

在Anyconnect/远程接入VPN客户端上配置与Active Directory和ISE的双核集成，以实现双因素身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图和场景](#)

[通信用程](#)

[Active Directory配置](#)

[Duo配置](#)

[Duo Auth代理配置](#)

[Cisco ISE配置](#)

[Cisco ASA RADIUS/ISE配置](#)

[Cisco ASA远程访问VPN配置](#)

[测试](#)

[故障排除](#)

[工作调试](#)

简介

本文档介绍作为连接到ASA的AnyConnect客户端的双因素身份验证与AD和ISE集成的双重Push。

先决条件

要求

Cisco 建议您了解以下主题：

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

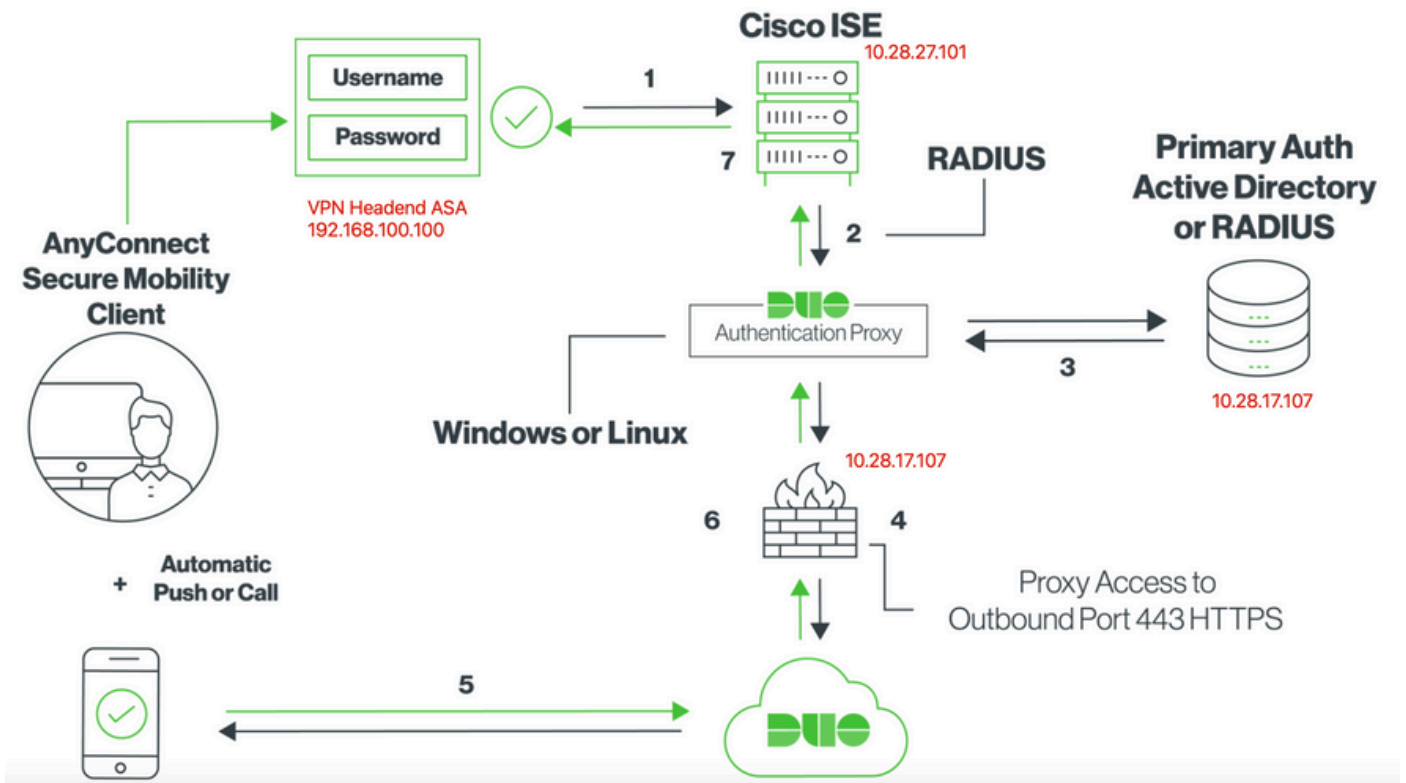
使用的组件

本文档中的信息基于以下软件和硬件版本：

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

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

[Cisco ISE的双重RADIUS身份验证](#)

1. 主身份验证启动到Cisco ISE。
2. Cisco ASA向Duo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. 已建立Duo Authentication Proxy连接，以通过TCP端口443实现Duo Security。
5. 通过Duo Security的服务进行辅助身份验证。
6. Duo认证代理接收认证响应。
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，以允许双重身份验证代理绑定到Active Directory服务器进行主要身份验证。

- Active Directory测试用户
- Duo测试用户进行辅助身份验证

Active Directory配置

Windows服务器预配置了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，则可能会发生冲突并影响性能。

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。

必须先Microsoft服务器上创建或收集所有这些详细信息，然后才能在ASA和Duo Auth代理服务器上配置。

主要值包括：

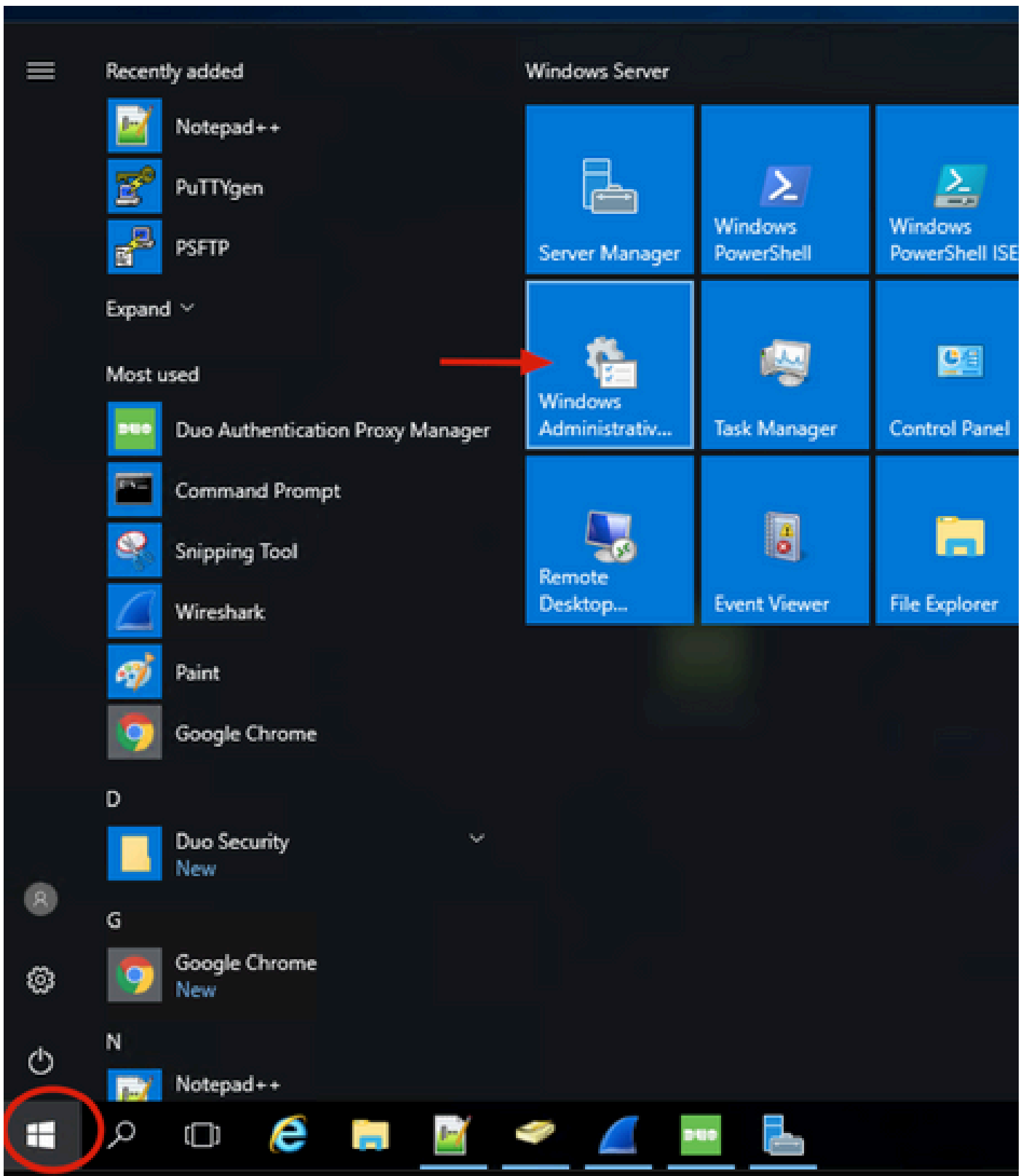
- 域名.这是服务器的域名。在本配置指南中，agarciam.cisco是域名。
- 服务器IP/完全限定域名(FQDN)地址。用于连接Microsoft服务器的IP地址或FQDN。如果使用FQDN，则必须在ASA和双重身份验证代理中配置DNS服务器以解析FQDN。

