

# 使用ISE和TACACS+配置裝置管理的APIC

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[驗證程式](#)

[APIC配置](#)

[ISE組態](#)

[驗證](#)

[疑難排解](#)

---

## 簡介

本文檔介紹將APIC與ISE整合以便管理員使用者通過TACACS+協定進行身份驗證的過程。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 應用程式原則基礎架構控制器(APIC)
- 身分識別服務引擎 (ISE)
- TACACS通訊協定

### 採用元件

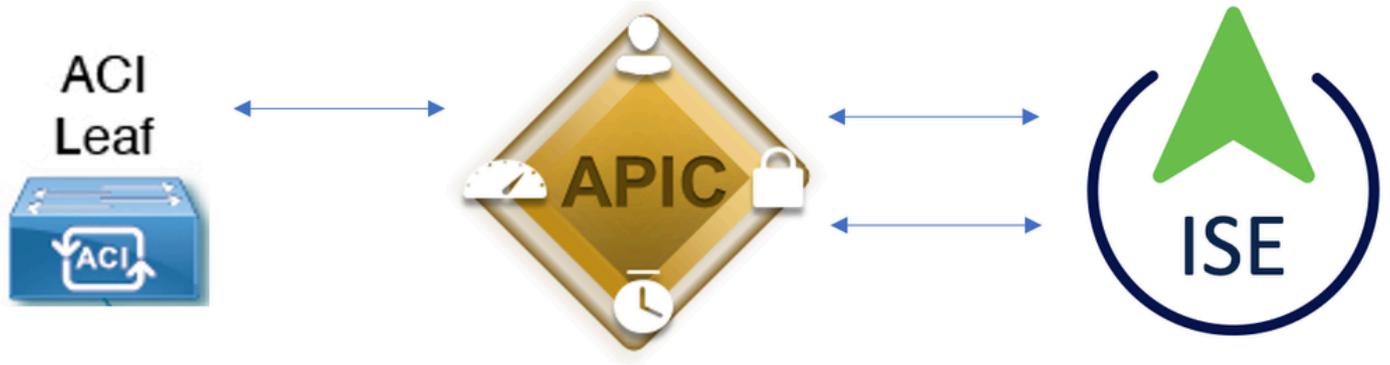
本文中的資訊係根據以下軟體和硬體版本：

- APIC 4.2(7u)版
- ISE版本3.2補丁1

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



整合圖表

## 驗證程式

步驟1. 使用管理員使用者憑據登入APIC應用程式。

步驟2. 身份驗證過程觸發和ISE在本地或通過Active Directory驗證憑證。

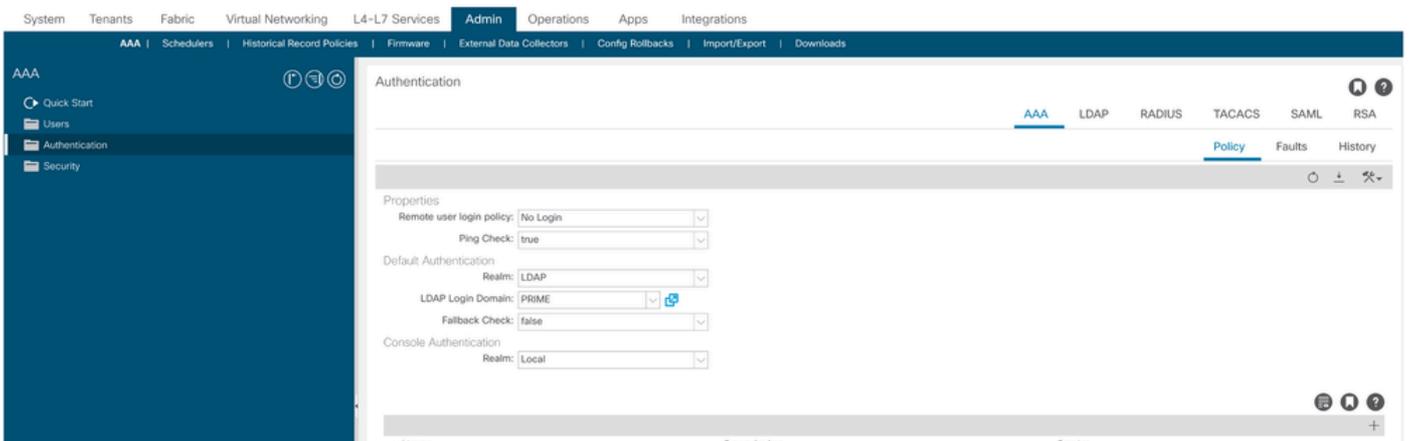
步驟3. 身份驗證成功後，ISE傳送允許資料包以授權對APIC的訪問。

步驟4. ISE顯示成功的身份驗證即時日誌。

 附註：APIC將TACACS+配置複製到屬於交換矩陣的枝葉交換機。

## APIC配置

步驟1. 導覽至Admin > AAA > Authentication > AAA，然後選擇+ icon，以便建立新的登入網域。



APIC登入管理員配置

步驟2. 定義新登入域的名稱和領域，然後按一下+「提供程式」下的以便建立新提供程式。

## Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
------	----------	-------------

Cancel

Submit

APIC登入管理員

Providers:

Name	Priority	Description
<input type="text" value="select an option"/> <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>

APIC TACACS提供程式

步驟3. 定義ISE IP地址或主機名，定義共用金鑰，並選擇管理端點策略組(EPG)。按一下Submit將TACACS+提供程式新增到登入管理員。

## Create TACACS+ Provider



Host Name (or IP Address):

Description:

Port:

Authorization Protocol:  CHAP  MS-CHAP  PAP

Key:

Confirm Key:

Timeout (sec):

Retries:

Management EPG:

Server Monitoring:  Disabled  Enabled

APIC TACACS提供程式設定

## Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
52.13.89	1	

Host Name	Description	Port	Timeout (sec)	Retries
52.13.89		49	5	1

TACACS提供程式檢視

## ISE 組態

步驟1. 導覽至 **三** > 網路資源 > 網路裝置群組。在 All Device Types 下建立網路裝置組。

### **三** Cisco ISE

Network Devices **Network Device Groups** Network Device Profiles External

## Network Device Groups

All Groups

Choose group **▼**

**↻** **Add** Duplicate Edit **🗑️** Trash **👁️** Show group members **↓** Import **↑** Export **▼** **☰**

<input type="checkbox"/> Name	Description
<input type="checkbox"/> <b>▼</b> All Device Types	All Device Types
<input type="checkbox"/> APIC	

ISE網路裝置組

步驟2. 導覽至 Administration > Network Resources > Network Devices。選擇 Add 「定義APIC名稱和IP地址」，在「裝置型別」和「TACACS+」覈取方塊下選擇「APIC」，並定義APIC TACACS+提供程式配置中使用的密碼。按一下 Submit。

Network Devices   Network Device Groups   Network Device Profiles   External RADIUS Servers   RADIUS Server

Network Devices

Default Device

Device Security Settings

[Network Devices List](#) > APIC-LAB

### Network Devices

Name

Description

IP Address  \* IP :

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location   [Set To Default](#)

IPSEC   [Set To Default](#)

Device Type   [Set To Default](#)

