

为FMC管理访问配置双因素身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[身份验证流程](#)

[身份验证流程说明](#)

[配置](#)

[FMC的配置步骤](#)

[ISE的配置步骤](#)

[Duo管理门户的配置步骤](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍在Firepower管理中心(FMC)上为管理访问配置外部双因素身份验证所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower管理中心(FMC)对象配置
- 身份服务引擎(ISE)管理

使用的组件

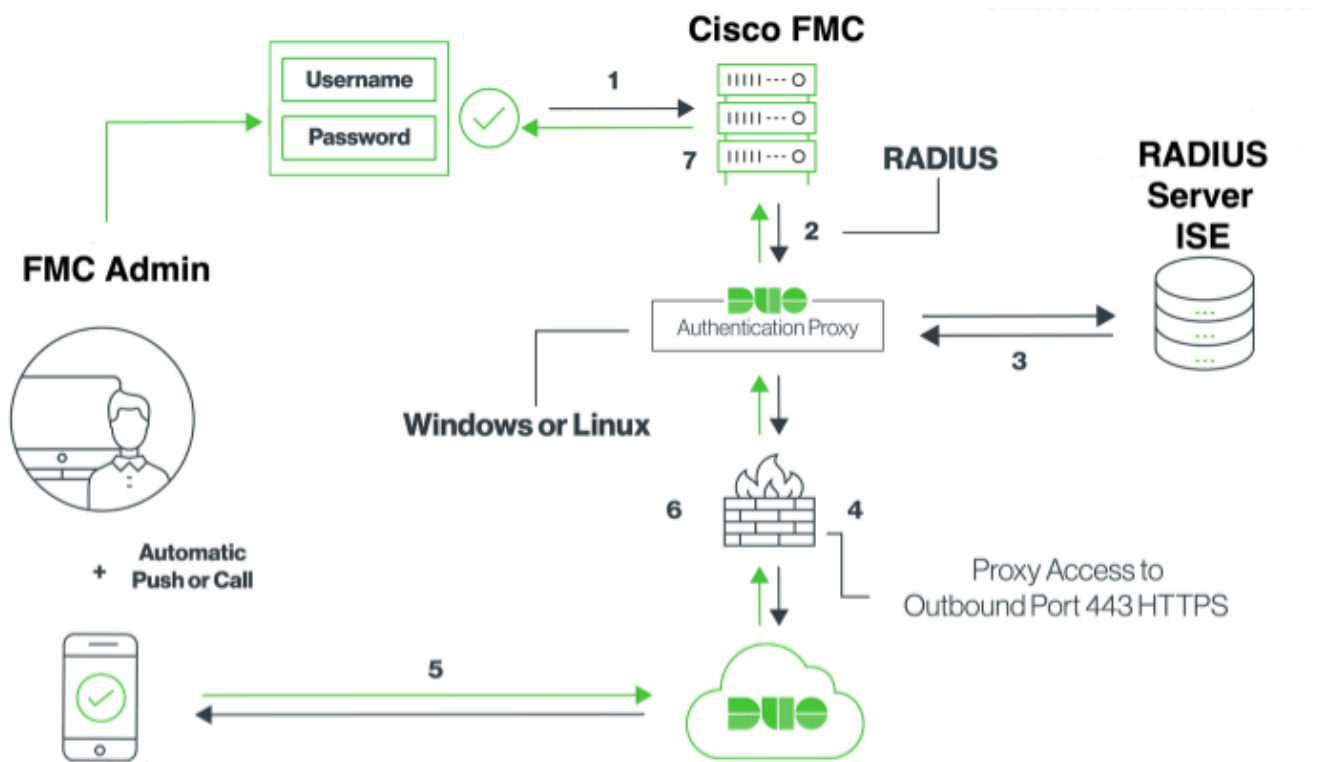
- 运行版本6.3.0的思科Firepower管理中心(FMC)
- 运行版本2.6.0.156的思科身份服务引擎(ISE)
- 支持版本的Windows(<https://duo.com/docs/authproxy-reference#new-proxy-install>)，可连接到FMC、ISE和Internet以充当Duo身份验证代理服务器
- 访问FMC、ISE和Duo管理门户的Windows计算机
- Duo Web帐户

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

FMC管理员根据ISE服务器进行身份验证，Duo Authentication Proxy服务器将向管理员的移动设备发送推送通知形式的附加身份验证。

身份验证流程



身份验证流程说明

1. 向Cisco FMC发起主要身份验证。
2. 思科FMC向双身份验证代理发送身份验证请求。
3. 主要身份验证必须使用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. 思科FMC GUI访问权限已授予。


