為ISE管理訪問配置雙因素身份驗證

目錄

簡介

本文檔介紹為身份服務引擎(ISE)管理訪問配置外部雙因素身份驗證所需的步驟。在本示例中，ISE管理員根據RADIUS令牌伺服器進行身份驗證，Duo身份驗證代理伺服器向管理員的流動裝置傳送推送通知形式的附加身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- RADIUS通訊協定
- 配置ISE RADIUS令牌伺服器和身份

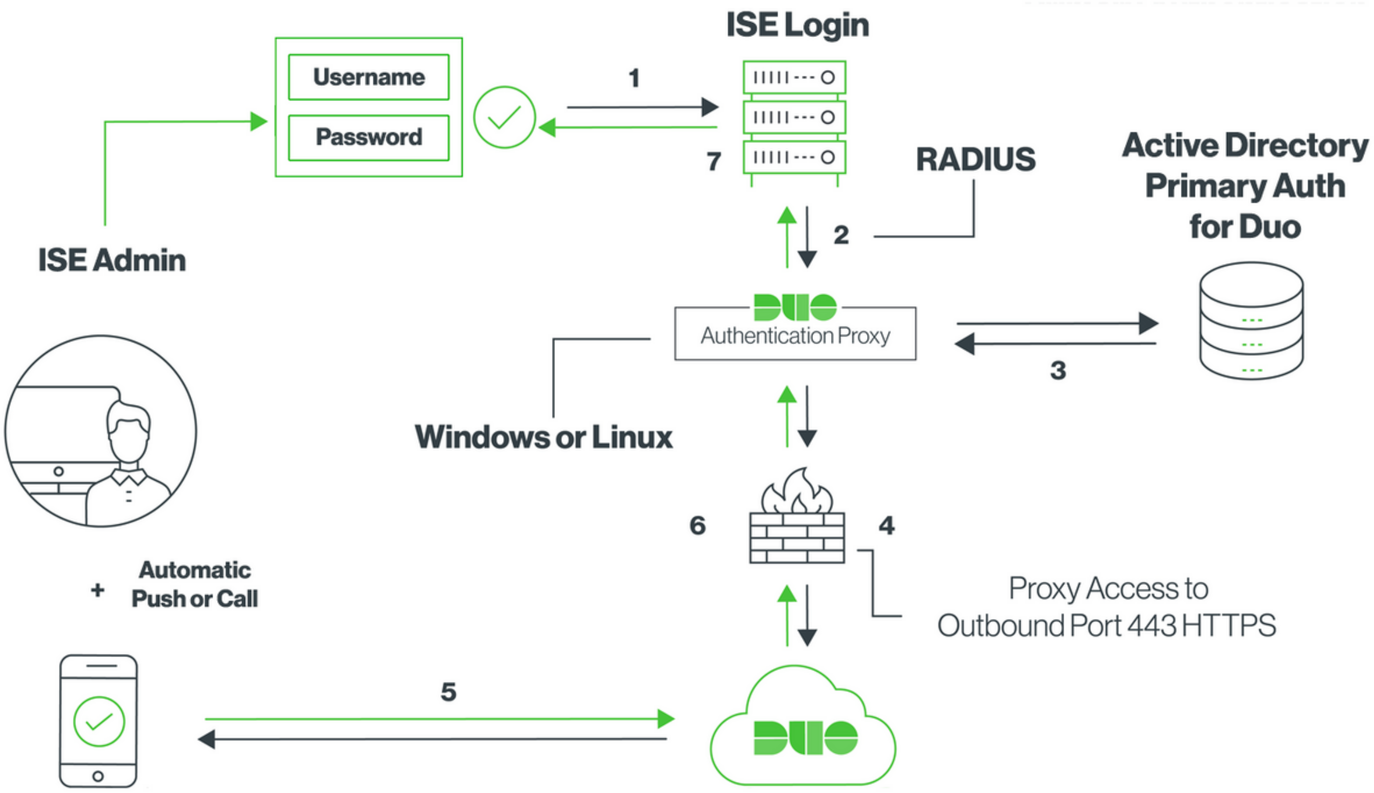
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 身分識別服務引擎 (ISE)
- Active Directory(AD)
- Duo驗證代理伺服器
- Duo Cloud Service

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表



組態

Duo配置

步驟1. 在Windows或Linux電腦上下載並安裝Duo Authentication Proxy伺服器：https://duo.com/docs/ciscoise-radius#install-the-duo-authentication-proxy

> 附註：此電腦必須能夠訪問ISE和Duo Cloud（網際網路）

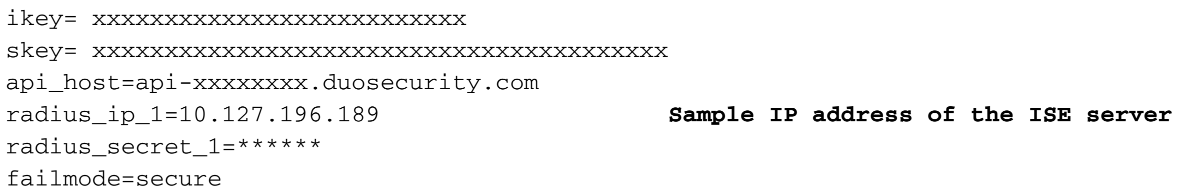
步驟2.配置authproxy.cfg檔案。

在文本編輯器（如記事本或寫字板）++開啟此檔案。

> 注意：預設位置位於**C:\Program Files(x86)\Duo Security Authentication Proxy\conf\authproxy.cfg**

步驟3. 在Duo Admin Panel中建立「Cisco ISE RADIUS」應用：https://duo.com/docs/ciscoise-radius#first-steps

