

配置具有Duo SSO的RA-VPNaaS的安全訪問和具有ISE的狀況評估

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[網路圖表](#)

[設定](#)

[Duo配置](#)

[安全訪問配置](#)

[在IP池上配置Radius組](#)

[配置VPN配置檔案以使用ISE](#)

[一般設定](#)

[驗證、授權和記帳](#)

[TrafficSteering](#)

[思科安全客戶端配置](#)

[ISE配置](#)

[配置網路裝置清單](#)

[配置組](#)

[配置本地使用者](#)

[配置策略集](#)

[配置策略集授權](#)

[配置Radius本地或Active Directory使用者](#)

[配置ISE終端安全評估](#)

[配置狀態條件](#)

[配置狀態要求](#)

[配置狀態策略](#)

[設定使用者端啟動設定](#)

[配置客戶端調配策略](#)

[建立授權配置檔案](#)

[配置狀態策略集](#)

[驗證](#)

[狀態驗證](#)

[電腦上的連線](#)

[如何驗證ISE中的日誌](#)

[合規性](#)

[不合規性](#)

[安全訪問和ISE整合的第一步](#)

[疑難排解](#)

[如何下載ISE終端安全評估調試日誌](#)

[如何驗證安全訪問遠端訪問日誌](#)

簡介

本文檔介紹如何為使用身份服務引擎(ISE)的遠端訪問VPN使用者配置安全評估以及使用Duo的安全訪問。

必要條件

- [在Secure Access上配置使用者調配](#)
- 使用認證代理或第三方IDP配置Duo [SSO](#)
- 思科ISE透過隧道連線到安全訪問

需求

思科建議您瞭解以下主題：

- [身分辨識服務引擎](#)
- [安全存取](#)
- [思科安全使用者端](#)
- [雙因素身份驗證指南- Duo Security](#)
- ISE終端安全評估
- 驗證、授權和記帳

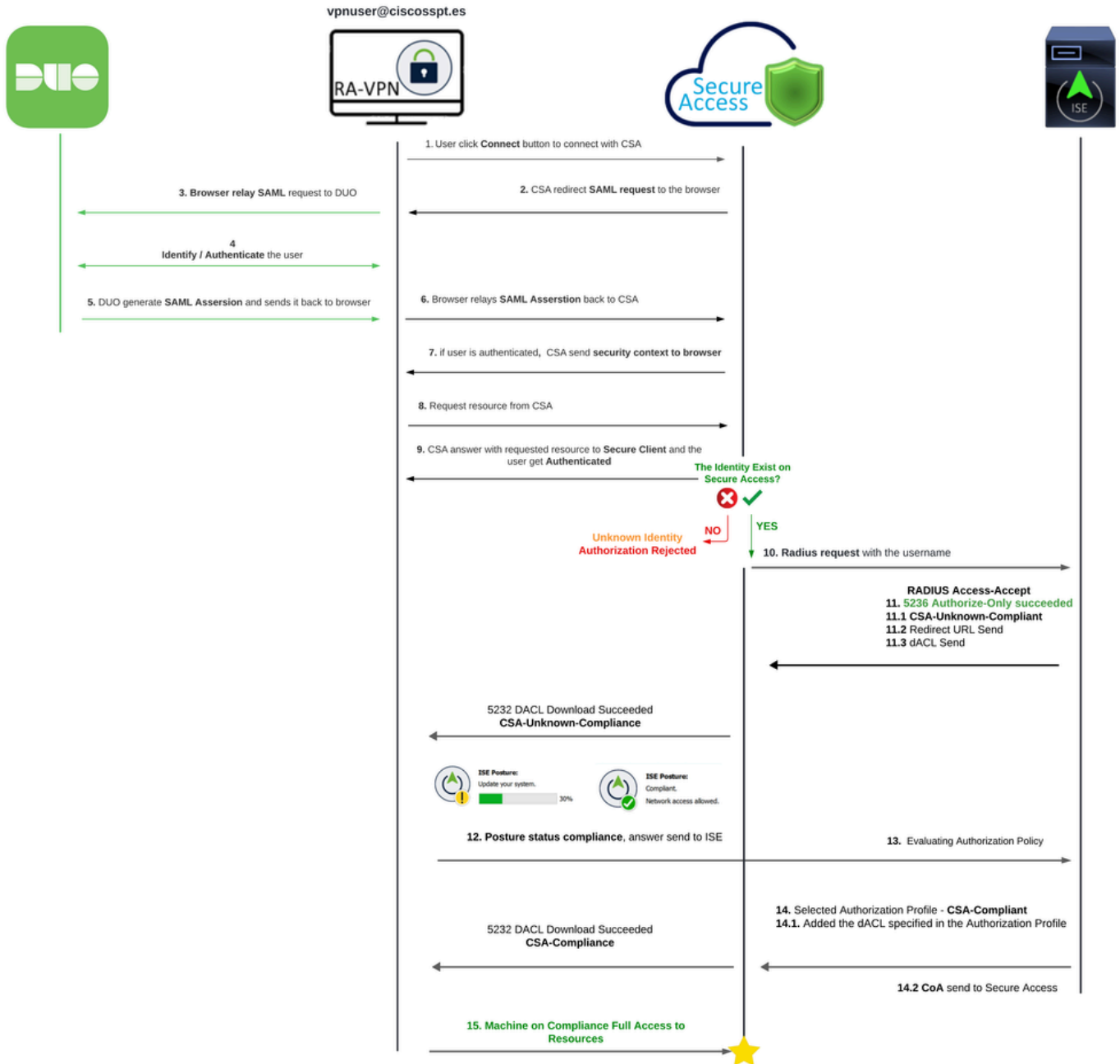
採用元件

本文檔中的資訊基於：

- 身分辨識服務引擎(ISE)版本3.3修補程式1
- 安全存取
- 思科安全客戶端- Anyconnect VPN版本5.1.2.42

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



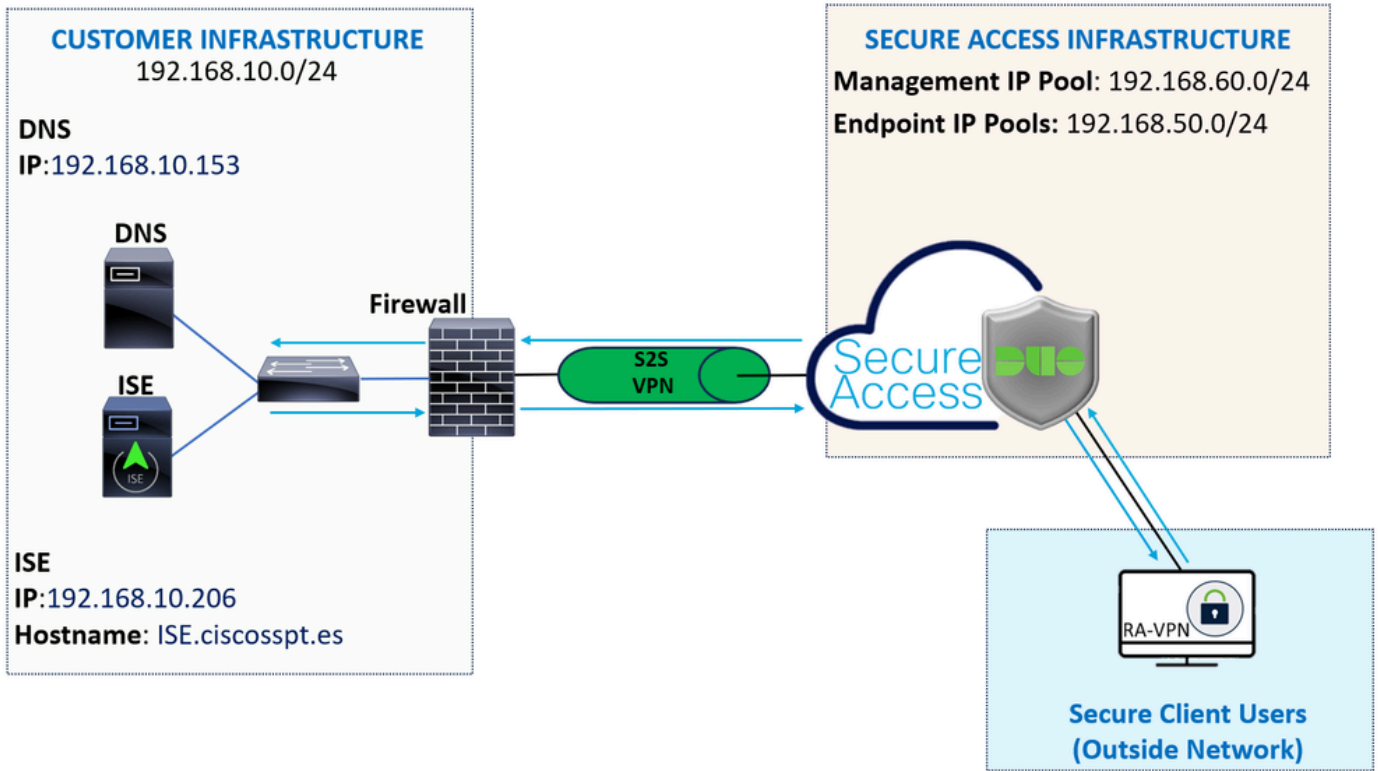
將Duo SAML與思科身份服務引擎(ISE)整合可增強身份驗證過程，為思科安全訪問解決方案增加一層安全保護。Duo SAML提供單一登入(SSO)功能，可簡化使用者登入程式，同時確保高安全性標準。

一旦透過Duo SAML進行身份驗證，授權過程由Cisco ISE處理。這允許根據使用者身份和裝置狀態做出動態訪問控制決策。ISE可以實施詳細策略，規定使用者可以訪問哪些資源、何時訪問以及從哪些裝置訪問哪些資源。



注意：要配置RADIUS整合，您需要確保兩個平台之間有通訊。

網路圖表



設定

注意：在開始配置過程之前，您必須完成[安全訪問和ISE整合的第一步](#)。

Duo配置

要配置RA-VPN應用，請繼續執行以下步驟：

導航至[Duo管理面板](#)

- 導覽至 Applications > Protect an Application
 - 搜尋 Generic SAML Service Provider
 - 按一下 Protect

Protect an Application

Generic SAML Service Provider

Application

Protection Type



Generic SAML Service Provider

2FA with SSO hosted by Duo
(Single Sign-On)

[Documentation](#)

Protect

您必須在螢幕上顯示應用程式；請記住VPN配置的應用程式名稱。

Successfully added Generic SAML Service Provider - Single Sign-On to protected applications.
[Add another.](#)

Dashboard > Applications > Generic SAML Service Provider - Single Sign-On

Generic SAML Service Provider - Single Sign-On

[Authentication Log](#) | [Remove Application](#)

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/metadata</code>	Copy
Single Sign-On URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/sso</code>	Copy
Single Log-Out URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/slo</code>	Copy
Metadata URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNNK5L9LR7Z/metadata</code>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<code>05:76:95:6B:E1:7C:F7:D1:79:12:2C:23:B6:1A:63:59:32:01:88:B1</code>	Copy
SHA-256 Fingerprint	<code>CF:CB:25:7C:41:0D:81:49:E5:83:48:79:EA:6B:45:C9:9F:4A:9A:21:A9:72:32:D3:C1:7F:86:4</code>	Copy

在本例中為 **Generic SAML Service Provider**。

安全訪問配置

在IP池上配置Radius組

要使用Radius配置VPN配置檔案，請繼續執行以下步驟：

導航到[安全訪問控制台](#)。



- 按一下 **Connect > Enduser Connectivity > Virtual Private Network**
- 在「您的池配置」(Manage IP Pools)下，按一下Manage

Manage IP Pools

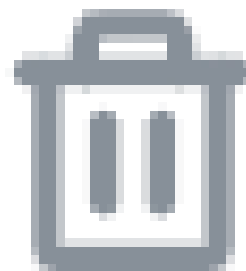
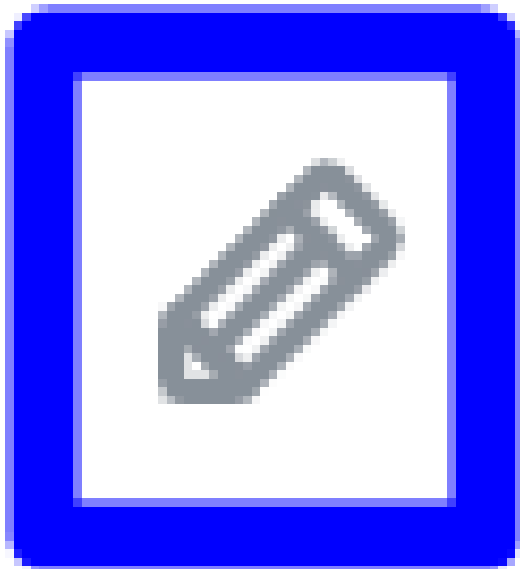
Manage

2 Regions mapped

- 選擇IP Pool Region 並配置 Radius Server

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	 

- 按一下要編輯的鉛筆



- 現在，在IP Pool section configuration **Radius Group (Optional)**
- 按一下 Add RADIUS Group

RADIUS Groups (optional)

Associate one RADIUS group per AAA method to this IP pool.



No RADIUS groups created

Add RADIUS Group

← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings



RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA ×



+ Add

#	Server Name	IP Address		
1	ISE_CSA	192.168.10.206		

整合的名稱

- **AAA method**

- **Authentication**：標籤Authentication 的覈取方塊，並選擇埠，預設值為1812

- 如果身份驗證需要Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2)，請選中覈取方塊

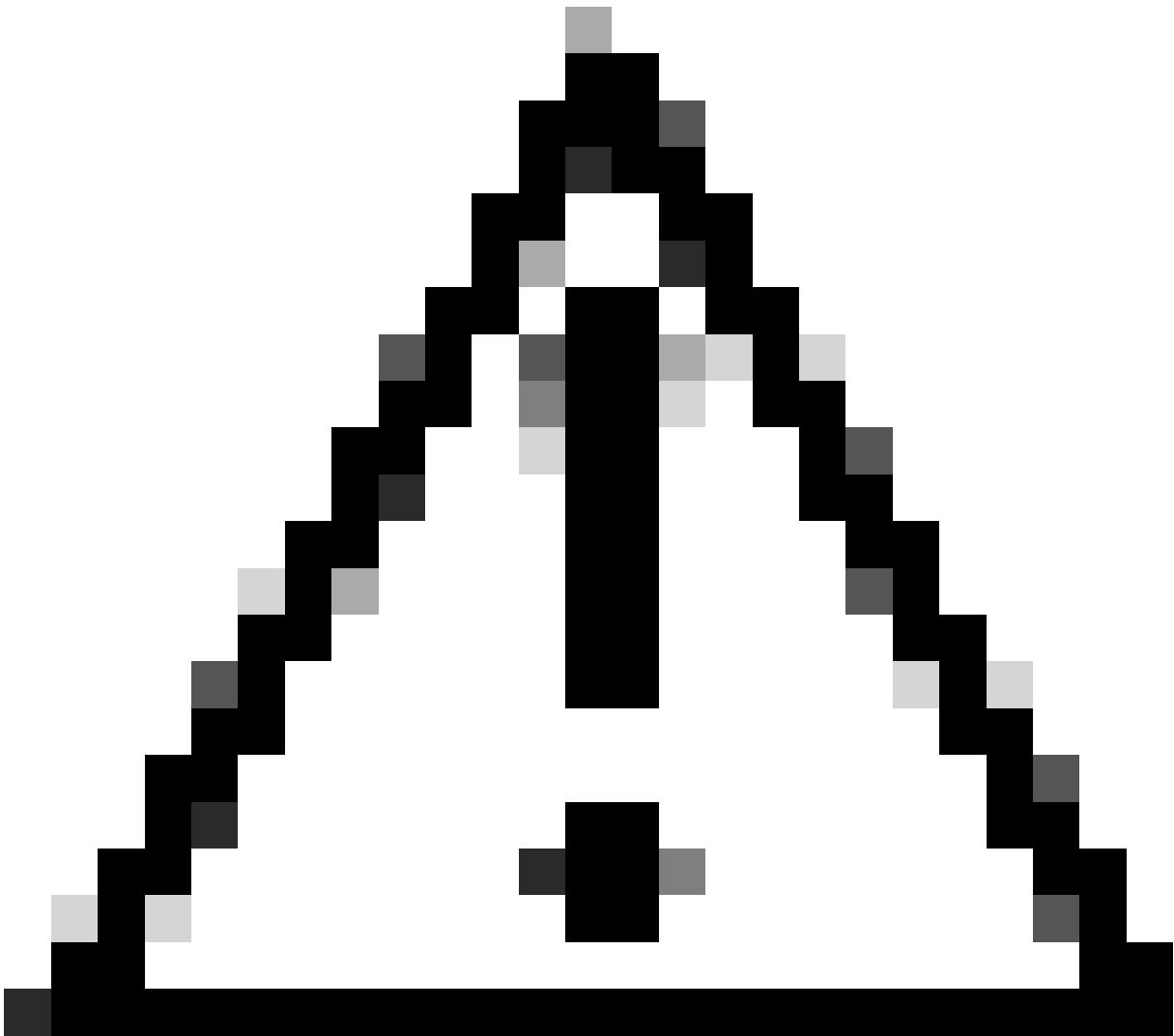
- **Authorization**：標籤Authorization覈取方塊並選擇埠，預設情況下為1812

- 標籤Authorization mode Only Change of Authorization (CoA) mode 覈取方塊，然後允許來自ISE的狀態和更改

- **Accounting**：選中Authorization覈取方塊，並選擇預設埠為1813

- 選擇Single or Simultaneous (在單模式中，記帳資料僅傳送到一台伺服器。在同步模式中，將資料記賬到群組中的所有伺服器)

- 選中 Accounting update 覈取方塊，以啟用定期生成RADIUS interim-accounting-update消息。



注意：選取時Authentication和Authorization 方法必須使用相同的連線埠。

-
- 之後，您需要在 **RADIUS Servers**部分配置用於透過AAA進行身份驗證的**RADIUS Servers (ISE)**：
 - 按一下 + Add

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

+ Add

#	Server Name	IP Address
---	-------------	------------

- 然後，配置以下選項：

Add RADIUS Server

Server name

IP Address

Password type

Secret Key

Show

Password

Show

Cancel

Save & Add server

Save

- **Server Name** : 配置名稱以標識您的ISE伺服器。
 - **IP Address** : 配置可透過安全訪問訪問的思科ISE裝置的IP
 - **Secret Key** : 配置您的RADIUS金鑰
 - **Password** : 配置您的Radius密碼
-
- 點選**Save** 並在Assign Server選項下分配您的RADIUS伺服器，然後選擇您的ISE伺服器：

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

^

ISE_CSA

[+ Add](#)

- 再次**Save** 按一下以儲存完成的所有配置

← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings



RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE_CSA ×



+ Add

#	Server Name	IP Address		
1	ISE_CSA	192.168.10.206		

◦ **Protocols:選擇 SAML**

- 按一下 Download Service Provider XML file
- 替換步驟 [Duo Configuration](#) 中配置的應用程式中的資訊

The screenshot shows the Duo configuration interface for a Service Provider. On the left, there is an XML snippet for SAML metadata. On the right, there are configuration fields for the Service Provider. Arrows indicate the mapping between the XML fields and the configuration fields:

- Entity ID:** The XML field `entityID="https://...vpn.sse.cisco.com/saml/sp/metadata/ISE_CSA_SAML"` is mapped to the `Entity ID *` field in the configuration, which contains `https://...vpn.sse.cisco.com/saml/sp/metadata/ISE_CSA_SAML`.
- Assertion Consumer Service (ACS) URL:** The XML field `Location="https://...vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=ISE_CSA_SAML"` is mapped to the `Assertion Consumer Service (ACS) URL *` field in the configuration, which contains `http://...vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname`.
- Single Logout URL:** The XML field `Location="https://...vpn.sse.cisco.com/+CSCOE+/saml/sp/logout"` is mapped to the `Single Logout URL` field in the configuration, which contains `http://...vpn.sse.cisco.com/+CSCOE+/saml/sp/logout`.

- 配置好該資訊後，請將Duo的名稱更改為與您正在進行的整合相關的名稱

Settings

Type Generic SAML Service Provider - Single Sign-On

Name

ISE - SAML

Duo Push users will see this when approving transactions.

- 在DuoSave 上按一下您的應用程式。
- 點選Save後，必須點選SAML Metadata 該按鈕下載 **Download XML**

ISE - SAML

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

Metadata

Entity ID	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadat</code>	Copy
Single Sign-On URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/sso</code>	Copy
Single Log-Out URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/slo</code>	Copy
Metadata URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadat</code>	Copy

Certificate Fingerprints

SHA-1 Fingerprint	<code>53:0E:25:4F:29:3A:B5:DF:09:A2:0D:BB:08:C7:F6:E8:D9:DB:DE:6B</code>	Copy
SHA-256 Fingerprint	<code>C5:6F:35:44:F8:FC:74:C6:E6:2B:C1:8F:92:9C:E2:80:91:B1:61:C9:75:0B:F9:C5:4B:81:B8:F</code>	Copy

Downloads

Certificate	Download certificate	Copy certificate	Expires: 01-19-2038
SAML Metadata	Download XML		

- 上傳SAML Metadata 選項下的Secure Access3. Upload IdP security metadata XML file 並按一下 Next

VPN Profile name


ISE_CSA_SAML

- ✓ **General settings**
Default Domain: ciscosspt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IPsec (IKEv2)
- 2 Authentication, Authorization, and Accounting SAML**
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 1 Exceptions
- ✓ **Cisco Secure Client Configuration**


Authenticate with CA certificates
Select to use CA certificates to authenticate this VPN profile.


