

为ISE管理访问配置双核双因素身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[配置](#)

[双核配置](#)

[ISE配置](#)

[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。在本示例中，ISE管理员根据RADIUS令牌服务器进行身份验证，并且双核身份验证代理服务器以推送通知形式向管理员的移动设备发送附加身份验证。

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

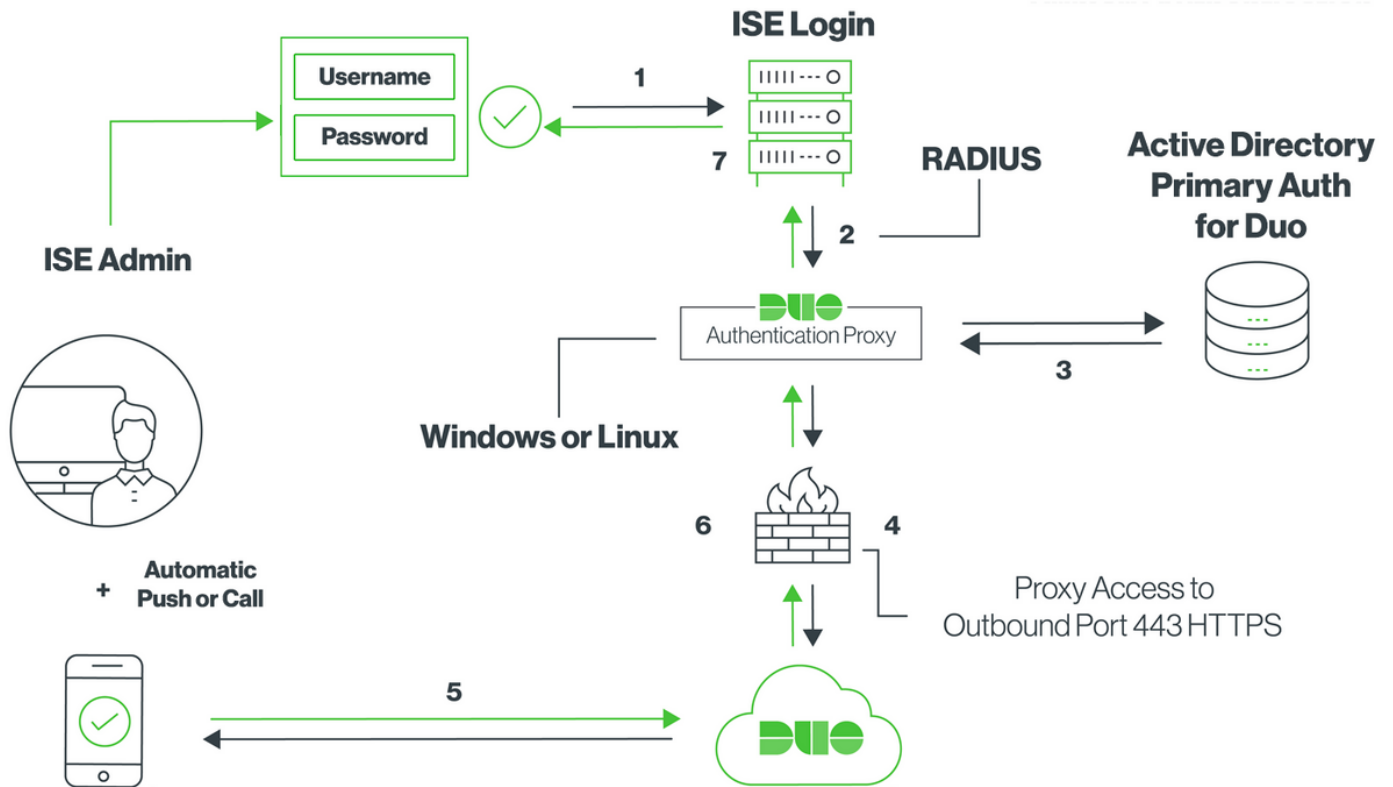
使用的组件

本文档中的信息基于以下软件和硬件版本：

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

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图



配置

双核配置

步骤1.在Windows或Linux计算机上下载并安装Duo身份验证代理服务器：
<https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy>

