CSM TACACS與ISE整合

目錄

簡介

本檔案介紹將思科安全管理員(CSM)與身份服務引擎(ISE)相整合的過程，用於管理員使用者使用TACACS+協定進行身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- 思科安全管理員(CSM)。
- 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：

- CSM伺服器版本4.22
- ISE版本3.0

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。

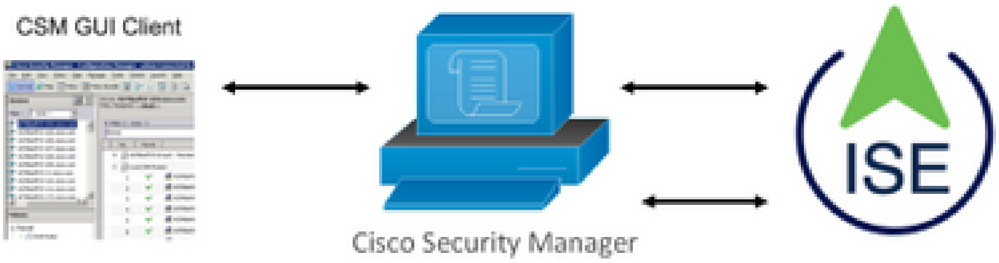
背景資訊

預設情況下，思科安全管理器(CSM)使用稱為Ciscoworks的身份驗證模式在本地對使用者進行身份

驗證和授權，以便採用集中身份驗證方法，您可通過TACACS協定使用思科身份服務引擎。

設定

網路圖表



驗證程式

步驟1.使用管理員使用者的憑據登入CSM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。

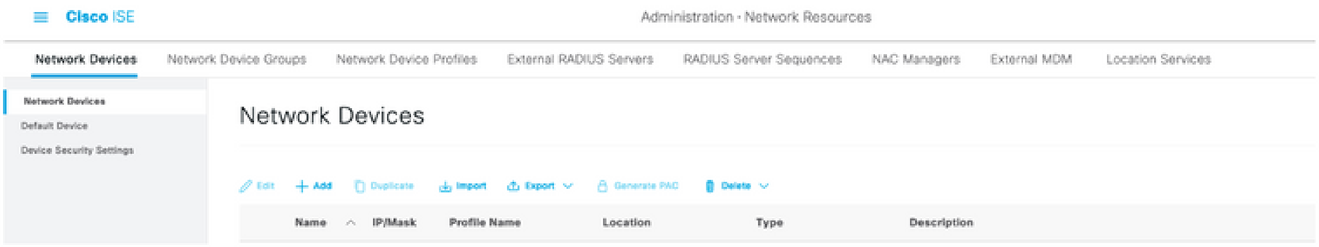
步驟3.身份驗證成功後，ISE傳送允許資料包以授權對CSM的訪問。

步驟4. CSM將使用者名稱與本地使用者角色分配進行對映。

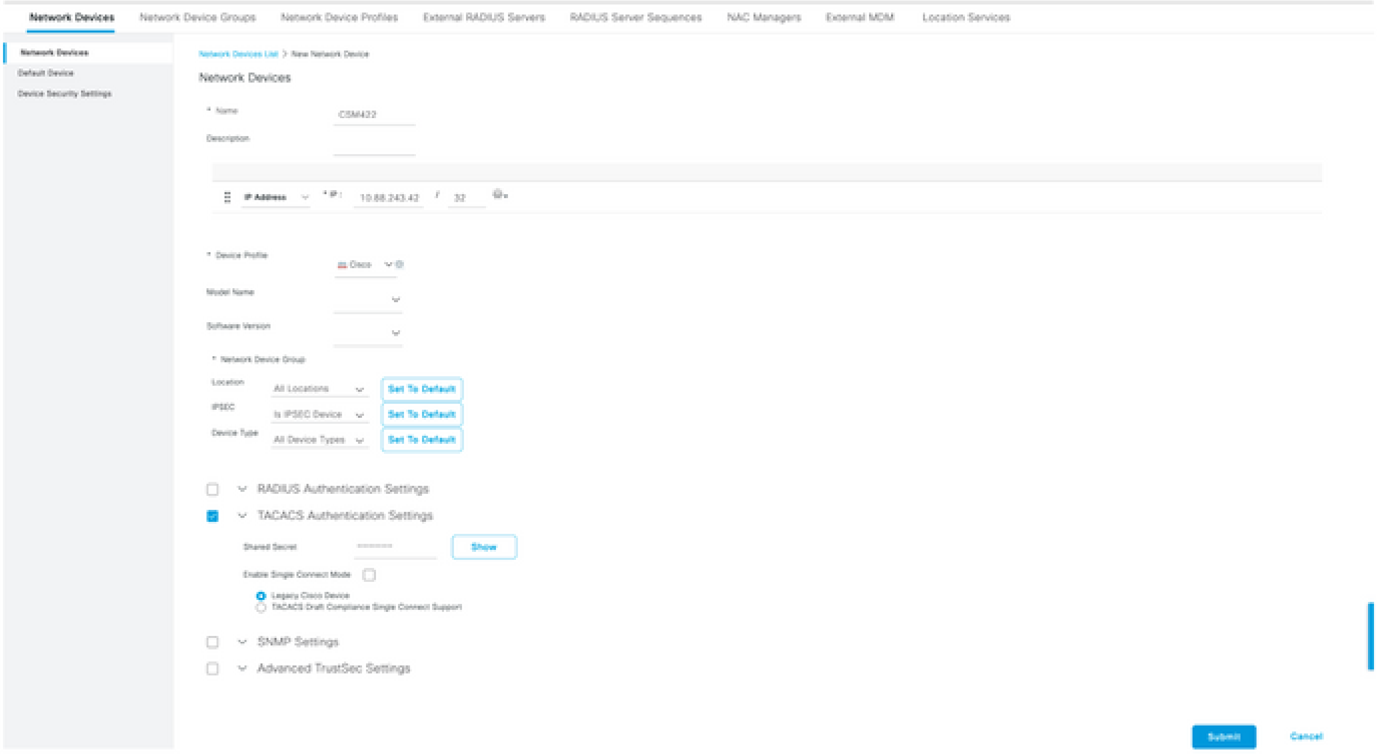
步驟5. ISE顯示成功的身份驗證即時日誌。

ISE 組態

步驟1.選擇三行圖示 ☰ 位於左上角，導航到**管理>網路資源>網路裝置。**



步驟2.選擇+Add按鈕並輸入網路訪問裝置名稱和IP地址的正確值，然後驗證**TACACS身份驗證設定**覈取方塊並定義共用金鑰。選擇「**Submit**」按鈕。



Network Devices

* Name: CSM422

Description:

IP Address * IP : 10.88.243.42 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations [Set To Default]

IPSEC: Is IPSEC Device [Set To Default]

Device Type: All Device Types [Set To Default]

□ RADIUS Authentication Settings

☑ TACACS Authentication Settings

Shared Secret: ········· [Show]

Enable Single Connect Mode □

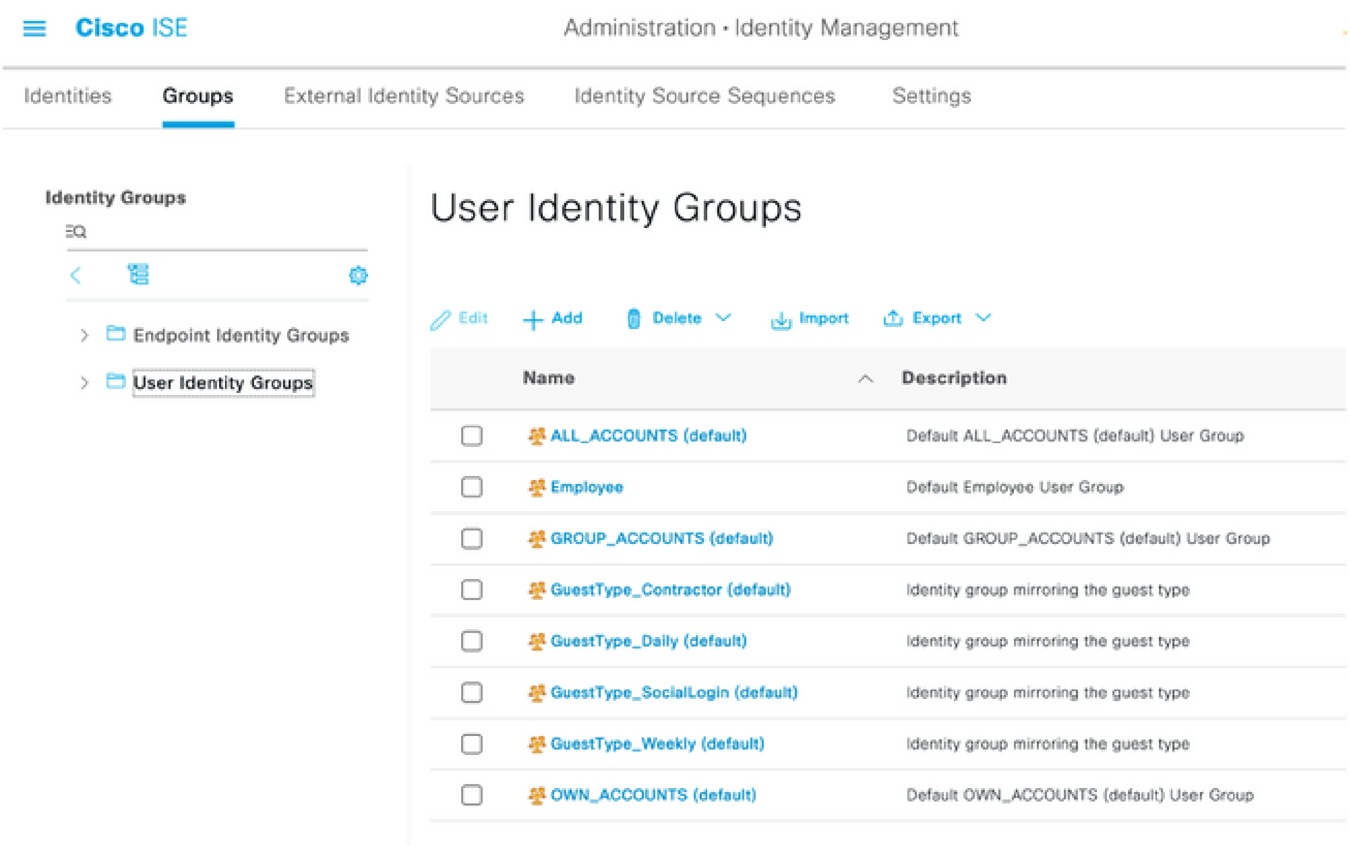
● Legacy Cisco Device

○ TACACS Draft Compliance Single Connect Support

□ SNMP Settings

□ Advanced TrustSec Settings

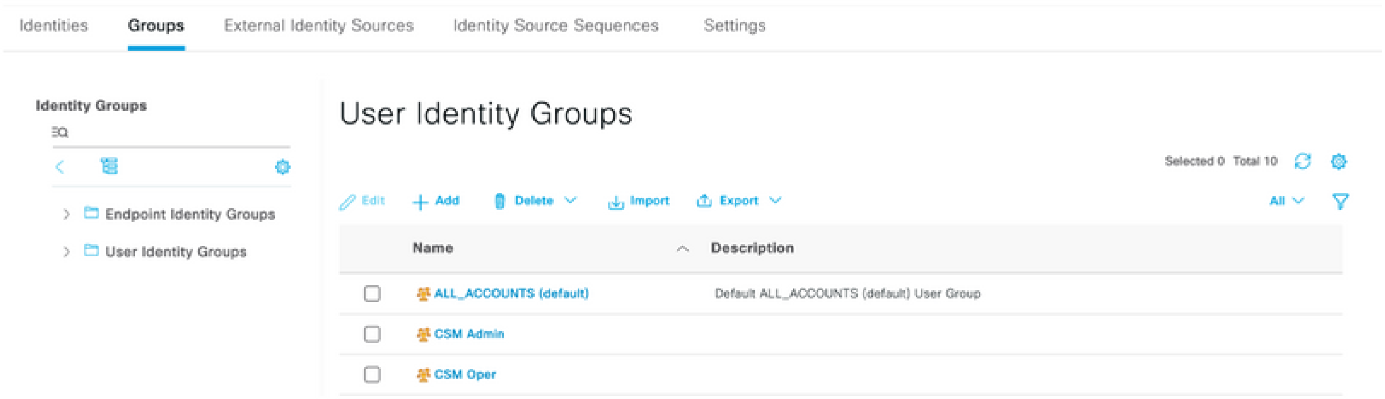
步驟3.選擇三行圖示 位於左上角，導航到**Administration > Identity Management > Groups。**



User Identity Groups

	Name	Description
□	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
□	Employee	Default Employee User Group
□	GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
□	GuestType_Contractor (default)	Identity group mirroring the guest type
□	GuestType_Daily (default)	Identity group mirroring the guest type
□	GuestType_SocialLogin (default)	Identity group mirroring the guest type
□	GuestType_Weekly (default)	Identity group mirroring the guest type
□	OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

步驟4.導航到**User Identity Groups檔案**夾，然後選擇**+Add按**鈕。定義名稱並選擇**提交**按鈕。

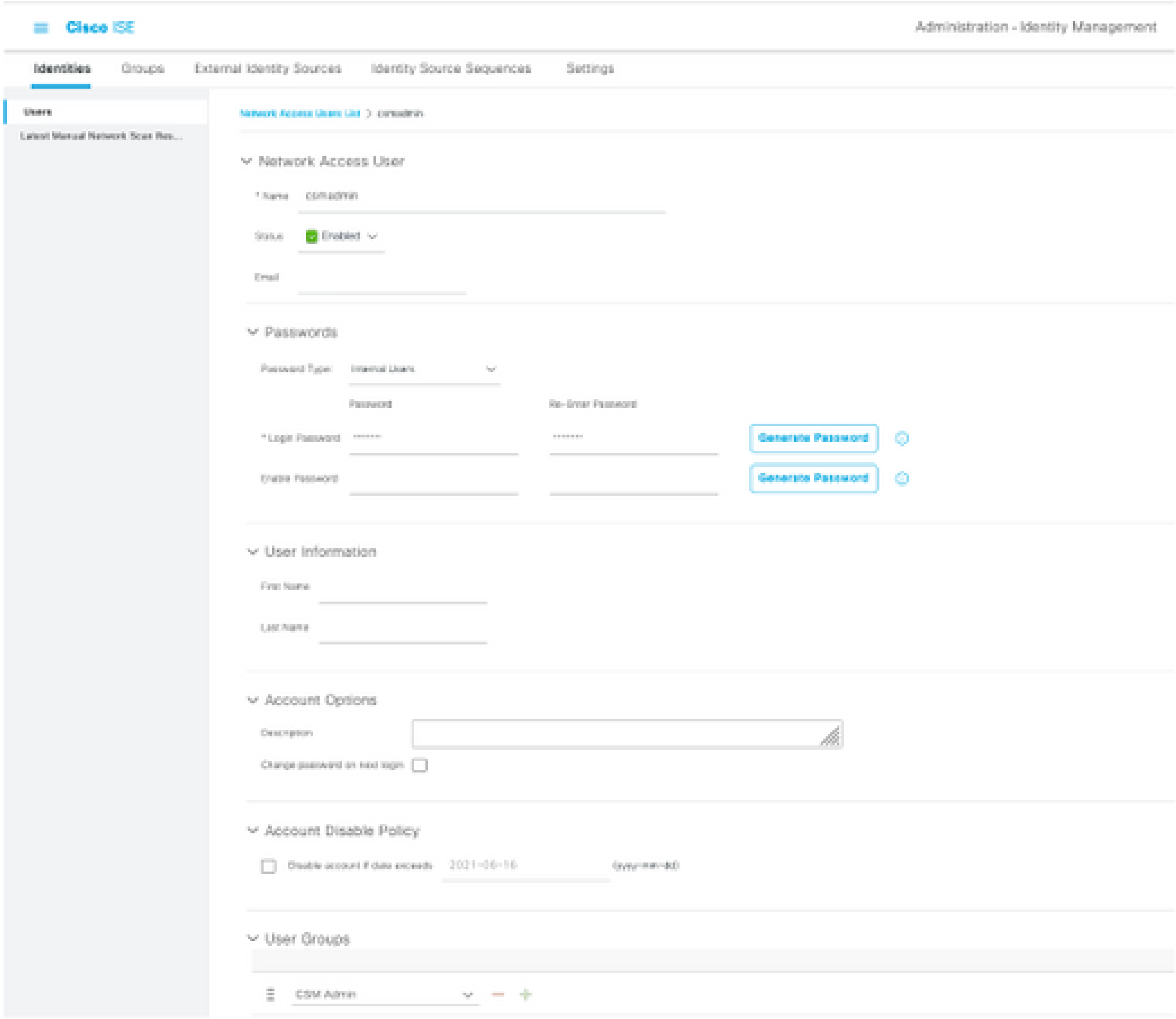


User Identity Groups

	Name	Description
□	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
□	CSM Admin	
□	CSM Oper	

