为ISE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

网络图

配置

- Duo配置
- ISE 配置
- 将ISE与双身份验证代理集成

验证

故障排除

相关信息

简介

本文档介绍为身份服务引擎(ISE)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：

- RADIUS协议
- 配置ISE RADIUS令牌服务器和身份

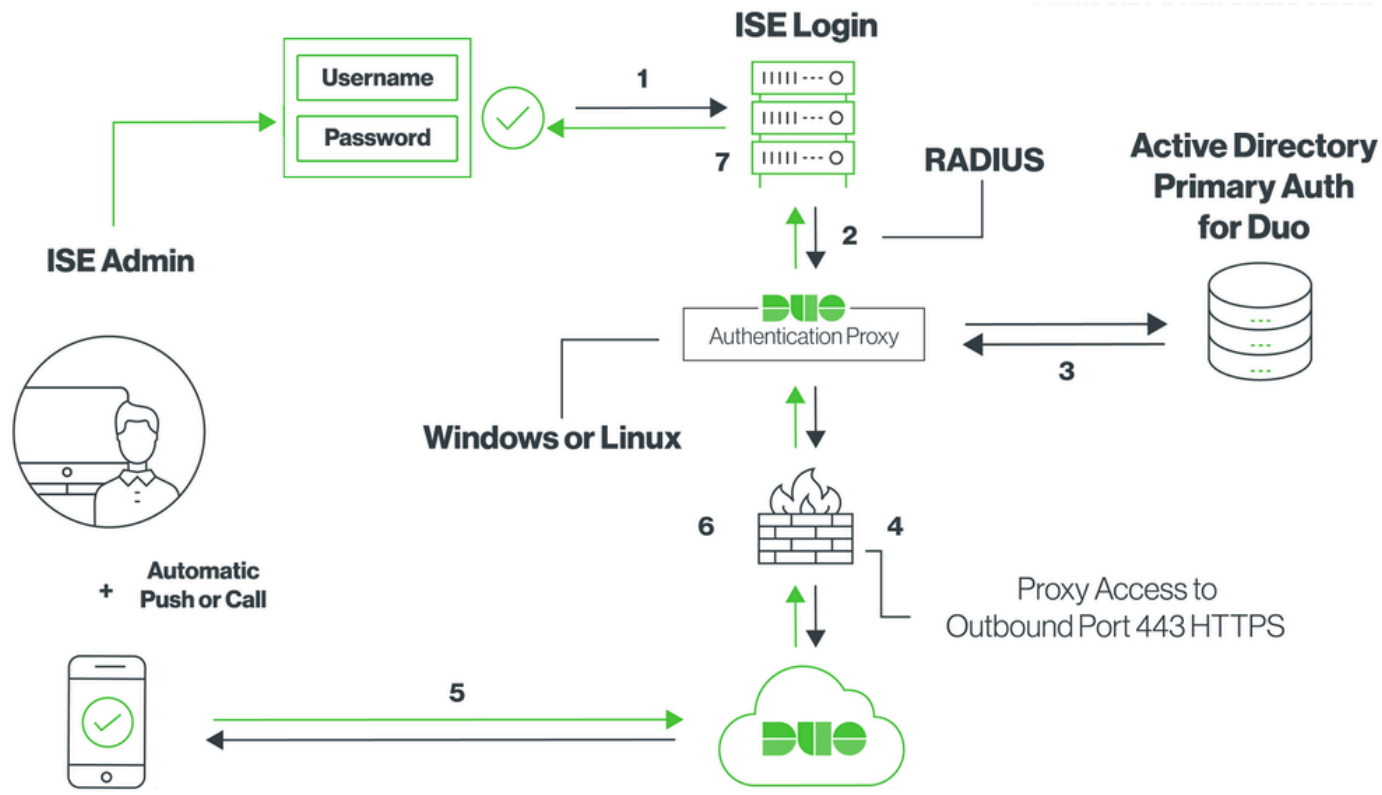
使用的组件

本文档中的信息基于以下软件和硬件版本：

- Duo云服务
- Active Directory (AD)
- 身份服务引擎 (ISE)
- Duo身份验证代理服务器

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



配置

Duo配置

1. 在Windows或Linux计算机上下载并安装Duo Authentication Proxy Server - Duo Authentication Proxy

---

注意：此计算机必须能够访问ISE和双核云（互联网）

2.配置authproxy.cfg文件。在文本编辑器(如“记事本”或“写字板”++打开此文件。

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

3.在Duo Admin面板中创建“Cisco ISE RADIUS”应用。

4.编辑authproxy.cfg文件并添加以下配置：

<#root>

```
        ikey= xxxxxxxxxxxxxxxxxxxxxxxx
        skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
        api_host=api-xxxxxxxx.duosecurity.com
        radius_ip_1=10.127.196.189
```

Sample IP address of the ISE server

```
        radius_secret_1=******
        failmode=secure
        client=ad_client
        port=1812
```

