Catalyst 1200 및 1300 스위치의 중간 인증서 및 인증서 체인

목표

이 문서의 목적은 펌웨어 4.1.3.36의 Catalyst 1200 및 1300 스위치의 중간 인증서 기능 및 인증서 체인과 이를 구성하는 단계를 살펴보는 것입니다.

적용 가능한 디바이스 | 소프트웨어 버전

- Catalyst 1200 스위치 | 4.1.3.36
- Catalyst 1300 스위치 | 4.1.3.36

소개

인증서는 네트워크에서 보안 액세스를 제공하는 데 사용됩니다. 인증서는 외부 CA(Certificate Authority)에 의해 자체 서명되거나 디지털 서명될 수 있습니다. 인증서 체인의 구성 요소는 다음과 같습니다.

- 루트 CA 인증서: 루트 CA 또는 CA 인증서는 인증서 체인의 계층 구조 상단에 있으며 자체 서명됩니다. 궁극적인 신뢰 앵커이며 중간 인증서의 진위 여부를 확인하는 데 사용됩니다.
- 중간 인증서: 중간 인증서는 다른 중간 CA 또는 루트 CA인 상위 레벨 CA에서 발급됩니다. 경우에 따라 인증서 체인을 형성하는 중간 인증서가 여러 개 있을 수 있습니다. 일반적으로 중간 CA는 서버 인증서 서명을 담당합니다.
- 서버 인증서: 이 인증서는 웹 사이트와 같은 특정 서버에 대해 발급됩니다. 서버의 공개 키가 포함되어 있으며 CA에서 서명합니다. CA는 루트 또는 중간 CA일 수 있습니다.

스위치(HTTPS 서버)와 브라우저(HTTPS 클라이언트) 간의 SSL/TLS 핸드셰이크 중에 스위치는 서명된 인증서를 제공합니다. 신뢰할 수 있는 저장소에 CA 인증서가 있는 브라우저는 CA의 공개 키를 사용하여 서버 인증서의 서명을 확인합니다. 이 프로세스는 서버 ID의 신뢰성을 설정합니다. 검증이 완료되면 서버와 브라우저는 암호화 매개변수를 교환하여 이들 간에 전송되는 데이터의 암호화를 활성화함으로써 HTTPS를 통한 데이터 전송을 위해 안전하고 인증된 연결을 보장합니다.

서버 인증서는 루트 CA 인증서로 직접 서명할 수 있지만 중간 인증서를 사용하면 서명 프로세스를 개선하는 계층 구조가 도입됩니다. 중간 인증서는 서버 인증서와 루트 CA 간의 중개인 역할을 하며, 키 보안 침해 격리를 통한 보안 강화, 인증서 관리의 유연성, 서명 권한 위임 등의 이점을 제공합니다. 이러한 계층적 접근 방식은 확장성을 개선하고, 인증서 갱신 프로세스를 용이하게 하며, 철회를 보다 세부적으로 제어할 수 있도록 합니다. 기본적으로 중간 인증서를 사용하면 향상된 보안, 유연성 및 간소화된 인증서 관리를 통해 서명 프로세스를 강화할 수 있습니다.

Catalyst 1200 및 1300 스위치의 펌웨어 4.1.3.36에서 중간 인증서를 가져오고 설치된 서버 인증서의 인증서 체인을 볼 수 있습니다. Catalyst 스위치는 중간 인증서 및 HTTPS 서버 인증서 체인과 관련된 다음 기능을 지원합니다.

- 하나 이상의 중간 인증서 설치
- HTTPS 클라이언트와의 TLS 핸드셰이크에 중간 인증서 포함
- 중간 인증서 표시
- 디바이스의 HTTPS 서버 인증서의 인증서 체인 표시

더 많은 것을 알아보려면 계속 읽으세요!

