스위치에서 SSH(Secure Shell) 서버 인증 설정 구성

목표

이 문서에서는 스위치에 연결하는 방법이 아니라 관리되는 스위치에서 서버 인증을 구성하는 방법에 대한 지침을 제공합니다. SSH + Putty를 통해 스위치에 연결하는 방법에 대한 기사를 보려면 여기를 클릭하여 해당 기사를 확인하십시오.

SSH(Secure Shell)는 특정 네트워크 디바이스에 대한 보안 원격 연결을 제공하는 프로토콜입니다. 이 연결은 암호화된다는 점을 제외하면 텔넷 연결과 유사한 기능을 제공합니다. SSH를 사용하면 관리자가 서드파티 프로그램으로 CLI(Command Line Interface)를 통해 스위치를 구성할 수 있습니다. 스위치는 네트워크 내 사용자에게 SSH 기능을 제공하는 SSH 클라이언트 역할을 합니다. 스위치는 SSH 서버를 사용하여 SSH 서비스를 제공합니다. SSH 서버 인증이 비활성화되면 스위치는 모든 SSH 서버를 신뢰할 수 있는 서버로 간주하므로 네트워크의 보안이 저하됩니다. 스위치에서 SSH 서비스가 활성화되면 보안이 강화됩니다.

적용 가능한 디바이스

- Sx200 시리즈
- Sx300 시리즈
- Sx350 시리즈
- SG350X 시리즈
- Sx500 시리즈
- Sx550X 시리즈

소프트웨어 버전

- 1.4.5.02 - Sx200 시리즈, Sx300 시리즈, Sx500 시리즈
- 2.2.0.66 - Sx350 Series, SG350X Series, Sx550X Series

SSH 서버 인증 설정 구성

SSH 서비스 사용

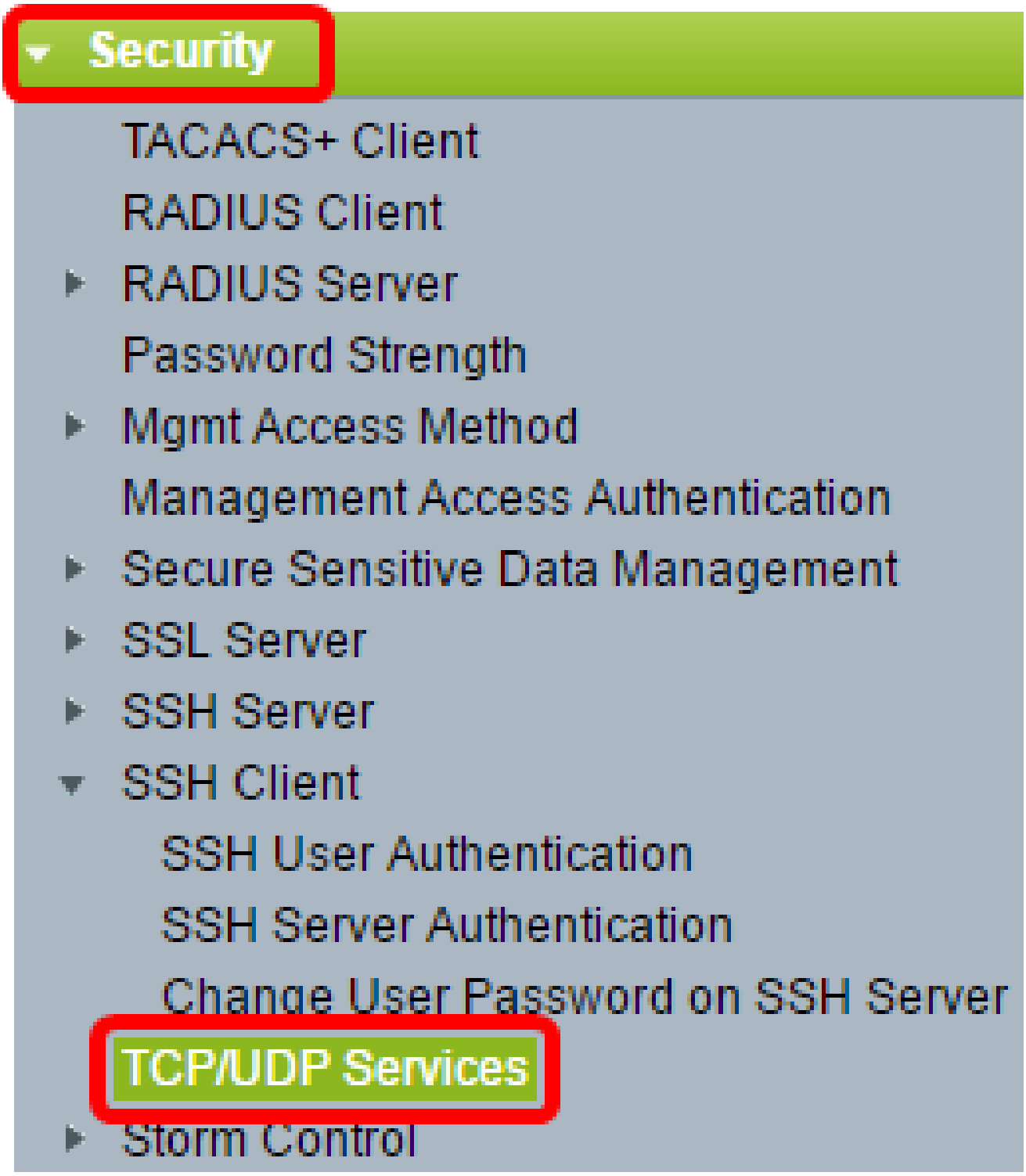
SSH 서버 인증이 활성화된 경우 디바이스에서 실행 중인 SSH 클라이언트가 다음 인증 프로세스를 사용하여 SSH 서버를 인증합니다.

