Catalyst 1300交换机中的可下载ACL

目标

本文的目的是演示可下载访问控制列表(DACL)如何在具有思科身份服务引擎(ISE)的Cisco Catalyst 1300交换机上运行。

适用设备 | 软件版本

- Catalyst 1300 系列 |4.1.6.54

简介

动态ACL是根据策略或条件（如用户帐户组成员资格、时间等）分配给交换机端口的ACL。它们可以是通过filter-ID指定的本地ACL或可下载ACL(DACL)。

可下载ACL是从思科ISE服务器创建和下载的动态ACL。它们根据用户身份和设备类型动态应用访问控制规则。DACL的优点是允许您为ACL设置一个中央存储库，因此您无需在每台交换机上手动创建它们。当用户连接到交换机时，他们只需进行身份验证，交换机将从思科ISE服务器下载适用的ACL。

可下载ACL的使用案例

1. 不同用户在连接到交换机时将收到不同的ACL（本地ISE用户）。
2. 网络连接受限的用户可以登录中央Web门户进行完全网络访问（中央Web身份验证）。
3. 高级 — 使用MAC身份验证绕行(MAB)允许与Windows Active Directory(AD)和某些相关服务的通信，同时将ISE服务器连接到AD并监控用户身份验证。在Windows AD登录之前，网络将仅允许访问非常有限的资源，但AD身份验证将基于Windows组下载不同的ACL并允许完整的网络访问。
4. 高级 — 由于ISE服务器上的策略，用户根据星期几、时间或其他因素收到不同的ACL。

本文将详细讨论第一种使用案例。

目录

- 配置RADIUS客户端
- 配置802.1x身份验证
- 可下载ACL的思科ISE服务器配置
- 客户端配置
- DACL验证

先决条件

- 确保您的Catalyst 1300交换机升级到最新固件（交换机固件应为4.1.6或更高版本）。
- 为交换机分配静态IP以用于管理。

配置RADIUS客户端

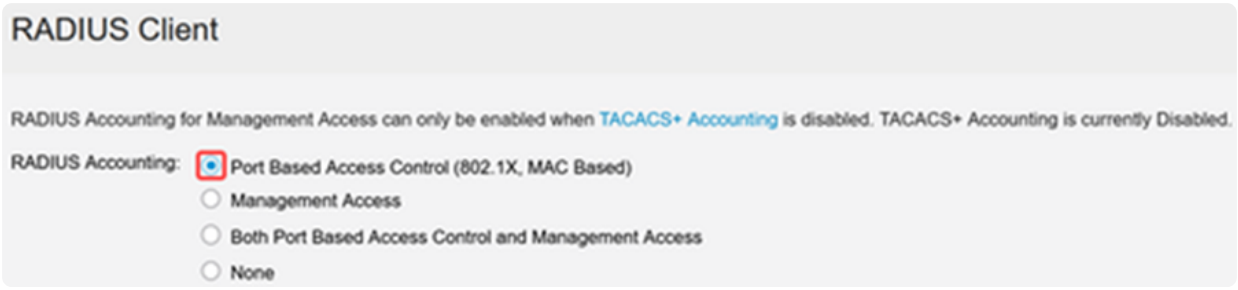
第 1 步

登录到Catalyst 1300交换机，然后导航到Security > RADIUS Client菜单。



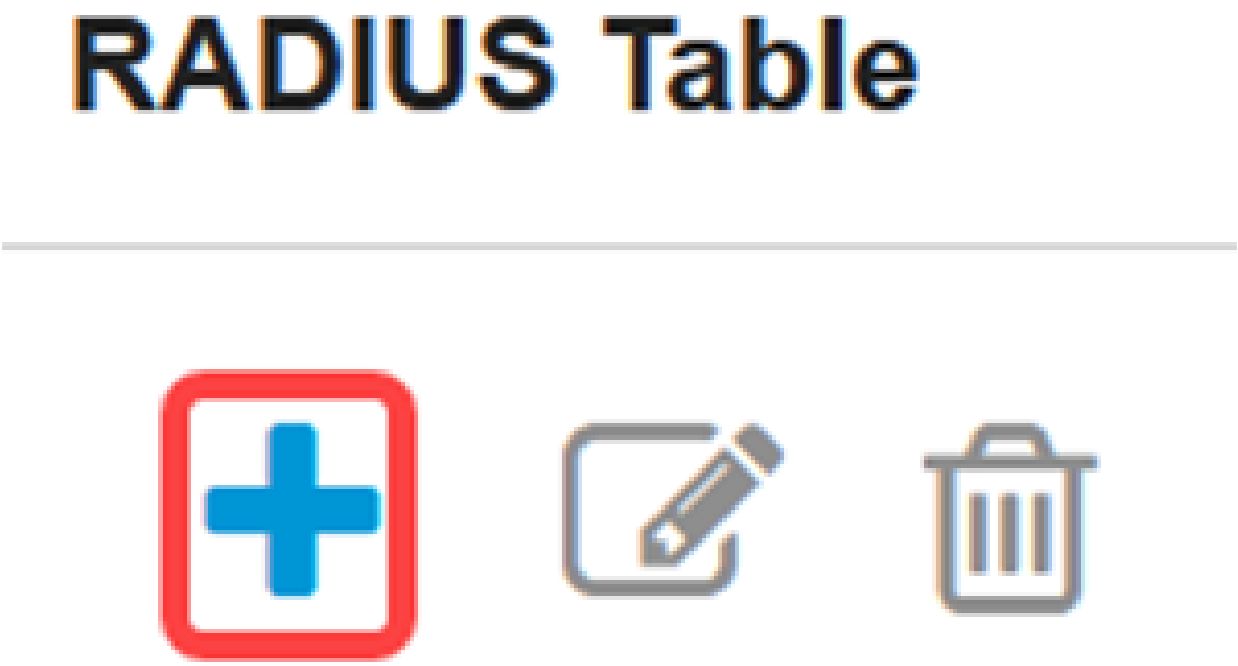
第 2 步

对于RADIUS Accounting，选择Port Based Access Control选项。



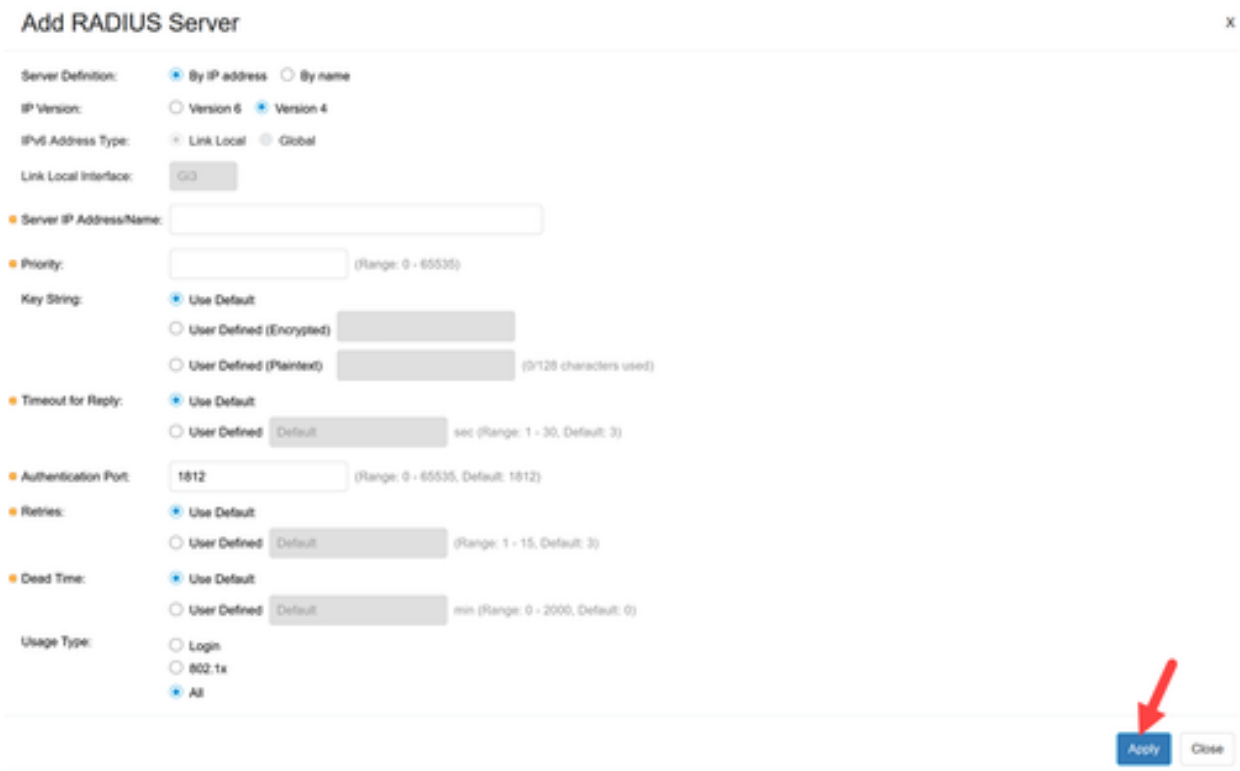
第 3 步

在RADIUS Table下，点击加号图标以添加Cisco ISE服务器。



第 4 步

输入思科ISE服务器详细信息，然后单击Apply。



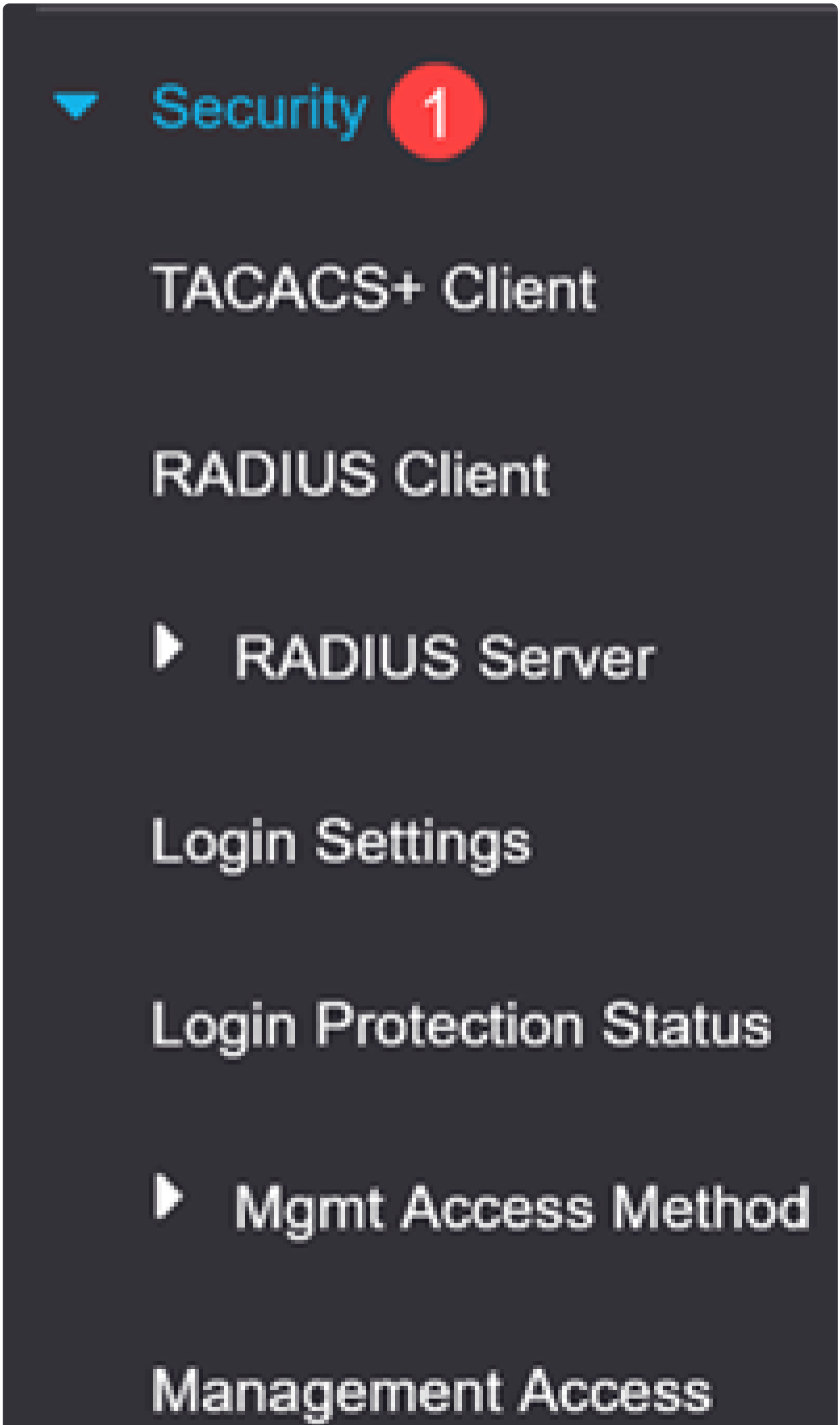
Note:

Usage Type必须选为802.1x。

配置802.1x身份验证

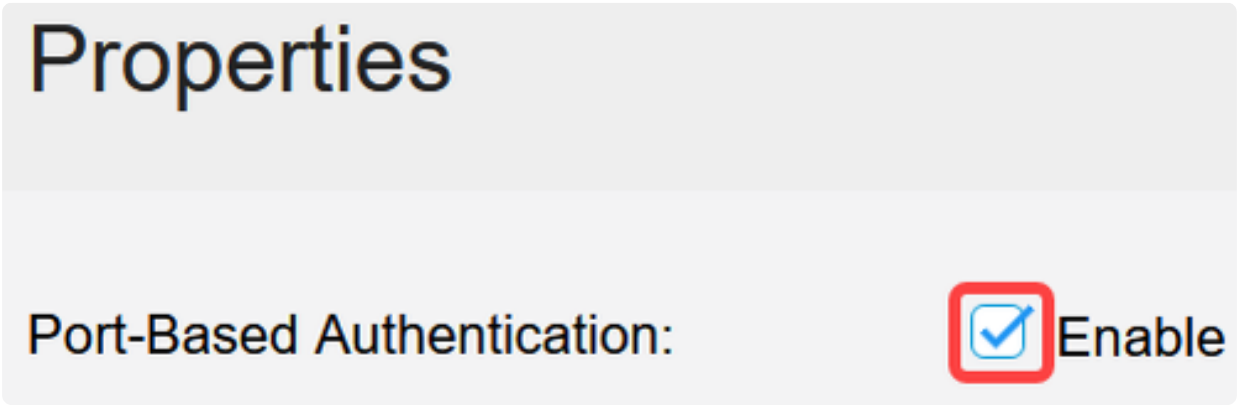
第 1 步

导航到安全> 802.1X身份验证>属性菜单。


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

第 2 步

单击此复选框可启用基于端口的身份验证。



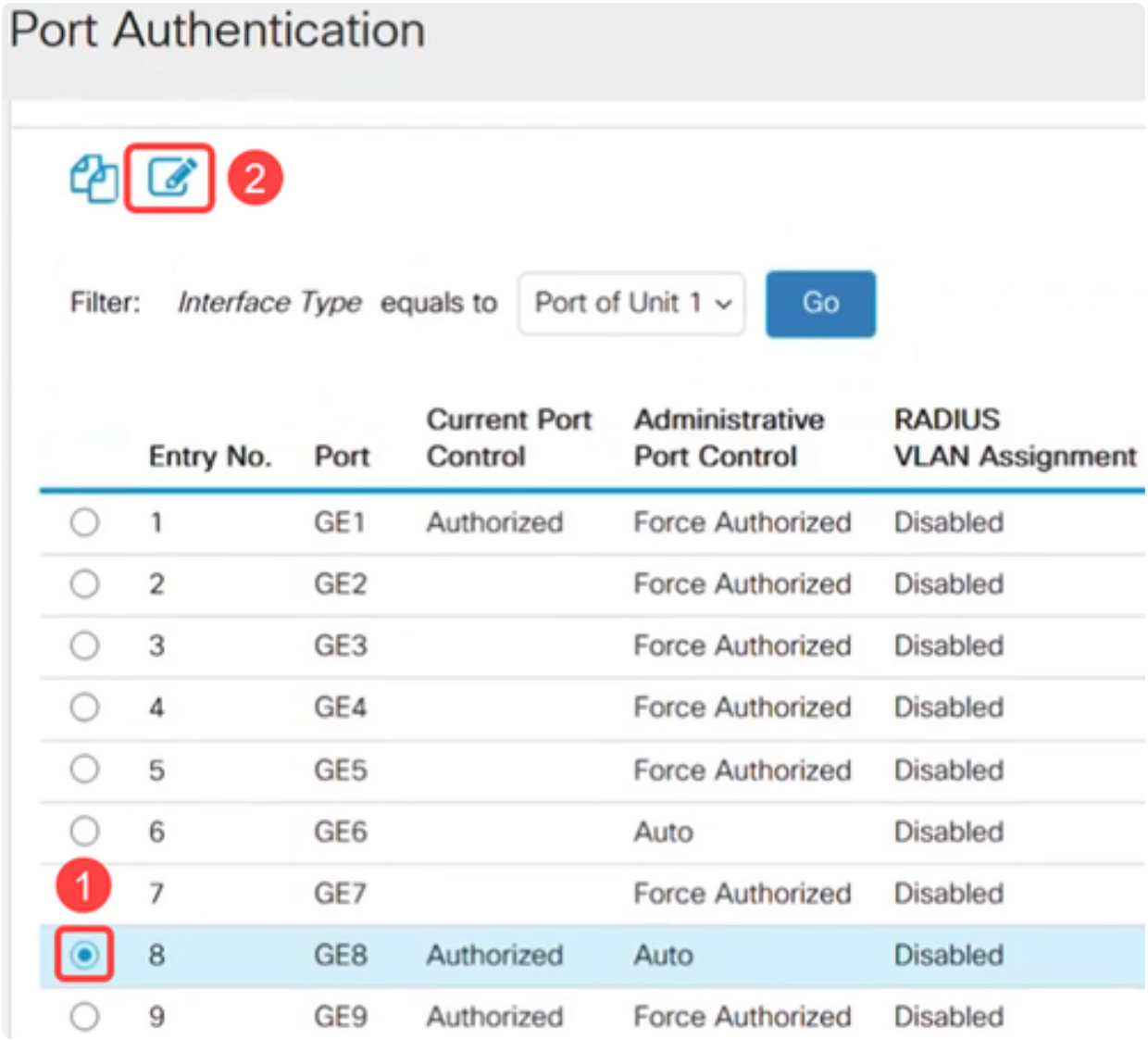
第 3 步

在Authentication Method下，选择RADIUS，然后单击Apply。



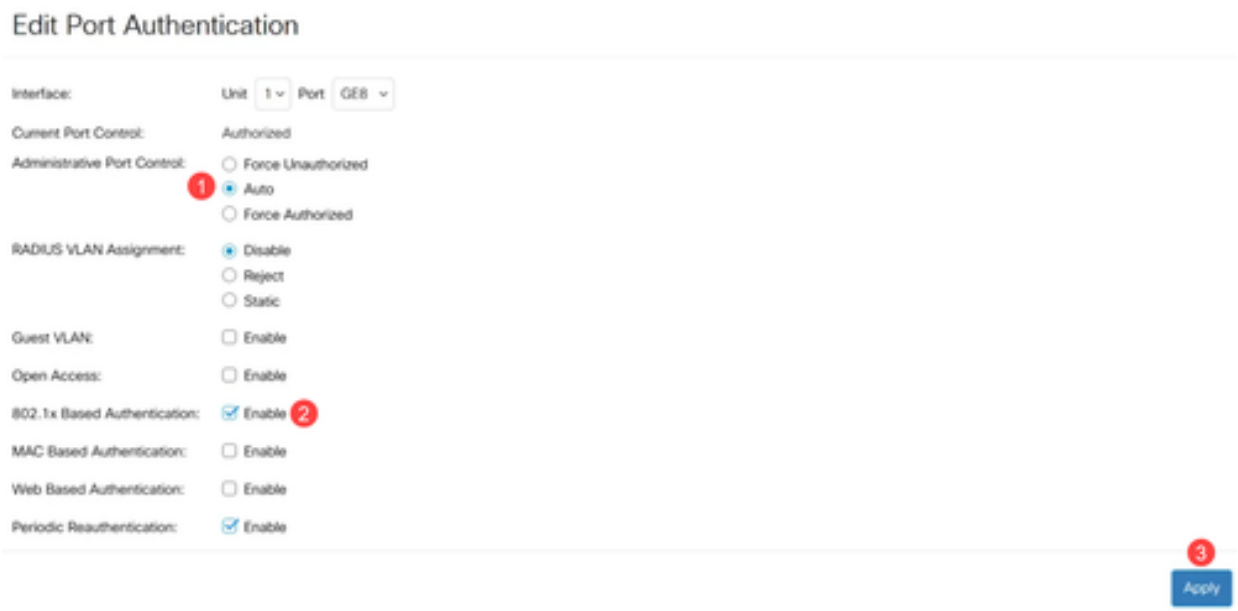
第 4 步

转至Security > 802.1X Authentication > Port Authentication菜单。选择您的笔记本电脑所连接的端口，然后单击edit图标。在本示例中，GE8处于选中状态。