5.使用您的Active Directory详细信息配置ad_client。Duo Auth Proxy使用下一个示例中的信息对主要身份验证的AD进行身份验证：

<#root>

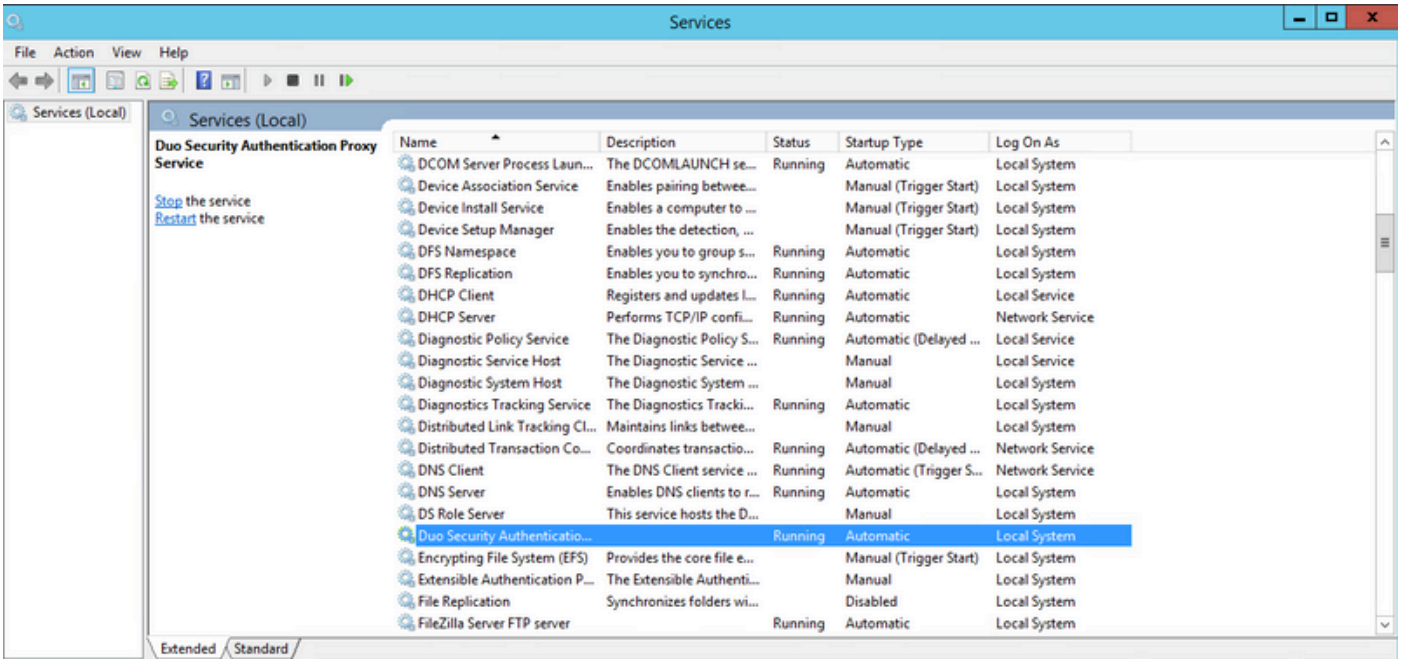
```
        [ad_client]
        host=10.127.196.230
```

Sample IP address of the Active Directory

```
        service_account_username=< AD-username >
        service_account_password=< AD-password >
        search_dn=CN=Users,DC=gce,DC=iselab,DC=local
```

