

# 排除ISE 3.2和Windows中的有線Dot1x問題

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

---

## 簡介

本文說明如何為身份服務引擎(ISE) 3.2和Windows本地請求方配置基本802.1X PEAP身份驗證。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 受保護的可延伸驗證通訊協定(PEAP)
- PEAP 802.1x

### 採用元件

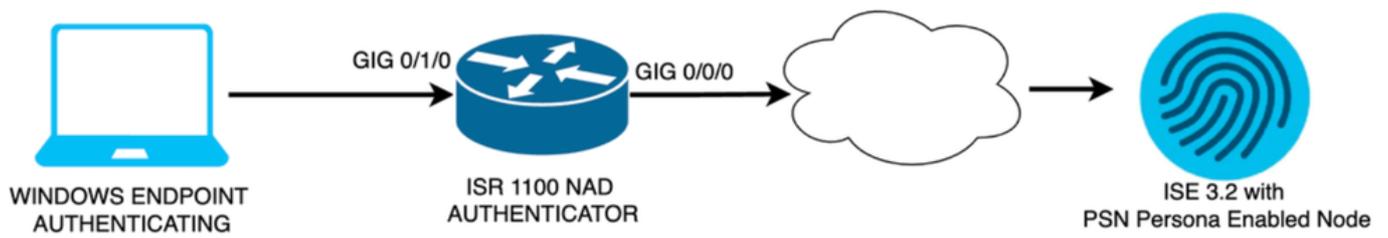
本文中的資訊係根據以下軟體和硬體版本：

- 思科身份服務引擎(ISE)版本
- 思科C1117 Cisco IOS® XE軟體，版本17.12.02
- 使用Windows 10的筆記型電腦

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

### 網路圖表



網路圖表

## 組態

執行下列步驟進行配置：

步驟 1. 配置ISR 1100路由器。

步驟 2. 配置身份服務引擎3.2。

步驟 3. 配置Windows本地請求方。

步驟 1. 配置ISR 1100路由器

本部分介紹至少需要NAD才能使dot1x正常運行的基本配置。

---

注意：對於多節點ISE部署，請配置已啟用PSN角色的節點的IP。如果在Administration > System > Deployment頁籤下導航到ISE，則可以啟用此功能。

---

```
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
  client A.B.C.D server-key <Your shared secret>
!
!
radius server ISE-PSN-1
  address ipv4 A.B.C.D auth-port 1645 acct-port 1646
  timeout 15
  key <Your shared secret>
!
!
```

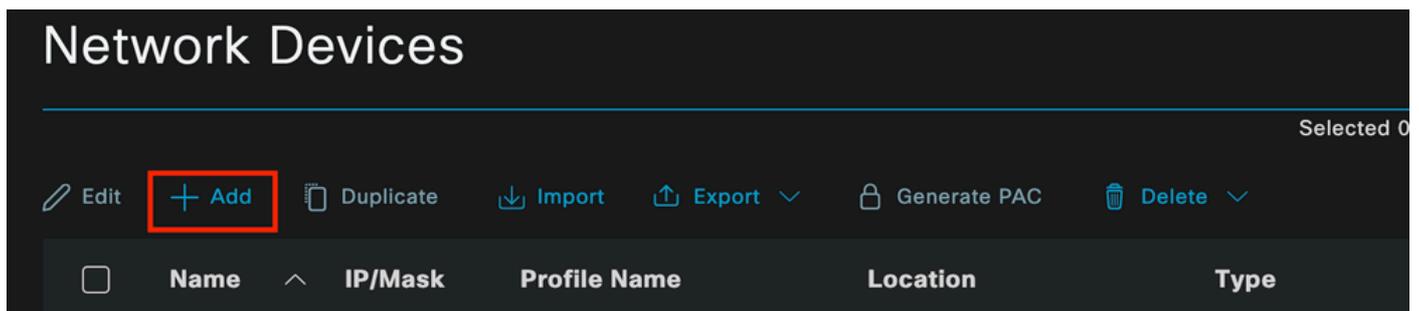
```
aaa group server radius ISE-CLUSTER
  server name ISE-PSN-1
!
interface GigabitEthernet0/1/0
  description "Endpoint that supports dot1x"
  switchport access vlan 15
  switchport mode access
  authentication host-mode multi-auth
  authentication order dot1x mab
  authentication priority dot1x mab
  authentication port-control auto
  dot1x pae authenticator
  spanning-tree portfast
```

步驟 2. 配置身份服務引擎3.2。

2. a. 配置並增加用於身份驗證的網路裝置。

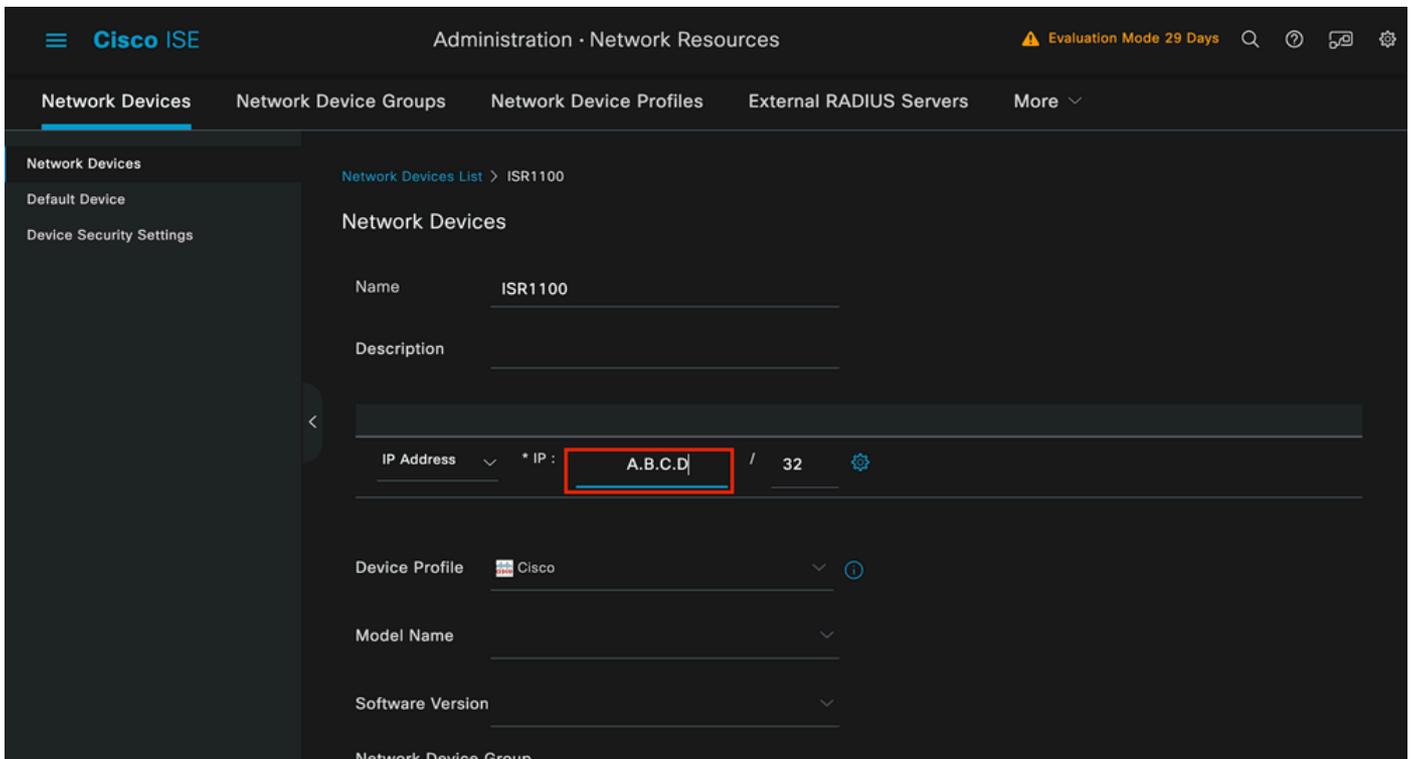
將網路裝置增加到ISE網路裝置部分。

按一下Add按鈕開始。



ISE網路裝置

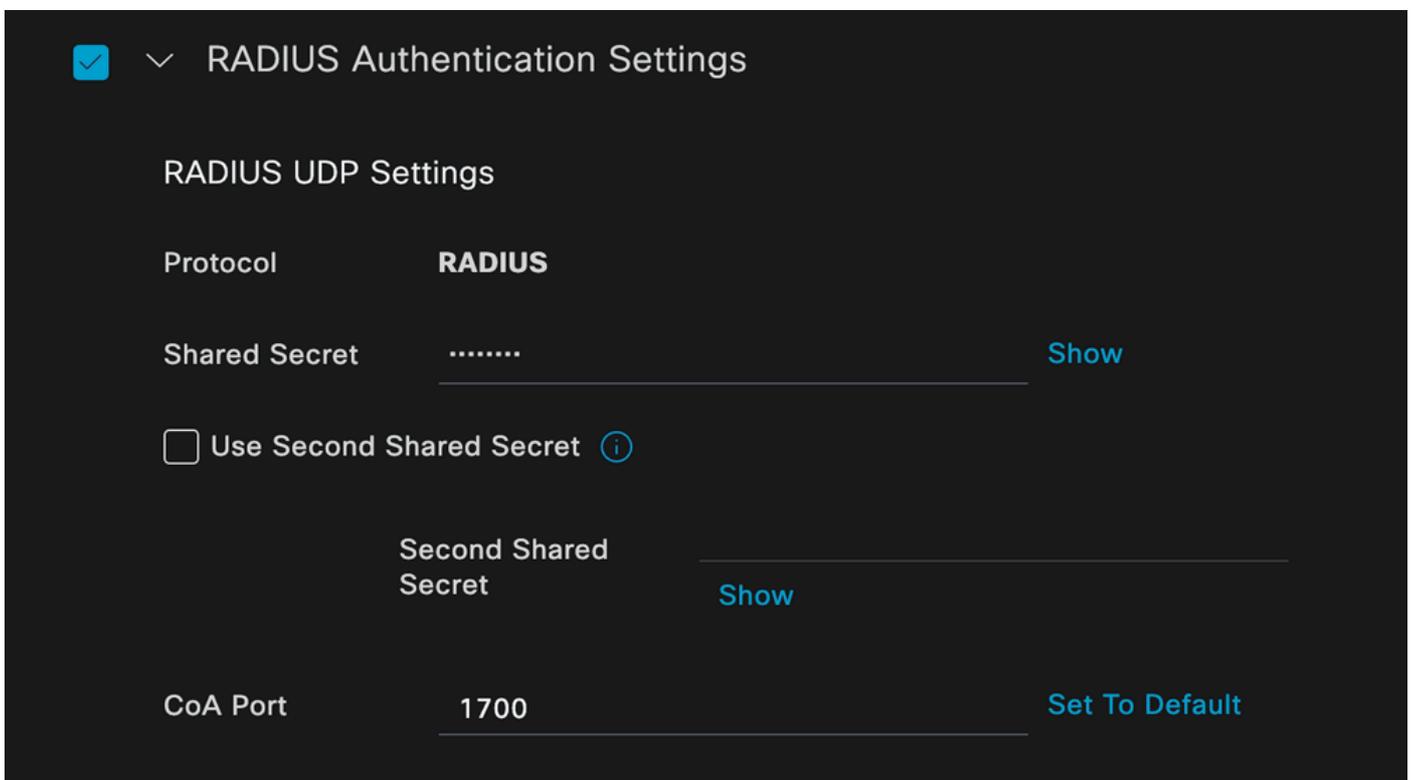
輸入值，為您建立的NAD指定名稱，並增加網路裝置用於聯絡ISE的IP。



網路裝置建立頁面

在此同一頁中，向下滾動以查詢Radius Authentication Settings。如下圖所示。

增加在NAD配置下使用的共用金鑰。



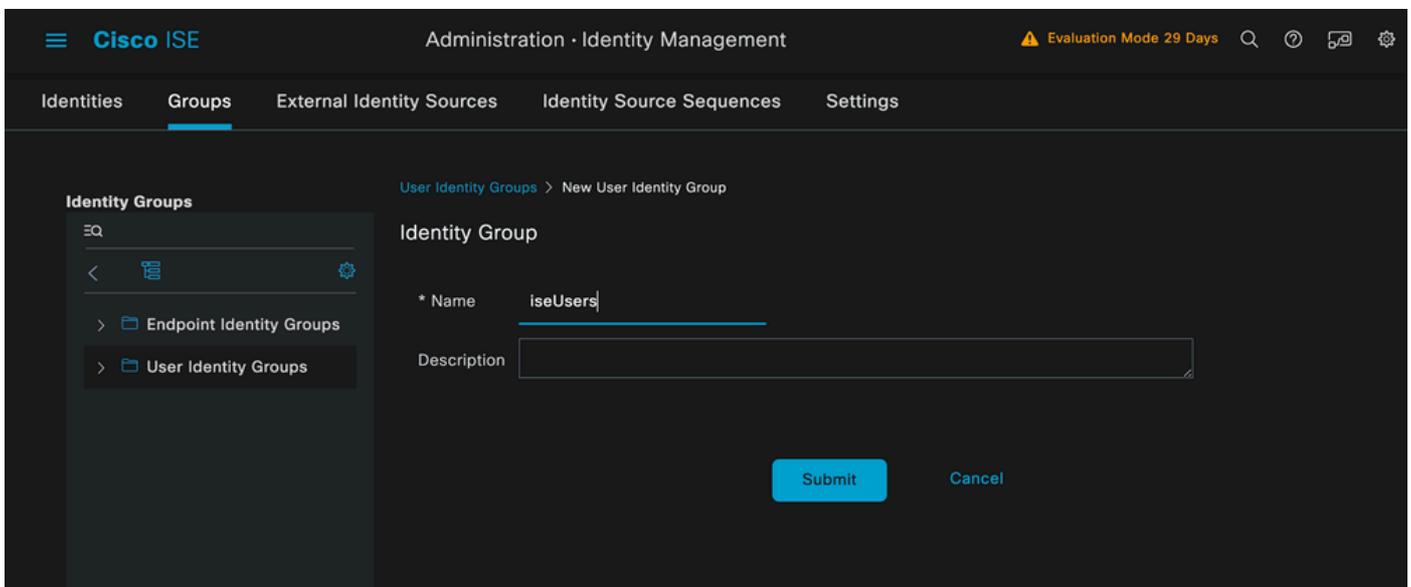
Radius配置

儲存變更。

2. b.配置用於驗證終端的身份。

注意：為了保持此配置指南不變，將使用簡單的ISE本地身份驗證。

導航到管理>身份管理>組頁籤。建立組和身份，為此演示建立的組為iseUsers。



The screenshot displays the Cisco ISE Administration interface for Identity Management. The breadcrumb trail is "User Identity Groups > New User Identity Group". The "Identity Group" configuration form is visible, with the following fields:

- \* Name: iseUsers
- Description: (empty text box)

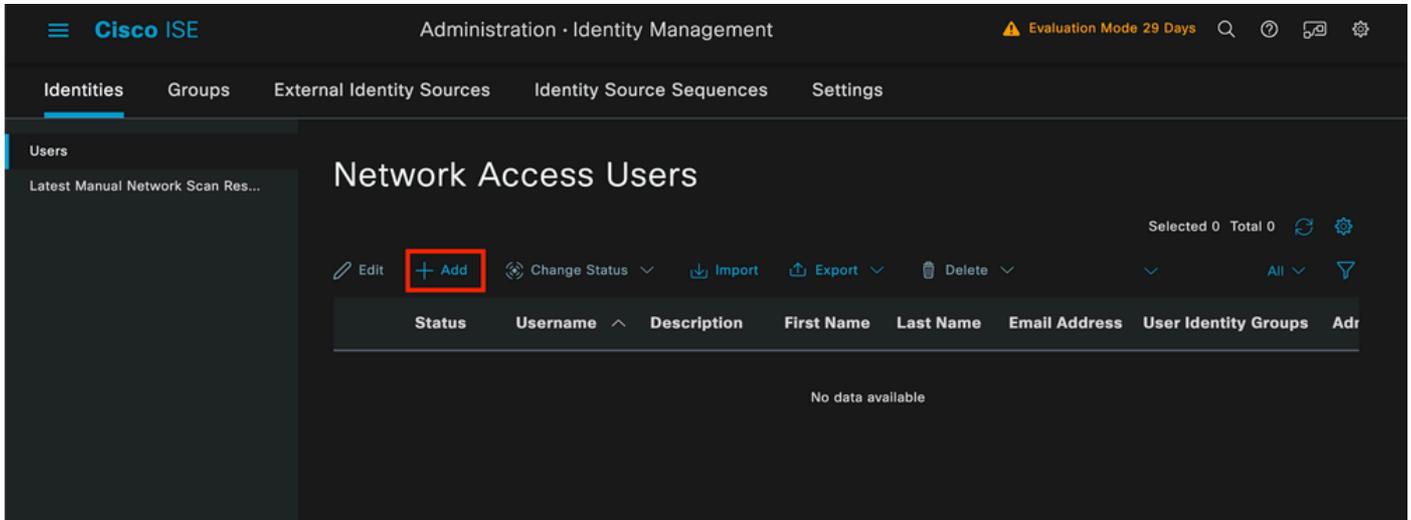
At the bottom of the form, there are "Submit" and "Cancel" buttons. The left sidebar shows the "Identity Groups" menu with "Endpoint Identity Groups" and "User Identity Groups" options.