목차

- 중간 인증서 가져오기
- 인증서 체인
- 인증서 체인 예

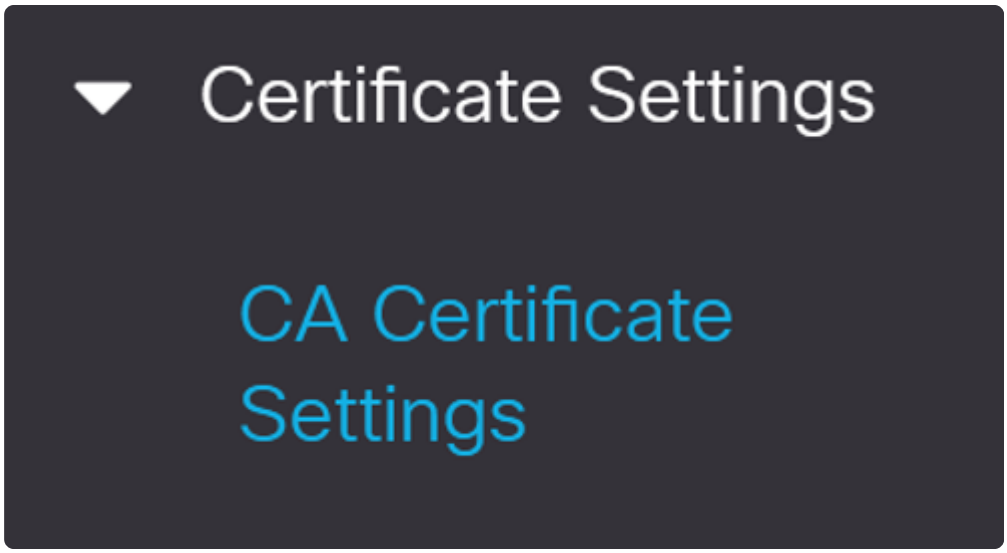
중간 인증서 가져오기

Catalyst 1200 및 1300 스위치의 펌웨어 버전 4.1.3.36에는 스위치의 웹 사용자 인터페이스를 사용하여 중간 인증서를 가져오는 옵션이 있습니다.

> **Note:**
> CA를 기반으로 인증서 공급업체는 루트 인증서와 중간 인증서를 번들로 제공하여 서버 인증서를 지원합니다.

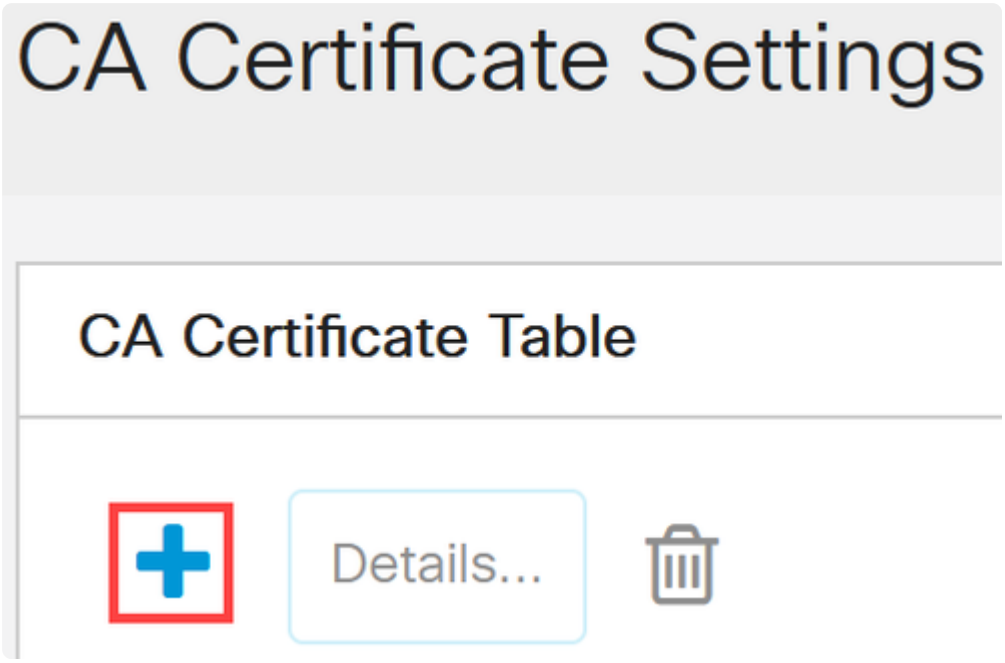
1단계

Advanced(고급) 보기 아래의 탐색 창에서 Security(보안) > Certificate Settings(인증서 설정) > CA Certificate Settings(CA 인증서 설정)로 이동합니다.



