

# 액세스 포인트(AP)에서 SSH(Secure Shell) 활성화

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[Aironet AP에서 CLI\(Command-Line Interface\) 액세스](#)

[구성](#)

[CLI 컨피그레이션](#)

[단계별 지침](#)

[GUI 컨피그레이션](#)

[단계별 지침](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[SSH 비활성화](#)

[관련 정보](#)

---

## 소개

이 문서에서는 SSH(Secure Shell) 기반 액세스를 사용하도록 AP(액세스 포인트)를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

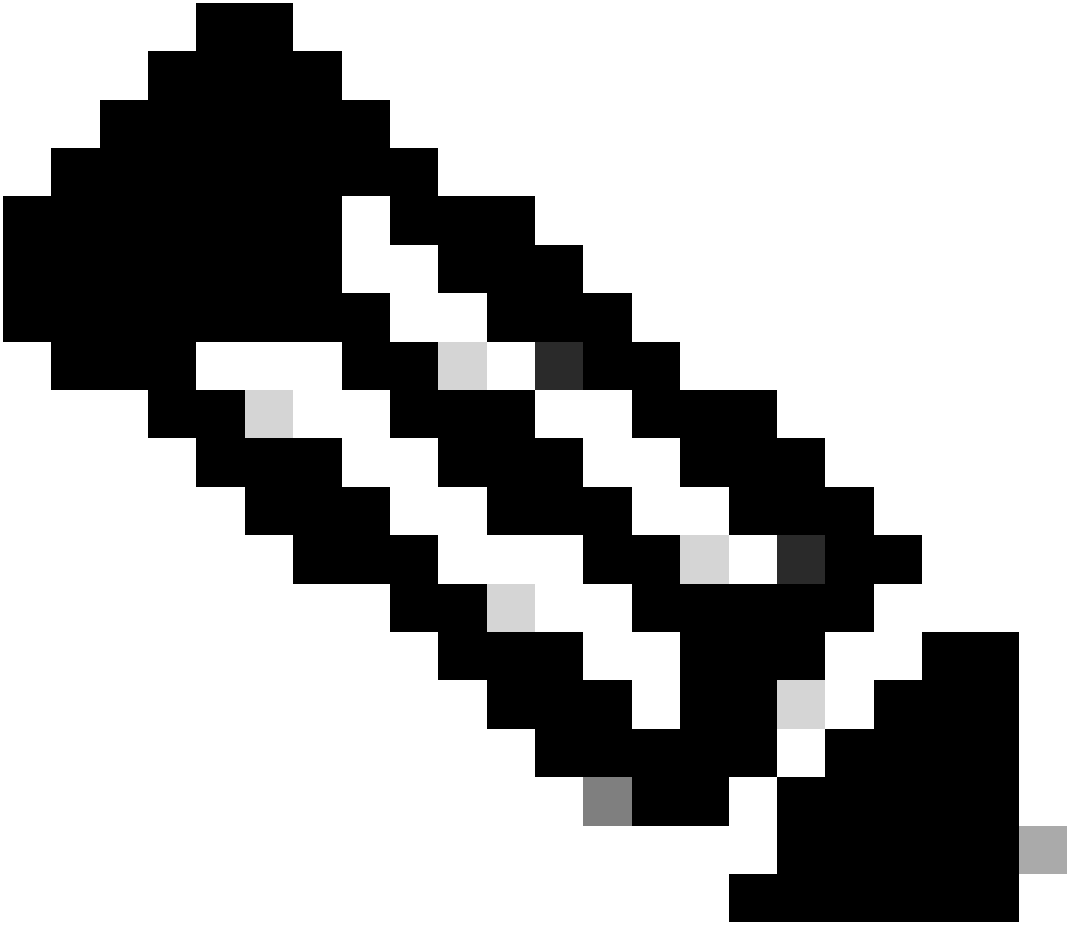
- Cisco Aironet AP 구성 방법에 대한 지식
- SSH 및 관련 보안 개념에 대한 기본 지식

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® Software 릴리스 12.3(8)JEB를 실행하는 Aironet 1200 Series AP
- SSH 클라이언트 유틸리티가 있는 PC 또는 노트북

---



참고: 이 문서에서는 SSH 클라이언트 유틸리티를 사용하여 컨피그레이션을 확인합니다. SSH를 사용하여 AP에 로그인하려면 모든 서드파티 클라이언트 유틸리티를 사용할 수 있습니다.

---

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

## 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

## Aironet AP에서 CLI(Command-Line Interface) 액세스

다음 방법 중 하나를 사용하여 Aironet AP의 CLI(Command Line Interface)에 액세스할 수 있습니다

- 콘솔 포트
- Telnet
- SSH

AP에 콘솔 포트가 있고 AP에 대한 물리적 액세스 권한이 있는 경우 콘솔 포트를 사용하여 AP에 로그인하고 필요한 경우 컨피그레이션을 변경할 수 있습니다. AP에 로그인하기 위해 콘솔 포트를 사용하는 방법에 대한 자세한 내용은 문서의 1200 Series 액세스 포인트에 로컬로 연결 액세스 포인트 처음 구성 섹션을 참조하십시오.

이더넷을 통해서만 AP에 액세스할 수 있는 경우 텔넷 프로토콜 또는 SSH 프로토콜을 사용하여 AP에 로그인합니다.

