Catalyst 1300交換器中的可下載ACL

目標

本文旨在說明可下載存取控制清單(DACL)在搭載Cisco Identity Service Engine(ISE)的Cisco Catalyst 1300交換器上如何運作。

適用裝置 | 軟體版本

- Catalyst 1300 系列 | 4.1.6.54

簡介

動態ACL是根據策略或條件（如使用者帳戶組成員資格、一天中的時間等）分配給交換機埠的ACL。它們可能是由filter-ID或可下載ACL(DACL)指定的本地ACL。

可下載ACL是從思科ISE伺服器建立和下載的動態ACL。它們根據使用者身份和裝置型別動態應用訪問控制規則。DACL的優點是允許您為ACL建立一個中央儲存庫，因此您無需在每個交換機上手動建立它們。當使用者連線到交換機時，他們只需要進行身份驗證，交換機將從思科ISE伺服器下載適用的ACL。

可下載ACL的使用案例

1. 不同的使用者在連線到交換機時將收到不同的ACL（本地ISE使用者）。
2. 網路連線受限的使用者可以登入中央Web門戶進行完全網路訪問（中央Web身份驗證）。
3. 高級 — 使用MAC Authentication Bypass(MAB)允許與Windows Active Directory(AD)和某些相關服務的通訊，同時將ISE伺服器連線到AD並監控使用者身份驗證。在Windows AD登入之前，網路將僅允許訪問非常有限的資源，但AD身份驗證將基於Windows組下載不同的ACL並允許完整的網路訪問。
4. 高級 — 由於ISE伺服器上的策略，使用者根據星期幾、一天中的時間或其他因素收到不同的ACL。