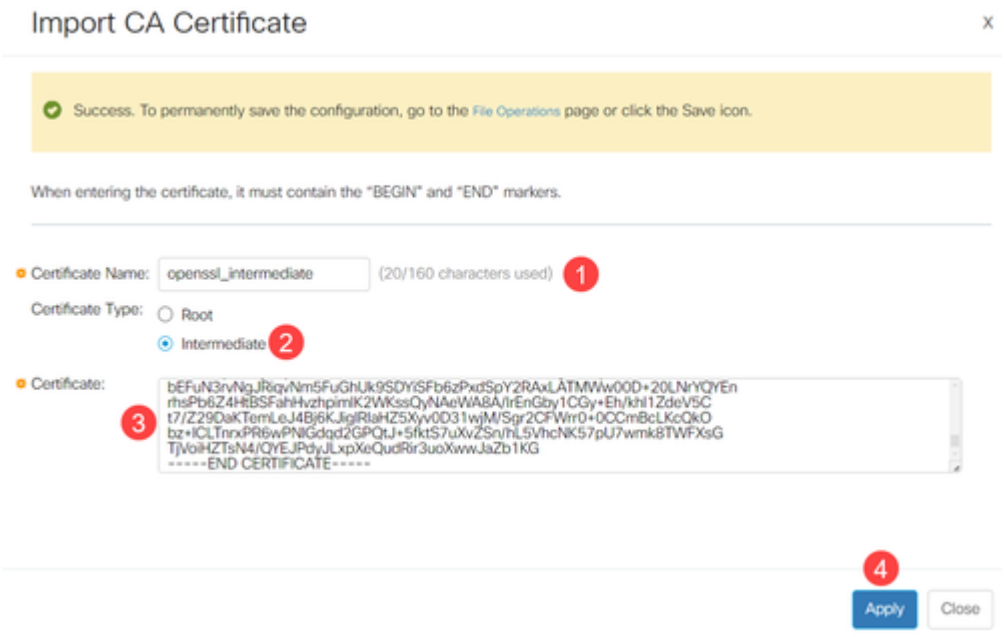
2단계

인증서를 가져오려면 더하기 아이콘을 클릭합니다.



3단계

Certificate Name(인증서 이름)을 입력하고 인증서 유형으로 Intermediate(중간)를 선택한 다음 제공된 상자에 인증서를 붙여넣고 Apply(적용)를 클릭합니다.



화면 상단에 성공 알림이 나타납니다.

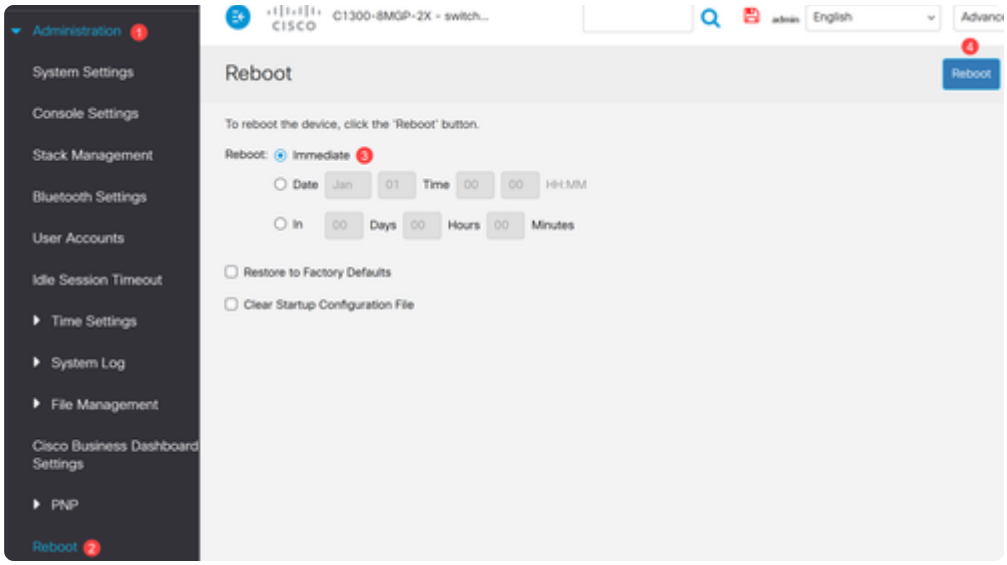
> **Note:**
> 인증서 유형이 설치 중인 인증서와 일치하지 않으면 오류 메시지가 표시됩니다.