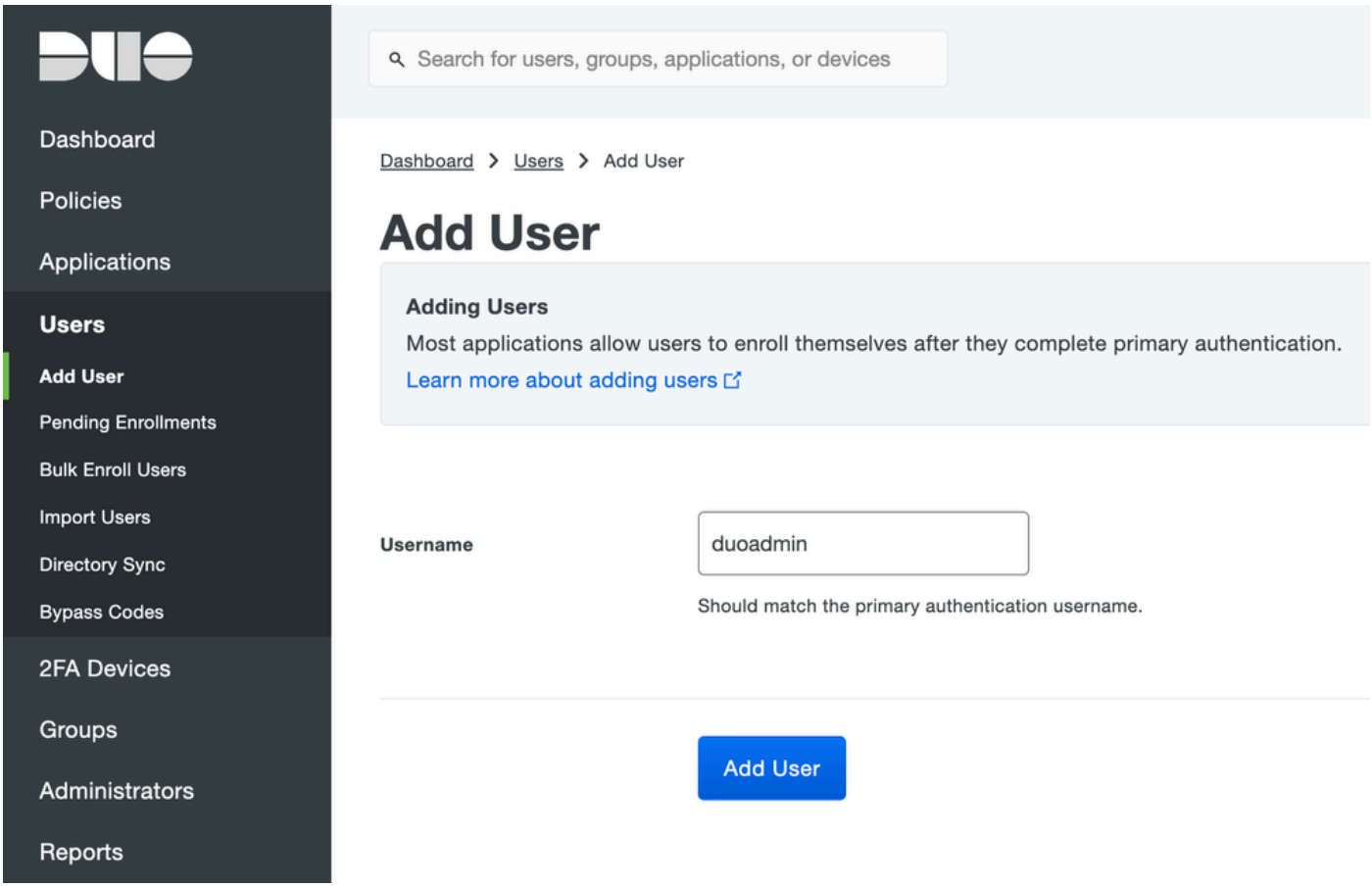
注意：如果您的网络需要HTTP代理连接才能访问Internet，请在authproxy.cfg中添加http_proxy详细信息。

6.重新启动Duo Security Authentication Proxy服务。保存文件并在Windows计算机上重新启动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：