附註：此示例建立CSM Admin和CSM Oper Identity組。您可以對CSM上每種型別的管理員使用者重複步驟4

步驟5.選擇三行圖示 ☰ 並導航到**管理>身份管理>身份。選擇+Add**按鈕並定義使用者名稱和密碼，然後選擇使用者所屬的組。在本示例中，分別建立**csmadmin**和**csmoper**使用者並分配給CSM Admin和CSM Oper組。



Cisco ISE
Administration - Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Res...
Network Access Users List > csmadmin

Network Access User

* Name: csmadmin

Status: 🟩 Enabled

Email:

Passwords

Password Type: Internal Users

	Password	Re-Enter Password	
* Login Password	·······	·······	Generate Password
Enable Password			Generate Password

User Information

First Name:

Last Name:

Account Options

Description:

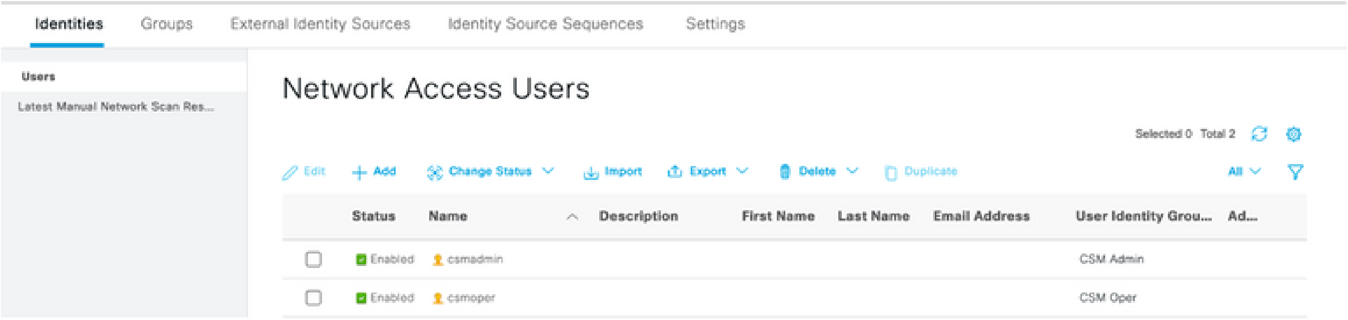
Change password on next login □

Account Disable Policy

□ Disable account if date exceeds 2021-06-16 (yyyy-mm-dd)

User Groups

CSM Admin



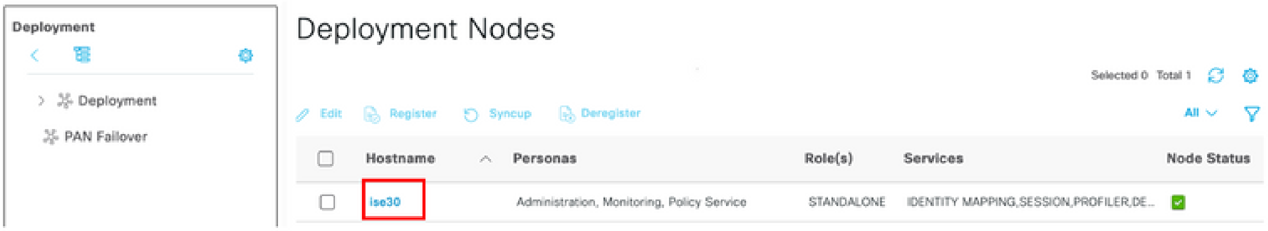
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Res...
Edit
Add
Change Status
Import
Export
Delete
Duplicate
All

Network Access Users

Selected 0 Total 2

	Status	Name	Description	First Name	Last Name	Email Address	User Identity Grou...	Ad...
□	🟩 Enabled	csmadmin					CSM Admin	
□	🟩 Enabled	csmoper					CSM Oper	

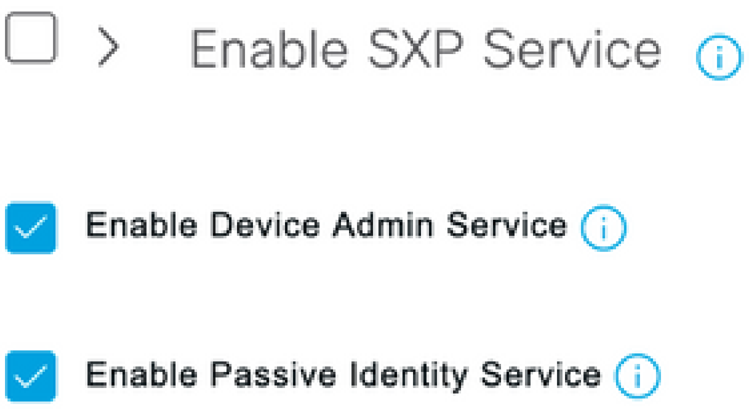
步驟6.選擇 ☰ 並導航到**管理>系統>部署。**選擇主機名節點並啟用**Device Admin Service**



Deployment Nodes

Selected 0 Total 1

Hostname	Personas	Role(s)	Services	Node Status
ise30	Administration, Monitoring, Policy Service	STANDALONE	IDENTITY MAPPING,SESSION,PROFILER,DE...	✓



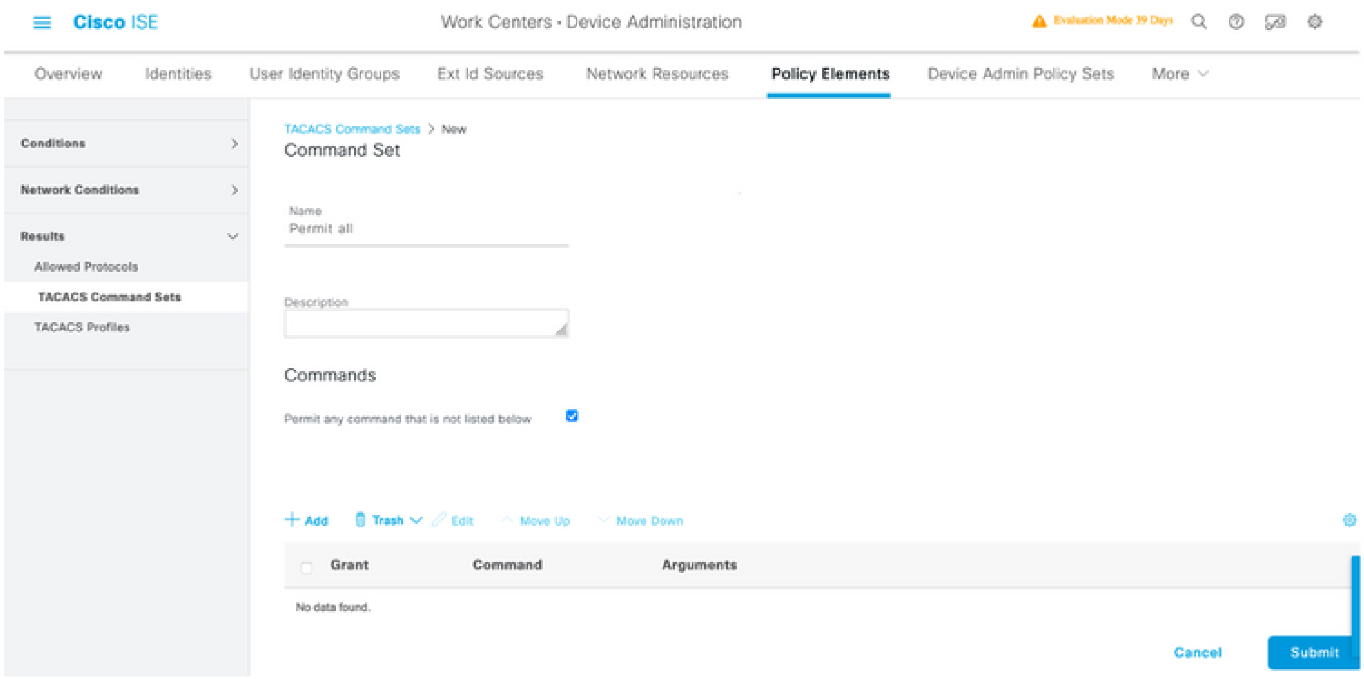
□ > Enable SXP Service

☑ Enable Device Admin Service

☑ Enable Passive Identity Service

附註：如果是分散式部署，請選擇處理TACACS請求的PSN節點

步驟7.選擇三行圖示並導航到**管理>裝置管理>策略元素。導覽至**Results > TACACS Command Sets**。選擇+Add**按鈕，為Command Set定義名稱，並啟用**Permit any command that not listed** below覈取方塊。選擇**提交。**



Command Set

Name
Permit all

Description

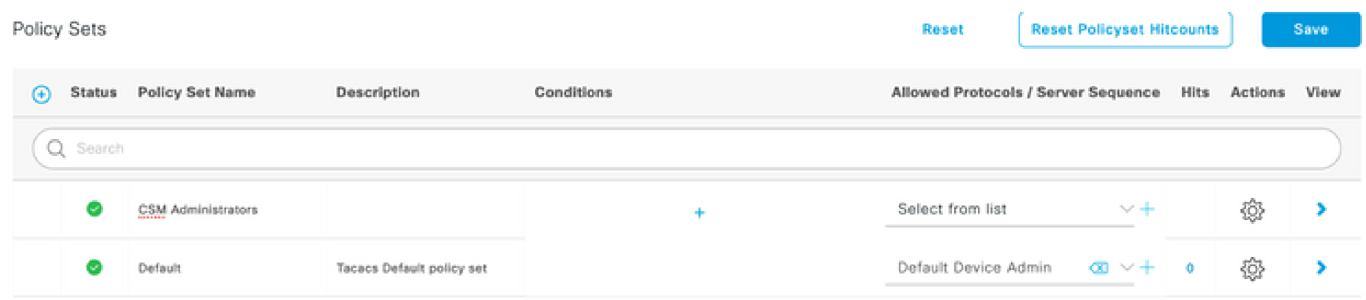
Commands

Permit any command that is not listed below ☑

Grant	Command	Arguments
No data found.		

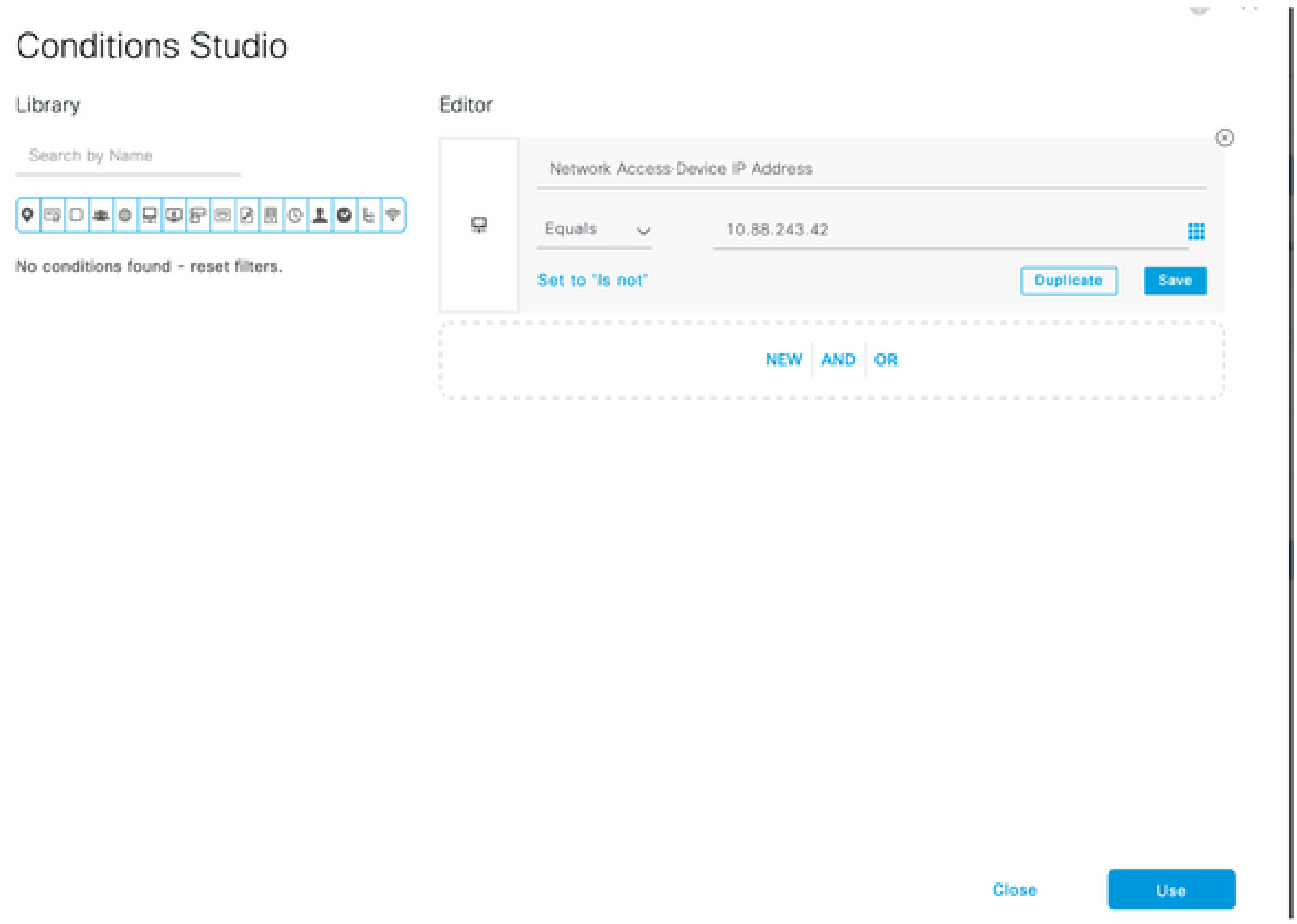
步驟8.選擇位於左上角的三行圖示，然後導航到**Administration -> Device Administration -> Device Admin Policy Sets**。選擇 ⊕ 位於Policy Sets標題下方，定義名稱並選擇中間**的**+按鈕以新增新條

件。



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	CSM Administrators		+	Select from list		⚙	>
●	Default	Tacacs Default policy set		Default Device Admin	0	⚙	>

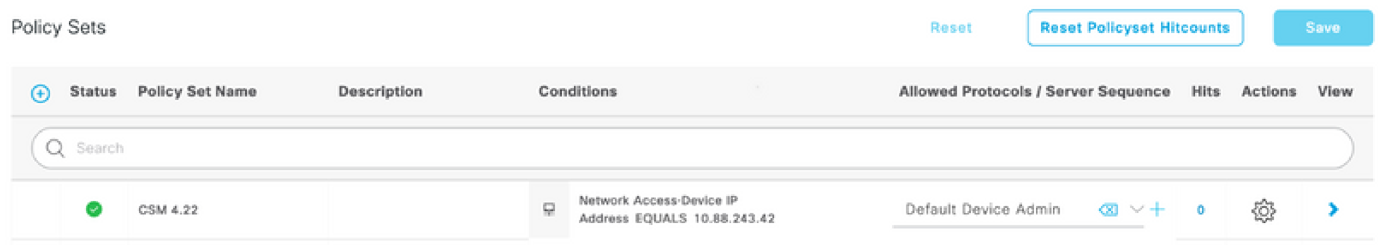
步驟9.在 Condition（條件）視窗中，選擇add a attribute（新增屬性），然後選擇**Network Device** Icon（網路裝置圖示），後跟Network access device IP address（網路訪問裝置IP地址）。 選擇**Attribute Value**並新增CSM IP地址。選擇**Use** once done。



No conditions found - reset filters.