SAML Configuration

SAML Metadata XML Configuration

 **1. Download Service Provider XML file**
This XML file contains metadata required to configure your IdP.

[Download service provider XML file](#)

 **2. Generate IdP Security Metadata XML File**
a. Upload the Service Provider XML file to your IdP.
b. From your IdP, create and download an IdP Security Metadata XML file.

 **3. Upload IdP security metadata XML file**

✓ File 'ISE - SAML - IDP Metadata.xml' uploaded. [Replace](#) [Delete](#)

Manual Configuration

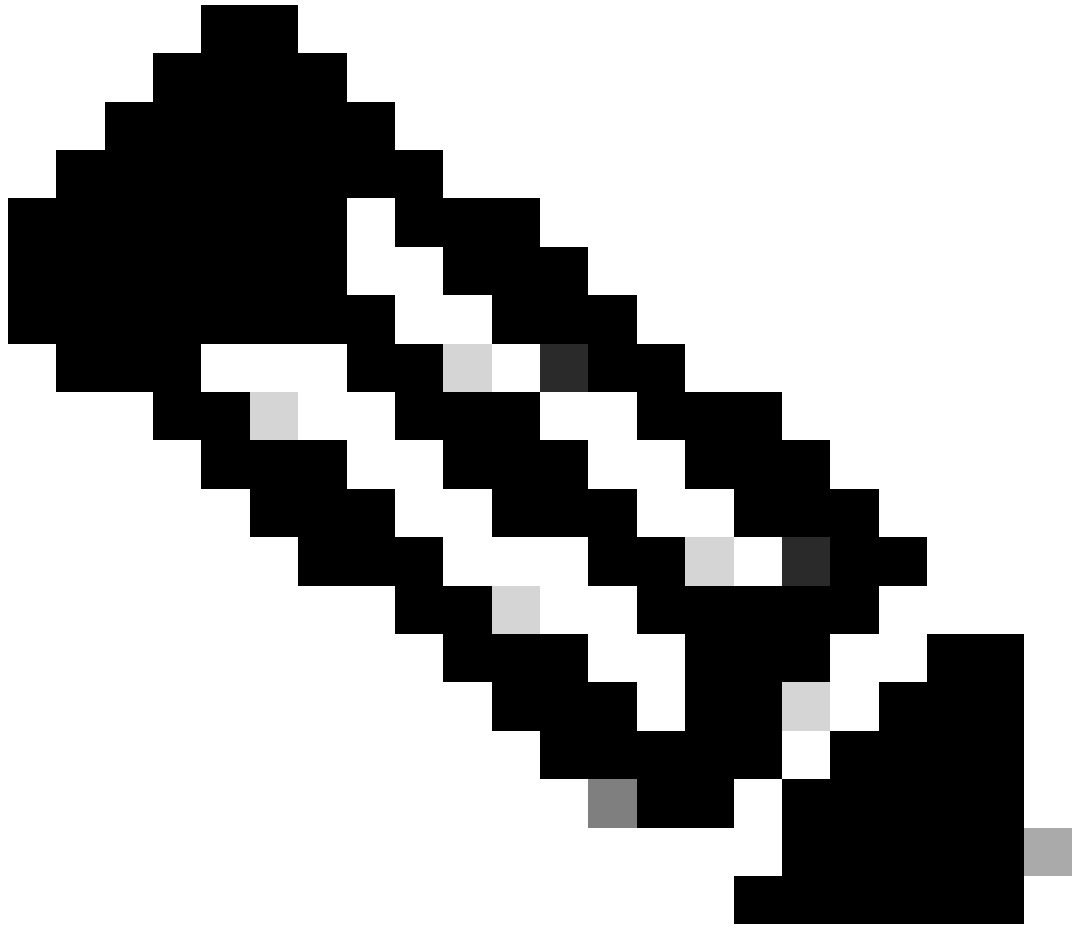


Cancel

Back

Next

繼續進行授權。



注意：配置使用SAML的身份驗證後，您將透過ISE對其進行授權，這意味著安全訪問傳送的RADIUS資料包將僅包含使用者名稱。此處的密碼欄位不存在。

Authorization

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication **Authorization** Accounting

Enable Radius Authorization

Use defaults or customize groups to map to regions

Select one group for all regions

[+ Group](#)

ISE_CSA

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)



Cancel

Back

Next

- **Authorization**

- **Enable Radius Authorization** : 選中該覈取方塊以啟用RADIUS授權

- 為所有區域選擇一個組 : 選中該覈取方塊, 為所有遠端訪問-虛擬專用網路(RA-VPN)池使用一個特定RADIUS伺服器, 或為每個池單獨定義該伺服器

- 按一下 **Next**

配置完所有**Authorization** 部件後, 請繼續執行 **Accounting**。



注意：如果您不啟用 **Radio Authorization**，狀態將無法工作。

- ✓ **General settings**
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication Authorization Accounting

Enable Radius Accounting
Use defaults or customize groups to map to regions

Select one group for all regions

[+ Group](#)

ISE_CSA

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)



Cancel

Back

Next

- **Accounting**
 - **Map Authorization groups to regions** : 選擇地區並選擇 **Radius Groups**

- 按一下 **Next**

After you have done configured the Authentication, Authorization and Accounting 請繼續Traffic Steering。

流量引導

在流量引導下，您需要透過安全訪問配置通訊型別。

Tunnel Mode

Connect to Secure Access

All traffic is steered through the tunnel.



Tunnel Mode

Bypass Secure Access

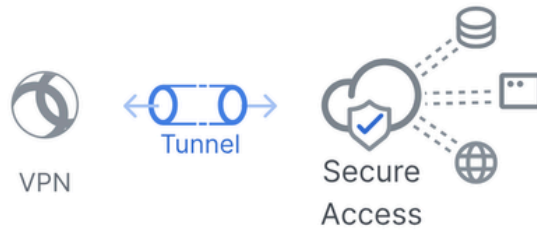
All traffic is steered outside the tunnel.



- 如果您選擇 **Connect to Secure Access**，您的所有Internet流量都將透過 **Secure Access**

Connect to Secure Access

All traffic is steered through the tunnel.



Add Exceptions

Destinations specified here will be steered **OUTSIDE** the tunnel.

+ Add

Destinations

Exclude Destinations

Actions

proxy-
8195126.zpc.sse.cisco.com,
ztna.sse.cisco.com,acme.sse.
cisco.com,devices.api.umbrell
a.com,sseposture-routing-
commercial.k8s.5c10.org,sse
posture-routing-
commercial.posture.duosecuri
ty.com,data.eb.thousandeyes.

-

-

Cancel

Back

Next

如果要為Internet域或IP增加排除項，請按一下+ Add 按鈕，然後按一下Next。

- 如果您決定 **Bypass Secure Access**，則所有網際網路流量都將透過您的網際網路提供商，而不是透過Secure Access（無網際網路保護）

Tunnel Mode

Bypass Secure Access ▼

All traffic is steered outside the tunnel.



Add Exceptions

Destinations specified here will be steered **INSIDE** the tunnel.

[+ Add](#)

Destinations

Exclude Destinations

Actions



No matches found

[Cancel](#)

[Back](#)

[Next](#)



注意：請在選擇Bypass Secure Access時增加enroll.cisco.com 用於ISE終端安全評估。

在此步驟中，選擇希望透過VPN訪問的所有專用網路資源。要執行此操作，請按一下 + Add，然後按一下Next 何時增加所有資源。

思科安全客戶端配置

在此步驟中，您可以將所有內容均保留為預設值並按一下 **Save**，但如果要自定義配置的詳細資訊，請檢視 [Cisco Secure Client 管理員指南](#)。

Name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL
ISE_CSA_SAML	ciscospt.es TLS, IPsec (IKEv2)	SAML RADIUS	Connect to Secure Access 1 Exception(s)	13 Settings	vpn.sse.cisco.com/ISE_CSA_SAML

ISE 配置

配置網路裝置清單


要配置透過思科ISE的身份驗證，您需要配置可以向思科ISE進行查詢的允許裝置：

- 導覽至 **Administration > Network Devices**
- 按一下 **+ Add**

Network Devices

Name CSA

Description _____

IP Address * IP : 192.168.60.0 / 24 


Device Profile  Cisco 

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](#)

- **Name** : 使用名稱標識安全訪問
- **IP Address** : 配置步驟的Management Interface , [IP池區域](#)
- **Device Profile** : 選擇思科
 - **Radius Authentication Settings**
 - **Shared Secret** : 配置在步驟中配置的相同共用金鑰 , 即[金鑰](#)
 - **CoA Port** : 將其設為預設值 ; 1700也用於安全訪問

完成後 , 按一下Save要驗證整合是否正常工作 , 請繼續建立本地使用者進行整合驗證。

配置組

要配置用於本地使用者的組 , 請繼續執行以下步驟 :

- 按一下 **Administration > Groups**
- 按一下 **User Identity Groups**
- 按一下 + Add
- 為組建立Name一個並按一下 **Submit**

The screenshot displays the 'Administration' menu on the left, with 'Identities' > 'Groups' selected (2). The 'Identity Groups' sidebar on the right shows 'User Identity Groups' selected (3). The main area is titled 'User Identity Groups' and shows a 'New User Identity Group' form. The 'Name' field is filled with 'CSA-ISE' (5). The 'Add' button is highlighted (4), and the 'Submit' button is highlighted (6). A table on the right lists existing groups: 'ALL_ACCOUNTS (default)', 'CSA-ISE' (with a 'GROUP CREATED' status), and 'Employee'.

配置本地使用者

設定本機使用者以驗證您的整合：

- 導覽至 **Administration > Identities**
- 按一下 **Add +**

Network Access User

* Username

Status Enabled ▼

Account Name Alias ⓘ

Email

Passwords

Password Type: ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

	Password	Re-Enter Password	
* Login	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ
Enable	<input type="text"/>	<input type="text"/>	<input type="button" value="Generate Password"/> ⓘ

User Groups

⋮
CSA-ISE ▼
🗑️
+

- **Username** : 在Secure Access中使用已知UPN調配配置使用者名稱；這基於步驟[前提條件](#)
- **Status** : 活動
- **Password Lifetime** : 您可以根據您的**With Expiration** 或**Never Expires**配置它
- **Login Password** : 為使用者建立密碼
- **User Groups** : 選擇在步驟[配置組](#)上建立的組

注意：基於UPN的身份驗證被設定為在即將推出的安全訪問版本中更改。

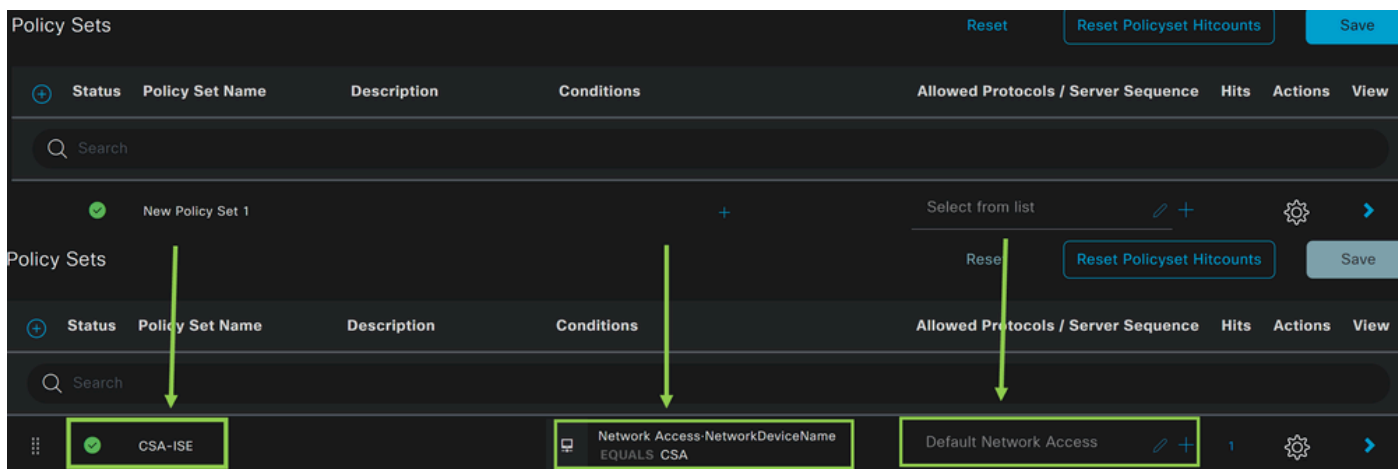
之後，您可以進Save 行組態設定，並繼續步驟 **Configure Policy Set**。

配置策略集

在策略集下，配置ISE在身份驗證和授權期間執行的操作。此場景演示了配置簡單策略以提供使用者訪問許可權的使用案例。首先，ISE驗證RADIUS身份驗證的源並檢查ISE使用者資料庫中是否存在用於提供訪問許可權的身份

要配置該策略，請導航到您的Cisco ISE控制台：

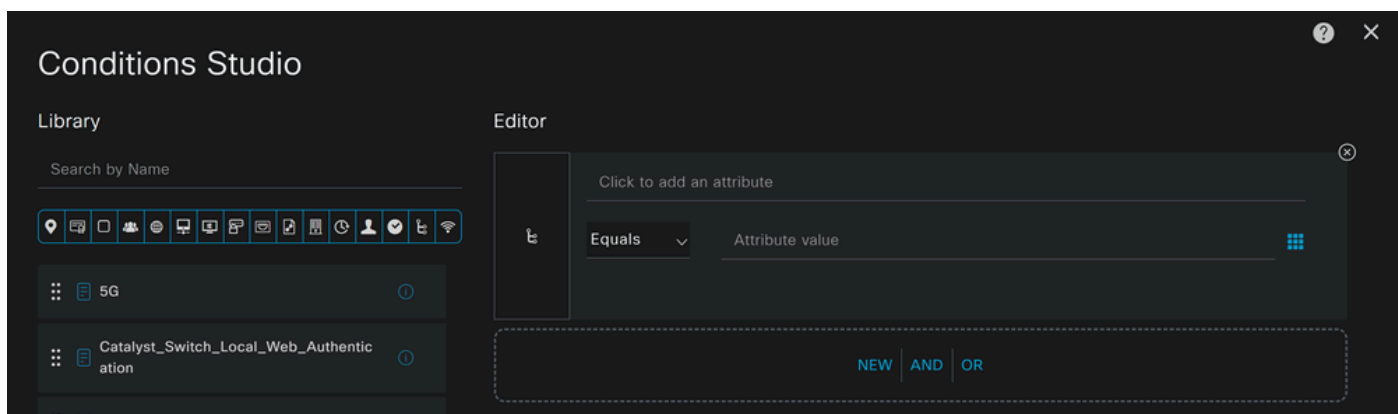
- 按一下 Policy > Policy Sets
- 點選+ 以增加新策略集



在這種情況下，請建立一個新的策略集，而不是使用預設策略集。然後，根據該策略集配置身份驗證和授權。配置的策略允許訪問在 [配置網路裝置清單](#) 步驟中定義的網路裝置，以驗證這些身份驗證來自CSA Network Device List，然後以Conditions的身份進入策略。最後是允許的協定，如Default Network Access。

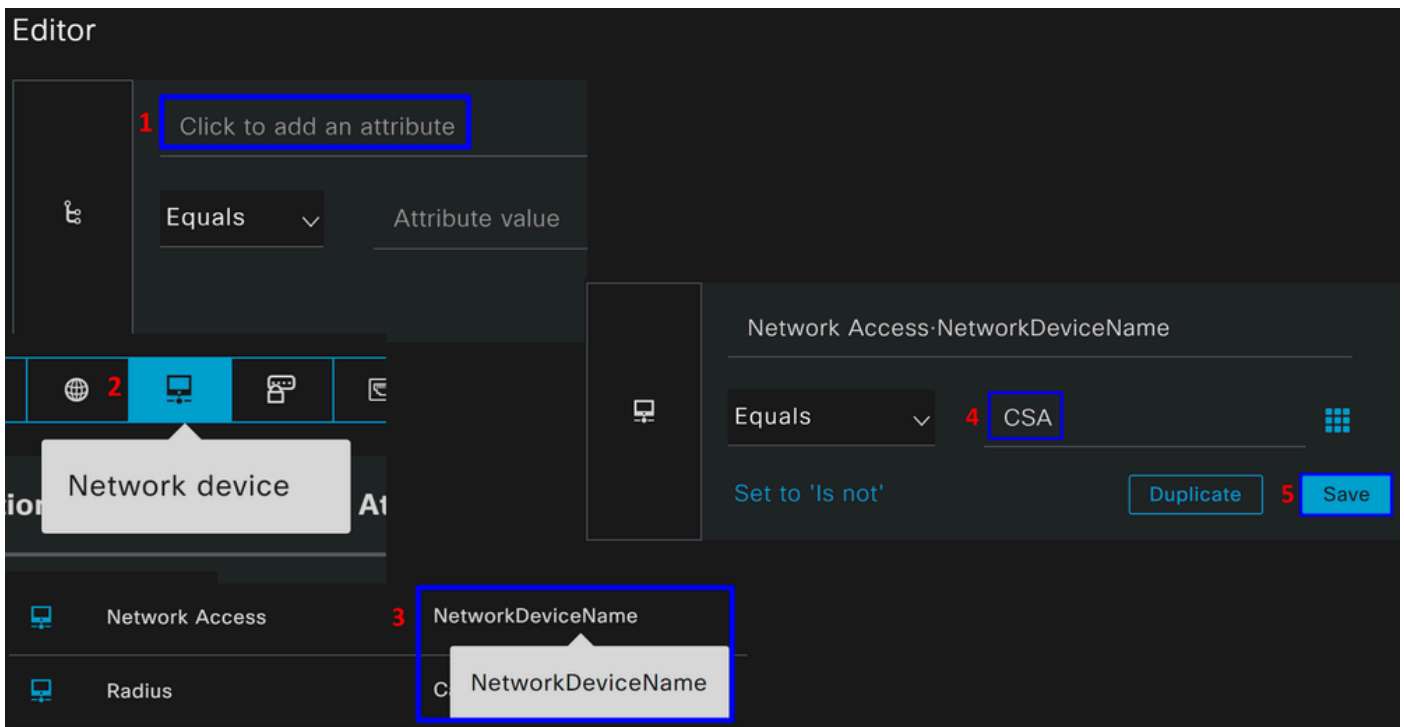
要建立與策略集匹配的condition 策略，請按照以下說明進行操作：

- 按一下 +
- 在 Condition Studio下，可用的資訊包括：



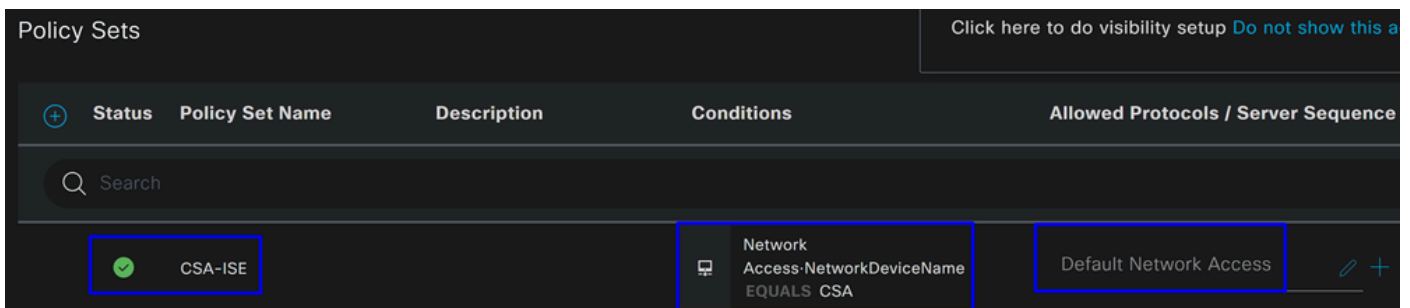
- 若要建立條件，請按一下 Click to add an attribute
- 按一下Network Device 按鈕
- 在後面的選項下，按一下Network Access -Network Device Name 選項
- 在Equals選項下，在步驟[Configure Network Devices List](#)下寫入Network Device 的名稱

- 按一下 **Save**



此策略僅批准源CSA的請求以繼續策略集 **CSA-ISE**下的**Authentication** 和**Authorization** 設定，並且還會根據允許協定 **Default Network Access** 的來驗證允許的協定。