注意：此计算机必须能够访问ISE和双核云（互联网）

步骤2.配置authproxy.cfg文件。

在文本编辑器（如Notepad++或WordPad）中打开此文件。

注意：默认位置位于C:\Program Files (x86)\Duo安全身份验证Proxy\conf\authproxy.cfg。

步骤3.在Duo Admin Panel（双核管理面板）中创建“Cisco ISE RADIUS”应用：
<https://duo.com/docs/ciscoise-radius#first-steps>

步骤4.编辑authproxy.cfg文件并添加此配置。

```

ikey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxx.duosecurity.com
radius_ip_1=10.127.196.189
radius_secret_1=*****
failmode=secure
client=ad_client

```

Sample IP address of the ISE server

port=1812

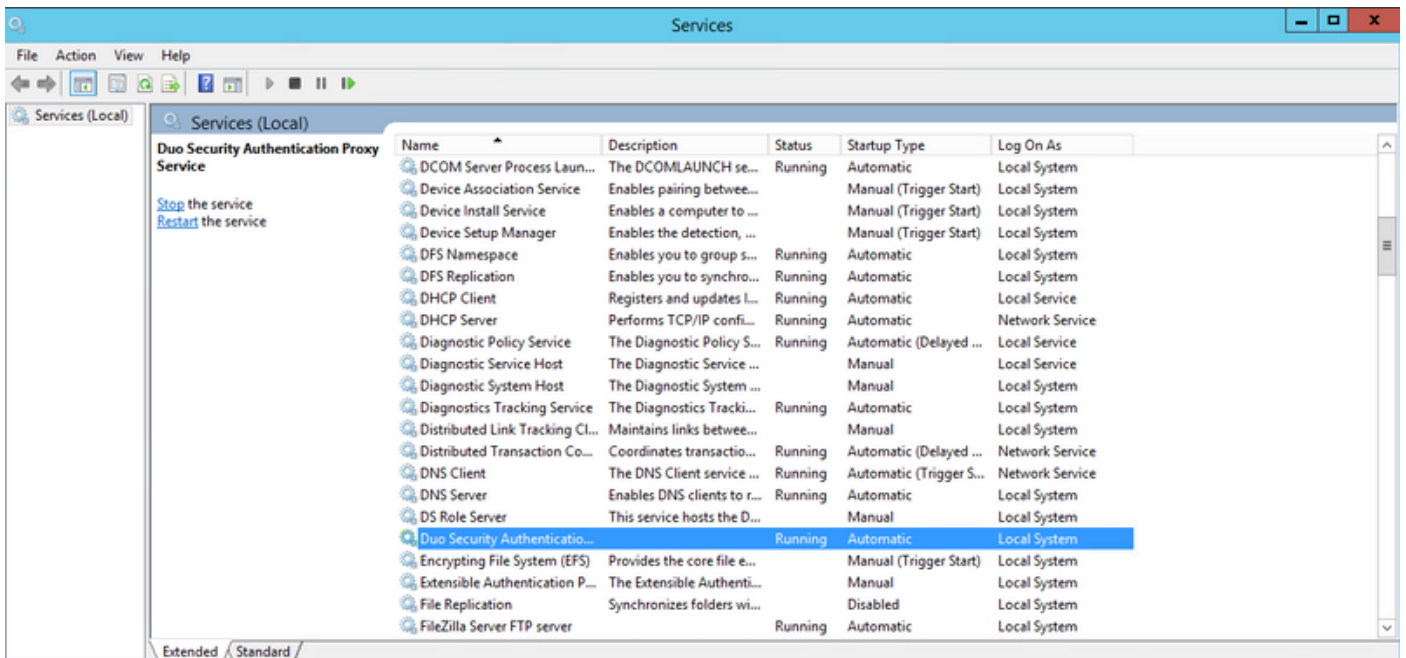
步骤5.使用Active Directory详细信息配置ad_client。Duo Auth代理使用以下信息根据AD进行身份验证以进行主身份验证。

```
[ad_client]
host=10.127.196.230
service_account_username=< AD-username >
service_account_password=< AD-password >
search_dn=CN=Users,DC=gce,DC=iselab,DC=local
```