Network Access-Device IP Address
Equals 10.88.243.42
Set to 'Is not'

步驟10.在allow protocols部分下，選擇**Device Default Admin**。選擇保存

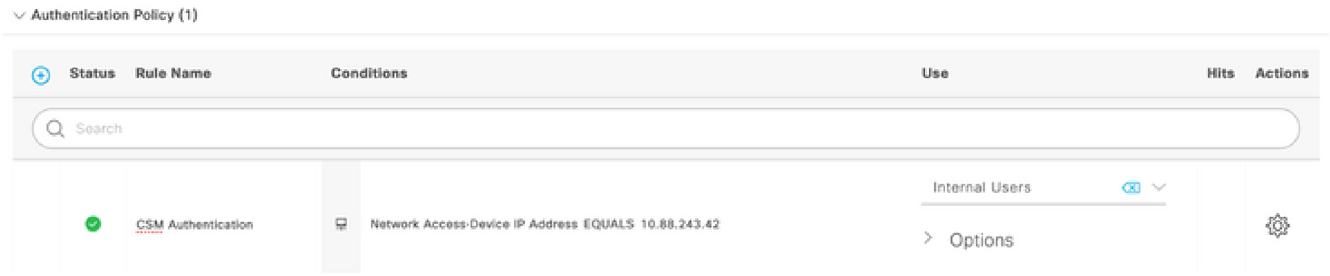


Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	CSM 4.22		Network Access-Device IP Address EQUALS 10.88.243.42	Default Device Admin	0	⚙	>

步驟11.選擇右箭頭 ❯ 用於定義身份驗證和授權策略的策略集的圖示

步驟12.選擇 ⊕ 位於身份驗證策略標題下方，定義名稱並選擇中間的+以新增新條件。在「條件」視窗中，選擇新增屬性，然後選擇**網路裝置**圖示，後跟網路訪問裝置IP地址。 選擇**Attribute Value**並新增CSM IP地址。選擇**使用一**次

步驟13.選擇**Internal Users作為Identity Store並選擇Save**

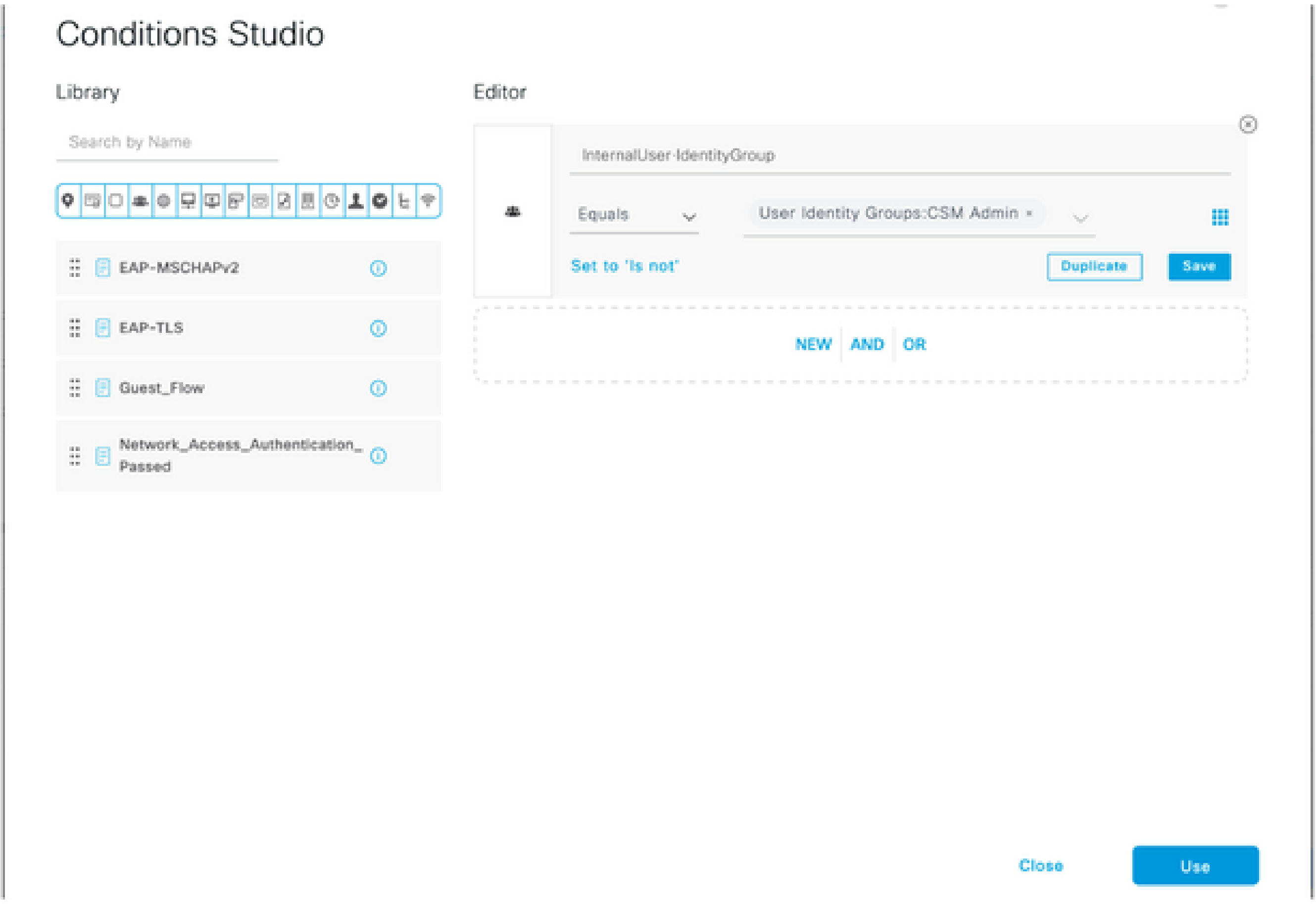


Authentication Policy (1)

⊕	Status	Rule Name	Conditions	Use	Hits	Actions
	●	CSM Authentication	Network Access-Device IP Address EQUALS 10.88.243.42	Internal Users Options		⚙

附註：如果ISE加入到Active Directory，可以將身份儲存更改為AD儲存。

步驟14.選擇 ⊕ 位於Authorization Policy標題下方，定義名稱並選擇中間的**+**按鈕以新增新條件。在「條件」視窗中，選擇新增屬性，然後選擇**身份組圖示**，後跟**Internal User:身份組。選擇CSM Admin Group，然後選擇Use**。



Conditions Studio

Library

Search by Name

- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- Network_Access_Authentication_Passed

Editor

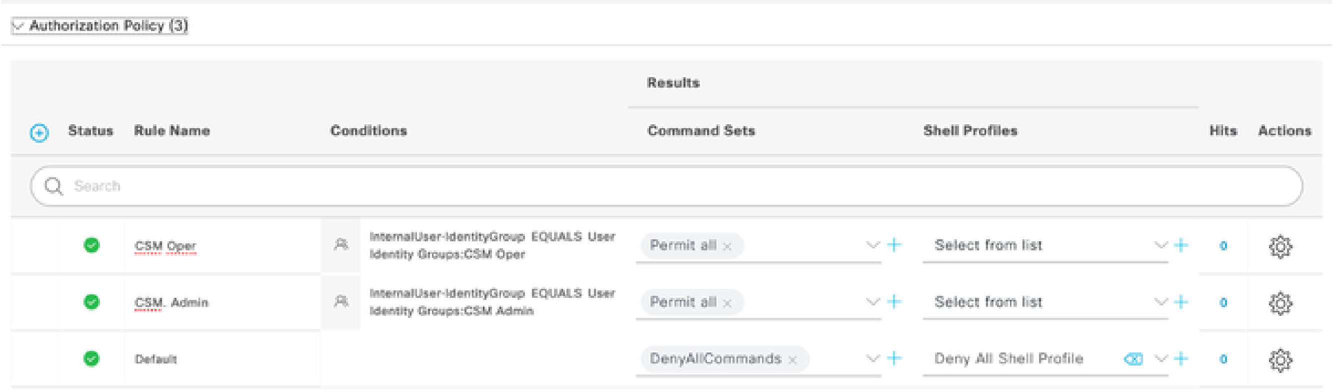
InternalUser·IdentityGroup

Equals — User Identity Groups:CSM Admin

Set to 'Is not'

步驟15.在命令集下，選擇允許在第7步中建立的所有命令集，然後選擇保**存**

對CSM Oper組重複步驟14和15

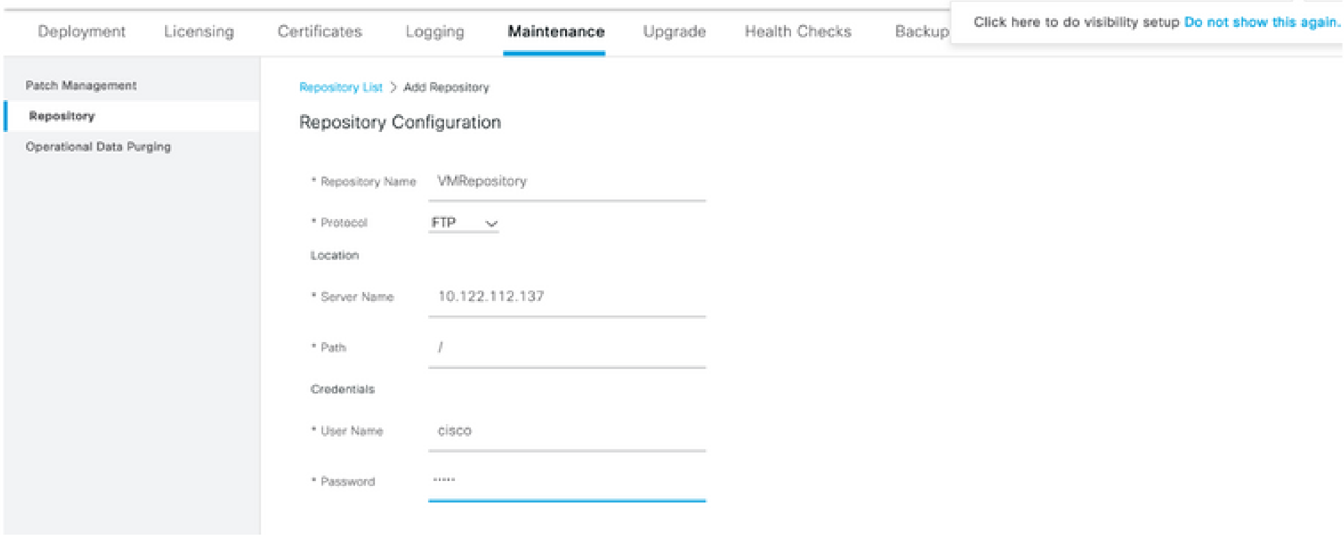


Authorization Policy (3)

			Results			
Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
✓	CSM Oper	InternalUser·IdentityGroup EQUALS User Identity Groups:CSM Oper	Permit all	Select from list	0	⚙
✓	CSM_Admin	InternalUser·IdentityGroup EQUALS User Identity Groups:CSM Admin	Permit all	Select from list	0	⚙
✓	Default		DenyAllCommands	Deny All Shell Profile	0	⚙

