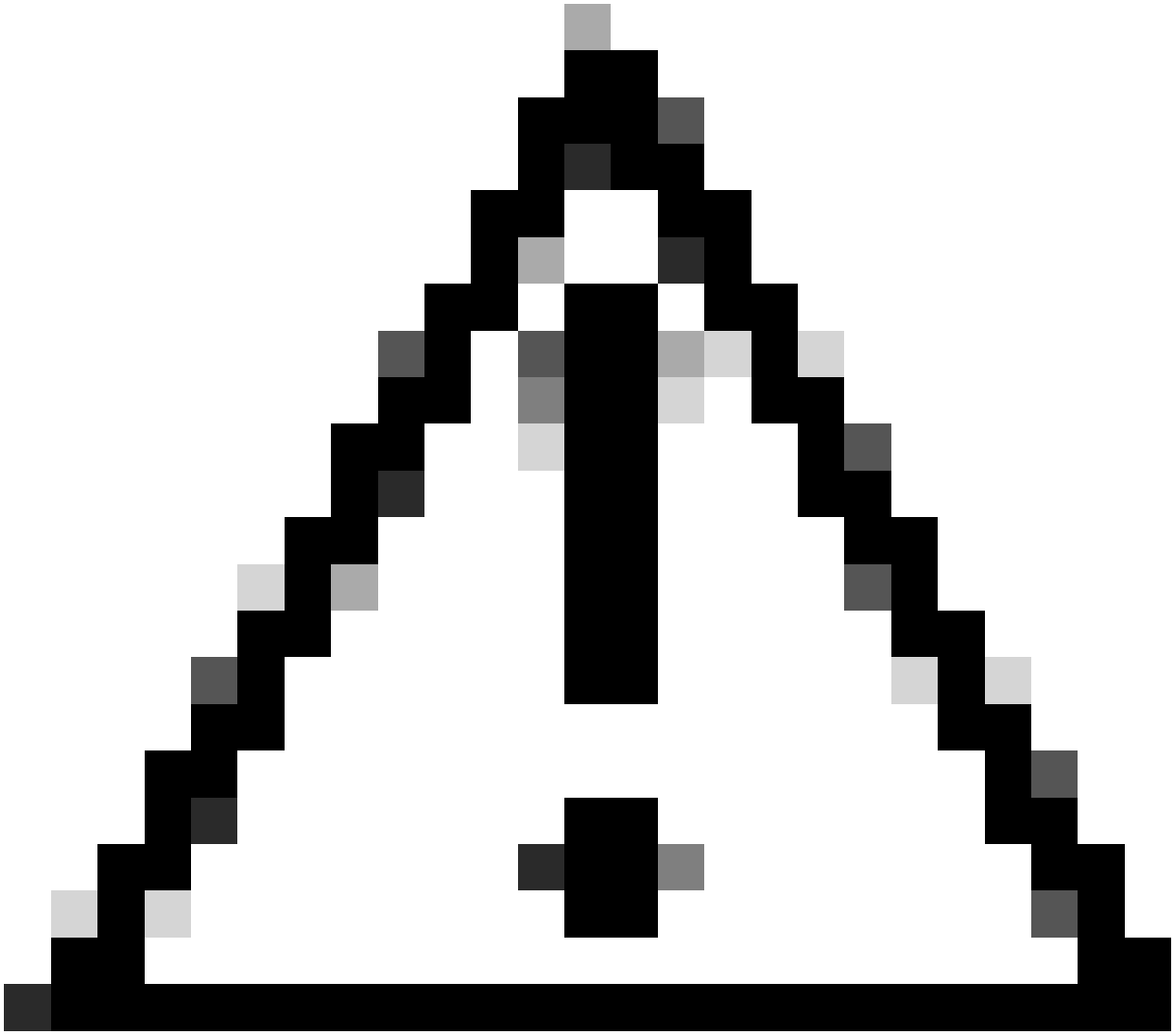
*DUO*代理管理器

7.（可选）如果您的DUO代理服务器需要代理配置才能连接到DUO云，请输入以下参数：

```
[main]
http_proxy_host=



http_proxy_port=
```



警告：确保用您的实际代理详细信息替换和。

8.现在，利用之前复制的信息完成集成配置。

```
[radius_server_auto]
ikey=


skey=


api_host=
```

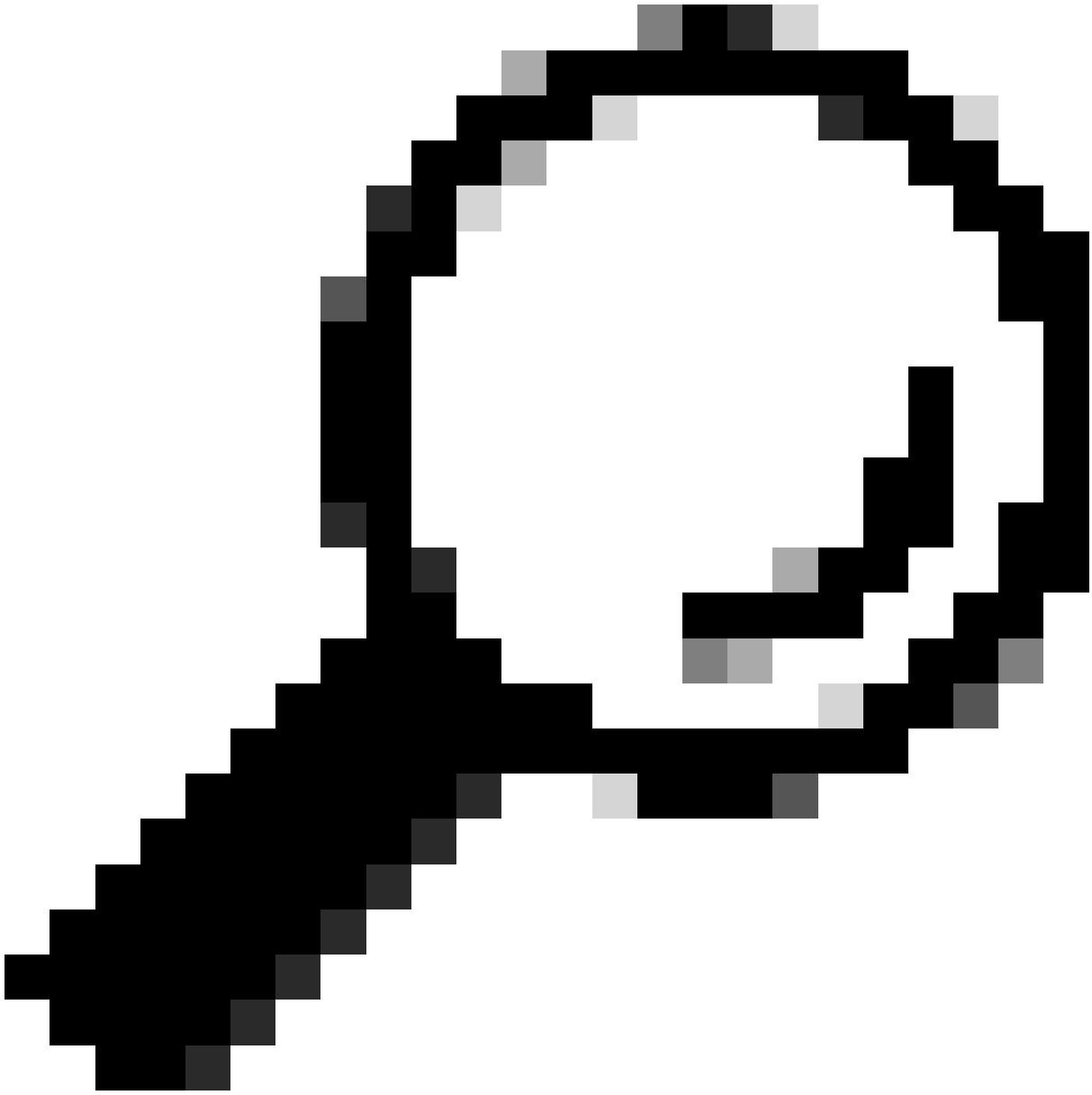
```
radius_ip_1=



radius_secret_1=



failmode=safe
port=1812
client=ad_client
```



