

# 配置Duo與Active Directory和ISE的整合，以便在Anyconnect/遠端訪問VPN客戶端上進行雙因素身份驗證

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

#### [背景資訊](#)

#### [網路圖表和案例](#)

#### [通訊過程](#)

#### [Active Directory配置](#)

### [Duo配置](#)

### [Duo Auth Proxy設定](#)

### [Cisco ISE配置](#)

### [Cisco ASA RADIUS/ISE配置](#)

### [Cisco ASA遠端訪問VPN配置](#)

### [測試](#)

### [疑難排解](#)

#### [工作調試](#)

---

## 簡介

本文檔介紹與AD和ISE的Duo Push整合，作為連線到ASA的AnyConnect客戶端的雙因素身份驗證。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ASA上的RA VPN配置
- ASA上的RADIUS配置
- ISE
- Active Directory
- Duo應用程式

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

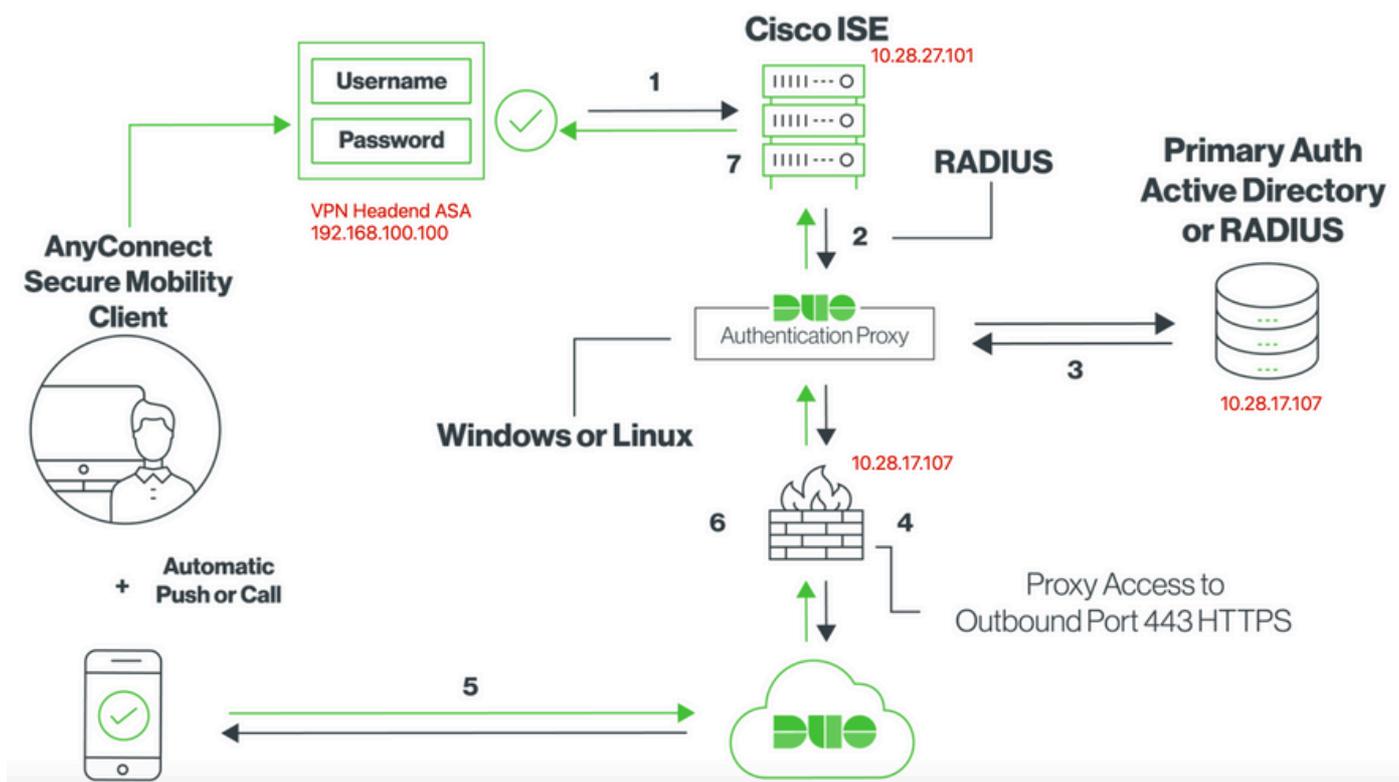
- Microsoft 2016伺服器
- ASA 9.14(3)18
- ISE伺服器3.0
- Duo伺服器
- Duo Authentication Proxy Manager

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

本文檔介紹如何配置與Active Directory(AD)和Cisco Identity Service Engine(ISE)的Duo Push整合，作為連線到思科自適應安全裝置(ASA)的AnyConnect客戶端的雙因素身份驗證。

## 網路圖表和案例



## 通訊過程

<https://duo.com/docs/ciscoise-radius>

1. 對思科ISE發起的主要身份驗證
2. Cisco ASA向Duo Authentication Proxy傳送身份驗證請求
3. 主身份驗證使用Active Directory或RADIUS
4. Duo Authentication Proxy連線建立到Duo Security over TCP埠443
5. 通過Duo Security的服務進行輔助身份驗證
6. Duo身份驗證代理收到身份驗證響應

## 7. 已授予思科ISE訪問許可權

使用者帳戶：

- Active Directory管理員：此帳戶用作目錄帳戶，以允許Duo Auth Proxy繫結到Active Directory伺服器以進行主身份驗證。
- Active Directory測試使用者
- Duo測試使用者進行輔助身份驗證

## Active Directory配置

Windows伺服器預配置了Active Directory域服務。

---

 注意：如果RADIUS Duo Auth Proxy Manager在同一Active Directory主機上運行，則必須解除安裝/刪除網路策略伺服器(NPS)角色；如果兩個RADIUS服務都運行，則它們可能衝突並影響效能。