第16步（可選）。 選擇左上角的三行圖示並選擇**管理>系統>維護>儲存庫**，選擇**+新增**以新增用於儲存TCP轉儲檔案以進行故障排除的儲存庫。

第17步（可選）。 定義儲存庫名稱、協定、伺服器名稱、路徑和憑據。選擇**Submit** once done。



Repository Configuration

* Repository Name: VMRepository

* Protocol: FTP

Location

* Server Name: 10.122.112.137

* Path: /

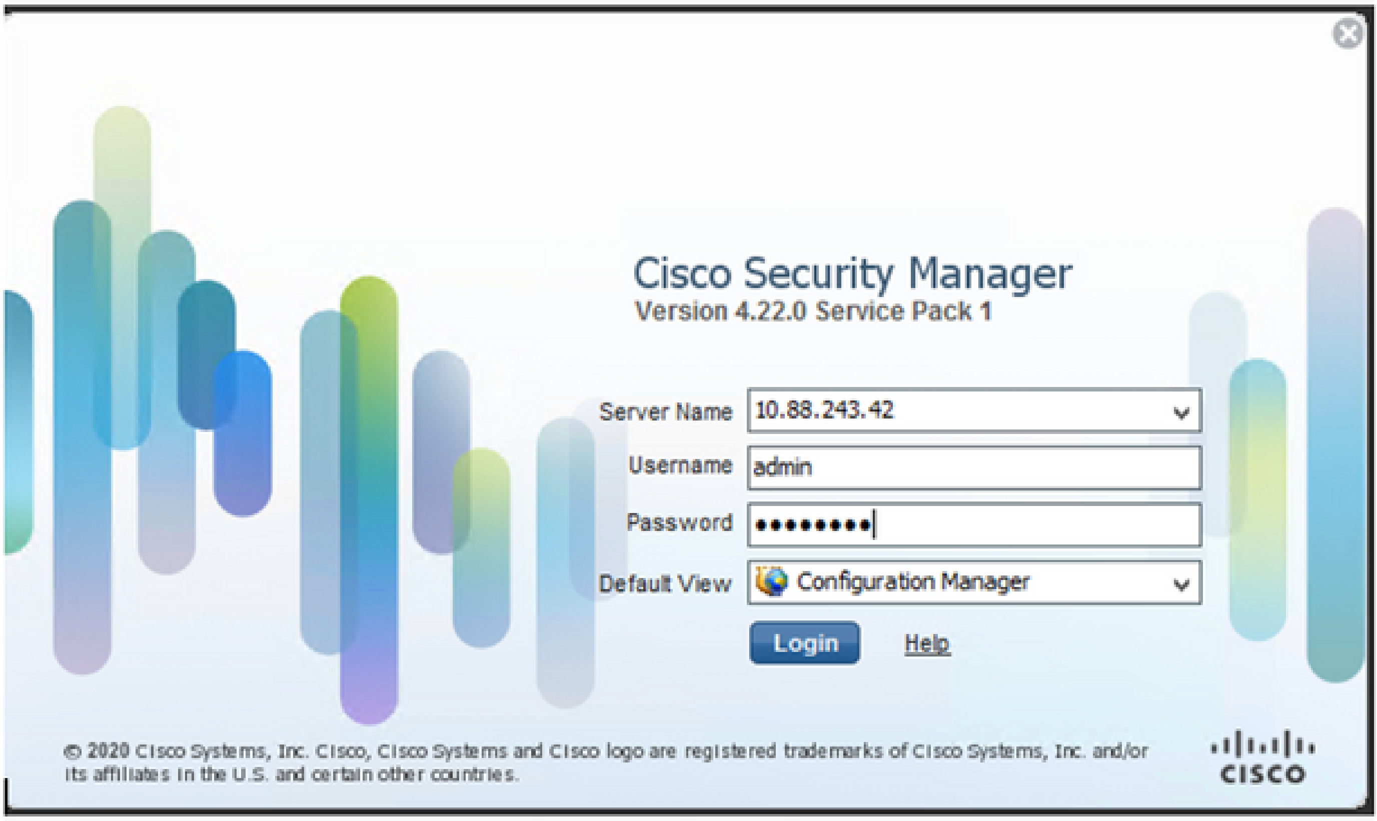
Credentials

* User Name: cisco

* Password: *****

CSM配置

步驟1.使用本地管理員帳戶登入到思科安全管理器客戶端應用程式。從選單導航到**工具>安全管理器管理**

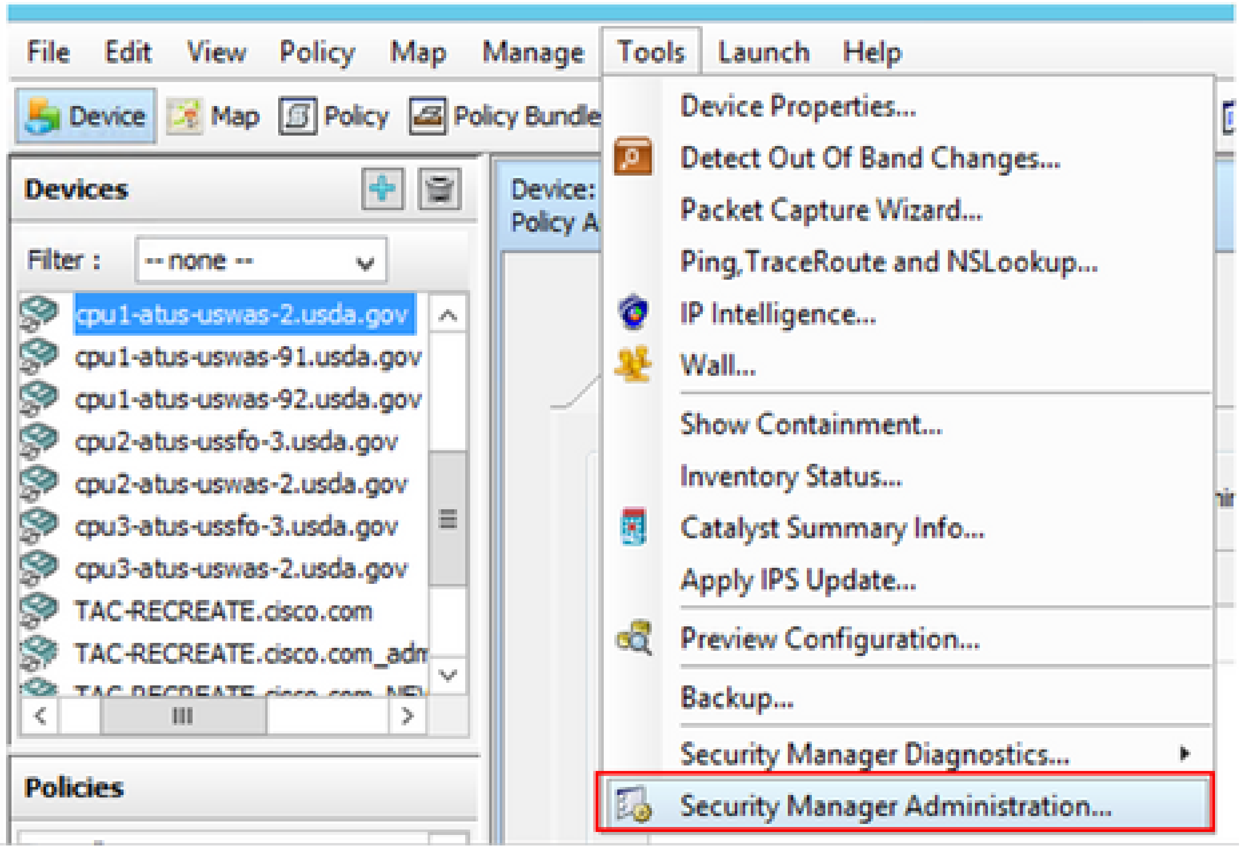

Cisco Security Manager
Version 4.22.0 Service Pack 1
Login
Help
© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
cisco

Server Name: 10.88.243.42

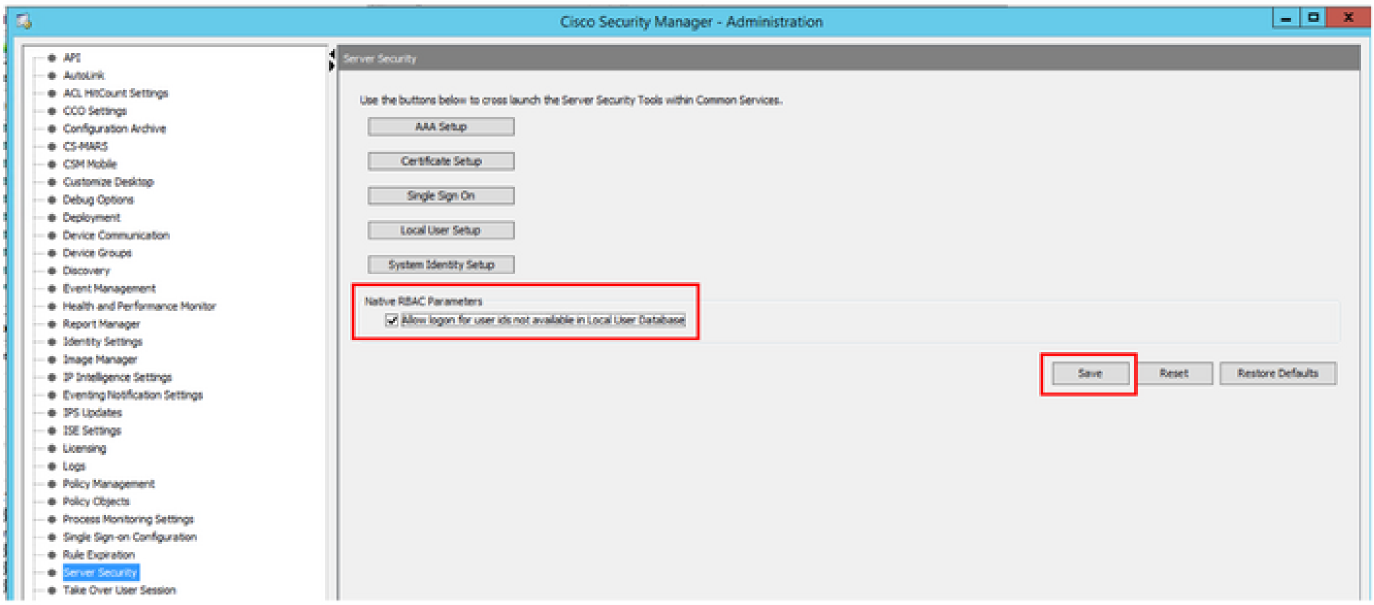
Username: admin

Password: ●●●●●●●●●

Default View: Configuration Manager


File
Edit
View
Policy
Map
Manage
Tools
Launch
Help
Device
Map
Policy
Policy Bundle
Devices
Filter :
-- none --
cpu1-atus-uswas-2.usda.gov
cpu1-atus-uswas-91.usda.gov
cpu1-atus-uswas-92.usda.gov
cpu2-atus-ussfo-3.usda.gov
cpu2-atus-uswas-2.usda.gov
cpu3-atus-ussfo-3.usda.gov
cpu3-atus-uswas-2.usda.gov
TAC-RECREATE.cisco.com
TAC-RECREATE.cisco.com_adm
Policies
Device:
Policy A
Device Properties...
Detect Out Of Band Changes...
Packet Capture Wizard...
Ping,TraceRoute and NSLookup...
IP Intelligence...
Wall...
Show Containment...
Inventory Status...
Catalyst Summary Info...
Apply IPS Update...
Preview Configuration...
Backup...
Security Manager Diagnostics...
Security Manager Administration...

步驟2.選中**Native RBAC Parameters下的框。**選擇**儲存**並關閉



Use the buttons below to cross launch the Server Security Tools within Common Services.

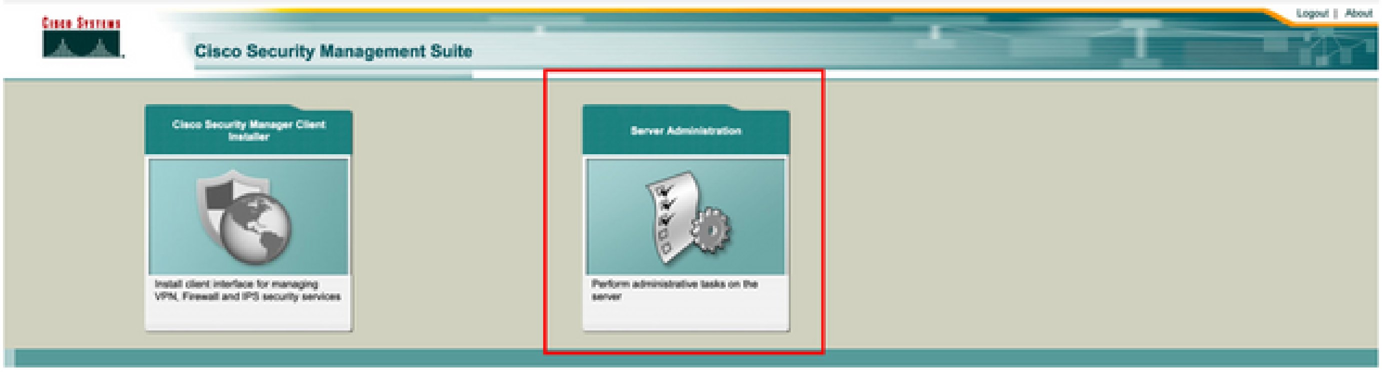
Native RBAC Parameters

☑ Allow logon for user ids not available in Local User Database

步驟3.從選單中選擇文**件>提交。「檔案」>「提交」。**

附註：所有更改都必須儲存，以防配置更改需要提交和部署。

步驟4.導覽至CSM Management UI，鍵入https://<enter_CSM_IP_Address，**然後選擇Server Administration。**



Cisco Security Manager Client Installer

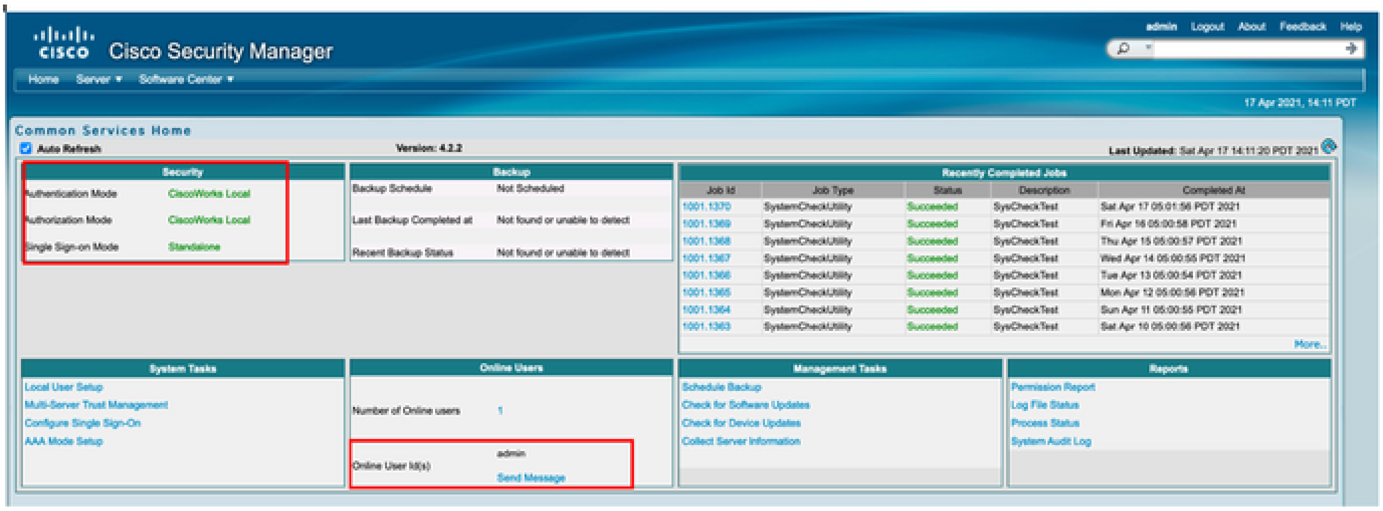
Install client interface for managing VPN, Firewall and IPS security services

Server Administration

Perform administrative tasks on the server

附註：第4步至第7步顯示了為ISE中未定義的所有管理員定義預設角色的過程。這些步驟是可選的。

步驟5.驗證身份驗證模式設定為**CiscoWorks Local 並且Online** userID是在CSM上建立的本地管理員帳戶。



17 Apr 2021, 14:11 PDT

Common Services Home

☑ Auto Refresh

Version: 4.2.2

Last Updated: Sat Apr 17 14:11:20 PDT 2021

Security	
Authentication Mode	CiscoWorks Local
Authorization Mode	CiscoWorks Local
Single Sign-on Mode	Standalone

Backup	
Backup Schedule	Not Scheduled
Last Backup Completed at	Not found or unable to detect
Recent Backup Status	Not found or unable to detect

Recently Completed Jobs

Job Id	Job Type	Status	Description	Completed At
1001.1370	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 17 05:01:56 PDT 2021
1001.1369	SystemCheckUtility	Succeeded	SysCheckTest	Fri Apr 16 05:00:58 PDT 2021
1001.1368	SystemCheckUtility	Succeeded	SysCheckTest	Thu Apr 15 05:00:57 PDT 2021
1001.1367	SystemCheckUtility	Succeeded	SysCheckTest	Wed Apr 14 05:00:55 PDT 2021
1001.1366	SystemCheckUtility	Succeeded	SysCheckTest	Tue Apr 13 05:00:54 PDT 2021
1001.1365	SystemCheckUtility	Succeeded	SysCheckTest	Mon Apr 12 05:00:56 PDT 2021
1001.1364	SystemCheckUtility	Succeeded	SysCheckTest	Sun Apr 11 05:00:55 PDT 2021
1001.1363	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 10 05:00:56 PDT 2021

More...

