# Cisco Business 350 Series 스위치에 SSH(Secure Shell) 사용자 인증 설정 구성

## 목표

이 문서에서는 Cisco Business 350 Series 스위치에서 클라이언트 사용자 인증을 구성하는 방법에 대한 지침을 제공합니다.

### 소개

SSH(Secure Shell)는 특정 네트워크 디바이스에 대한 보안 원격 연결을 제공하는 프로토콜입니다 .이 연결은 암호화된다는 점을 제외하고 텔넷 연결과 유사한 기능을 제공합니다.관리자는 SSH를 사용하여 서드파티 프로그램을 사용하여 CLI(Command Line Interface)를 통해 스위치를 구성할 수 있습니다.

SSH를 통한 CLI 모드에서는 관리자가 보안 연결에서 고급 컨피그레이션을 실행할 수 있습니다 .SSH 연결은 네트워크 관리자가 네트워크 사이트에 물리적으로 존재하지 않는 경우 원격으로 네트워크 문제를 해결하는 데 유용합니다.이 스위치를 사용하면 관리자가 사용자를 인증하고 관리하여 SSH를 통해 네트워크에 연결할 수 있습니다.인증은 사용자가 특정 네트워크에 대한 SSH 연결을 설정하는 데 사용할 수 있는 공개 키를 통해 발생합니다.

SSH 클라이언트 기능은 디바이스 인증 및 암호화를 제공하기 위해 SSH 프로토콜을 통해 실행되는 애플리케이션입니다.SSH 서버를 실행하는 다른 디바이스에 안전하고 암호화된 연결을 설정할 수 있습니다.인증 및 암호화를 통해 SSH 클라이언트는 비보안 텔넷 연결을 통한 보안 통신을 허용합니다.

### 적용 가능한 디바이스 | 소프트웨어 버전

- CBS350(데이터 시트) | 3.0.0.69 (최신 다운로드)
- CBS350-2X (데이터 시트) | 3.0.0.69 (최신 다운로드)
- CBS350-4X (데이터 시트) | 3.0.0.69 (최신 다운로드)

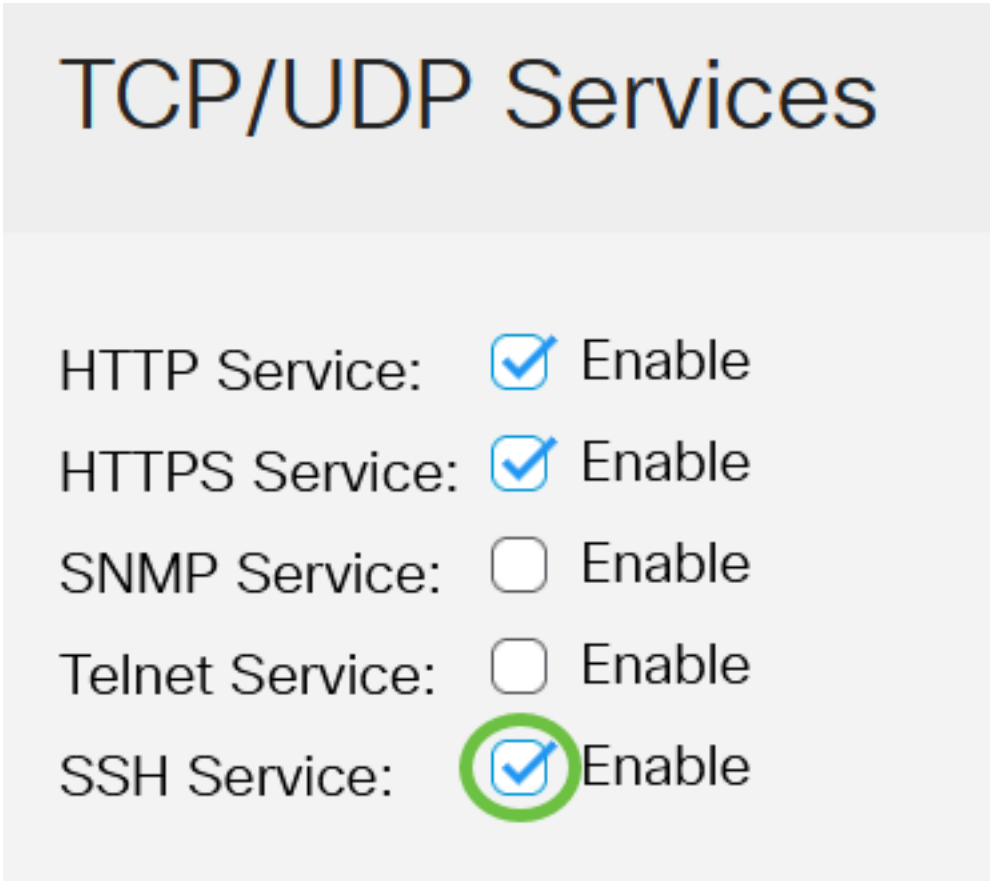
## SSH 클라이언트 사용자 인증 설정 구성

### SSH 서비스 사용

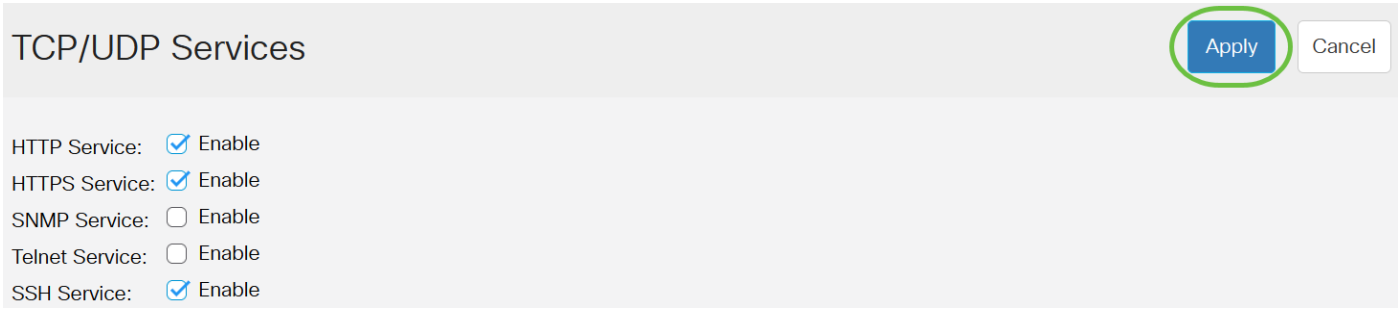
기본 디바이스(공장 기본 컨피그레이션이 있는 디바이스)의 자동 컨피그레이션을 지원하기 위해 SSH 서버 인증은 기본적으로 비활성화되어 있습니다.

1단계. 웹 기반 유틸리티에 로그인하고 **보안 > TCP/UDP Services**를 선택합니다.


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




3단계. SSH 서비스를 활성화하려면 Apply를 클릭합니다.