本文將對第一個用例進行詳細討論。

目錄

必要條件

- 確保Catalyst 1300交換機升級到最新韌體（交換機韌體應為4.1.6或更高版本）。
- 為交換機分配靜態IP以進行管理。

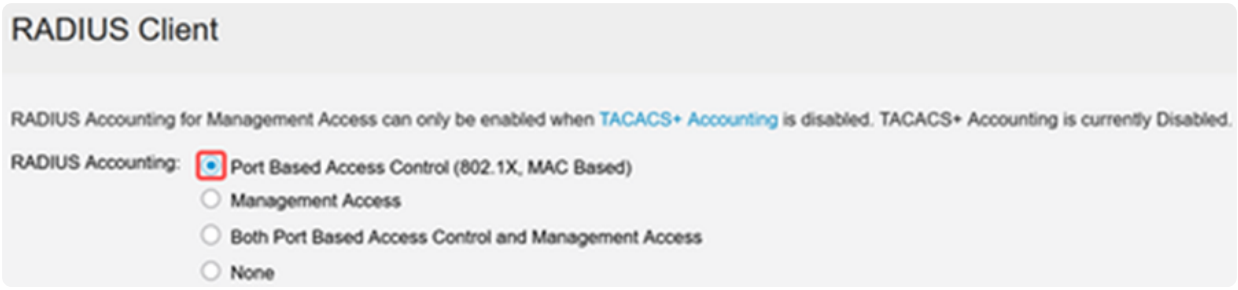
設定RADIUS使用者端

步驟 1

登入Catalyst 1300交換器，然後導覽至Security > RADIUS Client功能表。

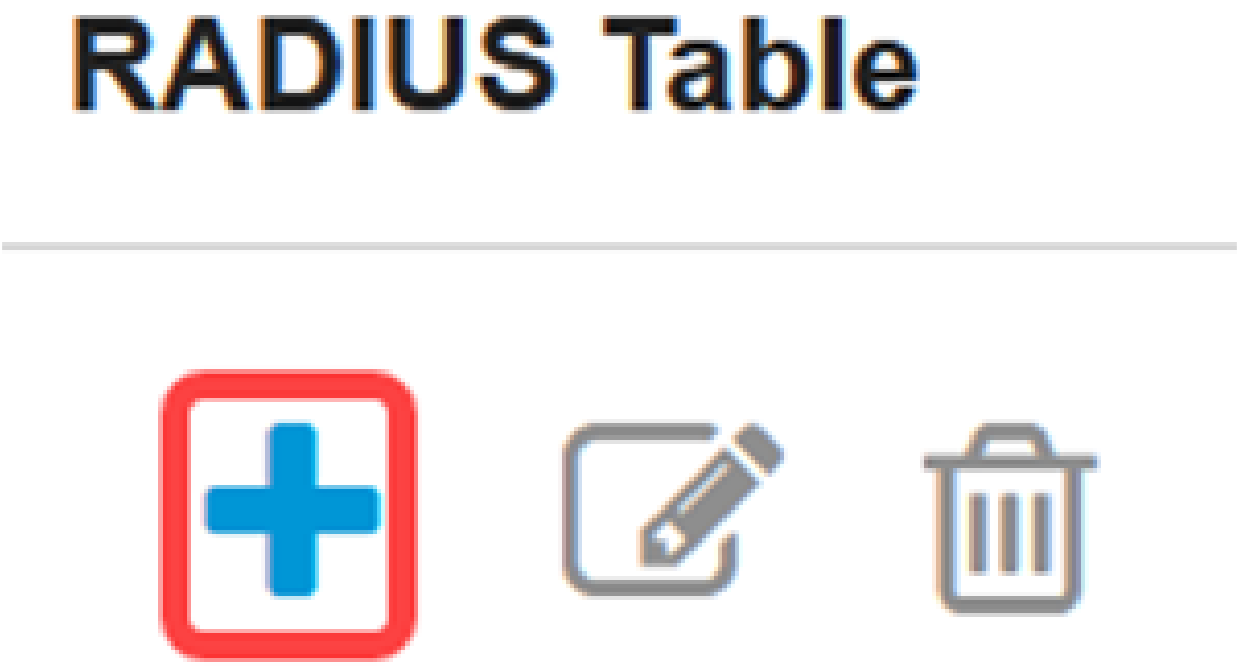
步驟 2

針對RADIUS記帳，選擇連線埠型存取控制選項。



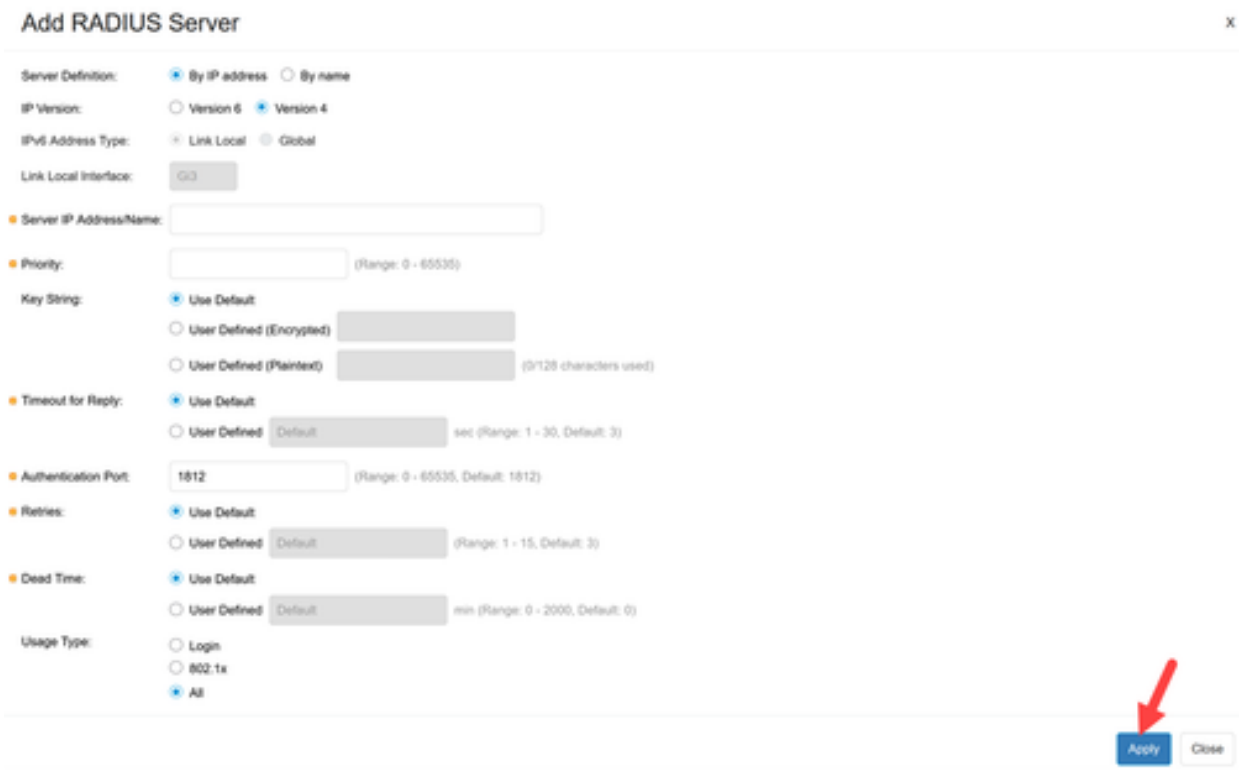
步驟 3

在RADIUS Table下，按一下plus圖示以新增Cisco ISE伺服器。



步驟 4

輸入思科ISE伺服器詳細資訊，然後按一下Apply。

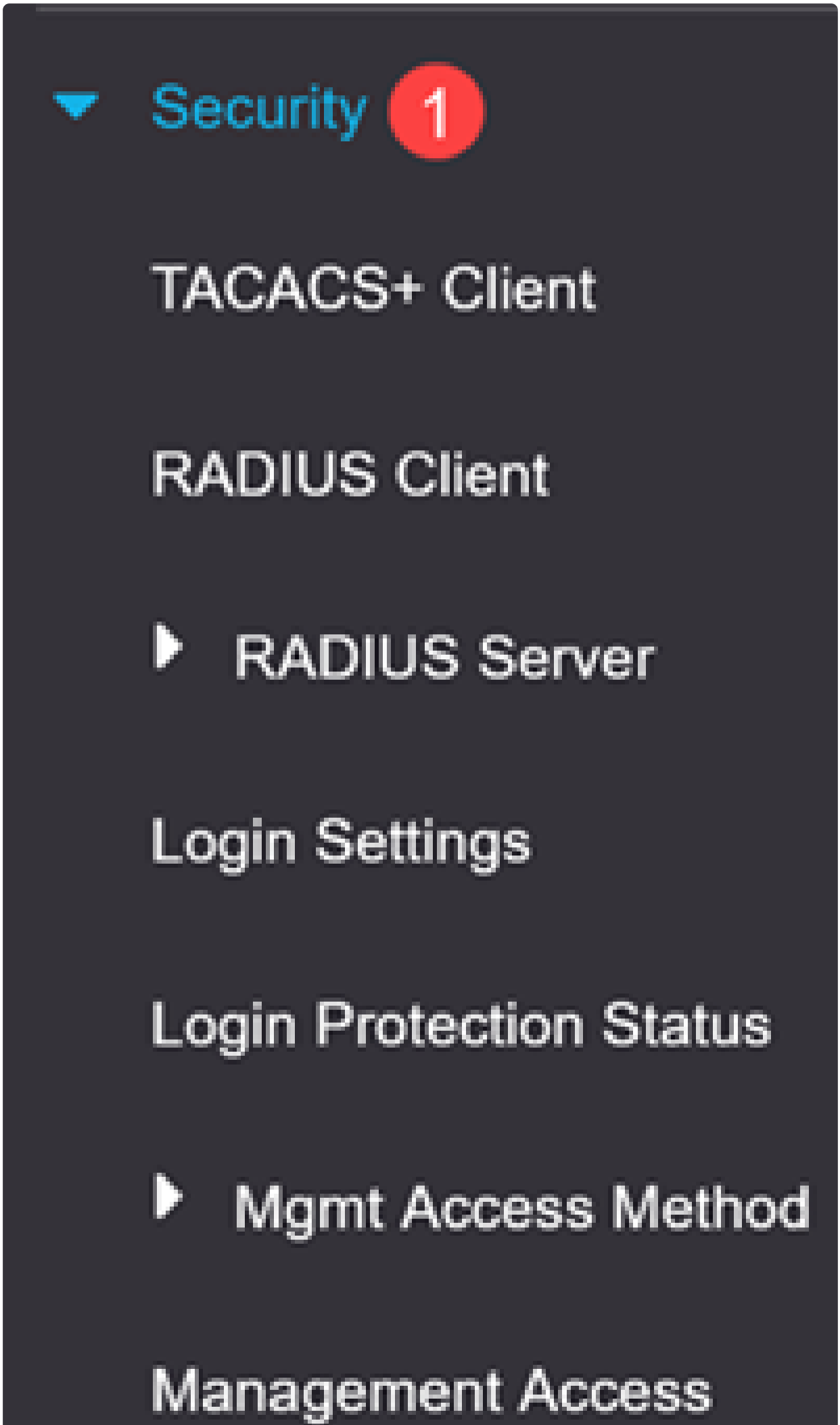


> **Note:**
> Usage Type必須選為802.1x。

配置802.1x身份驗證

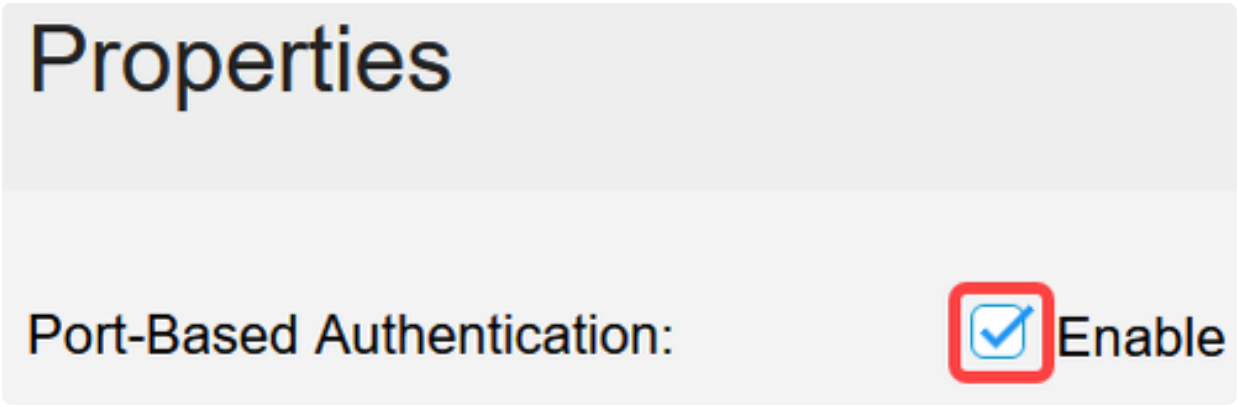
步驟 1

導航到Security > 802.1X Authentication > Properties選單。


Security 1
TACACS+ Client
RADIUS Client
RADIUS Server
Login Settings
Login Protection Status
Mgmt Access Method
Management Access

步驟 2

按一下覈取方塊以啟用基於埠的身份驗證。

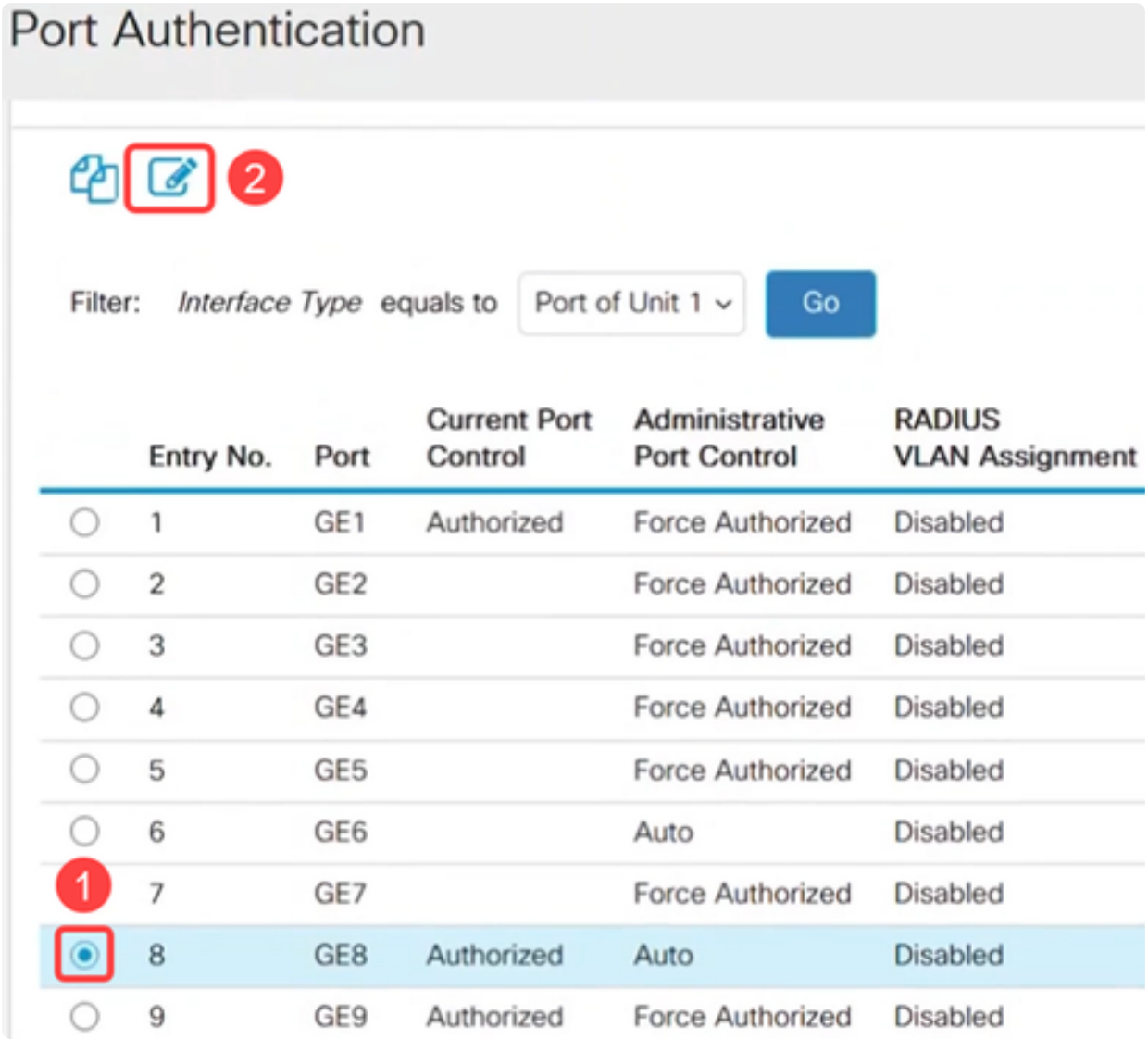


步驟 3

在Authentication Method下，選擇RADIUS，然後按一下Apply。

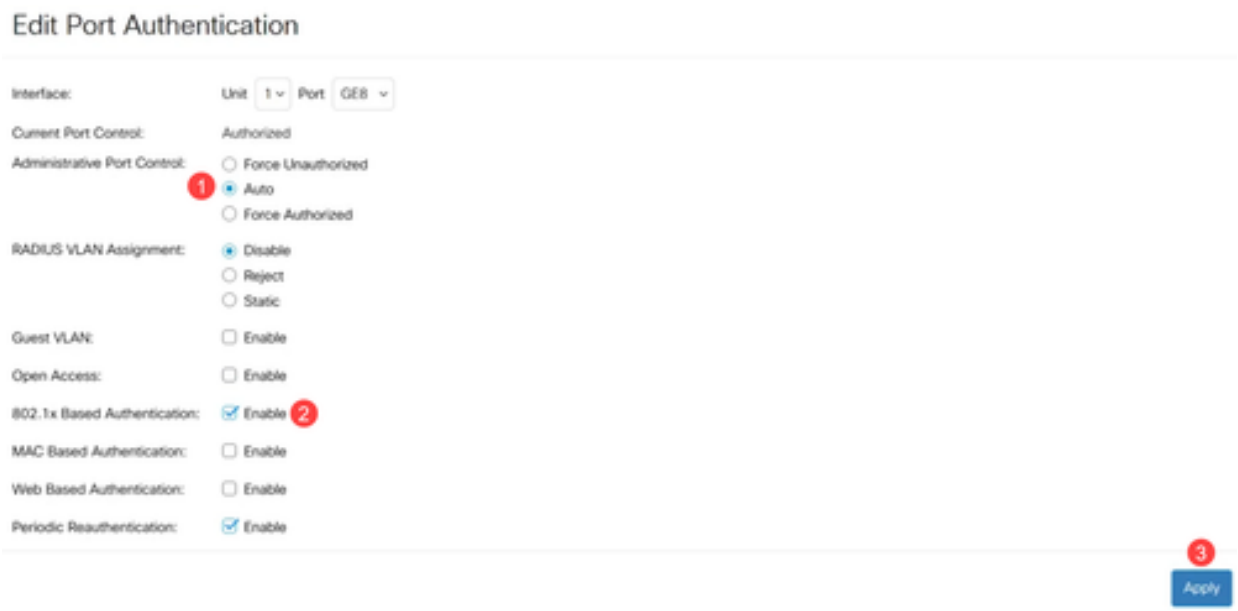
步驟 4

轉至Security > 802.1X Authentication > Port Authentication選單。選擇筆記型電腦所連線的埠，然後按一下edit圖示。在本示例中，GE8被選中。



步驟 5

選擇Administrative Port Control作為Auto，然後啟用802.1x Based Authentication。按一下「Apply」。



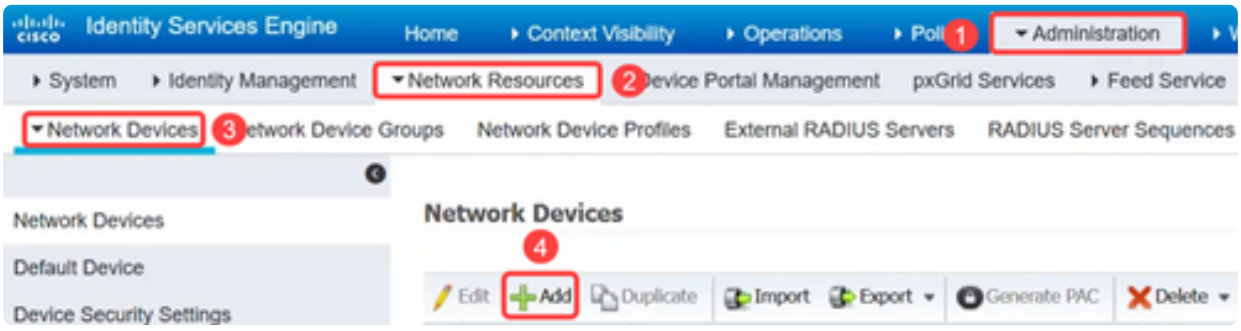
適用於可下載ACL的Cisco ISE伺服器配置

> **Note:**
> ISE配置超出思科業務支援的範圍。有關詳細資訊，請參閱ISE管理員指南。

本文中所示的配置是可下載ACL與Cisco Catalyst 1300系列交換機配合使用的示例。

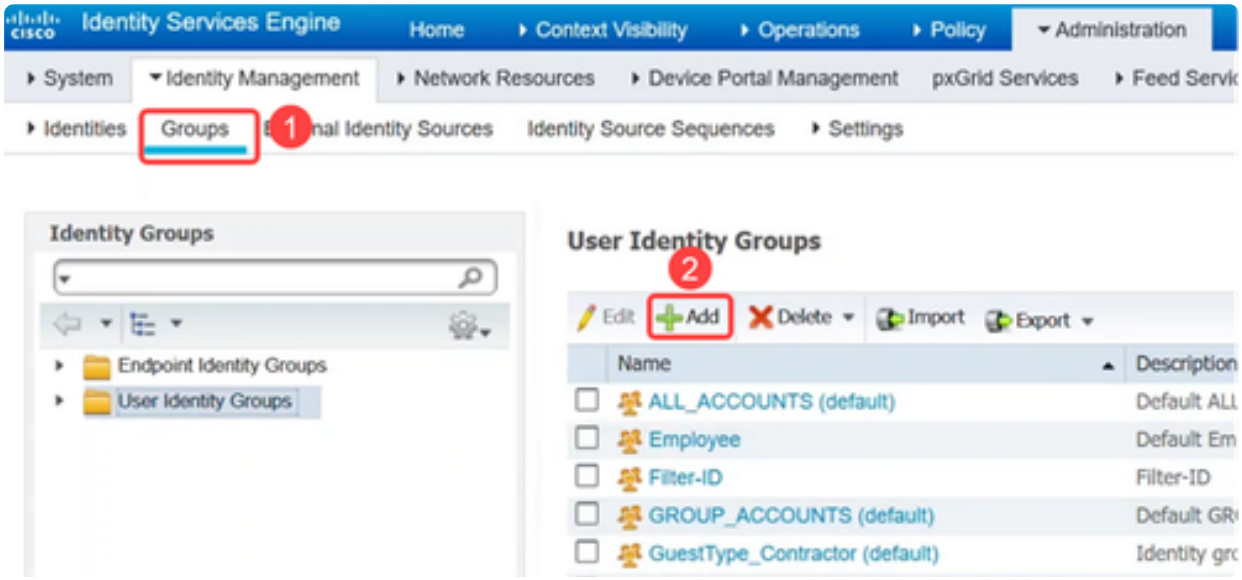
步驟 1

登入到您的Cisco ISE伺服器並導航到Administration > Network Resources > Network Devices，然後新增Catalyst交換機裝置。