---

要在遠端訪問VPN使用者上實現身份驗證和使用者身份的AD配置，需要幾個值。

在ASA和Duo Auth Proxy伺服器上完成配置之前，必須在Microsoft伺服器上建立或收集所有這些詳細資訊。

主要值包括：

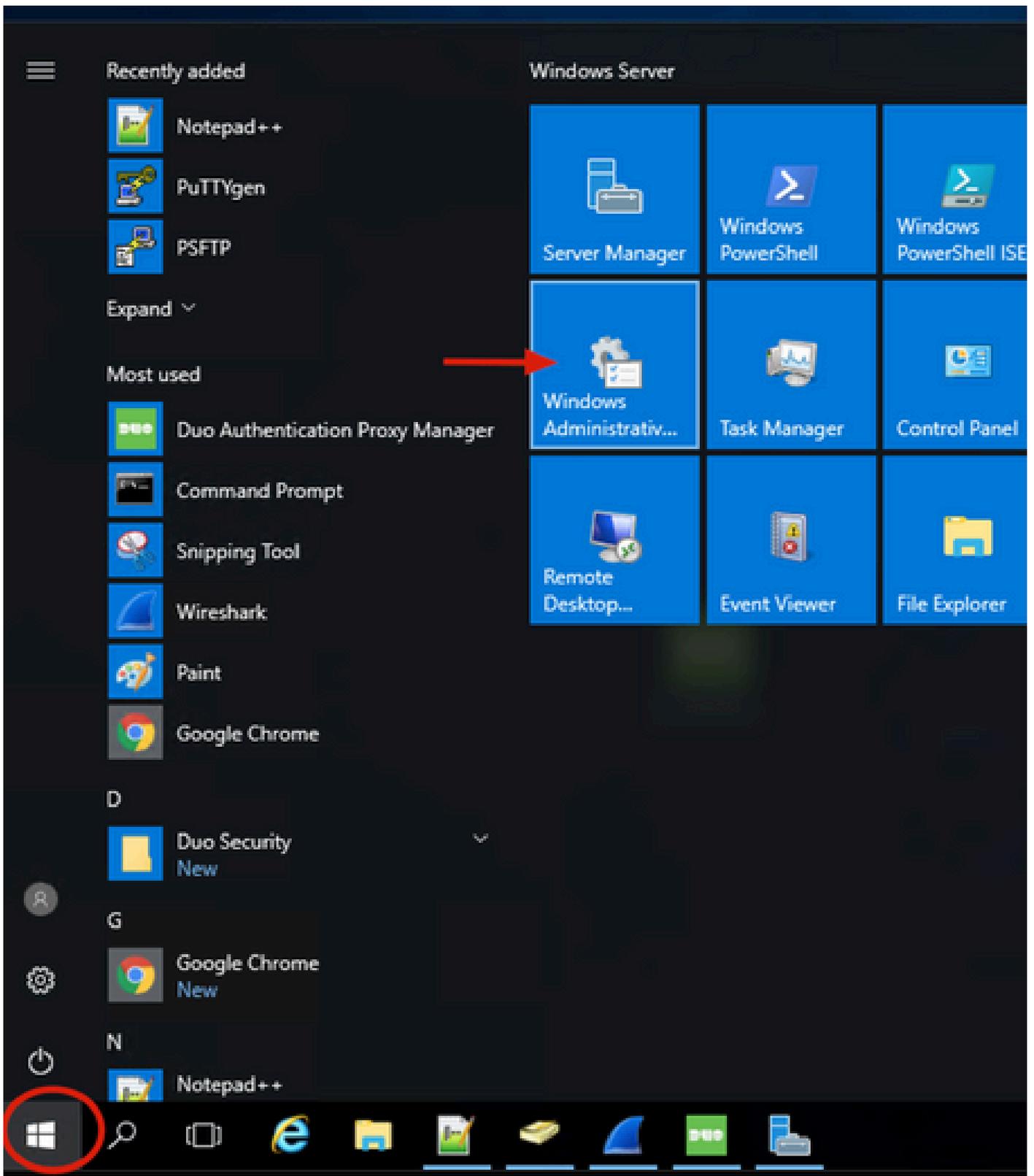
- 域名。這是伺服器的域名。在本配置指南中，agarciam.cisco是域名。
- 伺服器IP/FQDN地址。用於訪問Microsoft伺服器的IP地址或FQDN。如果使用FQDN，則必須在ASA和Duo Auth Proxy中配置DNS伺服器以解析FQDN。

在本配置指南中，此值為agarciam.cisco ( 解析為10.28.17.107 )。

- 伺服器埠。LDAP服務使用的埠。預設情況下，LDAP和STARTTLS將TCP埠389用於LDAP，而LDAP over SSL(LDAPS)使用TCP埠636。
- 根CA。如果使用LDAPS或STARTTLS，則需要使用根CA來對LDAPS使用的SSL證書進行簽名。
- 目錄使用者名稱和密碼。這是Duo Auth Proxy伺服器用於繫結到LDAP伺服器並對使用者進行驗證和搜尋使用者與群組的帳戶。
- 基本和群組可分辨名稱(DN)。基礎DN是Duo Auth Proxy的出發點，並通知Active Directory開始搜尋和驗證使用者。

在本配置指南中，根域agarciam.cisco用作基礎DN，組DN為Duo-USERS。

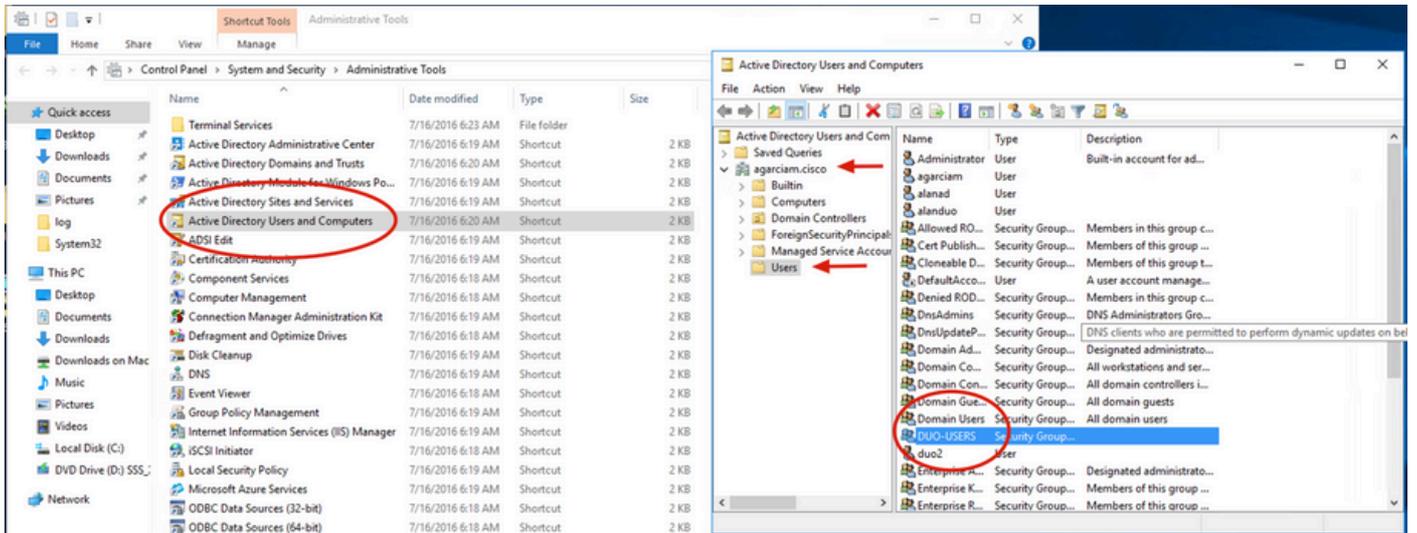
1.要新增新的Duo使用者，請在Windows Server上導航到左下角的Windows圖示，然後按一下Windows管理工具，如下圖所示。



