

透過FTD、ISE、DUO和Active Directory配置SSL VPN身份驗證

目錄

[簡介](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[組態](#)

[FTD組態。](#)

[在Firepower管理中心\(FMC\)中整合RADIUS伺服器](#)

[配置遠端VPN。](#)

[ISE配置。](#)

[將DUO整合為外部Radius伺服器。](#)

[將FTD整合為網路存取裝置。](#)

[DUO配置。](#)

[DUO代理安裝。](#)

[將DUO Proxy與ISE和DUO Cloud整合。](#)

[將DUO與Active Directory整合。](#)

[透過DUO Cloud從Active Directory \(AD\)匯出使用者帳戶。](#)

[在Cisco DUO雲中註冊使用者。](#)

[配置驗證過程。](#)

[常見問題。](#)

[工作場景。](#)

[錯誤11353沒有其他外部RADIUS伺服器：無法執行故障切換](#)

[RADIUS會話不會出現在ISE即時日誌中。](#)

[其他疑難排解。](#)

簡介

本文檔介紹如何使用Cisco ISE和DUO Security for AAA在Firepower威脅防禦中整合SSLVPN。

需求

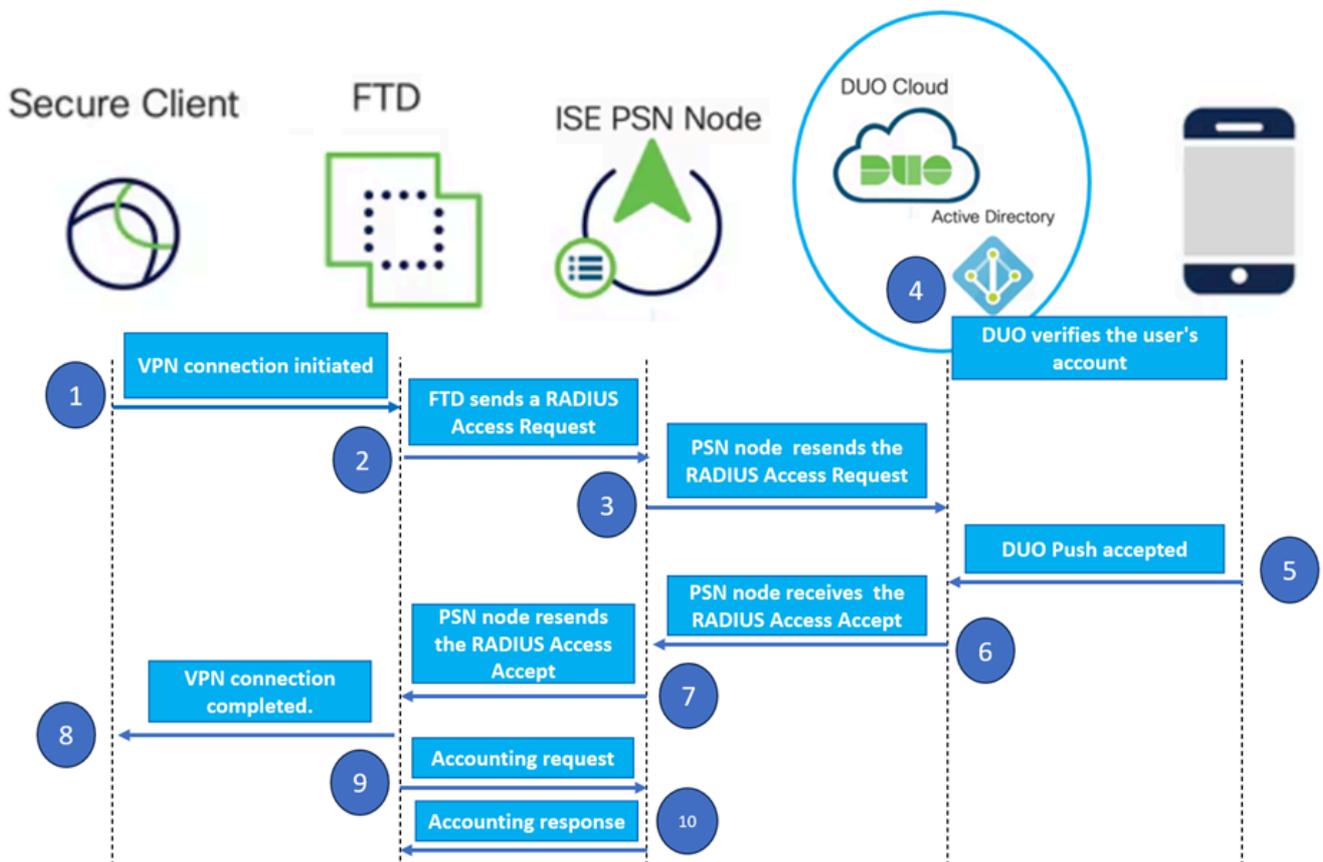
- ISE 3.0或更高版本。
- FMC 7.0或更高版本。
- FTD 7.0或更高版本。
- DUO驗證代理。
- ISE基礎版許可
- DUO Essentials授權。

採用元件

- ISE 3.2修補3
- FMC 7.2.5
- FTD 7.2.5
- Proxy DUO 6.3.0
- Any Connect 4.10.08029

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。

網路圖表



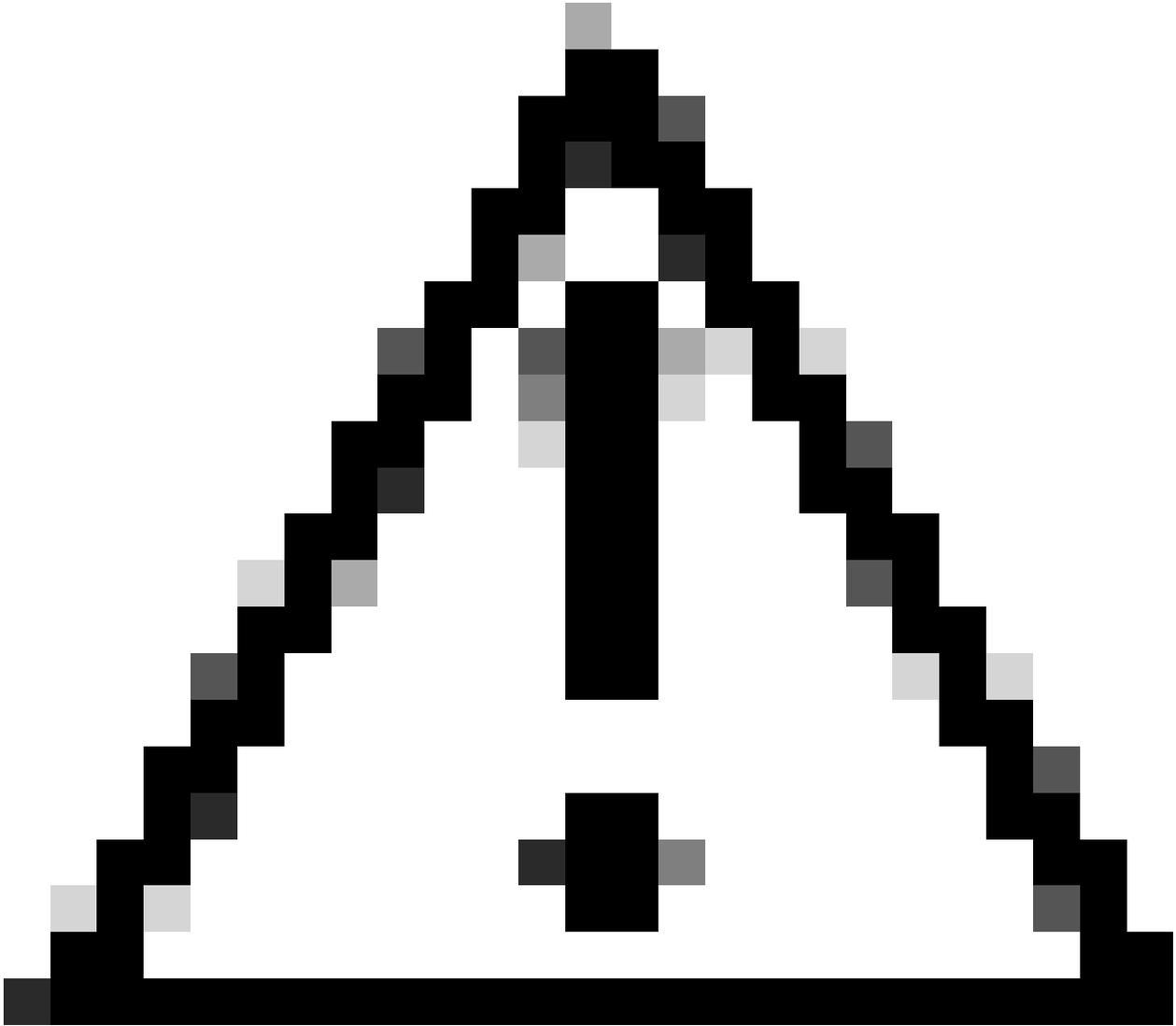
拓撲.