4단계

화면 상단에 있는 저장 아이콘을 클릭합니다.

5단계

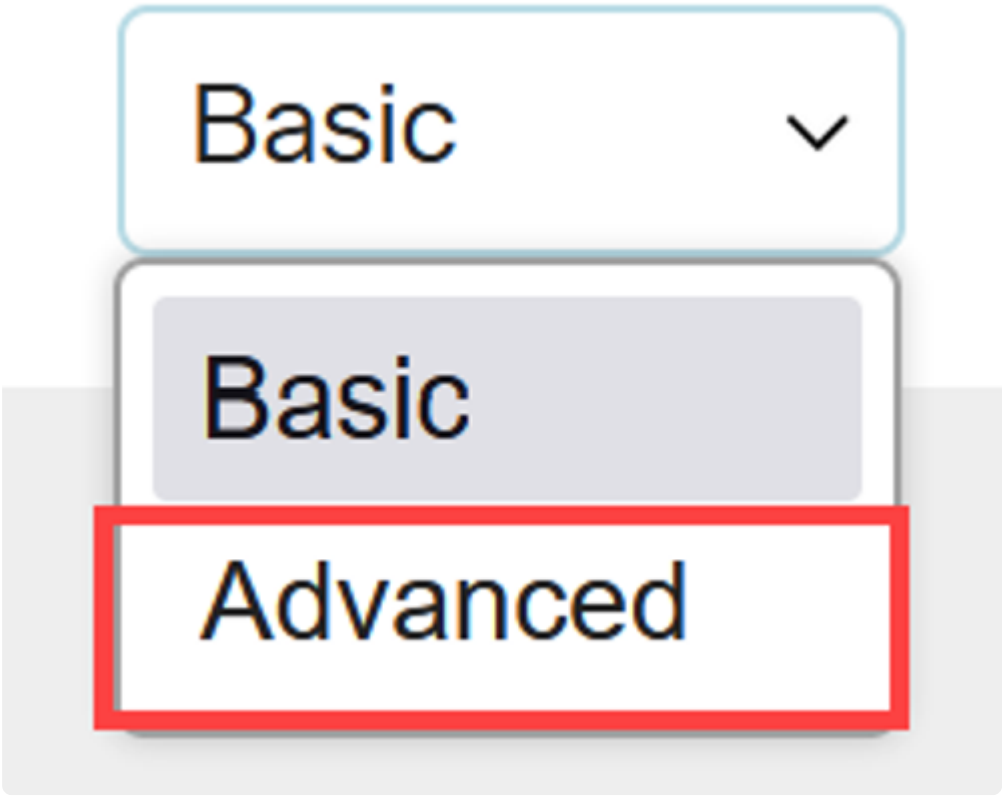
모든 변경 사항을 적용하려면 스위치를 재부팅합니다. 재부팅하려면 Administration(관리) > Reboot(재부팅) 메뉴로 이동하고 Immediate reboot(즉시 재부팅) 옵션이 선택되어 있는지 확인합니다. Reboot(재부팅) 버튼을 클릭합니다.



