웹 사용자 인터페이스를 사용하여 Catalyst 1300에서 권한 부여 변경 구성

목표

이 문서의 목적은 웹 UI(사용자 인터페이스)를 사용하여 Catalyst 1300 스위치에서 CoA(Change of Authorization)를 구성하는 방법을 설명하는 것입니다.

적용 가능한 장치 및 소프트웨어 버전

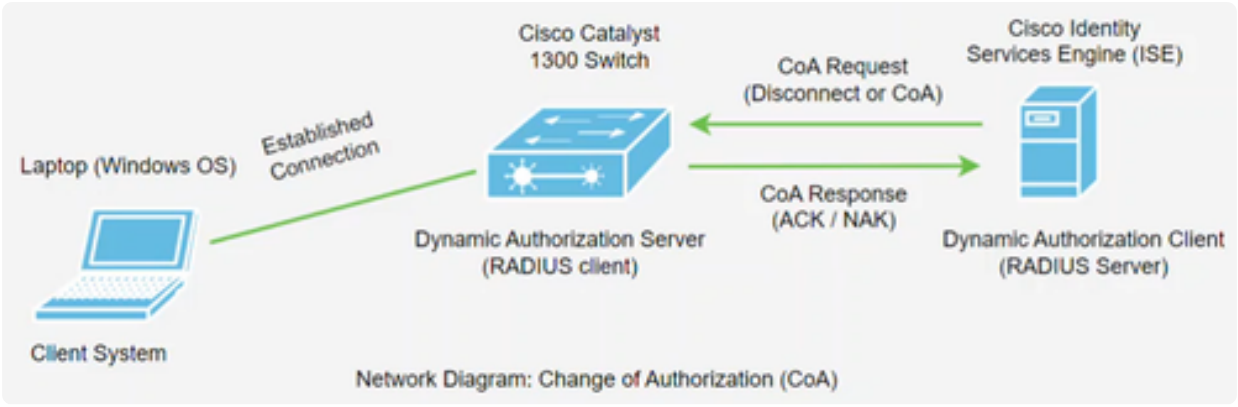
- Catalyst 1300 스위치 | 4.1.6.53

소개

CoA(Change of Authorization)는 RADIUS 프로토콜의 확장으로, 인증된 후 AAA(Authentication, Authorization, and Accounting) 또는 dot1x 사용자 세션의 속성을 변경할 수 있습니다. AAA의 사용자 또는 그룹에 대한 정책이 변경되면 관리자는 AAA 서버(예: Cisco ISE)에서 RADIUS CoA 패킷을 전송하여 인증을 다시 초기화하고 새 정책을 적용할 수 있습니다.

Cisco ISE(Identity Services Engine)는 완전한 기능을 갖춘 네트워크 기반 액세스 제어 및 정책 시행 엔진입니다. 보안 분석 및 시행, RADIUS 및 TACACS 서비스, 정책 배포 등을 제공합니다. Cisco ISE는 현재 Catalyst 1300 스위치에 대해 지원되는 유일한 CoA 동적 권한 부여 클라이언트입니다. 자세한 내용은 ISE 관리 가이드를 참조하십시오.

이 기능을 사용하려면 RADIUS 서버(Dynamic Authorization Client)와 Catalyst 스위치(Dynamic Authorization Server) 간의 통신이 필요합니다. 아래 네트워크 다이어그램에서 볼 수 있듯이 Dynamic Authorization Server는 Dynamic Authorization Server에 연결 끊기 또는 CoA 메시지를 보내고 스위치는 응답을 제공합니다.



Network Diagram: Change of Authorization (CoA)

펌웨어 버전 4.1.3.36의 Catalyst 1300 스위치에 CoA 지원이 추가되었습니다. 여기에는 사용자 연결을 끊고 사용자 세션에 적용할 수 있는 권한 부여를 변경하는 지원이 포함됩니다. 디바이스는 다음 CoA 작업을 지원합니다.

- 세션 연결 끊기
- 호스트 포트 CoA 명령 비활성화
- 바운스 호스트 포트 CoA 명령
- 호스트 CoA 재인증 명령

CLI(Command Line Interface)를 사용하여 CoA를 구성하려면 CLI를 사용하여 Catalyst 1300 Switch의 Change of Authorization 구성을 참조하십시오.

목차

ISE에서 Catalyst 1300 RADIUS 클라이언트 구성

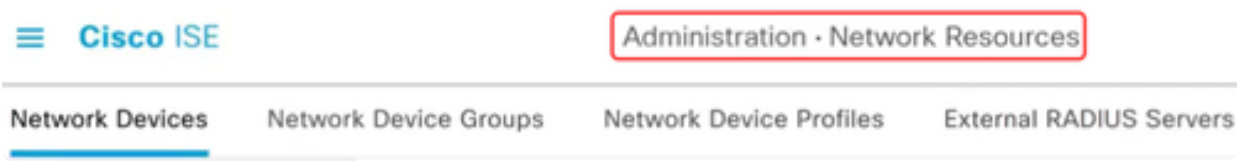
이 예에서는 Cisco ISE 서버 버전 3.2가 사용됩니다. ISE에 대한 개요는 Cisco Identity Services Engine 제품 페이지에서 확인하십시오.

> **Note:**
> CoA는 ISE 버전 2.7 이상에서 지원됩니다.

Cisco ISE 서버를 구축한 후 웹 UI에 액세스하려면 로그인합니다.

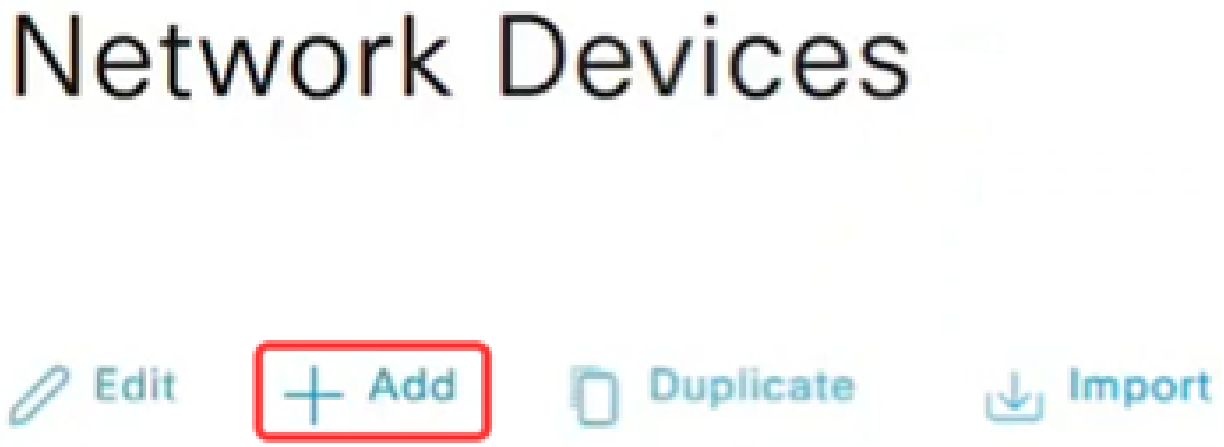
1단계

네트워크 디바이스를 추가하려면 Administration(관리) > Network Resources(네트워크 리소스) 메뉴로 이동합니다.



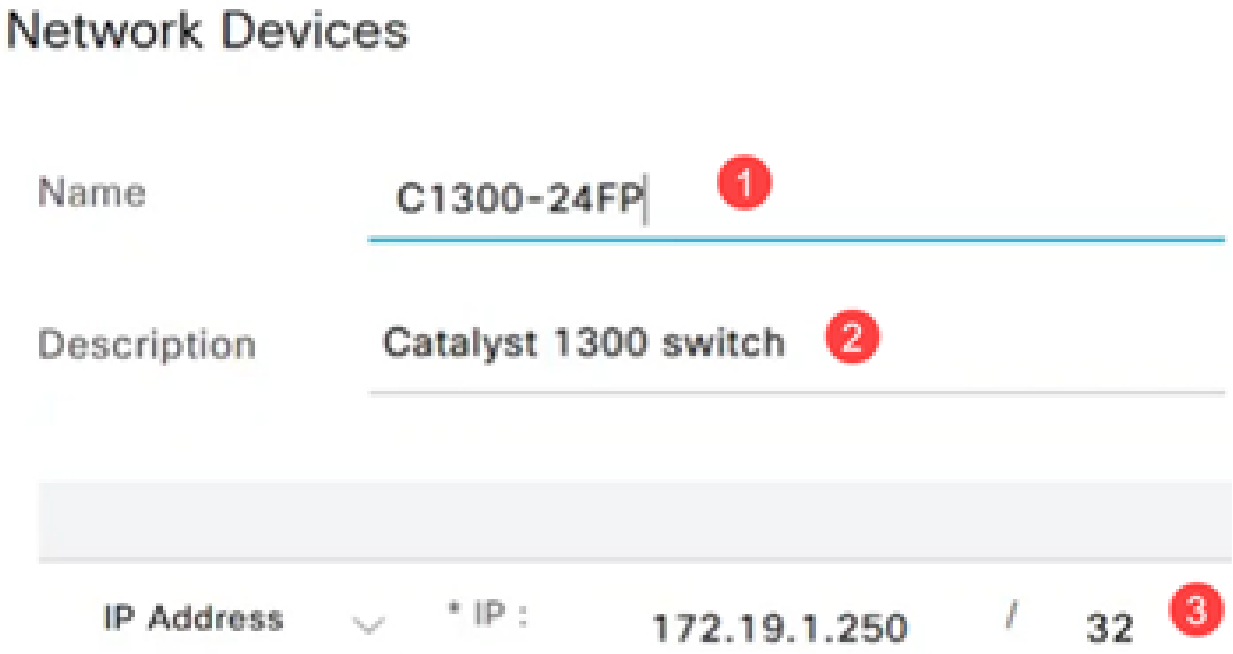
2단계

+ Add(추가) 버튼을 클릭합니다.



3단계

Catalyst 스위치의 이름, 설명 및 IP 주소를 입력합니다.