提示：line client=ad_client表示DUO代理使用Active Directory帐户进行身份验证。确保此信息正确无误，以完成与Active Directory的同步。

将DUO与Active Directory集成。

1.将DUO身份验证代理与Active Directory集成。

```
[ad_client]
host=
```

```
service_account_username=
```

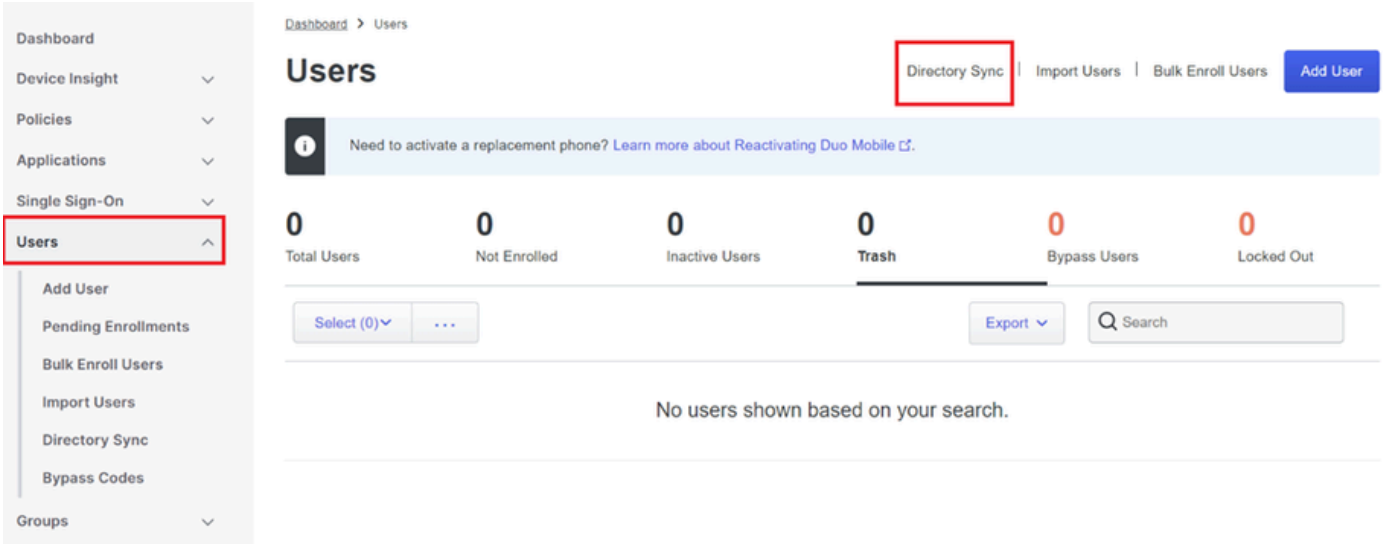
```
service_account_password=


search_dn=DC=

           ,DC=
```

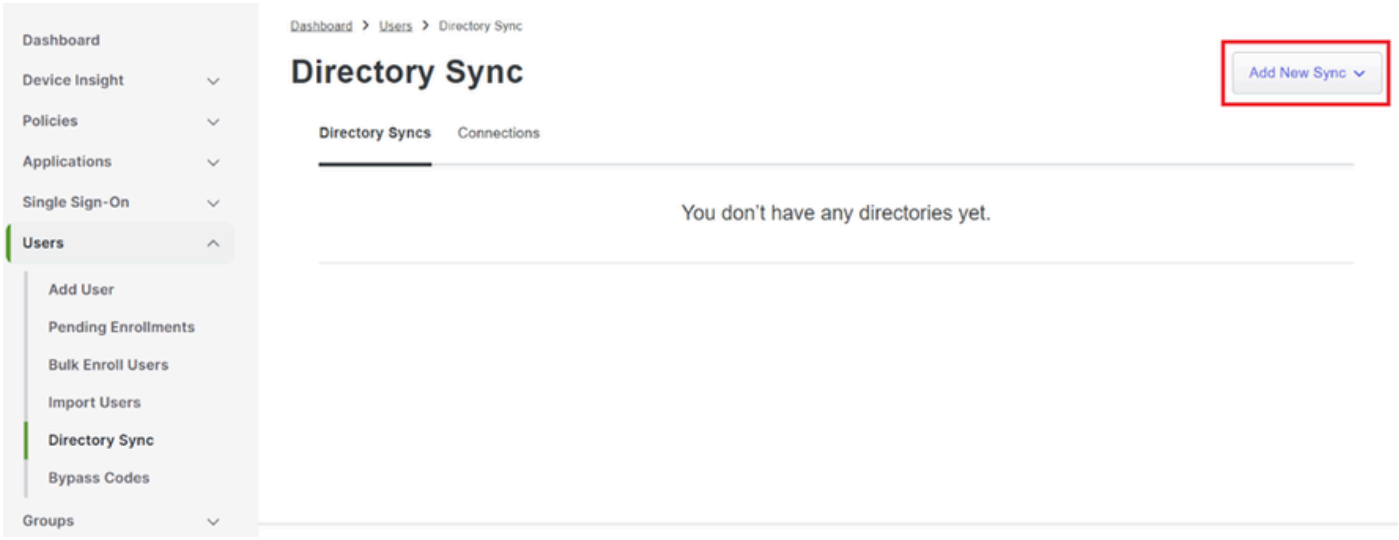
2.使用DUO云服务加入Active Directory。登录https://duo.com/。