步骤 5

选择Administrative Port Control作为Auto并启用基于802.1x的身份验证。单击 Apply。



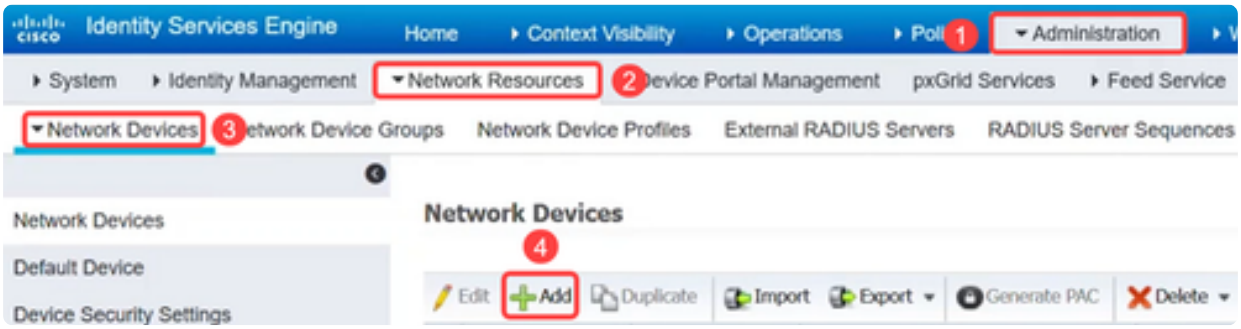
可下载ACL的思科ISE服务器配置

> **Note:**
> ISE配置不属于思科业务支持的范围。有关详细信息，请参阅ISE管理员指南。

本文中所示的配置是可下载ACL与Cisco Catalyst 1300系列交换机配合使用的示例。

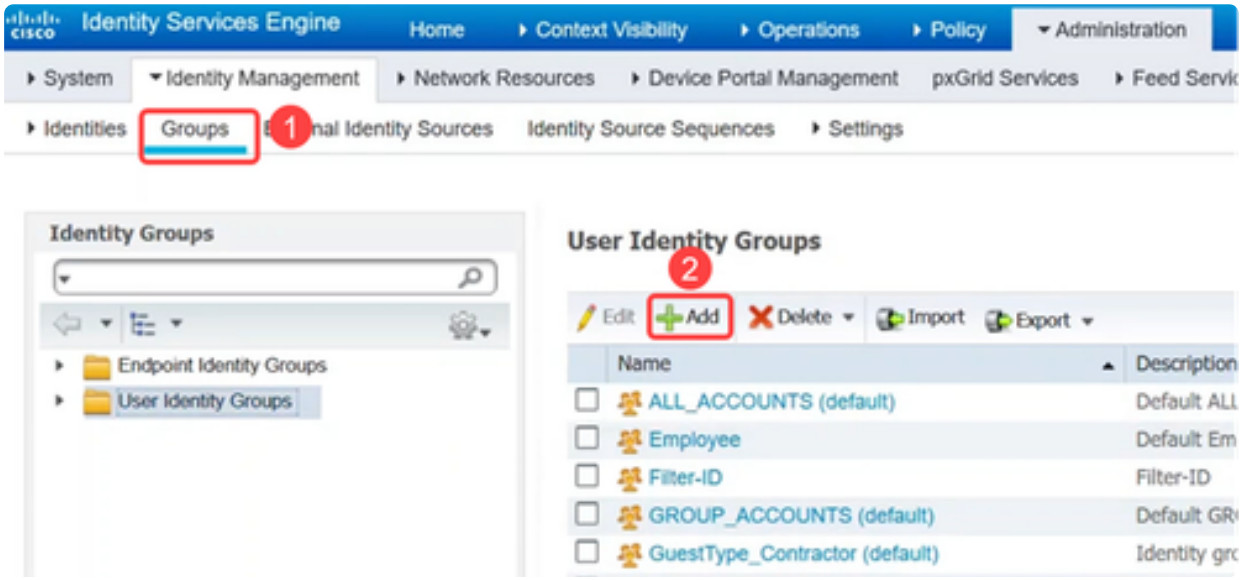
第 1 步

登录到您的Cisco ISE服务器并导航到管理>网络资源>网络设备，然后添加Catalyst交换机设备。



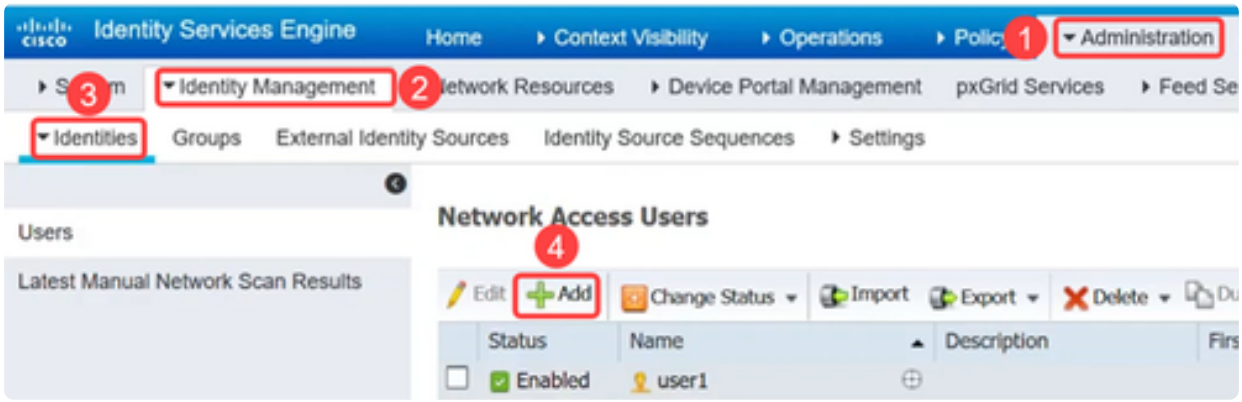
第 2 步

要创建用户身份组，请导航到组选项卡并添加用户身份组。



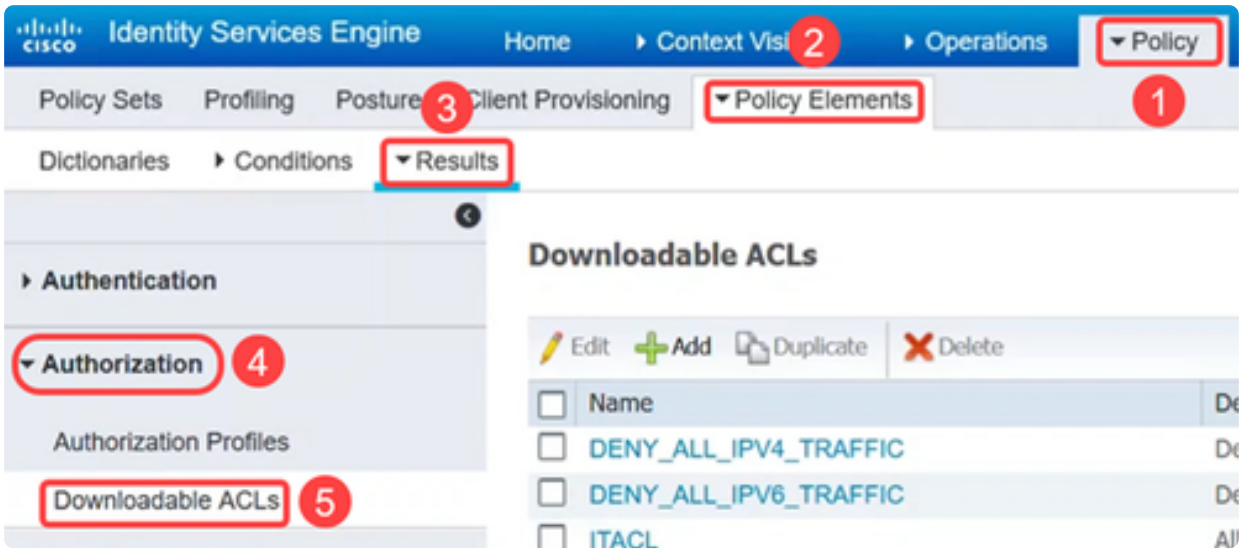
第 3 步

转至Administration > Identity Management > Identities菜单以定义用户并将用户映射到组。



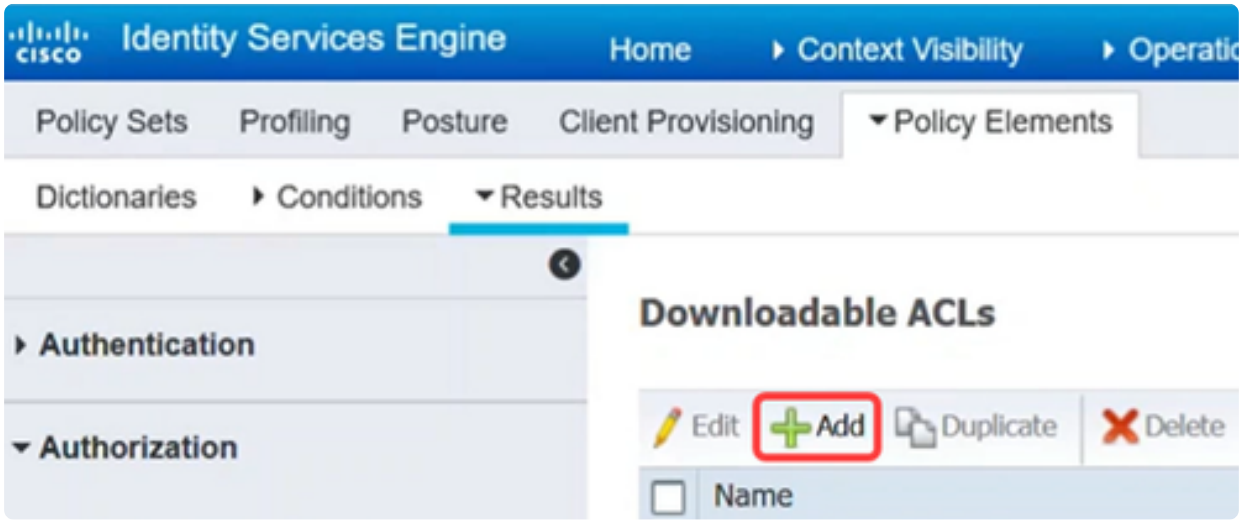
第 4 步

导航到Policy > Policy Elements > Results菜单。在Authorization下，单击Downloadable ACLs。



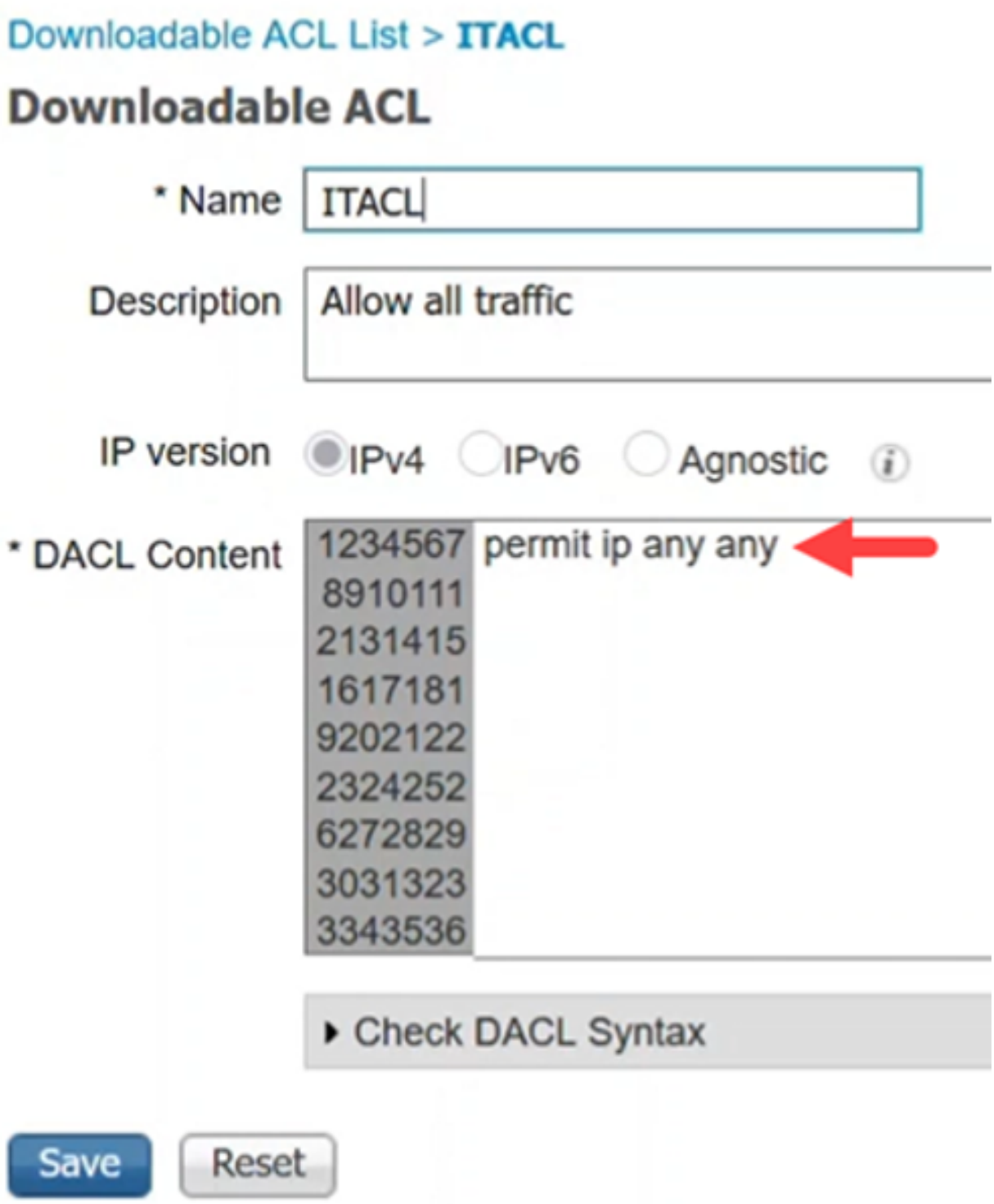
步骤 5

单击Add图标以创建可下载的ACL。



第 6 步

配置Name、Description，选择IP版本，并在DACL Content字段中输入将构成可下载ACL的访问控制条目(ACE)。Click Save.