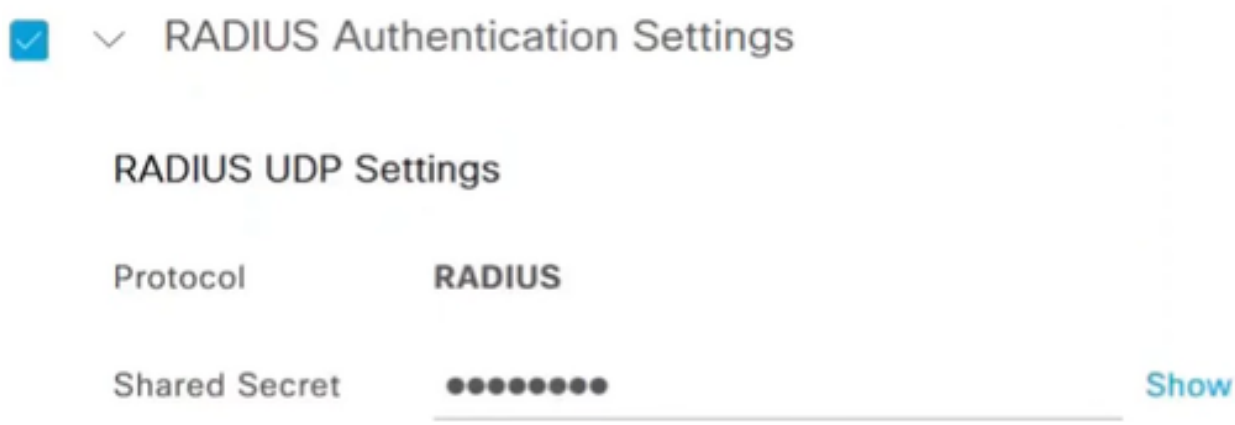


4단계

Device Profile 드롭다운 메뉴에서 Cisco를 선택합니다.

5단계

Shared Secret(공유 암호)을 입력하여 RADIUS 인증 설정을 구성합니다.

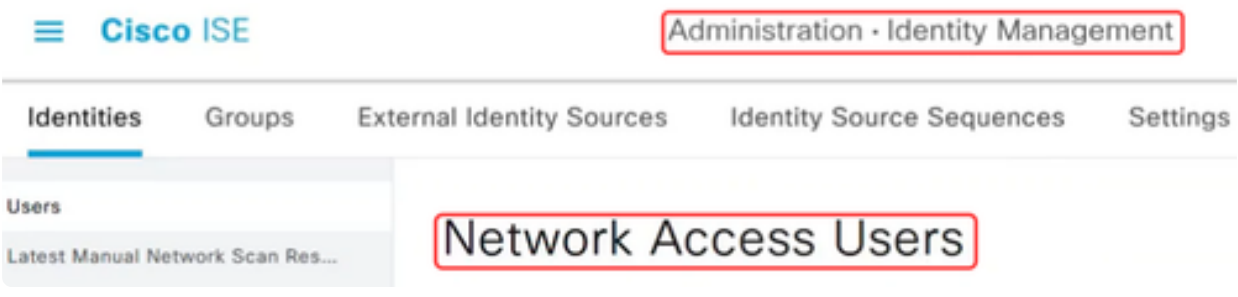


6단계

CoA 포트 번호를 입력합니다. 기본 포트는 1700입니다.

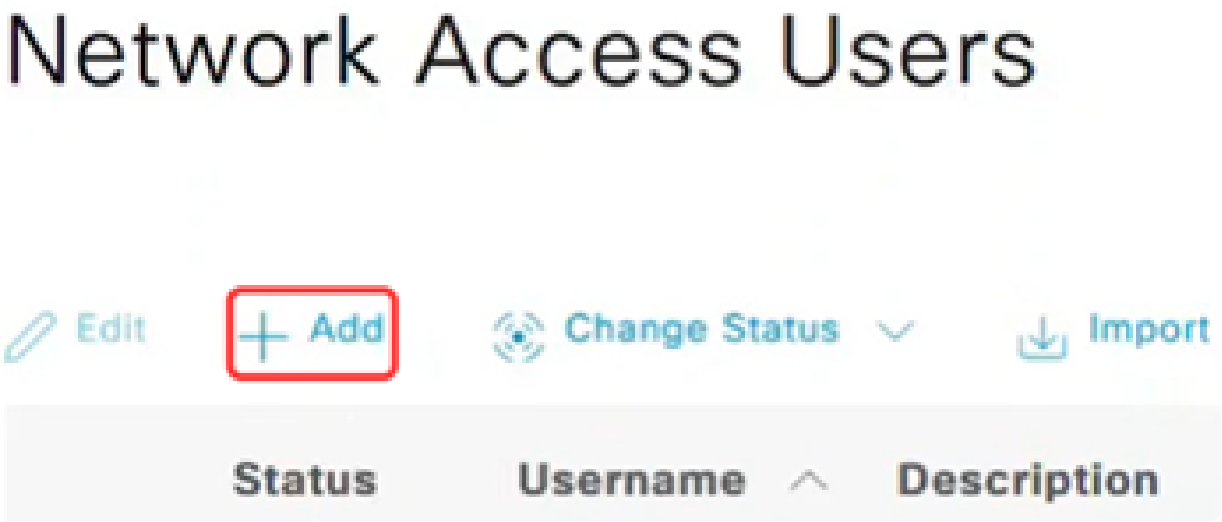
7단계

다음으로, Administration(관리) > Identity Management(ID 관리)로 이동하고 Network Access Users(네트워크 액세스 사용자)를 선택합니다.



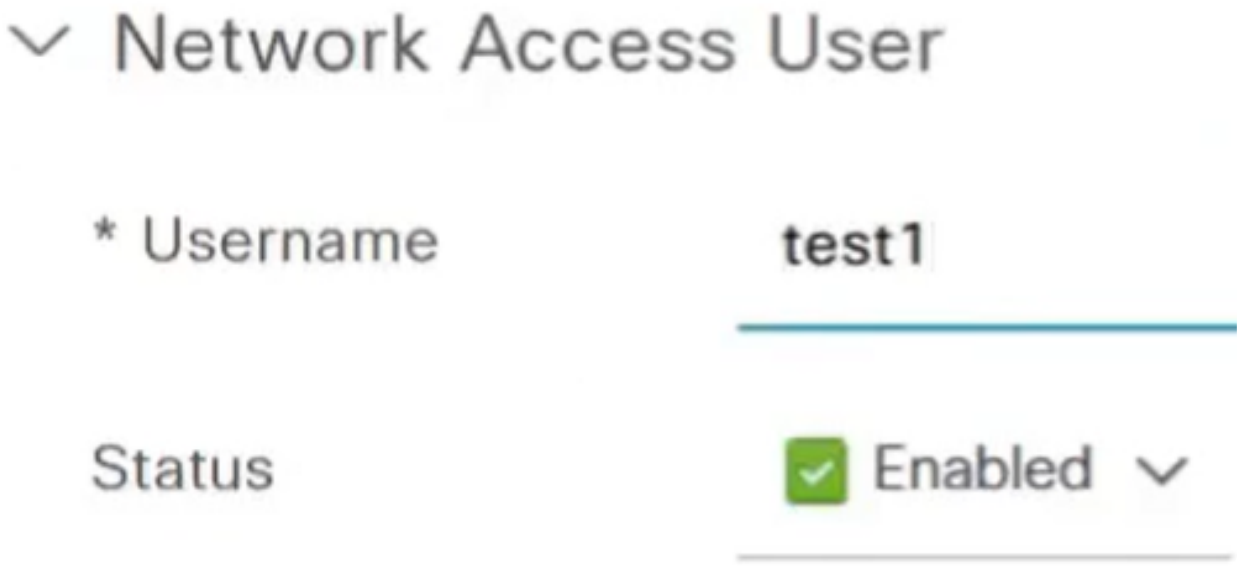
8단계

사용자 이름 및 비밀번호를 정의하려면 +Add 기호를 클릭합니다.



9단계

사용자 이름, 비밀번호를 입력하고 페이지 하단에서 Save(저장)를 클릭합니다.



Catalyst 1300 스위치의 구성

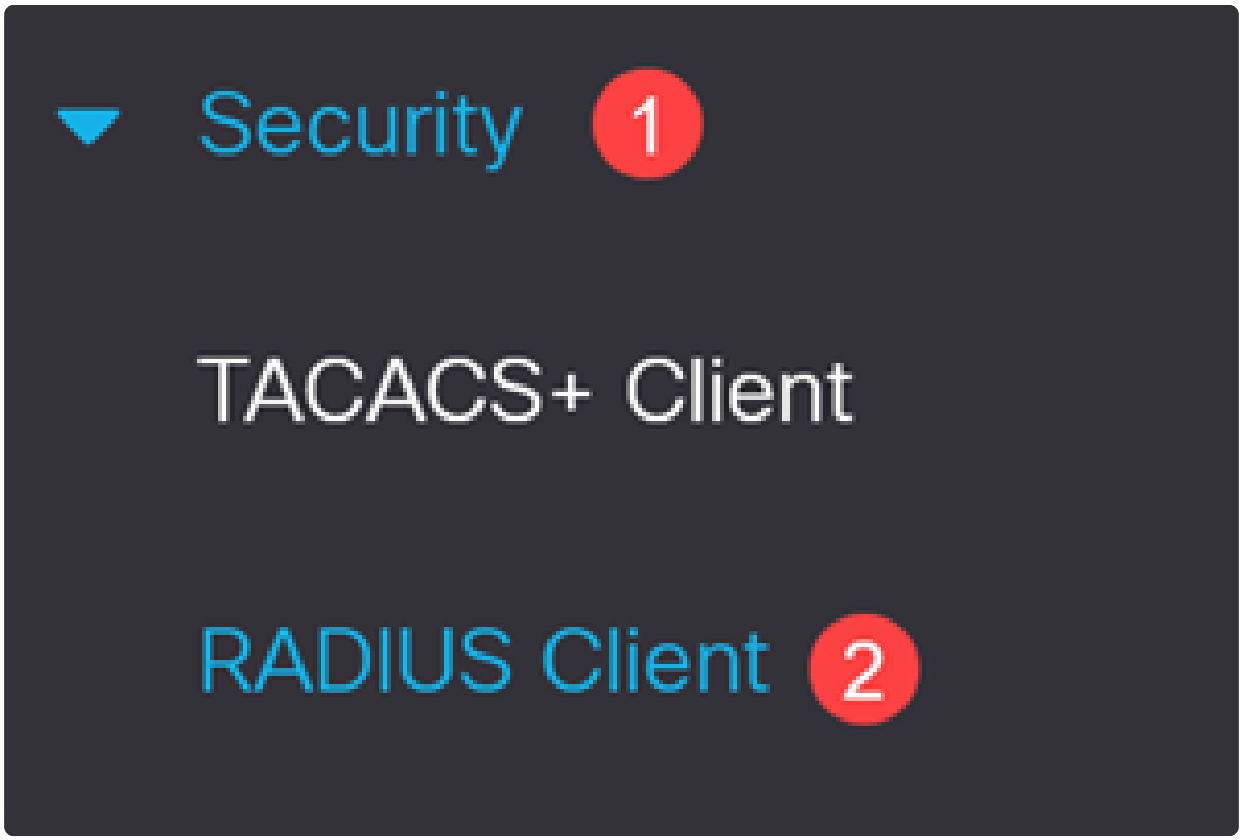
1단계

Catalyst 1300 스위치에 로그인하고 Advanced(고급) 모드를 선택합니다. 이 예제에서는 C1300-24FP-4X를 사용합니다.