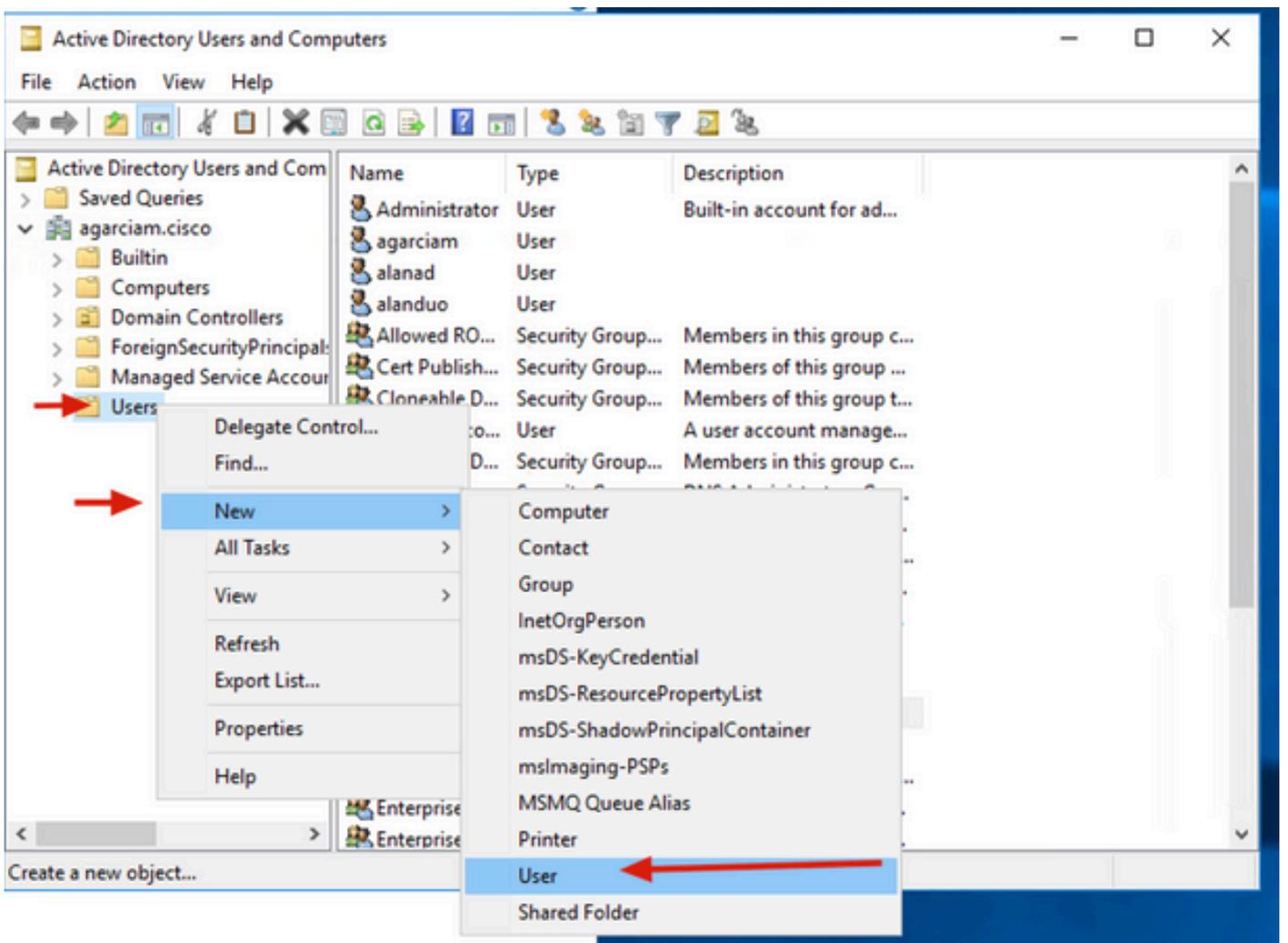
2.在「Windows管理工具」視窗中，導航至Active Directory使用者和電腦。

在Active Directory使用者和電腦面板上，展開域選項並導航到Users資料夾。

在此配置示例中，Duo-USERS用作輔助身份驗證的目標組。



3. 按一下右鍵Users資料夾，然後選擇New > User，如下圖所示。



4. 在「新對象 — 使用者」視窗中，指定此新使用者的身份屬性，然後按一下下一步，如下圖所示。

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. 確認密碼，並在驗證使用者資訊後按一下Next，然後按一下Finish。