3.导航到“用户”，然后选择“目录同步”管理同步设置。



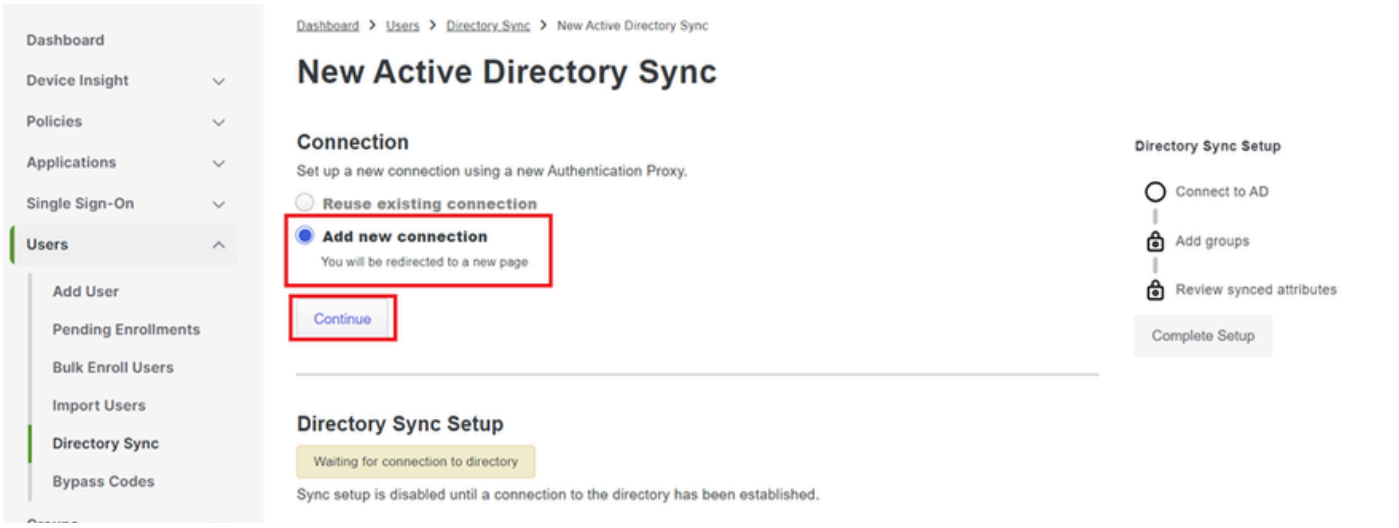
目录同步

4.单击“添加新同步”，然后从提供的选项中选择“Active Directory”。



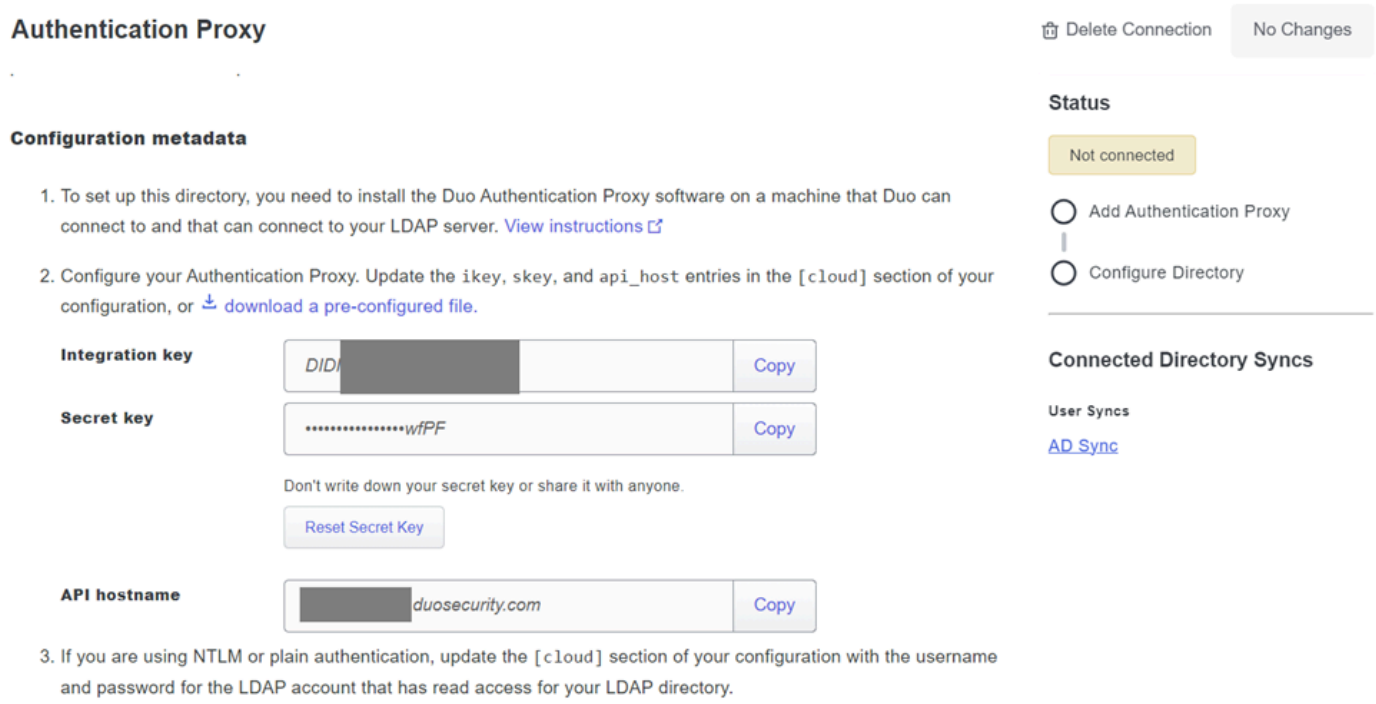
添加新同步

5.选择Add new connection，然后单击Continue。



添加新的*Active Directory*

6.复制生成的集成密钥、密钥和API主机名。



身份验证代理详细信息

7.返回DUO身份验证代理配置并使用您获得的新参数以及Active Directory管理员的服务帐户凭据配置[cloud]部分：

```
[cloud]
ikey=



skey=



api_host=



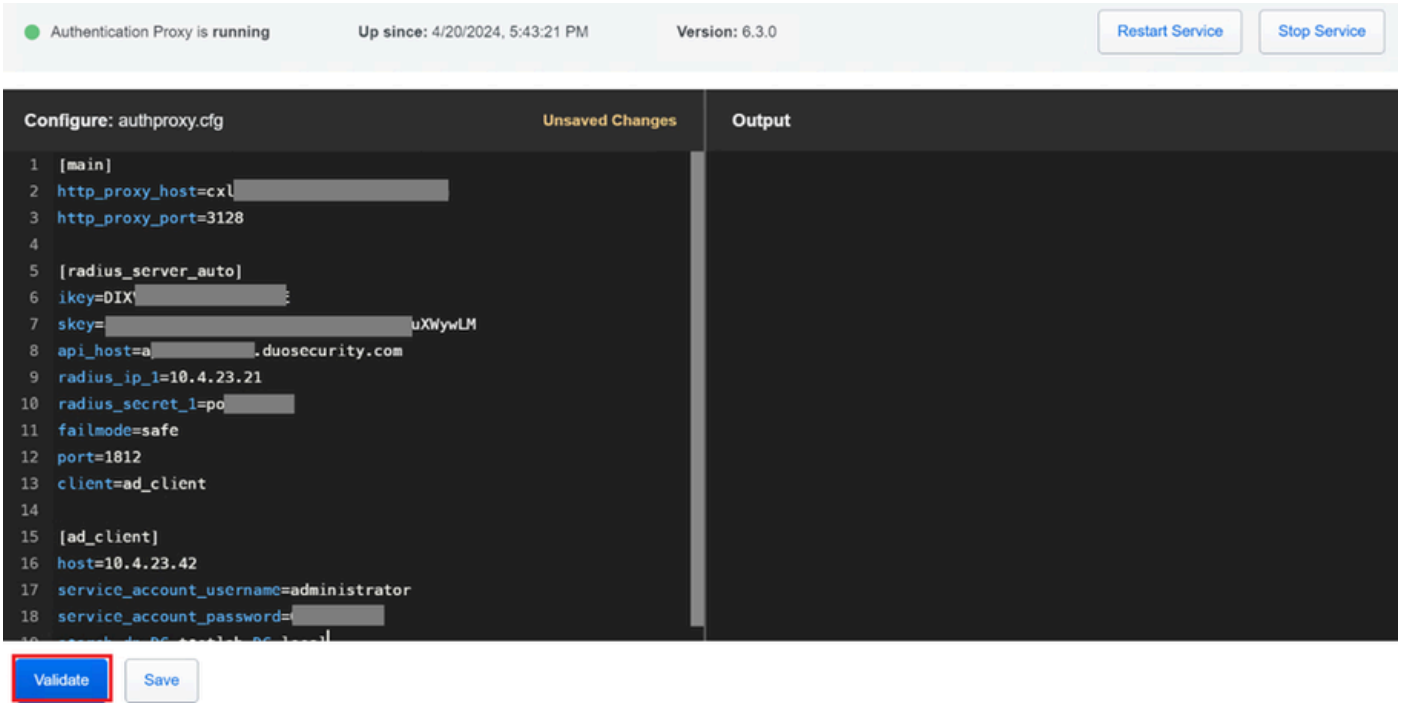
service_account_username=

          \



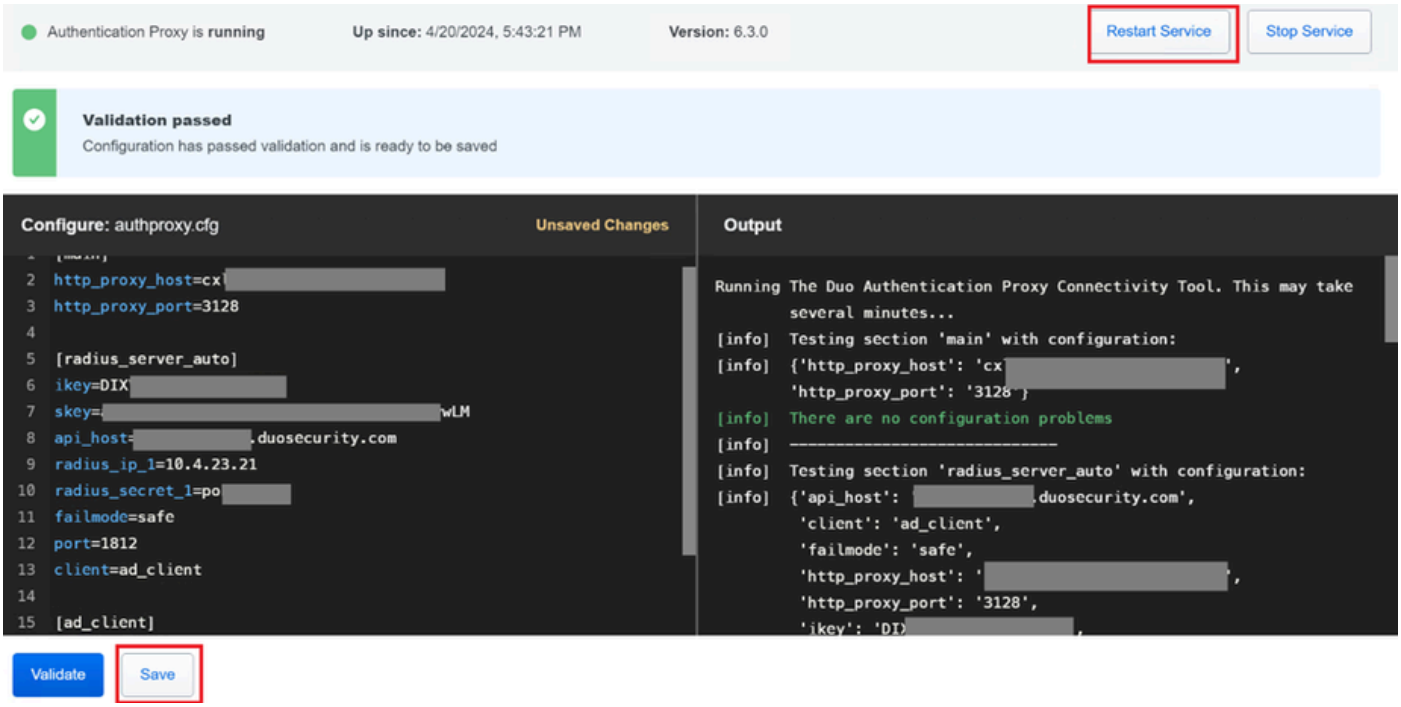
service_account_password=
```

