

使用DUO配置ISE 3.3本機多重身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[流程圖](#)

[組態](#)

[選擇要保護的應用程式](#)

[將ISE與Active Directory整合](#)

[啟用開放式API](#)

[啟用MFA身份源](#)

[配置MFA外部身份源](#)

[將使用者註冊到DUO](#)

[配置策略集](#)

[限制](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何將身份服務引擎(ISE)3.3補丁1與DUO整合以實現多重身份驗證。從3.3版補丁1開始，ISE可配置為與DUO服務進行本機整合，因此無需身份驗證代理。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- ISE
- DUO

採用元件

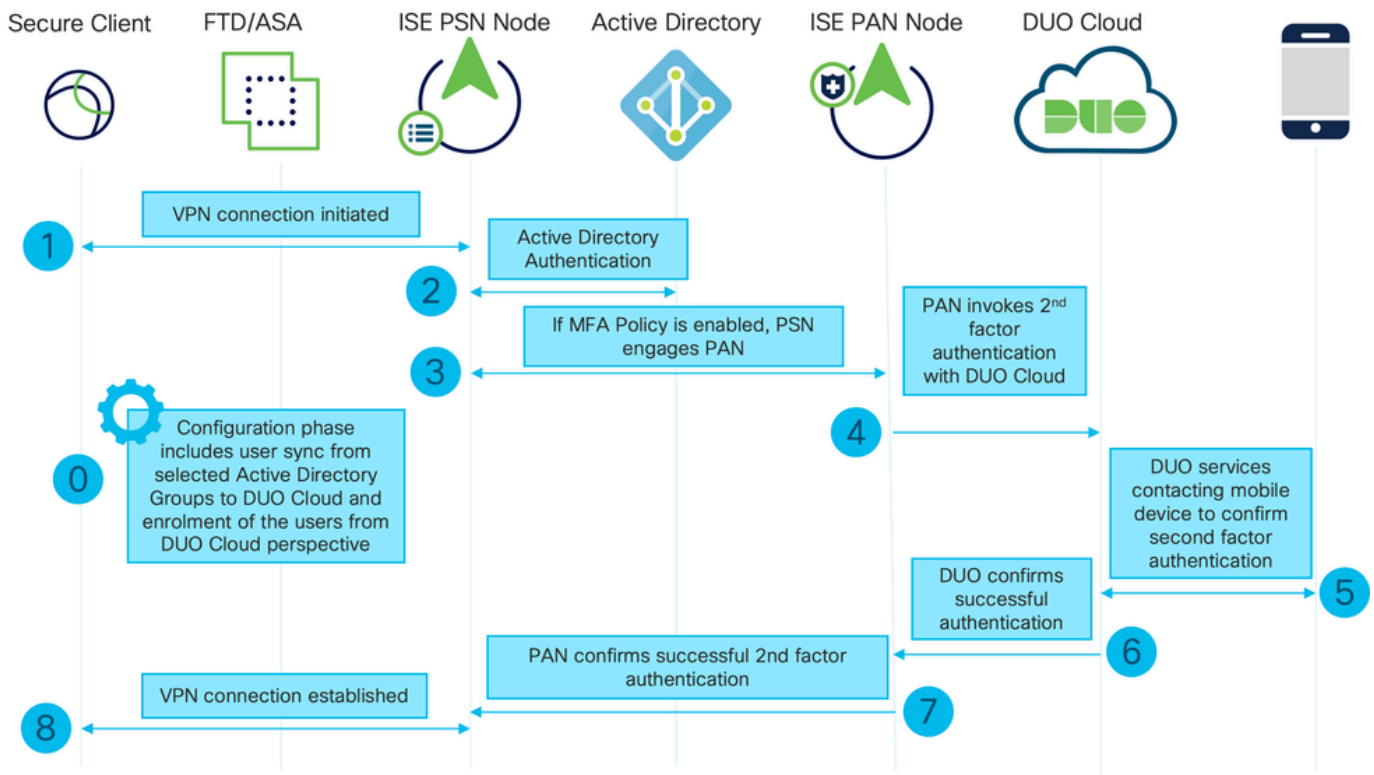
本檔案中的資訊是根據：

- Cisco ISE版本3.3補丁1
- DUO
- Cisco ASA版本9.16(4)
- 思科安全使用者端5.0.04032版

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。

設定

流程圖



流程圖

步驟

0. 配置階段包括選擇Active Directory組，使用者從其中進行同步，同步在MFA嚮導完成之後進行。它由兩個步驟組成。查詢Active Directory以獲取使用者和某些屬性的清單。通過管理API呼叫DUO Cloud將使用者推送到那裡。管理員需要註冊使用者。註冊可包括啟用Duo Mobile使用者的可選步驟，這允許使用者使用帶有Duo Push的單點選身份驗證
1. 啟動VPN連線，使用者輸入使用者名稱和密碼，然後點選OK。網路裝置傳送RADIUS Access-Request傳送到PSN
2. PSN節點通過Active Directory驗證使用者
3. 身份驗證成功並配置MFA策略後，PSN會與PAN聯絡，以便聯絡DUO Cloud
4. 呼叫Auth API的DUO Cloud以呼叫DUO的二級身份驗證
5. 進行第二因素身份驗證。使用者完成第二因素身份驗證過程
6. DUO響應PAN時採用了第二因素身份驗證的結果

