

使用ISE配置Catalyst Center外部身份驗證TACACS

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[思科身分識別服務引擎\(ISE\)](#)

[許可並啟用TACACS+服務](#)

[建立管理員使用者並新增網路裝置](#)

[設定TACACS+設定檔](#)

[配置TACACS+策略](#)

[Cisco Catalyst Center](#)

[配置ISE/AAA伺服器](#)

[啟用和配置外部身份驗證。](#)

[驗證](#)

[疑難排解](#)

[1.屬性配置錯誤](#)

[2.共用金鑰不匹配](#)

簡介

本檔案介紹將思科身分識別服務引擎與Catalyst Center整合以啟用TACACS+驗證所需的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 對Cisco ISE和Cisco Catalyst Center的管理員訪問許可權。
- 對AAA(驗證、授權和記帳)概念有基本瞭解。
- 有關TACACS+通訊協定的使用知識。
- Catalyst Center和ISE服務器之間的網絡連線。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- Cisco Catalyst中心版本2.3.7.x
- Cisco Identity Services Engine(ISE)版本3.x(或更高版本)
- 適用於外部使用者驗證的TACACS+通訊協定

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

此整合允許外部使用者登入到Catalyst Center進行管理訪問和管理。

設定

思科身分識別服務引擎(ISE)

許可並啟用TACACS+服務

開始使用ISE中的TACACS+配置之前，必須確認已安裝正確的許可證並啟用該功能。

1. 驗證您在[思科智慧軟體管理](#)或[思科許可證中心](#)門戶中擁有PID許可證L-ISE-TACACS-ND=。

在ISE許可門戶中啟用裝置管理。

- Device Admin許可證(PID:L-ISE-TACACS-ND=)在策略服務節點(PSN)上啟用TACACS+服務。
- 導覽至：
管理>系統>許可
- 選中Tier options下的Device Admin覈取方塊。

Tier ☒ Essential ☒ Advantage ☒ Premier ☒ Device Admin

Virtual Appliance ☒ ISE VM License

This enables the ISE features for the purchased licenses to be tracked by Cisco Smart Licensing.

By clicking Register you will agree to the Terms&Conditions. You can download Terms&Conditions on [Smart Licensing Resources](#).

[Reset](#)

[Update](#)

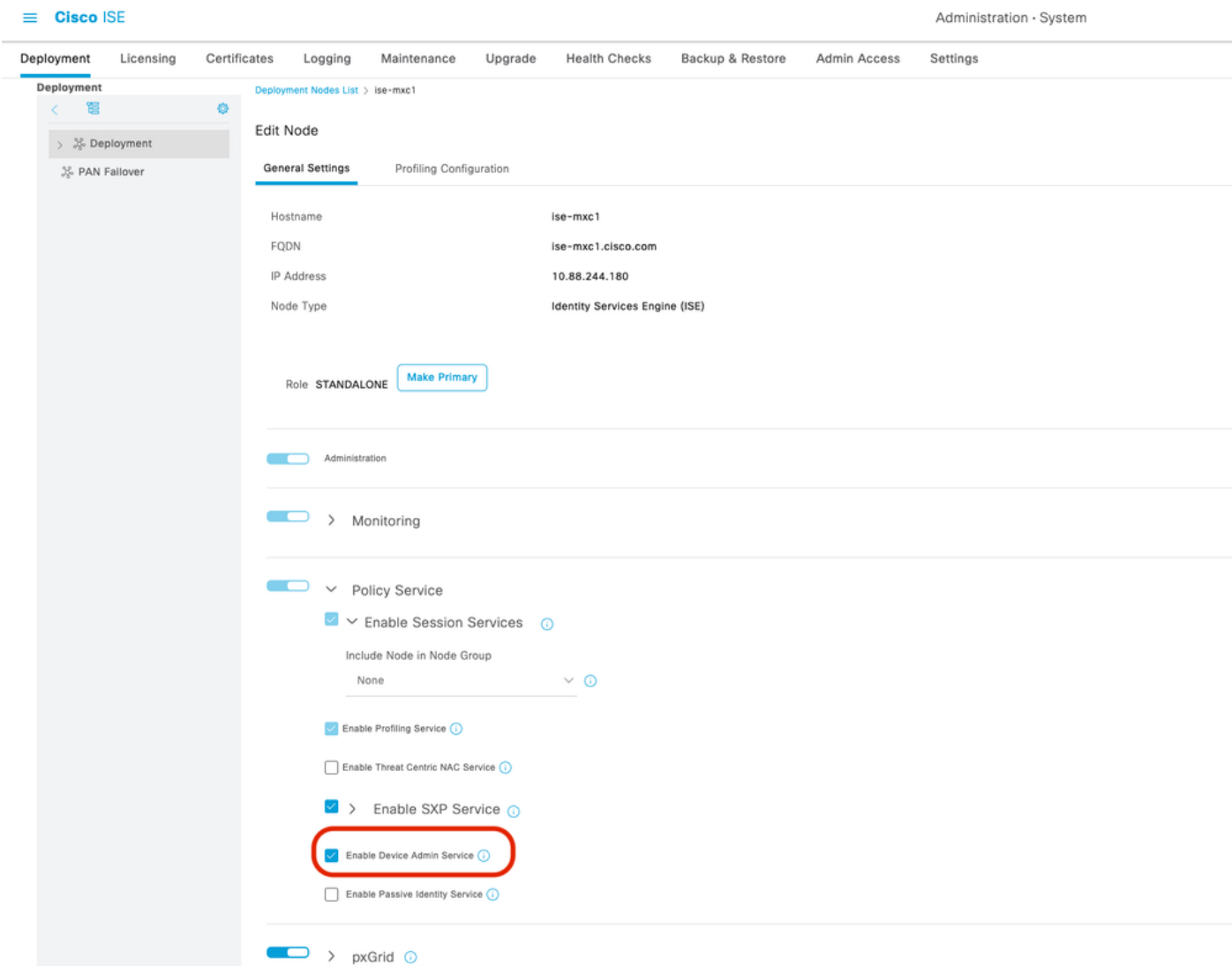
☐	Premier	Enabled	Released Entitlement	0	-	Dec 27,2024 18:16:00 PM
☐	Device Admin	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM
Virtual Appliance						
	ISE VM License	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM

許可證裝置管理員

3.在運行TACACS+服務的ISE節點上啟用Device Admin Service。

- 導覽至：

管理>系統>部署>選擇節點
- 選中Enable Device Admin Service選項。



啟用裝置管理服務

建立管理員使用者並新增網路裝置

1.建立管理員使用者。

- 此使用者帳戶用於通過ISE身份驗證登錄Catalyst Center UI。

- 導覽至：

工作中心(Work Centers)>網路訪問(Network Access)>身份(Identities)>網路訪問使用者(Network Access User)

- 新增新使用者(例如catc-user)。
- 如果該使用者已存在，請繼續執行下一步。

2.建立網絡裝置。

- 導覽至：

工作中心(Work Centers)>網路訪問(Network Access)>身份(Identities)>網路資源(Network Resource)

- 新增Catalyst Center的IP地址，或定義Catalyst Center IP所在的子網。
- 如果裝置已經存在，請驗證它是否包含引數：
 - TACACS身份驗證設置已啟用。
 - Shared Secret已配置且已知（請儲存此值，因為稍後在Catalyst Center中需要儲存此值）。

Network Devices List > Catalyst-Center_6

Network Devices

Name Catalyst-Center_6

Description

IP Address 10.88.244.160 / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations [Set To Default](#)

IPSEC No [Set To Default](#)

Device Type All Device Types [Set To Default](#)

DNAC DNAC Devices [Set To Default](#)

☐ RADIUS Authentication Settings

☒ TACACS Authentication Settings

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

☐ Enable Single Connect Mode

☒ Legacy Cisco Device

☐ TACACS Draft Compliance Single Connect Support

設定TACACS+設定檔

1.建立新的TACACS+配置檔案。

- 導覽至：

工作中心(Work Centers)>裝置管理(Device Administration)>策略元素(Policy Elements)>結果(Results)> TACACS配置檔案(TACACS Profiles)

- 新增配置檔名稱。
 - Type:必填
 - 名稱:cisco-av-pair
 - 值：Role=SUPER-ADMIN-ROLE
- 儲存配置檔案。

Cisco ISE

Work Centers - Device Administration

OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork ResourcesPolicy ElementsDevice Admin Policy SetsReportsSettings

Conditions>Network Conditions>Results▼Allowed ProtocolsTACACS Command SetsTACACS Profiles

TACACS Profiles > CatC_TACACS_Profile

TACACS Profile

NameCatC_TACACS_Profile

DescriptionCatalyst Center External Authentication

Task Attribute ViewRaw View

Common Tasks

Common Task TypeShell▼

☐ Default Privilege (Select 0 to 15)