辨識群組建立頁面

按一下Submit按鈕。

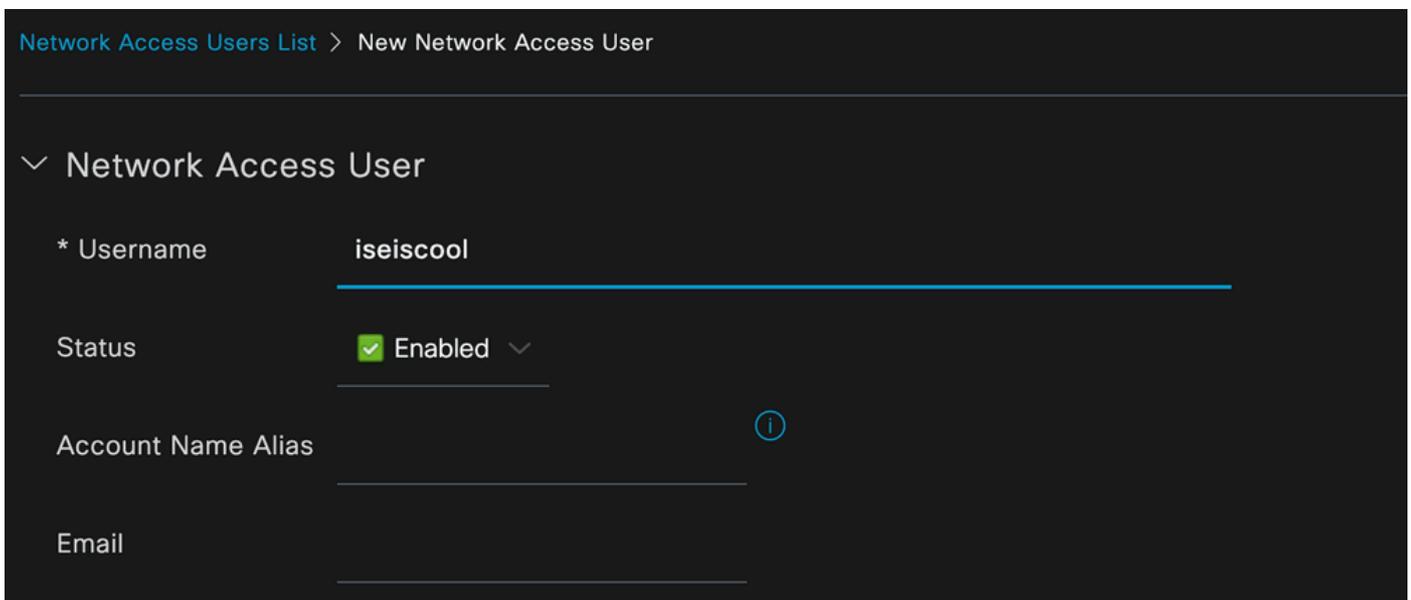
然後，導航到Administration > Identity Management > Identity頁籤。

按一下Add。



使用者建立頁面

作為必填欄位的一部分，以使用者名稱稱開頭。本示例中使用使用者名稱iseiscool。



指定給使用者名稱的名稱

下一步是為建立的使用者名稱分配密碼。VainillaISE97用於此演示。

Passwords  
 Password Type: Internal Users  
 Password Lifetime:  
 With Expiration  
 Password will expire in 60 days  
 Never Expires  
 Password Re-Enter Password  
 \* Login Password .....  
 Enable Password .....  
 Generate Password  
 Generate Password

密碼建立

將使用者分配到iseUsers組。

User Groups  
 iseUsers

指定使用者群組

## 2. c. 配置策略集

導航到ISE選單>策略>策略集。

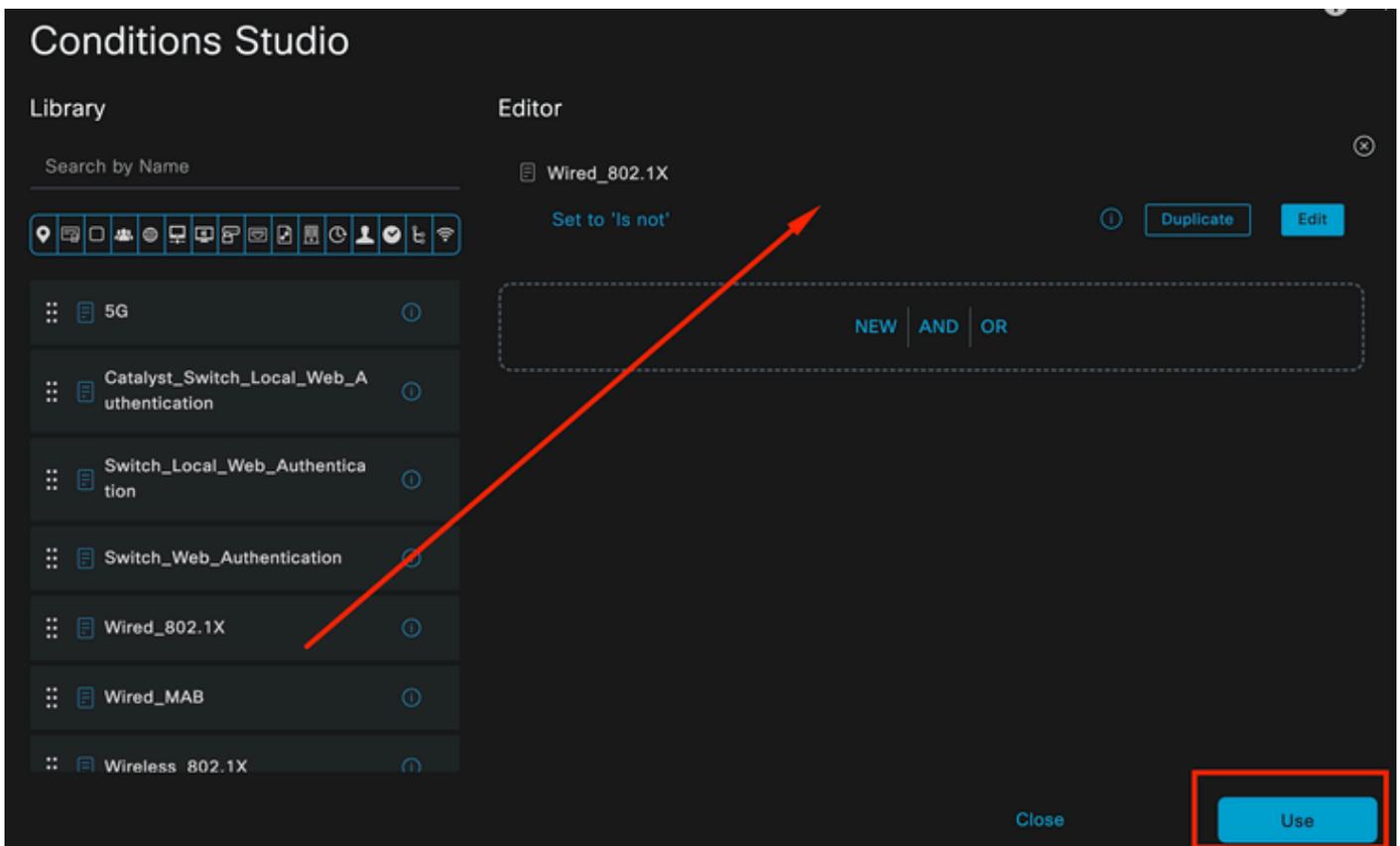
可以使用預設策略集。但是本示例中建立了一個策略集，稱為有線。對策略集進行分類和區分有助於進行故障排除，