配置

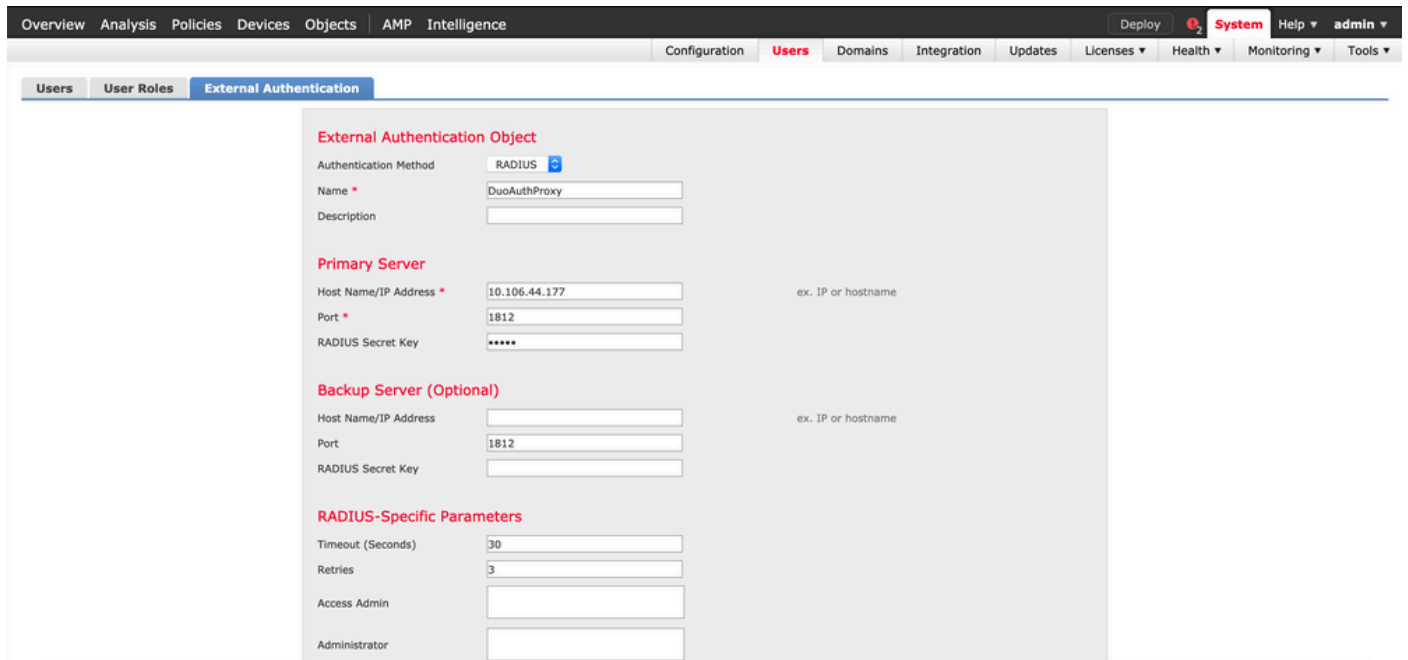
要完成配置，请考虑以下部分：

FMC的配置步骤

步骤1:导航到System > Users > External Authentication。 创建外部身份验证对象并将身份验证方

法设置为RADIUS。 确保在Default User Role下选择了Administrator， 如图所示：

 注意:10.106.44.177是Duo身份验证代理服务器的示例IP地址。



External Authentication Object

Authentication Method: RADIUS

Name: DuoAuthProxy

Description:

Primary Server

Host Name/IP Address: 10.106.44.177 (ex. IP or hostname)

Port: 1812

RADIUS Secret Key: ****

Backup Server (Optional)

Host Name/IP Address: (ex. IP or hostname)

Port: 1812

RADIUS Secret Key:

RADIUS-Specific Parameters

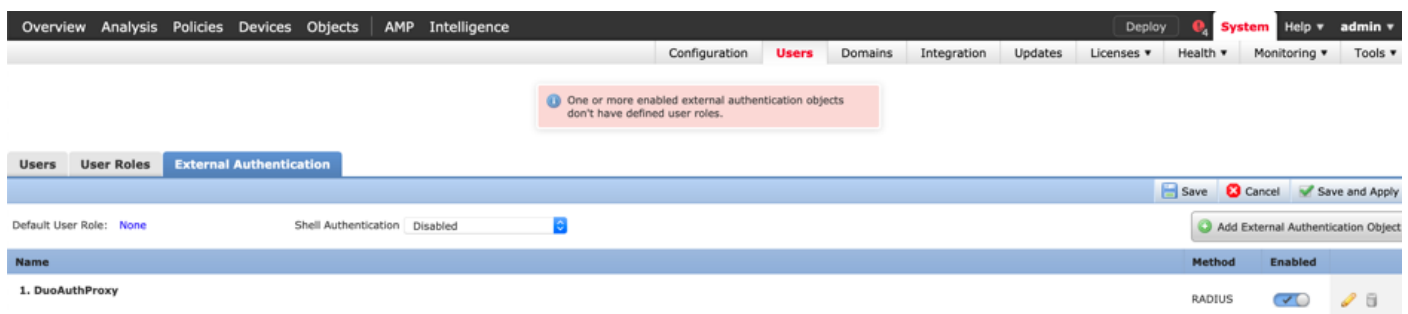
Timeout (Seconds): 30

Retries: 3

Access Admin:

Administrator:

单击Save和Apply。 忽略如图所示的警告：



One or more enabled external authentication objects don't have defined user roles.

Save Cancel Save and Apply

Default User Role: None Shell Authentication: Disabled

Name	Method	Enabled
1. DuoAuthProxy	RADIUS	<input checked="" type="checkbox"/>

第二步： 导航到System > Users > Users。 创建用户， 然后检查身份验证方法作为外部， 如图所示：

User Configuration

User Name

Authentication



Use External Authentication Method

Options



Exempt from Browser Session Timeout

User Role Configuration

Default User Roles



Administrator



External Database User



Security Analyst



Security Analyst (Read Only)



Security Approver



Intrusion Admin



Access Admin



Network Admin



Maintenance User



Discovery Admin



Threat Intelligence Director (TID) User

Save

Cancel

步骤1: 下载并安装Duo身份验证代理服务器。


登录到Windows计算机并安装[Duo Authentication Proxy Server](#)

建议使用至少具有1个CPU、200 MB磁盘空间和4 GB RAM的系统

 注意：此计算机必须能够访问FMC、RADIUS服务器（在本例中为ISE）和双核云（互联网）

第二步：配置authproxy.cfg文件。

在文本编辑器(如记事本++或写字板)中打开此文件。

 注意：默认位置位于C:\Program Files(x86)\Duo Security Authentication Proxy\conf\authproxy.cfg

编辑authproxy.cfg文件并添加以下配置：

```
<#root>
```

```
[radius_client]
```

```
host=10.197.223.23          Sample IP Address of the ISE server
```

```
secret=cisco
```

Password configured on the ISE server in order to register the network device

FMC的IP地址必须与RADIUS密钥一起配置。

```
<#root>
```

```
[radius_server_auto]
```

```
ikey=xxxxxxxxxxxxxxxx
```

```
skey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
api_host=api-xxxxxxx.duosecurity.com
```

```
radius_ip_1=10.197.223.76
```

```
IP of FMC
```

```
radius_secret_1=cisco
```

```
Radius secret key used on the FMC
```

```
failmode=safe
```

```
client=radius_client
```

```
port=1812
```

```
api_timeout=
```

确保配置ikey、skey和api_host参数。要获取这些值，请登录您的双核帐户([Duo Admin Login](#))并导航到应用>保护应用。接下来，选择RADIUS身份验证应用，如图所示：

RADIUS

See the [RADIUS documentation](#) to integrate Duo into your RADIUS-enabled platform.

Details

Integration key	<input type="text" value="REDACTED"/>	select
Secret key	Click to view.	select
Don't write down your secret key or share it with anyone.		
API hostname	<input type="text" value="REDACTED"/>	select