步驟4.編輯**authproxy.cfg**檔案並新增此配置。



```
ikey= xxxxxxxxxxxxxxxxxxxxxxxxxxx
skey= xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
api_host=api-xxxxxxxx.duosecurity.com
radius_ip_1=10.127.196.189
radius_secret_1=******
failmode=secure
```

Sample IP address of the ISE server

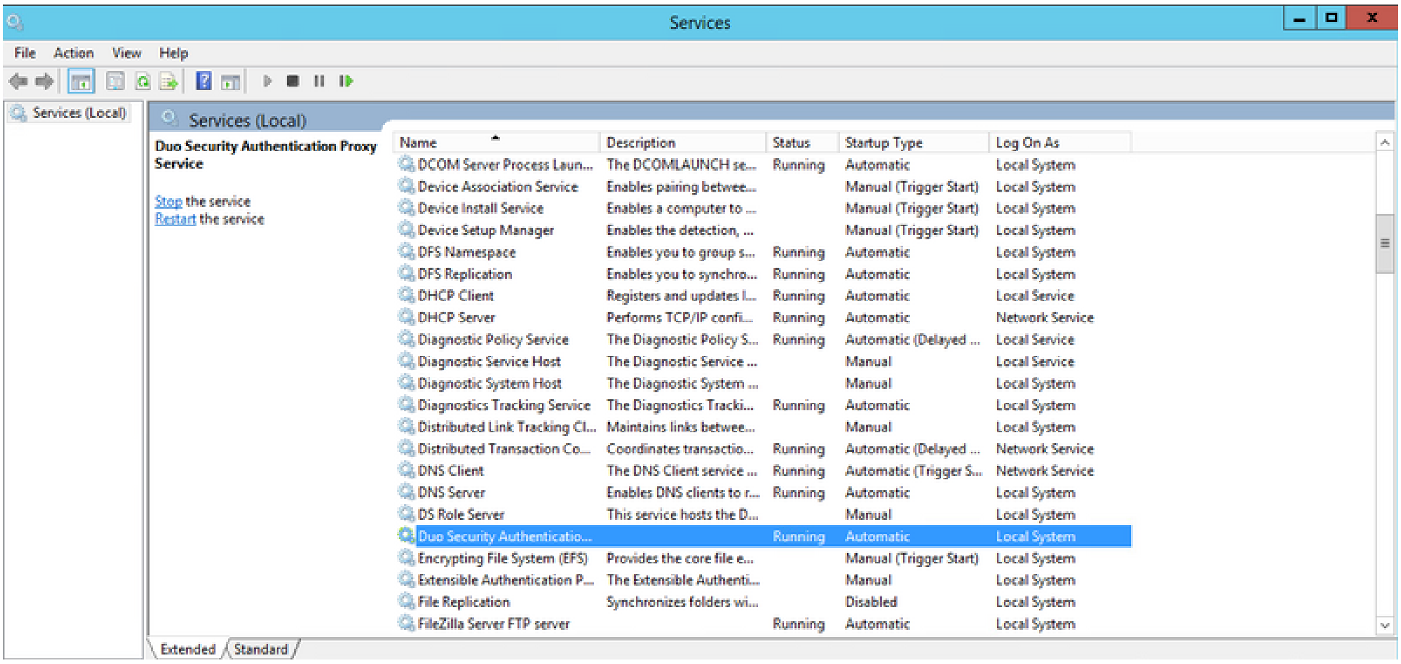
```
client=ad_client
port=1812
```

步驟5.使用Active Directory詳細資訊配置ad_client。Duo Auth Proxy使用以下資訊根據AD對主要身份驗證進行身份驗證。

```
[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
```

附註：如果您的網路需要HTTP代理連線才能訪問Internet，請在authproxy.cfg中新增http_proxy詳細資訊。

步驟6.重新啟動Duo Security Authentication Proxy服務。在Windows電腦上儲存檔案並重新啟動**Duo服務**。開啟Windows服務控制檯(services.msc)，在服務清單中找到**Duo Security Authentication Proxy Service**，然後按一下**重新啟動**，如下圖所示：