7. PAN使用第二因素身份驗證的結果響應PSN

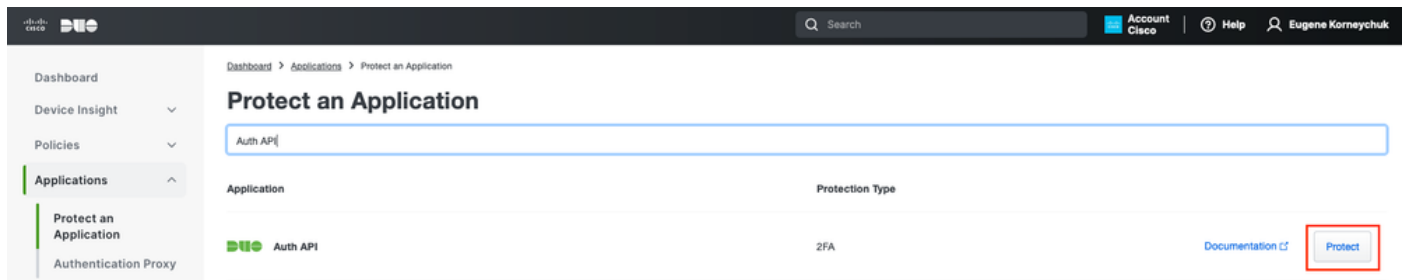
8.將Access-Accept傳送到網路裝置，建立VPN連線

組態

選擇要保護的應用程式

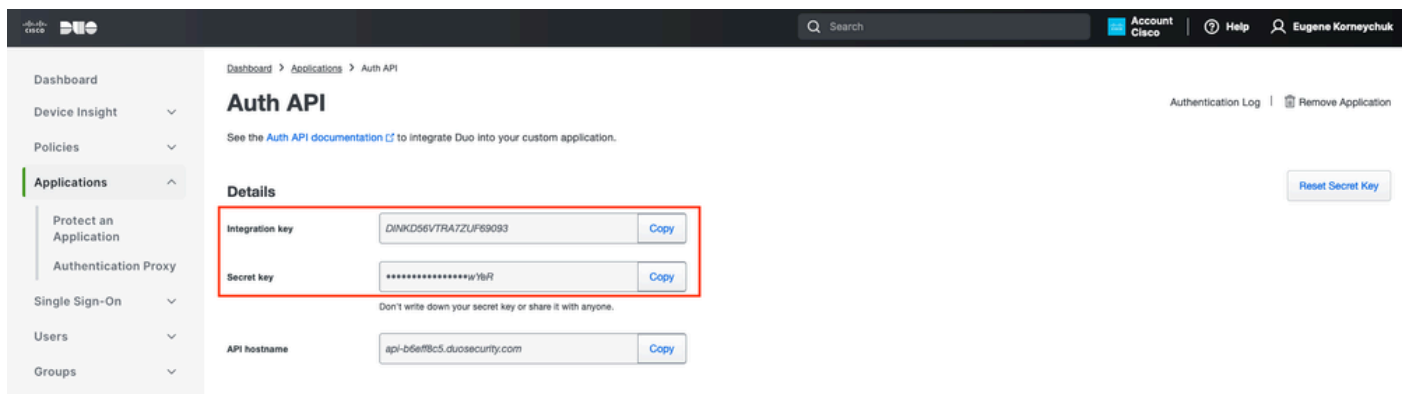
導航至DUO Admin Dashboard <https://admin.duosecurity.com/login>。使用管理員憑據登入。