如果看不到「增加」或「加號」圖示，則可以按一下任何策略集的齒輪圖示。選取齒輪圖示，然後選取「在上方插入新列」。

Default Default policy set Default Network Access 63  
 Insert new row above

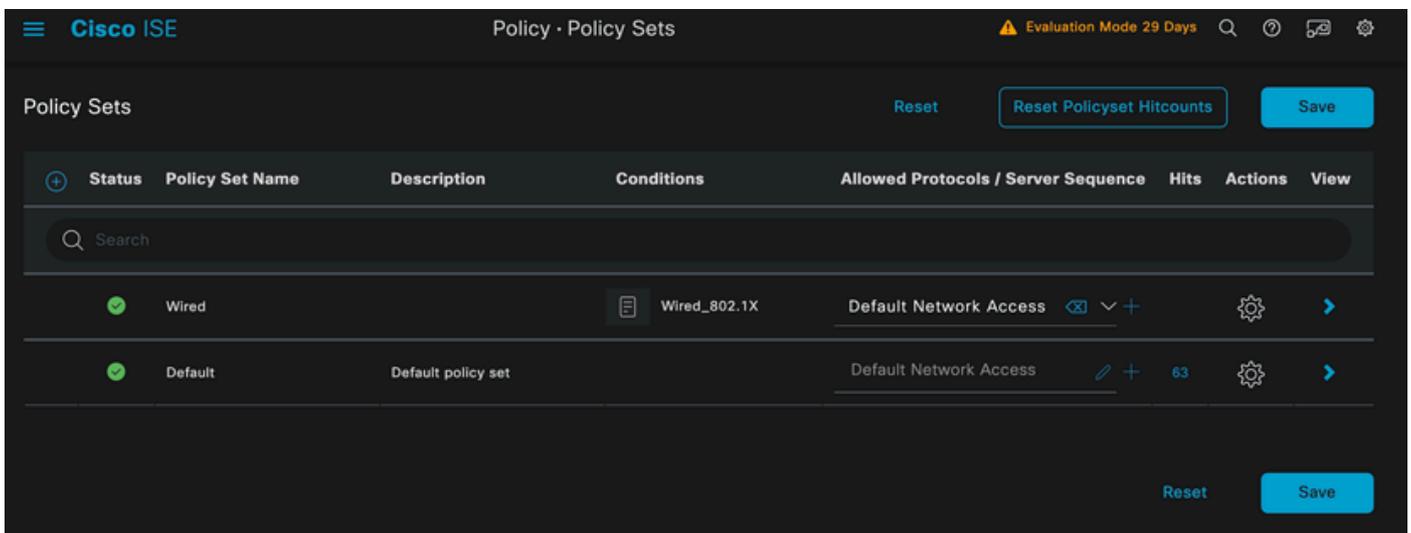
策略建立

本示例中配置的條件是有線8021x，這是在ISE新部署中預配置的條件。拖動它，然後按一下Use。



條件工作室

最後，選擇Default Network Access預配置的允許協定服務。



策略集檢視

按一下Save。

2. d.配置身份驗證和授權策略。

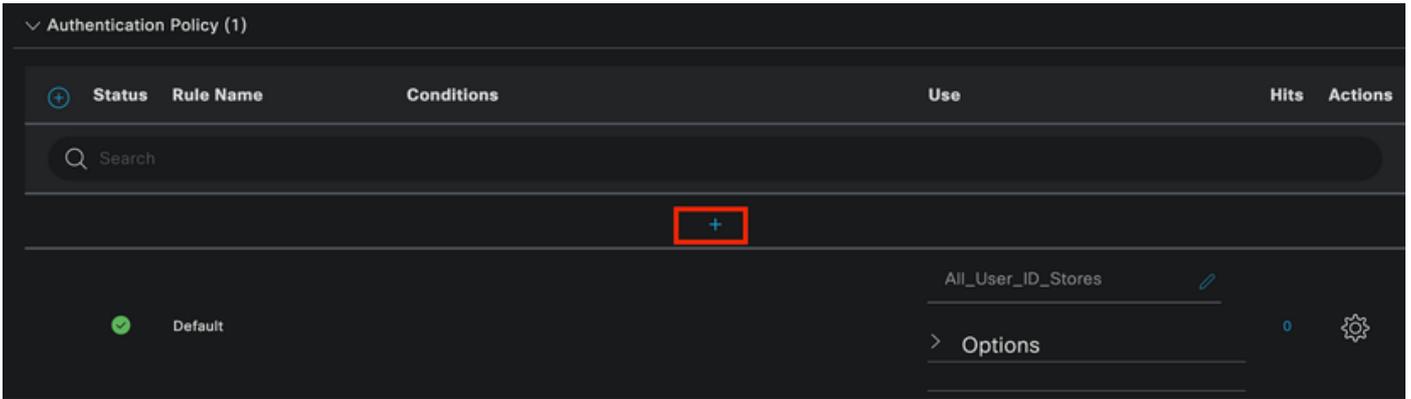
點選剛剛建立的策略集右側的箭頭。



有線策略集

## 展開身份驗證策略

按一下+圖示。



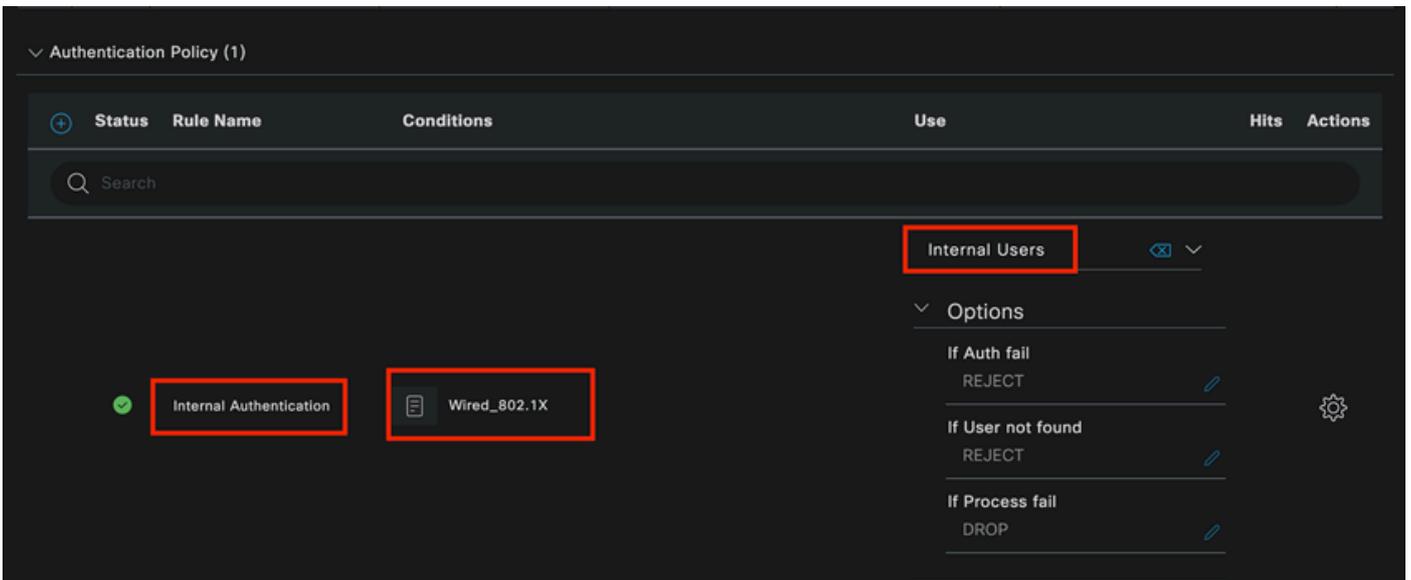
增加身份驗證策略

為身份驗證策略分配名稱，例如，使用內部身份驗證。

按一下此新身份驗證策略的「條件」列上的+圖示。

可以採用隨附的預配置條件Wired Dot1x ISE。

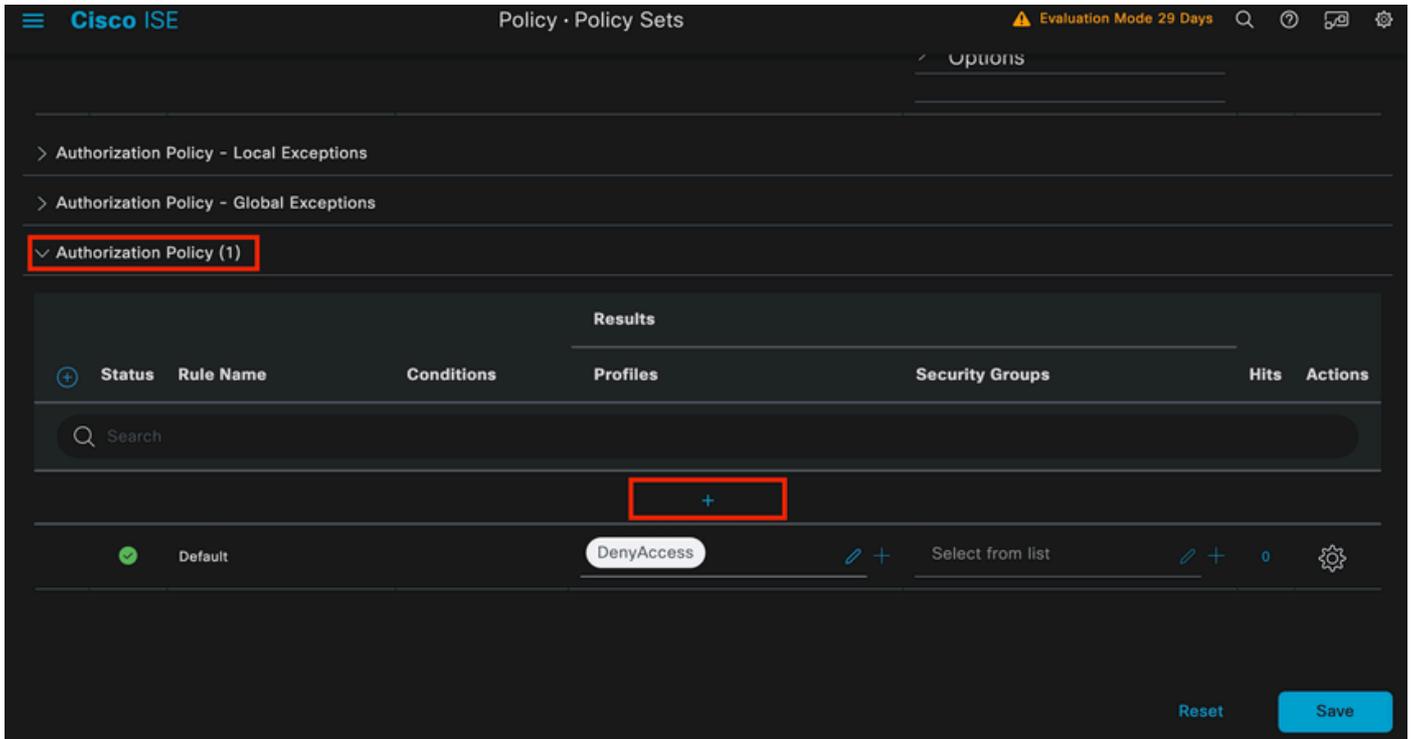
最後，在使用列下，從下拉選單中選擇「內部使用者」。



身份驗證策略

## 授權策略

Authorization Policy部分位於頁面底部。展開它並按一下+圖示。



#### 授權策略

為您剛增加的授權策略命名，在此配置示例中，使用名稱Internal ISE Users。

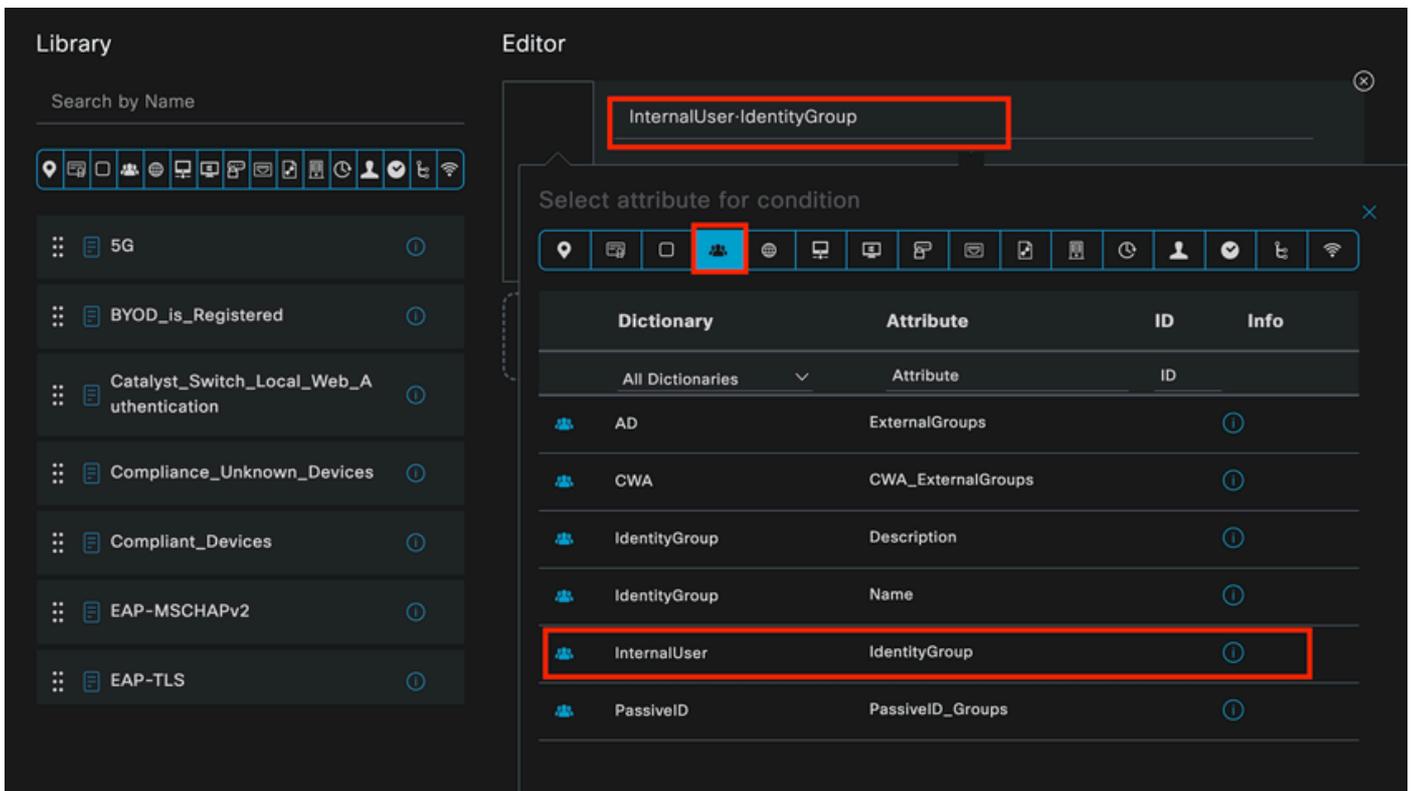
要為此授權策略建立條件，請點選條件列下的+圖示。

之前建立的使用者是IseUsers組的一部分。

在編輯器中按一下Click to add an attribute部分。

選取「身份群組」圖示。

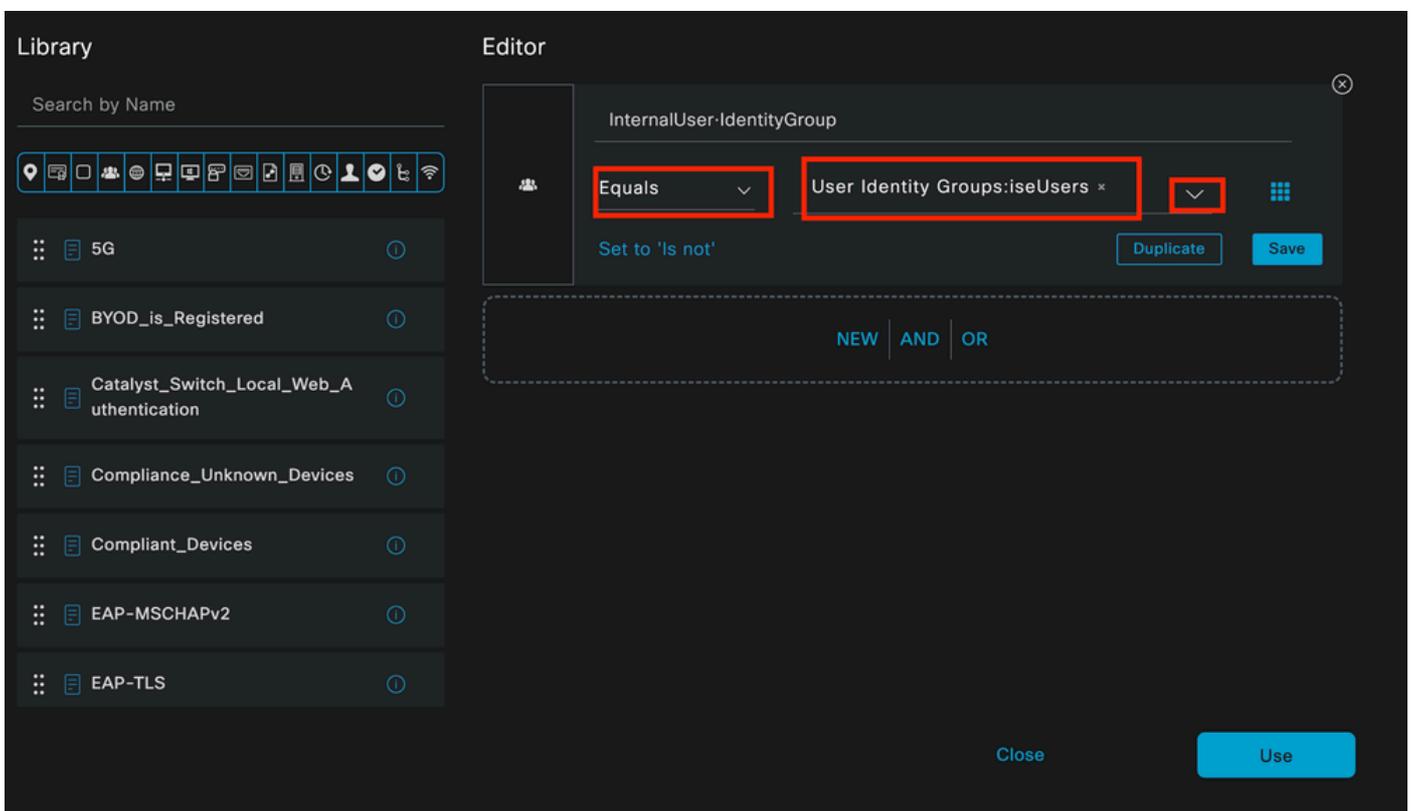
從詞典中，選取Identity Group屬性隨附的InternalUser詞典。



