# SG350XG 및 SG550XG 스위치에 대한 SSH(Client Secure Shell) 사용자 인증

## 목표

SSH(Secure Shell)는 특정 디바이스에 대한 보안 원격 연결을 제공하는 프로토콜입니다 .350XG 및 550XG Series Managed Switch를 사용하면 SSH를 통해 디바이스에 연결할 사용자를 인증하고 관리할 수 있습니다.인증은 공개 키를 통해 이루어지므로 사용자는 이 키를 사용하여 특정 디바이스에 대한 SSH 연결을 설정할 수 있습니다.SSH 연결은 네트워크 관리자가 네트워크 사이트에 없는 경우 원격으로 네트워크 문제를 해결하는 데 유용합니다.

이 문서에서는 SG350XG 및 SG550XG Series Managed Switch에서 클라이언트 사용자 인증을 구성하는 방법에 대해 설명합니다.

## 적용 가능한 디바이스

- SG350XG
- SG550XG

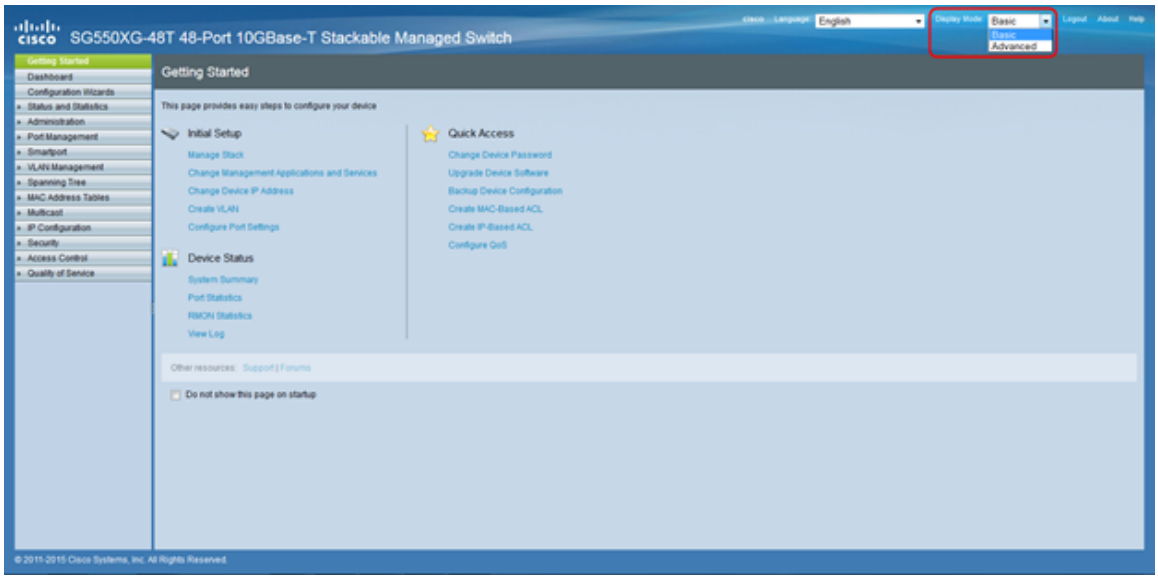
## 소프트웨어 버전

- v2.0.0.73

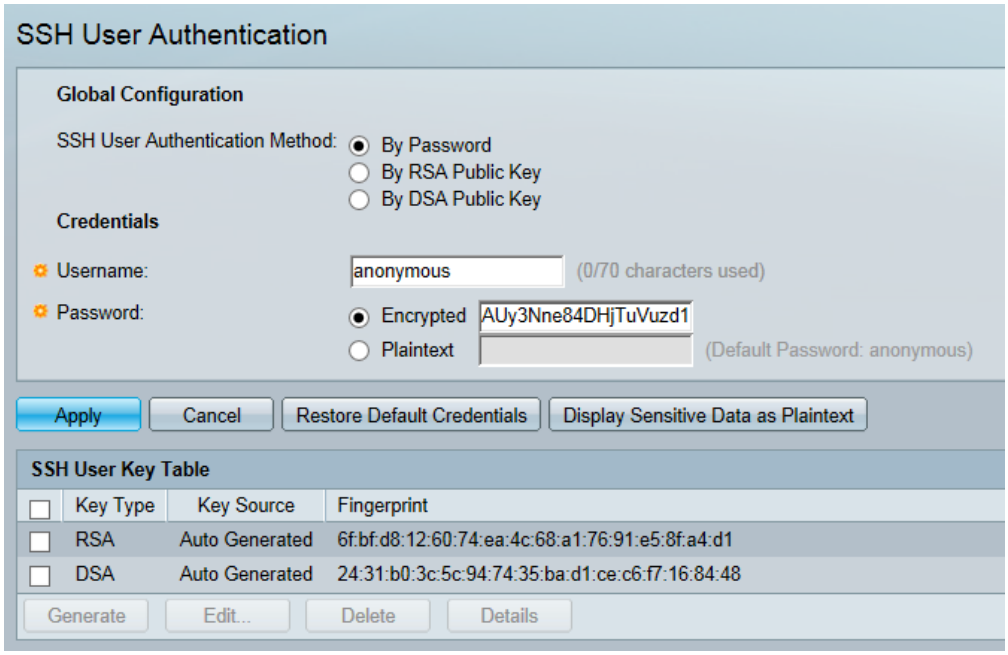
## SSH 구성 클라이언트 인증

### 전역 구성

**참고:**다음 스크린샷은 고급 디스플레이에서 가져온 것입니다.화면 오른쪽 상단에 있는 *Display Mode* 드롭다운 목록을 클릭하여 이를 전환할 수 있습니다.




1단계. 웹 구성 유틸리티에 로그인하고 **Security > SSH Client > SSH User Authentication**을 선택합니다.SSH *User Authentication* 페이지가 열립니다.