導航到控制面板>應用程式>保護應用程式。尋找Auth API，然後選擇Protect。



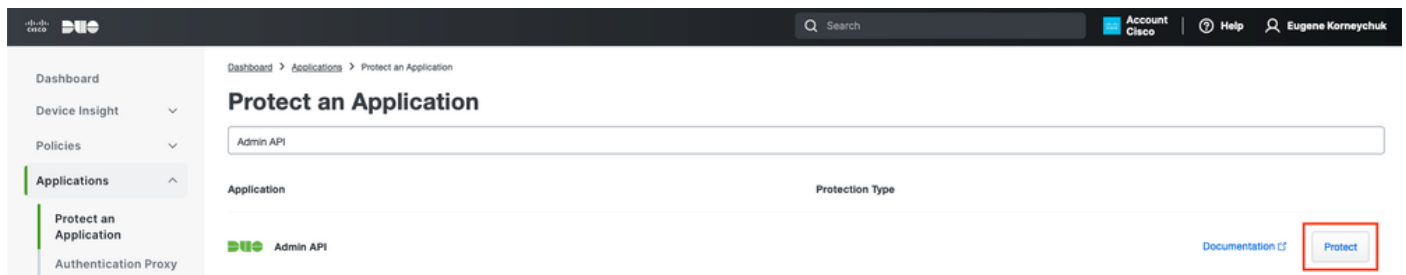
Auth API 1

記下Integration 金鑰和Secret金鑰。



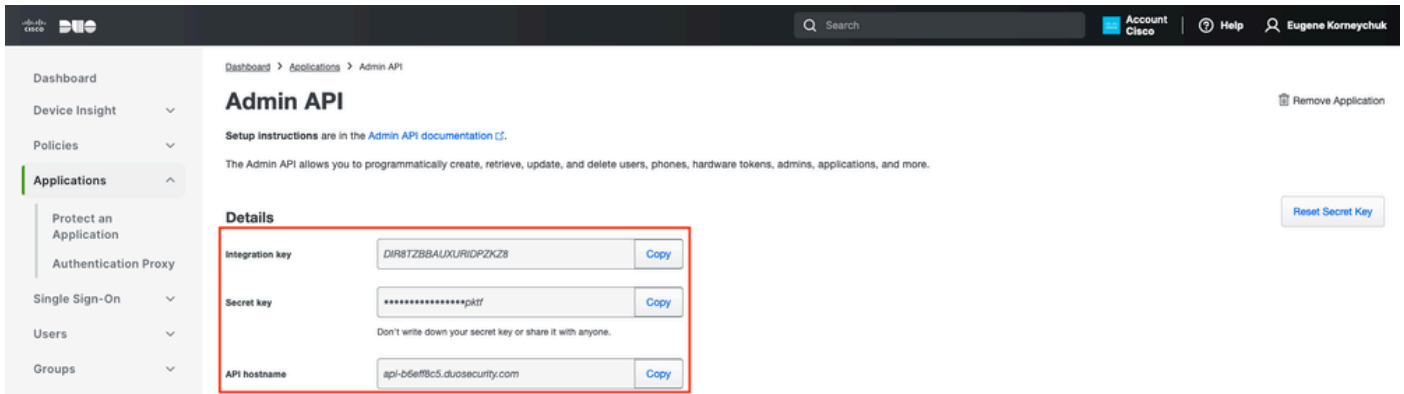
身份驗證API 2

導航到控制面板>應用程式>保護應用程式。查詢Admin API並選擇Protect。



Auth API 1

記下Integration 金鑰和Secret key以及API主機名。

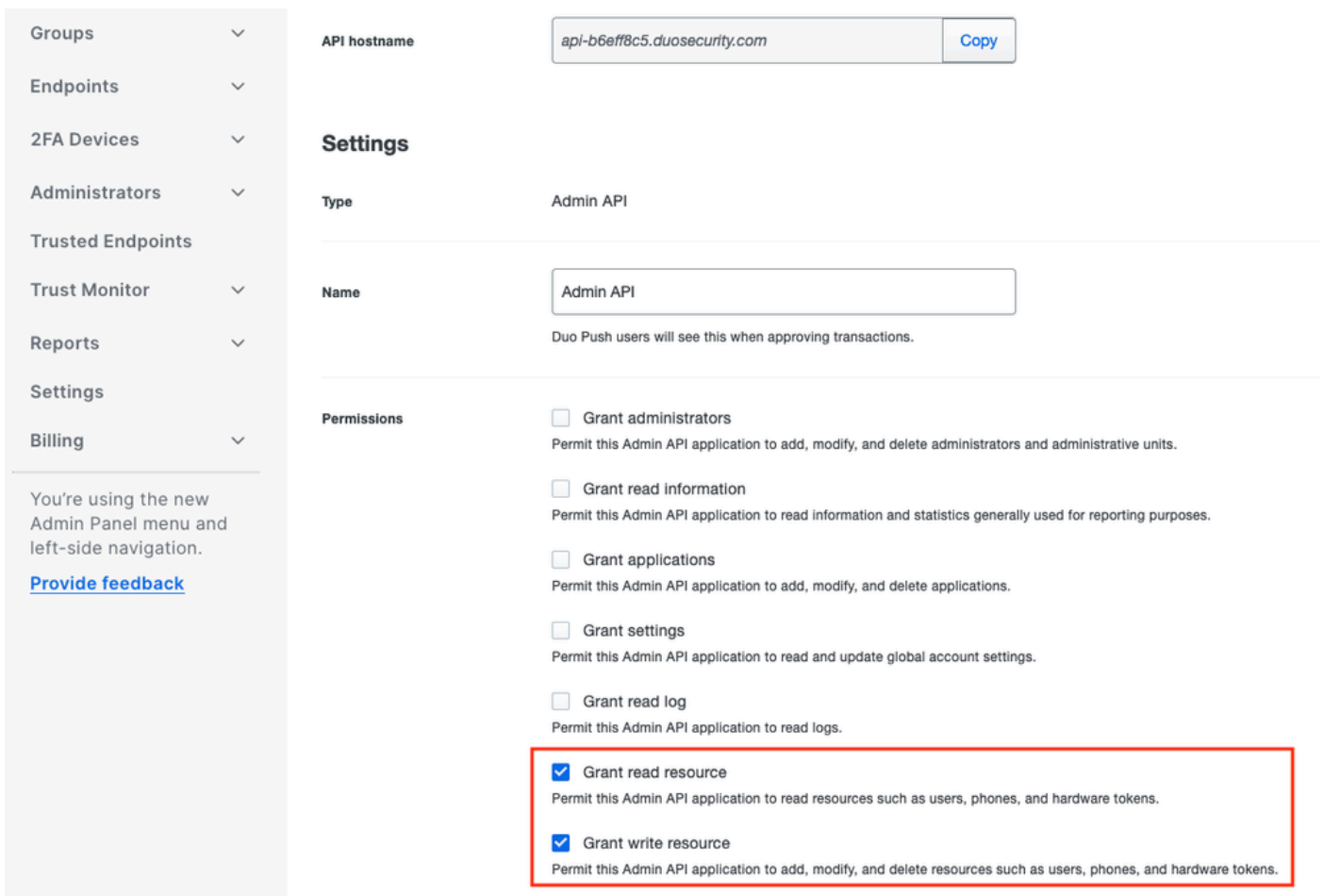


管理API 2

配置API許可權

導航到控制面板>應用程式>應用程式。選擇Admin API。

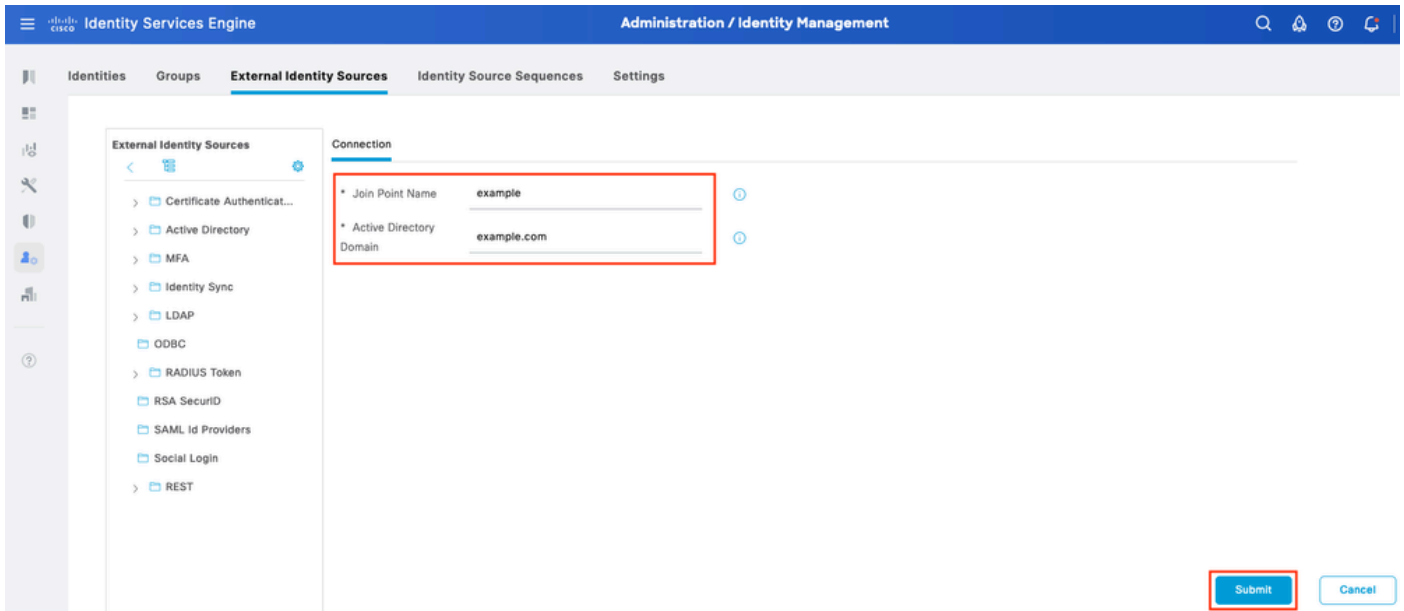
選中Grant Read Resource和Grant Write Resource許可權。按一下Save Changes。