New Object - User X

 Create in: agarciam.cisco/Users

---

Password:  ←

Confirm password:  ←

User must change password at next logon

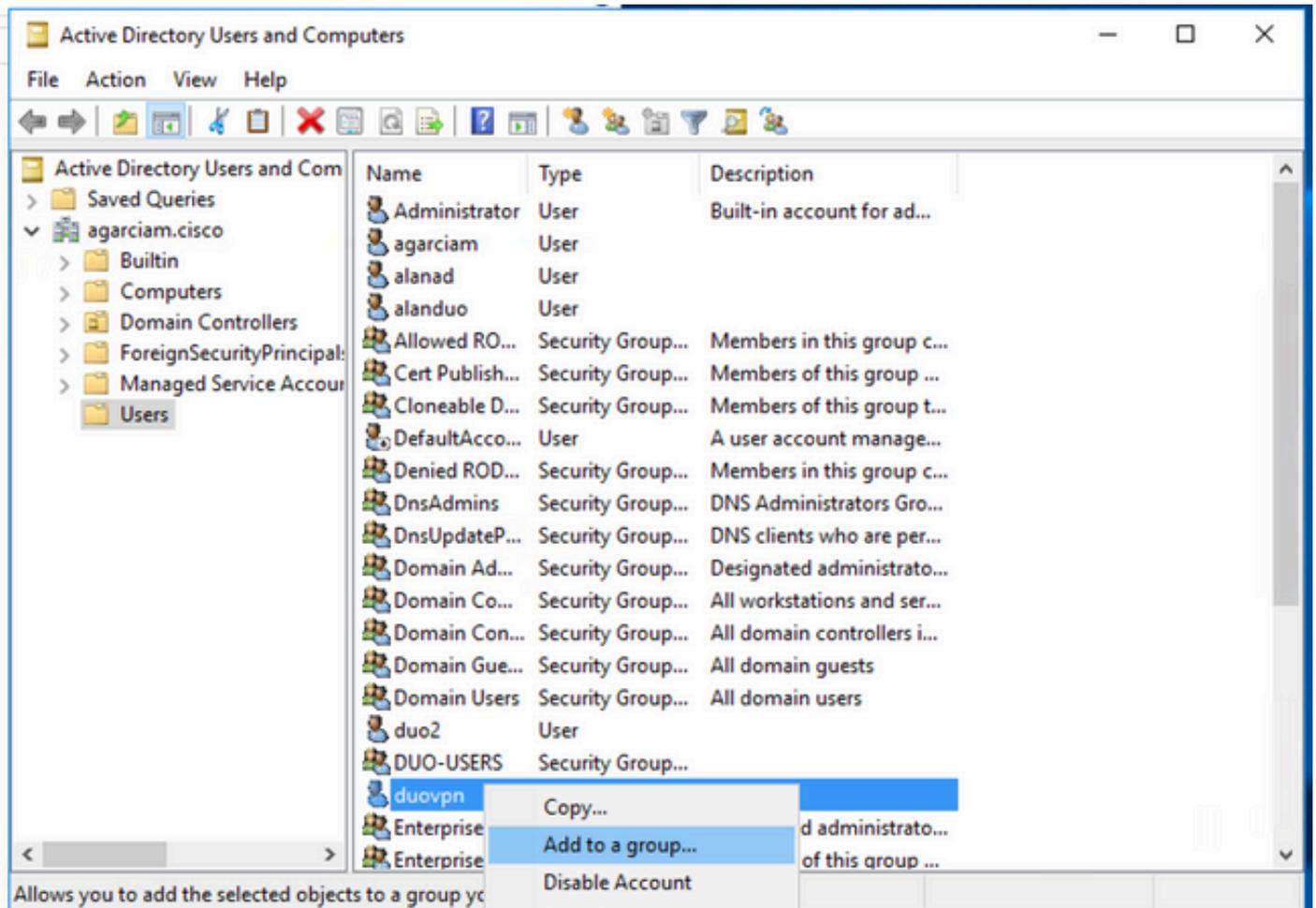
User cannot change password

Password never expires

Account is disabled

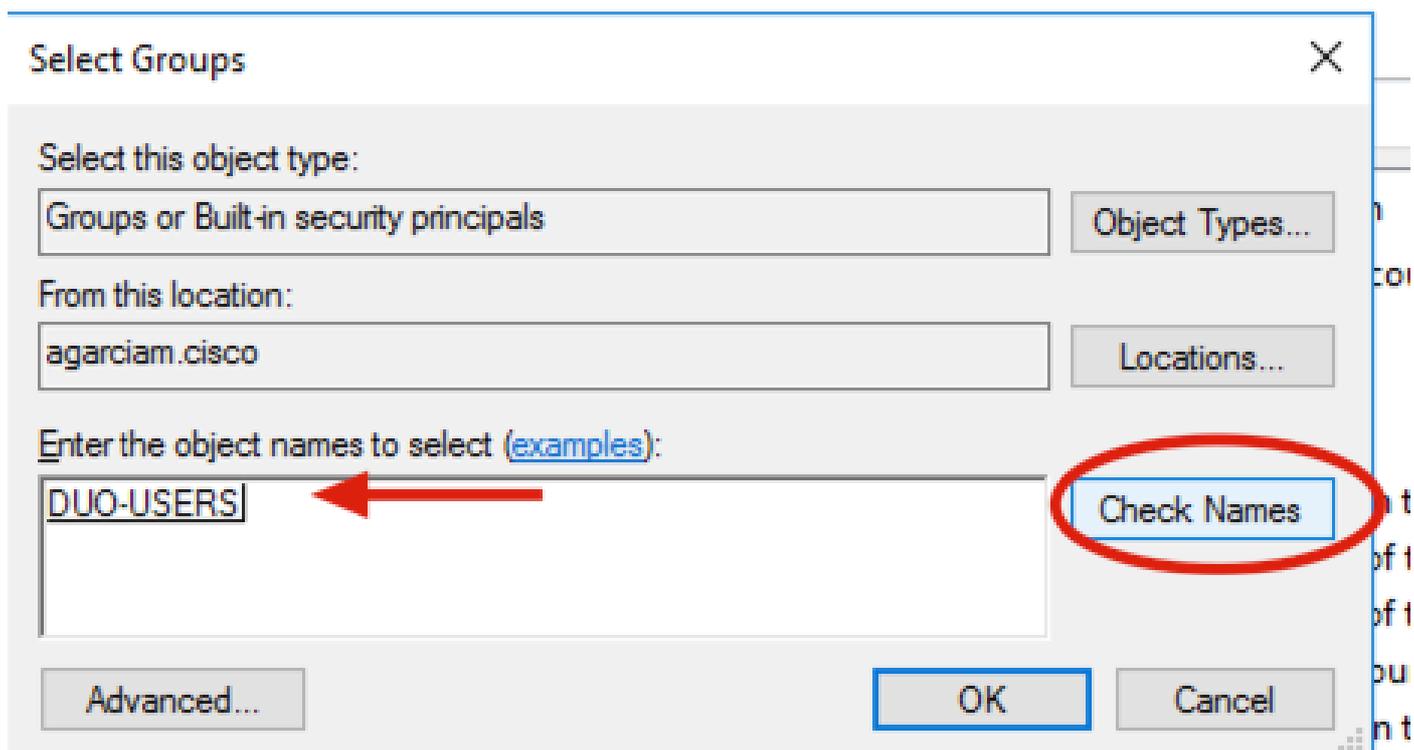
---

6.將新使用者分配給特定組，按一下右鍵該使用者並選擇「新增到組」，如下圖所示。



7.在「選擇組」面板上，鍵入所需組的名稱，然後按一下檢查名稱。

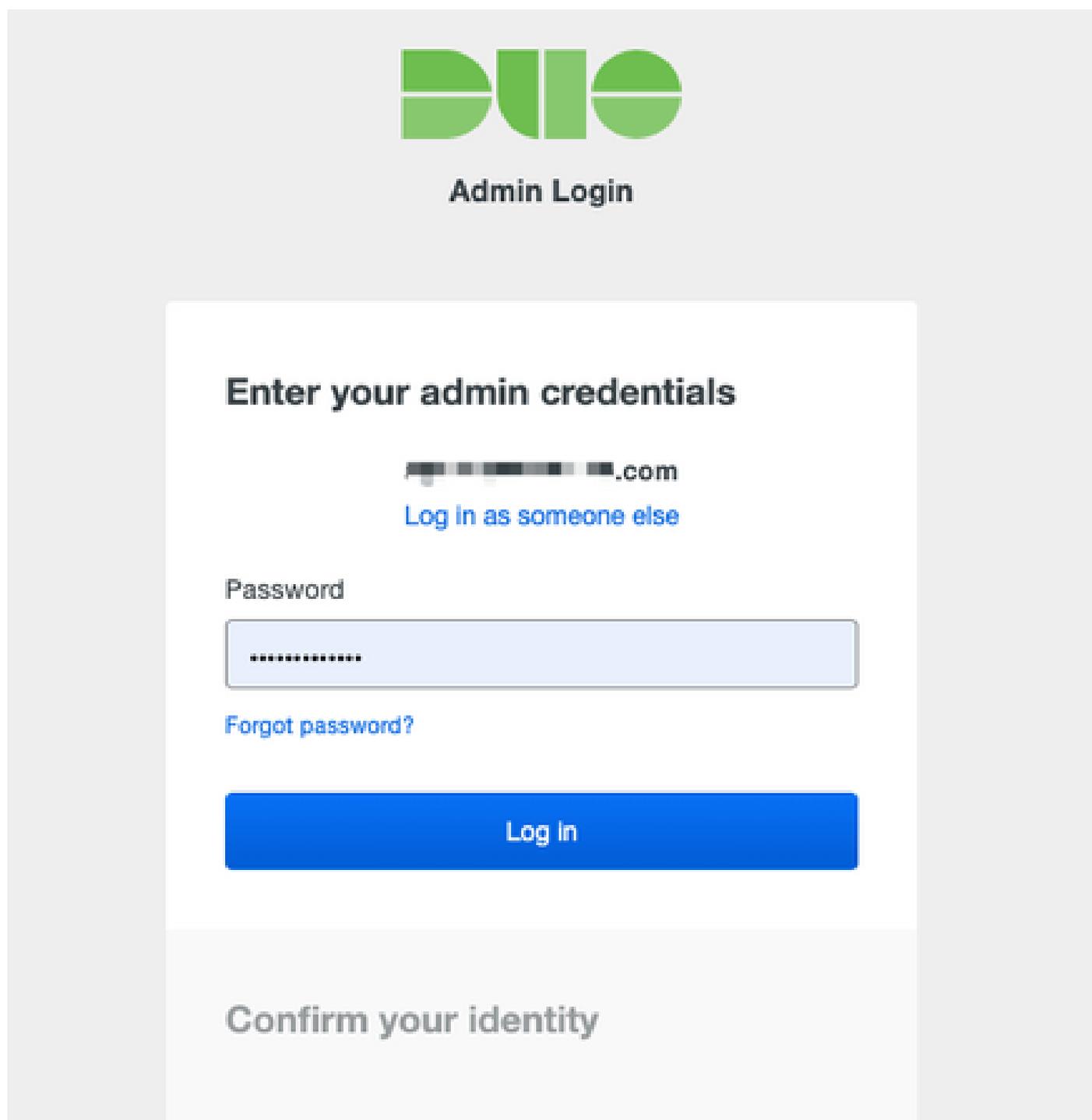
然後，選擇符合條件的名稱，然後按一下Ok。



8.此使用者用作本文檔的示例。

## Duo配置

1.登入您的Dudo Admin門戶。



**Admin Login**

**Enter your admin credentials**

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

Password

.....

[Forgot password?](#)

**Log In**

Confirm your identity

2.在左側面板上，導航到Users，按一下Add User，然後鍵入與活動域使用者名稱匹配的使用者名稱，然後按一下Add User。

**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「新使用者」面板上，將所有必要資訊填入空白。

# 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「使用者裝置」下，指定輔助身份驗證方法。

 注意：在本文檔中，使用Duo push for mobile devices方法，因此需要新增電話裝置。

按一下「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. 鍵入使用者電話號碼，然後按一下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.在左側的Duo Admin面板上，導航到Users，然後按一下新使用者。

Dashboard > Users

## Users

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

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

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

<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：如果您目前沒有訪問電話的許可權，您可以選擇電子郵件選項。

