

使用Web使用者介面配置Catalyst 1300中的授權更改

目標

本文的目的是顯示如何使用Web使用者介面(UI)在Catalyst 1300交換機中配置授權更改 (CoA)。

適用裝置和軟體版本

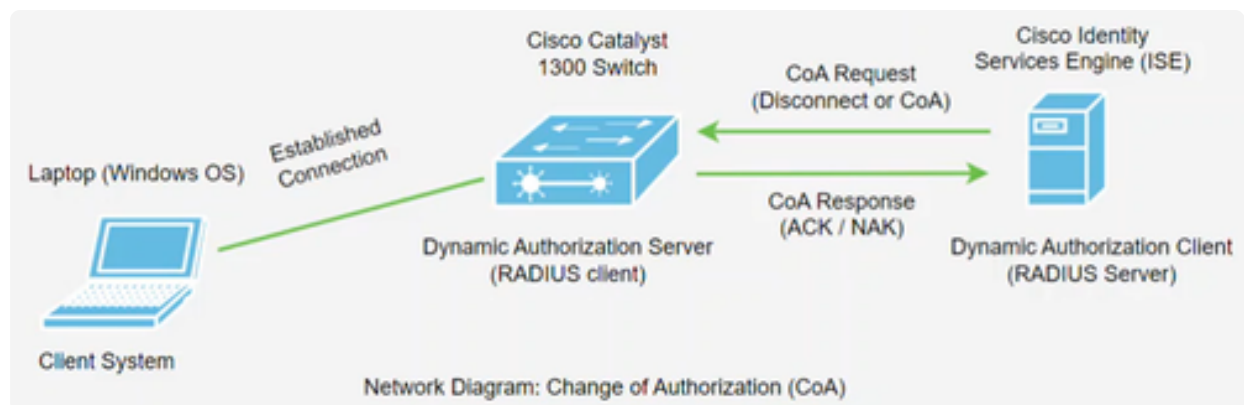
- Catalyst 1300交換器 | 4.1.6.53

簡介

授權變更(CoA)是RADIUS通訊協定的延伸，允許您變更驗證、授權及計量(AAA)或dot1x使用者作業階段的屬性（經過驗證）。當AAA中使用者或組的策略發生更改時，管理員可以從AAA伺服器(例如思科身份服務引擎(ISE))傳輸RADIUS CoA資料包，以重新初始化身份驗證並應用新策略。

思科身份服務引擎（或ISE）是一個功能全面的基於網路的訪問控制和策略實施引擎。其提供安全分析和執行、RADIUS和TACACS服務、原則發佈等。Cisco ISE是目前唯一支援Catalyst 1300交換機的CoA動態授權客戶端。有關詳細資訊，請參閱[ISE管理員指南](#)。

此功能需要動態授權使用者端（RADIUS伺服器）和動態授權伺服器（Catalyst交換器）之間的通訊。如下面的網路圖所示，動態授權伺服器向動態授權客戶端傳送斷開連線或CoA消息，交換機提供響應。



CoA支援已新增到韌體版本4.1.3.36中的Catalyst 1300交換機。這包括支援斷開使用者連線以及更改適用於使用者會話的授權。裝置支援以下CoA操作：

- 斷開會話
- 禁用主機埠CoA命令
- 退回主機埠CoA命令
- 重新驗證主機CoA命令

要使用命令列介面(CLI)配置CoA，請參閱[使用CLI在Catalyst 1300交換機中配置授權更改](#)。

目錄

- [在ISE上配置Catalyst 1300 RADIUS客戶端](#)
- [Catalyst 1300交換器中的設定](#)
- [CoA操作](#)

在ISE上配置Catalyst 1300 RADIUS客戶端

在本示例中，使用Cisco ISE伺服器版本3.2。有關ISE的概述，請檢視[Cisco Identity Services Engine產品](#)頁面。

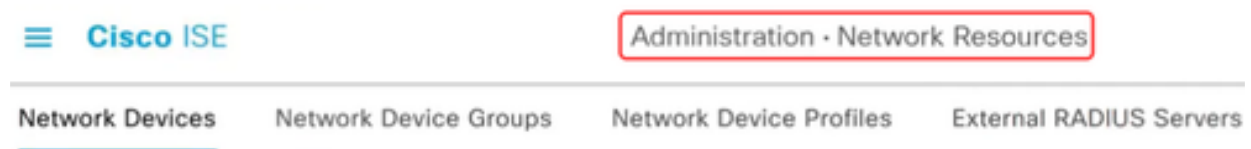
Note:

ISE版本2.7及更高版本支援CoA。

部署Cisco ISE伺服器後，登入以訪問Web UI。

步驟 1

要新增網路裝置，請導航到管理>網路資源選單。



步驟 2

按一下+ Add按鈕。

Network Devices



步驟 3

輸入Catalyst交換器的名稱、說明和IP地址。

Network Devices

Name	C1300-24FP	1	
Description	Catalyst 1300 switch	2	
IP Address	* IP :	172.19.1.250 / 32	3