授權策略的Condition Studio

選取等於運算子。

從User Identity Groups下拉選單中，選擇組iseUsers。

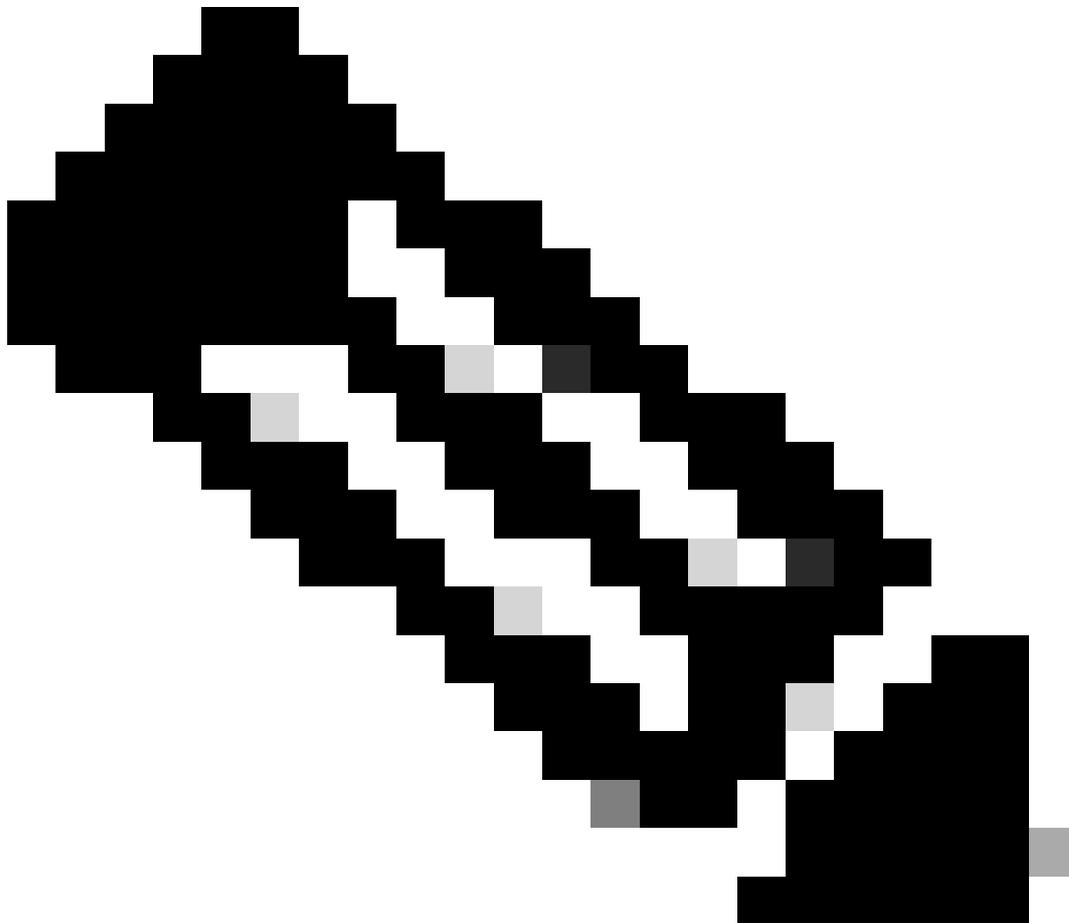


授權策略條件已完成

按一下Use。

最後，選擇接收此身份組的身份驗證部分的Result Authorization Profile。

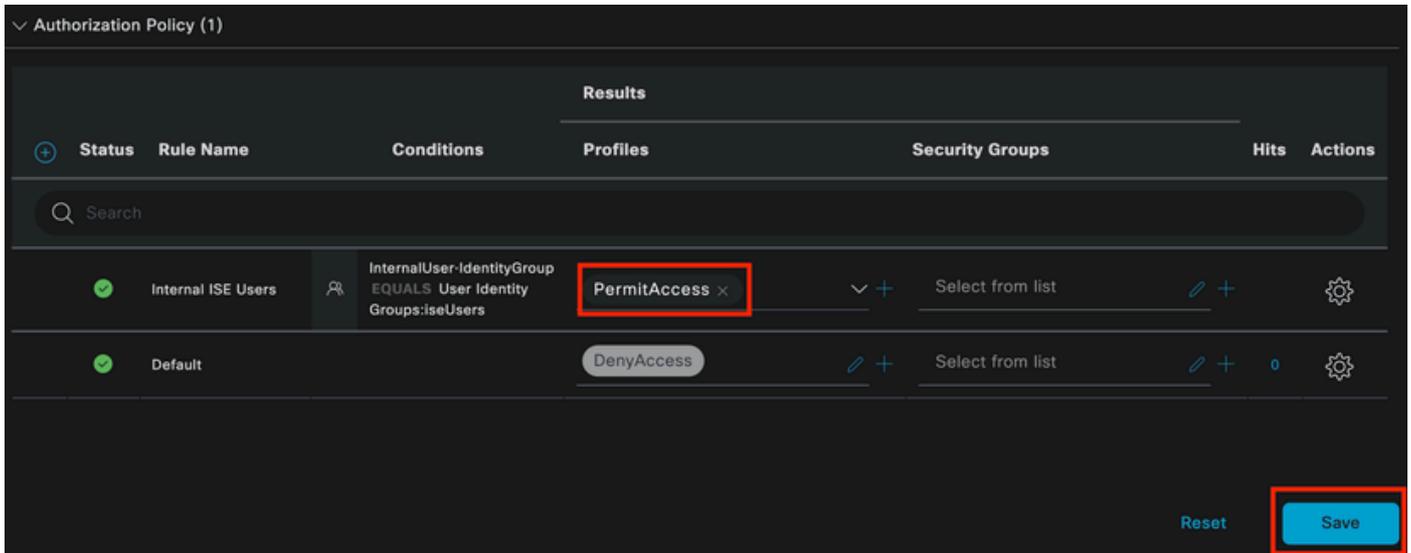
---



注意：請注意，到達ISE且到達此有線Dot1x策略集的身份驗證不屬於使用者身份組ISEUsers，現在到達預設授權策略。配置檔案結果為DenyAccess。

---

ISE已透過允許訪問配置檔案進行預配置。選擇它。



授權策略已完成

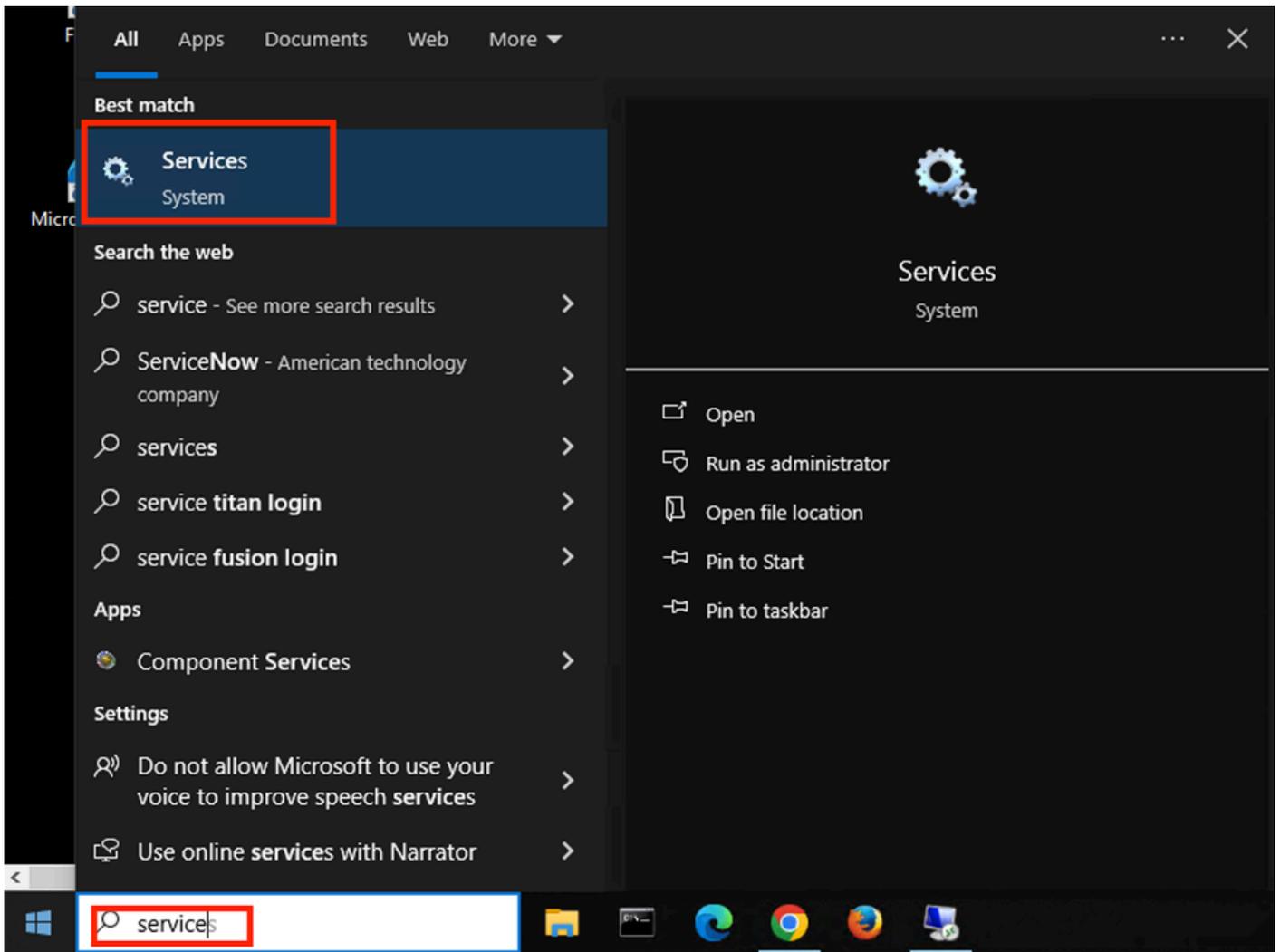
按一下Save。

ISE的配置已完成。

步驟 3.Windows原生Supplicant客戶端配置

3. a.在Windows上啟用Wired dot1x。

從Windows搜尋欄打開Services。



Windows搜尋列

在Services清單的底部，找到Wired Autoconfig。

按一下右鍵「Wired AutoConfig」並選擇屬性。

# Wired AutoConfig Properties (Local Computer)



General Log On Recovery Dependencies

Service name: dot3svc

Display name: Wired AutoConfig

Description: responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X

Path to executable:

C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p

Startup type: Manual

Service status: Stopped

Start

Stop

Pause

Resume

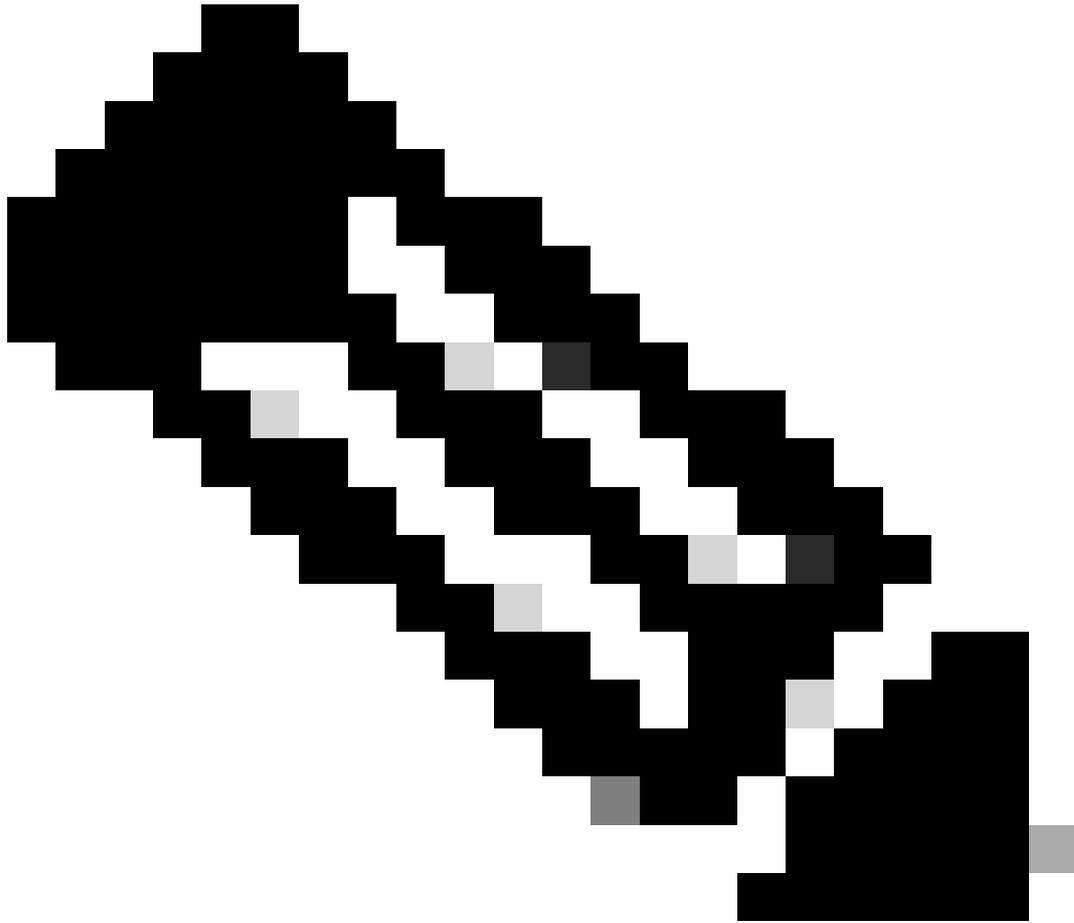
You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK

Cancel

Apply



注意：有線自動配置(DOT3SVC)服務負責在乙太網介面上執行IEEE 802.1X身份驗證。

---

已選擇Manual啟動型別。

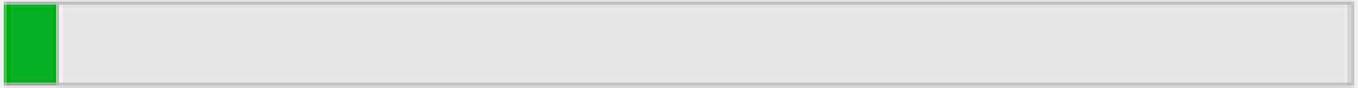
因為服務狀態為Stopped。按一下Start。

## Service Control



Windows is attempting to start the following service on Local Computer...

Wired AutoConfig



Close

服務控制

然後，按一下OK。

此服務之後正在運行。

Windows Update	Enables the ...	Running	Manual (Trig...	Local System...
Windows Update Medic Service	Enables rem...		Manual	Local System...
WinHTTP Web Proxy Auto-Discovery Service	WinHTTP i...	Running	Manual	Local Service
Wired AutoConfig	The Wired A...	Running	Manual	Local System...
WLAN AutoConfig	The WLANS...		Manual	Local System...
WMI Performance Adapter	Provides pe...		Manual	Local System...
Work Folders	This service ...		Manual	Local Service

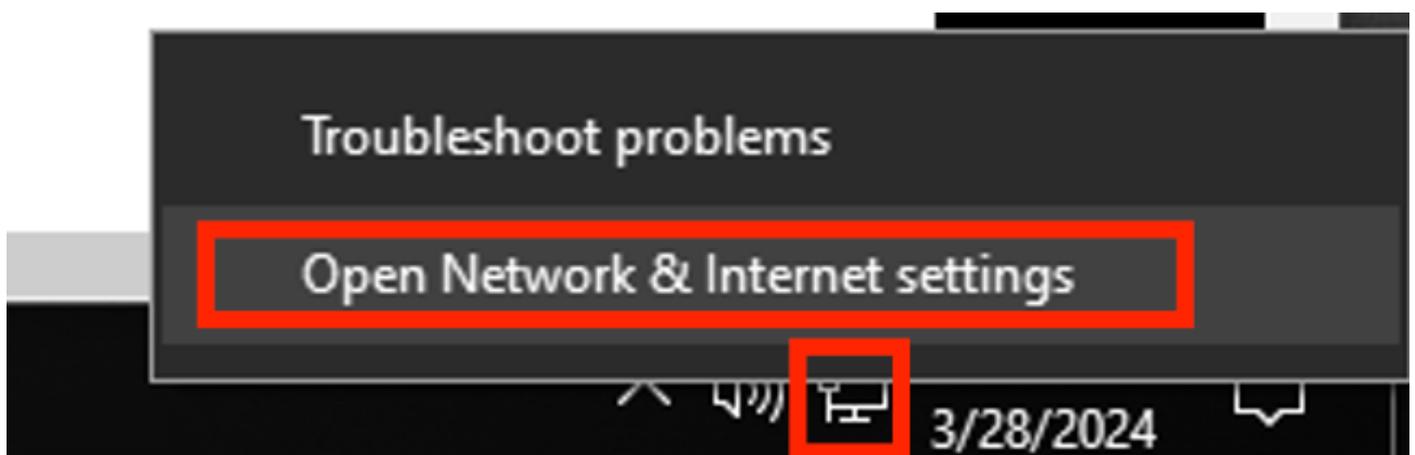
有線自動設定服務

3. b. 配置連線到NAD身份驗證器(ISR 1100)的Windows筆記型電腦介面。

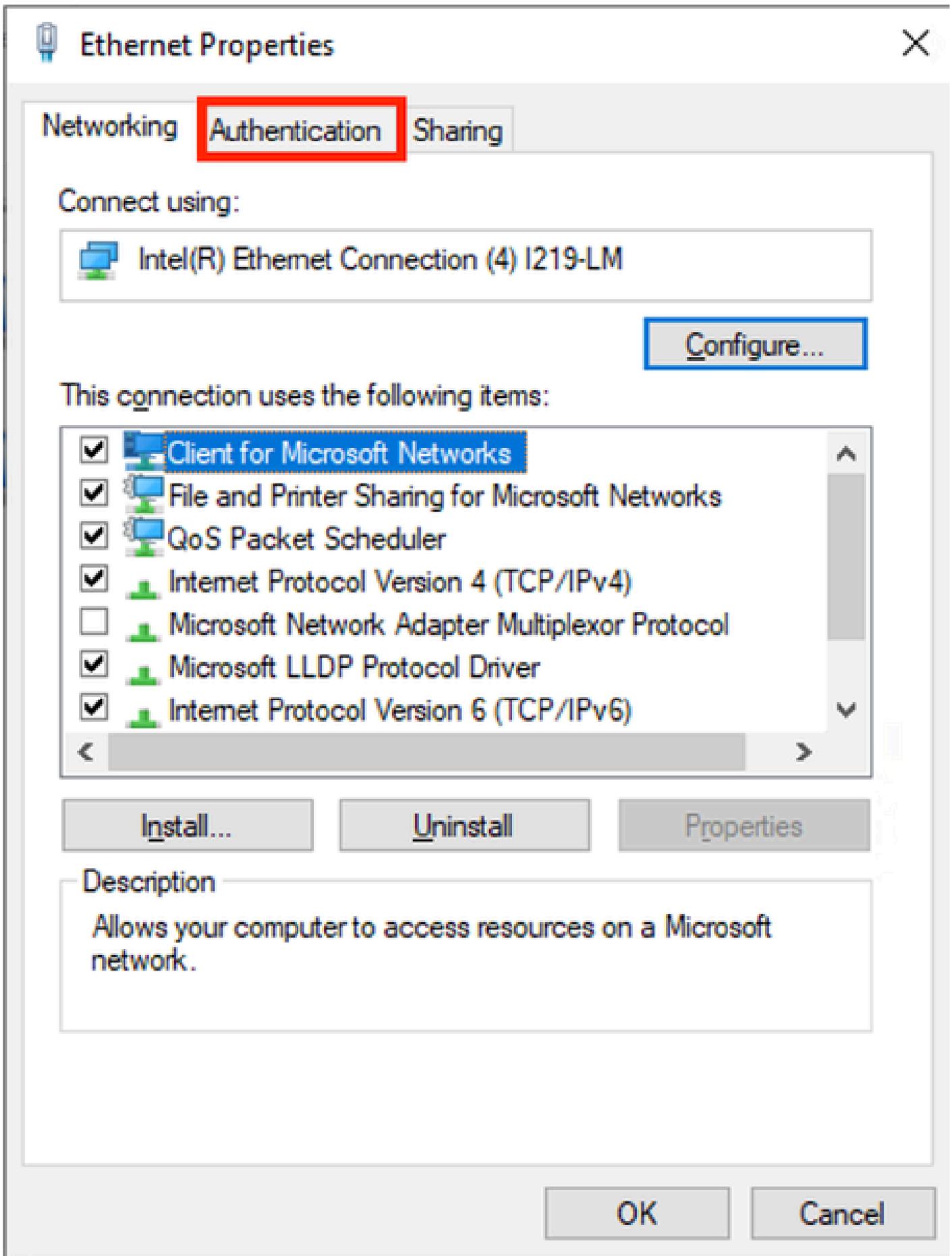
從工作列找到右邊角，然後使用電腦圖示。

按兩下電腦圖示。

選擇Open Network & Internet Settings。



打開網路連線窗口後，按一下右鍵連線到ISR Gig 0/1/0的乙太網介面。按一下Properties選項。  
按一下Authentication頁籤。



介面乙太網路內容

選中Enable IEEE 802.1X authentication覈取方塊。



# Ethernet Properties



Networking

Authentication

Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) ▾

Settings

Remember my credentials for this connection each time I'm logged on

Fallback to unauthorized network access

Additional Settings...

OK

Cancel

選擇受保護的EAP (PEAP)。

取消選中每次登入時記住此連線的憑據選項。

按一下設定。

## Protected EAP Properties



When connecting:

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1;srv2;. \*\.srv3\.com):

Trusted Root Certification Authorities:

- AAA Certificate Services
- Baltimore CyberTrust Root
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA
- DigiCert Global Root G2

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

Configure...