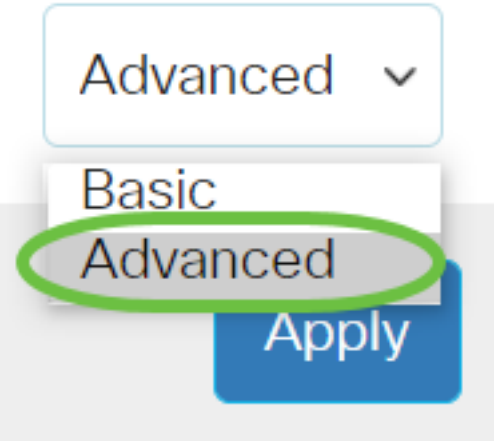



## SSH 사용자 인증 설정 구성

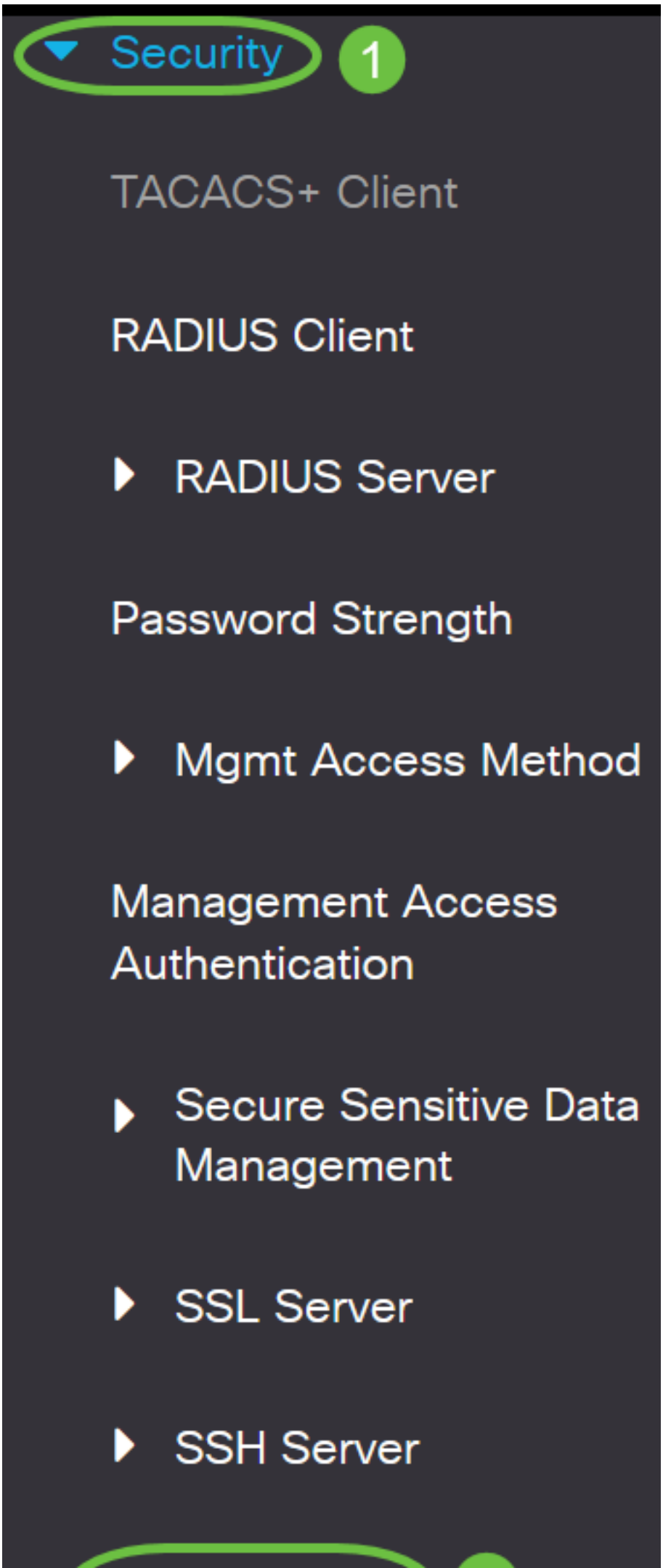
이 페이지에서는 SSH 사용자 인증 방법을 선택할 수 있습니다.비밀번호 방법을 선택한 경우 디바이스에서 사용자 이름과 비밀번호를 설정할 수 있습니다.공개 또는 개인 키 방법을 선택한 경우 Ron Rivest, Adi Shamir 및 Leonard Adleman(RSA) 또는 DSA(Digital Signature Algorithm) 키를 생성할 수도 있습니다.

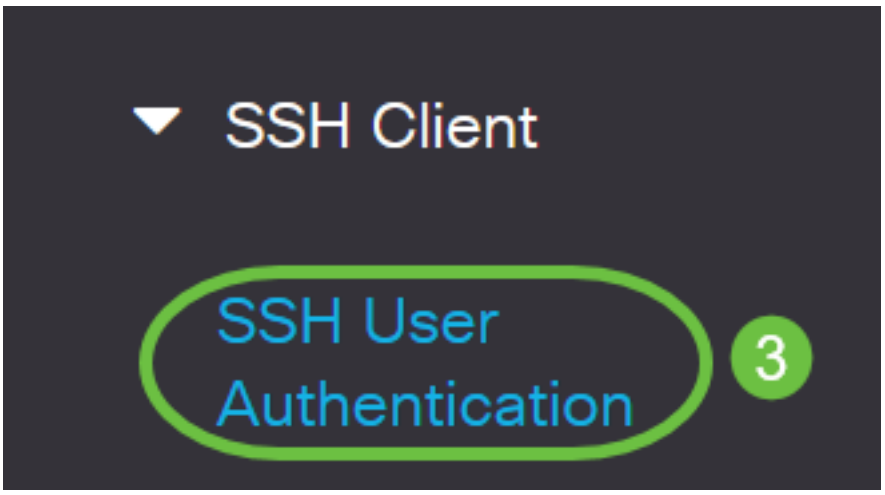
RSA 및 DSA 기본 키 쌍은 부팅 시 디바이스에 대해 생성됩니다.이러한 키 중 하나는 SSH 서버에서 다운로드 중인 데이터를 암호화하는 데 사용됩니다.RSA 키는 기본적으로 사용됩니다.사용자가 이러한 키 중 하나 또는 모두를 삭제하면 해당 키가 다시 생성됩니다.

1단계. 스위치의 웹 기반 유틸리티에 로그인한 다음 Display Mode 드롭다운 목록에서 Advanced를 선택합니다.

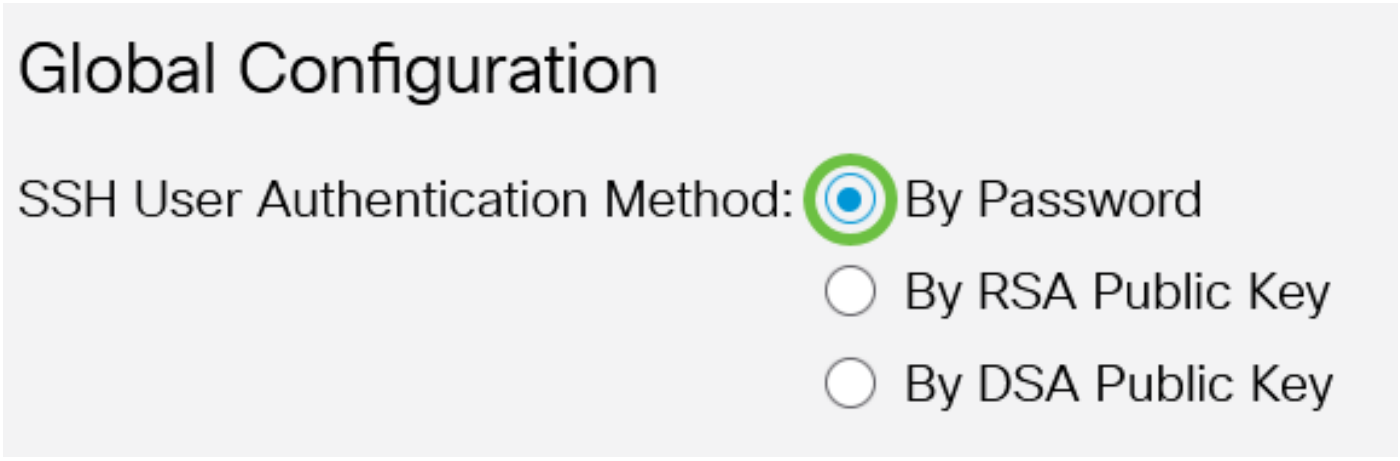



2단계. 메뉴에서 **Security > SSH Client > SSH User Authentication**을 선택합니다.


Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Password Strength
Mgmt Access Method
Management Access Authentication
Secure Sensitive Data Management
SSL Server
SSH Server




3단계. Global Configuration(전역 컨피그레이션)에서 원하는 SSH 사용자 인증 방법을 클릭합니다.




