Catalyst 1300 스위치에서 다운로드 가능한 ACL

목표

이 문서의 목적은 Cisco Catalyst 1300 스위치와 Cisco ISE(Identity Service Engine)에서 DACL(Downloadable Access Control List)이 어떻게 작동하는지 설명하는 것입니다.

적용 가능한 디바이스 | 소프트웨어 버전

- Catalyst 1300 시리즈 | 4.1.6.54

소개

동적 ACL은 사용자 계정 그룹 구성원 자격, 시간 등과 같은 정책 또는 기준을 기반으로 스위치 포트에 할당되는 ACL입니다. 필터 ID 또는 다운로드 가능한 ACL(DACL)에 의해 지정된 로컬 ACL일 수 있습니다.

다운로드 가능 한 ACL는 Cisco ISE 서버에서 작성 하고 다운로드 하는 동적 ACL입니다. 사용자 ID 및 디바이스 유형에 따라 액세스 제어 규칙을 동적으로 적용합니다. DACL은 ACL을 위한 하나의 중앙 리포지토리를 가질 수 있으므로 각 스위치에서 수동으로 생성할 필요가 없다는 장점이 있습니다. 사용자가 스위치에 연결할 때 인증만 하면 되고 스위치는 Cisco ISE 서버에서 해당 ACL을 다운로드합니다.

다운로드 가능한 ACL의 활용 사례

1. 사용자가 스위치에 연결할 때 서로 다른 ACL을 수신합니다(로컬 ISE 사용자).
2. 네트워크 연결이 제한된 사용자는 중앙 웹 포털에 로그인하여 전체 네트워크 액세스(중앙 웹 인증)를 수행할 수 있습니다.
3. 고급 - ISE 서버를 AD에 연결하고 사용자 인증을 모니터링하는 동안 MAB(MAC Authentication Bypass)를 사용하여 Windows AD(Active Directory) 및 일부 관련 서비스에 대한 통신을 허용합니다. Windows AD 로그인 전에 네트워크는 매우 제한된 리소스에 대한 액세스만 허용하지만, AD 인증은 Windows 그룹을 기반으로 다른 ACL을 다운로드하고 전체 네트워크 액세스를 허용합니다.
4. 고급 - 사용자는 요일, 시간 또는 ISE 서버의 정책 때문에 다른 요인에 따라 다른 ACL을 받습니다.

이 글에서는 첫 번째 활용 사례에 대해 자세히 설명합니다.

목차

- 다운로드 가능한 ACL을 위한 Cisco ISE 서버 컨피그레이션
- 클라이언트 컨피그레이션
- DACL 확인

사전 요구 사항

- Catalyst 1300 스위치가 최신 펌웨어로 업그레이드되었는지 확인합니다(스위치 펌웨어는 4.1.6 이상이어야 함).
- 관리를 위해 스위치에 고정 IP를 할당합니다.

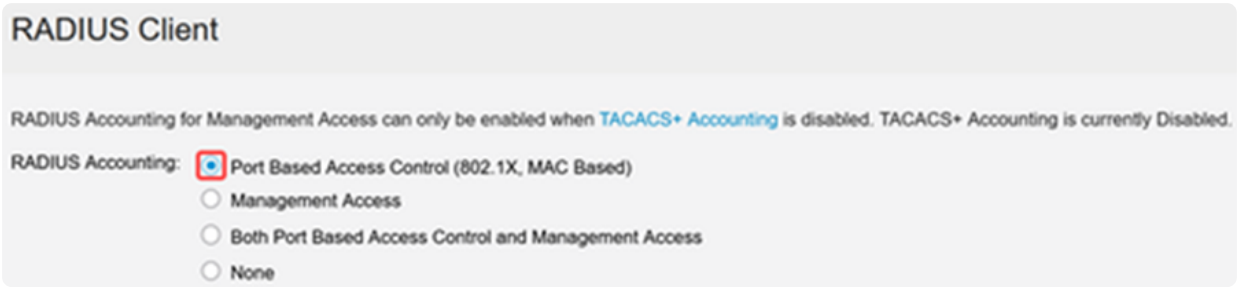
RADIUS 클라이언트 구성

1단계

Catalyst 1300 스위치에 로그인하고 Security(보안) > RADIUS Client(RADIUS 클라이언트) 메뉴로 이동합니다.

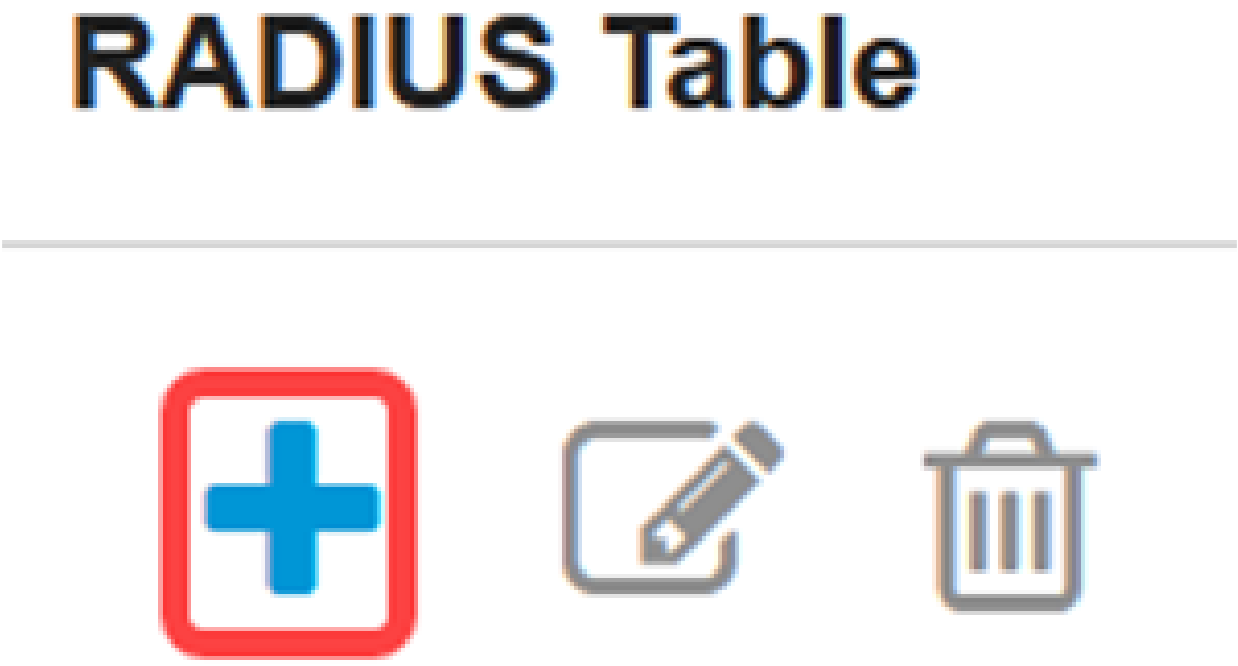
2단계

RADIUS Accounting(RADIUS 어카운팅)의 경우 Port Based Access Control(포트 기반 액세스 제어) 옵션을 선택합니다.



3단계

RADIUS Table(RADIUS 테이블)에서 더하기 아이콘을 클릭하여 Cisco ISE 서버를 추가합니다.



4단계

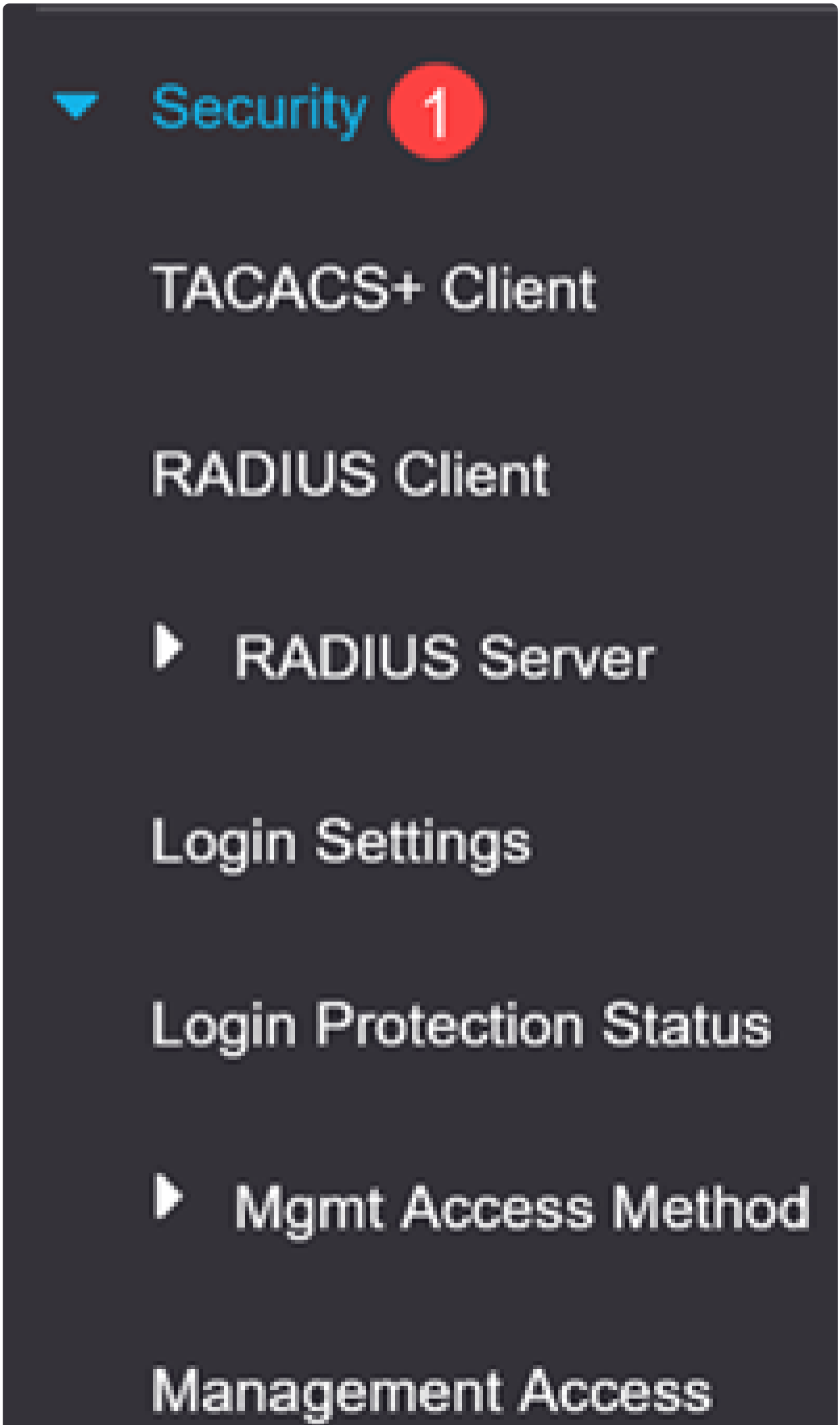
Cisco ISE 서버 세부 정보를 입력 하고 적용을 클릭 합니다.

> **Note:**
> 사용 유형은 802.1x로 선택해야 합니다.

802.1x 인증 구성

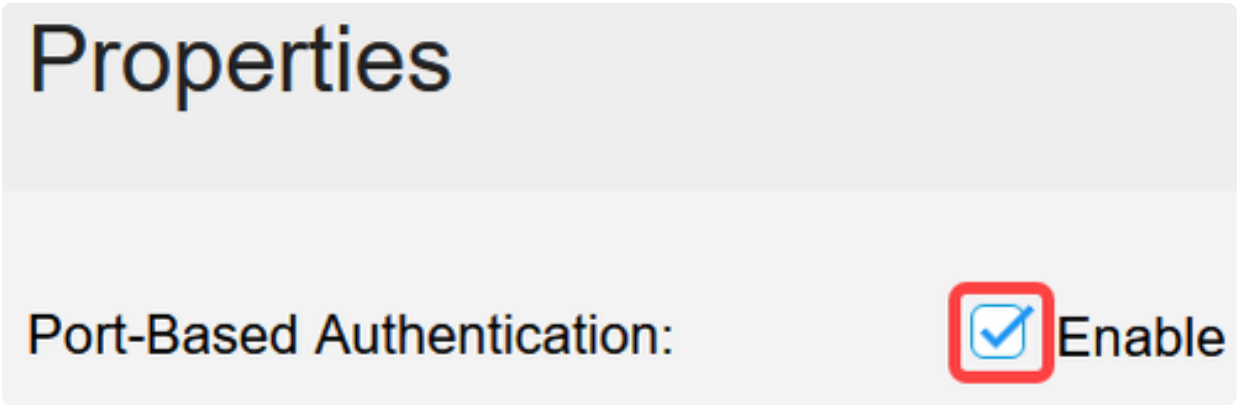
1단계

Security(보안) > 802.1X Authentication(802.1X 인증) > Properties(속성) 메뉴로 이동합니다.