Enable Fast Reconnect

Disconnect if server does not present cryptobinding TLV

Enable Identity Privacy

OK

Cancel

Interface: GigabitEthernet0/1/0  
IIF-ID: 0x08767C0D  
MAC Address: 8c16.450d.f42b  
IPv6 Address: Unknown  
IPv4 Address: Unknown  
User-Name: iseiscool <----- The username configured for Windows Native Supplicant  
Status: Authorized <----- An indication that this session was authorized by the PSN  
Domain: DATA  
Oper host mode: multi-auth  
Oper control dir: both  
Session timeout: N/A  
Common Session ID: 22781F0A0000000C83E28461  
Acct Session ID: 0x00000003  
Handle: 0xc6000002  
Current Policy: POLICY\_Gi0/1/0

Local Policies:

Service Template: DEFAULT\_LINKSEC\_POLICY\_SHOULD\_SECURE (priority 150)  
Security Policy: Should Secure

Server Policies:

Method status list:

Method	State
dot1x	Authc Success <----- An indication that dot1x is used for this authentication

Router#

## ISE日誌

導航到操作> Radius >即時日誌頁籤。

按使用者名稱標識過濾，在本示例中，使用使用者名稱iseiscool。

Operations · RADIUS

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 1 Client Stopped Responding 0 Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authc
×				iseiscool	Endpoint ID	Endpoint Pr	Authentication Policy	Authc
Mar 28, 2024 07:04:35.4...			0	iseiscool	8C:16:45:0D:F4:...	Unknown	Wired >> Internal Authentication	Wired
Mar 28, 2024 07:04:35.3...				iseiscool	8C:16:45:0D:F4:...	Unknown	Wired >> Internal Authentication	Wired

Last Updated: Thu Mar 28 2024 01:29:12 GMT-0600 (Central Standard Time) Records Shown: 2

ISE即時日誌

Operations · RADIUS

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 1 Client Stopped Responding 0 Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 3 hours

Reset Repeat Counts Export To Filter

Authorization Policy	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server
Wired >> Internal ISE Users	PermitAcc...	IP Address		GigabitEthernet0/1/0			PSN01
Wired >> Internal ISE Users	PermitAcc...	ISR1100	GigabitEthernet0/1/0	User Identity Groups:iseUsers			PSN01

Last Updated: Thu Mar 28 2024 01:34:19 GMT-0600 (Central Standard Time) Records Shown: 2

ISE即時日誌

請注意，從這個快速檢視，即時記錄提供重要資訊：

- 身份驗證的時間戳。
- 使用的身分辨識。
- 終端MAC地址。
- 原則集和命中的驗證原則。
- 策略集和已命中的授權策略。
- 授權配置檔案結果。
- 向ISE傳送RADIUS請求的網路裝置。
- 終端所連線的介面。
- 透過身份驗證的使用者的身份組。
- 處理身份驗證的策略伺服器節點(PSN)。

## 疑難排解

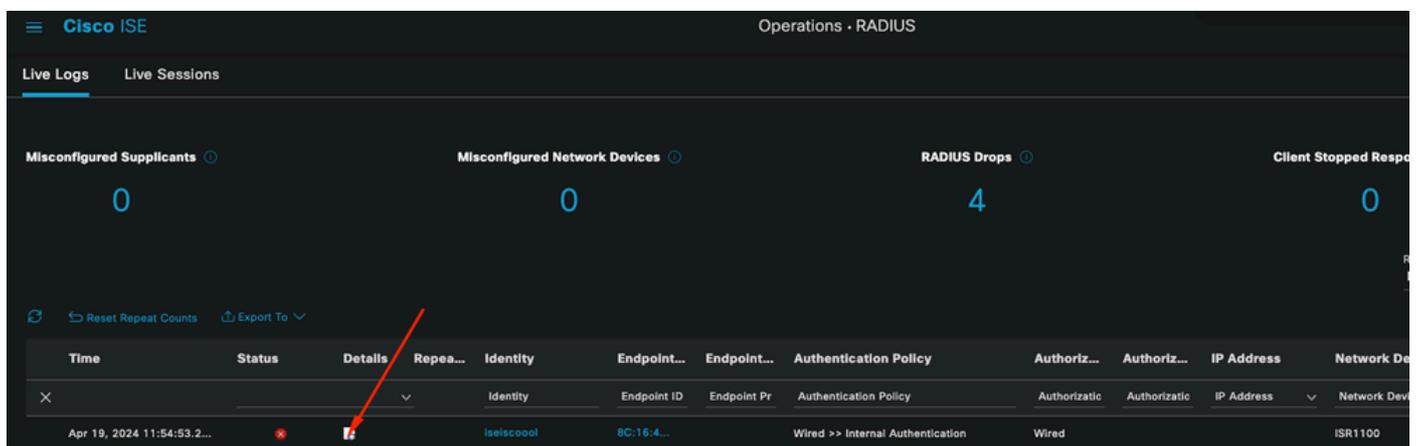
### 1 - 讀取ISE即時日誌詳細資訊

導航到操作> Radius > Live logs頁籤，按Auth status：Failed進行過濾，或按使用的使用者名稱或按MAC地址進行過濾，或按使用的網路訪問裝置進行過濾。

訪問操作> Radius > 即時日誌> 所需身份驗證> 即時日誌詳細資訊。

在同一頁上，過濾身份驗證後，按一下Search圖示。

第一種情況：使用者輸入其使用者名稱時帶有輸入錯誤。



The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are tabs for 'Live Logs' and 'Live Sessions'. Below the tabs, there are four summary cards: 'Misconfigured Suppliants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (4), and 'Client Stopped Respo' (0). Below these cards, there are buttons for 'Reset Repeat Counts' and 'Export To'. A table with columns for Time, Status, Details, Repea..., Identity, Endpoint..., Authentication Policy, Authoriz..., Authoriz..., IP Address, and Network De is visible. A red arrow points to the 'Details' column header. Below the table, there is a search bar with a magnifying glass icon and a red 'X' icon. The search results show a failed authentication attempt for the user 'Iselscoool' on 'Apr 19, 2024 11:54:53.2...' with the status 'Failed'.

開啟Live Log詳細資料

打開即時日誌詳細資訊後，您會看到身份驗證失敗了，並且還會列出使用的使用者名稱。

## Overview

Event	5400 Authentication failed
Username	iseiscoool
Endpoint Id	<ENDPOINT MAC ADDRESS>#
Endpoint Profile	
Authentication Policy	Wired >> Internal Authentication
Authorization Policy	Wired
Authorization Result	

### 概觀段落

然後，在同一即時日誌詳細資訊中，您可以在「身份驗證詳細資訊」部分找到錯誤的失敗原因、根本原因和解決方案。

Event	5400 Authentication failed
Failure Reason	22056 Subject not found in the applicable identity store(s)
Resolution	Check whether the subject is present in any one of the chosen identity stores. Note that some identity stores may have been skipped due to identity resolution settings or if they do not support the current authentication protocol.
Root cause	Subject not found in the applicable identity store(s).
Username	iseiscoool

### 身份驗證詳細資訊

在此場景中，身份驗證失敗的原因是因為使用者名稱有拼寫錯誤，但是，如果使用者不是在ISE中建立，或者ISE無法驗證使用者存在於其他身份庫（例如LDAP或AD）中，也會出現同樣的錯誤。

### 步驟段落

15041 Evaluating Identity Policy

15013 Selected Identity Source - Internal Users ←

24210 Looking up User in Internal Users IDStore - iseiscoool ←

24216 The user is not found in the internal users identity store ←

22056 Subject not found in the applicable identity store(s) ←

22058 The advanced option that is configured for an unknown user is used

22061 The 'Reject' advanced option is configured in case of a failed authentication request ←

11815 Inner EAP-MSCHAP authentication failed ←

11520 Prepared EAP-Failure for inner EAP method

22028 Authentication failed and the advanced options are ignored

12305 Prepared EAP-Request with another PEAP challenge

11006 Returned RADIUS Access-Challenge

11001 Received RADIUS Access-Request

11018 RADIUS is re-using an existing session

12304 Extracted EAP-Response containing PEAP challenge-response

61025 Open secure connection with TLS peer

12307 PEAP authentication failed ←

11504 Prepared EAP-Failure

11003 Returned RADIUS Access-Reject ←

即時記錄詳細資訊步驟段落

步驟部分詳細描述了ISE在RADIUS會話期間運行的過程。

您可以在此處找到以下資訊：

- 通話是如何開始的。
- SSL握手過程。
- 協商的EAP方法。
- EAP方法進程。

在此示例中，可以看到ISE剛剛簽入了此身份驗證的內部身份。找不到使用者，因此，ISE作為響應傳送了Access-Reject。

第二個場景：ISE管理員停用了Policy Set Allowed protocols中的PEAP。

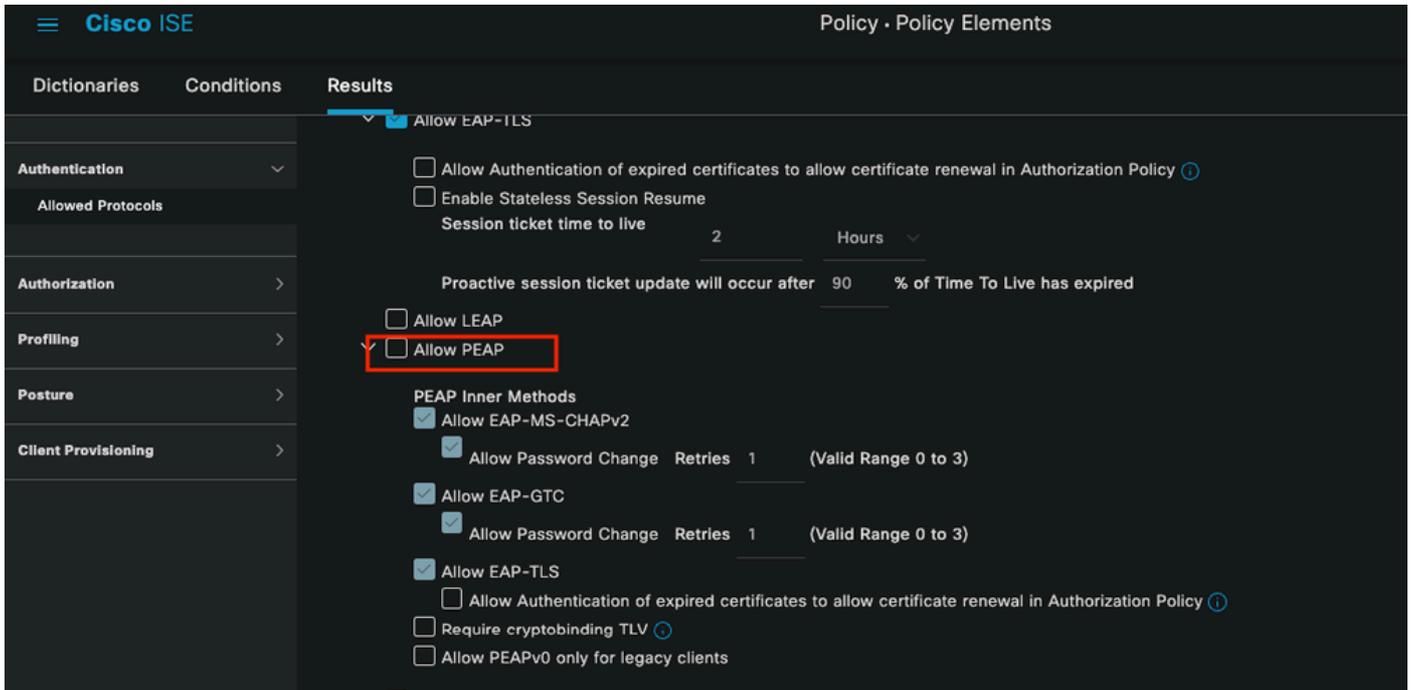
## 2 -已停用PEAP

打開會話失敗的即時日誌詳細資訊後，將顯示錯誤消息「PEAP is not allowed in the Allowed Protocols」。

Event	5400 Authentication failed
Failure Reason	12303 Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols
Resolution	Ensure that the PEAP protocol is allowed by ISE in Allowed Protocols.
Root cause	The client's supplicant sent an EAP-Response/NAK packet rejecting the previously-proposed EAP-based protocol, and requesting to use PEAP instead. However, PEAP is not allowed in Allowed Protocols.
Username	iseiscool

即時日誌詳細資訊報告

此錯誤很容易解決，解決方法是導航到策略>策略元素>身份驗證>允許的協定。驗證是否停用了Allow PEAP選項。



允許的Portocols部分

第三種情況：身份驗證失敗，因為終端不信任ISE證書。

導航到即時日誌詳細資訊。查詢身份驗證失敗的記錄並檢查即時日誌詳細資訊。

## Authentication Details

Source Timestamp 2024-04-20 04:37:42.007

Received Timestamp 2024-04-20 04:37:42.007

Policy Server ISE PSN

Event 5411 Supplicant stopped responding to ISE

Failure Reason 12934 Supplicant stopped responding to ISE during PEAP tunnel establishment

Resolution Check whether the proper server certificate is installed and configured for EAP in the Local Certificates page ( Administration > System > Certificates > Local Certificates ). Also ensure that the certificate authority that signed this server certificate is correctly installed in client's supplicant. Check the previous steps in the log for this EAP-TLS conversation for a message indicating why the handshake failed. Check the OpenSSLErrorMessage and OpenSSLErrorStack for more information.

Root cause PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

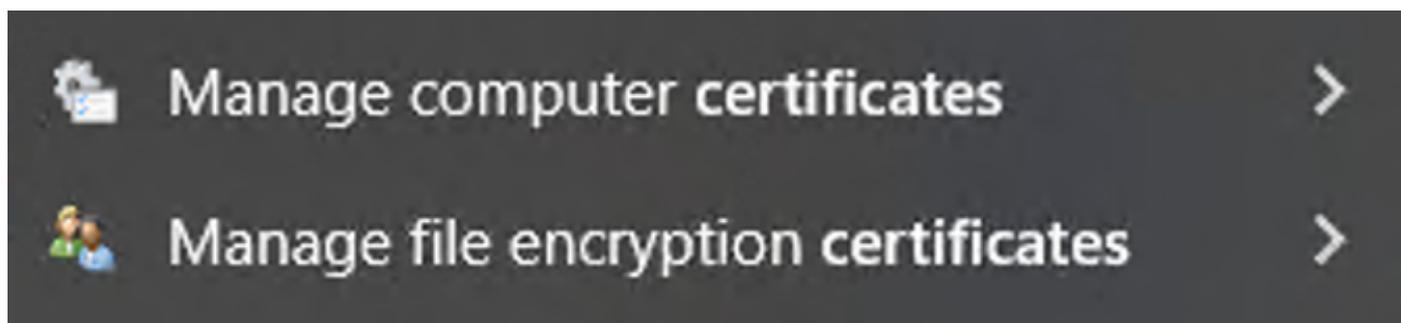
Username iseiscool

即時日誌詳細資訊

端點拒絕用於PEAP通道建立的憑證。

要解決此問題，請在存在問題的Windows終端中驗證簽署ISE證書的CA鍵是否在管理使用者證書 > 受信任的根證書頒發機構或管理電腦證書 > 受信任的根證書頒發機構部分中。