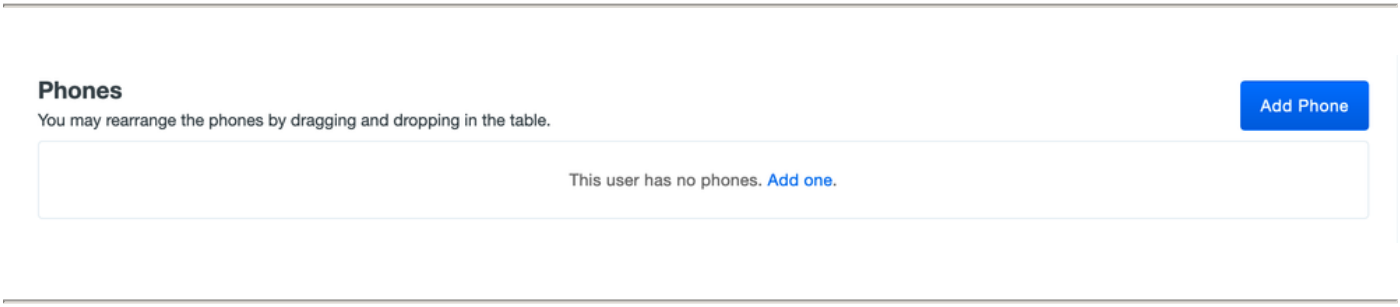


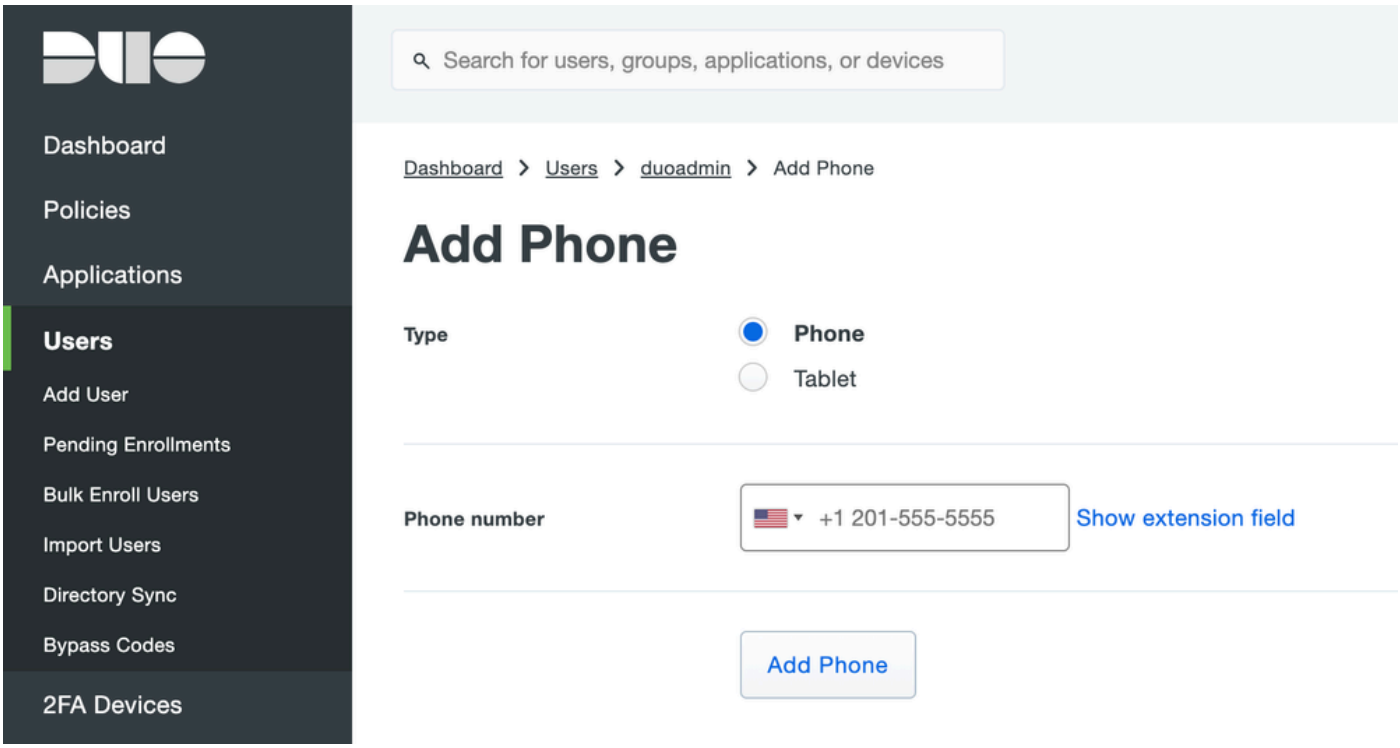
7.创建用户名并在终端设备上激活Duo Mobile。

8.在Duo Admin Panel上添加用户。导航到Users > Add Users，如图所示：



9.确保最终用户在手机上安装了双核应用程序。

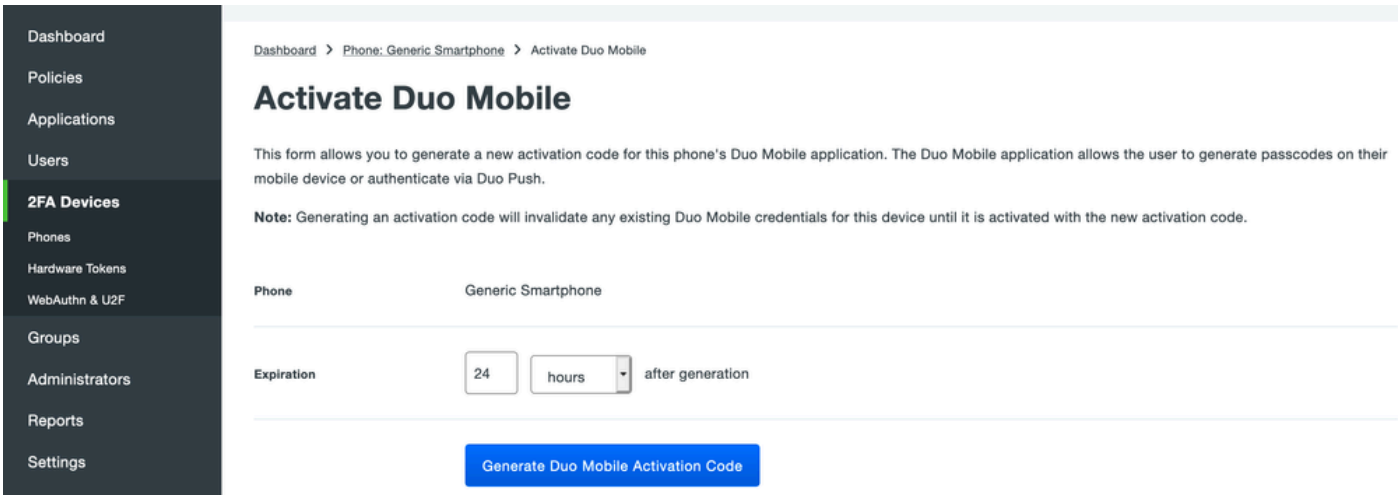