인증서 체인

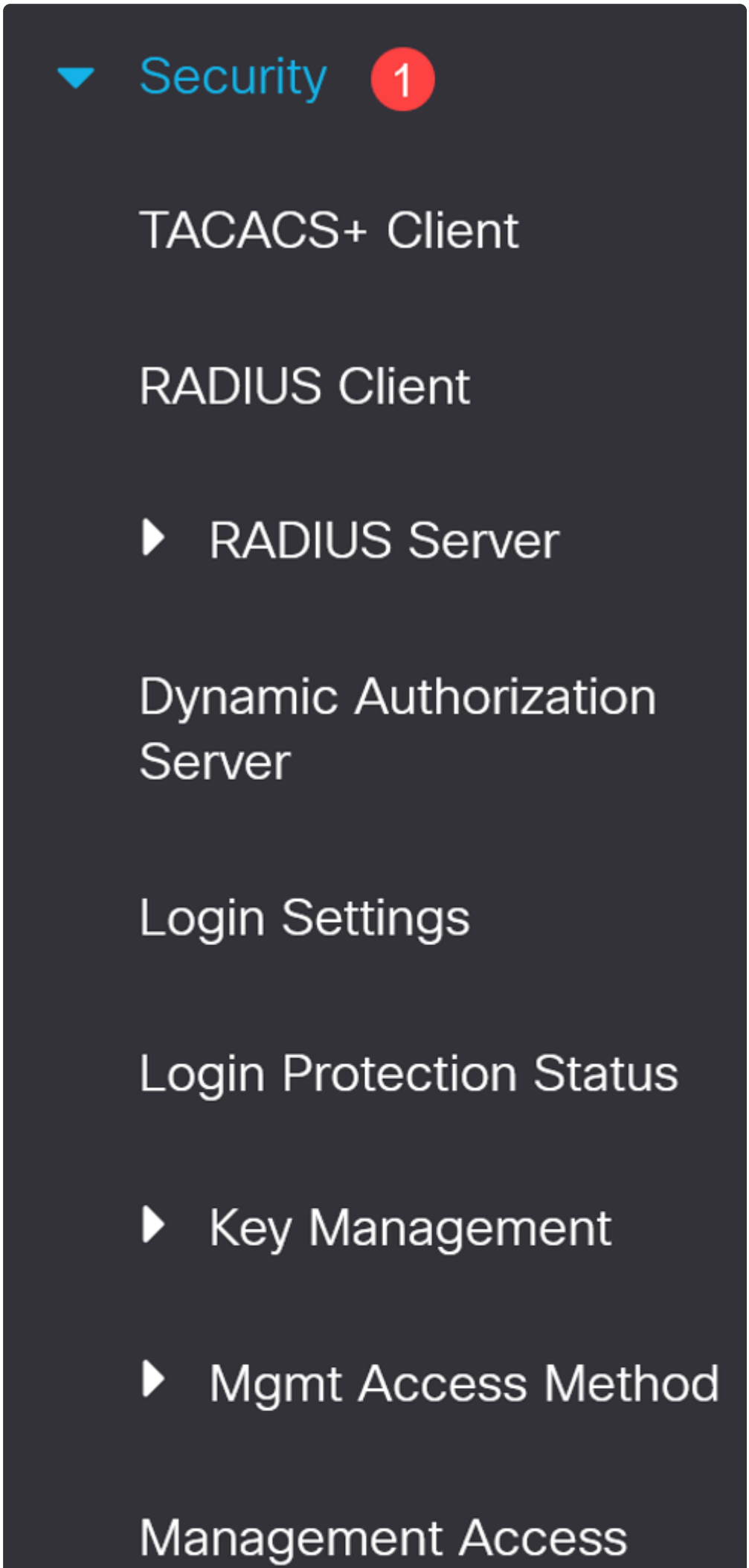
1단계

Catalyst 1300 스위치에 로그인하고 사용자 인터페이스 오른쪽 상단 모서리에 있는 드롭다운 메뉴에서 Advanced(고급) 보기로 전환합니다.