您可以在Windows搜尋列中搜尋Windows裝置上的此組態區段。

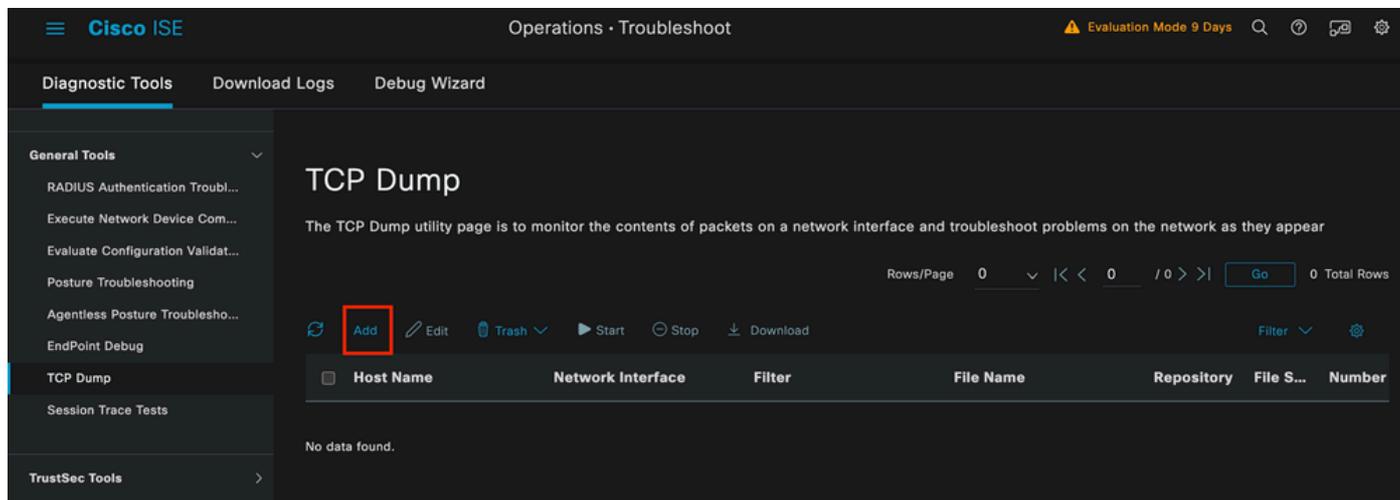


Windows搜尋列結果

### 3 - ISE TCP轉儲工具 ( 資料包捕獲 )

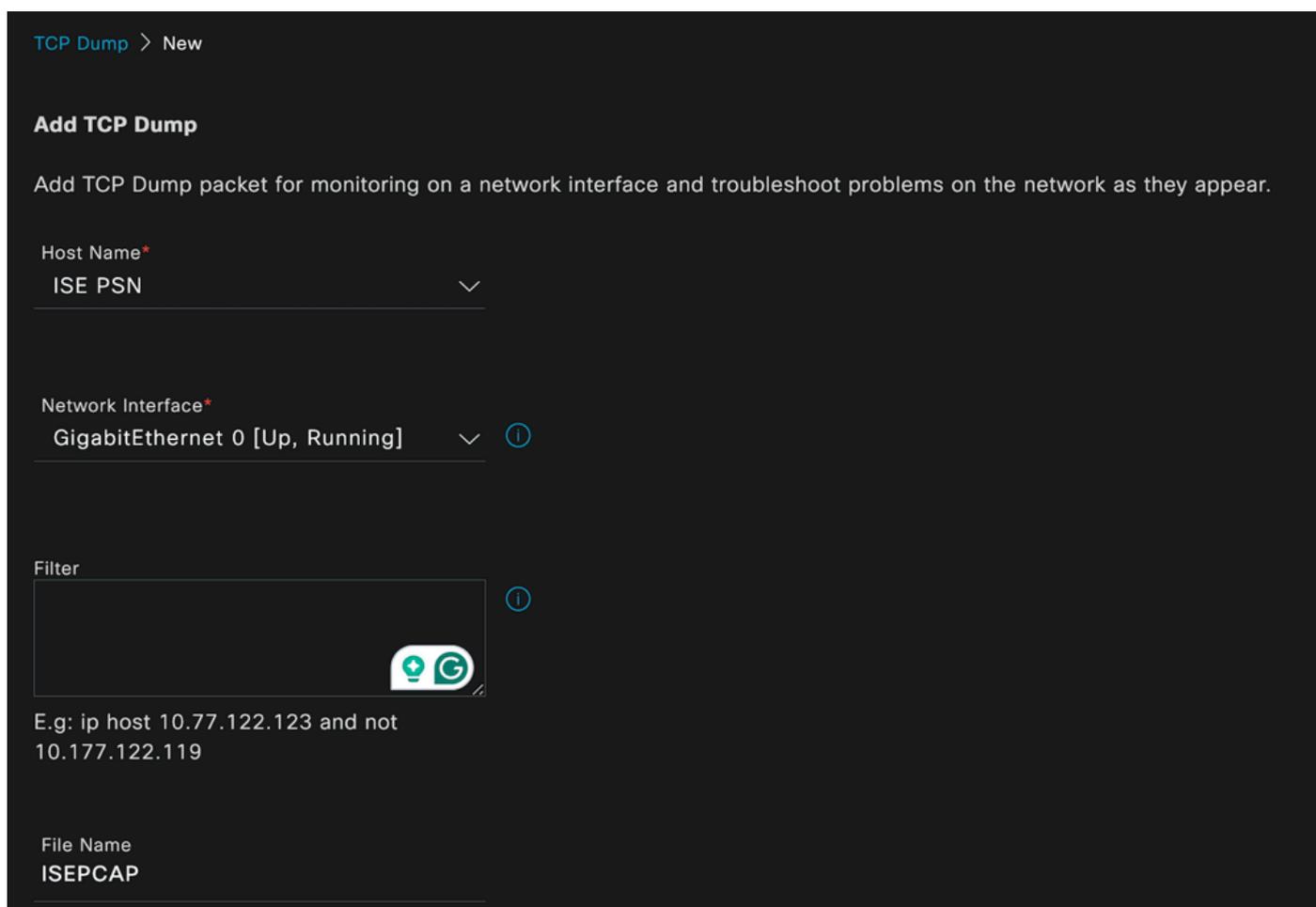
資料包捕獲分析在故障排除時非常重要。直接從ISE資料包捕獲可在所有節點和節點的任何介面上進行。

要訪問此工具，請導航到操作>診斷工具>常規工具> TCP轉儲。



TCP轉儲部分

按一下Add按鈕開始配置pcap。



Repository

File Size  
10  
Mb

Limit to  
1  
File(s)

Time Limit  
5  
Minute(s)

Promiscuous Mode

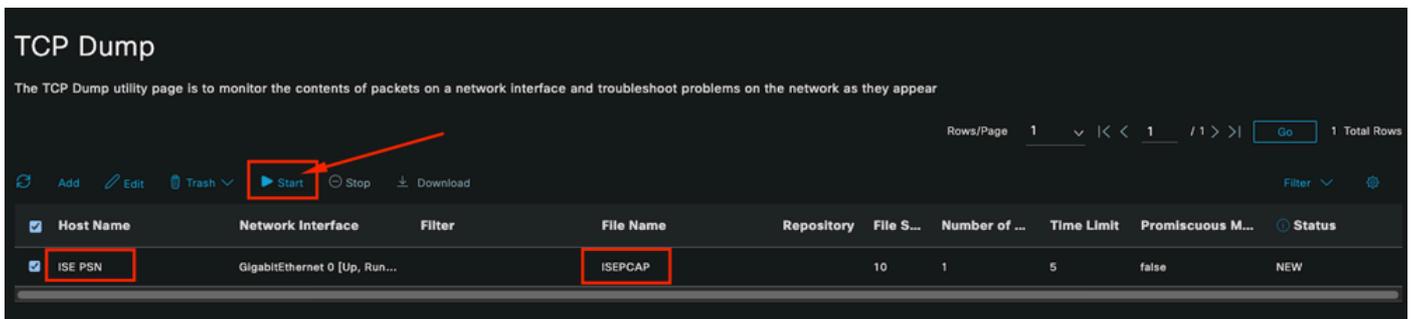
Cancel Save Save and Run

TCP轉儲部分

要在ISE中建立pcap，您必須輸入以下資料：

- 選取您需要在其中取得pcap的節點。
- 選擇用於pcap的ISE節點介面。
- 如果需要捕獲特定流量，請使用過濾器，ISE會提供一些示例。
- 為pcap命名。在此場景中，我們使用ISEPCAP。
- 選擇儲存庫，如果未選擇儲存庫，則捕獲儲存在ISE本地磁碟上，並且可以從GUI下載。
- 此外，如有必要，請修改pcap檔案大小。
- 如有必要，請使用1個以上的檔案，所以如果pcap超過檔案大小，之後會建立一個新檔案。
- 如果需要，可以延長pcap的流量捕獲時間。

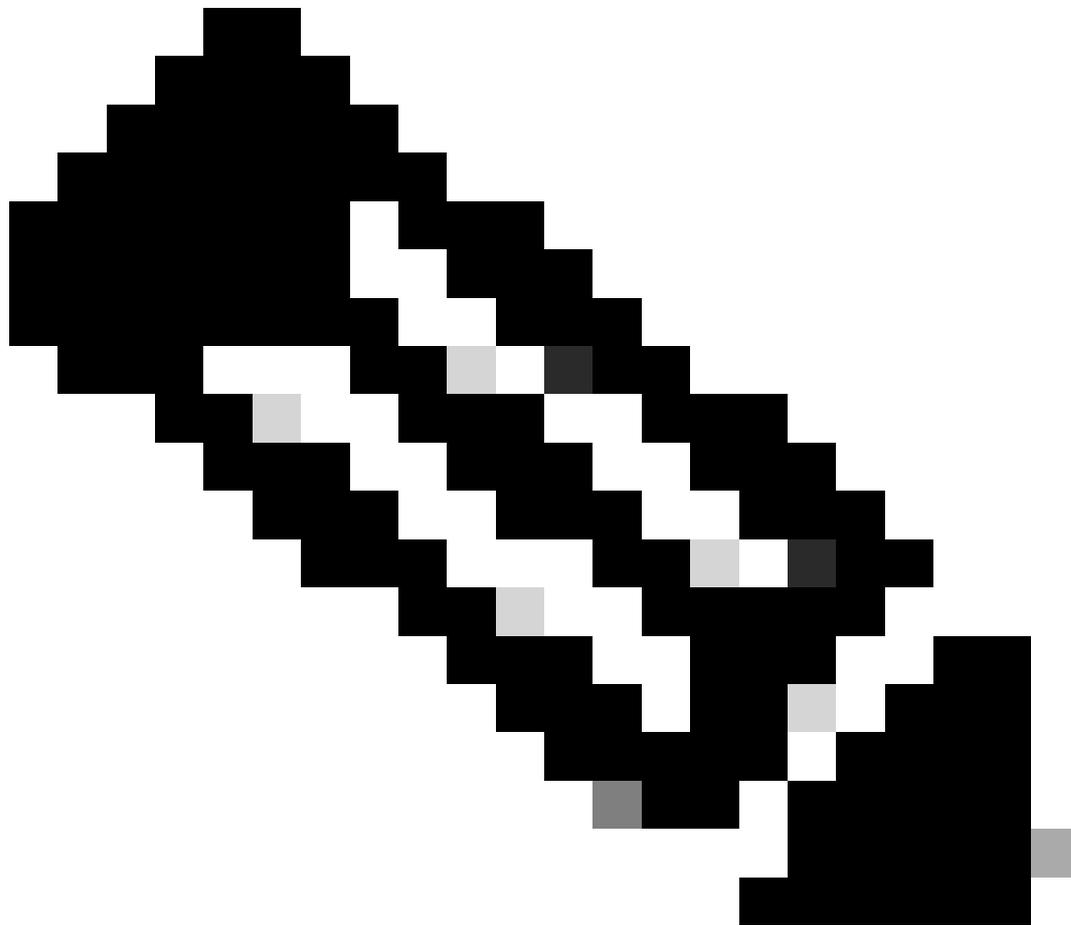
最後，按一下Save按鈕。



TCP轉儲部分

然後，在準備就緒時選擇pcap，然後按一下開始按鈕。

點選開始後，狀態列將更改為運行狀態。



注意：當PCAP處於運行狀態時，會複製失敗方案或需要捕獲的行為。完成後，RADIUS、會話的詳細資訊將顯示在PCAP中。

在PCAP運行期間捕獲所需資料後，請完成pcap收集。再次選擇它並按一下Stop。

### 3 – 1個ISE報告

如果需要更深入的分析，ISE會提供有用的報告以調查過去的事件。

要找到這些報告，請導航到操作>報告>端點和使用者

The screenshot shows the Cisco ISE interface. The top right corner has a red box around the text "Operations · Reports". The left sidebar has a red box around the "Reports" menu item and another red box around the "Endpoints and Users" sub-menu item. The main content area displays "RADIUS Authentications" for the period "From 2024-04-14 00:00:00.0 To 2024-04-21 20:14:56.0". Below this, there is a table with the following data:

Logged At	RADIUS Status	Details	Identity
× Last 7 Days ×	↓		Identity
2024-04-20 05:10:59.176	×	🏠	iselscool
2024-04-20 05:00:59.153	×	🏠	iselscool
2024-04-20 04:50:59.135	×	🏠	iselscool
2024-04-20 04:40:59.097	×	🏠	iselscool

ISE報告部分

## Endpoints and Users



Agentless Posture

Authentication Summary

Client Provisioning

Current Active Sessions

Endpoint & Logical Profi...

Endpoint Scripts Provisi...

External Mobile Device ...

Manual Certificate Provi...

PassiveID

即時日誌部分，您可以選擇最多24小時的過去資料。有時需要舊的身份驗證。當過去運行良好的身份驗證突然開始失敗時，您必須將實際未運行的身份驗證與過去運行的身份驗證進行比較。您可以使用「Radius驗證報告」來達到此目的。

該報告允許您選擇最長30天的時間範圍。另外，保留每個身份驗證的即時日誌詳細資訊報告。

Logged At	RADIUS Status	Details	Identity	Endpoint ID	Endpoint Profile	Authorization Rule
Last 7 Days	Pass		Identity	Endpoint ID	Endpoint Profile	Authorization Rule
2024-04-20 01:24:38.101	✓	🚫	iseiscool	8C:16:45:0D:F4:2B	Unknown	Internal ISE Users
2024-04-19 23:24:51.641	✓	🚫	iseiscool	8C:16:45:0D:F4:2B	Unknown	Internal ISE Users

#### 驗證報告

### 3-3個拒絕或釋放的終端

驗證拒絕的終端的失敗原因是什麼。您可以檢查「已拒絕」或「已釋放的終端」報告。在ISE部署中的所有PSN節點上更新EAP證書，然後整個區域的PEAP身份驗證開始失敗。可以檢查此報告，而不檢查即時日誌詳細資訊，您會知道客戶端拒絕且不信任ISE證書。

Changed At	Endpoint ID	Status	Failure Reason
Last 30 Days			
2024-04-10 21:17:00.64	8C:16:45:0D:F4:2B	Released	
2024-04-10 21:11:34.05	8C:16:45:0D:F4:2B	Rejected	12321 PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate
2024-04-10 20:57:42.11	8C:16:45:0D:F4:2B	Rejected	12321 PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate

#### 拒絕的端點報告

### 3-4 RADIUS記帳報告

當發現過度許可使用問題時，通常使用此選項。在這些情況下，ISE不會釋放許可證，因為它無法確定會話是否完成。ISE使用網路裝置傳送的記帳資料包來確定這一點。從網路裝置到ISE正確共用記賬時，情況如下：

RADIUS Accounting 🔍

From 2024-04-14 00:00:00.0 To 2024-04-21 20:28:47.0

Reports exported in last 7 days 0

Logged At	Details	Account Status Type	Identity	Endpoint ID
×	Last 7 Days	×		
2024-04-20 01:40:50.31		Stop	iseiscool	8C:16:45:0D:F4:2B
2024-04-20 01:37:25.22		Start	iseiscool	8C:16:45:0D:F4:2B
2024-04-20 01:27:42.012		Stop	iseiscool	8C:16:45:0D:F4:2B
2024-04-20 01:24:38.128		Start	iseiscool	8C:16:45:0D:F4:2B
2024-04-19 23:33:11.907		Stop	iseiscool	8C:16:45:0D:F4:2B
2024-04-19 23:24:51.744		Start	iseiscool	8C:16:45:0D:F4:2B

## RADIUS記帳報告

## 3-5身份驗證摘要報告

這些是ISE提供的常用和有用報告。它允許您選擇最多30天的舊資料。在此報告中，您可以看到如下資訊：

- 按天列出的透過身份驗證和失敗身份驗證的百分比。



圖表：按天透過身份驗證

- 每天的身份驗證次數（在圖表中），並可選擇按一下藍色值檢視詳細資料。

## Authentications By Day and Quick Link

Day	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak Response Time (ms)
2024-04-20 00:00:00.0	2	30	32	93.75	33.28	95
2024-04-19 00:00:00.0	1	7	8	87.5	90.63	197
2024-04-10 00:00:00.0	2	3	5	60	544.2	2146
2024-04-09 00:00:00.0	23	3	26	11.54	155.46	863
2024-03-28 00:00:00.0	1	0	1	0	310	310
2024-03-27 00:00:00.0	1	0	1	0	171	171
2024-03-25 00:00:00.0	3	2	5	40	169.6	566
2024-03-22 00:00:00.0	3	0	3	0	30	34

Rows/Page 8 | << 1 >> | 8 Total Rows

按天和快速連結進行身份驗證

- 按失敗原因進行身份驗證，列在頂部清單中，重複次數最多，重複次數較少。

## Authentications By Failure Reason

Failure Reason	Total
12303 Failed to negotiate EAP because PEAP not allowed in the Allowed Protocols	22
22056 Subject not found in the applicable identity store(s)	19
12321 PEAP failed SSL/TLS handshake because the client rejected the ISE local-certificate	2

Rows/Page 3 | << 1 >> | 3 Total Rows

按失敗原因進行的身份驗證

- 用於檢視部署身份驗證中常用身份組的選項。

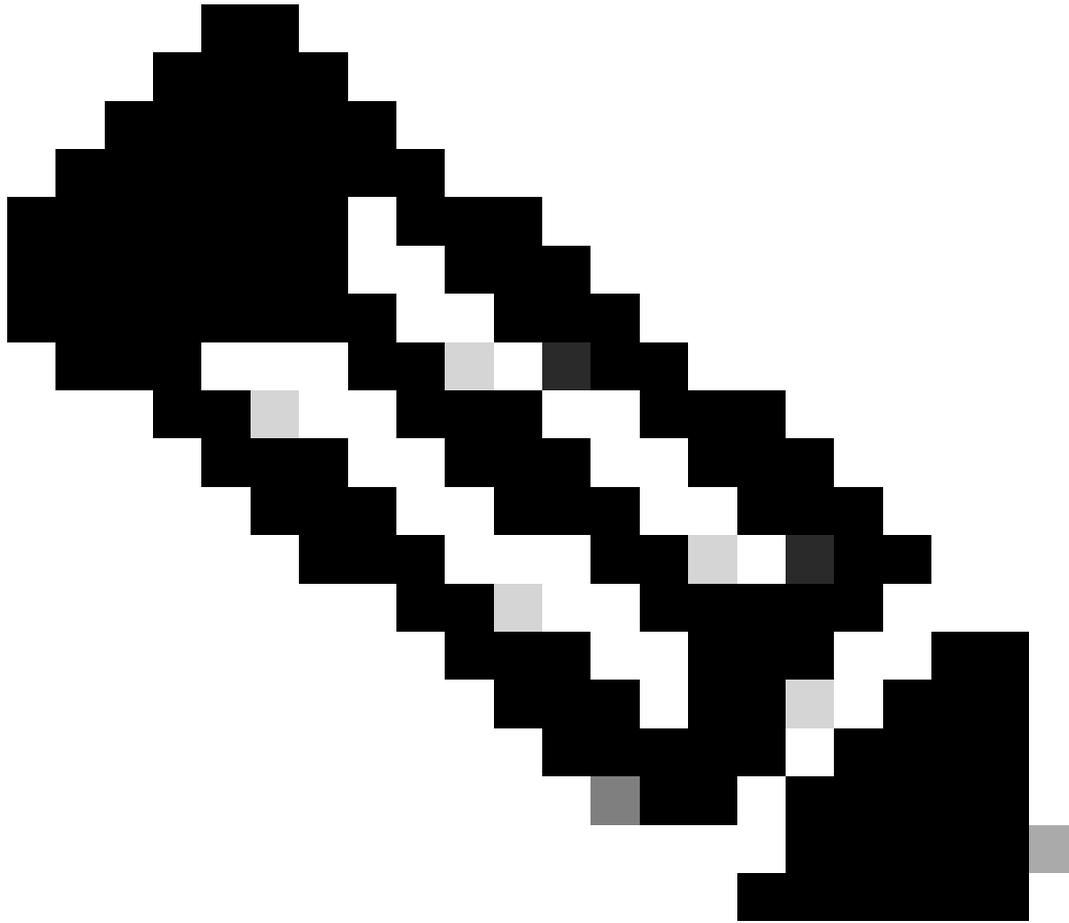
## Authentications By Identity Group

Identity Group	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak Response Time (ms)
RegisteredDevices	7	0	7	0	53.71	171
User Identity Groups:iseUsers_Unknown	4	0	4	0	137.75	197
User Identity Groups:iseUsers_RegisteredDevices	1	0	1	0	310	310
User Identity Groups:iseUsers	1	0	1	0	190	190