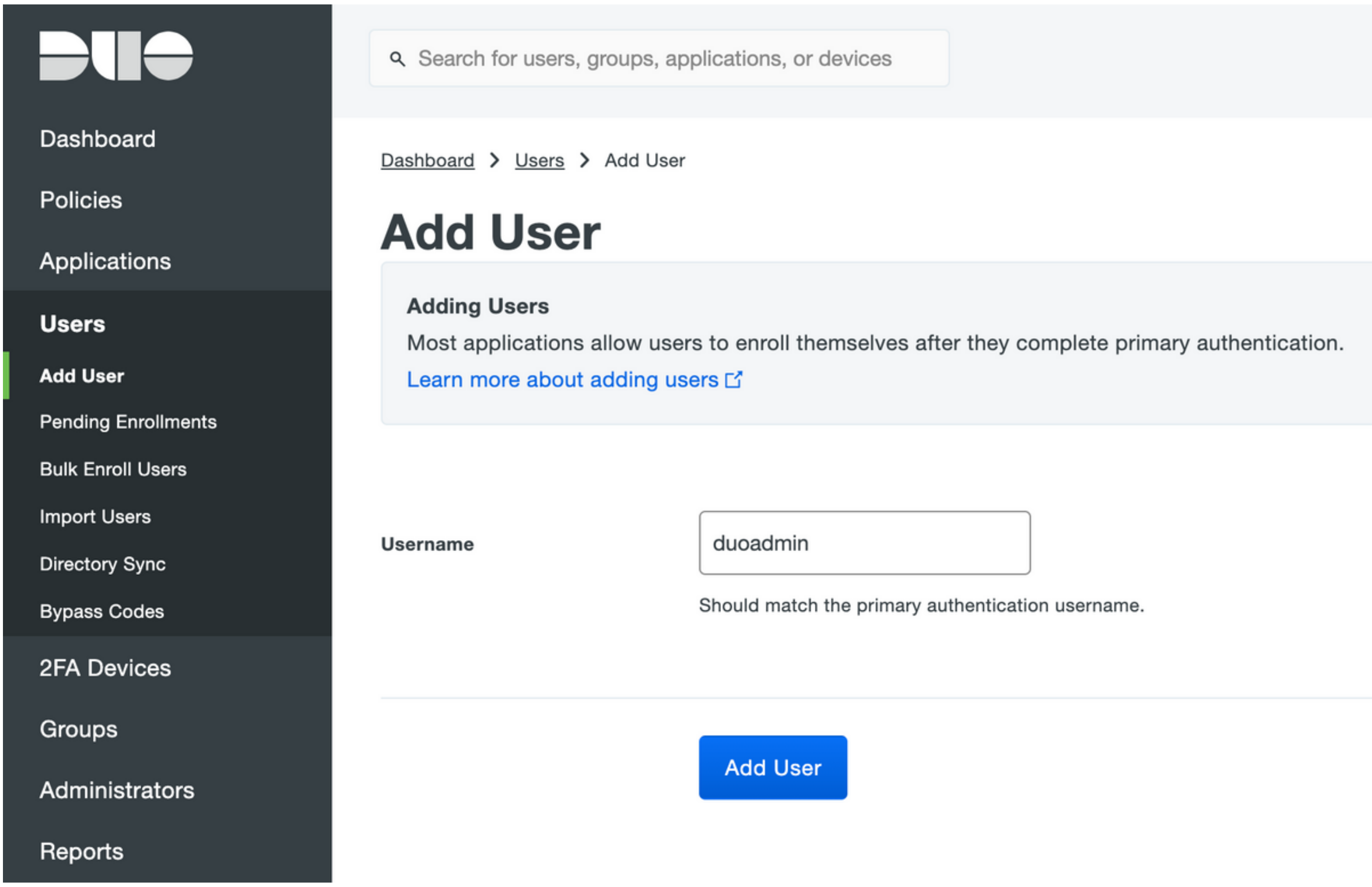
Duo Security Authentication Proxy Service

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
DCOM Server Process Laun...	The DCOMLAUNCH se...	Running	Automatic	Local System
Device Association Service	Enables pairing betwee...		Manual (Trigger Start)	Local System
Device Install Service	Enables a computer to ...		Manual (Trigger Start)	Local System
Device Setup Manager	Enables the detection, ...		Manual (Trigger Start)	Local System
DFS Namespace	Enables you to group s...	Running	Automatic	Local System
DFS Replication	Enables you to synchro...	Running	Automatic	Local System
DHCP Client	Registers and updates I...	Running	Automatic	Local Service
DHCP Server	Performs TCP/IP confi...	Running	Automatic	Network Service
Diagnostic Policy Service	The Diagnostic Policy S...	Running	Automatic (Delayed ...	Local Service
Diagnostic Service Host	The Diagnostic Service ...		Manual	Local Service
Diagnostic System Host	The Diagnostic System ...		Manual	Local System
Diagnostics Tracking Service	The Diagnostics Tracki...	Running	Automatic	Local System
Distributed Link Tracking Cl...	Maintains links betwee...		Manual	Local System
Distributed Transaction Co...	Coordinates transactio...	Running	Automatic (Delayed ...	Network Service
DNS Client	The DNS Client service ...	Running	Automatic (Trigger S...	Network Service
DNS Server	Enables DNS clients to r...	Running	Automatic	Local System
DS Role Server	This service hosts the D...		Manual	Local System
Duo Security Authenticatio...		Running	Automatic	Local System
Encrypting File System (EFS)	Provides the core file e...		Manual (Trigger Start)	Local System
Extensible Authentication P...	The Extensible Authenti...		Manual	Local System
File Replication	Synchronizes folders wi...		Disabled	Local System
FileZilla Server FTP server		Running	Automatic	Local System

步驟7.創建使用者名稱，並在終端裝置上啟用Duo Mobile:https://duo.com/docs/administration-users#creating-users-manually

在Duo Admin Panel上新增使用者。導覽至**Users > add users**，如下圖所示：



Add User

Adding Users

Most applications allow users to enroll themselves after they complete primary authentication.

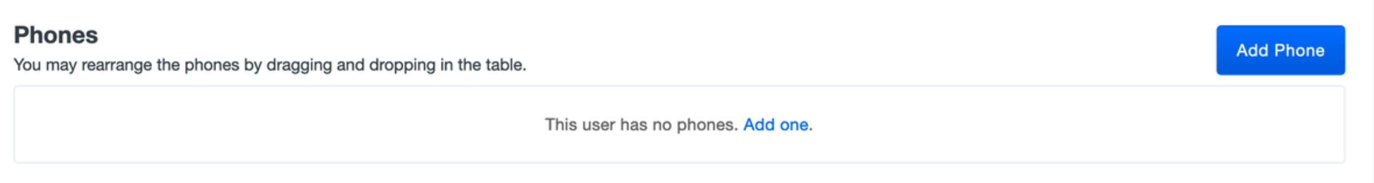
Learn more about adding users

Username: duoadmin

Should match the primary authentication username.