> Note:
> 펌웨어 버전 4.1.3.36의 Catalyst 1300 스위치에 CoA 지원이 추가되었습니다.

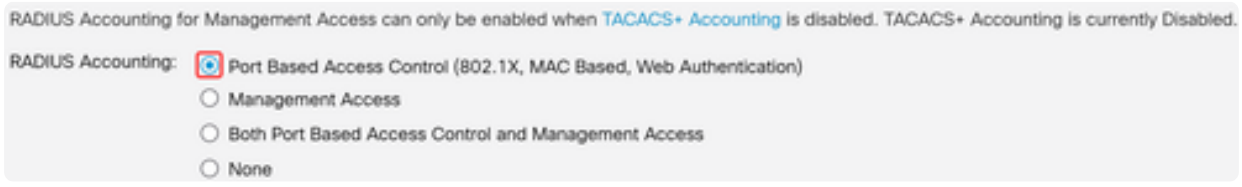
2단계

탐색 창에서 Security(보안) > RADIUS Client(RADIUS 클라이언트)로 이동합니다.



3단계

RADIUS 어카운팅을 포트 기반 액세스 제어로 설정합니다.



4단계

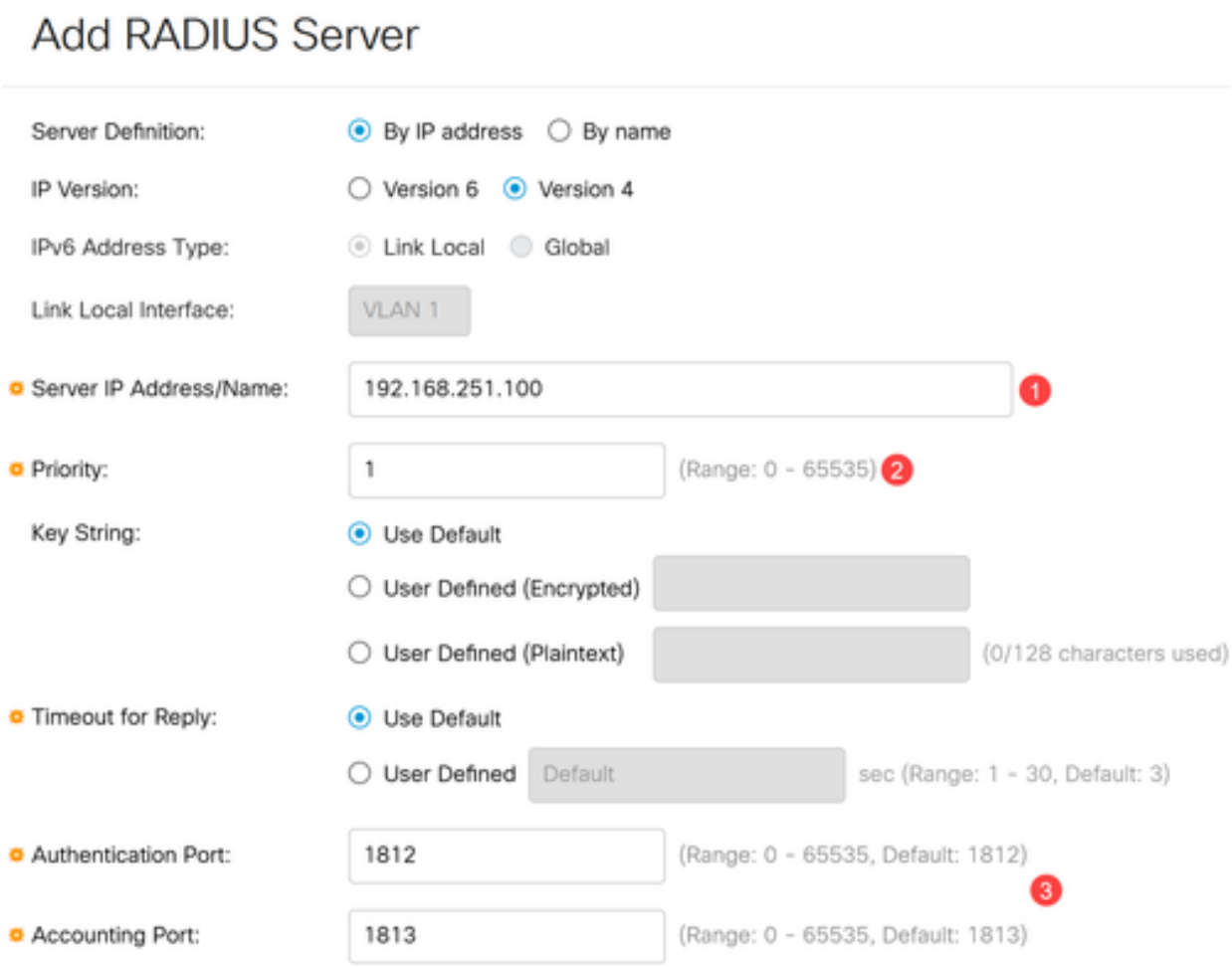
ISE 서버를 추가하려면 RADIUS Table(RADIUS 테이블)까지 아래로 스크롤하고 더하기 아이콘을 클릭합니다.

5단계

RADIUS 서버 설정을 구성합니다.

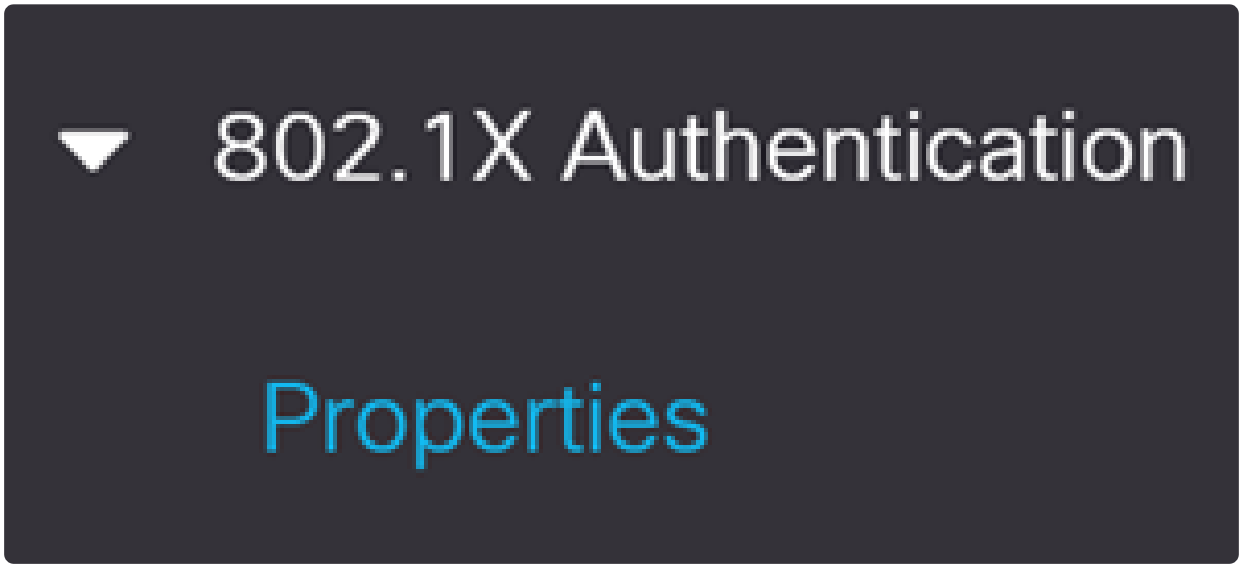
- Server Definition(서버 정의)을 선택합니다. 이 예에서는 By IP address(IP 주소 기준)가 선택됩니다. Server IP Address /Name(서버 IP 주소/이름) 필드에 IP 주소를 입력합니다.
- RADIUS 우선순위를 설정합니다.
- 인증 및 계정 관리 포트는 기본값으로 설정됩니다.
- 사용 유형은 802.1x입니다.

적용을 클릭합니다.