Rows/Page 4 | << 1 >> | 4 Total Rows

按身份組進行身份驗證

- 哪個PSN接收更多身份驗證。



注意：在用於本文檔的部署中，只使用了一個PSN；但是，對於較大的部署，此資料對於檢視是否需要負載均衡十分有用。

Server	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak Response Time (ms)
ISE PSN	36	45	81	55.56	123.43	2146

Rows/Page 1 | << 1 >> | 1 Total Rows

按ISE伺服器進行身份驗證

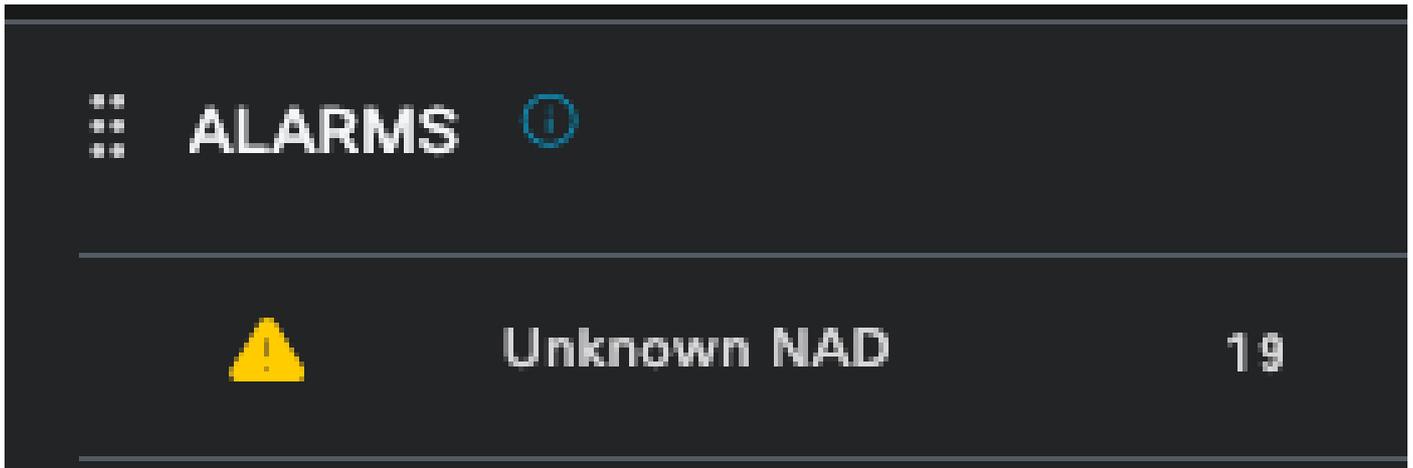
#### 4 - ISE警報

在ISE Dashboard下，Alarms部分顯示部署問題。

以下是幫助進行故障排除的幾個ISE警報。

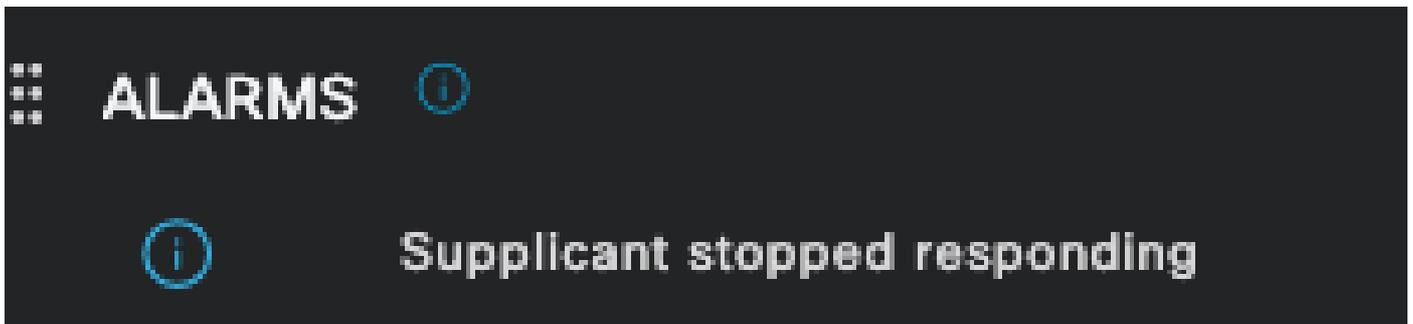
Unknown NAD —當存在網路裝置驗證終端並訪問ISE時，會顯示此警報。但是，ISE不信任它，它會丟棄RADIUS連線。最常見的原因是網路裝置未建立，或者網路裝置使用的IP與ISE註冊的IP不同

o



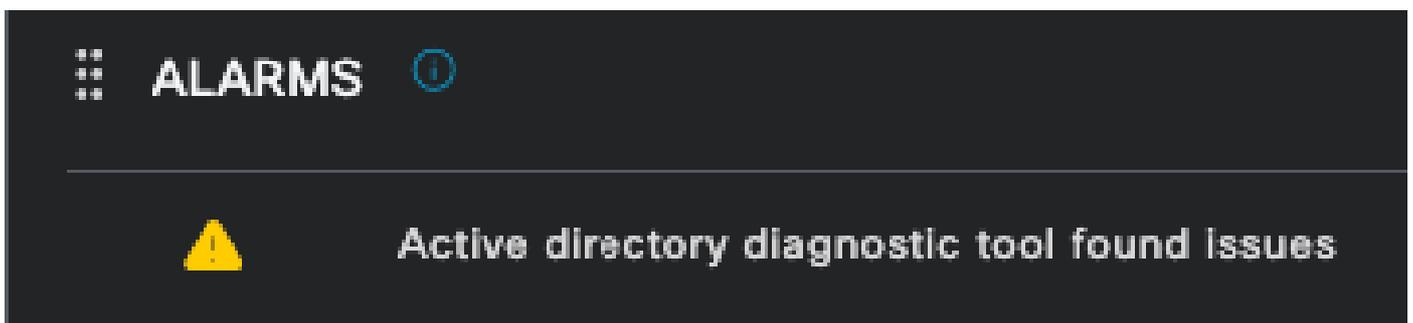
未知的NAD

Supplicant Stop Responding — 當請求方通訊存在問題時，會發生此警報，因為大多數時間請求方配置錯誤，需要在終端端檢查和調查。



請求方停止響應

Active directory診斷工具發現問題— 使用Active Directory驗證使用者身份時，如果通訊進程出現問題，或者連線中斷，您將看到此警報。然後，您會明白為什麼在AD上存在該身份的身份驗證失敗。



AD診斷失敗

COA ( 授權更改 ) 失敗— ISE中的多個流使用CoA，此警報會通知您在與任何網路裝置進行CoA埠通訊期間是否遇到問題。



# COA Failed

Coa失敗

## 5 - ISE調試配置和日誌收集

要繼續身份驗證過程的詳細資訊，必須啟用DEBUG中有關mab和dot1x問題的後續元件：

問題：dot1x/mab

要設定為除錯層級的屬性。

- runtime-AAA (prrt-server.log)
- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

要使元件處於調試級別，首先需要確定哪個PSN接收了失敗的身份驗證或需要進行調查。您可以從即時日誌獲取此資訊。之後，您必須轉到ISE選單>故障排除>調試嚮導>調試日誌配置>選擇PSN >按一下編輯按鈕。

隨即顯示下一個功能表。按一下篩選圖示：

Component Name	Log Level	Description	Log file Name
<input type="radio"/> accessfilter	INFO	RBAC resource access filter	ise-psc.log
<input type="radio"/> Active Directory	WARN	Active Directory client internal messages	ad_agent.log
<input type="radio"/> admin-ca	INFO	CA Service admin messages	ise-psc.log
<input type="radio"/> admin-Infra	INFO	infrastructure action messages	ise-psc.log
<input type="radio"/> admin-license	INFO	License admin messages	ise-psc.log
<input type="radio"/> ai-analytics	INFO	AI Analytics	ai-analytics.log
<input type="radio"/> anc	INFO	Adaptive Network Control (ANC) debug messages	ise-psc.log
<input type="radio"/> api-gateway	INFO	API Gateway native objects logs	api-gateway.log
<input type="radio"/> apiservice	INFO	ISE API Service logs	api-service.log
<input type="radio"/> bootstrap-wizard	INFO	Bootstrap wizard messages	ise-psc.log
<input type="radio"/> ca-service	INFO	CA Service messages	caservice.log

調試日誌配置

在元件名稱列中，搜尋前面列出的屬性。選擇每個日誌級別並將其更改為DEBUG。儲存變更。

# Debug Level Configuration

The screenshot shows the 'Debug Level Configuration' interface. At the top, there are 'Edit' and 'Reset to Default' buttons. Below is a table with columns: Component Name, Log Level, Description, and Log file Name. A search bar at the top left contains 'runtim'. The table lists several components: 'runtime-AAA' (selected with a radio button), 'runtime-config', 'runtime-logging', and 'va-runtime'. A dropdown menu is open for the 'runtime-AAA' component, showing log levels: OFF, FATAL, ERROR, WARN, INFO, **DEBUG** (highlighted), and TRACE. A 'Save' button is visible next to the 'runtime-config' row.

Component Name	Log Level	Description	Log file Name
runtime-AAA	WARN	AAA runtime messages (prrt)	prrt-server.log
runtime-config	OFF	AAA runtime configuration	prrt-server.log
runtime-logging	FATAL	customer logs center messages (prrt)	prrt-server.log
va-runtime	ERROR	Vulnerability Assessment Runtime messages	varuntime.log

運行時AAA元件設定

完成配置每個元件後，使用DEBUG對其進行過濾，以便可以看到是否所有元件都配置正確。

# Debug Level Configuration

The screenshot shows the 'Debug Level Configuration' interface after applying a filter. The search bar at the top left now contains 'debug'. The table lists components with their log levels set to 'DEBUG': 'nsf', 'nsf-session', 'prrt-JNI', and 'runtime-AAA'. The 'Log file Name' column shows 'ise-psc.log' for 'nsf' and 'nsf-session', and 'prrt-management.log' for 'prrt-JNI' and 'prrt-server.log' for 'runtime-AAA'. There are 'Edit' and 'Reset to Default' buttons at the top left, and a 'Quick Filter' dropdown at the top right.

Component Name	Log Level	Description	Log file Name
nsf	DEBUG	NSF related messages	ise-psc.log
nsf-session	DEBUG	Session cache messages	ise-psc.log
prrt-JNI	DEBUG	prrt policy decision request processing layer related ...	prrt-management.log
runtime-AAA	DEBUG	AAA runtime messages (prrt)	prrt-server.log

調試日誌配置

如果需要立即分析日誌，可透過導航到路徑ISE選單>操作>故障排除>下載日誌>裝置節點清單>PSN並啟用DEBUGS > Debug Logs來下載這些日誌。

在這種情況下，您必須在prrt-server.log和ise-psc.log中下載dot1x和mab問題。必須下載的日誌是包含上次測試日期的日誌。

只要按一下此影像中顯示的記錄檔並下載即可（以藍色文字顯示）。

Support Bundle		Debug Logs	
Debug Log Type	Log File	Description	Size
▼ ise-psc (16) (111 MB)			
<input type="checkbox"/>	ise-psc (all logs)	Main ise debug log messages	111 MB
<input type="checkbox"/>	<a href="#">ise-psc.log</a>		5.8 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-03-1</a>		7.0 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-04-1</a>		6.9 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-05-1</a>		6.9 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-06-1</a>		7.0 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-07-1</a>		6.9 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-08-1</a>		6.9 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-09-1</a>		7.6 MB
<input type="checkbox"/>	<a href="#">ise-psc.log.2024-04-10-1</a>		8.0 MB

來自PSN節點的調試日誌

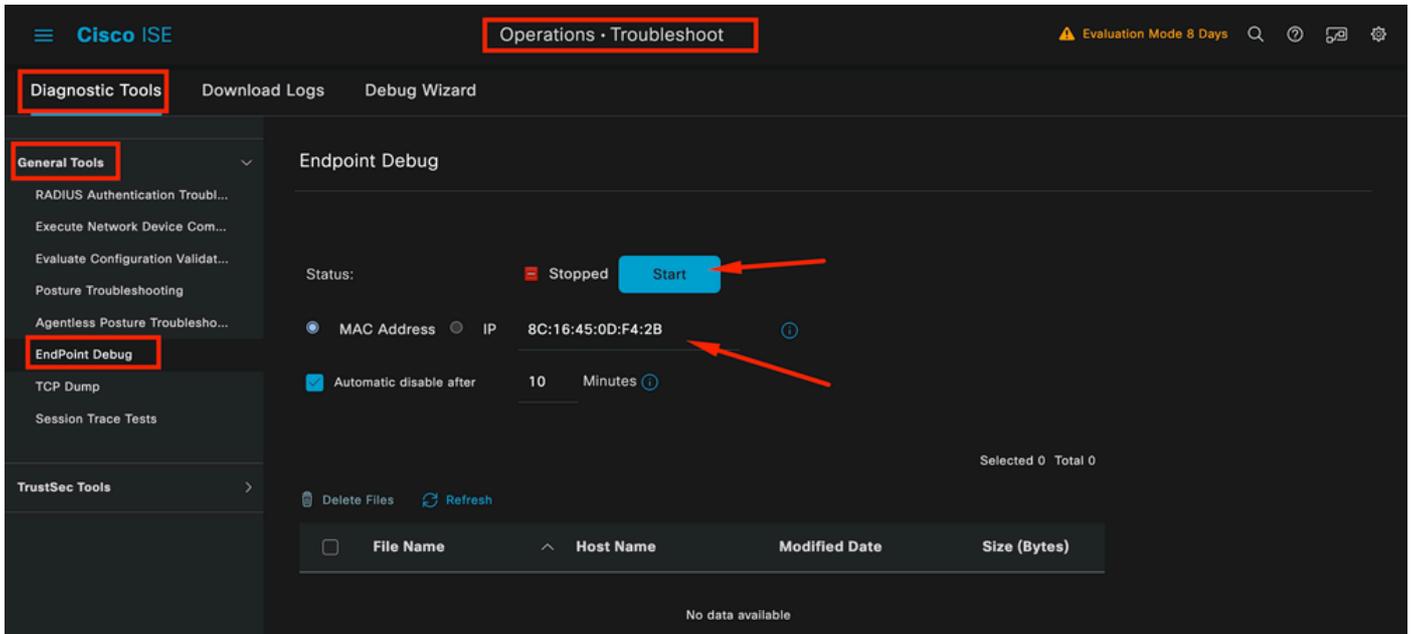
Support Bundle		Debug Logs	
Debug Log Type	Log File	Description	Size
▼ prrt-server (1) (7.8 MB)			
<input type="checkbox"/>	prrt-server (all logs)	Protocol Runtime runtime configuration, debug and customer logs messages	7.8 MB
<input type="checkbox"/>	<a href="#">prrt-server.log</a>		7.8 MB
▶ pxcloud (4) (20 KB)			