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对LDAP使用TCP端口389，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使用的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服务器并对用户进行身份验证以及搜索用户和组的帐户。
- 基本和组可分辨名称(DN)。基础DN是Duo Auth代理的出发点，它告知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。

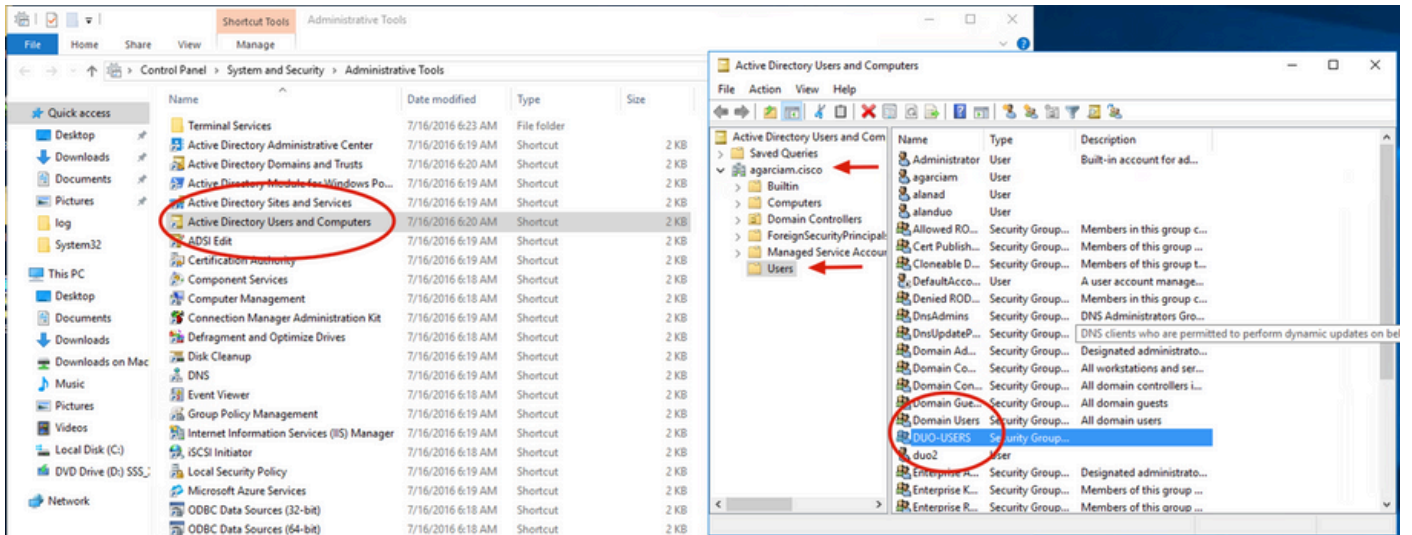
1. 为了添加新的Duo用户，请在Windows Server上导航到左下方的Windows图标，然后单击Windows管理工具，如图所示。



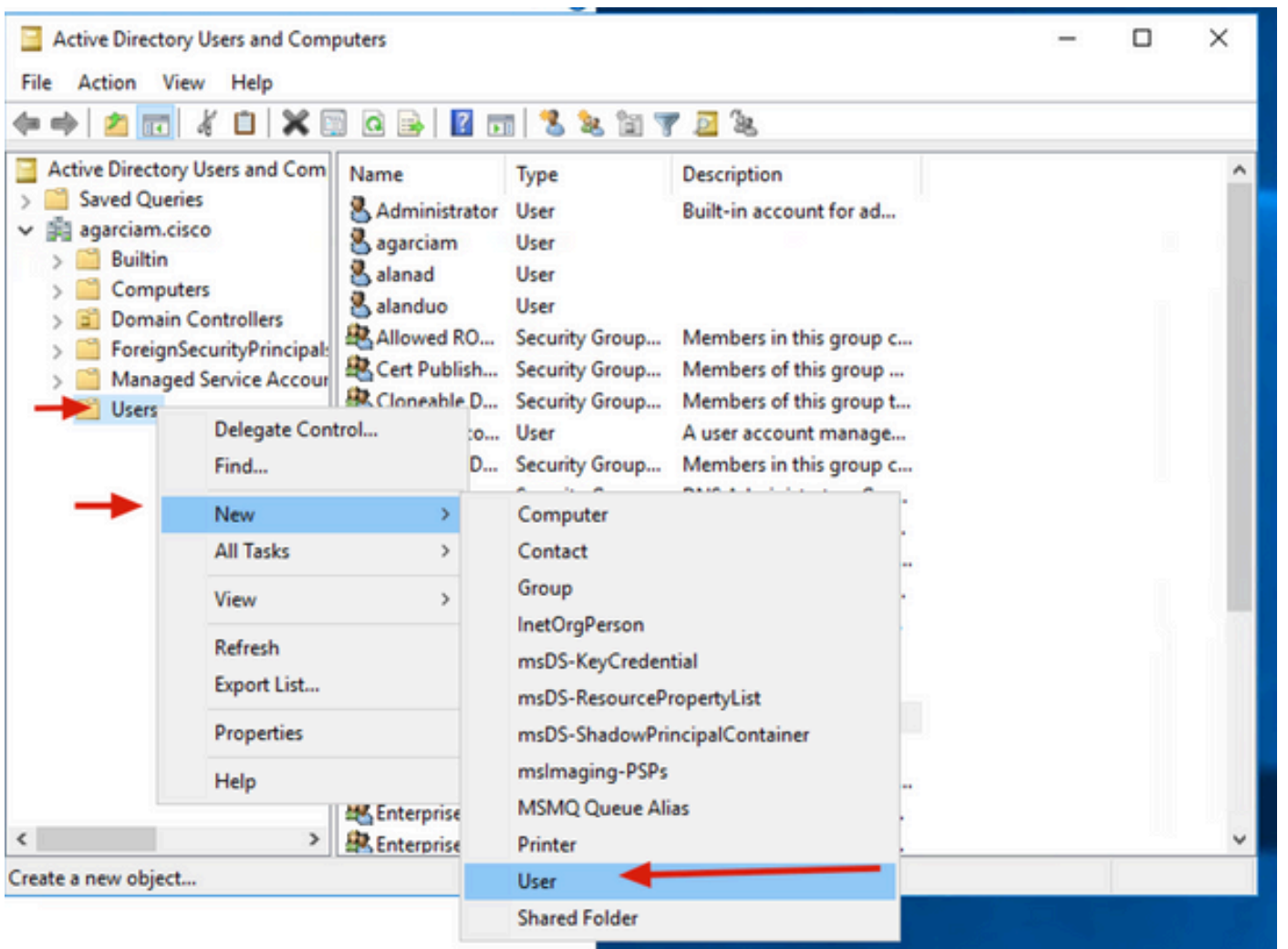
2. 在“Windows管理工具”窗口中，导航到Active Directory用户和计算机。