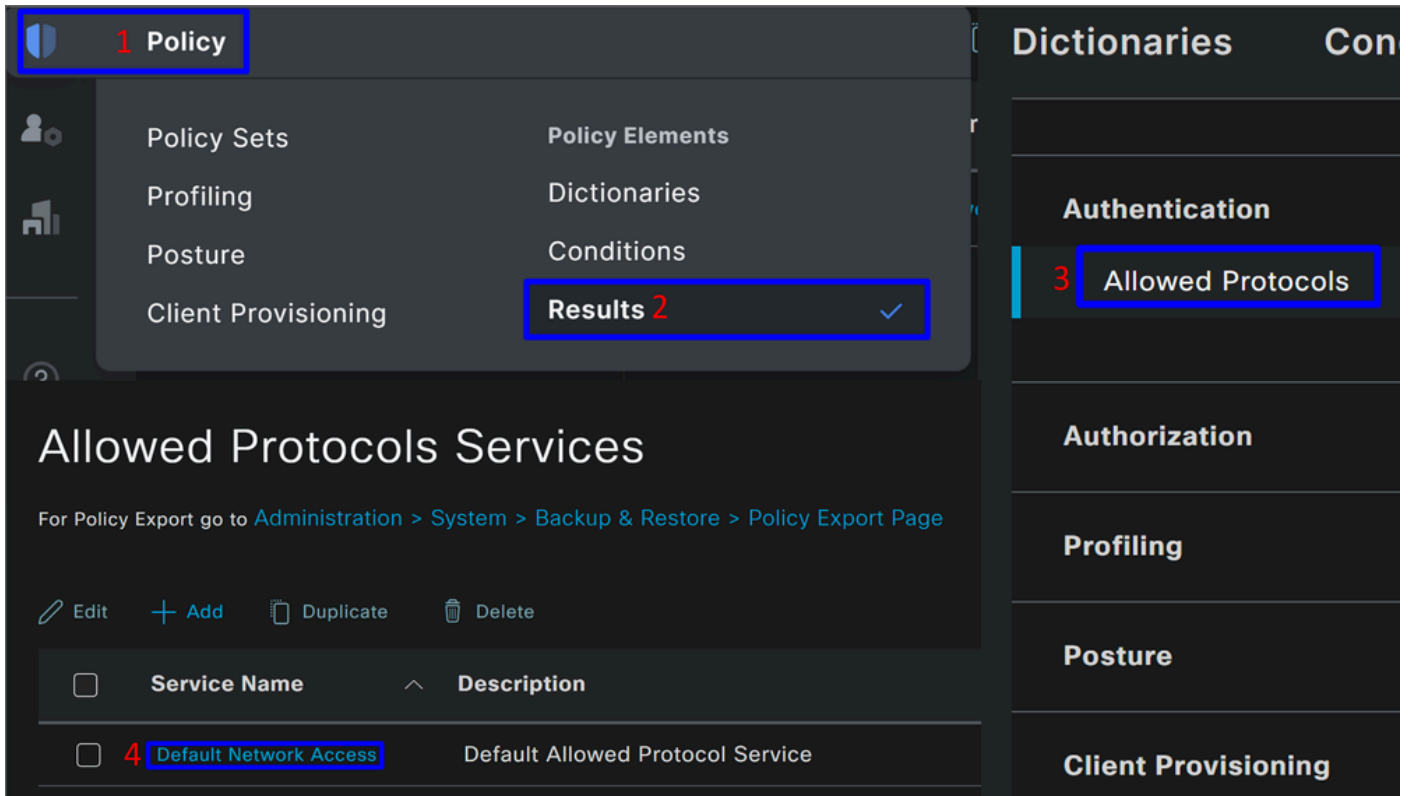
定義的策略的結果必須是：



- 要驗證**Default Network Access Protocols** 允許的情況，請繼續下面的說明：

- 按一下 **Policy > Results**

- 按一下 **Allowed Protocols**
- 按一下 **Default Network Access**

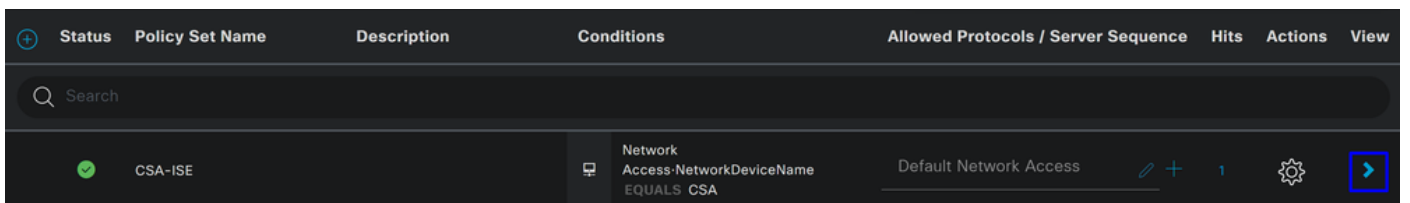


- 然後，您會看到在上允許的所有協定 **Default Network Access**

配置策略集授權

要在 **Policy Set** 下建立策略 **Authorization** 略，請執行以下步驟：

- 按一下 >



- 之後，您會看到顯示 **Authorization** 的策略：

Policy Sets → CSA-ISE Click here to do visibility setup Do not show this again.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	27
<ul style="list-style-type: none"> > Authentication Policy(2) > Authorization Policy - Local Exceptions > Authorization Policy - Global Exceptions <li style="border: 1px solid blue; padding: 2px;">> Authorization Policy(7) 					

此策略與[配置策略集](#)步驟中定義的策略相同。

授權策略

可以透過多種方式配置授權策略。在這種情況下，僅授權在[配置組](#)步驟中定義的組中的使用者。請參閱以下示例配置您的授權策略：

Authorization Policy(2)

			Results		
+ Status	Rule Name	Conditions	Profiles	Security Groups	
✓	Authorization Rule 1		Select from list	Select from list	
<ul style="list-style-type: none"> > Authorization Policy(2) 					
+ Status	Rule Name	Conditions	Profiles	Security Groups	
✓	Authorization Secure Access	InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list	

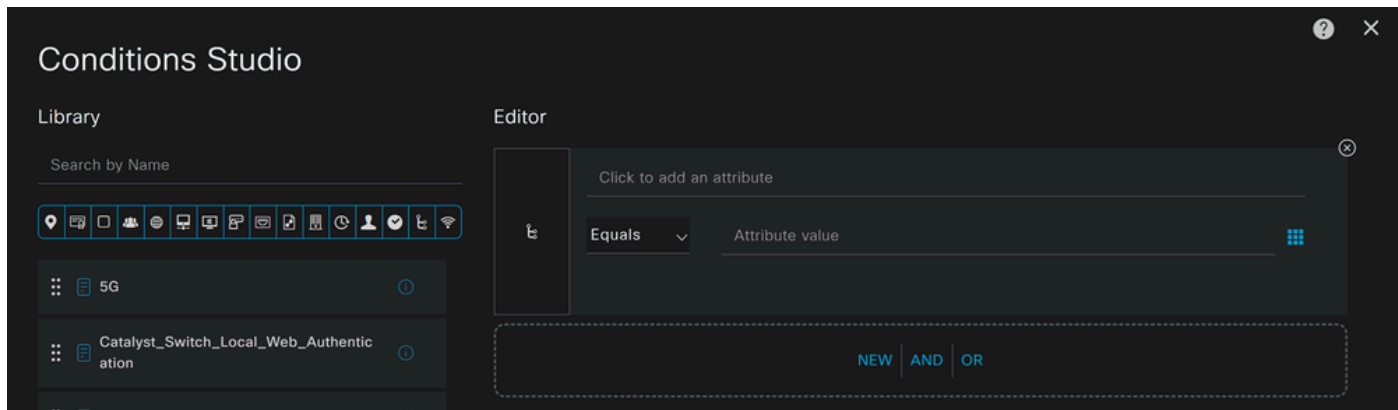
- 按一下 **Authorization Policy**
- 點選+ 以定義授權策略，如下所示：

Authorization Policy(2)

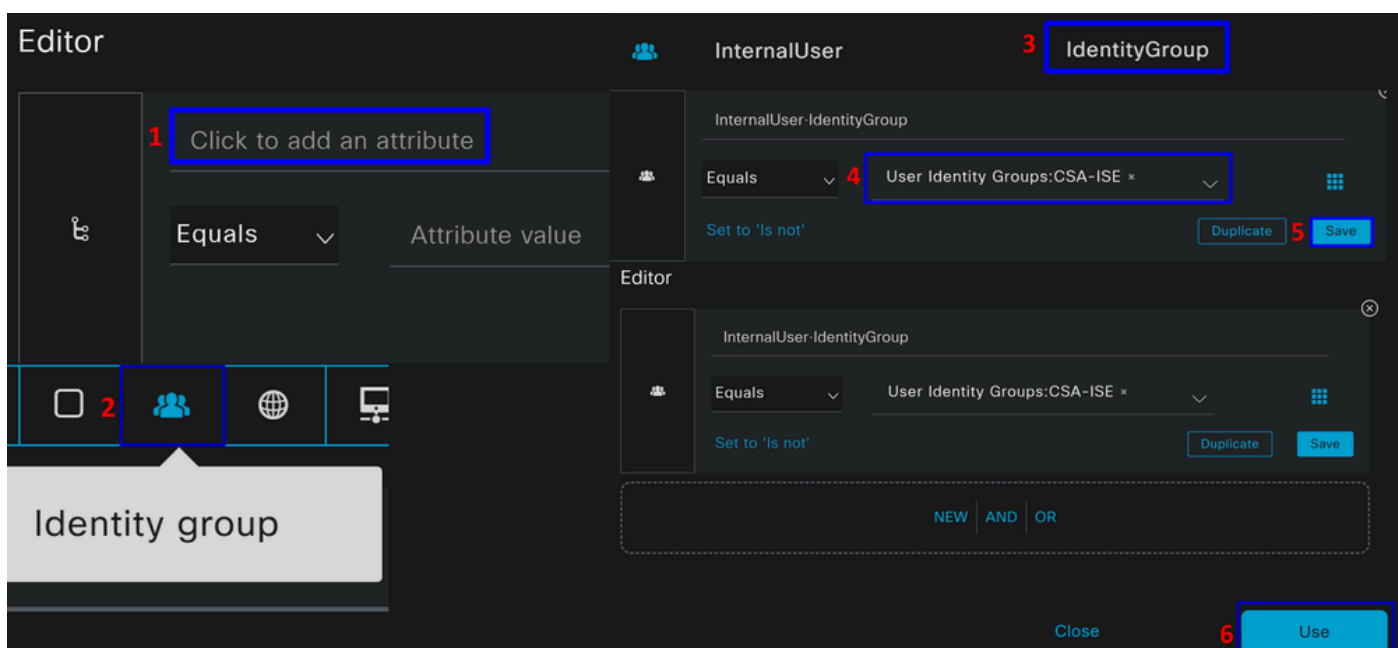
			Results		
+ Status	Rule Name	Conditions	Profiles	Security Groups	
✓	Authorization Rule 1		Select from list	Select from list	

- 在下一步中，更改Rule Name，和Conditions Profiles

- 設定Name 配置名稱以輕鬆辨識授權策略時
- 要配置 Condition，請點選 +
- 在 Condition Studio下，您可以找到以下資訊：



- 若要建立條件，請按一下 Click to add an attribute
- 按一下Identity Group 按鈕
- 在後面的選項下，按一下Internal User - IdentityGroup option
- 在Equals 選項下，使用下拉選單查詢步驟配置組中的Group 批准進行身份驗證
- 按一下 Save
- 按一下 Use



之後，您需要定義 Profiles, which help approve user access under the authorization policy once the user authentication matches the group

selected on the policy.

- 在 **Authorization Policy** 下，按一下 **Profiles**
- 搜尋允許
- 選取 **PermitAccess**
- 按一下 **Save**

The screenshot displays the configuration page for an Authorization Policy in Cisco ISE. The policy is named 'InternalUser-IdentityGroup' and is associated with the 'EQUALS User Identity Groups:CSA-ISE'. The 'Profiles' section shows a list of profiles, with 'PermitAccess' selected. The 'Save' button is highlighted in blue, and a red '4' points to it. A red '1' points to a dropdown arrow in the top right corner. A red '2' points to the 'PermitAccess' profile name in the main list. A red '3' points to the 'PermitAccess' profile name in the 'Profiles' section.

之後，您便定義了策略 **Authorization**。驗證使用者是否連線沒有問題，以及您是否能夠看到安全訪問和ISE上的日誌。

要連線到VPN，您可以使用在Secure Access上建立的配置檔案，並透過Secure Client與ISE配置檔案進行連線。

- 當身份驗證獲得批准時，如何在Secure Access中顯示日誌？
 - 導航到[安全訪問控制台](#)
 - 按一下 **Monitor > Remote Access Log**

28 Events

User	Connection Event	Event Details	Internal IP Address	Public IP Address	VPN Profile
vpn user (vpnuser@ciscosst.es)	Connected		192.168.50.2	151.248.21.152	ISE_CSA

- 當身份驗證獲得批准時，日誌如何在ISE中顯示？

◦ 導航至 [Cisco ISE Dashboard](#)

- 按一下 **Operations > Live Logs**

Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
▼		Identity	Authentication Policy	Authorization Policy	Authorization Profiles
		vpnuser@ciscosst.es	CSA-ISE	CSA-ISE >> Authorization CSA	PermitAccess
		vpnuser@ciscosst.es	CSA-ISE	CSA-ISE >> Authorization CSA	PermitAccess

身份驗證獲得批准後，日誌如何在Duo中顯示？

- 導航至 [Duo控制台](#)
- 按一下 **Reports > Authentication Log**

Timestamp (UTC) ▼	Result	User	Application	Risk-Based Policy Assessment	Access Device	Authentication Method
10:02:34 14 DE ABR. DE 2024	Granted User approved	vpnuser	ISE - SAML	N/A	▼ iOS 17.4.1 AnyConnect 5.0.05207 Flash Not installed Java Not installed Krakow, 12, Poland 83.29.26.111 Endpoint trust is unknown because there are no active Trusted Endpoints Configurations.	▼ Duo Push Apple iPhone 15 Pro Max DPFK77EPVMXGJ7H7TMD3 Krakow, 12, Poland 83.29.26.111

配置Radius本地或Active Directory使用者

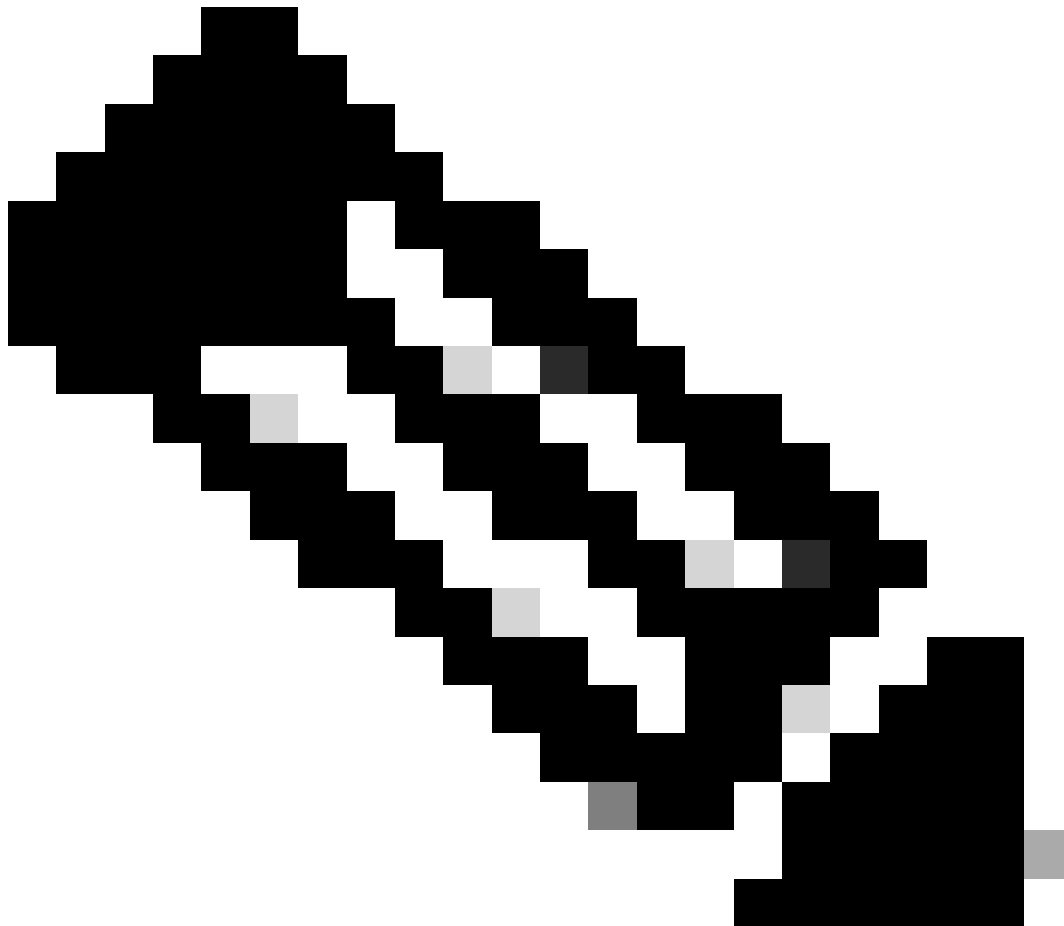
配置ISE終端安全評估

在此場景中，建立配置以驗證終端合規性，然後授予或拒絕對內部資源的訪問許可權。

要配置它，請繼續執行以下步驟：

配置狀態條件

- 導航到您的ISE控制台
 - 按一下 **Work Center > Policy Elements > Conditions**
 - 按一下 **Anti-Malware**
-



注意：您可以在此處找到許多選項，用於驗證裝置的狀態並根據內部策略進行正確的評估。

Conditions



Anti-Malware

Anti-Spyware

Anti-Virus

Application

Compound

Dictionary Compound

Dictionary Simple

Disk Encryption

External DataSource










File

Firewall

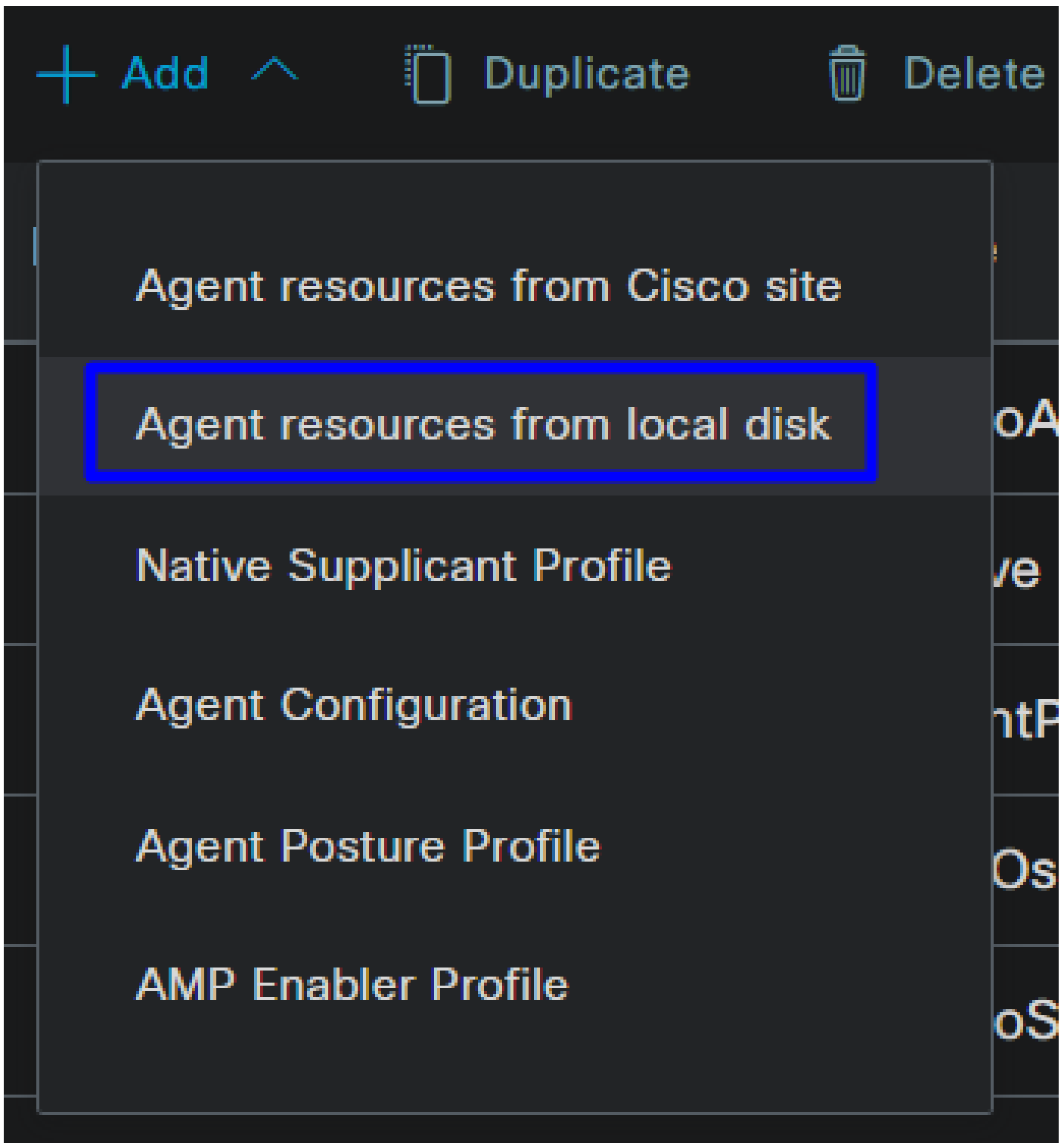
1. Agent Resources	安全使用者端Web布建套件。
2. Compliance Module	Cisco ISE合規性模組
3. Agent Profile	控制設定配置檔案。
3. Agent Configuration	使用代理配置檔案和代理資源，透過設定調配門戶來定義要調配的模組。