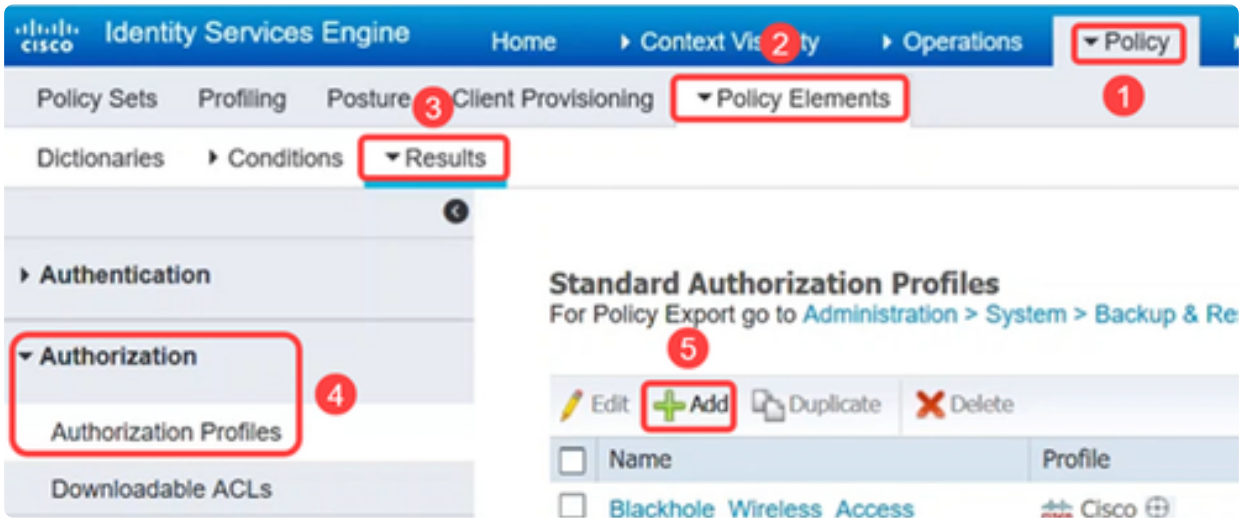
Note:

仅支持IP ACL，并且源必须为ANY。对于ISE上的ACL，现在仅支持IPv4。如果使用其他源输入ACL，尽管对于ISE来说语法可能不错，但应用到交换机时语法会失败。

第 7 步

创建用于在ISE策略集内将DACL和其他策略逻辑关联的授权配置文件。

为此，请导航到Policy > Policy Elements > Results > Authorization > Authorization Profiles，然后点击Add。

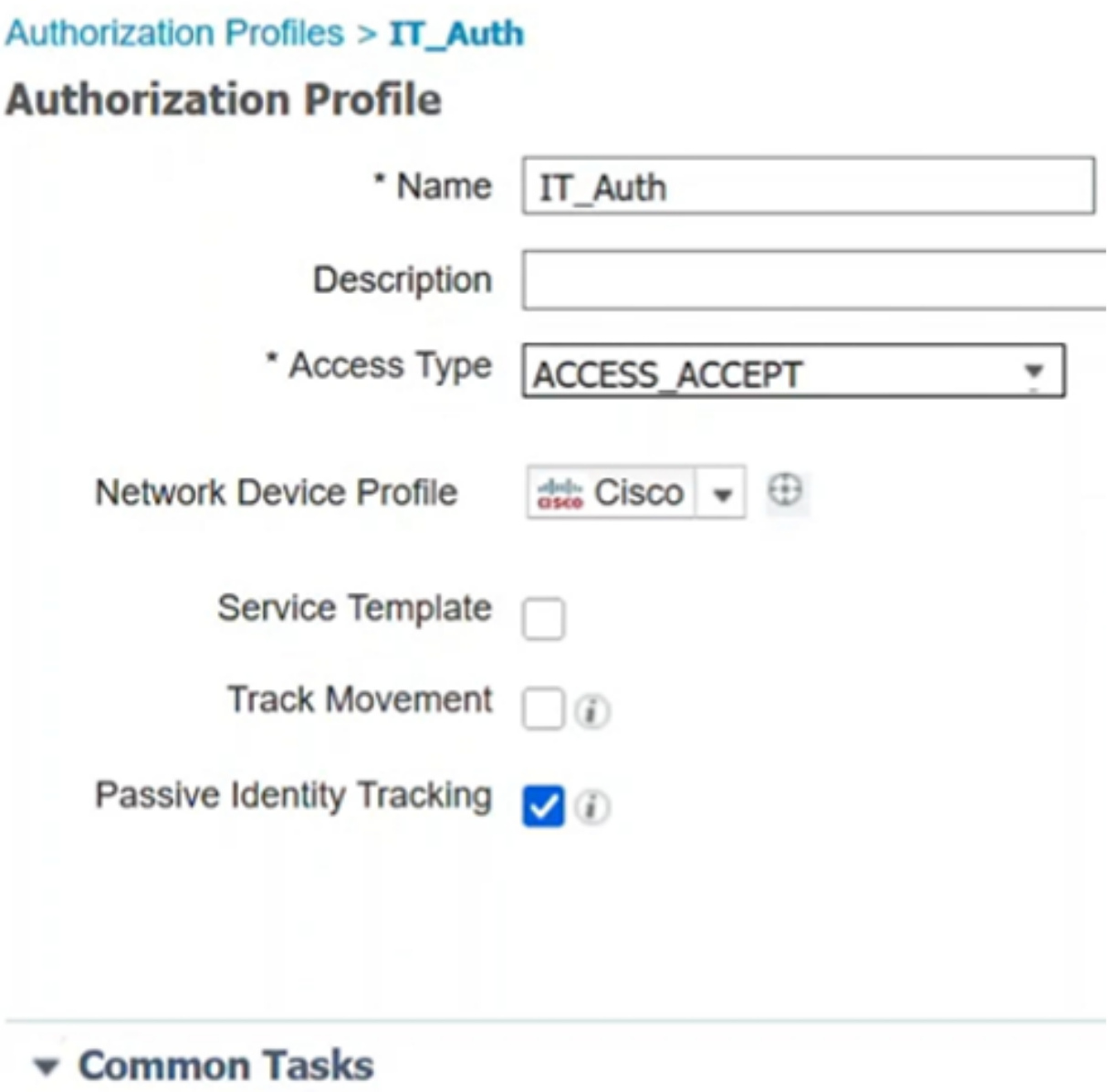


步骤 8

在Authorization Profile页面中，配置以下内容：

- 名称
- 描述
- 访问类型 — 应将其设置为ACCESS_ACCEPT。如果设置为ACCESS_REJECT，它将拒绝身份验证。
- Network Device Profile — 应将其选为Cisco。
- 被动身份跟踪 — 对于某些身份验证方案，可能需要启用。链接到AD的EasyConnect_PassiveID方案需要此参数。
- 常见任务 — 此部分有许多选项。在本示例中，配置了DACL Name。

Click Save.

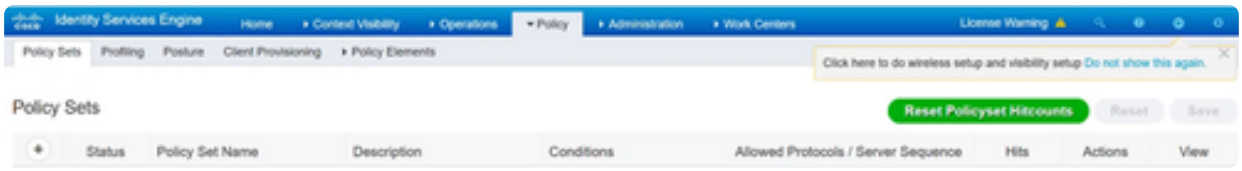


步骤 9

要配置作为身份验证和授权策略的逻辑分组的策略集，请点击Policy > Policy Sets菜单。

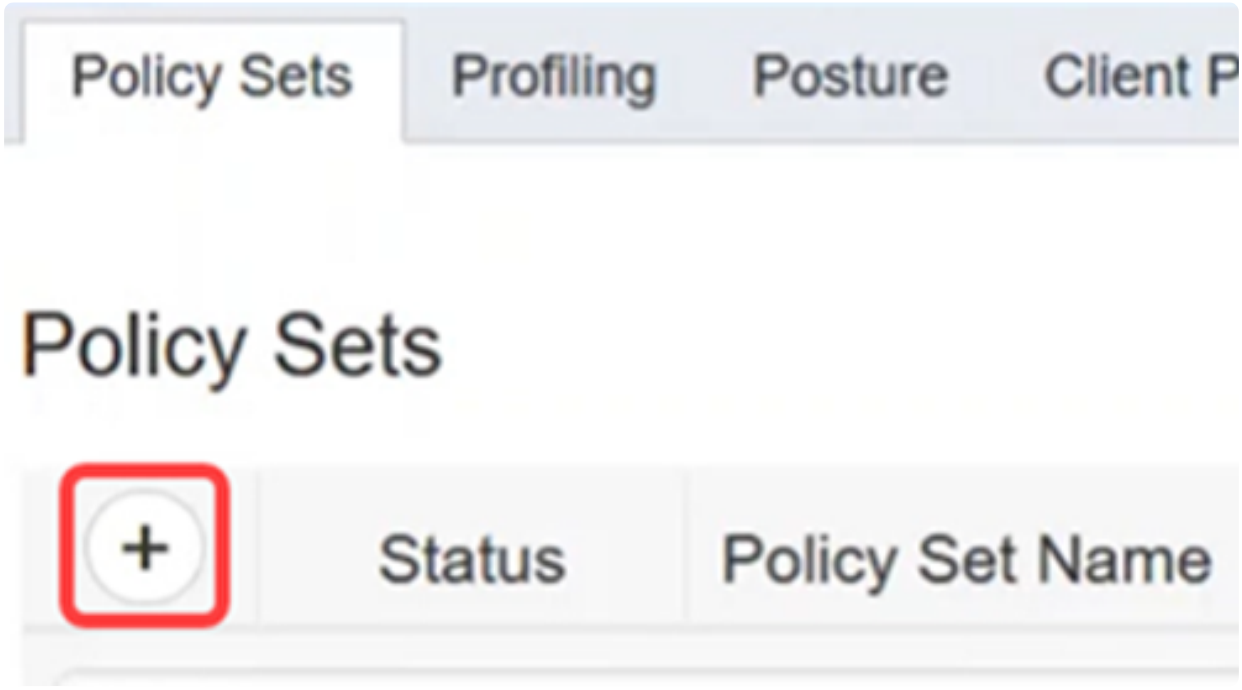
查看策略集列表时，可以查看以下内容：

- 状态 — 绿色勾选表示启用，空的白色圆圈表示禁用，眼睛图标表示仅监控配置。
- 策略集名称和说明 — 不言自明
- 条件 — 定义策略集适用的位置。
- Allowed Protocols/Server Sequence — 设置更高级的控制。
- Hits — 显示策略集已被使用的次数。
- 操作 — 允许您更改可以应用策略集的顺序、复制现有策略集或删除现有策略集。
- View — 允许您编辑策略集详细信息。