Add User

確保終端使用者已在電話上安裝Duo應用。

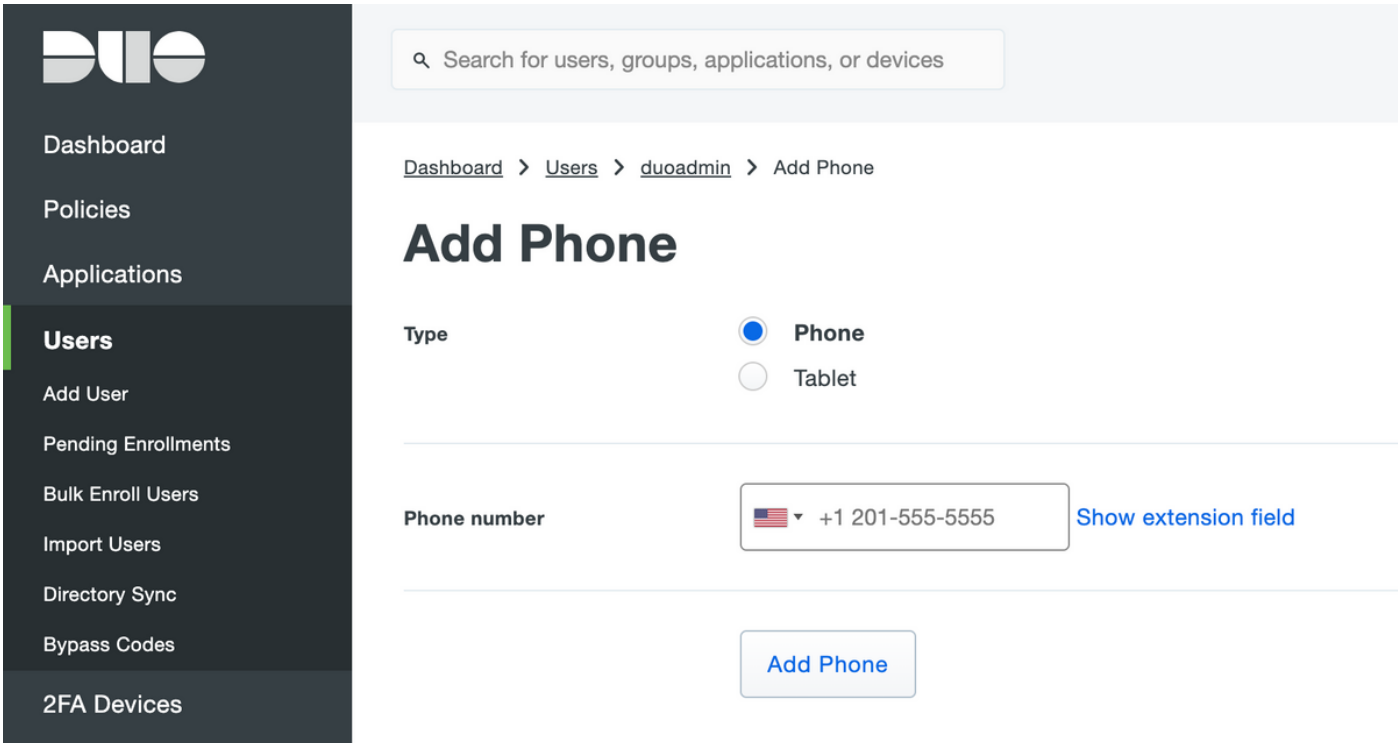


Phones

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

Add Phone

This user has no phones. Add one.