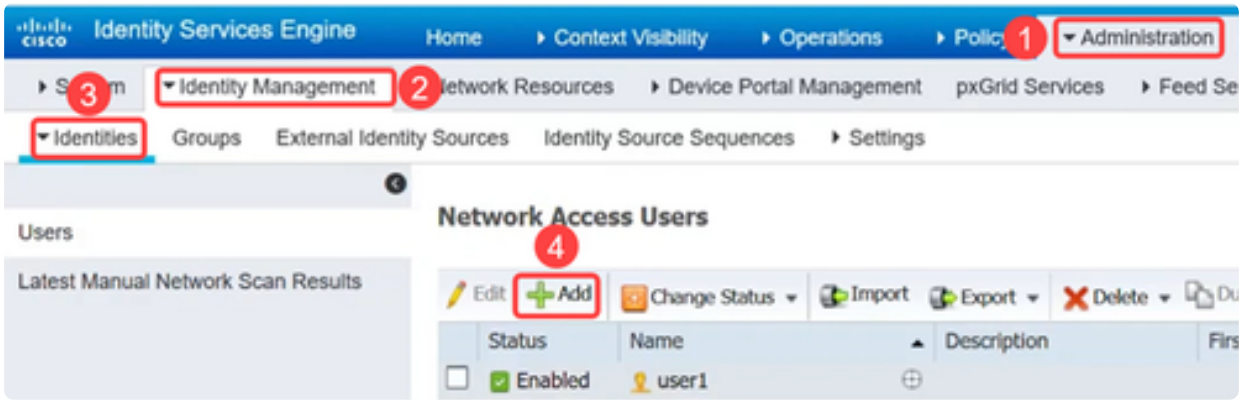
步驟 2

要建立使用者身份組，請導航到Groups頁籤並新增使用者身份組。



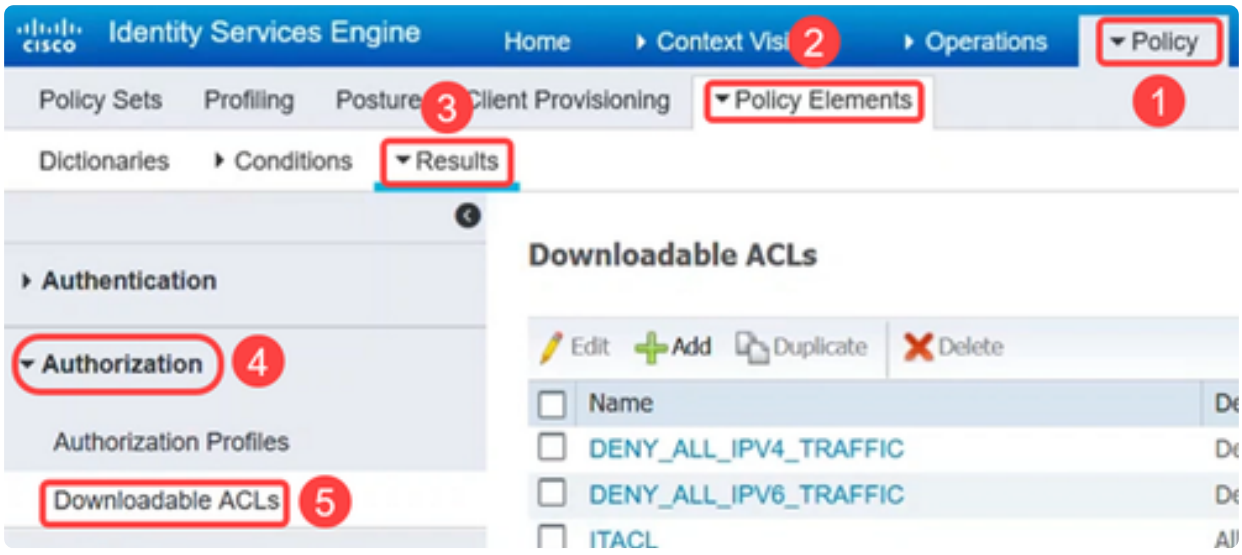
步驟 3

轉到Administration > Identity Management > Identities選單以定義使用者並將使用者對映到組。



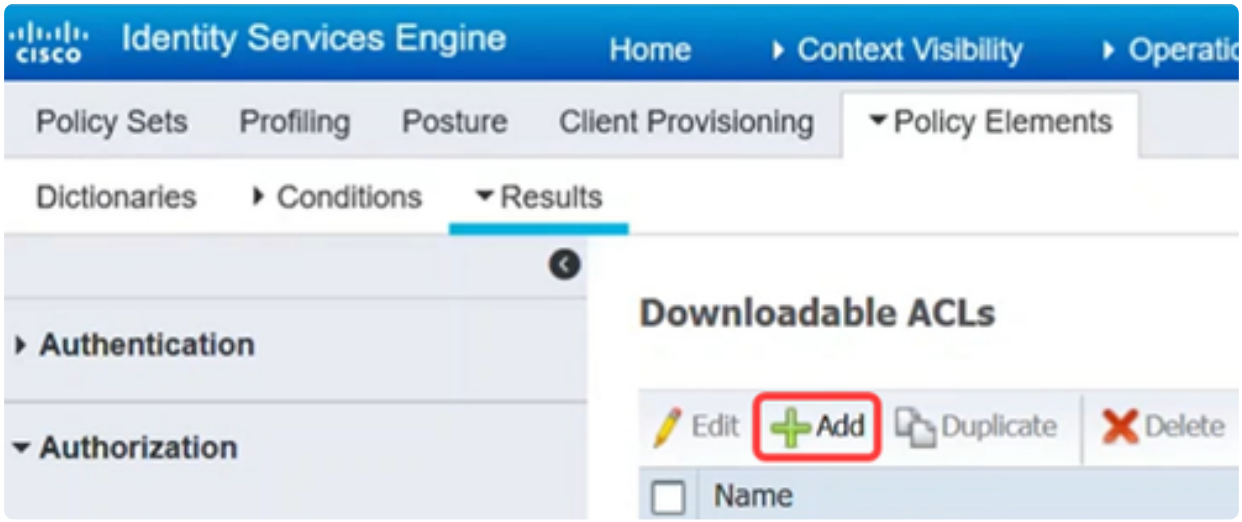
步驟 4

導航到Policy > Policy Elements > Results選單。在Authorization下，按一下Downloadable ACLs。



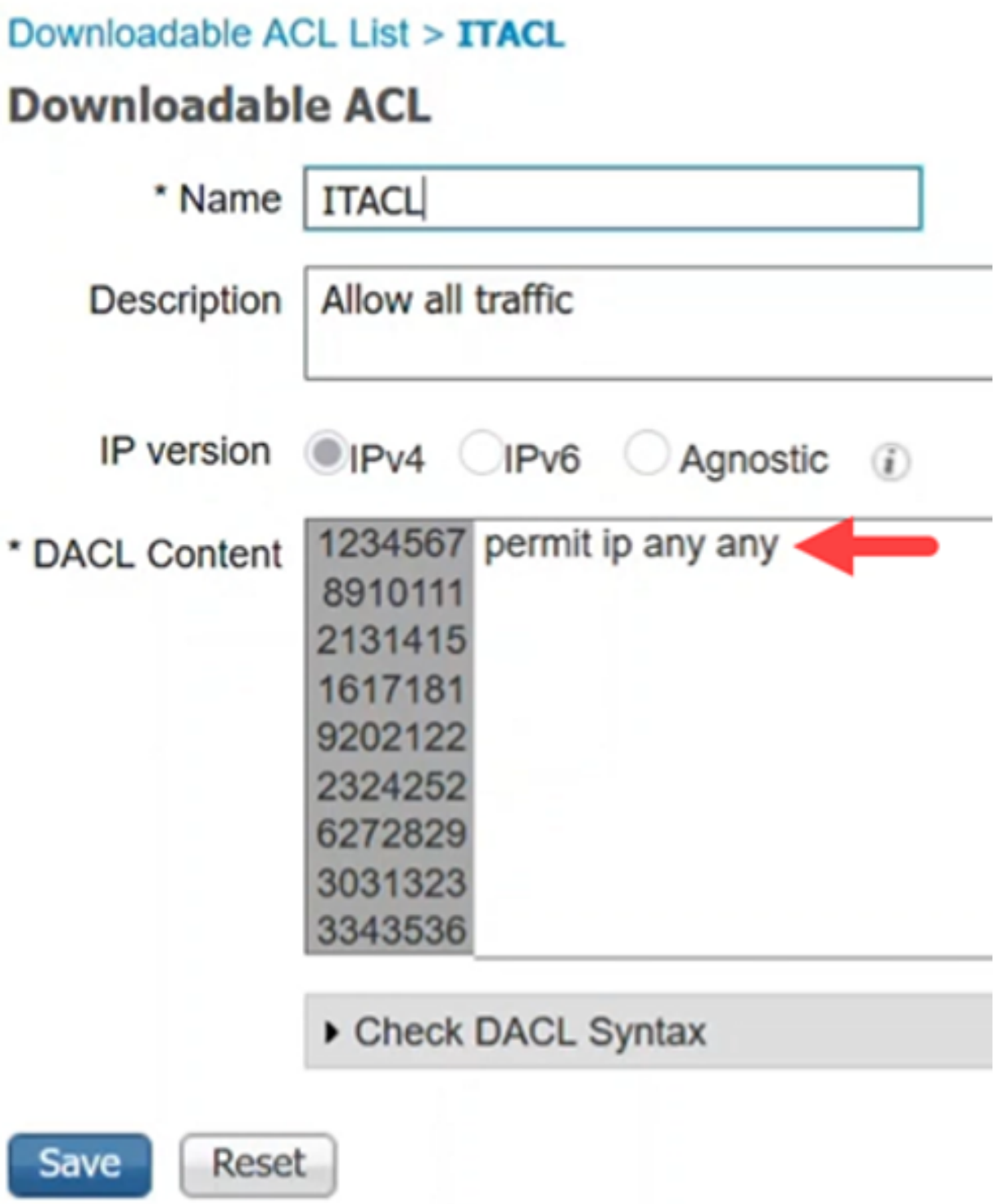
步驟 5

按一下Add圖示以建立可下載ACL。



步驟 6

配置名稱、說明，選擇IP版本，並在DACL內容(DACL Content)欄位中輸入將構成可下載ACL的訪問控制條目(ACE)。按一下「Save」。



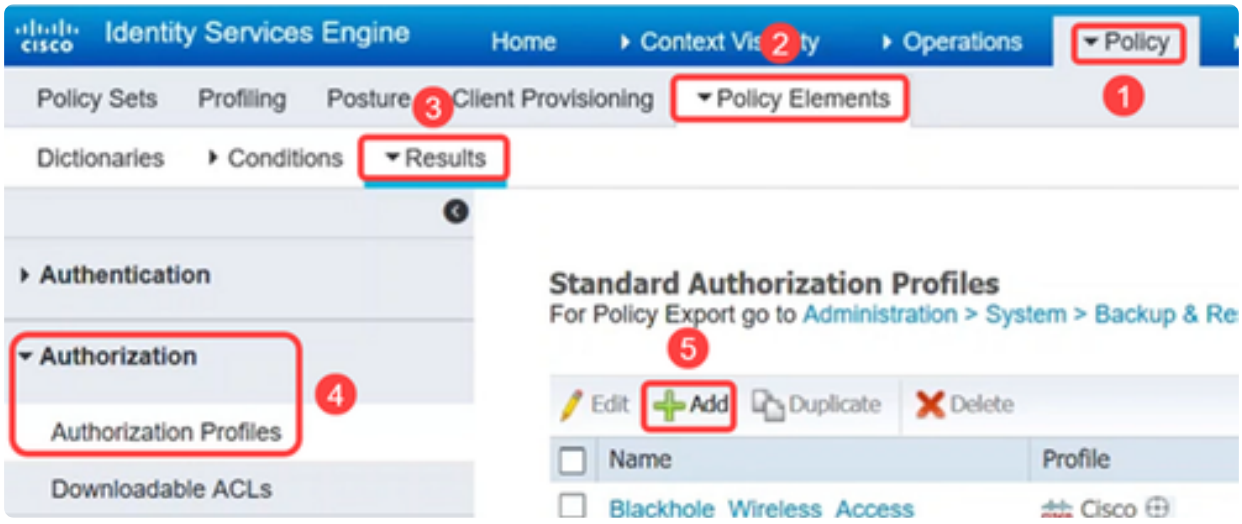
Note:

僅支援IP ACL，且源必須為ANY。對於ISE上的ACL，現在僅支援IPv4。如果使用其他源輸入ACL，而對於ISE而言，語法可能沒問題，但應用於交換機時，語法會失敗。

步驟 7

建立用於在ISE策略集中將DACL和其他策略邏輯關聯在一起的授權配置檔案。

為此，請導航到Policy > Policy Elements > Results > Authorization > Authorization Profiles，然後點選Add。

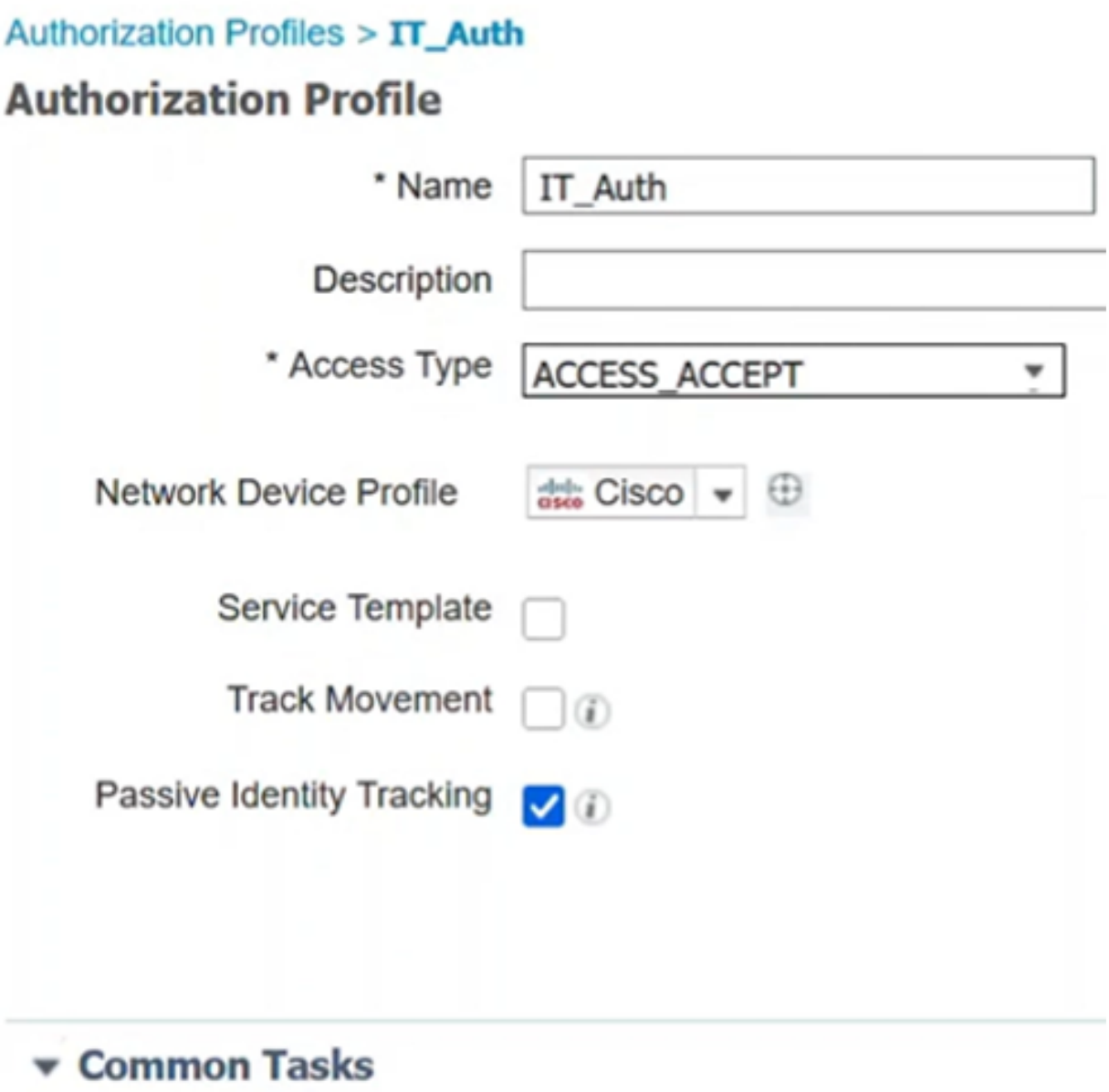


步驟 8

在Authorization Profile頁面中，配置以下內容：

- 名稱
- 說明
- Access Type — 應設定為ACCESS_ACCEPT。如果設定為ACCESS_REJECT，它將拒絕身份驗證。
- 網路裝置配置檔案 — 應將其選為思科。
- 被動身份跟蹤 — 對於某些身份驗證方案，可能需要啟用。連結到AD的EasyConnect_PassiveID方案需要此引數。
- 常見任務 — 此部分有許多選項。在本例中，配置了DACL Name。

按一下「Save」。

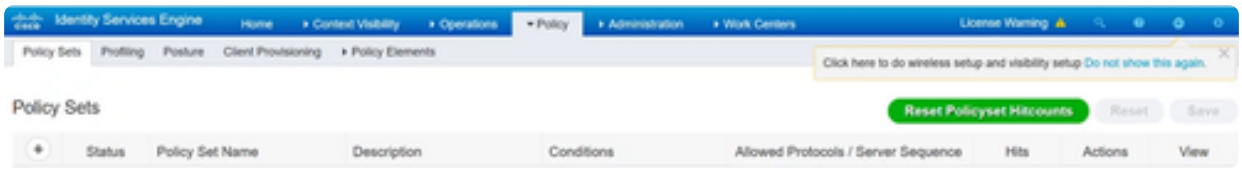


步驟 9

要配置作為身份驗證和授權策略的邏輯分組的策略集，請按一下Policy > Policy Sets選單。

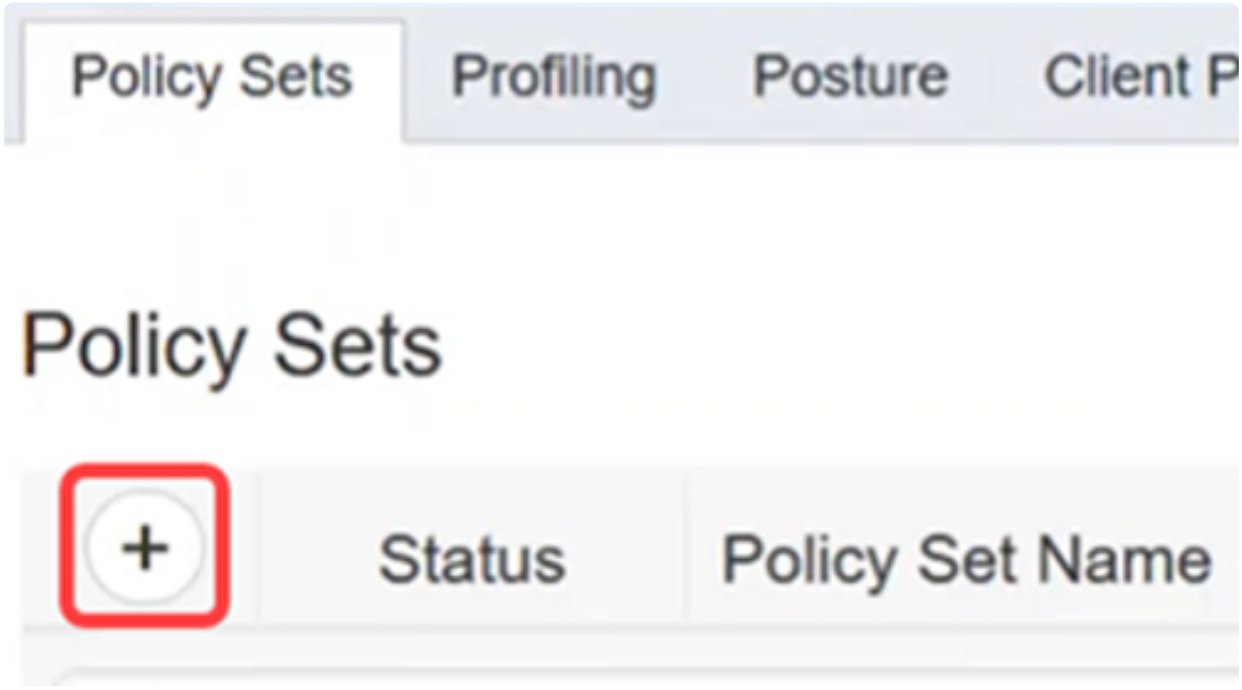
檢視策略集清單時，可以檢視以下內容：

- 狀態 — 綠色勾選表示啟用，空白白圈表示禁用，眼睛圖示表示僅監控配置。
- 策略集名稱和說明 — 不言自明
- 條件 — 定義策略集適用的位置。
- 允許的協定/伺服器序列 — 設定更多高級控制。
- Hits — 顯示策略集已被使用的次數。
- 操作 — 允許您更改策略集可以應用的順序、複製現有策略集或刪除現有策略集。
- 檢視 — 允許您編輯策略集詳細資訊。



