200/220/300 Series 스위치의 802.1X 호스트 및 세션 인증 컨피그레이션

목표

802.1X는 포트에 연결된 장치에 인증 방법을 제공하는 PNAC(Port-based Network Access Control)에 대한 IEEE 표준입니다. 스위치의 Administration GUI에 있는 Host and Session Authentication(호스트 및 세션 인증) 페이지는 포트별로 어떤 인증 유형을 사용할지 정의하는 데 사용됩니다. 포트별 인증은 네트워크 관리자가 원하는 인증 유형에 따라 스위치 포트를 나눌 수 있는 기능입니다. Authenticated Hosts(인증된 호스트) 페이지에는 인증된 호스트에 대한 정보가 표시됩니다.

이 문서에서는 포트별로 호스트 및 세션 인증을 구성하는 방법과 200/220/300 Series Managed Switch의 802.1X 보안 설정에서 인증된 호스트를 보는 방법에 대해 설명합니다.

적용 가능한 디바이스

- Sx200 시리즈
- Sx220 시리즈
- Sx300 시리즈

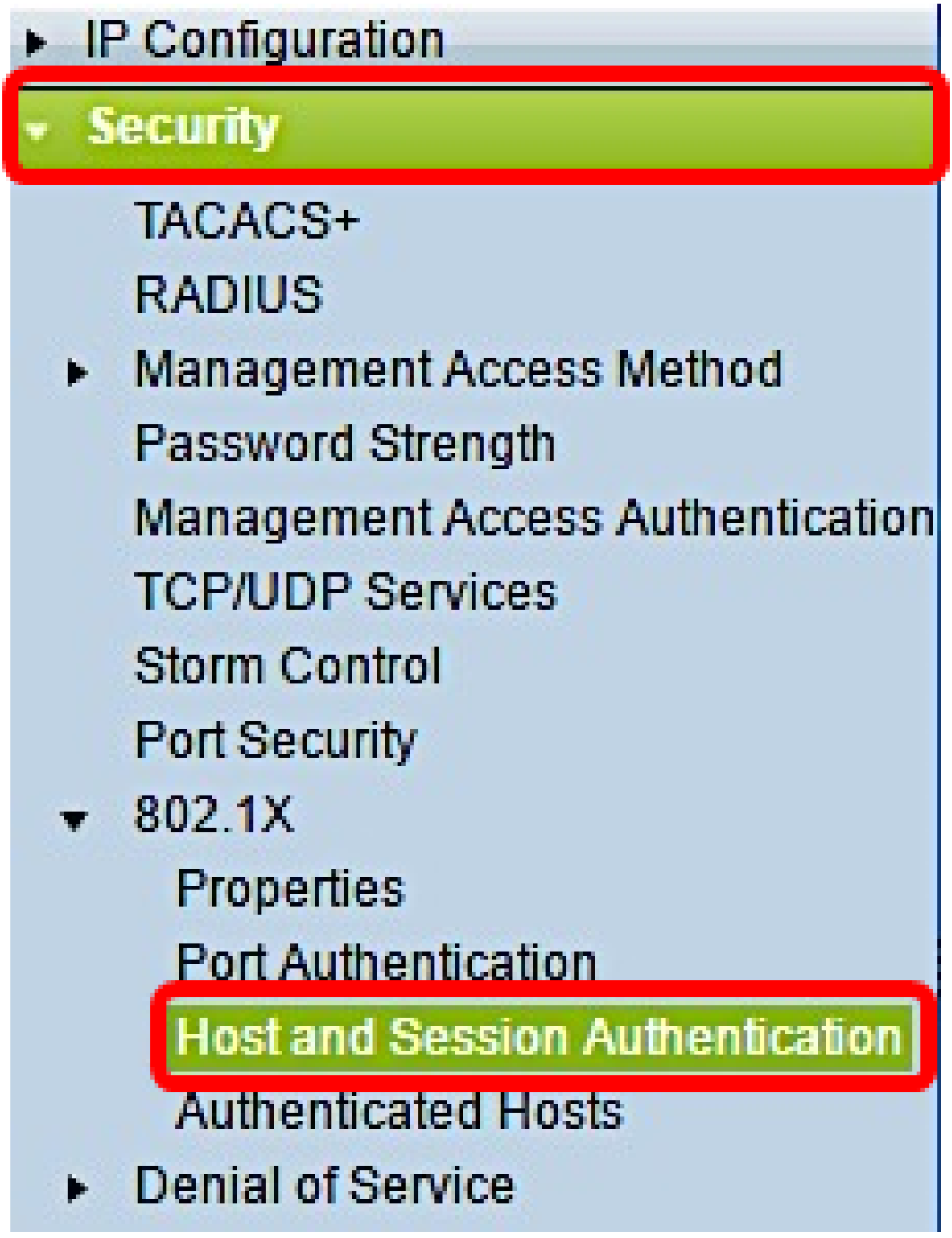
소프트웨어 버전

- 1.4.5.02 — Sx200 시리즈, Sx300 시리즈
- 1.1.0.14 — Sx220 시리즈

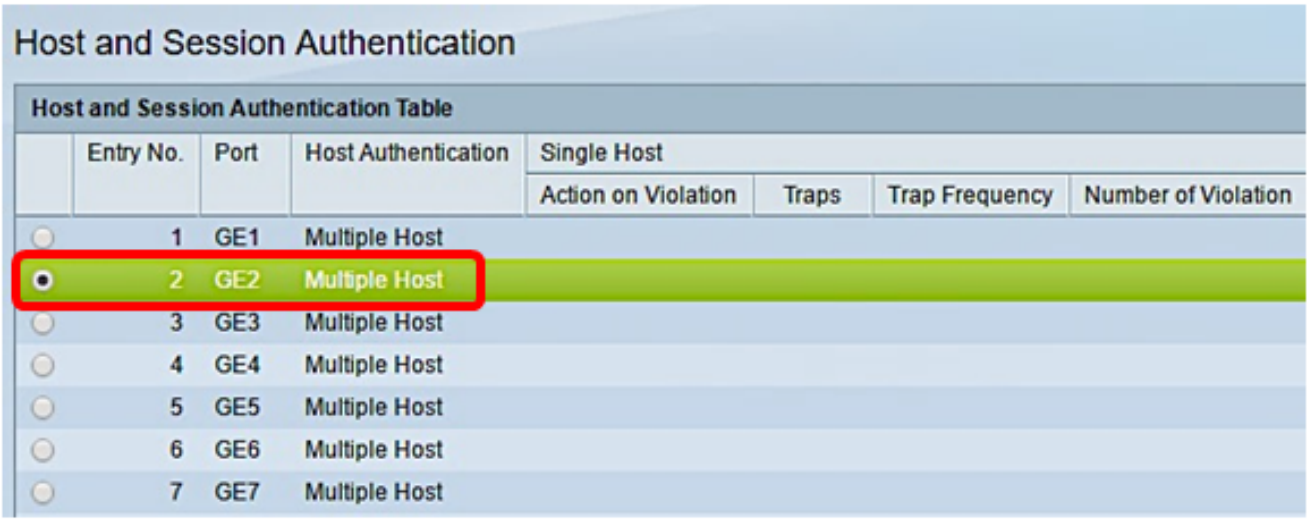
호스트 및 세션 인증

1단계. 웹 기반 유틸리티에 로그인하고 Security(보안) > 802.1X > Host and Session Authentication(호스트 및 세션 인증)을 선택합니다.

참고: 아래 이미지는 SG220-26P Smart 스위치에서 가져온 것입니다.

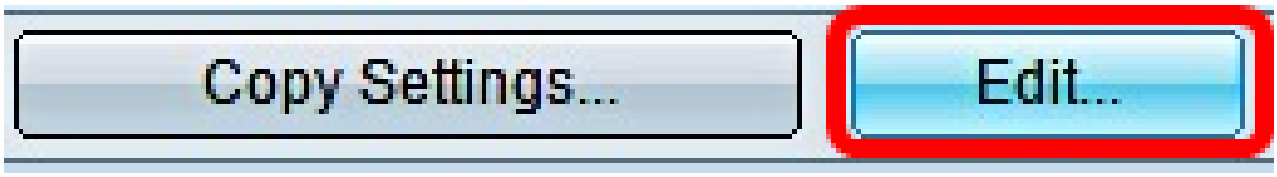


2단계. 수정할 포트의 라디오 버튼을 클릭합니다.