8.通过选择“validate”选项验证您的配置，以确保所有设置都正确。



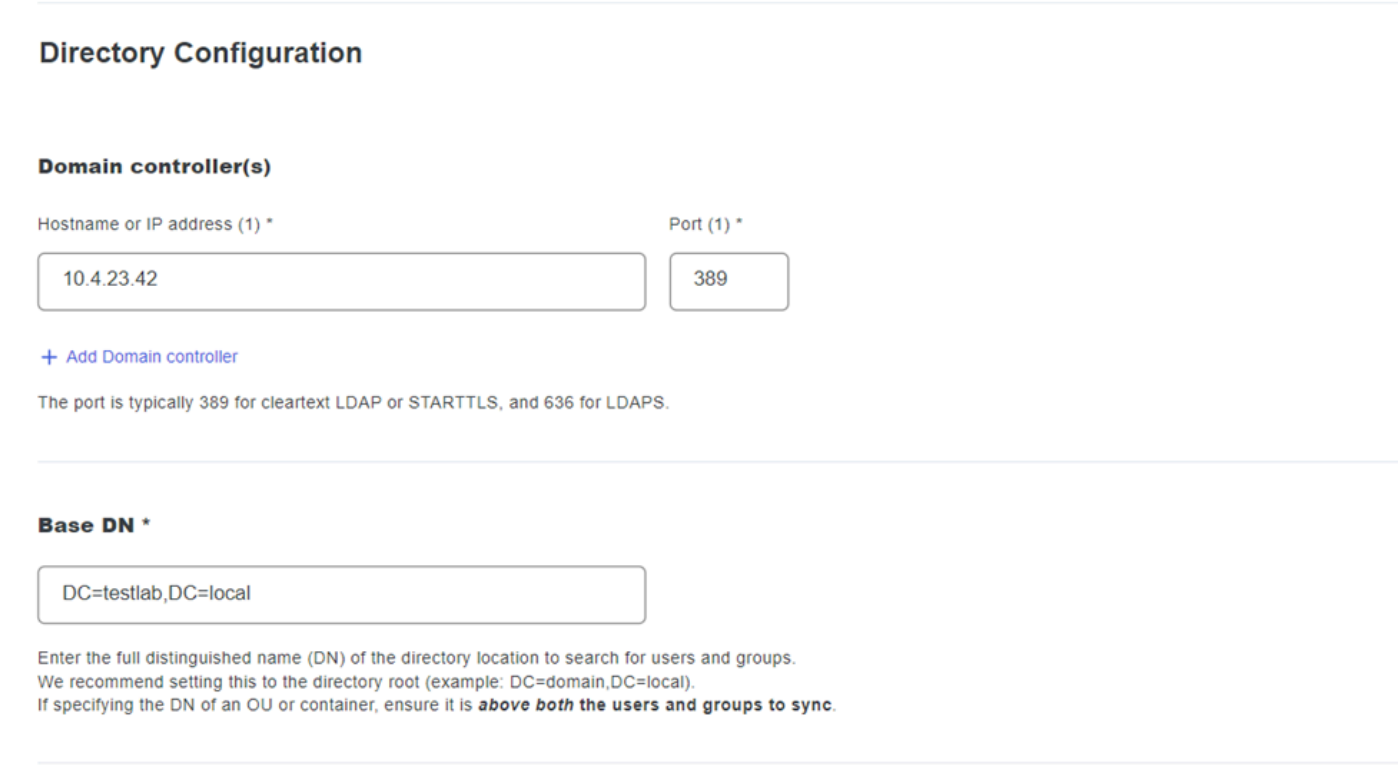
代理*DUO*的配置。

9.验证后，保存配置并重新启动DUO身份验证代理服务以应用更改。



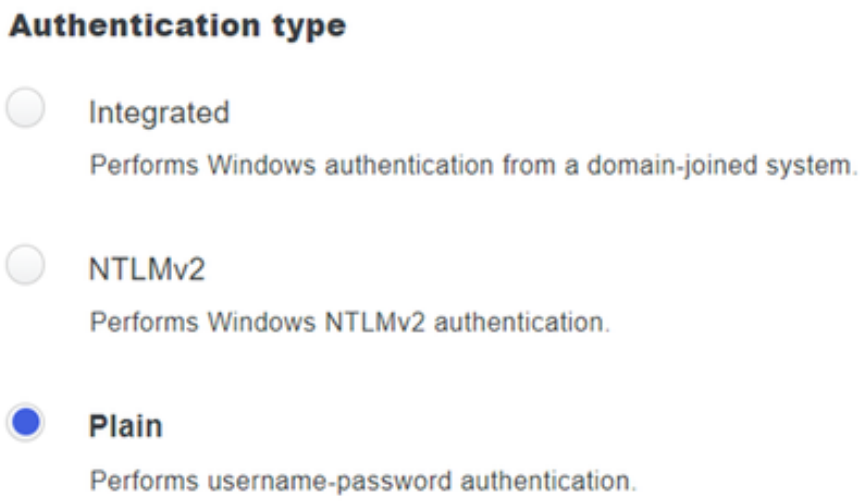
*Restart Service*选项。