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

2단계

포트 기반 인증을 활성화 하려면 확인 란을 클릭 합니다.

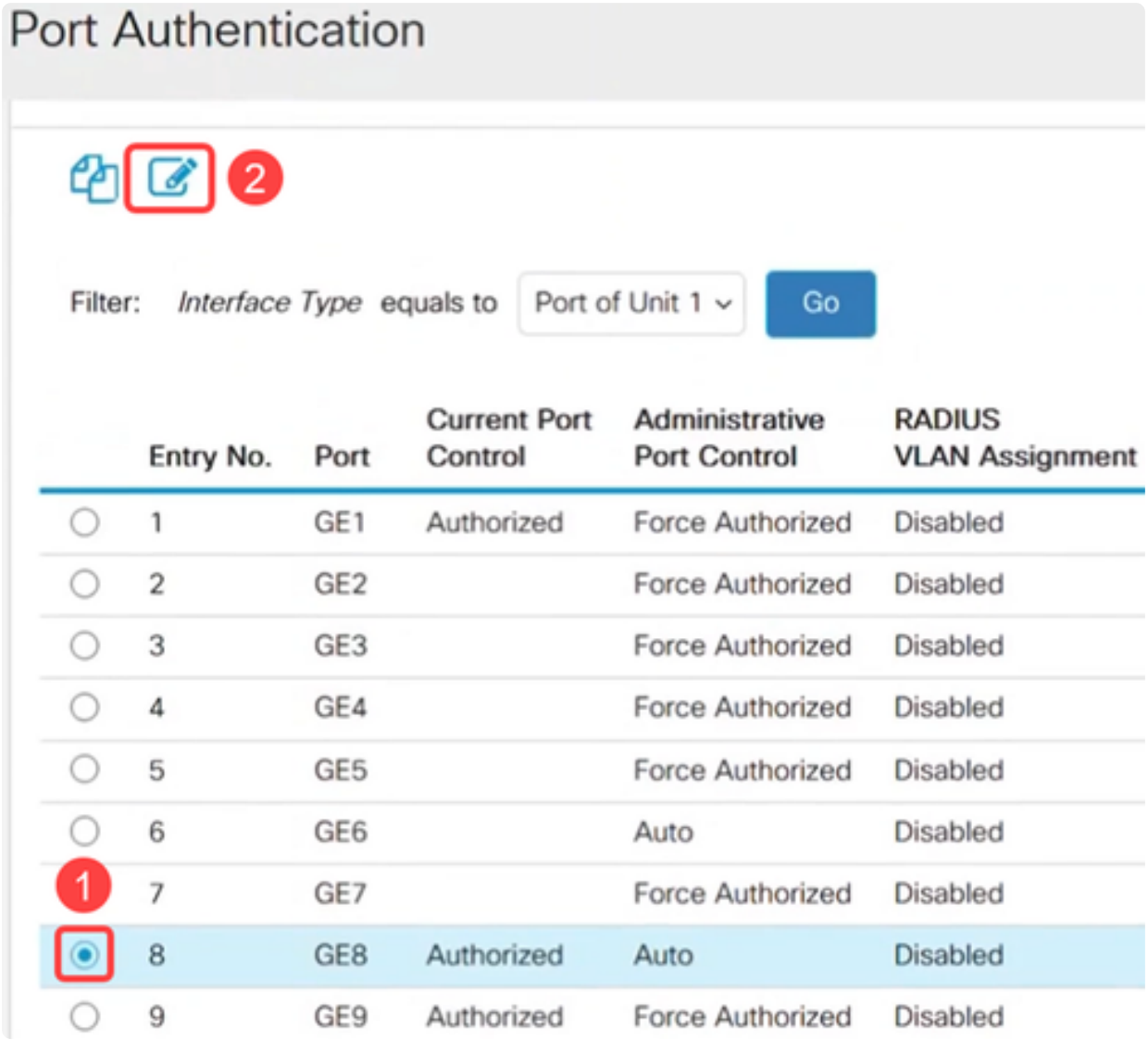


3단계

Authentication Method(인증 방법) 아래에서 RADIUS를 선택하고 Apply(적용)를 클릭합니다.

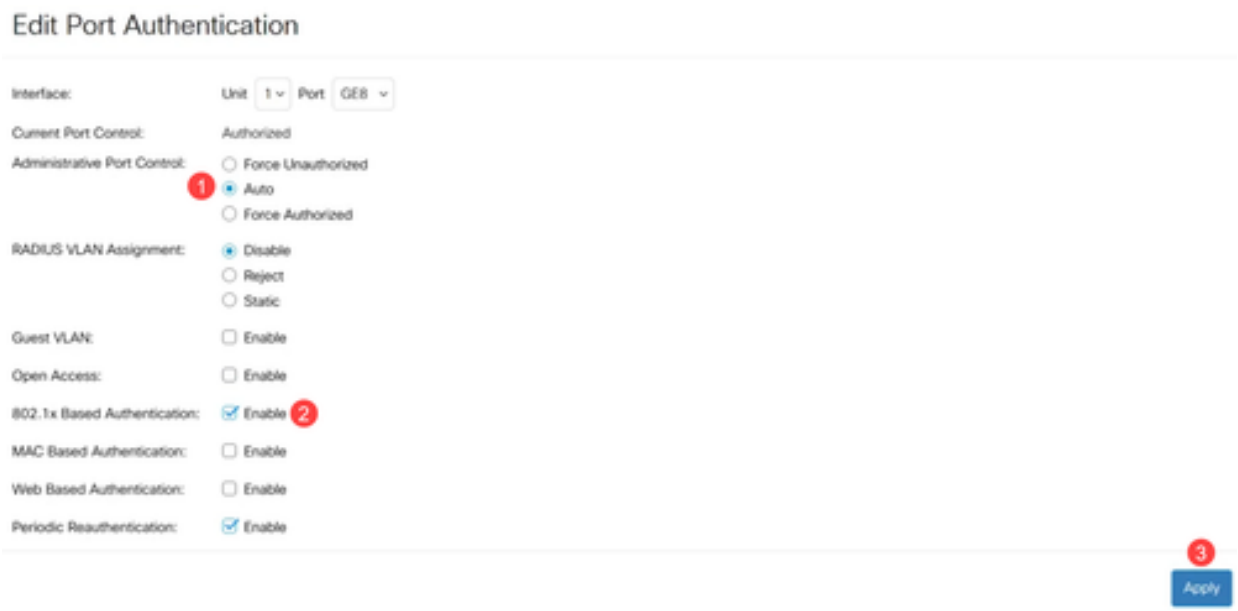
4단계

Security(보안) > 802.1X Authentication(802.1X 인증) > Port Authentication(포트 인증) 메뉴로 이동합니다. 노트북 컴퓨터가 연결된 포트를 선택하고 수정 아이콘을 클릭합니다. 이 예제에서는 GE8을 선택합니다.



5단계

관리 포트 제어를 자동으로 선택하고 802.1x 기반 인증을 활성화합니다. 적용을 클릭합니다.



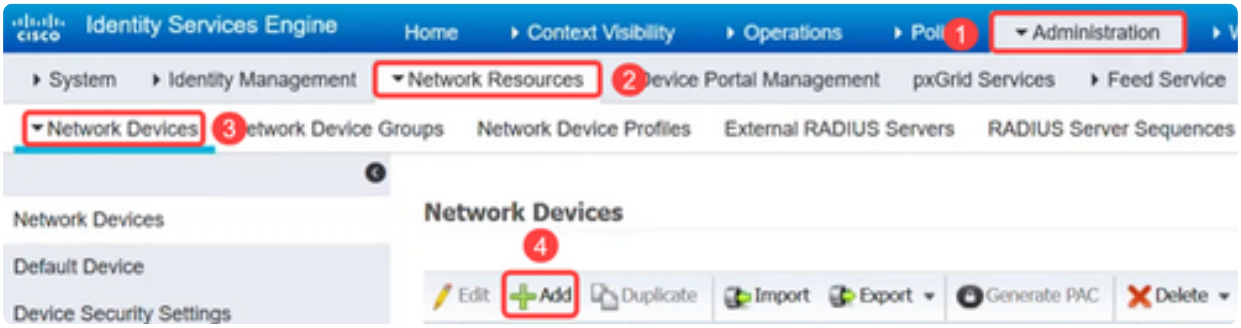
다운로드 가능한 ACL을 위한 Cisco ISE 서버 컨피그레이션

> **Note:**
> ISE 컨피그레이션은 Cisco Business 지원 범위를 벗어납니다. 자세한 내용은 ISE 관리 가이드를 참조하십시오.

이 문서의 구성은 Cisco Catalyst 1300 Series 스위치와 함께 사용할 수 있는 다운로드 가능한 ACL의 예입니다.

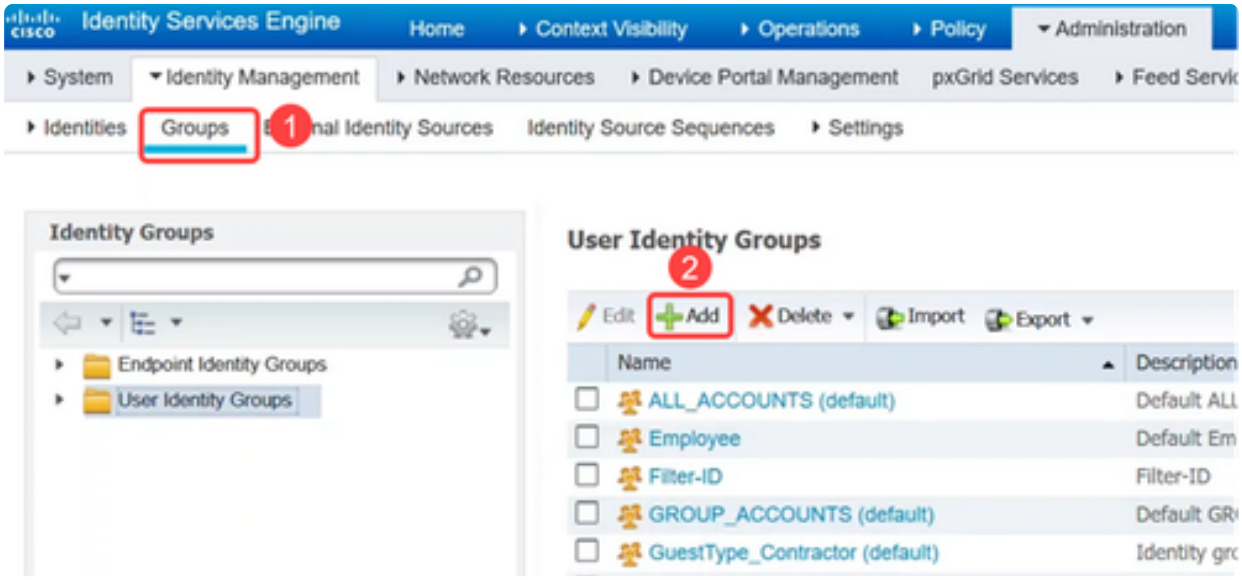
1단계

Cisco ISE 서버에 로그인하고 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동하여 Catalyst 스위치 디바이스를 추가합니다.