2단계. *SSH User Authentication Method* 필드*에서* 원하는 전역 인증 방법에 대한 라디오 버튼을 클릭합니다.


사용 가능한 옵션은 다음과 같습니다.

- By Password(비밀번호별) - 이 옵션을 사용하여 사용자 인증을 위한 비밀번호를 구성할 수 있습니다.비밀번호를 입력하거나 기본값인 "anonymous"를 유지합니다.
- RSA 공개 키별 - 이 옵션을 사용하면 사용자 인증에 RSA 공개 키를 사용할 수 있습니다.RSA는 암호화 및 서명에 사용됩니다.이 옵션을 선택한 경우 SSH User Key Table(SSH 사용자 키 테이블) 블록에서 RSA 공개 및 개인 키를 생성합니다.
- DSA 공개 키별 - 이 옵션을 사용하면 사용자 인증에 DSA 공개 키를 사용할 수 있습니다.DSA는 서명에만 사용됩니다.이 옵션을 선택한 경우 SSH User Key Table(SSH 사용자 키 테이블) 블록에서 DSA 공개/개인 키를 생성합니다.

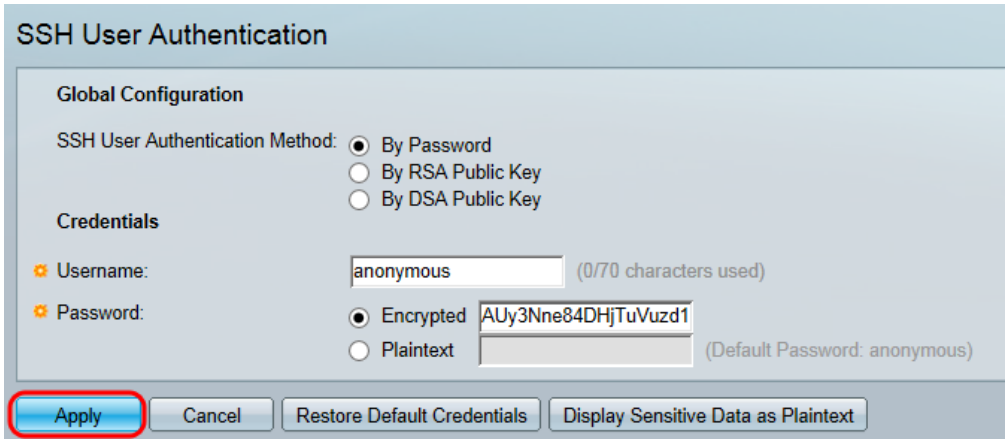
3단계. Credentials(자격 증명) 영역을 찾습니다.Username(*사용자 이름*) 필드에 사용자 이름을 입력합니다.