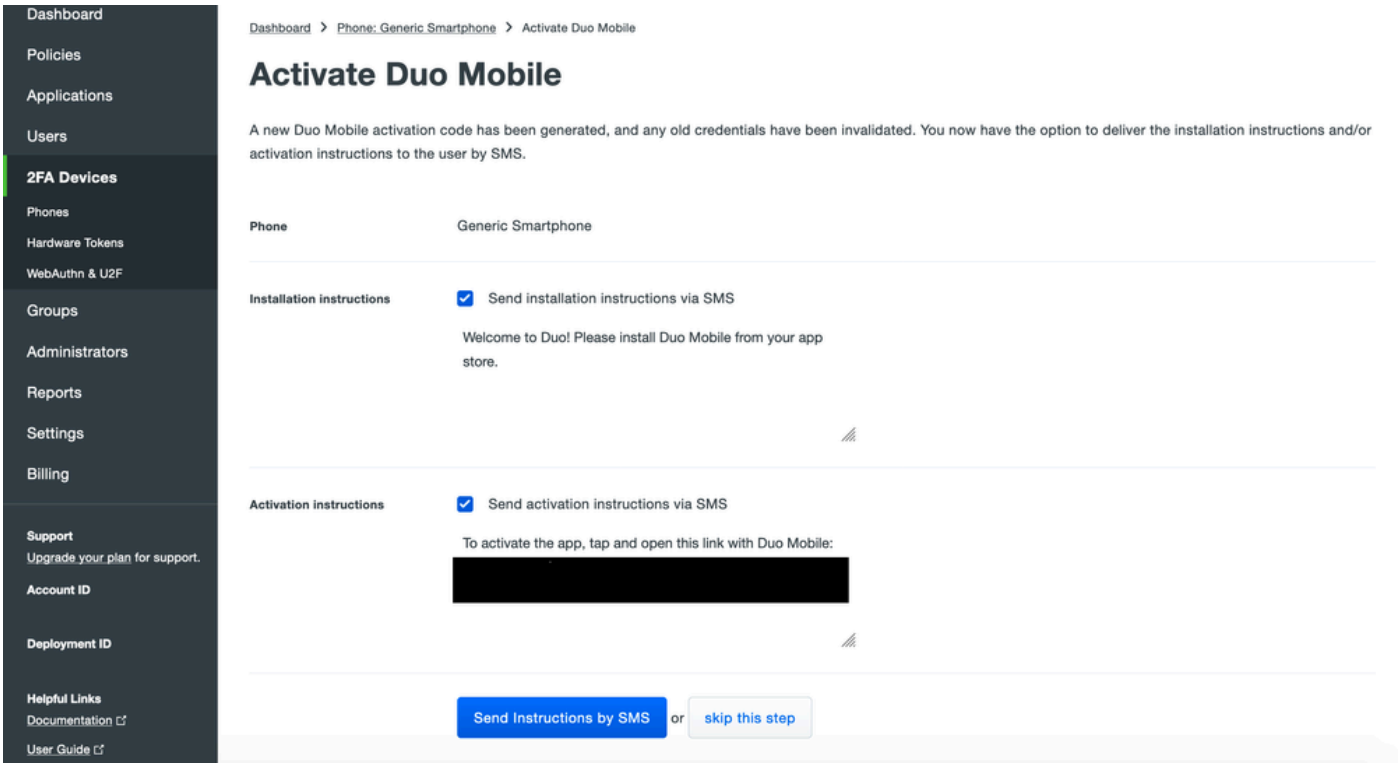
10.选择Activate Duo Mobile，如图所示：



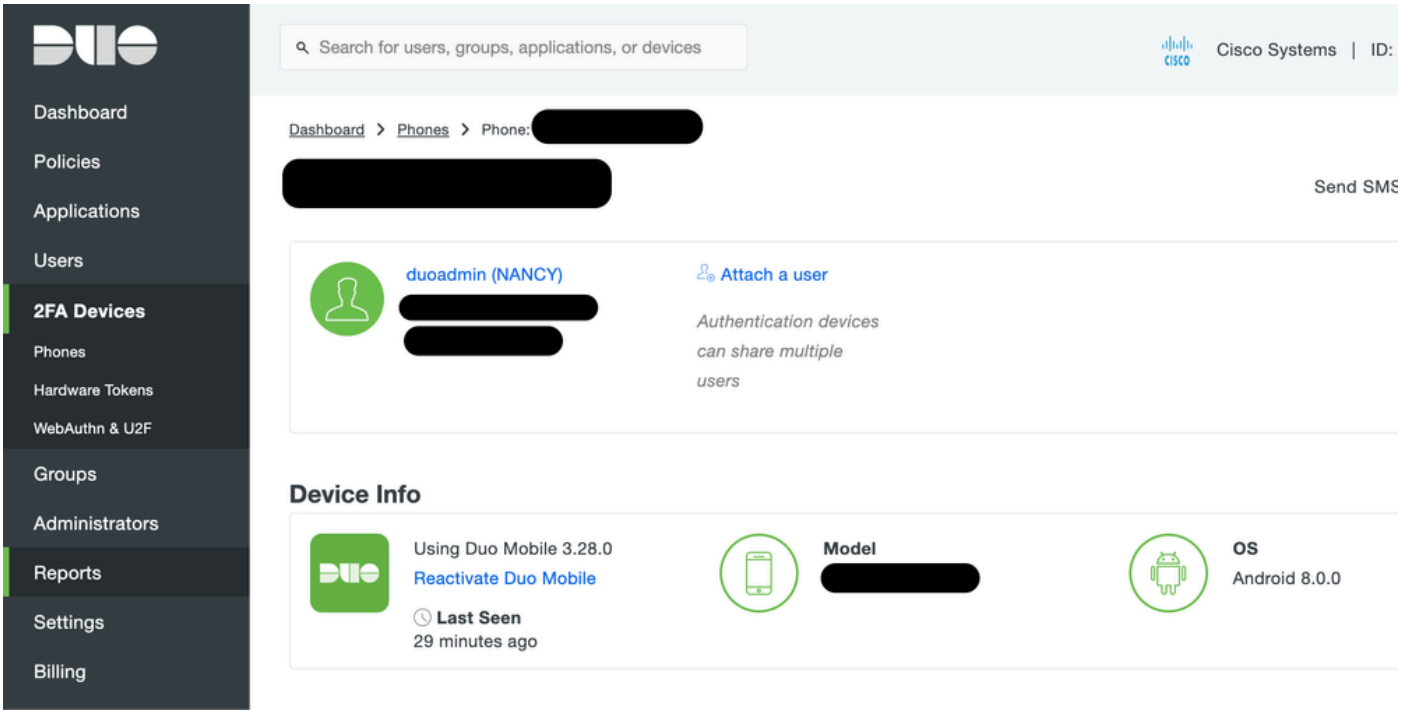
11.选择Generate Duo Mobile Activation Code（生成Duo Mobile Activation Code），如图所示：