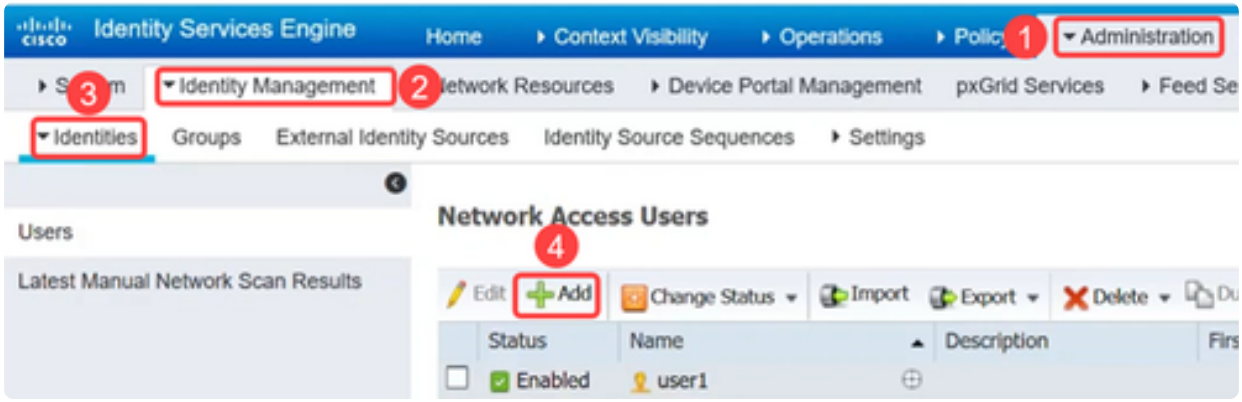
2단계

사용자 ID 그룹을 생성하려면 Groups(그룹) 탭으로 이동하여 User Identity Groups(사용자 ID 그룹)를 추가합니다.



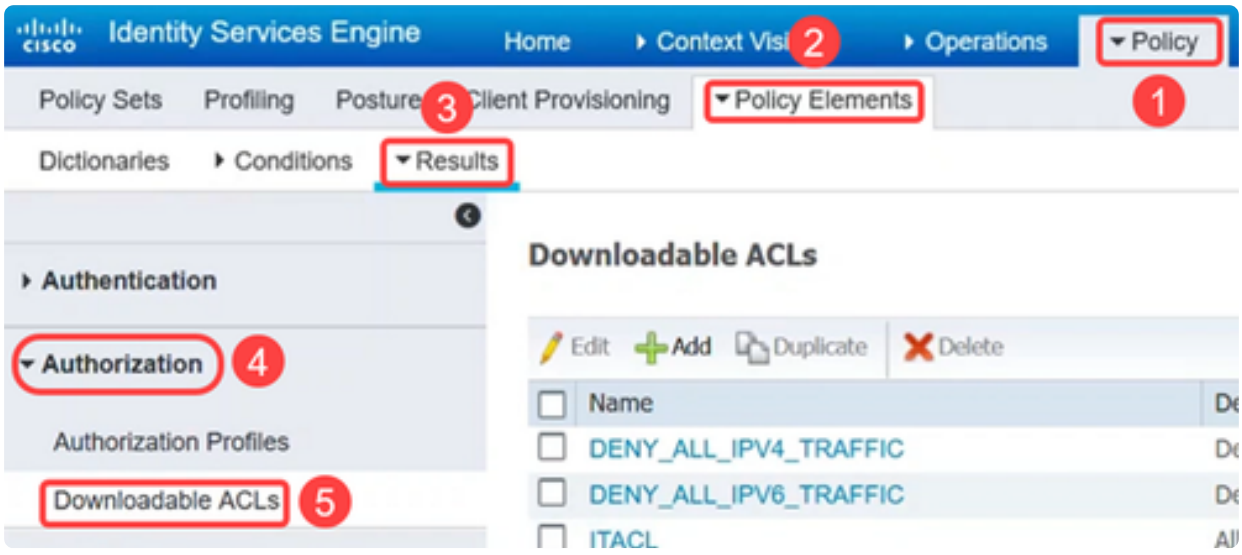
3단계

Administration(관리) > Identity Management(ID 관리) > Identities(ID) 메뉴로 이동하여 사용자를 정의하고 사용자를 그룹에 매핑합니다.



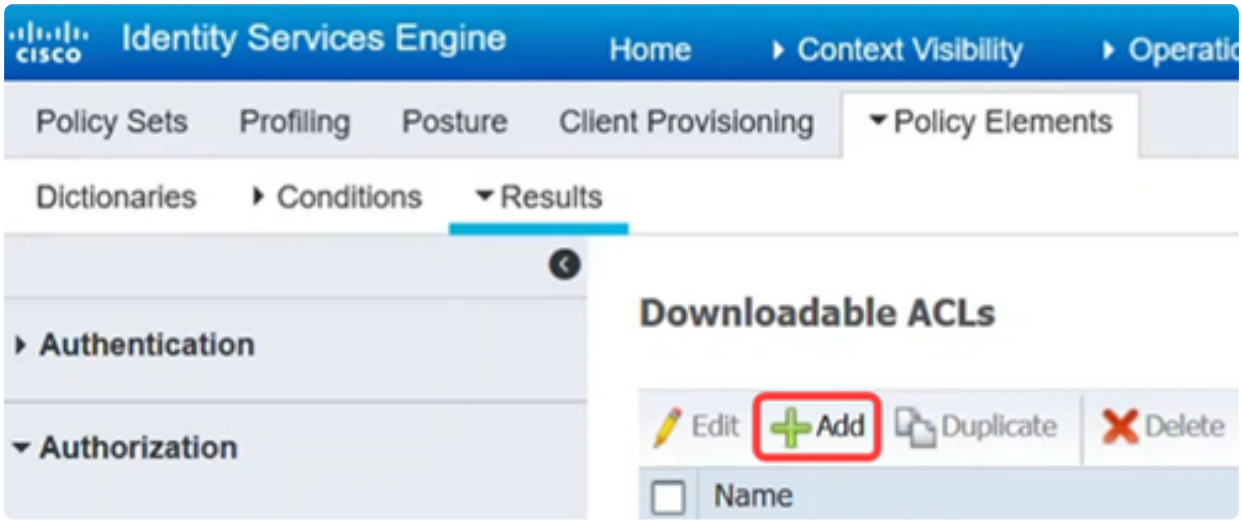
4단계

Policy(정책) > Policy Elements(정책 요소) > Results(결과) 메뉴로 이동합니다. Authorization(권한 부여)에서 Downloadable ACLs(다운로드 가능한 ACL)를 클릭합니다.



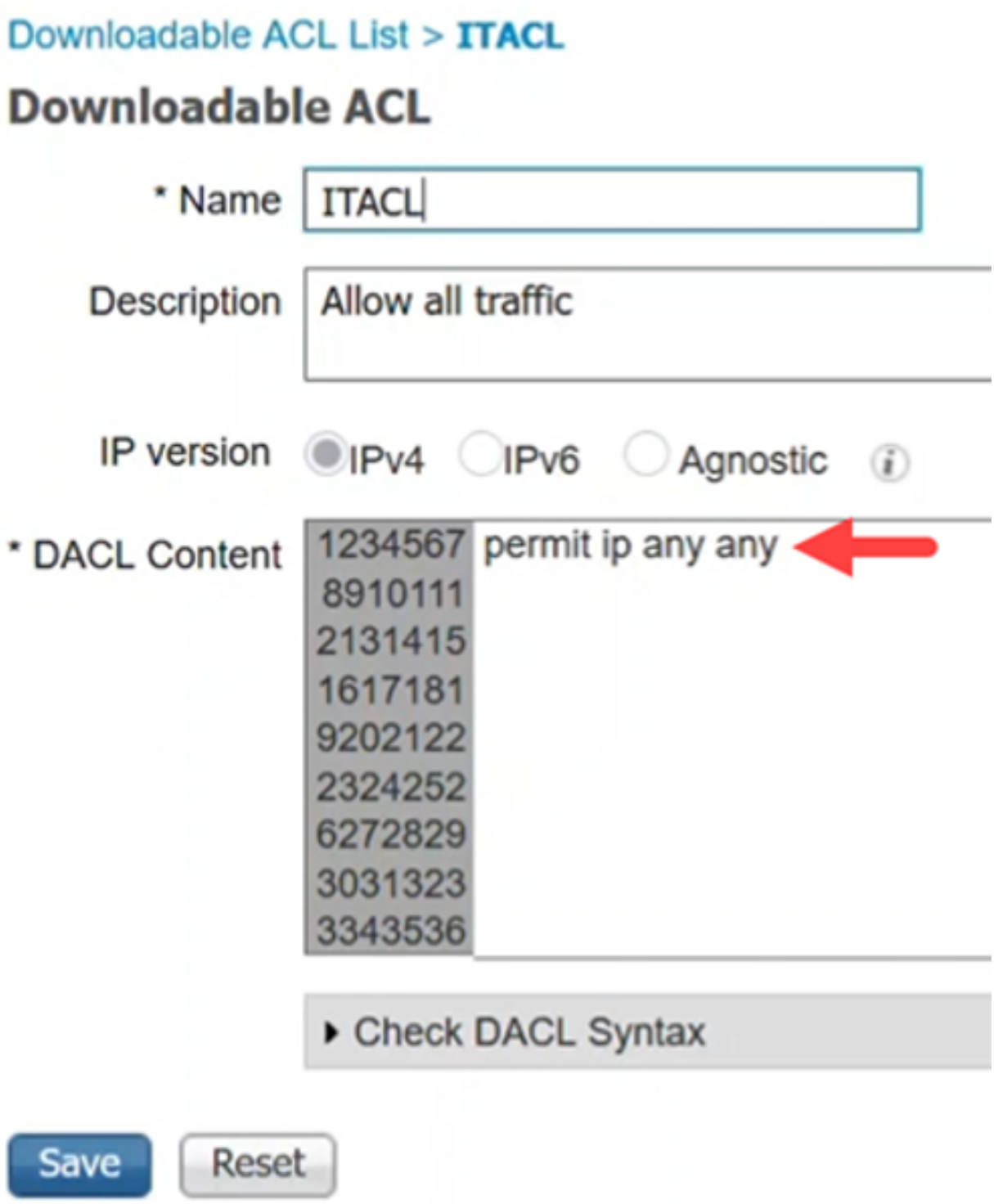
5단계

Add(추가) 아이콘을 클릭하여 다운로드 가능한 ACL을 생성합니다.



6단계

Name(이름), Description(설명)을 구성하고, IP 버전을 선택하고, DACL Content(DACL 콘텐츠) 필드에 다운로드 가능한 ACL을 구성할 ACE(액세스 제어 항목)를 입력합니다. 저장을 클릭합니다.



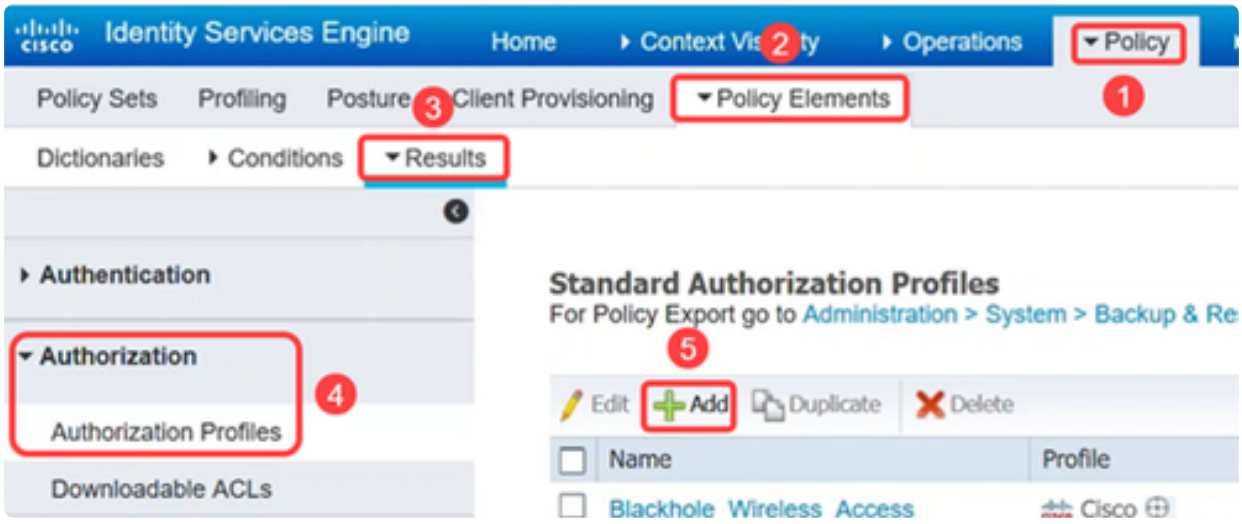
Note:

IP ACL만 지원되며 소스는 ANY여야 합니다. ISE의 ACL에서는 IPv4만 지원됩니다. ACL을 다른 소스와 함께 입력하면 ISE에 관한 한 구문이 정상이지만 스위치에 적용하면 실패합니다 .