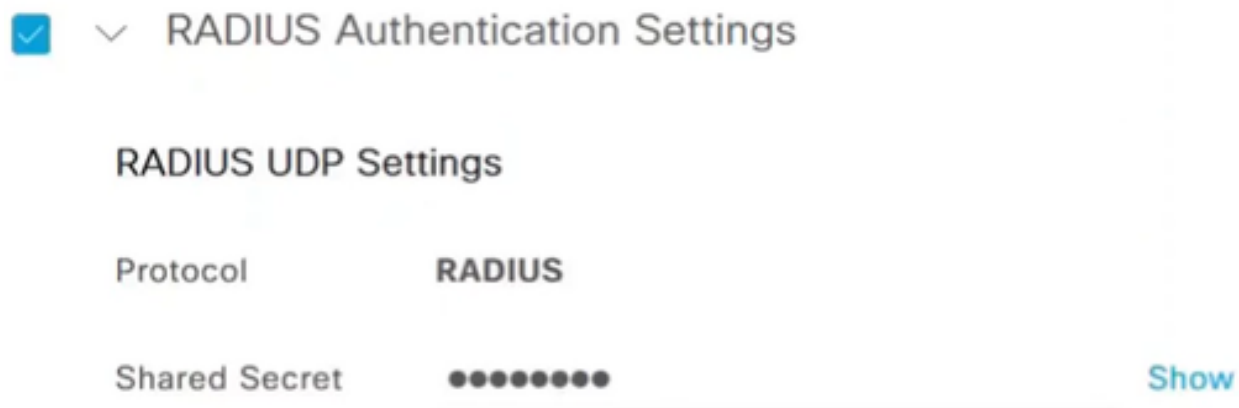
步驟 4

從Device Profile下拉選單中選擇Cisco。

Device Profile	Cisco	▼	i
----------------	-------	---	---

步驟 5

輸入Shared Secret配置RADIUS身份驗證設定。



☒ **RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol	RADIUS
Shared Secret	●●●●●●●● Show

步驟 6

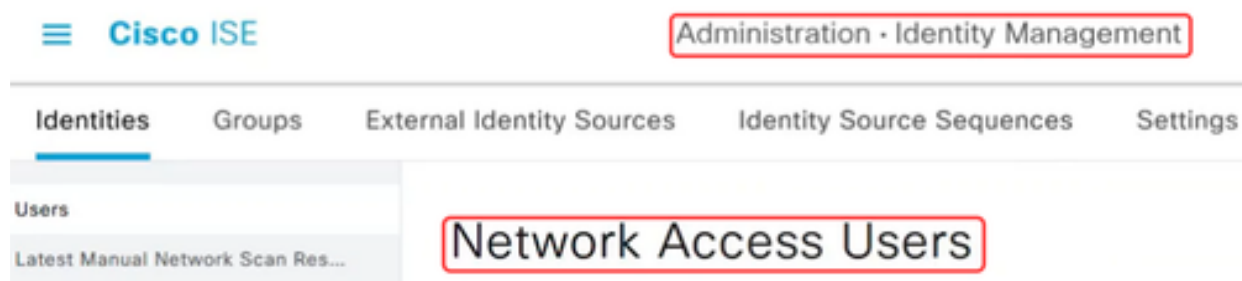
輸入CoA埠號。預設連線埠為1700。



CoA Port	1700 Set To Default
----------	-------------------------------------

步驟 7

接下來，導航到Administration > Identity Management，然後選擇Network Access Users。



Cisco ISE Administration · Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

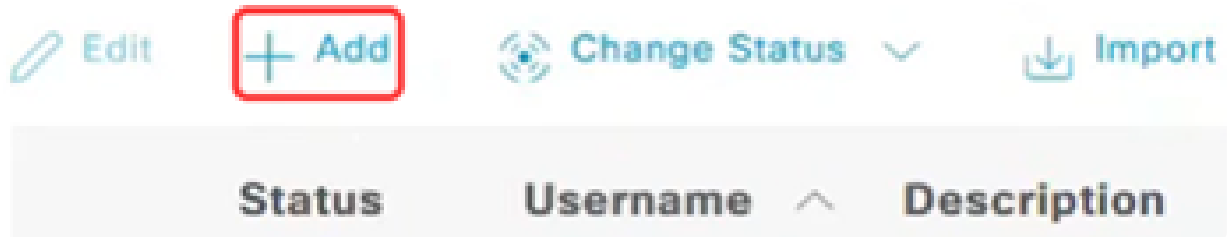
Users
Latest Manual Network Scan Res...

Network Access Users

步驟 8

要定義使用者名稱和密碼，請按一下+Add符號。

Network Access Users



步驟 9

輸入使用者名稱和密碼，然後按一下頁面底部的Save。

Network Access User

* Username

test1

Status

☒ Enabled

Catalyst 1300交換器中的設定

步驟 1

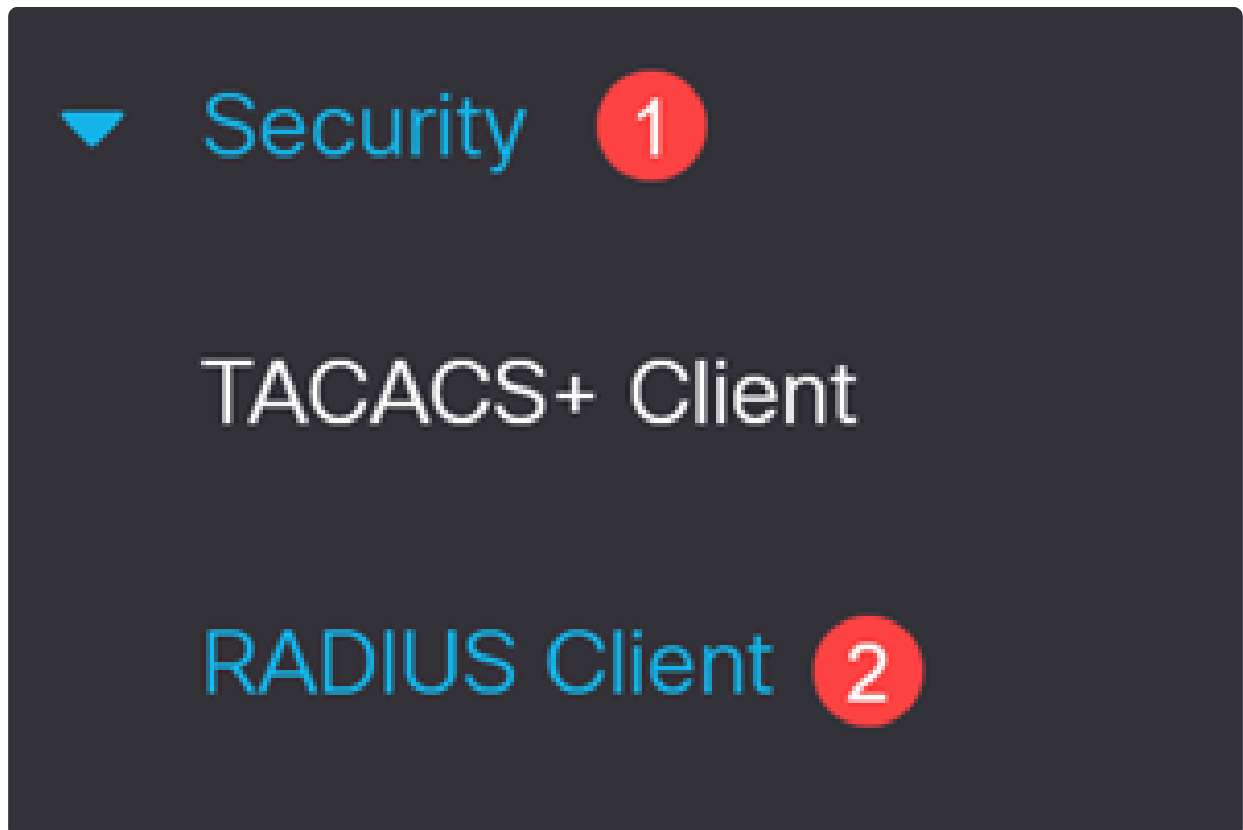
登入Catalyst 1300交換器並選擇Advanced模式。本範例中使用的是C1300-24FP-4X。