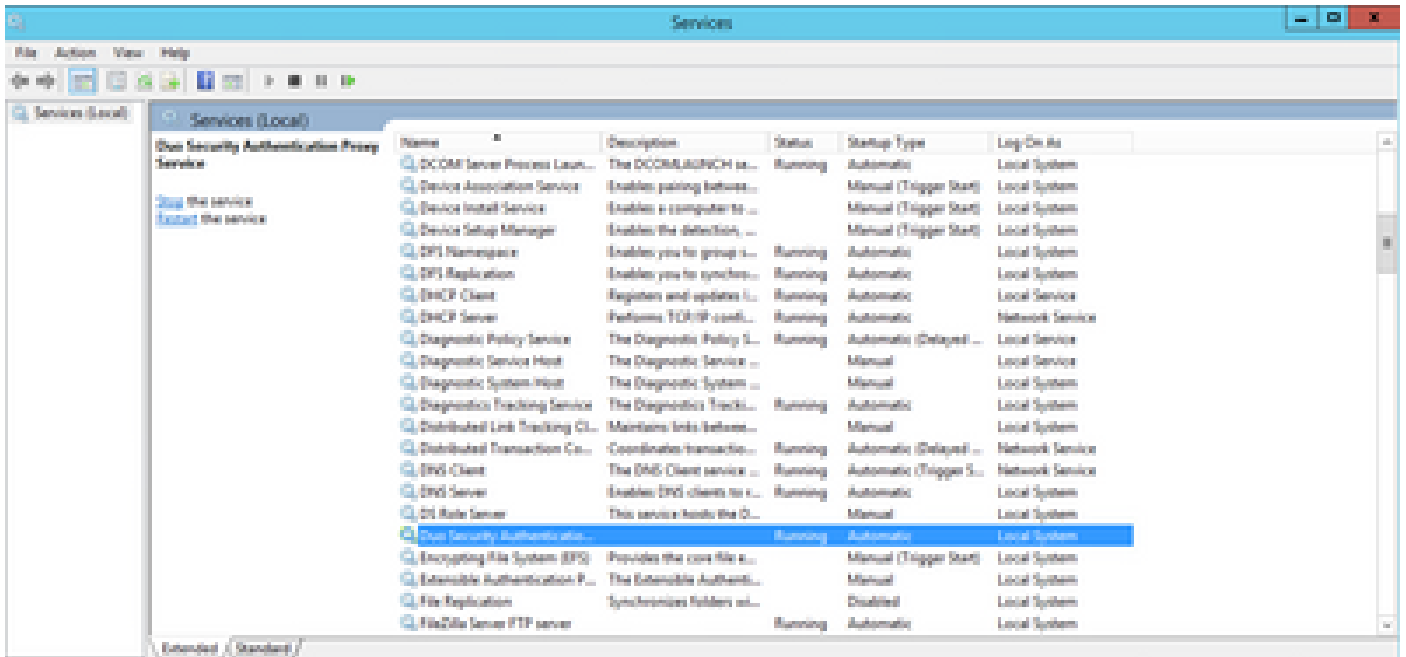
集成密钥= ikey

secret key = skey

API主机名= api_host


第三步：重新启动Duo Security Authentication Proxy服务。保存文件并重新启动Windows计算机上的Duo服务。

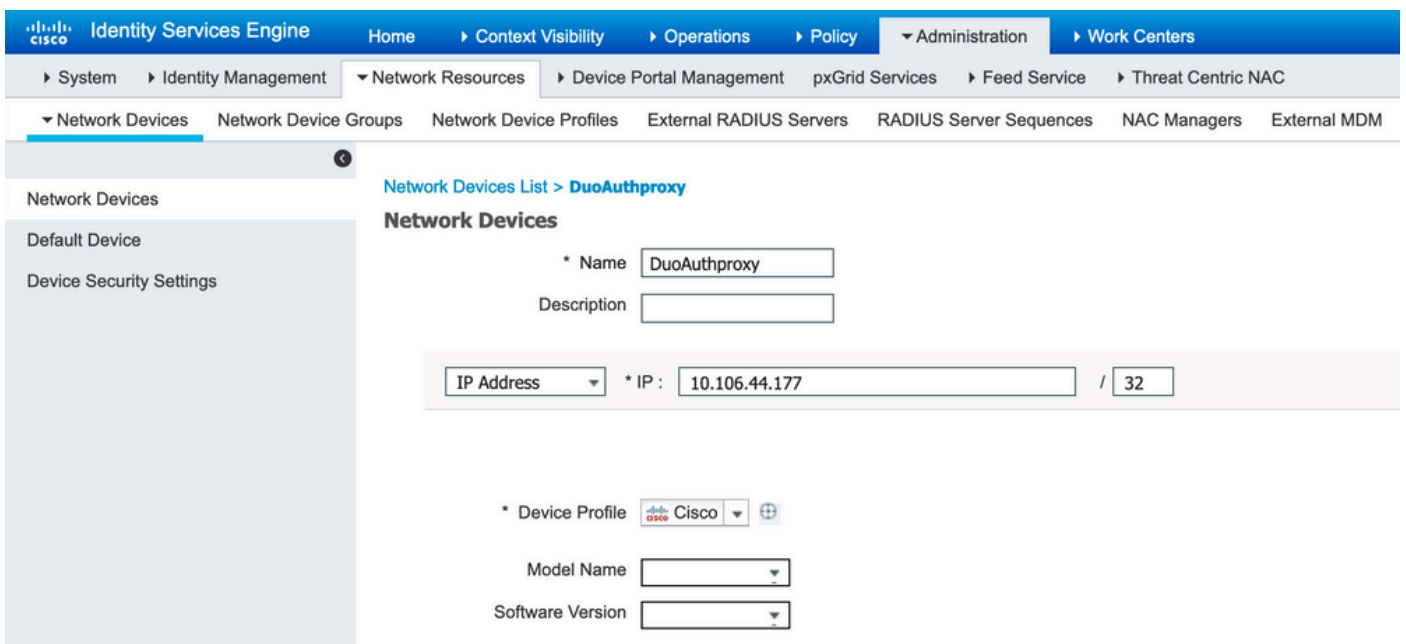
打开Windows服务控制台(services.msc)。在服务列表中找到Duo Security Authentication Proxy Service，然后单击Restart，如图所示：