4단계. 2단계에서 **비밀번호별**을 선택한 경우 *비밀번호* 필드에서 원하는 비밀번호 방법에 대한 라디오 버튼을 클릭합니다.기본 비밀번호는 "anonymous"입니다.

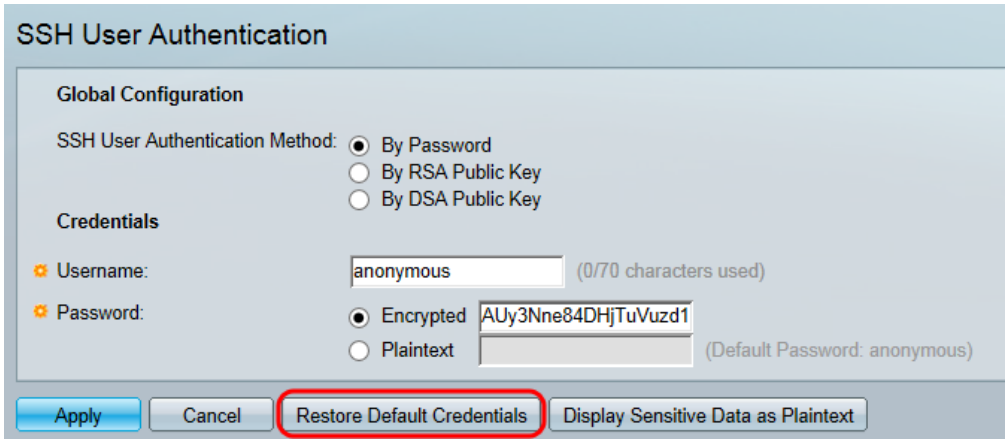

사용 가능한 옵션은 다음과 같이 설명합니다.

- Encrypted(암호화) - 암호화된 비밀번호를 입력합니다.
- 일반 텍스트 - 일반 텍스트로 비밀번호를 입력합니다.

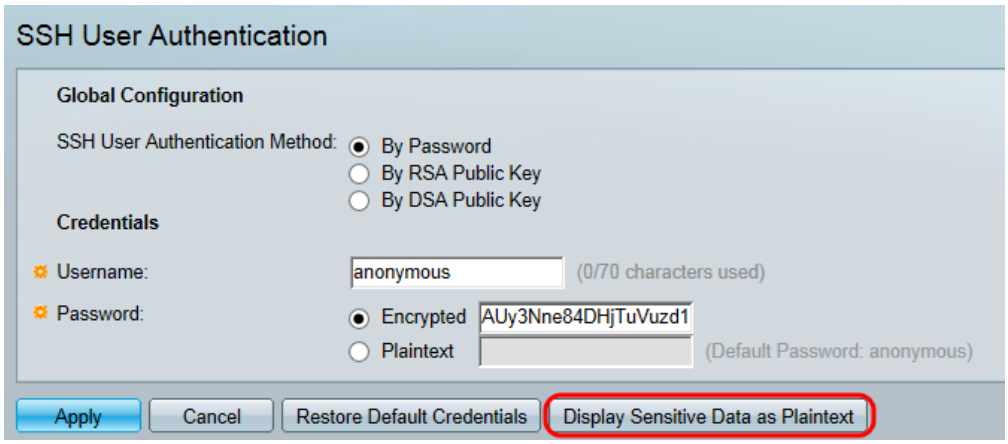
5단계. Apply(**적용**)를 클릭하여 인증 컨피그레이션을 저장합니다.




6단계. (선택 사항) 기본 사용자 이름 및 비밀번호를 복원하려면 **Restore Default Credentials(기본 자격 증명 복원)를** 클릭합니다.기본값은 "anonymous"입니다.




7단계. (선택 사항) 민감한 데이터를 일반 텍스트 또는 암호화된 텍스트로 보려면 **Display Sensitive Data as Plaintext/Encrypted**를 클릭합니다.