System Tasks

- Local User Setup
- Multi-Server Trust Management
- Configure Single Sign-On
- AAA Mode Setup

Online Users	
Number of Online users	1
Online User Id(s)	admin Send Message

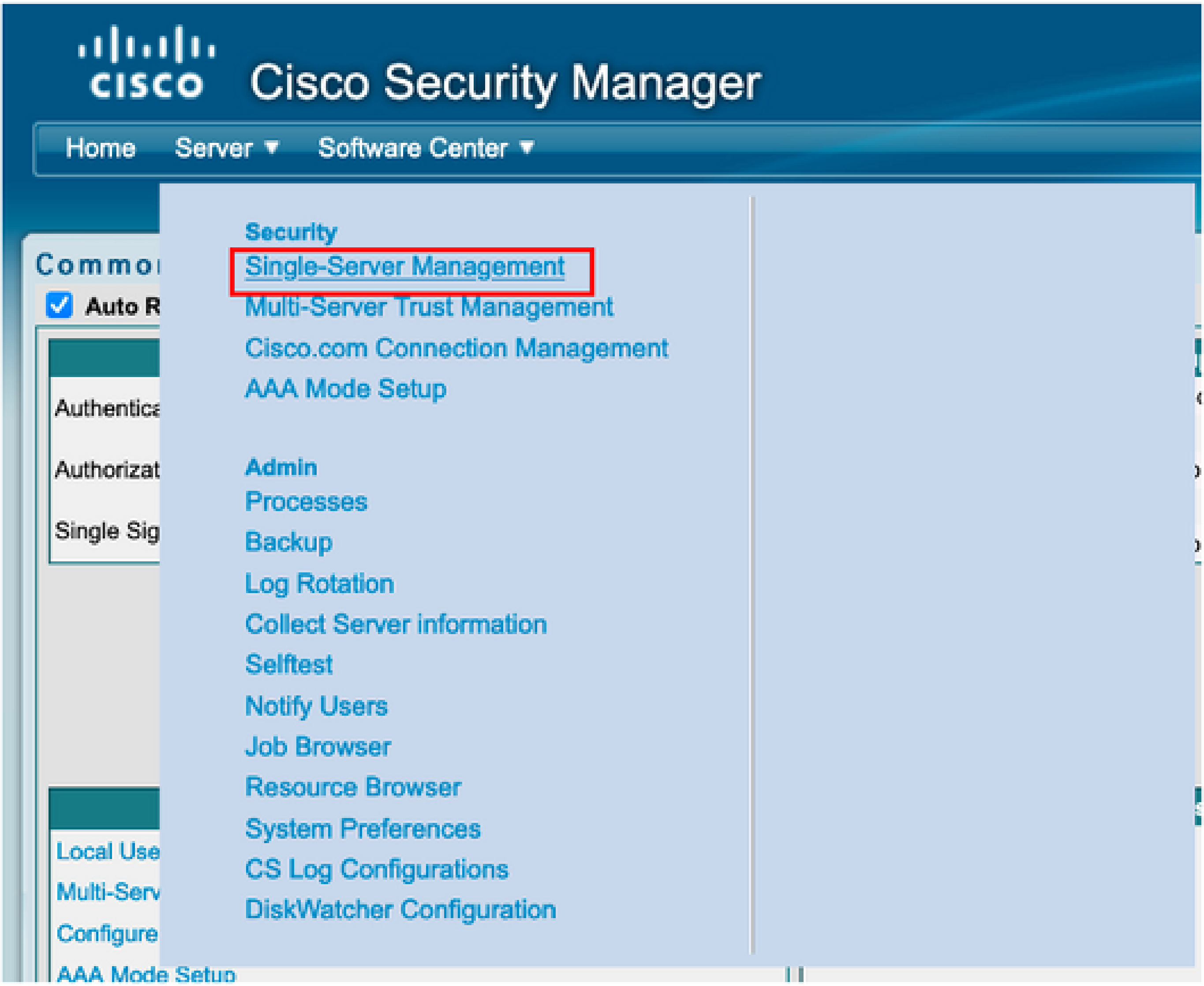
Management Tasks

- Schedule Backup
- Check for Software Updates
- Check for Device Updates
- Collect Server Information

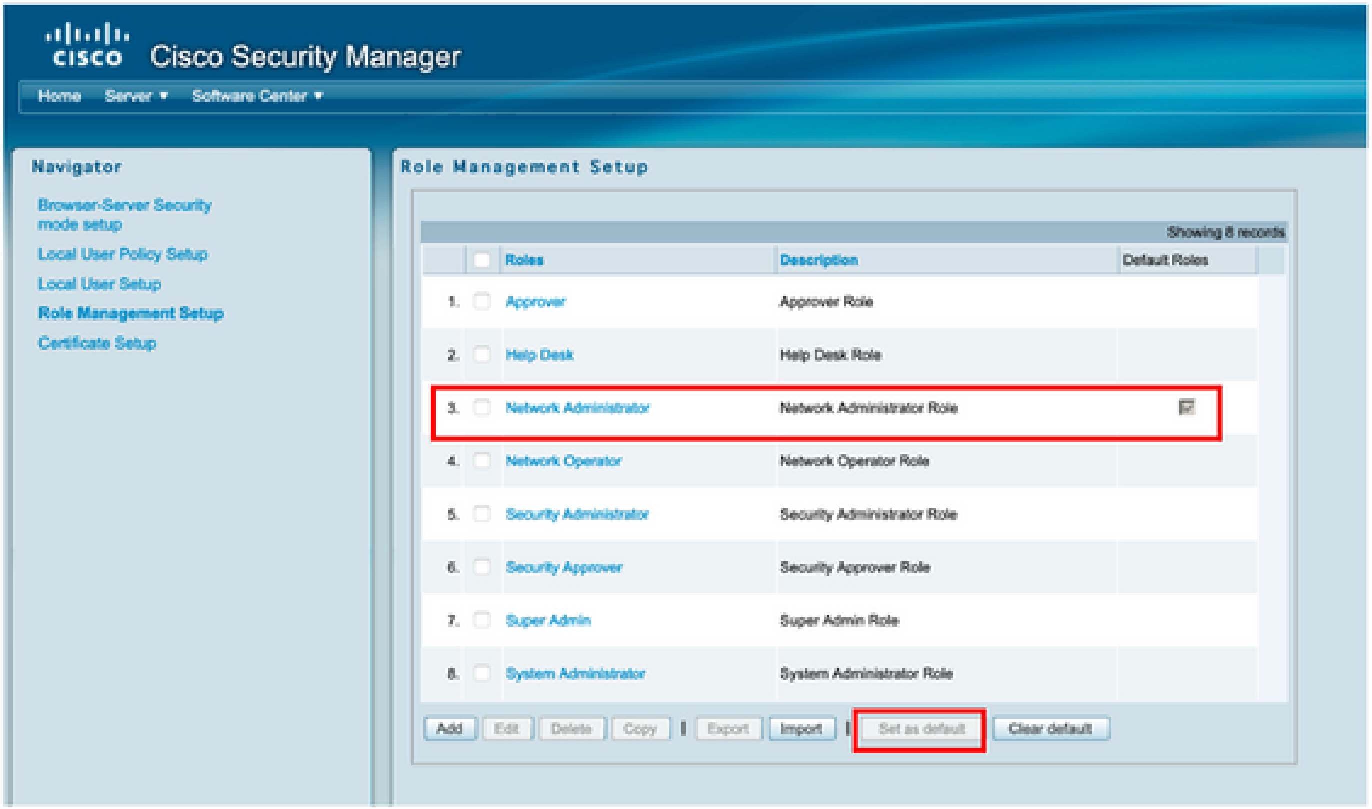
Reports

- Permission Report
- Log File Status
- Process Status
- System Audit Log

步驟6.導覽至**Server 並選擇Single-Server Management**



步驟7.選擇Role Management Setup，並選擇所有管理員使用者在身份驗證時獲得的預設許可權。在本示例中，使用Network Administrator。選中後，選擇**設定為預設值。**

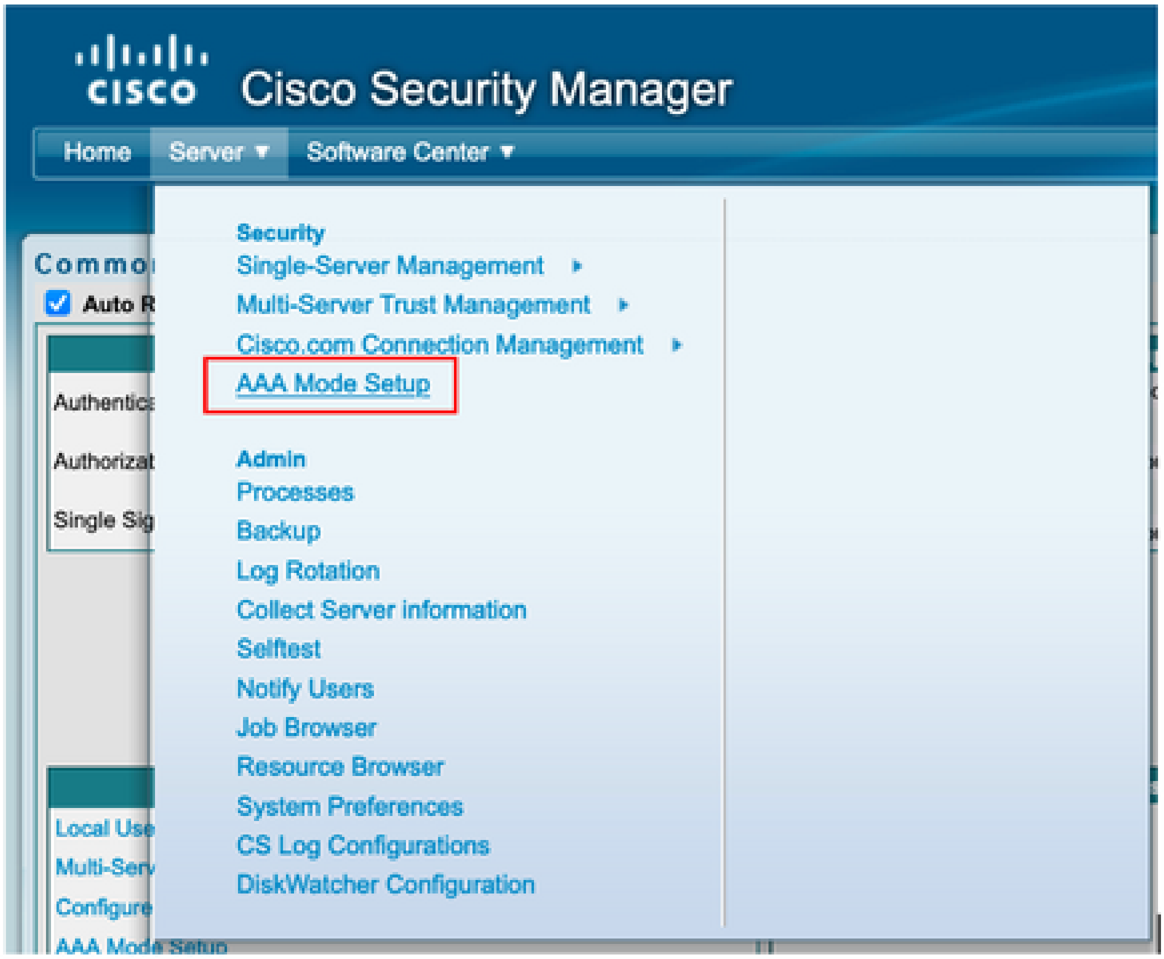


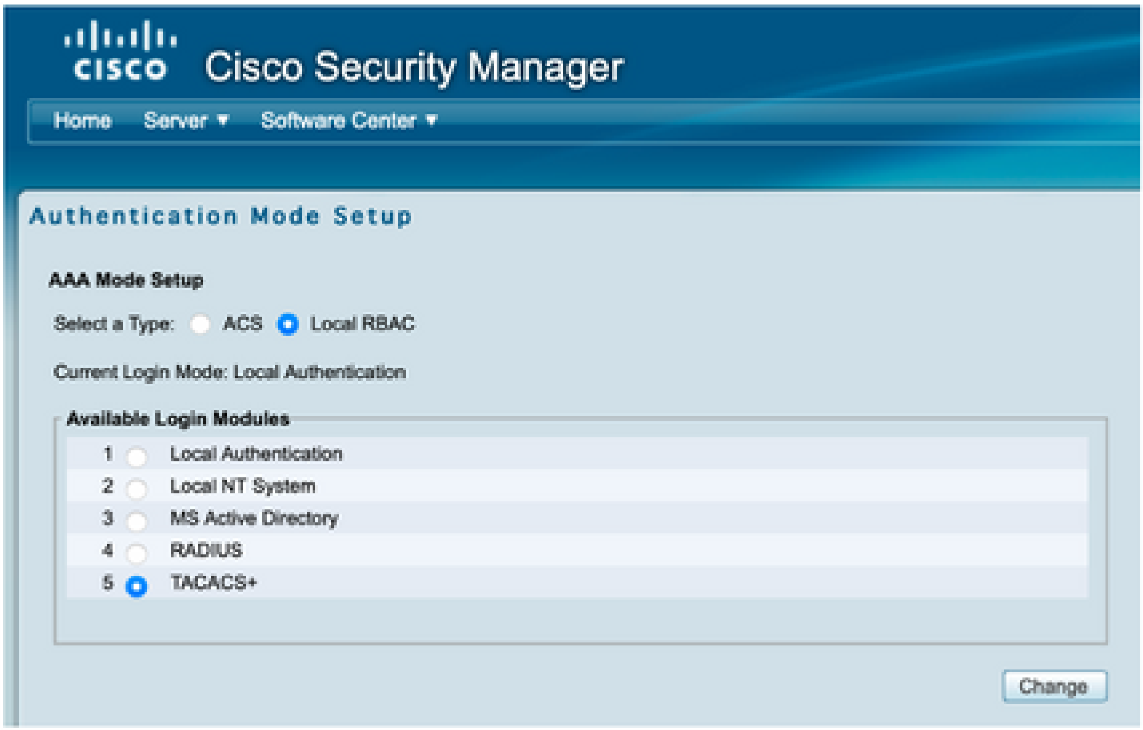
Role Management Setup

Showing 8 records

	□	Roles	Description	Default Roles
1.	□	Approver	Approver Role	
2.	□	Help Desk	Help Desk Role	
3.	□	Network Administrator	Network Administrator Role	☑
4.	□	Network Operator	Network Operator Role	
5.	□	Security Administrator	Security Administrator Role	
6.	□	Security Approver	Security Approver Role	
7.	□	Super Admin	Super Admin Role	
8.	□	System Administrator	System Administrator Role	