Note:

CoA支援已新增到韌體版本4.1.3.36中的Catalyst 1300交換機。

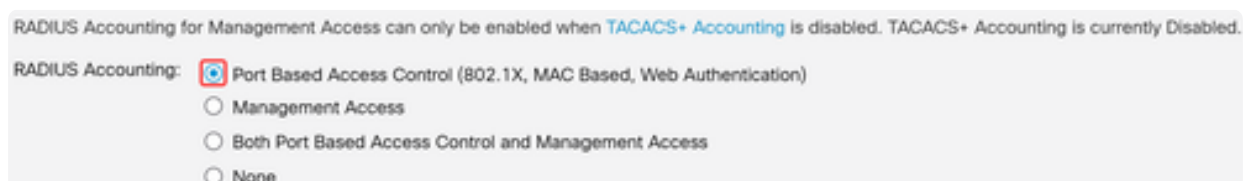
步驟 2

導覽至導覽窗格中的Security > RADIUS Client。



步驟 3

將RADIUS Accounting設定為Port Based Access Control。



步驟 4

要新增ISE伺服器，向下滾動到RADIUS表，然後按一下plus圖示。

步驟 5

配置RADIUS伺服器設定。

- 選擇伺服器定義。在此示例中，By IP address處於選中狀態。在Server IP Address/Name 欄位中輸入IP地址。
- 設定RADIUS優先順序。
- 身份驗證和記帳埠設定為預設值。
- 使用類型為802.1x。

按一下「Apply」。

Add RADIUS Server

Server Definition:	☒ By IP address ☐ By name
IP Version:	☐ Version 6 ☒ Version 4
IPv6 Address Type:	☒ Link Local ☐ Global
Link Local Interface:	VLAN 1
Server IP Address/Name:	192.168.251.100 1
Priority:	1 (Range: 0 - 65535) 2
Key String:	☒ Use Default ☐ User Defined (Encrypted) ☐ User Defined (Plaintext) (0/128 characters used)
Timeout for Reply:	☒ Use Default ☐ User Defined Default sec (Range: 1 - 30, Default: 3)
Authentication Port:	1812 (Range: 0 - 65535, Default: 1812) 3
Accounting Port:	1813 (Range: 0 - 65535, Default: 1813)

步驟 6

要配置802.1x身份驗證，請導航至安全> 802.1X身份驗證>「屬性」選單。

▼ 802.1X Authentication

Properties

步驟 7

確保Port-Based Authentication已啟用，且Authentication Method已設定為RADIUS。

Properties

Port-Based Authentication:

☒ Enable

Authentication Method:

☐ RADIUS, None

☒ RADIUS

☐ None

步驟 8

導航到Port Authentication選單，選擇所需的埠，然後按一下edit。

▼ 802.1X Authentication

Properties

Port Authentication

步驟 9

對於Administrative Port Control，選擇Auto選項，該選項將根據RADIUS響應在授權和未經授權的狀態之間切換埠。

Edit Port Authentication

Interface:

Unit

1 ▼

Port

GE4 ▼

Current Port Control:

Authorized

Administrative Port Control:

☐ Force Unauthorized

☒ Auto

☐ Force Authorized

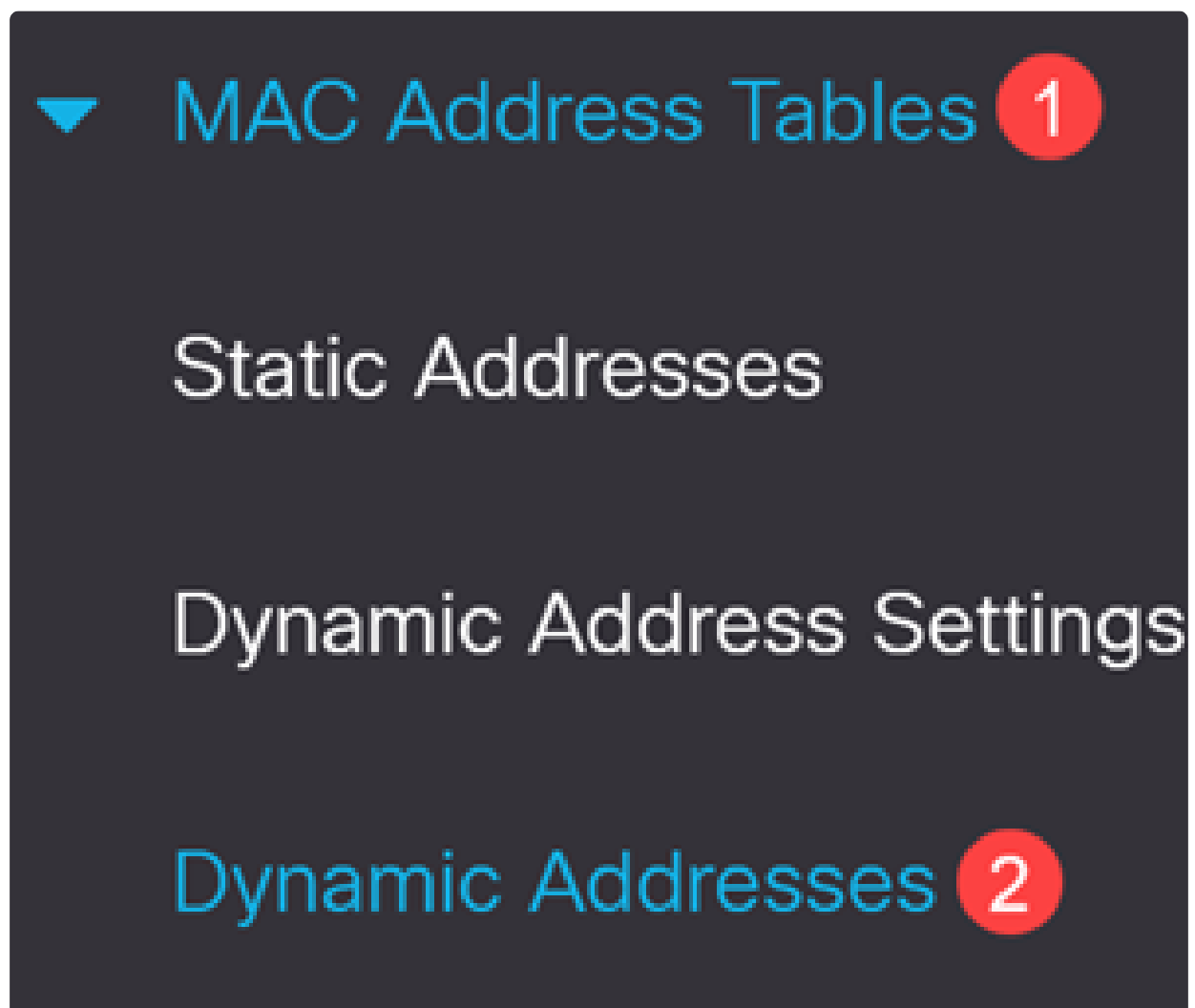
步驟 10

啟用802.1x Based Authentication，然後按一下Apply。

802.1x Based Authentication: ☒ Enable

步驟 11

您將需要埠上裝置的MAC地址。ISE上的CoA操作將應用到該MAC地址。在本例中，它是埠9。要獲取該埠，請導航到MAC地址表>動態地址。

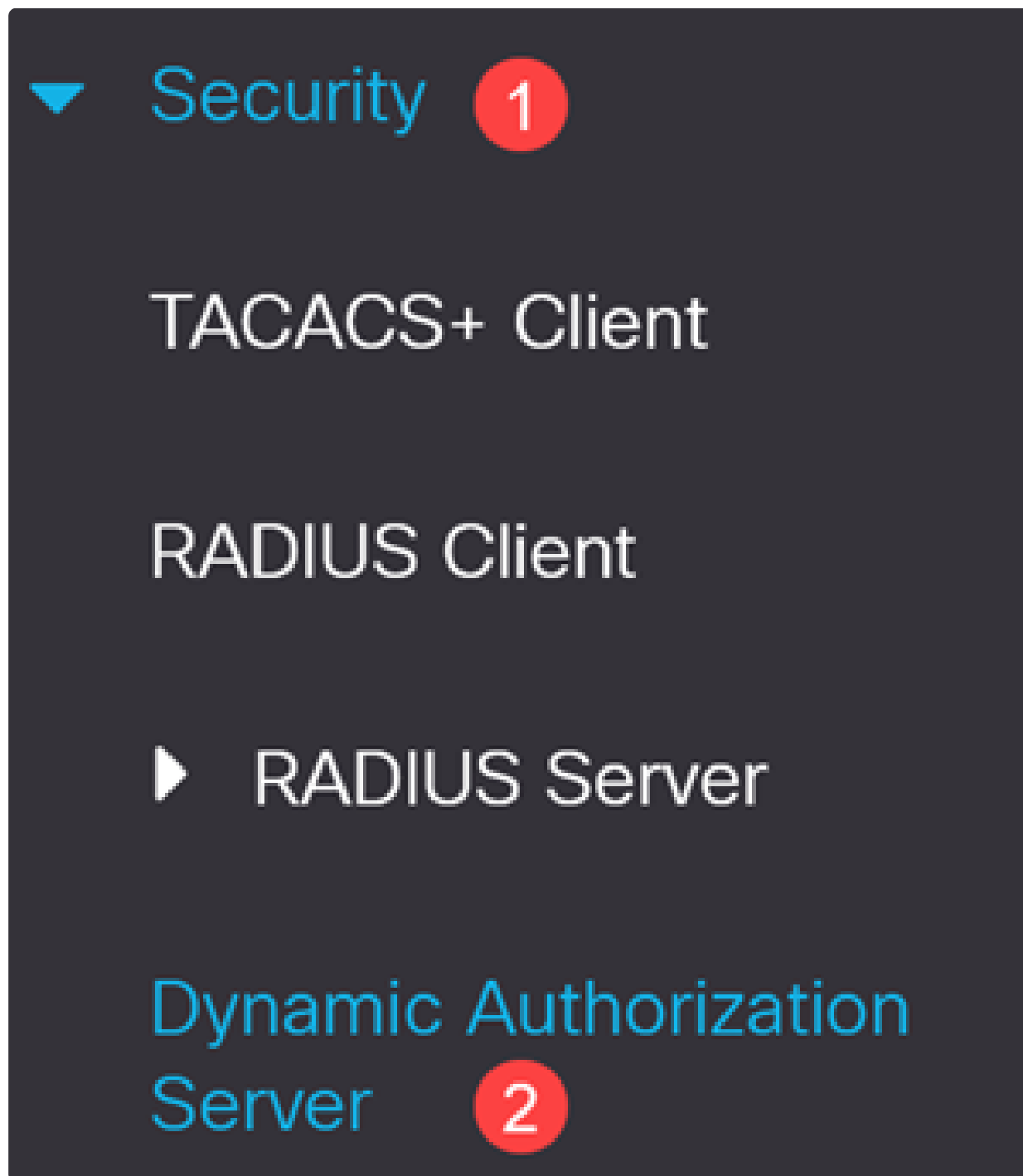


步驟 12

向下滾動到埠並記下MAC地址。

步驟 13

導覽至Security > Dynamic Authorization Server。



步驟 14

啟用以下功能：

- 強制伺服器金鑰匹配

- 在Rx上強制時間戳
- 處理禁用埠命令
- 處理退回埠命令

Dynamic Authorization Server

Enforce Server Key Match: ☒ Enable

Enforce Timestamp on Rx: ☒ Enable

Handle Disable Port Commands: ☒ Enable

Handle Bounce Port Commands: ☒ Enable

步驟 15

將UDP Port保留為預設值1700。

UDP Port: (Range: 0 - 59999, Default: 1700)