RADIUS Authentication Settings

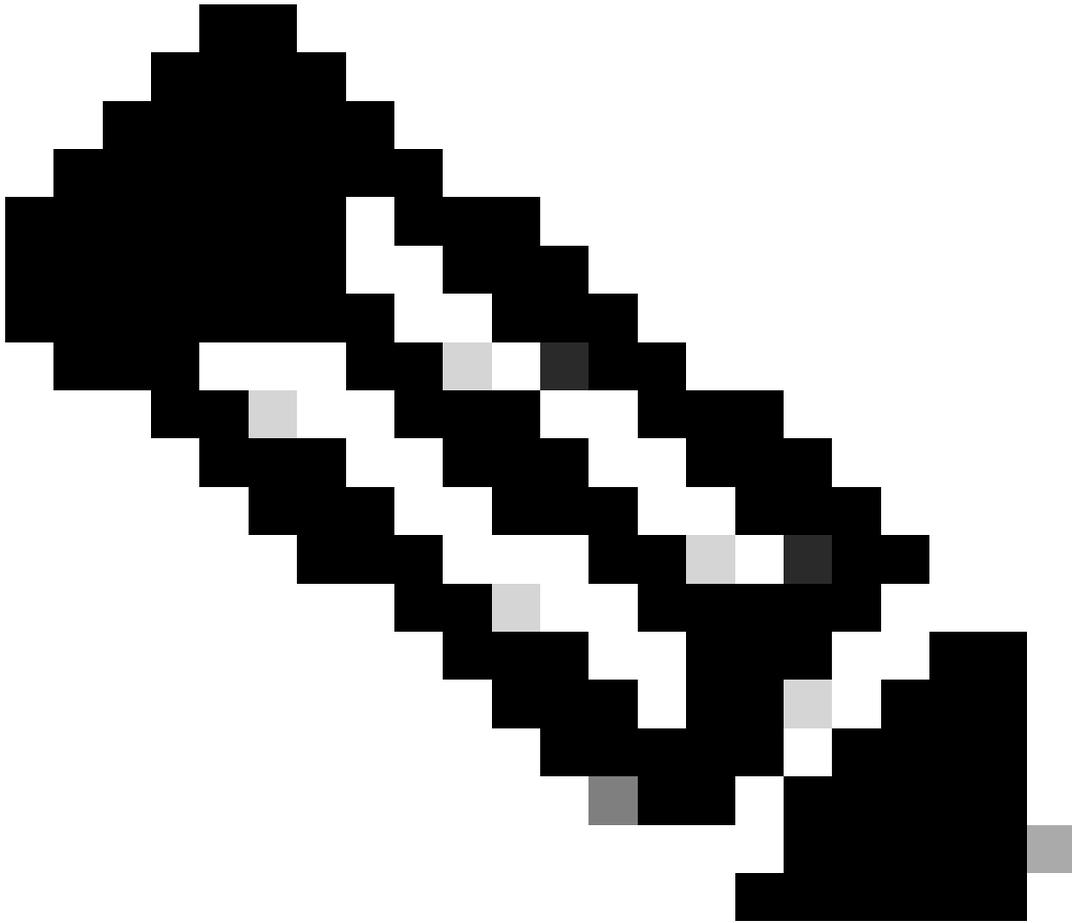
TACACS Authentication Settings

Shared Secret  [Show](#) [Retire](#)

對枝葉交換機重複步驟1和步驟2。

步驟3.使用此連結上的說明將ISE與Active Directory整合；

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html>。



附註：本文檔將內部使用者和AD管理員組都作為身份源，但是，將使用內部使用者的身份源執行測試。AD組的結果相同。

---

步驟4. (可選) 導覽至 **☰** >Administration > Identity Management > Groups。選擇 User Identity Groups 並按一下 Add。為只讀管理員用戶和管理員用戶建立一個組組。

Identity Groups

EQ

< [List Icon] [Settings Icon]

- > Endpoint Identity Groups
- > **User Identity Groups**

# User Identity Groups

Edit Add Delete Import Export

	Name	Description
<input type="checkbox"/>	ALL_ACCOUNTS (default)	Default ALL_
<input type="checkbox"/>	APIC_RO	
<input type="checkbox"/>	APIC_RW	

身份組

步驟5. (可選) 導覽至☰ > Administration > Identity Management > Identity. Click Add並建立一個使Read Only Admin用者和Admin使用者。將每個使用者分配到步驟4中建立的每個組。

Users

Latest Manual Network Scan Res...