- 디바이스는 SSH 서버의 수신된 공개 키의 지문을 계산합니다.
- 디바이스는 SSH Trusted Servers 테이블에서 SSH 서버의 IP 주소 및 호스트 이름을 검색합니다. 다음 세 가지 결과 중 하나가 발생할 수 있습니다.

1. 서버의 주소 및 호스트 이름과 핑거프린트에 대한 일치 항목이 발견되면 서버가 인증됩니다.
2. 일치하는 IP 주소 및 호스트 이름이 발견되었지만 일치하는 핑거프린트가 없는 경우 검색이 계속됩니다. 일치하는 핑거프린트가 없으면 검색이 완료되고 인증이 실패합니다.
3. 일치하는 IP 주소 및 호스트 이름이 없으면 검색이 완료되고 인증이 실패합니다.
    - SSH 서버에 대한 항목이 신뢰할 수 있는 서버 목록에 없으면 프로세스가 실패합니다.

참고: 공장 기본 컨피그레이션을 사용하는 기본 스위치의 자동 컨피그레이션을 지원하기 위해 SSH 서버 인증은 기본적으로 비활성화되어 있습니다.

1단계. 웹 기반 유틸리티에 로그인하고 Security(보안) > TCP/UDP Services(TCP/UDP 서비스)를 선택합니다.

