为RAVPN 2FA配置与AD和ISE的双核集成

目录

简介

先决条件

- 要求
- 使用的组件

网络图和场景

- 通信过程

Active Directory配置

Duo配置

Duo Auth代理配置

思科ISE配置

Cisco ASA RADIUS/ISE配置

- CLI 配置

Cisco ASA远程访问VPN配置

测试

故障排除

- 工作调试

常见问题

- 1.连接问题、错误的IP、Active Directory配置上无法解析的FQDN/主机名
- 2. Active Directory上管理员用户的密码错误
- 3.错误的基域
- 4.错误的iKey RADIUS值
- 5.验证ISE服务器发送访问请求数据包
- 6.使用NTRadPing实用程序验证Duo身份验证代理是否正常工作

简介

本文档介绍与AD和Cisco ISE的双向推送集成，作为连接到ASA的Cisco安全客户端的2FA。

先决条件

要求

Cisco 建议您了解以下主题：

- Duo应用程序
- Active Directory (AD)
- 身份服务引擎 (ISE)
- ASA上的RADIUS配置
- 自适应安全设备(ASA)上的远程访问VPN(RAVPN)配置

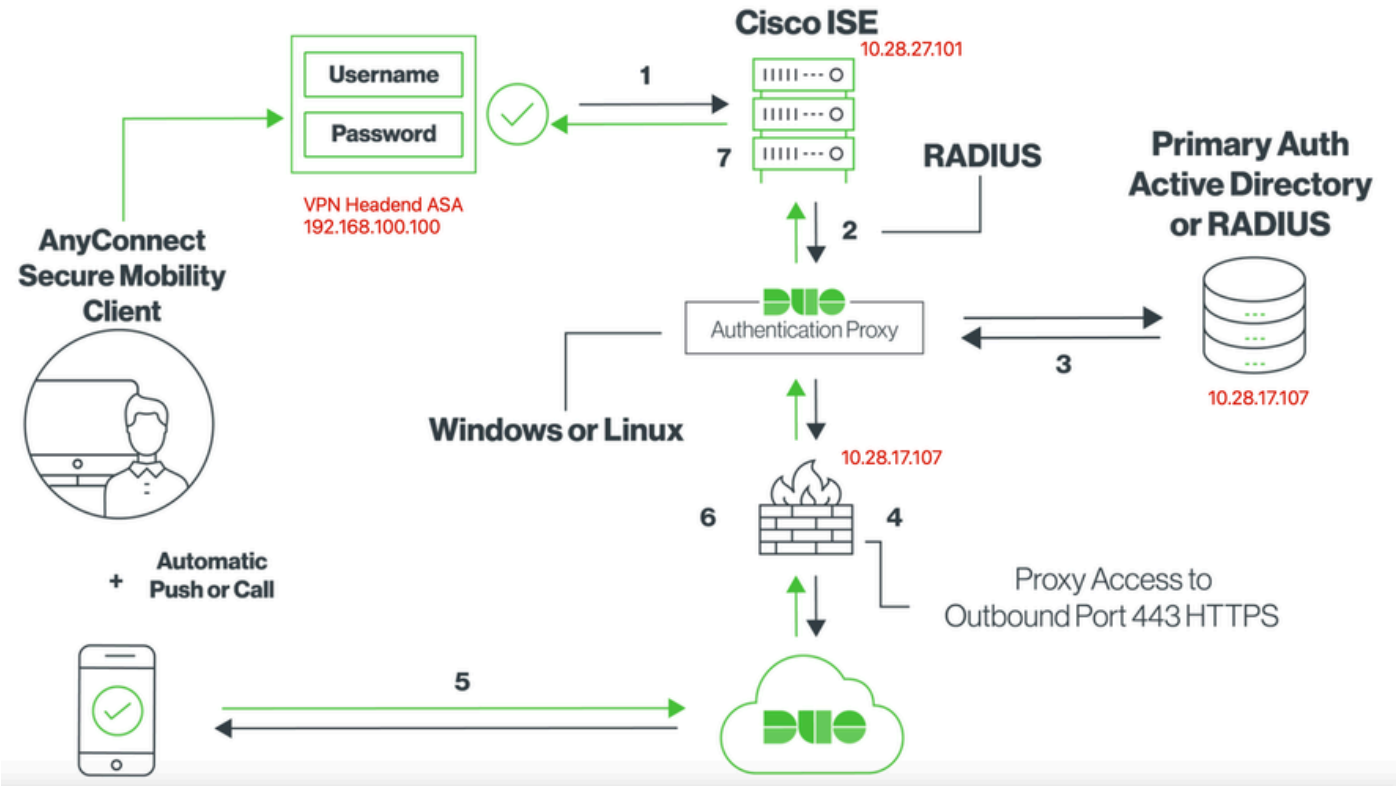
使用的组件

本文档中的信息基于以下软件和硬件版本：

- Duo服务器
- ISE服务器3.0
- ASA 9.14(3)18
- Microsoft 2016服务器
- Duo身份验证代理管理器

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。

网络图和场景



通信过程

思科ISE的双因素RADIUS身份验证

1. 主身份验证启动到Cisco ISE。
2. Cisco ASA向双身份验证代理发送身份验证请求。
3. 主身份验证使用Active Directory或RADIUS。
4. Duo Authentication Proxy connection established to Duo Security over TCP端口443。
5. 通过Duo Security的服务进行辅助身份验证。
6. Duo身份验证代理收到身份验证响应。
7. 已授予思科ISE访问权限。

用户帐户：

- Active Directory管理员：此帐户用作目录帐户，以允许Duo Auth代理绑定到Active Directory服务器以进行主身份验证。
- Active Directory测试用户
- Duo测试用户是否使用辅助2FA。

Active Directory配置

Windows Server已预配置了Active Directory域服务。

注意：如果RADIUS Duo Auth代理管理器在同一Active Directory主机上运行，则必须卸载/删除网络策略服务器(NPS)角色。如果两个RADIUS服务都运行，它们可能会冲突并影响性能。

要在远程访问VPN用户上实现身份验证和用户身份的AD配置，需要几个值。必须在Microsoft服务器上创建或收集所有这些详细信息，才能在ASA和双核身份验证代理服务器上完成配置。

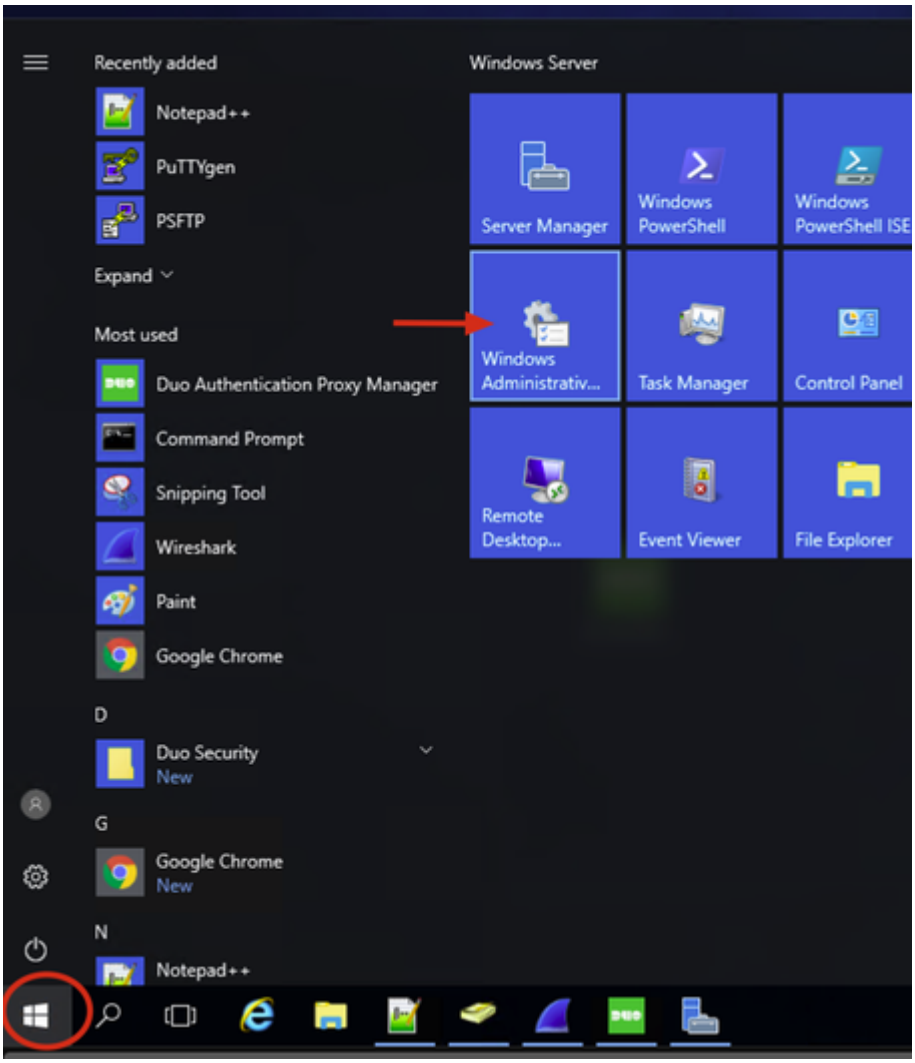
主要值包括：

- 域名：这是服务器的域名。在本配置指南中，agarciam.cisco是域名。
- 服务器IP/完全限定域名(FQDN)地址：用于访问Microsoft服务器的IP地址或FQDN。如果使用FQDN，则必须在ASA和Duo Auth代理中配置DNS服务器以解析FQDN。在本配置指南中，此值为agarciam.cisco，解析为10.28.17.107。
- 服务器端口:LDAP服务使用的端口。默认情况下，LDAP和STARTTLS使用TCP端口389进行LDAP，LDAP over SSL(LDAPS)使用TCP端口636。
- 根 CA:如果使用LDAPS或STARTTLS，则需要用于签署LDAPS所用SSL证书的根CA。

- 目录用户名和密码:这是Duo Auth代理服务器用于绑定到LDAP服务器并对用户和组进行身份验证和搜索的帐户。
- 基本和组可分辨名称(DN):基础DN是Duo Auth代理的出发点，并提醒Active Directory开始搜索和验证用户。

在本配置指南中，根域agarciam.cisco用作基础DN，组DN为Duo-USERS。

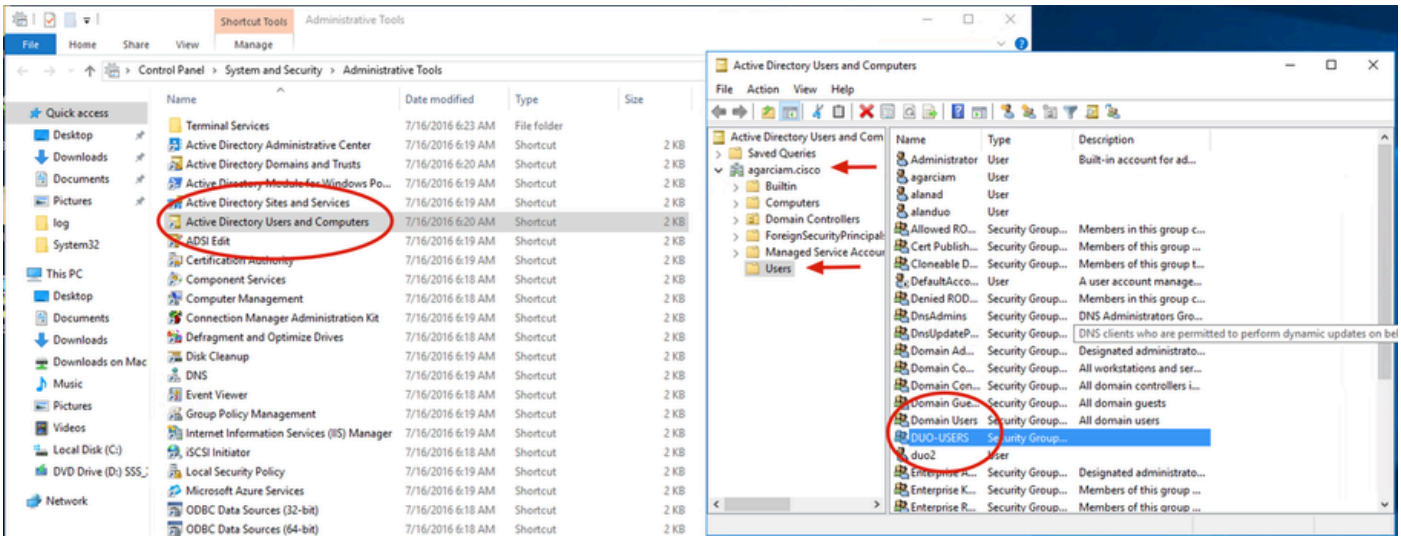
1.要在Windows Server上添加新的Duo用户，请导航到左下角的Windows图标，然后单击Windows管理工具:



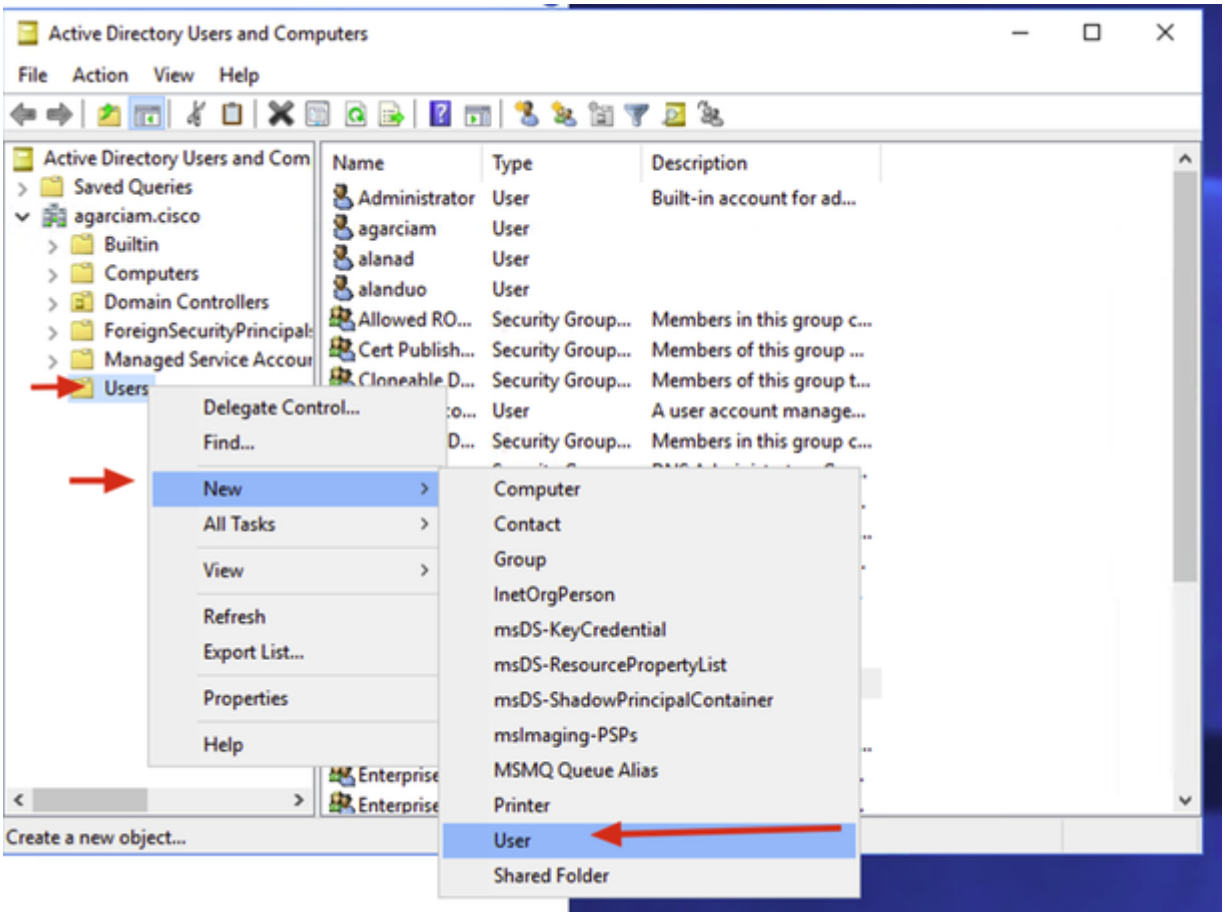
2.在“Windows管理工具”窗口中，导航到Active Directory用户和计算机。