管理API 3

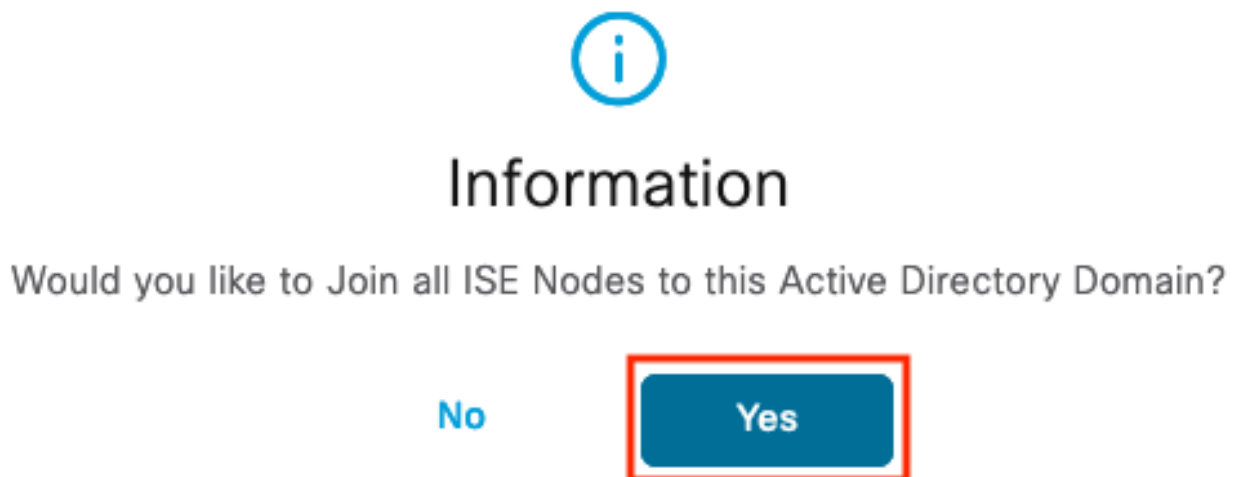
將ISE與Active Directory整合

1.導航到管理>身份管理>外部身份庫> Active Directory >新增。提供加入點名稱、Active Directory域並點選提交。



Active Directory 1

2. 當系統提示將所有ISE節點加入此Active Directory域時，按一下Yes。




Active Directory 2

3. 提供AD使用者名稱和密碼，然後按一下OK。




Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name  Administrator

* Password

Specify Organizational Unit 

Store Credentials 


Cancel

OK

Active Directory 3

在ISE中訪問域所需的AD帳戶可以具有以下任一項：

- 將工作站新增到相應域中的域使用者許可權
- 在建立ISE電腦帳戶的ISE電腦加入ISE電腦到域之前，在相應的電腦容器上建立電腦對象或刪除電腦對象許可權

 **注意：**思科建議禁用ISE帳戶的鎖定策略，並配置AD基礎設施，以便在該帳戶使用錯誤密碼時向管理員傳送警報。輸入錯誤密碼時，ISE不會在必要時建立或修改其電腦帳戶，因此可能會拒絕所有身份驗證。

4. AD的狀態為運行。

* Join Point Name **example** ⓘ
 * Active Directory Domain **example.com** ⓘ

[+ Join](#)
[+ Leave](#)
[Test User](#)
[Diagnostic Tool](#)
[Refresh Table](#)

<input type="checkbox"/>	ISE Node	ISE Node R...	Status	Domain Controller	Site
<input type="checkbox"/>	ise331.example.com	PRIMARY	Operational	WIN2022.example.com	Default-First-Site-Name
<input type="checkbox"/>	ise332.example.com	SECONDARY	Operational	WIN2022.example.com	Default-First-Site-Name

Active Directory 4

5. 定位至「組」>「新增」>「從目錄選擇組」>「檢索組」。選中您選擇的AD組（用於同步使用者和授權策略）對應的覈取方塊，如下圖所示。

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain example.com

Name * SID * Type
Filter Filter Filter ALL

Retrieve Groups... 50 Groups Retrieved.

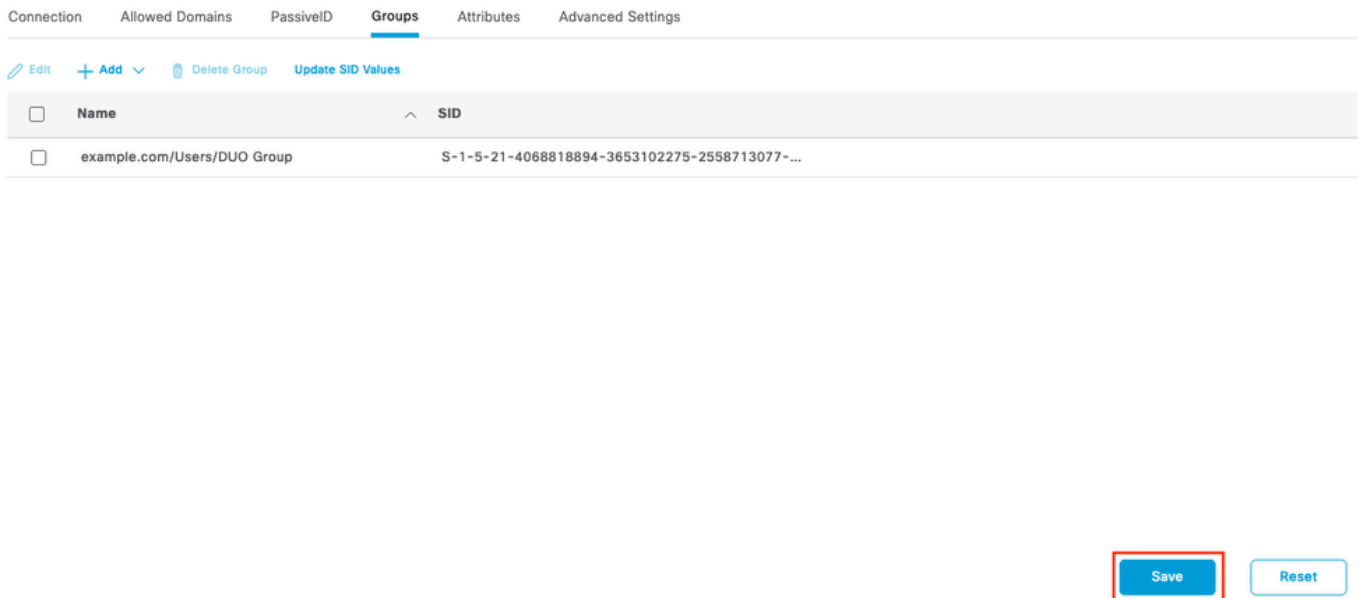
<input type="checkbox"/>	Name	Group SID	Group Type
<input type="checkbox"/>	example.com/Users/Cert Publishers	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/Cloneable Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input checked="" type="checkbox"/>	example.com/Users/DUO Group	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Denied RODC Password Re...	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/DnsAdmins	S-1-5-21-4068818894-3653102275-25587130...	DOMAIN LOCAL
<input type="checkbox"/>	example.com/Users/DnsUpdateProxy	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Admins	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Computers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Controllers	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Guests	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Domain Users	S-1-5-21-4068818894-3653102275-25587130...	GLOBAL
<input type="checkbox"/>	example.com/Users/Enterprise Admins	S-1-5-21-4068818894-3653102275-25587130...	UNIVERSAL