# Network Access Users

Edit Add Change Status Import Export Delete Duplicate

	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups
<input type="checkbox"/>	Enabled	APIC_ROUser					APIC_RO
<input type="checkbox"/>	Enabled	APIC_RWUser					APIC_RW

步驟6.導覽至☰ >Administration > Identity Management > Identity Source Sequence。從清單中選擇Add，定義名稱，AD Join Points然後選擇Internal Users和Identity Source。在Treat as if the user was not found and proceed to the next store in the sequence下選擇Advanced Search List Settings，然後按一下Save。

∨ Identity Source Sequence

\* Name

Description

∨ Certificate Based Authentication

Select Certificate Authentication Profile

∨ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
Internal Endpoints		iselab
Guest Users		Internal Users
All_AD_Join_Points		

Navigation buttons: > < >> << (between columns) and ^ > < > (within Selected column)

∨ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

身份源序列

☰ 7. 導航至 > Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. 選擇Add , 定義名稱

，並取消選中Allow CHAP和Allow MS-CHAPv1 from Authentication protocol清單。選擇Save。

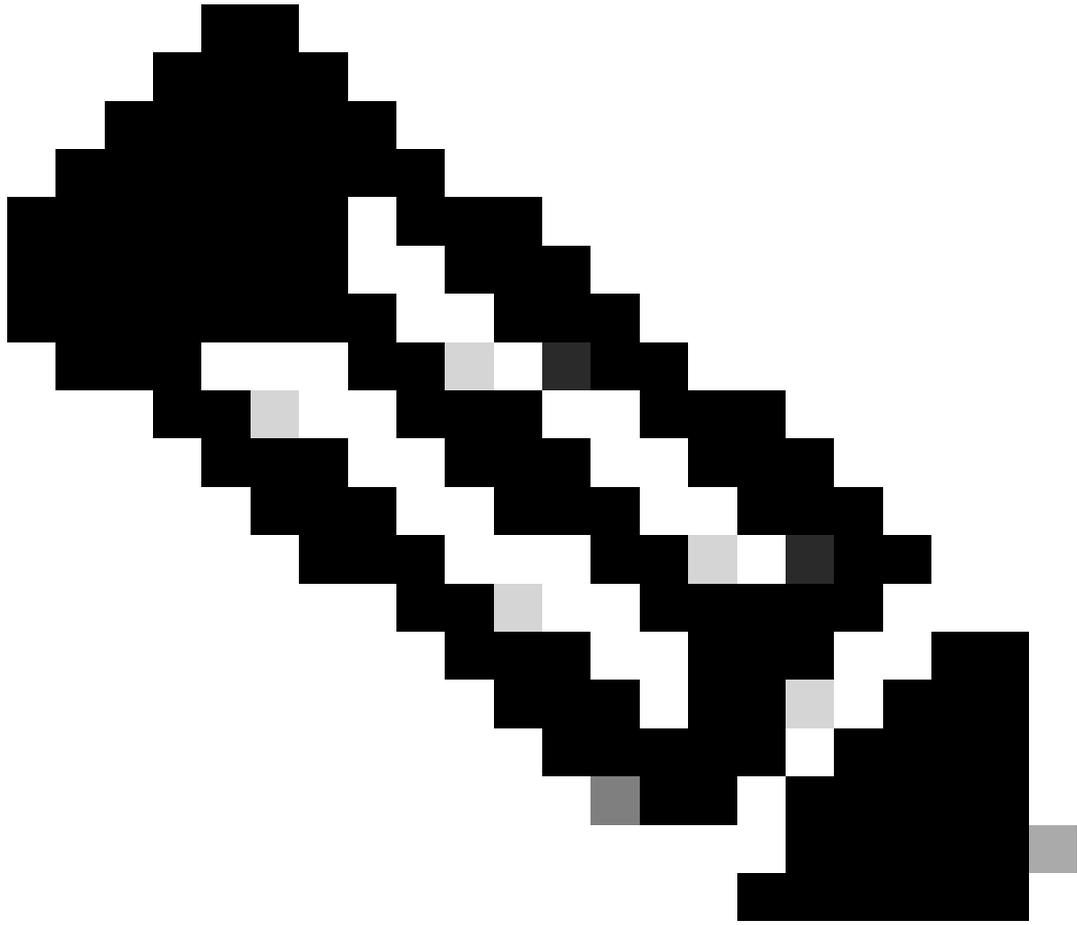
## ☰ Cisco ISE

The screenshot shows the Cisco ISE configuration interface. At the top, there are navigation tabs: Overview, Identities, User Identity Groups, Ext Id Sources, and Network Resources. On the left, a sidebar menu is visible with options: Conditions, Network Conditions, Results, Allowed Protocols, TACACS Command Sets, and TACACS Profiles. The main content area is titled 'Allowed Protocols Services List > TACACS Protocol'. Below this, the 