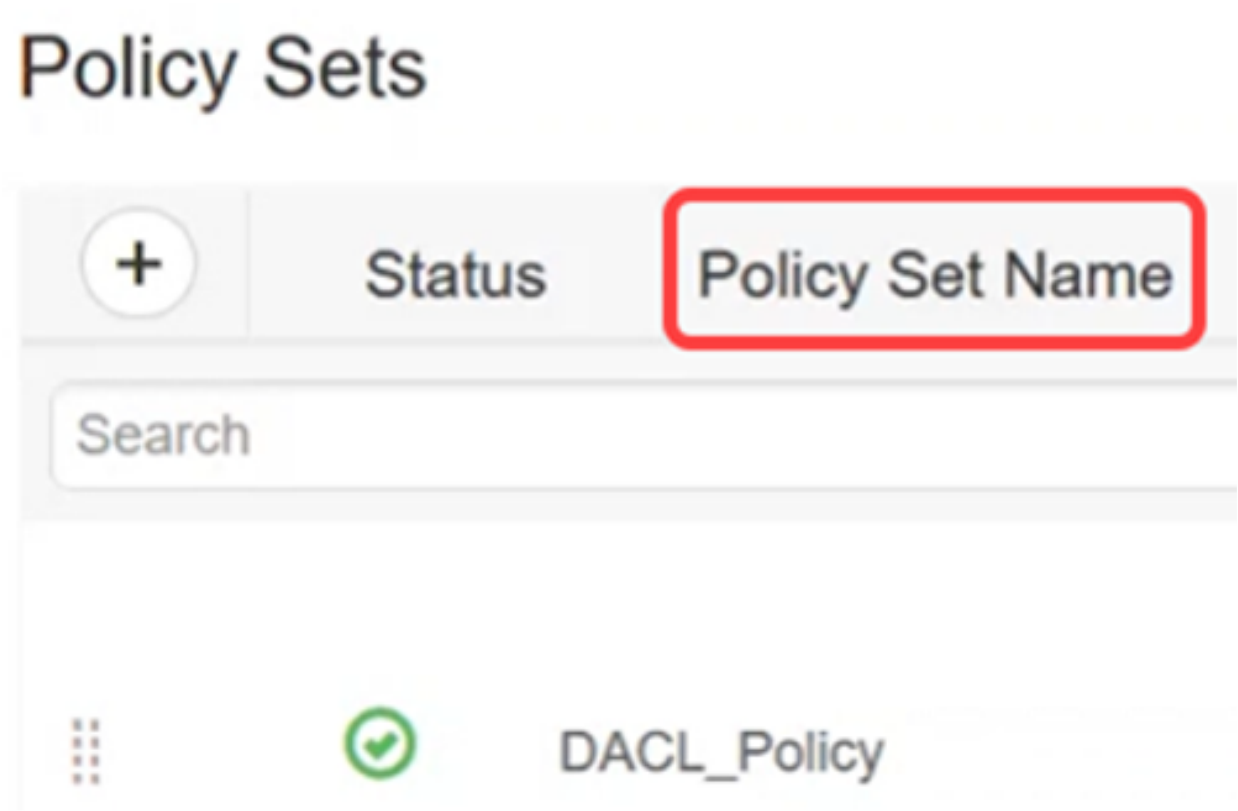
步驟 10

要建立策略集，請按一下add按鈕。



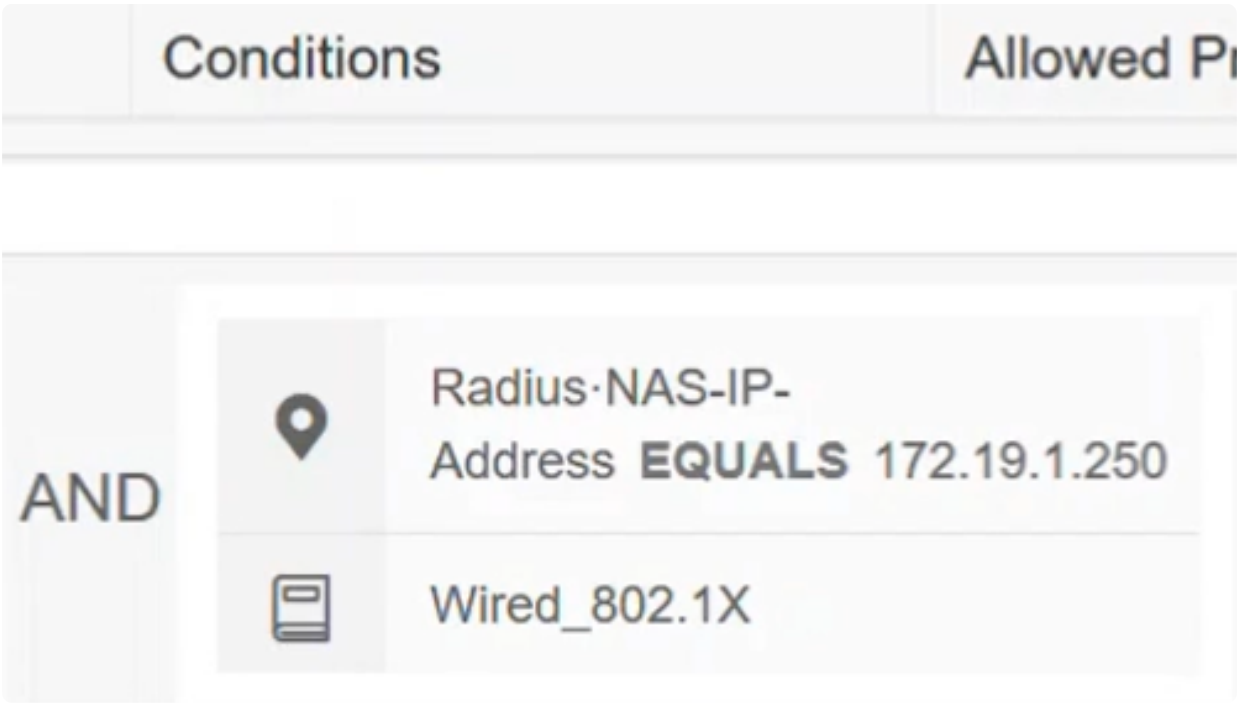
步驟 11

定義策略集名稱。



步驟 12

在Conditions下，按一下add按鈕。這將開啟Conditions Studio，您可以在其中定義使用此身份驗證配置檔案的位置。在本範例中，此指令已套用到Radius-NAS-IP-Address（交換器），即172.19.1.250和wired_802.1x流量。