10.返回DUO管理控制面板，输入Active Directory服务器的IP地址以及用户同步的基本DN。



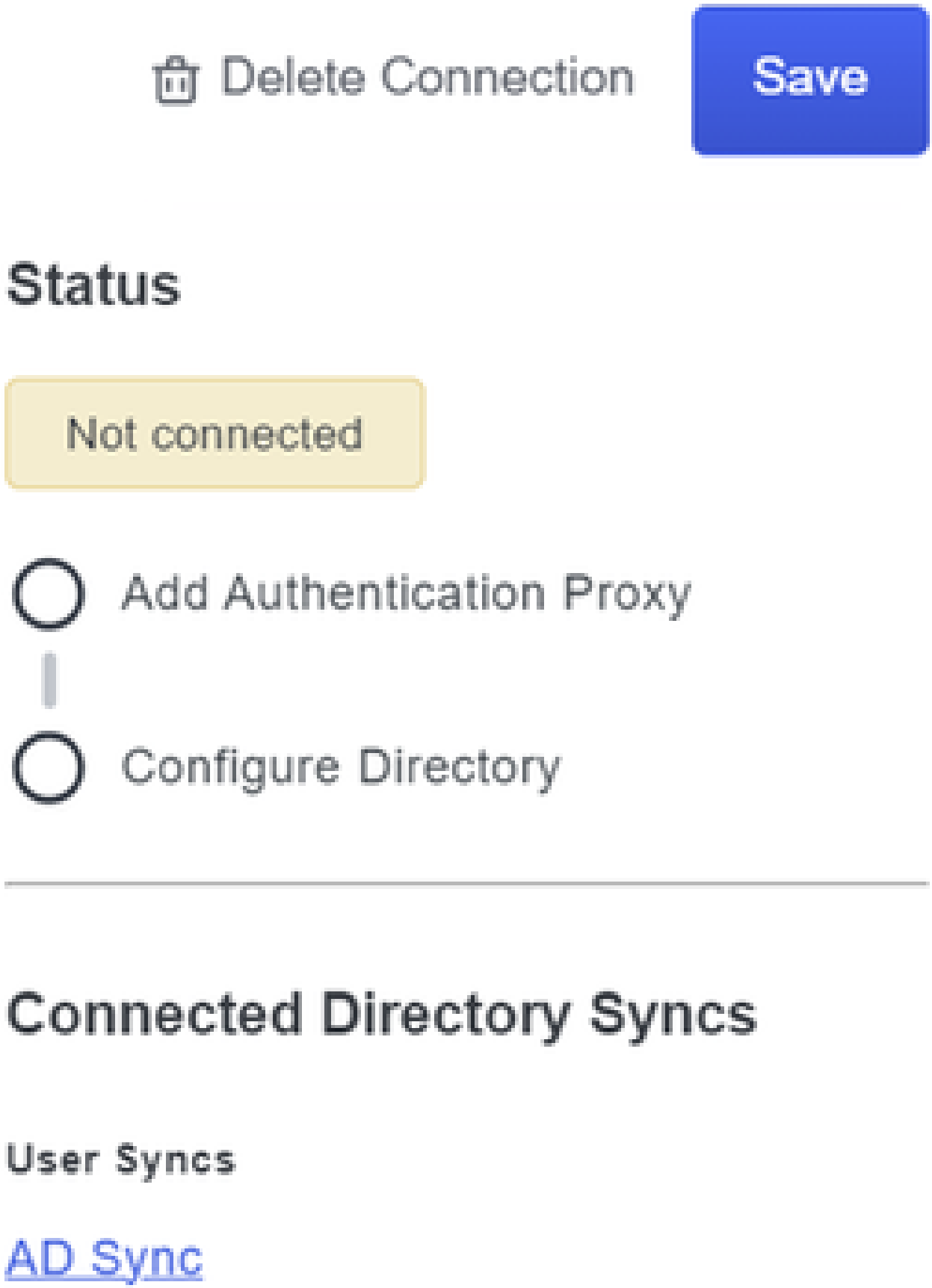
目录设置。

11.选择Plain选项以配置系统以进行非NTLMv2身份验证。



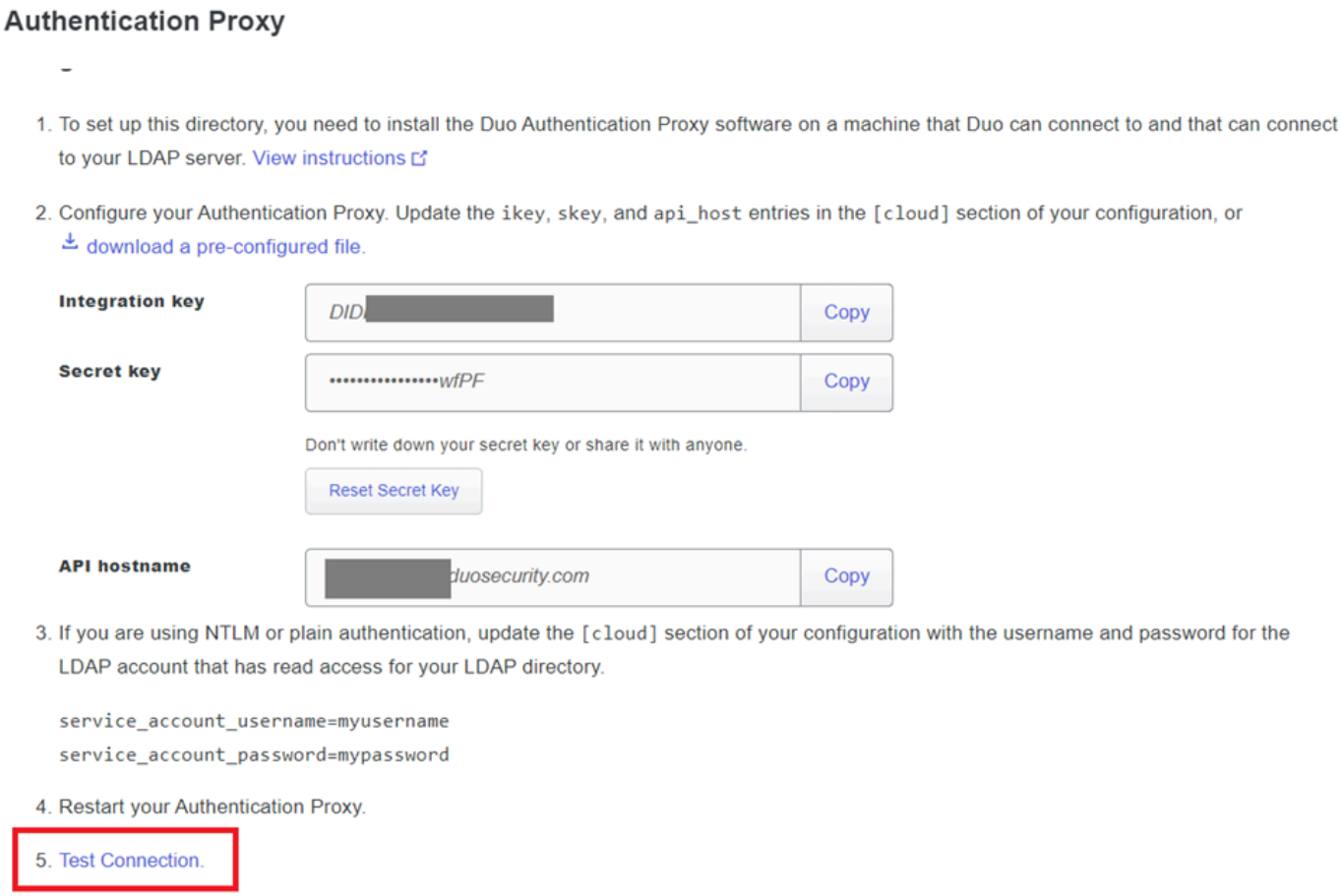
认证类型.