步驟 16

在客戶端表下，確保使用正確的伺服器金鑰新增ISE伺服器。按一下「Apply」。

Client Table



Counters

☐	Client Address	Server Key MD5
☐	192.168.1.115	121a6

步驟 17

按一下紅色閃爍的Save圖示以儲存配置。



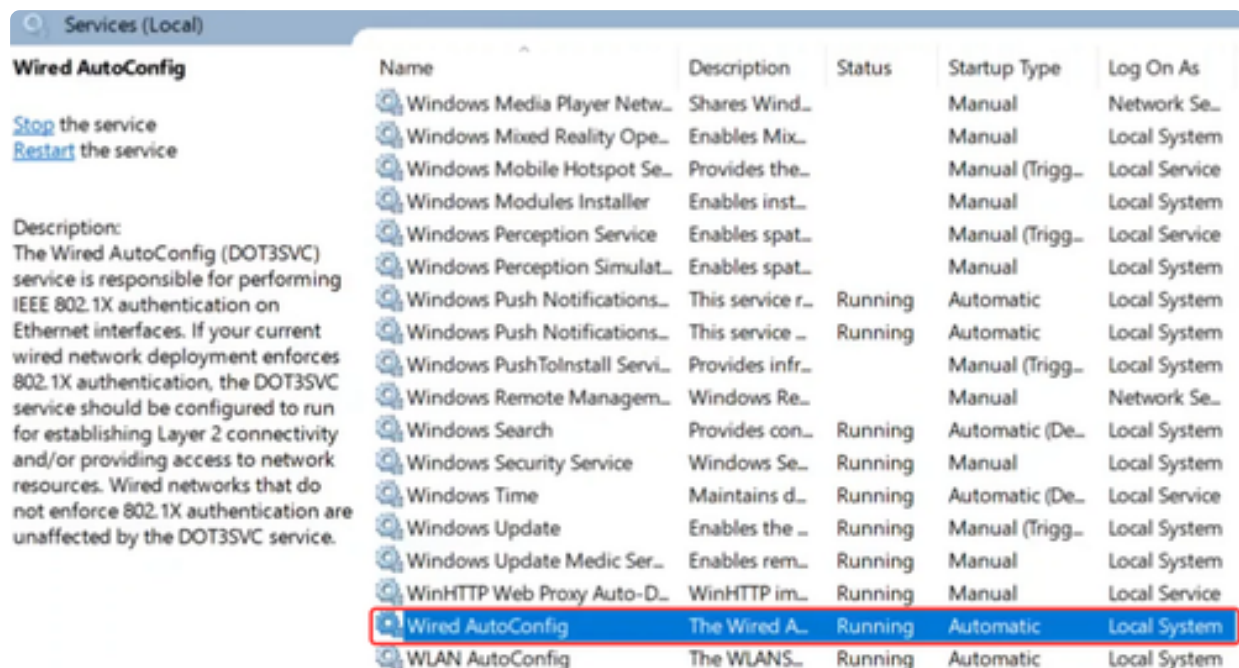
ciscolab

English



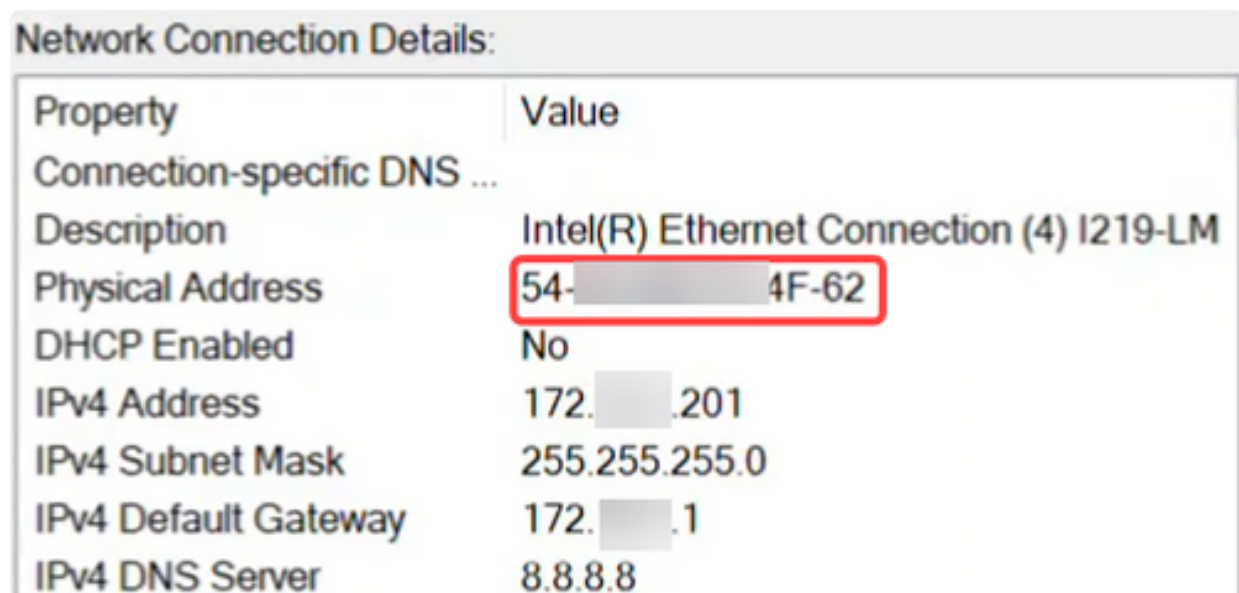
步驟 18

在連線到埠9的客戶端筆記型電腦上，驗證是否已為802.1 X身份驗證啟用有線自動配置服務。