3.在Active Directory用户和计算机面板上，展开域选项并导航到Users文件夹。

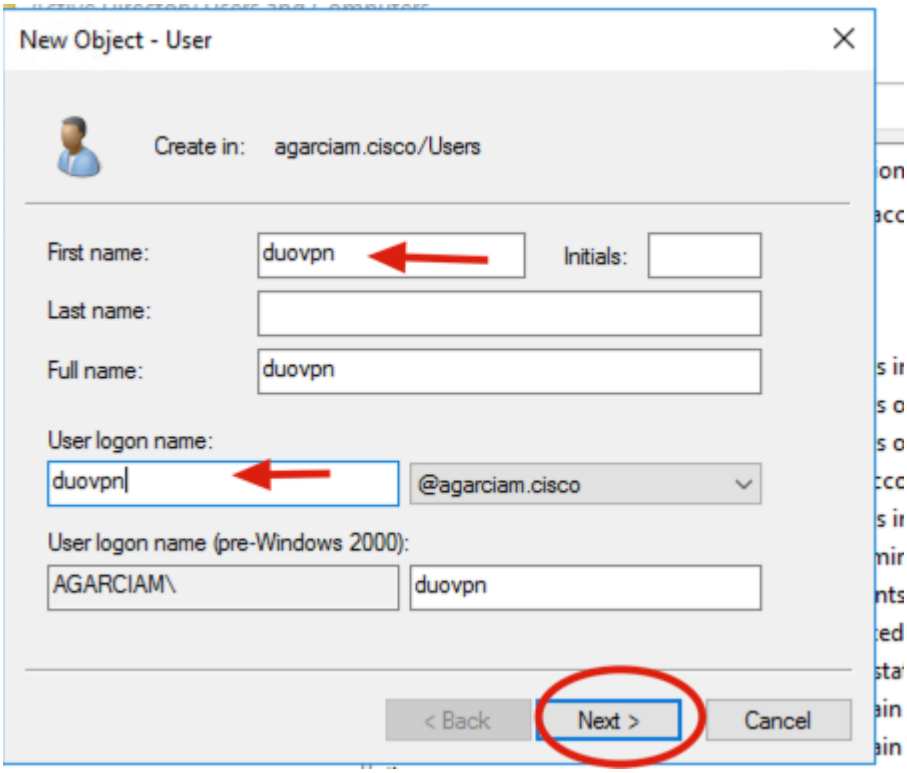
4.在此配置示例中，Duo-USERS用作辅助身份验证的目标组。



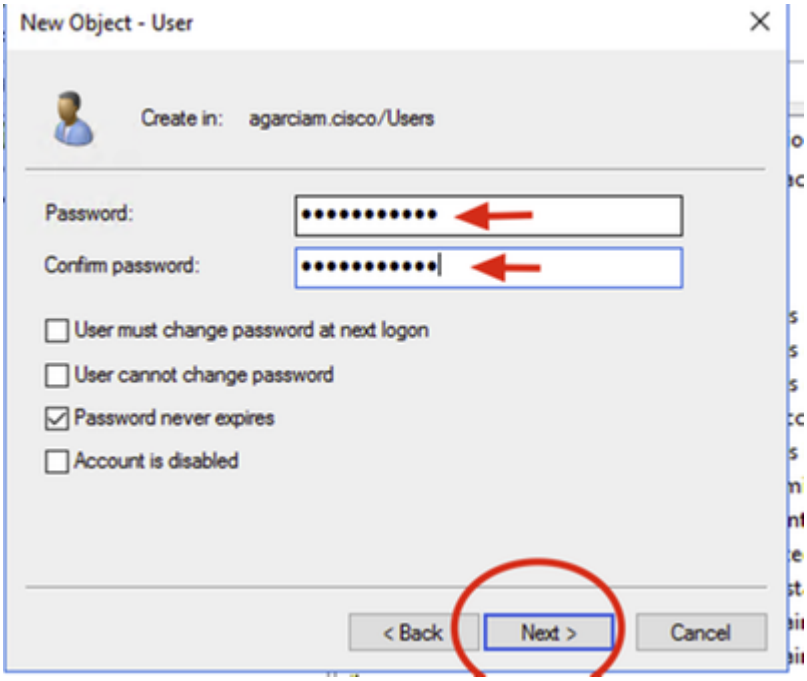
5.右键单击Users文件夹，然后选择New > User:



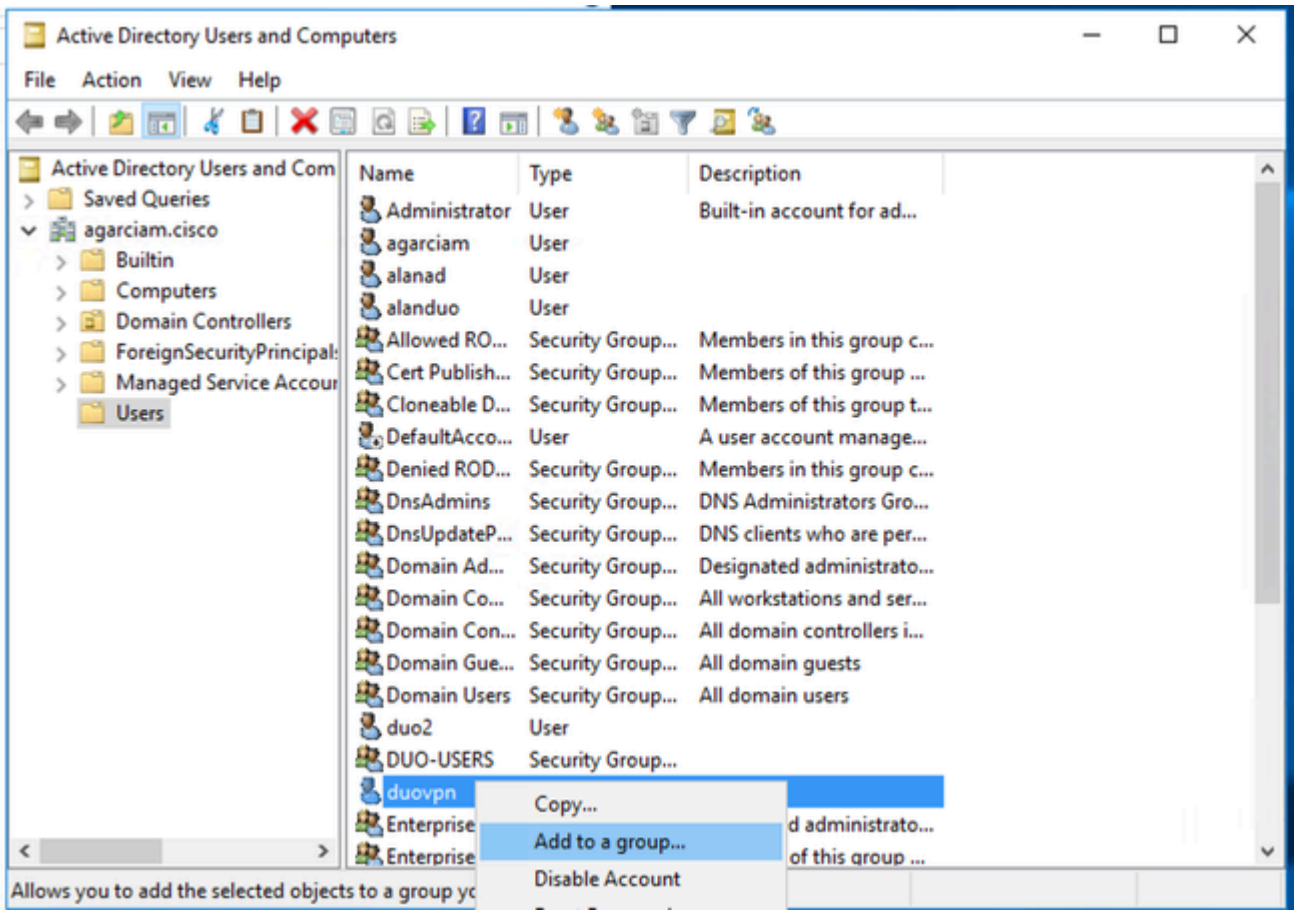
6.在“新建对象 — 用户”窗口中，指定新用户的身份属性，然后单击下一步:



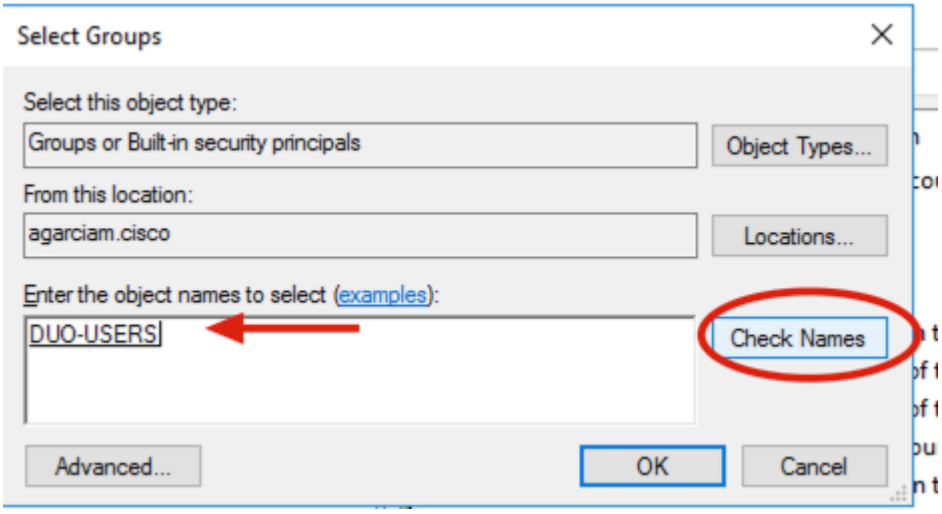
7.确认密码，并在验证用户信息后单击下一步，然后单击完成。



8.将新用户分配给特定组，右键单击并选择“添加到组”:



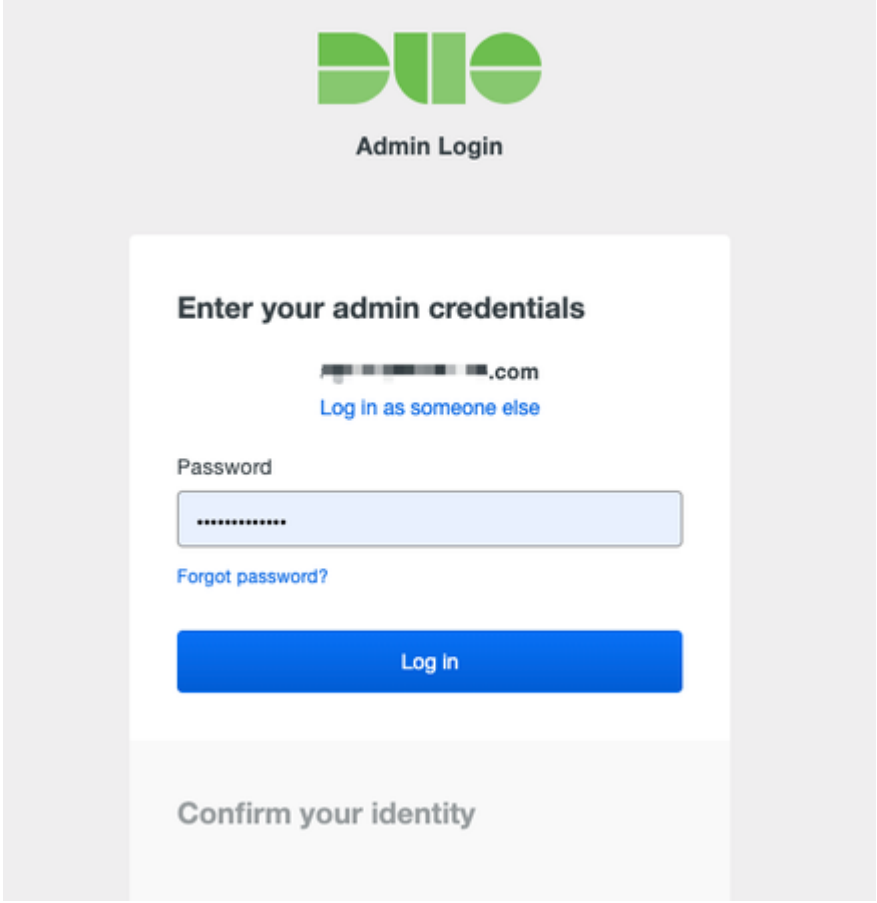
9.在“选择组”面板上，键入所需组的名称，然后单击检查名称。然后，选择符合条件的名称，然后单击Ok。