7단계

ISE 정책 집합 내에서 DACL 및 기타 정책을 논리적으로 연결하는 데 사용할 권한 부여 프로파일을 생성합니다.

이렇게 하려면 정책 > 정책 구성 요소 > 결과 > 인증 > 인증 프로파일로 이동 하고 추가를 클릭 합니다.

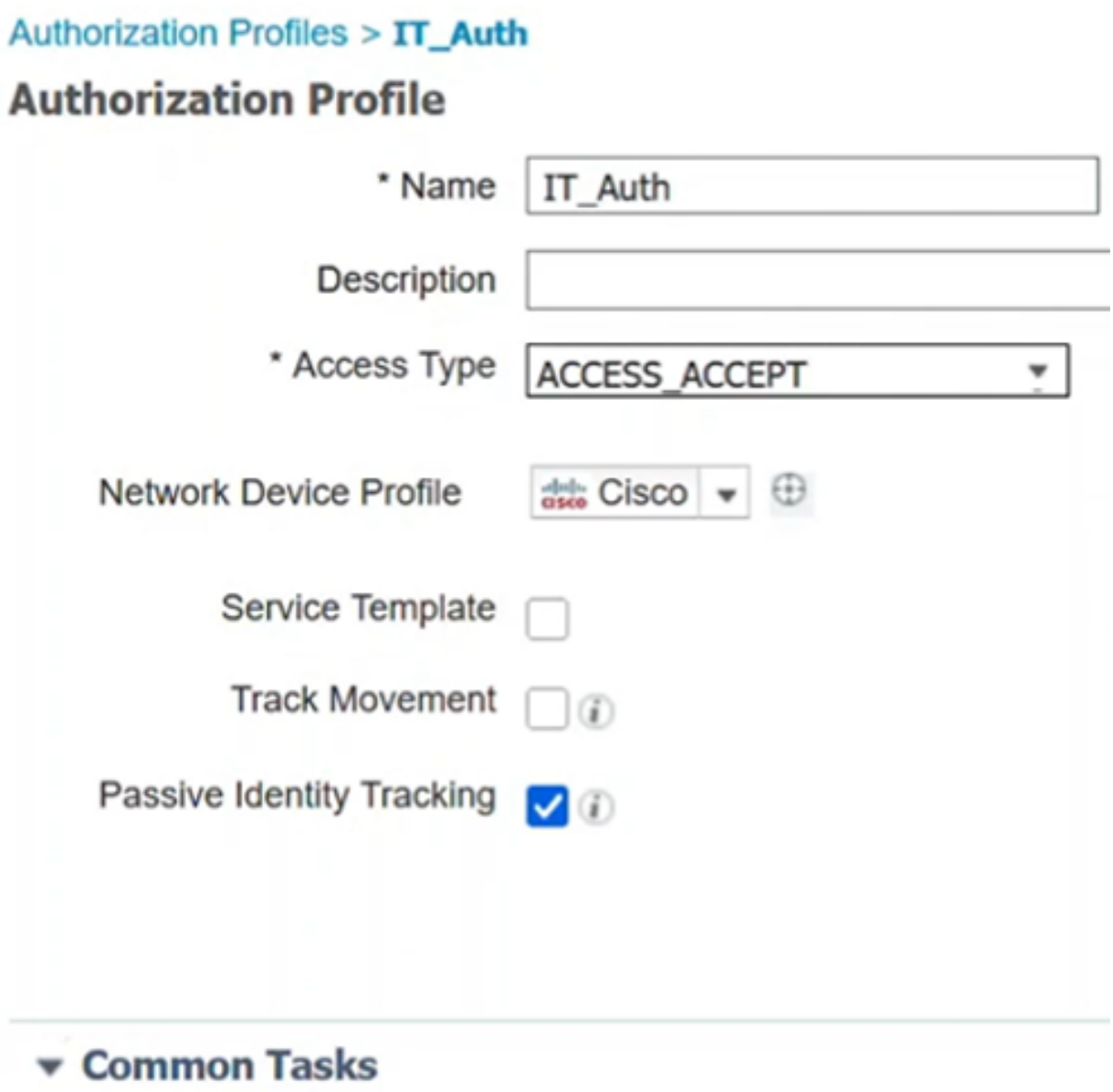


8단계

Authorization Profile(권한 부여 프로파일) 페이지에서 다음을 구성합니다.

- 이름
- 설명
- 액세스 유형 - ACCESS_ACCEPT로 설정해야 합니다. ACCESS_REJECT로 설정하면 인증이 거부됩니다.
- Network Device Profile(네트워크 디바이스 프로필) - Cisco로 선택해야 합니다.
- 수동 ID 추적 - 일부 인증 시나리오에서 활성화해야 할 수 있습니다. AD에 연결된 EasyConnect_PassiveID 시나리오에 필요합니다.
- 일반 작업 - 이 섹션에는 다양한 옵션이 있습니다. 이 예에서는 DACL Name(DACL 이름)이 구성됩니다.

저장을 클릭합니다.



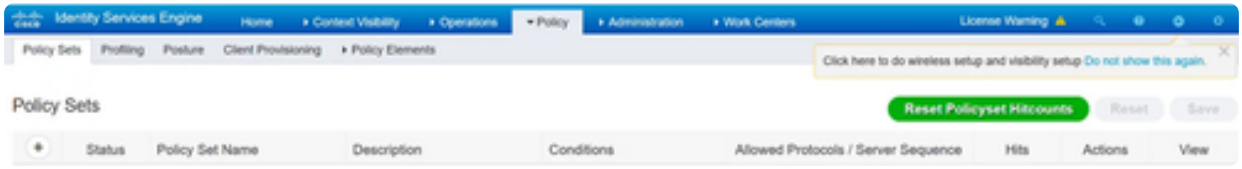
9단계

인증 및 권한 부여 정책의 논리적 그룹인 정책 집합을 구성하려면 Policy(정책) > Policy Sets(정책 집합) 메뉴를 클릭합니다.

정책 집합 목록을 볼 때 다음을 볼 수 있습니다.

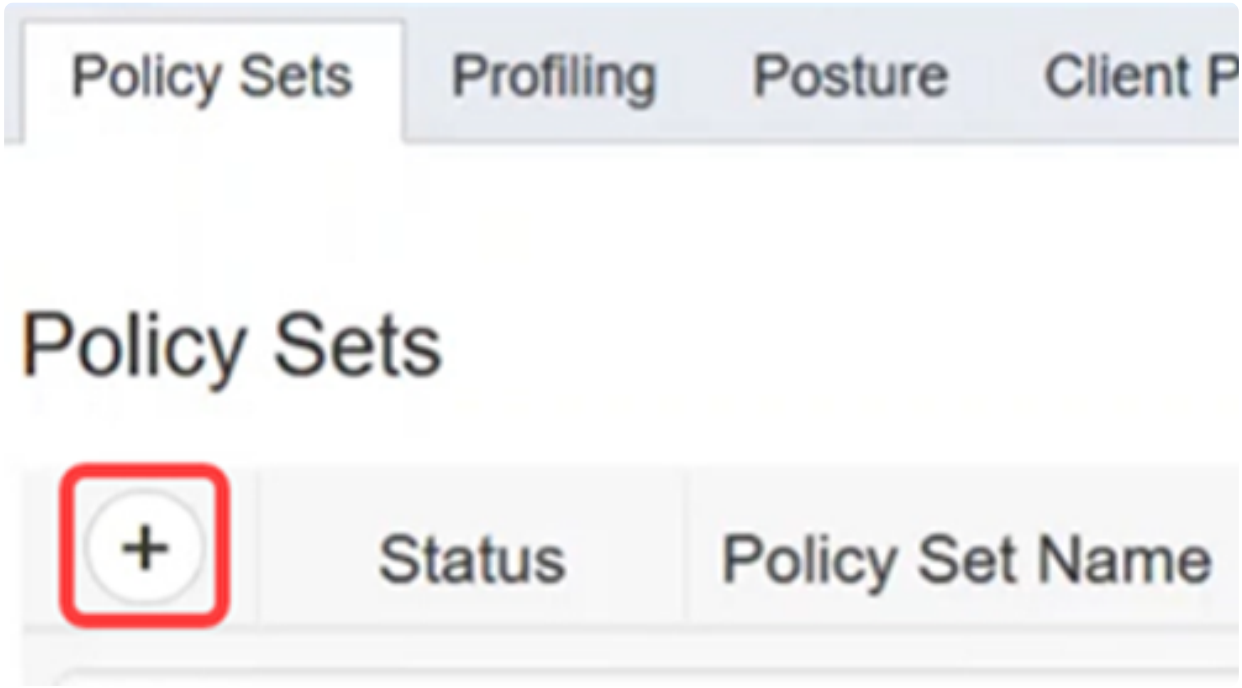
- 상태 - 녹색 확인 표시는 활성화됨을 나타내고 빈 흰색 원은 비활성화됨을 나타내며 눈 모양 아이콘은 모니터 전용 컨피그레이션용입니다.
- 정책 집합 이름 및 설명 - 설명이 간단합니다.
- 조건 - 정책 집합이 적용되는 위치를 정의합니다.
- Allowed Protocols/Server Sequence(허용된 프로토콜/서버 시퀀스) - 고급 컨트롤을 설정합니다.
- Hits(적중) - 정책 집합이 사용된 횟수를 표시합니다.
- Actions(작업) - 정책 집합을 적용할 수 있는 순서를 변경하거나, 기존 정책 집합을 복사하거나, 기존 정책 집합을 삭제할 수 있습니다.

- View(보기) - 정책 집합 세부사항을 수정할 수 있습니다.



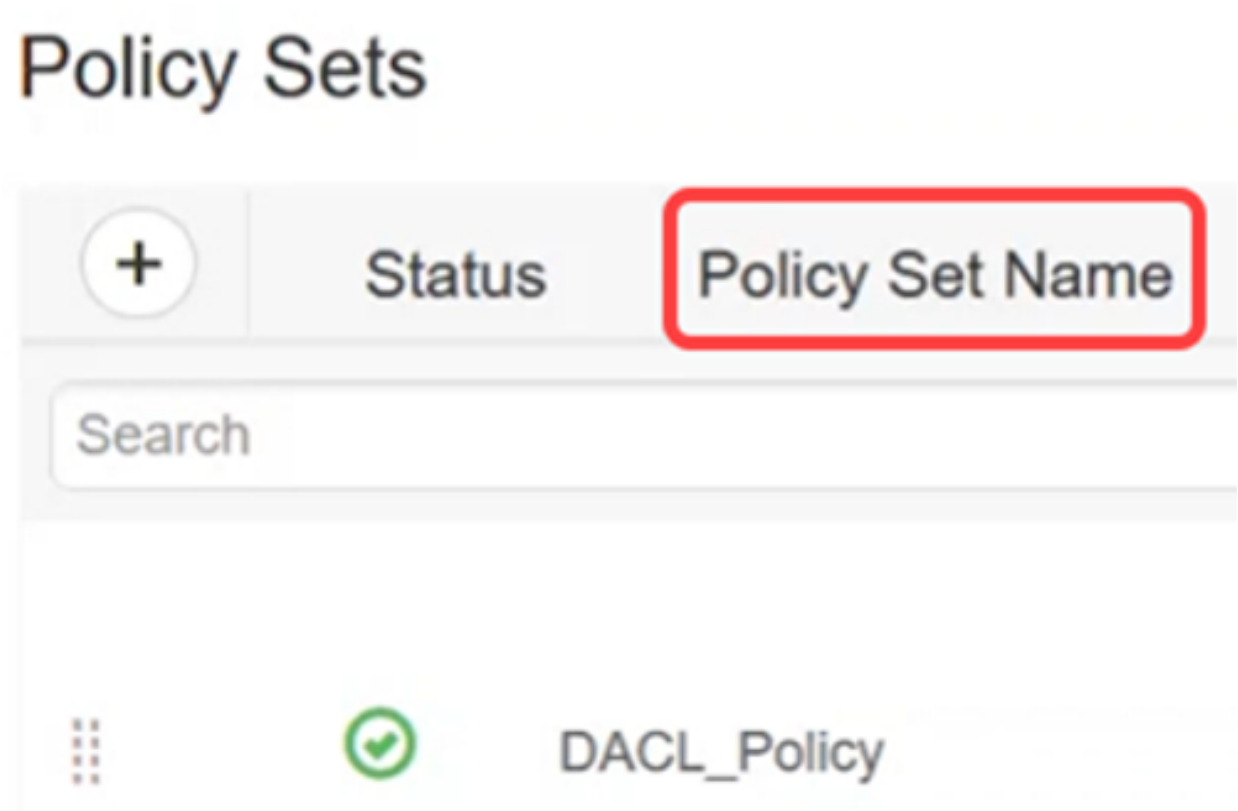
10단계

정책 집합을 생성하려면 add(추가) 버튼을 클릭합니다.