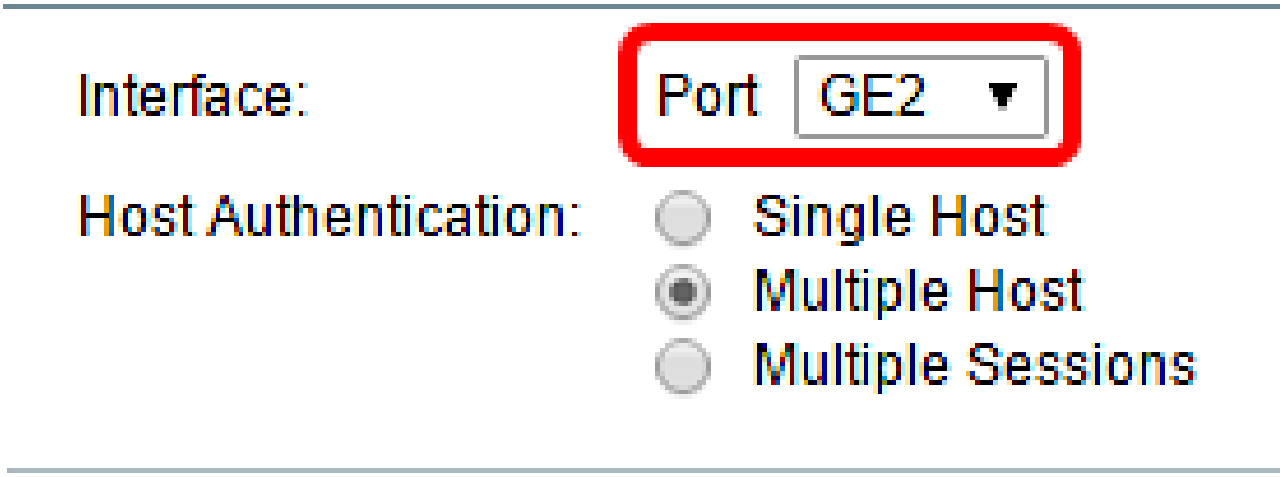


참고: 이 예제에서는 포트 GE2를 선택합니다.

3단계. 지정된 포트에 대한 호스트 및 세션 인증을 수정하려면 Edit를 클릭합니다.



4단계. 그러면 Edit Port Authentication(포트 인증 수정) 창이 팝업됩니다. Interface 드롭다운 목록에서 지정된 포트가 2단계에서 선택한 포트인지 확인합니다. 그렇지 않으면 드롭다운 화살표를 클릭하고 오른쪽 포트를 선택합니다.

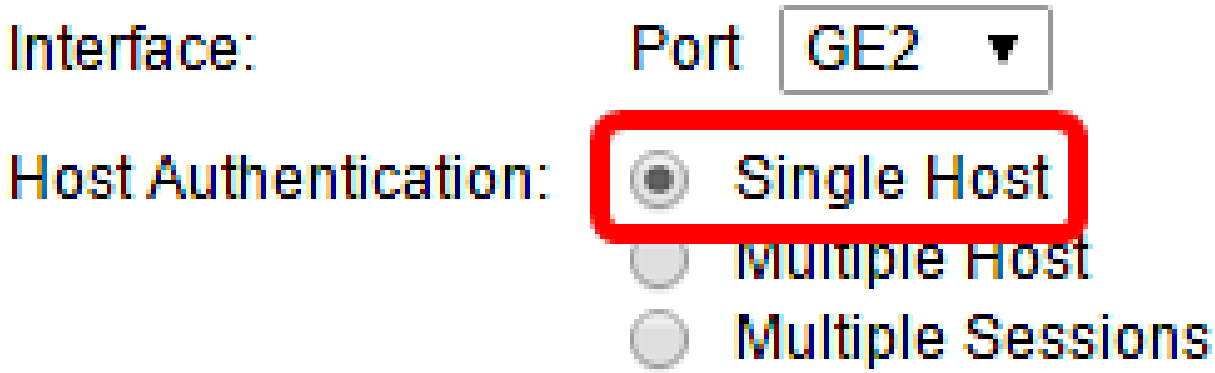


참고: 200 또는 300 Series를 사용 중인 경우 Edit Host and Session Authentication 창이 나타납니다.