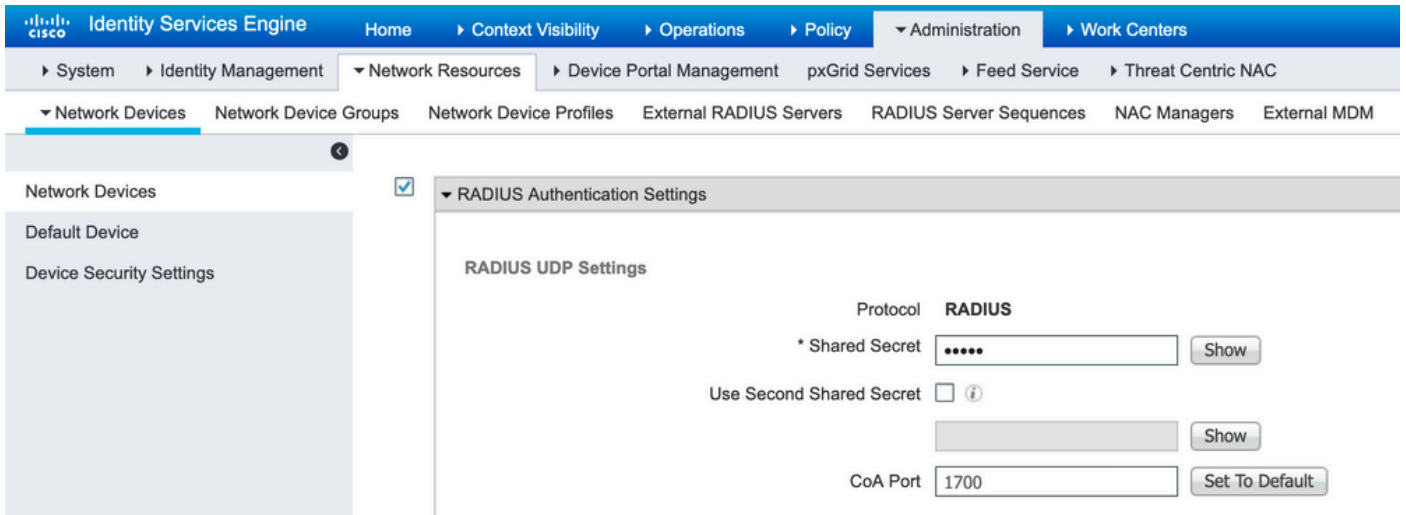
ISE的配置步骤

步骤1:导航到Administration > Network Devices，单击Add以配置网络设备，如图所示：

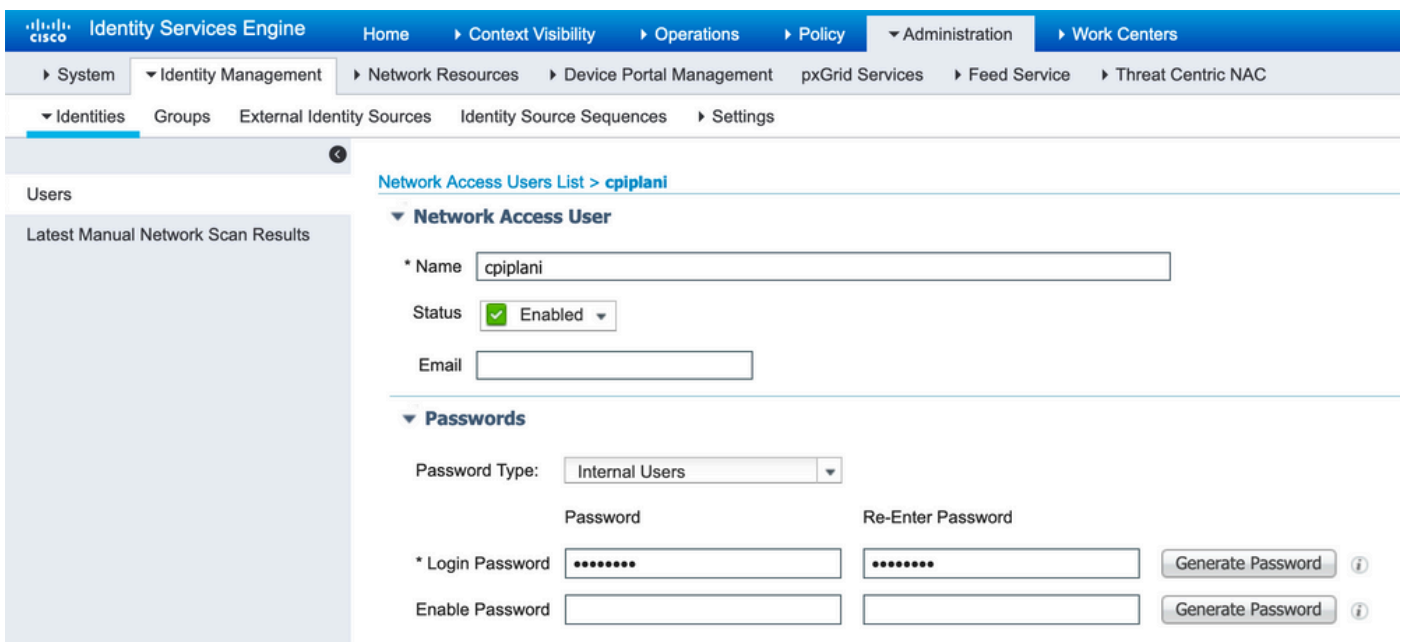
 注意:10.106.44.177是Duo身份验证代理服务器的示例IP地址。



按照authproxy.cfg中所述配置secret中的共享密钥，如图所示：



第二步：导航到管理>身份。单击Add以配置身份用户，如图所示：



Duo管理门户的配置步骤

步骤1:创建用户名并在终端设备上激活Duo Mobile。

将该用户添加到双核云管理网页上。导航到Users > Add users，如图所示：

Learn more about adding users'. A form field for 'Username' contains the text 'cpiplani' and has a note below it: 'Should match the primary authentication username.' At the bottom right of the form is a blue 'Add User' button."/>


Dashboard > Users > Add User

Add User

Adding Users
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](#)

 注意：确保最终用户安装了Duo应用。

[手动安装IOS设备Duo应用程序](#)

[手动安装适用于Android设备的Duo应用程序](#)