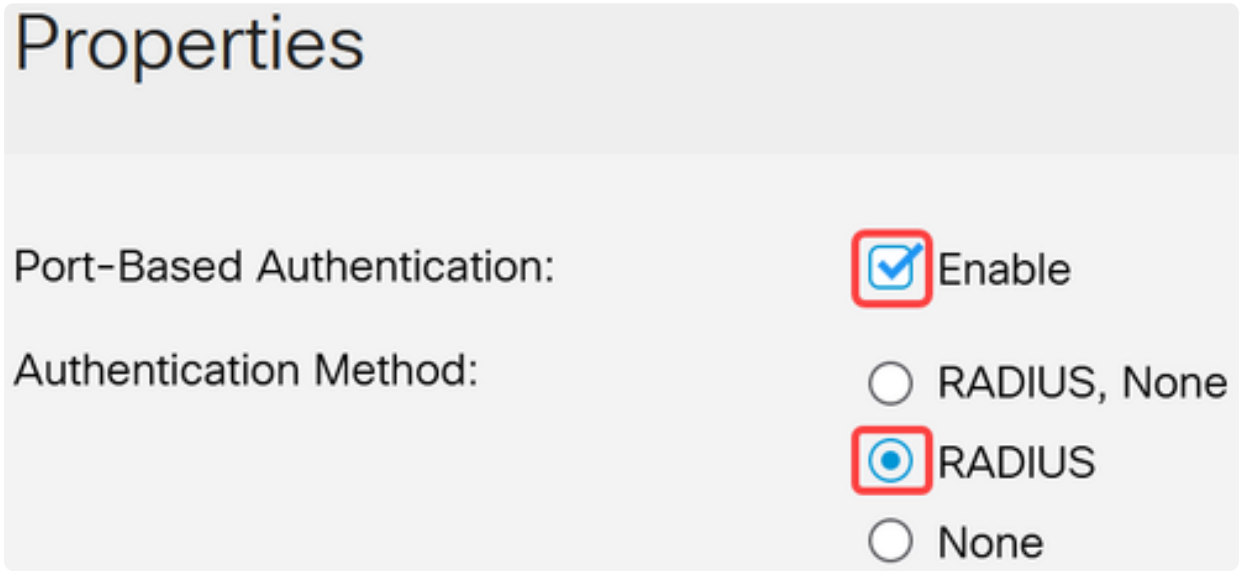
6단계

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



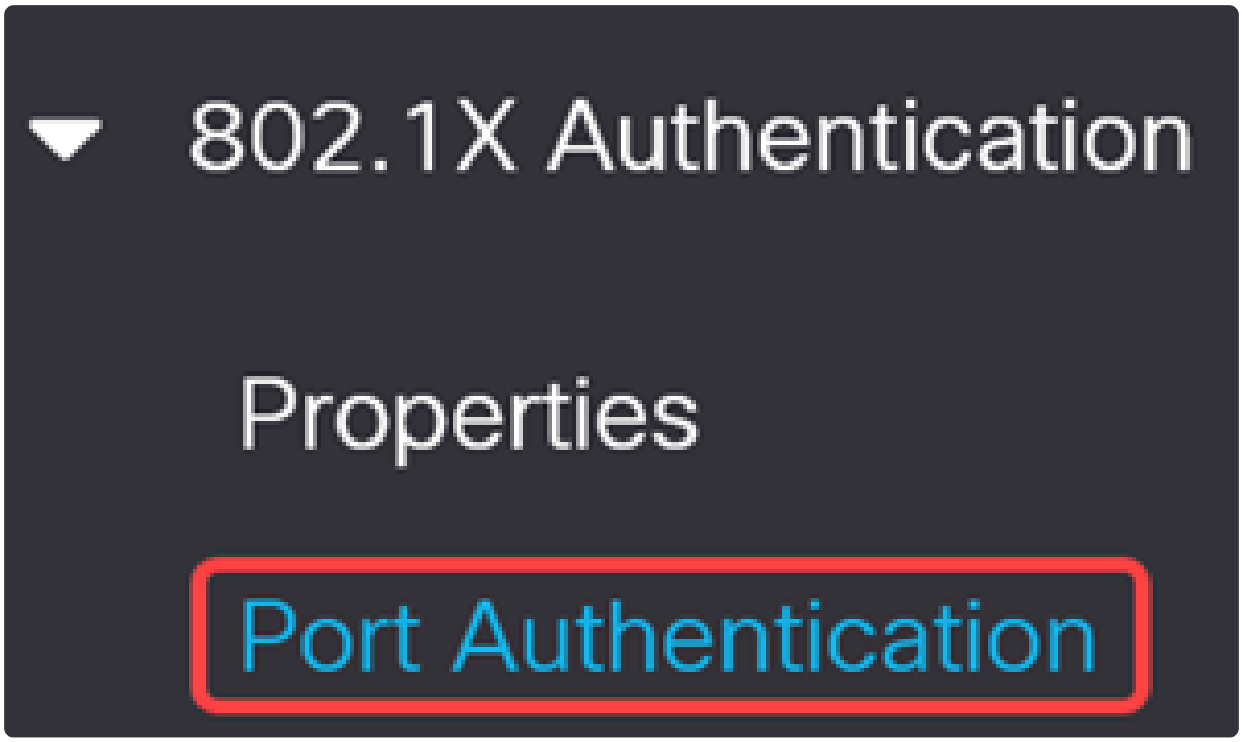
7단계

포트 기반 인증이 활성화되고 인증 방법이 RADIUS로 설정되었는지 확인합니다.



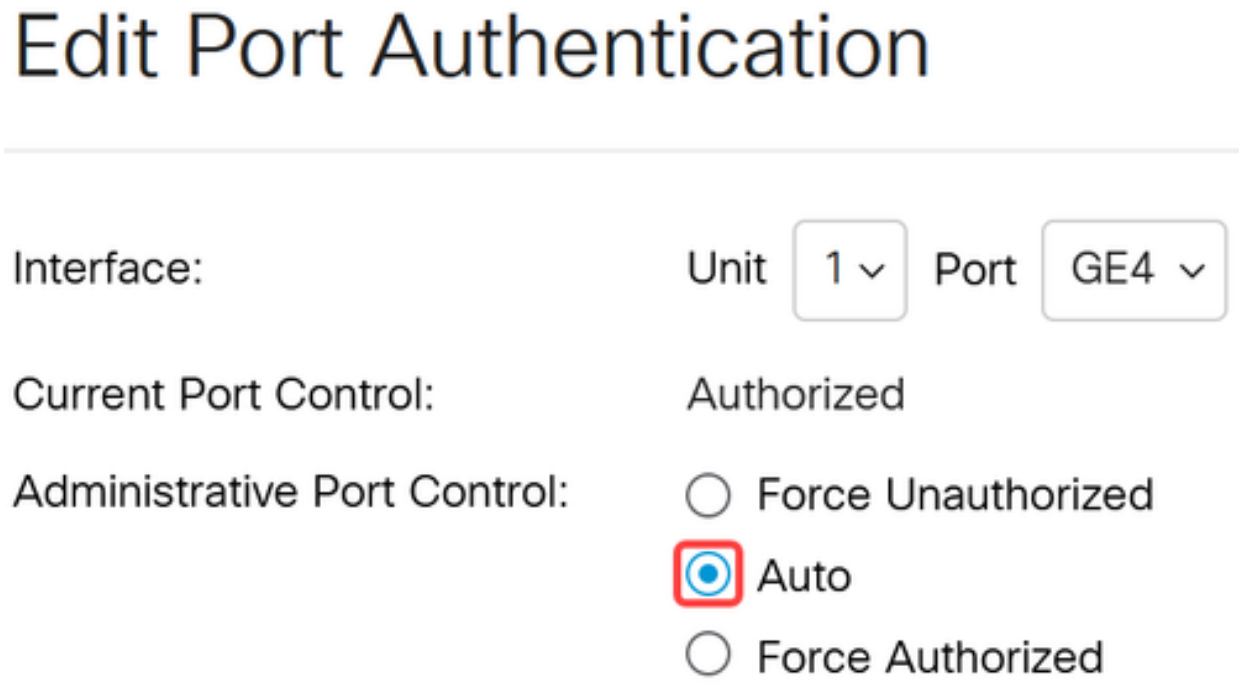
8단계

Port Authentication(포트 인증) 메뉴로 이동하여 원하는 포트를 선택하고 edit(수정)를 클릭합니다.



9단계

Administrative Port Control(관리 포트 제어)에서 Auto(자동) 옵션을 선택하면 RADIUS 응답에 따라 포트를 인증된 상태와 권한이 없는 상태 간에 전환합니다.

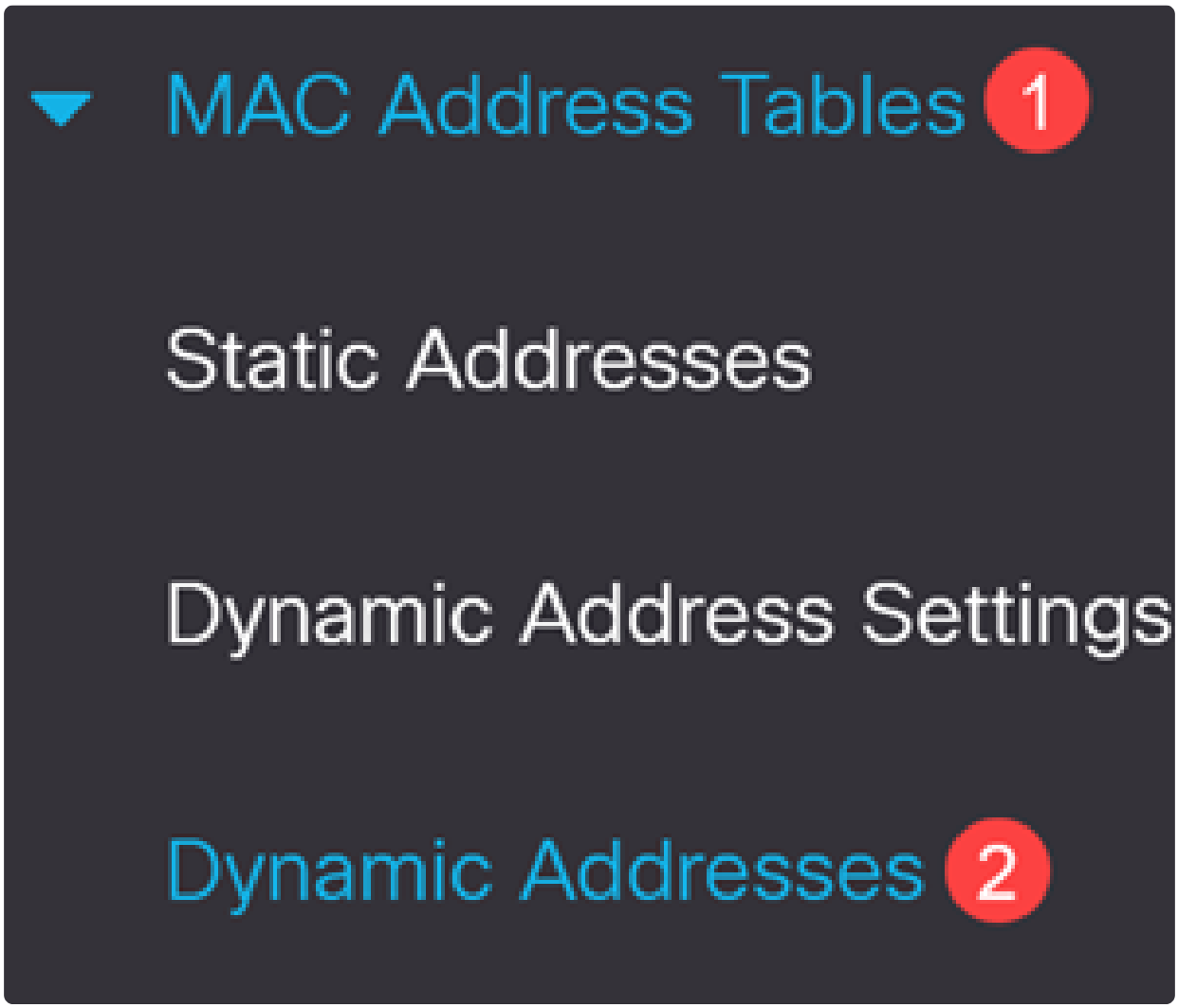


10단계

802.1x Based Authentication(802.1x 기반 인증)을 활성화하고 Apply(적용)를 클릭합니다.