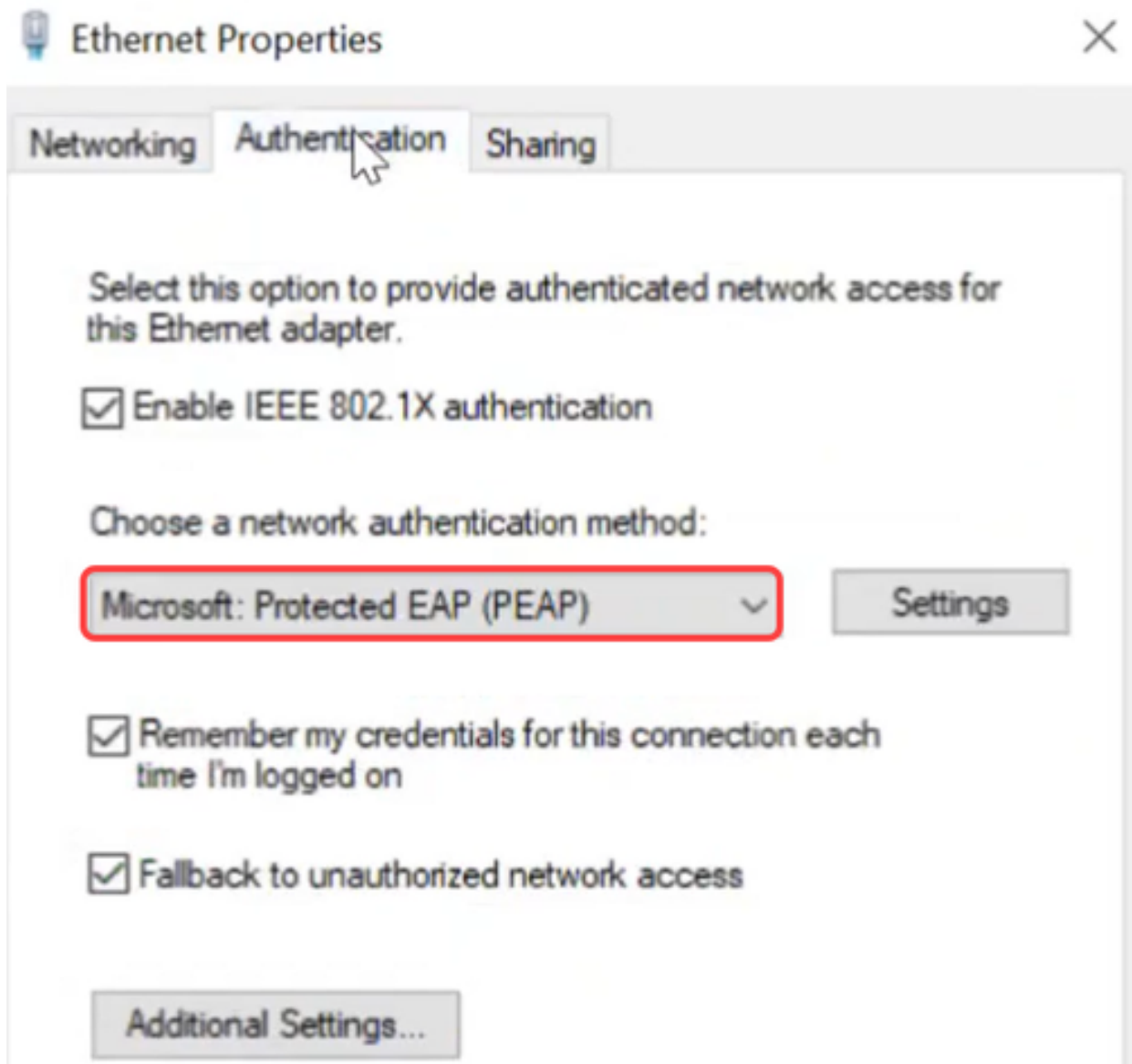
步驟 19

在Ethernet介面卡設定上，驗證MAC地址是否匹配。



步驟 20

按一下Ethernet settings下的Properties按鈕，然後按一下Authentication頁籤下的Properties按鈕，確保覈取方塊處於啟用狀態。此外，請確保身份驗證方法是受保護的EAP(PEAP)。



步驟 21

按一下Settings按鈕以確保取消選中Verify the server's identity by validating the certificate旁邊的覈取方塊。