Step 1 下載並上傳代理資源

- 要增加新的代理資源，請導航到[Cisco下載門戶](#)並下載Web部署包；Web部署檔案必須是.pkg格式。

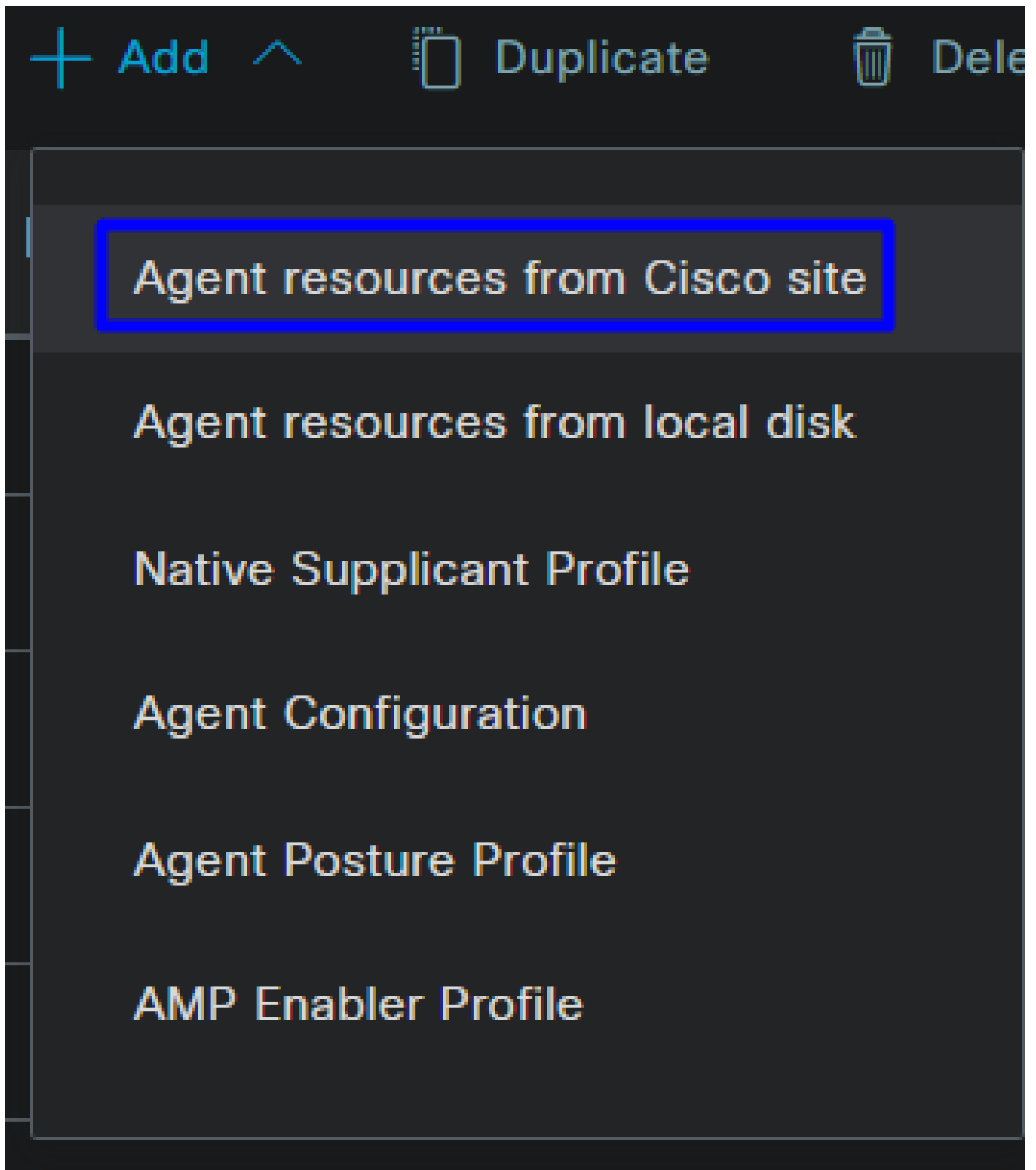
Cisco Secure Client Headend Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	58.06 MB	  
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	111.59 MB	  
Cisco Secure Client Headend Deployment Package (Mac OS) - Administrator rights or managed device required for install or upgrade. See Administrator Guide and Release Notes for details. cisco-secure-client-macos-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	118.88 MB	  

- 點選+ Add > Agent resources from local disk 並上傳包



Step 2 下載合規性模組

- 按一下 + Add > Agent resources from Cisco Site



- 選中所需每個合規性模組的覈取方塊，然後按一下 Save

Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3064.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3104.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3432.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3472.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3940.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3980.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3940....	Cisco Secure Client WindowsARM64 Compliance
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3980....	Cisco Secure Client WindowsARM64 Compliance

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save

Step 3 配置代理配置檔案

- 按一下 + Add > Agent Posture Profile

+ Add ^

☰ Duplicate

🗑️ Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- 為建Name立 Posture Profile

Agent Posture Profile

Name *



Description:

- 在「伺服器名稱規則」下，放置一個* 並在之後按一下Save

Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com*
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Step 4 配置代理配置

- 按一下 + Add > Agent Configuration

+ Add ^

☰ Duplicate

🗑 Delete

Agent resources from Cisco site

Agent resources from local disk


Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile


- 之後，配置以下引數：

* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

* Configuration Name:

Description:

Description Value Notes

* Compliance Module CiscoSecureClientComplianceModuleWi 

Cisco Secure Client Module Selection

ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input type="checkbox"/>

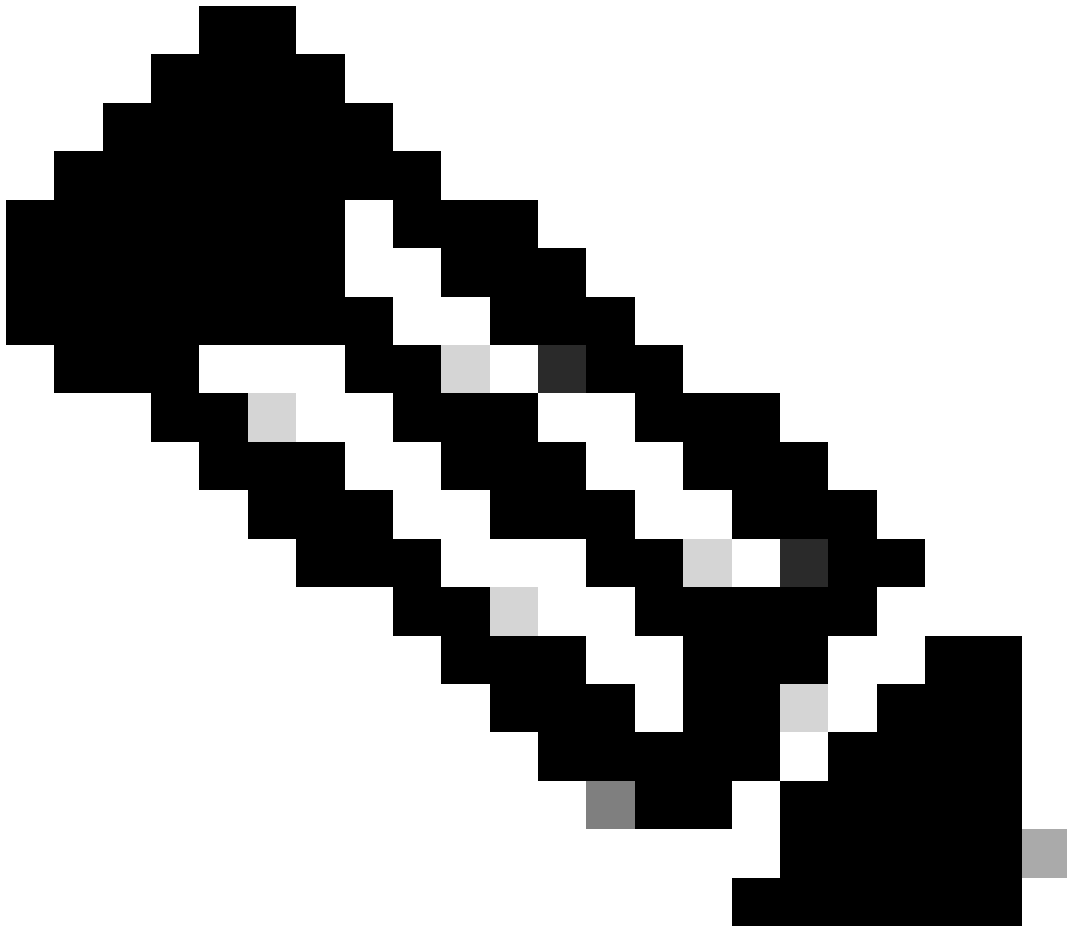
Profile Selection

* ISE Posture	1.CSA_PROFILE	∨
VPN		∨

- Select Agent Package : 選擇上傳到[步驟1下載和上傳代理資源的包](#)
- Configuration Name : 選擇一個名稱以辨識 Agent Configuration
- Compliance Module : 選擇在[步驟2下載合規性模組](#)上下載的合規性模組
- Cisco Secure Client Module Selection
 - ISE Posture : 選中覈取方塊
- Profile Selection

。 ISE Posture : 在[第3步配置代理配置檔案](#)中選擇配置的ISE配置檔案

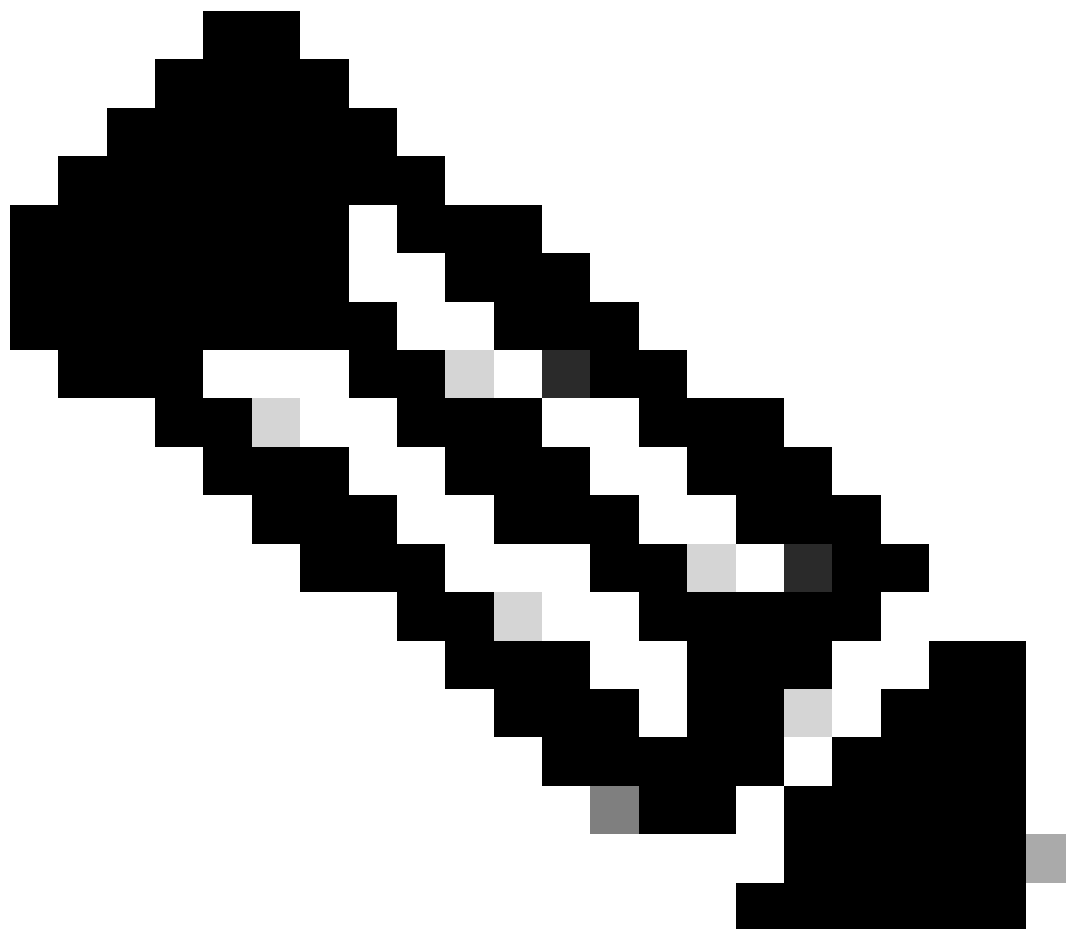
- 按一下 Save



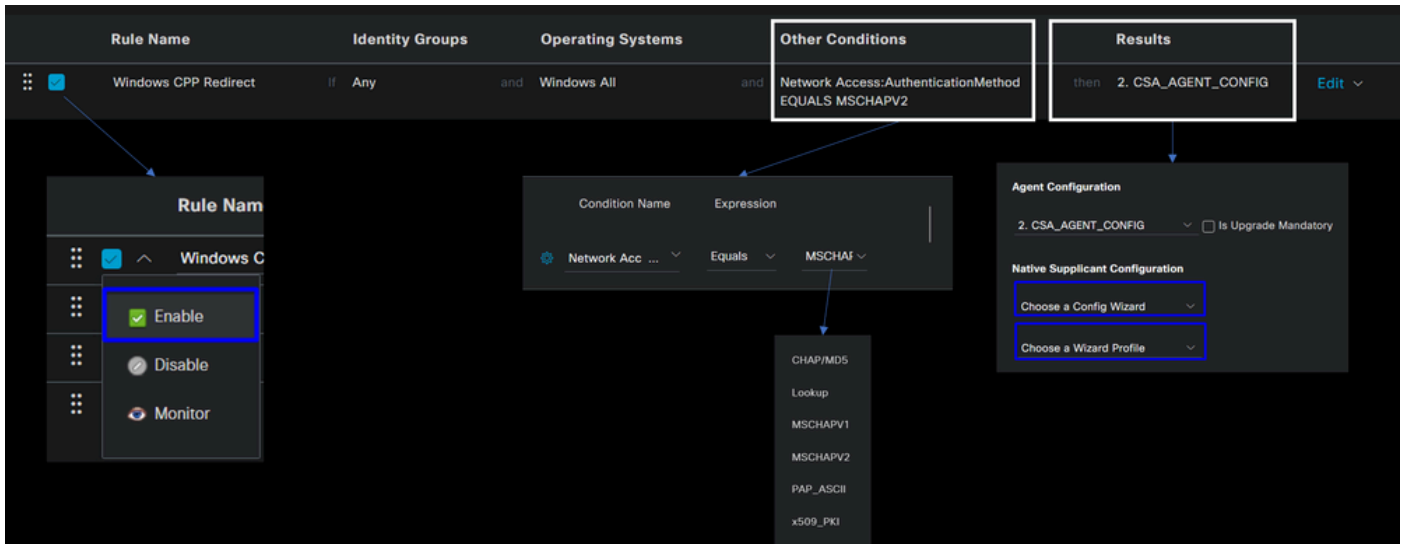
注意：建議每個作業系統（Windows、Mac OS或Linux）都獨立於「客戶端配置」。

要啟用調配在上一步配置的ISE終端安全評估和模組，您需要配置策略以進行調配。

- 導航到您的ISE控制台
 - 按一下 **Work Center > Client Provisioning**
-



注意：建議每個作業系統（Windows、Mac OS或Linux）都有一個客戶端配置策略。



- **Rule Name**：根據裝置型別和身份組選擇配置策略名稱，以輕鬆辨識每個策略
- **Identity Groups**：選擇要在策略上評估的標識
- **Operating Systems**：根據在步驟「選取代理程式套件」中選取的代理程式套件選擇作業系統
- **Other Condition**：根據Network Access 據步驟中配置的方法的Authentication MethodEQUALS選擇增加RADIUS組，或者您可以保留為空
- **Result**：在步驟4配置代理配置中選擇已配置的代理配置
 - **Native Supplicant Configuration**：選擇Config Wizard Wizard Profile
- 如果策略未列示為已啟用核取方塊，請將策略標示為已啟用。

建立授權配置檔案

授權配置檔案根據身份驗證透過後的使用者狀態限制對資源的訪問。必須驗證授權，以根據狀態確定使用者可訪問哪些資源。

授權配置檔案	說明
相容	使用者相容-已安裝代理-狀態已驗證
未知的相容	使用者未知合規性-重定向以安裝代理-狀態待驗證待處理

拒絕存取	使用者不相容-拒絕訪問
------	-------------

要配置DACL，請導航到ISE控制台：

- 按一下 **Work Centers > Policy Elements > Downloadable ACLs**
- 按一下 **+Add**
- 建立 **Compliant DACL**

The screenshot shows the configuration interface for a Compliant DACL. The name is set to 'CSA-Compliant'. The IP version is set to 'IPv4'. The DACL content is a list of IP addresses followed by the command 'permit ip any any'.

* Name	CSA-Compliant	
Description		
IP version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Agnostic ①	
* DACL Content	1234567 8910111 2131415 1617181 9202122 2324252 6272829 3031323 3343536 3738394 0441040	permit ip any any

- **Name**：增加一個名稱，該名稱引用與DACL相容的
- **IP version**:選擇 **IPv4**
- **DACL Content**：建立可下載訪問控制清單(DACL)，用於訪問網路的所有資源

<#root>

permit ip any any

按一下**Save** 並建立未知符合性DACL

- 按一下 **Work Centers > Policy Elements > Downloadable ACLs**
- 按一下 **+Add**

- 建立 Unknown Compliant DACL

* Name **CSA_Redirect_To_ISE**

Description

IP version IPv4 IPv6 Agnostic ⓘ

* DACL Content

1234567	permit udp any any eq 67
8910111	permit udp any any eq 68
2131415	permit udp any any eq 53
1617181	permit tcp any host 192.168.10.206 eq 8443
9202122	permit tcp any any eq 80
2324252	
6272829	
3031323	
3343536	
3738394	

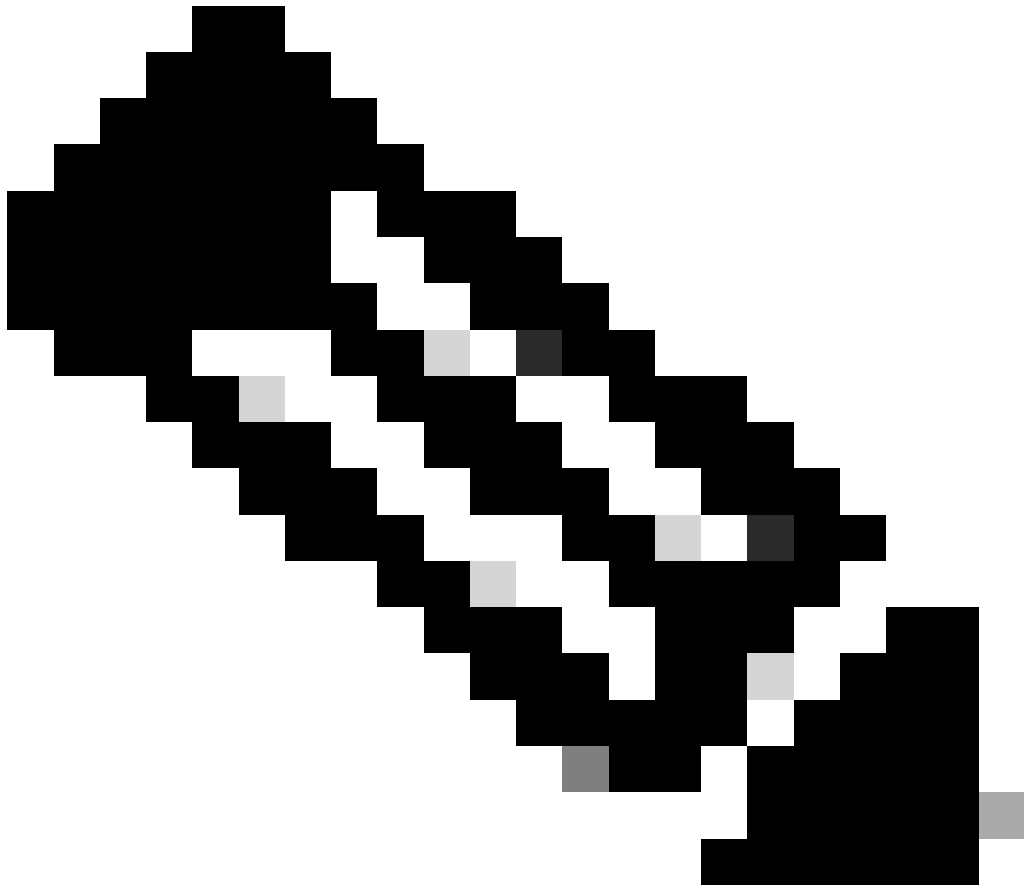
Check DACL Syntax

- Name : 增加一個名稱，用於引用DACL相容 (未知)
- IP version: 選擇 IPv4
- DACL Content: 建立一個DACL，允許透過埠8443對網路、DHCP、DNS、HTTP和調配門戶進行有限訪問

```

permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any any eq 80
permit tcp any host 192.168.10.206 eq 8443

```



注意：在此場景中，IP地址192.168.10.206對應於Cisco Identity Services Engine (ISE)伺服器，埠8443指定用於調配門戶。這意味著允許透過埠8443到IP地址192.168.10.206的TCP流量，從而便於訪問調配門戶。

此時，您擁有建立授權配置檔案所需的DACL。

要配置授權配置檔案，請導航到ISE控制台：

- 按一下 **Work Centers > Policy Elements > Authorization Profiles**

•

按一下 +Add

- 建立 Compliant Authorization Profile

Authorization Profile

* Name


CSA-Compliant

Description

* Access Type

ACCESS_ACCEPT

Network Device Profile

 Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

DACL Name

CSA-Compliant

IPv6 DACL Name

ACL

ACL IPv6 (Filter ID)





- **Name** : 建立引用合規授權配置檔案的名稱
- **Access Type**: 選擇 **ACCESS_ACCEPT**

- **Common Tasks**
 - **DACL NAME** : 選擇在[相容DACL](#)步驟中配置的DACL

點選**Save** 並建立 Unknown Authorization Profile

- 按一下 **Work Centers > Policy Elements > Authorization Profiles**
- 按一下 **+Add**

- 建立 Unknown Compliant Authorization Profile

* Name	CSA-Unknown-Compliant
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	 Cisco
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> 
Agentless Posture	<input type="checkbox"/> 
Passive Identity Tracking	<input type="checkbox"/> 

Common Tasks

<input checked="" type="checkbox"/> DACL Name	CSA_Redirect_To_ISE
---	---------------------