'Allowed Protocols' section is expanded, showing the 'Name' as 'TACACS Protocol' and a 'Description' field. Underneath, the 'Allowed Protocols' section is further expanded to show 'Authentication Protocols'. A note states: 'Only Authentication Protocols relevant to TACACS are displayed.' There are three checkboxes: 'Allow PAP/ASCII' (checked), 'Allow CHAP' (unchecked), and 'Allow MS-CHAPv1' (unchecked).

TACACS允許通訊協定

8. 導覽至☰ > Work Centers > Device Administration > Policy Elements > Results > TACACS Profile。按一下add並根據下方的清單上的屬性建立兩個配置檔案Raw View。按一下Save。

- 管理員使用者： cisco-av-pair=shell:domains=all/admin/
- 只讀管理員使用者： cisco-av-pair=shell:domains=all/read-all



附註：如果出現空格或其他字元，授權階段將失敗。

---

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Administration

TACACS Profiles > APIC ReadWrite Profile

### TACACS Profile

Name  
APIC ReadWrite Profile

Description

Task Attribute View **Raw View**

Profile Attributes

cisco-av-pair=shell:domains=all/admin/

Cancel Save

TACACS設定檔

Overview Identities User Identity Groups Ext Id Sources Network Resources

## TACACS Profiles

Refresh Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	APIC ReadOnly Profile	Shell	
<input type="checkbox"/>	APIC ReadWrite Profile	Shell	

TACACS管理員和只讀管理員配置檔案

步驟9. 導覽至 **Work Centers > Device Administration > Device Admin Policy Set**。建立新策略集，定義名稱，並選擇在步驟1中建立的裝置類APIC型。選擇在步驟7中建立TACACS Protocol的。作為允許的協定，然後單擊Save。

Policy Sets Reset [Reset Polycyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">●</span>	APIC		DEVICE-Device Type EQUALS All Device Types#APIC	TACACS Protocol	55		