11단계

포트의 디바이스에 대한 MAC 주소가 필요합니다. ISE의 CoA 작업은 해당 MAC 주소에 적용됩니다. 이 예에서는 포트 9입니다. 이 포트를 가져오려면 MAC 주소 테이블 > 동적 주소로 이동합니다.

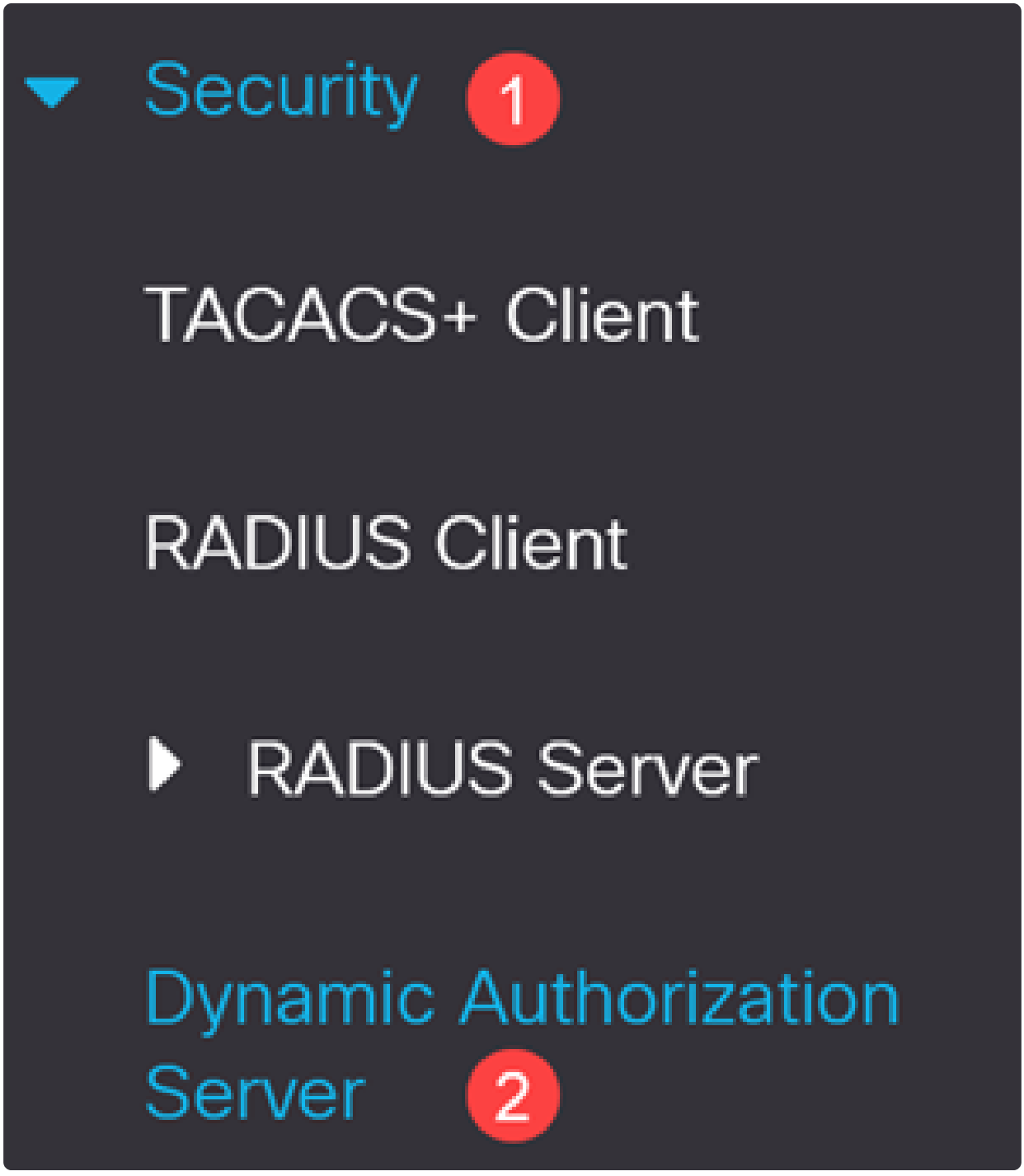


12단계

아래로 스크롤하여 포트로 이동하고 MAC 주소를 기록합니다.

13단계

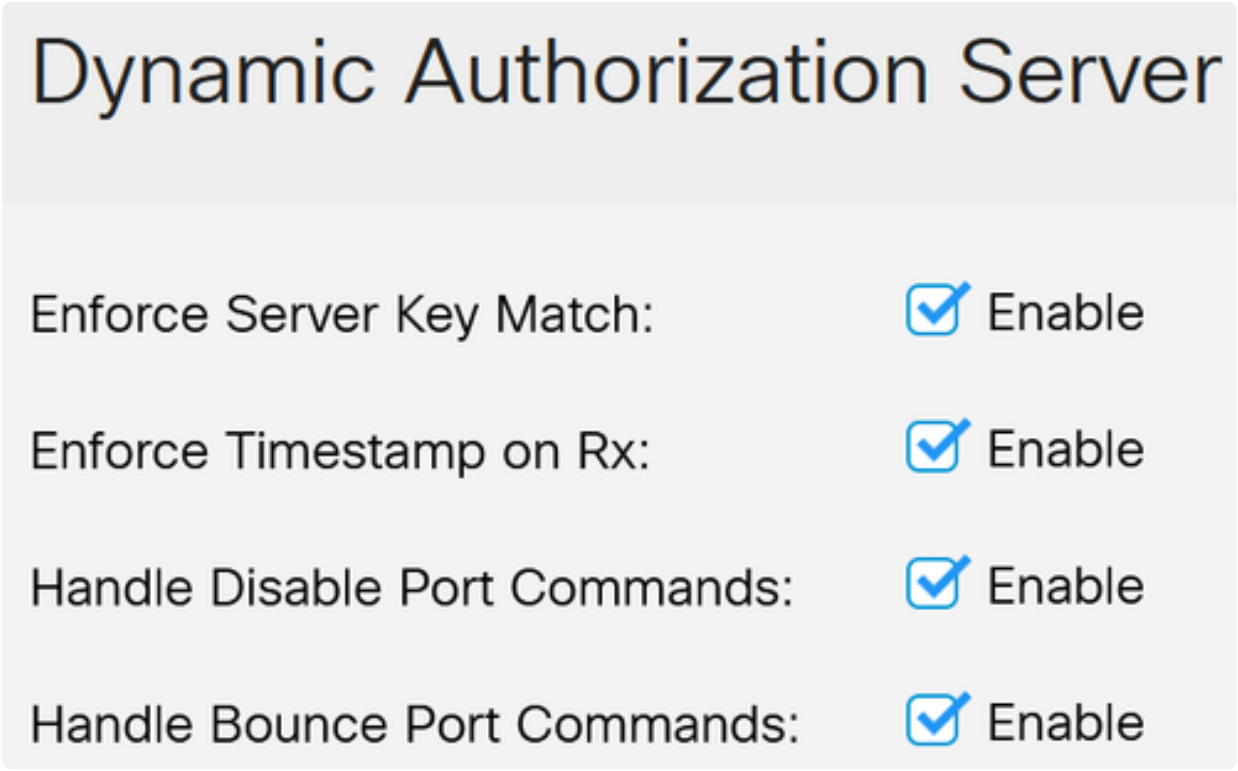
Security(보안) > Dynamic Authorization Server(동적 권한 부여 서버)로 이동합니다.



14단계

다음을 활성화합니다.

- 서버 키 일치 적용
- Rx에 타임스탬프 적용
- Disable Port 명령 처리
- Bounce Port 명령 처리

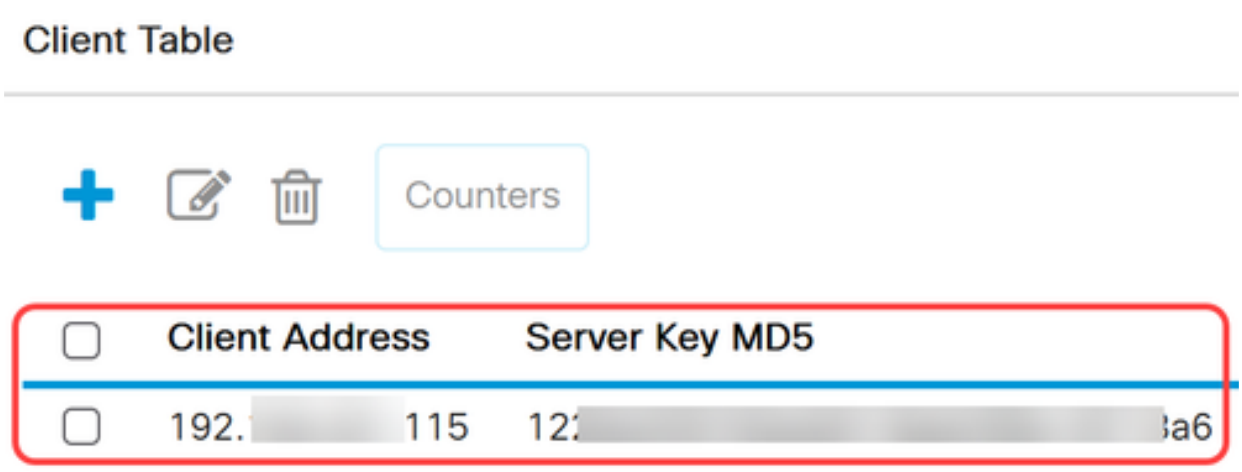


15단계

UDP Port를 기본값 1700으로 둡니다.