7. 導航到Phones部分，然後按一下Activate Duo Mobile。

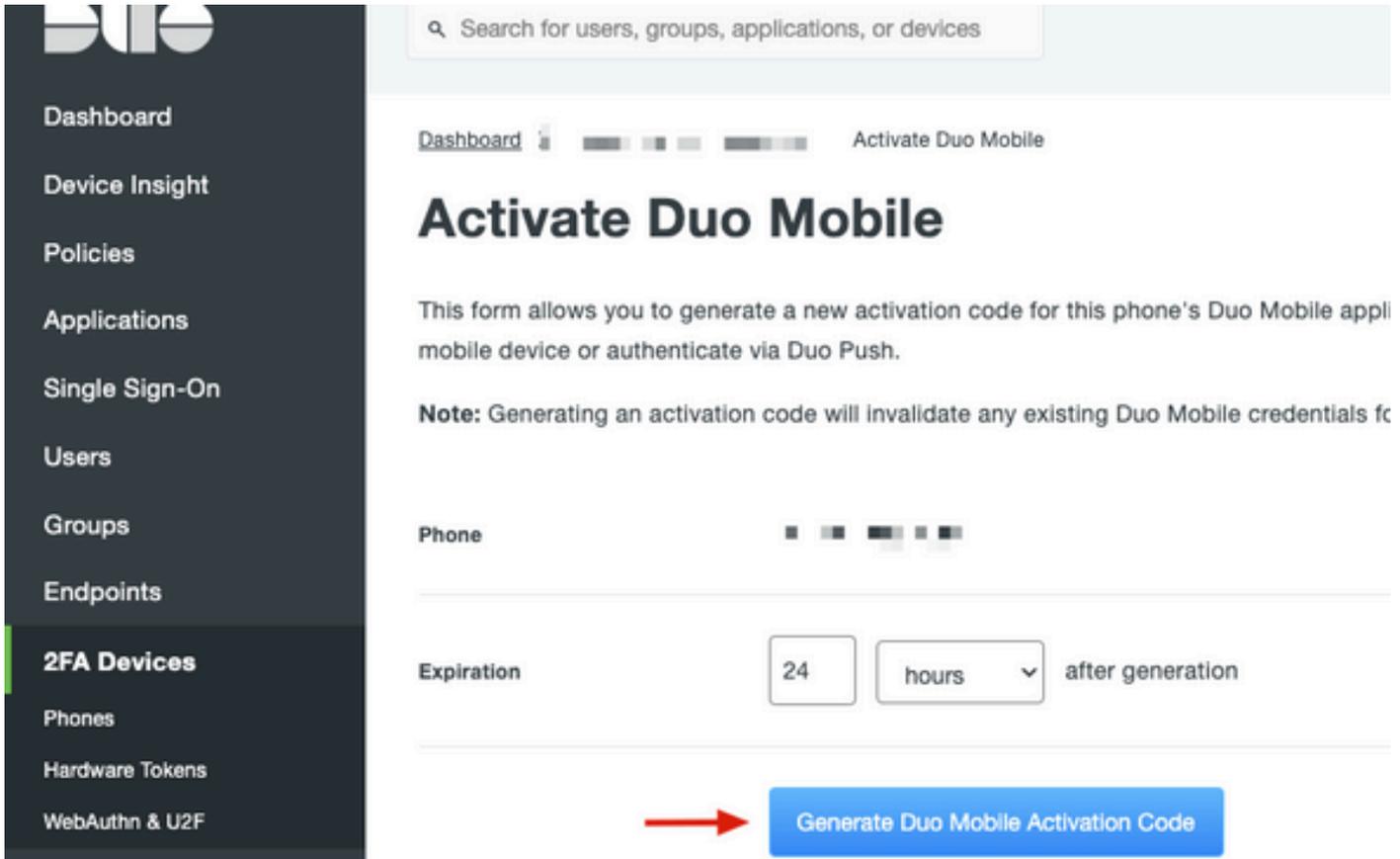
### Phones

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

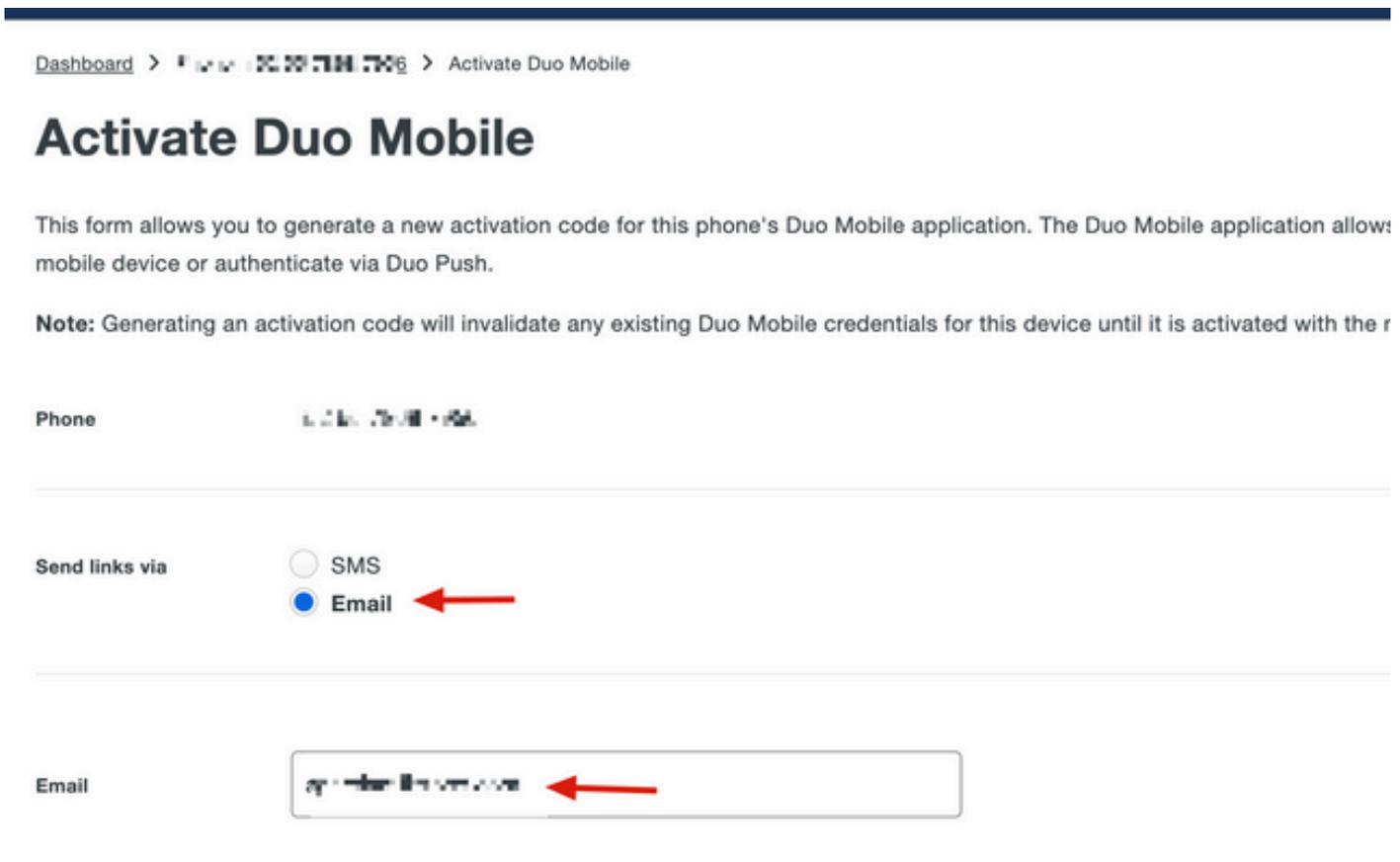
[Add Phone](#)

Alias	Device	Platform	Model	Security Warnings	
phone1		Android 10		✓ No warnings	<a href="#">Activate Duo Mobile</a> 