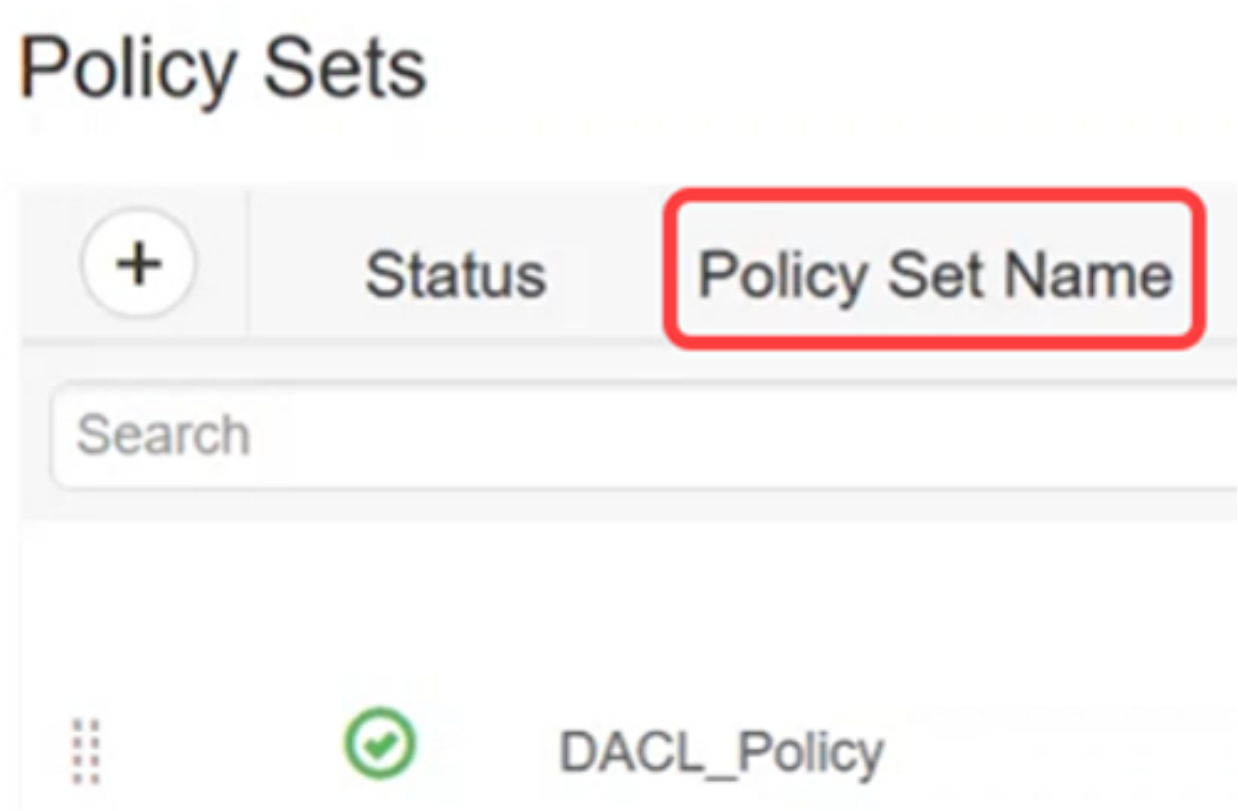
步骤 10

要创建策略集，请点击add按钮。



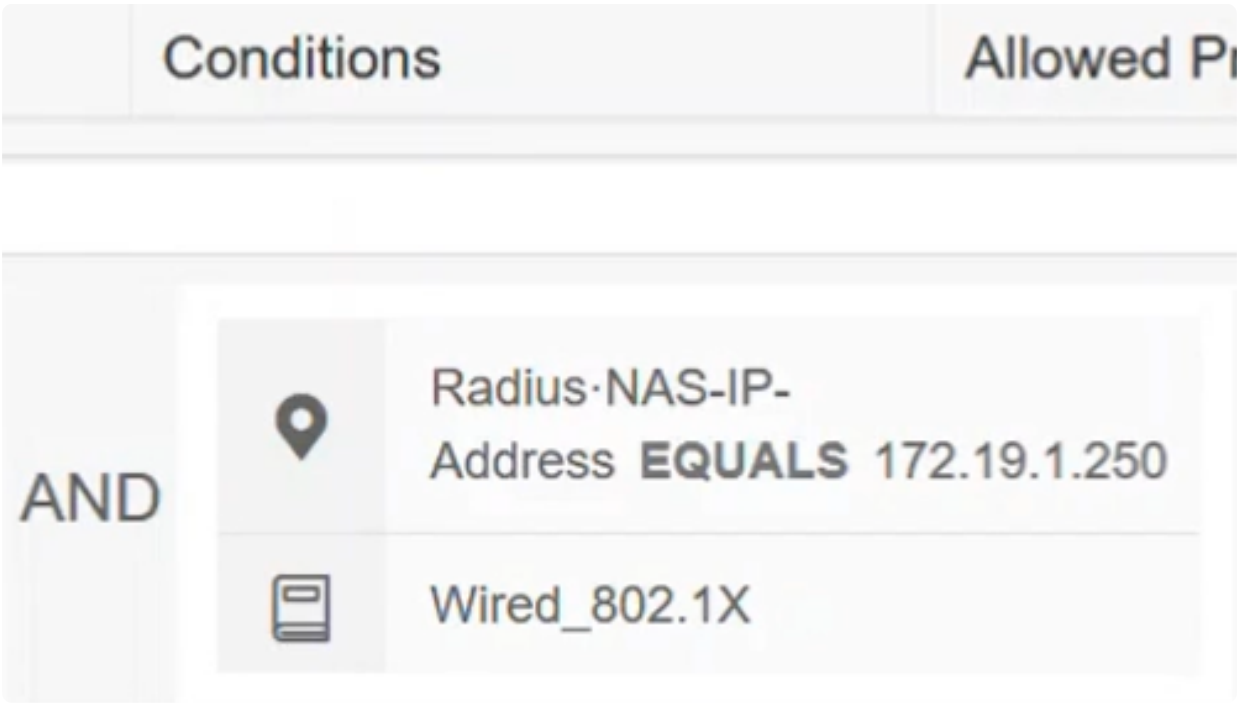
步骤 11

定义策略集名称。



步骤 12

在Conditions下，单击add按钮。这将打开Conditions Studio，您可以在其中定义使用此身份验证配置文件的位置。在本示例中，它应用到Radius-NAS-IP-Address（交换机），即172.19.1.250和wired_802.1x流量。