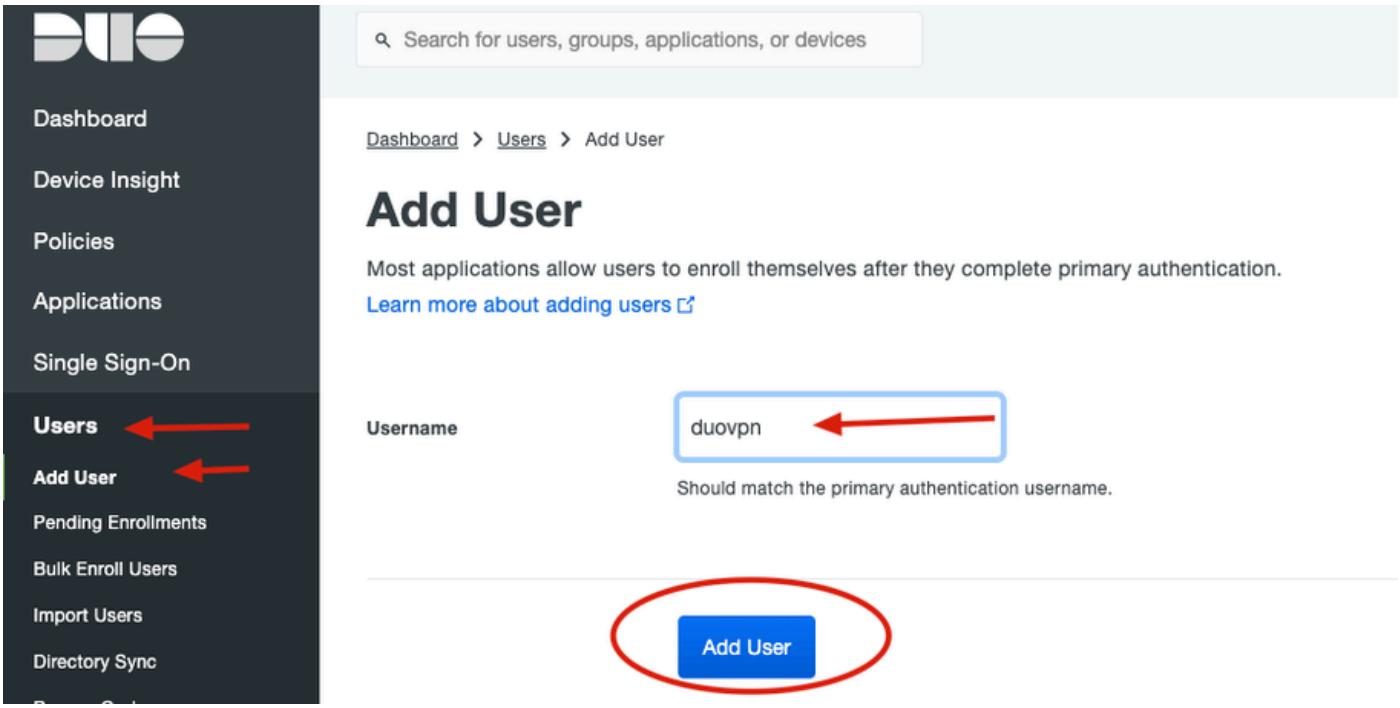
10.这是本文档中用作示例的用户。

Duo配置

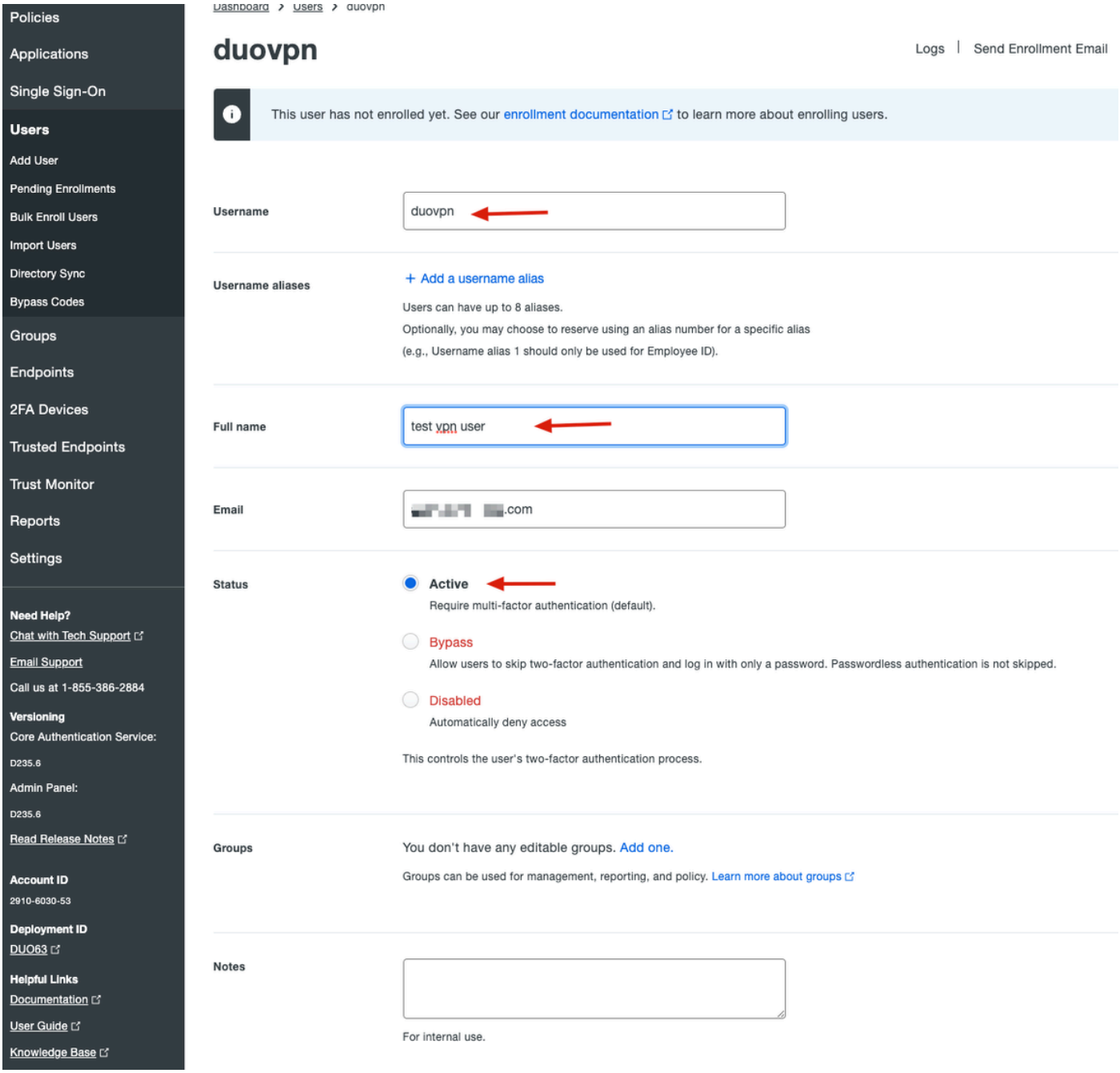
1.登录您的Duo管理员门户。



2.在左侧面板上，导航到Users，单击Add User，然后键入与Active Domain用户名匹配的用户的名称，然后单击Add User。



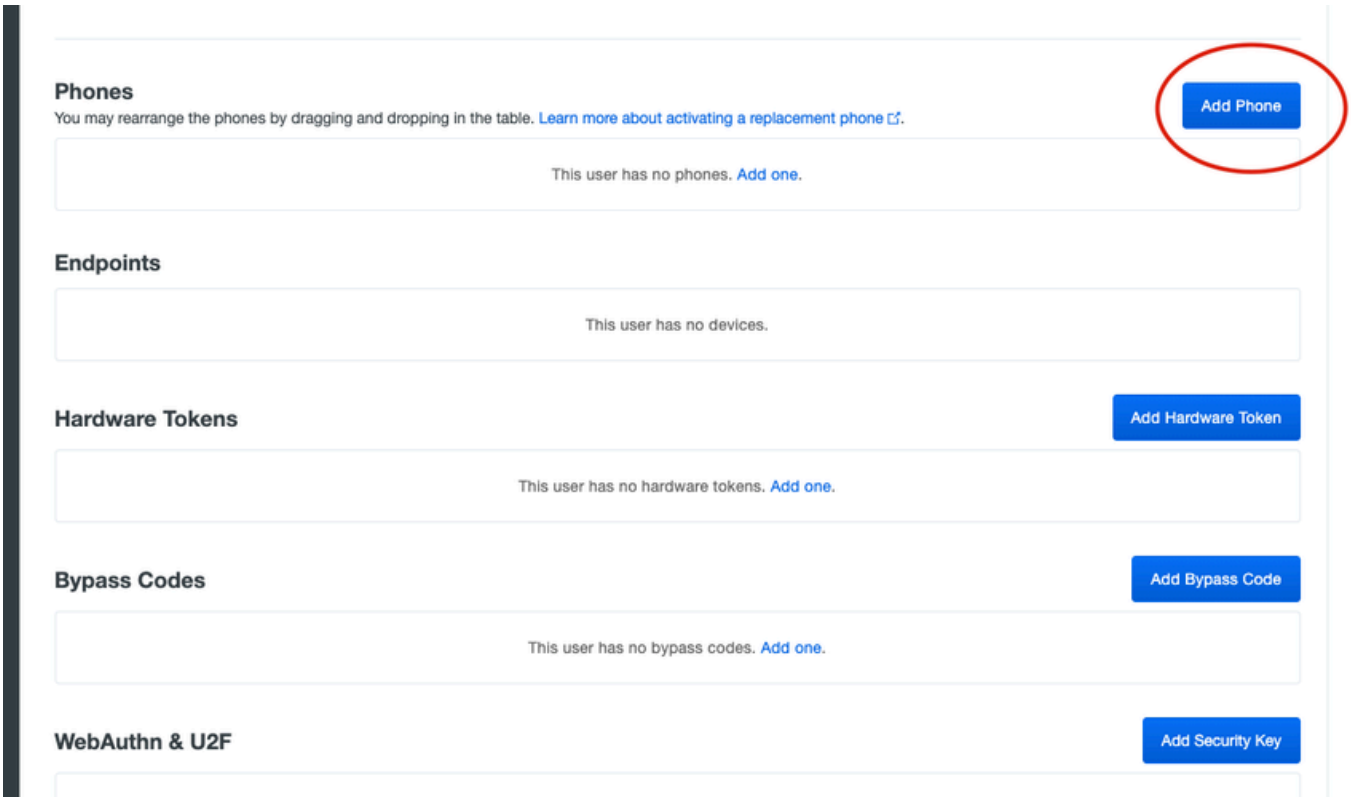
3.在新用户面板上，填写所有必要信息。



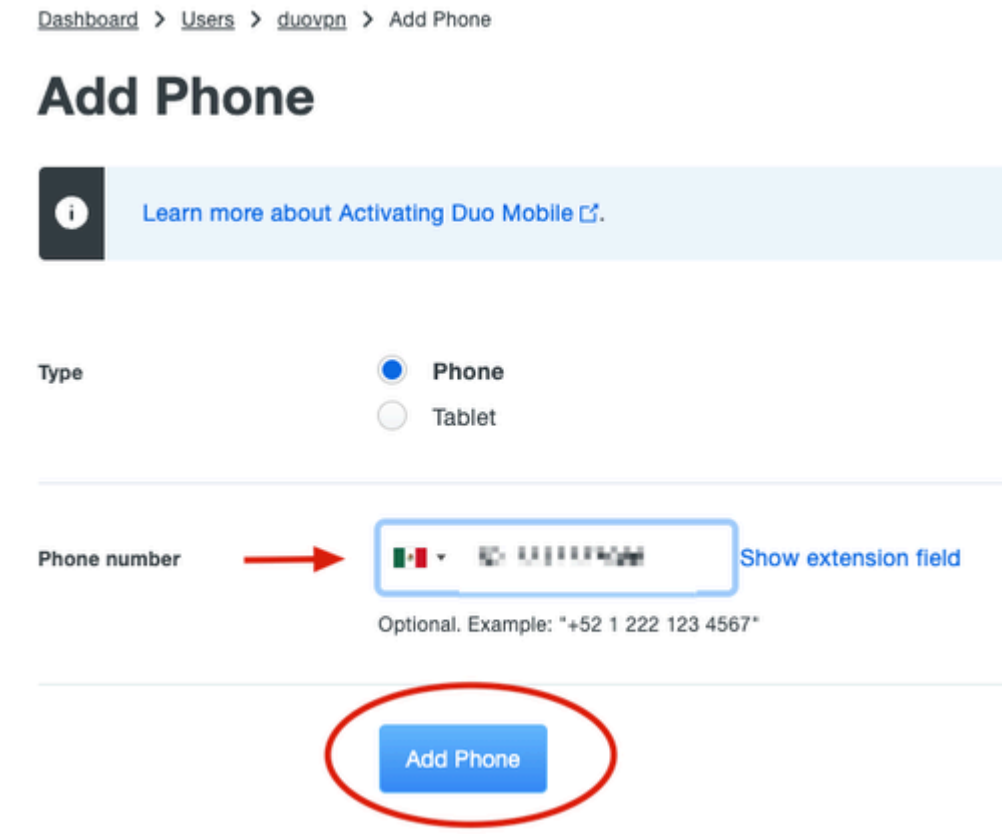
4.在“用户设备”下，指定辅助身份验证方法。

注意：在本文档中，使用Duo推送移动设备方法，因此必须添加电话设备。

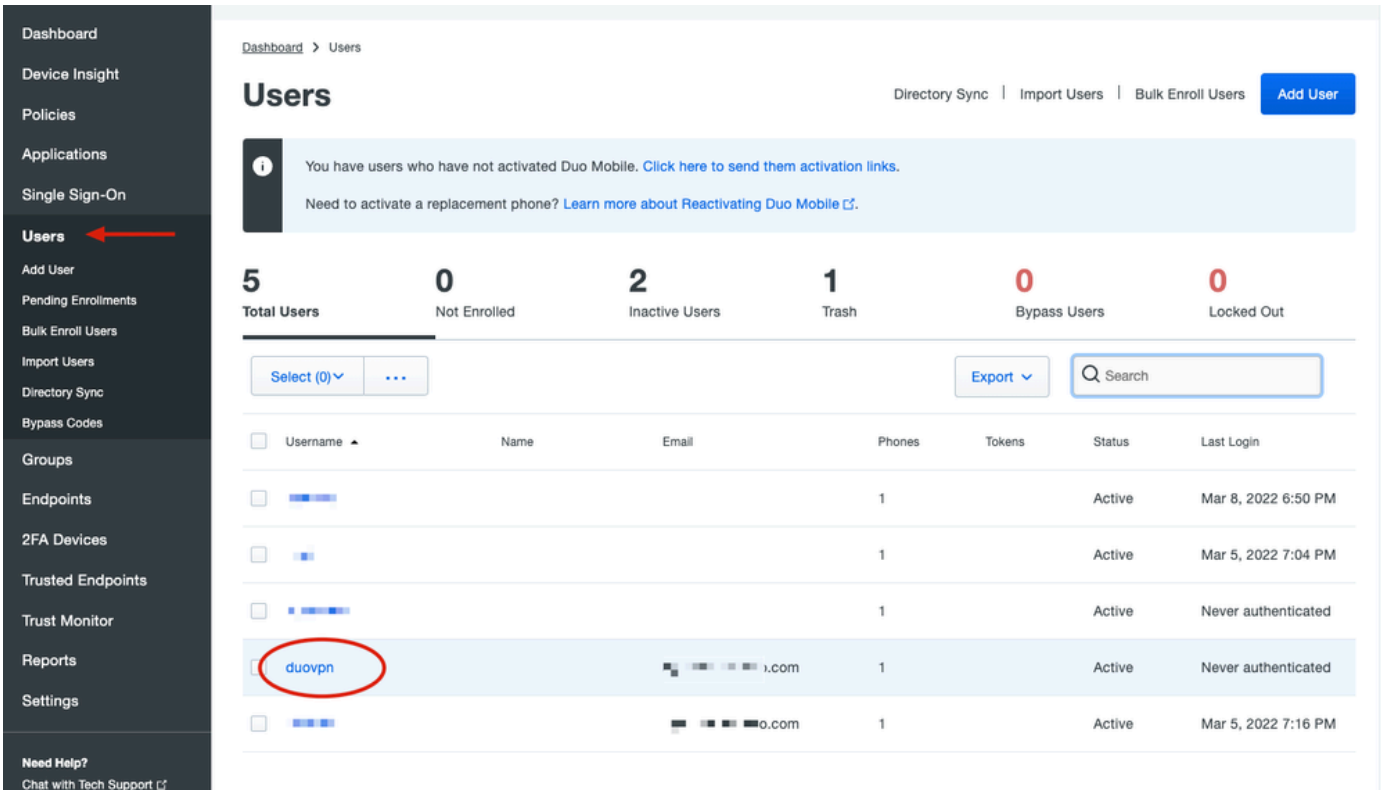
5.单击Add Phone。



6.键入用户电话号码，然后单击Add Phone。

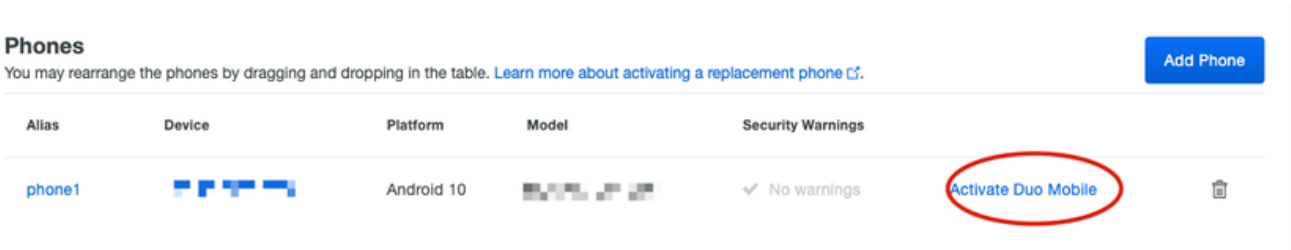


7.在Duo Admin左面板上，导航到Users，然后单击新用户。

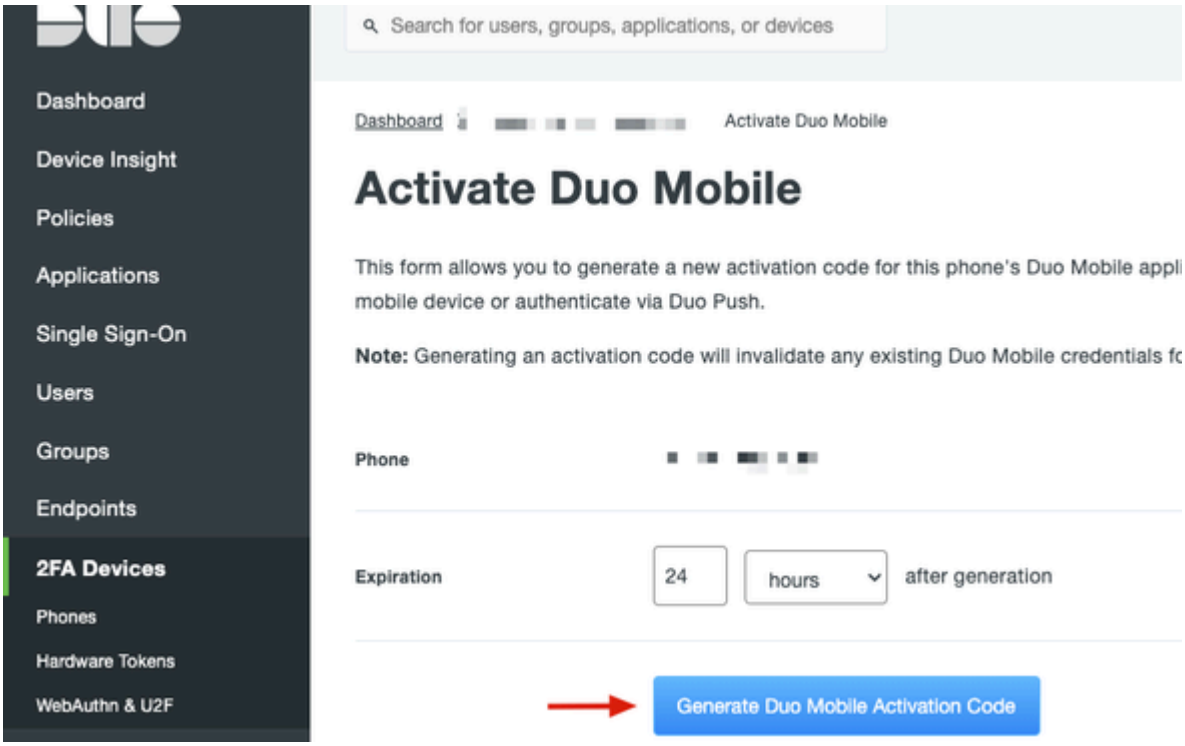


注意：如果您在设置时无权访问您的电话，则可以选择电邮选项。

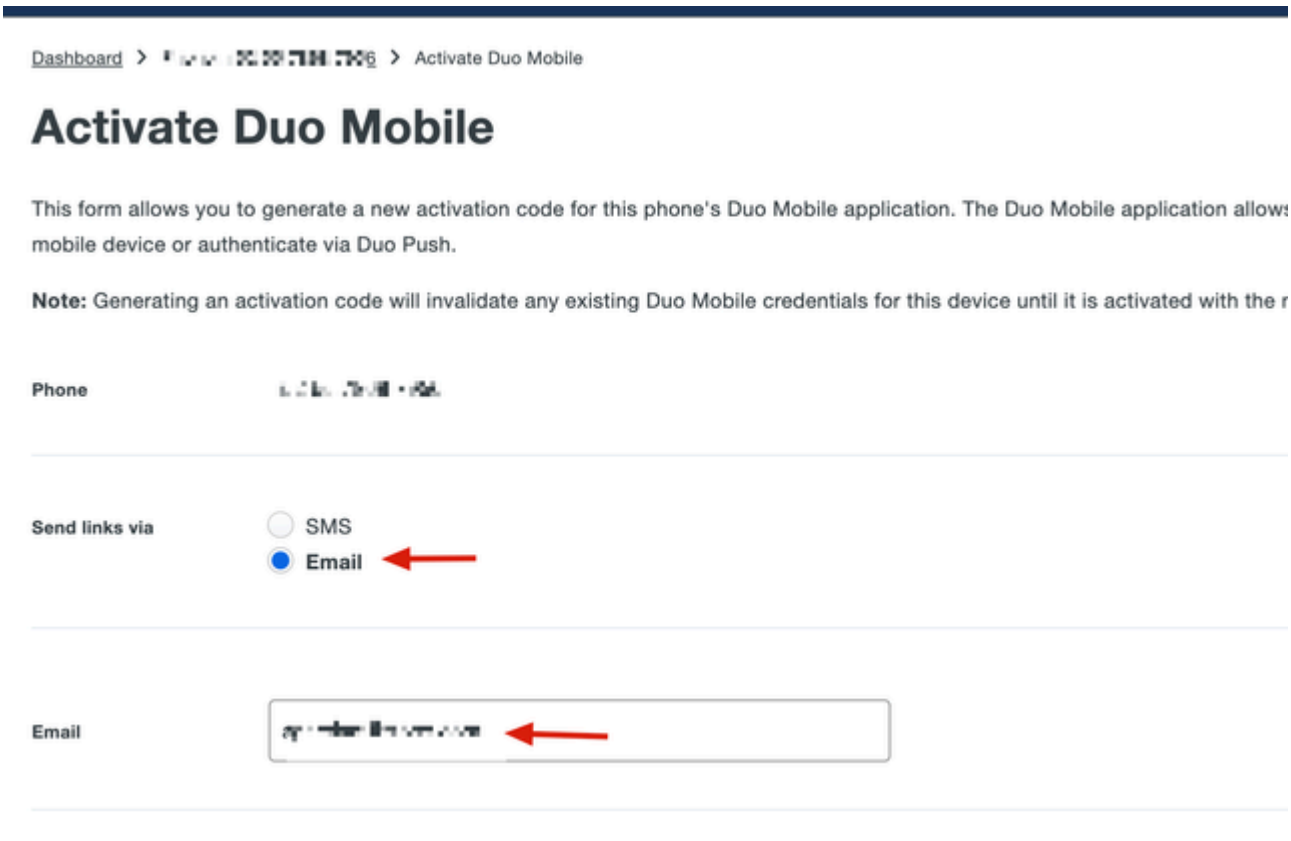
8.导航到电话部分，然后单击激活双移动。



9.单击生成Duo Mobile激活码。



10.选择Email以通过电子邮件接收说明，键入您的电子邮件地址，然后单击Send Instructions by email。



11.您会收到一封包含说明的电子邮件。



This is an automated email from Duo Security.

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Cisco account to Duo Mobile on this device:

Just tap this link from + [redacted] or copy and paste it into Duo Mobile manually:

If you're not reading this from + [redacted] Duo Mobile on your phone and scan this barcode:

Don't have Duo Mobile yet? Install it first:

iPhone: https://itunes.apple.com/us/app/duo-mobile/id422663827

Android: https://play.google.com/store/apps/details?id=com.duosecurity.duomobile

---

12.从您的移动设备打开Duo Mobile App，然后单击Add，然后选择Use QR Code并扫描电子邮件中的代码。

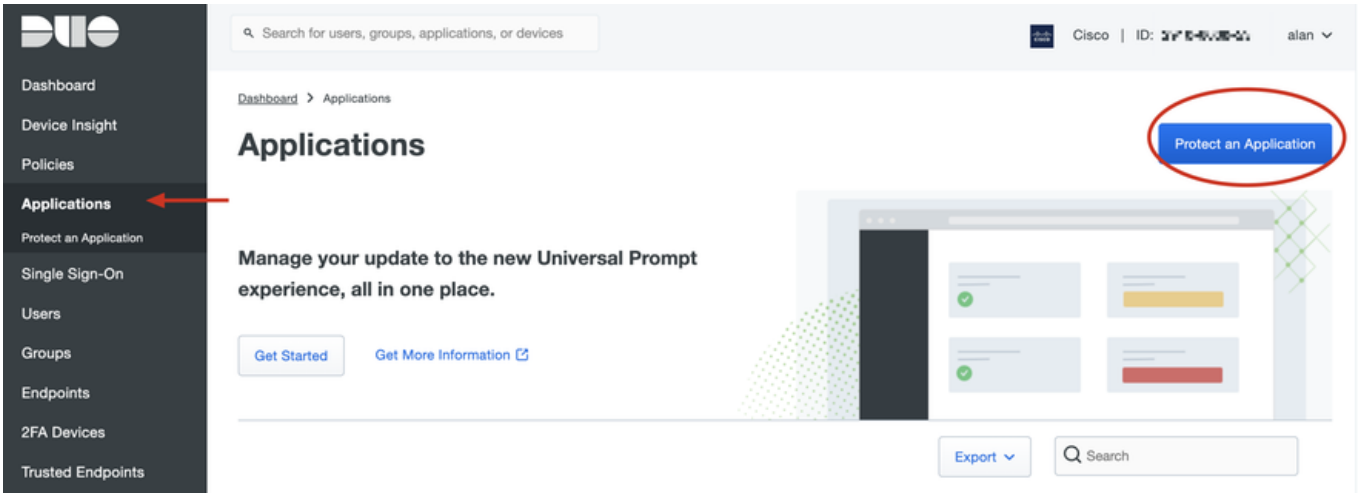
13.新用户将添加到您的Duo移动应用。

Duo Auth代理配置

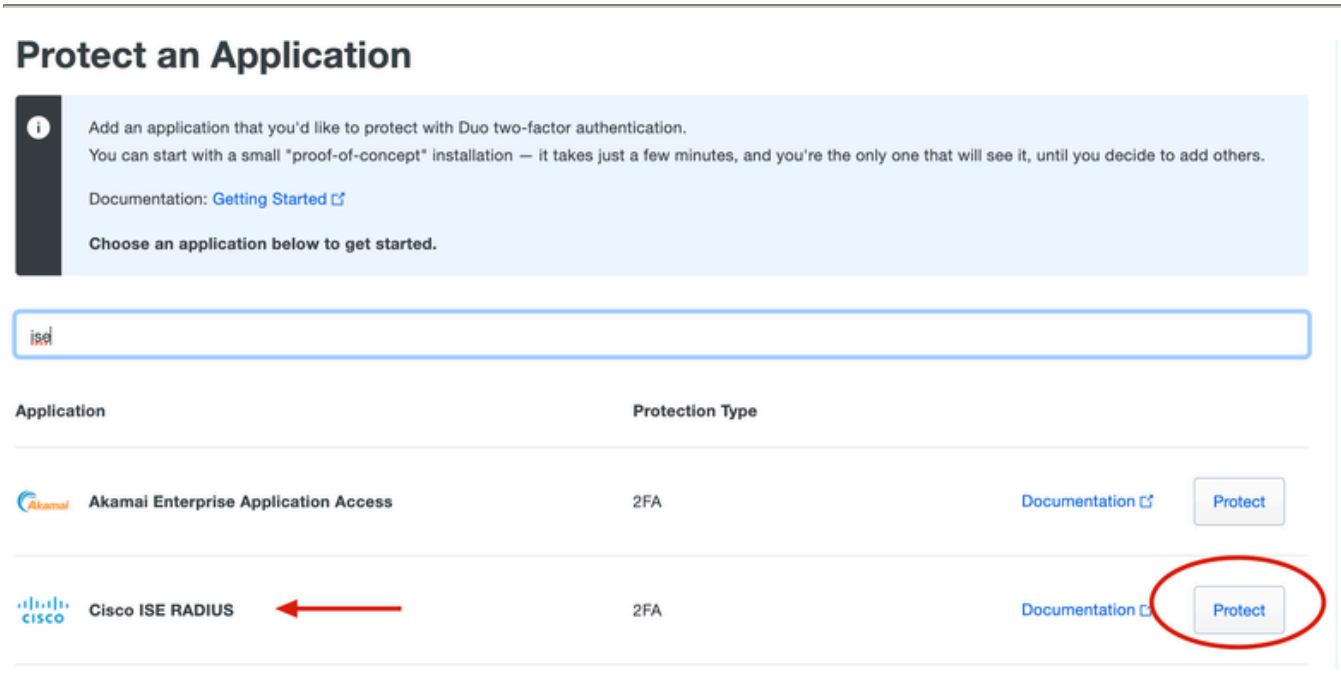
1.从Cisco Duo Authentication下载并安装Duo Auth Proxy Manager。

注意：在本文档中，Duo Auth代理管理器安装在承载Active Directory服务的同一Windows服务器上。

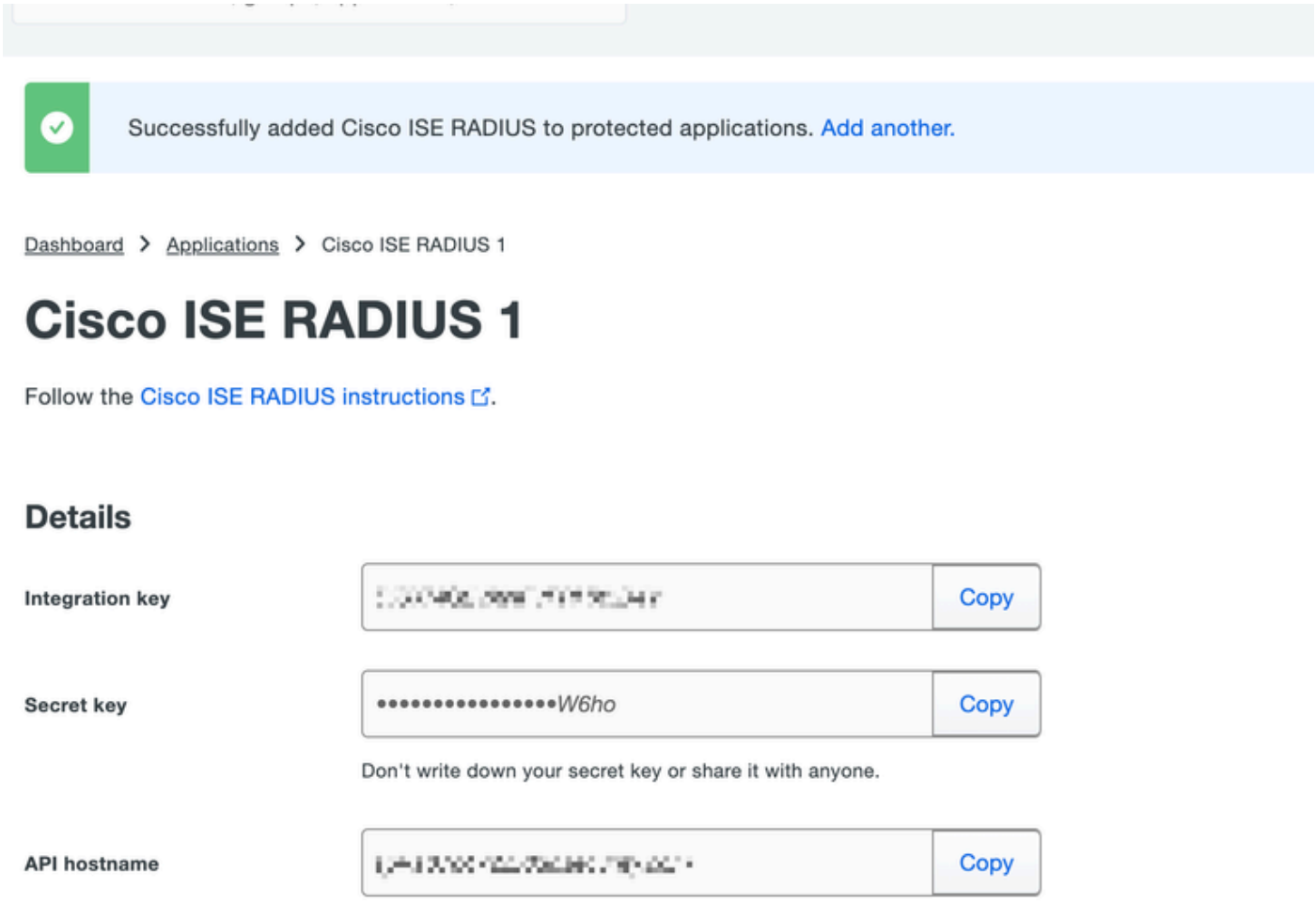
2.在Duo Admin Panel上，导航至Applications（应用），然后点击Protect an Application（保护应用）。



3.在搜索栏上，查找Cisco ISE Radius。

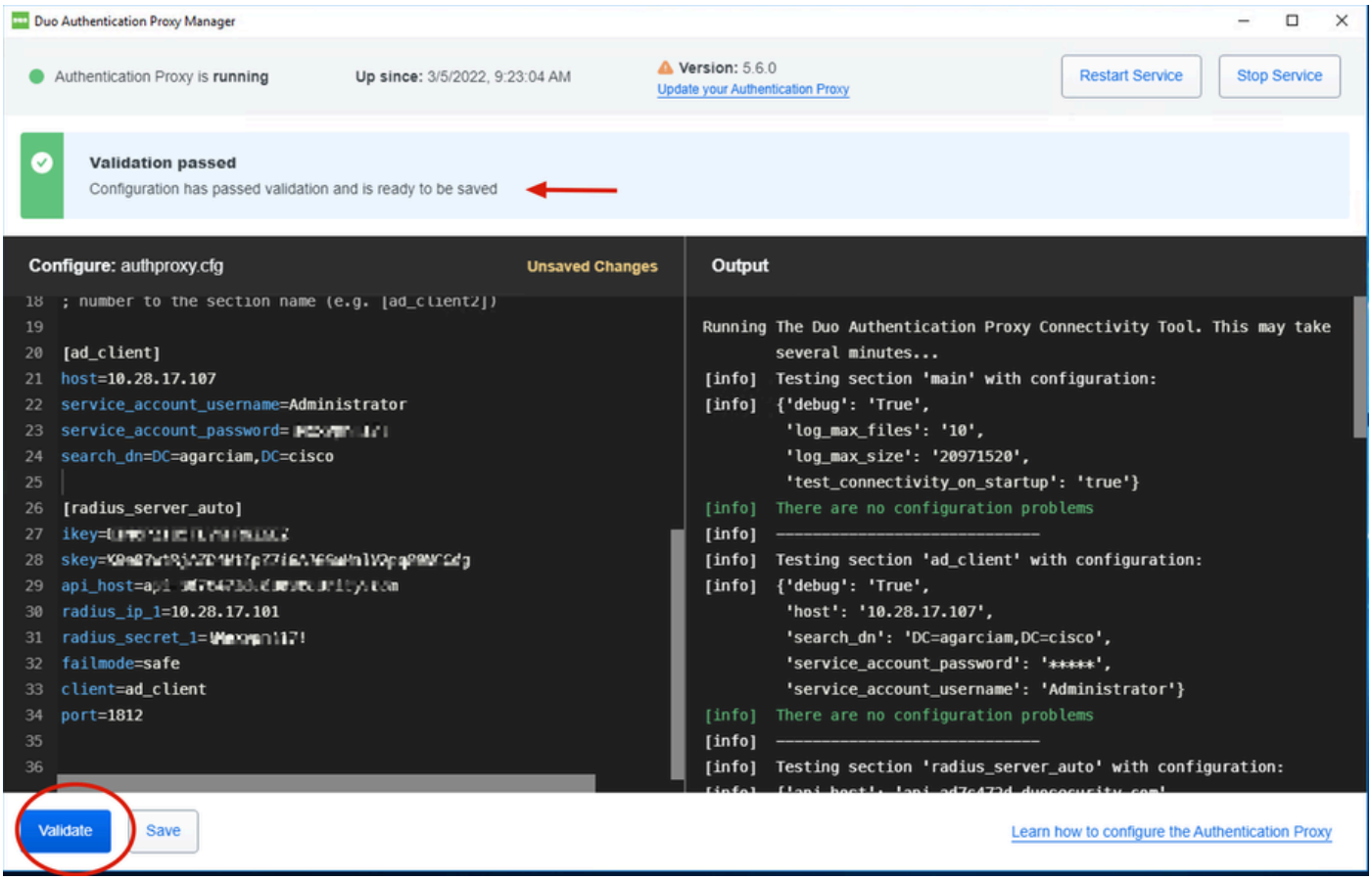


4.复制集成密钥、密钥和API主机名。您需要此信息进行Duo身份验证代理配置。



5.运行Duo Authentication Proxy Manager应用并完成Active Directory客户端和ISE Radius服务器的配置，然后点击Validate。