디바이스(SSH 클라이언트)가 SSH 서버에 대한 SSH 세션을 설정하려고 할 때 SSH 서버는 클라이언트 인증에 다음 방법 중 하나를 사용합니다.

- By Password(비밀번호별) - 이 옵션을 사용하여 사용자 인증을 위한 비밀번호를 구성할 수 있습니다.기본 설정이며 기본 비밀번호는 익명입니다.이 옵션을 선택한 경우 SSH 서버에 사용자 이름 및 비밀번호 자격 증명이 설정되었는지 확인합니다.
- RSA 공개 키별 - 이 옵션을 사용하면 사용자 인증에 RSA 공개 키를 사용할 수 있습니다.RSA 키는 큰 정수의 계화를 기반으로 하는 암호화 키입니다.이 키는 SSH 사용자 인증에 사용되는 가장 일반적인 키 유형입니다.
- DSA 공개 키별 - 이 옵션을 사용하면 사용자 인증에 DSA 공개 키를 사용할 수 있습니다.DSA 키는 ElGamal 개별 알고리즘을 기반으로 하는 암호화 키입니다.이 키는 인증 프로세스에 더 많은 시간이 필요하므로 SSH 사용자 인증에 일반적으로 사용되지 않습니다.

이 예에서는 [비밀번호별]이 선택됩니다.

4단계. Credentials(자격 증명) 영역의 Username(사용자 이름) 필드에 사용자 이름을 입력합니다.


이 예에서는 ciscosbuser1이 사용됩니다.

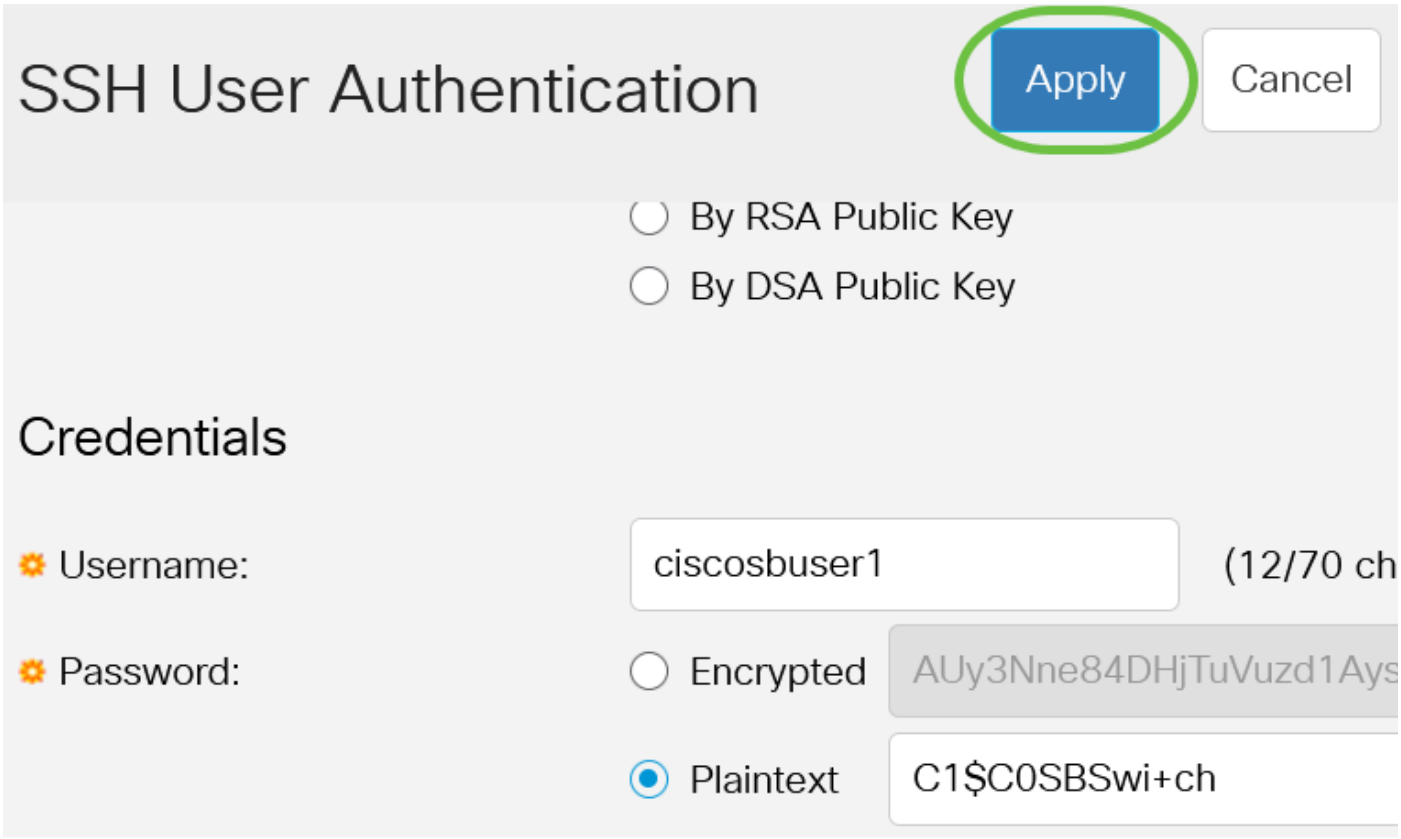
5단계. (선택 사항) 2단계에서 By Password(비밀번호별)를 선택한 경우 방법을 누른 다음 Encrypted(*암호화*) 또는 Plaintext(일반 텍스트) 필드에 비밀번호를 입력합니다.


옵션은 다음과 같습니다.

- Encrypted(암호화) - 이 옵션을 사용하면 비밀번호의 암호화된 버전을 입력할 수 있습니다.
- 일반 텍스트 - 이 옵션을 사용하면 일반 텍스트 비밀번호를 입력할 수 있습니다.

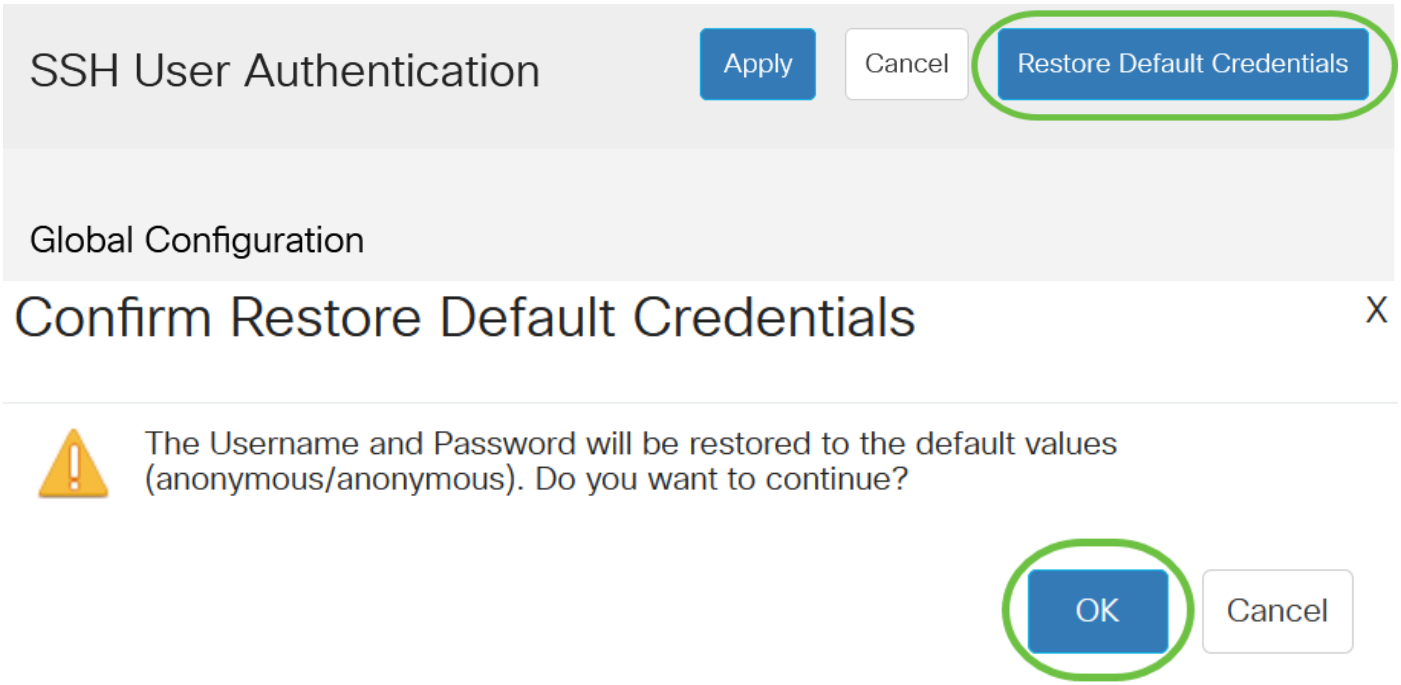
이 예에서는 일반 텍스트가 선택되고 일반 텍스트 비밀번호가 입력됩니다.