在我們推薦的解決方案中，思科ISE是重要的RADIUS伺服器代理。ISE配置為將RADIUS資料包從FTD轉發到DUO身份驗證代理，而不是直接評估身份驗證或授權策略。

DUO認證代理作為此認證流程中的專用中間體運行。它安裝在Windows伺服器上，可以彌合Cisco ISE和DUO雲之間的差距。代理主要功能是將身份驗證請求 (封裝在RADIUS資料包中) 傳輸到DUO雲。DUO Cloud最終基於雙因素身份驗證配置允許或拒絕網路訪問。

1. 使用者透過輸入其唯一使用者名稱和密碼啟動VPN身份驗證過程。
2. 防火牆威脅防禦(FTD)將身份驗證請求傳送到思科身份服務引擎(ISE)。

3. 策略服務節點(PSN)將身份驗證請求轉發到DUO身份驗證代理伺服器。隨後，DUO認證伺服器透過DUO雲服務驗證憑證。
4. DUO Cloud根據同步資料庫驗證使用者名稱和密碼。

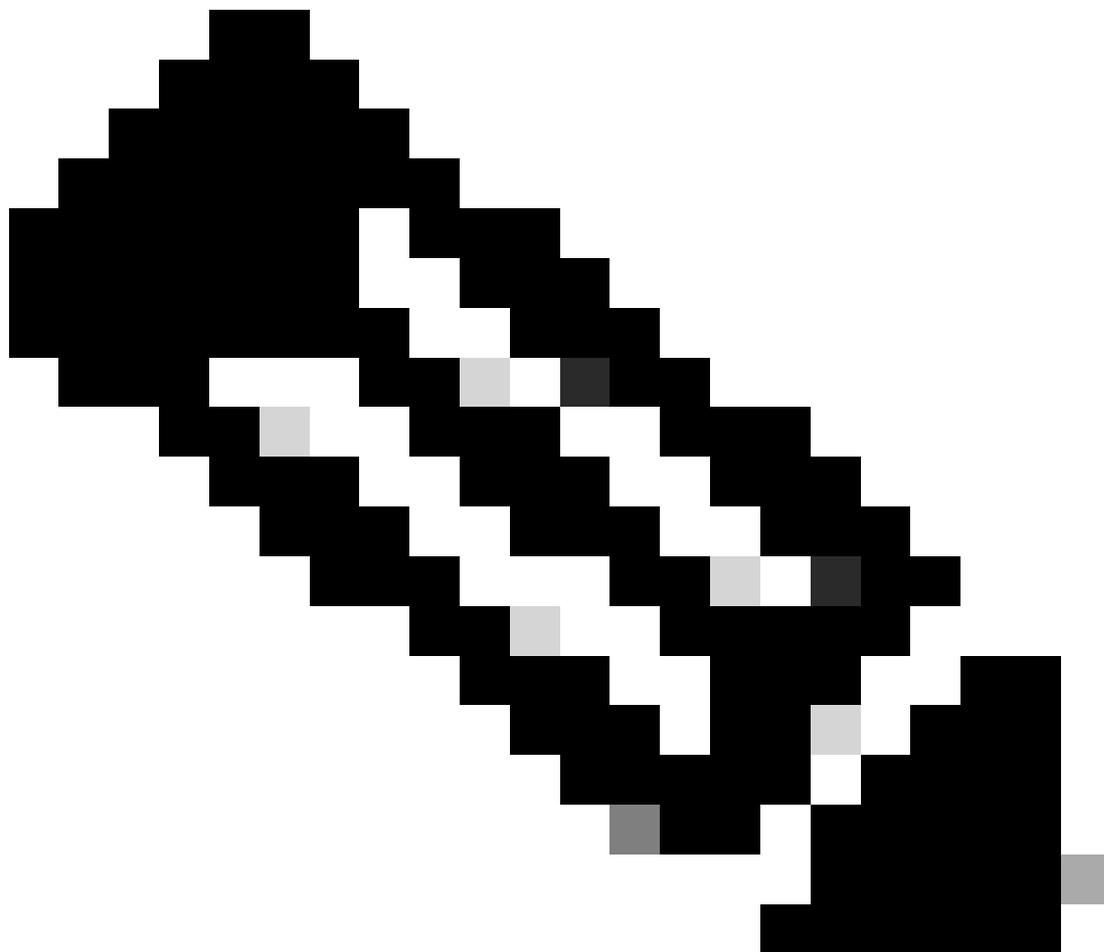


注意：DUO Cloud與組織Active Directory之間的同步需要處於活動狀態，以維護DUO Cloud中的最新使用者資料庫。

5. 身份驗證成功後，DUO Cloud透過安全、加密的推送通知向註冊流動裝置的使用者啟動DUO Push。然後，使用者必須批准DUO Push以確認其身份並繼續。
6. 一旦使用者核准DUO Push，DUO Authentication Proxy伺服器就會傳回確認訊息給PSN，表示使用者已接受驗證請求。
7. PSN節點會傳送確認訊息給FTD，通知使用者已經透過驗證。
8. FTD收到驗證確認訊息，並在採取適當安全措施的情況下與終端建立VPN連線。

9. FTD會記錄成功的VPN連線的詳細資訊，並將會計資料安全傳輸回ISE節點，以進行記錄儲存及稽核。

10. ISE節點將會計資訊記錄在其即時日誌中，確保所有記錄都安全地儲存並可訪問以便將來進行審計或合規檢查。



附註：

本指南中的設定使用以下網路引數：

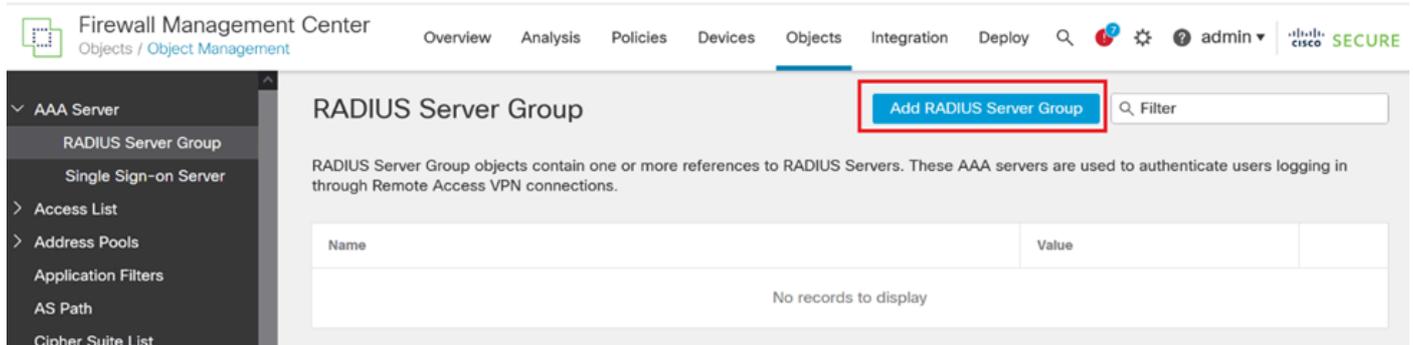
- 主要網路伺服器(PNS)節點IP：10.4.23.21
- 對等VPN的Firepower威脅防禦(FTD) IP：10.4.23.53
- DUO驗證代理IP：10.31.126.207
- 域名：testlab.local

組態

FTD組態。

在Firepower管理中心(FMC)中整合RADIUS伺服器

1. 啟動Web瀏覽器並輸入FMC的IP地址以打開圖形使用者介面(GUI)，從而訪問FMC。
2. 導航到對象選單，選擇AAA伺服器，然後繼續執行RADIUS伺服器組選項。
3. 按一下Add RADIUS Server Group按鈕為RADIUS伺服器建立新組。



RADIUS伺服器組。

4. 輸入新「AAA RADIUS伺服器群組」的描述性名稱，以確保您的網路基礎架構中有清楚的辨識。
5. 在組配置中選擇適當的選項，繼續增加新的RADIUS伺服器。

RADIUS Servers (Maximum 16 servers)

| IP Address/Hostname |
|-----------------------|
| No records to display |

A red box highlights a plus sign (+) icon in the top right corner of the table area.

RADIUS伺服器。

6. 指定RADIUS伺服器IP地址並輸入共用金鑰。



注意：必須確保與ISE伺服器安全共用此金鑰以成功建立RADIUS連線。

New RADIUS Server



IP Address/Hostname:*

10.4.23.21

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535)

1812

Key:*

●●●●●●●●

Confirm Key:*

●●●●●●●●

Accounting Port: (1-65535)

1813

Timeout: (1-300) Seconds

10

Connect using:

Routing Specific Interface 

Cancel

Save

新建RADIUS伺服器。

7. 在配置RADIUS伺服器詳細資訊之後，按一下Save以保留RADIUS伺服器組的設定。

Add RADIUS Server Group



Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

Port:* (1024-65535)

1700

RADIUS Servers (Maximum 16 servers)



IP Address/Hostname

10.4.23.21



Cancel

Save

伺服器組詳細資訊。

8. 要在整個網路中完成並實施AAA伺服器配置，請導航到部署選單，然後選擇全部部署以應用設定。

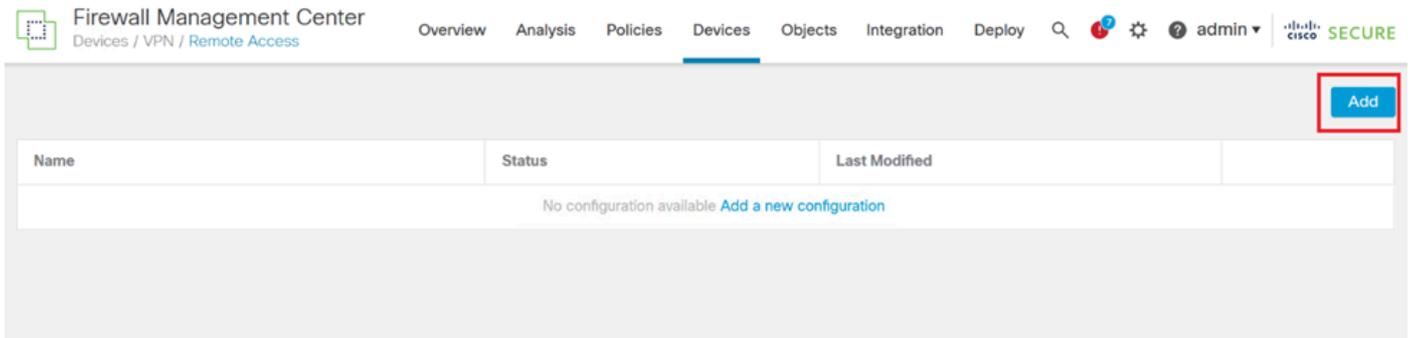
o

The screenshot shows the 'Firewall Management Center' interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', and 'Deploy'. The 'Deploy' button is highlighted with a red box. Below the navigation bar, the left sidebar shows a tree view with 'AAA Server' expanded, and 'RADIUS Server Group' selected. The main content area displays the 'RADIUS Server Group' configuration page, which includes a search bar, a table with one entry 'FTD_01' in 'Ready for Deployment' status, and two buttons: 'Advanced Deploy' and 'Deploy All'. The 'Deploy All' button is highlighted with a red box.

