

為FMC管理訪問配置雙因素身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[身份驗證流程](#)

[驗證流程說明](#)

[設定](#)

[FMC的配置步驟](#)

[ISE的配置步驟](#)

[Duo Administration Portal的配置步驟](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹在Firepower管理中心(FMC)上為管理訪問配置外部雙因素身份驗證所需的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower管理中心(FMC)對象配置
- 身分識別服務引擎(ISE)管理

採用元件

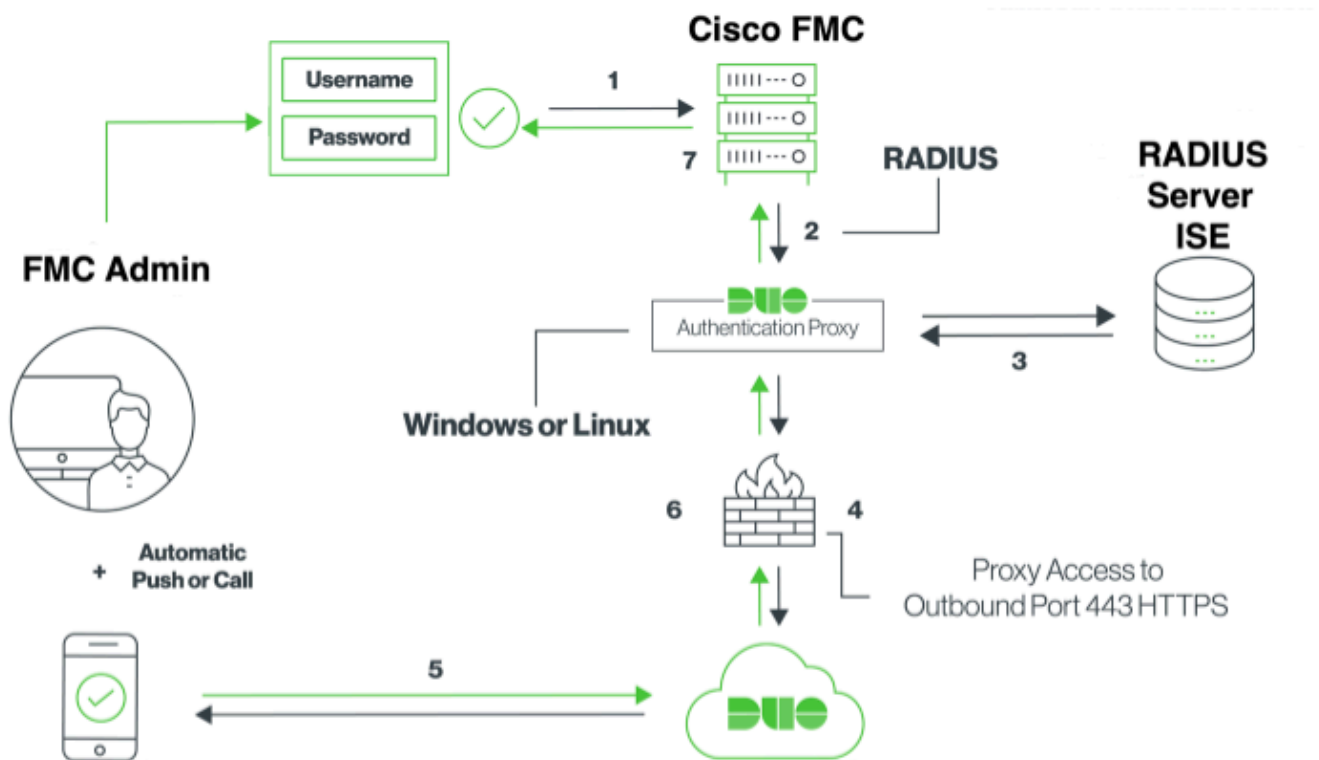
- 運行版本6.3.0的Cisco Firepower管理中心(FMC)
- 運行版本2.6.0.156的思科身份服務引擎(ISE)
- 支援版本的Windows(<https://duo.com/docs/authproxy-reference#new-proxy-install>)，可連線到FMC、ISE和Internet以充當Duo身份驗證代理伺服器
- Windows機器訪問FMC、ISE和Duo管理門戶
- Duo Web帳戶

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

FMC管理員根據ISE伺服器進行身份驗證，Duo Authentication Proxy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。

身份驗證流程



驗證流程說明

1. 主身份驗證已啟動到Cisco FMC。
2. Cisco FMC向Duo Authentication Proxy傳送驗證要求。
3. 主身份驗證必須使用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 authentication proxy接收身份驗證響應。
7. 已授予Cisco FMC GUI訪問許可權。