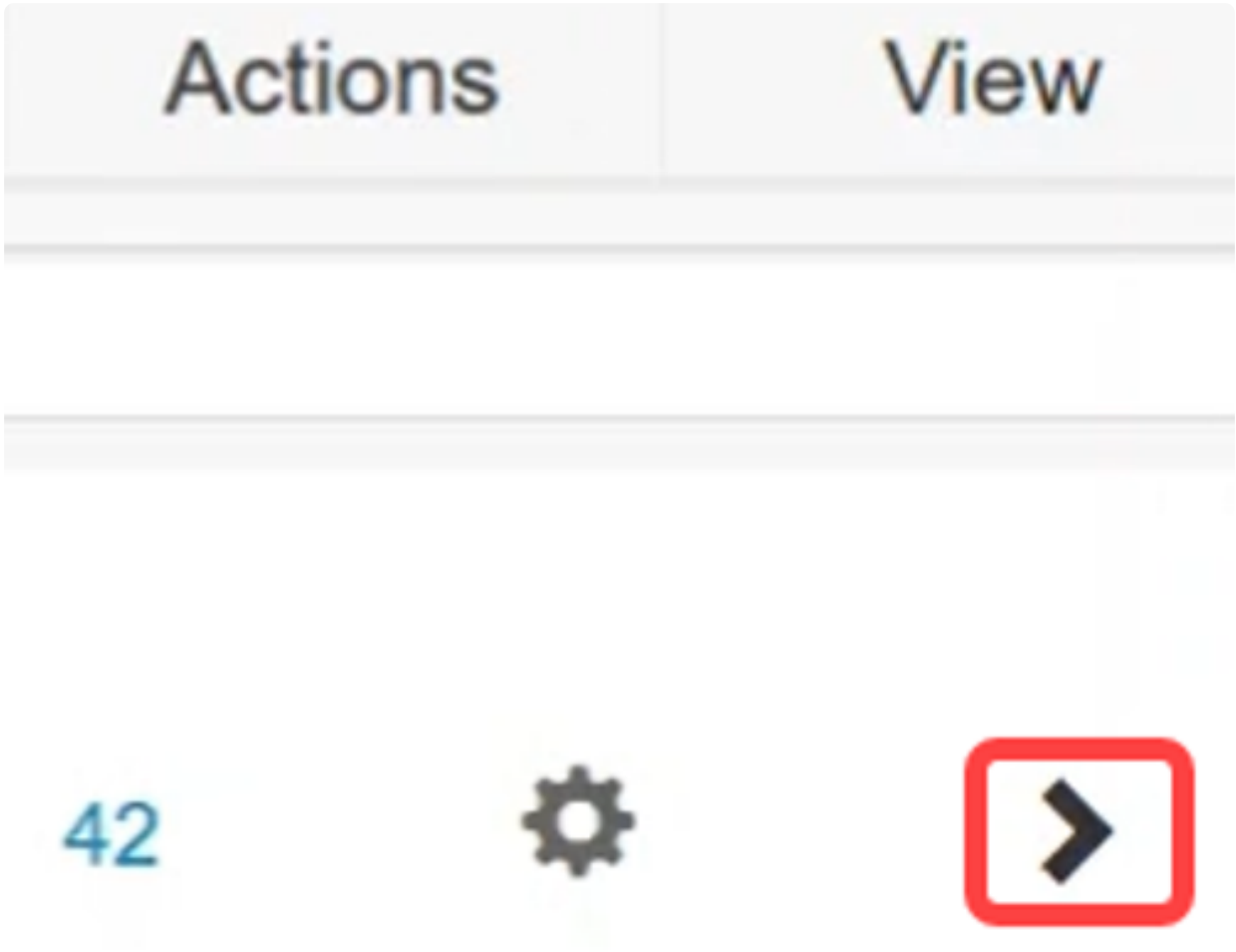


步驟 13

將Allowed Protocols配置為Default Network Access，然後按一下Save。

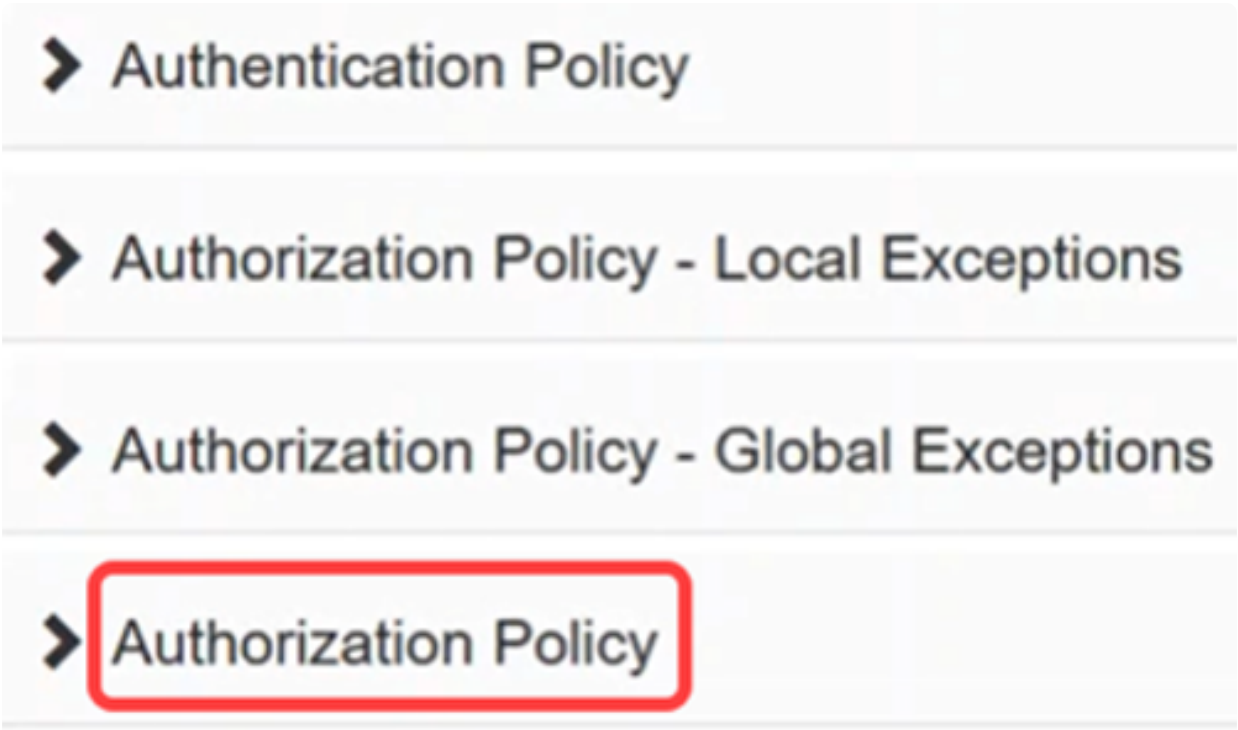
步驟 14

在View下，按一下箭頭圖示根據您的網路設定和要求配置身份驗證和授權策略，或者您可以選擇預設設定。在本示例中，按一下Authorization policy。



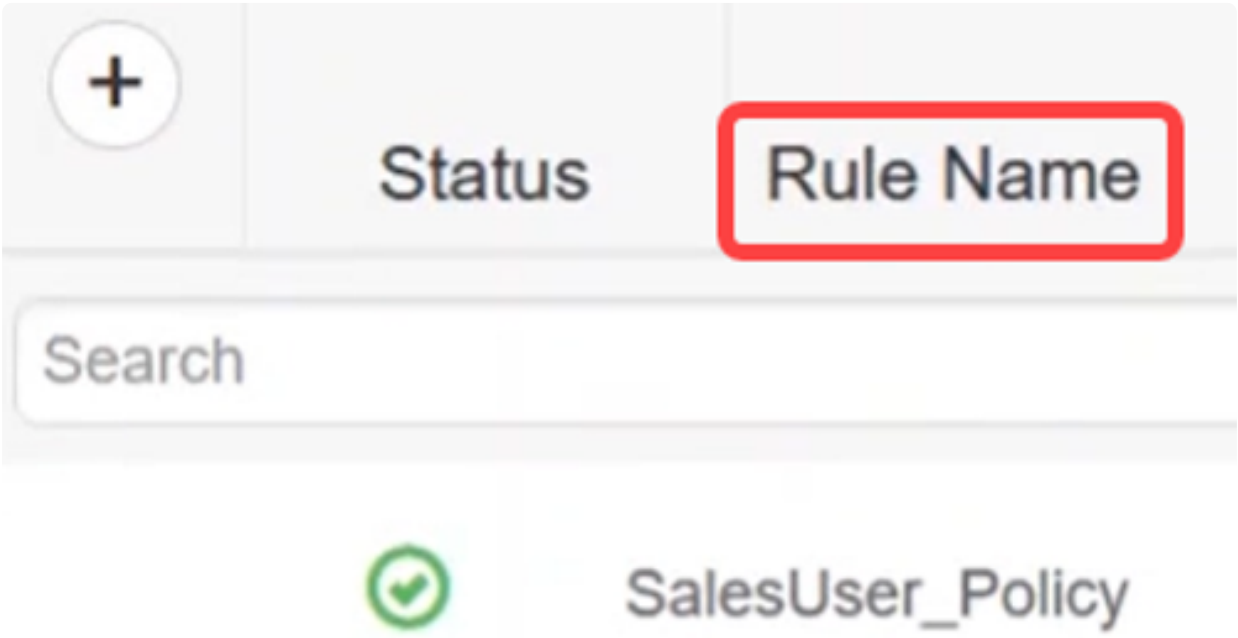
步驟 15

按一下plus圖示新增策略。



步驟 16

輸入規則名稱。

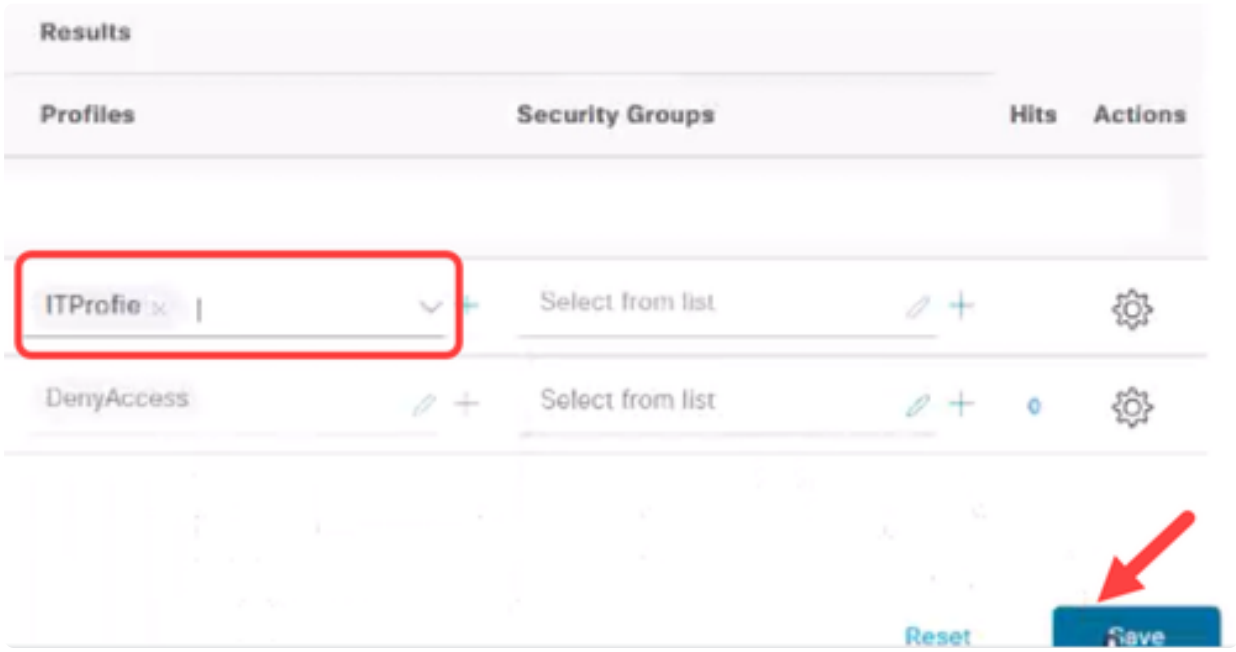


步驟 17

在Conditions下，按一下plus圖示並選擇身份組。按一下「Use」。

步驟 18

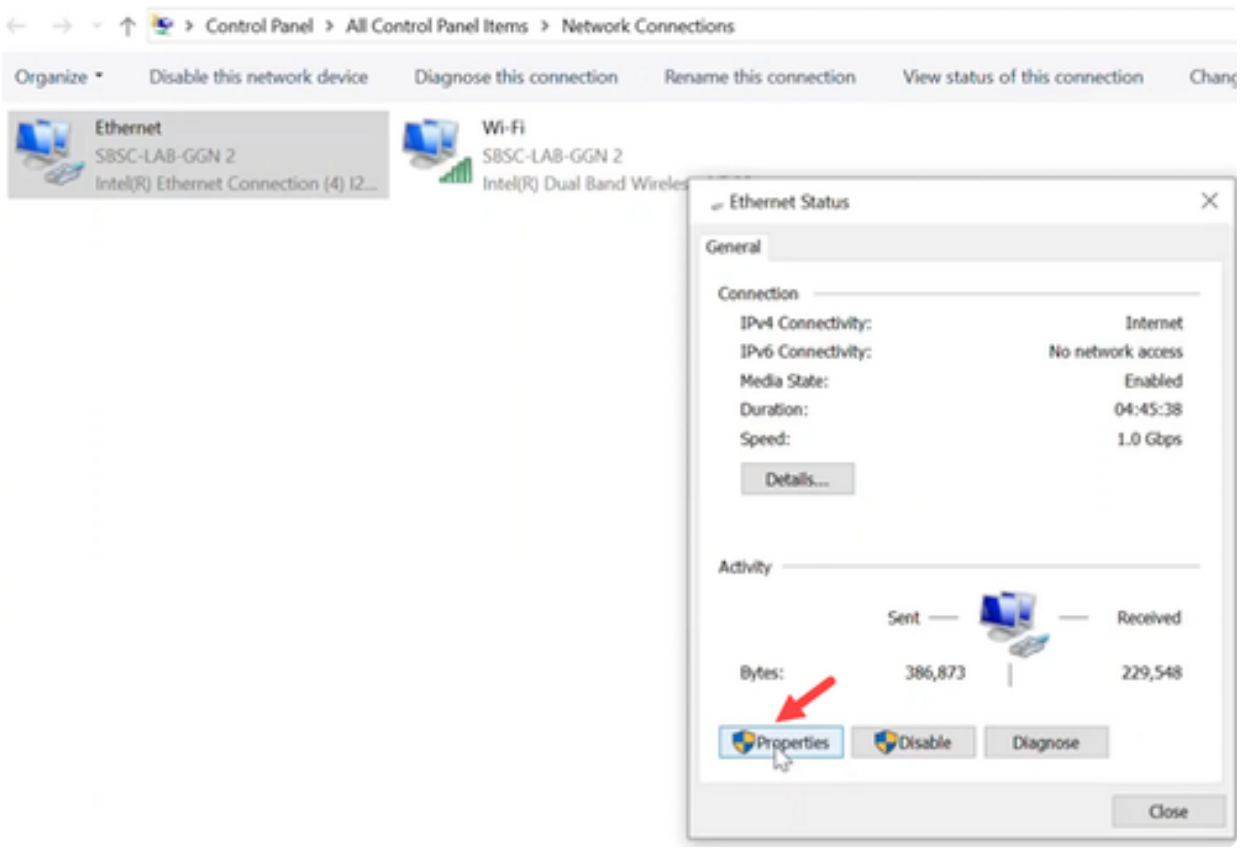
應用所需的配置檔案，然後按一下Save。



客戶端配置

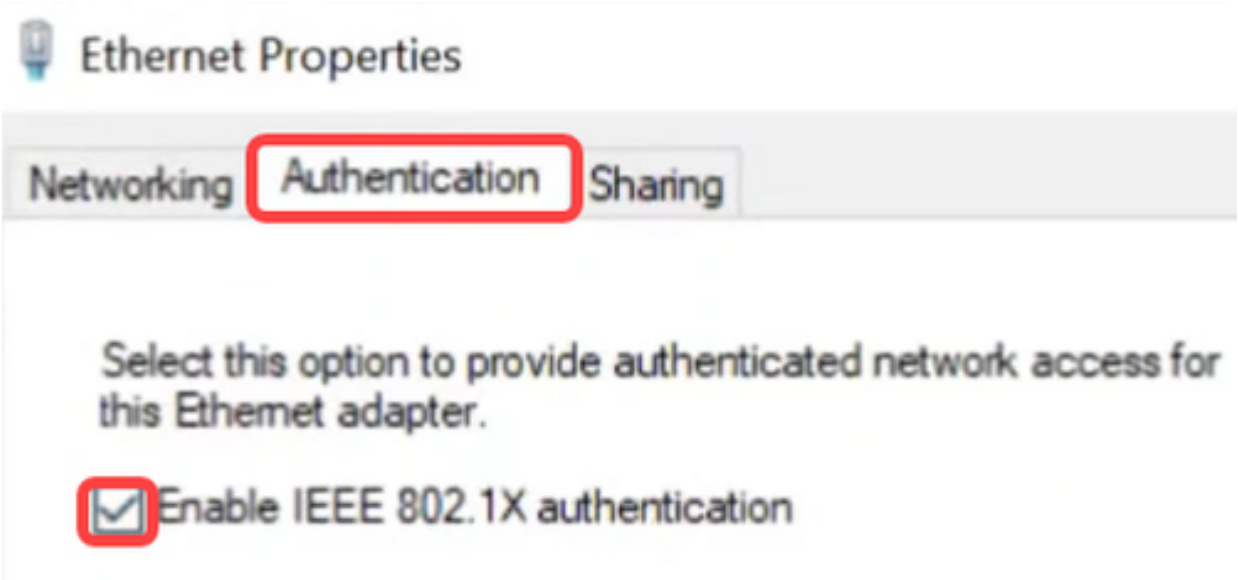
步驟 1

在客戶端筆記型電腦上，導航到網路連線>乙太網，然後按一下屬性。



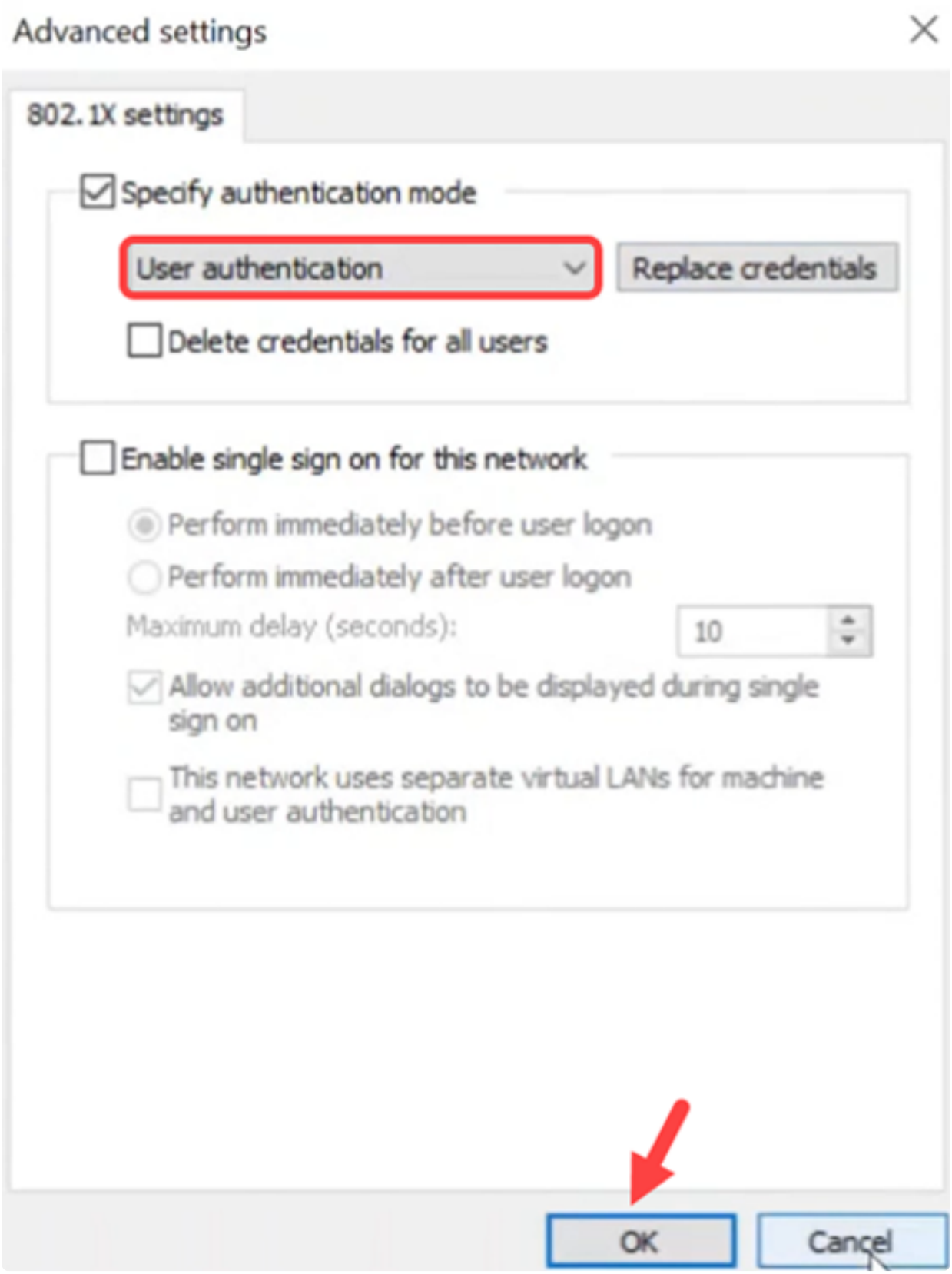