5단계. Host Authentication(호스트 인증) 필드에서 원하는 인증 모드에 해당하는 라디오 버튼을 클릭합니다. 옵션은 다음과 같습니다.

- 단일 호스트 — 스위치는 포트에 대한 단일 권한 있는 호스트 액세스만 허용합니다.
- 다중 호스트(802.1X) — 다중 호스트가 단일 포트에 액세스할 수 있습니다. 기본 모드입니다. 스위치에서는 첫 번째 호스트만 인증하면 되므로, 포트에 연결된 다른 모든 클라이언트는 네트워크에 액세스할 수 있습니다. 인증이 실패할 경우 첫 번째 호스트 및 연결된 모든 클라이언트의 네트워크 액세스가 거부됩니다.
- 다중 세션 — 다중 호스트가 단일 포트에 액세스할 수 있지만 각 호스트는 인증되어야 합니다.

참고: 이 예에서는 단일 호스트를 선택합니다.

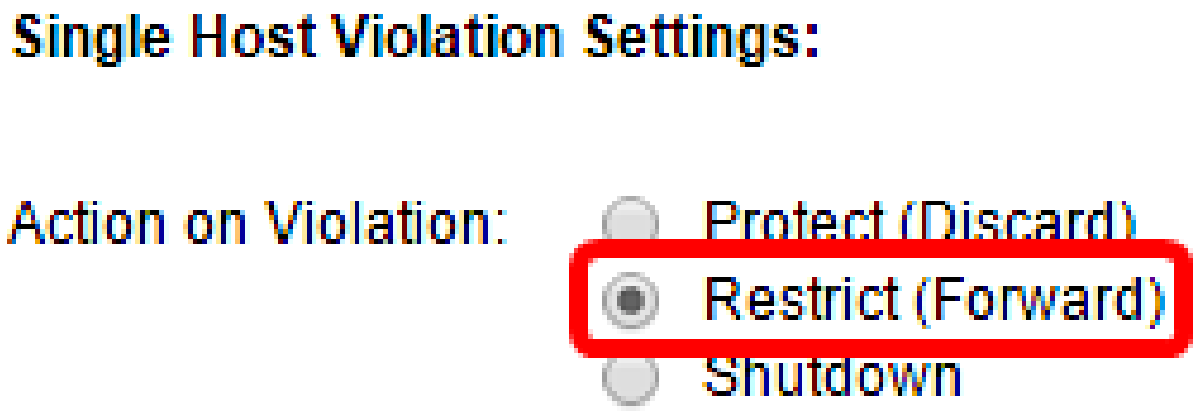


참고: Multiple Host(다중 호스트) 또는 Multiple Sessions(다중 세션)를 선택한 경우 9단계로 건너뜁니다.