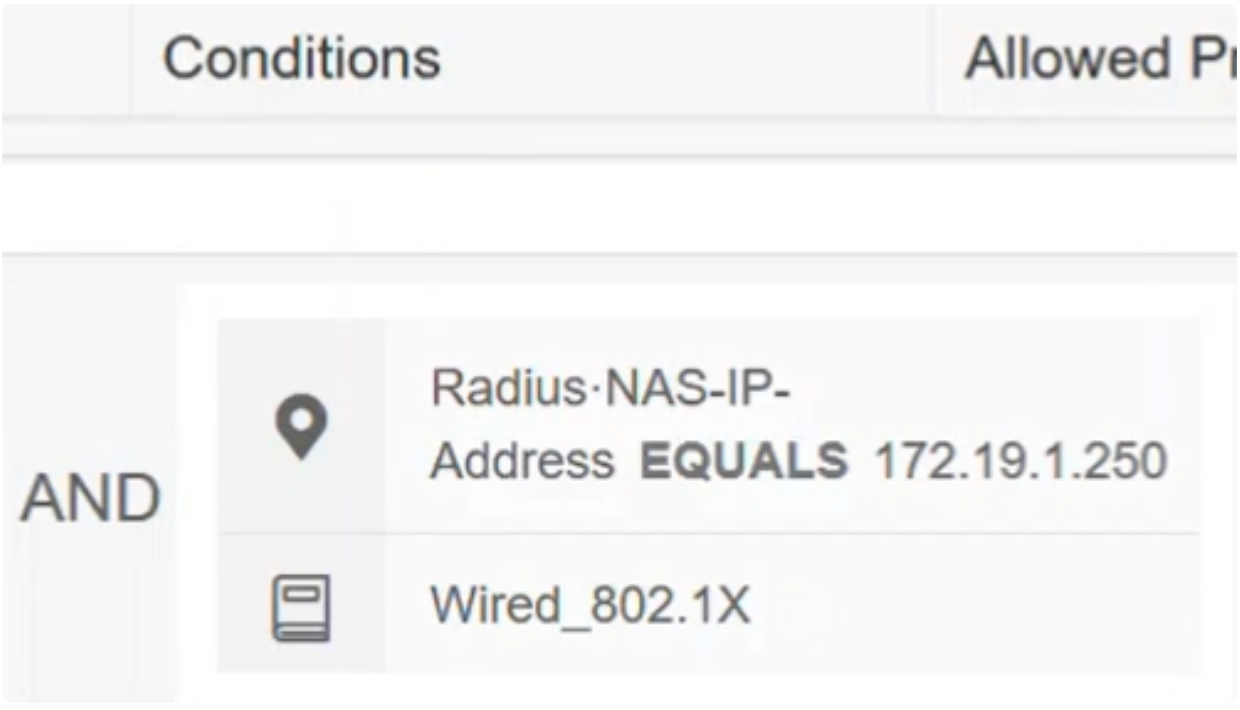
11단계

정책 세트 이름을 정의합니다.



12단계

Conditions(조건)에서 add(추가) 버튼을 클릭합니다. 그러면 이 인증 프로파일이 사용될 위치를 정의할 수 있는 Conditions Studio가 열립니다. 이 예에서는 172.19.1.250 및 wired_802.1x 트래픽인 Radius-NAS-IP-Address(스위치)에 적용되었습니다.

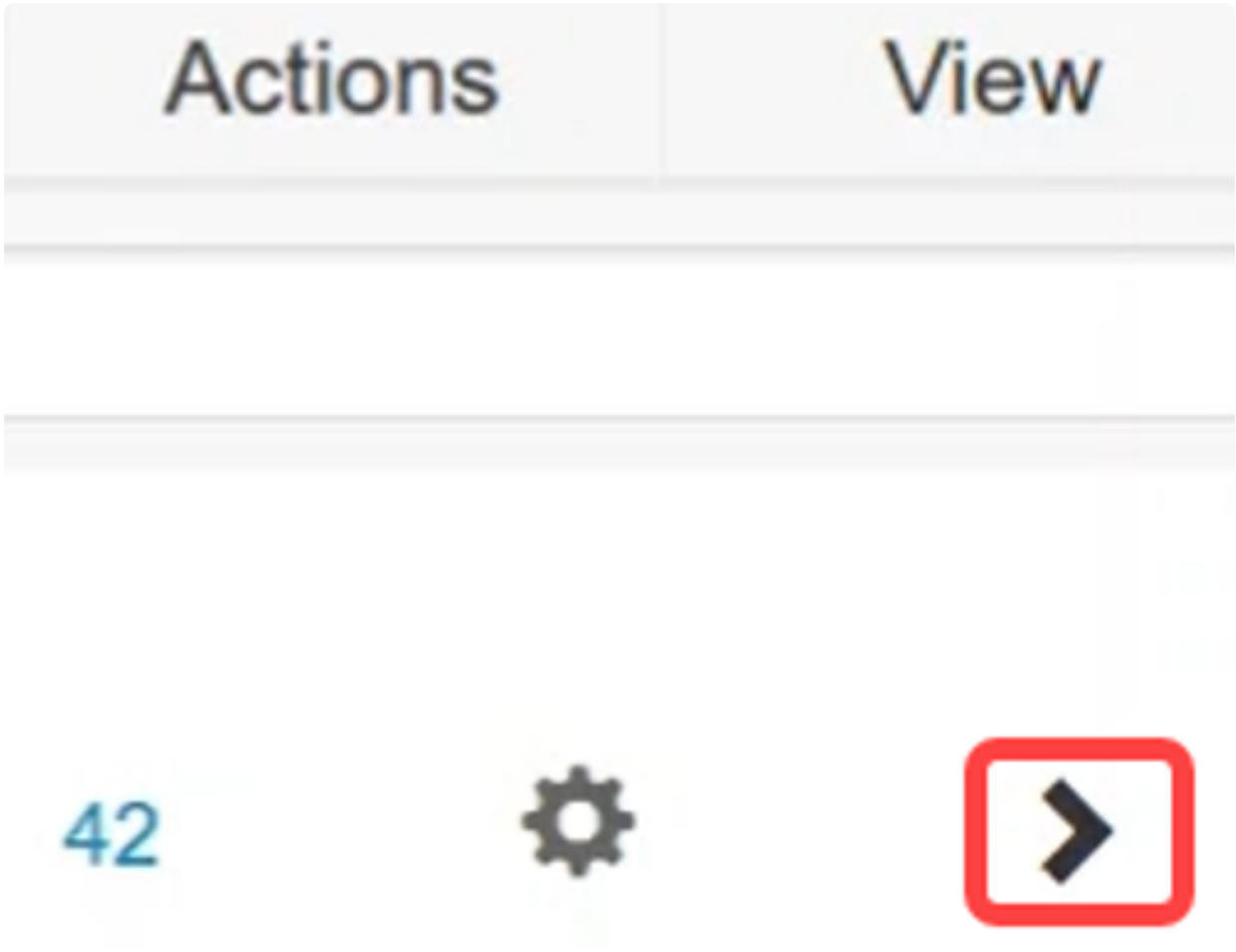


13단계

Allowed Protocols to the Default Network Access(기본 네트워크 액세스에 대해 허용되는 프로토콜)를 구성하고 Save(저장)를 클릭합니다.

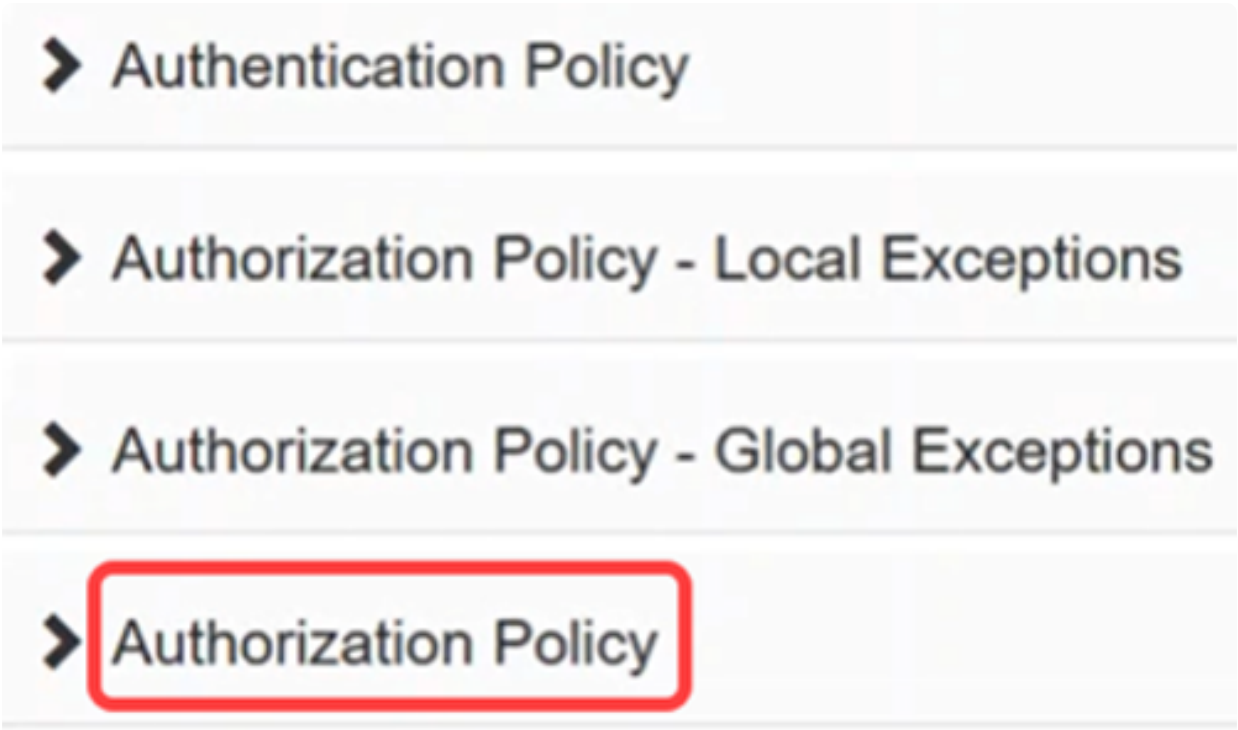
14단계

보기에서 화살표 아이콘을 클릭하여 네트워크 설정 및 요구 사항에 따라 인증 및 권한 부여 정책을 구성하거나 기본 설정을 선택할 수 있습니다. 이 예에서는 Authorization policy(권한 부여 정책)를 클릭합니다.