步驟8.選擇Sever>AAA Mode Setup Role，然後選擇**TACACS+選**項，最後選擇**change**以新增ISE資訊。





Authentication Mode Setup

AAA Mode Setup

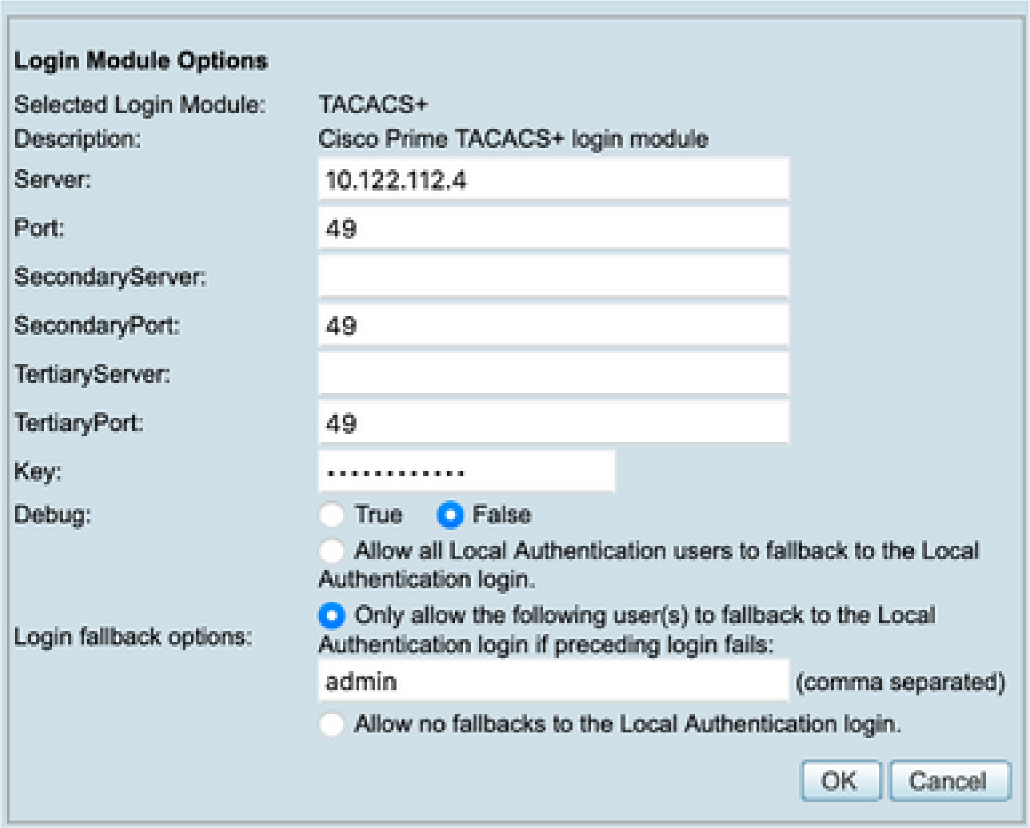
Select a Type: ○ ACS ● Local RBAC

Current Login Mode: Local Authentication

Available Login Modules

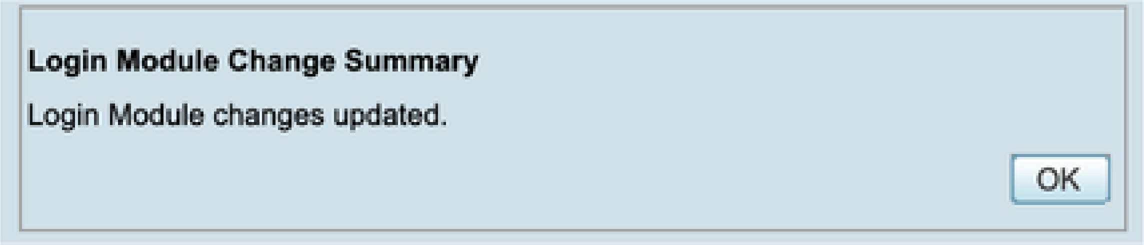
1	○	Local Authentication
2	○	Local NT System
3	○	MS Active Directory
4	○	RADIUS
5	●	TACACS+

步驟9.定義ISE IP地址和金鑰（可選），您可以選擇允許所有本地身份驗證使用者的選項，或者在登入失敗時僅允許一個使用者。在本示例中，僅管理員使用者被允許作為回退方法。選擇**確定**以儲存更改。



Login Module Options

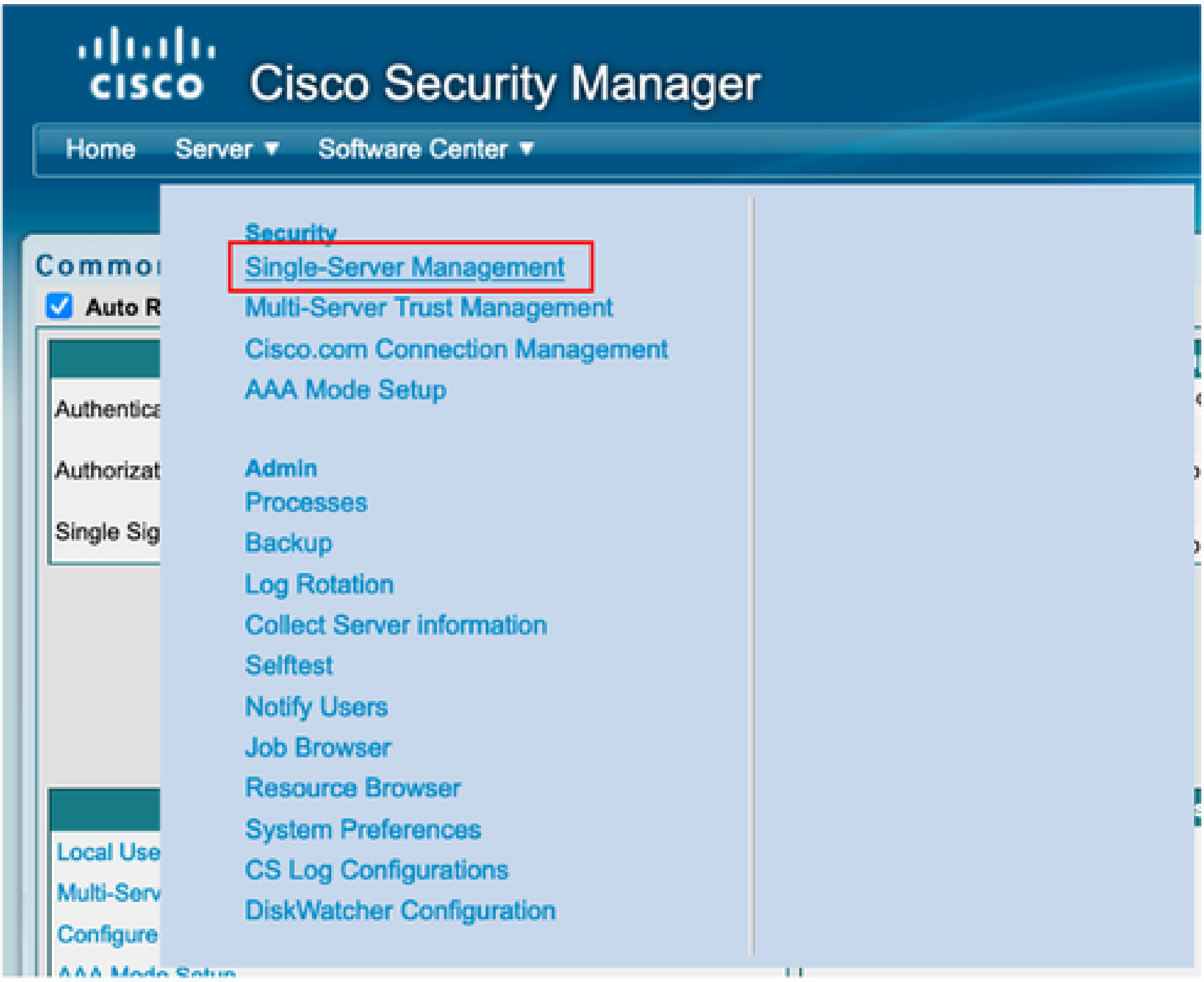
Selected Login Module:	TACACS+
Description:	Cisco Prime TACACS+ login module
Server:	10.122.112.4
Port:	49
SecondaryServer:	
SecondaryPort:	49
TertiaryServer:	
TertiaryPort:	49
Key:	•••••••••••••
Debug:	○ True ● False
Login fallback options:	○ Allow all Local Authentication users to fallback to the Local Authentication login. ● Only allow the following user(s) to fallback to the Local Authentication login if preceding login fails: admin (comma separated) ○ Allow no fallbacks to the Local Authentication login.

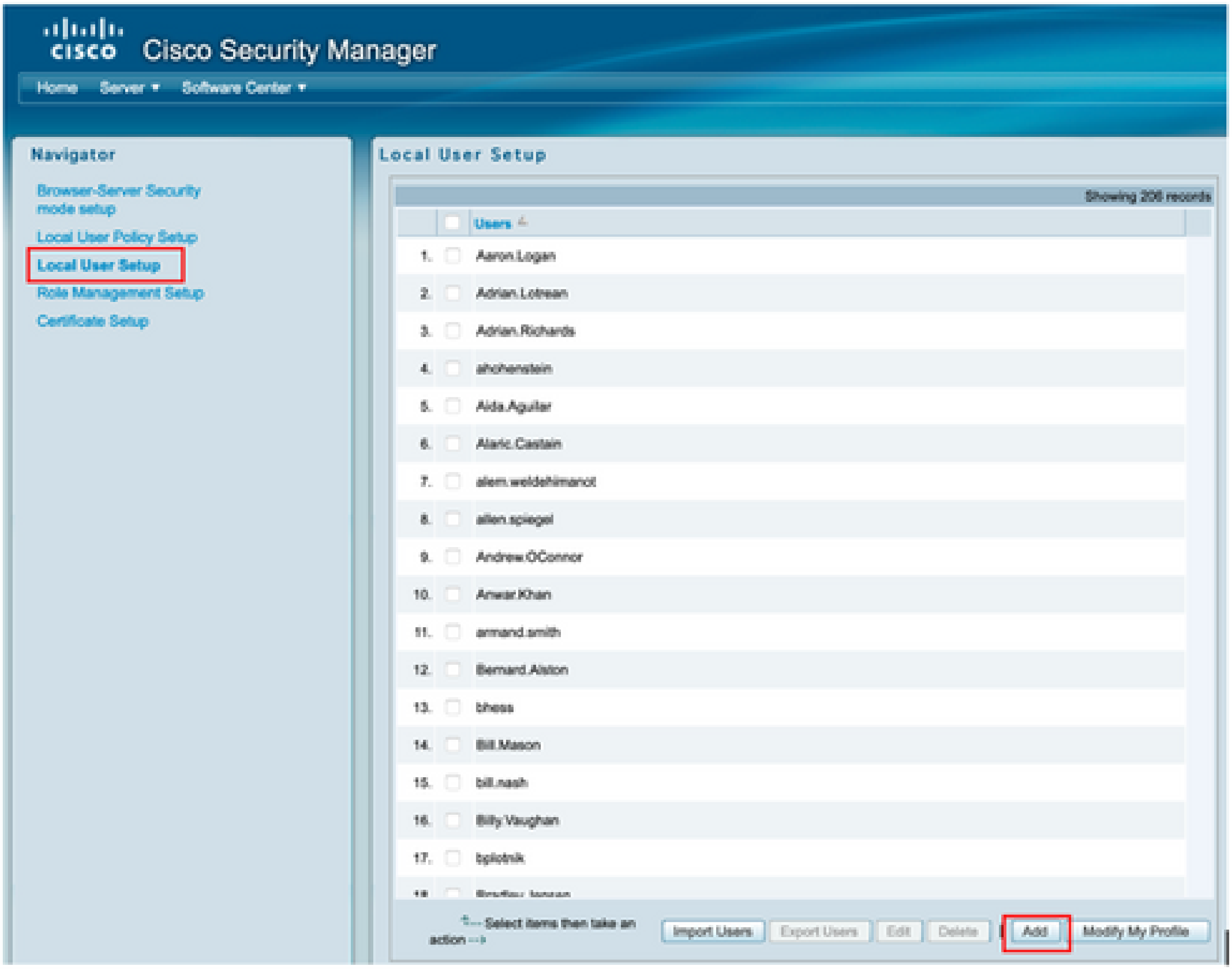


Login Module Change Summary

Login Module changes updated.

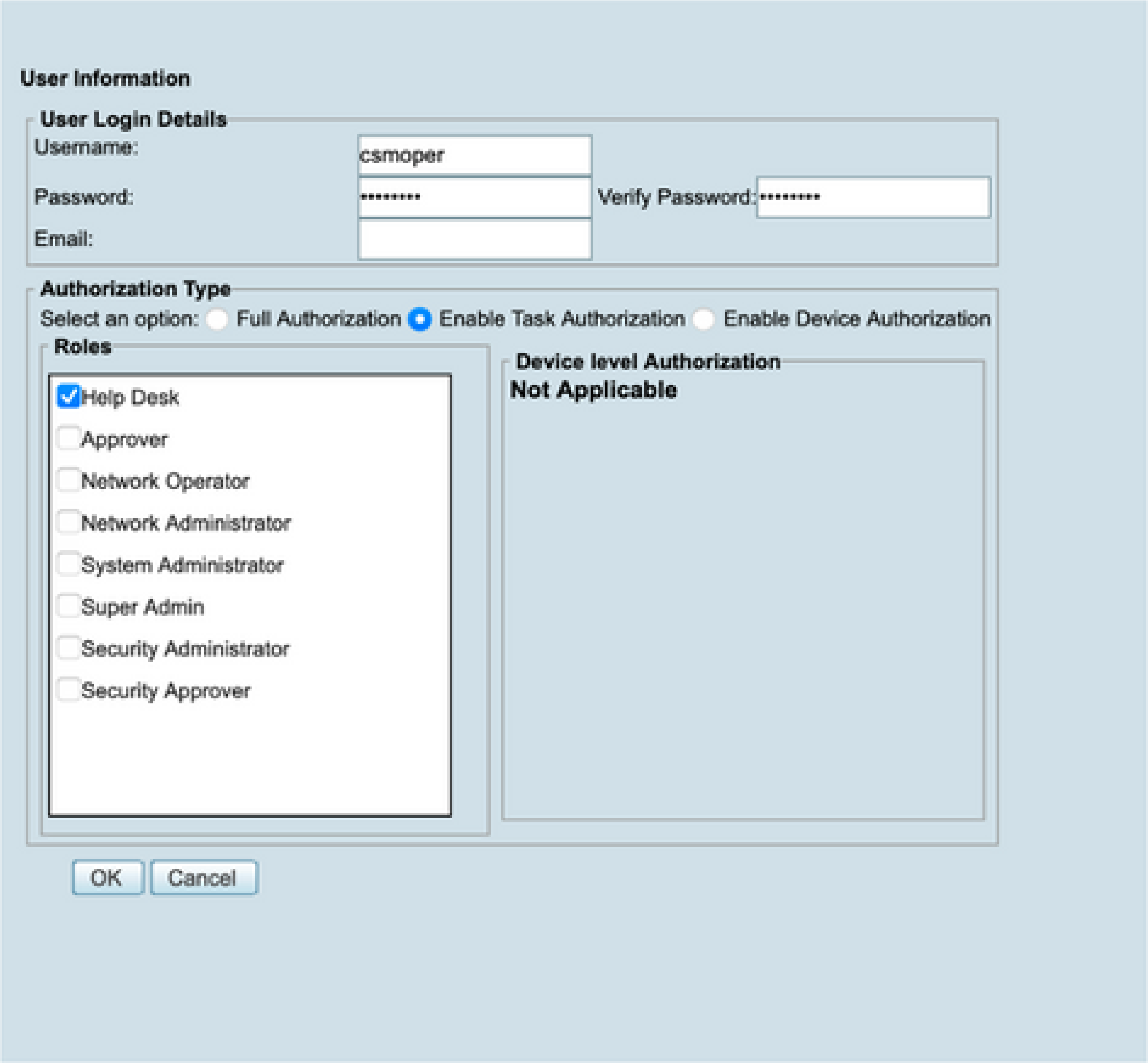
步驟10.選擇Server> Single Server Management，然後選擇Local User Setup並選擇add。





	□	Users
1.	□	Aaron.Logan
2.	□	Adrian.Lotrean
3.	□	Adrian.Richards
4.	□	ahohenstein
5.	□	Aida.Aguilar
6.	□	Alaric.Castain
7.	□	alem.weldehimanot
8.	□	allen.spiegel
9.	□	Andrew.OConnor
10.	□	Anwar.Khan
11.	□	armand.smith
12.	□	Bernard.Alston
13.	□	bhess
14.	□	Bill.Mason
15.	□	bill.nash
16.	□	Billy.Vaughan
17.	□	bplotnik
18.	□	[illegible]

步驟11.在ISE配置部分的第5步中，定義在ISE上建立的相同使用者名稱和密碼，本示例使用**csmoper和Help Desk任務授權**角色。選擇**OK**以儲存管理員使用者。



User Information

User Login Details

Username: csmoper

Password: ********* Verify Password: *********

Email:

Authorization Type

Select an option: ○ Full Authorization ● Enable Task Authorization ○ Enable Device Authorization