第二步：代码的自动生成。

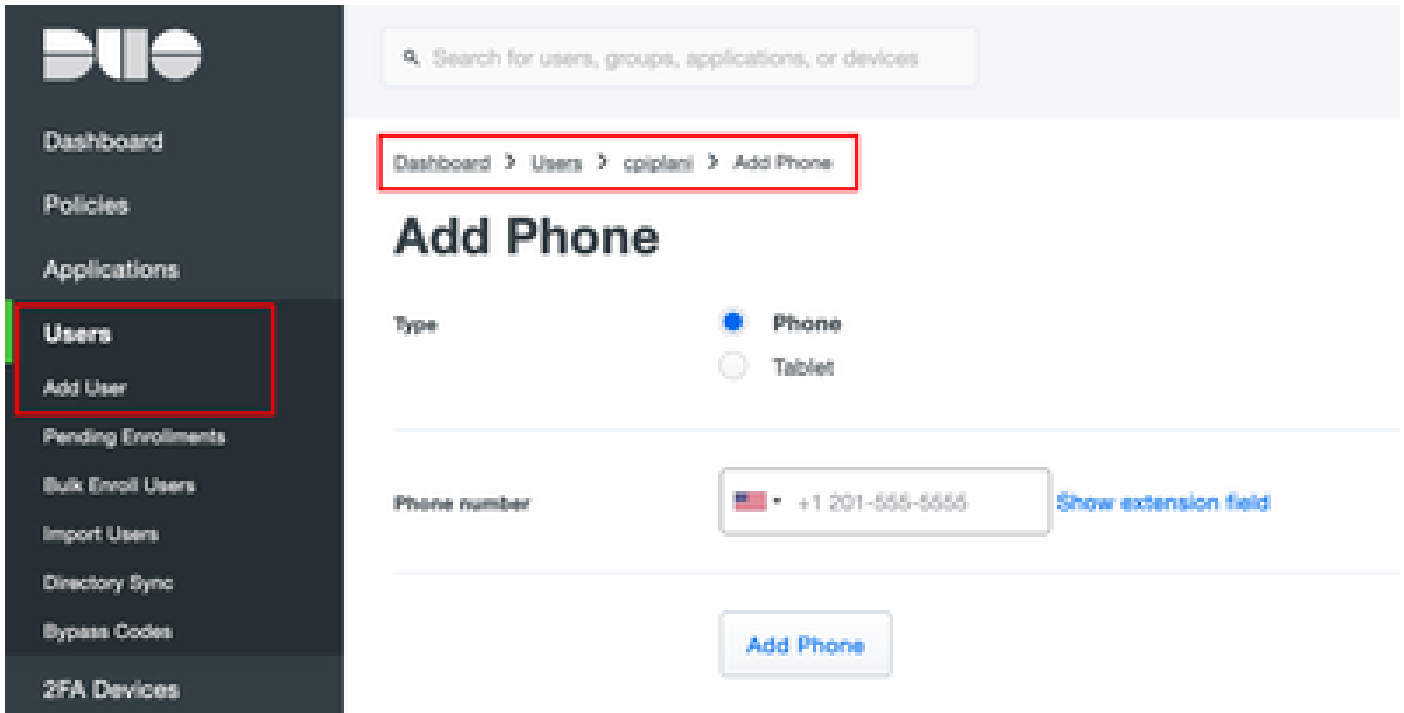
添加用户的电话号码，如图所示：

Add one.' centered inside."/>

Phones [Add Phone](#)

You may rearrange the phones by dragging and dropping in the table.