步驟 2

按一下Authentication頁籤，並確保802.1X authentication已啟用。



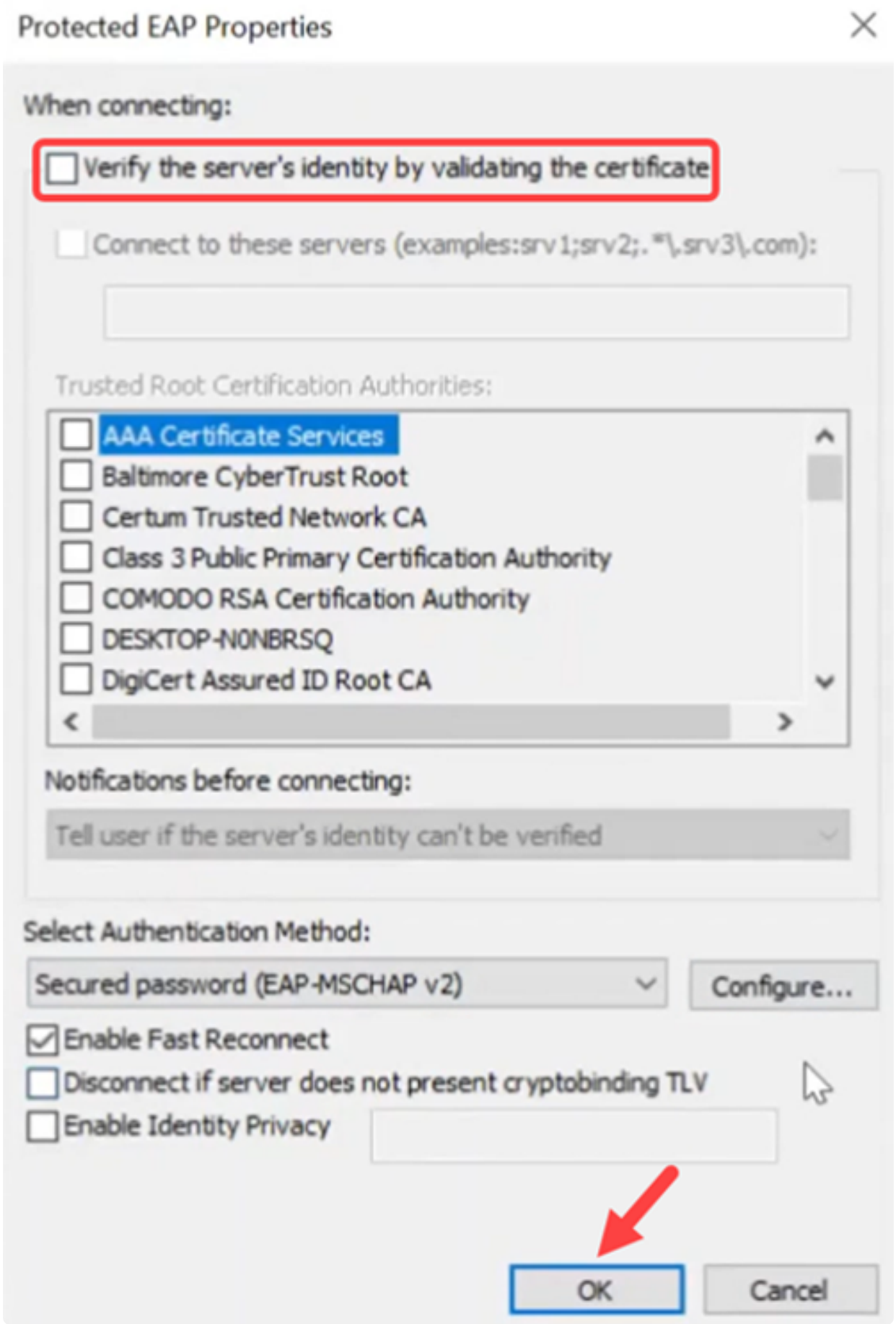
步驟 3

在Additional Settings下，選擇User authentication作為身份驗證模式。按一下「Save Credentials」，然後「OK」。



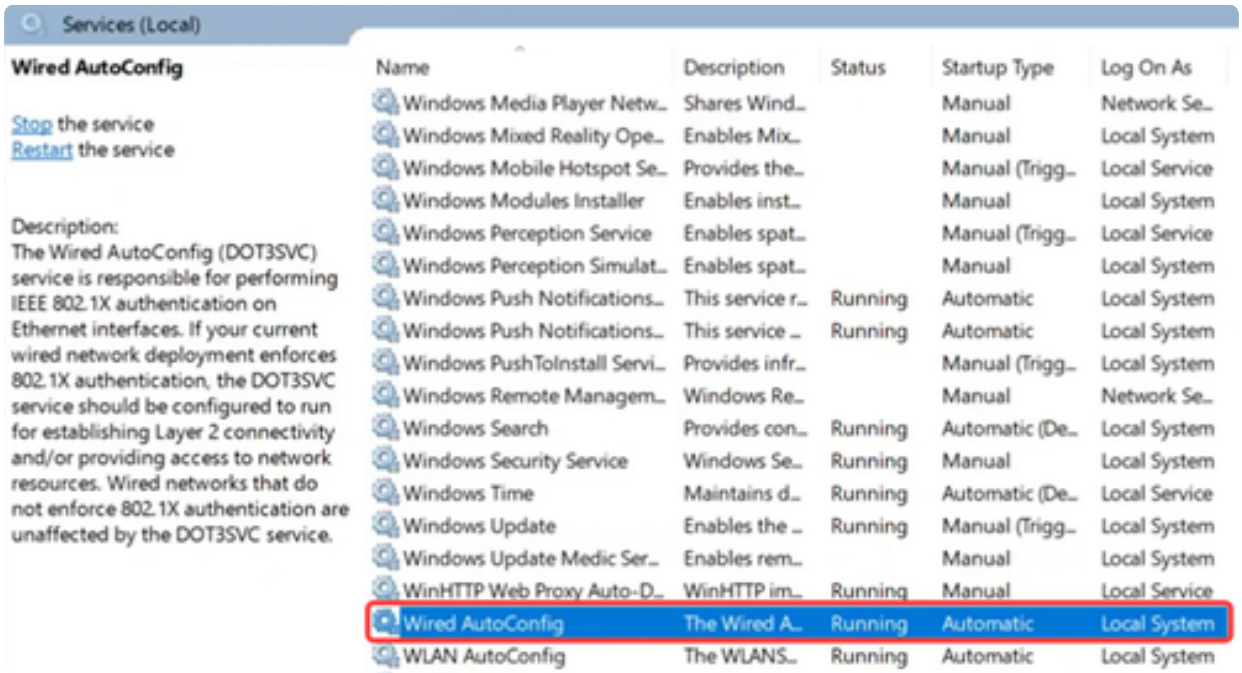
步驟 4

按一下Settings，確保取消選中Verify the server's identity by validating the certificate旁邊的框。按一下「OK」（確定）。


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
Certum Trusted Network CA
Class 3 Public Primary Certification Authority
COMODO RSA Certification Authority
DESKTOP-N0NBRSQ
DigiCert Assured ID Root CA
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