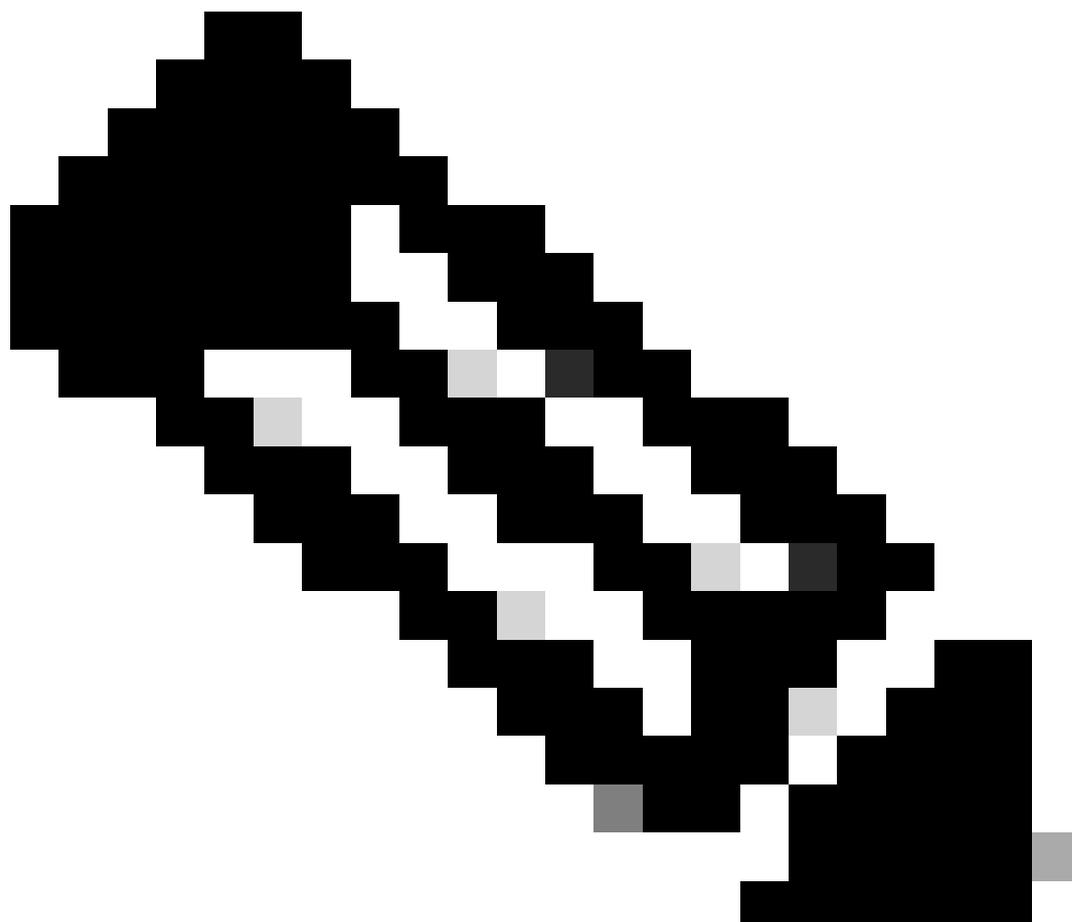
### TACACS策略集

步驟10.在new下Policy Set，按一下右箭頭>，建立身份驗證策略。定義名稱並選擇裝置IP地址作為條件。然後選擇在步驟6中建立的身份源序列。

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
<span style="color: green;">●</span>	APIC Authentication Policy	Network Access-Device IP Address EQUALS 188.21	APIC_ISS	55	

### 身份驗證策略



附註：位置或其他屬性可用作身份驗證條件。

步驟11.為每個管理員使用者型別建立授權配置檔案，定義名稱，並選擇內部使用者和/或AD使用者組作為條件。可以使用其他條件，如APIC。在每個授權策略上選擇適當的外殼配置檔案，然後按一下Save。

Authorization Policy (3)

Status	Rule Name	Conditions	Results	Command Sets	Shell Profiles	Hits	Actions
●	APIC Admin RO	AND Network Access Device IP Address EQUALS 10.10.10.188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RO	APIC ReadOnly Profile			34	⚙️
●	APIC Admin User	AND Network Access Device IP Address EQUALS 10.10.10.188.21 OR IdentityGroup-Name EQUALS User Identity Groups:APIC_RW Iselab-ExternalGroups EQUALS ciscoise.lab/Bullfin/Administrators	APIC ReadWrite Profile			18	⚙️
●	Default		Deny All Shell Profile	DenyAllCommands		0	⚙️

TACACS授權配置檔案

## 驗證

步驟1.使用使用者管理員憑據登入APIC UI。從清單中選擇TACACS選項。

APIC  
Version 4.2(7u)  
CISCO

User ID  
APIC\_ROUser

Password  
.....