6단계. **Apply(적용)**를 클릭하여 인증 컨피그레이션을 저장합니다.



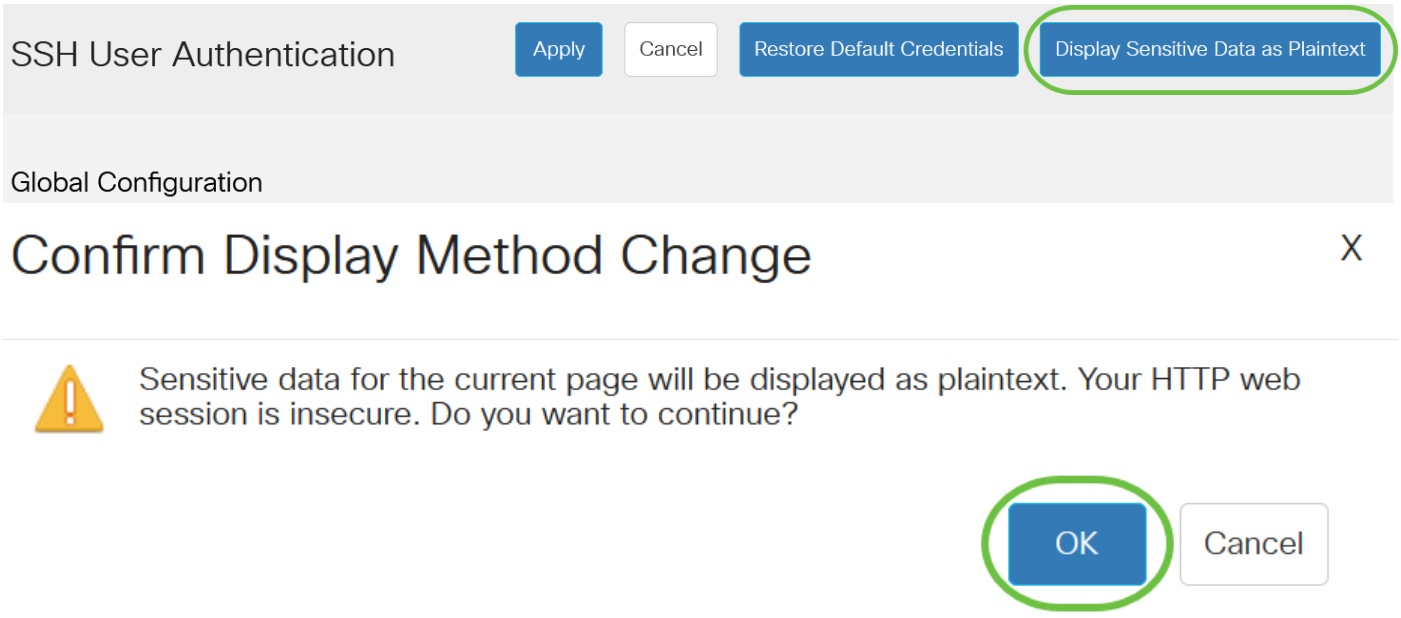

7단계. (선택 사항) Restore **Default Credentials(기본 자격 증명 복원)**를 클릭하여 기본 사용자 이름

과 암호를 복원한 다음 **OK(확인)**를 클릭하여 계속 진행합니다.



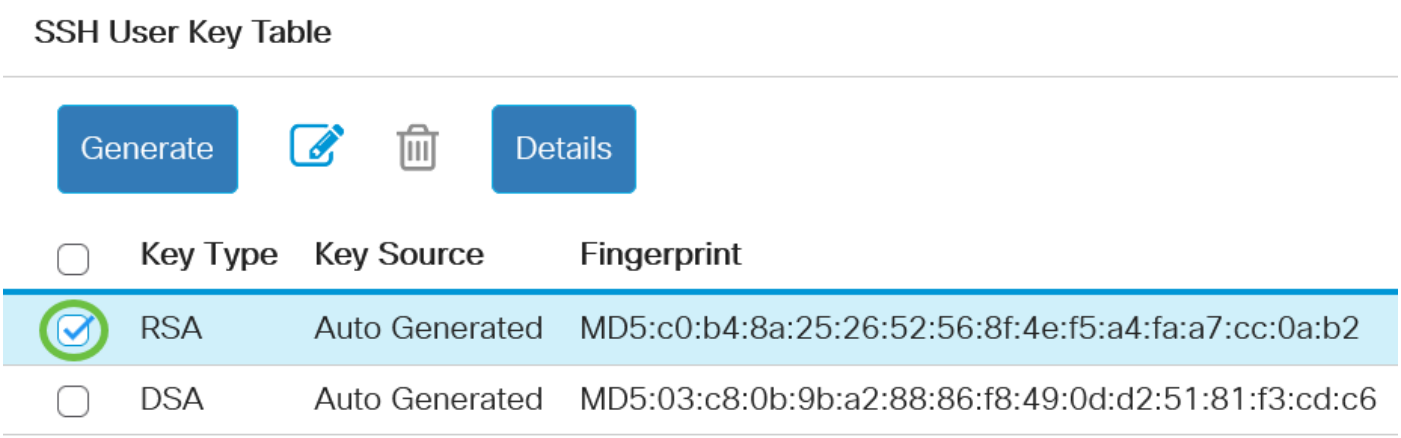

사용자 이름 및 비밀번호가 기본값으로 복원됩니다.익명/익명.

8단계. (선택 사항) **Display Sensitive Data as Plaintext**를 클릭하여 페이지의 민감한 데이터를 일반 텍스트 형식으로 표시한 다음 **OK**를 클릭하여 계속 진행합니다.