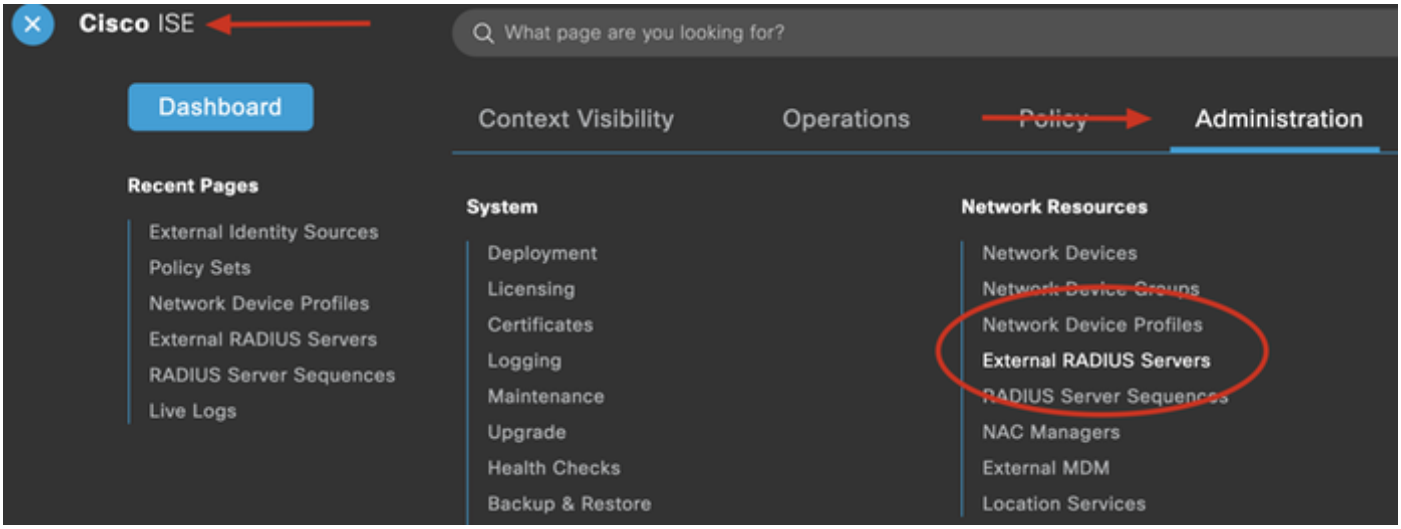
注意：如果验证不成功，请参阅调试选项卡了解详细信息并相应更正。



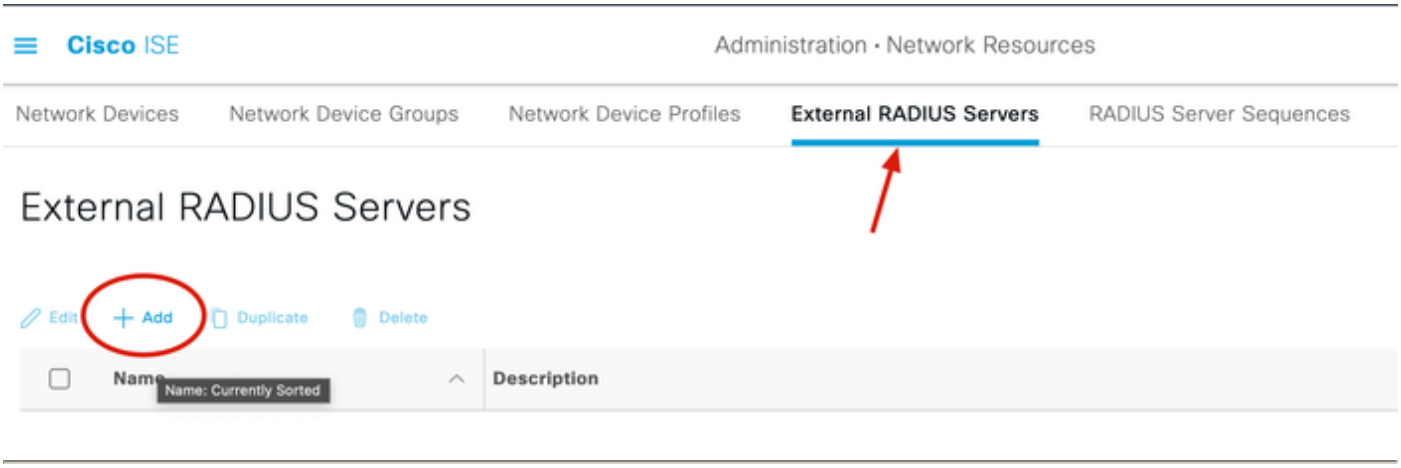
思科ISE配置

1.登录ISE管理员门户。

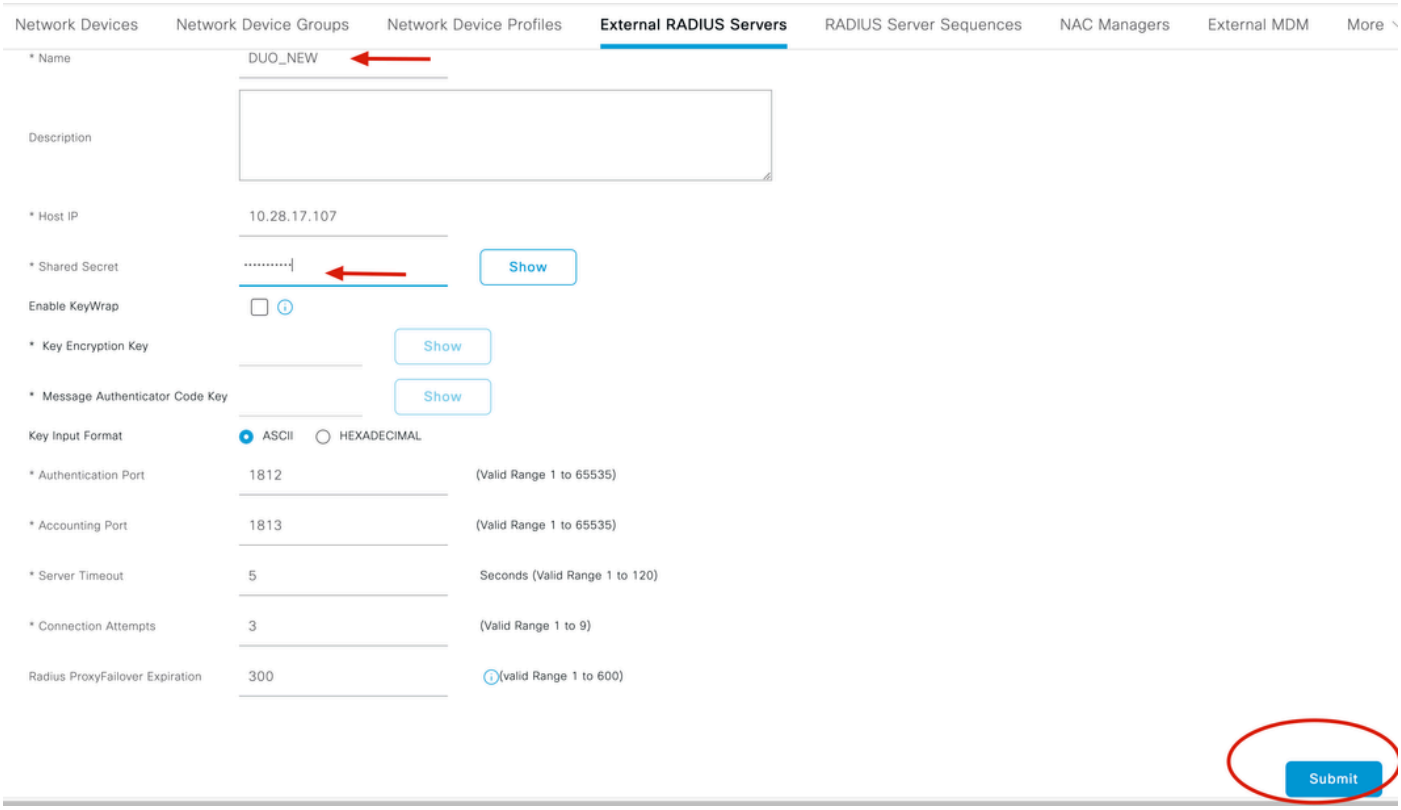
2.展开Cisco ISE选项卡并导航到Administration，然后点击Network Resources，然后点击External RADIUS Servers。



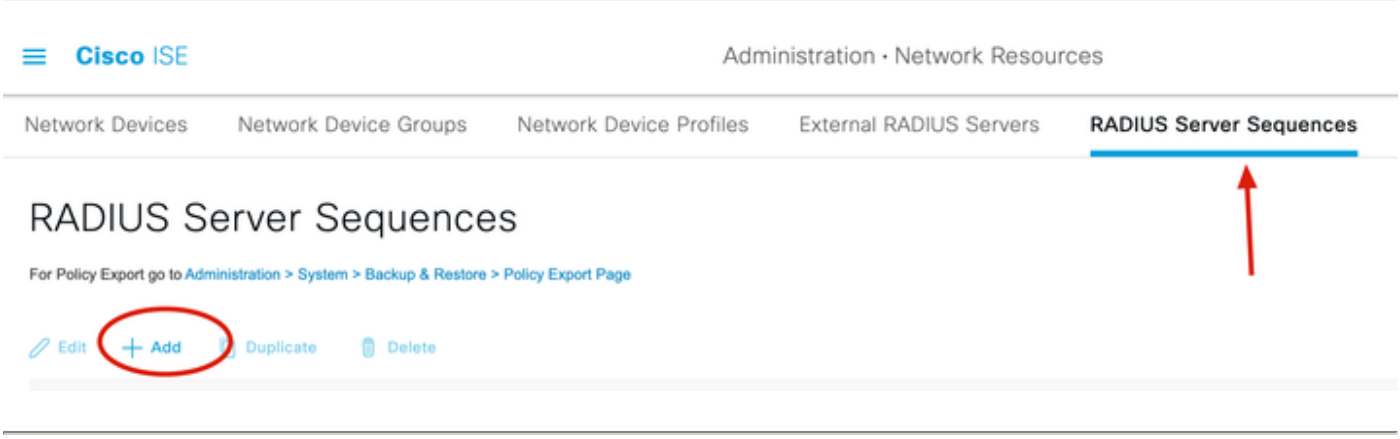
3.在External Radius Servers选项卡上，单击Add。



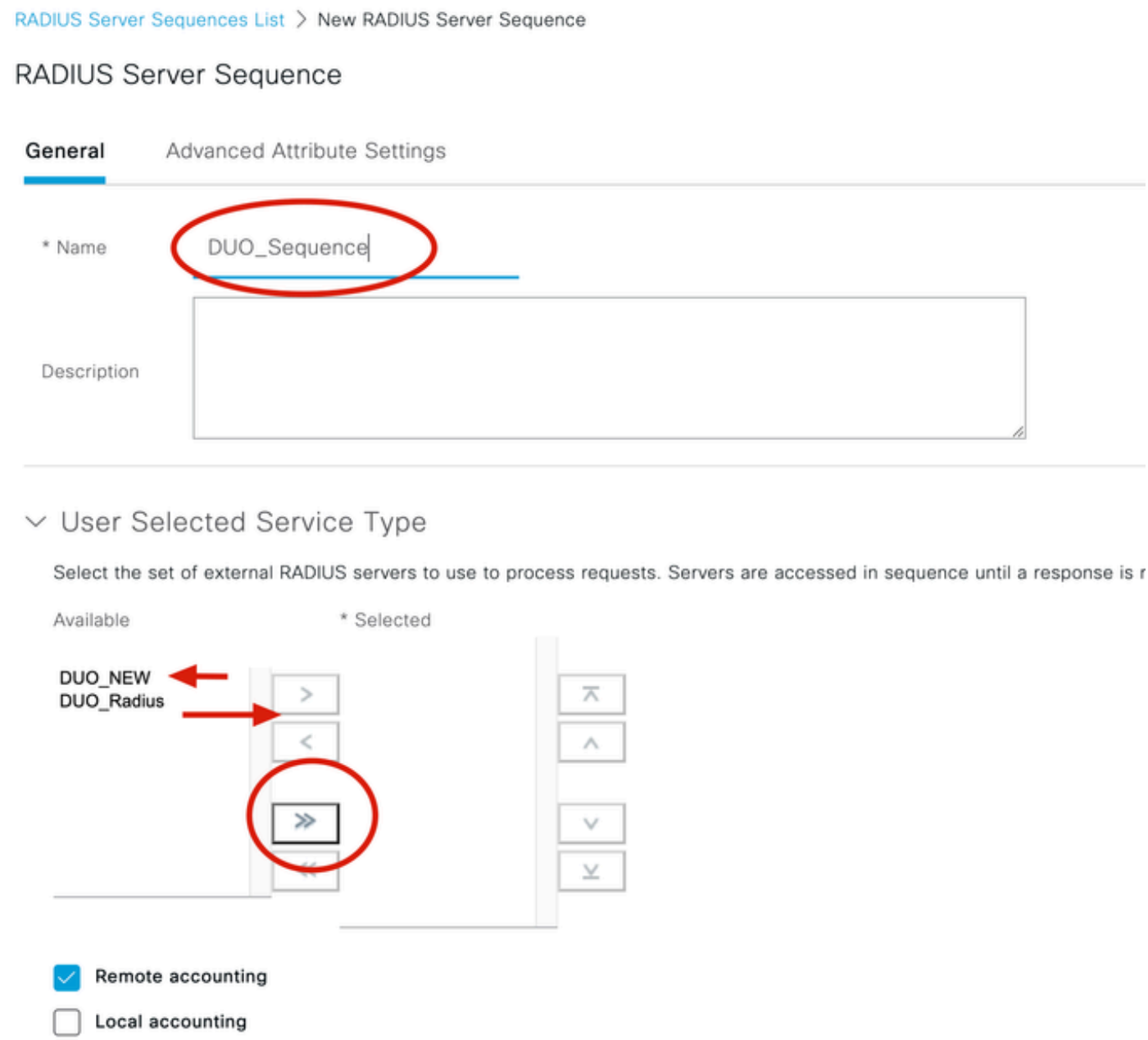
4.使用Duo Authentication Proxy Manager中使用的RADIUS配置填空并点击Submit。



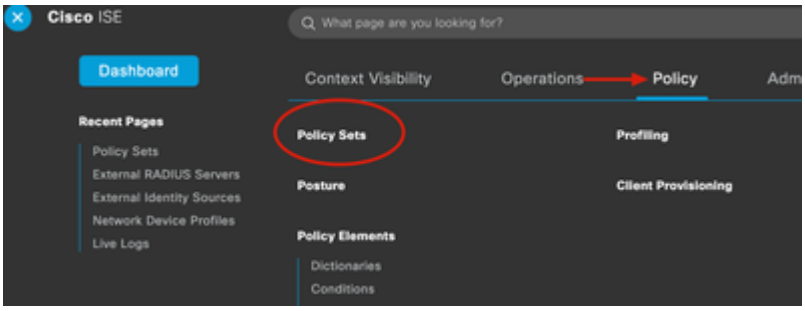
5.导航到RADIUS Server Sequences选项卡，然后单击Add。