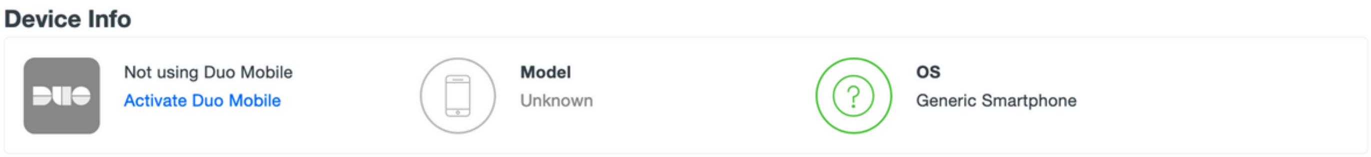
Add Phone

Type: ● Phone ○ Tablet

Phone number: +1 201-555-5555 Show extension field

Add Phone

選擇Activate Duo Mobile，如下圖所示：



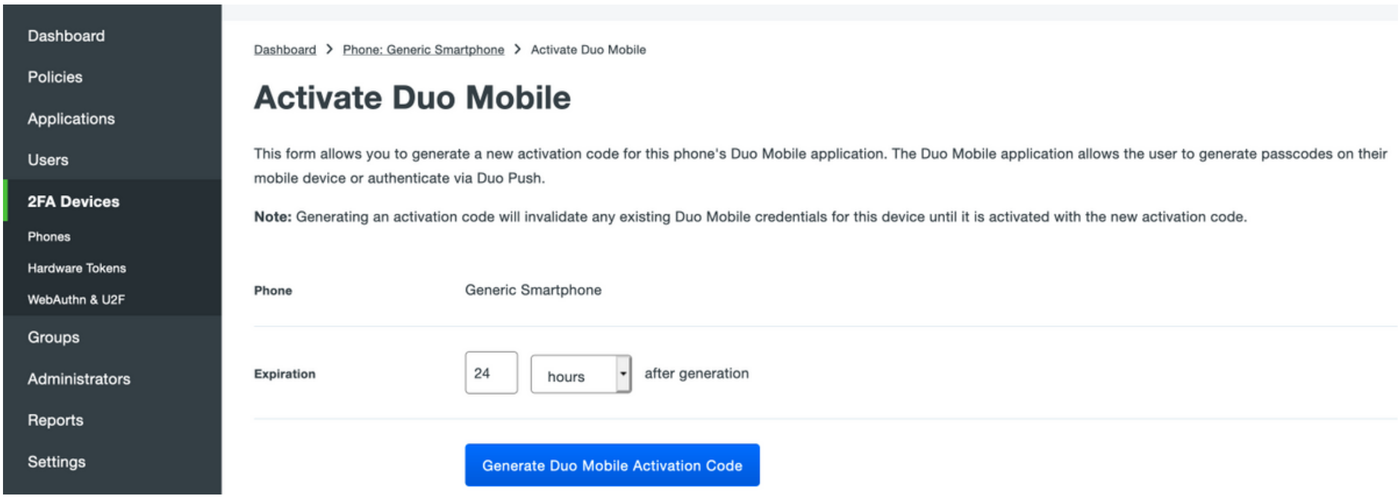
Device Info

Not using Duo Mobile
Activate Duo Mobile

Model
Unknown

OS
Generic Smartphone

選擇**Generate Duo Mobile Activation Code**，如下圖所示：



Dashboard > Phone: Generic Smartphone > Activate Duo Mobile

Activate Duo Mobile

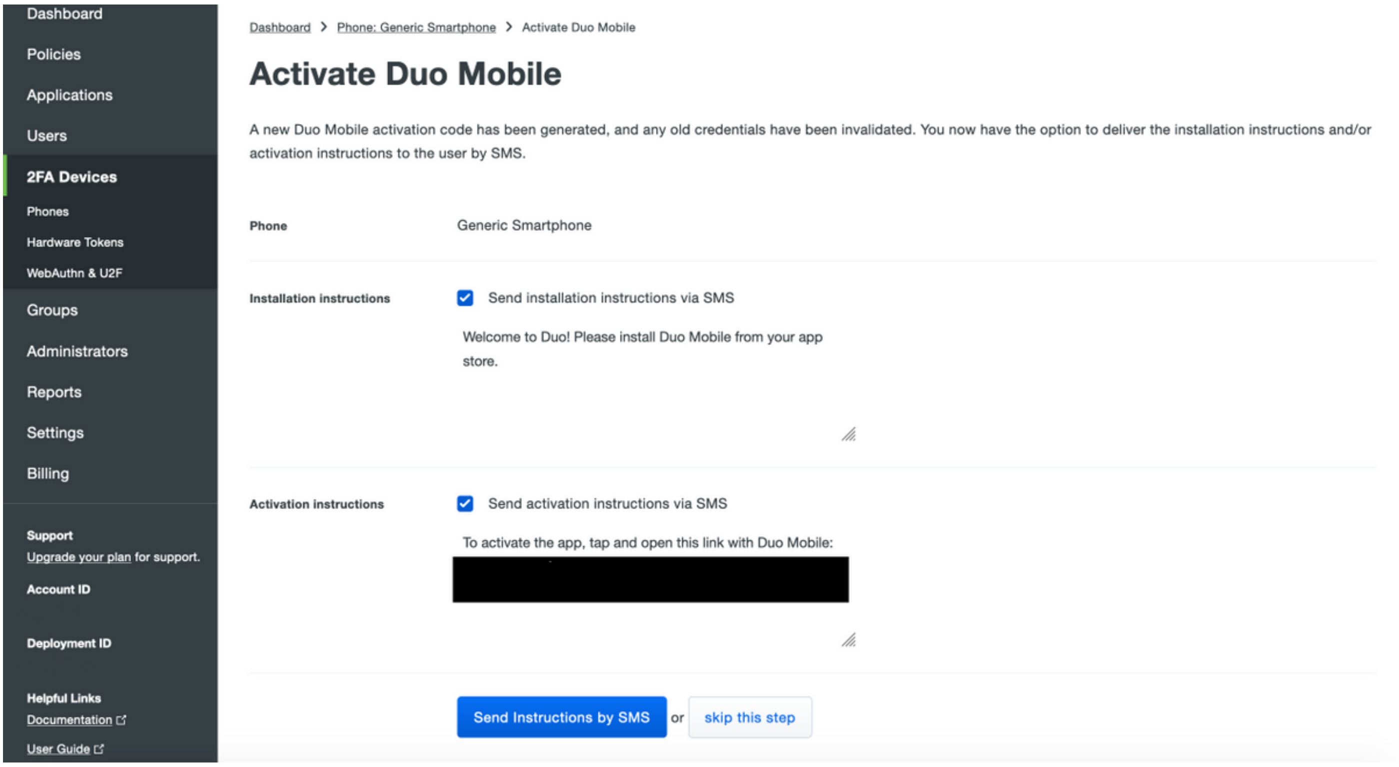
This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

