# PuTTYgen Generation of SSH Authorized Keys and RSA Authentication on Cisco Secure IDS Configuration 예

## 목차



## 소개

이 문서에서는 PuTTY(PuTTYgen)용 키 생성기를 사용하여 Cisco IDS(Secure Intrusion Detection System)에서 사용할 SSH(Secure Shell) 인증 키 및 RSA 인증을 생성하는 방법에 대해 설명합니다. SSH 인증 키를 설정할 때 가장 큰 문제는 이전 RSA1 키 형식만 허용된다는 것입니다.즉, 키 생성기에 RSA1 키를 생성하도록 지시해야 하며 SSH1 프로토콜을 사용하도록 SSH 클라이언트를 제한해야 합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 최근 PuTTY - 2004년 2월 7일
- Cisco 보안 IDS

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

# 구성

이 섹션에서는 이 문서에서 설명하는 기능을 구성하는 데 필요한 정보를 제공합니다.

**참고:** 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에서 사용하는 명령에 대한 추가 정보를 찾습니다.

## PuTTYgen 구성

PuTTYgen을 구성하려면 다음 단계를 완료하십시오.

1. PuTTYgen 시작
2. SSH1 키 유형을 클릭하고 생성된 키의 비트 수를 대화 상자 하단의 Parameters 그룹에서 **2048**로 설정합니다.
3. Generate(**생성**)를 클릭하고 지침을 따릅니다.키 정보가 대화 상자의 위쪽 섹션에 표시됩니다.
4. Key Comment(키 설명) 편집 상자를 지웁니다.
5. authorized_keys 파일에 붙여넣으려면 공개 키의 모든 텍스트를 선택하고 **Ctrl-C를 누릅니다**.
6. Key passphrase(키 패스프레이즈) 및 Confirm passphrase(암호 확인) 수정 상자에 패스프레이즈를 입력합니다.
7. Save **private key를 클릭합니다**.
8. Windows 로그인(Windows 2000/XP의 Documents and Settings/(사용자 ID)/My Documents 하위 트리)에 있는 디렉토리 개인 디렉토리에 PuTTY 개인 키 파일을 저장합니다.
9. PuTTY를 시작합니다.
10. 다음과 같이 새 PuTTY 세션을 생성합니다.**세션:IP 주소:**IDS 센서의 IP 주소**프로토콜:**SSH**포트:**22**연결:자동 로그인 사용자 이름:**cisco(센서에서 사용하는 로그인 가능)**연결/SSH:기본 설정 SSH 버전:**1만**연결/SSH/인증:인증을 위한 개인 키 파일:**8단계에 저장된 .PPK 파일을 찾습니다.**세션:**(맨 위로)**저장된 세션:**(센서 이름을 입력하고 Save(저장)를 **클릭합니다**)
11. Open(**열기**)을 클릭하고 비밀번호 인증을 사용하여 센서 CLI에 연결합니다. 아직 센서에 공개 키가 없기 때문입니다.
12. configure **terminal** CLI 명령을 입력하고 Enter를 **누릅니다**.
13. ssh authorized-**key mykey** CLI 명령을 입력하지만 지금은 Enter 키를 누르지 마십시오.끝에 공백을 입력하십시오.
14. PuTTY 터미널 창을 마우스 오른쪽 버튼으로 클릭합니다.5단계에서 복사한 클립보드 자료는 CLI에 입력됩니다.
15. Enter**를 누릅니다**.
16. exit 명령을 **입력하고 Enter**를 **누릅니다**.
17. 인증된 키가 올바르게 입력되었는지 확인합니다.show ssh authorized-**keys mykey** 명령**을** 입력하고 Enter 키를 **누릅니다**.
18. exit 명령을 입력하여 IDS CLI를 종료하고 Enter를 **누릅니다**.

# 다음을 확인합니다.

## RSA 인증

다음 단계를 완료합니다.

1. PuTTY를 시작합니다.
2. 10단계에서 생성된 저장된 세션을 찾아 두 번 클릭합니다.PuTTY 터미널 창이 열리고 다음 텍스트가 나타납니다.
   ```
   Sent username "cisco"
   Trying public key authentication.
   Passphrase for key "":
   ```
3. 6단계에서 생성한 개인 키 패스프레이즈를 입력하고 Enter를 **누릅니다**.자동으로 로그인됩니다.

## 문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

## 관련 정보

- 네트워크 침입 탐지 기술 지원 페이지
- 기술 지원 및 문서 – Cisco Systems