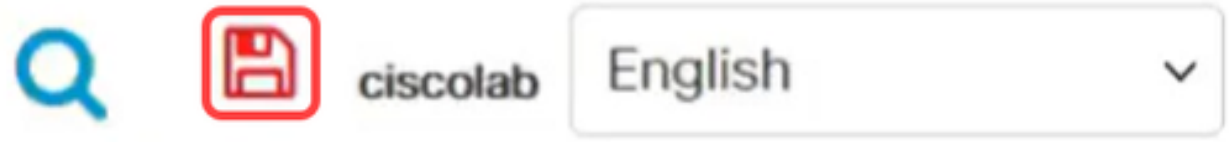
16단계

Client Table(클라이언트 테이블)에서 ISE 서버가 올바른 서버 키로 추가되었는지 확인합니다. 적용을 클릭합니다.



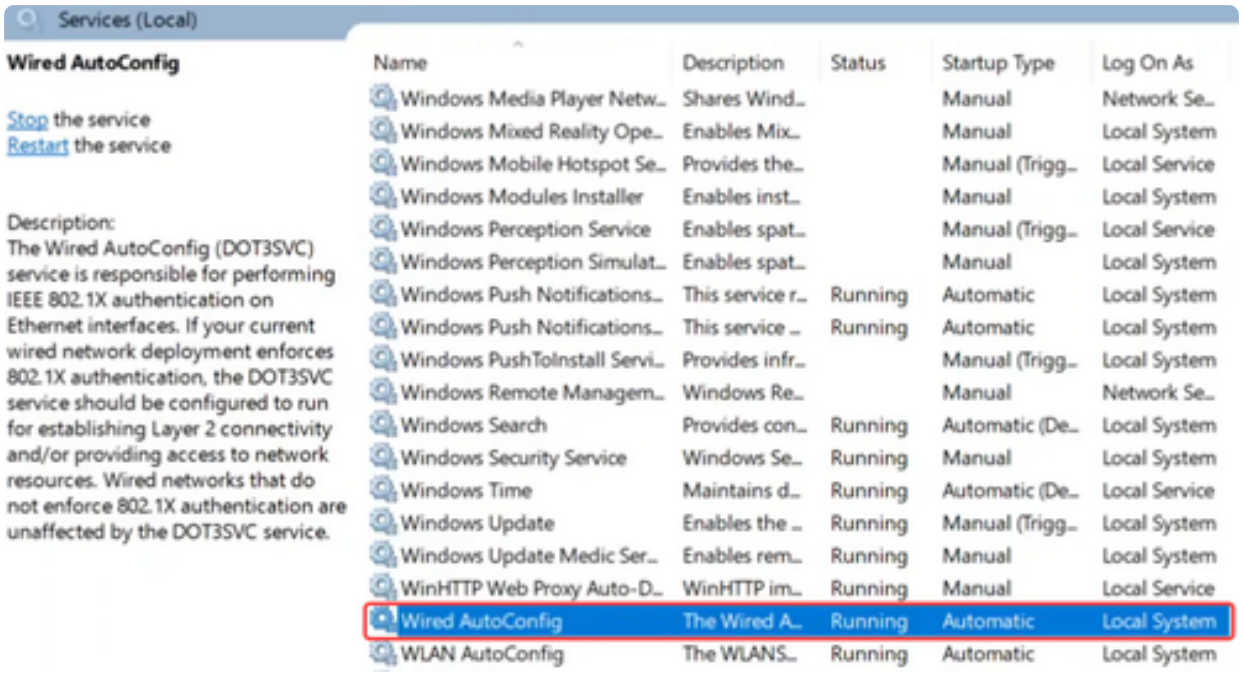
17단계

빨간색으로 깜박이는 저장 아이콘을 클릭하여 컨피그레이션을 저장합니다.



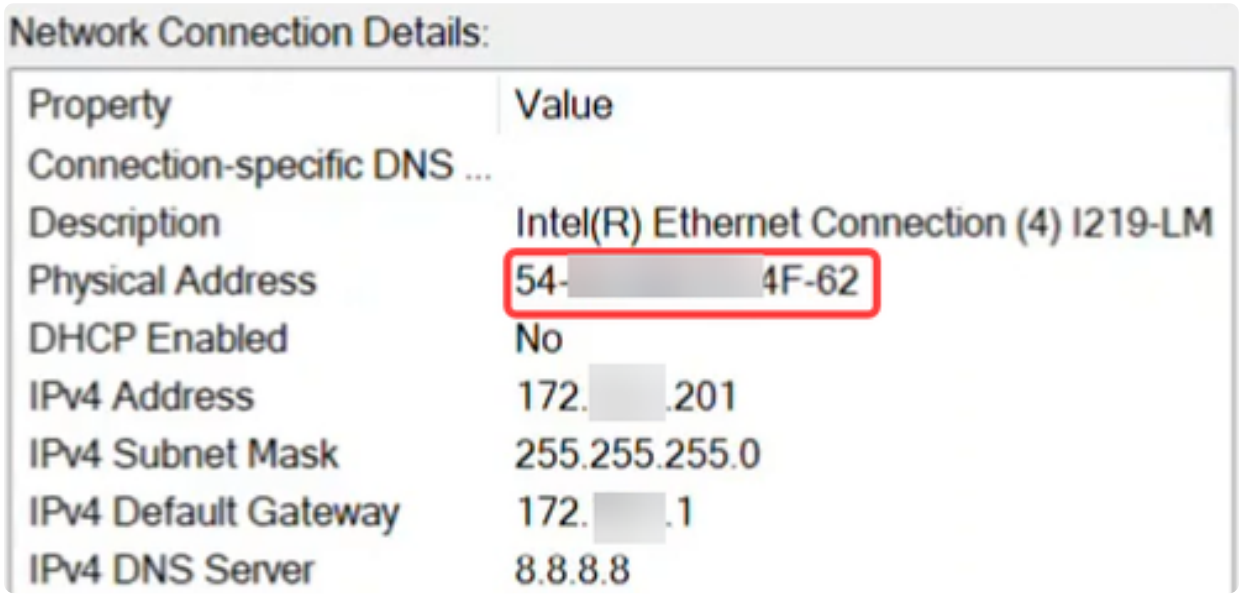
18단계

포트 9에 연결된 클라이언트 노트북 컴퓨터에서 802.1 X 인증에 대해 유선 자동 구성 서비스가 활성화되어 있는지 확인합니다.



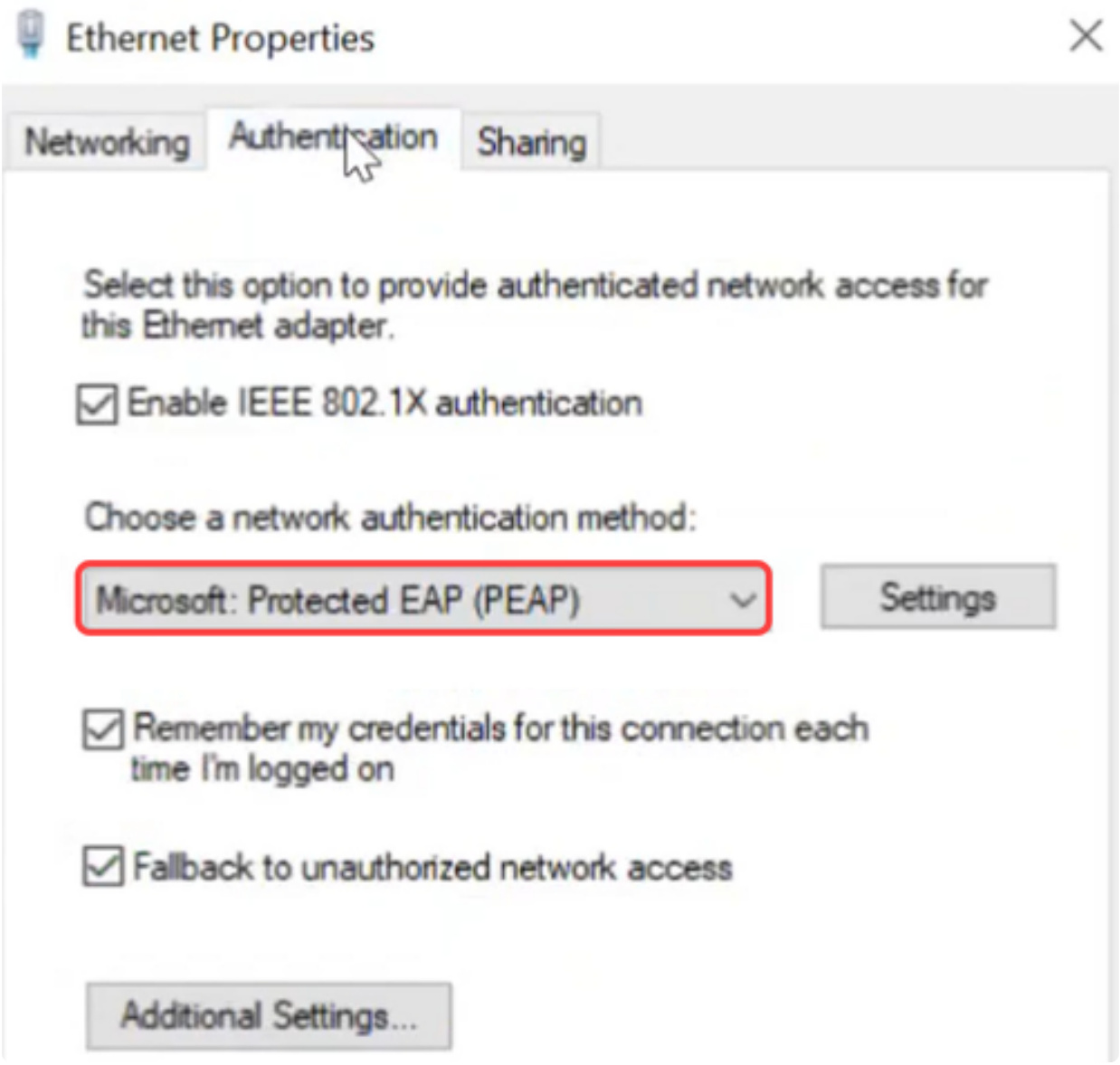
19단계

이더넷 어댑터 설정에서 MAC 주소가 일치하는지 확인합니다.



20단계

Ethernet settings(이더넷 설정) 아래의 Properties(속성) 버튼을 클릭하고 Authentication(인증) 탭 아래에서 확인란이 활성화되어 있는지 확인합니다. 또한 인증 방법이 PEAP(Protected EAP)인지 확인합니다.