Roles

☑ Help Desk
□ Approver
□ Network Operator
□ Network Administrator
□ System Administrator
□ Super Admin
□ Security Administrator
□ Security Approver

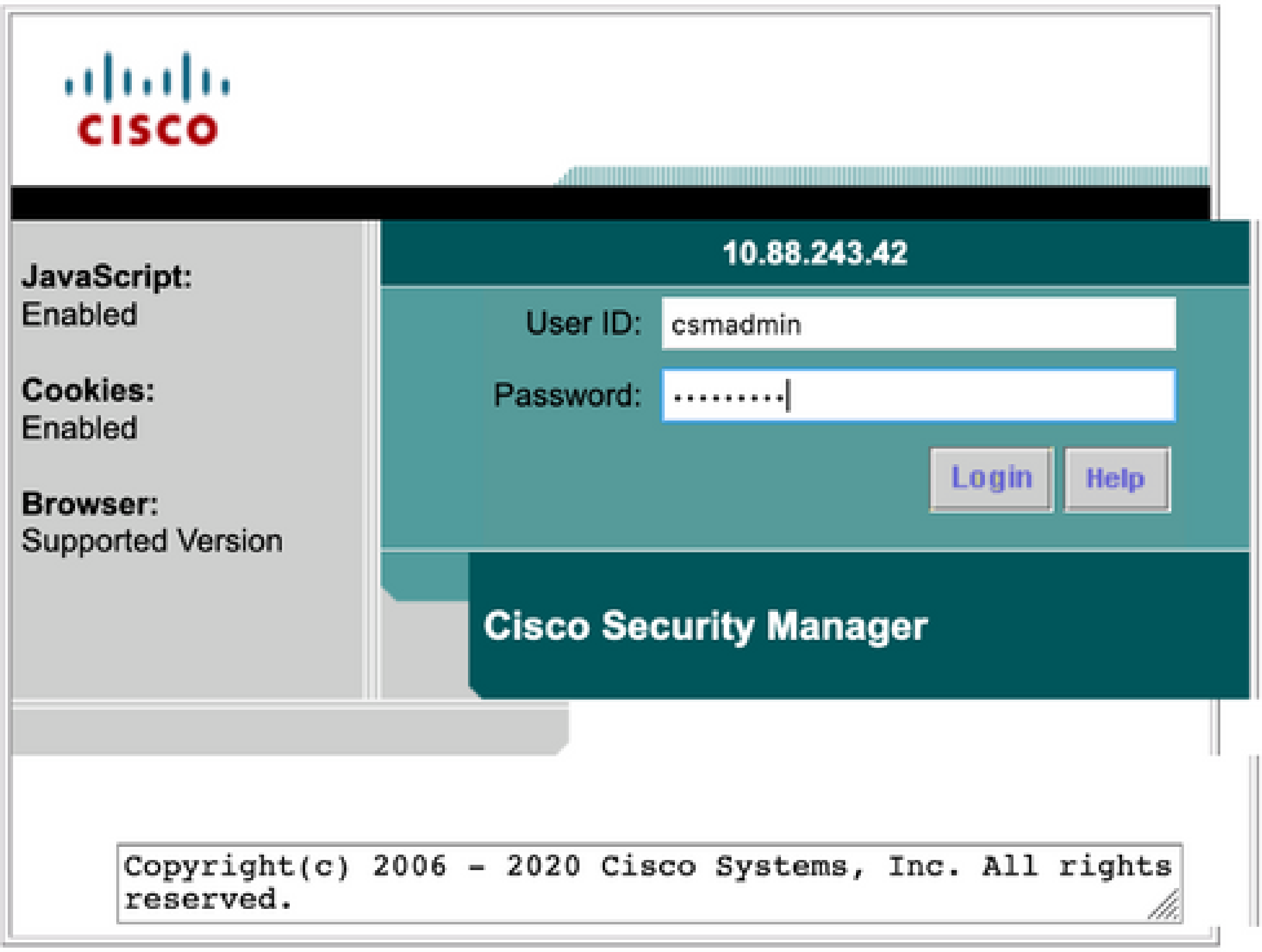
Device level Authorization

Not Applicable

驗證

思科安全管理器客戶端UI

步驟1.開啟新視窗瀏覽器，在ISE配置部分下鍵入https://<enter_CSM_IP_Address，使用csmadmin在第5步中建立的使用者名稱和密碼。


10.88.243.42

JavaScript: Enabled

Cookies: Enabled

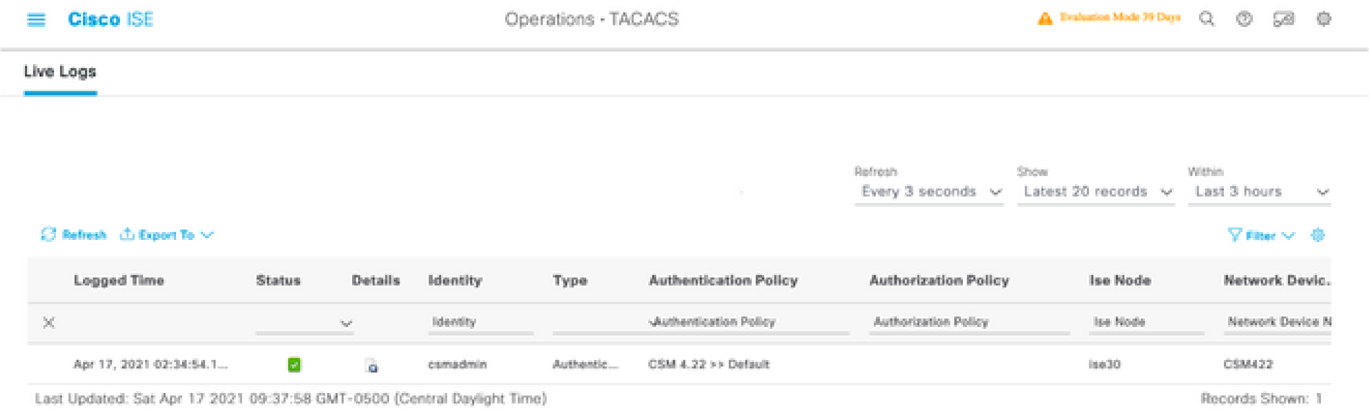
Browser: Supported Version

User ID: csmadmin

Password: ••••••••••

Copyright(c) 2006 - 2020 Cisco Systems, Inc. All rights reserved.

在ISE TACACS即時日誌上可以驗證登入嘗試是否成功



Refresh: Every 3 seconds

Show: Latest 20 records

Within: Last 3 hours

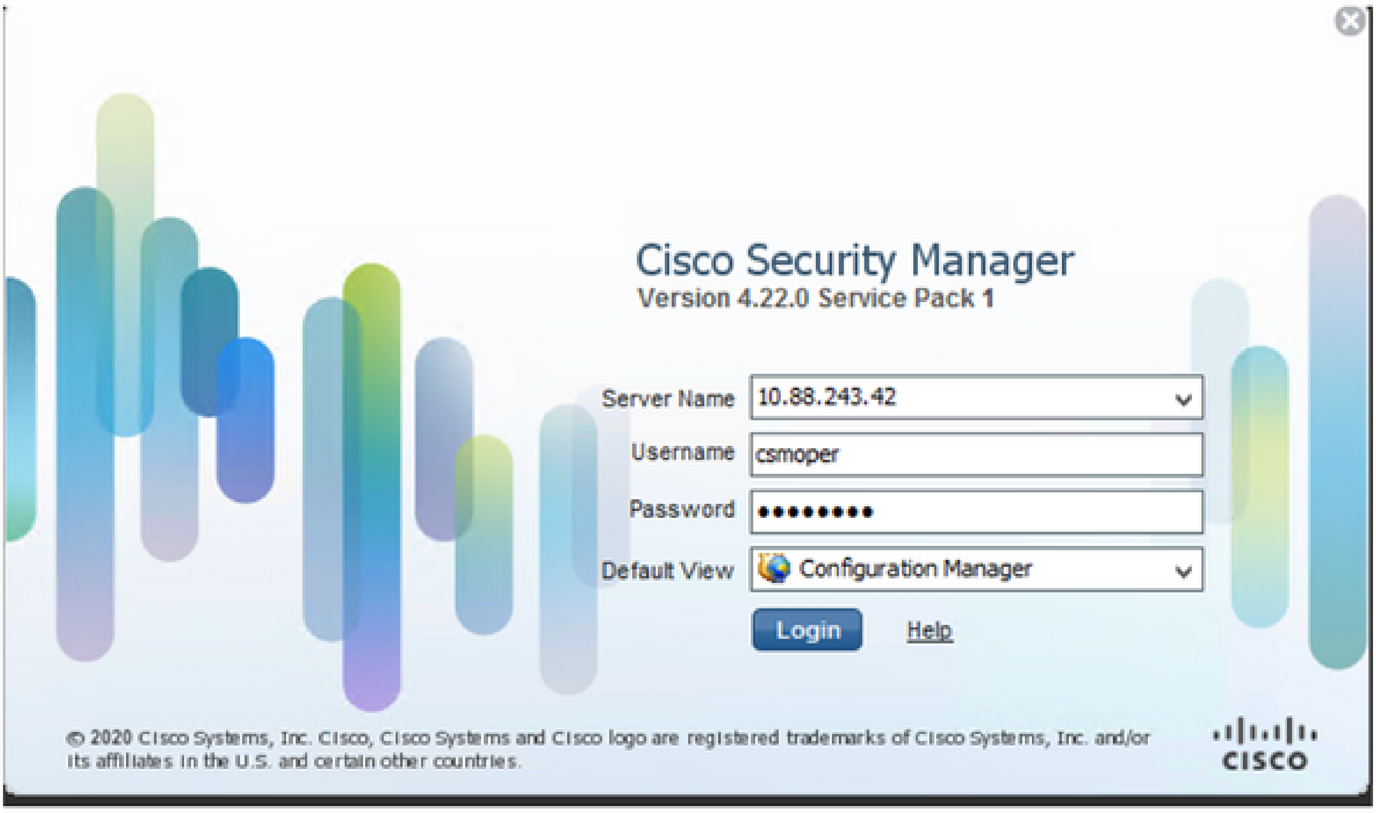
Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic.
Apr 17, 2021 02:34:54.1...	✓		csmadmin	Authentic...	CSM 4.22 >> Default		ise30	CSM422

Last Updated: Sat Apr 17 2021 09:37:58 GMT-0500 (Central Daylight Time)

Records Shown: 1

思科安全管理員使用者端應用程式

步驟1.使用服務檯管理員帳戶登入到思科安全管理器客戶端應用程式。

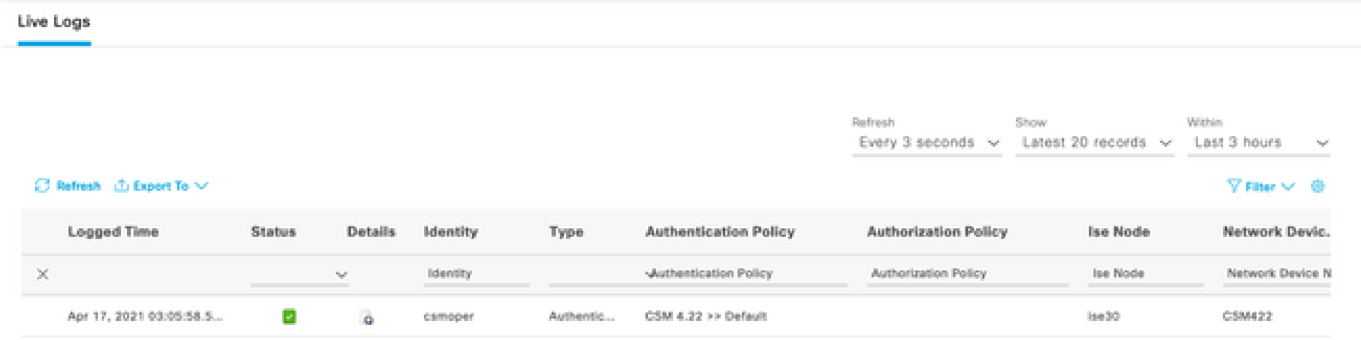


Cisco Security Manager
Version 4.22.0 Service Pack 1

Server Name: 10.88.243.42
Username: csmoper
Password: ●●●●●●●●●
Default View: Configuration Manager

Login
Help
© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
cisco

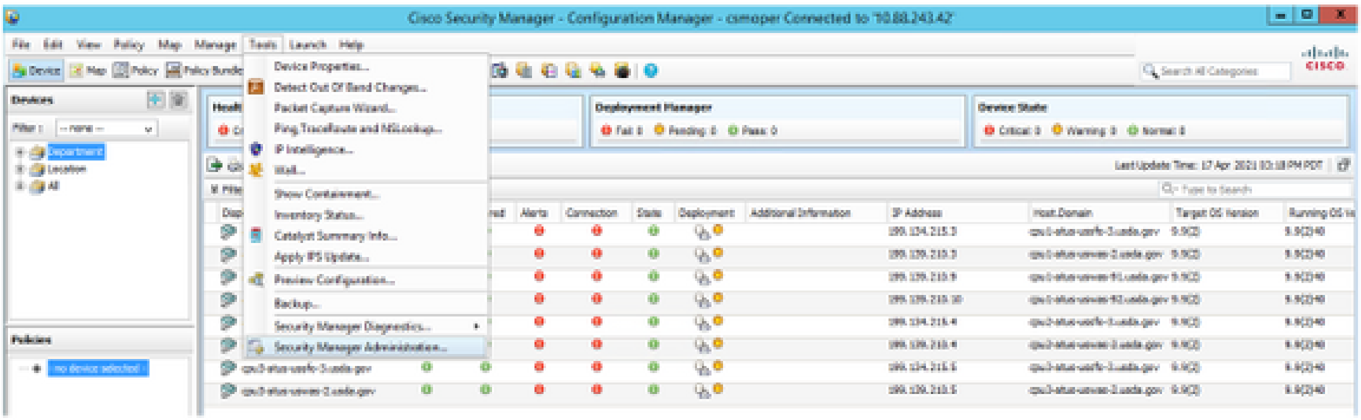
在ISE TACACS即時日誌上可以驗證登入嘗試是否成功

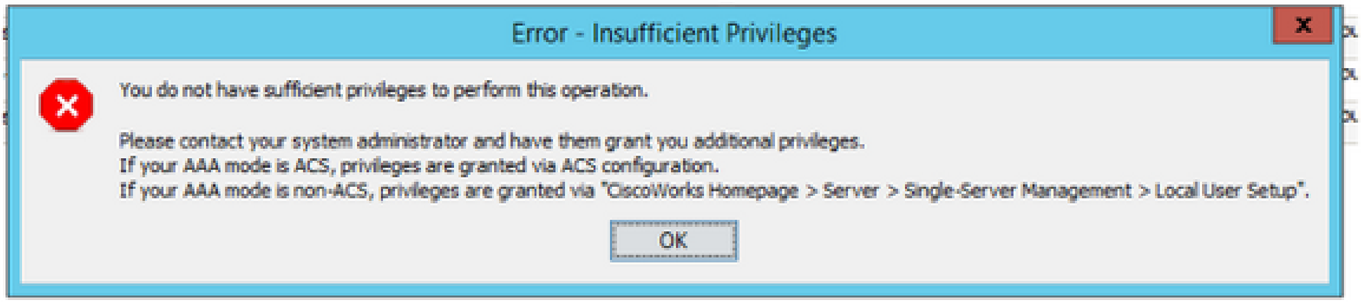


Refresh: Every 3 seconds
Show: Latest 20 records
Within: Last 3 hours

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic..
Apr 17, 2021 03:05:58.5...	✓		csmoper	Authentic...	CSM 4.22 >> Default		ise30	CSM422

步驟2.從CSM客戶端應用程式選單中選擇**「工具」>「安全管理**器管理」，將顯示一條錯誤消息，指示必須缺少許可權。





Error - Insufficient Privileges

You do not have sufficient privileges to perform this operation.