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture) ▾ ACL redirect

Value Client Provisioning Portal (... ▾

- **Name** : 建立引用未知合規授權配置檔案的名稱
- Access Type:選擇 ACCESS_ACCEPT

- **Common Tasks**

- **DACL NAME** : 選擇在[未知的相容DACL](#)步驟中配置的DACL

- **Web Redirection (CWA,MDM,NSP,CPP)**

- 選擇 **Client Provisioning (Posture)**

- **ACL** : 必須是 redirect

- **Value** : 選擇預設調配門戶，或者如果定義了其他門戶，請選擇該門戶



注意：對於所有部署，在Secure Access上重定向ACL的名稱為 **redirect**。

定義完所有這些值後，您都必須在Attributes Details下有類似的東西。

```
Attributes Details
Access Type = ACCESS_ACCEPT
DAACL = CSA_Redirect_To_ISE
cisco-av-pair = url-redirect-acl=redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=
&action=cpp
```

點選Save 結束配置並繼續下一步。

配置狀態策略集







您建立的這三個策略基於您配置的授權配置檔案；對於 DenyAccess，您不需要建立另一個策略。

策略集-授權	授權配置檔案
相容	授權配置檔案-相容
未知的相容	授權配置檔案-未知相容
不符合	拒絕存取






導航到您的ISE控制台

- 按一下 **Work Center > Policy Sets**

- 點選> 以訪問已建立的策略

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
 Search							
	CSA-ISE		 Network Access:NetworkDeviceName EQUALS: CSA	Default Network Access  +	370		

- 按一下 Authorization Policy

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
 Search					
	CSA-ISE		 Network Access:NetworkDeviceName EQUALS: CSA	Default Network Access  +	370
> Authentication Policy(2)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
 > Authorization Policy(4)					

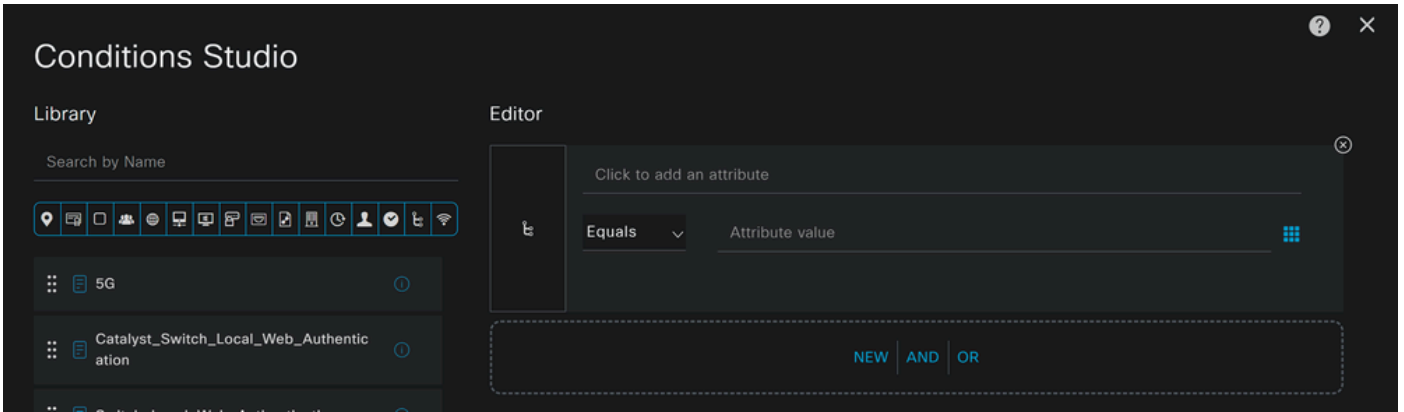
- 按下一個順序建立接下來的三個策略：

✓	SAML-Compliant	AND	<div>Compliant_Devices</div> <hr/> <div>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</div>	CSA-Compliant
✓	SAML-Unknown-Compliant	AND	<div>Compliance_Unknown_Devices</div> <hr/> <div>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</div>	CSA-Unknown-Compliant
✓	SAML-Non-Compliant	AND	<div>Non_Compliant_Devices</div> <hr/> <div>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</div>	DenyAccess

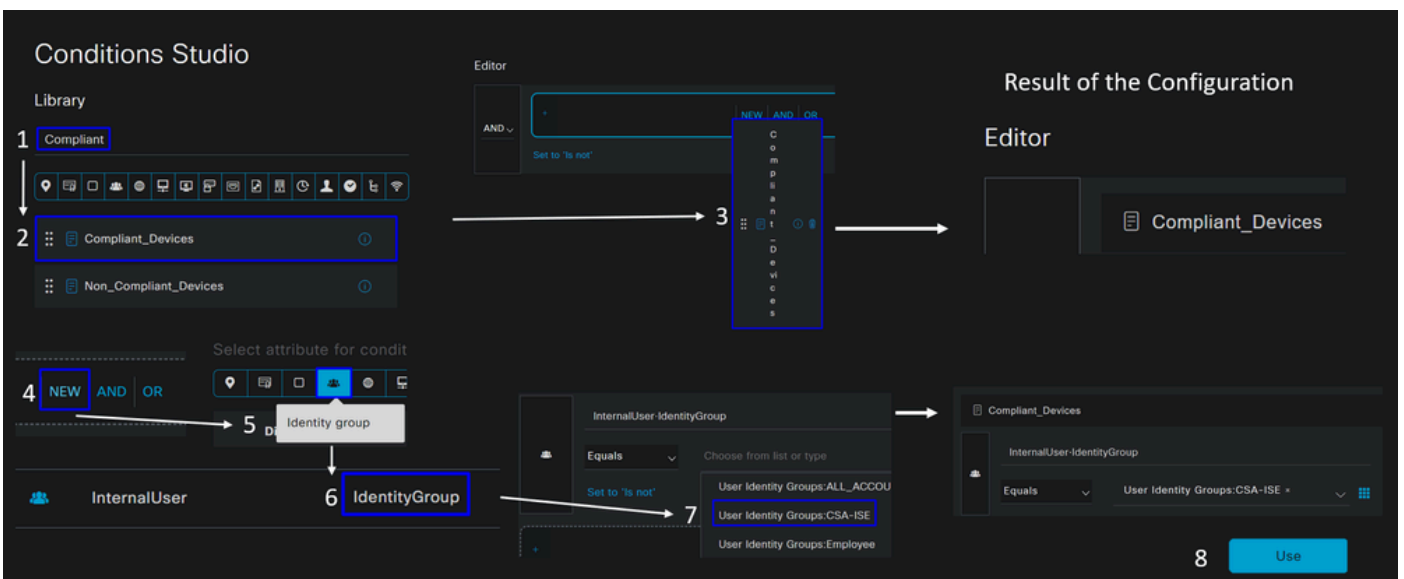
- 點選+ 以定義策CSA-Compliance 略：

			Results
Status	Rule Name	Conditions	Profiles
+			
Search			
✓	Authorization Rule 1	+	Select from list
			Select from list

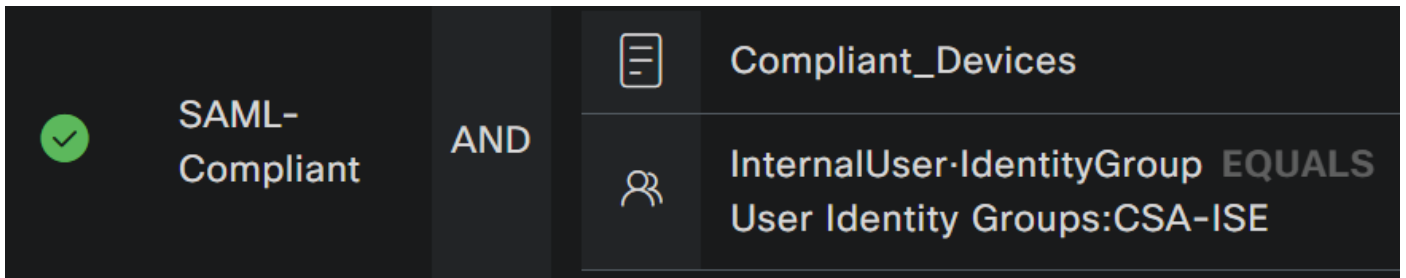
- 在下一步中，更改Rule Name，和Conditions Profiles
- 將名稱Name 設定為 CSA-Compliance
- 要配置 Condition，請點選 +
- 在 Condition Studio下，您可以找到以下資訊：



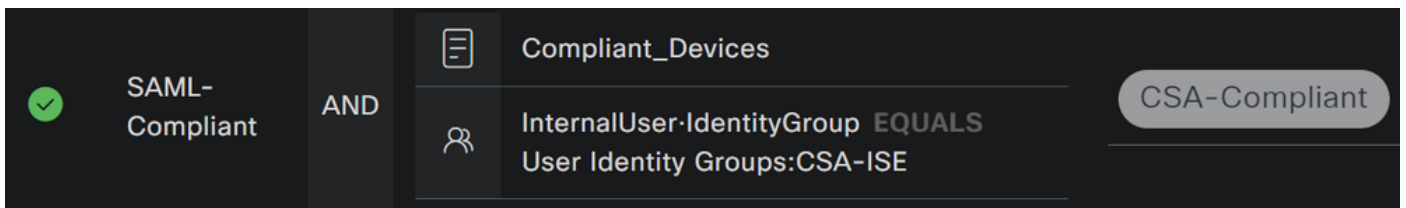
- 若要建立條件，請搜尋 **compliant**
- 您必須已顯示 **Compliant_Devices**
- 拖放在 **Editor**
- 在Editor下，按一下 **New**
- 按一下**Identity Group** 圖示
- 選擇 **Internal User Identity Group**
- 在 **Equals**下，選擇**User Identity Group** 要匹配的
- 按一下 **Use**



- 因此，您會看到下一個影像

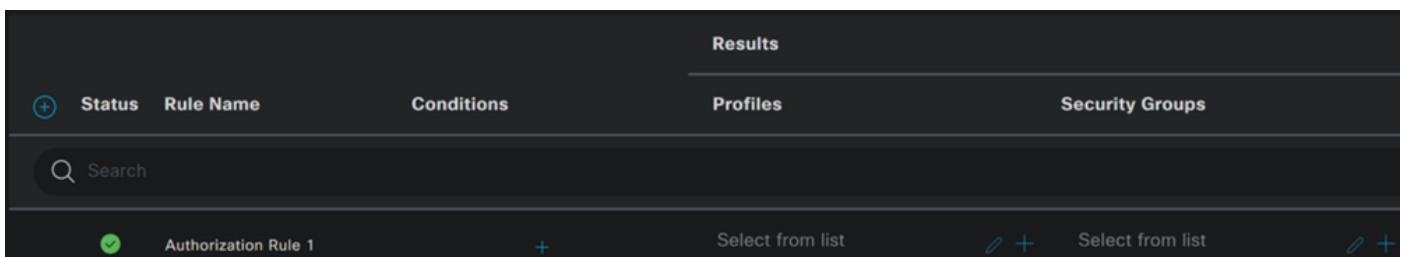


- 在Profile 點選下拉按鈕下並選擇步驟中配置的投訴授權配置檔案 [合規授權配置檔案](#)



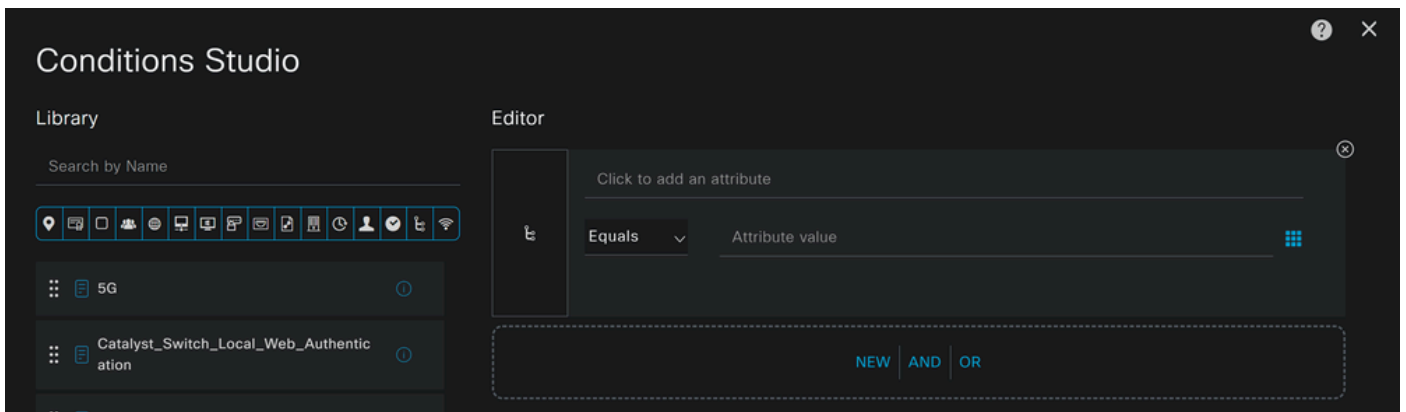
現在，您已經配置了 **Compliance Policy Set**。

- 點選+ 以定義策 **CSA-Unknown-Compliance** 略：

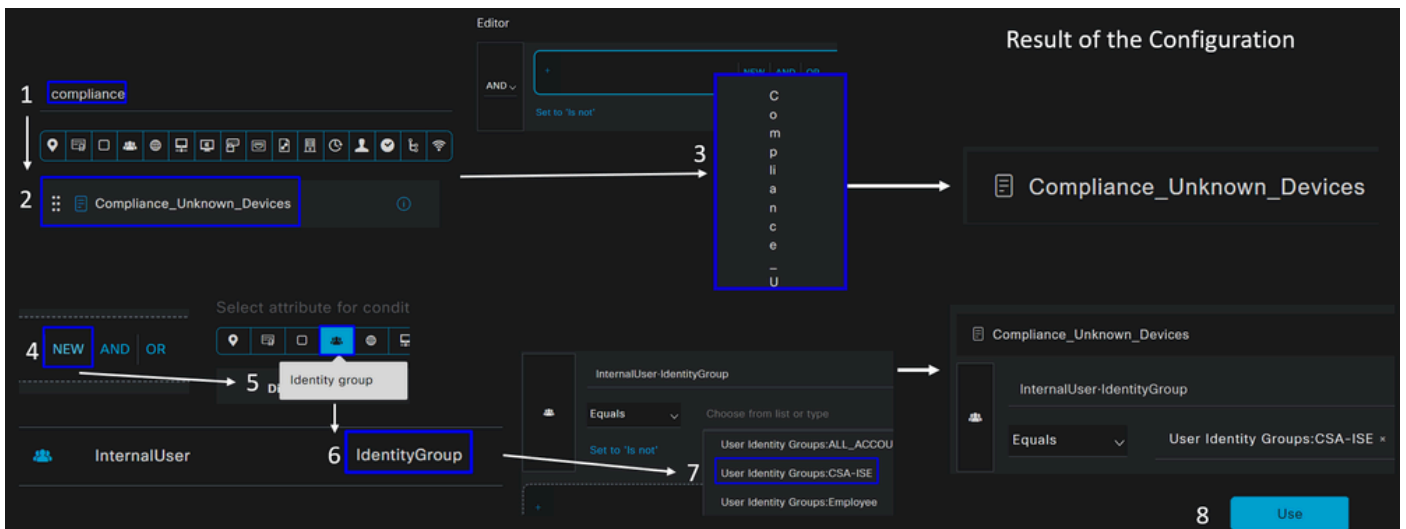


- 在下一步中，更改Rule Name，和Conditions Profiles
- 將名稱Name 設定為 **CSA-Unknown-Compliance**

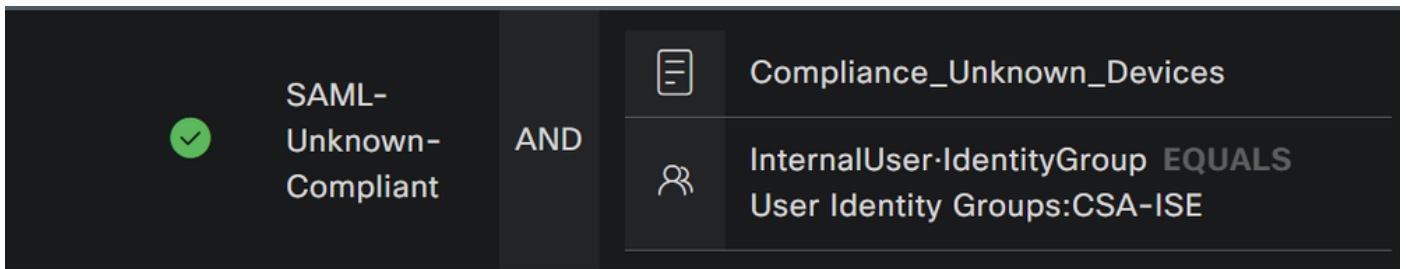
- 要配置 Condition，請點選 +
- 在 Condition Studio 下，您可以找到以下資訊：



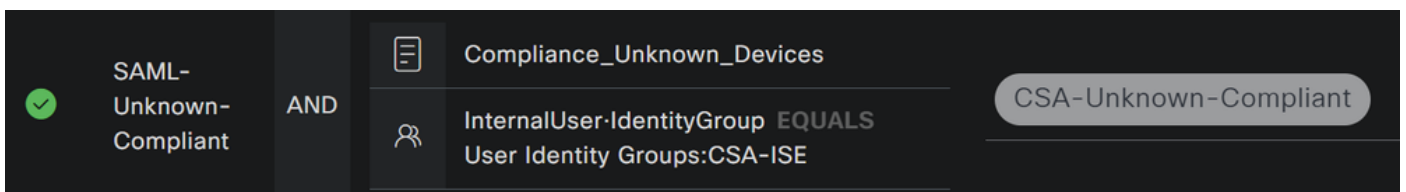
- 若要建立條件，請搜尋 **compliance**
- 您必須已顯示 **Compliant_Unknown_Devices**
- 拖放在 **Editor**
- 在 Editor 下，按一下 **New**
- 按一下 **Identity Group** 圖示
- 選擇 **Internal User Identity Group**
- 在 **Equals** 下，選擇 **User Identity Group** 要匹配的
- 按一下 **Use**



- 因此，您會看到下一個影像

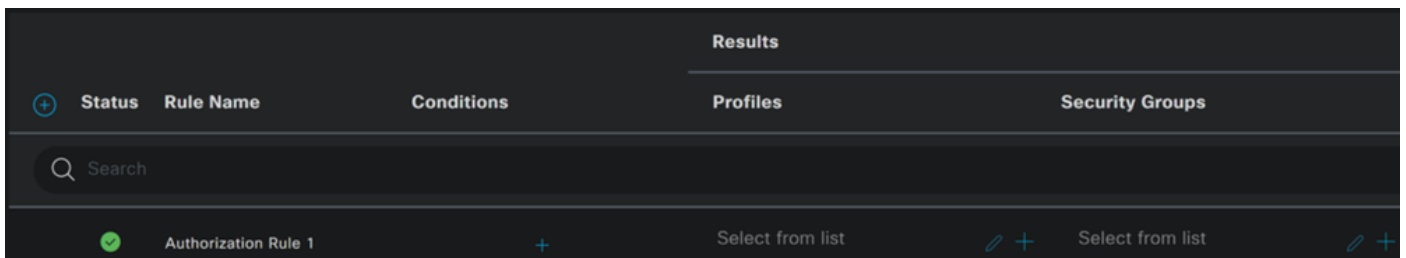


- 在Profile 點選下拉按鈕下並選擇步驟中配置的投訴授權配置檔案 [Unknown Compliant Authorization Profile](#)



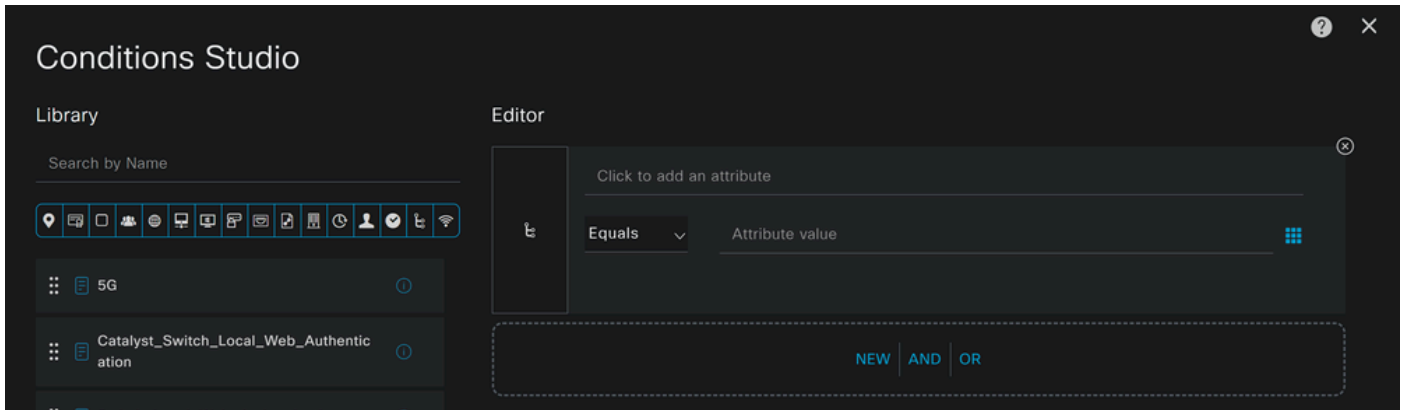
現在，您已經配置了 **Unknown Compliance Policy Set**。