Sample IP address of the Active Directory

注意：如果网络需要HTTP代理连接才能访问互联网，请在authproxy.cfg中添加http_proxy详细信息。

步骤6.重新启动Duo安全身份验证代理服务。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安全身份验证代理服务，然后单击重新启动，如图所示：



步骤7.创建用户名并激活终端设备上的Duo Mobile:<https://duo.com/docs/administration-users#creating-users-manually>

在Duo Admin Panel (双核管理面板) 上添加用户。导航至**用户>添加用户**，如图所示：

The screenshot shows the Duo Admin interface. On the left is a dark sidebar with the Duo logo and navigation menu items: Dashboard, Policies, Applications, Users (highlighted), Add User (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, 2FA Devices, Groups, Administrators, and Reports. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > Add User. The main heading is "Add User". A section titled "Adding Users" contains the text "Most applications allow users to enroll themselves after they complete primary authentication." and a link "Learn more about adding users". Below this is a form with a "Username" label and a text input field containing "duoadmin". A note below the field says "Should match the primary authentication username." At the bottom of the form is a blue "Add User" button.

确保最终用户在电话上安装了Duo应用。

The screenshot shows the "Phones" section of the Duo Admin interface. It has a heading "Phones" and a sub-heading "You may rearrange the phones by dragging and dropping in the table." On the right is a blue "Add Phone" button. Below the text is a large empty box with the message "This user has no phones. [Add one.](#)"

The screenshot shows the Duo Admin interface for adding a phone. The sidebar is the same as in the previous screenshot, but "Users" is highlighted and "Add User" is selected. The main content area has a search bar with "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > duoadmin > Add Phone. The main heading is "Add Phone". Under "Type", there are two radio buttons: "Phone" (selected) and "Tablet". Below this is a form with a "Phone number" label and a text input field containing "+1 201-555-5555" with a US flag icon on the left. To the right of the field is a link "Show extension field". At the bottom of the form is a blue "Add Phone" button.

选择激活Duo Mobile，如图所示：

Device Info



Not using Duo Mobile
[Activate Duo Mobile](#)