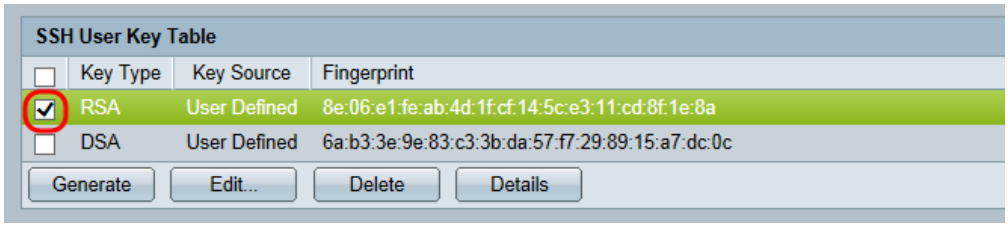



**참고:**현재 설정에 따라 단추 이름이 변경됩니다.이 단추는 항상 데이터 표시를 토글합니다.

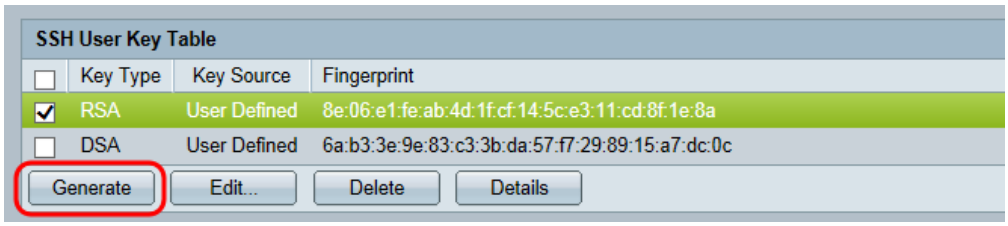
## SSH 사용자 키 테이블

이 섹션에서는 SSH 사용자 테이블을 관리하는 방법에 대해 설명합니다.

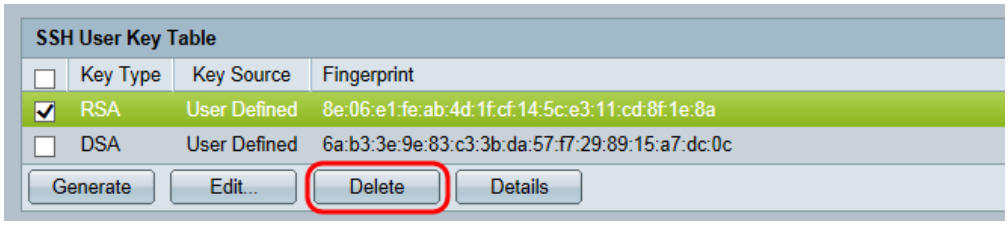
1단계. SSH *User Key Table로 이동합니다*.표시된 목록에서 관리하려는 키의 왼쪽 확인란을 선택합니다.



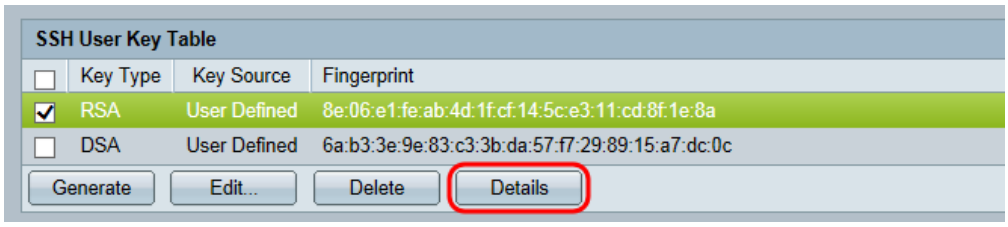

2단계. (선택 사항) Generate(**생성**)를 클릭하여 새 키를 생성합니다.새 키가 선택한 키를 재정의합니다.확인 창이 나타납니다.OK(**확인**)를 클릭하여 계속합니다.