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

在此配置示例中，Duo-USERS用作辅助身份验证的目标组。





3. 右键单击用户文件夹，然后选择新建>用户，如图所示。



4. 在“新建对象-用户”窗口中，指定此新用户的身份属性，然后单击下一步，如图所示。


New Object - User X

 Create in: `agarciam.cisco/Users`

First name:  Initials:

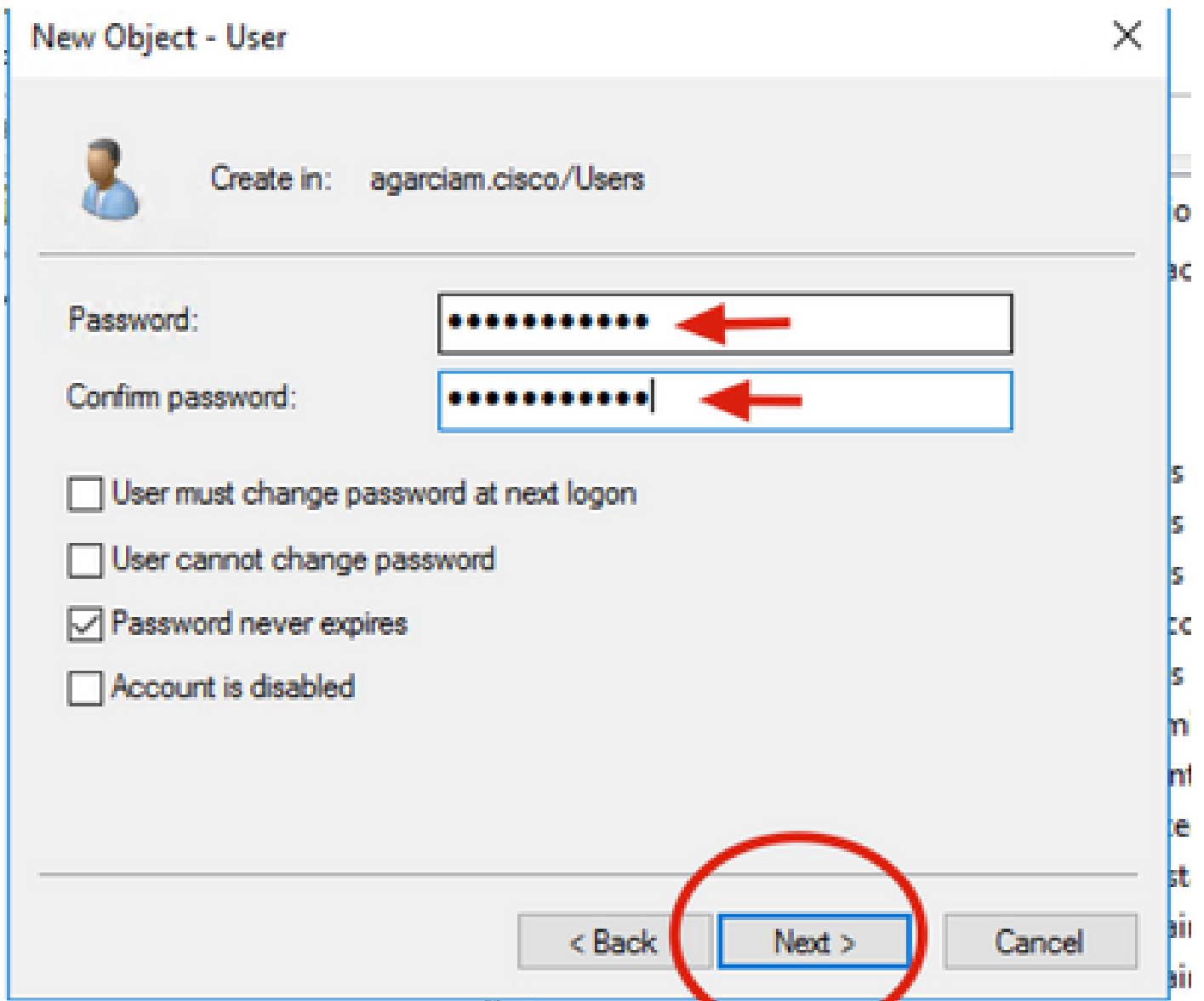
Last name:

Full name:

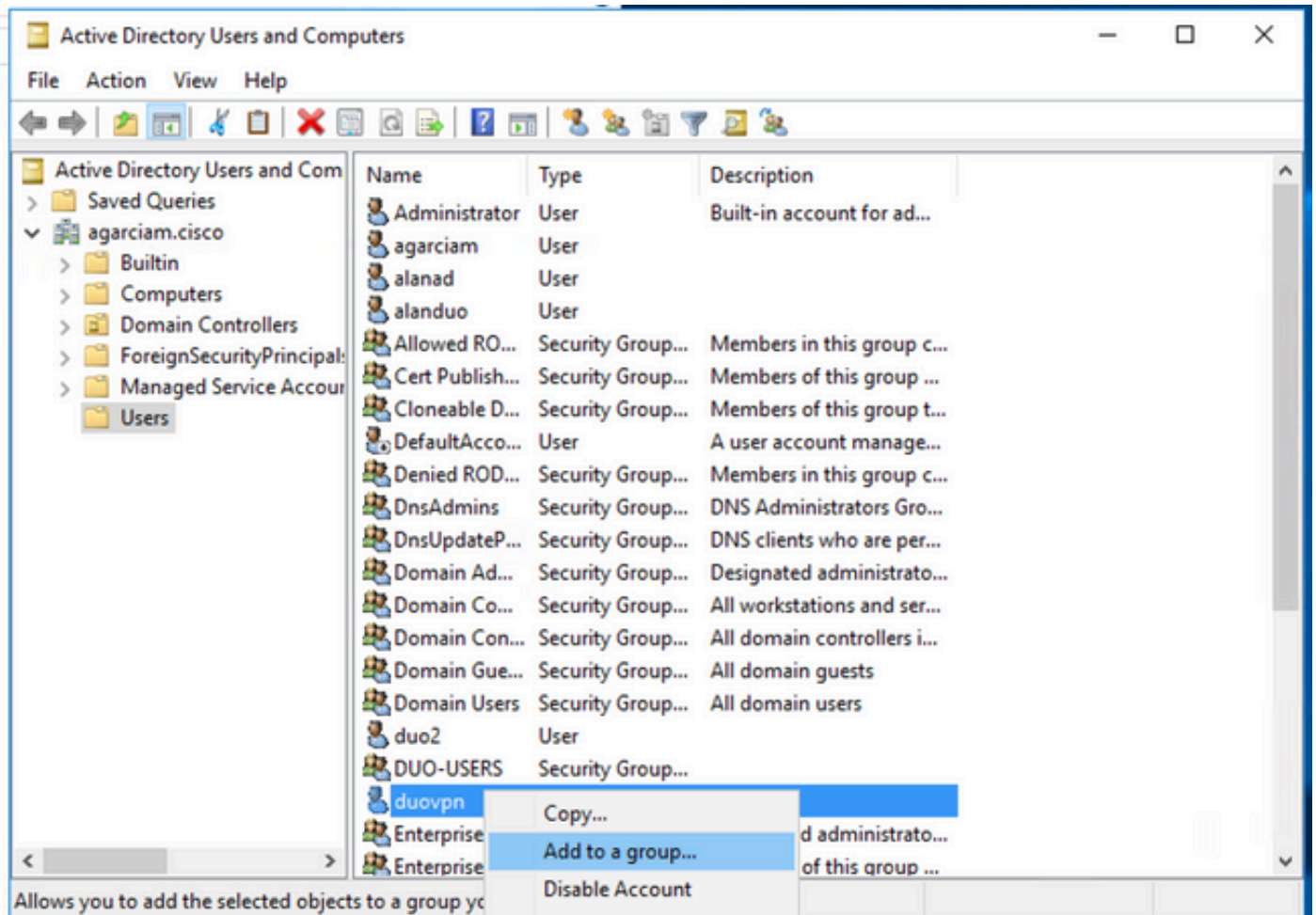
User logon name:
 

User logon name (pre-Windows 2000):