12.选择通过SMS发送指令，如图所示：



13.单击SMS中的链接，Duo应用将链接到Device Info（设备信息）部分中的用户帐户：

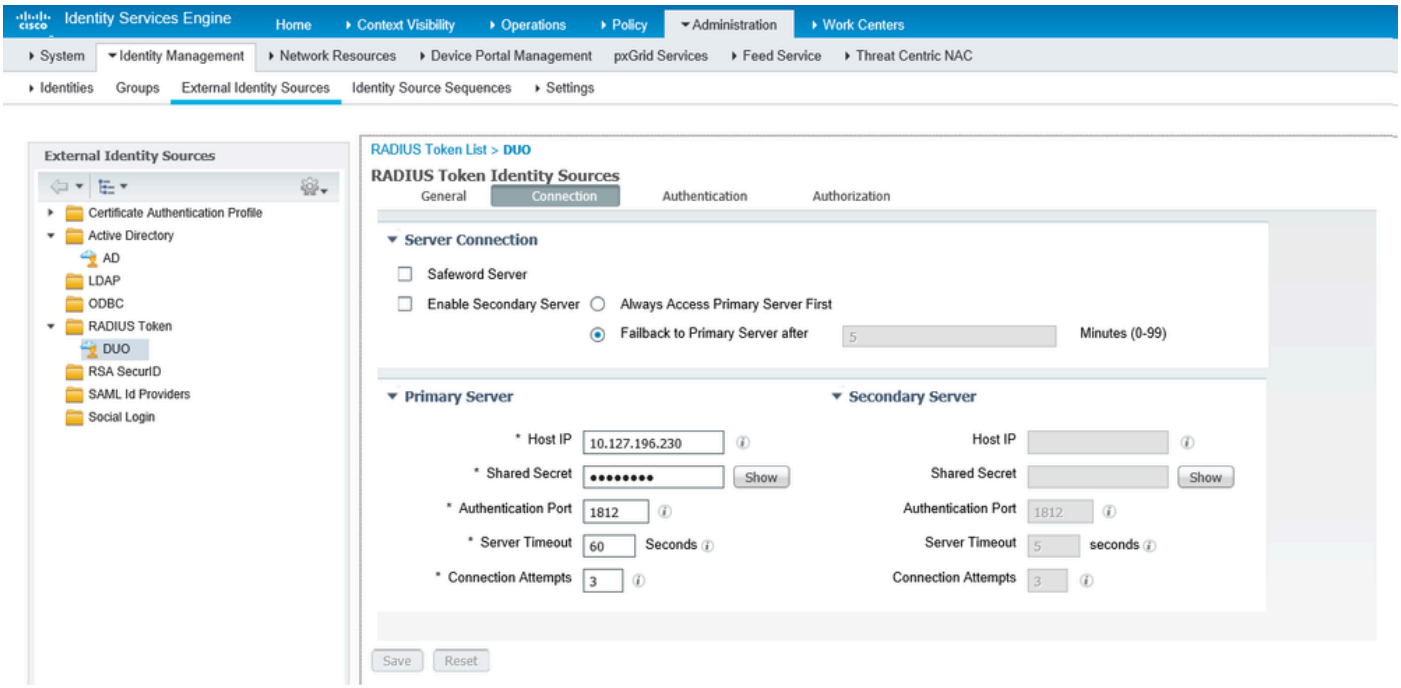


ISE 配置

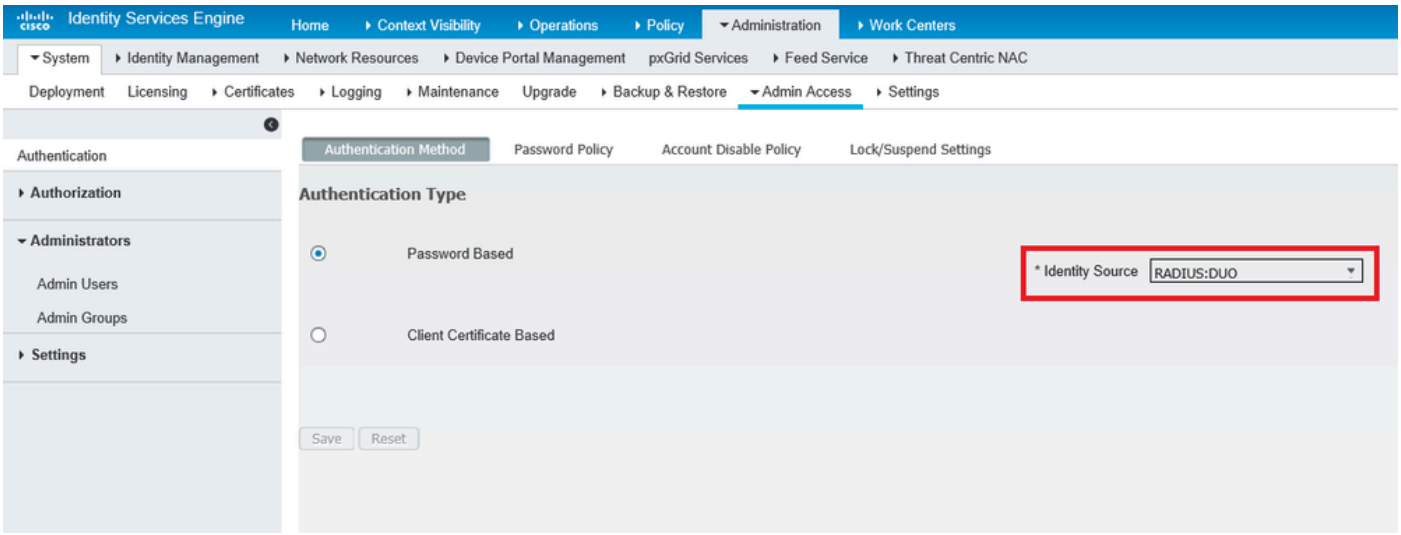
将ISE与双身份验证代理集成