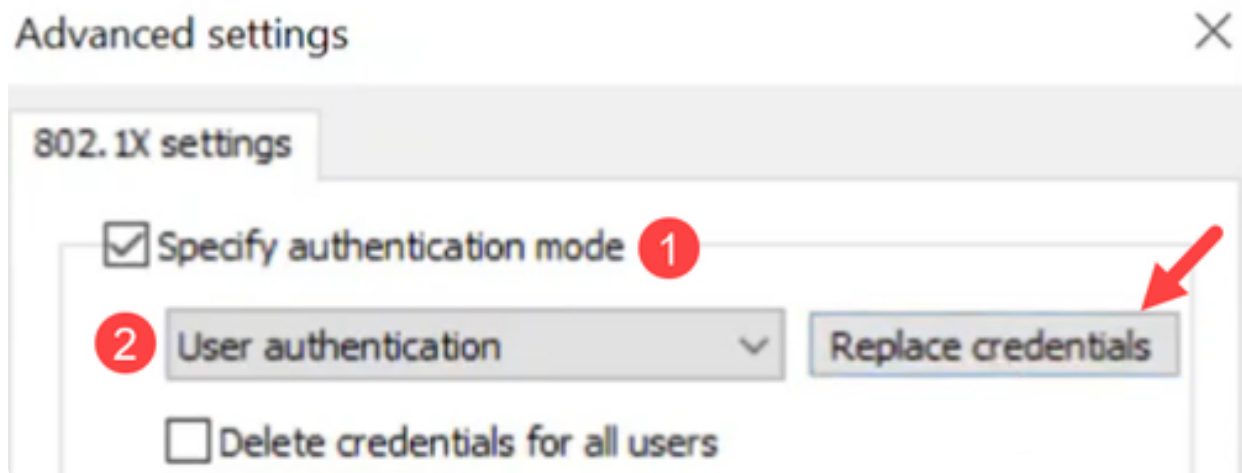
步驟 22

應選中Enable Fast Reconnect (啟用快速重新連線) 框。



步驟 23

在「Additional settings (其他設定)」下，確保Specify authentication mode已啟用，並從下拉選單中選擇User authentication。您可以儲存在ISE上建立的憑據，或使用替換憑據按鈕替換它。



CoA操作

在啟動CoA操作之前，請在交換機上啟用資料包捕獲。

步驟 1

在PuTTY上，登入您的Catalyst交換機，使用命令monitor capture cap1 buffer size 20

circular指定緩衝區大小和捕獲模式。

步驟 2

使用命令`monitor capture cap1 control-plane both`將控制平面指定為both。

步驟 3

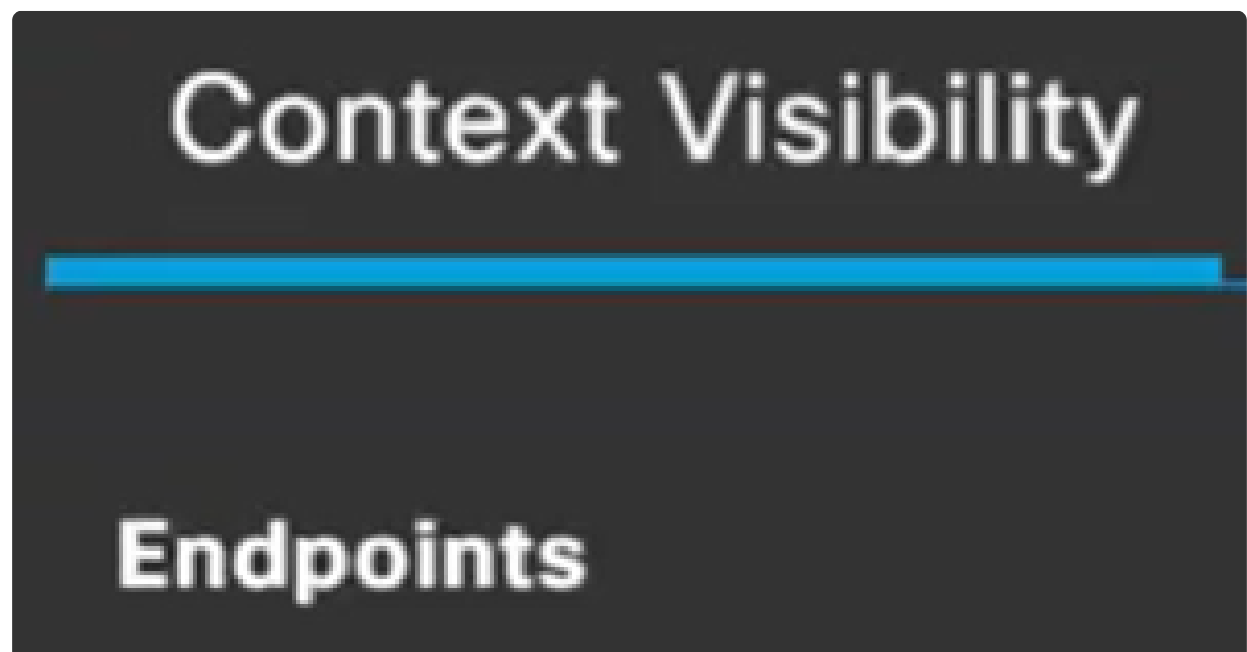
輸入任意匹配條件。此命令為`monitor capture cap1 match any`。