部署AAA伺服器。

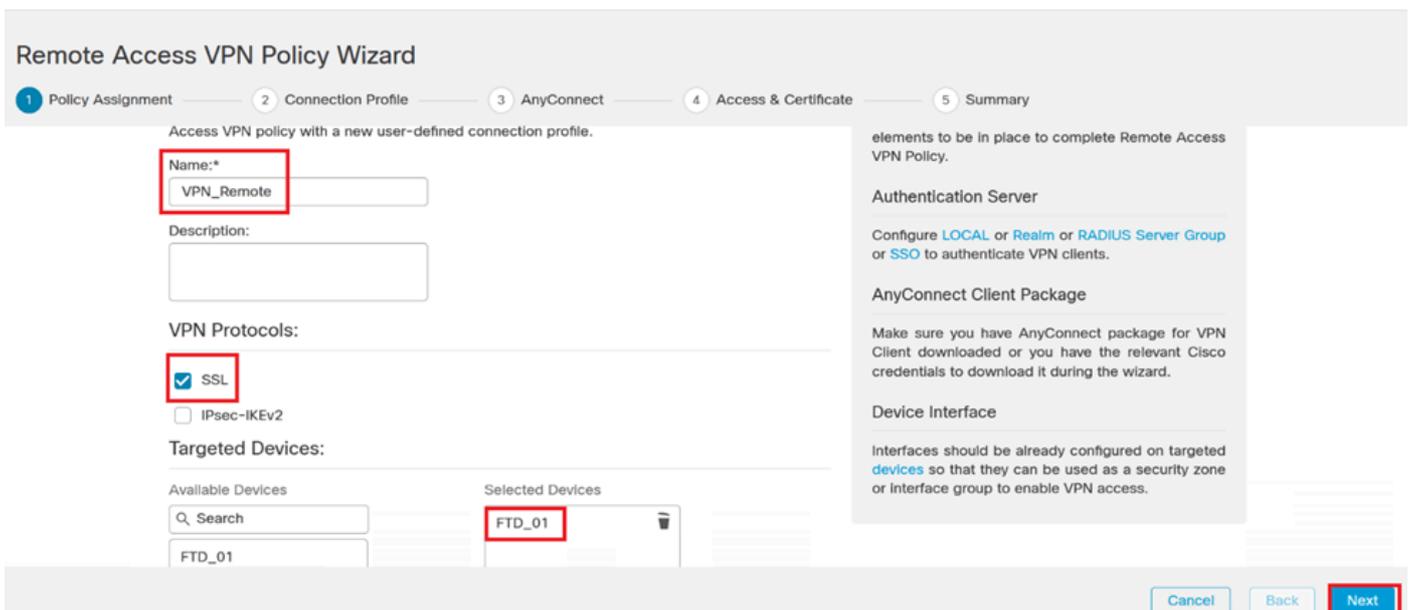
配置遠端VPN。

1. 在FMC GUI中導航到Devices > VPN > Remote Access，開始VPN配置過程。
2. 按一下Add按鈕建立新的VPN連線配置檔案。



VPN連線配置檔案。

3. 輸入VPN的唯一描述性名稱，以便在您的網路設定中辨識它。
4. 選擇SSL選項以確保使用SSL VPN協定的安全連線。
5. 從裝置清單中，選取特定的FTD裝置。



VPN設定。

6. 將AAA方法配置為使用身份驗證設定中的PSN節點。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: **AAA Only** ▼

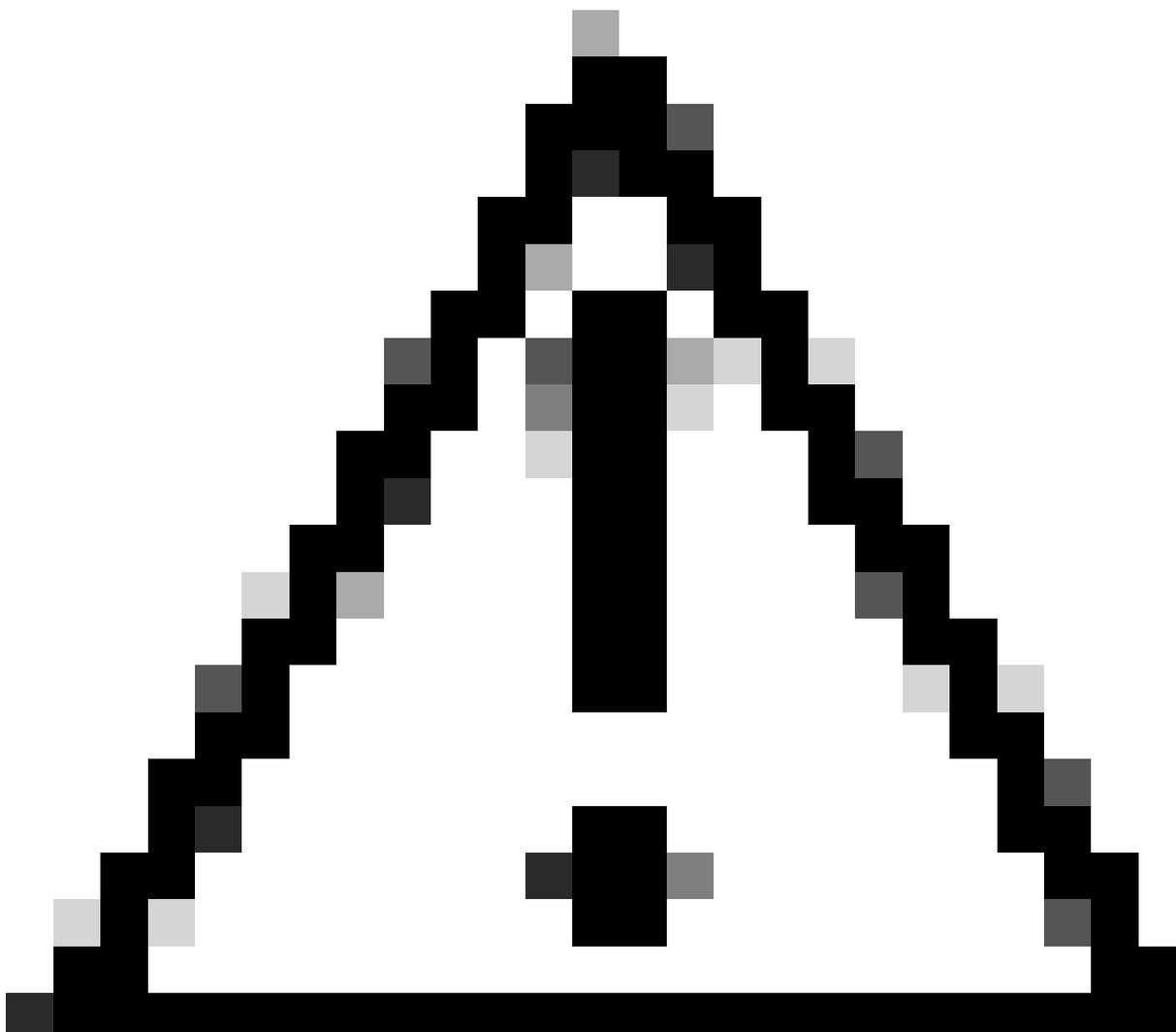
Authentication Server:* **ISE** ▼ +
(LOCAL or Realm or RADIUS)
 Fallback to LOCAL Authentication

Authorization Server: **Use same authentication server** ▼ +
(realm or RADIUS)

Accounting Server: **ISE** ▼ +
(RADIUS)

連線配置檔案。

7. 為VPN設定動態IP地址分配。



注意：例如，已選擇DHCP VPN池。

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: ⓘ

IPv6 Address Pools: ⓘ

IP地址池。

8. 繼續建立新的群組原則。

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* 

[Edit Group Policy](#)

組策略。

9. 在組策略設定中，確保選擇SSL協定。

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

VPN Tunnel Protocol:

Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

Cancel

Save

VPN協定。

10. 建立新的VPN池或選擇現有池以定義可用於VPN客戶端的IP地址範圍。

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IP Address Pools:



Name

IP Address Range

Cancel

Save

池VPN。

11. 指定VPN連線的DNS伺服器詳細資訊。

Add Group Policy



Name:*

VPN_Remote_Policy

Description:

General

AnyConnect

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

Primary DNS Server:

+

Secondary DNS Server:

+

Primary WINS Server:

+

Secondary WINS Server:

+

DHCP Network Scope:

+

Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

Cancel

Save

DNS設定。



警告：請注意，對於此配置，其他功能（如Banner、Split Tunneling、AnyConnect和Advanced選項）被視為可選的。

12. 配置完必要的詳細資訊後，按一下下一步繼續下一步的設定。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

optional, if address assignment is used on the client or VPN server, either server side or address pool.

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:*

[Edit Group Policy](#)

Cancel

Back

Next

組策略。

13. 為VPN使用者選擇適當的AnyConnect軟體套件。如果未列出所需的包，您可以選擇在此階段增加所需的包。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from [Cisco Software Download Center](#).

Select at least one AnyConnect Client image

[Show Re-order buttons](#)

| <input type="checkbox"/> | AnyConnect File Object Name | AnyConnect Client Package Name | Operating System |
|--------------------------|---------------------------------|---|------------------|
| <input type="checkbox"/> | anyconnect-win-4.10.08029-we... | anyconnect-win-4.10.08029-webdeploy-k9... | Windows |

Cancel

Back

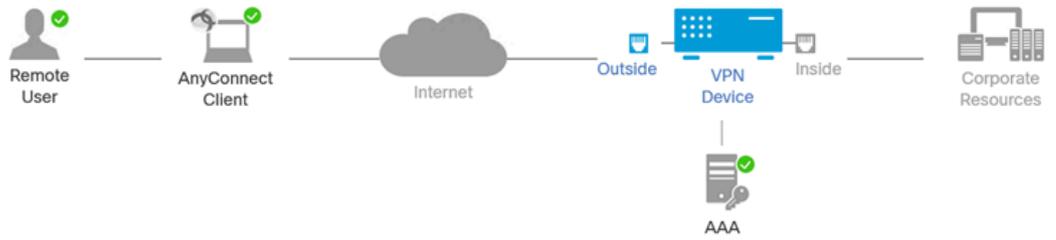
Next

套件安裝。

14. 選擇要啟用VPN Remote功能的FTD裝置上的網路介面。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