Cancel

OK

Active Directory 5

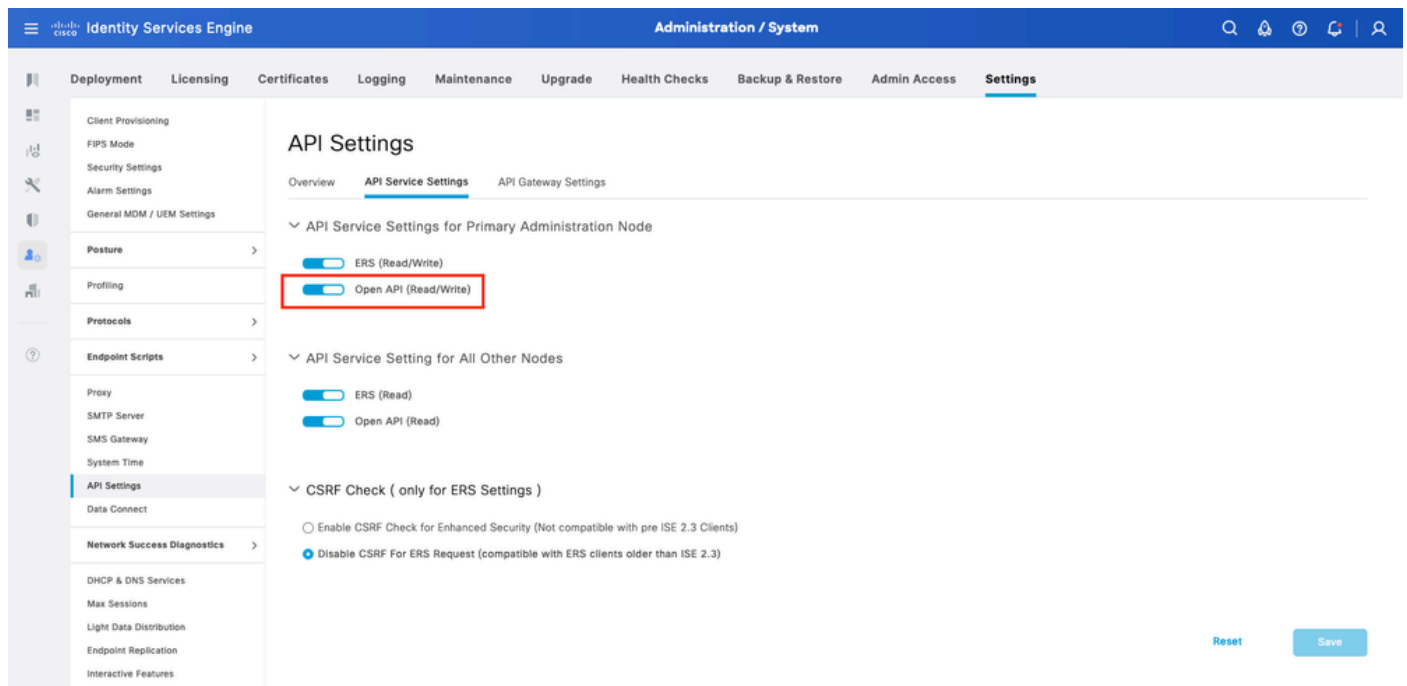
6. 按一下儲存以儲存檢索到的AD組。



Active Directory 6

啟用開放式API

導航到Administration > System > Settings > API Settings > API Service Settings。啟用Open API，然後按一下Save。



開放式API

啟用MFA身份源

導航到Administration > Identity Management > Settings > External Identity Sources Settings。啟用MFA，然後按一下Save。

The screenshot shows the Cisco Identity Services Engine Administration / Identity Management interface. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Features. The main content area is titled 'External Identity Sources Settings' and 'REST ID Store'. It includes a list of settings on the left: User Custom Attributes, User Authentication Settings, Endpoint Purge, Endpoint Custom Attributes, and External Identity Sources Settings (highlighted). The main content area contains the following text: 'To allow integration of REST identity stores with Cisco ISE, click the radio button below. It takes a few minutes to enable the REST ID Store settings. After the settings are enabled, you can add REST ID stores to Cisco ISE in the External Identity Source page.' Below this is a 'NOTE: ISE integration with Azure AD is released as a Controlled Introduction feature and should be thoroughly tested before being used in production environment.' There are two toggle switches: 'REST ID Store' (checked) and 'MFA' (checked and highlighted with a red box). At the bottom right, there are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted with a red box.

ISE MFA 1

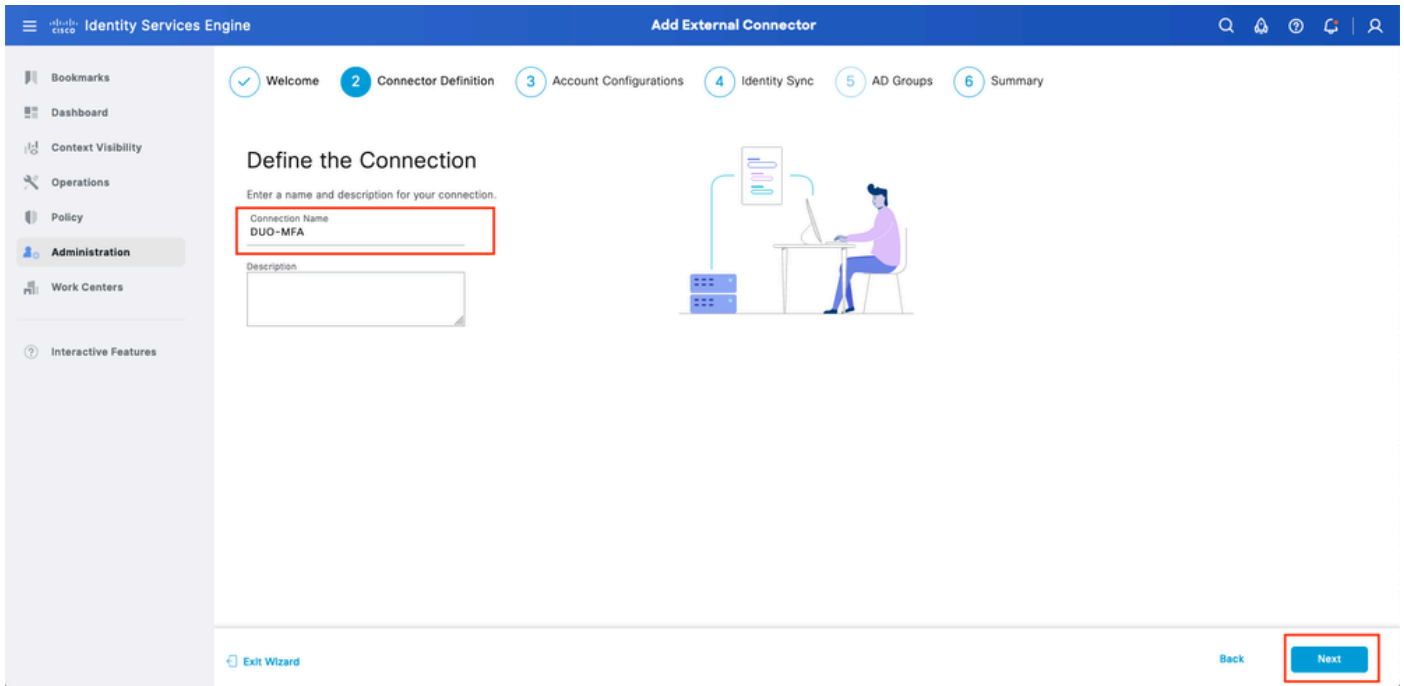
配置MFA外部身份源

導航到管理>身份管理>外部身份源。按一下「Add」。在「歡迎使用」螢幕上，按一下「開始執行操作」。

The screenshot shows the Cisco Identity Services Engine 'Add External Connector' wizard. The top navigation bar includes 'Add External Connector' and search, notification, and user icons. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Welcome' and contains the following text: 'This wizard takes you through setting up a connection between your Duo Account and Cisco ISE to enable seamless Multi-Factor Authentication workflows.' Below this is a section titled 'Before you begin, the following prerequisites apply:' followed by a list of six prerequisites: 1. Cisco ISE Advantage licenses are required. 2. The Cisco Duo license that enables MFA usage is required. 3. In your Duo portal, create a protected application that is enabled for Admin API and Authentication API usage. 4. Grant read/write access to Admin API. 5. Ensure your ISE has a stable connection to Duo (Either through direct internet or proxy). 6. For this application, note the integration keys (ikey), secret keys (skey) and API hostname values for the Admin and Authentication APIs. These values are required in the next steps of this setup wizard. To the right of the text is an illustration of a person at a laptop with a city skyline in the background. At the bottom left, there is an 'Exit Wizard' button. At the bottom right, there is a 'Let's Do It' button highlighted with a red box.