☐ Maximum Privilege (Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape (Select true or false)

☐ Timeout Minutes (0-9999)

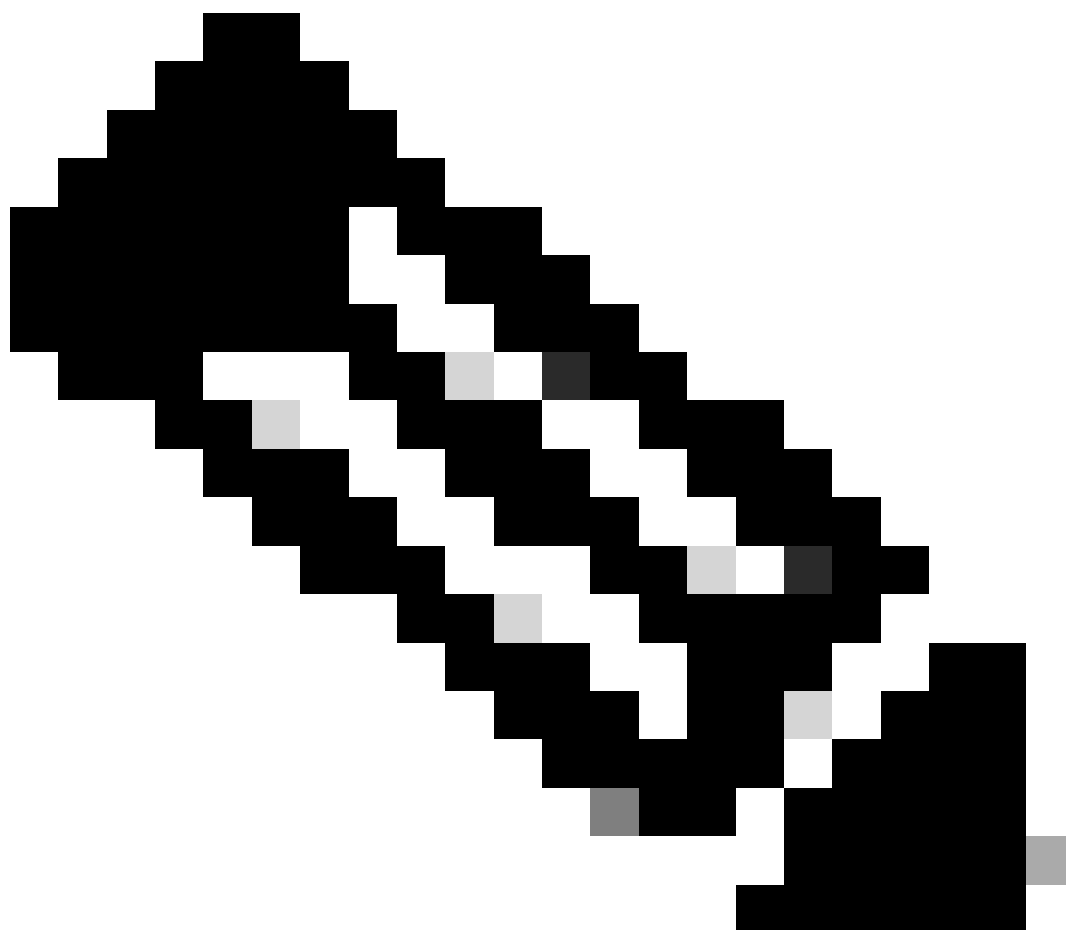
☐ Idle Time Minutes (0-9999)

Custom Attributes

AddTrash▼Edit

Type	Name	Value
☐ MANDATORY	cisco-av-pair	Role=SUPER-ADMIN-ROLE

CancelSave



附註：Cisco Catalyst Center支援用於訪問控制的外部身份驗證、授權和記帳(AAA)伺服器。如果您使用外部伺服器對外部使用者進行身份驗證和授權，則可以在Cisco Catalyst Center中啟用外部身份驗證。預設AAA屬性設定與預設使用者配置檔案屬性匹配。

TACACS協定的預設AAA屬性值為cisco-av-pair。

RADIUS通訊協定預設AAA屬性值為Cisco-AVPair。

只有當AAA伺服器在使用者配置檔案中具有自定義屬性時，才需要更改。在AAA伺服器上，AAA屬性值的格式為Role=role1。在思科身分識別服務引擎(Cisco ISE)伺服器上，在設定RADIUS或TACACS設定檔時，使用者可以選擇或輸入cisco av配對作為AAA屬性。