設定

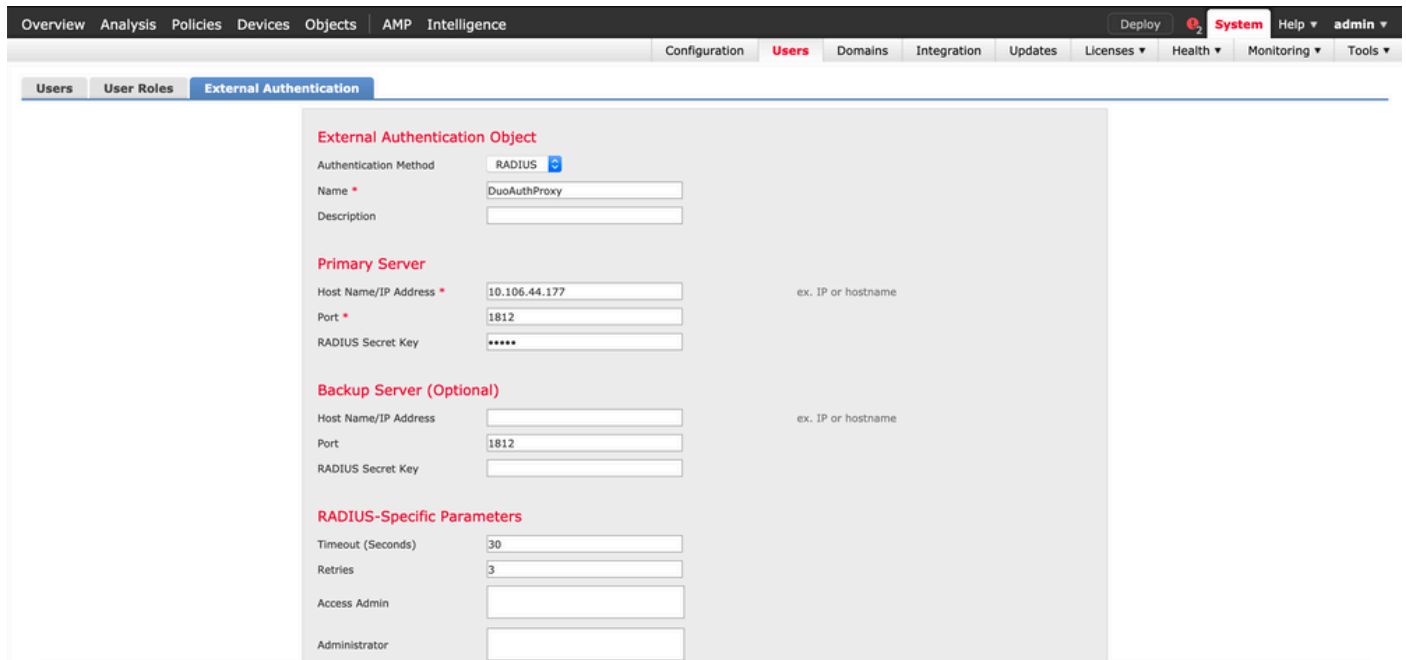
要完成配置，請考慮以下部分：

FMC的配置步驟

步驟 1. 導覽至System > Users > External Authentication。 建立外部身份驗證對象並將身份驗證方

法設定為RADIUS。確保在「Default User Role」下選擇了「Administrator」，如下圖所示：

 註:10.106.44.177是Duo Authentication Proxy伺服器的示例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

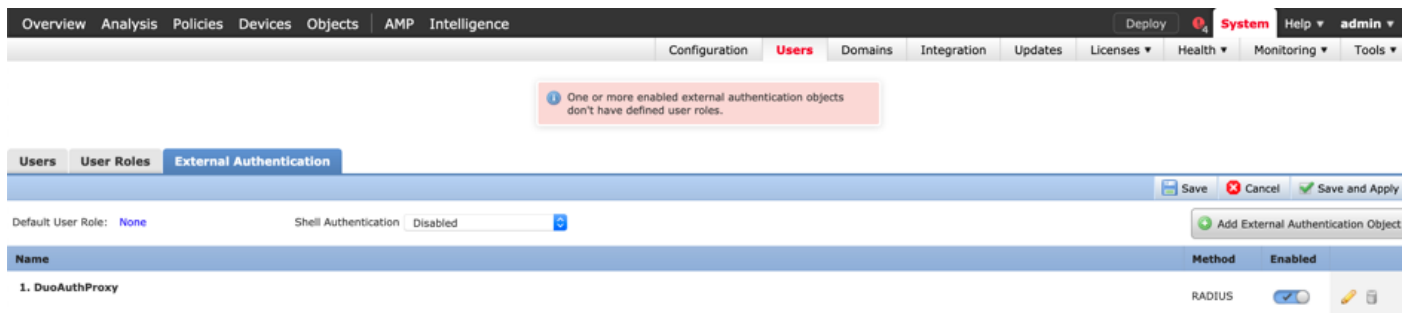
Timeout (Seconds): 30

Retries: 3

Access Admin:

Administrator:

按一下「Save」和「Apply」。忽略警告，如下圖所示：



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

Add External Authentication Object

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

步驟 2. 導航到System > Users > Users。建立使用者，並檢查外部的驗證方法，如下圖所示：

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

步驟 1. 下載並安裝 Duo Authentication Proxy Server。

登入到 Windows 機器並安裝 [Duo Authentication Proxy Server](#)