5. 确认口令并单击下一步，然后在验证用户信息之后单击完成。

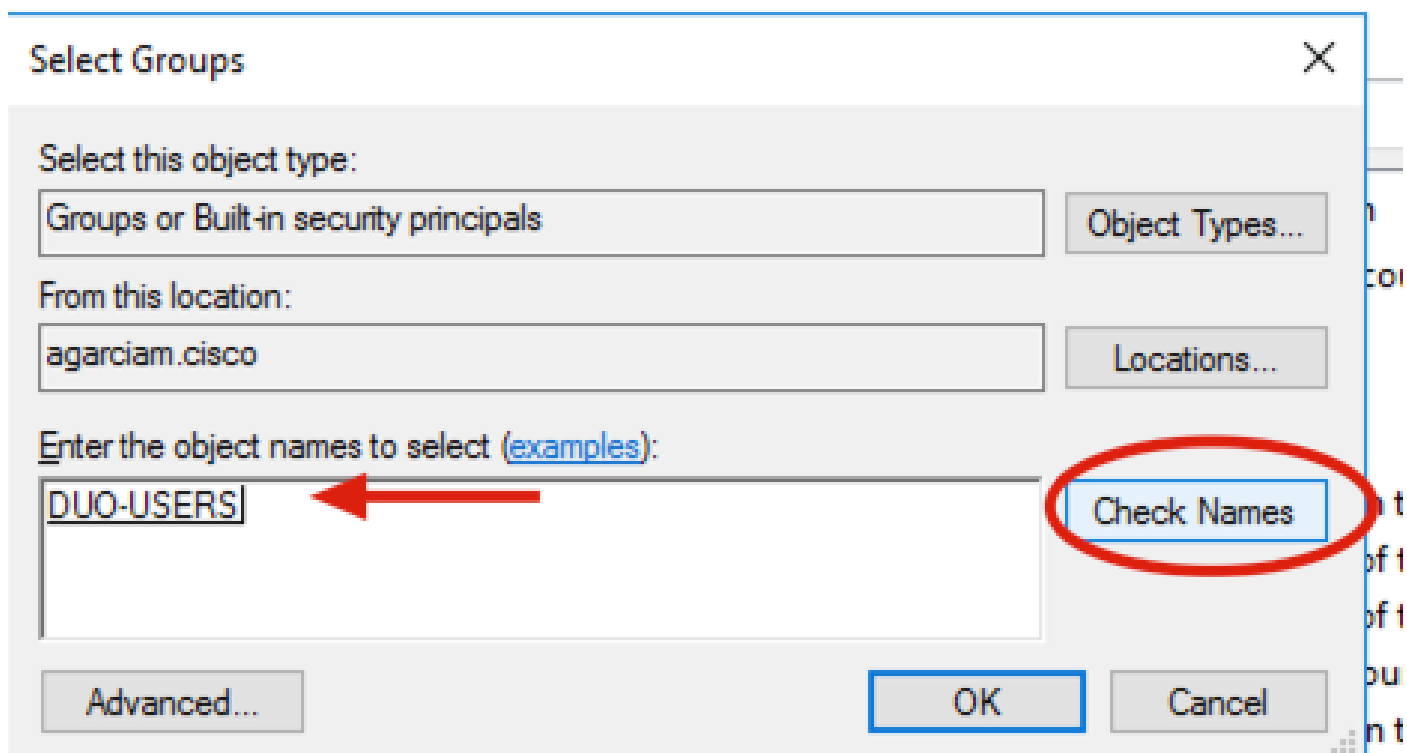


6. 将新用户分配给特定组，右键单击该用户并选择添加到组，如图所示。



7. 在“选择组”面板上，键入所需组的名称，然后单击检查名称。

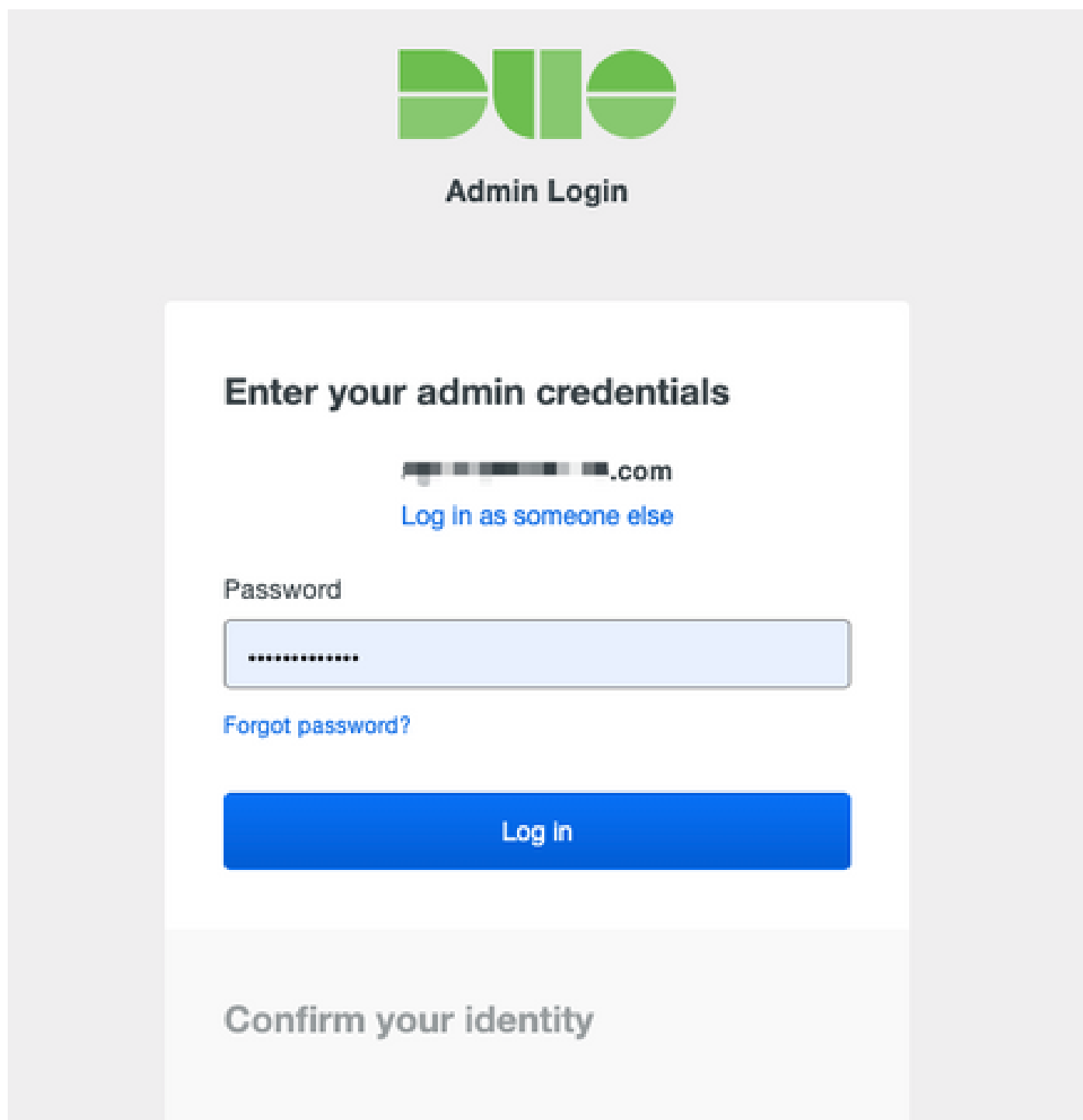
然后，选择符合条件的名称，然后单击Ok。



8. 此用户是本文档中使用的示例。

Duo配置

1. 登录您的Duo管理员门户。



Admin Login

Enter your admin credentials

██████████.com
[Log in as someone else](#)

Password

.....

[Forgot password?](#)

Log In

Confirm your identity

2. 在左侧面板上，导航到用户，单击添加用户并键入与我们的Active Domain用户名匹配的用户名，然后单击添加用户。

DUO

Search for users, groups, applications, or devices

Dashboard > Users > Add User

Add User

Most applications allow users to enroll themselves after they complete primary authentication. [Learn more about adding users](#)

Username: Should match the primary authentication username.