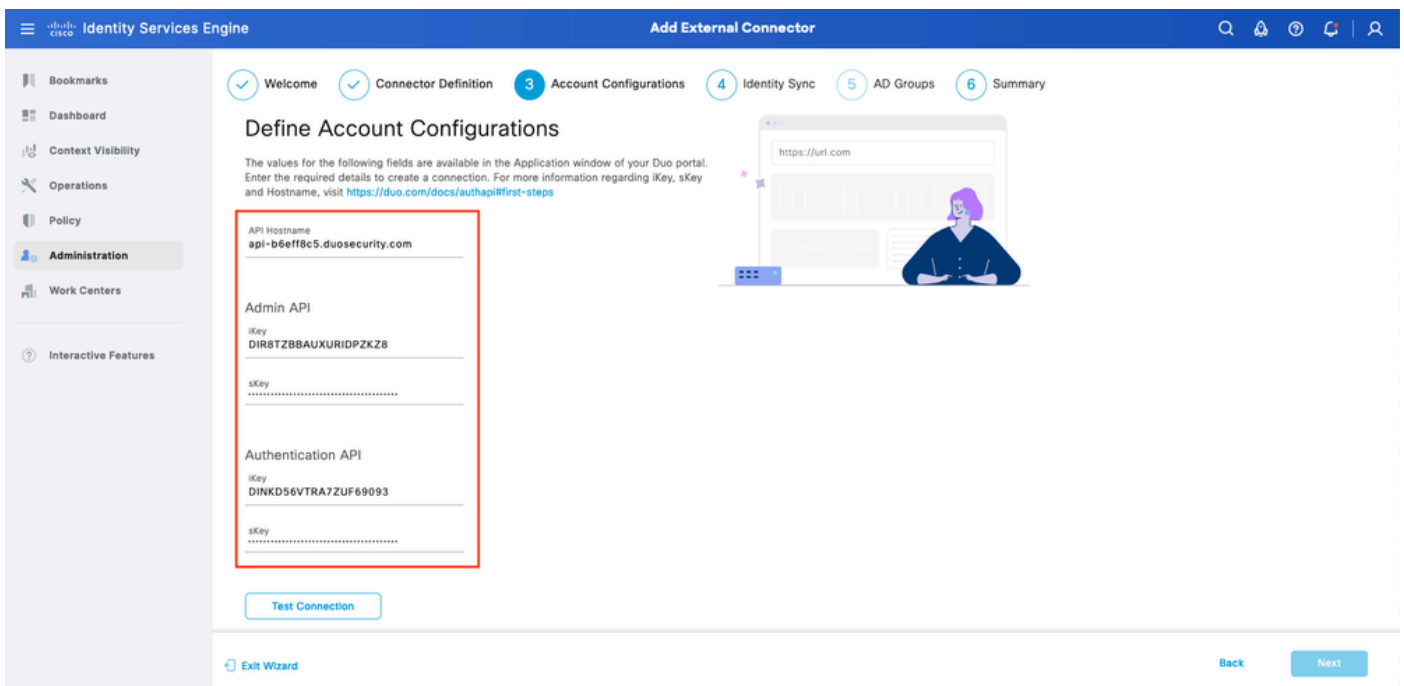
ISE DUO嚮導1

在下一個螢幕上，配置Connection Name，然後按一下Next。



ISE DUO嚮導2

在選擇要保護的應用程式中，配置API主機名、管理API集成和金鑰、Auth API集成和金鑰。




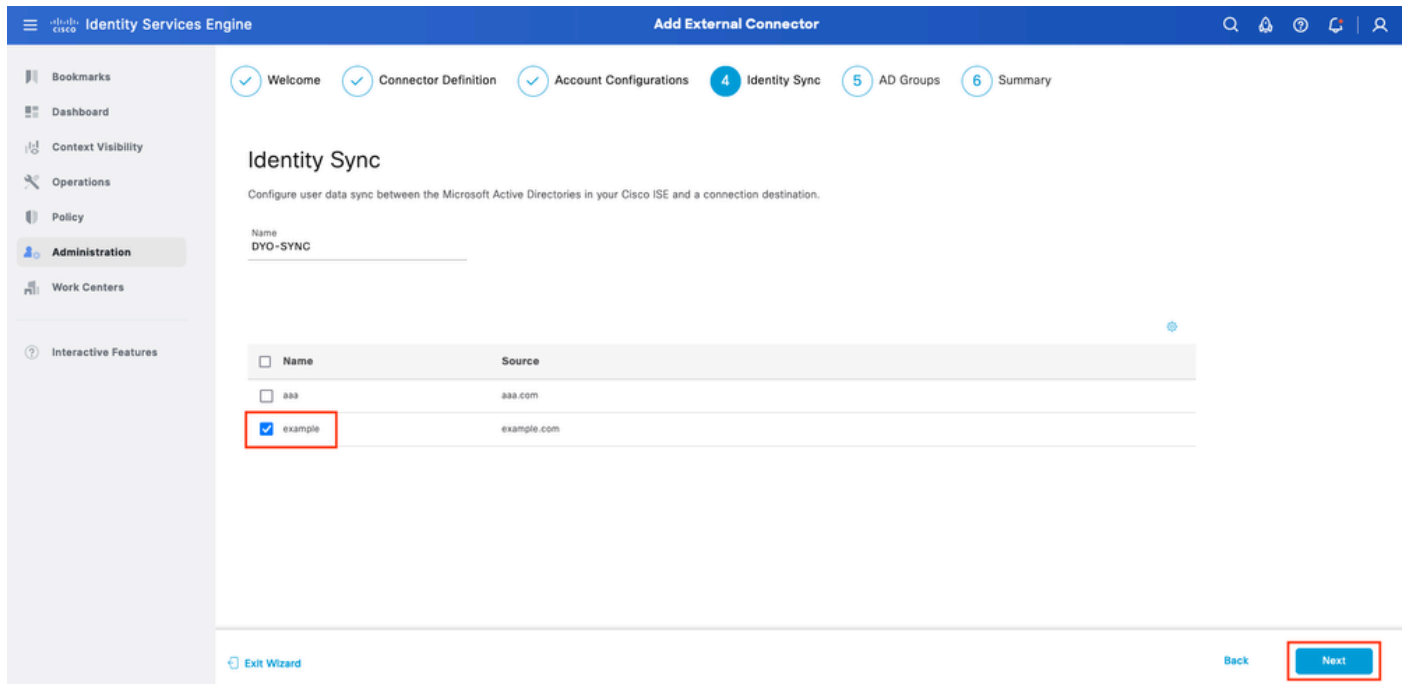
ISE DUO嚮導3

按一下Test Connection。測試連線成功後，可以按一下下一步。



配置身份同步。此過程使用之前提供的API憑據將您選擇的Active Directory組中的使用者同步到DUO帳戶。選擇Active Directory加入點。按一下Next。