建議使用至少具有 1 CPU、200 MB 磁碟空間和 4 GB RAM 的系統



注意：此電腦必須能夠訪問 FMC、RADIUS 伺服器（在我們的情況下為 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

編輯authproxy.cfg檔案並新增以下配置：

```
<#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地址必須與RADIUS金鑰一起配置。

```
<#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=
```

確保配置ikey、skey和api_host引數。要獲取這些值，請登入您的Duo帳戶([Duo Admin Login](#))並導航至Applications > Protect an Application。接下來，選擇RADIUS驗證應用程式，如下圖所示：

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

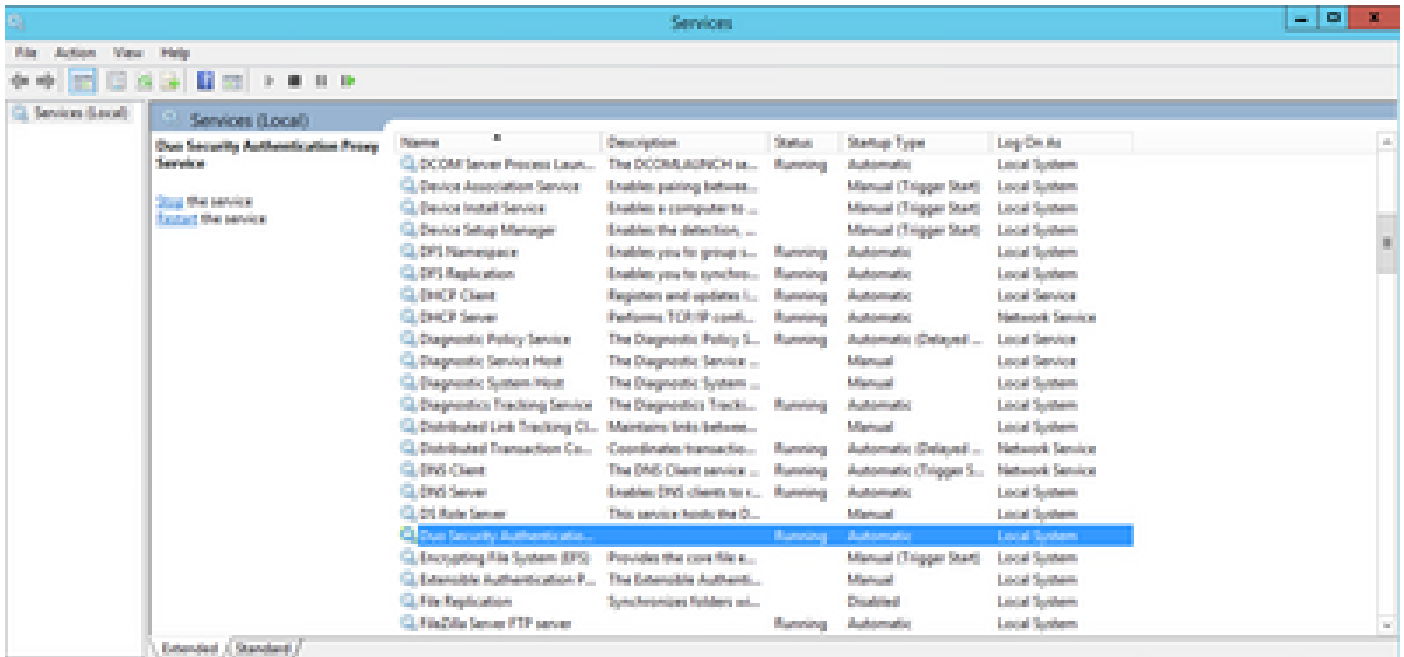
整合金鑰= ikey

secret key = skey

API主機名= api_host

步驟 3.重新啟動Duo Security身份驗證代理服務。儲存檔案並在Windows電腦上重新啟動Duo服務。

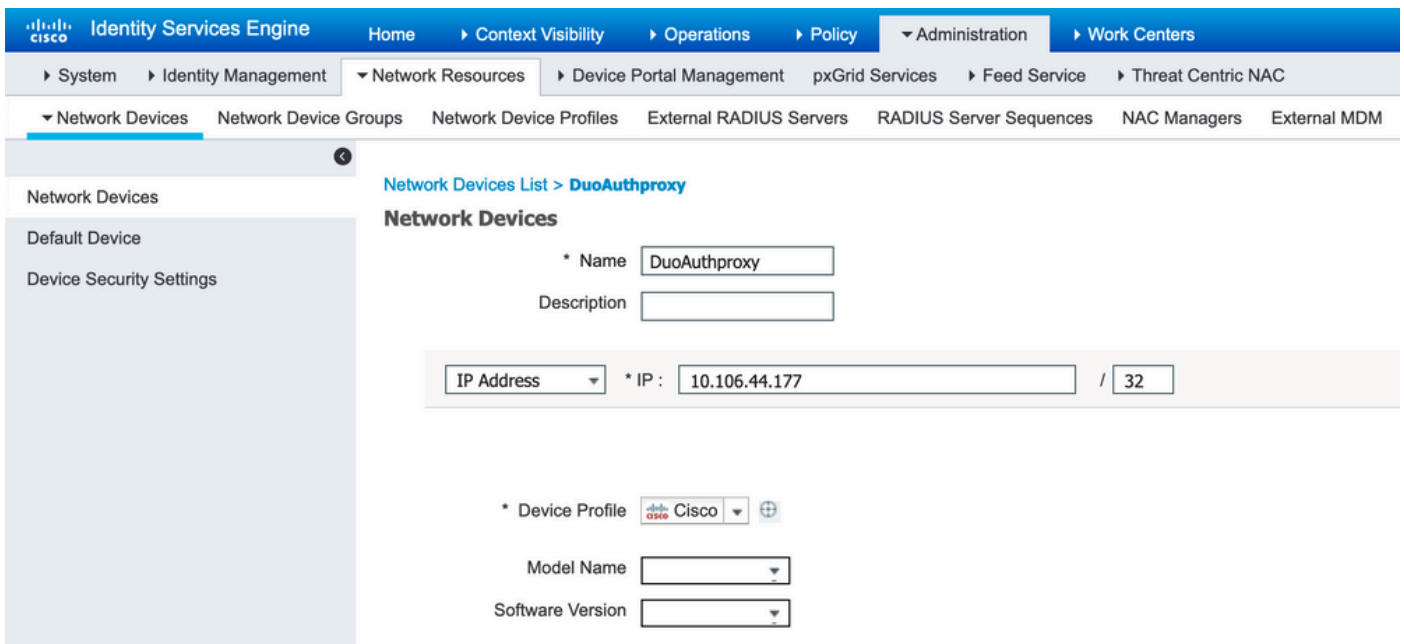
開啟Windows服務控制檯(services.msc)。在服務清單中找到Duo Security Authentication Proxy Service，然後按一下Restart，如下圖所示：



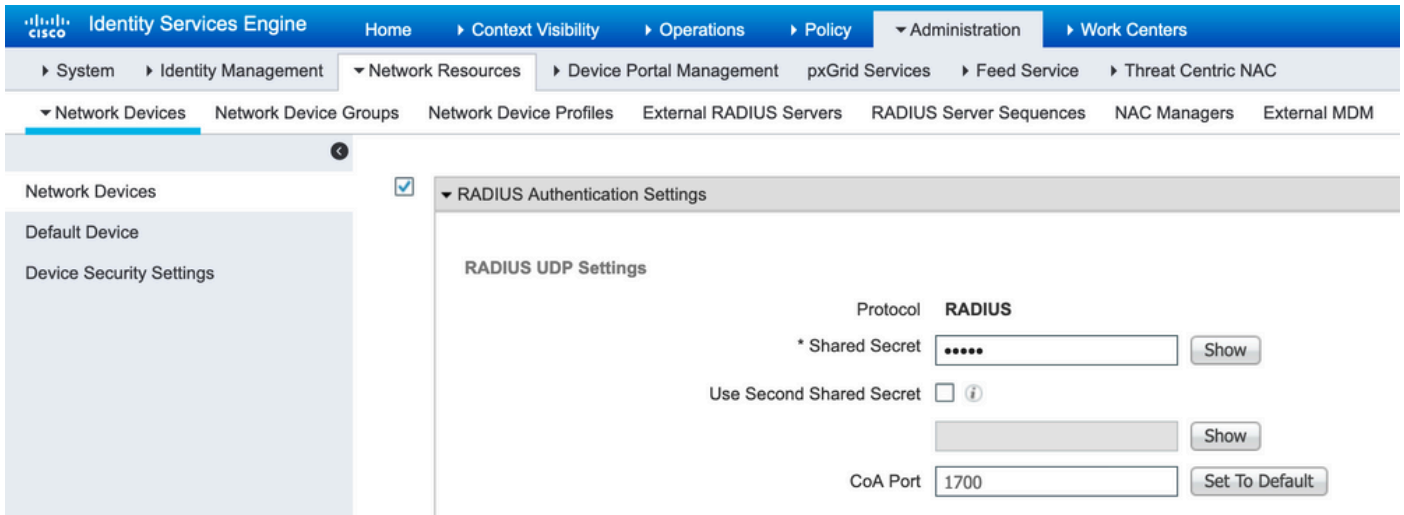