Add User

3. 在“新用户”面板中，填写所有必要信息。

duovpn


i This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.

Username

Username aliases [+ Add a username alias](#)
Users can have up to 8 aliases.
Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).

Full name


Email

Status **Active** 
Require multi-factor authentication (default).
 Bypass
Allow users to skip two-factor authentication and log in with only a password. Passwordless authentication is not skipped.
 Disabled
Automatically deny access.
This controls the user's two-factor authentication process.

Groups You don't have any editable groups. [Add one.](#)
Groups can be used for management, reporting, and policy. [Learn more about groups](#)

Notes
For internal use.

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，因此需要添加电话设备。

单击Add Phone。

Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#) ↗.

Add Phone

This user has no phones. [Add one.](#)

Endpoints

This user has no devices.

Hardware Tokens

Add Hardware Token

This user has no hardware tokens. [Add one.](#)

Bypass Codes

Add Bypass Code

This user has no bypass codes. [Add one.](#)

WebAuthn & U2F

Add Security Key

5. 键入用户电话号码并单击Add Phone。

Add Phone



[Learn more about Activating Duo Mobile](#)

Type

Phone

Tablet

Phone number



[Show extension field](#)

Optional. Example: "+52 1 222 123 4567"

Add Phone

6. 在左侧“Duo管理员”面板上，导航到用户，然后单击新用户。

Dashboard > Users

Users


Directory Sync | Import Users | Bulk Enroll Users [Add User](#)

i You have users who have not activated Duo Mobile. [Click here to send them activation links.](#)
Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

5 Total Users **0** Not Enrolled **2** Inactive Users **1** Trash **0** Bypass Users **0** Locked Out

Select (0) ... [Export](#) Search

<input type="checkbox"/>	Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/>	duovpn		...@... .com	1		Active	Mar 8, 2022 6:50 PM
<input type="checkbox"/>				1		Active	Mar 5, 2022 7:04 PM
<input type="checkbox"/>				1		Active	Never authenticated
<input type="checkbox"/>				1		Active	Never authenticated
<input type="checkbox"/>				1		Active	Mar 5, 2022 7:16 PM




 注意：如果您目前无权访问您的电话，可以选择电邮选项。

7. 导航到电话部分并单击激活Duo Mobile。

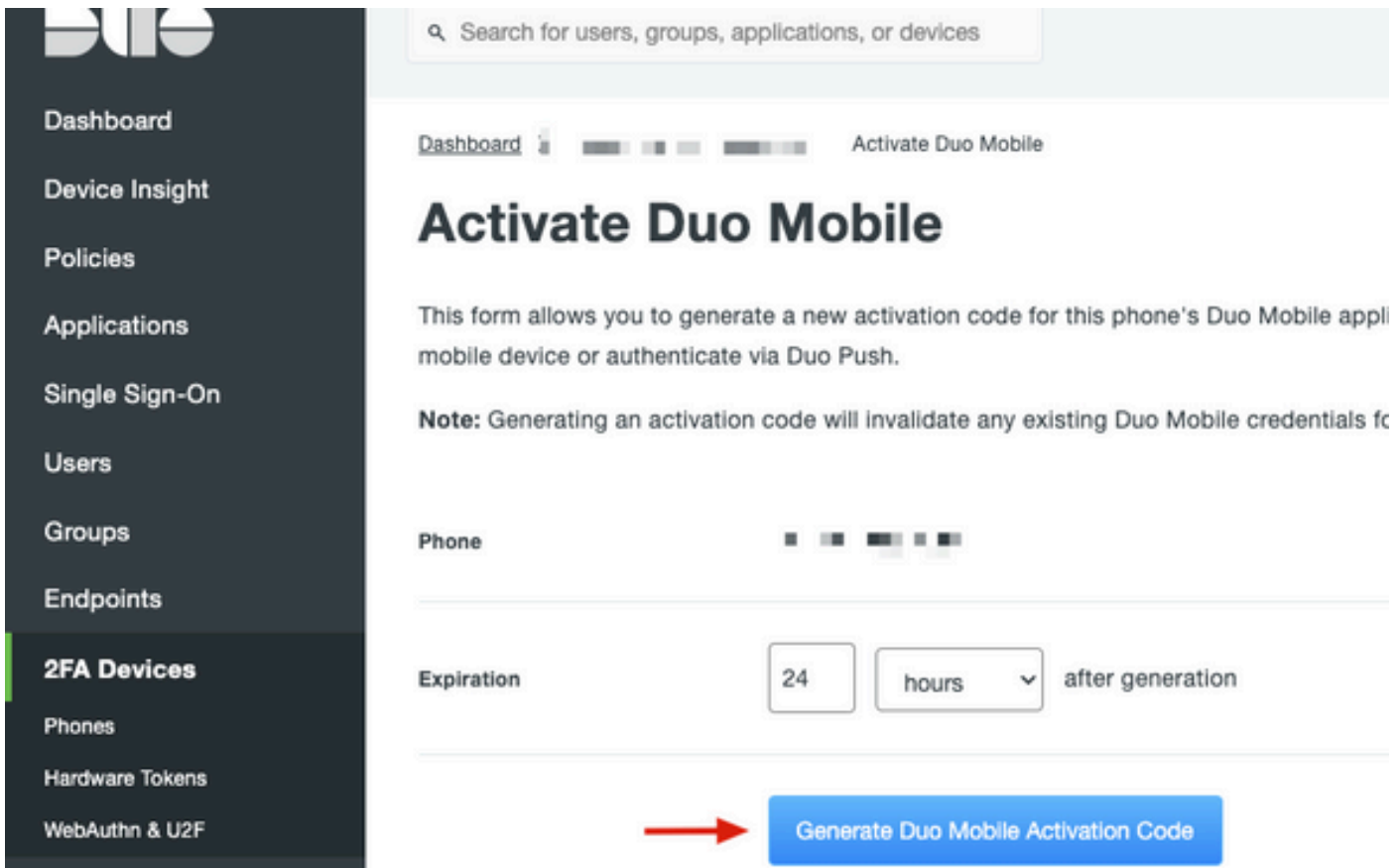
Phones

You may rearrange the phones by dragging and dropping in the table. [Learn more about activating a replacement phone](#).