- 點選+ 以定義策 **CSA- Non-Compliant** 略：

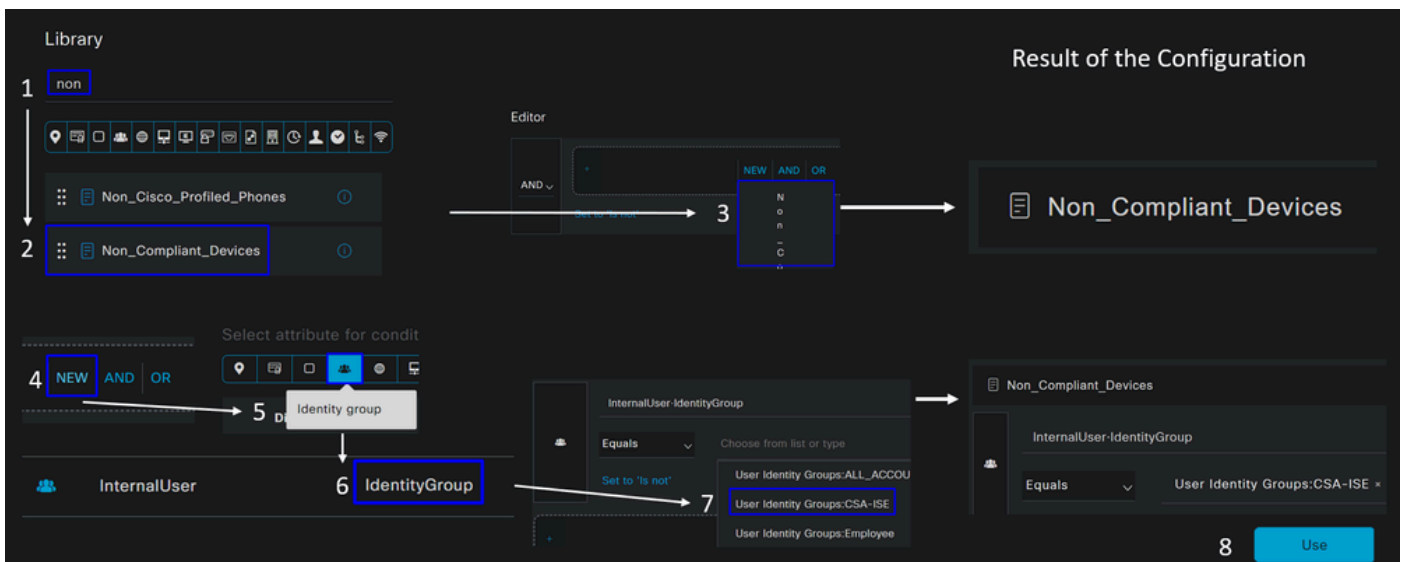


- 在下一步中，更改Rule Name，和Conditions Profiles
- 將名稱Name 設定為 **CSA-Non-Compliance**

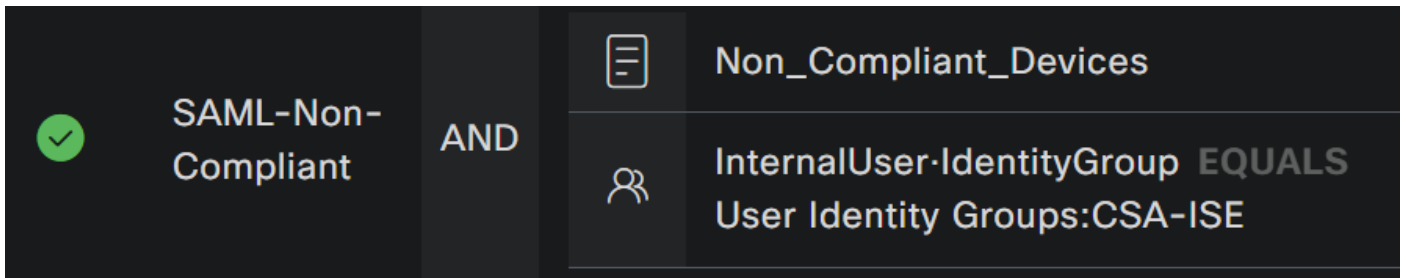
- 要配置 Condition，請點選 +
- 在 Condition Studio 下，您可以找到以下資訊：



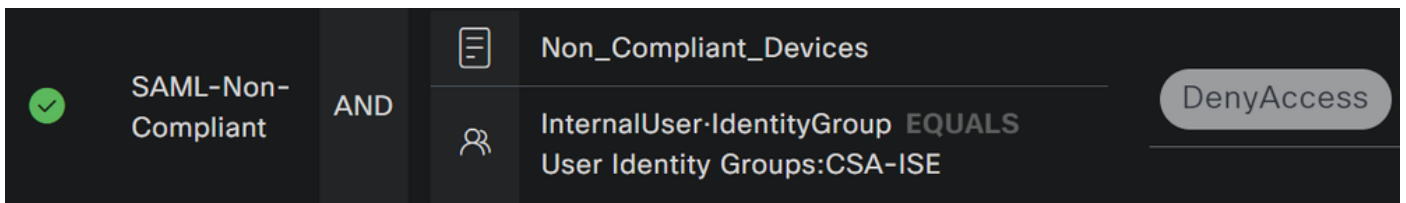
- 若要建立條件，請搜尋 **non**
- 您必須已顯示 **Non_Compliant_Devices**
- 拖放在 **Editor**
- 在 Editor 下，按一下 **New**
- 按一下 **Identity Group** 圖示
- 選擇 **Internal User Identity Group**
- 在 **Equals** 下，選擇 **User Identity Group** 要匹配的
- 按一下 **Use**



- 因此，您會看到下一個影像



- 在Profile 點選下拉按鈕下並選擇投訴授權配置檔案 DenyAccess



一旦您結束三個配置檔案的配置，您就可以開始測試與終端安全評估整合。

驗證

狀態驗證

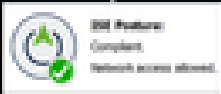
電腦上的連線

透過安全客戶端連線到安全訪問上提供的FQDN RA-VPN域。



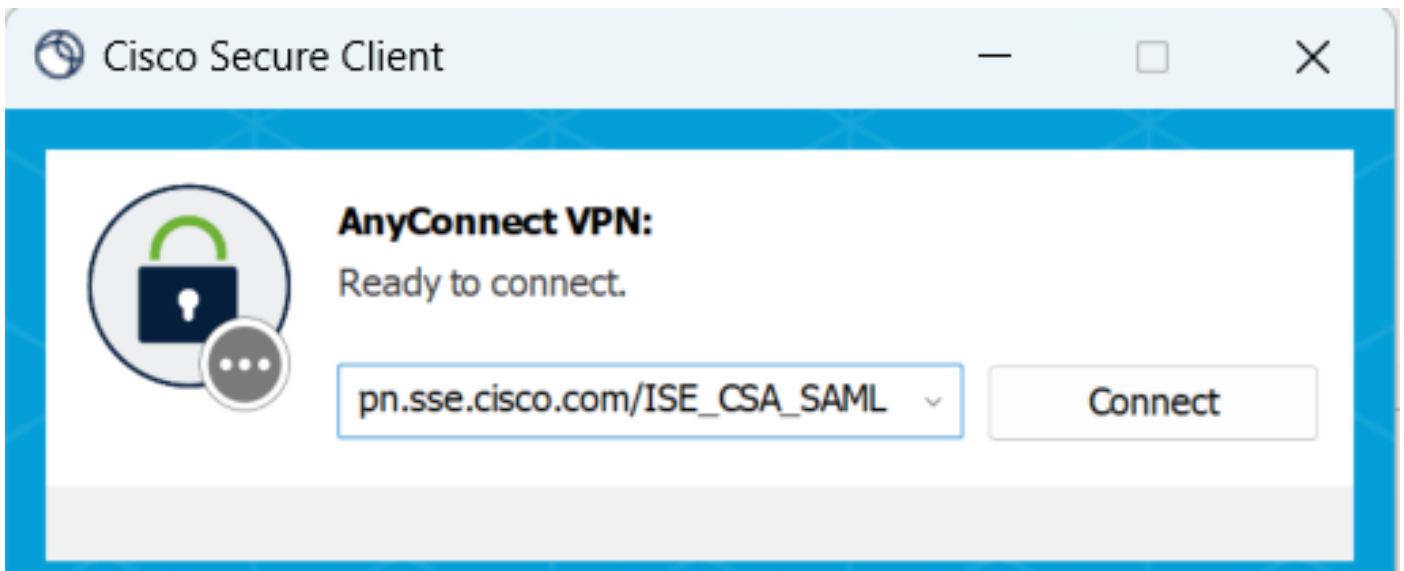
Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
ISE/SALE-IP-CSA-Compliant-MultiStep				
vphuser@cisconsp1.es	CSA-ISE	CSA-ISE => SAML-Compliant	CSA-Compliant	Compliant
vphuser@cisconsp1.es	CSA-ISE	CSA-ISE => SAML-Compliant	CSA-Compliant	Compliant
ISE/SALE-IP-CSA_Redirect_To_ISE-MultiStep				
vphuser@cisconsp1.es	CSA-ISE	CSA-ISE => SAML-Unknown...	CSA-Unknown-Compliant	Pending

1. Authorization Step = Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE DACL
5232 DACL Download Succeeded
3. Posture Status is verified on the machine
4. Authorization Step - CSA-Compliant
5205 Dynamic Authorization succeeded
5. Download CSA-Compliant
5232 DACL Download Succeeded

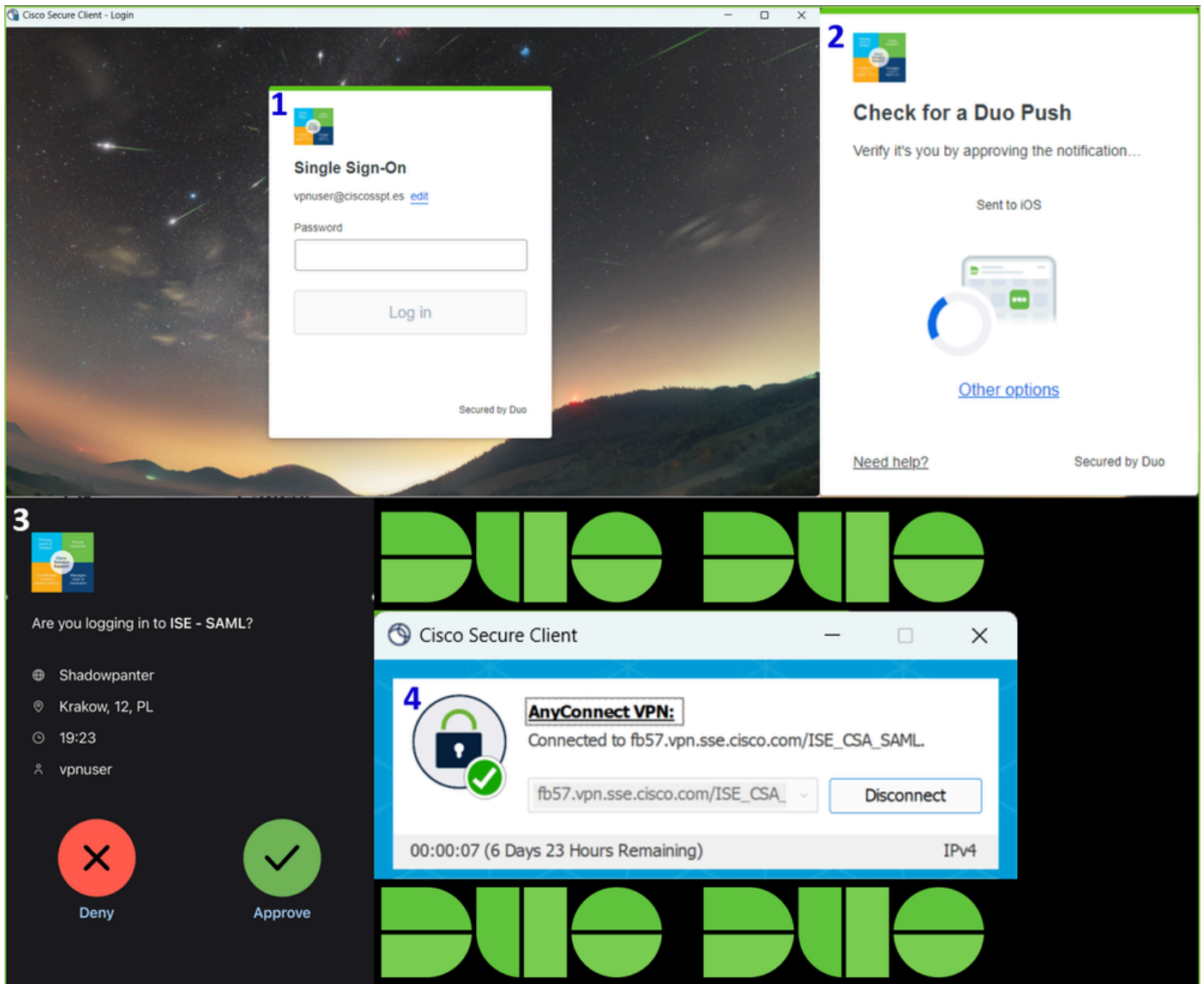


注意：此步驟中無需安裝ISE模組。

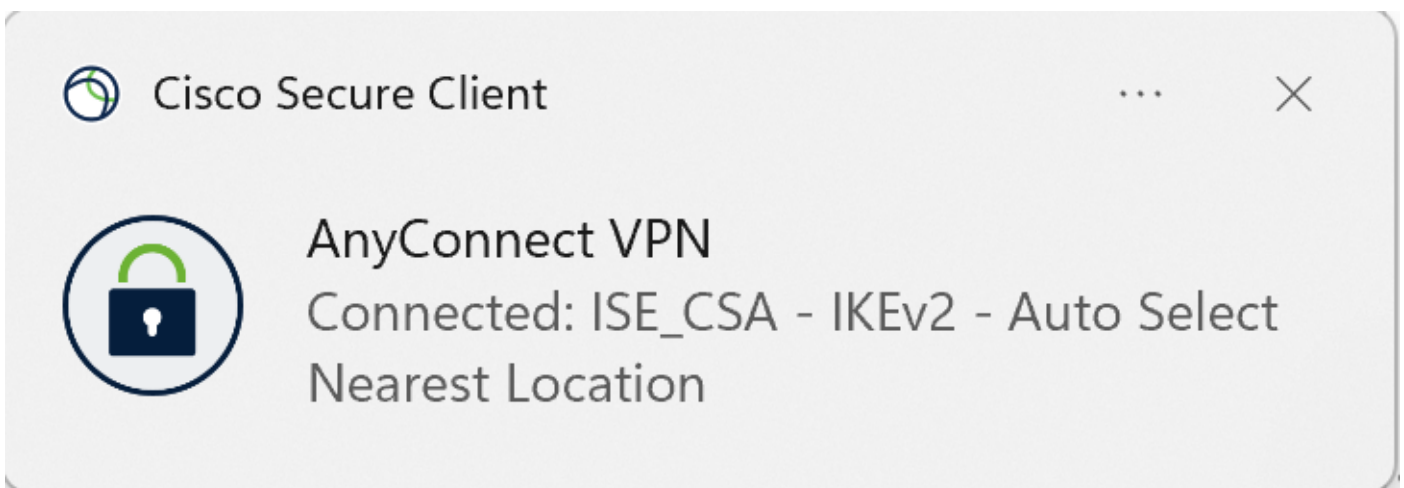
1. 使用安全客戶端連線。

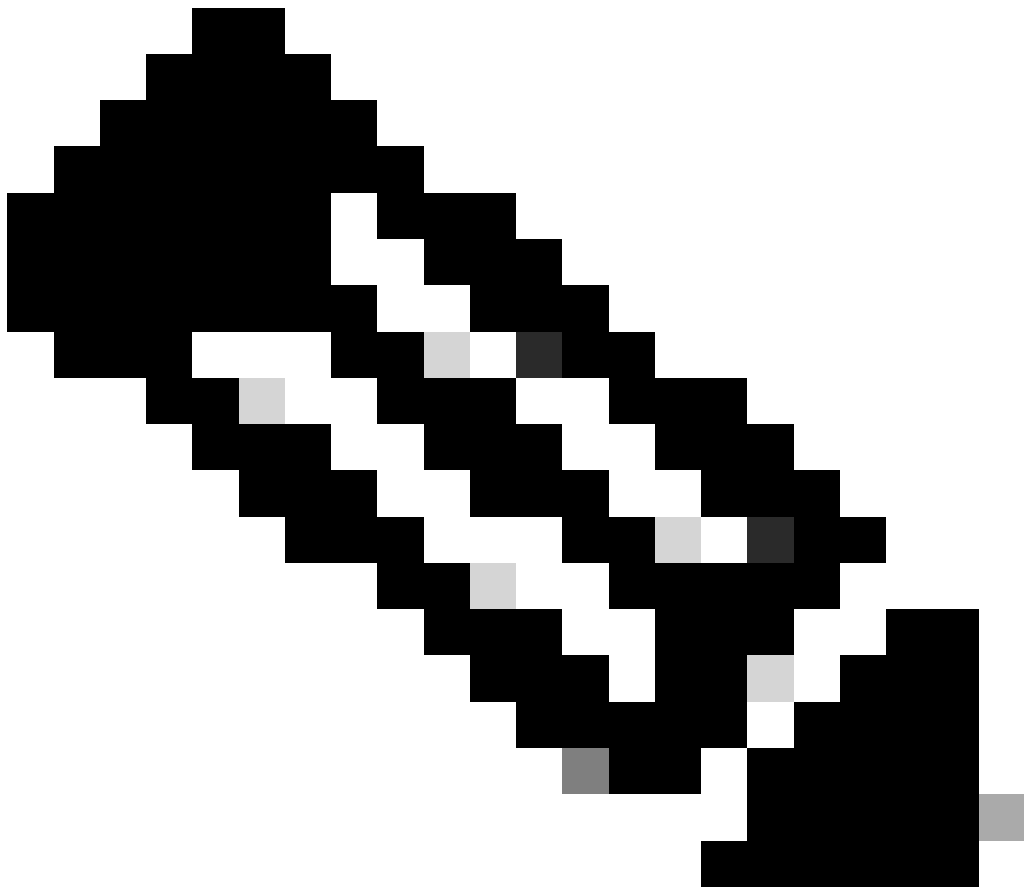
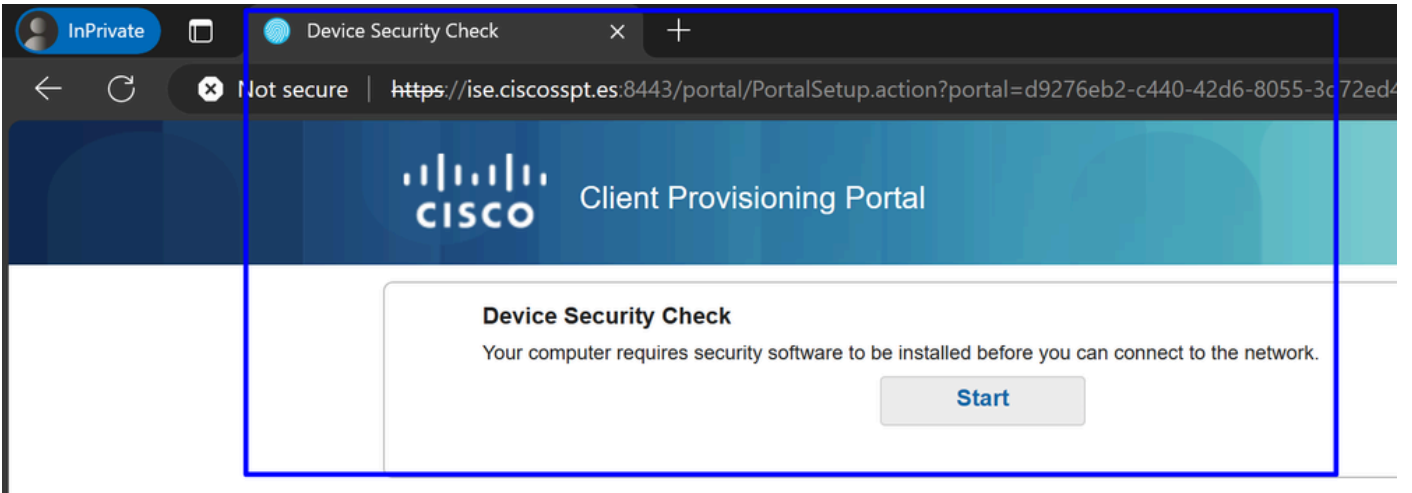


2. 提供憑證以透過Duo進行身份驗證。



3. 此時，您連線到VPN，很可能您被重定向到ISE；否則，您可以嘗試導航到http:1.1.1.1。





注意：此時您處於授權-策略集 [CSA-Unknown-Compliance](#) 下，因為您未在電腦上安裝ISE終端安全評估代理，並且您將重定向到ISE調配門戶以安裝代理。

4. 按一下「開始」以繼續代理程式啟動設定。

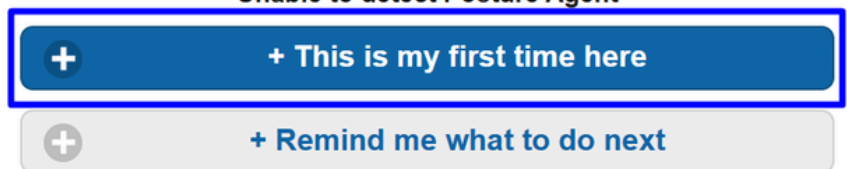


5. 按一下+ **This is my first time here.**

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect Posture Agent



6. 按一下 **Click here to download and install agent**



+ This is my first time here

1. You must install Agent to check your device before accessing the network. [Click here to download and install Agent](#)
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.



You have 4 minutes to install and for the compliance check to complete

7. 安裝代理

Downloads



cisco-secure-client-ise...aBf8STpS5Nr1nzotleQ.exe

[Open file](#)

[See more](#)



Network Setup Assistant



Installation is completed.

Quit

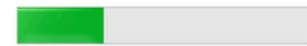
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

8. 安裝代理後，ISE終端安全評估開始驗證電腦的當前狀態。如果不符合策略要求，將顯示一個彈出窗口，指導您遵循合規性要求。



ISE Posture

1 Update(s) Required



30%

Time Remaining:

3 Minutes



Action Required to Enable Access

Updates are needed on your device before you can join the network.