步驟 4

開始資料包捕獲。

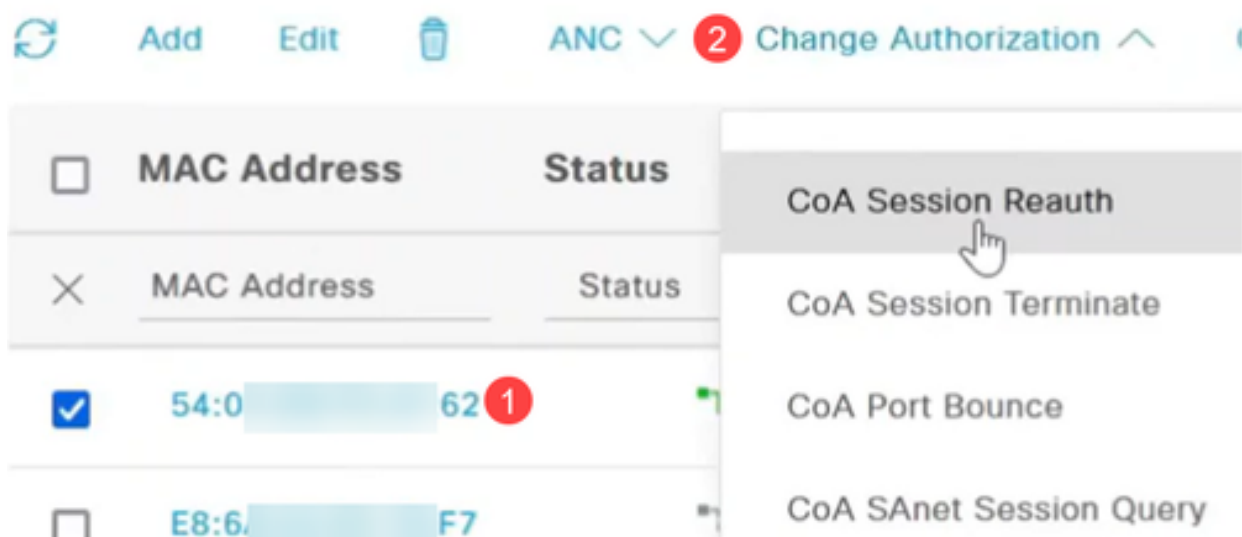
步驟 5

在ISE介面上，導航到情景可視性下的Endpoints選項。



步驟 6

選擇MAC地址，然後從Change of Authorization下拉選單中選擇CoA操作。在本範例中，選擇了CoA Session Reauth。這會透過使用reauthenticate命令傳送CoA封包在連線埠上強制重新驗證。



步驟 7

返回PuTTY終端檢查CoA操作是否成功。

```
Started capture point : cap1
Cat1300-1#04-Jul-2024 20:49:45 %SEC-W-COAREAUTHSESSN: 802.1x re-authentication initiated for host 5
4: 62 by CoA Request "reauthenticate"
```

步驟 8

如果您選擇CoA Session Terminate，它將根據管理請求傳送帶有終止命令的斷開連線請求。

```
Cat1300-1#04-Jul-2024 20:50:02 %SEC-W-PORTUNAUTHORIZED: Port gil/0/9 is unAuthorized
04-Jul-2024 20:50:02 %SEC-W-COADISCSESSN: 802.1x session for host 54: :62 on interface gi
1/0/9 has been terminated by Disconnect-Request. Authenticator state on the Interface will be re-in
itialized
04-Jul-2024 20:50:02 %SEC-I-PORTAUTHORIZED: Port gil/0/9 is Authorized
```

步驟 9

CoA Port Bounce選項將使用bounce host port命令傳送CoA請求資料包，從而禁用並重新啟用交換機上的埠。網路介面卡將離線10秒並變為未授權狀態。它將線上恢復、獲得授權並可轉發資料包。

```

Cat1300-1#04-Jul-2024 20:50:21 %SEC-W-COABNCEPORT: Interface gil/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54: :62
04-Jul-2024 20:50:21 %LINK-W-Down: gil/0/9
04-Jul-2024 20:50:34 %LINK-I-Up: gil/0/9
04-Jul-2024 20:50:34 %SEC-W-PORTUNAUTHORIZED: Port gil/0/9 is unauthorized
04-Jul-2024 20:50:36 %LINK-W-Down: gil/0/9
04-Jul-2024 20:50:39 %LINK-I-Up: gil/0/9
04-Jul-2024 20:50:39 %SEC-I-PORTAUTHORIZED: Port gil/0/9 is Authorized
Cat1300-1#04-Jul-2024 20:50:45 %STP-W-PORTSTATUS: gil/0/9: STP status Forwarding

```

步驟 10

使用埠退回的CoA會話終止將終止現有會話，退回埠10秒，並變為未授權狀態。然後，它返回聯機狀態，獲得授權並可轉發資料包。

```

Cat1300-1#04-Jul-2024 20:51:04 %SEC-W-COABNCEPORT: Interface gil/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54: :62
04-Jul-2024 20:51:04 %LINK-W-Down: gil/0/9
04-Jul-2024 20:51:22 %LINK-I-Up: gil/0/9
04-Jul-2024 20:51:22 %SEC-W-PORTUNAUTHORIZED: Port gil/0/9 is unauthorized
04-Jul-2024 20:51:22 %SEC-I-PORTAUTHORIZED: Port gil/0/9 is Authorized
04-Jul-2024 20:51:29 %STP-W-PORTSTATUS: gil/0/9: STP status Forwarding

```

步驟 11

使用埠關閉的CoA會話終止將終止會話並管理性關閉埠。

```

Cat1300-1#04-Jul-2024 20:51:47 %SEC-W-COADISPORT: Interface gil/0/9 suspended by CoA Request "disab
le host port" for host 54: :62
04-Jul-2024 20:51:47 %LINK-W-Down: gil/0/9

```

步驟 12

要停止資料包捕獲，請使用命令monitor capture cap1 stop。

步驟 13

要複製檔案，請導航到管理>檔案管理>檔案目錄。

▼ Administration 1

System Settings

Console Settings

Stack Management

Bluetooth Settings

User Accounts

Idle Session Timeout

▶ Time Settings

步驟 14

預設快閃記憶體可用。或者，您可以從Drive下拉選單中選擇USB。

File Directory

Auto Mirror Configuration: ☒ Enable

File Table



Free Space: 163144/305484 KB

Drive:

Flash 

Flash

USB

Go

☐	File Name	Permissions
☐	system	

結論

現在您已瞭解ISE以及如何在Catalyst 1300系列交換機中配置CoA。

有關詳細資訊，請檢視下面的影片。

觀看與本文相關的影片...

[按一下此處以觀看思科的技術演講](#)

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）。