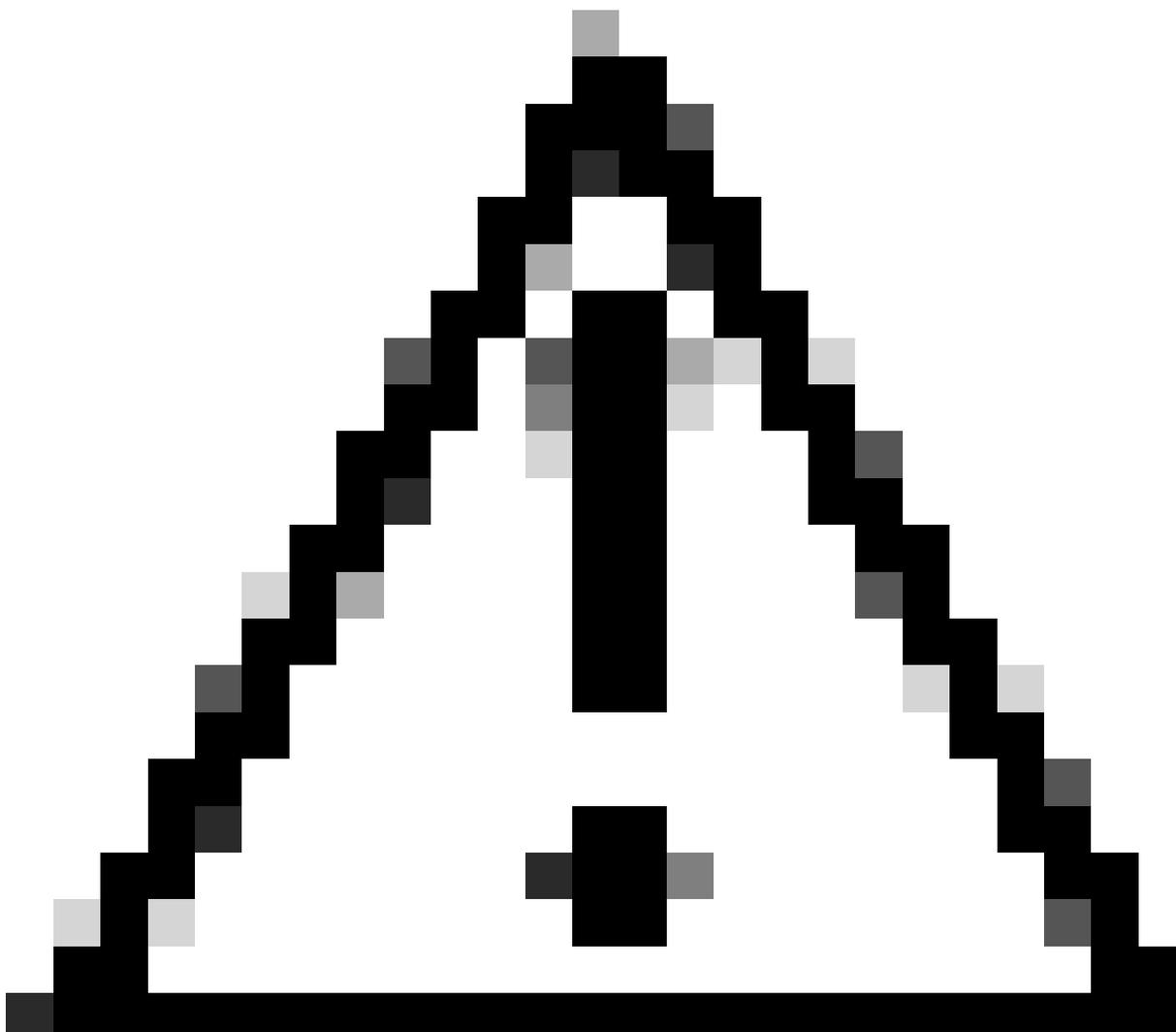
Interface group/Security Zone:* +

Enable DTLS on member interfaces

⚠ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

VPN介面

15. 透過選擇可用方法之一在防火牆上建立並安裝證書，建立證書註冊過程，這對於安全VPN連線至關重要。



注意：例如，本指南中選擇了一個自簽名證書。

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:*

 +

裝置證書。

Add Cert Enrollment



Name*

Description

CA Information

Certificate Parameters

Key

Revocation

Enrollment Type:

SCEP

Enrollment URL:*

Self Signed Certificate

EST

Challenge Password:

SCEP

Confirm Password:

Manual

PKCS12 File

Retry Period:

1 (Range 1-60)

Retry Count:

10

(Range 0-100)

Fingerprint:

Cancel

Save

證書註冊。

16. 配置證書註冊後，按一下Next。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

will access the VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Cancel

Back

Next

訪問和服務摘要

17. 複查所有組態的彙總，確保這些組態正確無誤，並反映您預期的設定。

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 AnyConnect — 4 Access & Certificate — 5 Summary

Firepower Management Center will configure an RA VPN Policy with the following settings

| | |
|------------------------|--|
| Name: | VPN_Remote |
| Device Targets: | FTD_01 |
| Connection Profile: | VPN_Remote |
| Connection Alias: | VPN_Remote |
| AAA: | |
| Authentication Method: | AAA Only |
| Authentication Server: | ISE (RADIUS) |
| Authorization Server: | ISE (RADIUS) |
| Accounting Server: | ISE |
| Address Assignment: | |
| Address from AAA: | - |
| DHCP Servers: | - |
| Address Pools (IPv4): | Pool_VPN |
| Address Pools (IPv6): | - |
| Group Policy: | VPN_Remote_Policy |
| AnyConnect Images: | anyconnect-win-4.10.08029-webdeploy-k9.pkg |
| Interface Objects: | Outside |
| Device Certificates: | Cert_Enrollment |

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

Access Control Policy Update

An **Access Control** rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption

If NAT is enabled on the targeted devices, you must define a **NAT Policy** to exempt VPN traffic.

DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using **FlexConfig Policy** on the targeted devices.

Port Configuration

SSL will be enabled on port 443. Please ensure that these ports are not used in **NAT Policy** or other services before deploying the configuration.

Network Interface Configuration

Make sure to add interface from targeted

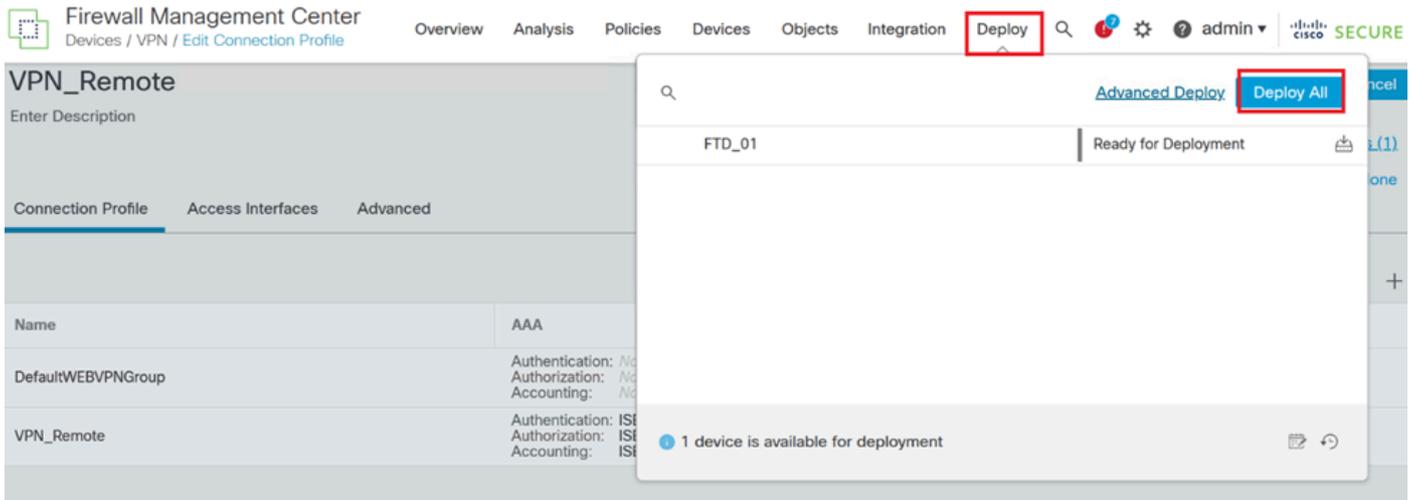
Cancel

Back

Finish

VPN設定的摘要。

18. 要應用和啟用VPN遠端訪問配置，請導航到Deploy > Deploy All，然後執行部署到所選FTD裝置的部署。



部署VPN設定。

ISE配置。

將DUO整合為外部Radius伺服器。

1. 在Cisco ISE管理介面中導航到Administration > Network Resources > External RADIUS Servers。
2. 按一下Add按鈕配置新的外部RADIUS伺服器。

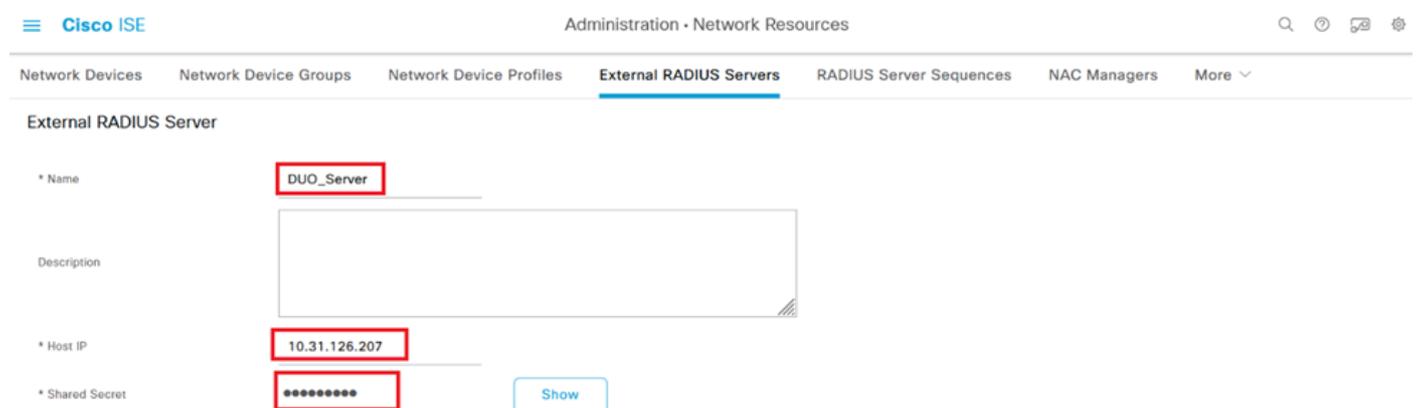


外部Radius伺服器

3. 輸入Proxy DUO伺服器的名稱。
4. 輸入Proxy DUO伺服器的正確IP位址，以確保ISE與DUO伺服器之間的正確通訊。
5. 設定共用金鑰。

注意：必須在Proxy DUO伺服器中配置此共用金鑰，以便成功建立RADIUS連線。

6. 正確輸入所有詳細資訊後，按一下**Submit**儲存新的Proxy DUO Server配置。



The screenshot shows the Cisco ISE Administration interface for configuring an External RADIUS Server. The breadcrumb path is Administration > Network Resources > External RADIUS Servers. The form fields are as follows:

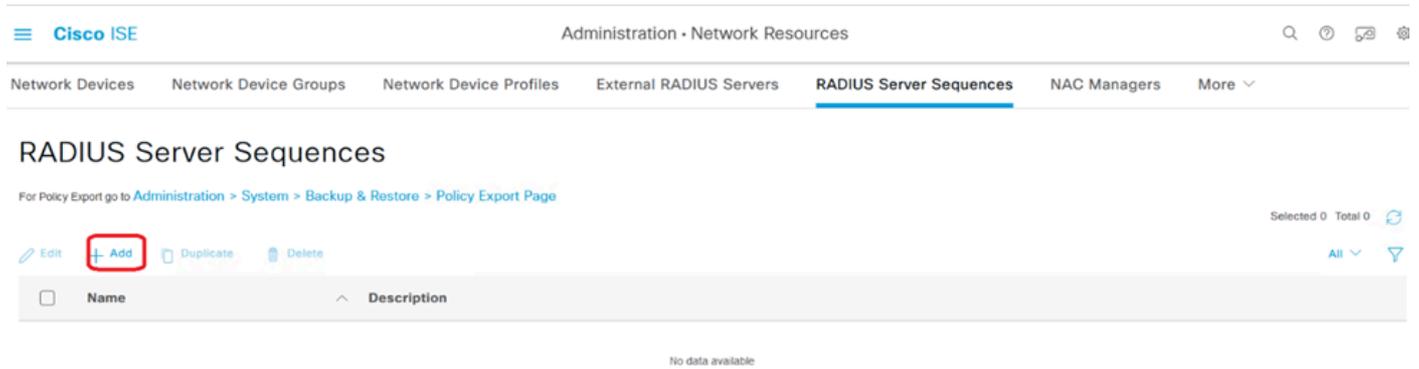
| Field | Value |
|-----------------|---------------|
| * Name | DUO_Server |
| Description | |
| * Host IP | 10.31.126.207 |
| * Shared Secret | ***** |

A "Show" button is located next to the Shared Secret field.

外部RADIUS伺服器

7. 繼續執行管理 > RADIUS伺服器序列。

8. 按一下Add建立新的RADIUS伺服器序列。

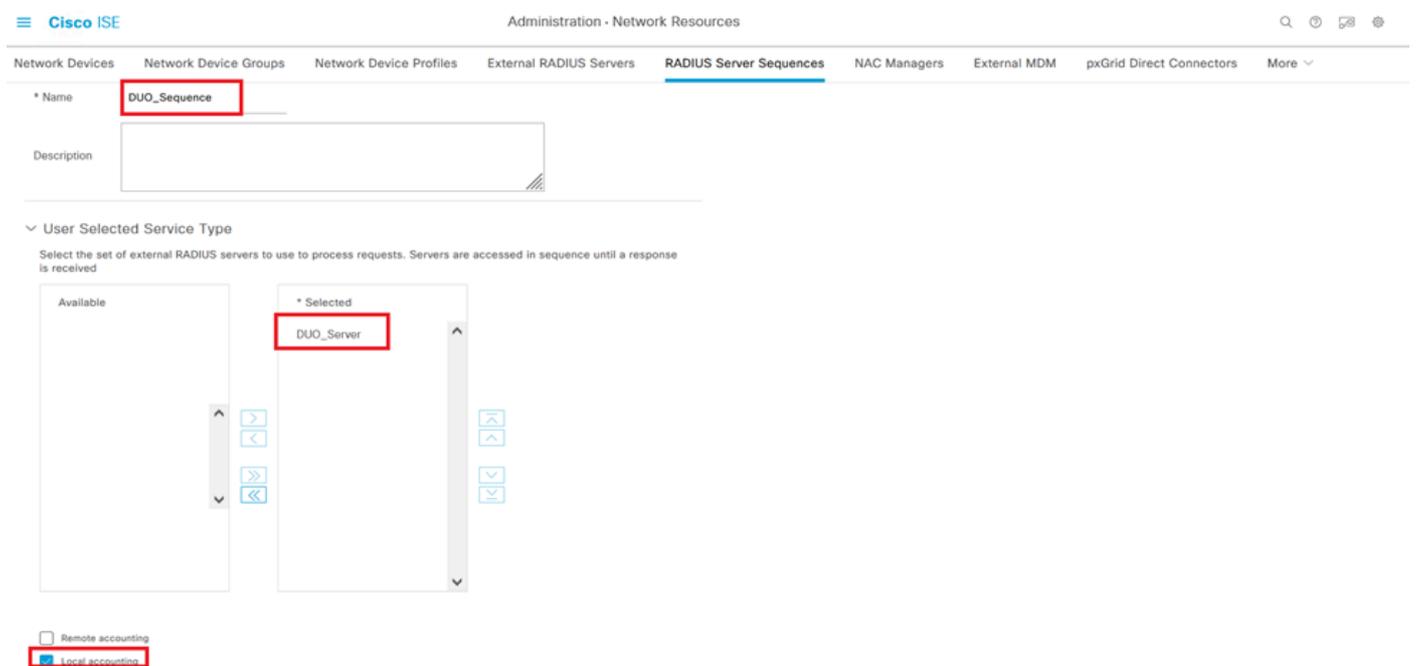


RADIUS伺服器序列

9. 為RADIUS伺服器序列提供一個不同的名稱以便於辨識。

10. 找到之前配置的DUO RADIUS伺服器(在本指南中稱為DUO_Server)，並將其移動到右側的選定清單中以將它包含在序列中。

11. 按一下Submit以完成並儲存RADIUS Server Sequence配置。



Radius伺服器序列配置。

將FTD整合為網路存取裝置。

1. 導航到系統介面中的管理部分，然後從該部分選擇網路資源以訪問網路裝置的配置區域。

2. 進入網路資源部分後，找到並點選增加按鈕以啟動增加新網路訪問裝置的過程。

Network Devices

Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers More ▾

Network Devices

Default Device

Device Security Settings

Network Devices

Selected 0 Total 0

ⓘ + Add Duplicate Import Export ▾ Generate PAC Delete ▾ All ▾

| <input type="checkbox"/> | Name | IP/Mask | Profile Name | Location | Type | Description |
|--------------------------|------|---------|--------------|----------|------|-------------|
| No data available | | | | | | |

網路訪問裝置。

3. 在所提供的欄位中，輸入「網路存取裝置」名稱，以辨識網路內的裝置。
4. 繼續指定FTD（Firepower威脅防禦）裝置的IP地址。
5. 輸入之前在FMC（Firepower管理中心）設定期間建立的金鑰。此金鑰對於裝置之間的安全通訊至關重要。
6. 按一下「提交」按鈕，完成處理。

Network Devices List > FTD

Network Devices

Name **FTD**

Description

IP Address ▾ * IP : **10.4.23.53** / **32** ⚙

將FTD新增為需求。

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret

●●●●●●●●

Show

Use Second Shared Secret ⓘ

Second Shared Secret

Show

CoA Port **1700**

Set To Default

RADIUS設定

DUO配置。

DUO代理安裝。

按一下下一個連結，訪問DUO Proxy下載和安裝指南：

<https://duo.com/docs/authproxy-reference>

將DUO Proxy與ISE和DUO Cloud整合。

1. 使用您的憑證登入DUO Security網站<https://duo.com/>。

2. 定位至申請部分，然後選擇保護申請以繼續。

Dashboard > Applications

Applications

Protect an Application

Manage your update to the new Universal Prompt experience, all in one place.

See My Progress Get More Information ⓘ

0 All Applications **0** End of Support

Export Search

3. 在清單中搜尋「Cisco ISE RADIUS」選項並按一下Protect以將其增加到您的應用。

The screenshot shows the Duo Applications management interface. On the left is a navigation menu with 'Applications' selected. The main content area has a search bar containing 'Cisco ISE RADIUS'. Below the search bar is a table of applications:

| Application | Protection Type | Documentation | Action |
|------------------------------------|---|-------------------------------|---------------------------|
| Cisco ISE Administrative Web Login | 2FA with SSO hosted by Duo (Single Sign-On) | Documentation | Configure |
| Cisco ISE RADIUS | 2FA | Documentation | Protect |
| Cisco RADIUS VPN | 2FA | Documentation | Protect |