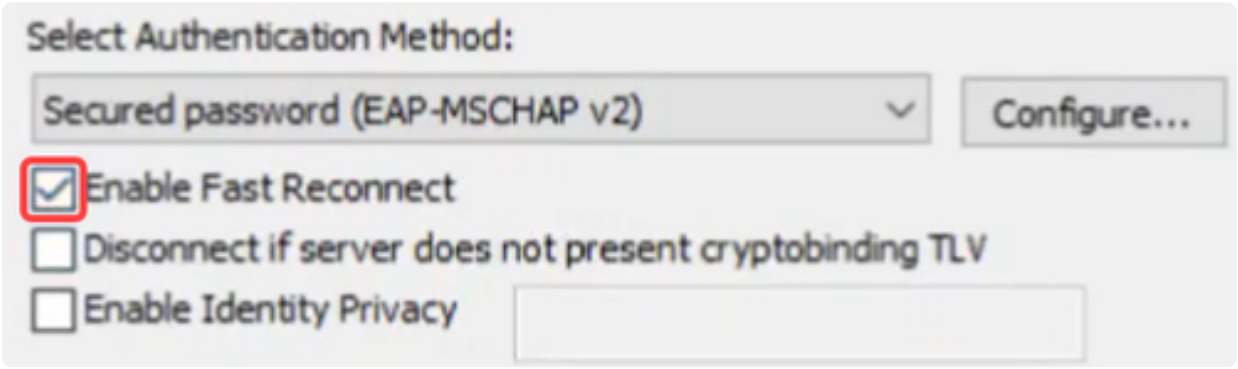


21단계

Settings(설정) 버튼을 클릭하여 Verify the server's identity by validating the certificate(인증서를 검증하여 서버 ID 확인) 옆에 있는 확인란이 선택되지 않았는지 확인합니다.

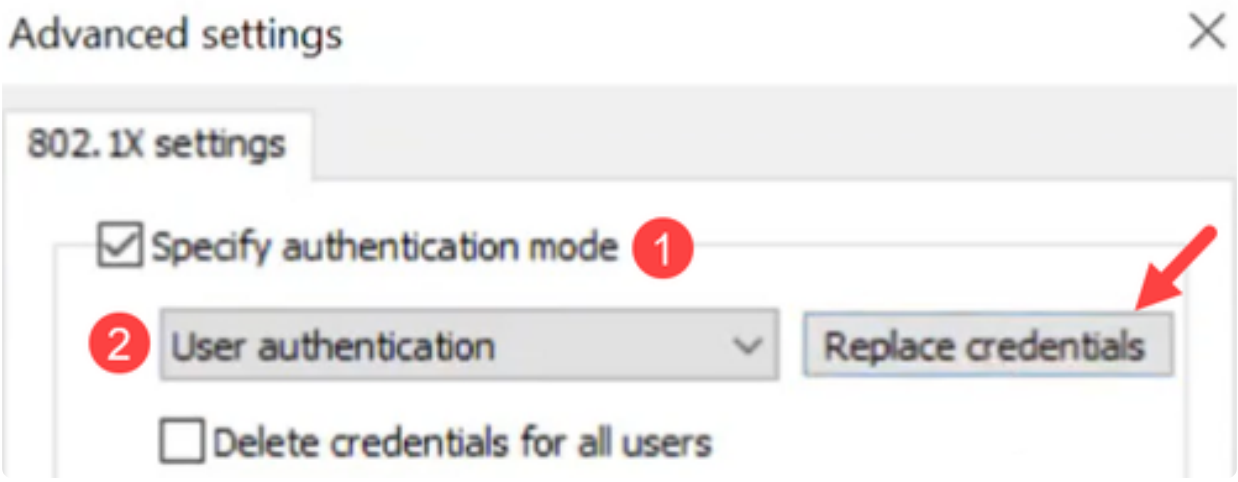
22단계

Enable Fast Reconnect(빠른 재연결 활성화) 상자를 선택해야 합니다.



23단계

Additional settings(추가 설정)에서 Specify authentication mode(인증 모드 지정)가 활성화되었는지, 그리고 드롭다운 메뉴에서 User authentication(사용자 인증)이 선택되어 있는지 확인합니다. ISE에서 생성한 자격 증명을 저장하거나 Replace credentials(자격 증명 바꾸기) 버튼을 사용하여 교체할 수 있습니다.



CoA 작업

CoA 작업을 시작하기 전에 스위치에서 패킷 캡처를 활성화합니다.

1단계

PuTTY에서 Catalyst 스위치에 로그인하고 monitor capture cap1 buffer size 20 circular 명령을 사용하여 버퍼 크기 및 캡처 모드를 지정합니다.

2단계

monitor capture cap1 control-plane both 명령을 사용하여 컨트롤 플레인을 both로 지정합니다.

3단계

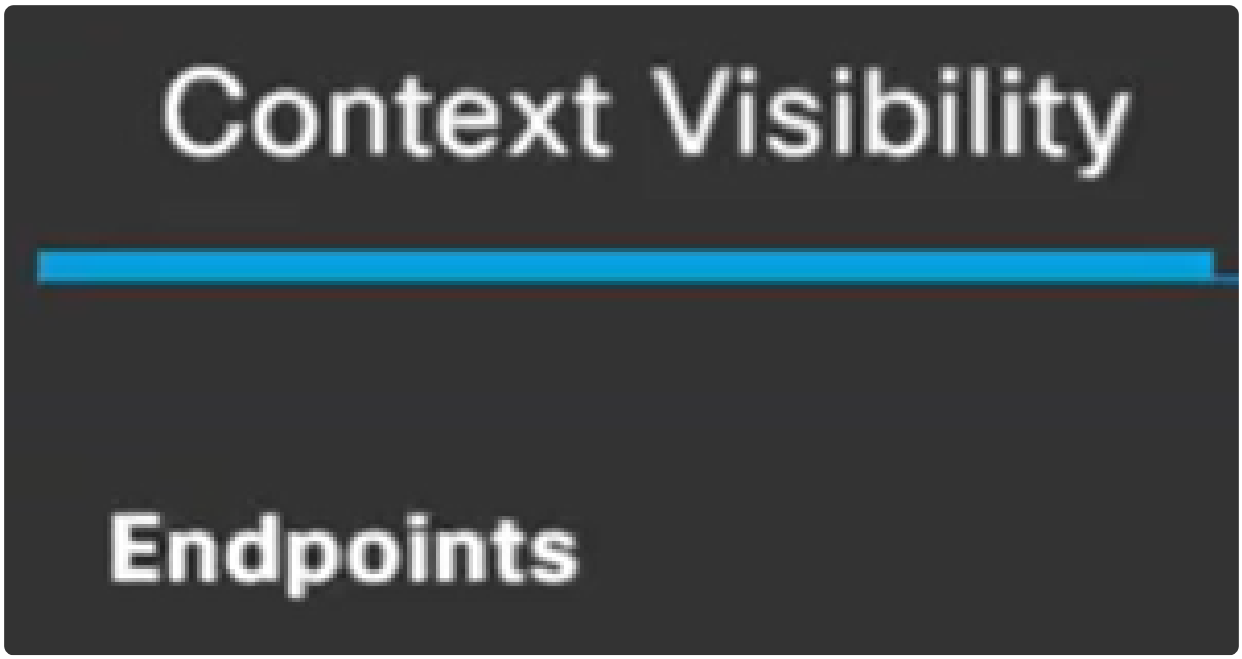
일치 기준을 any로 입력합니다. 이에 대한 명령은 monitor capture cap1 match any입니다.

4단계

패킷 캡처를 시작합니다.

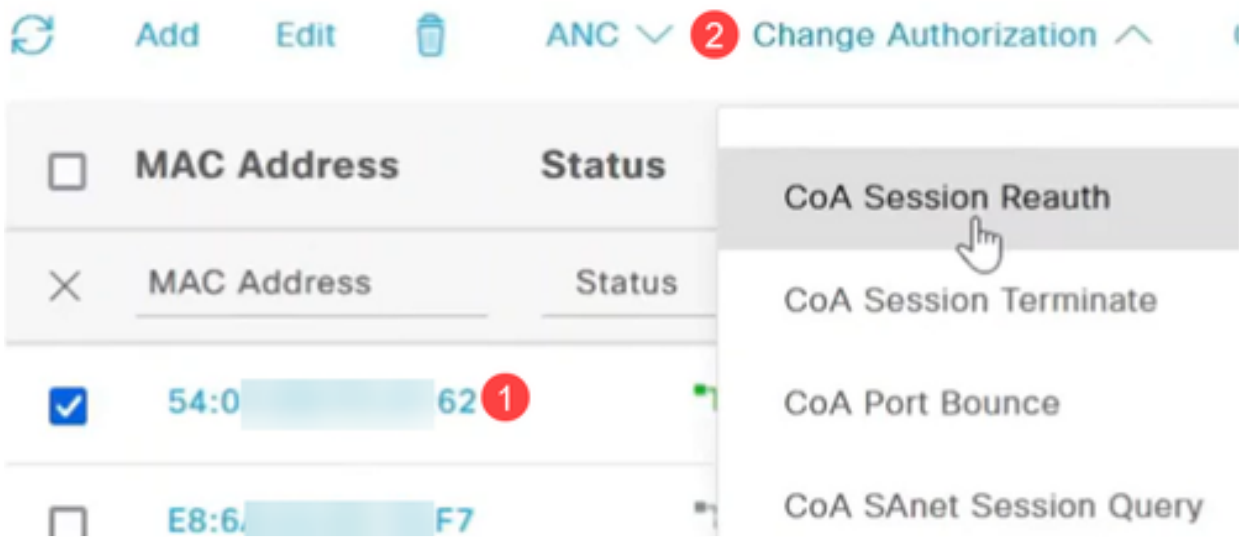
5단계

ISE 인터페이스의 Context Visibility(컨텍스트 가시성) 아래의 Endpoints(엔드포인트) 옵션으로 이동합니다.



6단계

MAC 주소를 선택하고 CoA 작업을 Change of Authorization 드롭다운 메뉴에서 선택합니다. 이 예에서는 CoA 세션 Reauth가 선택됩니다. 이렇게 하면 reauthenticate 명령으로 CoA 패킷을 전송하여 포트에서 강제로 재인증됩니다.



7단계

PuTTY 터미널로 돌아가 CoA 작업이 성공했는지 확인합니다.