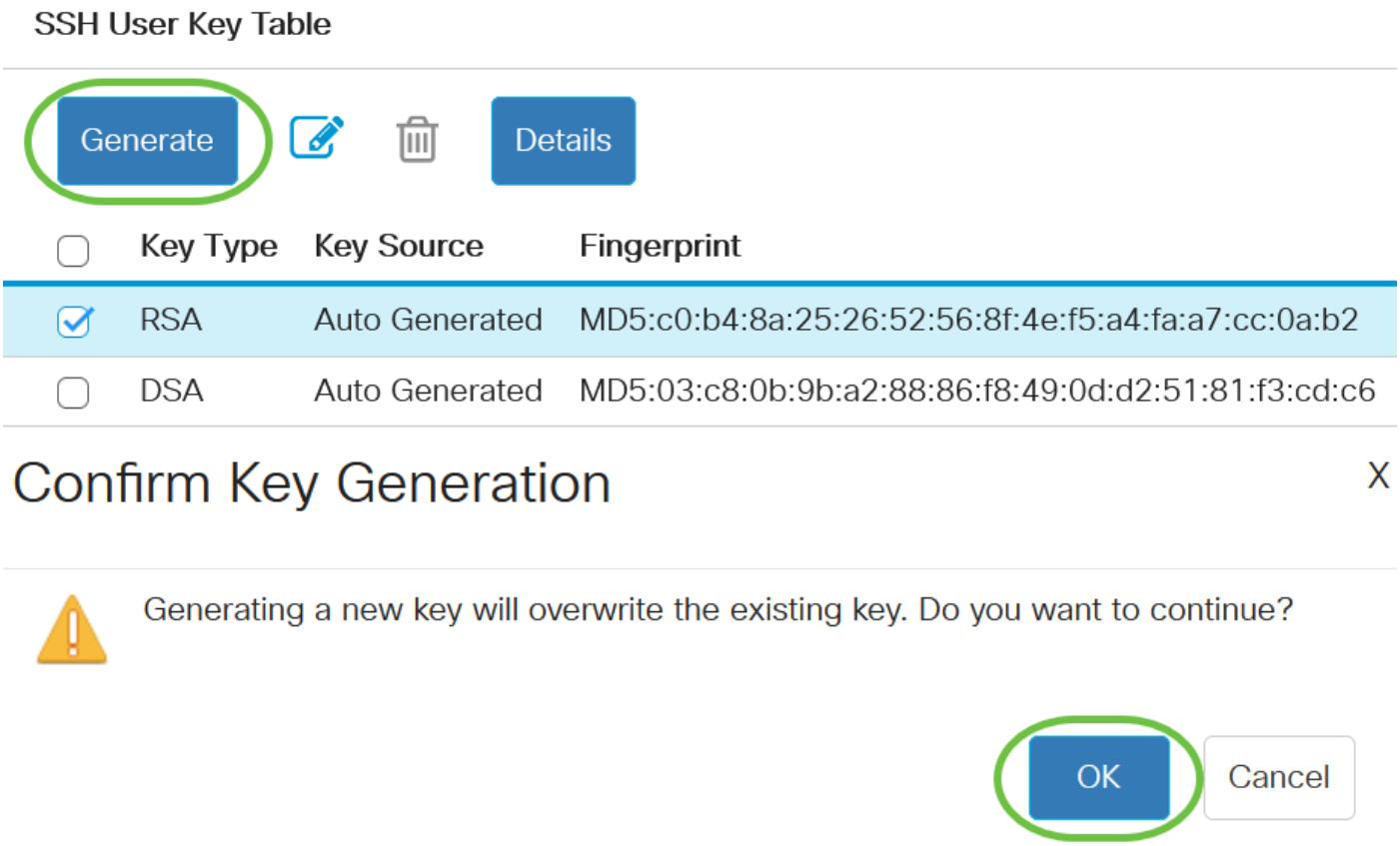

## SSH 사용자 키 테이블 구성

9단계. 관리할 키의 확인란을 선택합니다.

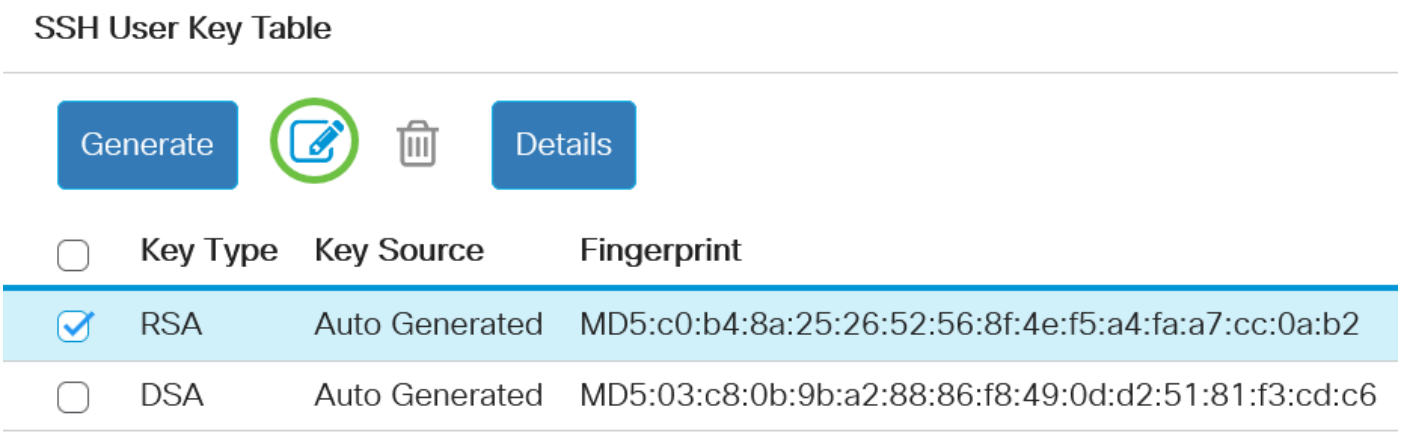



이 예에서는 RSA가 선택됩니다.

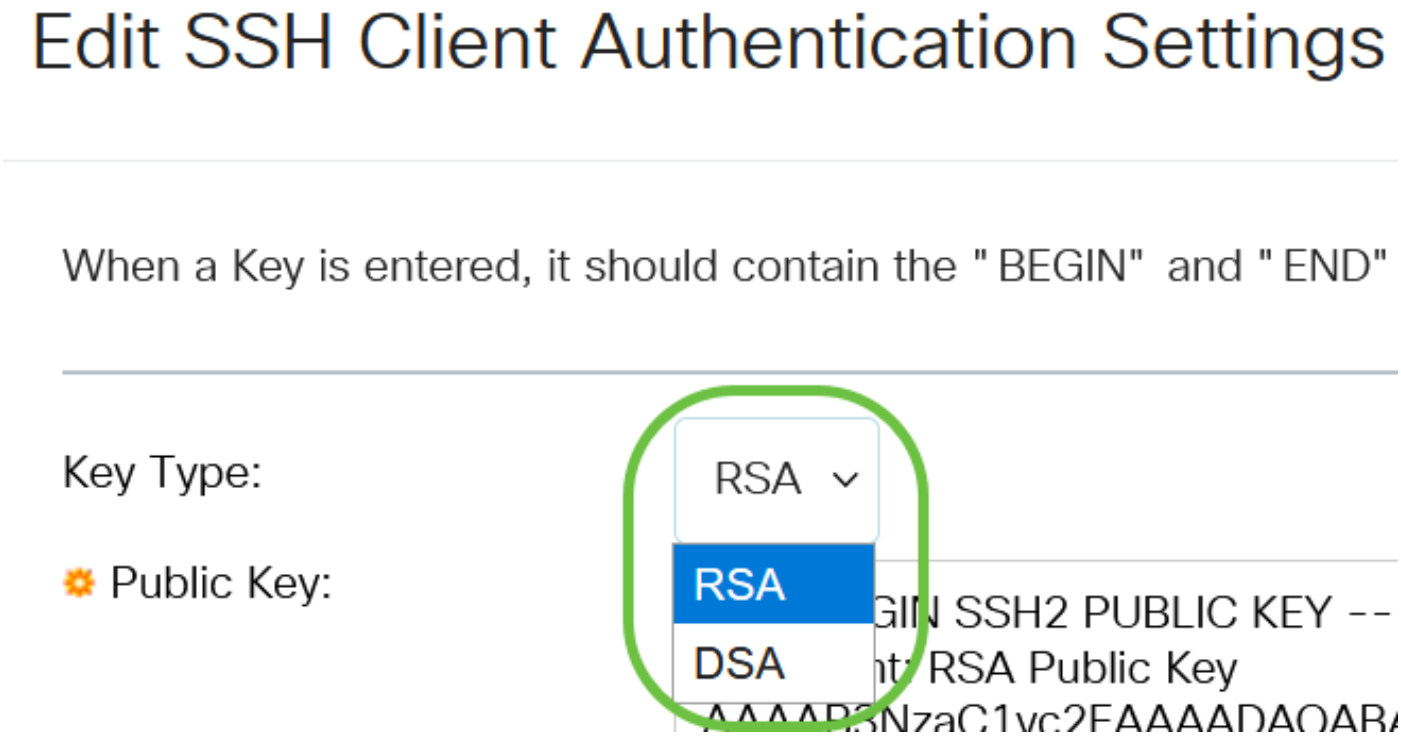
10단계. (선택 사항) **Generate**를 클릭하여 새 키를 생성합니다.새 키가 선택된 키를 재정의한 다음 **OK(확인)**를 클릭하여 진행합니다.