ISE RADIUS選項

4. 成功增加後，您將看到DUO應用程式的詳細資訊。向下滾動並按一下Save。

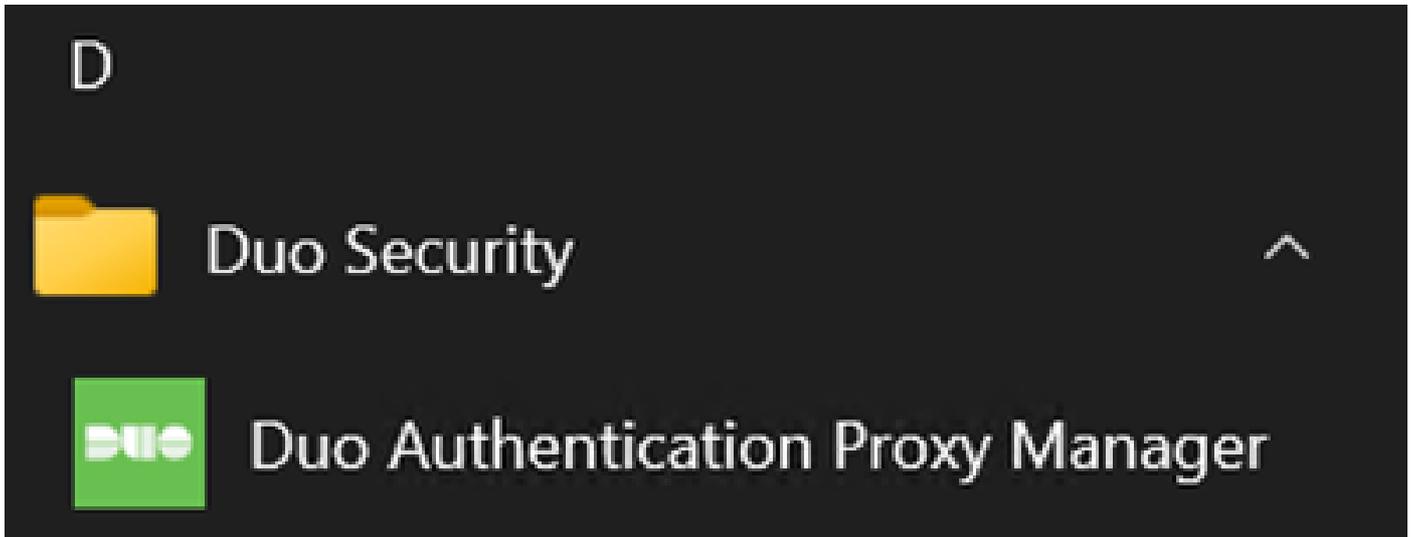
5. 複製提供的整合金鑰、秘密金鑰和API主機名稱；這些對於後續步驟至關重要。

The screenshot shows the 'Cisco ISE RADIUS' application details page. At the top, a green notification bar says 'Application modified successfully.' Below the breadcrumb 'Dashboard > Applications > Cisco ISE RADIUS', the title 'Cisco ISE RADIUS' is displayed. To the right are links for 'Authentication Log' and 'Remove Application'. A link 'Follow the Cisco ISE RADIUS instructions' is also present. A 'Reset Secret Key' button is located on the right. The 'Details' section contains three rows of information:

- Integration key:** A text field with a masked key and a 'Copy' button.
- Secret key:** A text field with a masked key and a 'Copy' button. Below it is a warning: 'Don't write down your secret key or share it with anyone.'
- API hostname:** A text field with a masked hostname and a 'Copy' button.

ISE伺服器詳細資訊

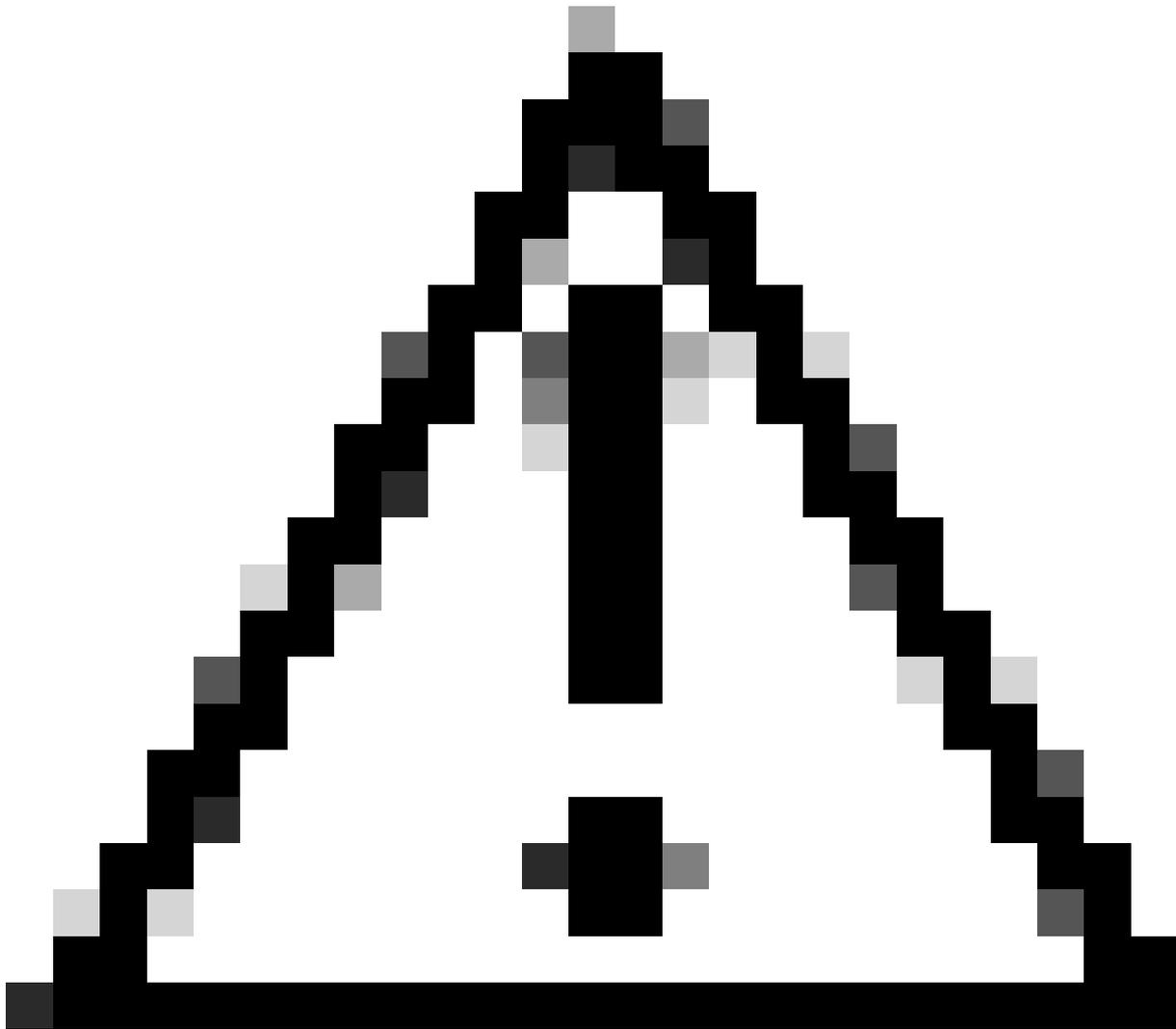
6. 啟動系統上的DUO Proxy Manager，繼續設定。



DUO代理管理員

7. (可選) 如果您的DUO代理伺服器需要代理配置才能連線到DUO雲，請輸入以下引數：

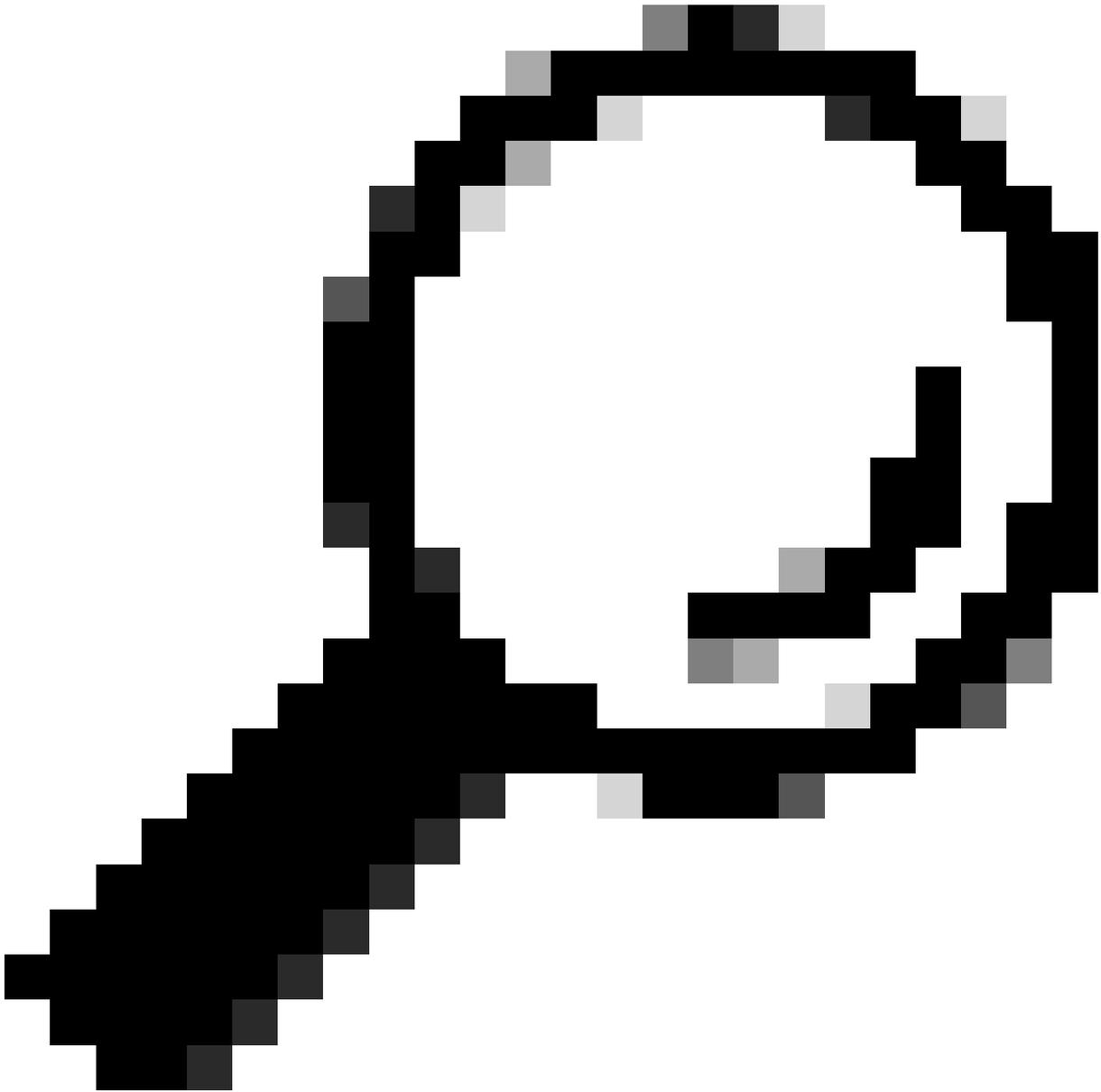
```
[main]  
http_proxy_host=<Proxy IP Address or FQDN >  
http_proxy_port=<port>
```



注意：請確保使用實際代理詳細資訊替換和。

8. 現在，利用您之前複製的資訊完成整合配置。

```
[radius_server_auto]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
radius_ip_1=<ISE IP address>
radius_secret_1=<secret key configured in the external RADIUS server section>
failmode=safe
port=1812
client=ad_client
```



提示：line client=ad_client表示DUO Proxy使用Active Directory帳戶進行身份驗證。確保此資訊正確無誤，以完成與Active Directory的同步。

將DUO與Active Directory整合。

1. 將DUO Authentication Proxy與Active Directory整合。

```
[ad_client]
host=<AD IP Address>
service_account_username=<service_account_username>
service_account_password=<service_account_password>
search_dn=DC=<domain>,DC=<TLD>
```

2. 使用DUO雲服務加入您的Active Directory。登入到<https://duo.com/>。

3. 導航到「使用者」，選擇「目錄同步」以管理同步設定。

Dashboard > Users

Users

Directory Sync | Import Users | Bulk Enroll Users | Add User

Need to activate a replacement phone? [Learn more about Reactivating Duo Mobile](#).

| | | | | | |
|-------------|--------------|----------------|-------|--------------|------------|
| 0 | 0 | 0 | 0 | 0 | 0 |
| Total Users | Not Enrolled | Inactive Users | Trash | Bypass Users | Locked Out |

Select (0) ... Export Search

No users shown based on your search.