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

選擇**Send Instructions by SMS**，如下圖所示：



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

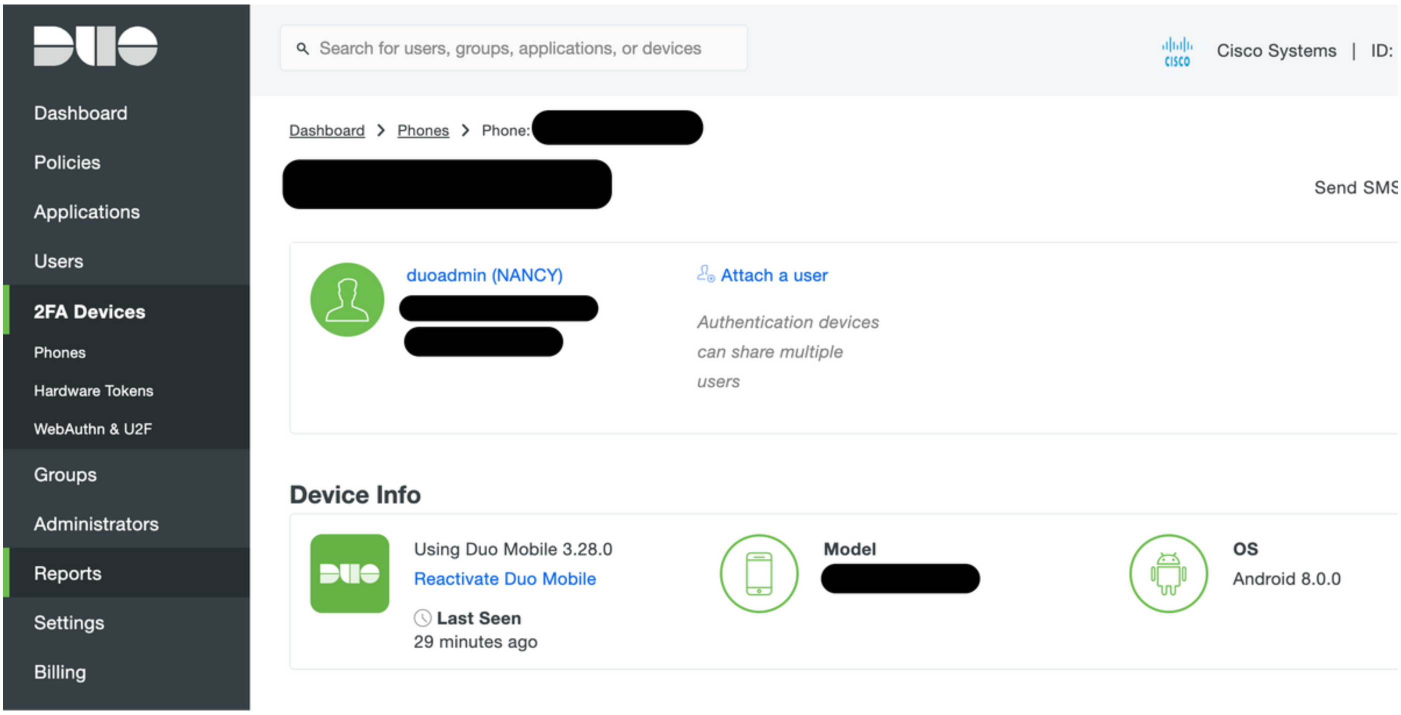
Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions ☑ Send activation instructions via SMS

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

Send Instructions by SMS or skip this step

單擊SMS中的連結，Duo應用將連結到**Device Info**部分中的用戶帳戶，如下圖所示：



Dashboard > Phones > Phone: [redacted]

[redacted]

duoadmin (NANCY)

[redacted]

Authentication devices can share multiple users

Device Info

Using Duo Mobile 3.28.0

Reactivate Duo Mobile

Last Seen
29 minutes ago

Model
[redacted]

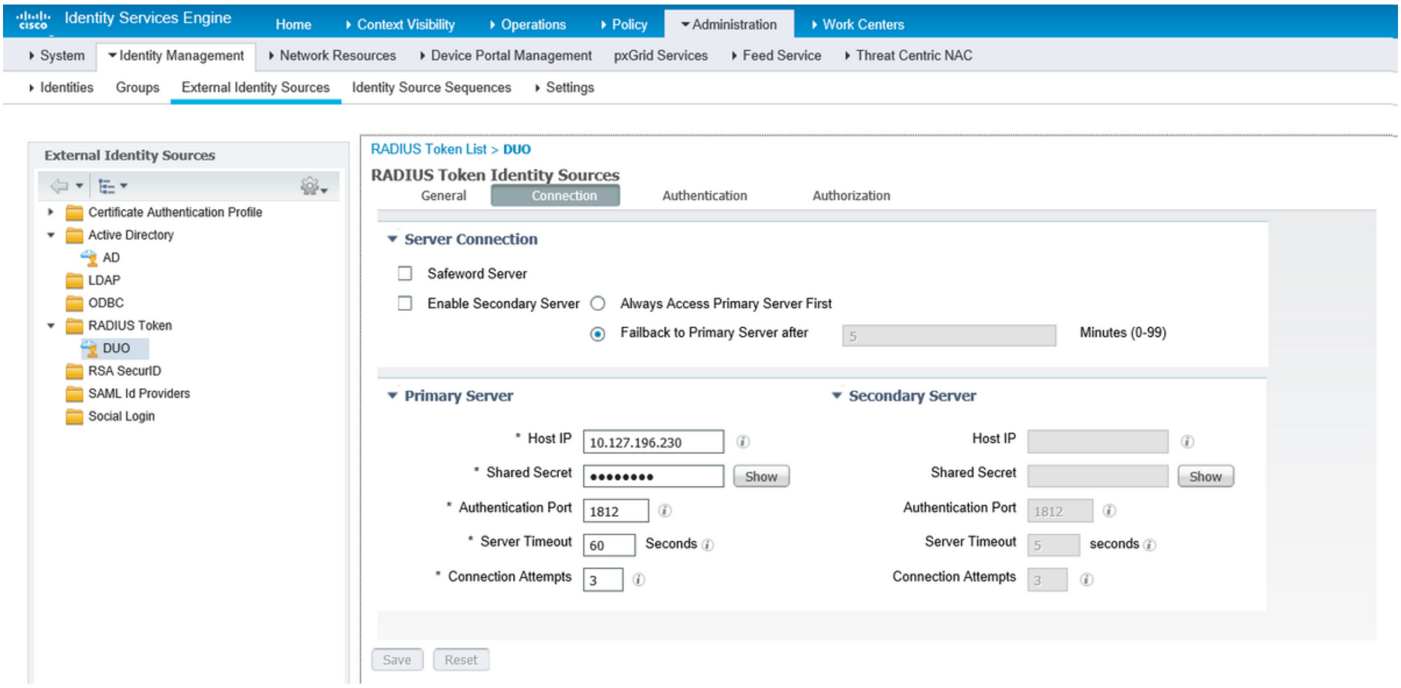
OS
Android 8.0.0

ISE 組態

步驟1.將ISE與Duo Auth Proxy整合。

導航到**Administration > Identity Management > External Identity Sources > RADIUS Token**，點選**Add**以新增新的RADIUS令牌伺服器。在「general」頁籤中定義伺服器名稱，在「connection」頁籤中定義IP地址和共用金鑰，如下圖所示：