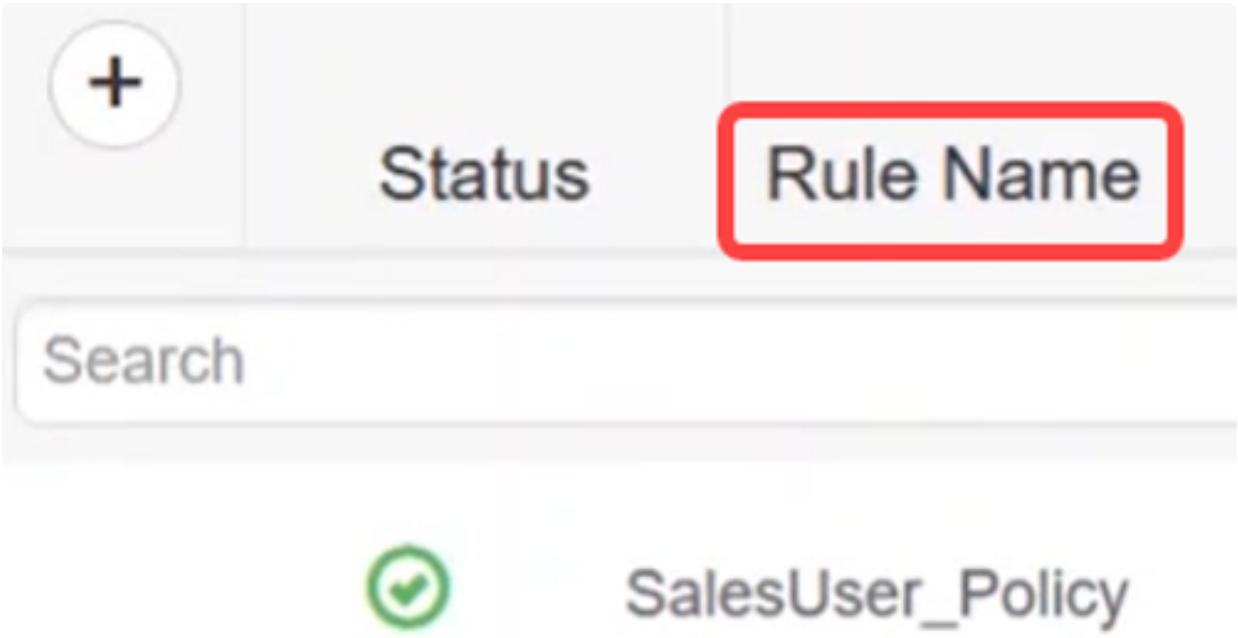
15단계

정책을 추가하려면 더하기 아이콘을 클릭합니다.



16단계

Rule Name을 입력합니다.



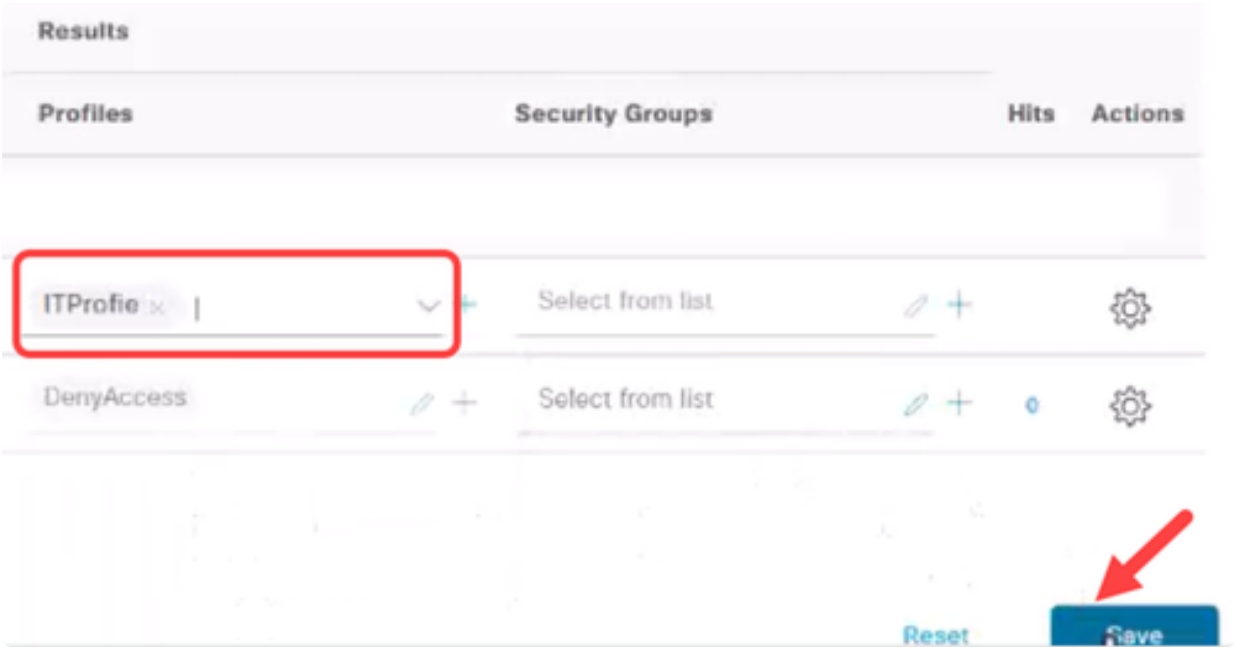
17단계

Conditions(조건)에서 더하기 아이콘을 클릭하고 ID 그룹을 선택합니다. Use(사용)를 클

릭합니다.

18단계

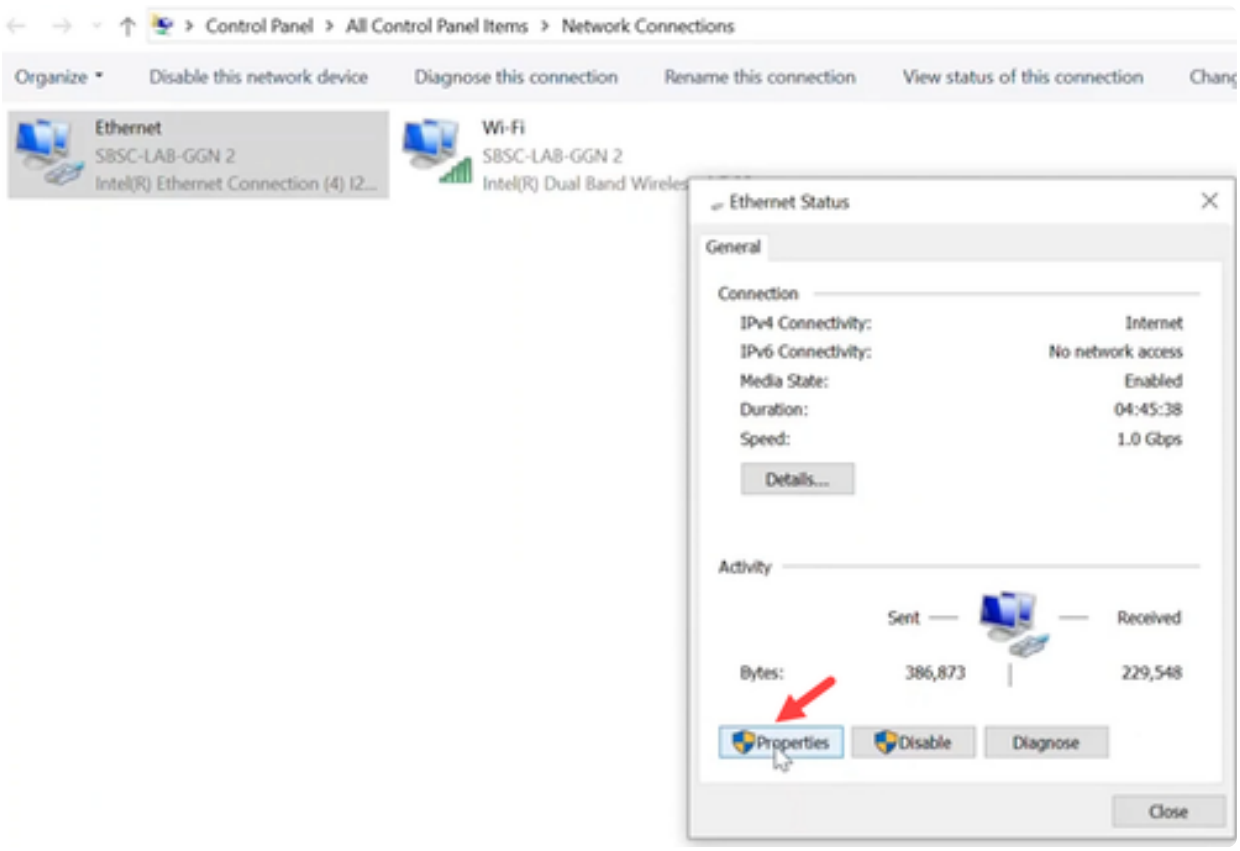
필요한 프로파일을 적용하고 Save(저장)를 클릭합니다.



클라이언트 컨피그레이션

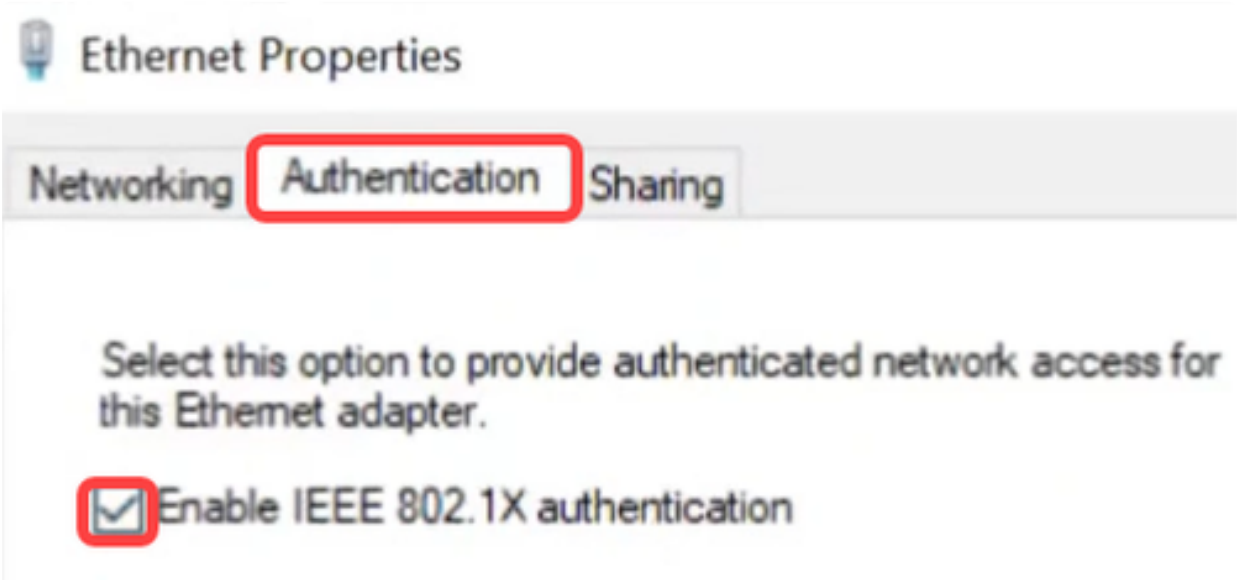
1단계

클라이언트 노트북 컴퓨터에서 Network Connections(네트워크 연결) > Ethernet(이더넷)으로 이동하고 Properties(속성)를 클릭합니다.