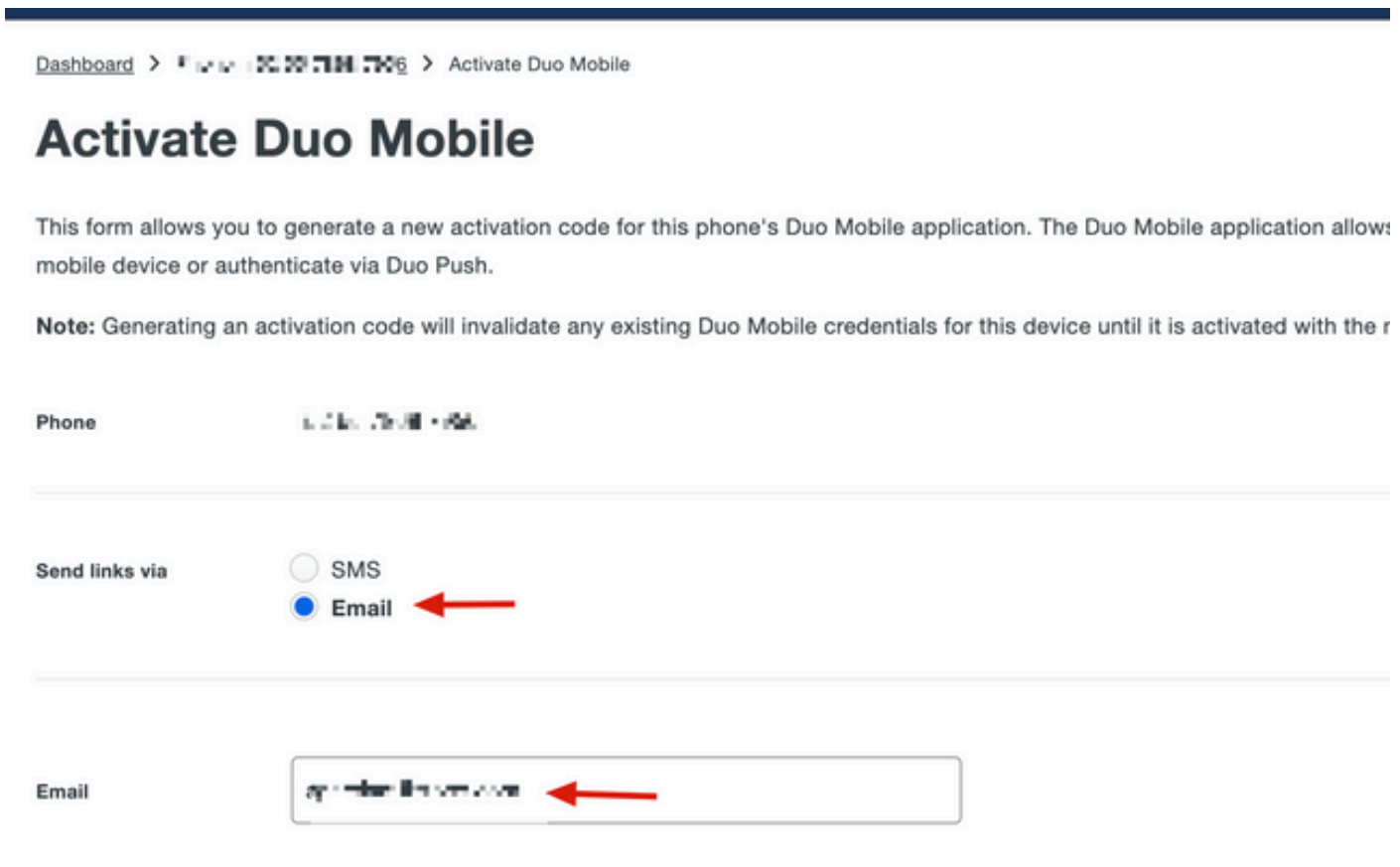
[Add Phone](#)

Alias	Device	Platform	Model	Security Warnings	
phone1		Android 10		✓ No warnings	Activate Duo Mobile 

8. 单击Generate Duo Mobile Activation Code。



9. 选择电子邮件以便通过电子邮件接收说明，键入您的电子邮件地址，然后单击通过电子邮件发送说明。



10. 您会收到一封包含说明的电子邮件，如图所示。

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>

11. 从移动设备打开Duo Mobile App，然后单击Add，然后选择Use QR code并从说明邮件扫描代码。

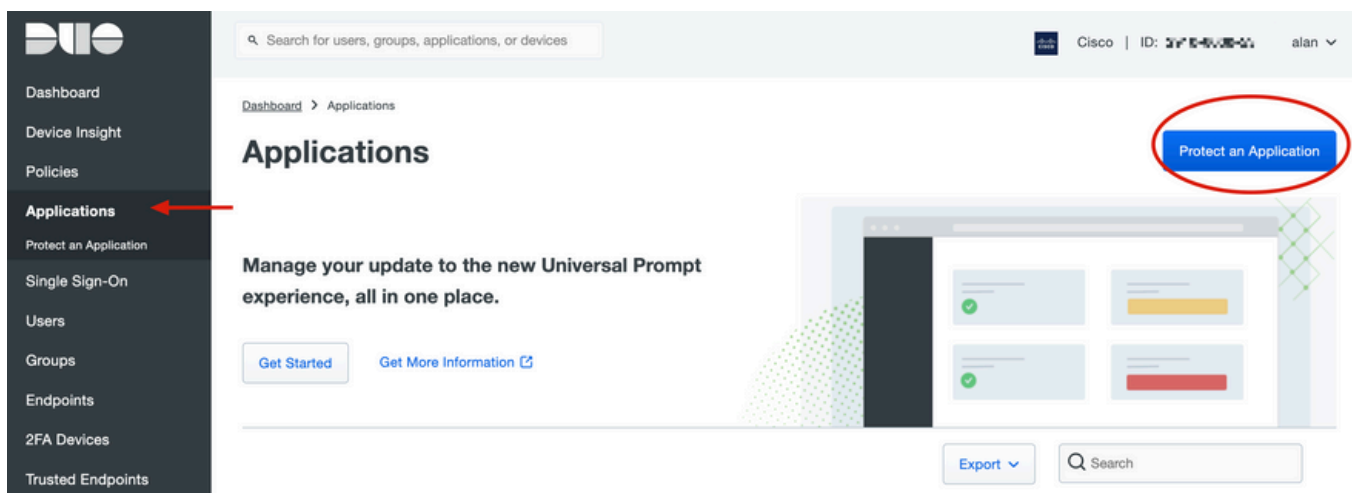
12. 新用户将添加到您的Duo移动应用。

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管理面板上，导航至“应用程序”，然后单击保护应用程序。






3. 在搜索栏中，查找Cisco ISE Radius。

Protect an Application

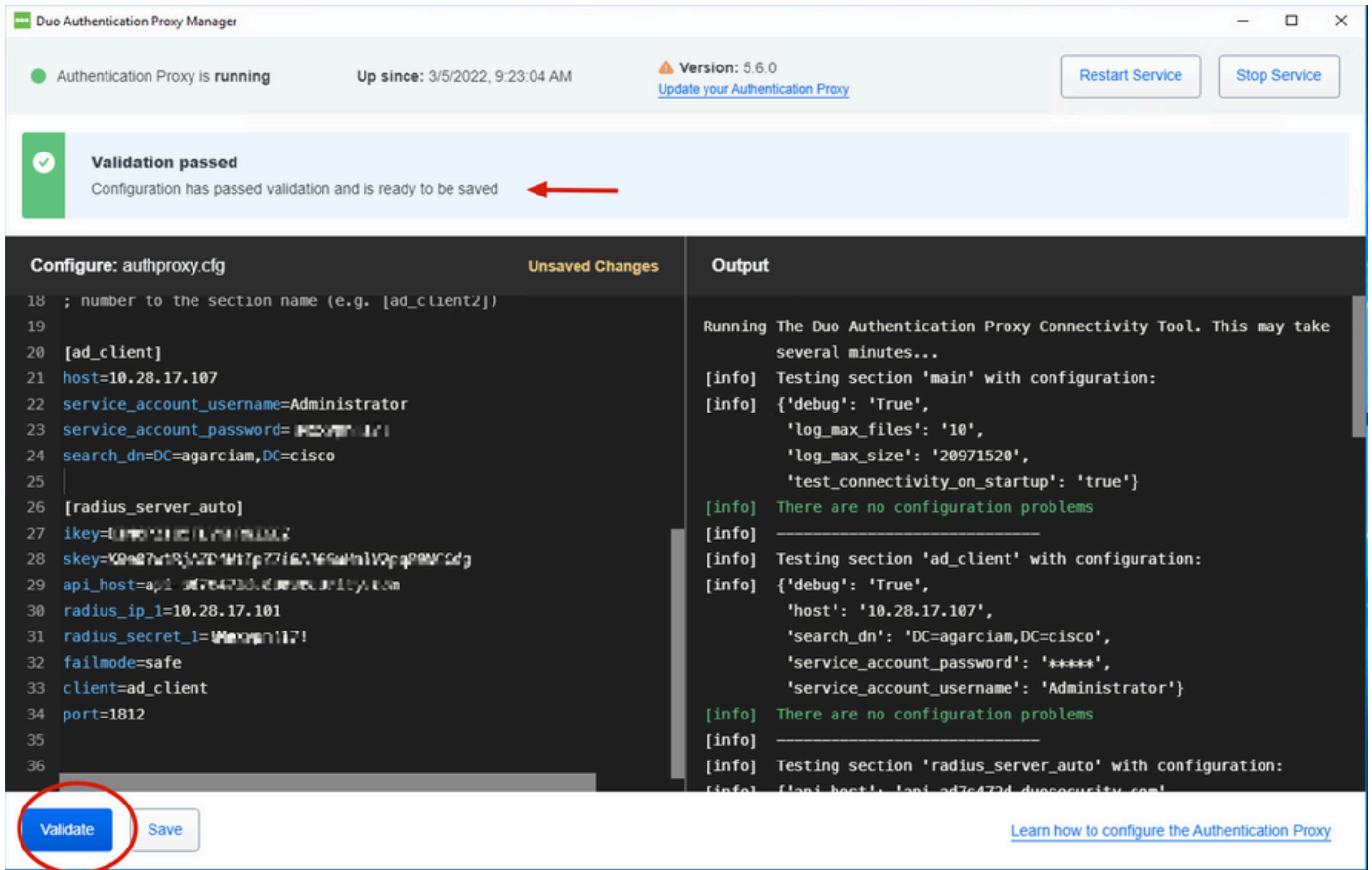
i Add an application that you'd like to protect with Duo two-factor authentication. You can start with a small "proof-of-concept" installation — it takes just a few minutes, and you're the only one that will see it, until you decide to add others.