11단계(선택 사항) **Edit**를 클릭하여 현재 키를 편집합니다.

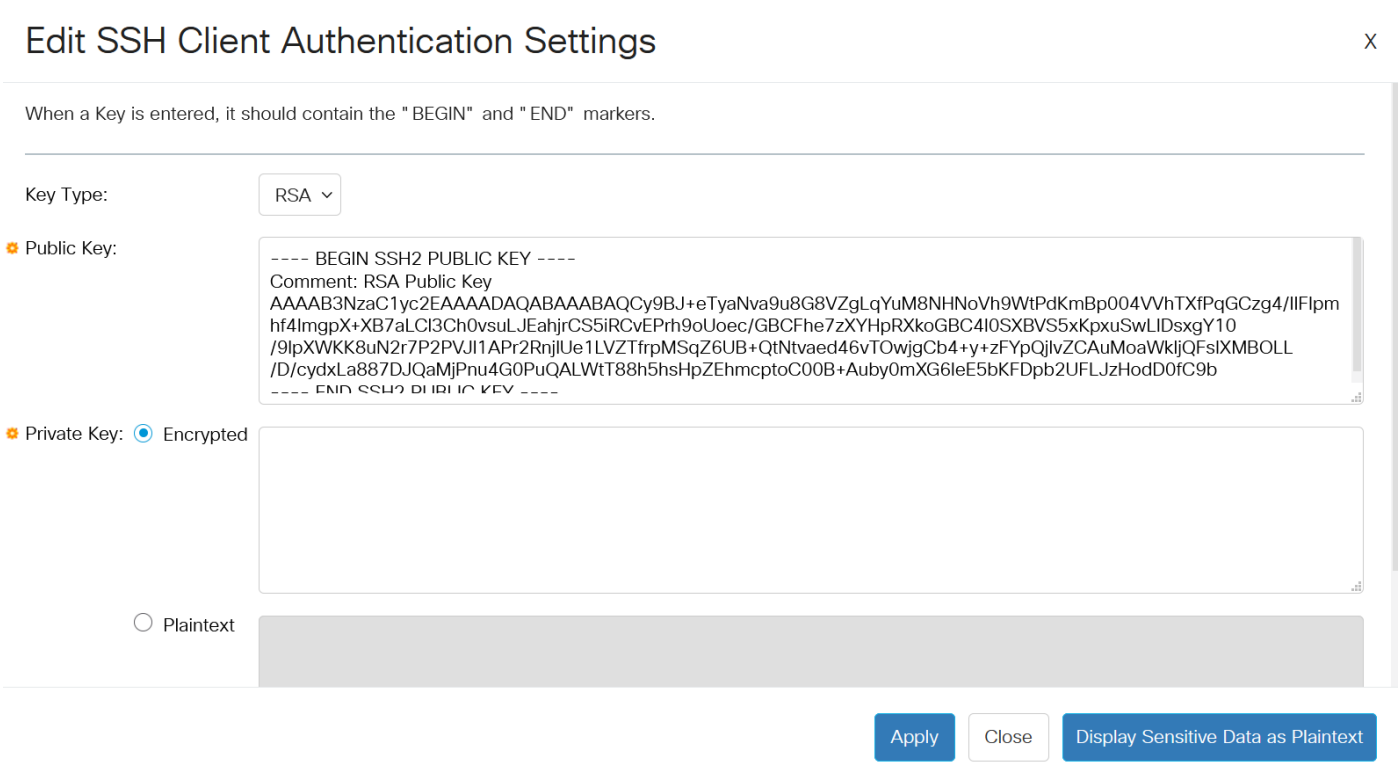



12단계(선택 사항) Key Type(키 유형) 드롭다운 목록에서 키 유형을 선택합니다.




이 예에서는 RSA가 선택됩니다.

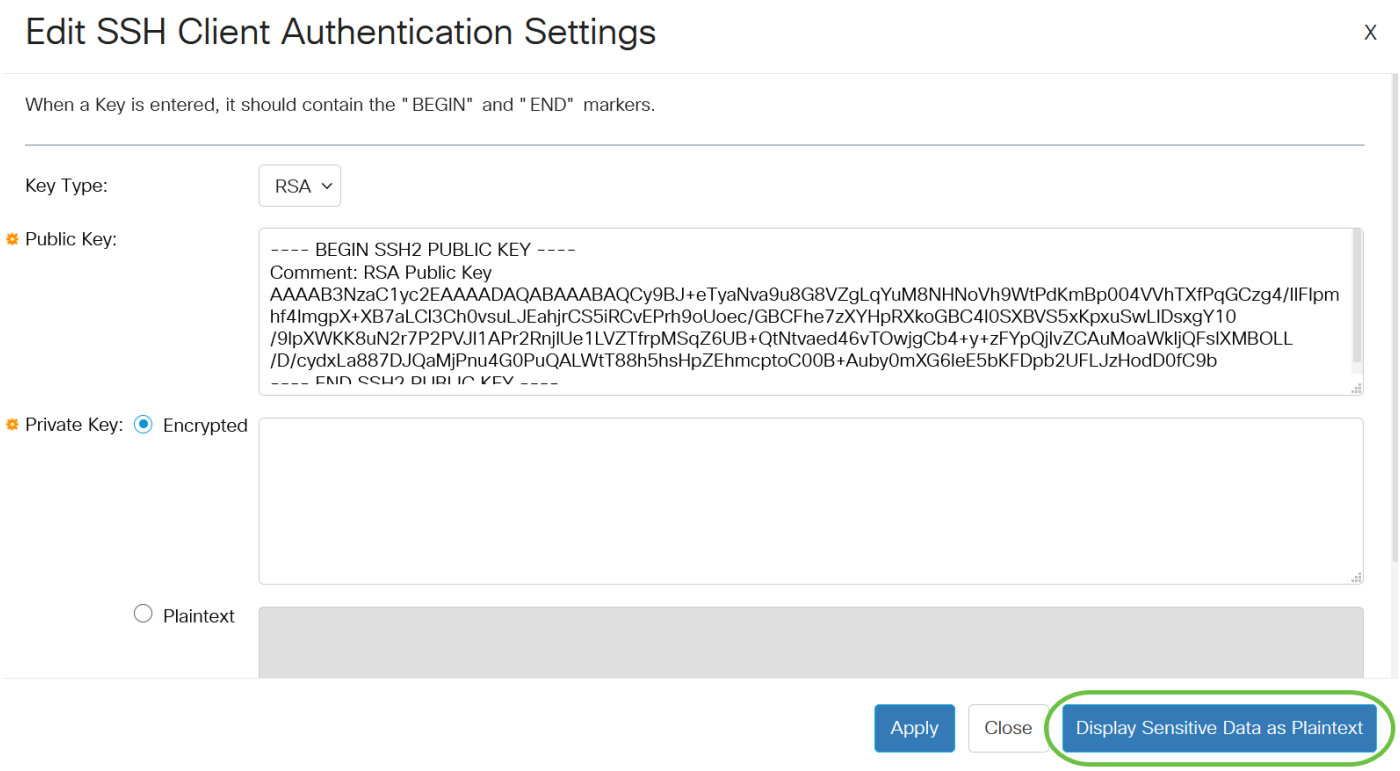
13단계. (선택 사항) *Public Key* 필드에 새 공개 키를 입력합니다.