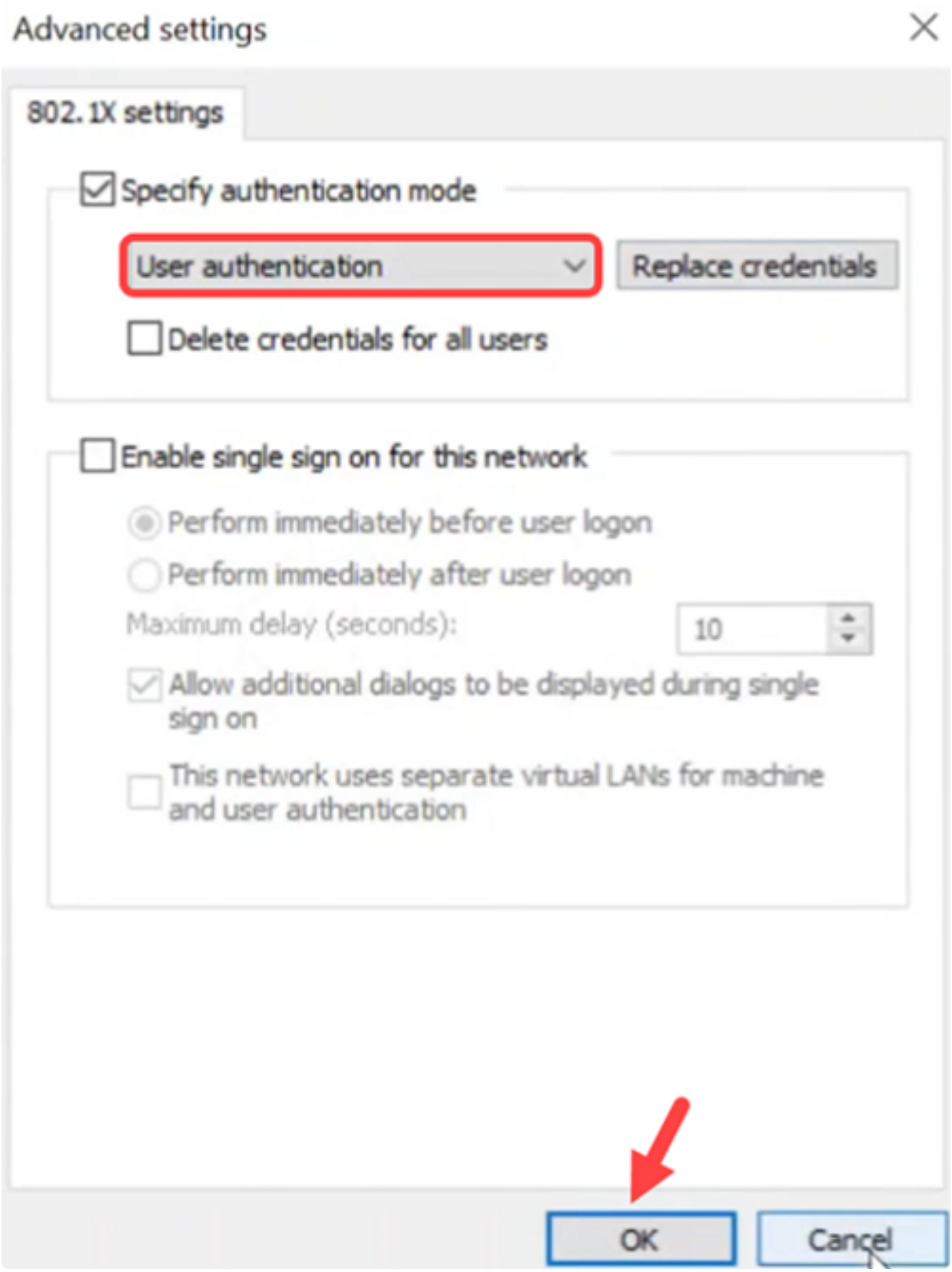
2단계

Authentication(인증) 탭을 클릭하고 802.1X 인증이 활성화되었는지 확인합니다.



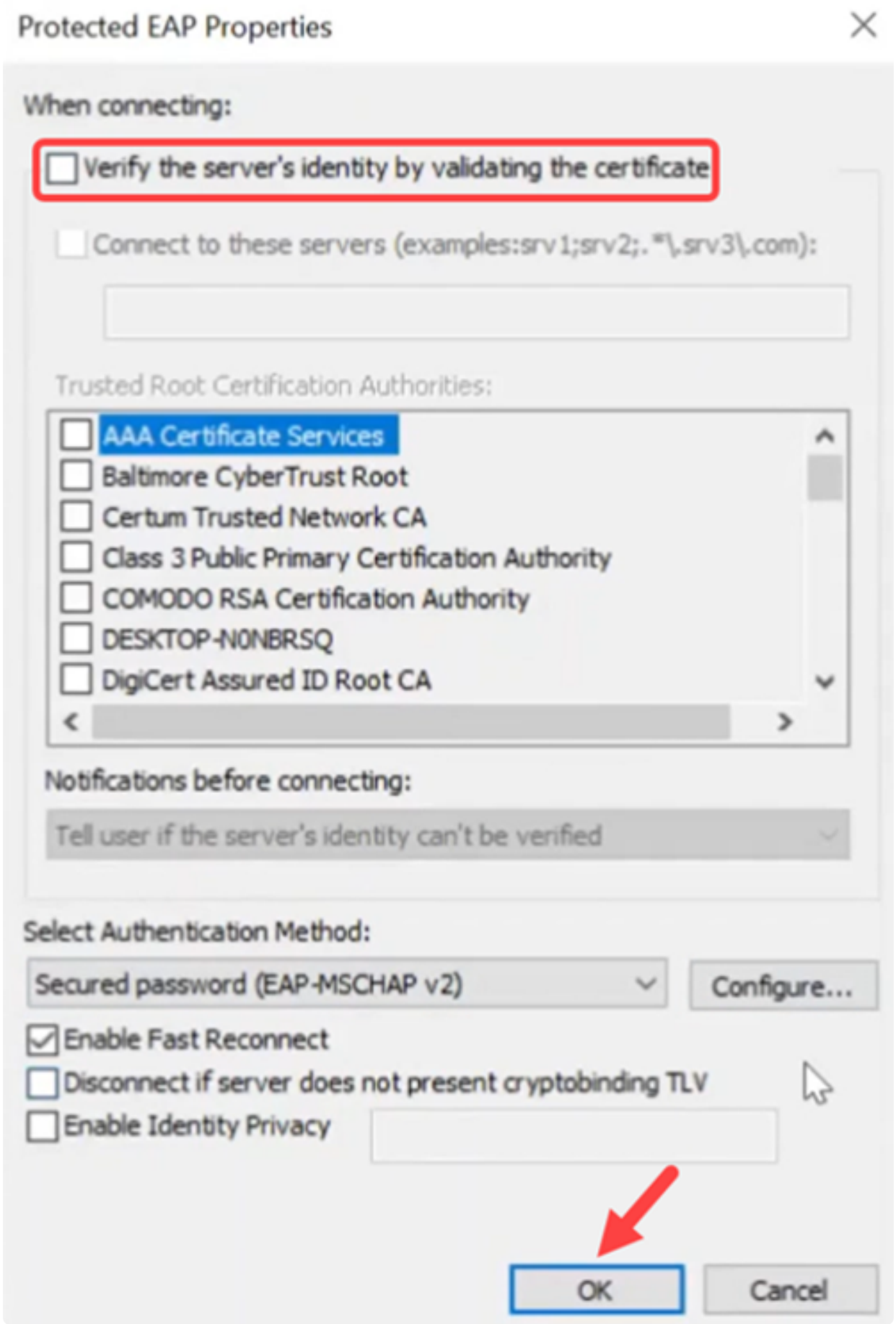
3단계

Additional Settings(추가 설정)에서 User authentication as authentication mode(인증 모드로 사용자 인증)를 선택합니다. Save Credentials(자격 증명 저장)를 클릭하고 OK(확인)를 클릭합니다.



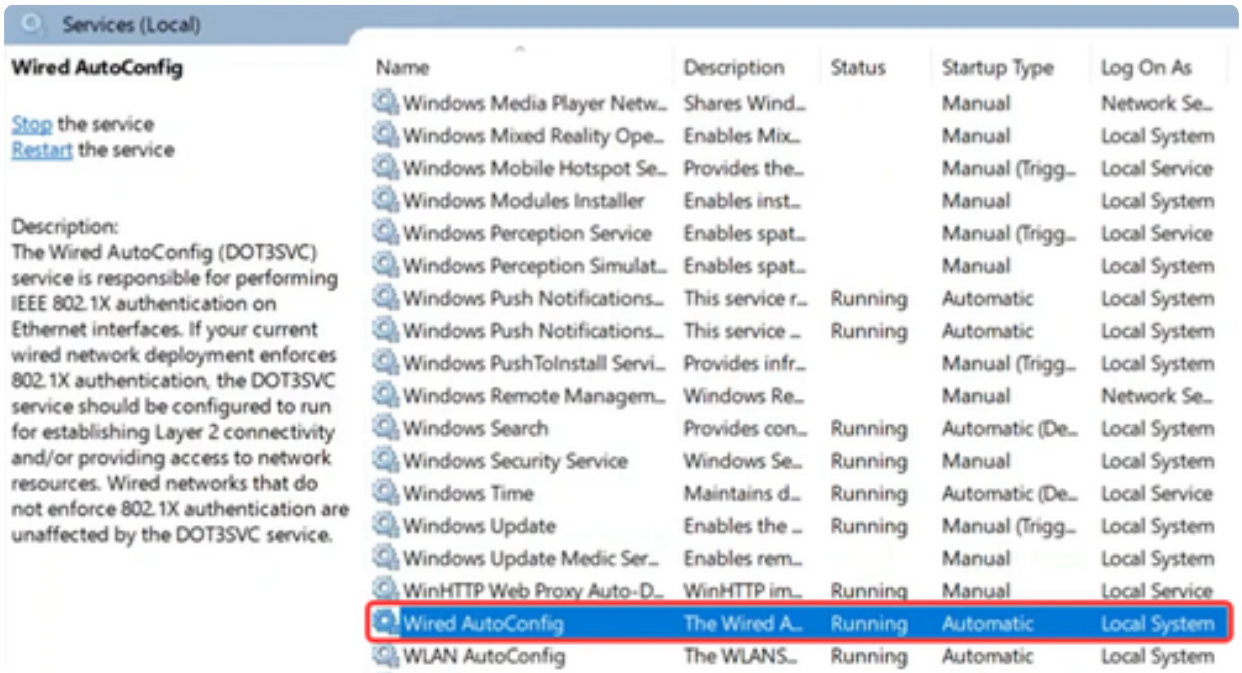
4단계

Settings(설정)를 클릭하고 Verify the server's identity by validating the certificate(인증서를 검증하여 서버 ID 확인) 옆에 있는 확인란의 선택이 취소되었는지 확인합니다. OK(확인)를 클릭합니다.


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

5단계

Services(서비스)에서 Wired AutoConfig 설정을 활성화합니다.

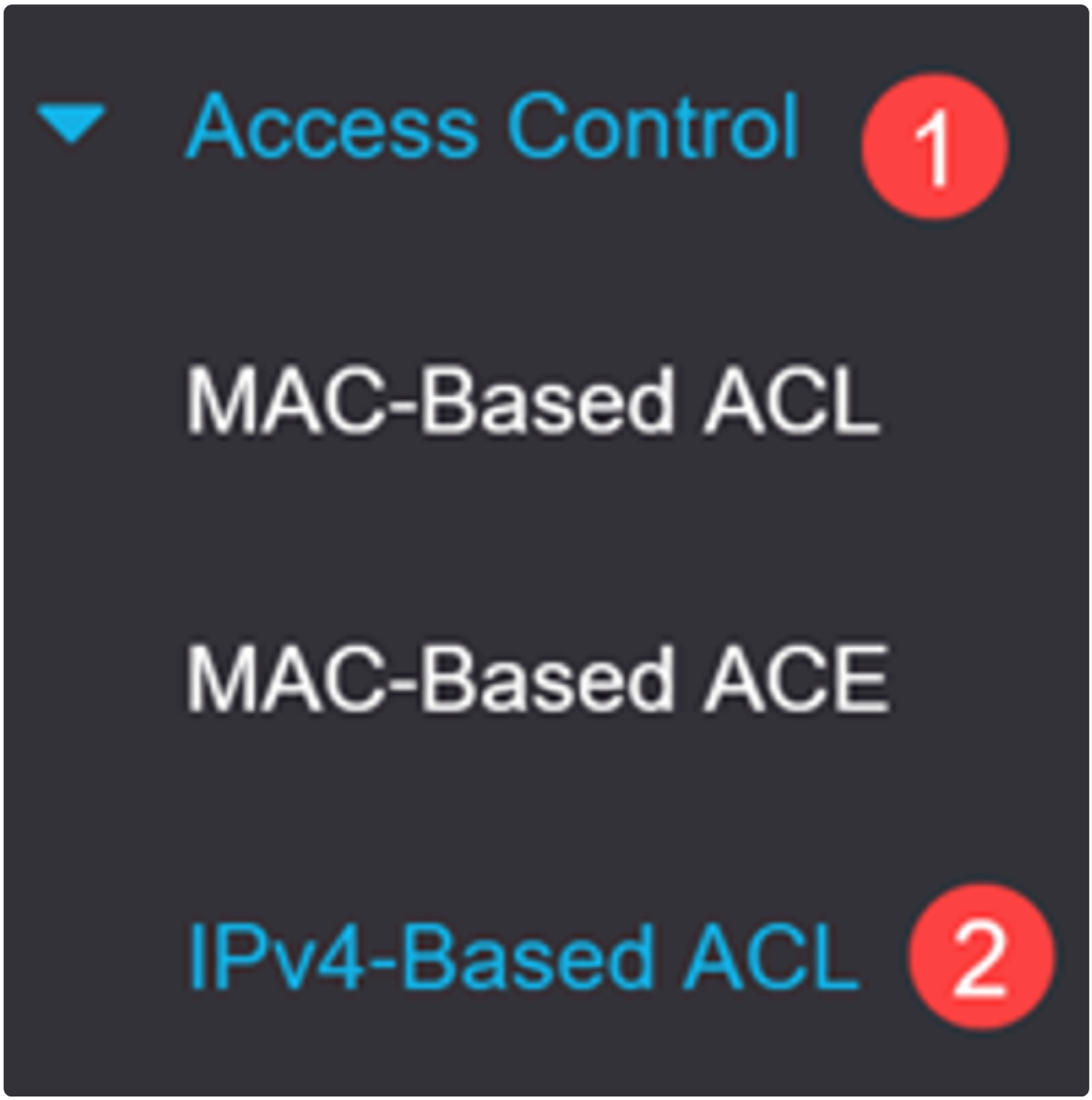


DACL 확인

사용자가 인증되면 다운로드 가능한 ACL을 확인할 수 있습니다.