Documentation: [Getting Started](#)

Choose an application below to get started.

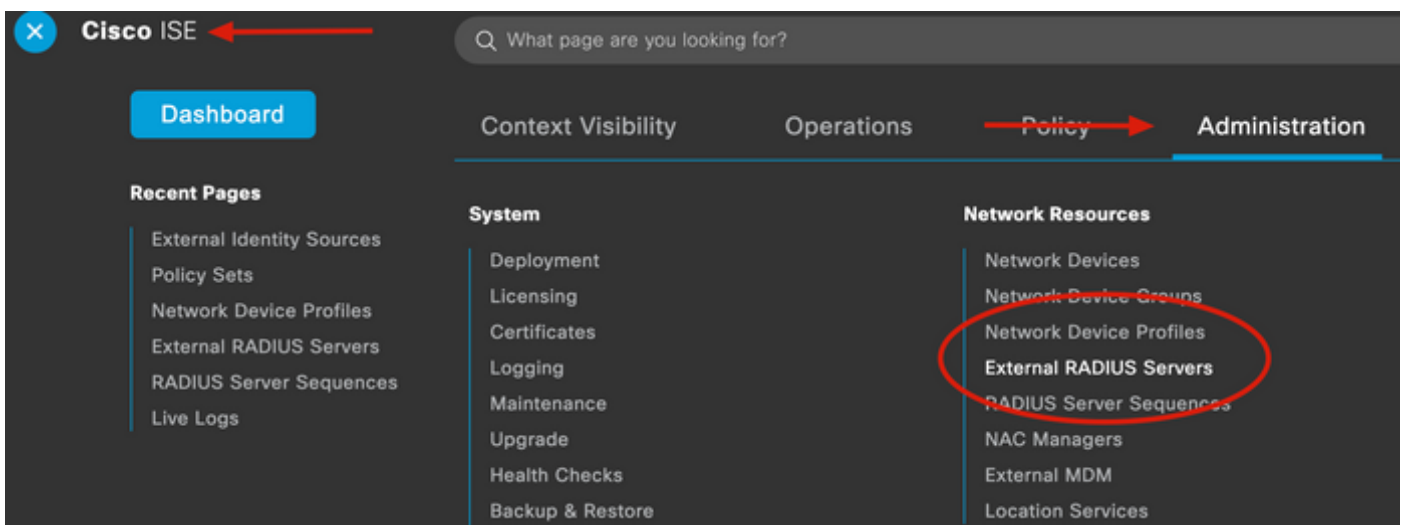
Application	Protection Type	
 Akamai Enterprise Application Access	2FA	Documentation Protect
 Cisco ISE RADIUS 	2FA	Documentation Protect

4. 复制集成密钥、密钥和API主机名。Duo认证代理配置需要此信息。

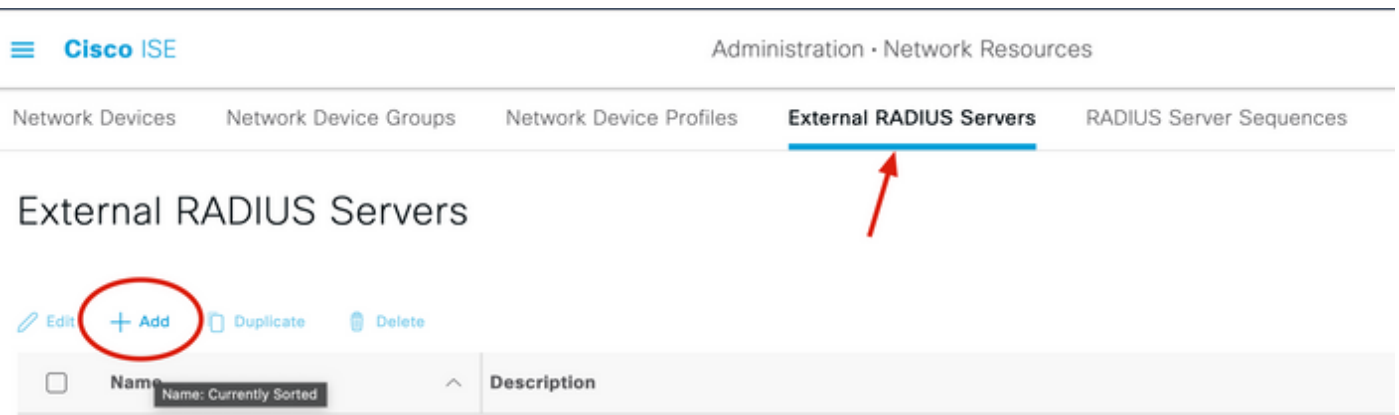


Cisco ISE配置

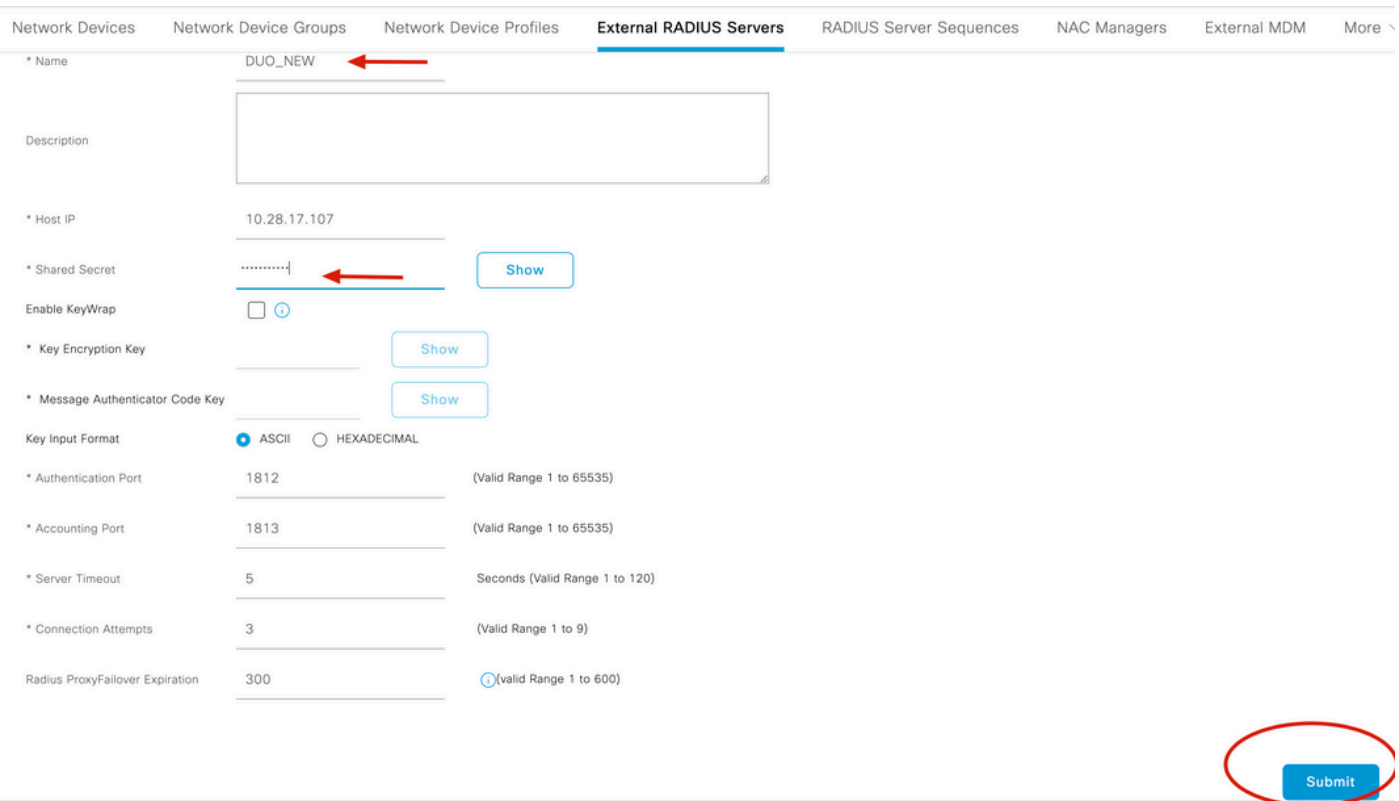
1. 登录ISE管理员门户。
2. 展开Cisco ISE选项卡并导航到Administration，然后单击Network Resources，再单击External RADIUS Servers。