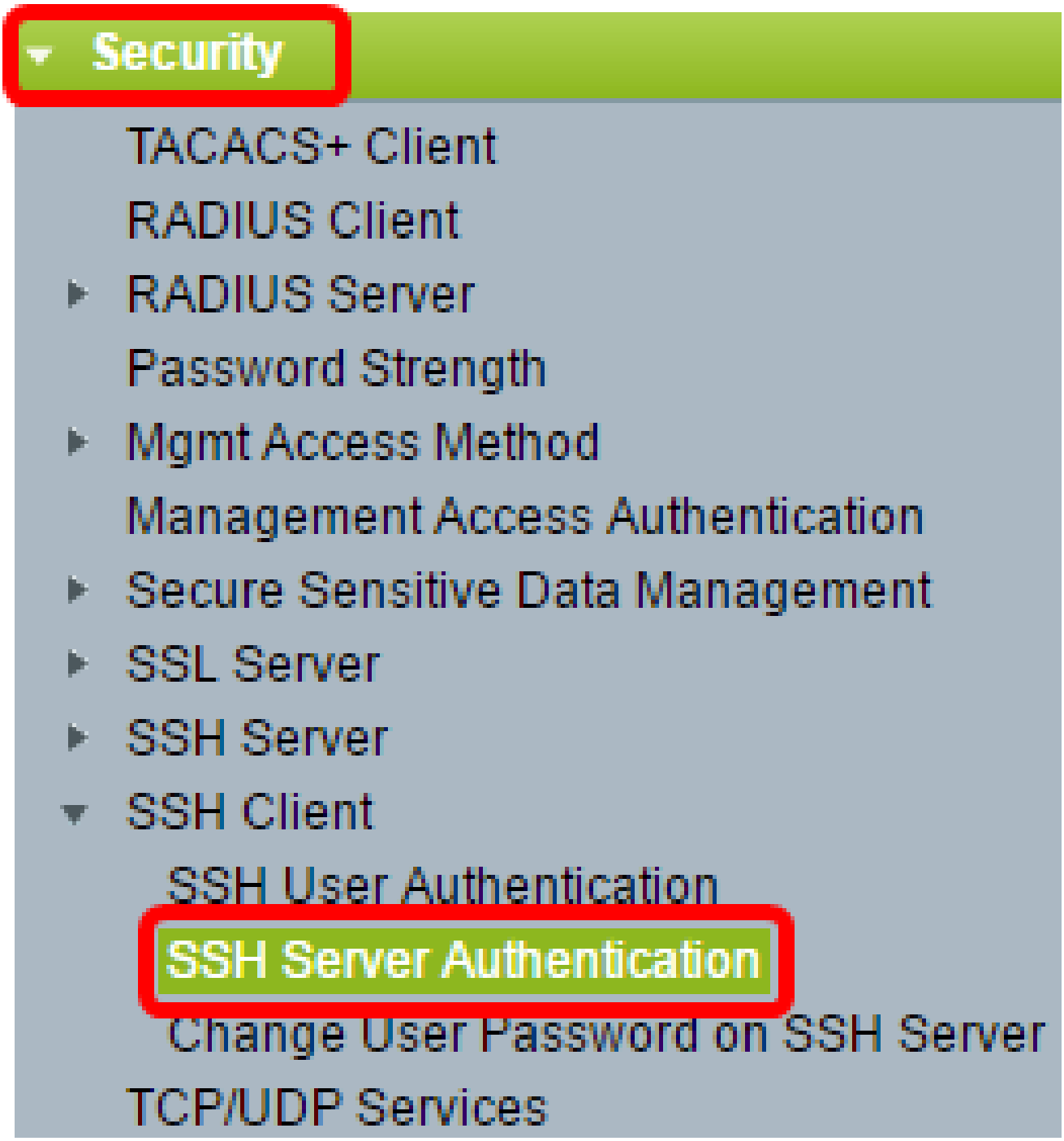


2단계. SSH를 통해 스위치 명령 프롬프트에 대한 액세스를 활성화하려면 SSH Service 확인란을 선택합니다.

3단계. SSH 서비스를 활성화하려면 Apply를 클릭합니다.

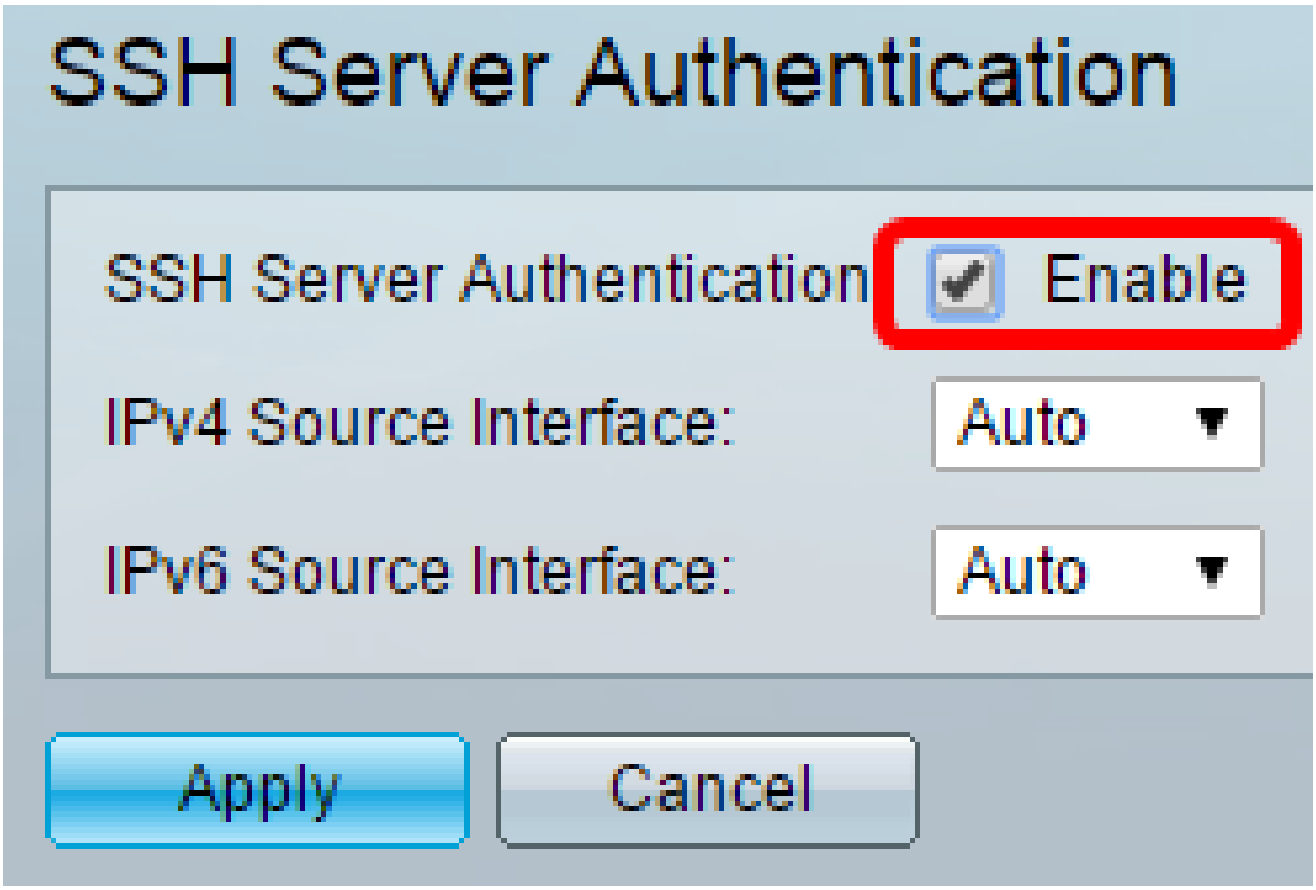
SSH 서버 인증 설정 구성

1단계. 웹 기반 유틸리티에 로그인하고 Security(보안) > SSH Client(SSH 클라이언트) > SSH Server Authentication(SSH 서버 인증)을 선택합니다.

