200/300 Series 관리 스위치에 대한 관리 액세스 인증

목표

SSH, 콘솔, 텔넷, HTTP, HTTPS 등의 관리 액세스 모드에서는 사용자가 디바이스에 액세스할 수 있습니다. 보안을 강화하기 위해 사용자에게 인증이 필요할 수 있습니다. 200 및 300 Series Managed Switch는 로컬로 또는 TACACS+ 또는 RADIUS 서버에서 인증할 수 있습니다. 이 문서에서는 200 및 300 Series 관리 스위치에 인증 방법을 할당하는 방법에 대해 설명합니다.

적용 가능한 디바이스

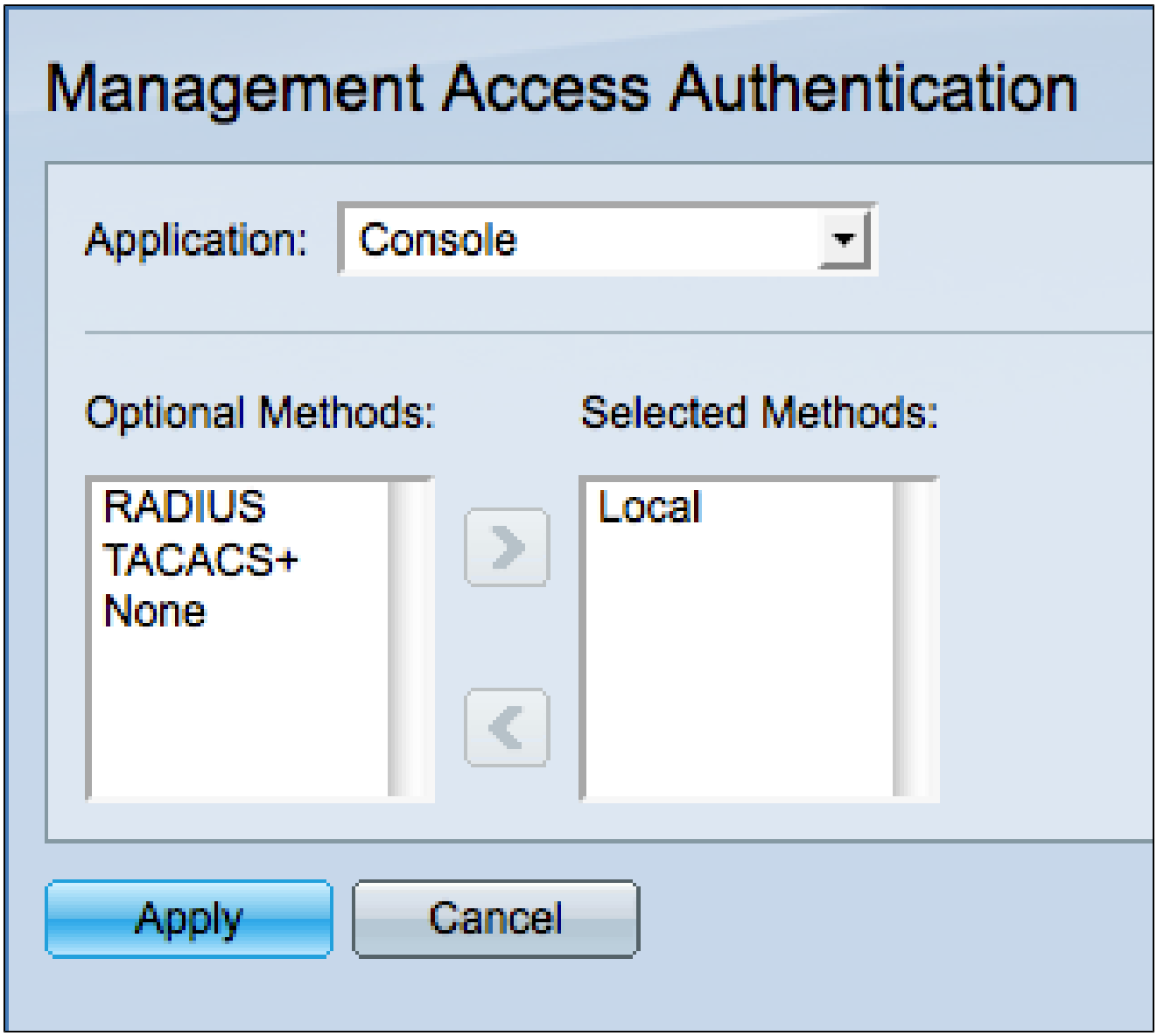
· SF/SG 200 및 SF/SG 300 Series Managed Switch

소프트웨어 버전

•1.3.0.62

관리 액세스 인증

1단계. 웹 컨피그레이션 유틸리티에 로그인하고 Security(보안) > Management Access Authentication(관리 액세스 인증)을 선택합니다. Management Access Authentication(관리 액세스 인증) 페이지가 열립니다.



2단계. Application(애플리케이션) 드롭다운 목록에서 인증을 할당할 애플리케이션의 유형을 선택합니다. 가능한 애플리케이션은 다음과 같습니다.

· Console — 콘솔 인터페이스로 스위치를 관리할 수 있습니다. 스위치의 IP 주소를 모르는 경우에도 스위치에 연결하고 일부 컨피그레이션을 수행할 수 있습니다.

· 텔넷 — TCP/IP 네트워크를 통해 스위치에 원격으로 연결할 수 있는 문자 기반 통신 프로토콜입니다. 텔넷은 암호화 부족으로 인해 권장되지 않습니다.

· SSH(Secure Telnet) — 텔넷 + 암호화와 동일한 기능을 수행합니다. 원격 연결에는 SSH를 사용하는 것이 좋습니다.

· HTTP — 스위치의 GUI(Graphical User Interface)에 액세스할 수 있는 프로토콜입니다. 이는 명령 프롬프트 기반인 텔넷 및 SSH와 대조됩니다.

· Secure HTTP(HTTPS) — 보안 통신을 추가하여 HTTP와 동일한 기능을 수행합니다.

3단계. Optional Methods 목록에서 인증 방법을 선택한 다음 > 버튼을 클릭하여 Selected Methods 목록으로 이동합니다. 각 방법은 각기 다른 보안 수준을 제공합니다.

참고: 인증 방법을 선택한 순서는 사용자 인증이 발생하는 순서입니다. RADIUS가 로컬 전에 선택된 경우 디바이스는 로컬 방법 전에 RADIUS 서버에 의해 사용자 인증을 시도합니다.

· RADIUS — RADIUS는 비밀번호만 암호화합니다. 인증은 RADIUS 서버에 있으며 구성된 RADIUS 서버가 필요합니다.

· TACACS+— TACACS+는 인증 과정에서 모든 데이터를 암호화합니다. 인증은 TACACS+ 서버에서 수행되며 구성된 TACACS+ 서버가 필요합니다.

· None(없음)— 스위치에 액세스하는 데 인증이 필요하지 않습니다.

· Local(로컬) - 스위치에 저장된 정보로 사용자 정보를 확인합니다.

4단계. Apply(적용)를 클릭하여 인증 설정을 저장하거나 Cancel(취소)을 클릭하여 변경 사항을 취소합니다.

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.