ISE的配置步驟

步驟 1. 導覽至Administration > Network Devices，按一下Add以設定網路裝置，如下圖所示：

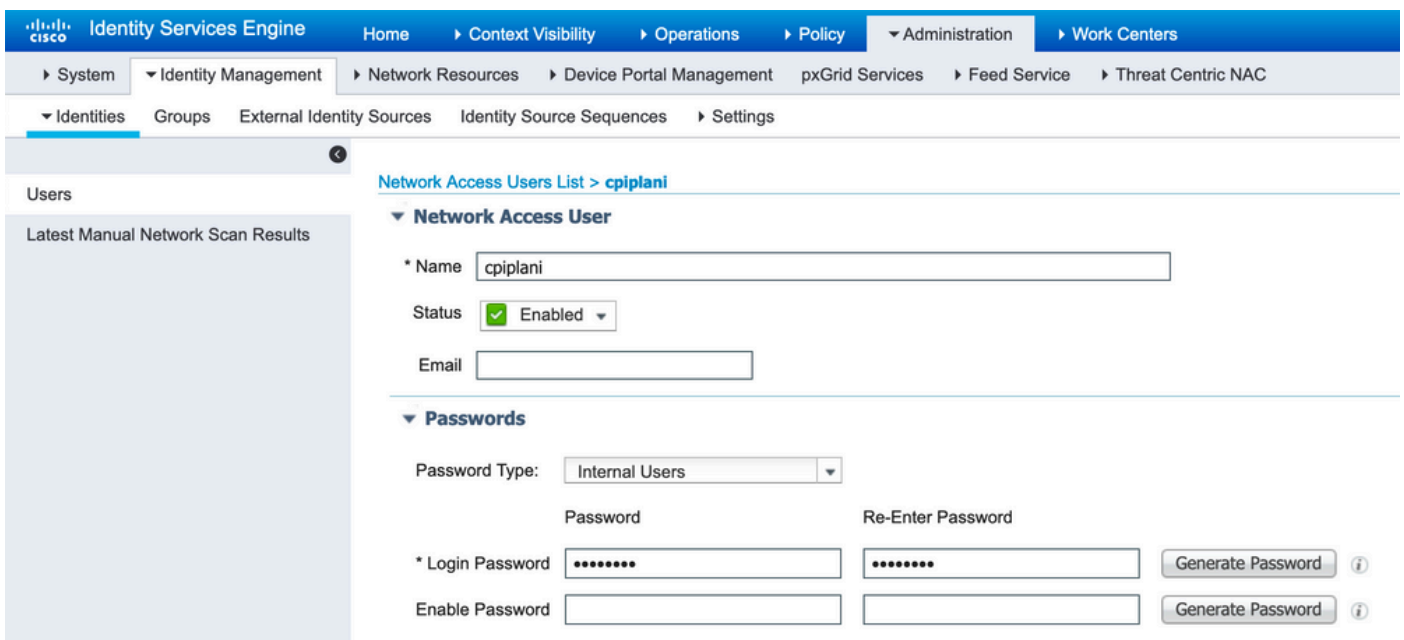
 註: 10.106.44.177是Duo Authentication Proxy伺服器的示例IP地址。



設定Shared Secret，如authproxy.cfg中的secret所述，如下圖所示：



步驟 2. 導航到Administration > Identities。按一下Add以設定Identity使用者，如下圖所示：



Duo Administration Portal的配置步驟

步驟 1. 建立使用者名稱並在終端裝置上啟用Duo Mobile。

在Duo雲管理網頁上新增使用者。導覽至Users > Add users，如下圖所示：

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：確保終端使用者安裝了Duo應用。

[手動安裝IOS裝置Duo應用程式](#)

[手動安裝用於Android裝置的Duo應用程式](#)

步驟 2. 代碼的自動生成。

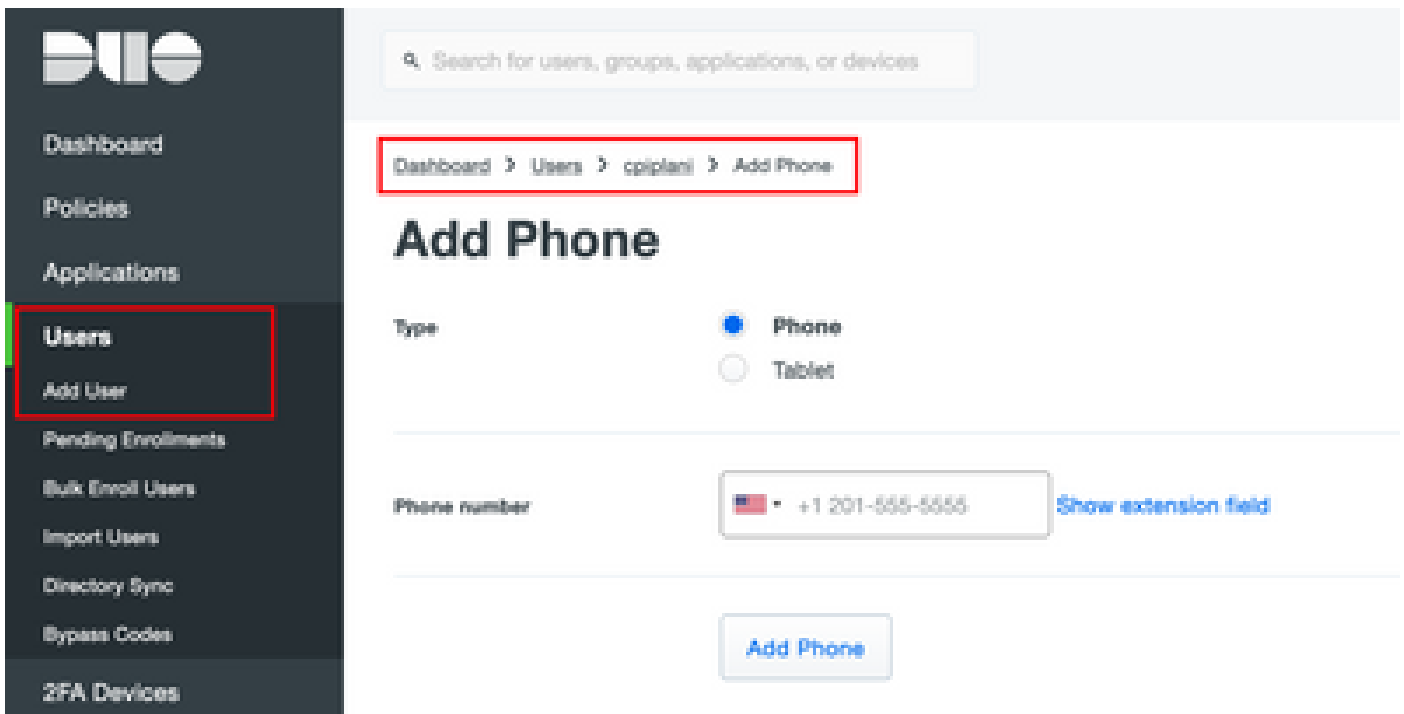
新增使用者的電話號碼，如下圖所示：

Add one.'"/>

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

[Add Phone](#)

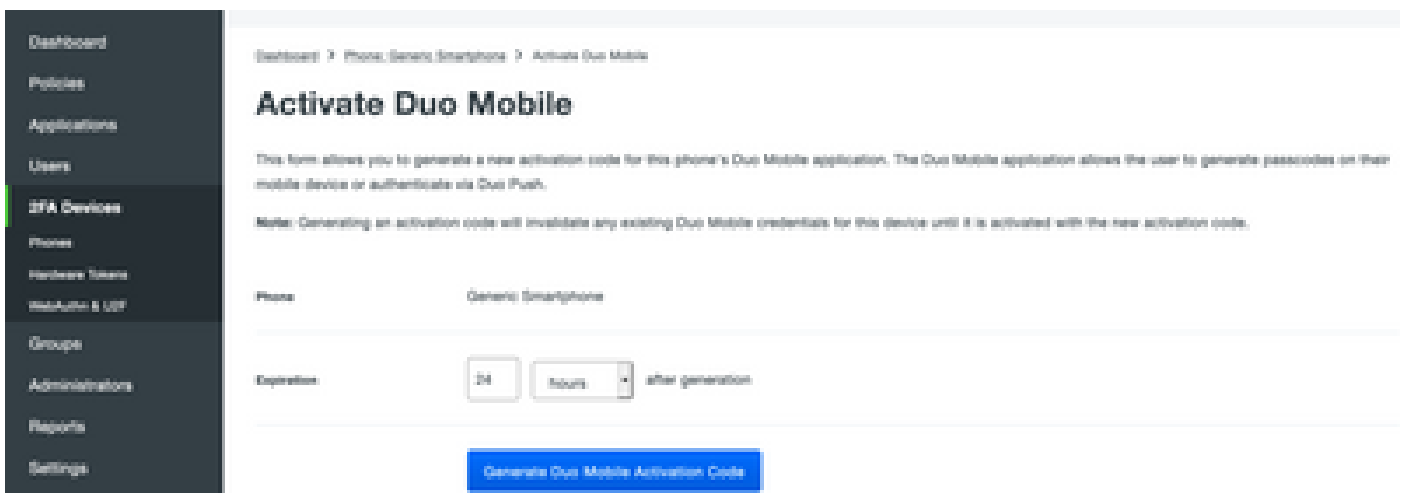
This user has no phones. [Add one.](#)



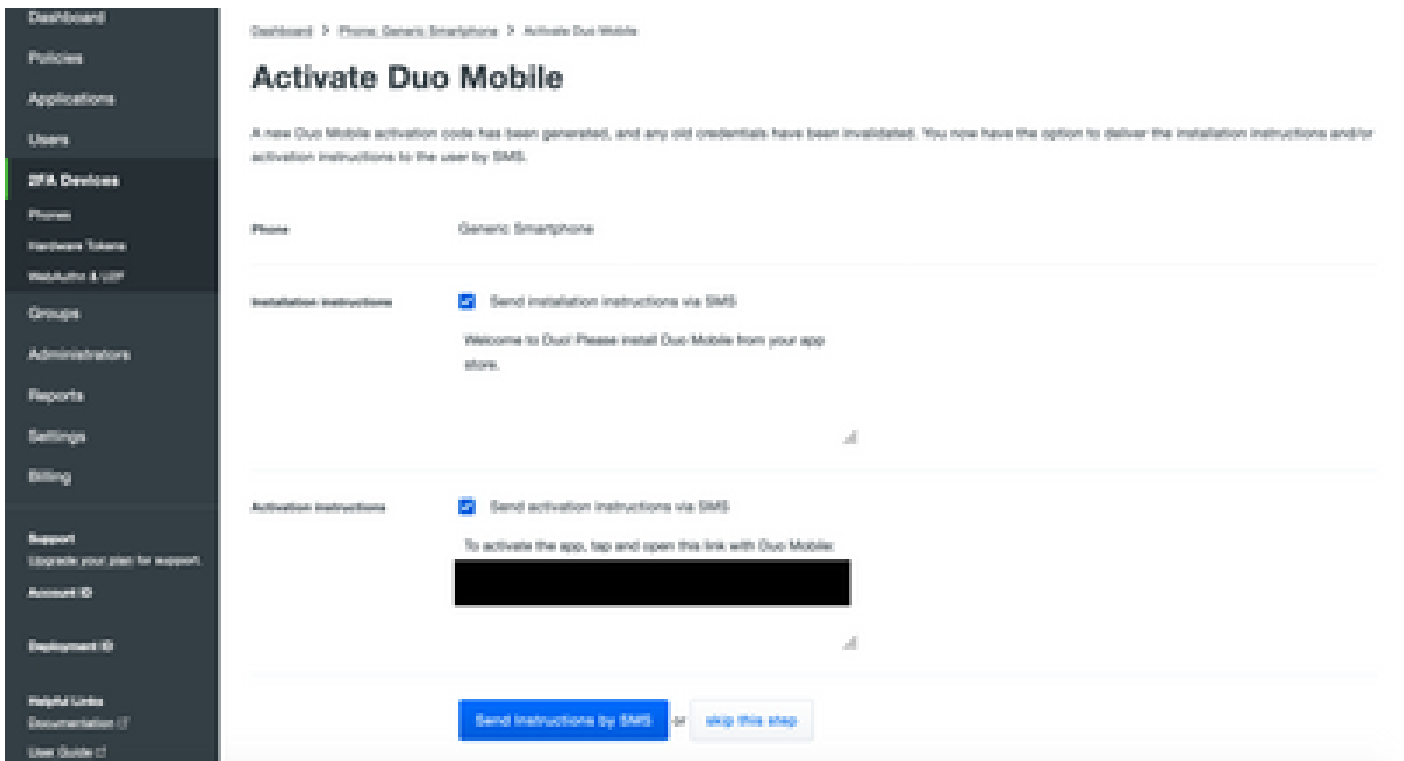