8. 按一下Generate Duo Mobile Activation Code。



9.選擇Email以通過電子郵件接收說明，鍵入您的電子郵件地址，然後按一下Send Instructions by email。



10. 您會收到一封包含說明的電子郵件，如下圖所示。

**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. 從您的流動裝置開啟Duo Mobile App，按一下Add，然後選擇Use QR code，然後從說明電子郵件中掃描該代碼。

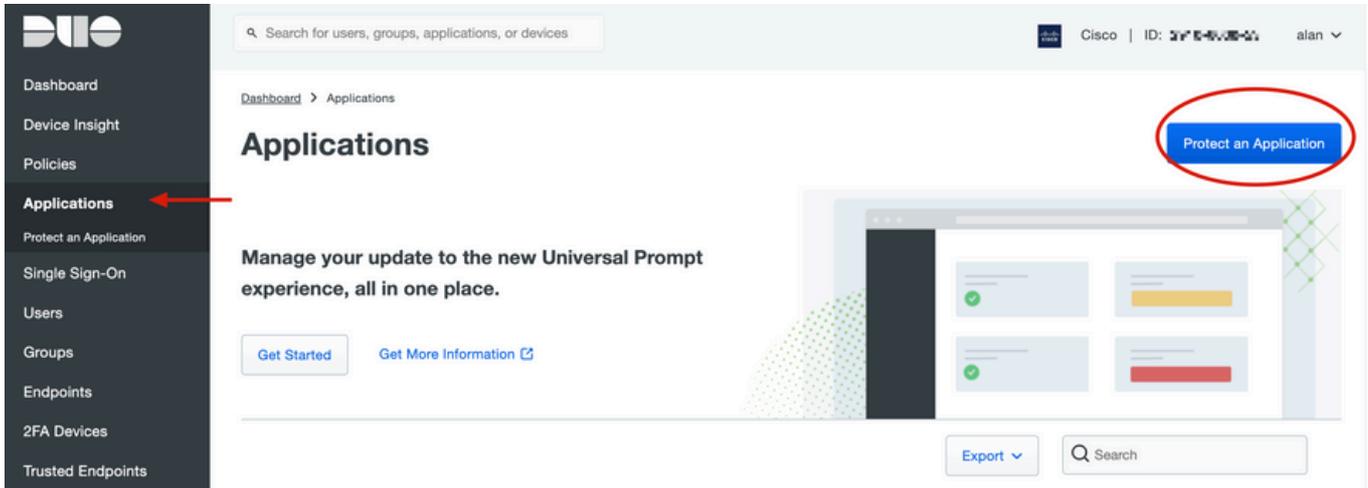
12. 新使用者將新增到您的Duo Mobile App中。

## Duo Auth Proxy設定

1. 從<https://duo.com/docs/authproxy-reference>下載並安裝Duo Auth Proxy Manager。

 注意：在本文檔中，Duo Auth Proxy Manager安裝在承載Active Directory服務的同一Windows伺服器上。

2. 在Duo Admin Panel上，導航至Applications，然後按一下Protect an Application。



3. 在搜尋欄上查詢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](#)

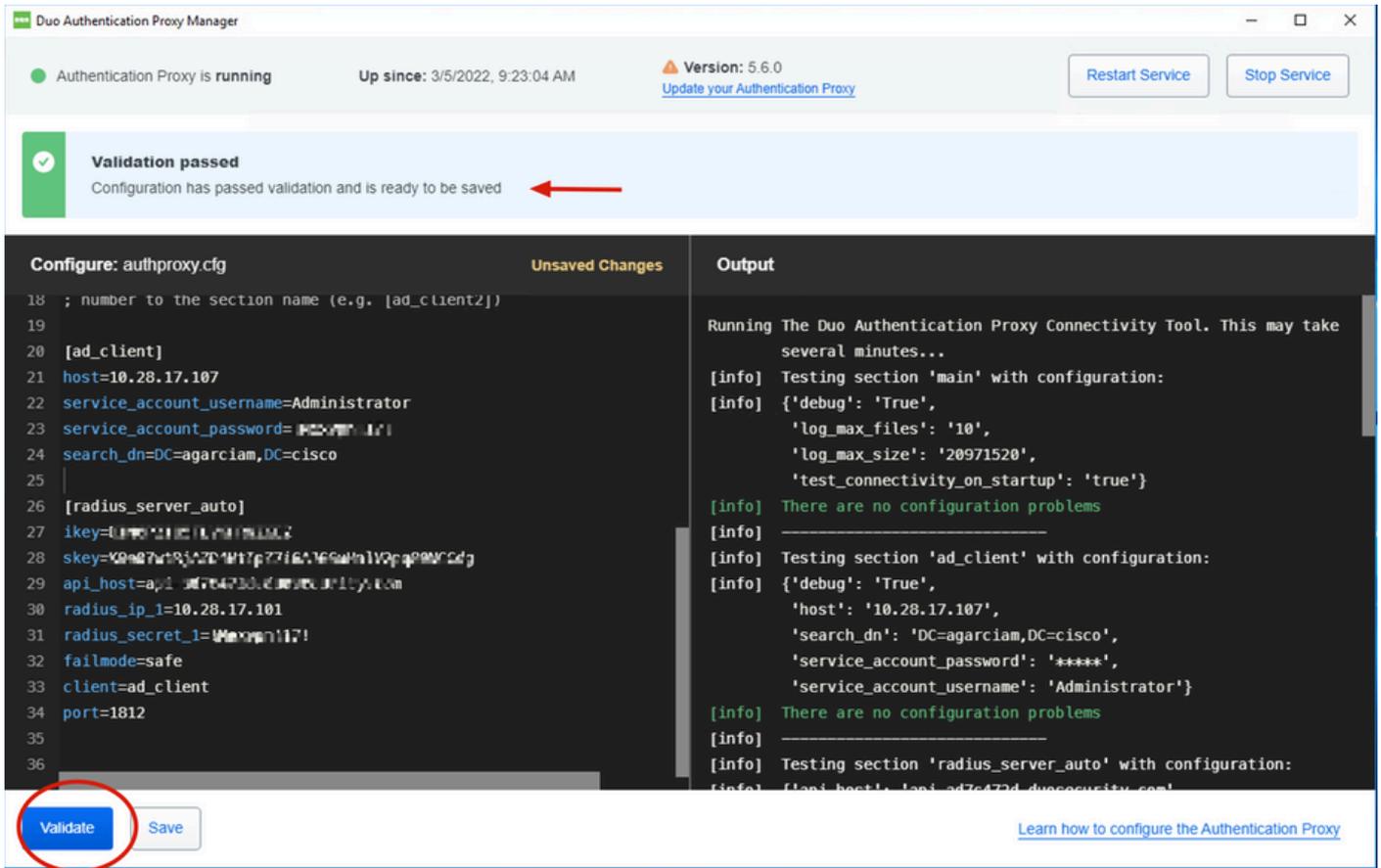
Choose an application below to get started.

Application	Protection Type	
 Akamai Enterprise Application Access	2FA	<a href="#">Documentation</a> <a href="#">Protect</a>
 Cisco ISE RADIUS 	2FA	<a href="#">Documentation</a> <a href="#">Protect</a>