1.导航到管理>身份管理>外部身份源> RADIUS令牌。单击Add以添加新的RADIUS令牌服务器。在“常规”选项卡中定义服务器名称，在“连接”选项卡中定义IP地址和共享密钥，如图所示：

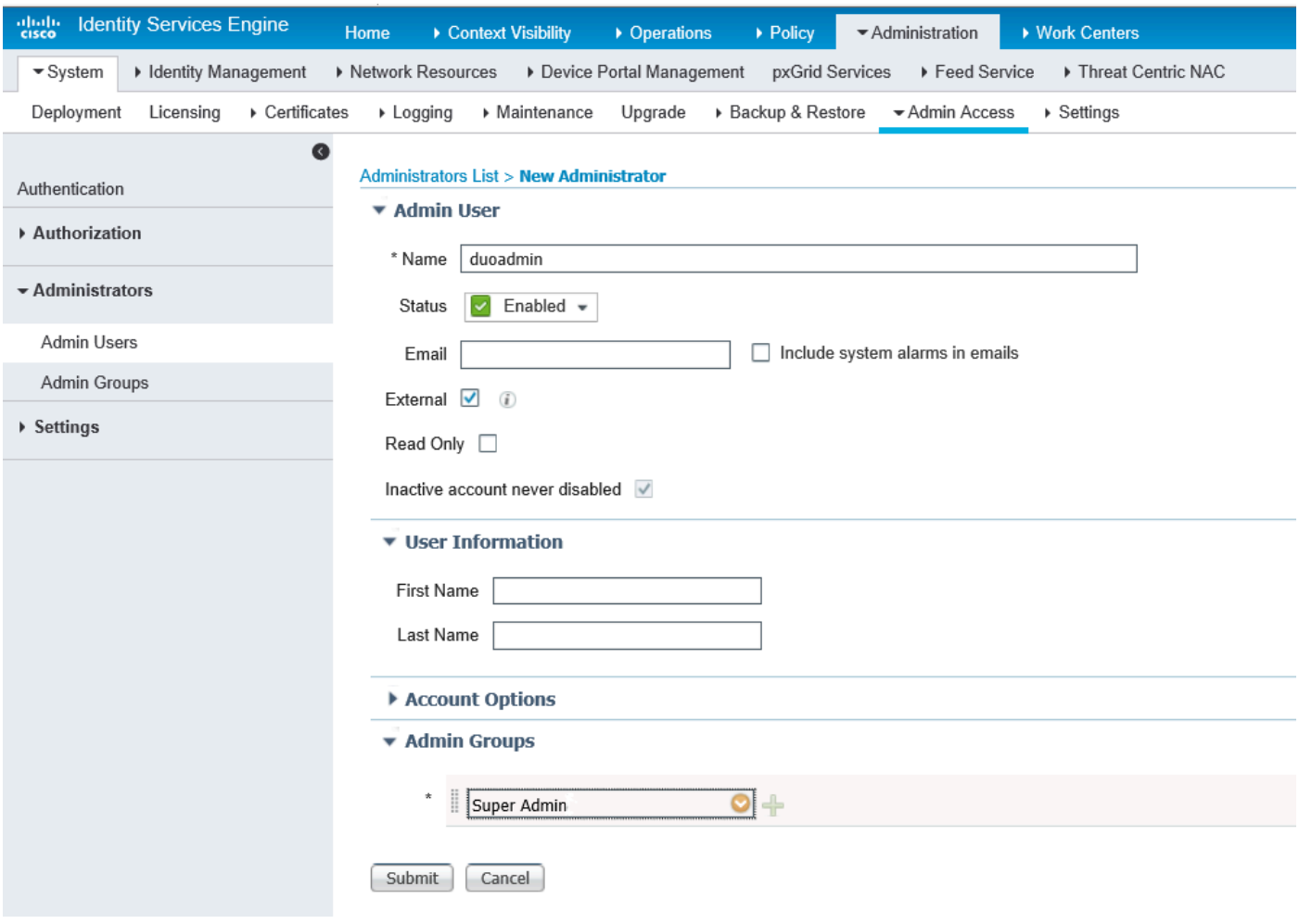
注意：将Server Timeout设置为60秒，以便用户有足够的时间对推送执行操作。