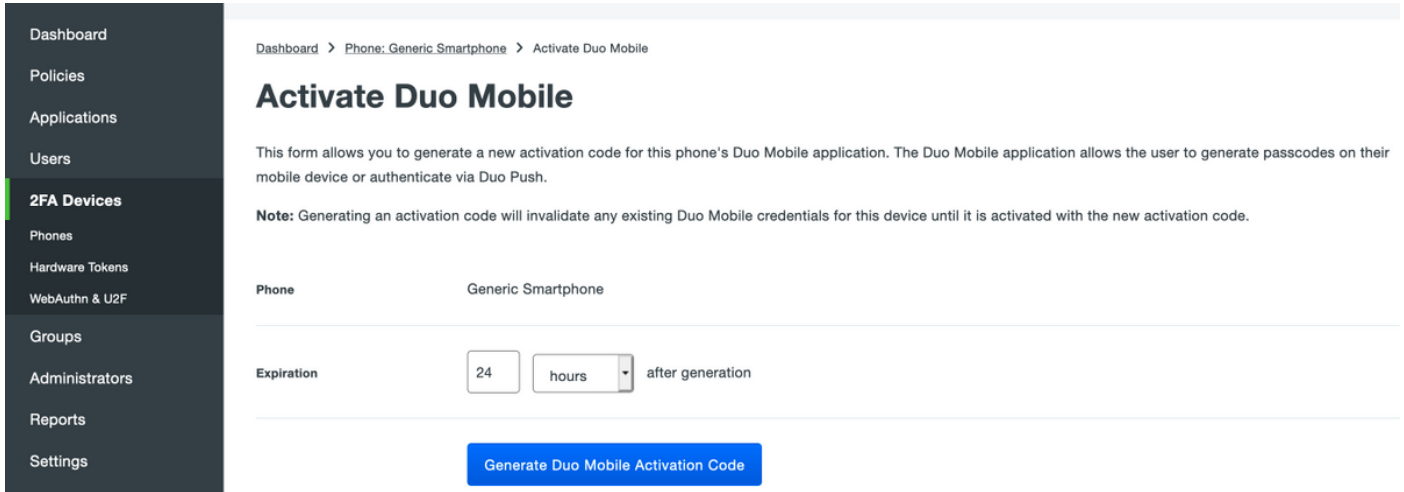


Model
Unknown



OS
Generic Smartphone

选择生成Duo Mobile Activation Code，如图所示：



Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

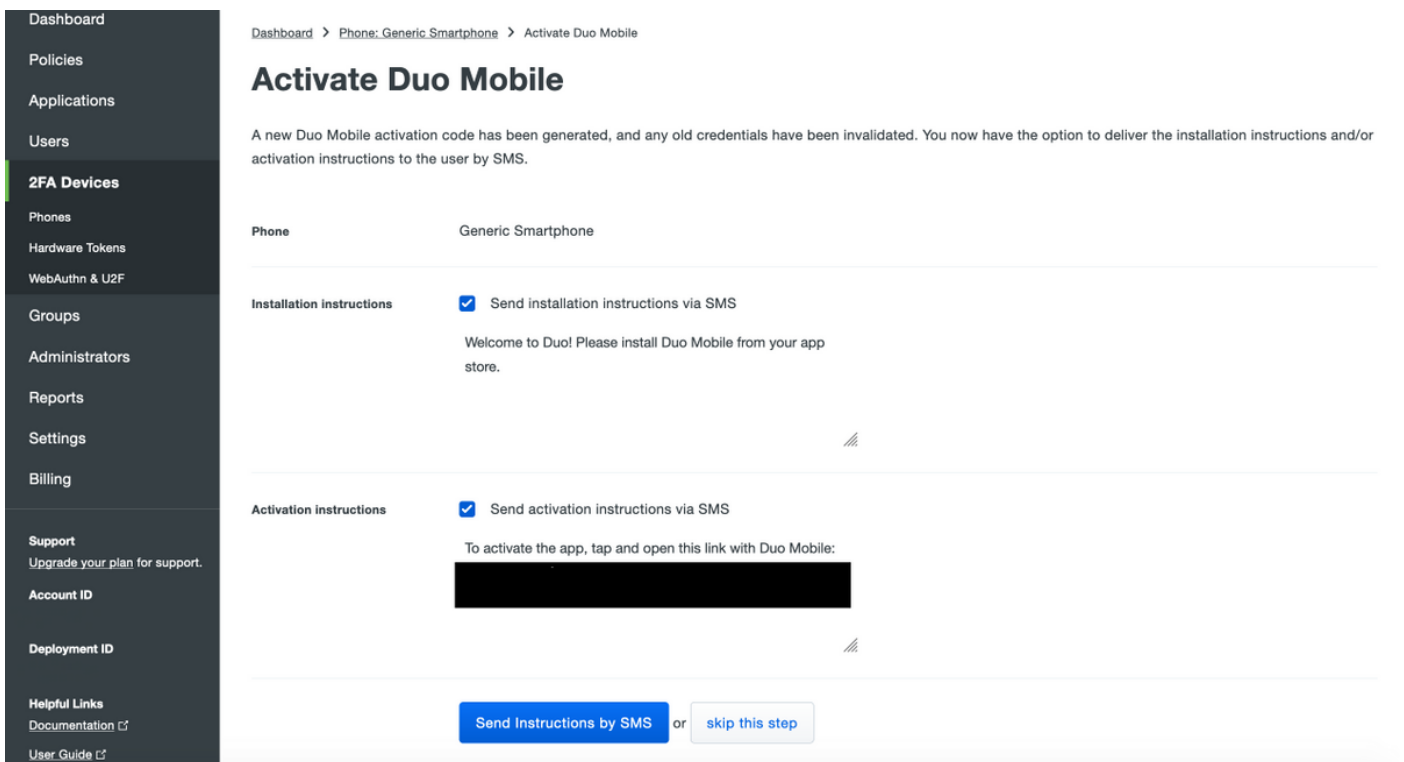
Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: Generic Smartphone