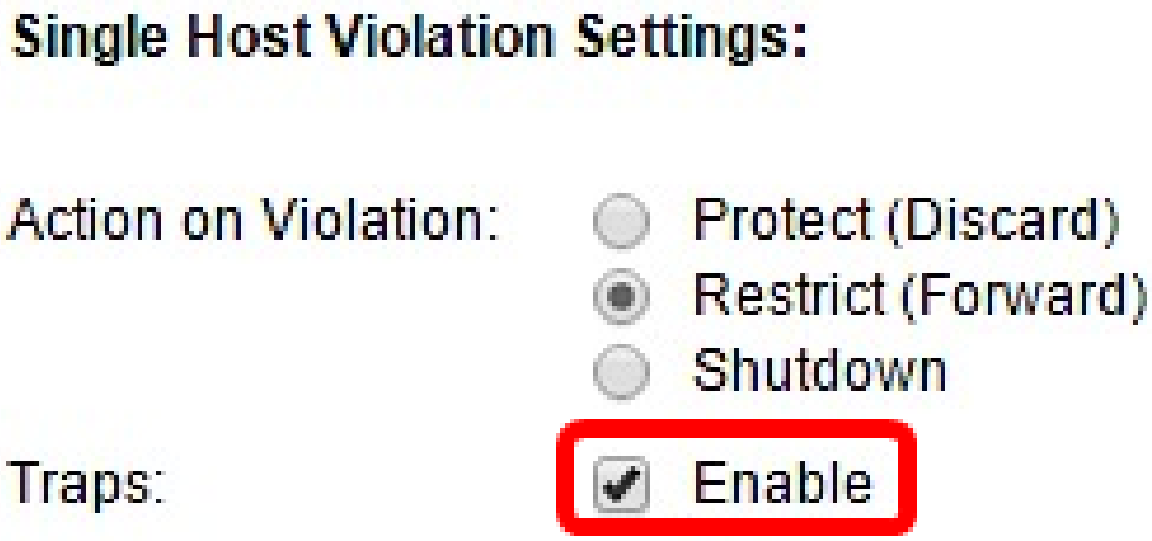
6단계. Single Host Violation Settings(단일 호스트 위반 설정) 영역에서 원하는 Action on Violation(위반 시 작업)에 해당하는 라디오 버튼을 클릭합니다. 원래 신청자의 MAC 주소와 일치하지 않는 MAC 주소를 가진 호스트에서 패킷이 도착하면 위반이 발생합니다. 이 경우 작업은 원래 신청자로 간주되지 않는 호스트에서 도착하는 패킷에 대해 어떤 일이 발생하는지 결정합니다. 옵션은 다음과 같습니다.

- Protect (Discard) — 패킷을 삭제합니다. 이것이 기본 작업입니다.
- Restrict (Forward) — 액세스 권한을 부여하고 패킷을 전달합니다.
- Shutdown — 패킷을 차단하고 포트를 종료합니다. 포트가 다시 활성화될 때까지 또는 스위치가 재부팅될 때까지 계속 중단됩니다.

주: 이 예제에서는 제한(전달)을 선택합니다.



7단계. (선택 사항) Traps(트랩) 필드에서 Enable(활성화)을 선택하여 트랩을 활성화합니다. 트랩은 시스템 이벤트를 보고하는 데 사용되는 SNMP(Simple Network Management Protocol) 메시지를 생성합니다. 위반이 발생하면 스위치의 SNMP 관리자에게 트랩이 전송됩니다.



8단계. Trap Frequency(트랩 빈도) 필드에 전송된 트랩 사이에 허용되는 시간을 초 단위로 입력합니다. 트랩이 전송되는 빈도를 정의합니다.