目錄同步

4. 按一下「增加新同步」，並從提供的選項中選擇「Active Directory」。

Dashboard > Users > Directory Sync

Directory Sync

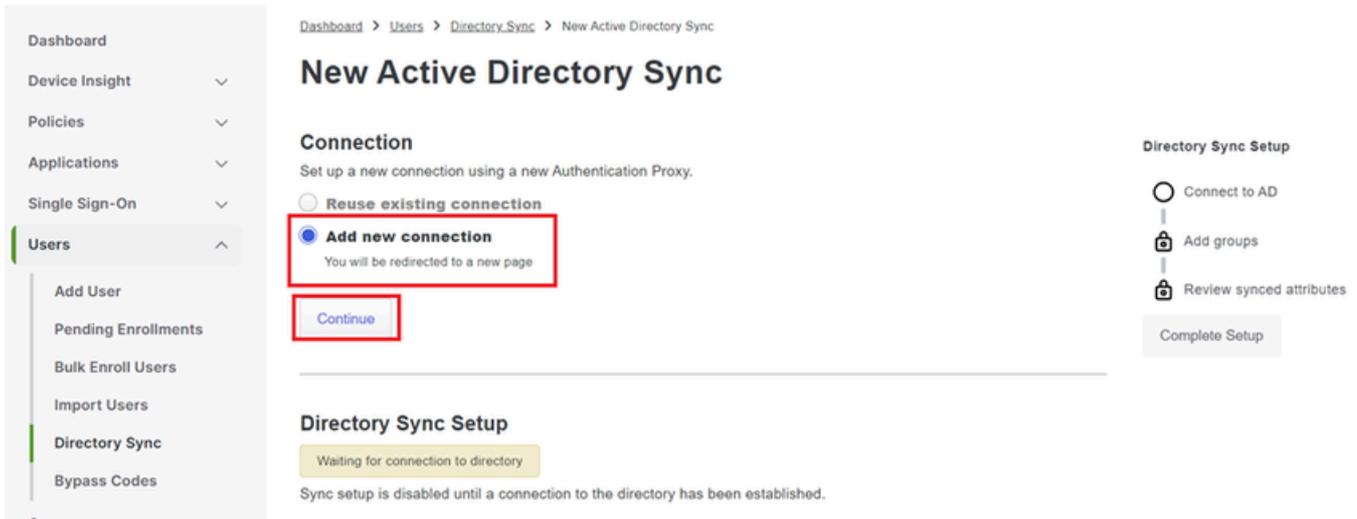
Add New Sync

Directory Syncs | Connections

You don't have any directories yet.

新增同步處理

5. 選擇增加新連線，然後按一下繼續。



新增新的Active Directory

6. 複製生成的整合金鑰、金鑰和API主機名。

Authentication Proxy

Configuration metadata

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
2. Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

Integration key [Copy](#)

Secret key [Copy](#)

Don't write down your secret key or share it with anyone.

[Reset Secret Key](#)

API hostname [Copy](#)

3. If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

[Delete Connection](#) [No Changes](#)

Status

Not connected

- Add Authentication Proxy
- Configure Directory

Connected Directory Syncs

User Syncs
[AD Sync](#)

驗證代理詳細資料

7. 返回DUO Authentication Proxy組態，使用您取得的新引數以及Active Directory管理員的服務帳戶認證設定[cloud]區段：

```
[cloud]
ikey=<integration key>
skey=<secret key>
api_host=<API hostname>
service_account_username=<your domain>\<service_account_username>
service_account_password=<service_account_password>
```

8. 選取「驗證」選項，驗證您的組態，以確保所有設定皆正確。

Authentication Proxy is running Up since: 4/20/2024, 5:43:21 PM Version: 6.3.0 Restart Service Stop Service

Configure: authproxy.cfg Unsaved Changes Output

```
1 [main]
2 http_proxy_host=cx[redacted]
3 http_proxy_port=3128
4
5 [radius_server_auto]
6 ikey=DIX[redacted]
7 skkey=[redacted]uXWYwLM
8 api_host=a[redacted].duosecurity.com
9 radius_ip_1=10.4.23.21
10 radius_secret_1=po[redacted]
11 failmode=safe
12 port=1812
13 client=ad_client
14
15 [ad_client]
16 host=10.4.23.42
17 service_account_username=administrator
18 service_account_password=[redacted]
```

Validate Save

Proxy DUO的組態。

9. 驗證之後，請儲存您的組態並重新啟動DUO Authentication Proxy服務以套用變更。

Authentication Proxy is running Up since: 4/20/2024, 5:43:21 PM Version: 6.3.0 Restart Service Stop Service

Validation passed Configuration has passed validation and is ready to be saved

Configure: authproxy.cfg Unsaved Changes Output

```
1 [main]
2 http_proxy_host=cx[redacted]
3 http_proxy_port=3128
4
5 [radius_server_auto]
6 ikey=DIX[redacted]
7 skkey=[redacted]wLM
8 api_host=[redacted].duosecurity.com
9 radius_ip_1=10.4.23.21
10 radius_secret_1=po[redacted]
11 failmode=safe
12 port=1812
13 client=ad_client
14
15 [ad_client]
```

Validate Save

Running The Duo Authentication Proxy Connectivity Tool. This may take several minutes...
[info] Testing section 'main' with configuration:
[info] {'http_proxy_host': 'cx[redacted]', 'http_proxy_port': '3128'}
[info] There are no configuration problems
[info] -----
[info] Testing section 'radius_server_auto' with configuration:
[info] {'api_host': '[redacted].duosecurity.com', 'client': 'ad_client', 'failmode': 'safe', 'http_proxy_host': '[redacted]', 'http_proxy_port': '3128', 'ikey': 'DI[redacted]'}

重新啟動服務選項。

10. 返回DUO管理控制台，輸入Active Directory伺服器的IP地址以及使用者同步的基本DN。

Directory Configuration

Domain controller(s)

Hostname or IP address (1) *

Port (1) *

[+ Add Domain controller](#)

The port is typically 389 for cleartext LDAP or STARTTLS, and 636 for LDAPS.

Base DN *

Enter the full distinguished name (DN) of the directory location to search for users and groups. We recommend setting this to the directory root (example: DC=domain,DC=local). If specifying the DN of an OU or container, ensure it is **above both the users and groups to sync**.

目錄設定。

11. 選擇Plain選項以配置用於非NTLMv2身份驗證的系統。

Authentication type

- Integrated**
Performs Windows authentication from a domain-joined system.
- NTLMv2**
Performs Windows NTLMv2 authentication.
- Plain**
Performs username-password authentication.

驗證型別。

12. 儲存新設定以確保配置已更新。

 Delete Connection

Save

Status

Not connected

Add Authentication Proxy



Configure Directory

Connected Directory Syncs

User Syncs

[AD Sync](#)

儲存選項

13. 使用「測試連線」功能驗證DUO雲服務是否可以與Active Directory通訊。

Authentication Proxy

1. To set up this directory, you need to install the Duo Authentication Proxy software on a machine that Duo can connect to and that can connect to your LDAP server. [View instructions](#)
2. Configure your Authentication Proxy. Update the `ikey`, `skey`, and `api_host` entries in the `[cloud]` section of your configuration, or [download a pre-configured file](#).

Integration key [Copy](#)

Secret key [Copy](#)

Don't write down your secret key or share it with anyone.

[Reset Secret Key](#)

API hostname [Copy](#)

3. If you are using NTLM or plain authentication, update the `[cloud]` section of your configuration with the username and password for the LDAP account that has read access for your LDAP directory.

```
service_account_username=myusername  
service_account_password=mypassword
```

4. Restart your Authentication Proxy.

5. [Test Connection](#).