選擇Activate Duo Mobile，如下圖所示：



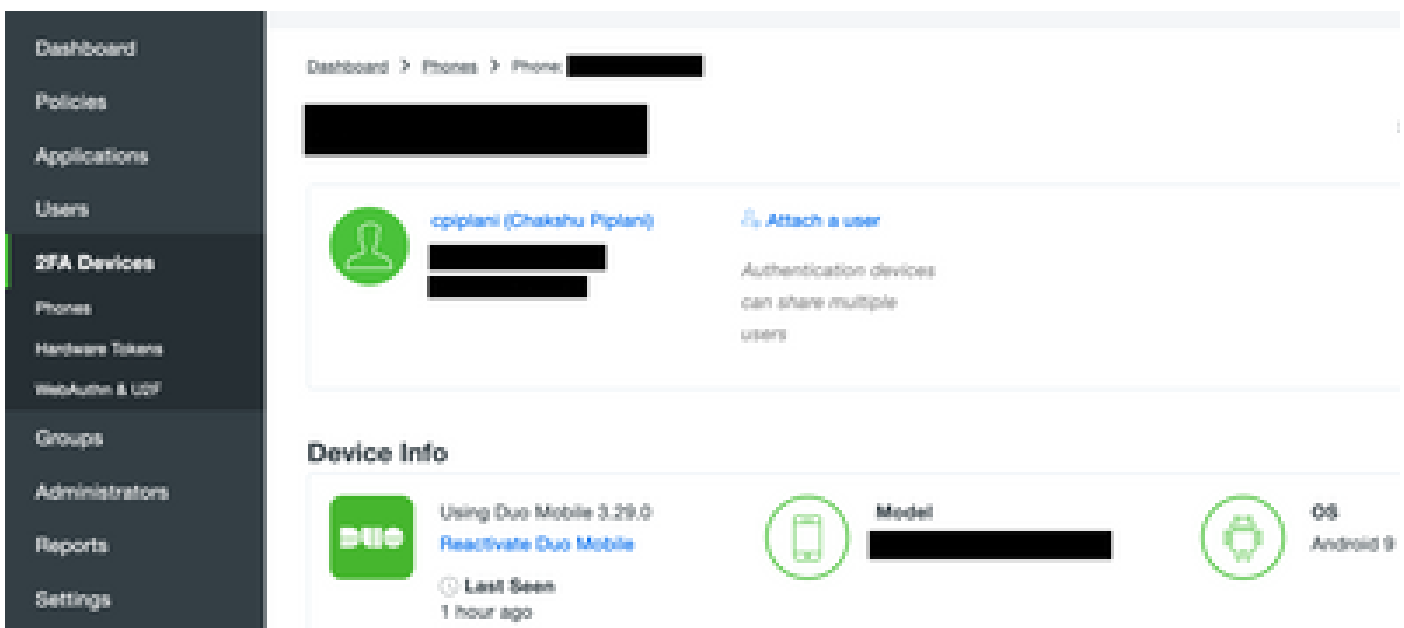
選擇Generate Duo Mobile Activation Code，如下圖所示：



選擇Send Instructions by SMS，如下圖所示：



單擊SMS中的連結，Duo應用將連結到「Device Info (裝置資訊)」部分中的使用者帳戶，如下圖所示：



驗證

使用本節內容，確認您的組態是否正常運作。

使用在ISE使用者身份頁面上新增的使用者憑據登入FMC。您必須在您的終端上獲取Duo PUSH通知以進行二元身份驗證(2FA)，請批准該通知，然後FMC將登入，如下圖所示：

Login Request



CISCO SYSTEMS



cpiplani



August 2, 2019, 7:37 PM



上用於身份驗證的使用者名稱，並選擇詳細列下的詳細身份驗證報告。在此處，必須驗證身份驗證是否成功，如下圖所示：

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". The main content area is divided into two primary sections: "Overview" and "Authentication Details".

Overview: This section provides a summary of the authentication event. It shows the event type as "5200 Authentication succeeded". The username is "cpiplani". The endpoint ID is blank. The authentication policy is "Default >> Default", and the authorization policy is "Default >> Basic_Authenticated_Access". The authorization result is "PermitAccess".

Authentication Details: This section provides more granular information about the authentication process. It shows the source and received timestamps as "2019-07-11 03:50:38.694". The policy server is "ROHAN-ISE". The event is "5200 Authentication succeeded". The username is "cpiplani", and the user type is "User". The authentication identity store is "Internal Users".

Steps: A list of 20 steps detailing the authentication process, such as "Received RADIUS Access-Request", "RADIUS created a new session", "Generated a new session ID", "Evaluating Policy Group", "Evaluating Service Selection Policy", "Evaluating Identity Policy", "Queried PIP - Normalised Radius.RadiusFlowType (4 times)", "Selected identity source sequence - All_User_ID_Stores", "Selected Identity Source - Internal Users", "Looking up User in Internal Users IDStore - cpiplani", "Found User in Internal Users IDStore", "Authentication Passed", "Evaluating Authorization Policy", "Queried PIP - Radius.NAS-Port-Type", "Queried PIP - Network Access.UserName", "Queried PIP - IdentityGroup.Name", "Queried PIP - EndPoints.LogicalProfile", "Queried PIP - Network Access.AuthenticationStatus", "Selected Authorization Profile - PermitAccess", "Max sessions policy passed", "New accounting session created in Session cache", and "Returned RADIUS Access-Accept".

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 檢查Duo Authentication Proxy伺服器上的調試。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。

當ISE伺服器輸入不正確的憑證並拒絕身份驗證時，記錄片段。