例如，您可以手動選擇並配置AAA屬性為cisco-av-pair=Role=SUPER-ADMIN-ROLE或Cisco-AVPair=Role=SUPER-ADMIN-ROLE。

- 導覽至：

工作中心(Work Centers)>裝置管理(Device Administration)>策略元素(Policy Elements)>結果(Results)> TACACS命令集(TACACS Command Sets)

- 新增名稱。
- 選中Permit any command that not listed below選項。
- 儲存命令集。

The screenshot shows the Cisco ISE interface for configuring TACACS Command Sets. The breadcrumb trail is: Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets. The left sidebar shows the navigation menu with 'TACACS Command Sets' selected. The main content area shows the configuration for a specific command set named 'PermitAllCommands'. The 'Name' field is filled with 'PermitAllCommands'. The 'Description' field is empty. Under the 'Commands' section, the checkbox 'Permit any command that is not listed below' is checked. Below this, there is a table with columns 'Grant', 'Command', and 'Arguments'. The table is currently empty, with a message 'No data found.' at the bottom. At the bottom right of the configuration area, there are 'Cancel' and 'Save' buttons.

TACACS命令集

配置TACACS+策略

1.建立新的TACACS+策略集。

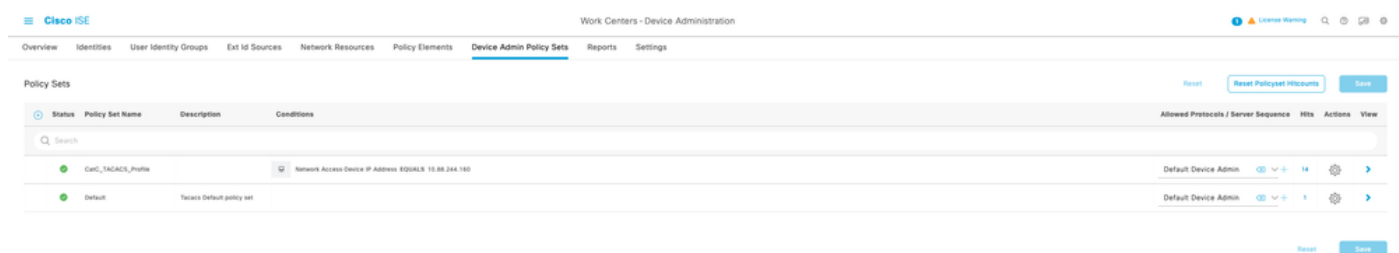
- 導覽至：

工作中心>裝置管理>裝置管理策略設定

- 為策略集新增名稱。
- 配置Condition。
 - 在本範例中，條件與Catalyst Center IP位址相符。

The screenshot shows the 'Conditions Studio' interface. On the left is the 'Library' pane with a search bar and a list of conditions. The main area is the 'Editor'. It shows a condition configuration for 'Network Access Device IP Address'. The condition is set to 'Equals' with the value '10.88.244.160'. Below the condition, there is a 'Set to 'is not'' link. At the bottom of the editor, there is a dashed box containing the text 'NEW AND OR'.

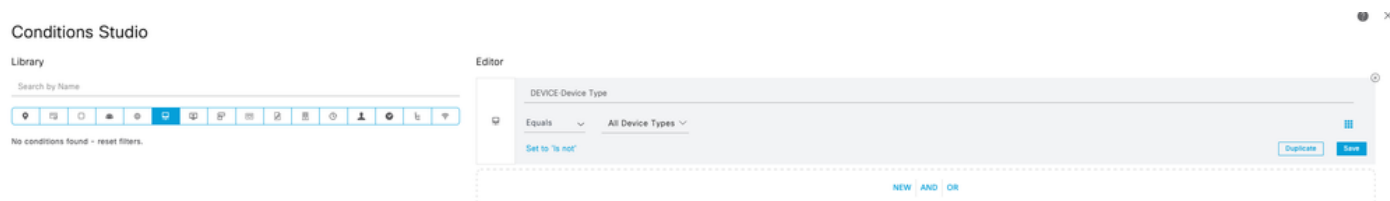
1.3在Allowed Protocols / Server Sequence上選擇Default Device Admin。