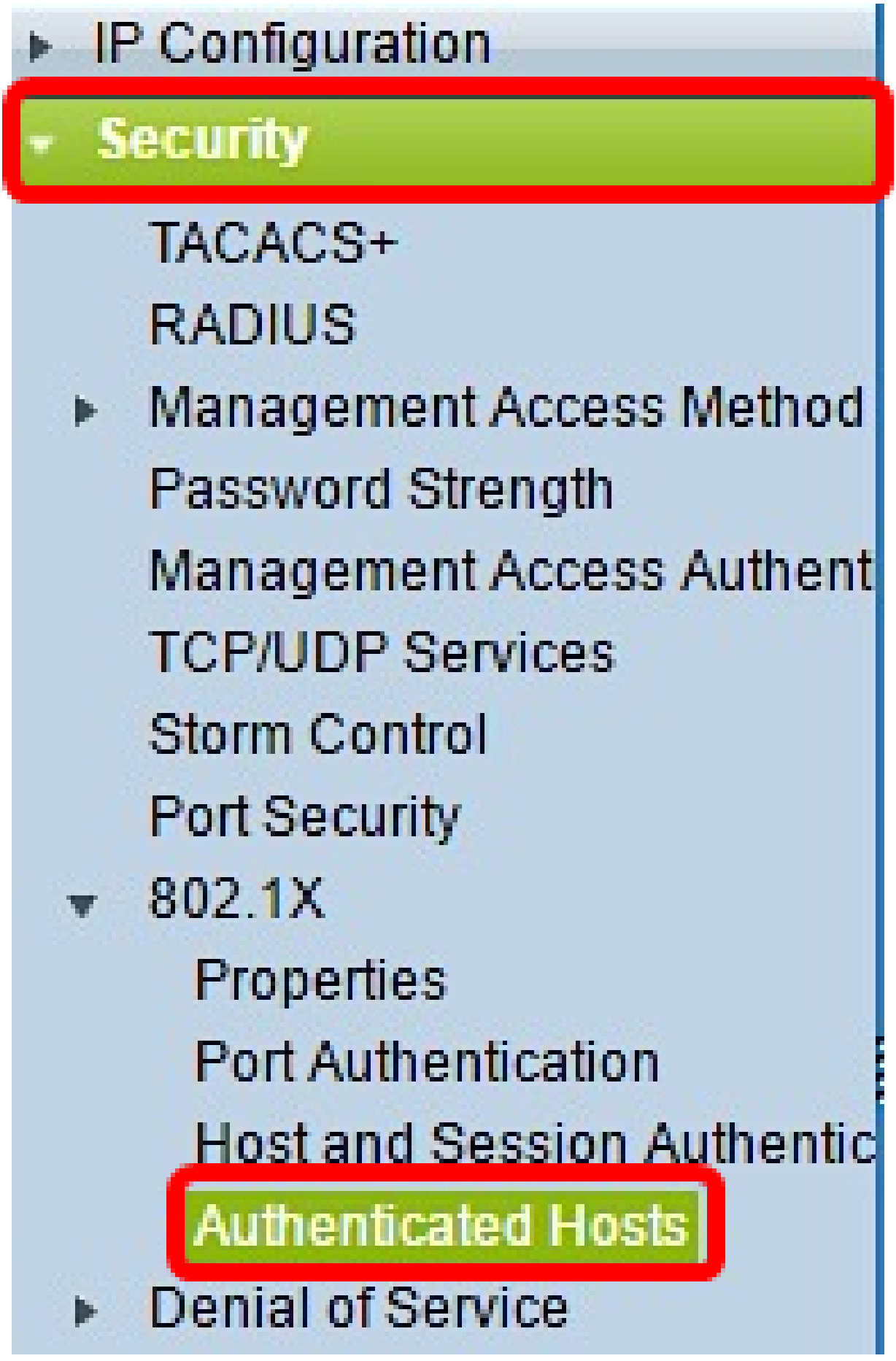
참고: 이 예에서는 30초가 사용됩니다.

9단계. 적용을 클릭합니다.

이제 스위치에 호스트 및 세션 인증을 구성해야 합니다.

인증된 호스트 보기

1단계. 웹 기반 유틸리티에 로그인하고 Security(보안) > 802.1X > Authenticated Host(인증된 호스트)를 선택합니다.


IP Configuration
Security
TACACS+
RADIUS
Management Access Method
Password Strength
Management Access Authent
TCP/UDP Services
Storm Control
Port Security
802.1X
Properties
Port Authentication
Host and Session Authentic
Authenticated Hosts
Denial of Service

Authenticated Hosts(인증된 호스트) 테이블에는 인증된 호스트에 대한 다음 정보가 표시됩니다.

- 사용자 이름 — 포트에서 인증된 신청자 이름을 지정합니다.
- Port — 신청자가 연결되는 포트 번호를 지정합니다.
- 세션 시간 — 신청자가 포트에 연결된 전체 시간을 지정합니다. 형식은 DD:HH:MM:SS(Day:Hour:Minute:Second)입니다.
- 인증 방법 — 인증에 사용되는 방법을 지정합니다. 가능한 값은 다음과 같습니다.
- None — 신청자가 인증되지 않았음을 지정합니다.
- Radius — 신청자가 RADIUS 서버에 의해 인증되었음을 지정합니다.
- MAC Address — 신청자의 MAC 주소를 지정합니다.
- VLAN ID — 호스트가 속한 VLAN을 지정합니다. VLAN ID 열은 220 Series Smart Plus 스위치에서만 사용할 수 있습니다.

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.