步驟 5

在Services下，啟用Wired AutoConfig 設定。

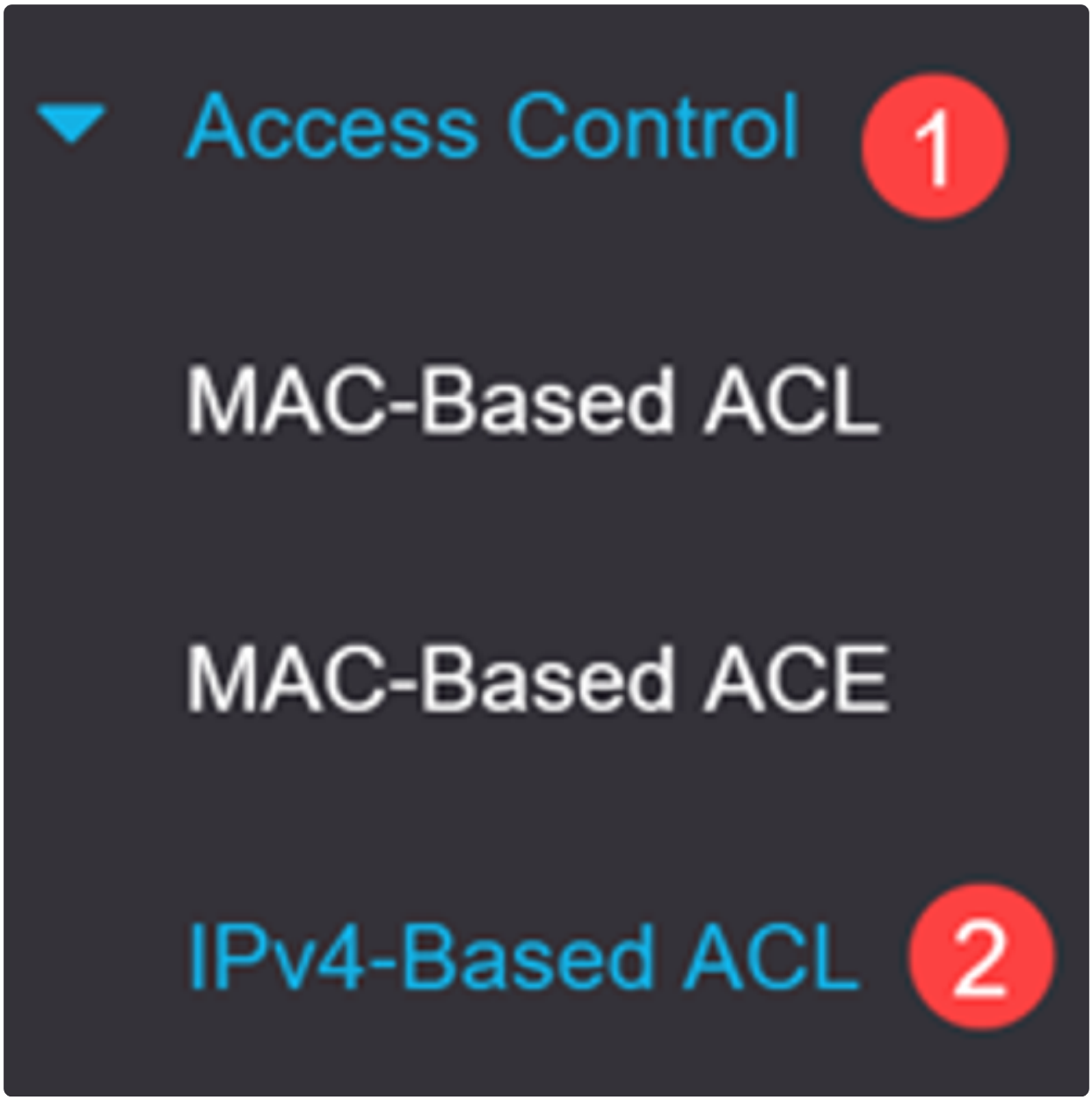


DACL驗證

使用者通過驗證後，您可以驗證可下載ACL。

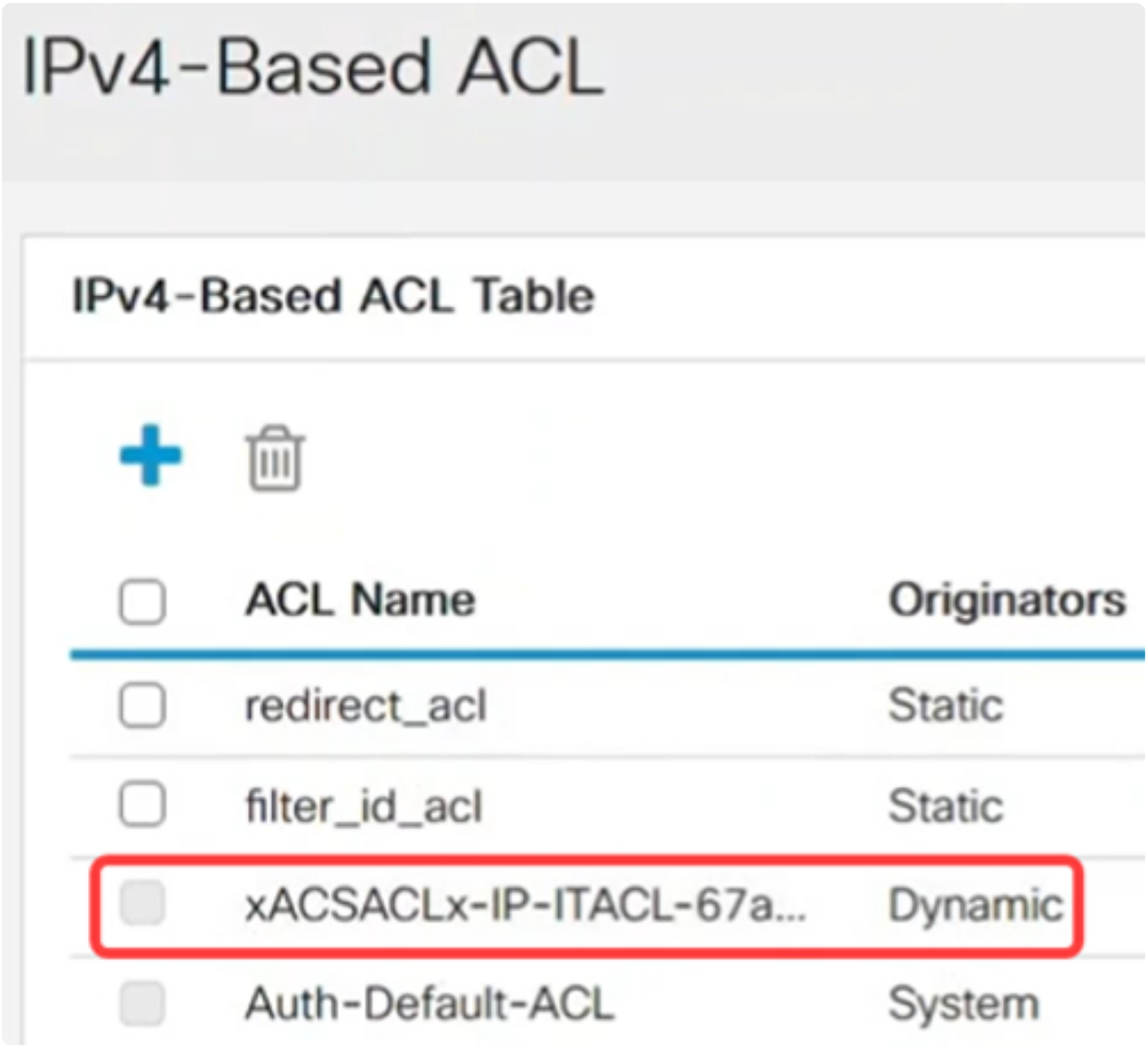
步驟 1

登入Catalyst 1300交換器，然後導覽至存取控制>基於IPv4的ACL功能表。



步驟 2

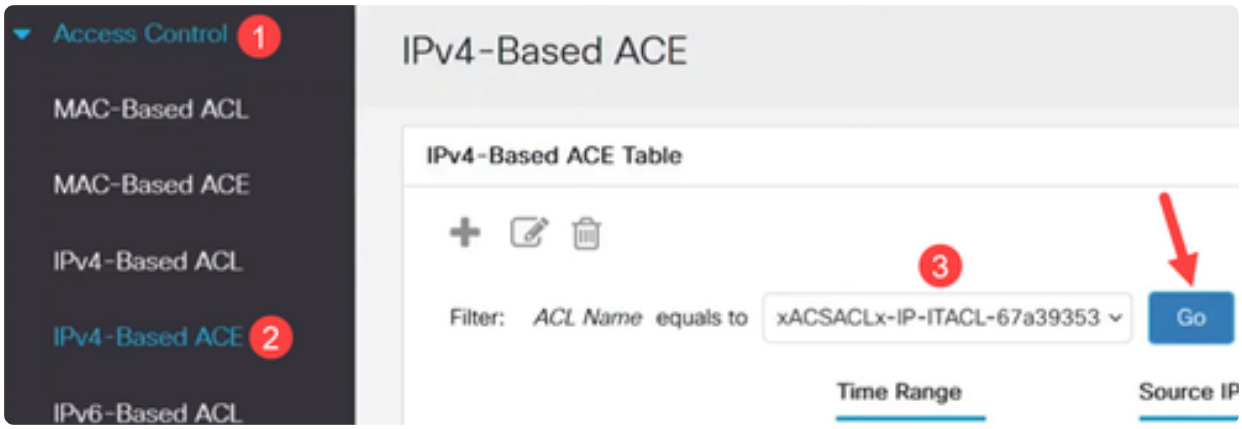
IPv4型ACL表會顯示下載的ACL。



Note:
無法編輯可下載的ACL。

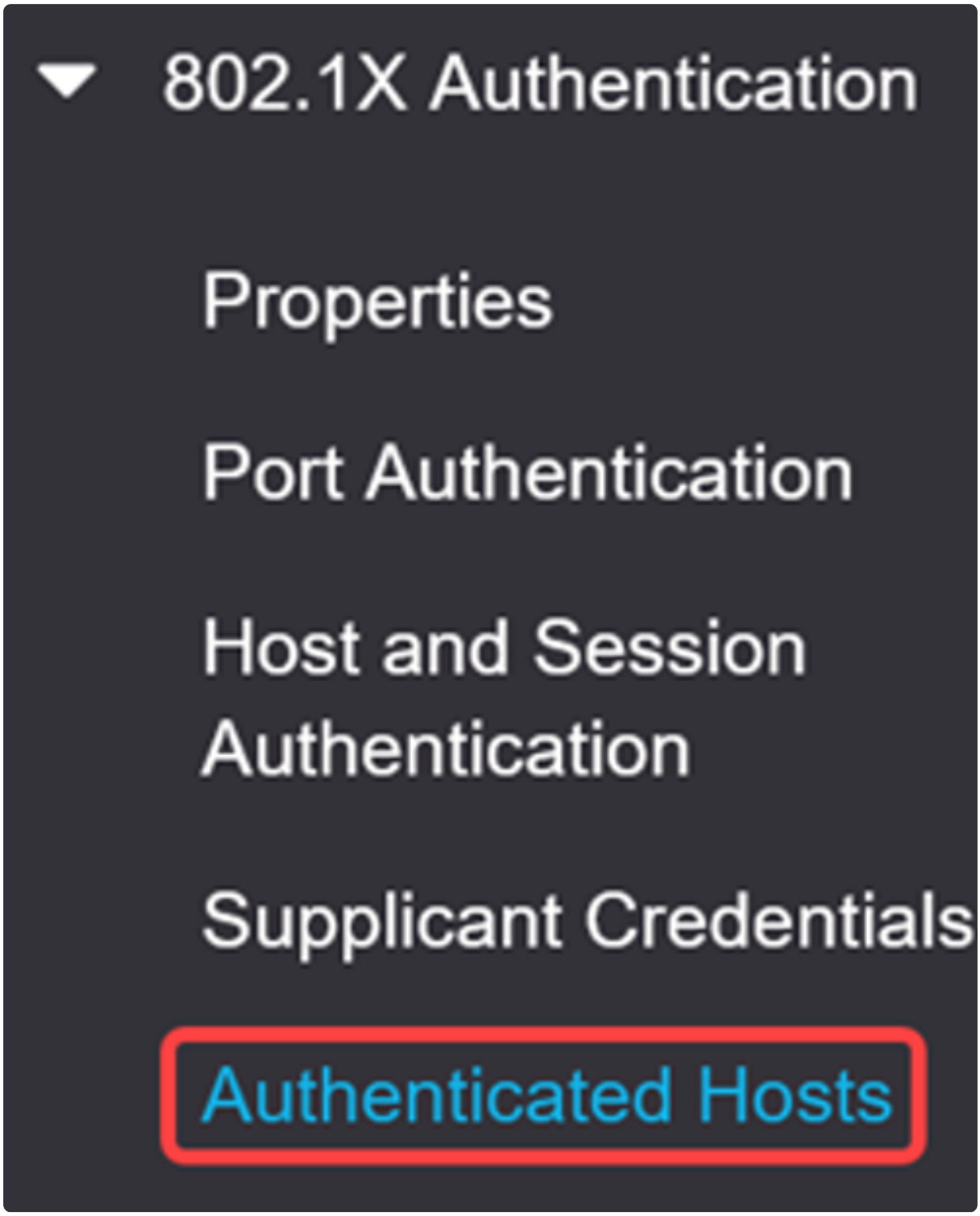
步驟 3

另一種驗證方法是導覽至基於IPv4的ACE，從ACL Name下拉選單中選擇可下載的ACL，然後按一下Go。將顯示在ISE中配置的規則。



步驟 4

導航到Security > 802.1 Authentication > Authenticated Hosts選單。您可以驗證通過驗證的使用者。按一下「Authenticated Sessions」，檢視更多詳細資訊。



步驟 5

在CLI中，運行命令show ip access-lists interface，然後運行介面ID。

在此範例中，可以看到應用於Gigabit乙太網路3的ACL和ACE。

```
switch4a7d55#show ip access-lists interface ge1/0/3
ip access-list extended xACSACLx-IP-SalesACL-6760399d
    deny    ip any host 192.168.251.10 ace-priority 1
    permit  ip any any ace-priority 2
ip access-list extended Auth-Default-ACL
    permit  udp any any any domain ace-priority 20
    permit  tcp any any any domain ace-priority 40
    permit  udp any bootps any any ace-priority 60
    permit  udp any any any bootpc ace-priority 80
    permit  udp any bootpc any any ace-priority 100
    deny    ip any any ace-priority 120
```

步驟 6

您還可以使用命令檢視與ISE連線和ACL下載相關的設定

show dot1x sessions interface <ID> detailed。您可以檢視狀態、802.1x驗證狀態和下載的ACL。

```
switch4a7d55#show dot1x sessions interface ge1/0/3 detailed

          Interface: gi1/0/3
        MAC Address: e4:[redacted]:31
       IPv4 Address: 192.168.251.11
          User-Name: user5
             Status: Authorized
    Oper host mode: multi-host
   Session timeout: N/A
    Session Uptime: 196 sec
 Common Session ID: 14FBA8C00500032222C35D9E
   Acct Session ID: 0x05000322
Server Policies:
           ACS ACL: xACSACLx-IP-SalesACL-6760399d

Method status list:
   Method                  State
   802.1x                  Authentication success
```

結論

這就對了！現在您已經知道可下載ACL在思科Catalyst 1300交換機上如何與思科ISE配

合使用。

如需詳細資訊，請檢視Catalyst 1300管理指南和Cisco Catalyst 1300系列支援頁面。

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）。