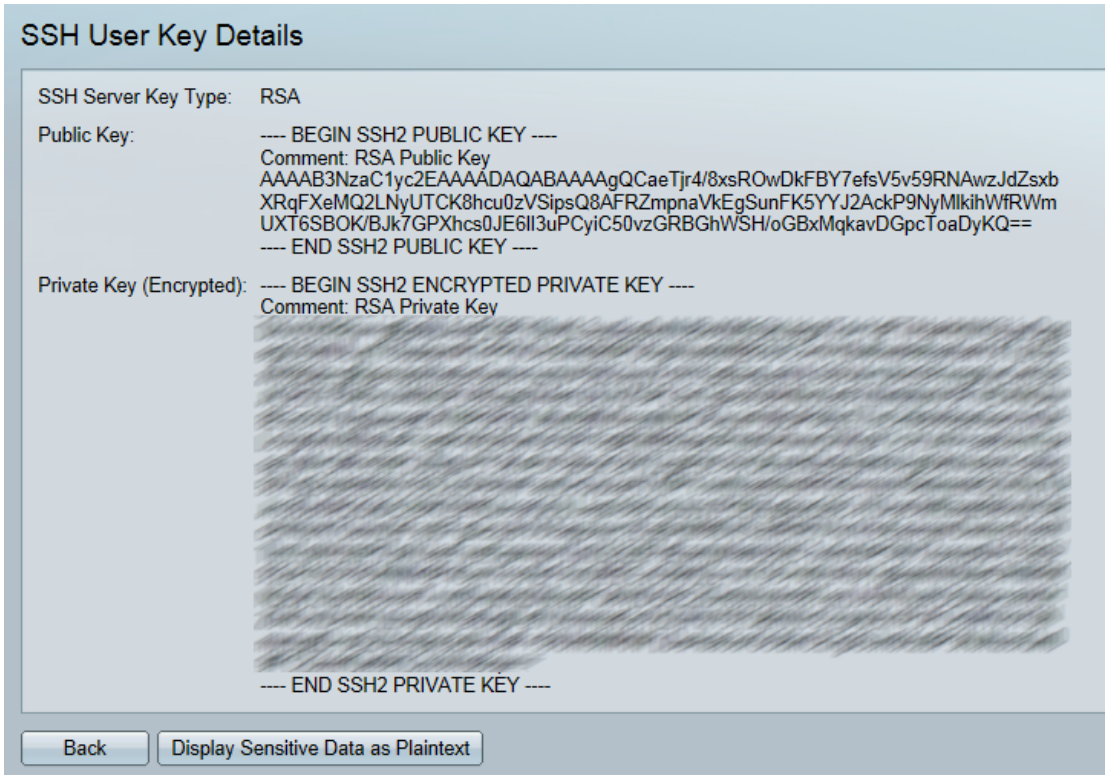

3단계. (선택 사항) **Delete(삭제)**를 클릭하여 선택한 키를 삭제합니다.확인 창이 나타납니다. **OK(확인)**를 클릭하여 계속합니다.



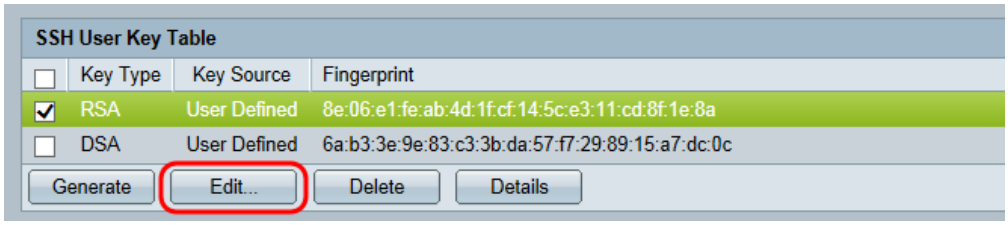

4단계. (선택 사항) **Details**를 클릭하여 선택한 키의 세부 정보를 봅니다.