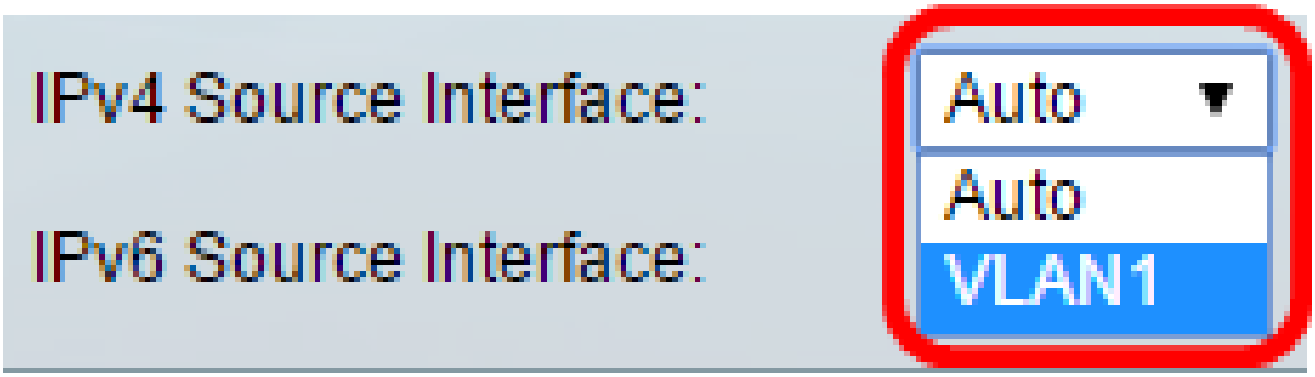


참고: Sx350, SG300X 또는 Sx500X가 있는 경우 Display Mode(표시 모드) 드롭다운 목록에서 Advanced(고급)를 선택하여 Advanced(고급) 모드로 전환합니다.

2단계. SSH 서버 인증을 활성화하려면 Enable SSH Server Authentication 확인란을 선택합니다.

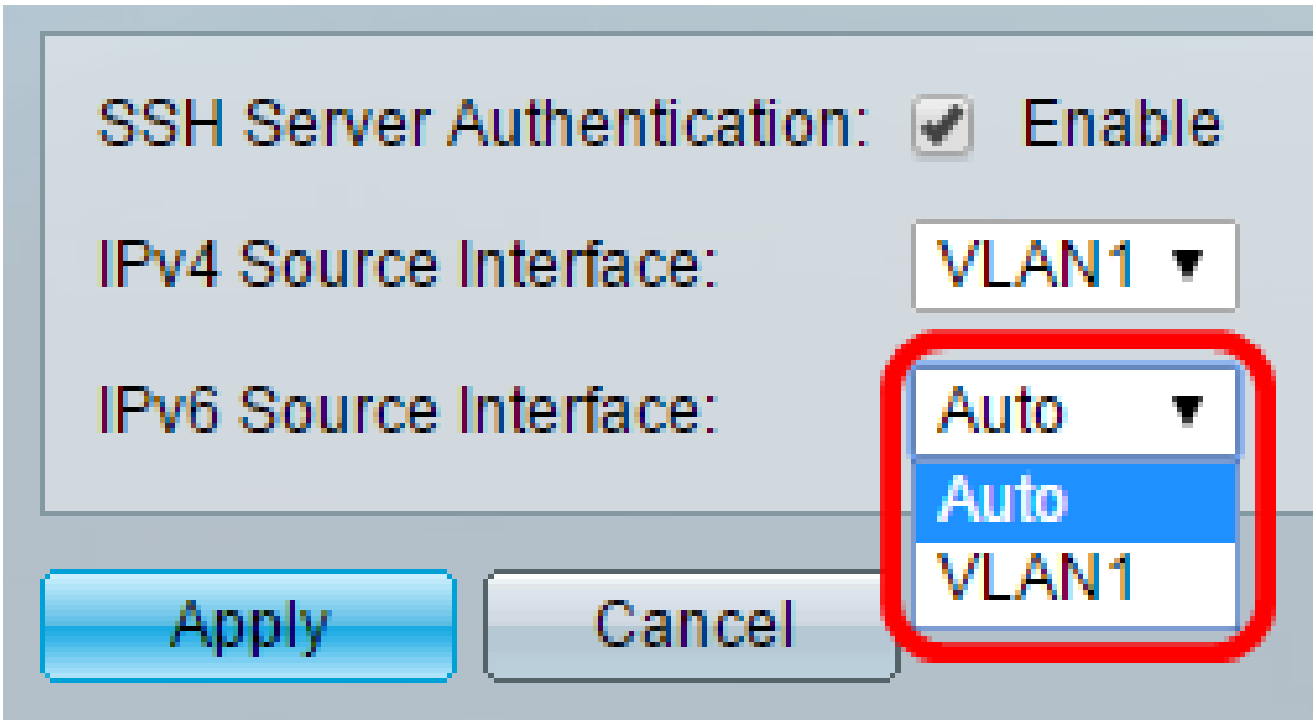


3단계(선택 사항) IPv4 Source Interface(IPv4 소스 인터페이스) 드롭다운 목록에서 IPv4 SSH 서버와의 통신에 사용되는 메시지의 소스 IPv4 주소로 IPv4 주소를 사용할 소스 인터페이스를 선택합니다.