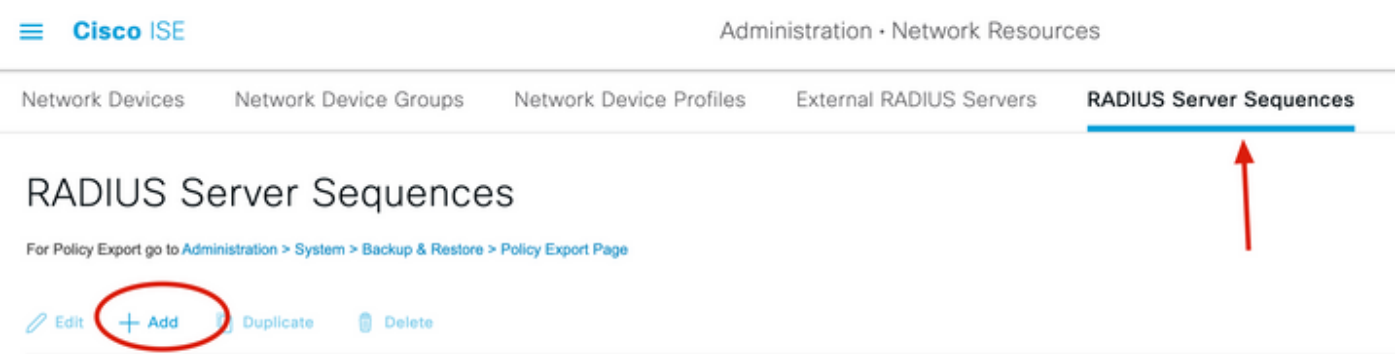
3. 在外部Radius服务器选项卡上，单击添加。



4. 使用Duo Authentication Proxy Manager中使用的RADIUS配置填写空白并单击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。

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

DUO_Sequence

Description

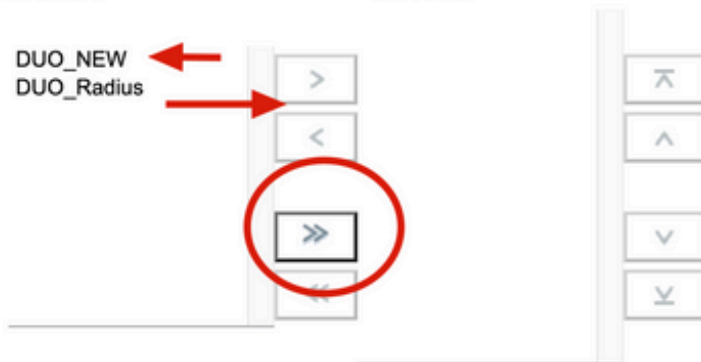
User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a response is r

Available

* Selected

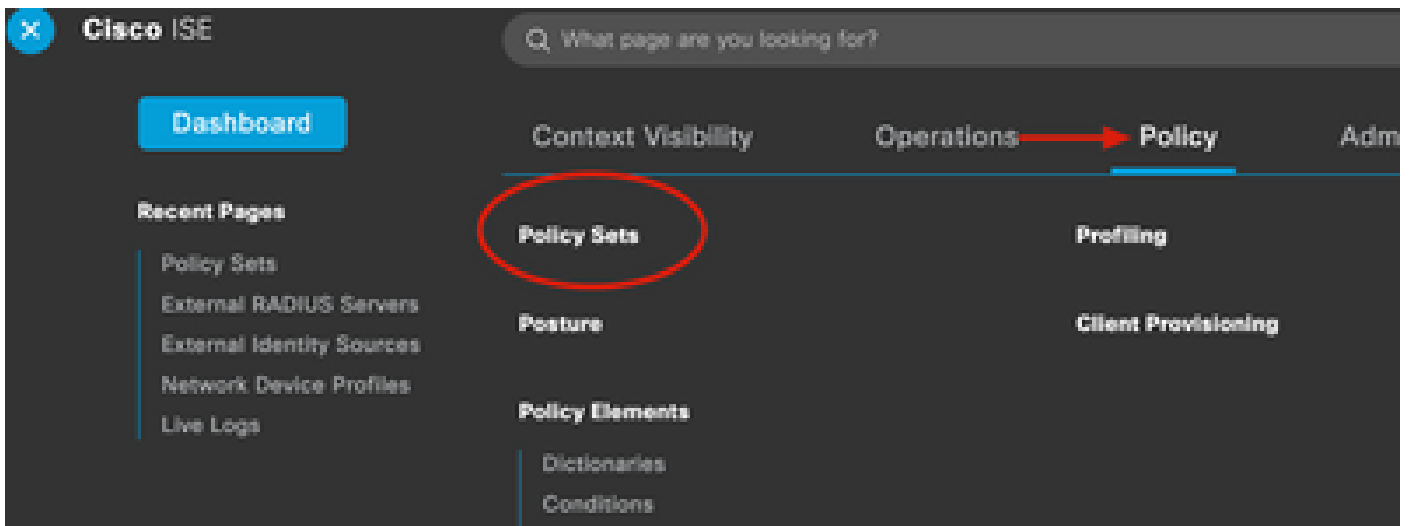
DUO_NEW
DUO_Radius




Remote accounting

Local accounting

7. 从“控制面板”菜单定位至策略，然后单击策略集。




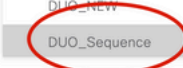
8. 将RADIUS序列分配给默认策略。

 注意：在本文档中，将应用所有连接的Duo序列，因此使用默认策略。策略分配可能因要求而异。

Policy Sets Reset [Reset Policyset Hitcount](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
			Radius-User-Name EQUALS isevpn	Default Network Access	3
			Radius-NAS-Port-Type EQUALS Virtual	DUO_Sequence	22
	Default	Default policy set		Default Network Access	0





EQ |

Allowed Protocols

- Default Network Access

Proxy Sequence

- DUO_NEW
- DUO_Sequence**

Cisco ASA RADIUS/ISE配置

1. 要在AAA服务器组下配置ISE RADIUS服务器，请导航到配置，然后单击设备管理，展开用户/AAA部分，然后选择AAA服务器组。

Bookmarks

To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".

Go Delete

Configuration

AAA Server Groups

Server Group	Pro
ISE	RA
LOCAL	LO
ad-agarciam	LD

Device Management

- > Management Access
- > Licensing
- > System Image/Configuration
- > High Availability and Scalability
- > Logging
- Smart Call-Home
- Cloud Web Security
- Service Module Settings
- Users/AAA
 - AAA Server Groups
 - LDAP Attribute Map
 - AAA Kerberos
 - Authentication Prompt
 - AAA Access
 - Dynamic Access Policies
 - User Accounts
 - Password Policy
 - Change My Password
 - Login History
- > Certificate Management
- > DHCP
- > DNS
- REST API Agent

Find:

Servers in the Selected

Server Name or IP Address
10.28.17.101

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）。