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

8단계

CoA 세션 종료를 선택하면 관리 요청을 기반으로 종료 명령과 함께 연결 끊기 요청을 보냅니다.

```
Cat1300-1#04-Jul-2024 20:50:02 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:50:02 %SEC-W-COADISCSESSN: 802.1x session for host 54:[redacted]: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 gi1/0/9 is Authorized
```

9단계

CoA Port Bounce(CoA 포트 반송) 옵션은 bounce host port(반송 호스트 포트) 명령이 포함된 CoA 요청 패킷을 전송하여 스위치의 포트를 비활성화했다가 다시 활성화합니다. 네트워크 어댑터가 10초 동안 오프라인 상태로 유지되며 무단 상태가 됩니다. 온라인에서 컴백되고 권한이 부여되며 패킷을 전달할 수 있습니다.

```
Cat1300-1#04-Jul-2024 20:50:21 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:[redacted]:62
04-Jul-2024 20:50:21 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:34 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:34 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:50:36 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:50:39 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:50:39 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized

Cat1300-1#04-Jul-2024 20:50:45 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

10단계

포트 바운스를 사용하는 CoA 세션 종료는 기존 세션을 종료하고, 10초 동안 포트를 바운스하며, 승인되지 않습니다. 그런 다음 다시 온라인 상태가 되고 권한이 부여되며 패킷을 전달할 수 있습니다.

```
Cat1300-1#04-Jul-2024 20:51:04 %SEC-W-COABNCEPORT: Interface gi1/0/9 suspended for 10 seconds by Co
A Request "bounce host port" for host 54:[redacted]:62
04-Jul-2024 20:51:04 %LINK-W-Down:  gi1/0/9
04-Jul-2024 20:51:22 %LINK-I-Up:  gi1/0/9
04-Jul-2024 20:51:22 %SEC-W-PORTUNAUTHORIZED: Port gi1/0/9 is unAuthorized
04-Jul-2024 20:51:22 %SEC-I-PORTAUTHORIZED: Port gi1/0/9 is Authorized
04-Jul-2024 20:51:29 %STP-W-PORTSTATUS: gi1/0/9: STP status Forwarding
```

11단계

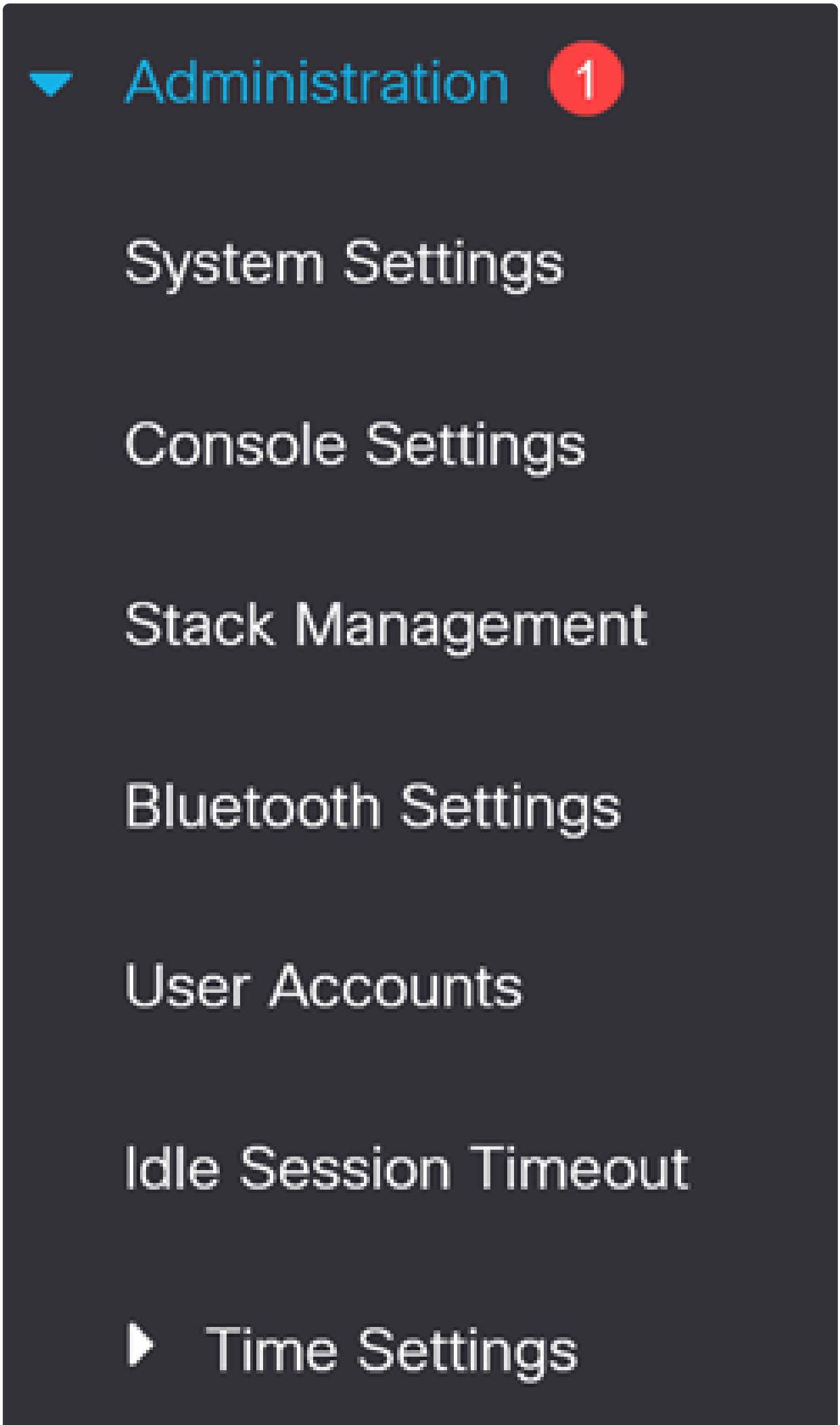
포트 종료 시 CoA 세션 종료는 세션을 종료하고 관리적으로 포트를 종료합니다.

12단계

패킷 캡처를 중지하려면 monitor capture cap1 stop 명령을 사용합니다.

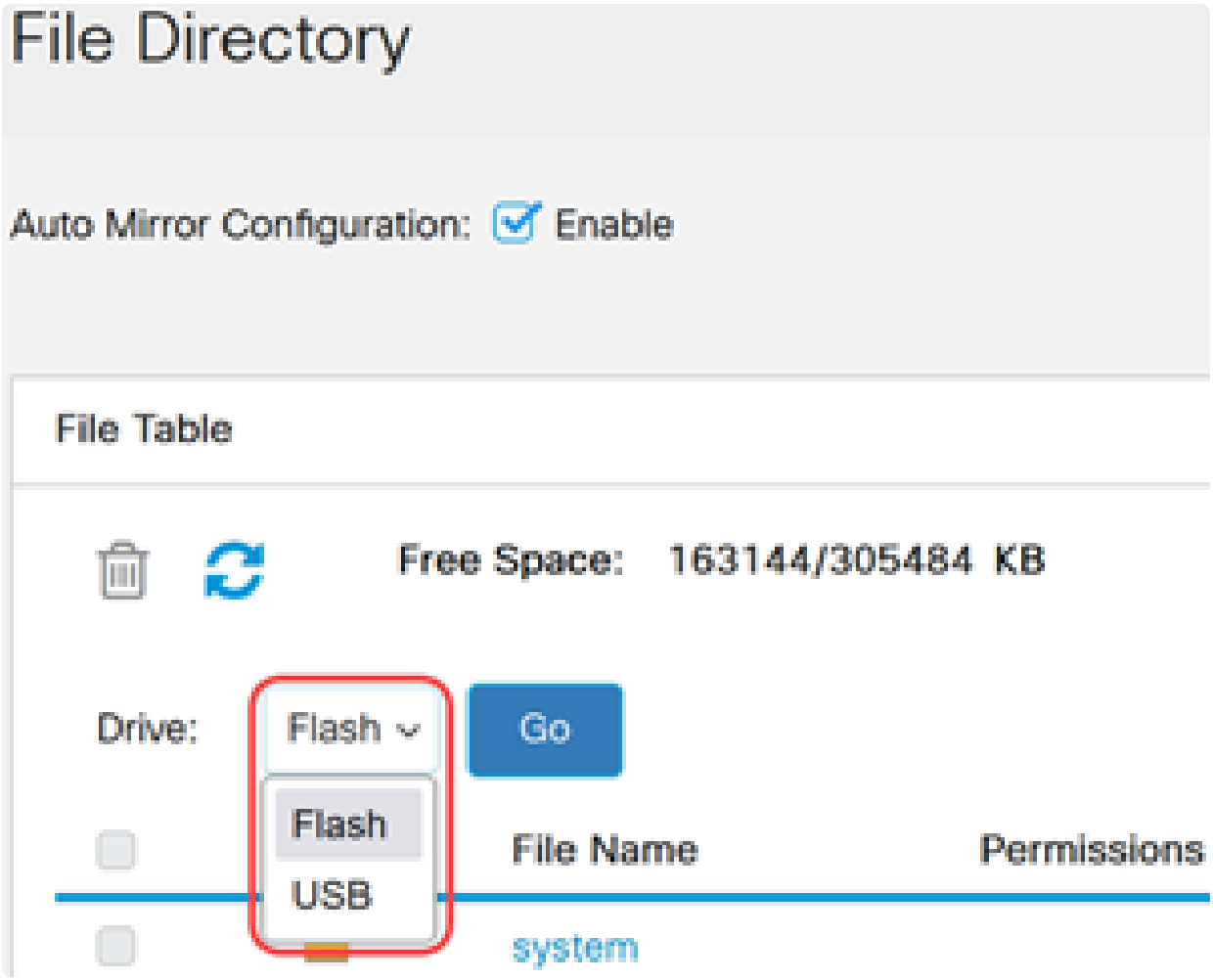
13단계

파일을 복사하려면 Administration(관리) > File Management(파일 관리) > File Directory(파일 디렉토리)로 이동합니다.


Administration
1
System Settings
Console Settings
Stack Management
Bluetooth Settings
User Accounts
Idle Session Timeout
Time Settings

14단계

기본 플래시를 사용할 수 있습니다. 또는 Drive(드라이브) 드롭다운 메뉴에서 USB를 선택할 수 있습니다.



결론

이제 ISE에 대한 모든 정보와 Catalyst 1300 Series 스위치에서 CoA를 구성하는 방법을 알 수 있습니다.

자세한 내용은 아래 비디오를 참조하십시오.

이 문서와 관련이 있는 비디오 시청...

시스코의 다른 Tech Talk을 보려면 여기를 클릭

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.