참고: Auto 옵션을 선택하면 시스템은 발신 인터페이스에 정의된 IP 주소에서 소스 IP 주소를 가져옵니다. 이 예에서는 VLAN1이 선택됩니다.

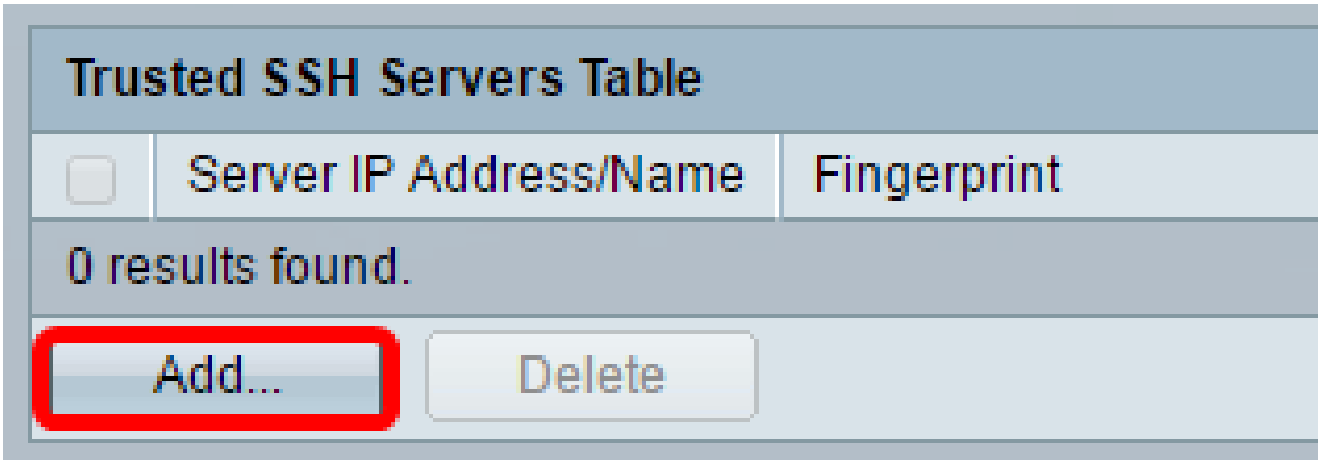
4단계(선택 사항) IPv6 Source Interface(IPv6 소스 인터페이스) 드롭다운 목록에서 IPv6 SSH 서버와의 통신에 사용되는 메시지의 소스 IPv6 주소로 IPv6 주소가 사용될 소스 인터페이스를 선택합니다.



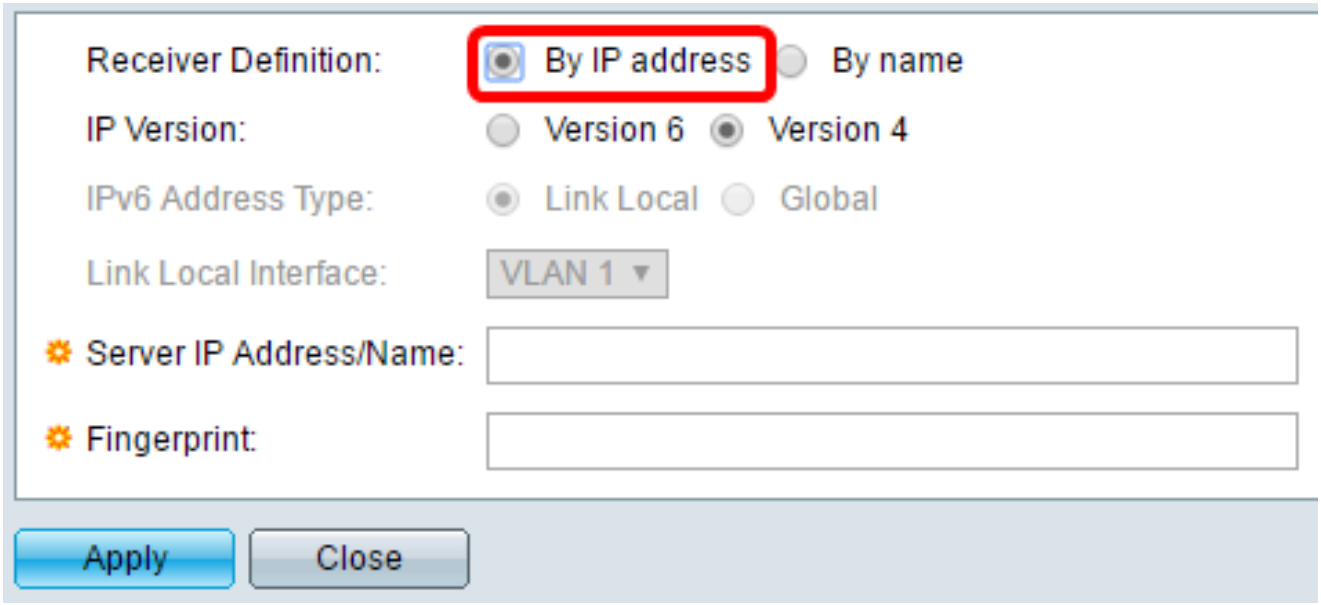
참고: 이 예제에서는 [자동] 옵션을 선택합니다. 시스템은 발신 인터페이스에 정의된 IP 주소에서 소스 IP 주소를 가져옵니다.