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

选择通过SMS发送指令，如图所示：



Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. You now have the option to deliver the installation instructions and/or activation instructions to the user by SMS.

Phone: Generic Smartphone

Installation instructions: Send installation instructions via SMS

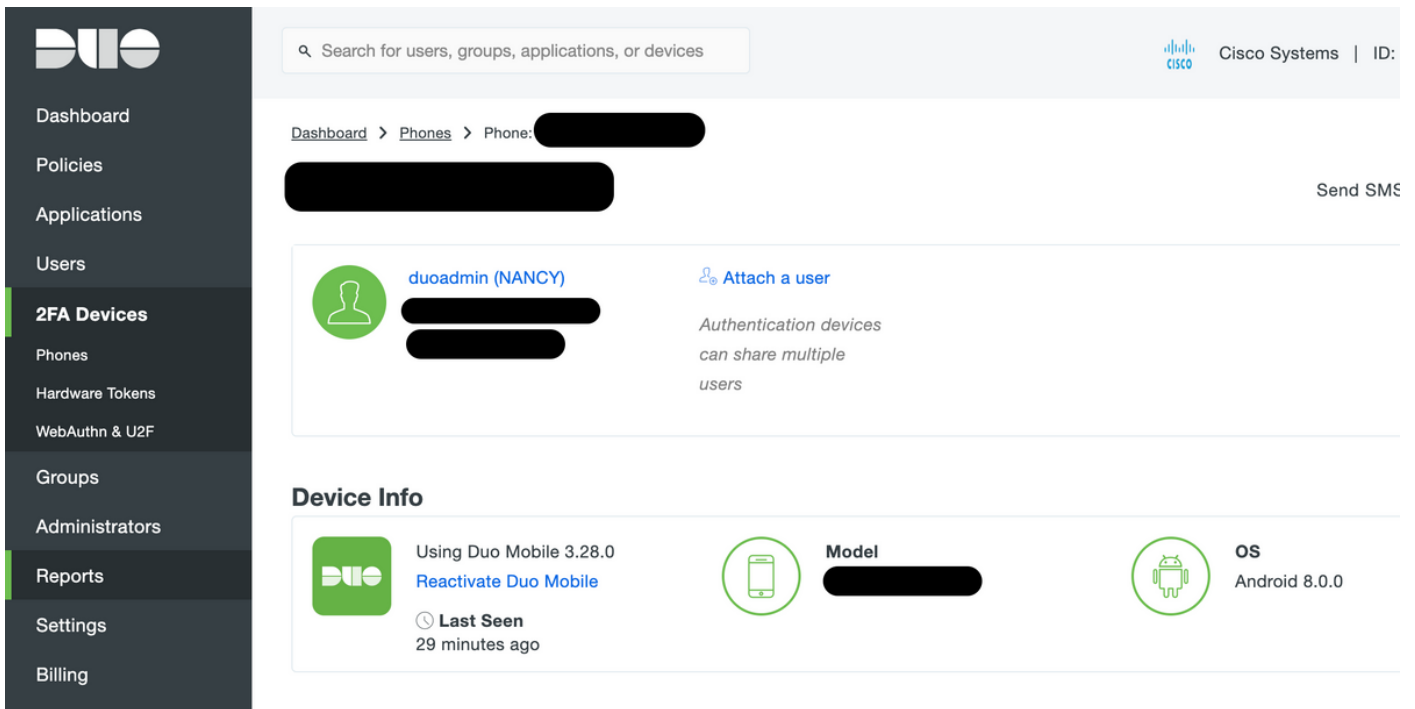
Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions: Send activation instructions via SMS