選擇Default Device Admin

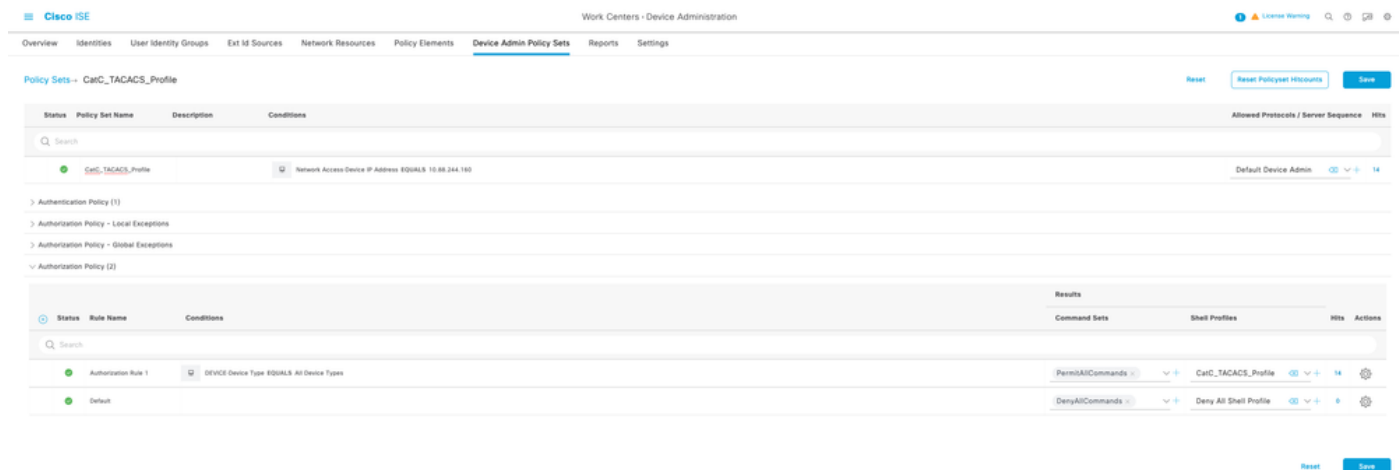
2.配置策略集。

- 按一下右側的箭頭(>)展開並配置策略集。
- 在Authorization Policy下新增新規則。
- 按如下方式配置新規則：
 - 名稱:輸入描述性規則名稱。
 - 條件：在本示例中，條件與All Device Types匹配。