5단계. 적용을 클릭합니다.

6단계. 신뢰할 수 있는 서버를 추가하려면 Trusted SSH Servers(신뢰할 수 있는 SSH 서버) 테이블에서 Add(추가)를 클릭합니다.



7단계. Receiver Definition 영역에서 사용 가능한 방법 중 하나를 클릭하여 SSH 서버를 정의합니다.

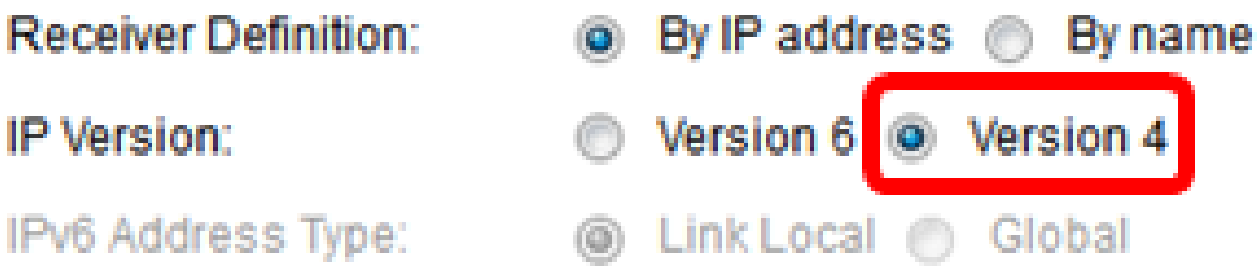


옵션은 다음과 같습니다.

- IP 주소별 — 이 옵션을 사용하면 IP 주소로 SSH 서버를 정의할 수 있습니다.
- 이름별 —이 옵션을 사용하면 정규화된 도메인 이름으로 SSH 서버를 정의할 수 있습니다.

참고: 이 예에서는 By IP address(IP 주소 기준)가 선택됩니다. [이름 기준]을 선택한 경우 11단계로 건너뜁니다.

8단계. 6단계에서 By IP address(IP 주소별)를 선택한 경우 IP Version(IP 버전) 필드에서 SSH 서버의 IP 버전을 클릭합니다(선택 사항).

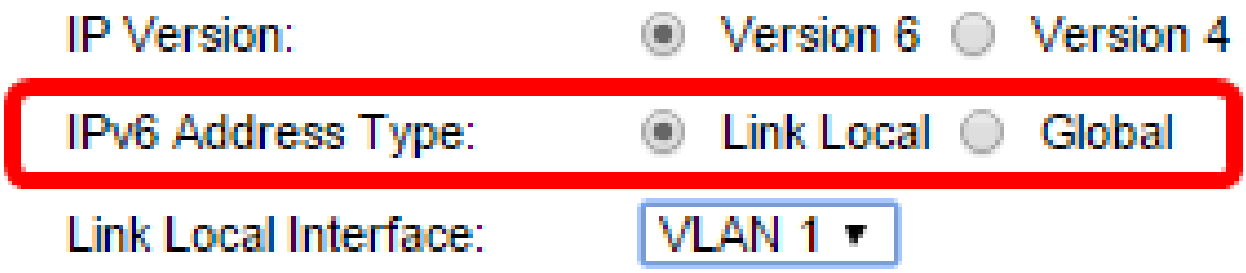


사용 가능한 옵션은 다음과 같습니다.

- 버전 6 — 이 옵션을 사용하여 IPv6 주소를 입력할 수 있습니다.
- 버전 4 — 이 옵션을 사용하여 IPv4 주소를 입력할 수 있습니다.

참고: 이 예에서는 버전 4가 선택됩니다. IPv6 라디오 버튼은 스위치에 IPv6 주소가 구성된 경우에만 사용할 수 있습니다.

9단계(선택 사항) 7단계에서 IP 주소 버전으로 버전 6을 선택한 경우 IPv6 Address Type(IPv6 주소 유형)에서 IPv6 주소의 유형을 클릭합니다.

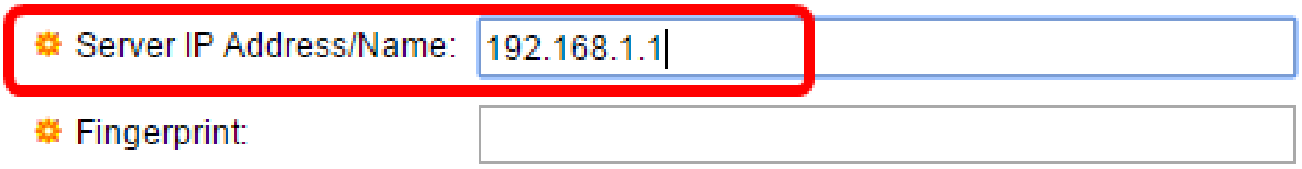


사용 가능한 옵션은 다음과 같습니다.