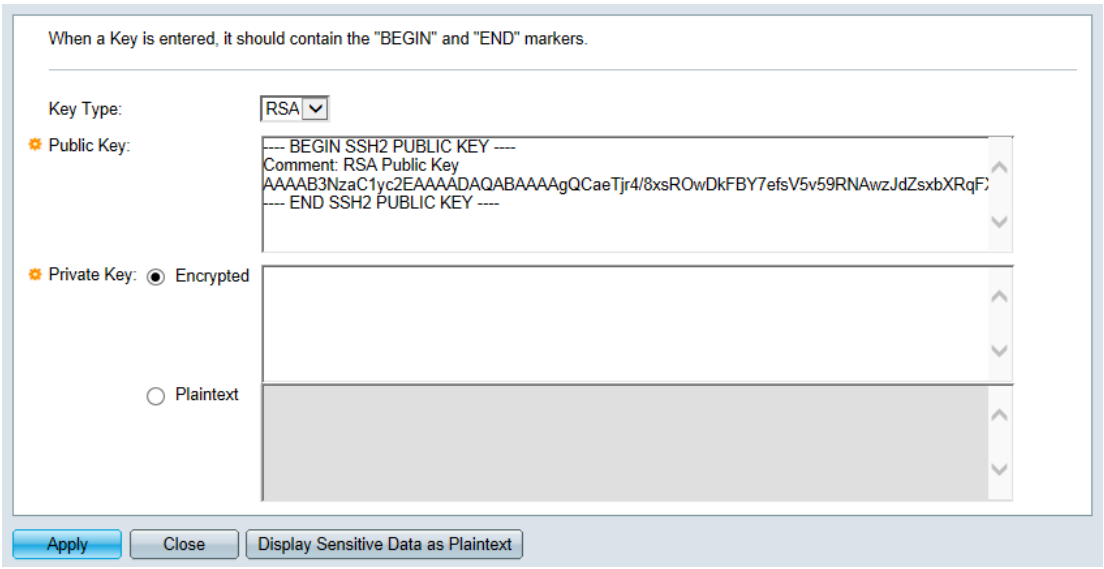

SSH User Key Details 페이지가 나타납니다.SSH User Key Table로 돌아가려면 Back을 클릭합니다.



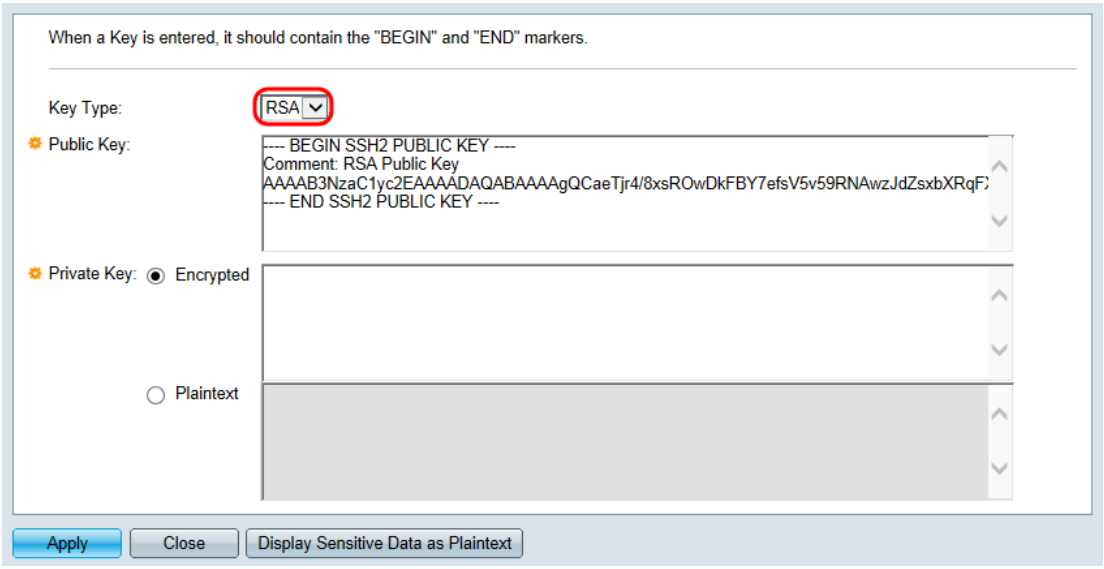

5단계. 선택한 키를 수정하려면 Edit를 클릭합니다.




Edit *SSH Client Authentication Settings(SSH 클라이언트 인증 설정 수정)* 창이 열립니다.