 注意：Active Directory配置不在文檔範圍之內，請按照本文件進行操作，以便將ISE與Active Directory整合。



Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations **4 Identity Sync** 5 AD Groups 6 Summary

Identity Sync

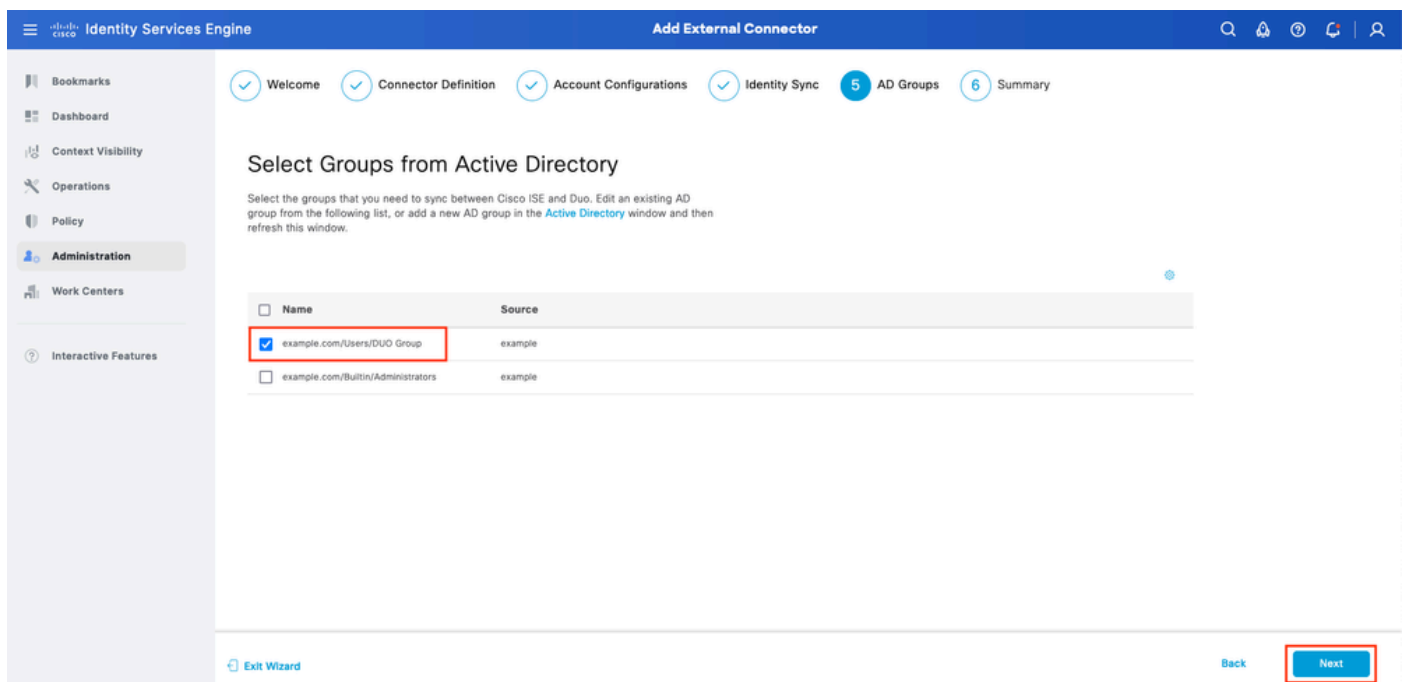
Configure user data sync between the Microsoft Active Directories in your Cisco ISE and a connection destination.

Name
DYO-SYNC

<input type="checkbox"/> Name	Source
<input type="checkbox"/> aaa	aaa.com
<input checked="" type="checkbox"/> example	example.com

Exit Wizard Back **Next**

選擇Active Directory Groups，您希望使用者從其中與DUO同步。按一下Next。



Identity Services Engine Add External Connector

Welcome Connector Definition Account Configurations Identity Sync **5 AD Groups** 6 Summary

Select Groups from Active Directory

Select the groups that you need to sync between Cisco ISE and Duo. Edit an existing AD group from the following list, or add a new AD group in the Active Directory window and then refresh this window.

<input type="checkbox"/> Name	Source
<input checked="" type="checkbox"/> example.com/Users/DOU Group	example
<input type="checkbox"/> example.com/Builtin/Administrators	example

Exit Wizard Back **Next**

驗證設定是否正確，然後按一下Done。


The screenshot shows the 'Add External Connector' wizard in Cisco ISE. The 'Summary' page is active, showing the following configuration details:

- Connector Definition:** Connection Name: DUO-MFA, VPN, TACACS.
- Define Account Configurations:** API Hostname: api-b6eff8c5.duosecurity.com, Authentication API, iKey: DIR8TZBBAUXURIDPZKZ8, sKey: [redacted], Admin API, iKey: DINKD56VTRA7ZUF69093, sKey: [redacted], Authentication: MFA Auth and Admin API Integration and Secret Keys are valid.
- Identity Sync:** [redacted]

At the bottom right, there are 'Back' and 'Done' buttons. The 'Done' button is highlighted with a red box.

ISE DUO嚮導7

將使用者註冊到DUO

 注意：DUO使用者註冊不在文檔範圍之內，請考慮使用本[文檔](#)以瞭解有關使用者註冊的詳細資訊。本文檔使用手動使用者註冊。

開啟DUO Admin Dashboard。導航到控制面板>使用者。點選從ISE同步的使用者。

The screenshot shows the Cisco Duo Admin Dashboard 'Users' page. The page displays a summary of user statistics and a table of users.

User Statistics:

- Total Users: 2
- Not Enrolled: 1
- Inactive Users: 1
- Trash: 0
- Bypass Users: 0
- Locked Out: 0

User Table:

Username	Name	Email	Phones	Tokens	Status	Last Login
<input type="checkbox"/> alice	alice	alice@wonderland.com	1		Active	Nov 14, 2023 1:43 AM
<input type="checkbox"/> bob	bob				Active	Never authenticated

The 'bob' user row is highlighted with a red box.