12.保存新设置以确保配置已更新。



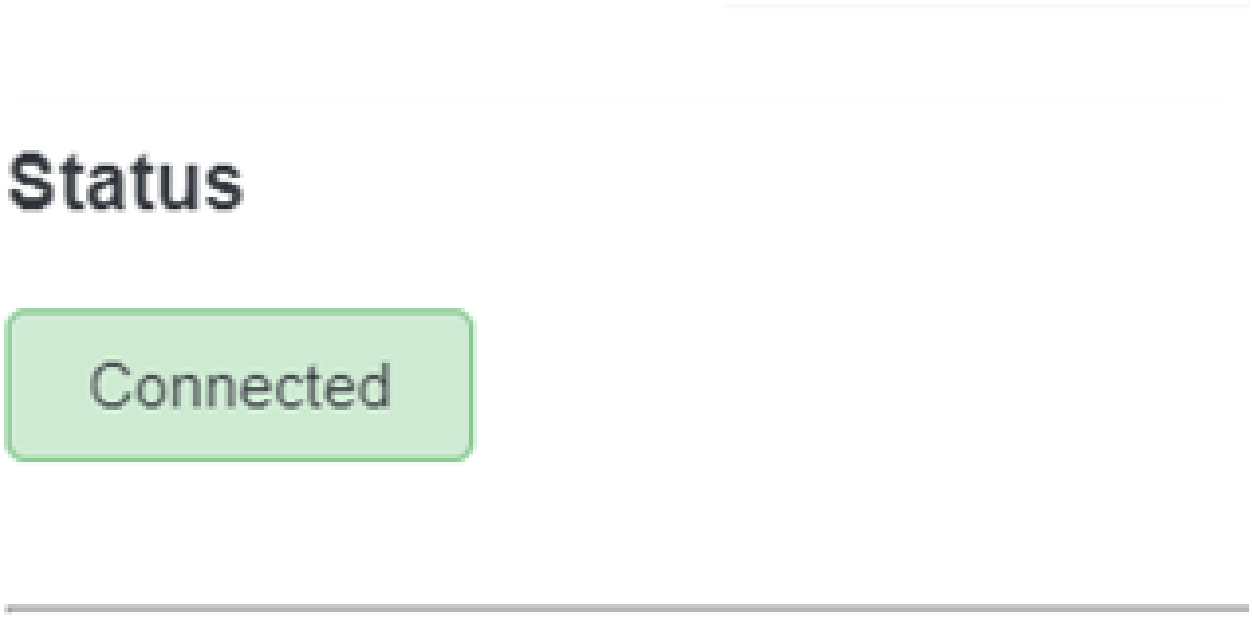
*Save*选项

13.使用“test connection”功能验证DUO云服务可以与您的Active Directory通信。



测试连接选项。

14.确认Active Directory状态显示为“Connected”，表示已成功集成。

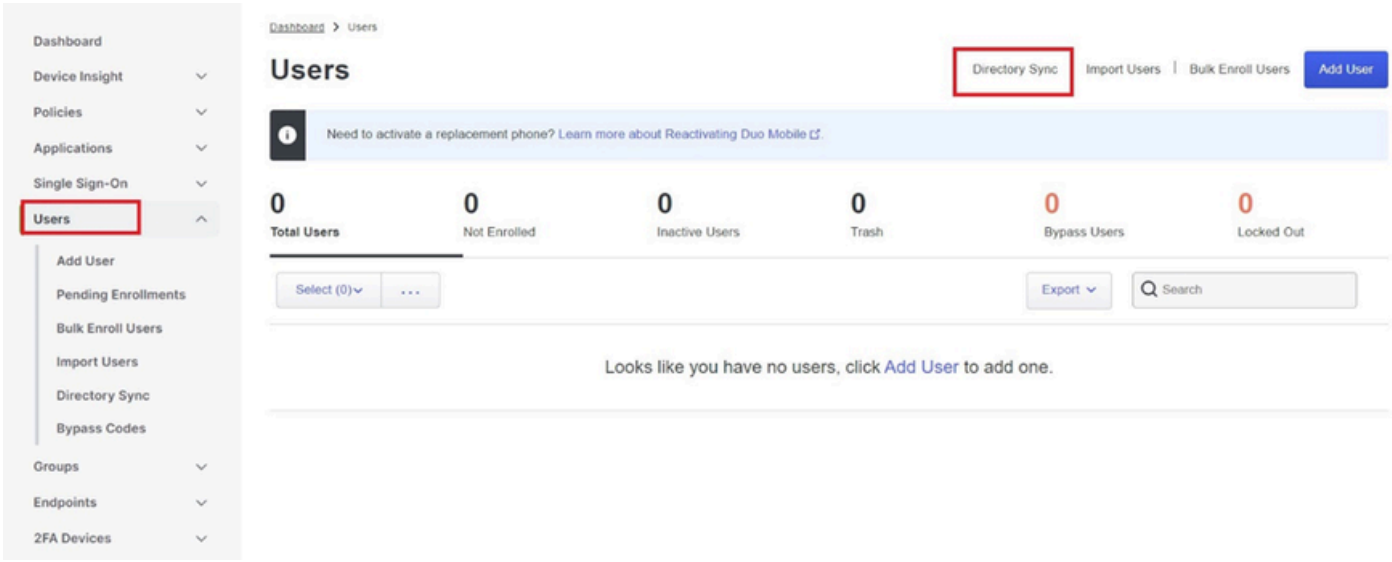


状态成功。

通过DUO云从Active Directory(AD)导出用户帐户。

1.在Duo Admin面板中导航到Users > Directory Sync，以查找与Active Directory进行目录同步相关

的设置。

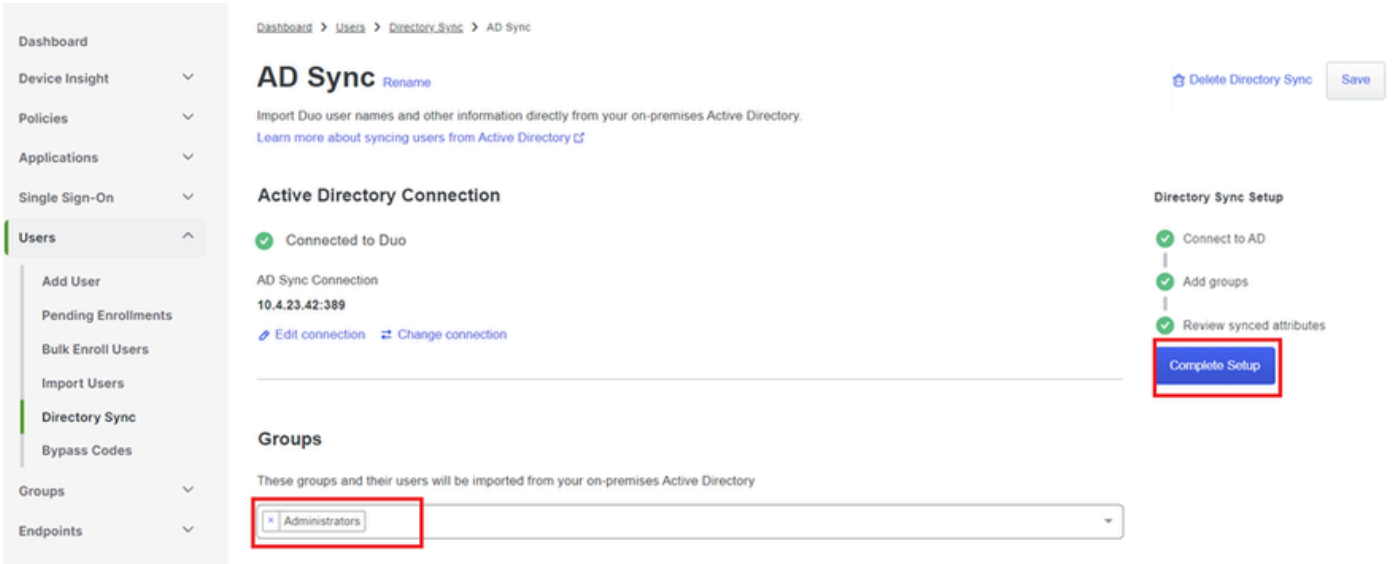


用户列表.