- Link Local — IPv6 주소는 단일 네트워크 링크에서 호스트를 고유하게 식별합니다. 링크 로컬 주소의 접두사는 FE80이며, 라우팅할 수 없으며, 로컬 네트워크에서만 통신에 사용할 수 있습니다. 링크 로컬 주소는 하나만 지원됩니다. 인터페이스에 링크 로컬 주소가 있는 경우 이 항목은 컨피그레이션의 주소를 대체합니다. 이 옵션은 기본적으로 선택되어 있습니다.
- 전역 — IPv6 주소는 다른 네트워크에서 볼 수 있고 연결할 수 있는 전역 유니캐스트입니다.

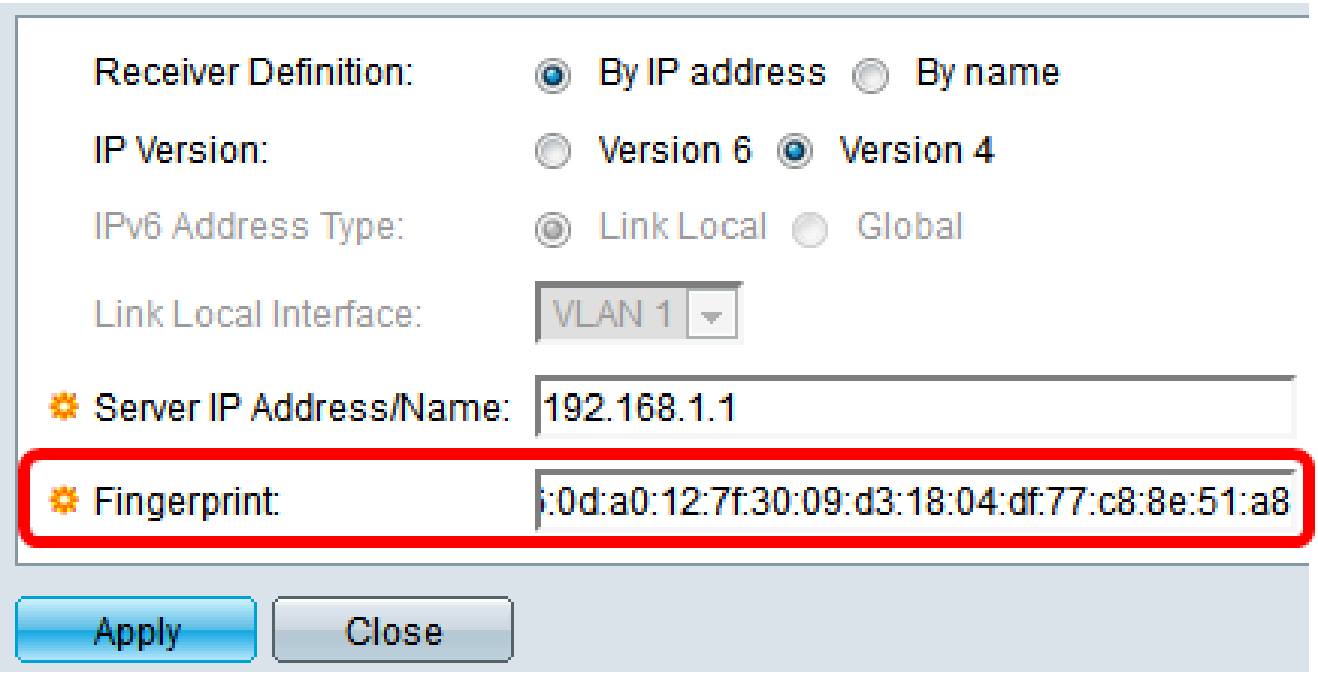
10단계. (선택 사항) 9단계에서 IPv6 주소 유형으로 Link Local을 선택한 경우 Link Local Interface 드롭다운 목록에서 적절한 인터페이스를 선택합니다.

11단계. Server IP Address/Name(서버 IP 주소/이름) 필드에 SSH 서버의 IP 주소 또는 도메인 이름을 입력합니다.



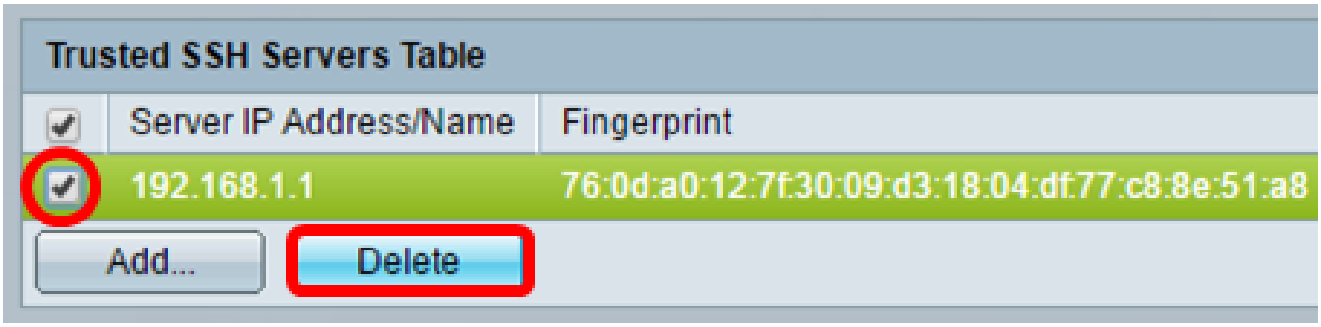
참고: 이 예에서는 IP 주소를 입력합니다.