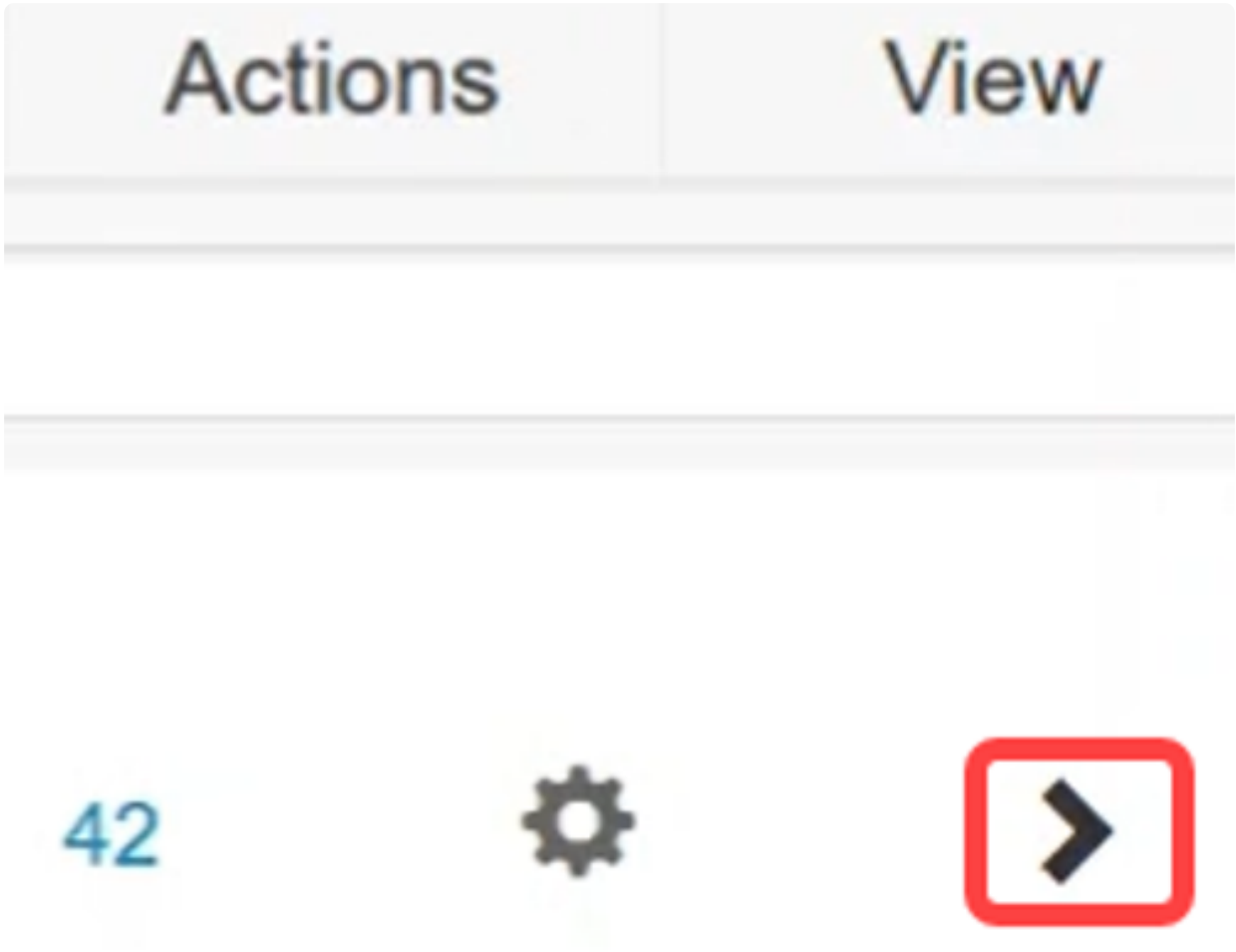
步骤 13

将Allowed Protocols配置为Default Network Access，然后单击Save。



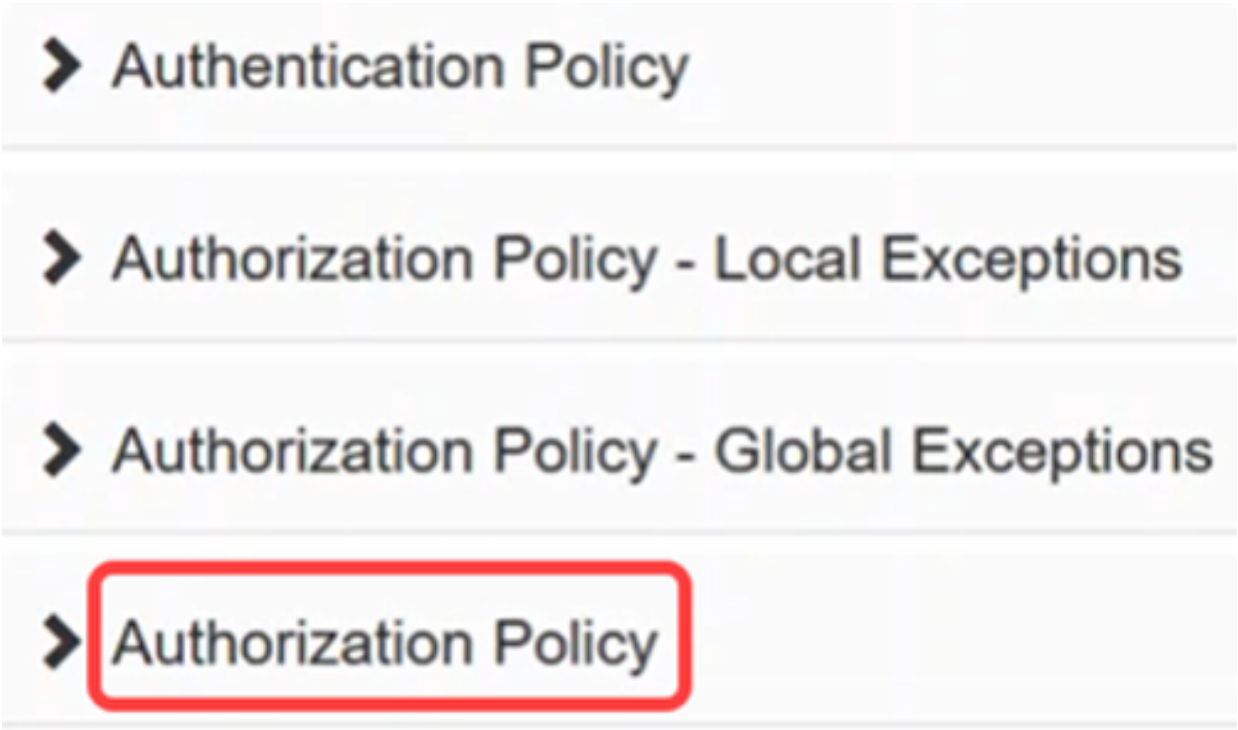
步骤 14

在View下，点击箭头图标，根据您的网络设置和要求配置身份验证和授权策略，或者您可以选择默认设置。在本示例中，点击Authorization policy。



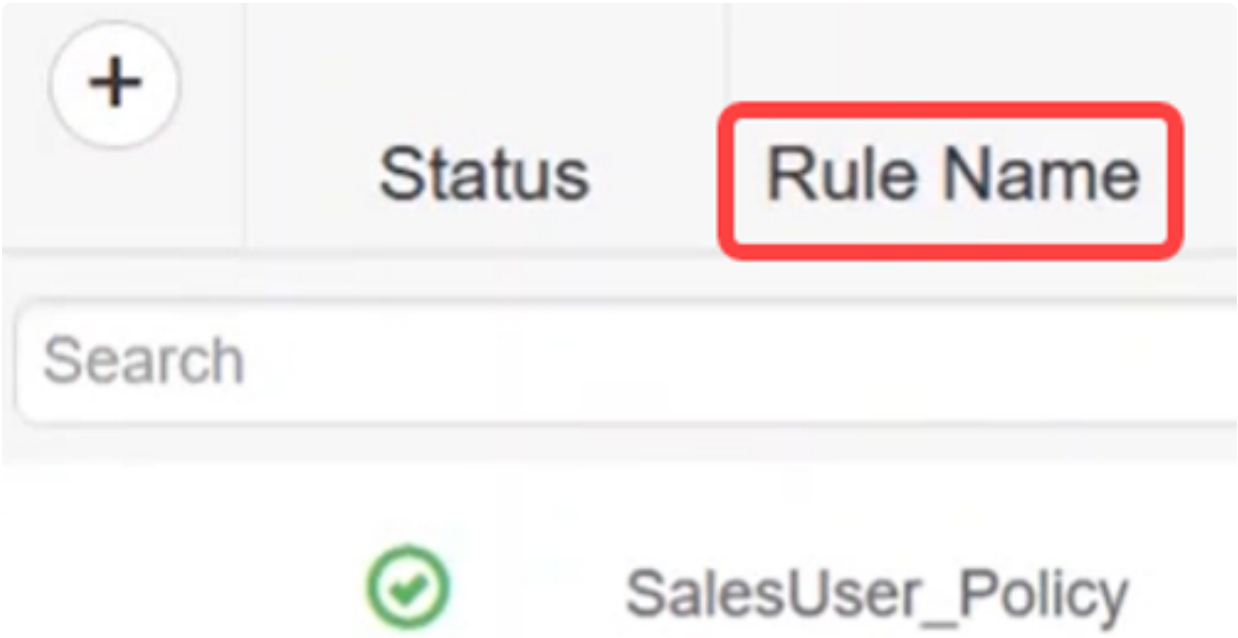
步骤 15

单击plus图标添加策略。



步骤 16

输入Rule Name。



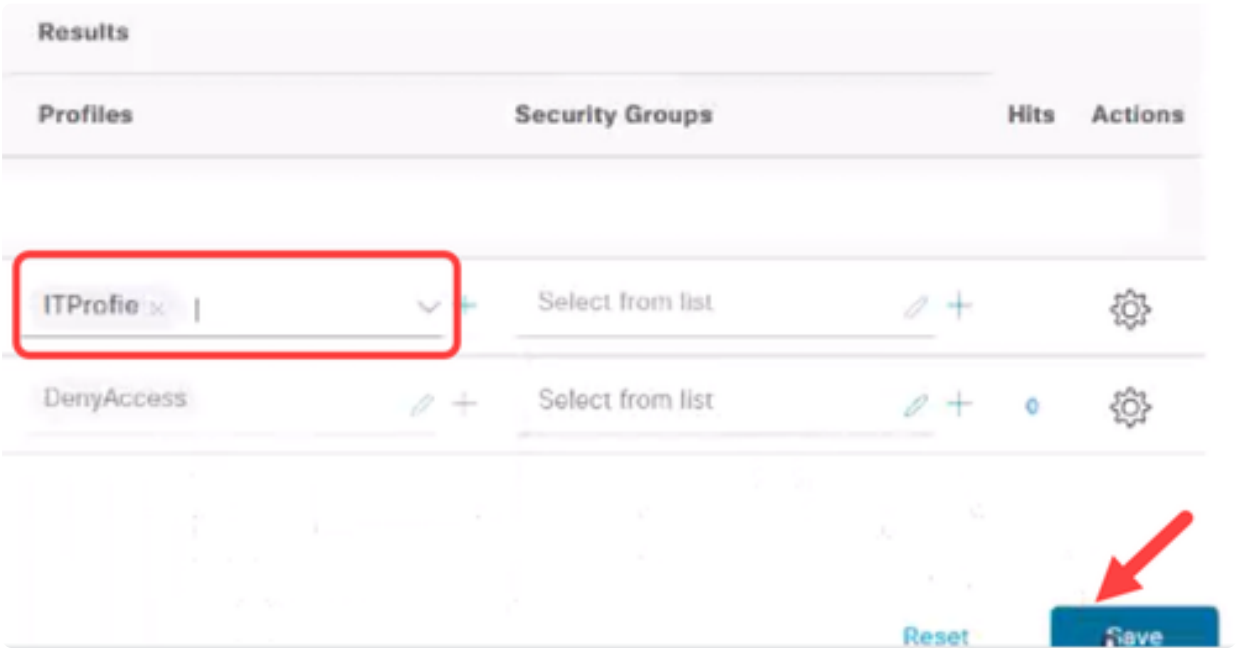
步骤 17

在Conditions下，点击加号图标并选择身份组。单击Use。



步骤 18

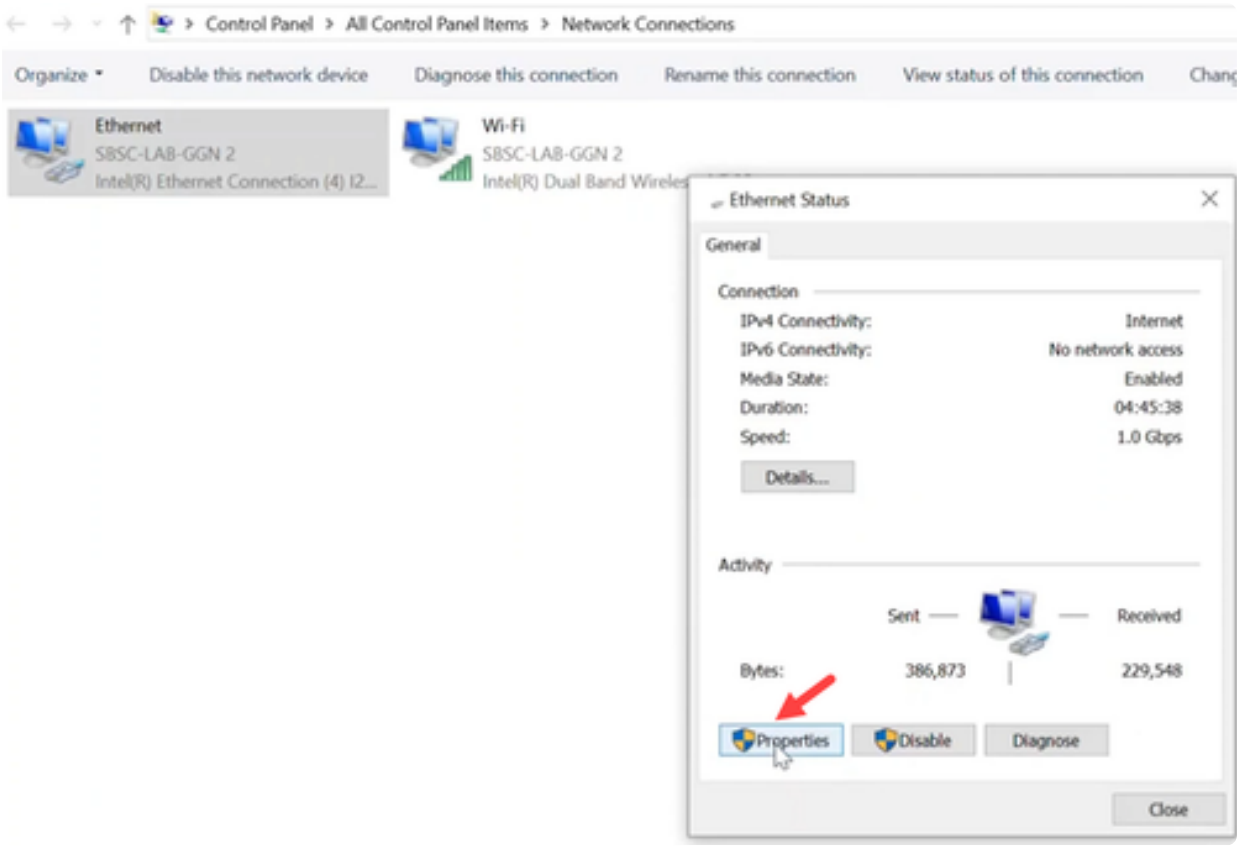
应用所需的配置文件，然后单击Save。