2.导航到Administration > System > Admin Access > Authentication > Authentication Method 并选择以前配置的RADIUS令牌服务器作为身份源：



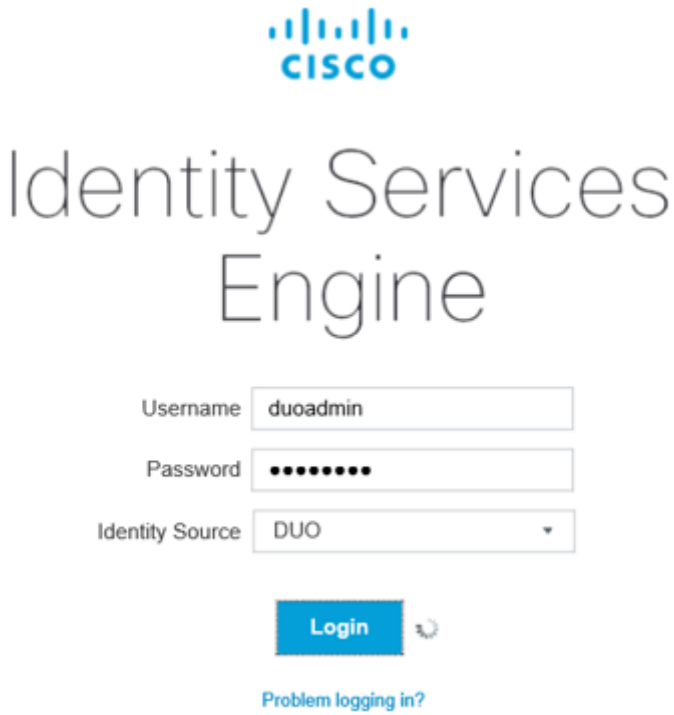
3.导航到管理>系统>管理员访问权限>管理员>管理员用户,创建管理员用户作为外部用户，并提供超级管理员权限：



验证

使用本部分可确定配置能否正常运行。

1.打开ISE GUI，选择RADIUS令牌服务器作为身份源并以管理员用户登录。



故障排除

本部分提供的信息可用于对配置进行故障排除。

要排除与使用云或Active Directory的Duo Proxy连接相关的问题，请在authproxy.cfg的主要部分下添加“debug=true”，以启用Duo Auth代理上的调试。

- 日志位于：C:\Program Files(x86)\Duo Security Authentication Proxy\log
- 在文本编辑器（如Notepad++或WordPad）中打开文件authproxy.log。

Duo Auth Proxy的日志片段从ISE接收请求并将其发送到Duo Cloud:

<#root>

```
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Sending request from 10.127.196.189 to radius_server_
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] Received new request id 2 from ('10.127.196.189', 620
2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)] (('10.127.196.189', 62001), duoadmin, 2):

login attempt for username u'duoadmin'

2019-08-19T04:59:27-0700 [DuoForwardServer (UDP)]

Sending AD authentication request for 'duoadmin' to '10.127.196.230'

2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Starting factory
```

Duo Auth Proxy unable to Duo Cloud的日志片段：

<#root>

```
2019-08-19T04:59:27-0700 [duoauthproxy.modules.ad_client._ADAuthClientFactory#info] Stopping factory
2019-08-19T04:59:37-0700 [-] Duo preauth call failed
Traceback (most recent call last):
File "twisted\internet\defer.pyc", line 654, in _runCallbacks
File "twisted\internet\defer.pyc", line 1475, in gotResult
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator

File "duoauthproxy\lib\radius\duo_server.pyc", line 111, in preauth
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator
File "duoauthproxy\lib\duo_async.pyc", line 246, in preauth
File "twisted\internet\defer.pyc", line 1416, in _inlineCallbacks
File "twisted\python\failure.pyc", line 512, in throwExceptionIntoGenerator
File "duoauthproxy\lib\duo_async.pyc", line 202, in call
File "twisted\internet\defer.pyc", line 654, in _runCallbacks
File "duoauthproxy\lib\duo_async.pyc", line 186, in err_func

duoauthproxy.lib.duo_async.DuoAPIFailOpenError: API Request Failed: DNSLookupError('api-xxxxxxxx.duosecu


2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Failmode Secure - Denied Duo log
2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3):

Returning response code 3: AccessReject

2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Sending response
```

相关信息

- 使用DUO的RA VPN身份验证
- 技术支持和文档 - Cisco Systems

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）。