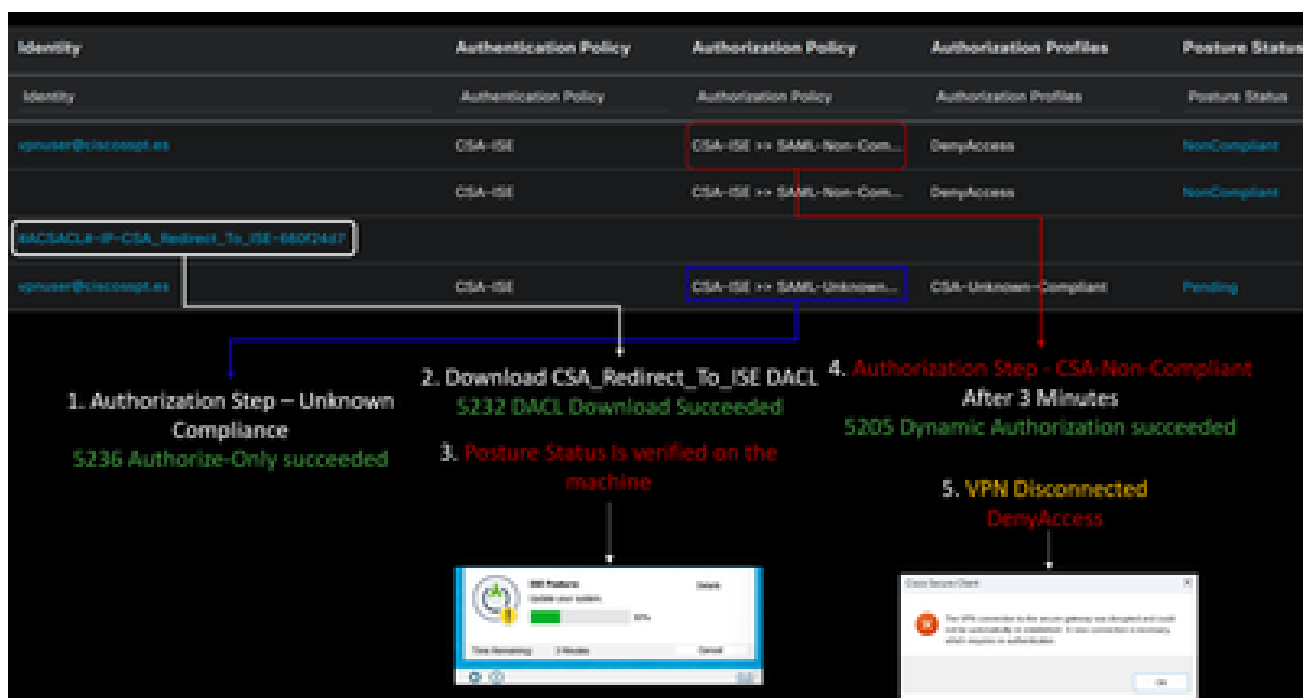
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

More Details

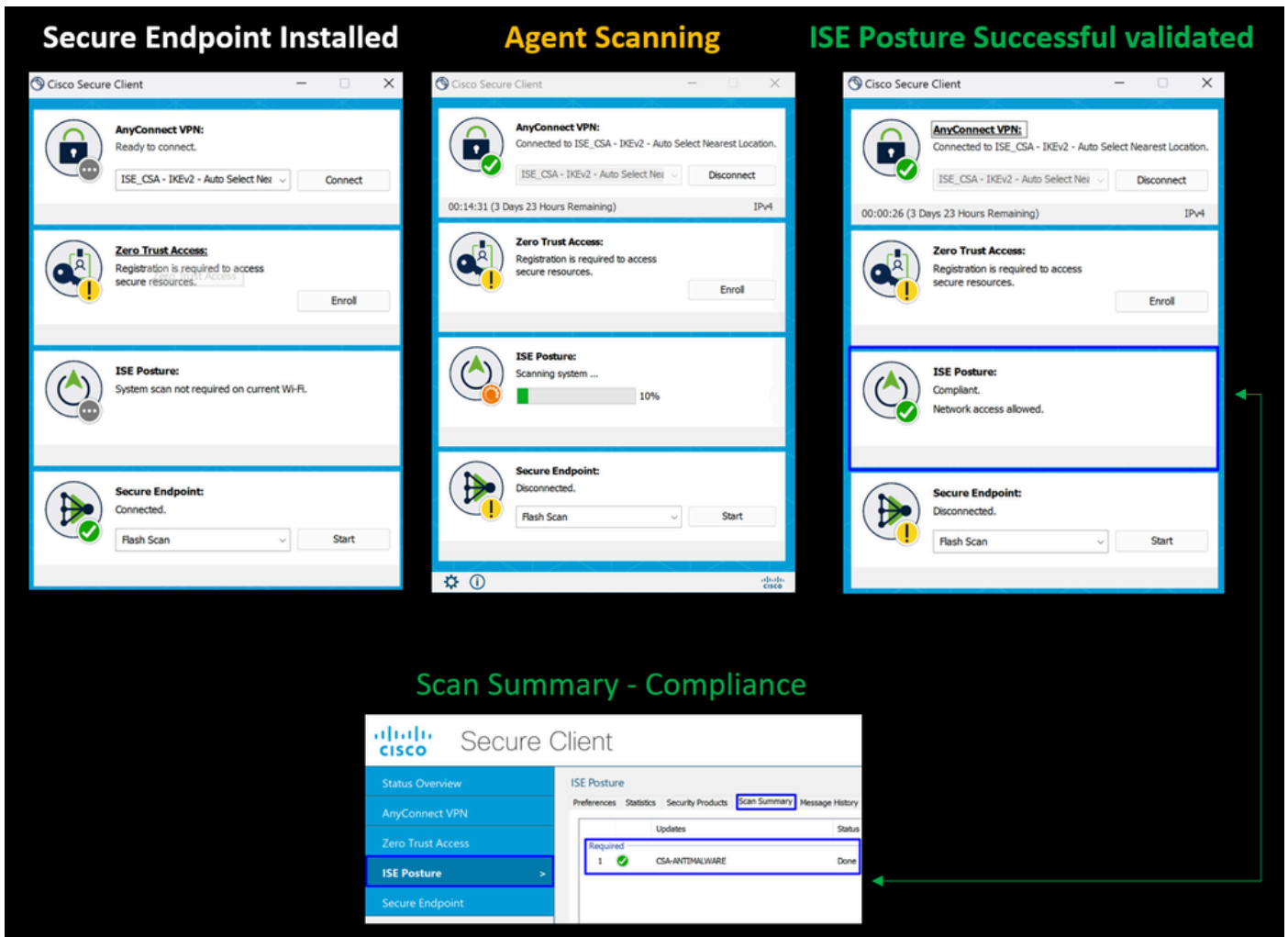


Cancel

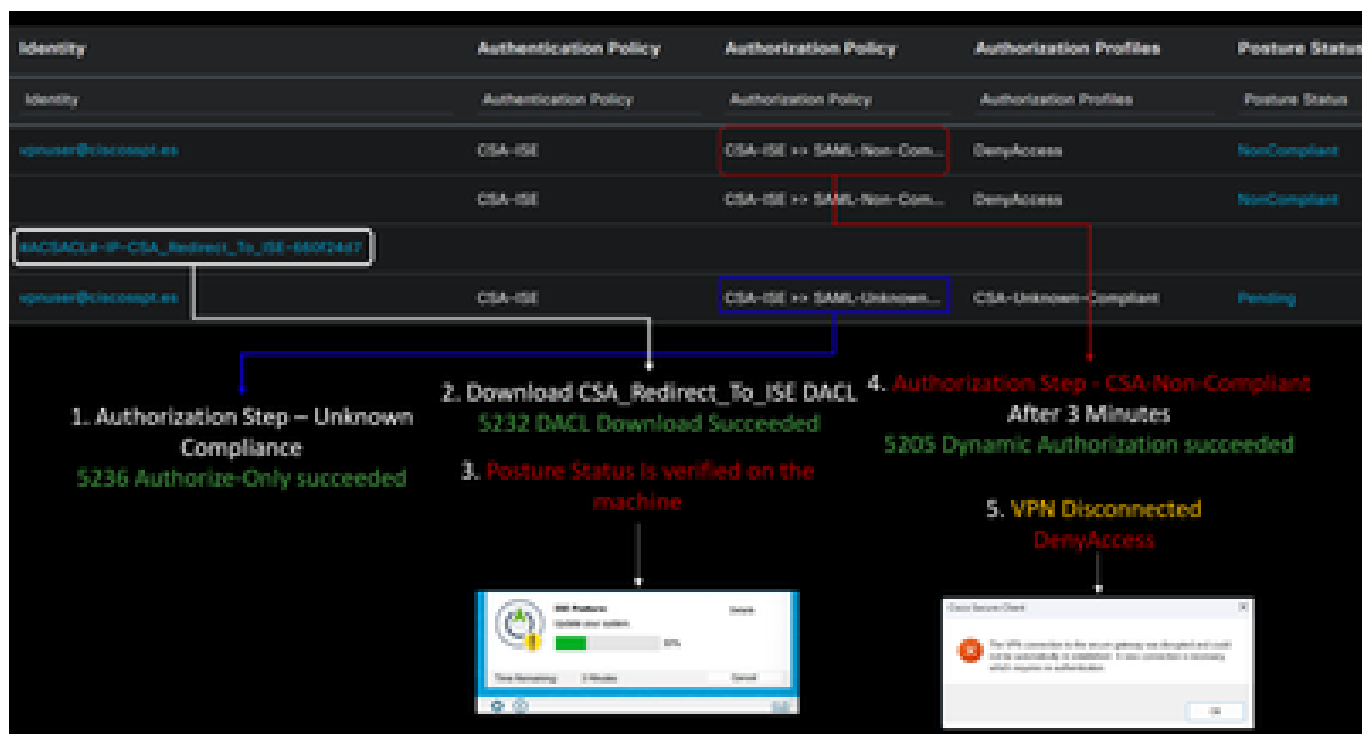


注意：如果Cancel您或剩餘時間結束，您將會自動變為不符合，受授權策略集CSA-Non-Compliance制約，並立即斷開VPN連線。

9. 安裝Secure Endpoint Agent並再次連線到VPN。



10. 在代理驗證電腦是否合規後，您的狀態將變為投訴，並允許訪問網路上的所有資源。



注意：在符合策略後，您將屬於授權策略集 [CSA-Compliance](#)，並且您可以立即訪問所有網路資源。

如何驗證ISE中的日誌

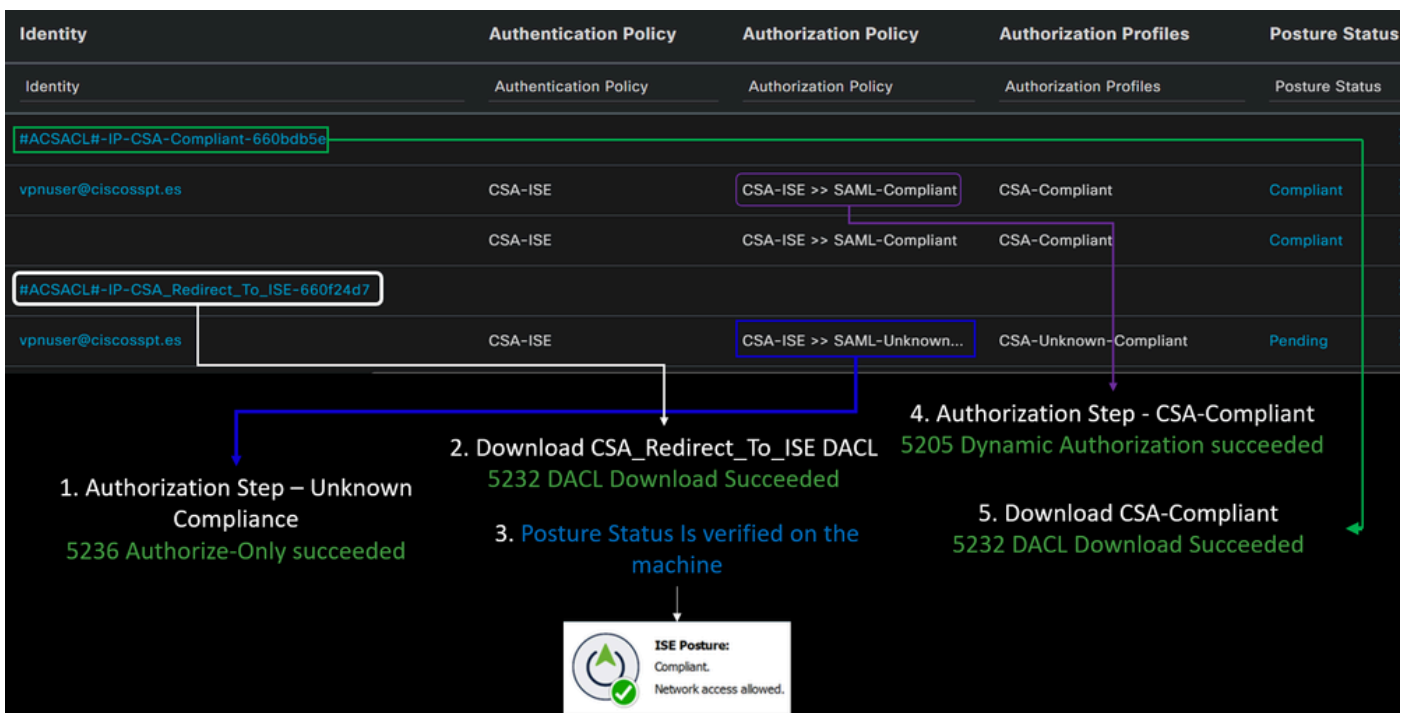
要驗證使用者的身份驗證結果，您有兩個遵循和不遵守的示例。要在ISE中檢視它，請遵循以下說明：

- 導航到您的ISE控制台
- 按一下 Operations > Live Logs

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter		
0	0	0	0	0		
Refresh: Never Show: Latest 50 records Within: Last 60 minutes						
Reset Repeat Counts Export To Filter Settings						
Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
		Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
🔵	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCom
✅	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCom
✅	📄	#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
✅	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending
✅	📄	#ACSACL#-IP-CSA-Compliant-660bdb5e				
✅	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Complia
✅	📄	#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				

下一個tho場景演示了成功的符合性和不符合性事件如何顯示在 Live Logs 下：

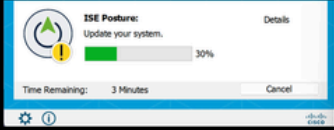

合規性



不合規性

Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
vpnuser@ciscosspt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
vpnuser@ciscosspt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
vpnuser@ciscosspt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending

1. Authorization Step – Unknown Compliance
5236 Authorize-Only succeeded
2. Download CSA_Redirect_To_ISE DACL
5232 DACL Download Succeeded
3. Posture Status Is verified on the machine
4. Authorization Step - CSA-Non-Compliant After 3 Minutes
5205 Dynamic Authorization succeeded
5. VPN Disconnected DenyAccess

安全訪問和ISE整合的第一步

在下一個示例中，思科ISE位於網路192.168.10.0/24下，需要透過隧道可達的網路配置需要增加到隧道配置下。

Step 1：驗證您的隧道配置：

要對此進行驗證，請導航到[安全訪問控制台](#)。

- 按一下 **Connect > Network Connections**
- 點選**Network Tunnel Groups >您的隧道**

HomeFTD	Connected	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1
---------	-----------	------------------	---------------	---	---------------

- 在彙總下，驗證隧道是否已配置您的Cisco ISE所在的地址空間：

Summary



Connected

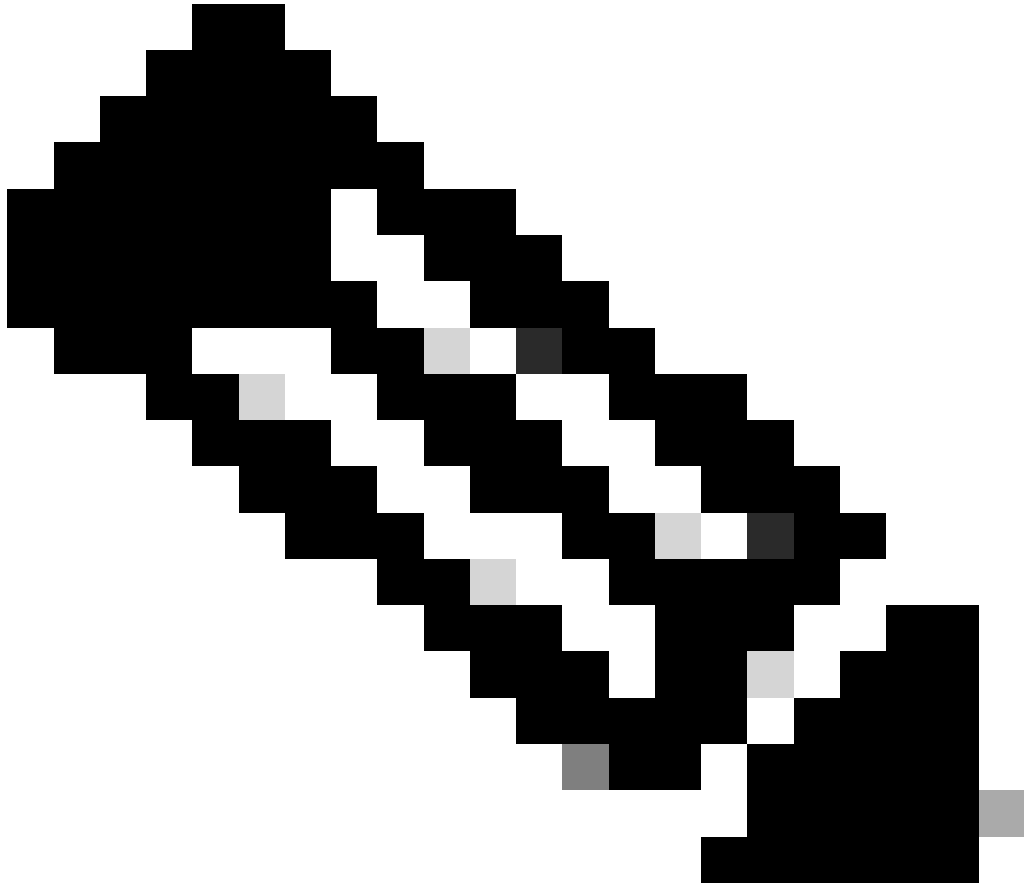
Region	Europe (Germany)
Device Type	FTD
Routing Type	Static Routing
IP Address Range	192.168.10.0/24
Last Status Update	Mar 19, 2024 11:13 AM

Step 2 : 允許防火牆上的流量。

要允許安全訪問使用您的ISE裝置進行RADIUS身份驗證，您需要配置從安全訪問到您的網路的規則以及所需的RADIUS埠：

規則	來源	目的地	目的地連線埠
使用ISE保護訪問 管理池	ISE_Server	管理IP池(RA-VPN)	COA UDP 1700 (預設埠)
ISE的安全訪問管理IP池	管理IP池	ISE_Server	驗證, 授權 UDP 1812 (預設埠) 計量 UDP 1813 (預設埠)
ISE的安全訪問終端IP池	終端IP池	ISE_Server	調配門戶 TCP 8443 (預設埠)
DNS伺服器的安全訪問端點IP池	終端IP池	DNS伺服器	DNS UDP與TCP 53

--	--	--	--



注意：如果要瞭解更多與ISE相關的埠，請檢視[使用手冊-埠參考](#)。



注意：如果已將ISE配置為透過某個名稱（如ise.ciscosspt.es）發現，則需要DNS規則

管理池和終端IP池

要驗證您的管理和終端IP池，請導航到[安全訪問控制台](#)：

- 按一下 **Connect > End User Connectivity**
- 按一下 **Virtual Private Network**

- 底下 **Manage IP Pools**
- 按一下 **Manage**

EUROPE						1	^
Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups		
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	ISE_CSA		 

第3步：驗證您的ISE是否在專用資源下配置

要允許透過VPN連線的使用者導航到**ISE Provisioning Portal**，您需要確保將裝置配置為提供訪問的私有資源，該資源用於允許透過VPN自動調配ISE Posture Module。

要驗證是否正確配置了ISE，請導航到[安全訪問控制台](#)：

- 按一下 **Resources > Private Resources**
- 點選ISE資源

Private Resource Name

CiscoISE

Description (optional)

Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address.

[Help](#)

Internally reachable address

(FQDN, Wildcard FQDN, IP Address, CIDR)



Protocol

Port / Ranges

[+ Protocol & Port](#)

192.168.10.206

TCP - (HTTP/HTTPS)

Any

[+ IP Address or FQDN](#)

VPN connections

Allow endpoints to connect to this resource when connected to the network using VPN.