Domain  
S\_TACACS

Login

APIC登入

步驟2.檢驗APIC UI上的訪問情況，並驗證TACACS Live日誌上應用了正確的策略。

# Welcome to APIC

What's new in version 4.2(7u)



## New Features

- Floating L3out
  - Docker EE (Kubernetes) container integration
  - L4-L7 Services support in vPod
  - Backup PBR destination
  - Support for 64 Remote Leaf pairs
- UI Enhancements:
    - User-defined UI banner
    - First Time Setup wizard
    - Simplified L3Out creation
    - EPG to leafs deployment view

[View Release Notes](#)

### Getting Started

[What's New in v4.2\(7u\)](#)

[Online Videos \(YouTube™\)](#)

[View All Tutorial Videos](#)

### Explore

[Configuration Guides](#)

[Knowledge Base Articles](#)

[APIC Communities](#)

### Support

[Online Help](#)

[Troubleshooting](#)

[Documentation](#)

Do not show on login

[Review First Time Setup](#)

[Get Started](#)

APIC歡迎資訊

對只讀管理員使用者重複步驟1和2。

☰ Cisco ISE

Operations · TACACS

Live Logs

🔄 Export To

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...
Apr 20, 2023 10:14:42.4...	✓	🔒	APIC_ROUser	Authorizat...		APIC >> APIC Admin RO	PAN32	APIC-LAB
Apr 20, 2023 10:14:42.2...	✓	🔒	APIC_ROUser	Authentic...	APIC >> APIC Authentication Po...		PAN32	APIC-LAB

Last Updated: Fri Apr 21 2023 00:14:53 GMT+0200 (Central European Summer Time)

TACACS+即時日誌

## 疑難排解

步驟1。導覽至☰ >Operations > Troubleshoot > Debug Wizard。選擇TACACS並按一下 Debug Nodes。

# Debug Profile Configuration

Debug Wizard contains predefined debug templates with the help of which you can troubleshoot issues on ISI

 [Add](#)  [Edit](#)  [Remove](#)  [Debug Nodes](#)

<input type="checkbox"/>	Name	Description	Status
<input type="checkbox"/>	802.1X/MAB	802.1X/MAB	DISABLED
<input type="checkbox"/>	Active Directory	Active Directory	DISABLED
<input type="checkbox"/>	Application Server Issues	Application Server Issues	DISABLED
<input type="checkbox"/>	BYOD portal/Onboarding	BYOD portal/Onboarding	DISABLED
<input type="checkbox"/>	Context Visibility	Context Visibility	DISABLED
<input type="checkbox"/>	Guest portal	Guest portal	DISABLED
<input type="checkbox"/>	Licensing	Licensing	DISABLED
<input type="checkbox"/>	MnT	MnT	DISABLED
<input type="checkbox"/>	Posture	Posture	DISABLED
<input type="checkbox"/>	Profiling	Profiling	DISABLED
<input type="checkbox"/>	Replication	Replication	DISABLED
<input checked="" type="checkbox"/>	TACACS	TACACS	DISABLED

調試配置檔案配置

步驟2.選擇接收流量的節點，然後按一下Save。

Diagnostic Tools   Download Logs   **Debug Wizard**

Debug Profile Configuration

Debug Log Configuration

Debug Profile Configuration > Debug Nodes

## Debug Nodes

Selected profile **TACACS**

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

 Filter  

<input type="checkbox"/>	Host Name	Persona	Role
<input checked="" type="checkbox"/>	PAN32.ciscoise.lab	Administration, Monitoring, Policy Service	PRI(A), PRI(M)
<input type="checkbox"/>	SPAN32.ciscoise.lab	Administration, Monitoring, Policy Service, ...	SEC(A), SEC(M)

[Cancel](#)   [Save](#)

調試節點選擇

步驟3.執行新測試並下載下的日誌，Operations > Troubleshoot > Download logs 如下所示：

AcsLogs, 2023-04-20 22:17:16, 866, DEBUG, 0x7f93cab7700, cntx=0004699242, sesn=PAN32/469596415/70, CPMSession

如果調試不顯示身份驗證和授權資訊，請驗證以下情況：

1. 在ISE節點上啟用裝置管理服務。
2. 已將正確的ISE IP地址新增到APIC配置。
3. 如果中間有防火牆，請驗證是否允許埠49(TACACS)。

## 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）。