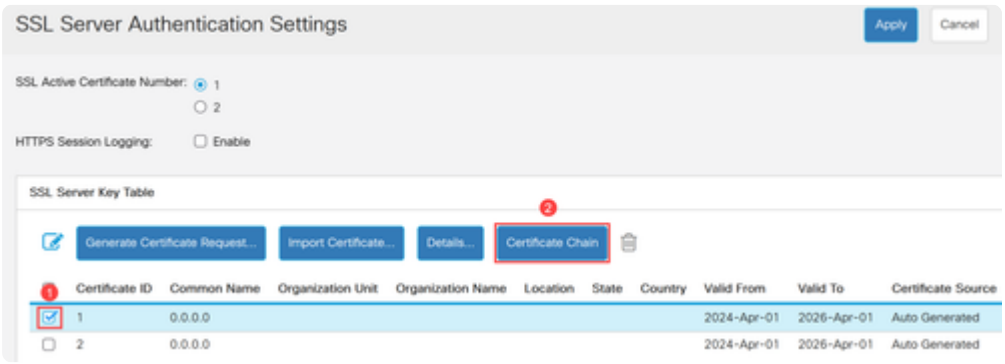
2단계

탐색 창에서 Security(보안) > SSL Server(SSL 서버) > SSL Server Authentication Settings(SSL 서버 인증 설정)로 이동합니다.

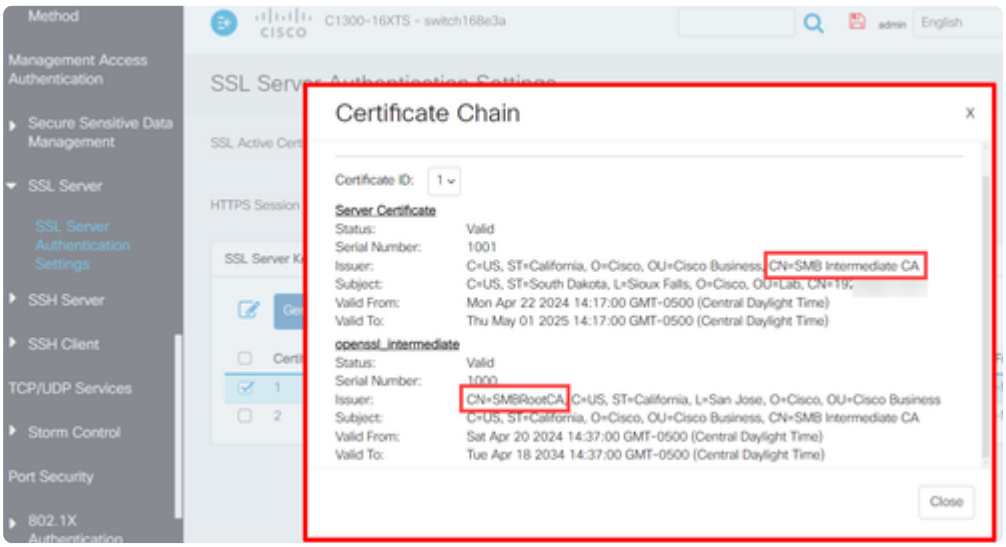

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Dynamic Authorization Server
Login Settings
Login Protection Status
Key Management
Mgmt Access Method
Management Access

3단계

테이블에서 인증서를 선택한 다음 Certificate Chain(인증서 체인) 버튼을 클릭합니다.