所有裝置型別

- 命令集：選擇先前建立的TACACS+命令集。
- 外殼配置檔案：選擇之前建立的TACACS+配置檔案。



TACACS+命令集

Cisco Catalyst Center

配置ISE/AAA伺服器

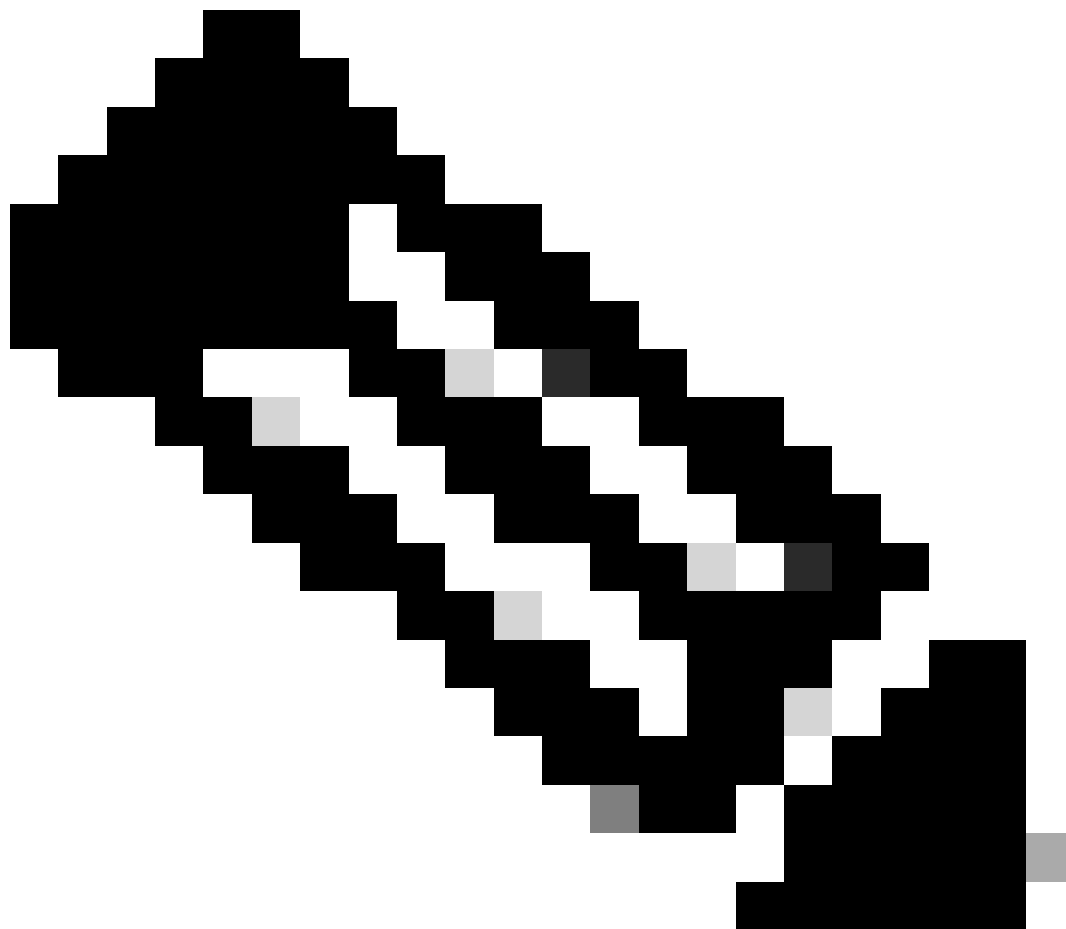
1.登入到Catalyst Center Web介面。

- 導覽至：

主選單>System >設定>外部服務>身份驗證和策略伺服器

2.新增新伺服器。您可以選擇ISE或AAA。

- 在本演示中，使用AAA服務器選項。



附註：Catalyst Center群集只能配置一個ISE群集。

3.配置這些選項，然後儲存：

- 輸入AAA伺服器的IP地址。
- 新增Shared Secret (思科ISE網路資源中配置的相同金鑰)。
- 將Advanced Settings切換到On。
- 檢查TACACS選項。

Add AAA server

Server IP Address*

10.88.244.180

Shared Secret*

.....

[SHOW](#)



Advanced Settings

Protocol



RADIUS



TACACS



Enable KeyWrap

Authentication Port*

1812

Accounting Port*

1813

Port

49

Retries*

3

Timeout (seconds)*

4

身份驗證和策略伺服器

Catalyst Center

External SerX

External Services

Umbrella

Authentication and Policy Servers

Integrity Verification

SD-Access Compatibility Matrix

IP Address Manager

Cloud Access Login

Cisco AI Analytics

Stealthwatch

Edge AI Recommendation

System / Settings

☆ 🔍 🔄 🏠 🔔 🔍 Eduardo

Settings / External Services

Authentication and Policy Servers

Use this form to specify the servers that authenticate Catalyst Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

AddExport

IP Address	Protocol	Type	Status	Actions
192.168.31.228	RADIUS	ISE	INACTIVE	⋮
10.88.244.180	RADIUS_TACACS	AAA	ACTIVE	⋮