6.指定序列名称并分配新的RADIUS外部服务器，单击Submit。

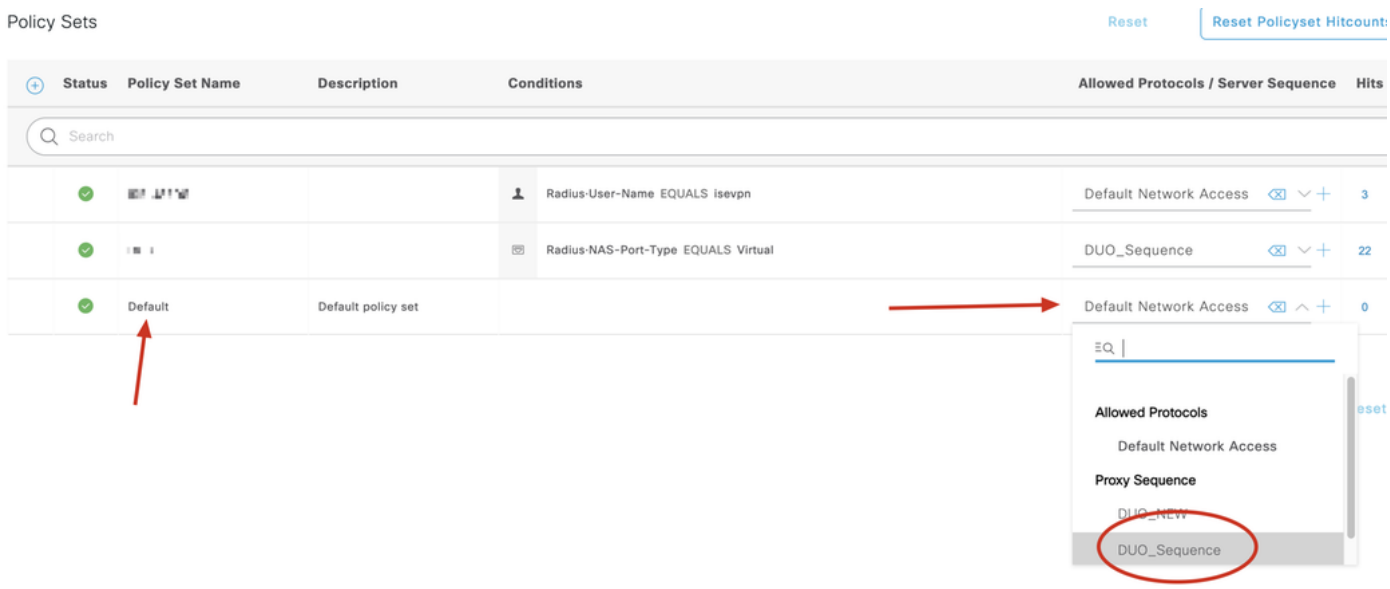


7.从“控制面板”菜单导航至策略，然后单击策略集。



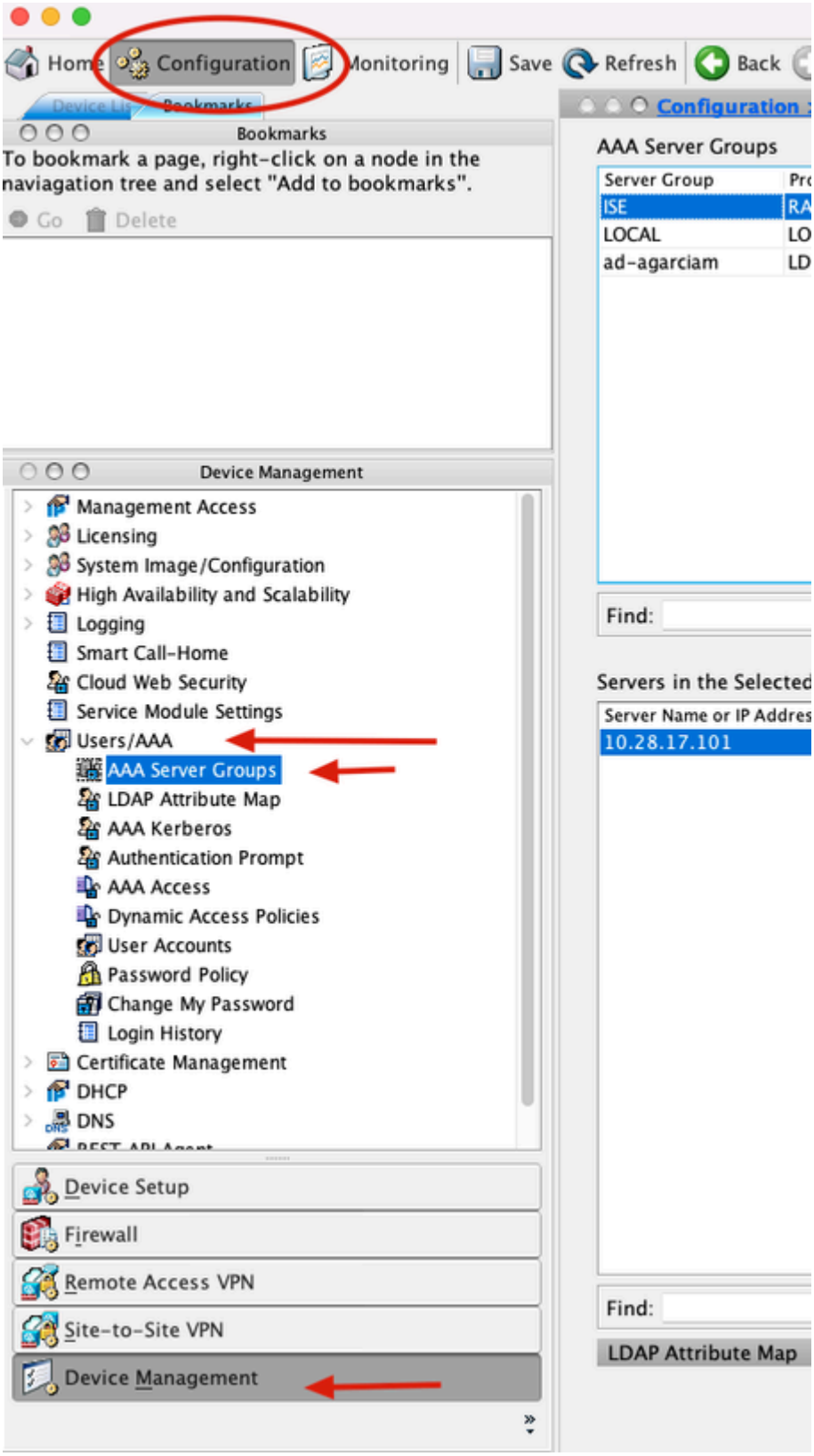
8.将RADIUS序列分配给默认策略。

注意：应用所有连接的双序列并使用默认策略；策略分配可能不同。

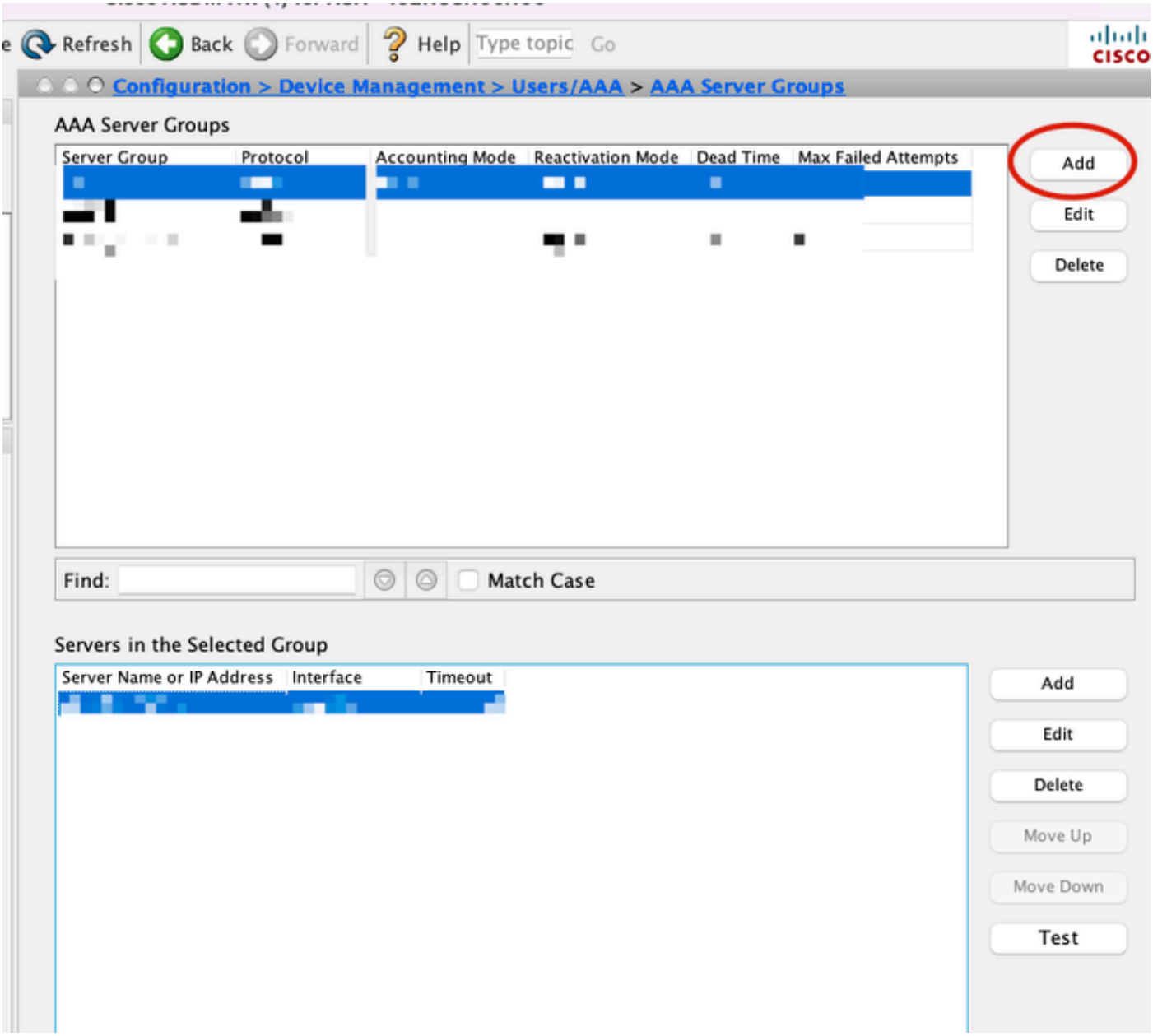


Cisco ASA RADIUS/ISE配置

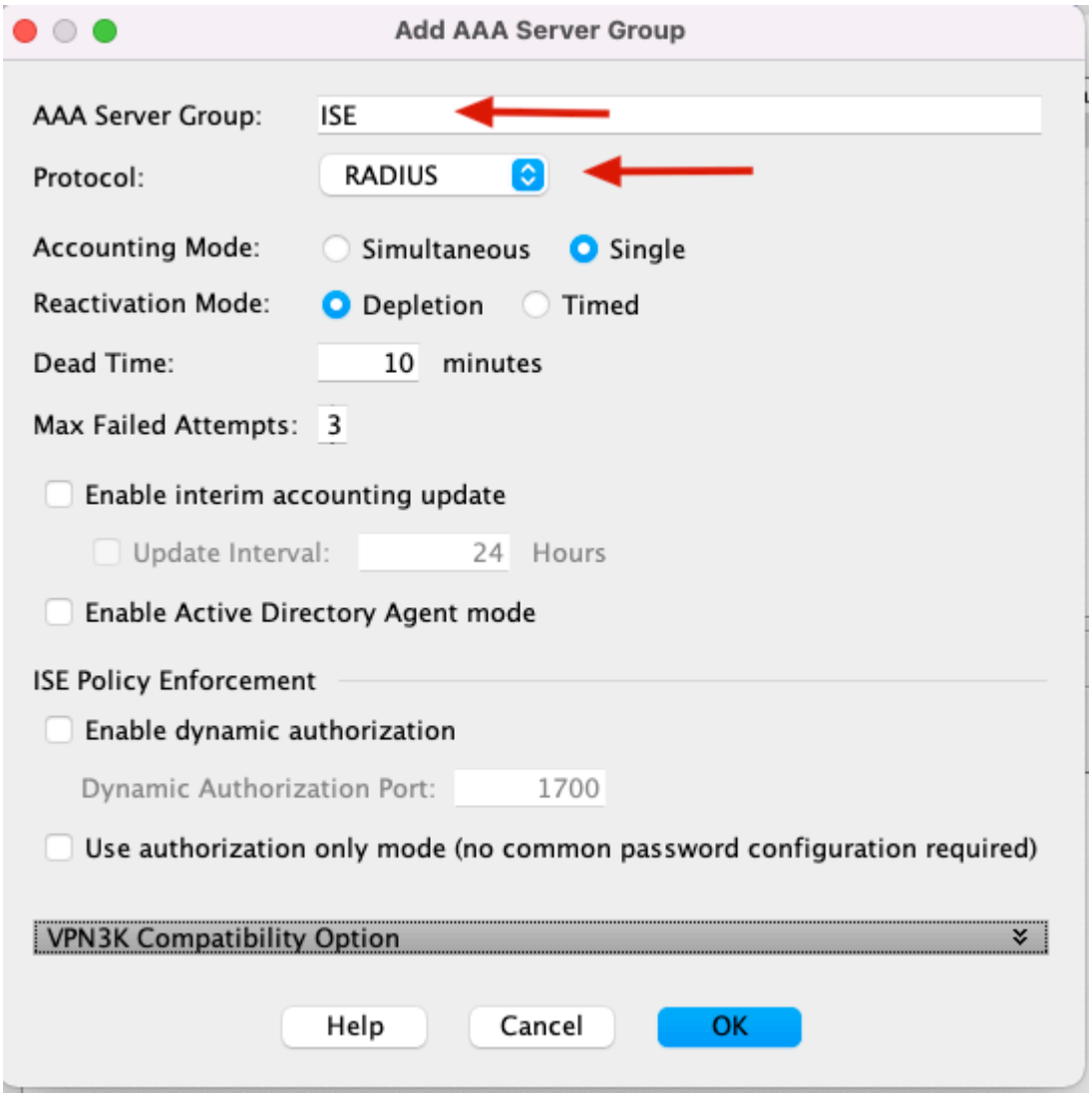
1.要在AAA服务器组下配置ISE RADIUS服务器，请导航到Configuration，然后单击Device Management，展开Users/AAA部分，然后选择AAA Server Groups。