DUO註冊1

向下滾動至電話。按一下「添加電話」。

DUO註冊2

輸入電話號碼，然後按一下Add Phone。

配置策略集

1. 配置身份驗證策略

導航到Policy > Policy Set。選擇要為其啟用MFA的策略集。將主身份驗證身份庫配置為Active Directory的身份驗證策略。

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	1	⚙️
●	DUO Authentication	Radius-NAS-Port-Type EQUALS Virtual	example > Options		⚙️
●	Default		All_User_ID_Stores > Options	7	⚙️

策略集 1


2. 配置MFA策略

在ISE上啟用MFA後，ISE策略集的新部分可用。展開MFA Policy，然後按一下+以新增MFA Policy。根據您的選擇配置MFA條件，選擇使用部分之前配置的DUO-MFA。按一下Save。

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	75

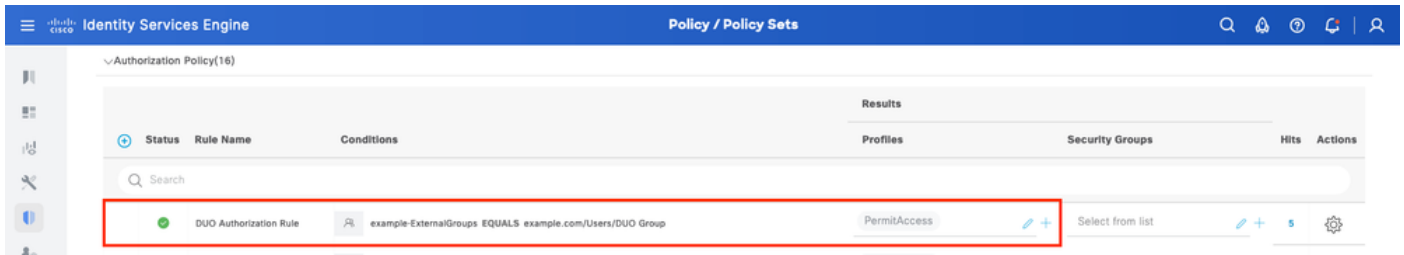
Status	Rule Name	Conditions	Use	Hits	Actions
●	DUO Rule	Cisco-VPN3000-CVPN3000/ASA/PIX7x-Tunnel-Group-Name EQUALS RA	DUO-MFA > Options	0	⚙️

ISE策略

 注意：上面配置的策略依賴於名為RA的隧道組。連線到RA隧道組的使用者將被強制執行MFA。ASA/FTD配置不在本文檔的討論範圍之內。使用此[文檔](#)設定ASA/FTD

3. 配置授權策略

使用Active Directory組條件和您選擇的許可權配置授權策略。



策略集3

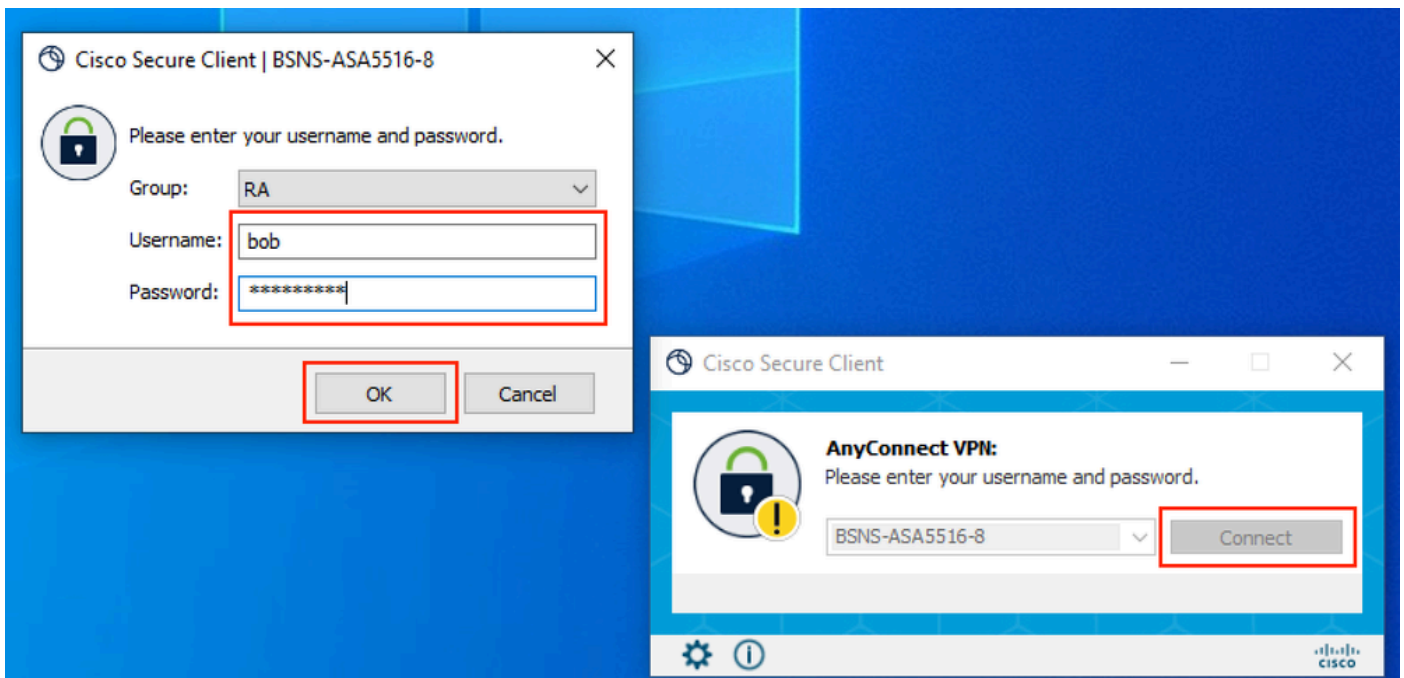
限制

撰寫本檔案時：

- 1.僅支援DUO按鍵和電話作為第二因素身份驗證方法
- 2.沒有組推送到DUO Cloud，僅支援使用者同步
- 3.僅支援以下多重身份驗證使用案例：
 - VPN使用者身份驗證
 - TACACS+管理員訪問身份驗證

驗證

開啟Cisco Secure Client，按一下Connect。提供Username和Password，然後按一下OK。



VPN使用者端

使用者流動裝置必須收到DUO推送通知。批准。已建立VPN連線。

1:52



Search

Accounts (8)

Add



Cisco
Cisco



Are you logging in to Auth API?

🌐 Cisco

🕒 1:52 PM

👤 bob

MFA相關日誌	policy-engine	ise-psc.log	DuoMfaAuthApiUtils -::: — 已向Duo Client Manager提交請求 DuoMfaAuthApiUtils → Duo響應
策略相關日誌	prrt-JNI	prrt-management.log	RadiusMfaPolicyRequestProcessor TacacsMfaPolicyRequestProcessor
身份驗證相關日誌	運行時AAA	prrt-server.log	MfaAuthenticator::onAuthenticateEvent MfaAuthenticator::sendAuthenticateEvent MfaAuthenticator::onResponseEvaluatePolicyEvent
DUO身份驗證、ID同步相關日誌		duo-sync-service.log	

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）。