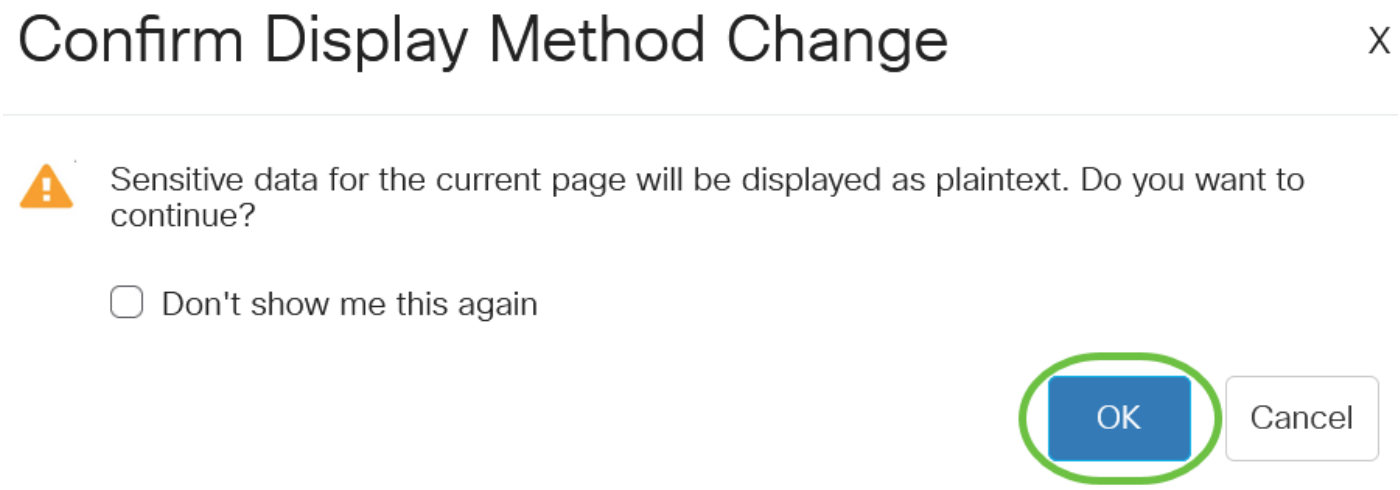



14단계. (선택 사항) *Private Key* 필드에 새 개인 키를 입력합니다.

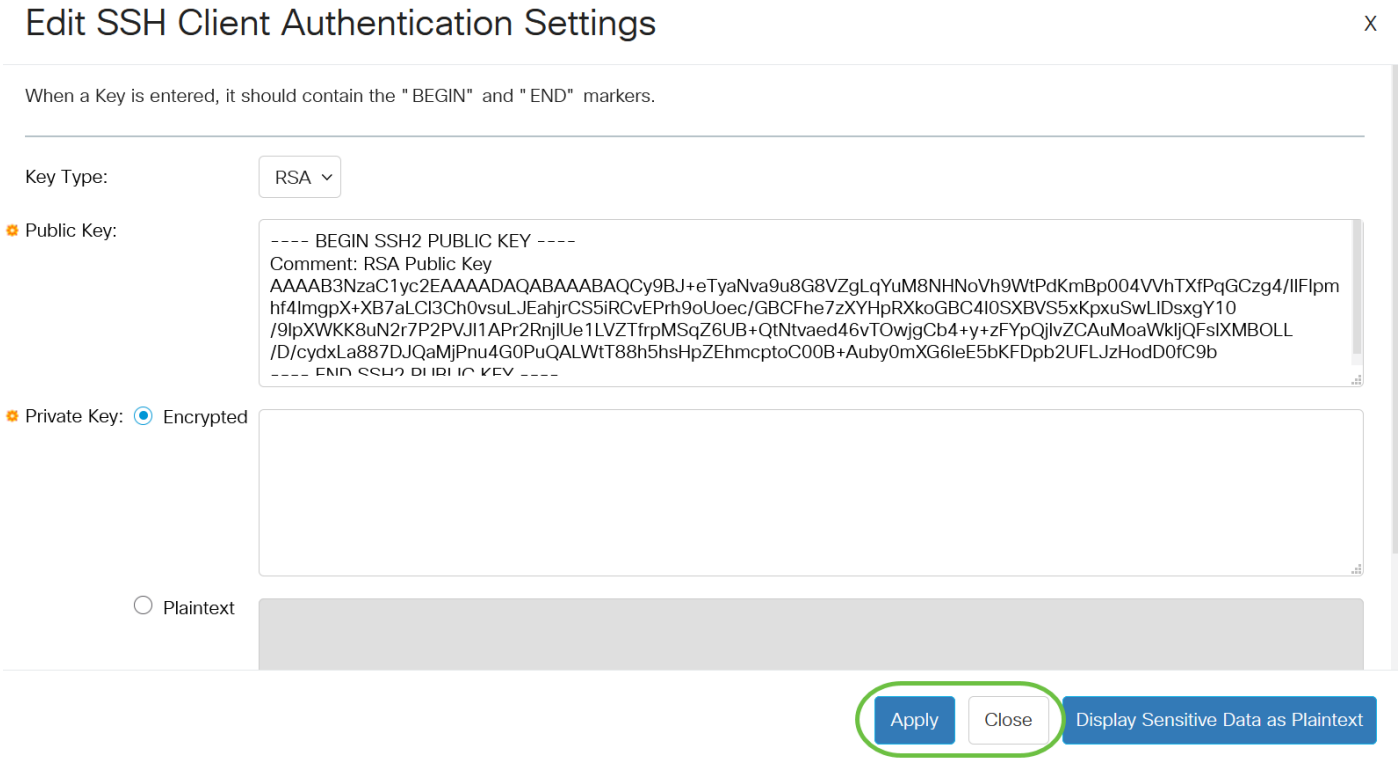
개인 키를 편집하고 Encrypted를 클릭하여 현재 개인 키를 암호화된 텍스트로 보거나 Plaintext를 클릭하여 현재 개인 키를 일반 텍스트로 볼 수 있습니다.

15단계. (선택 사항) **Display Sensitive Data as Plaintext**를 클릭하여 페이지의 암호화된 데이터를 일반 텍스트 형식으로 표시한 다음 **OK**(확인)를 클릭하여 계속 진행합니다.