2.选择要管理的Active Directory配置。

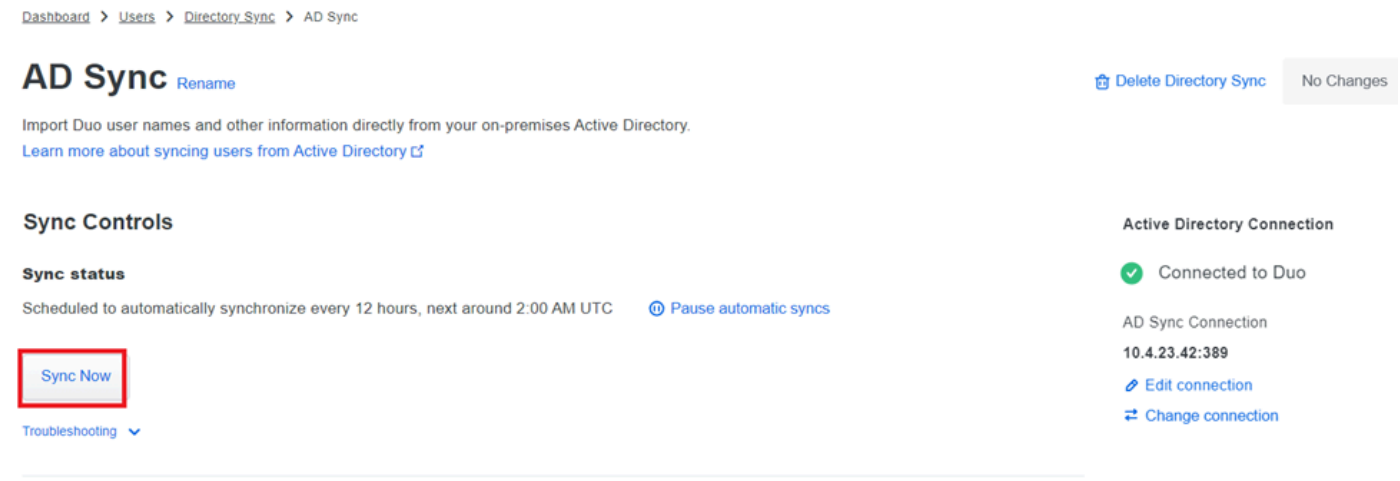
3.在配置设置中，确定并选择要与Duo Cloud同步的Active Directory中的特定组。考虑使用过滤选项进行选择。

4.单击完成设置。



*AD*同步。

5.要立即启动同步，请单击立即同步。这会将用户帐户从Active Directory中的指定组导出到双核云，从而允许它们在双核安全环境中进行管理。



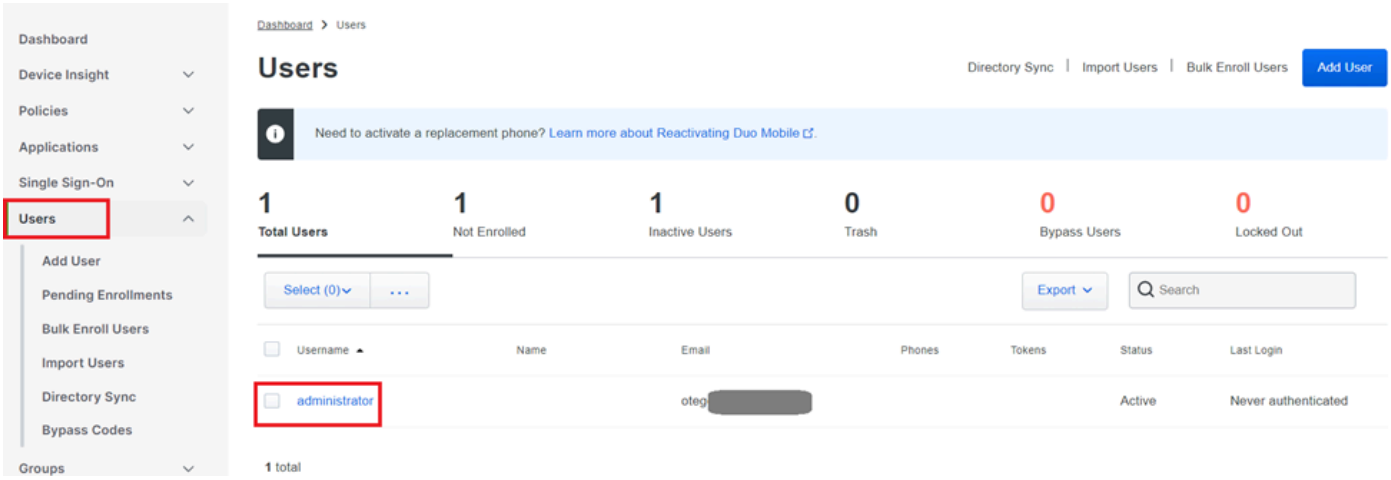
正在启动同步

在Cisco DUO云中注册用户。

用户注册通过各种方法启用身份验证，例如代码访问、DUO推送、SMS代码和令牌。

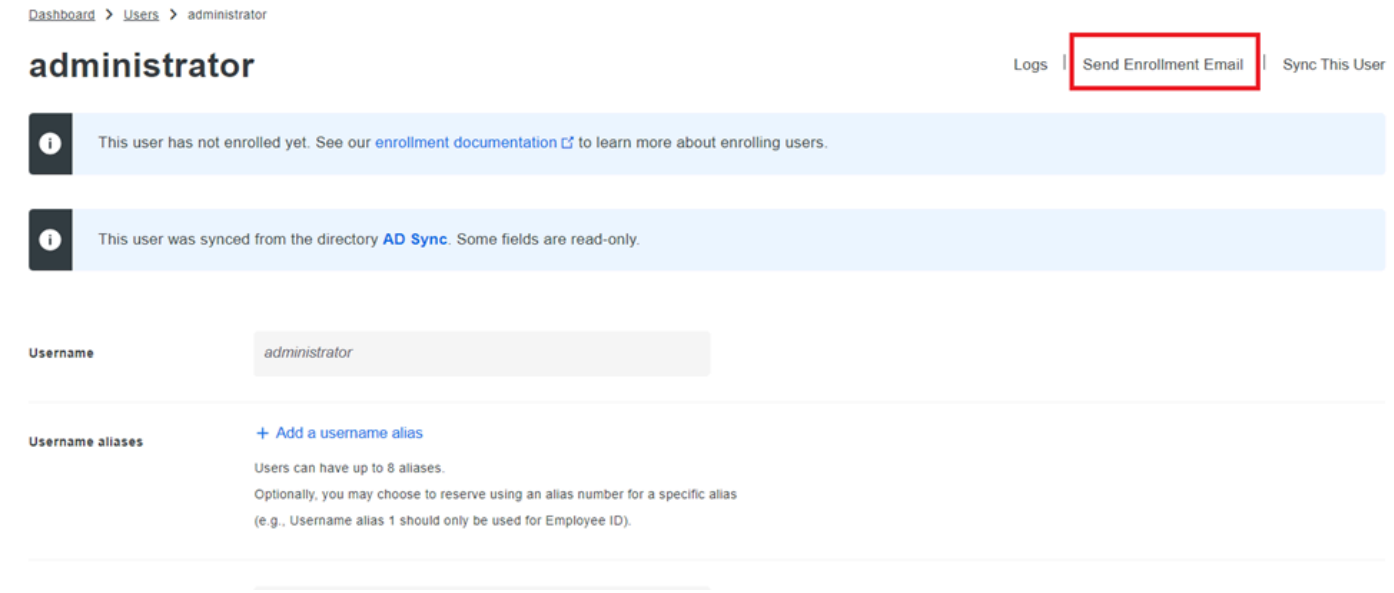
1.导航至Cisco Cloud控制面板中的Users部分。

2.找到并选择要注册的用户帐户。



用户帐户列表。

3.单击Send Enrollment Email按钮以启动登记流程。



通过电子邮件进行注册。

4.检查电子邮件收件箱并打开注册邀请以完成身份验证过程。

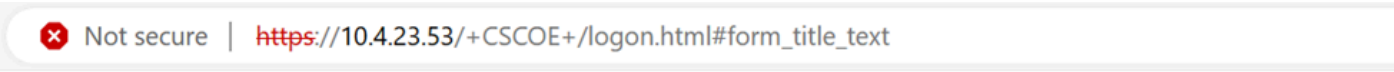
有关注册流程的其他详细信息，请参阅以下资源：

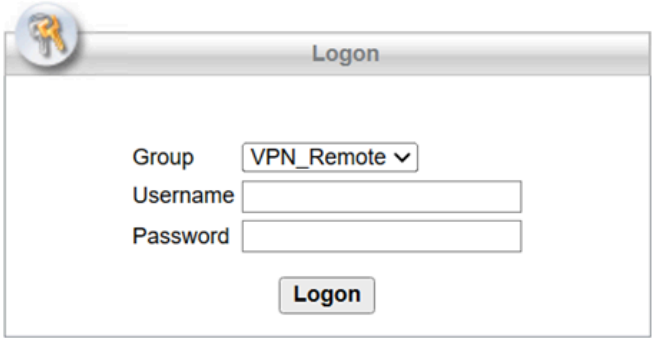
- 通用注册指南：https://guide.duo.com/universal-enrollment
- 传统注册指南：https://guide.duo.com/traditional-enrollment