除錯日誌段落

## 6 -每個終端的ISE調試

還有另一個選項可用於根據MAC地址或IP為每個終端獲取DEBUG日誌。您可以使用終端調試ISE工具。

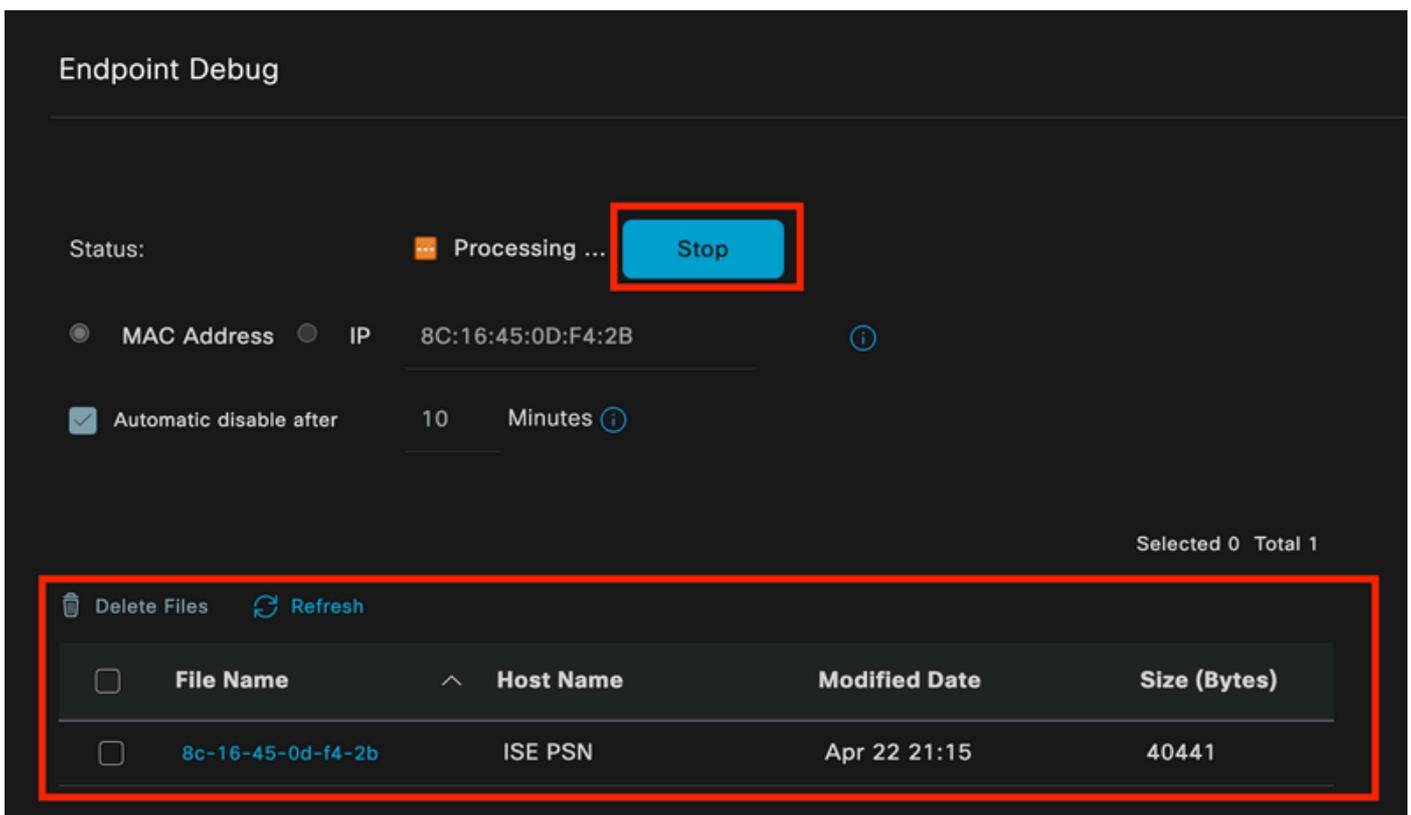
導航到ISE選單>操作>故障排除>診斷工具>常規工具>終端調試。



端點偵錯

然後輸入所需的終端資訊以開始捕獲日誌。按一下Start。

然後，在警告消息中按一下Continue。



端點偵錯

一旦捕獲到資訊，請按一下Stop。

按一下此影像中藍色顯示的檔案名稱。

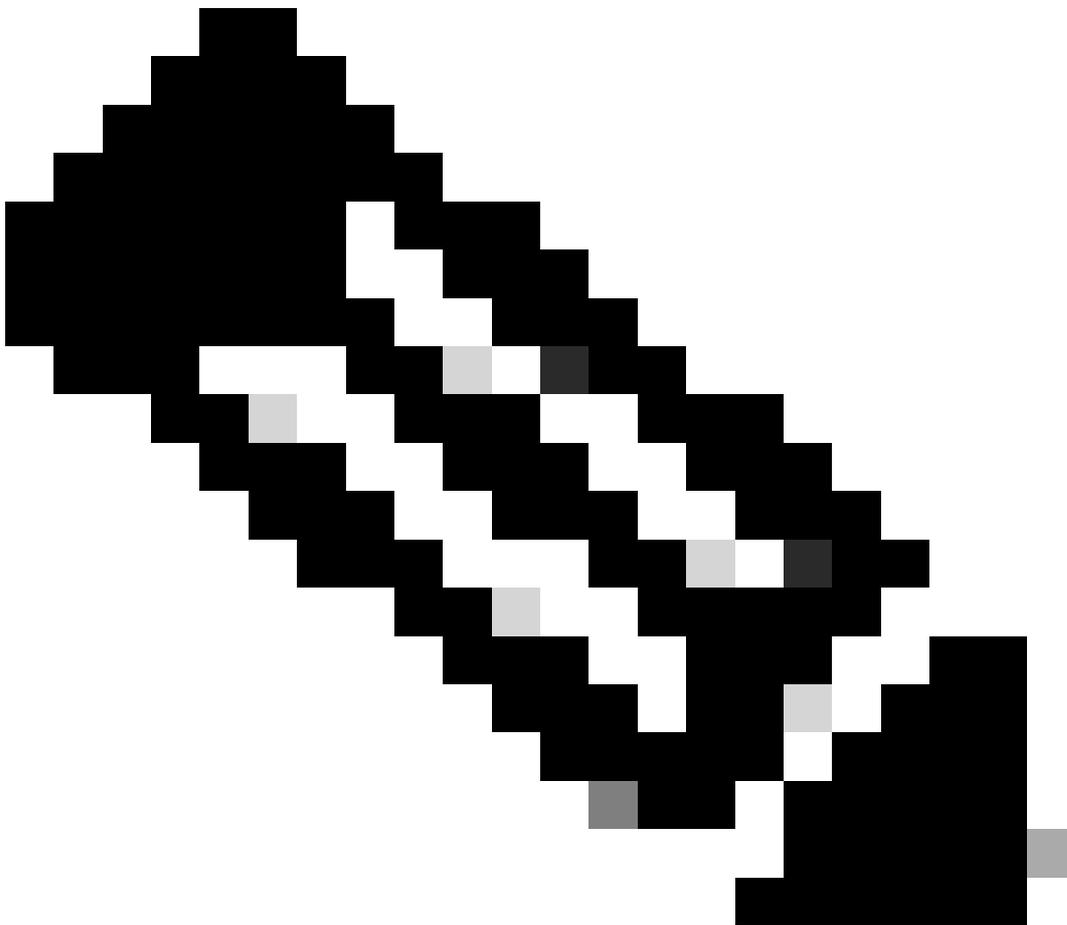
Selected 1 Total 1

Delete Files Refresh

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input checked="" type="checkbox"/>	8c-16-45-0d-f4-2b	ISE PSN	Apr 22 21:17	67959712

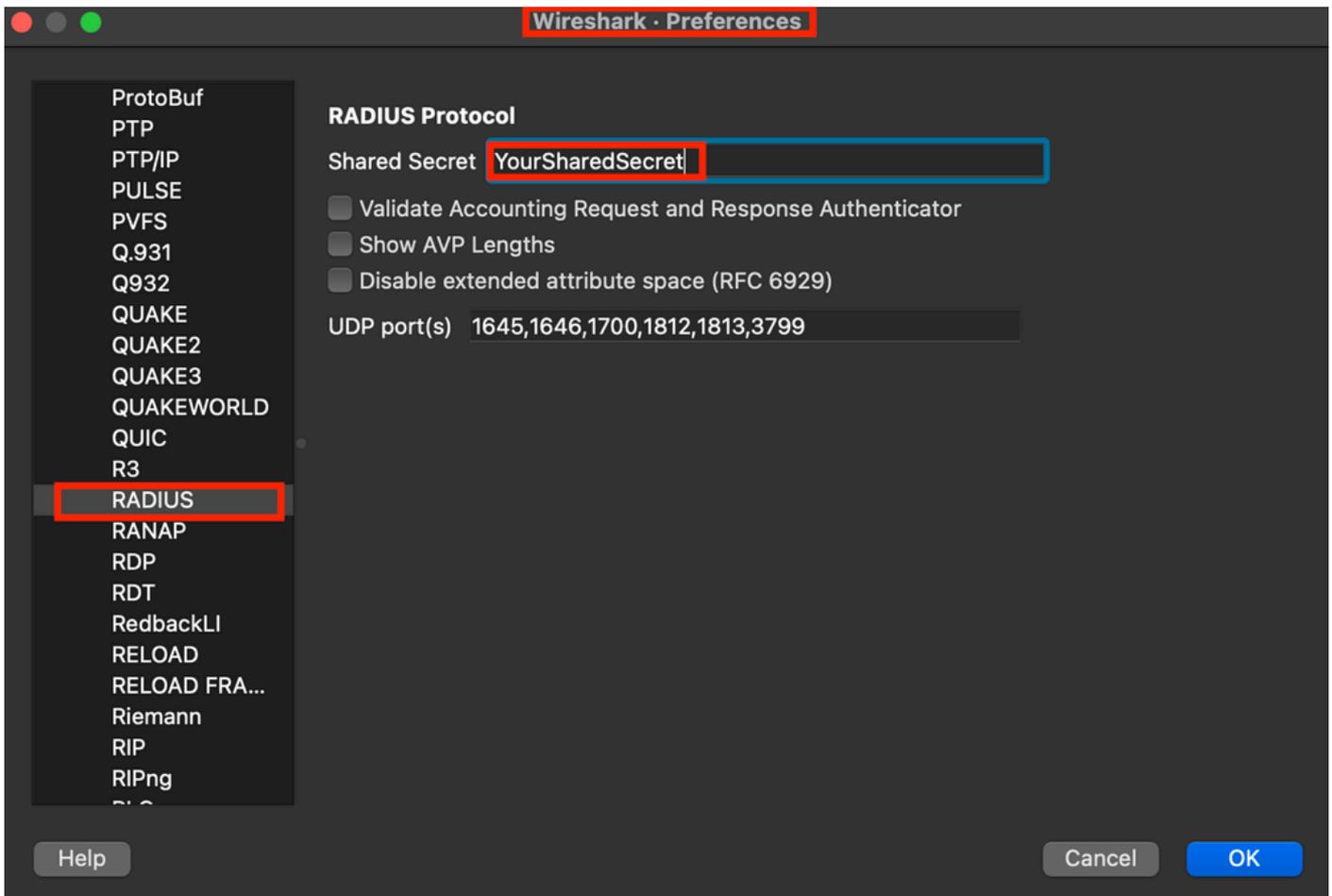
端點偵錯

您必須能夠檢視帶有DEBUG日誌的身份驗證日誌，而無需直接從Debug Log Configuration啟用它們。



注意：由於有些內容可能會在終端調試輸出中省略，因此您將得到一個更完整的日誌檔案，透過調試日誌配置生成該檔案，並從您需要的任何檔案下載所有必需的日誌。如前面的ISE調試配置和日誌收集部分所述。

除了user password欄位以外，RADIUS封包不會加密。但是，您需要驗證傳送的密碼。您可以導航到Wireshark > Preferences > Protocols > RADIUS 並增加ISE和網路裝置使用的RADIUS共用金鑰來檢視使用者傳送的資料包。之後，RADIUS資料包會解密顯示。



Wireshark半徑選項

## 8 -網路裝置故障排除命令

下一個命令有助於排除ISR 1100或有線NAD裝置上的故障。

8 – 1使用show aaa servers檢視AAA伺服器或ISE是否可從網路裝置訪問和訪問。

```
Router>show aaa servers
```

```
RADIUS: id 1, priority 1, host 10.88.240.80, auth-port 1645, acct-port 1646, hostname  
State: current UP, duration 2876s, previous duration 0s  
Dead: total time 0s, count 0
```

```
Platform State from SMD: current UP, duration 2876s, previous duration 0s  
SMD Platform Dead: total time 0s, count 0
```

```
Platform State from WNCN (1) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCN (2) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCN (3) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCN (4) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCN (5) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCN (6) : current UP, duration 3015s, previous duration 0s  
Platform State from WNCN (7) : current UP, duration 3015s, previous duration 0s
```

Platform State from WNCN (8) : current UP, duration 3015s, previous duration 0s

WNCN Platform Dead: total time 0s, count 0UP

Quarantined: No

Authn: request 11, timeouts 0, failover 0, retransmission 0

Response: accept 1, reject 0, challenge 10

Response: unexpected 0, server error 0, incorrect 0, time 33ms

Transaction: success 11, failure 0

Throttled: transaction 0, timeout 0, failure 0

Malformed responses: 0

Bad authenticators: 0

Dot1x transactions:

Response: total responses: 11, avg response time: 33ms

Transaction: timeouts 0, failover 0

Transaction: total 1, success 1, failure 0

MAC auth transactions:

Response: total responses: 0, avg response time: 0ms

Transaction: timeouts 0, failover 0

Transaction: total 0, success 0, failure 0

Author: request 0, timeouts 0, failover 0, retransmission 0

Response: accept 0, reject 0, challenge 0

Response: unexpected 0, server error 0, incorrect 0, time 0ms

Transaction: success 0, failure 0

Throttled: transaction 0, timeout 0, failure 0

Malformed responses: 0

Bad authenticators: 0

MAC author transactions:

Response: total responses: 0, avg response time: 0ms

Transaction: timeouts 0, failover 0

Transaction: total 0, success 0, failure 0

Account: request 6, timeouts 4, failover 0, retransmission 3

Request: start 1, interim 0, stop 0

Response: start 1, interim 0, stop 0

Response: unexpected 0, server error 0, incorrect 0, time 27ms

Transaction: success 2, failure 1

Throttled: transaction 0, timeout 0, failure 0

Malformed responses: 0

Bad authenticators: 0

Elapsed time since counters last cleared: 47m

Estimated Outstanding Access Transactions: 0

Estimated Outstanding Accounting Transactions: 0

Estimated Throttled Access Transactions: 0

Estimated Throttled Accounting Transactions: 0

Maximum Throttled Transactions: access 0, accounting 0

Consecutive Response Failures: total 0

SMD Platform : max 0, current 0 total 0

WNCN Platform: max 0, current 0 total 0

IOSD Platform : max 0, current 0 total 0

Consecutive Timeouts: total 3

SMD Platform : max 0, current 0 total 0

WNCN Platform: max 0, current 0 total 0

IOSD Platform : max 3, current 0 total 3

Requests per minute past 24 hours:  
high - 0 hours, 47 minutes ago: 4  
low - 0 hours, 45 minutes ago: 0  
average: 0

Router>

8-2要檢視埠狀態、詳細資訊、應用於會話的ACL、身份驗證方法以及更有幫助的資訊，請使用 show authentication sessions interface <筆記型電腦所連線的介面>詳細資訊。

```
Router#show authentication sessions interface gigabitEthernet 0/1/0 details
Interface: GigabitEthernet0/1/0
IIF-ID: 0x01D9BEFB
MAC Address: 8c16.450d.f42b
IPv6 Address: Unknown
IPv4 Address: Unknown
User-Name: iseiscool
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: N/A
Common Session ID: 22781F0A0000000C0777AECD
Acct Session ID: 0x00000003
Handle: 0x0a000002
Current Policy: POLICY_Gi0/1/0
```

```
Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Security Policy: Should Secure
```

```
Server Policies:
```

```
Method status list:
Method State
dot1x Authc Success
```

Router#

8-3要驗證全局配置中是否有aaa的所有必需命令，請運行show running-config aaa。

```
Router#sh run aaa
!
aaa authentication dot1x default group ISE-CLUSTER
aaa authorization network default group ISE-CLUSTER
aaa accounting system default start-stop group ISE-CLUSTER
aaa accounting dot1x default start-stop group ISE-CLUSTER
!
aaa server radius dynamic-author
client <A.B.C.D> server-key Cisc0123
```

```
!  
!  
radius server COHVSRAISE01-NEW  
address ipv4 <A.B.C.D> auth-port 1645 acct-port 1646  
timeout 15  
key Cisc0123  
!  
!  
aaa group server radius ISE-CLUSTER  
server name COHVSRAISE01-NEW  
!  
!  
!  
!  
aaa new-model  
aaa session-id common  
!  
!  
  
Router#
```

8-4另一個有用命令是test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy。

```
Router#test aaa group radius server <A.B.C.D> iseiscool VainillaISE97 legacy  
User was successfully authenticated.
```

```
Router#
```

## 9 -網路裝置相關調試

- debug dot1x all - 顯示所有dot1x EAP消息
- debug aaa authentication -顯示來自AAA應用程式的身份驗證調試資訊
- debug aaa authorization -顯示AAA授權的調試資訊
- debug radius authentication - 提供關於僅用於身份驗證的協定級活動的詳細資訊
- debug radius -提供關於協定級活動的詳細資訊

## 相關資訊

- [思科技術支援與下載](#)

## 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）。