Please contact your system administrator and have them grant you additional privileges.
If your AAA mode is ACS, privileges are granted via ACS configuration.
If your AAA mode is non-ACS, privileges are granted via "CiscoWorks Homepage > Server > Single-Server Management > Local User Setup".

OK

步驟3.使用csmadmin帳戶重複**步驟1**到3，以驗證已為此使用者提供了正確的許可權。

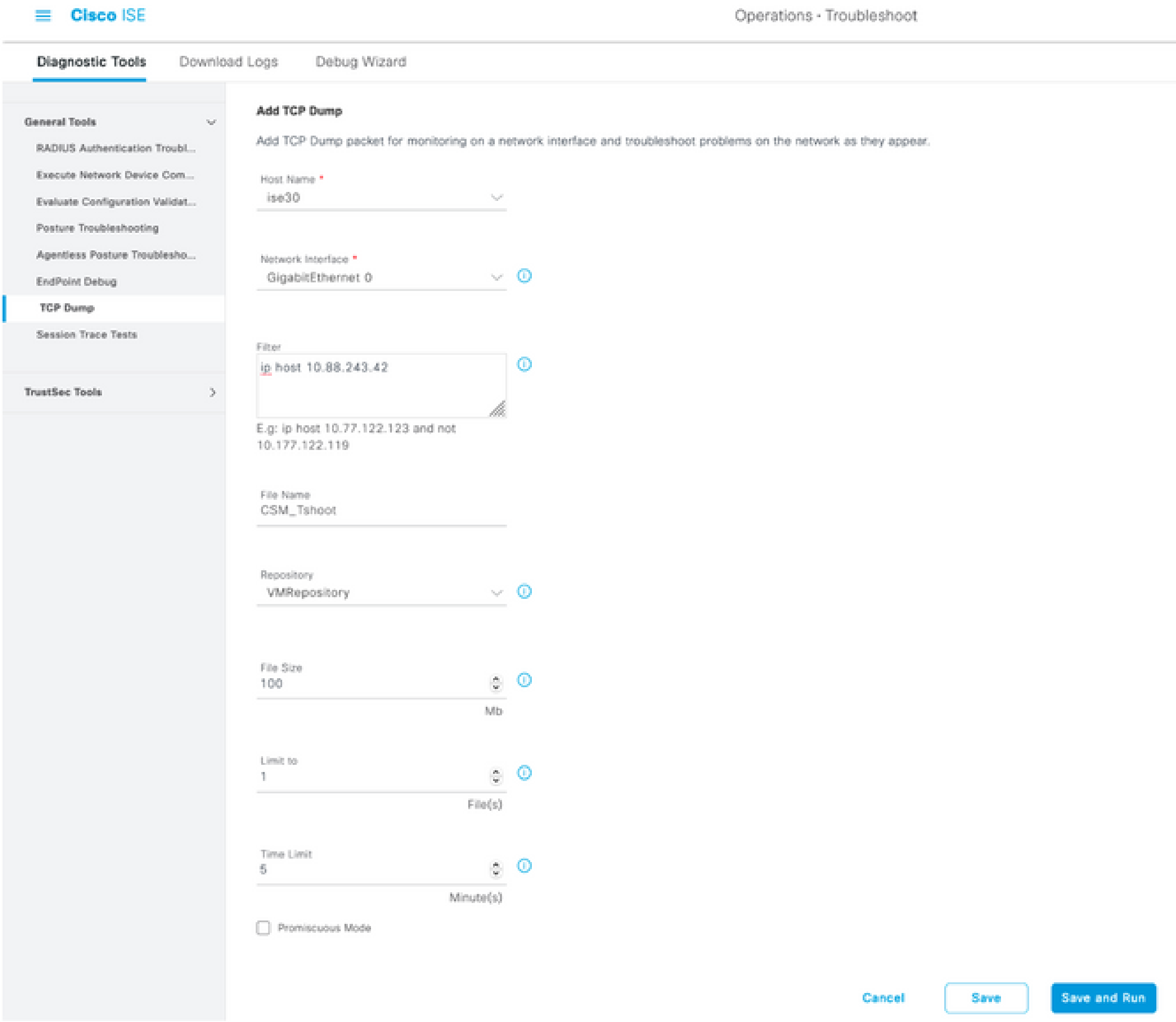
疑難排解

本節提供的資訊用於對組態進行疑難排解。

通過ISE上的TCP轉儲工具進行通訊驗證

步驟1.登入ISE並導航到位於左上角的三行圖示並選擇**操作>故障排除>診斷工具。**

步驟2. 在**General tools 下，選擇TCP Dumps ，然後選擇Add+。**選擇Hostname 、 Network Interface File Name 、 Repository ，也可以選擇過濾器以僅收集CSM IP地址通訊流。選擇**儲存並運行**



Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name * ise30

Network Interface * GigabitEthernet 0

Filter ip host 10.88.243.42

E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name CSM_Tshoot

Repository VMRepository

File Size 100 Mb

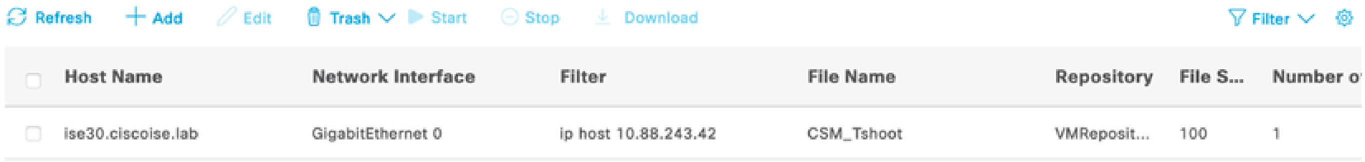
Limit to 1 File(s)

Time Limit 5 Minute(s)

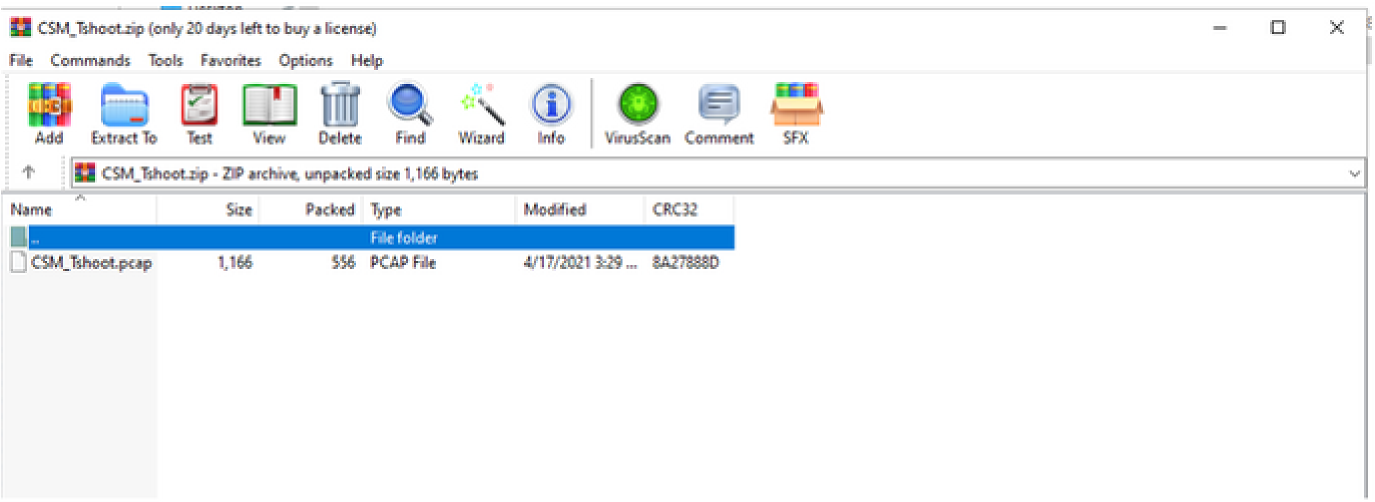
□ Promiscuous Mode

步驟3.登入CSM客戶端應用程式或客戶端UI並鍵入管理員憑據。

步驟4.在ISE上，選擇**停止**按鈕並驗證pcap檔案已傳送到定義的儲存庫。



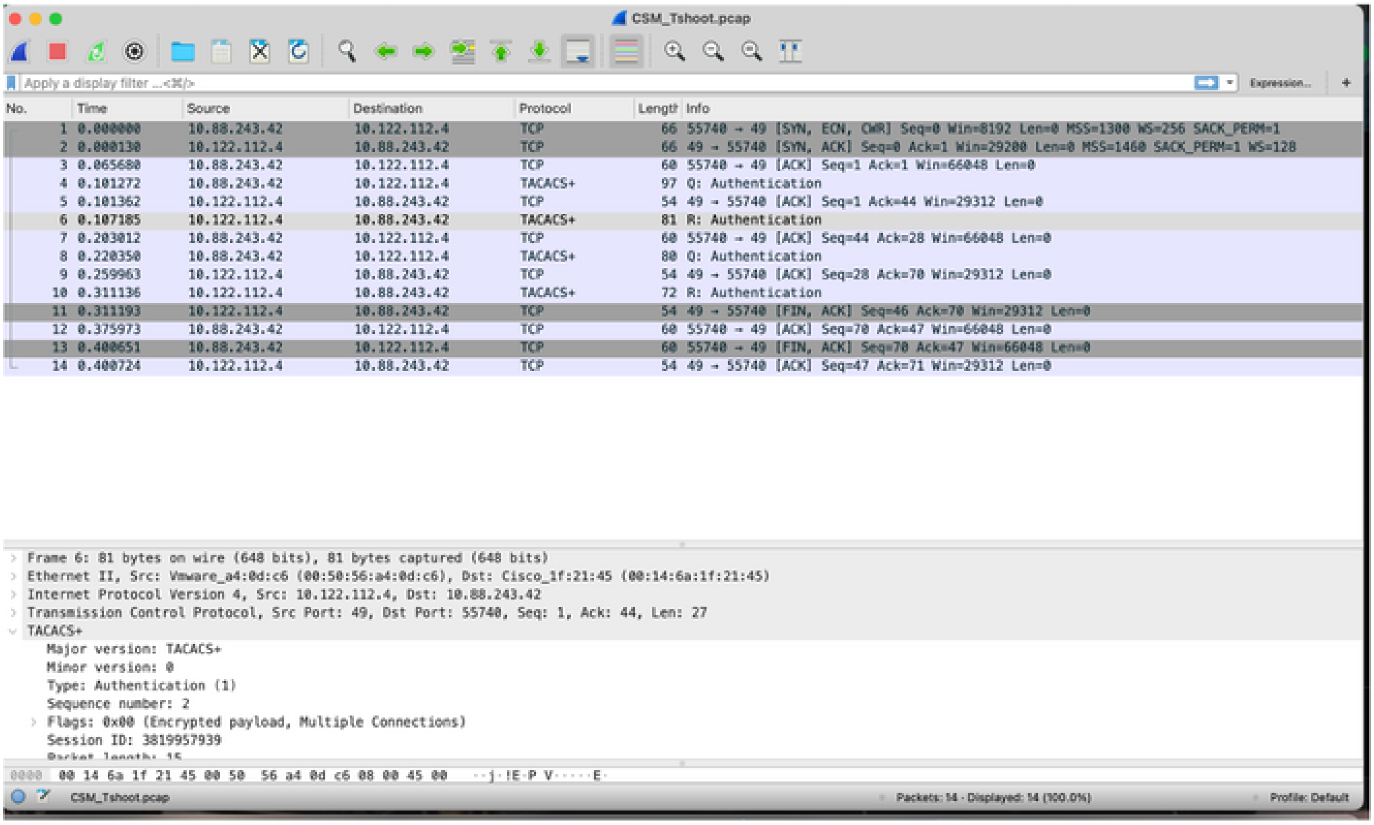
□	Host Name	Network Interface	Filter	File Name	Repository	File S...	Number o
□	ise30.ciscoise.lab	GigabitEthernet 0	ip host 10.88.243.42	CSM_Tshoot	VMReposit...	100	1



CSM_Tshoot.zip - ZIP archive, unpacked size 1,166 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
CSM_Tshoot.pcap	1,166	556	PCAP File	4/17/2021 3:29 ...	8A27888D

步驟5.開啟pcap檔案驗證CSM和ISE之間的成功通訊。



```
No.  Time      Source          Destination     Protocol  Length Info
   1 0.000000  10.88.243.42    10.122.112.4    TCP       66 55740 → 49 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1300 WS=256 SACK_PERM=1
   2 0.000130  10.122.112.4    10.88.243.42    TCP       66 49 → 55740 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
   3 0.065680  10.88.243.42    10.122.112.4    TCP       60 55740 → 49 [ACK] Seq=1 Ack=1 Win=66048 Len=0
   4 0.101272  10.88.243.42    10.122.112.4    TACACS+   97 Q: Authentication
   5 0.101362  10.122.112.4    10.88.243.42    TCP       54 49 → 55740 [ACK] Seq=1 Ack=44 Win=29312 Len=0
   6 0.107185  10.122.112.4    10.88.243.42    TACACS+   81 R: Authentication
   7 0.203012  10.88.243.42    10.122.112.4    TCP       60 55740 → 49 [ACK] Seq=44 Ack=28 Win=66048 Len=0
   8 0.220350  10.88.243.42    10.122.112.4    TACACS+   80 Q: Authentication
   9 0.259963  10.122.112.4    10.88.243.42    TCP       54 49 → 55740 [ACK] Seq=28 Ack=70 Win=29312 Len=0
  10 0.311136  10.122.112.4    10.88.243.42    TACACS+   72 R: Authentication
  11 0.311193  10.122.112.4    10.88.243.42    TCP       54 49 → 55740 [FIN, ACK] Seq=46 Ack=70 Win=29312 Len=0
  12 0.375973  10.88.243.42    10.122.112.4    TCP       60 55740 → 49 [ACK] Seq=70 Ack=47 Win=66048 Len=0
  13 0.400651  10.88.243.42    10.122.112.4    TCP       60 55740 → 49 [FIN, ACK] Seq=70 Ack=47 Win=66048 Len=0
  14 0.400724  10.122.112.4    10.88.243.42    TCP       54 49 → 55740 [ACK] Seq=47 Ack=71 Win=29312 Len=0
```

```
> Frame 6: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
> Ethernet II, Src: Vmware_a4:0d:c6 (00:50:56:a4:0d:c6), Dst: Cisco_1f:21:45 (00:14:6a:1f:21:45)
> Internet Protocol Version 4, Src: 10.122.112.4, Dst: 10.88.243.42
> Transmission Control Protocol, Src Port: 49, Dst Port: 55740, Seq: 1, Ack: 44, Len: 27
v TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authentication (1)
    Sequence number: 2
  > Flags: 0x00 (Encrypted payload, Multiple Connections)
    Session ID: 3819957939
    Packet length: 15
```

```
0000  00 14 6a 1f 21 45 00 50  56 a4 0d c6 08 00 45 00   ··j·!E·P V·····E·
```

CSM_Tshoot.pcap   Packets: 14 · Displayed: 14 (100.0%)   Profile: Default

如果在pcap檔案中未顯示任何條目，則驗證以下內容：

1. 在ISE節點上啟用裝置管理服務
2. 在CSM配置中新增了正確的ISE IP地址
3. 如果防火牆位於中間，驗證允許連線埠49(TACACS)。