As of Sep 11, 2025 5:52 PM🔄

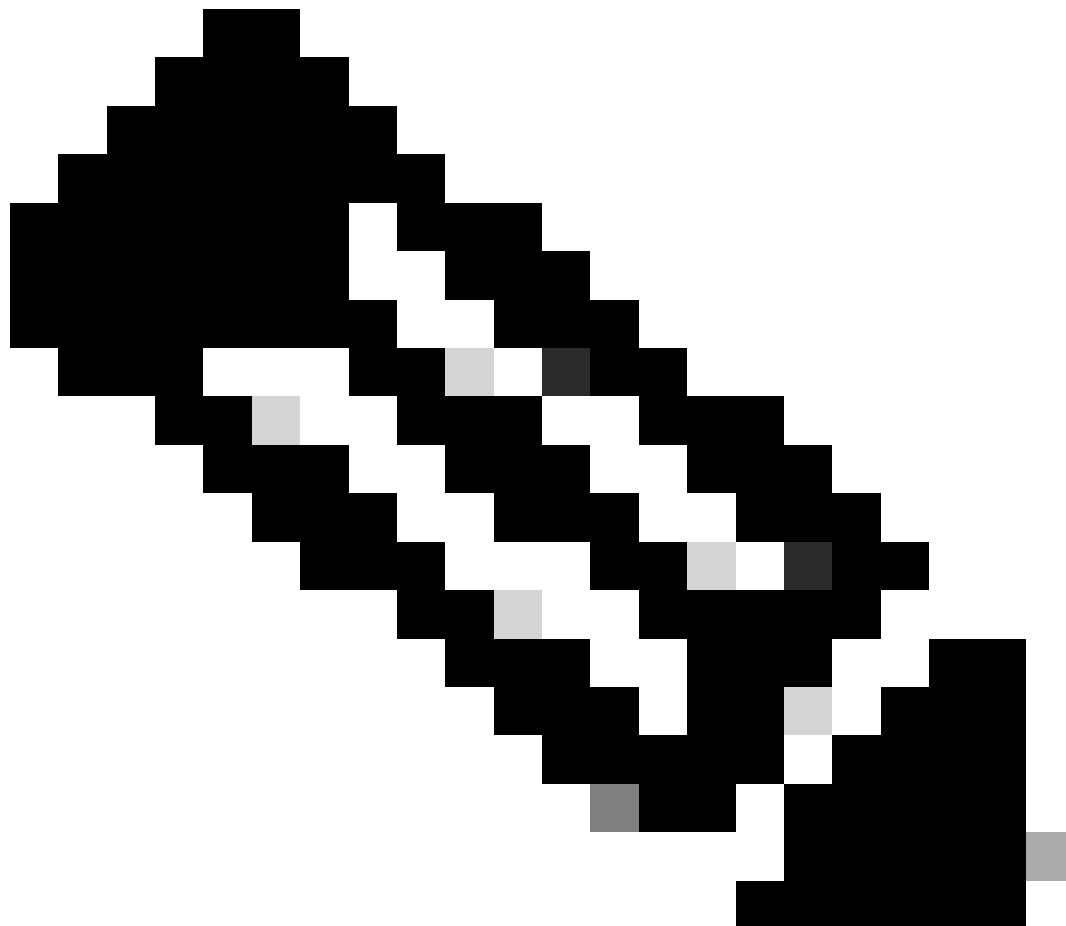
高級設定

啟用和配置外部身份驗證。

1.定位至「外部驗證」頁：

主選單>系統>使用者和角色>外部身份驗證

2.新增AAA屬性cisco-av-pair，然後按一下Update儲存更改。



附註：此步驟不是強制性的，因為TACACS+的預設屬性已經是cisco-av-pair，但此步驟被認為是明確設定此步驟的最佳實踐。

3.在主AAA伺服器下，選擇之前配置的AAA伺服器。

- 按一下View Advanced Settings以顯示其他選項。
- 選擇TACACS+選項。
- 輸入在Cisco ISE的網路資源中配置的Shared Secret。

- 按一下Update儲存更改。

4.啟用「外部使用者」復選框。

- 此操作會自動儲存配置。

External Authentication

Cisco Catalyst Center supports external Authentication, Authorization and Accounting (AAA) servers for access control. If you are using an external server for authentication and authorization of external users, you should enable external authentication in Cisco Catalyst Center. The default AAA attribute setting matches the default user profile attribute.

TACACS protocol default AAA attribute value is "cisco-av-pair".
RADIUS protocol default AAA attribute value is "Cisco-AVPair".

Change is only required if your AAA server has a custom attribute in the user profile.
On the AAA server, the format of the AAA attribute value is "Role=role1". On the Cisco Identity Services Engine (Cisco ISE) server, while configuring RADIUS or TACACS profile, the user may select or input "cisco-av-pair" as AAA attribute.
For example, you might manually select & configure the AAA attribute as "cisco-av-pair=role=SUPER-ADMIN-ROLE" or "Cisco-AVPair=role=SUPER-ADMIN-ROLE".

☒ **Enable External User**

AAA Attribute

AAA Attribute
cisco-av-pair

[Reset to Default](#) [Update](#)

AAA Server(s)

Primary AAA Server	Secondary AAA Server
IP Address 10.88.244.180	IP Address 10.88.244.180
Shared Secret Shared Secret	Shared Secret Shared Secret
Info	Info

Hide Advanced Settings **View Advanced Settings**

☐ RADIUS ☒ TACACS [Update](#)

Port
49

Retries
3

Timeout (seconds)
4

[Update](#)

Success
Successfully saved external authentication settings.