60



RADIUS Token Identity Sources

Server Connection

☐ Safeword Server

☐ Enable Secondary Server ○ Always Access Primary Server First

● Failback to Primary Server after 5 Minutes (0-99)

Primary Server

* Host IP 10.127.196.230

* Shared Secret •••••••• Show

* Authentication Port 1812

* Server Timeout 60 Seconds

* Connection Attempts 3

Secondary Server

Host IP

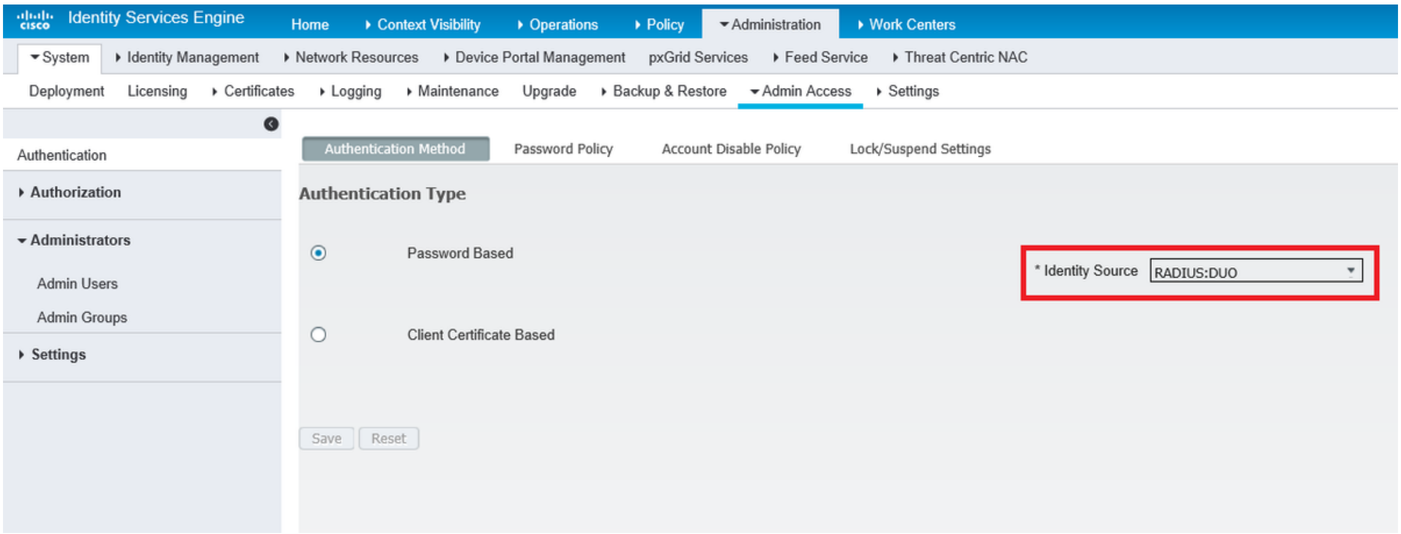
Shared Secret Show

Authentication Port 1812

Server Timeout 5 seconds

Connection Attempts 3

步驟2.導覽至**Administration > System > Admin Access > Authentication > Authentication Method 並Select** previously configured RADIUS token server as the Identity Source，如下圖所示：