12단계. Fingerprint 필드에 SSH 서버의 핑거프린트를 입력합니다. 핑거프린트는 인증에 사용되는 암호화된 키입니다. 이 경우 핑거프린트는 SSH 서버의 유효성을 인증하는 데 사용됩니다. 서버 IP 주소/이름과 핑거프린트가 일치하면 SSH 서버가 인증됩니다.

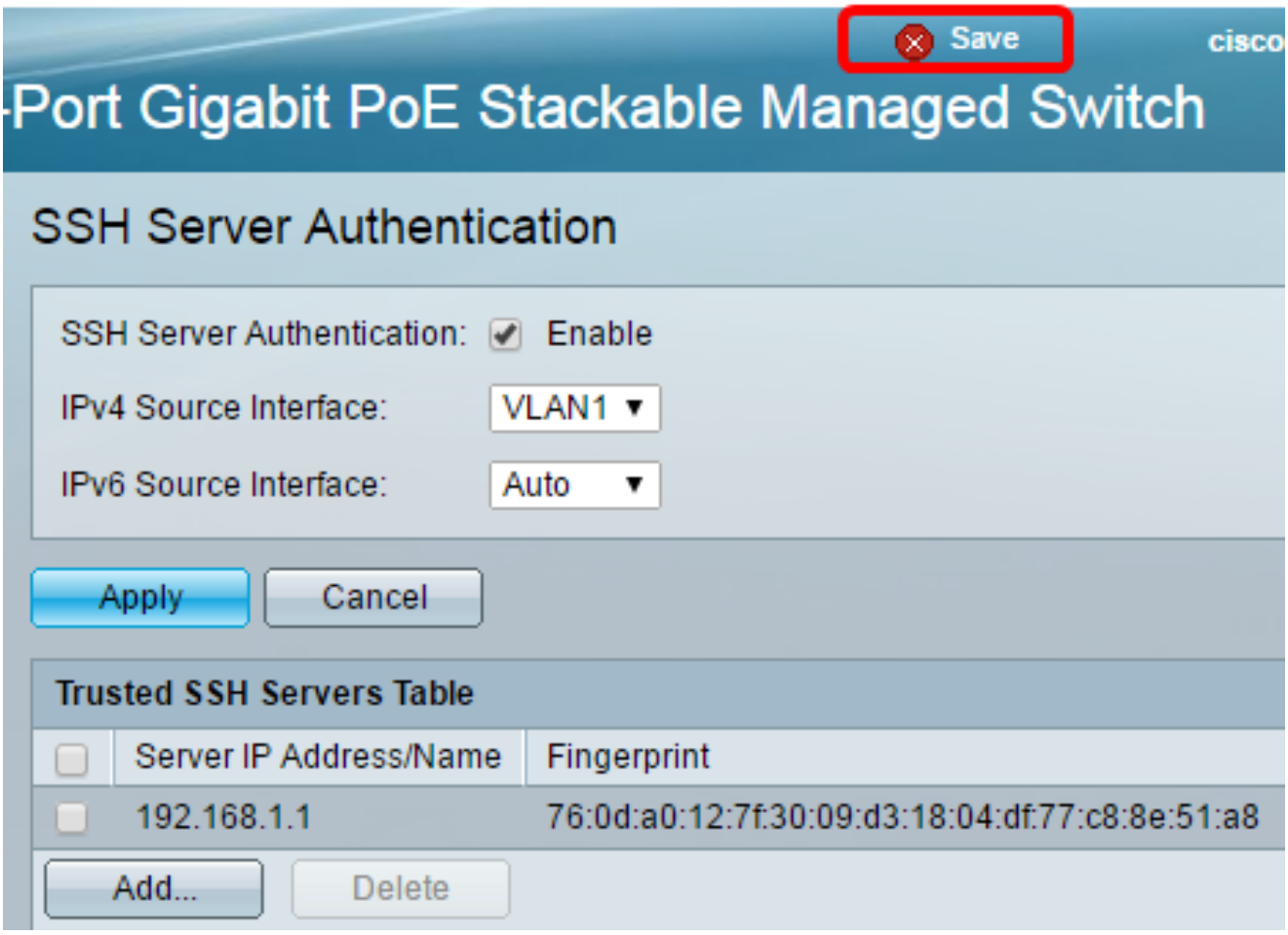


13단계. Apply(적용)를 클릭하여 컨피그레이션을 저장합니다.

14단계(선택 사항) SSH 서버를 삭제하려면 삭제할 서버의 확인란을 선택한 다음 Delete를 클릭합니다.



15단계. (선택 사항) 페이지 상단에서 Save(저장) 버튼을 클릭하여 변경 사항을 시작 구성 파일에 저장합니다.



이제 관리되는 스위치에 SSH 서버 인증 설정을 구성해야 합니다.

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.