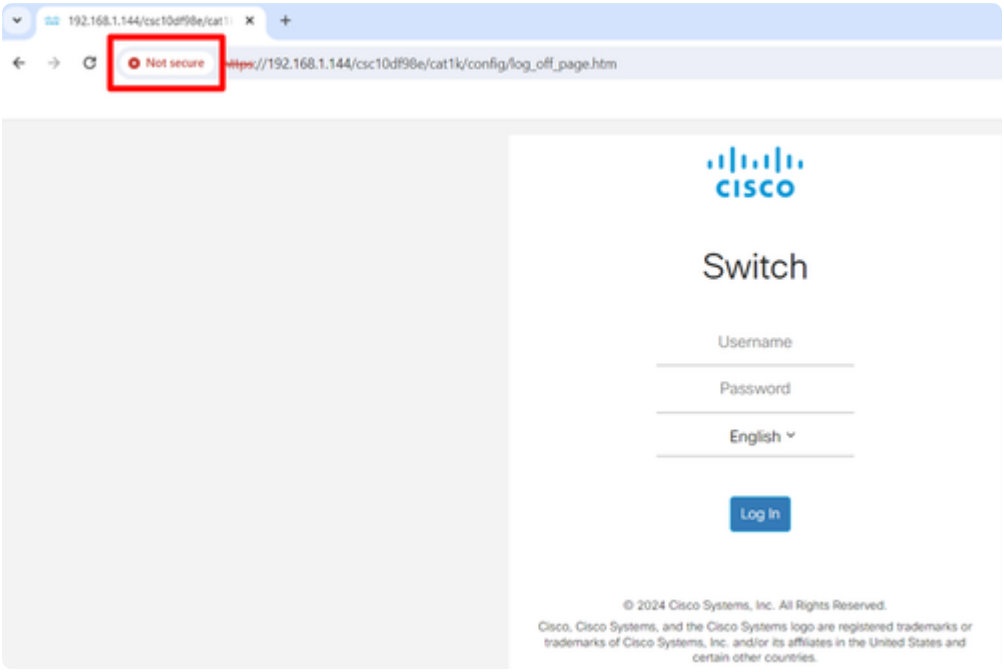


인증서 체인의 세부사항을 보여주는 팝업 창이 나타납니다. 이 예에서는 서버 인증서에 발급자의 CN(Common Name)으로 표시된 대로 "SMB Intermediate CA"라는 중간 CA가 서버 인증서에 서명했습니다. 중간 인증서의 발급자는 SMBRootCA입니다.

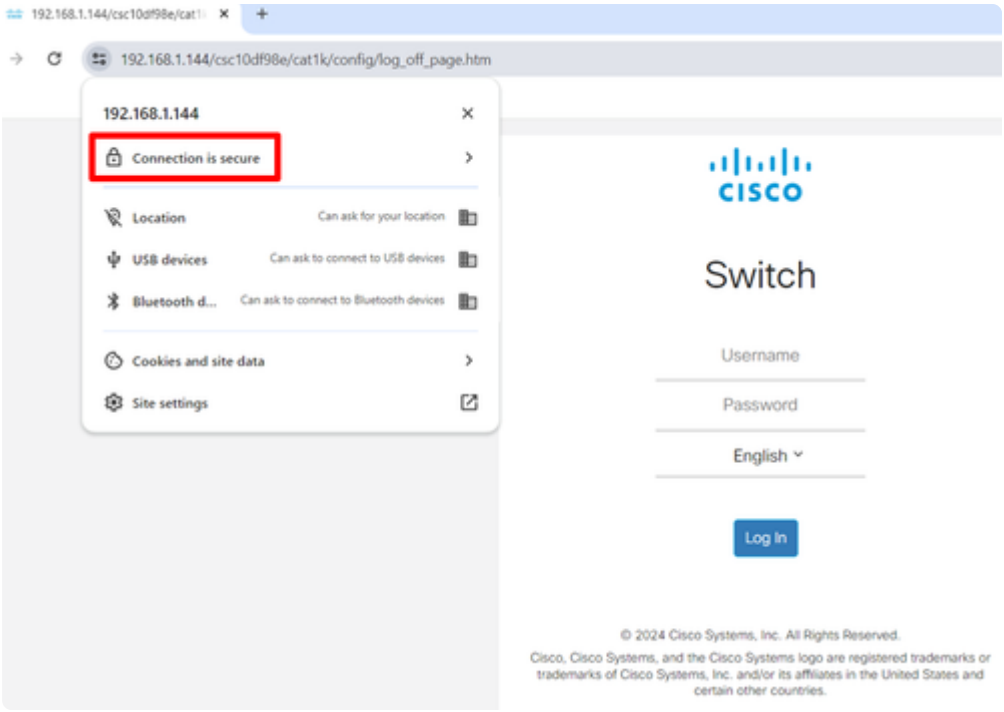


인증서 체인 예

스위치에서 기본적으로 자체 서명 인증서를 사용하는 경우 클라이언트 시스템, 이 경우 웹 브라우저에서 연결이 안전하지 않음을 알리는 메시지가 표시됩니다.



반면 루트 인증서, 중간 인증서 및 서버 인증서가 설치된 상태로 인증서 체인이 완료되면 연결이 안전하다고 브라우저에 표시됩니다.



결론

여기 있어요! 이제 중간 인증서를 업로드하고 Catalyst 1200 및 1300 스위치에서 인증서

체인을 확인하는 방법을 알 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.