如果需要，您可以將規則限制到調配門戶埠(8443)。

注意：請確保已標籤VPN連線的覈取方塊。

第4步：在訪問策略下允許ISE訪問

要允許透過VPN連線的使用者導航到ISE Provisioning Portal，您需要確保已配置Access Policy 以允許根據該規則配置的使用者訪問在Step3中配置的專用資源。

要驗證是否正確配置了ISE，請導航到[安全訪問控制台](#)：



- 按一下 **Secure > Access Policy**

- 點選配置為允許訪問VPN使用者的ISE的規則

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)


Action

 Allow Allow specified traffic if security requirements are met.	 Block Block specified traffic.
---	--


From Specify one or more sources. <input type="text" value="CSA (ciscospt.es\CSA)"/>	To Specify one or more destinations. <input type="text" value="CiscoISE"/>
<small>Information about sources, including selecting multiple sources. Help</small>	<small>Information about destinations, including selecting multiple destinations. Help</small>

Endpoint Requirements

For VPN connections:

 End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. [①](#)
Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:

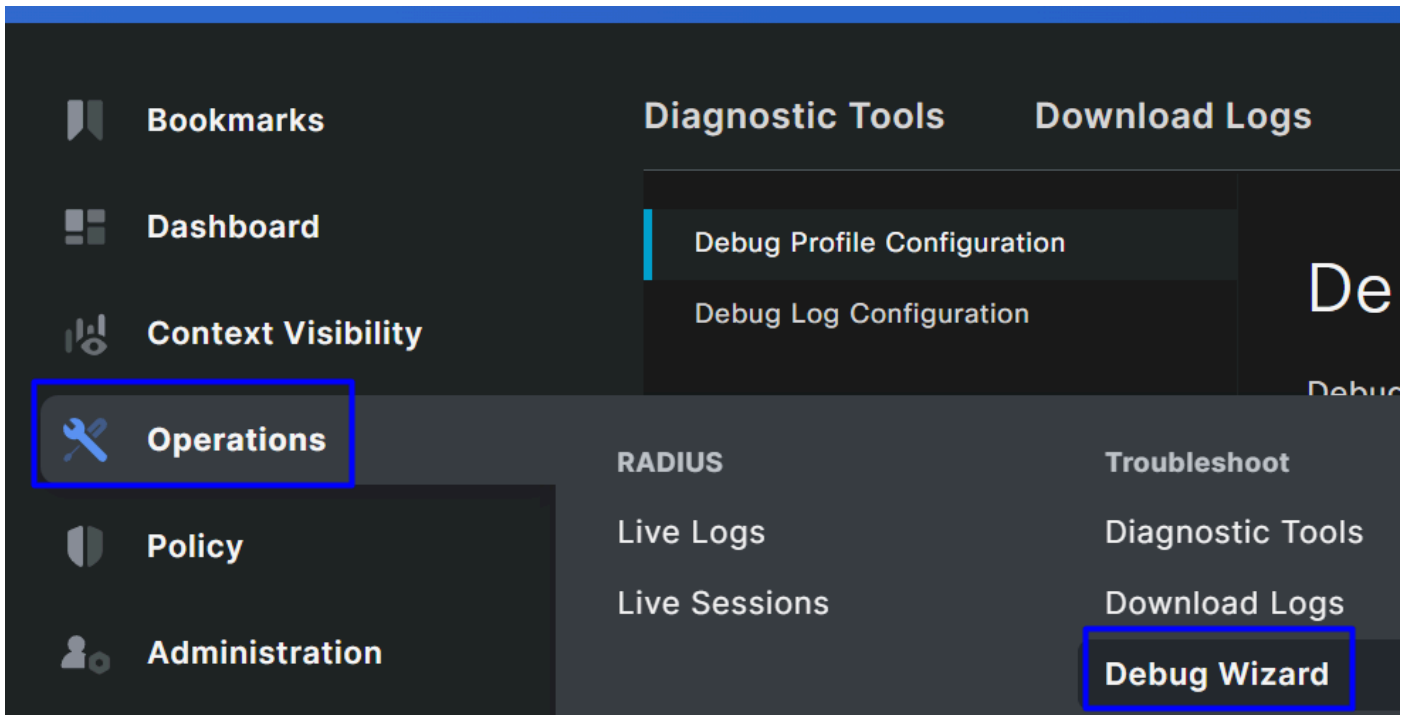
 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

疑難排解

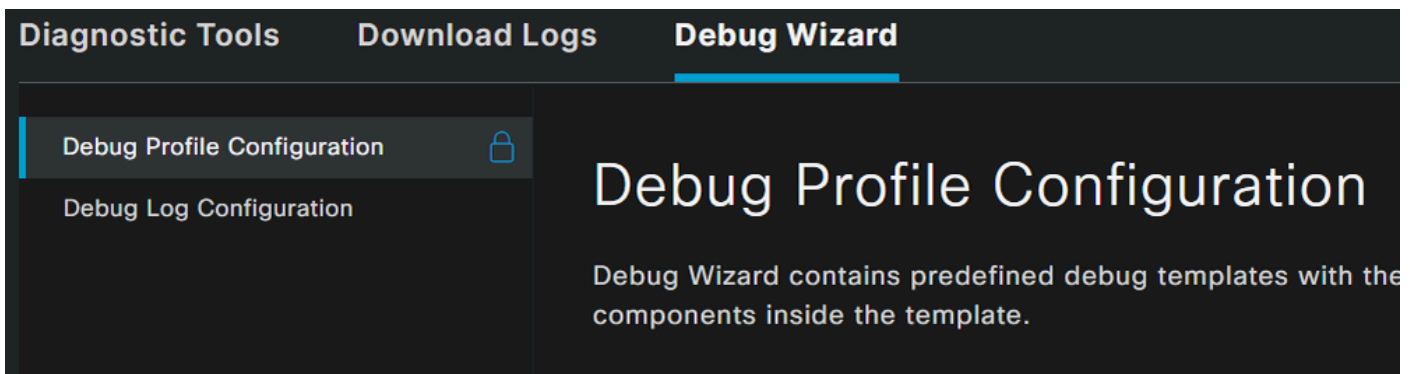
如何下載ISE終端安全評估調試日誌

要下載ISE日誌以驗證與終端安全評估相關的問題，請繼續執行以下步驟：

- 導航到您的ISE控制台
- 按一下 Operations > Troubleshoot > Debug Wizard



- 按一下 Debug Profile Configuration



- 標示核取方塊 Posture > Debug Nodes



Add



Edit



Remove 2



Debug Nodes



Name

Des



802.1X/MAB

802



Active Directory

Acti



Application Server Issues

App



BYOD portal/Onboarding

BYO



Context Visibility

Con



Guest portal

Gue



Licensing

Lice



MnT

MnT

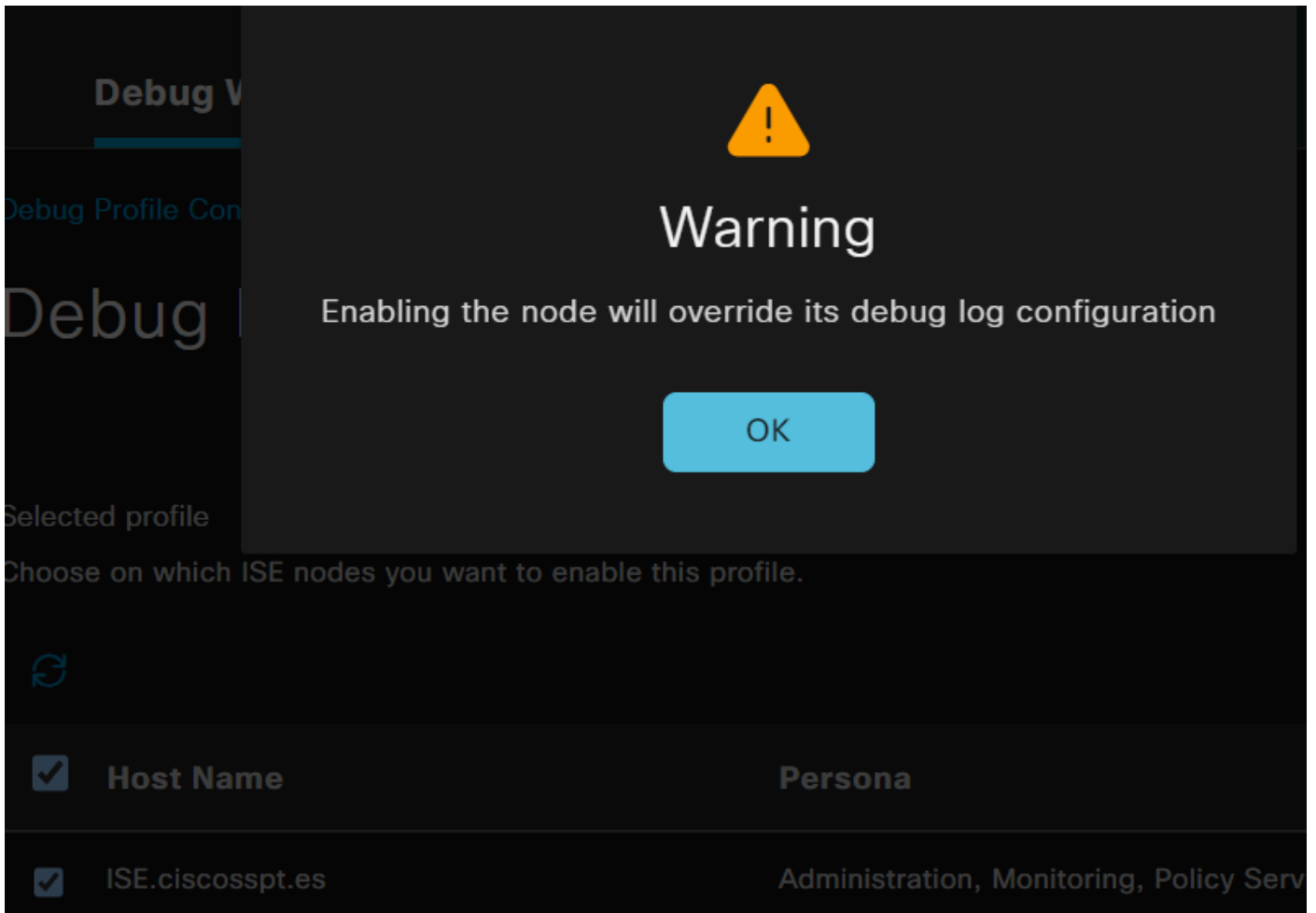
1



Posture

Pos

- 選中要啟用調試模式以解決問題的ISE節點的覈取方塊



- 按一下 Save

Debug Nodes

Selected profile Posture

Choose on which ISE nodes you want to enable this profile.



Filter



Host Name

Persona

Role



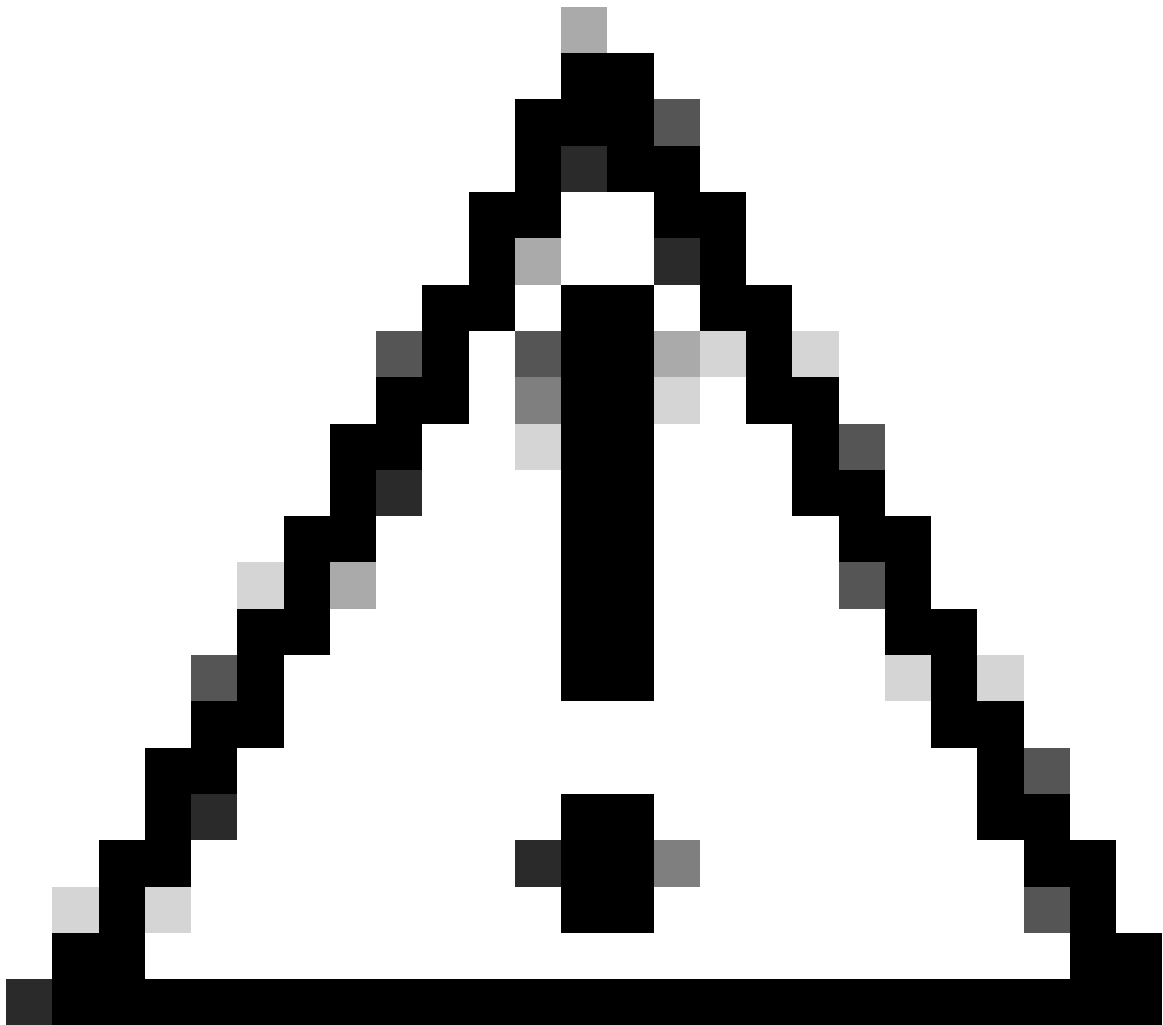
ISE.ciscosppt.es

Administration, Monitoring, Policy Service

STANDALONE

Cancel

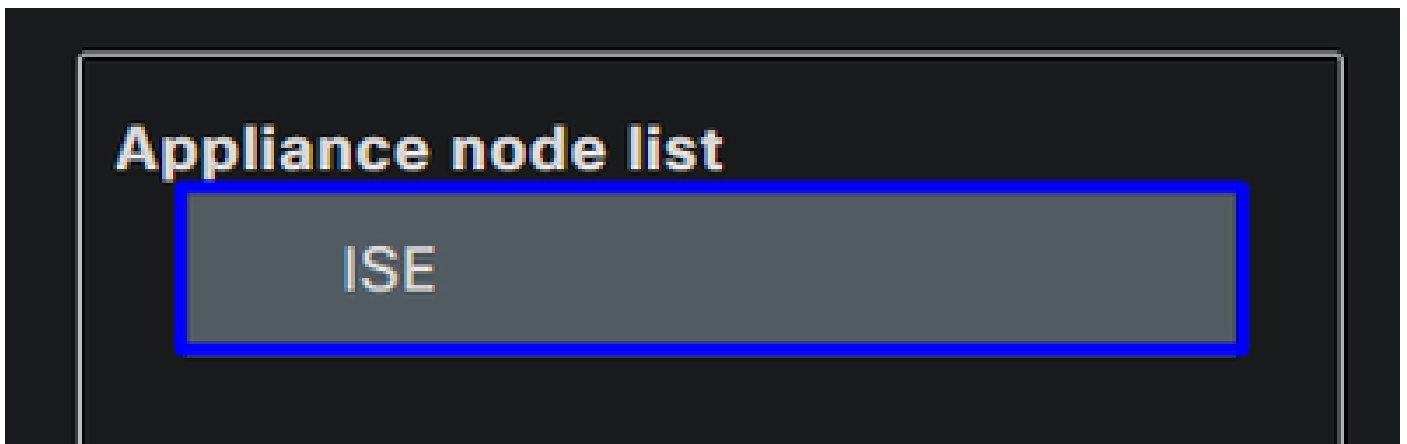
Save



注意：在此之後，您必須開始再現問題； **the debug logs can affect the performance of your device。**

在重現問題後，請繼續執行以下步驟：

- 按一下 Operations > Download Logs
- 選擇要從中獲取日誌的節點



- 在 **Support Bundle** 「下方」中，選擇下列選項：

Support Bundle

Debug Logs

- Include full configuration database ⓘ
- Include debug logs ⓘ
- Include local logs ⓘ
- Include core files ⓘ
- Include monitoring and reporting logs ⓘ
- Include system logs ⓘ
- Include policy configuration ⓘ
- Include policy cache ⓘ

From Date

(mm/dd/yyyy)

To Date

(mm/dd/yyyy)

* Note: Output from the 'show tech-support' CLI command will be included along with the selected entries.

Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

* Encryption key ⓘ

* Re-Enter Encryption key

Create Support Bundle

- Include debug logs
- 底下 **Support Bundle Encryption**
 - **Shared Key Encryption**
 - 填滿 **Encryption key** 和 **Re-Enter Encryption key**

- 按一下 **Create Support Bundle**
- 按一下 **Download**

✓ Support Bundle - Last Generated

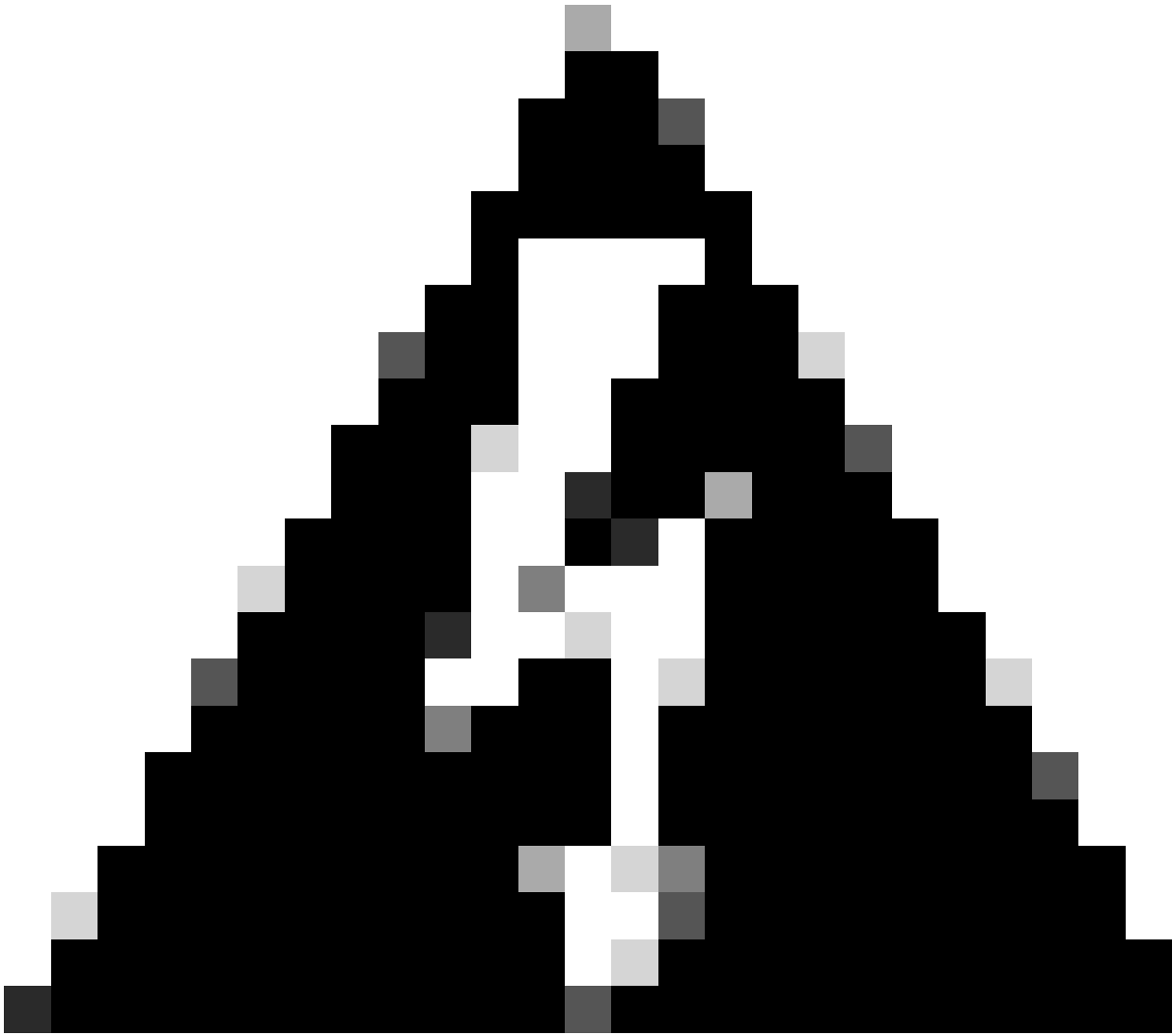
File Name: ise-support-bundle-ISE-admin-04-04-2024-14-27.tar.gpg

Time: Thu, 04 Apr 2024 14:35:35 UTC

Size(KB): 52165.0

[Download](#)

[Delete](#)


















警告：停用在步驟[Debug Profile Configuration](#)上啟用的偵錯模式

如何驗證安全訪問遠端訪問日誌

導航到您的安全訪問控制台：

- 按一下 Monitor > Remote Access Logs

100 Events

User	Connection Event	Event Details	Internal IP Address
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.1
<i>Unknown Identity</i>	 Failed	AUTHORIZATION-CHECK	

在安全客戶端上生成DART捆綁包

要在您的電腦上生成DART捆綁包，請驗證以下文章：

[Cisco Secure Client Diagnostic and Reporting Tool \(DART\)](#)



註：收集了故障排除部分中指明的日誌後，請透過TAC 建立案例，以繼續分析資訊。

相關資訊

- [思科技術支援與下載](#)
- [Secure Access文檔和使用手冊](#)

- [Cisco Secure Client軟體下載](#)
- [思科身份服務引擎管理員指南3.3版](#)

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）。