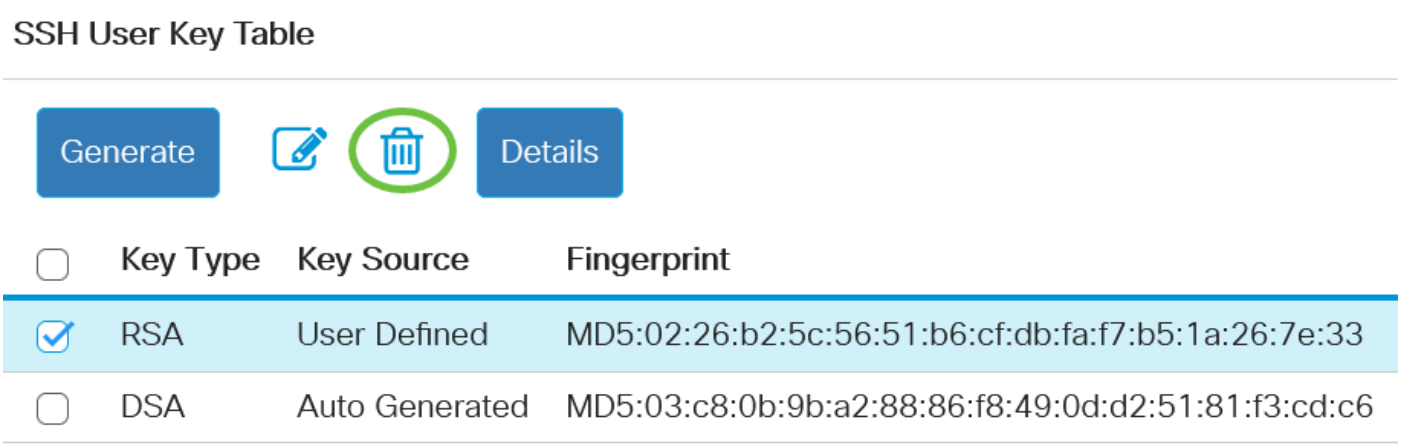




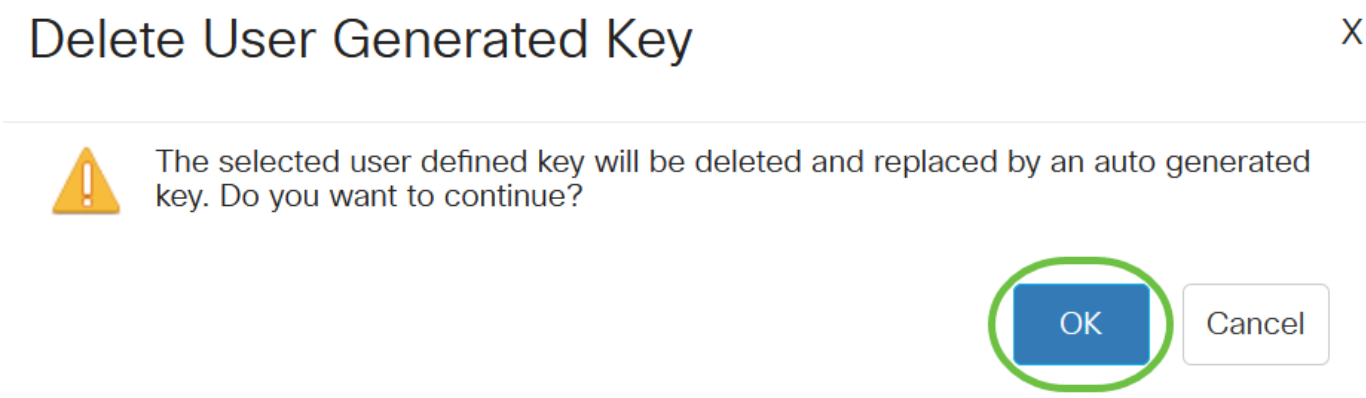

16단계. **적용**을 클릭하여 변경 사항을 저장한 다음 **닫기**를 클릭합니다.



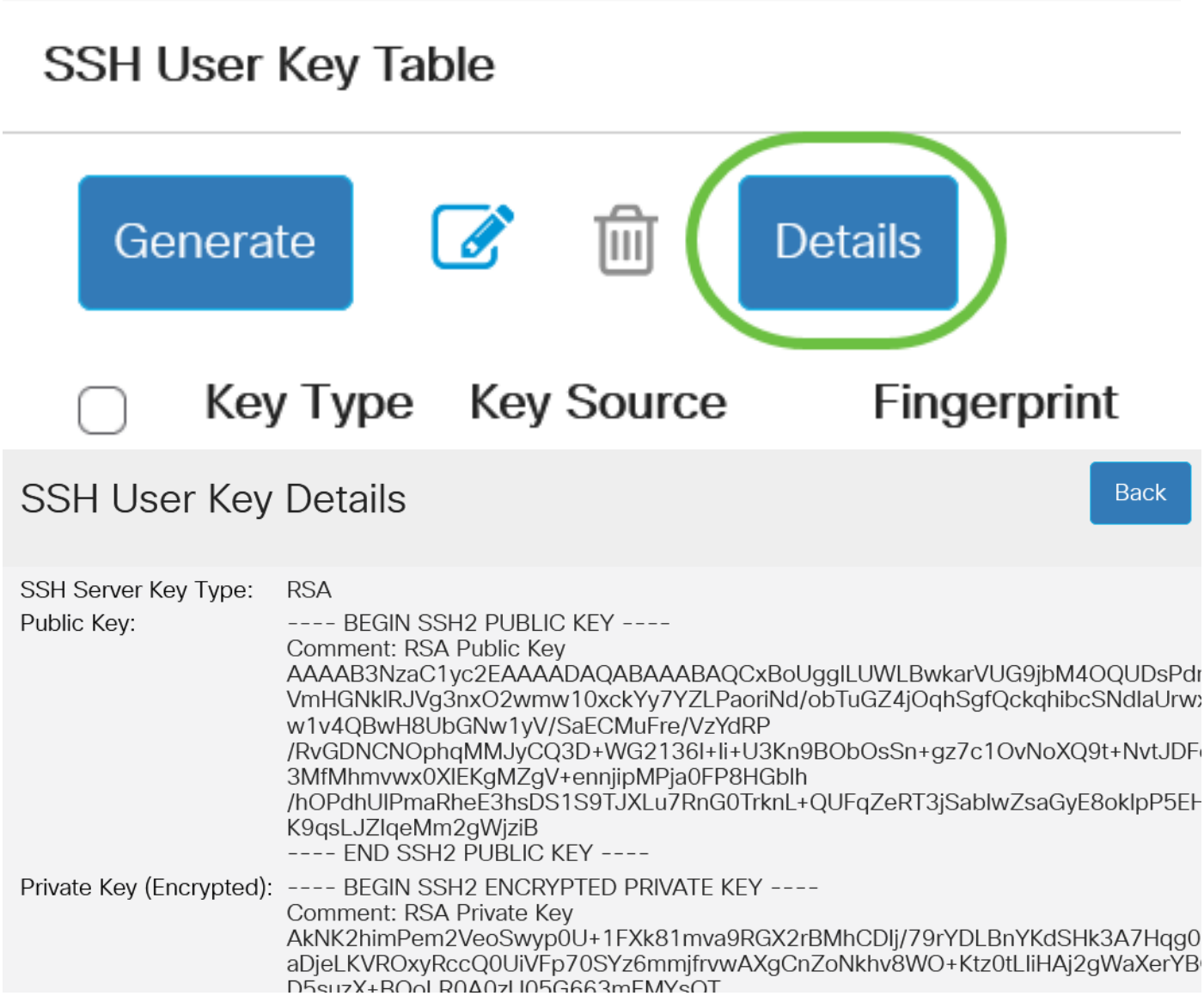

17단계. (선택 사항) **Delete**를 클릭하여 선택한 키를 삭제합니다.



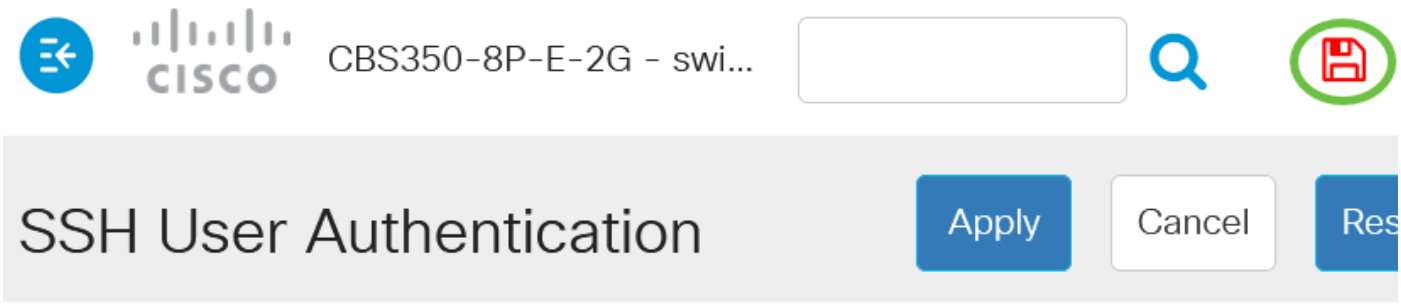

18단계. (선택 사항) 아래와 같이 확인 메시지가 표시되면 **OK**(확인)를 클릭하여 키를 삭제합니다.




19단계. (선택 사항) **Details**를 클릭하여 선택한 키의 세부 정보를 확인합니다.




20단계(선택 사항) 페이지 상단 부분에 있는 **Save**(저장) 버튼을 클릭하여 변경 사항을 시작 구성 파일에 저장합니다.




이제 Cisco Business 350 시리즈 스위치에 클라이언트 사용자 인증 설정을 구성했습니다.