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



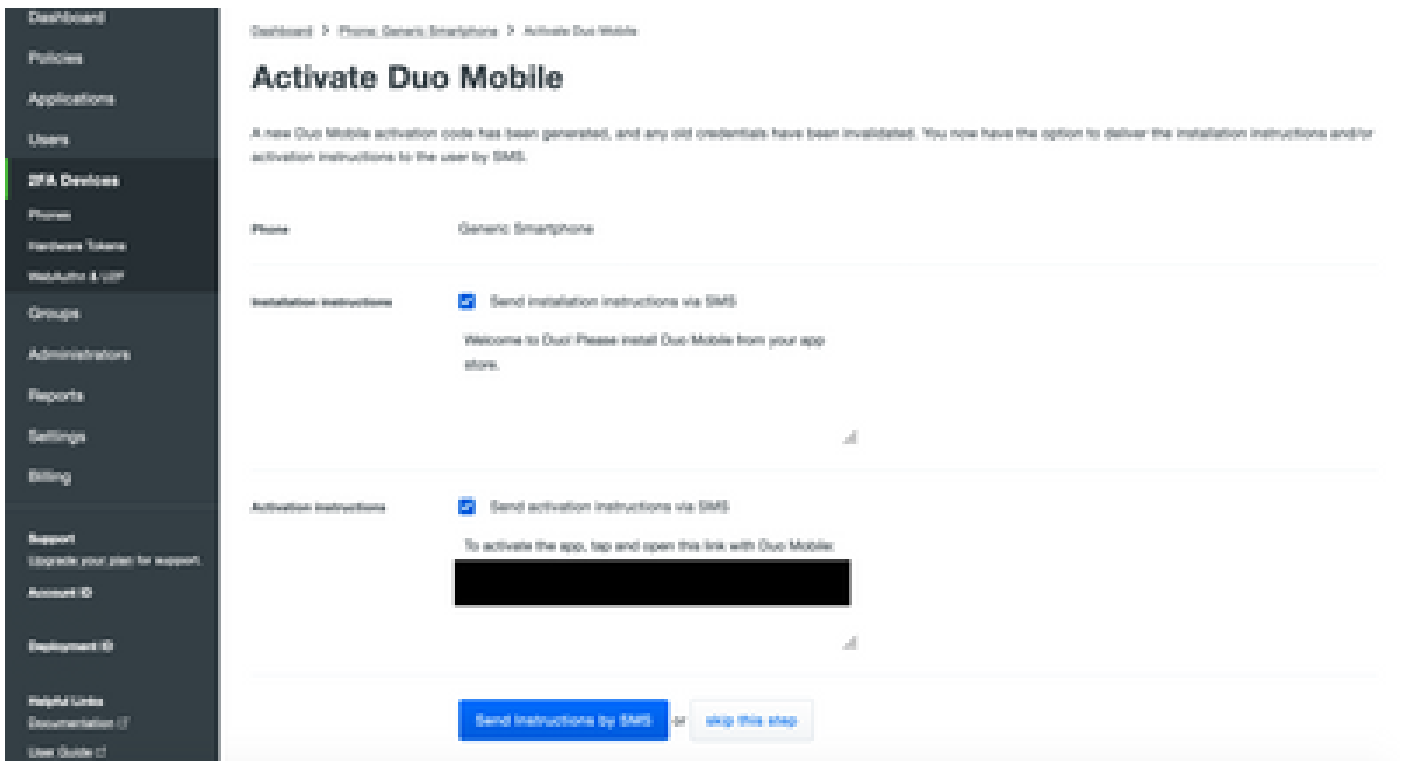
选择Activate Duo Mobile，如图所示：



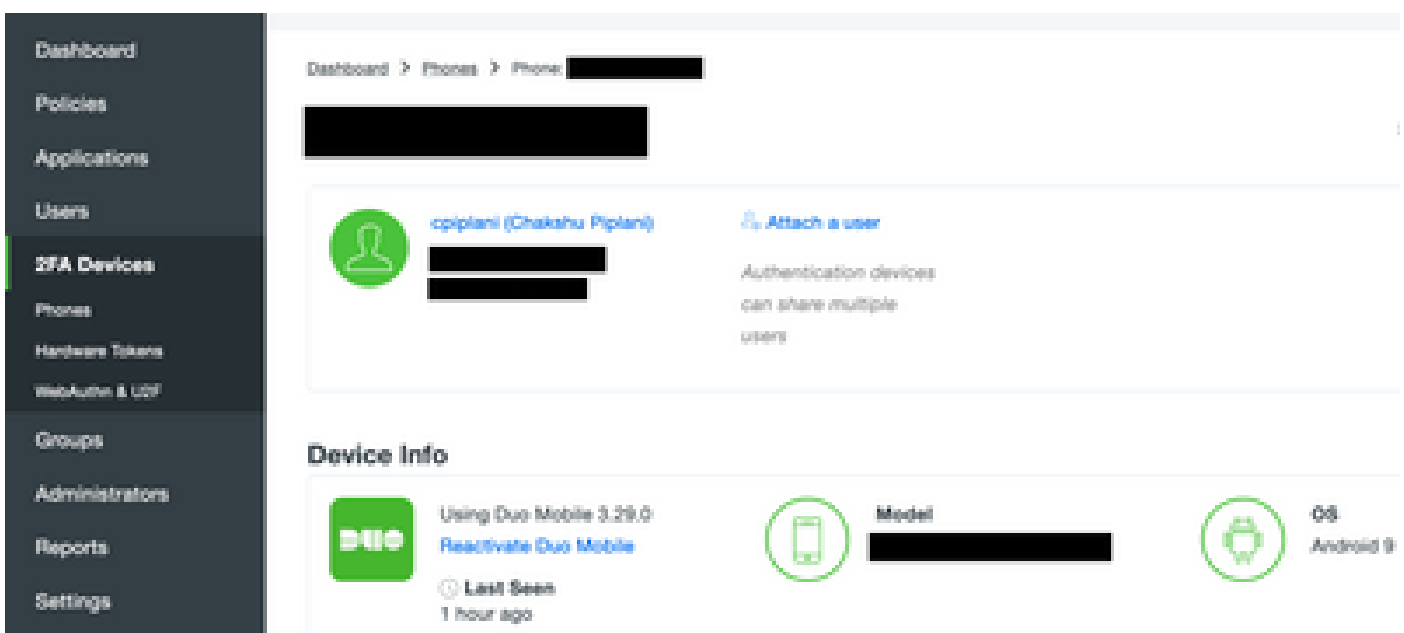
选择Generate Duo Mobile Activation Code，如图所示：



选择Send Instructions by SMS，如图所示：



单击SMS中的链接，Duo应用将链接到“设备信息”部分中的用户帐户，如图所示：



验证

使用本部分可确认配置能否正常运行。

使用在ISE用户身份页面添加的用户凭证登录到FMC。您必须在您的终端上收到双因素身份验证(2FA)的双重PUSH通知，请批准该通知，然后FMC将按如下图所示登录：

Login Request



CISCO SYSTEMS



cpiplani



August 2, 2019, 7:37 PM



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）。