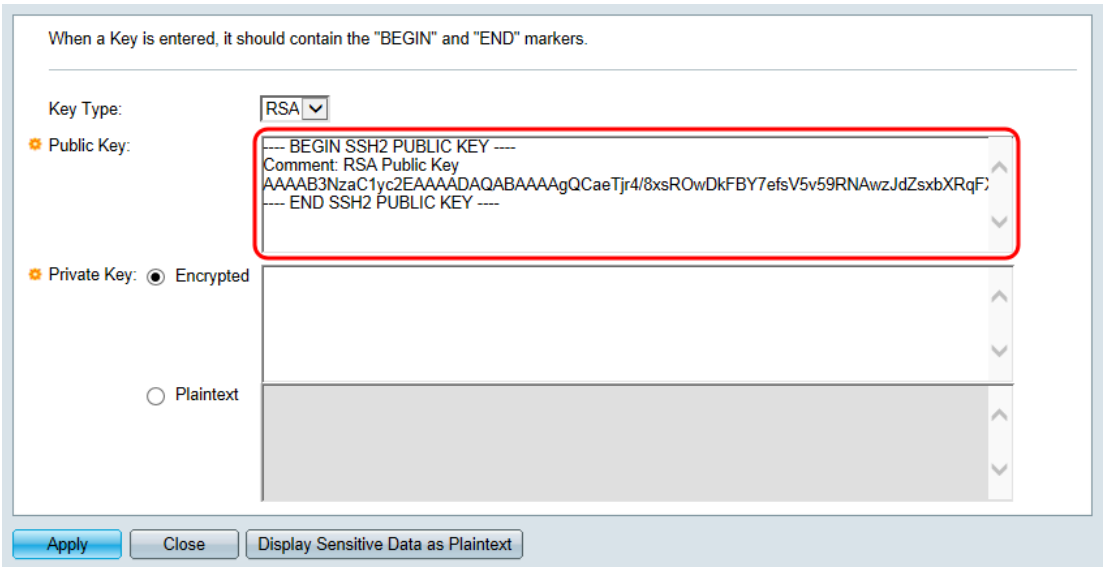

6단계. *키 유형* 드롭다운 목록에서 원하는 키 유형을 선택합니다.




사용 가능한 옵션은 다음과 같습니다.

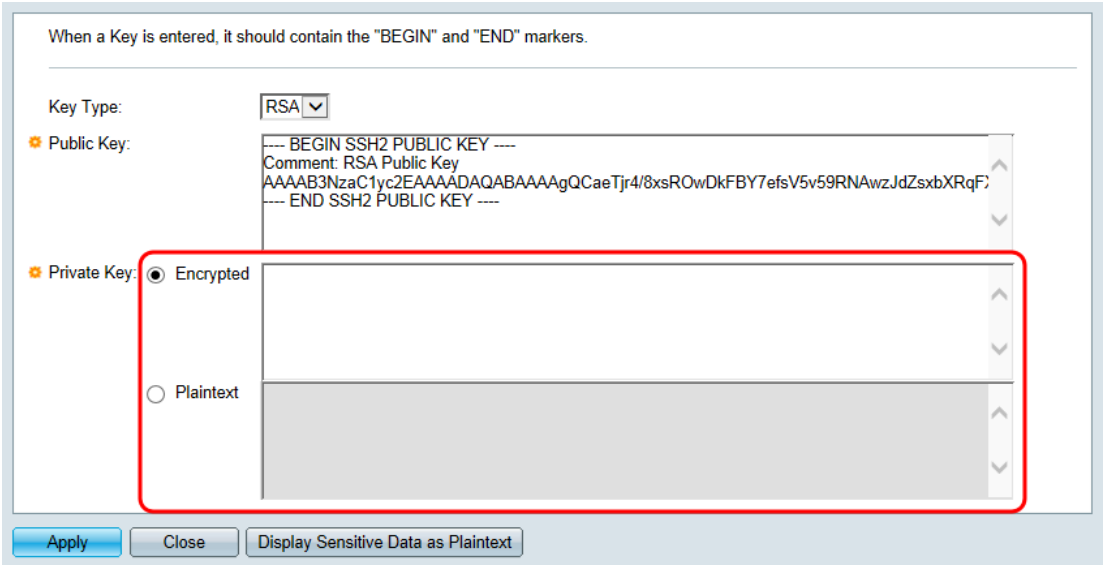
- RSA - RSA는 암호화 및 서명에 사용됩니다.
- DSA - DSA는 서명에만 사용됩니다.

7단계. *Public Key* 필드에서 현재 공개 키를 편집할 수 있습니다.




8단계. *Private Key* 필드에서 현재 개인 키를 편집할 수 있습니다.다음을 클릭합니다.

**암호화된** 라디오 버튼 - 현재 개인 키를 암호화된 상태로 표시합니다.그렇지 않으면 Plaintext 라디오 버튼을 클릭하여 현재 개인 키를 일반 텍스트로 표시합니다.




9단계. **적용**을 클릭하여 변경 사항을 저장합니다.