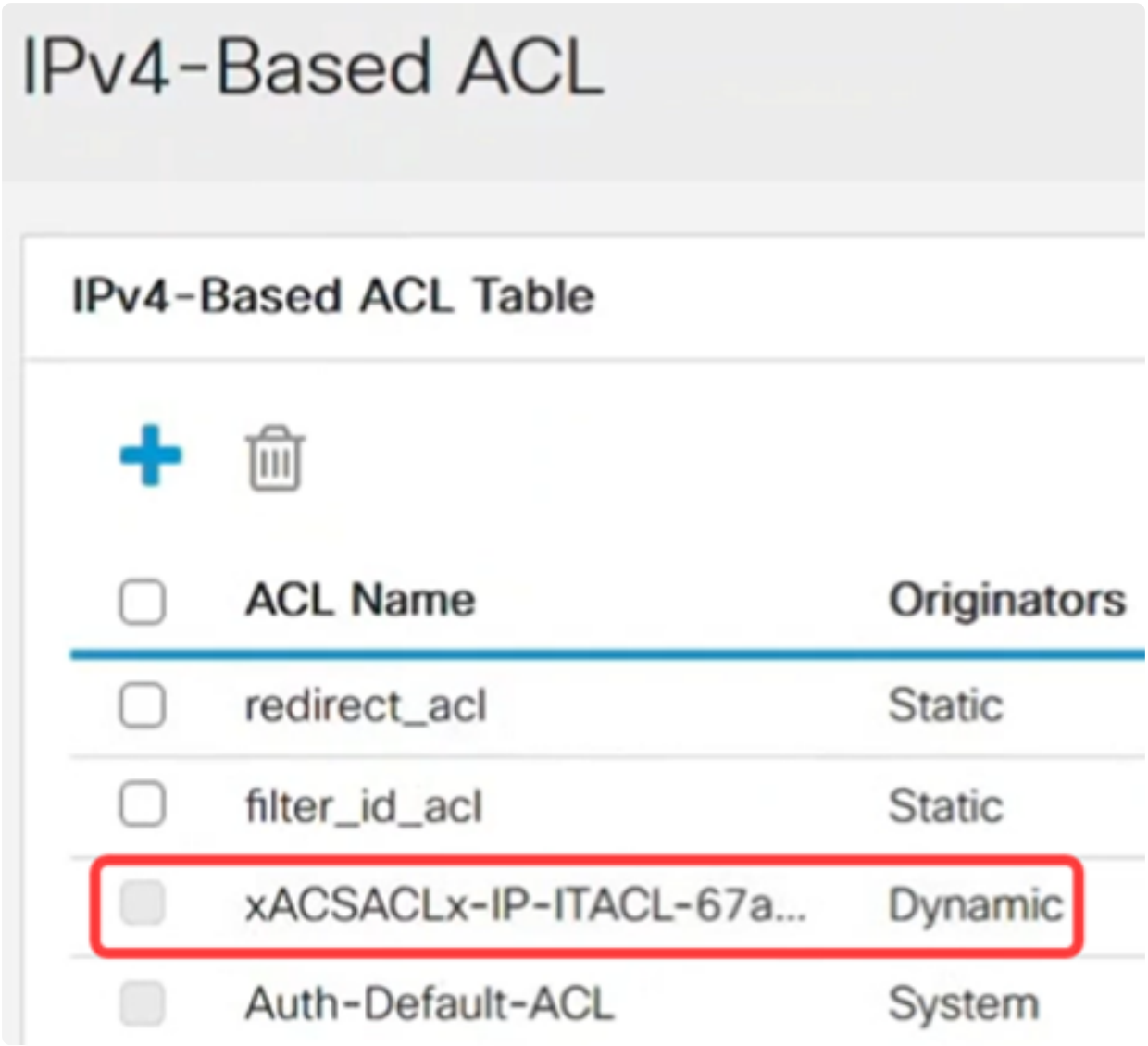
1단계

Catalyst 1300 스위치에 로그인하고 Access Control(액세스 제어) > IPv4-Based ACL(IPv4 기반 ACL) 메뉴로 이동합니다.



2단계

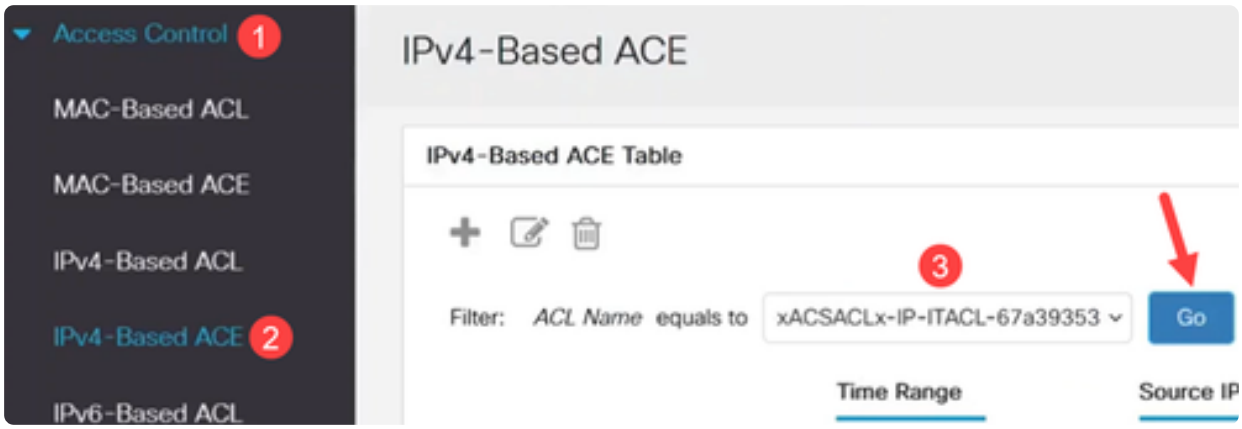
IPv4 기반 ACL 테이블에 다운로드한 ACL이 표시됩니다.



Note:
다운로드 가능한 ACL은 편집할 수 없습니다.

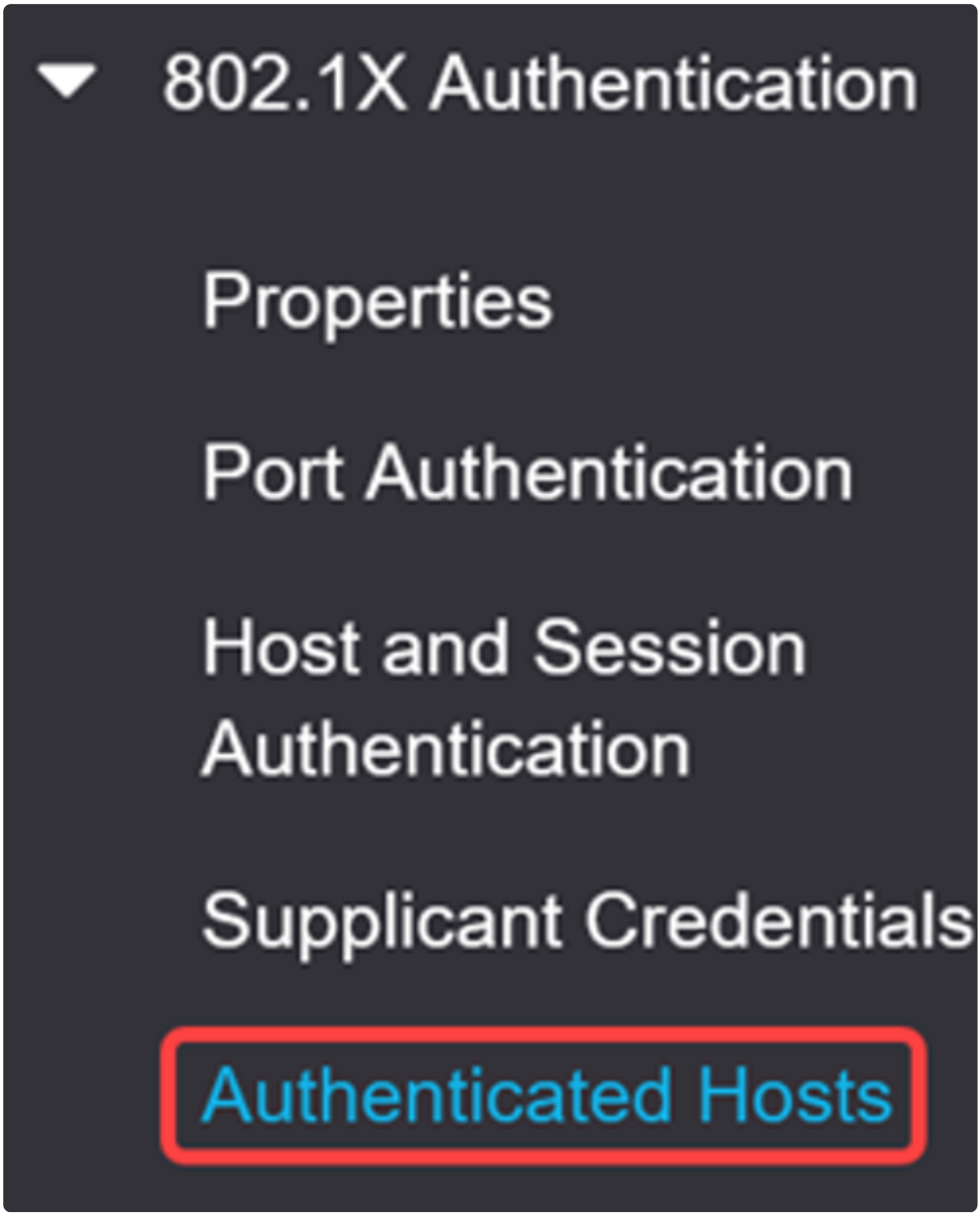
3단계

또 다른 확인 방법은 IPv4 기반 ACE로 이동하여 ACL Name 드롭다운 메뉴에서 다운로드 가능한 ACL을 선택하고 Go를 클릭하는 것입니다. ISE에서 구성된 규칙이 표시됩니다.



4단계

Security(보안) > 802.1 Authentication(802.1 인증) > Authenticated Hosts(인증된 호스트) 메뉴로 이동합니다. 인증된 사용자를 확인할 수 있습니다. Authenticated Sessions(인증된 세션)를 클릭하여 자세한 내용을 확인합니다.



5단계

CLI에서 show ip access-lists interface 명령과 인터페이스 ID를 실행합니다.

이 예에서는 기가비트 이더넷 3에 적용된 ACL 및 ACE를 볼 수 있습니다.

```
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
```

6단계

명령을 사용하여 ISE 연결 및 ACL 다운로드와 관련된 설정을 볼 수도 있습니다

show dot1x sessions interface <ID> 상세 정보. 상태, 802.1x 인증 상태 및 다운로드된 ACL을 볼 수 있습니다.

```
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
```

결론

여기 있어요! 이제 다운로드 가능한 ACL이 Cisco ISE를 사용하는 Cisco Catalyst 1300

스위치에서 어떻게 작동하는지 알 수 있습니다.

자세한 내용은 Catalyst 1300 관리 가이드 및 Cisco Catalyst 1300 Series 지원 페이지를 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.