客户端配置

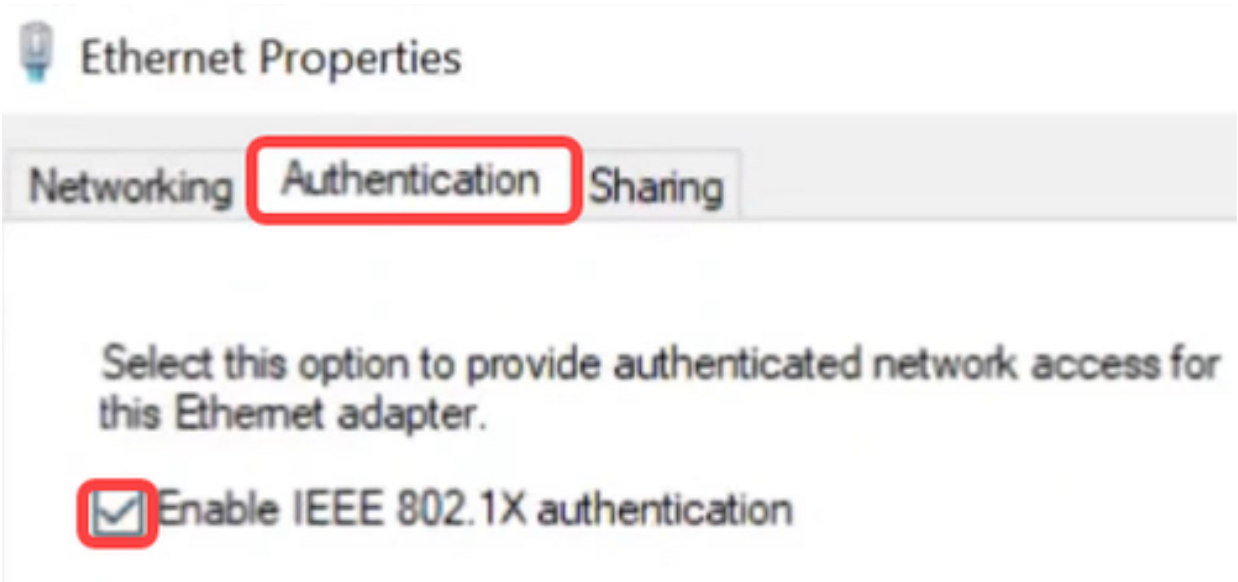
第 1 步

在客户端笔记本电脑上，导航到网络连接>以太网，然后单击属性。



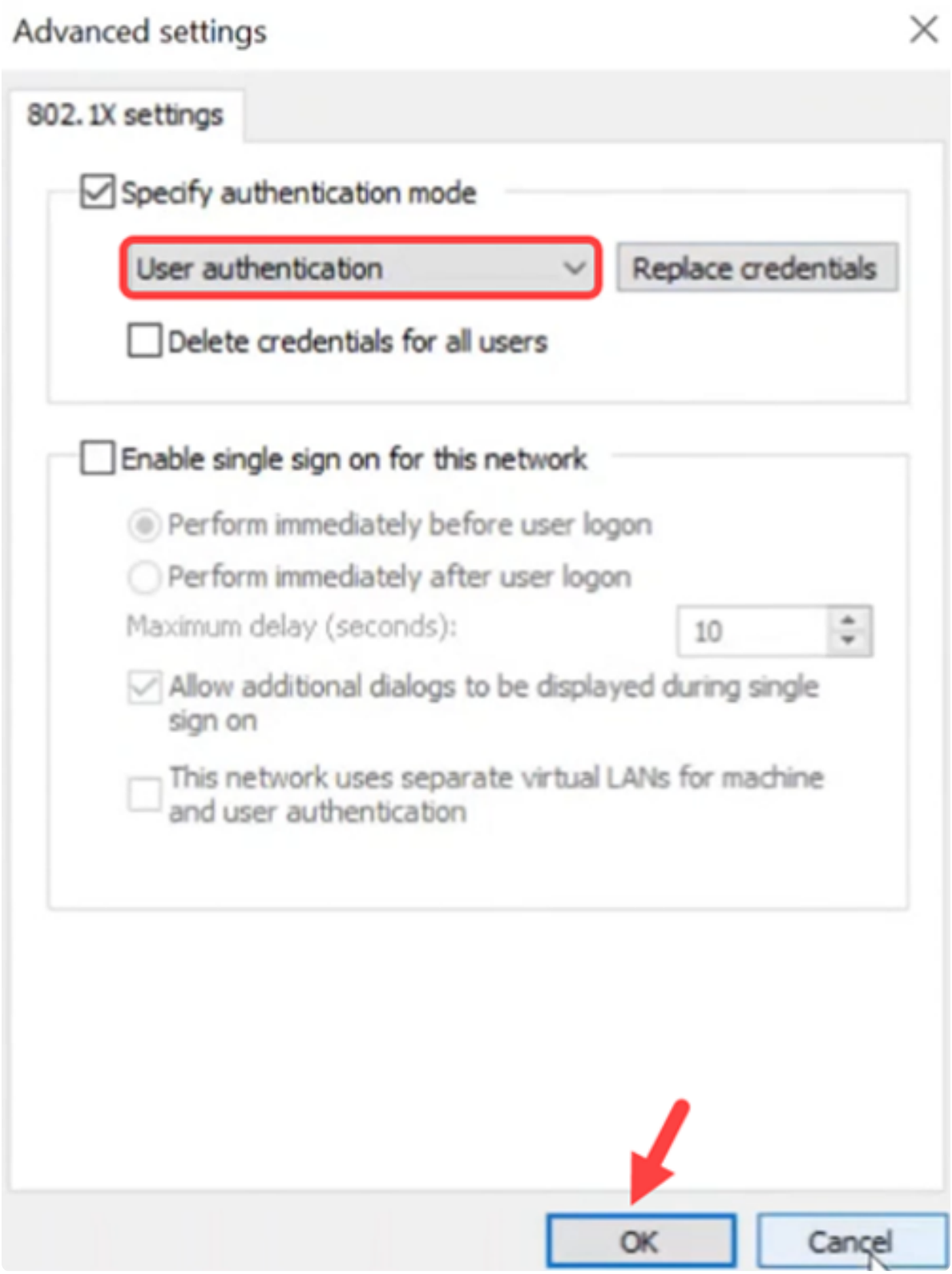
第 2 步

单击Authentication选项卡并确保已启用802.1X authentication。



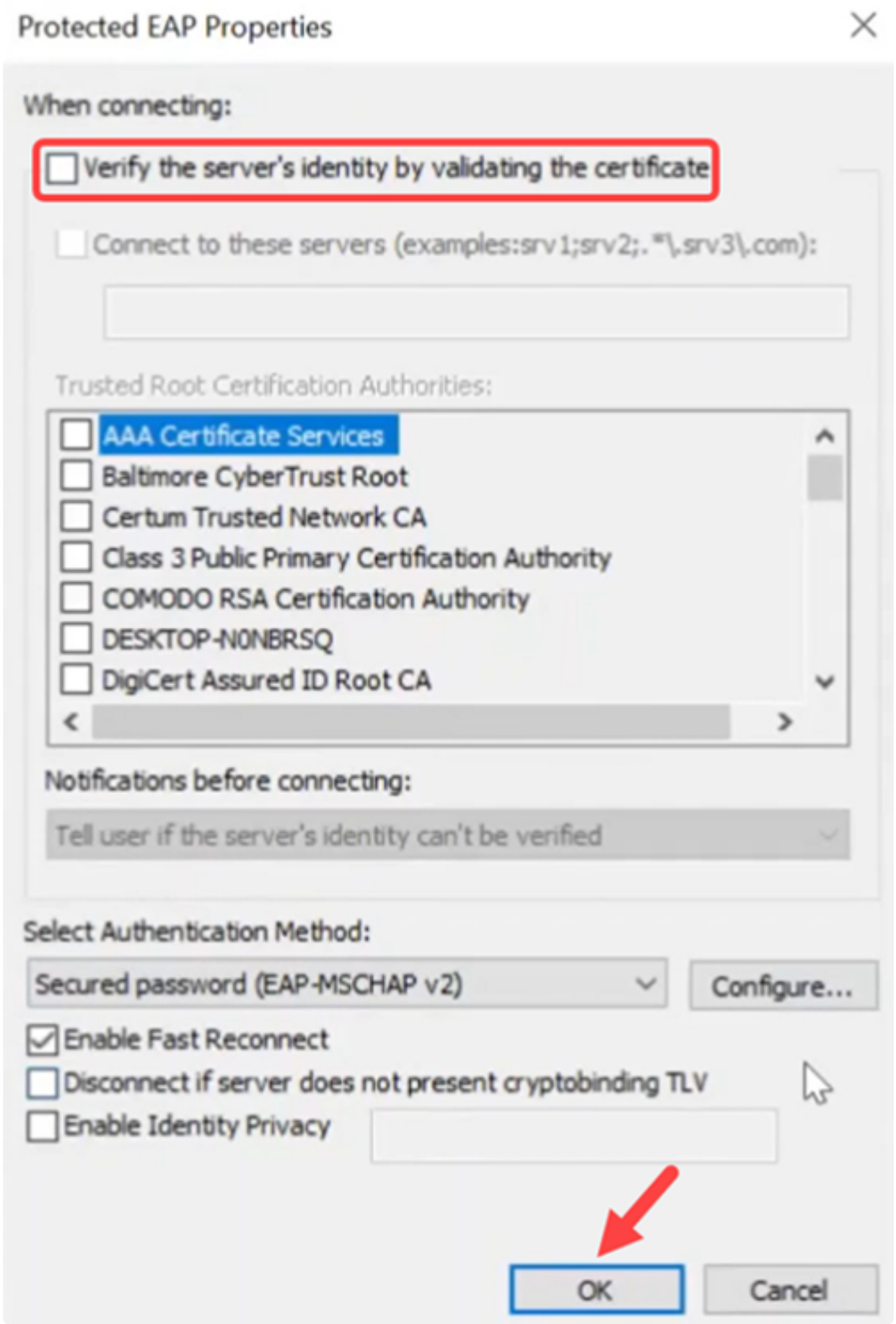
第 3 步

在Additional Settings下，选择User authentication作为身份验证模式。单击Save Credentials，然后单击OK。



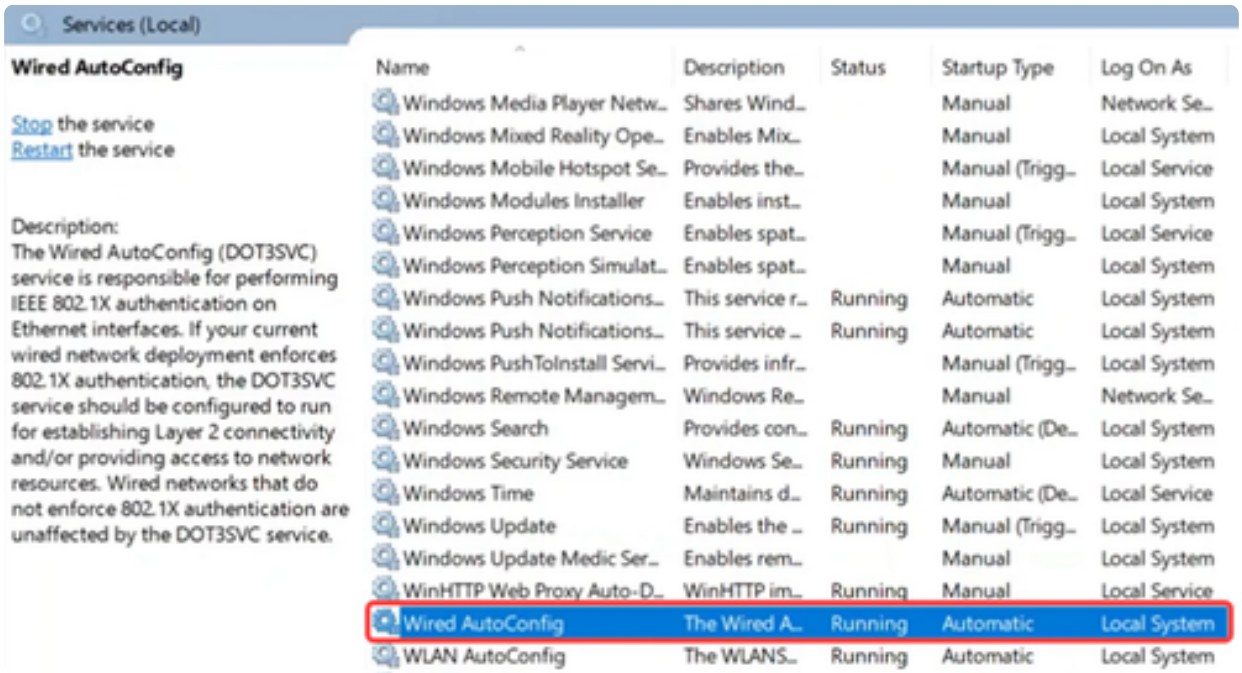
第 4 步

单击Settings，并确保未选中Verify the server’s identity by validating the certificate旁边的框。Click OK.