To activate the app, tap and open this link with Duo Mobile:

[Send Instructions by SMS](#) or [skip this step](#)

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

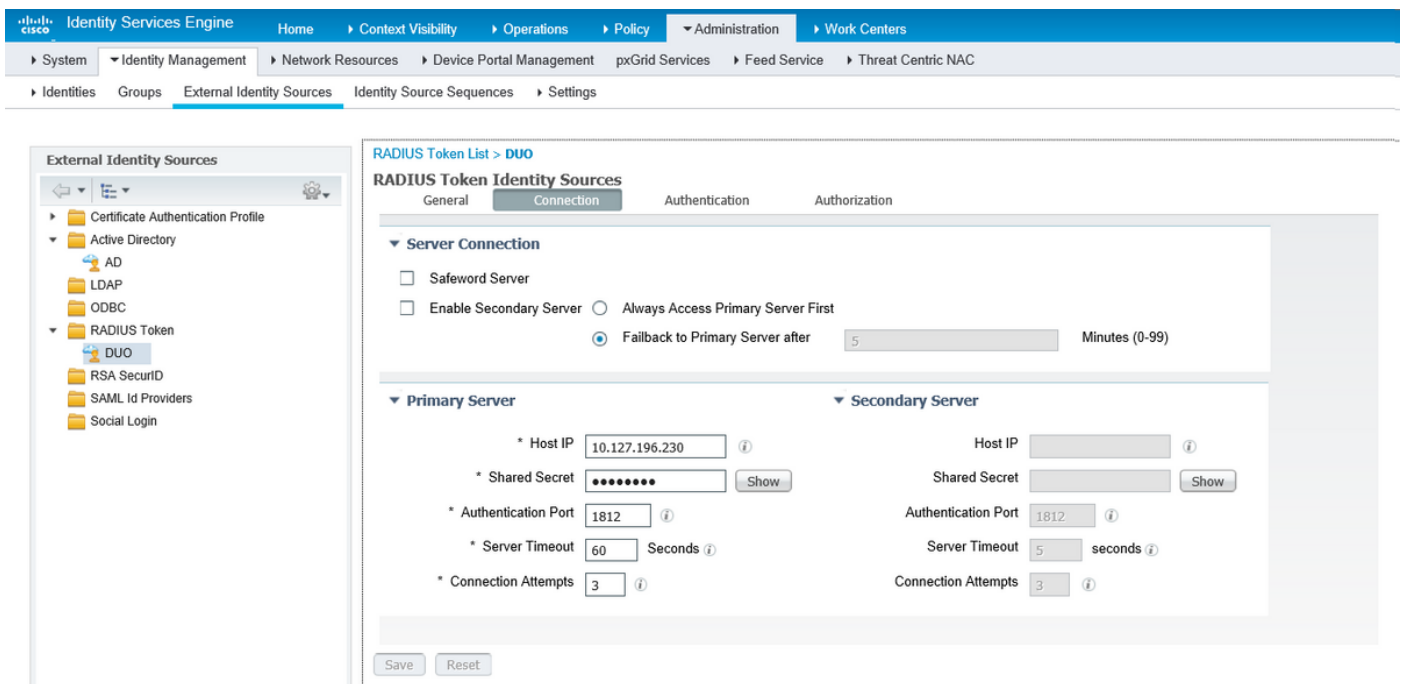


ISE配置

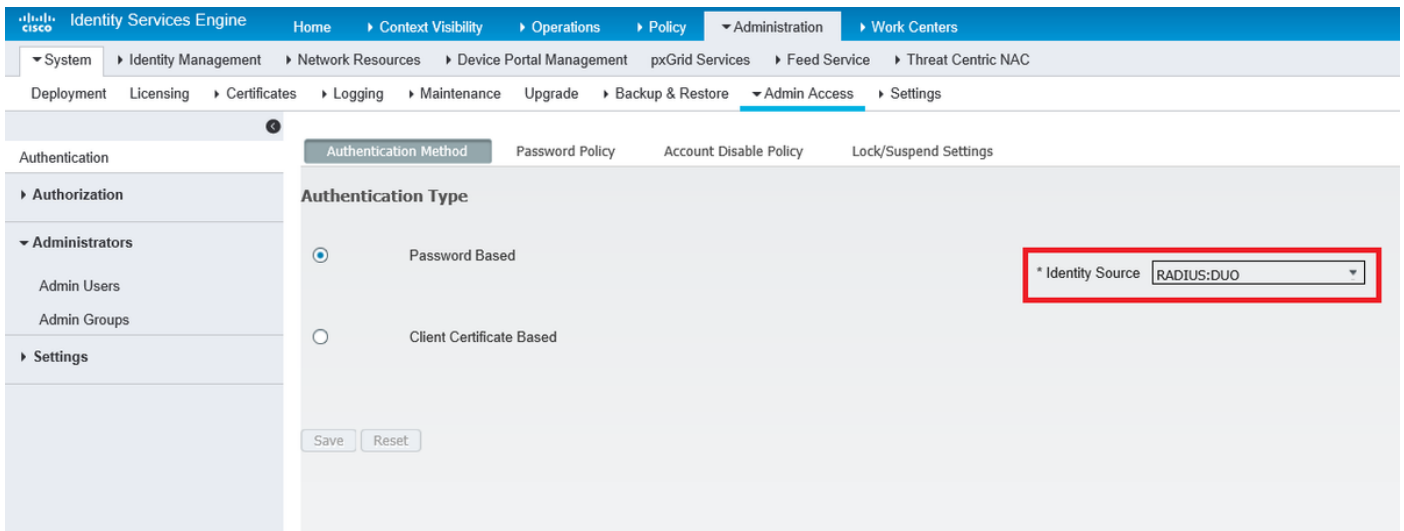
步骤1.将ISE与双核身份验证代理集成。

导航至**管理>身份管理>外部身份源>RADIUS令牌**，单击**添加**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：