```
<#root>
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request from
```

```
10.197.223.76
```

```
to radius_server_auto
```

```
10.197.223.76 is the IP of the FMC
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Received new request id 4 from ('10.197.223.76', 34524)
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34524), 4):
```

```
login attempt for username u'cpiplani'
```

```
2019-08-04T18:54:17+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.76', 34524)
```

```
2019-08-04T18:54:17+0530 [RadiusClient (UDP)]
```

```
Got response
```

```
for id 199 from ('
```

10.197.223.23

', 1812);

code 3 10.197.223.23 is the IP of the ISE Server.

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Primary credentials reject

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4):

Returning response code 3: AccessReject

2019-08-04T18:54:17+0530 [RadiusClient (UDP)] (('10.197.223.76', 34524), 4): Sending response

- 在ISE上，導航到操作> RADIUS >即時日誌以驗證身份驗證詳細資訊。

使用ISE和Duo成功身份驗證的日誌片段：

<#root>

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request from

10.197.223.76

to radius_server_auto

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Received new request id 5 from ('10.197.223.76', 34095)

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] (('10.197.223.76', 34095), 5): login attempt for user

2019-08-04T18:56:16+0530 [DuoForwardServer (UDP)] Sending request for user u'cpiplani' to ('10.197.223.76', 34524)

2019-08-04T18:56:16+0530 [RadiusClient (UDP)] Got response for id 137 from ('10.197.223.23', 1812);

10.197.223.23

', 1812);

code 2 <<<< At this point we have got successful authentication from ISE Server.

2019-08-04T18:56:16+0530 [RadiusClient (UDP)] http POST to https://api-f754c261.duosecurity.com:443/res

2019-08-04T18:56:16+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPClientFactory

2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] Invalid ip. Ip was None

2019-08-04T18:56:17+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] http POST to https://api-f754c261.duosecurity.com:443/res

2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_DuoHTTPClientFactory

2019-08-04T18:56:17+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPClientFactory

2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

Duo authentication returned 'allow': 'Success. Logging you in...

,

2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

Returning response code 2: AccessAccept <<<< At this point, user has hit the approve button

2019-08-04T18:56:30+0530 [HTTPPageGetter (TLSMemoryBIOProtocol),client] (('10.197.223.76', 34095), 5):

2019-08-04T18:56:30+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_DuoHTTPClientFactory

相關資訊

- [使用Duo的RA VPN身份驗證](#)

- [技術支援與文件 - Cisco Systems](#)

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）。