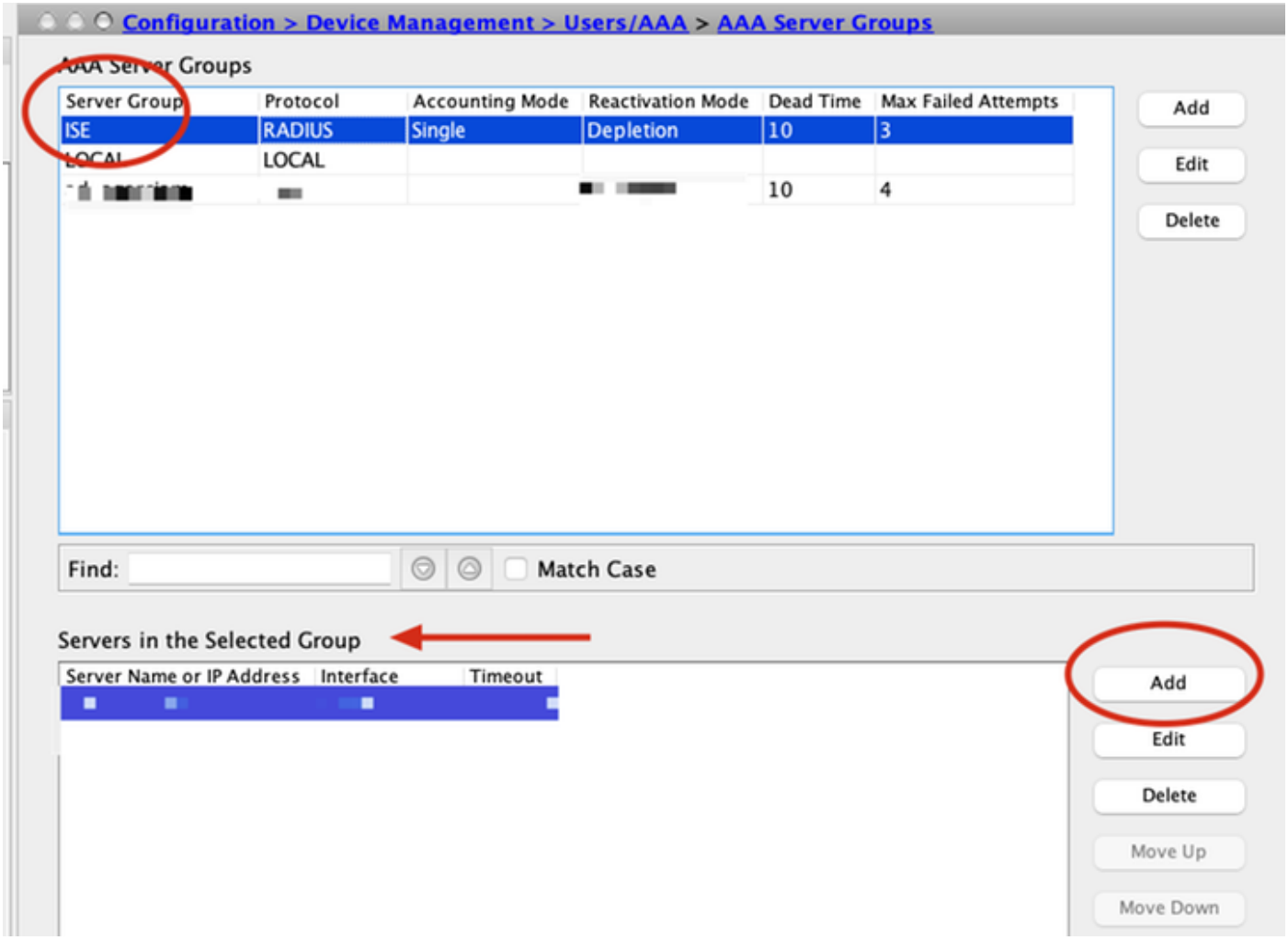
2.在AAA Server Groups面板上，单击Add。



3.选择服务器组的名称，并指定RADIUS作为要使用的协议，然后单击确定。

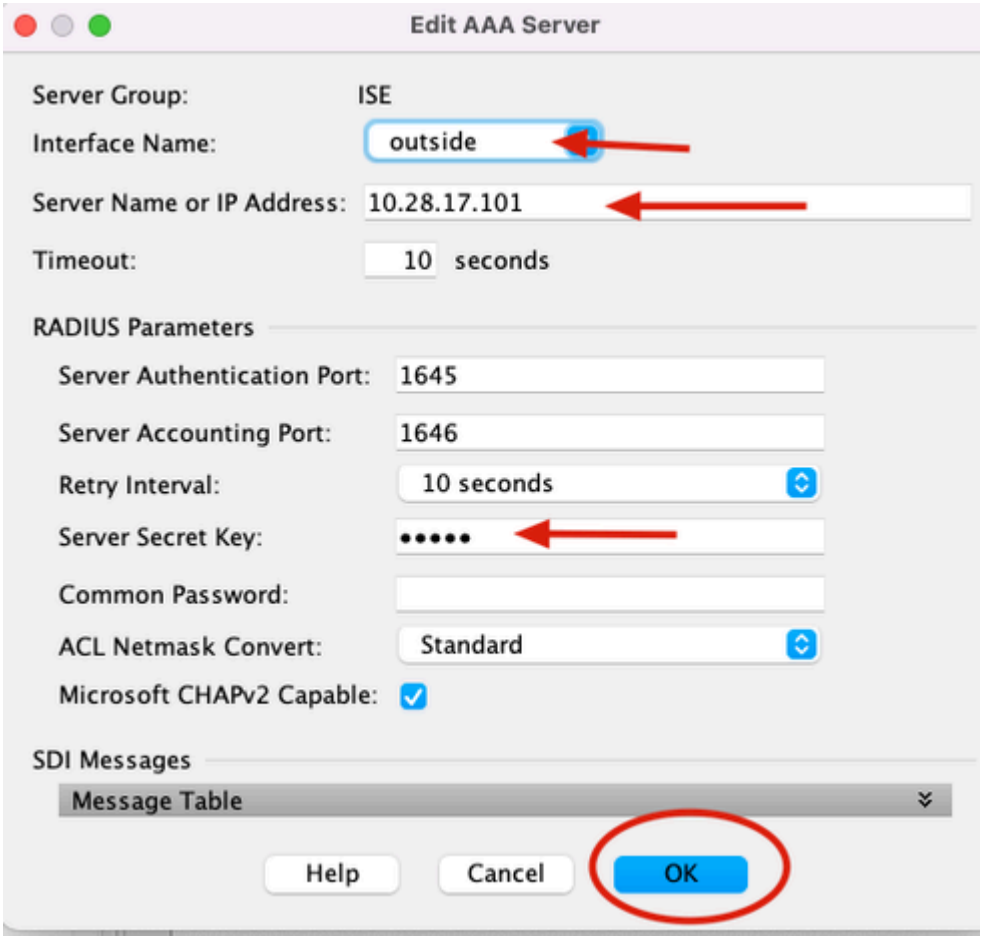


5.选择新的服务器组，然后单击“选定组”面板中Servers下的Add:



6.在“编辑AAA服务器”窗口上，选择Interface Name，指定ISE服务器的IP地址并键入RADIUS Secret Key，然后单击OK。

注意：所有信息必须与Duo Authentication Proxy Manager上指定的信息匹配。



CLI 配置

```
aaa-server ISE protocol radius
 dynamic-authorization
aaa-server ISE (outside) host 10.28.17.101
 key *****
```

Cisco ASA远程访问VPN配置

```
ip local pool agarciam-pool 192.168.17.1-192.168.17.100 mask 255.255.255.0

group-policy DUO internal
group-policy DUO attributes
 banner value This connection is for DUO authorized users only!
 vpn-tunnel-protocol ikev2 ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split-agarciam
 address-pools value agarciam-pool

tunnel-group ISE-users type remote-access
```

```
tunnel-group ISE-users general-attributes
 address-pool agarciam-pool
 authentication-server-group ISE
 default-group-policy DUO
tunnel-group ISE-users webvpn-attributes
 group-alias ISE enable
 dns-group DNS-CISCO
```

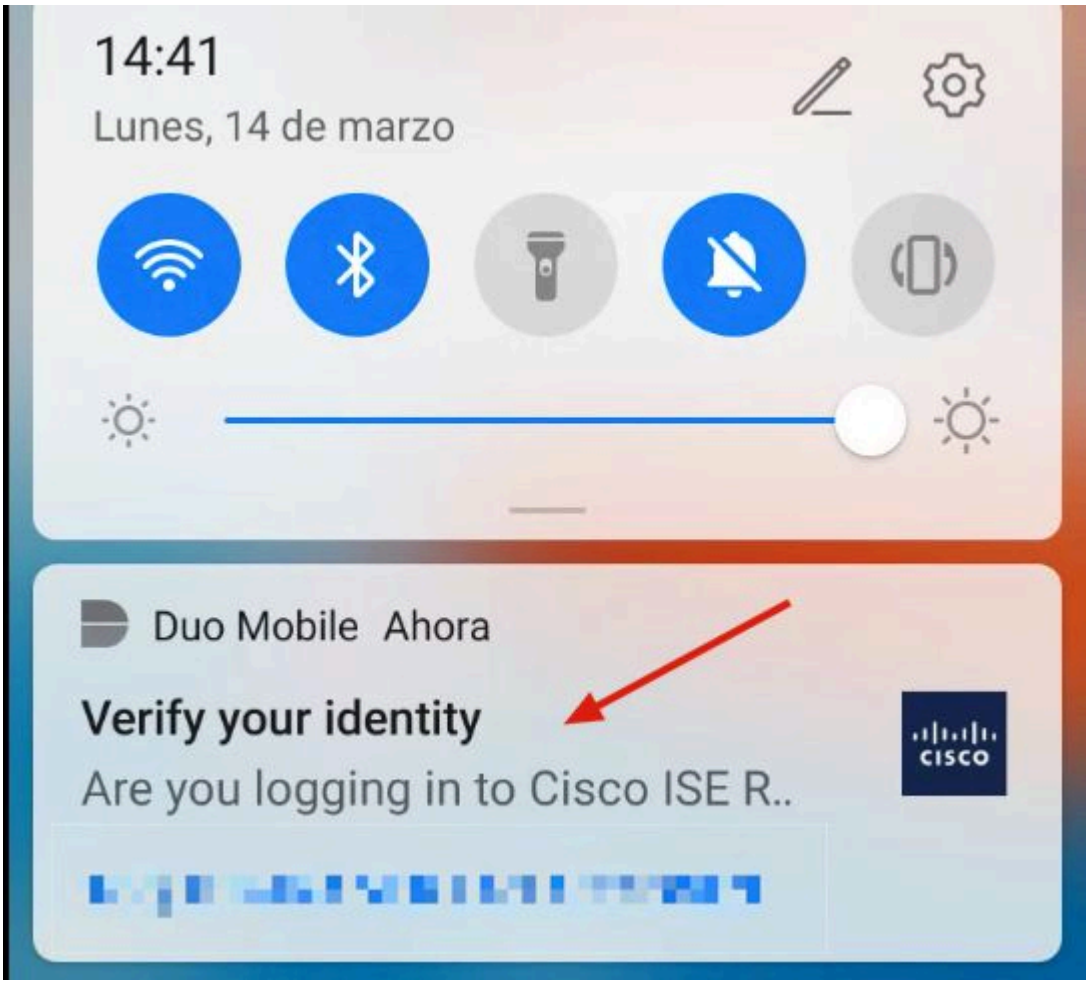
测试

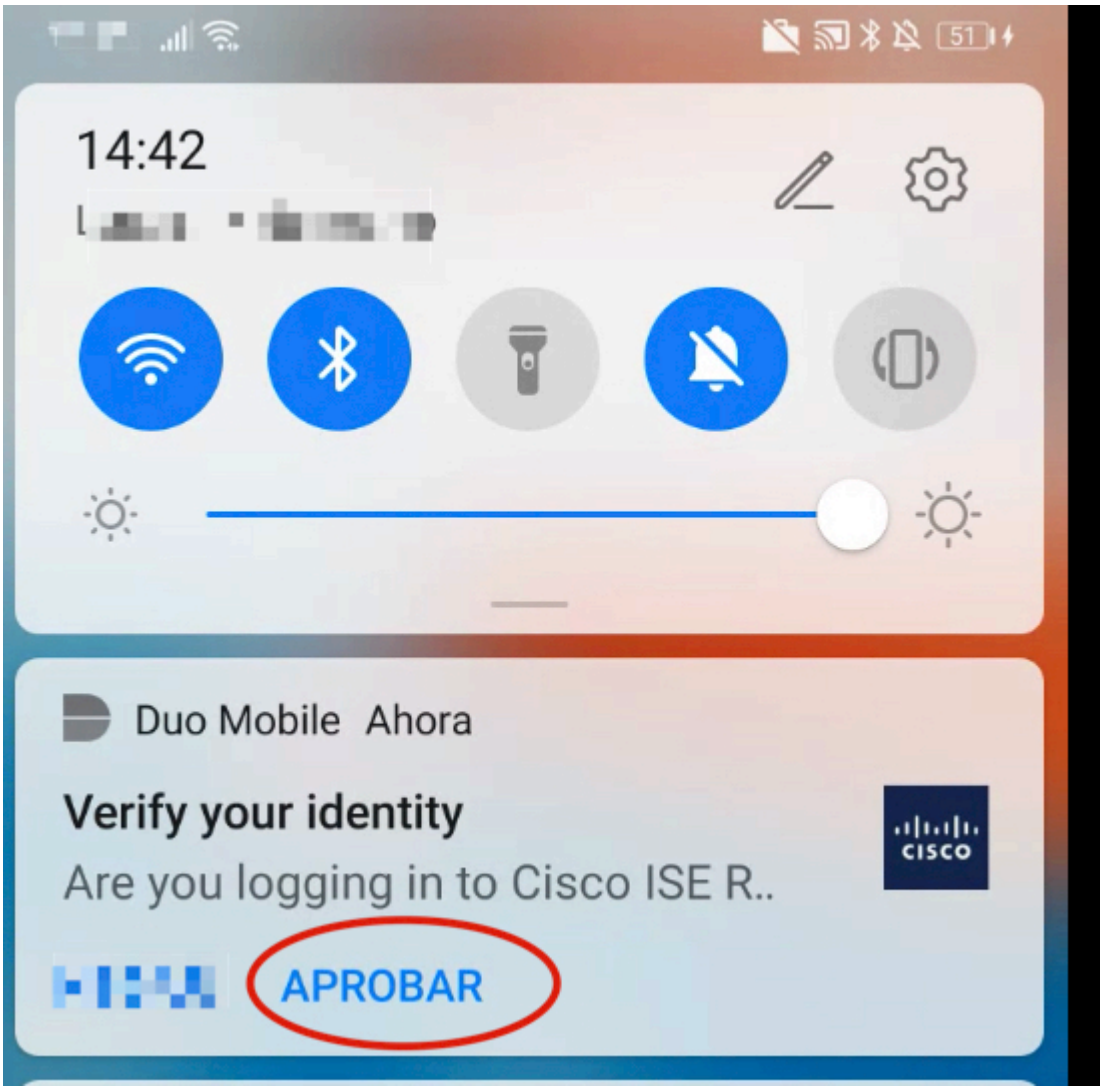
1.在PC上打开Cisco Secure Client/AnyConnect应用。指定VPN ASA头端的主机名，并使用为辅助Duo身份验证创建的用户登录，然后点击OK。



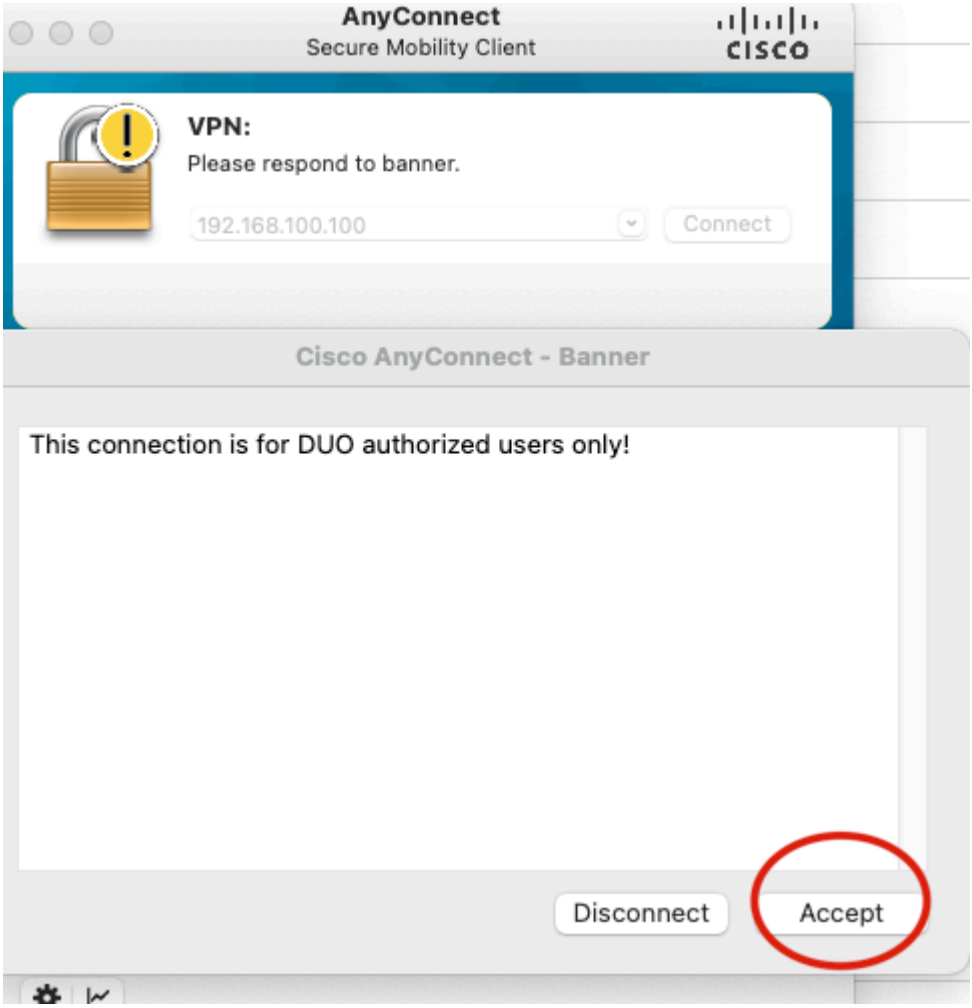
2.您在指定的用户Duo Mobile设备上收到Duo推送通知。

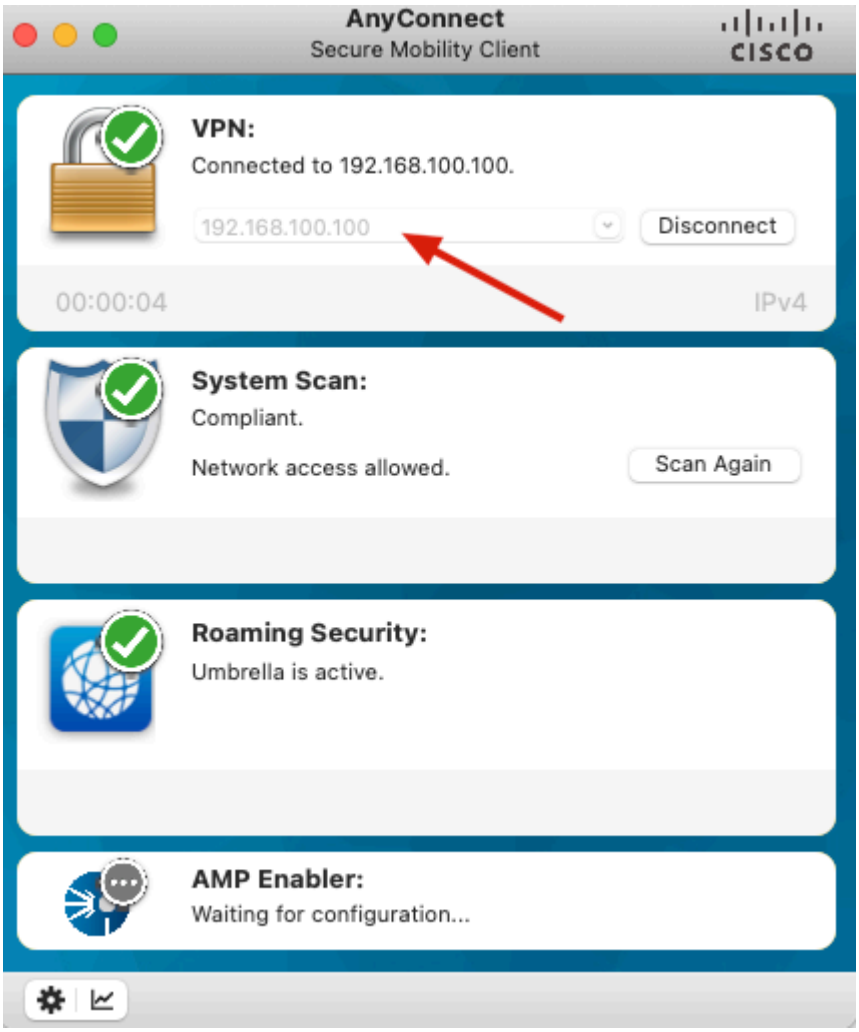
3.打开Duo Mobile App通知，然后单击Approve。


14:41
Lunes, 14 de marzo
Duo Mobile Ahora
Verify your identity
Are you logging in to Cisco ISE R..
cisco