測試連線選項。

14. 確認Active Directory的狀態顯示為「Connected」，表示整合成功。

Status

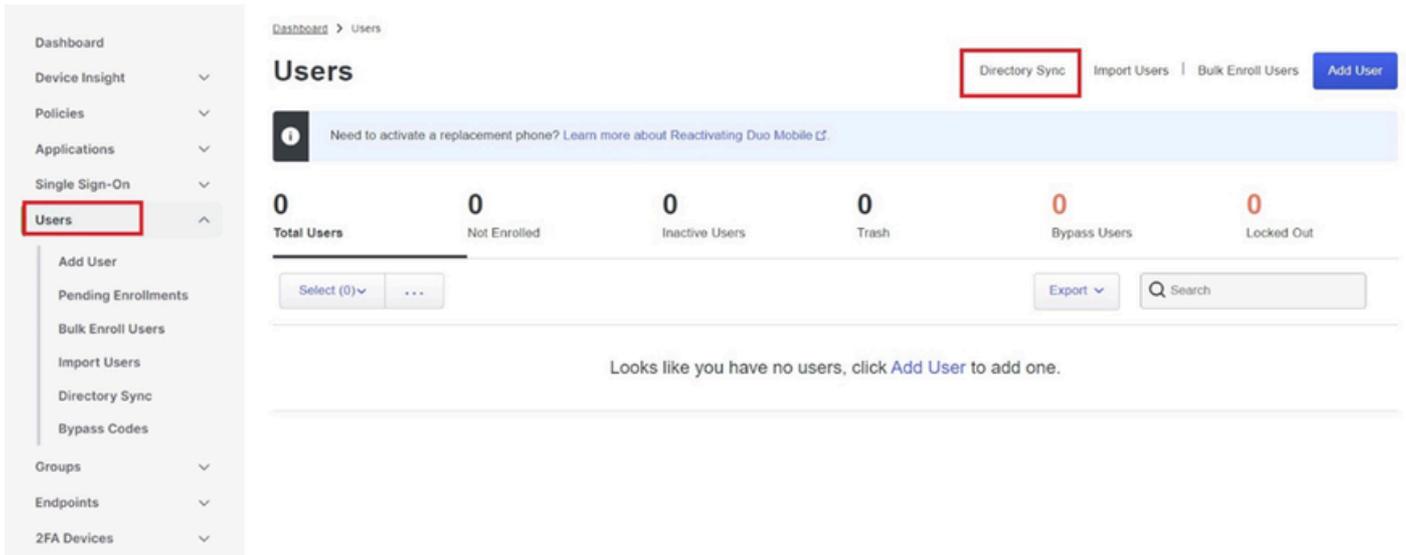
Connected

狀態成功。

透過DUO Cloud從Active Directory (AD)匯出使用者帳戶。

1. 在Duo管理面板中導航到使用者>目錄同步，找到與使用Active Directory進行目錄同步相關的設定

o

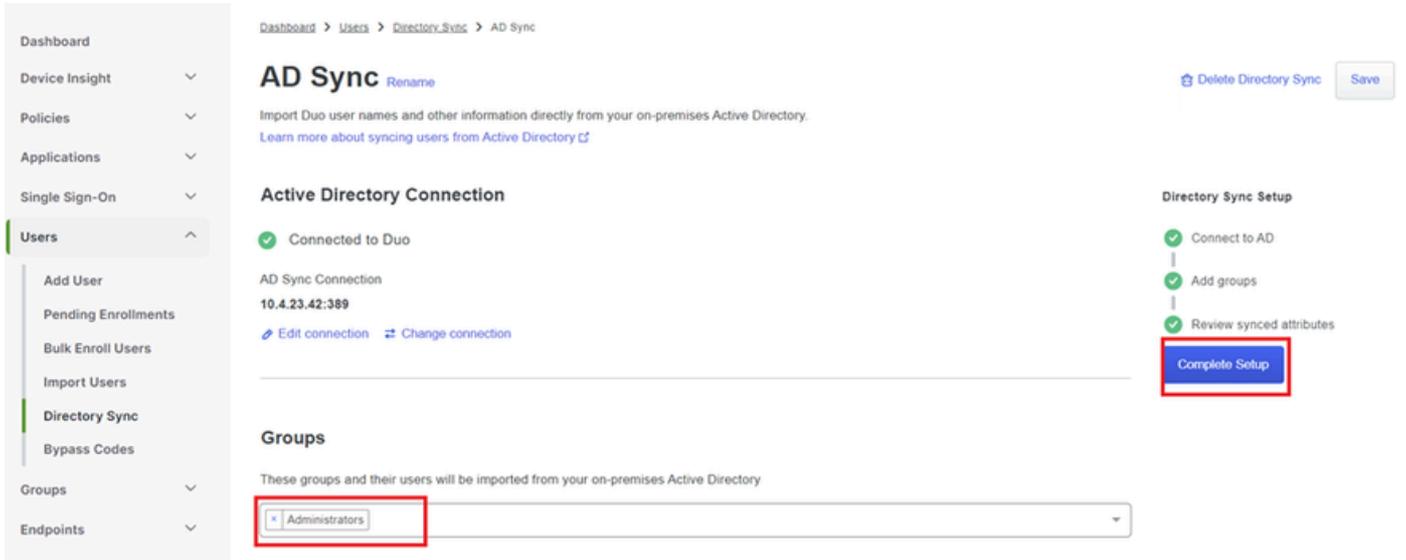


使用者清單。

2. 選擇要管理的Active Directory配置。

3. 在配置設定中，確定並選擇Active Directory中要與Duo Cloud同步的特定組。請考慮使用選取專案的篩選選項。

4. 按一下完成設定。



AD同步。

5. 要立即啟動同步，請按一下Sync Now。這會將Active Directory中指定群組的使用者帳戶匯出至Duo Cloud，以便在Duo Security環境中對其進行管理。

AD Sync Rename

Delete Directory Sync No Changes

Import Duo user names and other information directly from your on-premises Active Directory.
[Learn more about syncing users from Active Directory](#)

Sync Controls

Sync status

Scheduled to automatically synchronize every 12 hours, next around 2:00 AM UTC [Pause automatic syncs](#)

Sync Now

[Troubleshooting](#) ▾

Active Directory Connection

✓ Connected to Duo

AD Sync Connection

10.4.23.42:389

[Edit connection](#)

[Change connection](#)

啟動同步處理

在Cisco DUO雲中註冊使用者。

使用者註冊可透過各種方法啟用身份驗證，例如代碼訪問、DUO推送、SMS代碼和令牌。

1. 導航到Cisco Cloud控制台中的Users部分。
2. 找出並選取您要註冊的使用者帳戶。

Dashboard > Users

Users

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

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

Select (0) ▾ ... Export ▾ Search

| <input type="checkbox"/> | Username ▾ | Name | Email | Phones | Tokens | Status | Last Login |
|-------------------------------------|---------------|------|-----------------|--------|--------|--------|---------------------|
| <input checked="" type="checkbox"/> | administrator | | oteg [REDACTED] | | | Active | Never authenticated |

1 total

使用者帳戶清單。

3. 按一下Send Enrollment Email按鈕以啟動登記流程。

administrator

Logs

Send Enrollment Email

Sync This User



This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.



This user was synced from the directory **AD Sync**. Some fields are read-only.

Username

administrator

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).

透過電子郵件進行註冊。

4. 檢查電子郵件收件箱並打開註冊邀請以完成驗證過程。

有關註冊流程的其他詳細資訊，請參閱以下資源：

- 通用註冊指南：<https://guide.duo.com/universal-enrollment>
- 傳統註冊指南：<https://guide.duo.com/traditional-enrollment>

配置驗證過程。

為確保您的配置正確且運行正常，請驗證以下步驟：

1. 啟動Web瀏覽器並輸入Firepower威脅防禦(FTD)裝置的IP地址以訪問VPN介面。



Not secure | https://10.4.23.53/+CSCOE+/logon.html#form_title_text

Logon

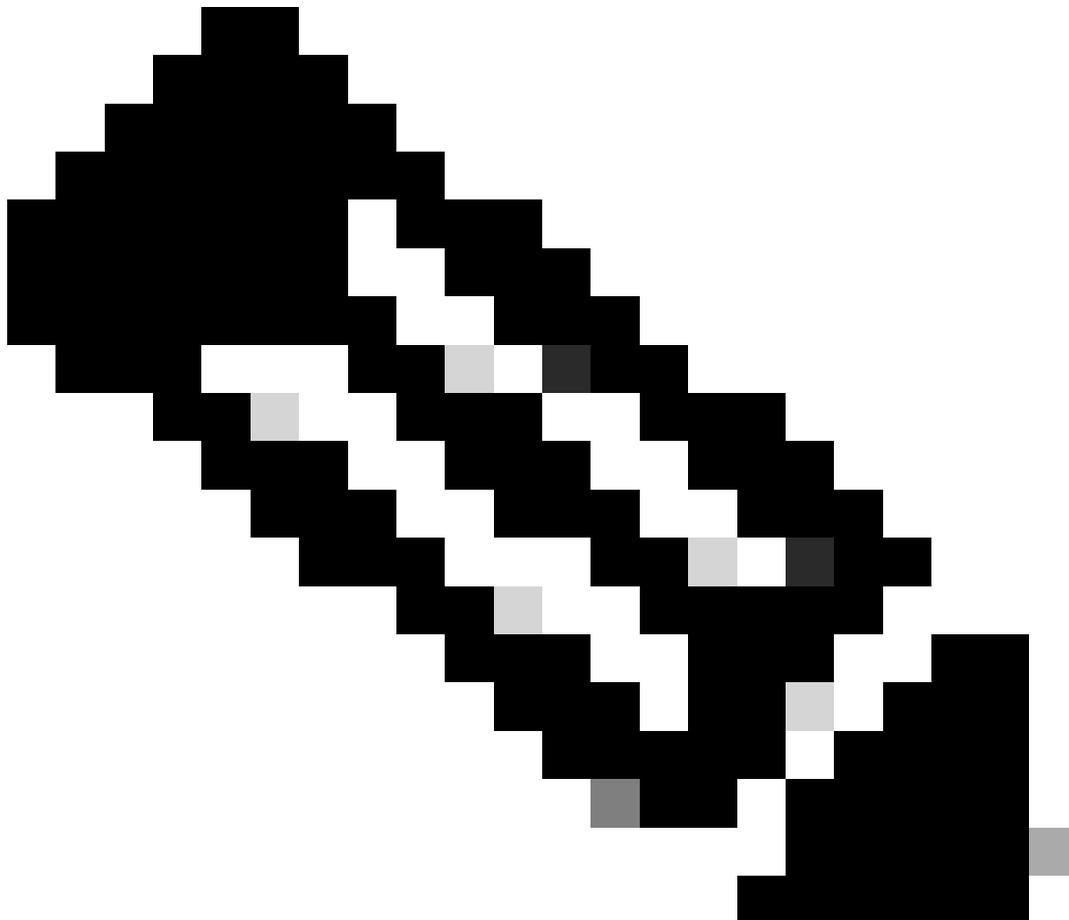
Group

Username

Password

VPN登入。

2. 系統提示時，輸入您的使用者名稱與密碼。



注意：認證是Active Directory帳戶的一部分。

3. 當您收到DUO Push通知時，請使用DUO Mobile軟體核准該通知，以繼續進行驗證程式。



(1) Login request waiting.

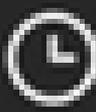
[Respond](#)



Are you logging in to Cisco ISE
RADIUS?



 Unknown

 3:13 PM CST

 administrator

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）。