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

步骤 5

在Services下，启用Wired AutoConfig 设置。

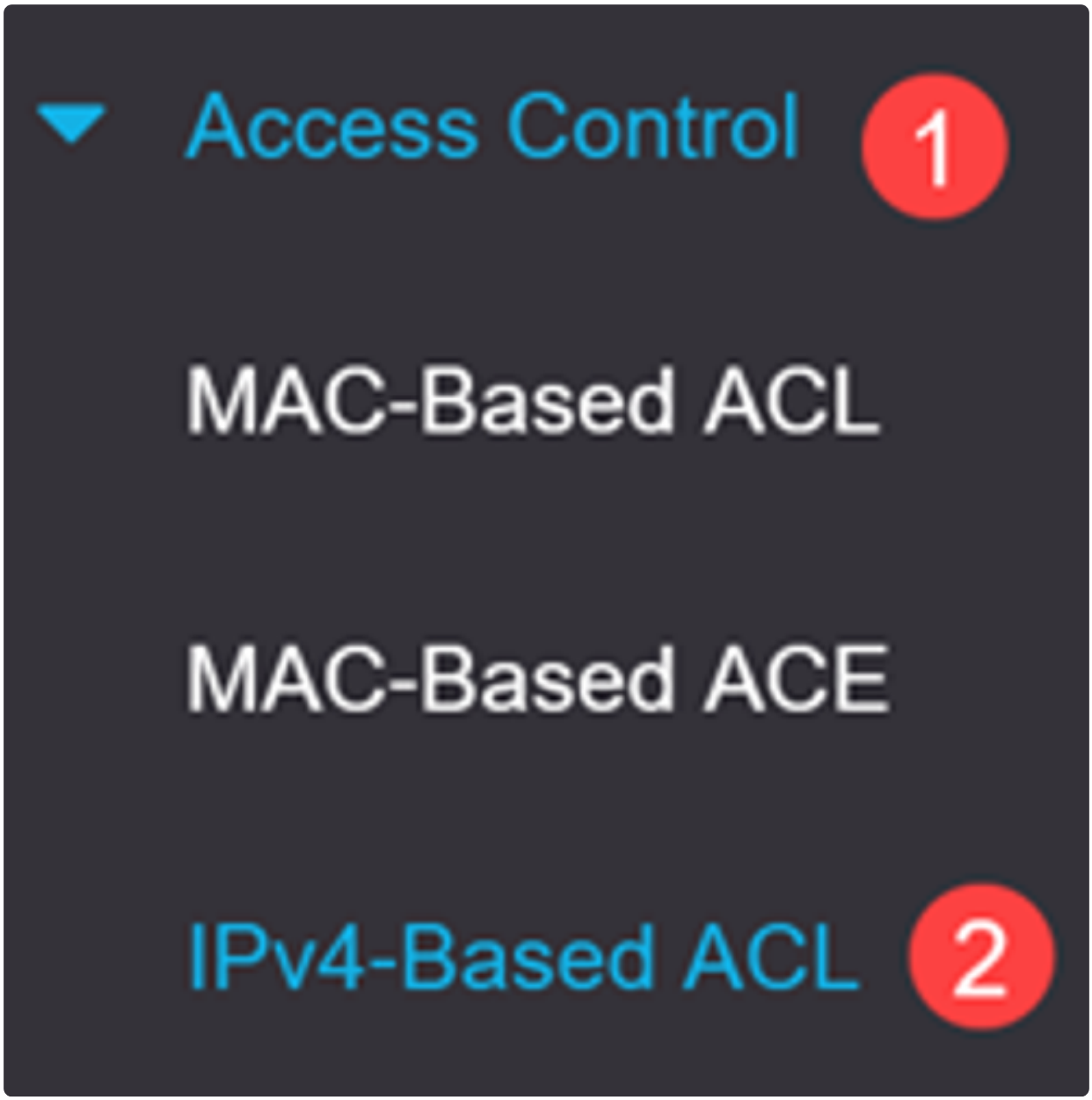


DACL验证

用户通过身份验证后，您可以验证可下载ACL。

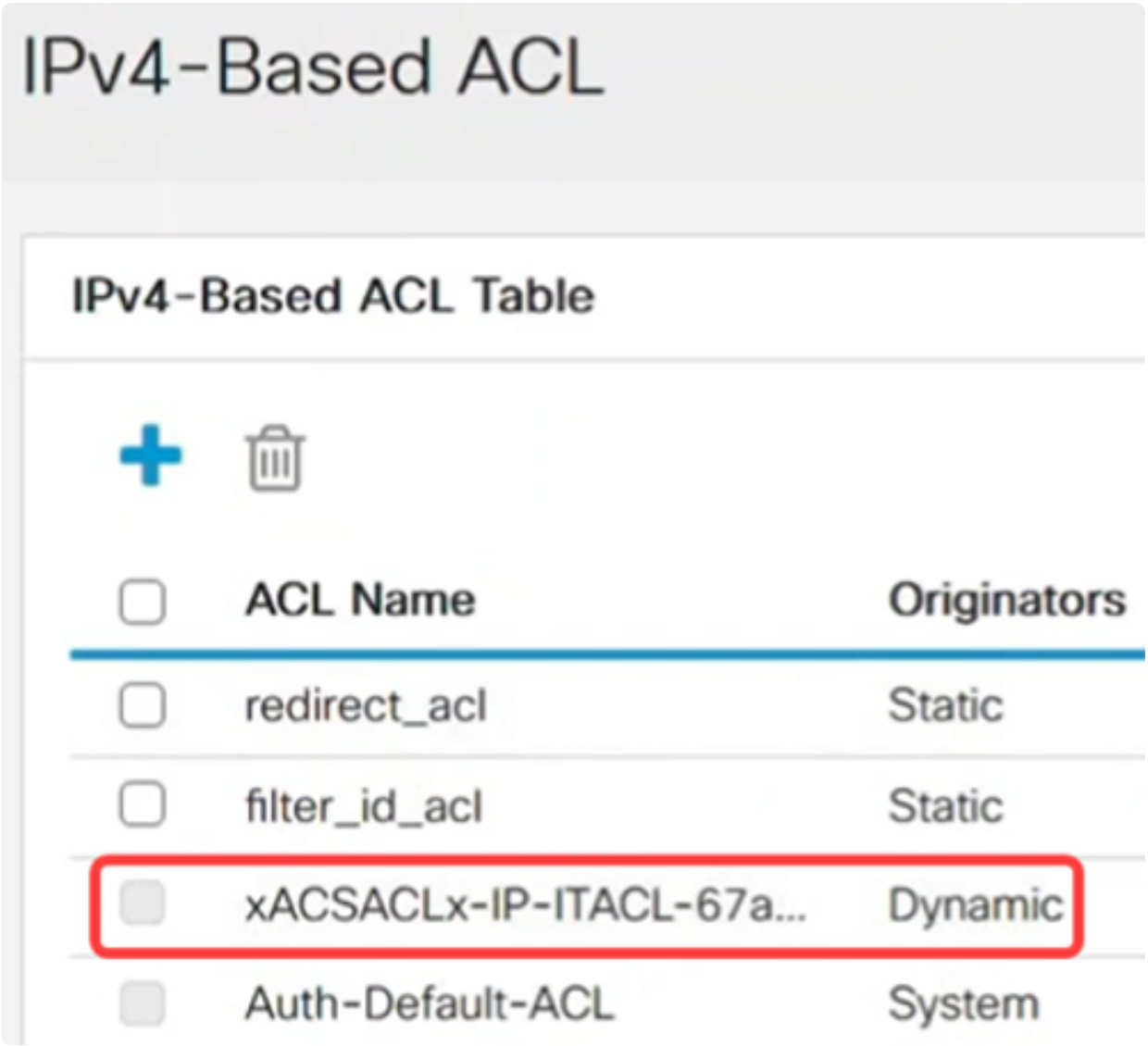
第 1 步

登录到Catalyst 1300交换机，然后导航到访问控制>基于IPv4的ACL菜单。



第 2 步

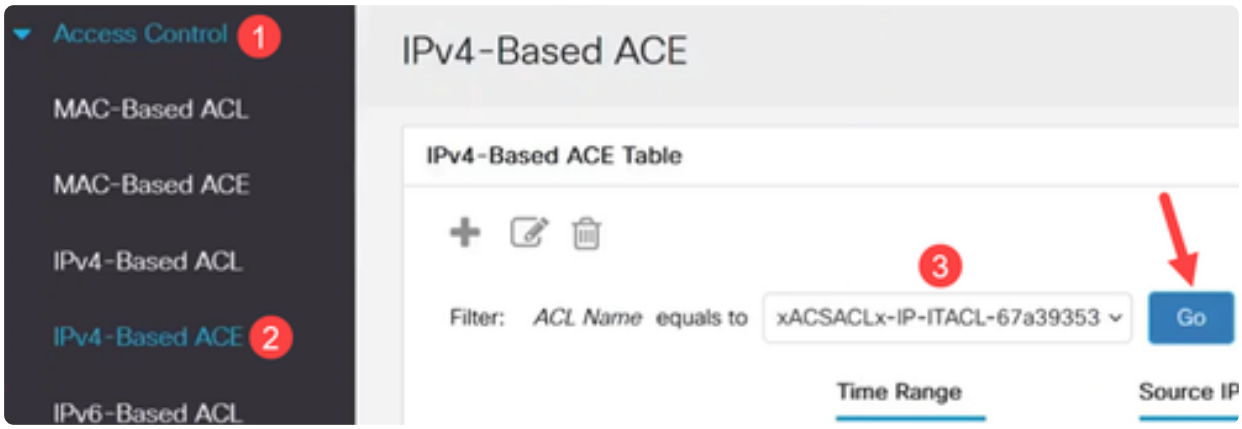
基于IPv4的ACL表将显示下载的ACL。



Note:
无法编辑可下载的ACL。

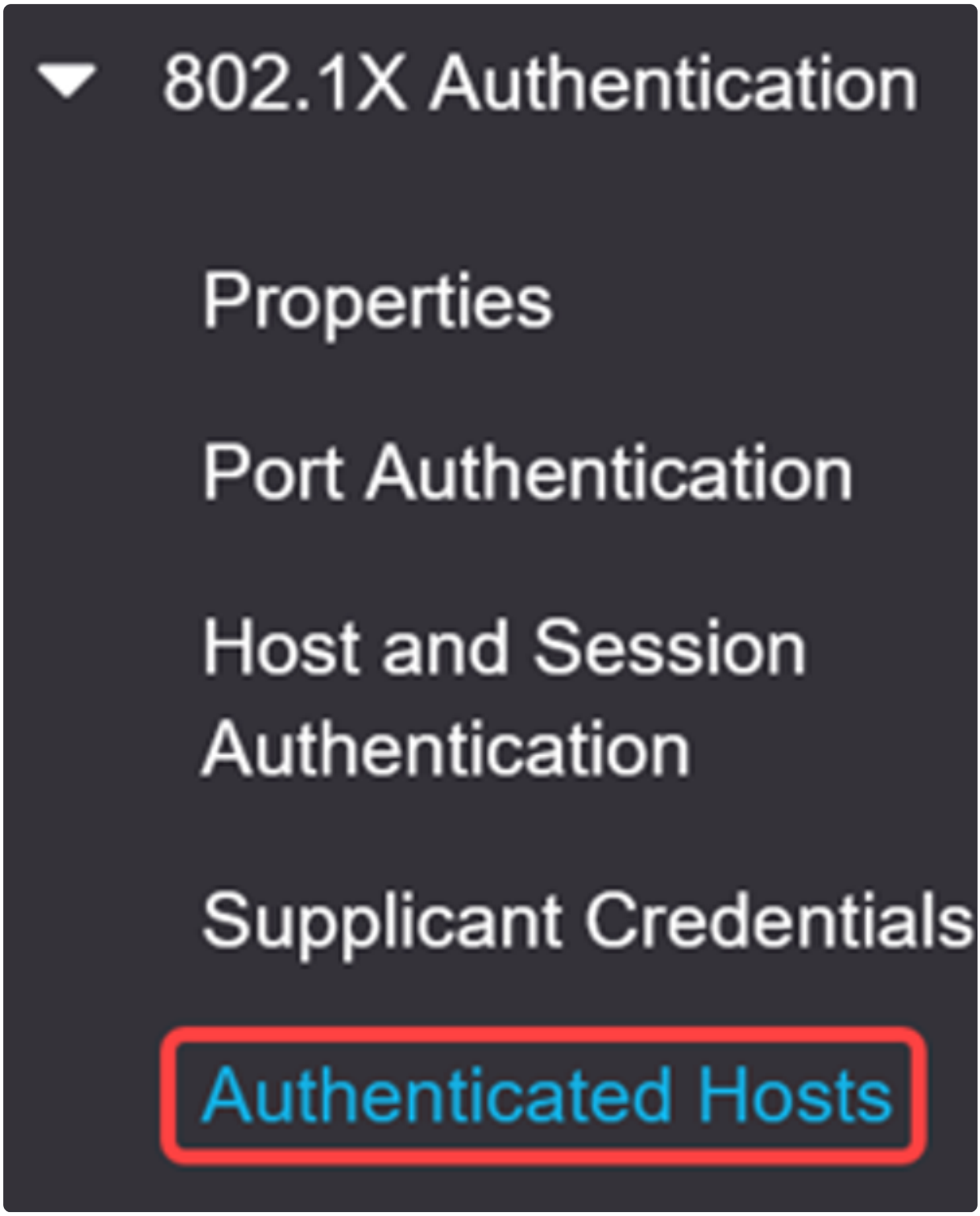
第 3 步

另一种验证方法是导航到基于IPv4的ACE，从ACL名称下拉菜单中选择可下载的ACL，然后单击Go。将显示在ISE中配置的规则。



第 4 步

导航到Security > 802.1 Authentication > Authenticated Hosts菜单。您可以验证经过身份验证的用户。单击Authenticated Sessions查看更多详细信息。



步骤 5

从CLI运行命令show ip access-lists interface，后跟接口ID。

在本例中，可以看到应用于千兆以太网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
```

第 6 步

您还可以使用命令查看与ISE连接和ACL下载相关的设置

show dot1x sessions interface <ID> detailed。您可以查看状态、802.1x身份验证状态以及下载的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
```

结论

好了！现在您已经知道可下载ACL如何在Cisco Catalyst 1300交换机和Cisco ISE上运行

。

有关详细信息，请参阅Catalyst 1300管理指南和Cisco Catalyst 1300系列支持页。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。