4.接受标语并且已建立连接。


AnyConnect
Secure Mobility Client
CISCO
VPN:
Please respond to banner.
192.168.100.100
Connect
Cisco AnyConnect - Banner
This connection is for DUO authorized users only!
Disconnect
Accept



故障排除

本部分提供的信息可用于对配置进行故障排除。Duo Authentication Proxy附带调试工具，用于显示错误和故障原因。

工作调试

注意：下一个信息存储在C:\Program Files\Duo Security Authentication Proxy\log\connectivity_tool.log中。

Output

```
Running The Duo Authentication Proxy Connectivity Tool. This may take
        several minutes...
[info]  Testing section 'main' with configuration:
[info]  {'debug': 'True',
         'log_max_files': '10',
         'log_max_size': '20971520',
         'test_connectivity_on_startup': 'true'}
[info]  There are no configuration problems
[info]  ------------------------------
[info]  Testing section 'ad_client' with configuration:
[info]  {'debug': 'True',
         'host': '10.28.17.107',
         'search_dn': 'DC=agarciam,DC=cisco',
         'service_account_password': '*****',
         'service_account_username': 'Administrator'}
[info]  There are no configuration problems
```

```
[info]  ------------------------------
[info]  Testing section 'radius_server_auto' with configuration:
[info]  {'api_host': [redacted],
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': [redacted],
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '*****',
         'skey': '*****[40]'}
[info]  There are no configuration problems
```

```
[info]  Testing section 'main' with configuration:
[info]  {'debug': 'True',
         'log_max_files': '10',
         'log_max_size': '20971520',
         'test_connectivity_on_startup': 'true'}
[info]  There are no connectivity problems with the section.
```

```
[info]  There are no connectivity problems with the section.
[info]  ----------------------------
[info]  Testing section 'ad_client' with configuration:
[info]  {'debug': 'True',
         'host': '10.28.17.107',
         'search_dn': 'DC=agarciam,DC=cisco',
         'service_account_password': '*****',
         'service_account_username': 'Administrator'}
[info]  The LDAP Client section has no connectivity issues.
[info]  ----------------------------
[info]  Testing section 'radius_server_auto' with configuration:
[info]  {'api_host': '[redacted]',
         'client': 'ad_client',
         'debug': 'True',
         'failmode': 'safe',
         'ikey': '[redacted]',
         'port': '1812',
         'radius_ip_1': '10.28.17.101',
         'radius_secret_1': '*****',
         'skey': '*****[40]'}
[info]  The RADIUS Server has no connectivity problems.
[info]  ----------------------------
[info]  SUMMARY
[info]  No issues detected
```

常见问题

1.连接问题、错误的IP、Active Directory配置上无法解析的FQDN/主机名

```
[ad_client]
host=10.28.17.106
service_account_username=Administrator
service_account_password=[redacted]
search_dn=DC=agarciam,DC=cisco
```

Output

```
        'host': '10.28.17.106',
        'search_dn': 'DC=agarciam,DC=cisco',
        'service_account_password': '*****',
        'service_account_username': 'Administrator'}
[warn]  The LDAP Client section has connectivity problems.
[warn]  The LDAP host clear connection to 10.28.17.106:389 has
       connectivity problems.
[error] The Auth Proxy was not able to establish a connection to 10
       .28.17.106:389.
```

---

2. Active Directory上管理员用户的密码错误

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!
search_dn=DC=agarciam,DC=cisco
```

调试:

```
[info]  The Auth Proxy was able to establish a connection to 10.28.17
       .107:389.
[info]  The Auth Proxy was able to establish an LDAP connection to 10
       .28.17.107:389.
[error] The Auth Proxy was unable to bind as Administrator.
[error] Please ensure that the provided service account credentials
       are correct.
[debug] Exception: invalidCredentials: 8009030C: LdapErr: DSID
       -0C090516, comment: AcceptSecurityContext error, data 52e,
       v3839
[warn]  The Auth Proxy did not run the search check because of the
       problem(s) with the bind check. Resolve that issue and rerun
       the tester.
```

3.错误的基域

```
[ad_client]
host=10.28.17.107
service_account_username=Administrator
service_account_password=!
search_dn=DC=agarciam,DC=ciscoo
```

调试:

```
[info]  The Auth Proxy was able to bind as Administrator.
[error] The Auth Proxy got an error searching the LDAP DN DC=agarciam
        ,DC=ciscoo.
[debug] Exception: referral: 0000202B: RefErr: DSID-031007F9, data 0,
        1 access points
                ref 1: 'agarciam.ciscoo'
```

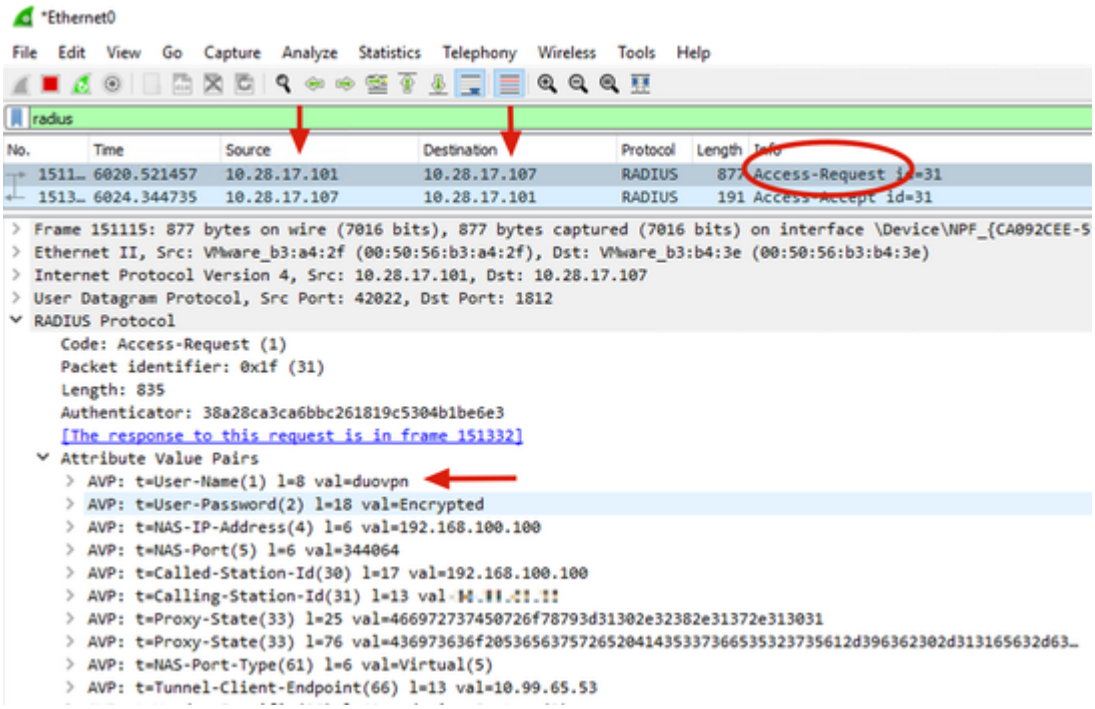
4.错误的iKey RADIUS值

```
[radius_server_auto]
ikey=[redacted]XHRNZ6EZ1
skey=[redacted]
api_host=[redacted]ity.com
radius_ip_1=10.28.17.101
radius_secret_1=!Mexvpn!17!
failmode=safe
client=ad_client
port=1812
```

调试:

```
[error] The ikey value provided is invalid.
[info]  ----------------------------
[info]  SUMMARY
[warn]  Checks for external connectivity were not run. Please fix the
        configuration and try again.
```

5.验证ISE服务器发送访问请求数据包



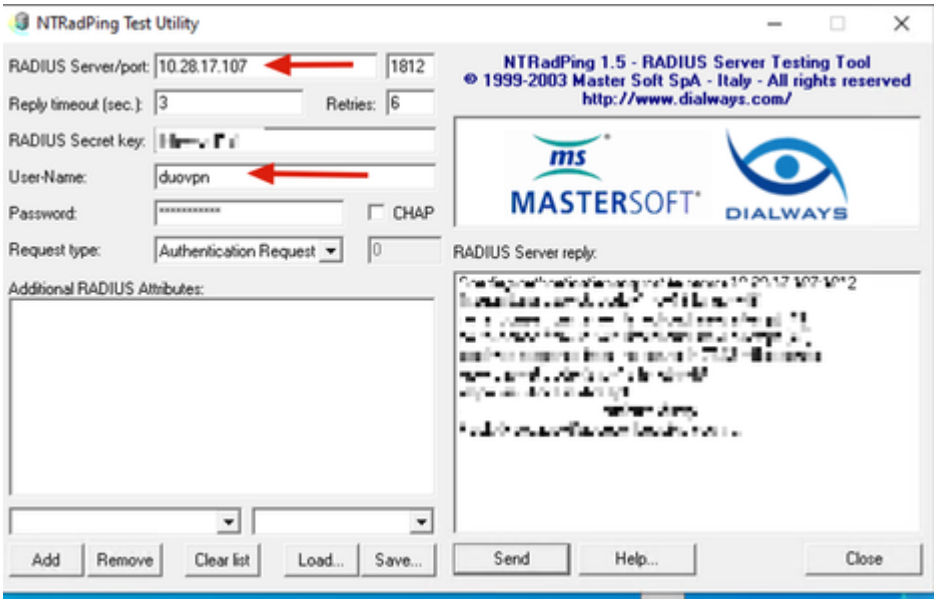
6.使用NTRadPing实用程序验证Duo身份验证代理是否正常工作

为确认Duo身份验证代理服务器正常工作，Duo提供NTRadPing工具来模拟Duo的接入请求数据包和响应。

6.1在不同的PC上安装NTRadPing并生成流量。

注意：在本示例中，使用10.28.17.3 Windows计算机。

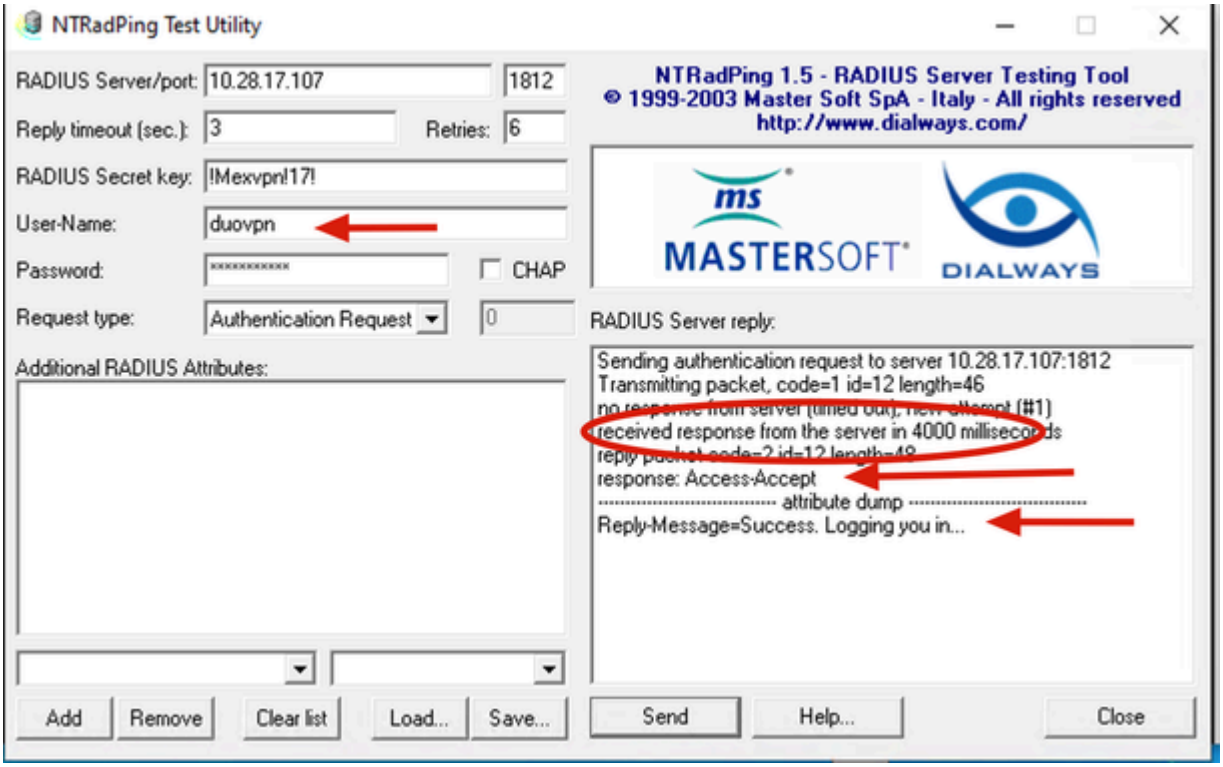
6.2使用ISE Radius配置中使用的属性进行配置。

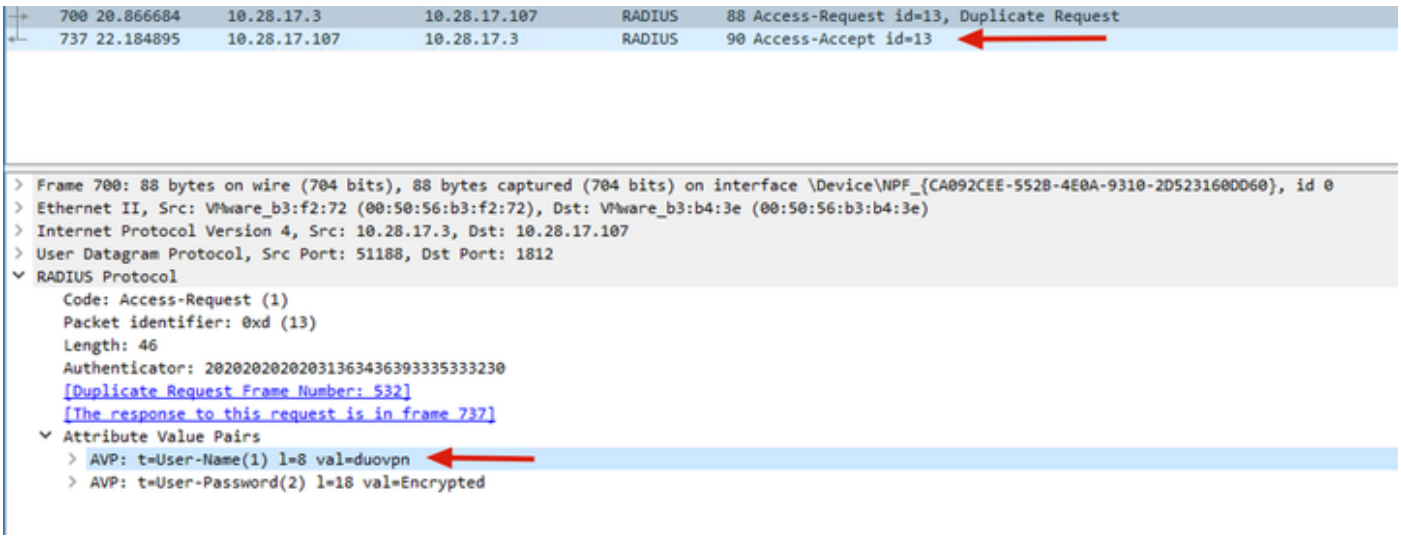


6.3像下一个示例一样配置Duo Authentication Proxy Manager:

```
[radius_server_auto]
ikey=
skey=Jac3                                    X02
api_host=a
radius_ip_1=10.28.17.101
radius_secret_1=!Mex      17!
radius_ip_2=10.28.17.3
radius_secret_2=!Me       17!
```

6.4.导航到NTRadPing工具，然后单击Send。您会在分配的移动设备上收到Duo推送通知。





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）。