外部驗證

驗證

1. 開啟新的瀏覽器作業階段或使用Incognito Mode並登入Catalyst Center網頁，使用思科ISE中設定的使用者帳戶。
2. 在Catalyst Center中，確認登入成功。



登入使用ISE配置Catalyst Center外部身份驗證TACACS

3. 從Cisco ISE驗證日誌：

操作> TACACS >即時日誌

- 驗證狀態：通過
- 授權狀態：通過

Cisco ISE

Operations - TACACS

License Warning

🔍

🔗

⚙️

Live Logs

🔗 Import to

Refresh: Never

Show: Latest 20 records

Filter: Last 3 hours

Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Isa Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
X			Identity		Authentication Policy	Authorization Policy	Isa Node	Network Device Host	Network Device	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Command	Shell Profile
Sep 12, 2025 12:12:20.801...	🟢	🔗	cisco-user	Authorization	CatC_TACACS_Profile >> Auth...	CatC_TACACS_Profile >> Authori...	isa-mac1	Catalyst-Center_8	10.88.244.160	Device Type6800 S...	LocationRAI Locat...	console		10.189.17.203		CatC_TACACS_Pt...
Sep 12, 2025 12:12:20.798...	🟢	🔗	cisco-user	Authentication	CatC_TACACS_Profile >> Default		isa-mac1	Catalyst-Center_8	10.88.244.160	Device Type6800 S...	LocationRAI Locat...	console		10.189.17.203		

Last Updated: Thu Sep 11 2025 18:16:58 GMT-0800 (Central Standard Time)

Records Shown: 2

即時日誌

4. 在Authorization Details中，與下一個輸出進行比較：
- 消息文本： Device-Administration:會話授權成功
 - 所有響應屬性： cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes	
All Response Attributes	cisco-av-pair=Role=SUPER-ADMIN-ROLE

cisco-av-pair=Role=SUPER-ADMIN-ROLE

疑難排解

以下是整合期間可能會遇到的一些常見問題，以及如何識別這些問題：

1. 屬性配置錯誤

Catalyst Center中的症狀：登入憑據無效



Cisco Catalyst Center

The bridge to possible

 Invalid Login Credentials

Username

catc-user

Password

[SHOW](#)

Log In

屬性配置錯誤

- 思科ISE中的症狀（TACACS日誌）：

- 驗證:通過
- Authorization:通過

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:26.861...			catc-user	Authorization	CatC_TACACS_Profile	CatC_TACACS_Profile >> Authoriz...	Ise-mst1	Catalyst-Center_8	10.88.244.160	Device TypeAAA S...	LocationAAA Locat...	console		10.188.17.203		CatC_TACACS_Pt...
Sep 12, 2025 12:12:26.788...			catc-user	Authentication	CatC_TACACS_Profile	CatC_TACACS_Profile >> Default	Ise-mst1	Catalyst-Center_8	10.88.244.160	Device TypeAAA D...	LocationAAA Locat...	console		10.188.17.203		

屬性配置錯誤

- 可能原因:
 - 屬性值中存在空格。

範例：

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes

All Response Attributes cisco-av-pair=Role=SUPER-ADMIN-ROLE

屬性配置錯誤

- 屬性配置錯誤，缺少Role=關鍵字。

範例：

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes

All Response Attributes cisco-av-pair=Role=SUPER-ADMIN-ROLE

屬性配置錯誤

2. 共用金鑰不匹配

- 症狀：Catalyst Center和Cisco ISE之間的身份驗證資料包失敗。

- 可能起因:在ISE的網路資源中配置的共用密碼與Catalyst Center > External Authentication頁面中配置的共用金鑰不匹配。

如何驗證：

- 檢查ISE中的網路資源配置。
- 比較共用金鑰與Catalyst Center > External Authentication下的配置。

範例：

Authentication Details

Generated Time 2025-09-11 18:22:24.078000 +00:00

Logged Time 2025-09-11 18:22:24.078

Epoch Time (sec) 1757614944

ISE Node ise-mxc1

Message Text Failed-Attempt: Authentication failed

Failure Reason 13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets

Resolution

Root Cause

Username

Network Device Name Catalyst-Center_6

Network Device IP 10.88.244.160

Network Device Groups IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types

Device Type Device Type#All Device Types

Location Location#All Locations

Device Port

Remote Address

共用金鑰不匹配

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）。