4. 複製整合金鑰、Secrety金鑰和API主機名。您需要此資訊才能進行Duo Authentication Proxy配置

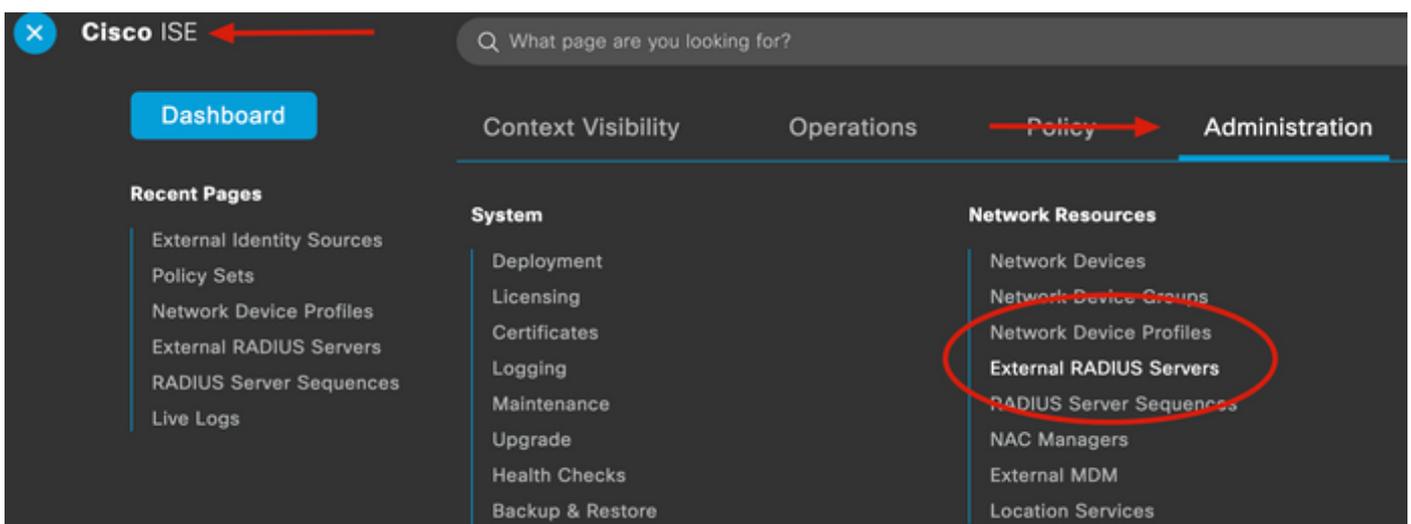
o





## Cisco ISE配置

1. 登入ISE管理員門戶。
2. 展開Cisco ISE頁籤，導航到Administration，然後點選Network Resources，然後點選External RADIUS Servers。



3. 在外部Radius伺服器索引標籤上，按一下Add。

Cisco ISE Administration · Network Resources

Network Devices Network Device Groups Network Device Profiles **External RADIUS Servers** RADIUS Server Sequences

## External RADIUS Servers

Edit **+ Add** Duplicate Delete

Name	Description
Name: Currently Sorted	

4. 使用 Duo Authentication Proxy Manager 中使用的 RADIUS 配置 填充并点击 Submit。

Network Devices Network Device Groups Network Device Profiles **External RADIUS Servers** RADIUS Server Sequences NAC Managers External MDM More

\* Name DUO\_NEW

Description

\* Host IP 10.28.17.107

\* Shared Secret ..... Show

Enable KeyWrap

\* Key Encryption Key Show

\* Message Authenticator Code Key Show

Key Input Format  ASCII  HEXADECIMAL

\* Authentication Port 1812 (Valid Range 1 to 65535)

\* Accounting Port 1813 (Valid Range 1 to 65535)

\* Server Timeout 5 Seconds (Valid Range 1 to 120)

\* Connection Attempts 3 (Valid Range 1 to 9)

Radius ProxyFailover Expiration 300 (Valid Range 1 to 600)

Submit

5. 導覽至 RADIUS Server Sequences 頁籤，然後按一下 Add。

Cisco ISE Administration · Network Resources

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers **RADIUS Server Sequences**

## RADIUS Server Sequences

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit **+ Add** Duplicate Delete

6. 指定序列名稱並分配新的 RADIUS 外部伺服器，按一下提交。

## RADIUS Server Sequence

General

Advanced Attribute Settings

\* Name

DUO\_Sequence

Description

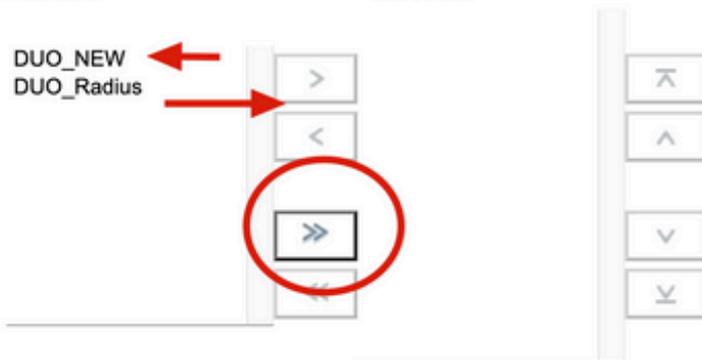
### ▼ User Selected Service Type

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

Available

\* Selected

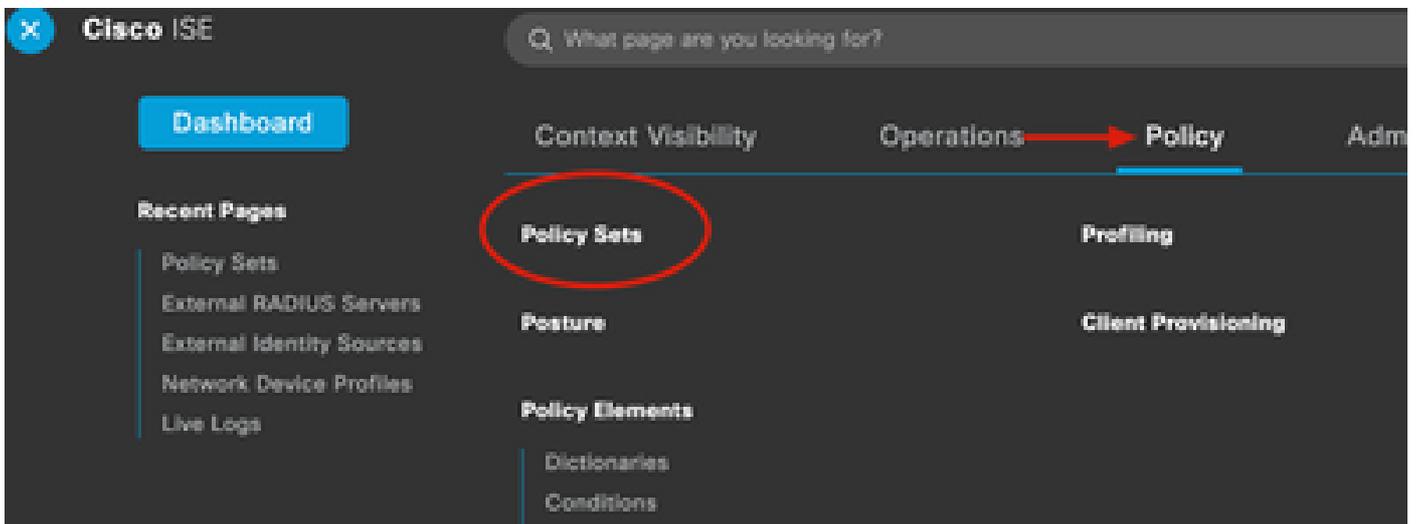
DUO\_NEW  
DUO\_Radius



Remote accounting

Local accounting

7. 從「控制面板」選單導航至策略，然後按一下策略集。



## 8.將RADIUS序列分配給預設策略。

 注意：在本文檔中，對所有連線應用Duo序列，因此使用預設策略。策略分配可能因要求而異。

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.在AAA伺服器組下配置ISE RADIUS伺服器，導航到Configuration，然後點選Device Management並展開Users/AAA部分，選擇AAA伺服器組。

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

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。