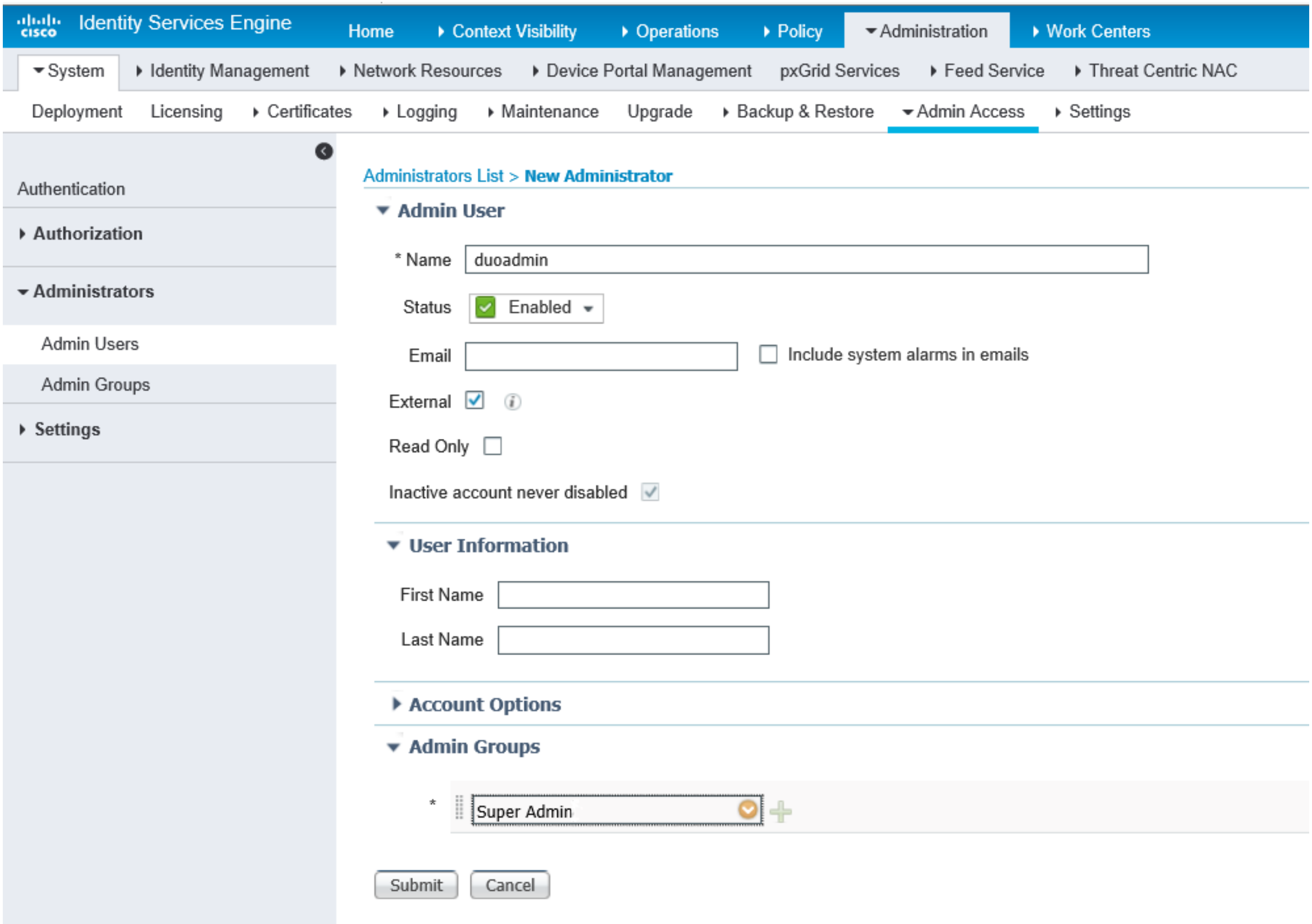
Authentication Type

● Password Based

○ Client Certificate Based

* Identity Source RADIUS:DUO

步驟3.導覽至Administration > System > Admin Access > Administrators > Admin Users，然後將admin使用者建立為External，並提供超級管理員許可權，如下圖所示：



Admin User

* Name duoadmin

Status ☑ Enabled

Email ☐ Include system alarms in emails

External ☑

Read Only ☐

Inactive account never disabled ☑

User Information

First Name

Last Name

Account Options

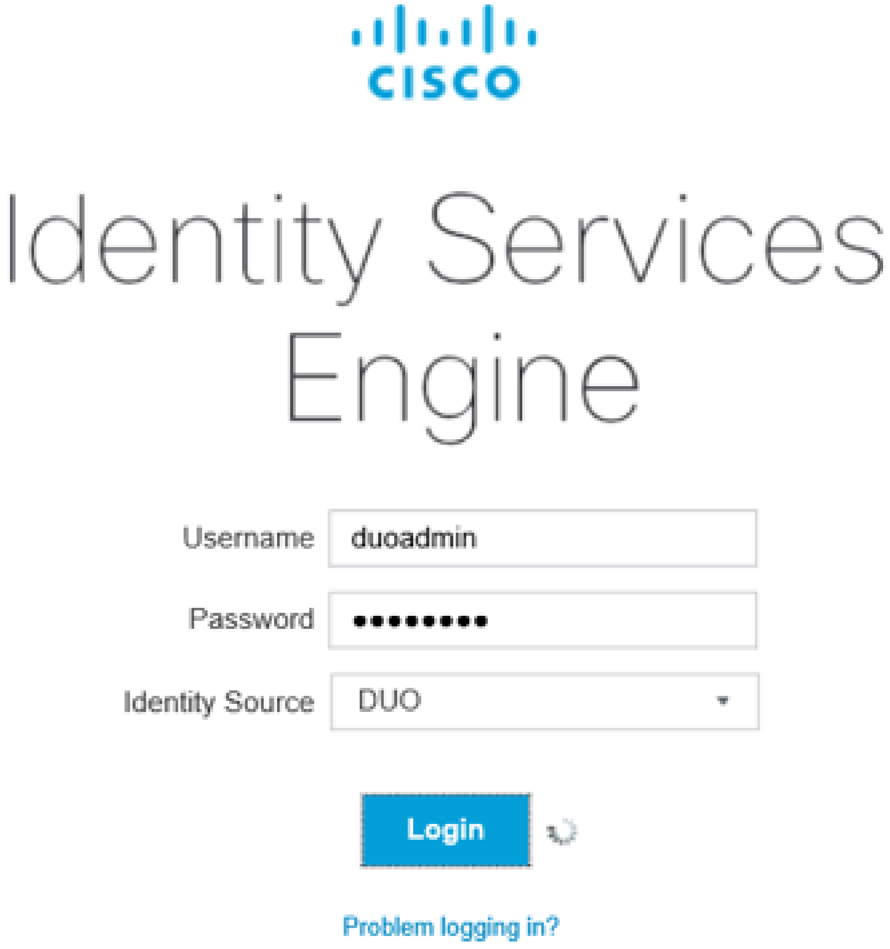
Admin Groups

* Super Admin

驗證

使用本節內容，確認您的組態是否正常運作。

開啟ISE GUI，選擇RADIUS Token Server作為身份源並以管理員使用者登入。



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

要排除與Cloud或Active Directory的Duo Proxy連線相關的問題，請在authproxy.cfg主部分下新增「debug=true」，以啟用Duo Auth Proxy上的調試。

日誌位於以下位置：

C:\Program檔案(x86)\Duo Security Authentication Proxy\log

在記事本或寫字板等文本編輯器中開啟**authproxy++log**檔案。

記錄Duo Auth Proxy從ISE接收請求並將其傳送到Duo Cloud。

```
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
```

無法訪問Duo Cloud的Duo Auth Proxy的日誌片段。

```
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.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
```

相關資訊

- 使用DUO的RA VPN身份驗證
- 技術支援與文件 - Cisco Systems