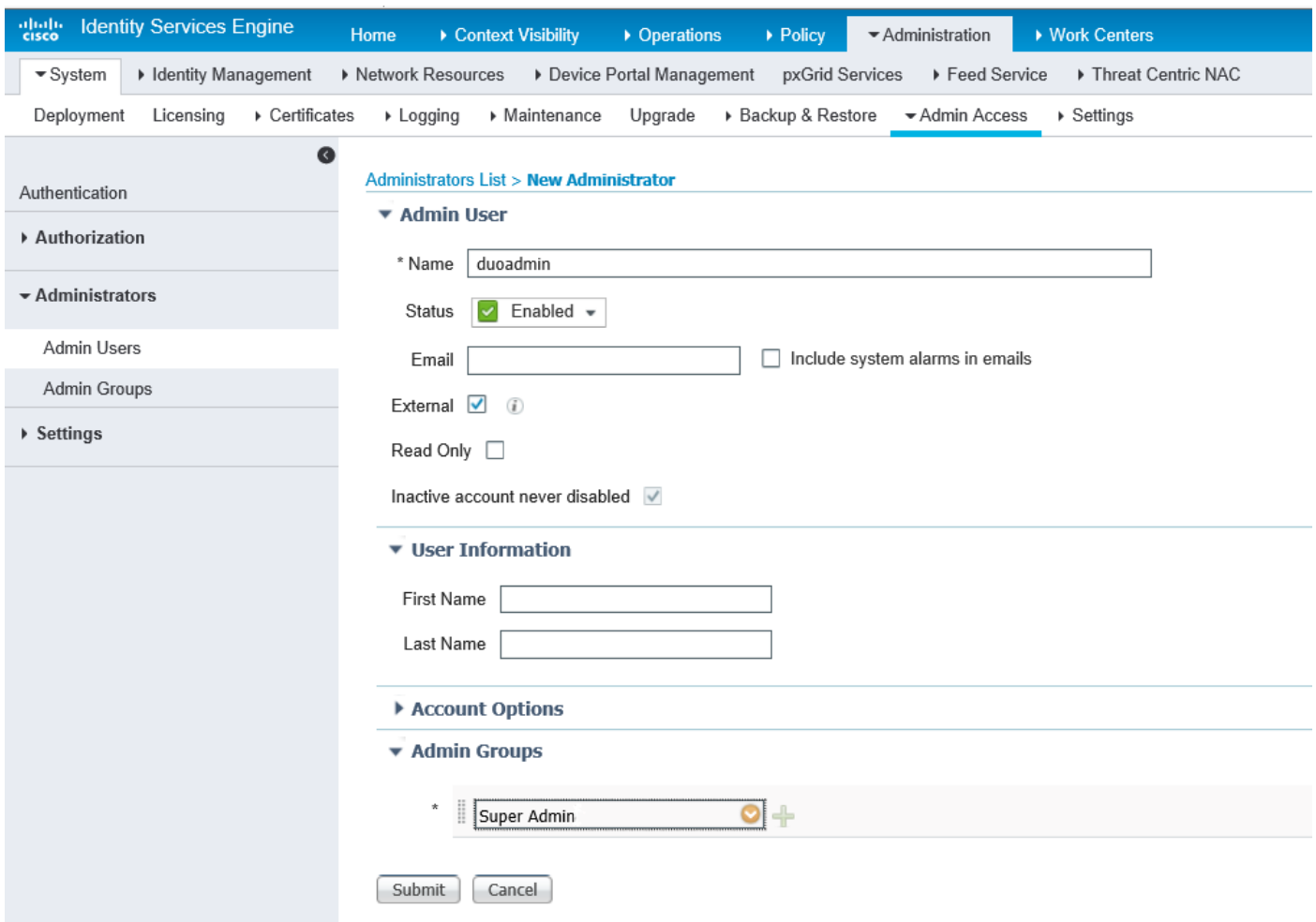
60



步骤2.导航至**Administration > System > Admin Access > Authentication > Authentication Method**并选择之前配置的RADIUS令牌服务器作为身份源，如图所示：



步骤3. 导航至Administration > System > Admin Access > Administrators > Admin Users，并创建管理员用户作为External，并提供超级管理员权限，如图所示：



验证

使用本部分可确认配置能否正常运行。

打开ISE GUI，选择RADIUS令牌服务器作为身份源并使用管理员用户登录。



Identity Services Engine

Username

Password

Identity Source

[Problem logging in?](#)

故障排除

本部分提供了可用于对配置进行故障排除的信息。

要排除与Duo代理与云或Active Directory连接相关的问题，请在authproxy.cfg的主部分下添加“debug=true”，以启用Duo Auth代理上的调试。

日志位于以下位置：

C:\Program Files (x86)\Duo安全身份验证代理\日志

在文本编辑器(如Notepad+或WordPad)中打开文件authproxy.log。

记录从ISE接收请求的双核身份验证代理的片段并将其发送到双核云。

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


双核身份验证代理的日志片段无法到达双核云。

```
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 getResult
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-
xxxxxxxxx.duosecurity.com',)

2019-08-19T04:59:37-0700 [-] (('10.127.196.189', 62001), duoadmin, 3): Failmode Secure - Denied
Duo login on preauth failure
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](#)