配置验证过程。

为确保您的配置准确且可操作，请验证后续步骤：

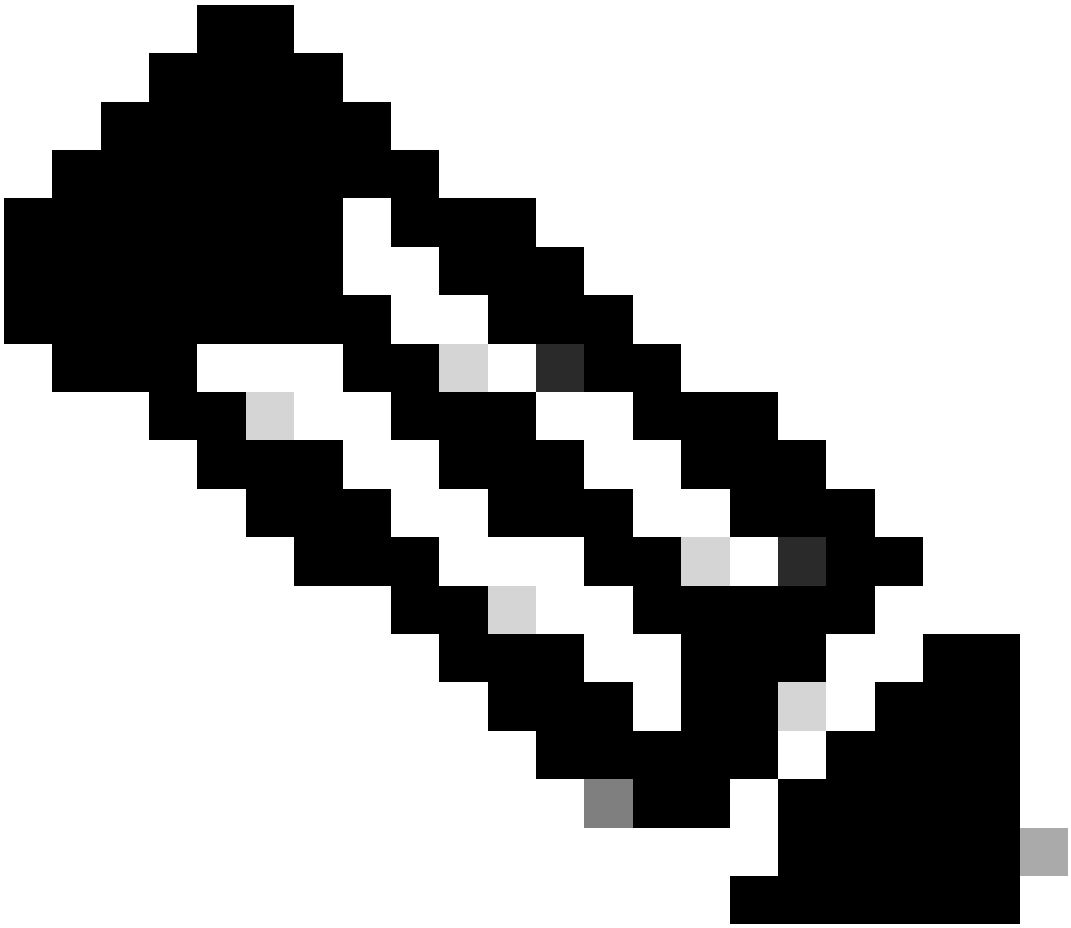
1.启动Web浏览器并输入Firepower威胁防御(FTD)设备的IP地址以访问VPN接口。





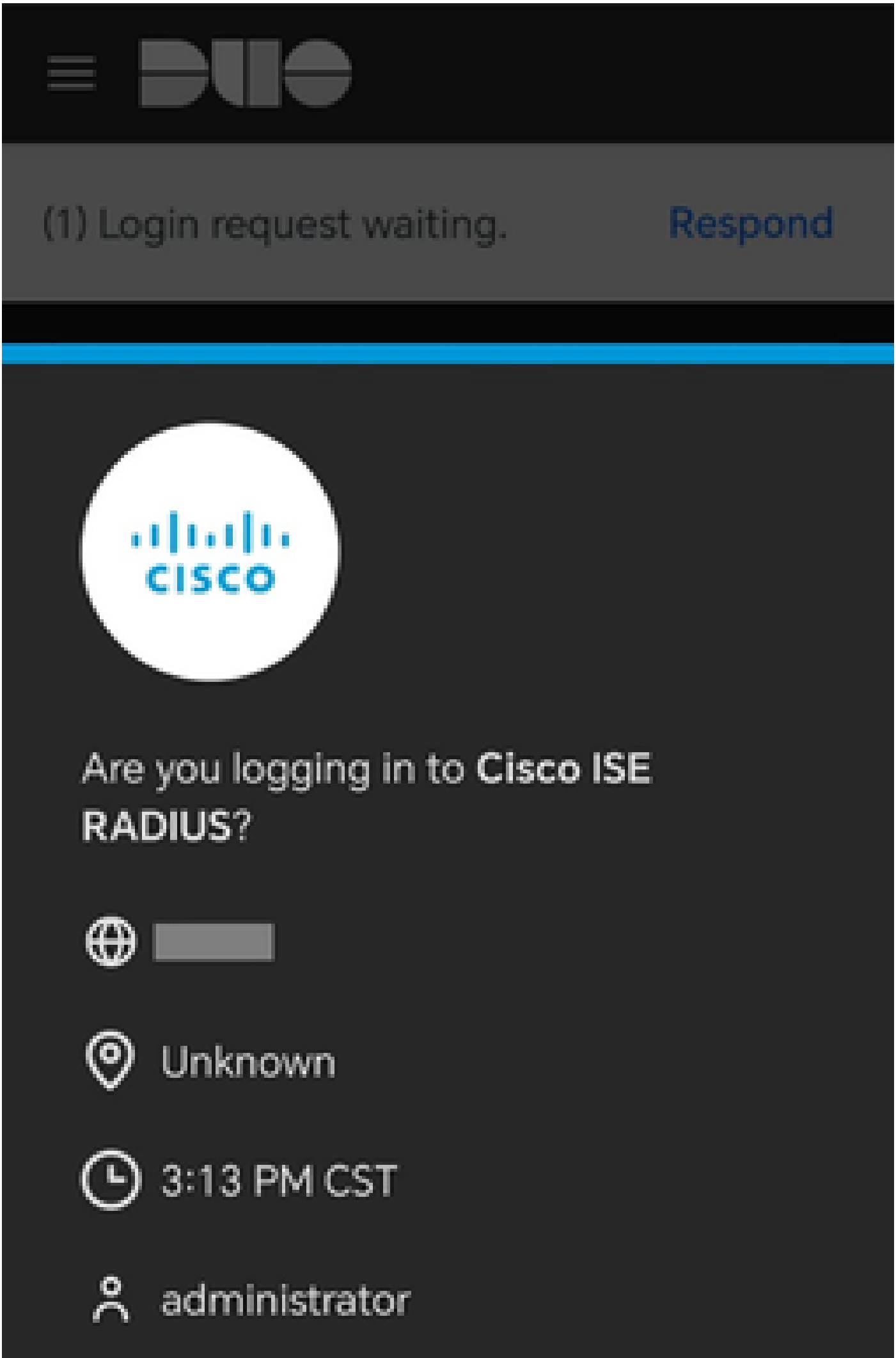
VPN登录。

2.根据提示输入用户名和密码。



注意：凭据是Active Directory帐户的一部分。

3.当您收到DUO Push通知时，请使用DUO Mobile软件批准该通知，以继续执行验证过程。


(1) Login request waiting.
Respond
Are you logging in to Cisco ISE RADIUS?
Unknown
3:13 PM CST
administrator

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）。

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）。