텔넷 프로토콜은 통신에 포트 23을 사용합니다. 텔넷은 일반 텍스트로 데이터를 전송하고 수신합니다. 데이터 통신은 일반 텍스트로 이루어지므로 해커가 비밀번호를 쉽게 손상시키고 AP에 액세스할 수 있습니다. RFC [854는 텔넷](#)을 정의하고 다른 여러 RFC에 의해 옵션으로 텔넷을 확장합니다.

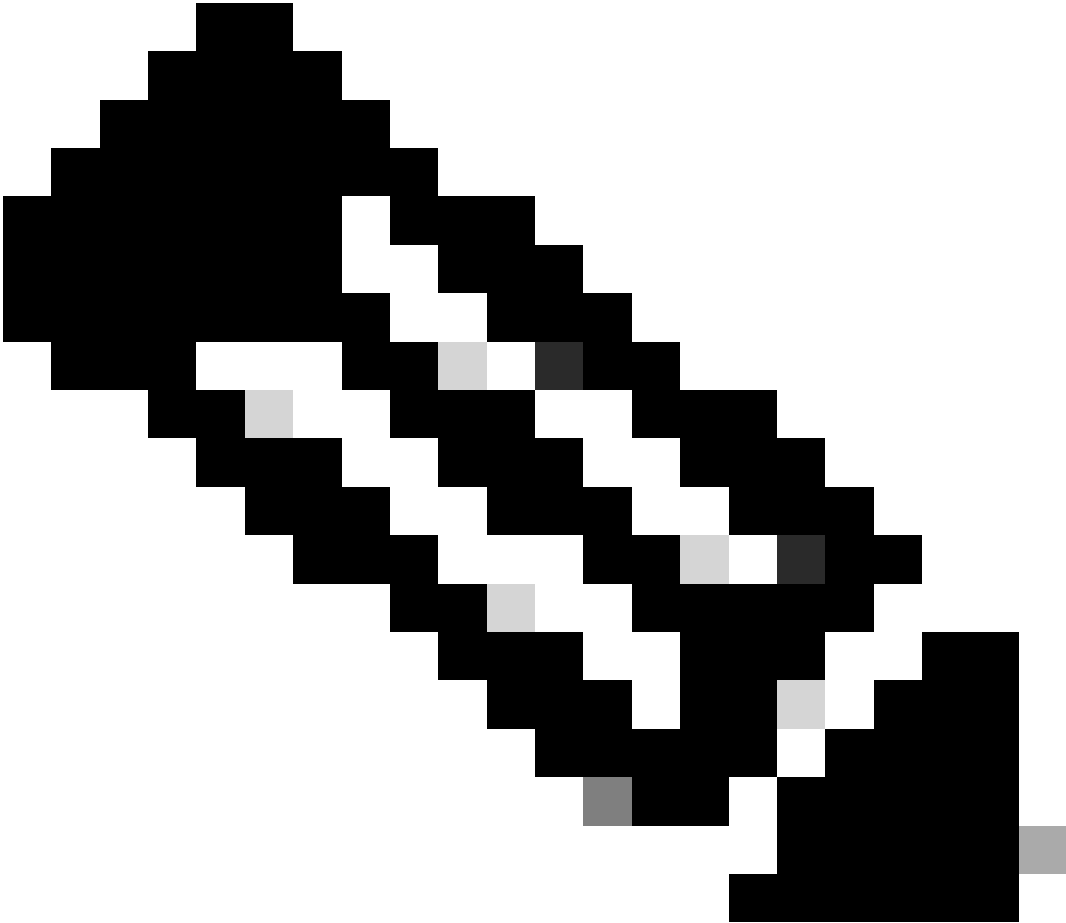
SSH는 Berkley r-tools를 안전하게 대체하는 애플리케이션 및 프로토콜입니다. SSH는 레이어 2 또는 레이어 3 디바이스에 대한 안전한 원격 연결을 제공하는 프로토콜입니다. SSH에는 SSH 버전 1과 SSH 버전 2의 두 가지 버전이 있습니다. 이 소프트웨어 릴리스는 두 가지 SSH 버전을 모두 지원합니다. 버전 번호를 지정하지 않으면 AP의 기본값은 버전 2입니다.

SSH는 장치가 인증될 때 강력한 암호화를 제공하므로 텔넷보다 원격 연결에 더 많은 보안을 제공합니다. 이 암호화는 일반 텍스트로 통신이 이루어지는 텔넷 세션보다 유리합니다. SSH에 대한 자세한 내용은 SSH([Secure Shell](#)) FAQ를 참조하십시오. SSH 기능에는 SSH 서버 및 SSH 통합 클라이언트가 있습니다.

클라이언트는 다음 사용자 인증 방법을 지원합니다.

- RADIUS
- 로컬 인증 및 권한 부여.

---



참고: 이 소프트웨어 릴리스의 SSH 기능은 IP 보안(IPSec)을 지원하지 않습니다.

---

CLI 또는 GUI를 사용하여 SSH용 AP를 구성할 수 있습니다. 이 문서에서는 두 가지 구성 방법에 대해 설명합니다.

## 구성

### CLI 컨피그레이션

이 섹션에서는 CLI를 사용하여 기능을 구성하는 방법에 대해 설명합니다.

#### 단계별 지침

AP에서 SSH 기반 액세스를 활성화하려면 먼저 AP를 SSH 서버로 구성해야 합니다. CLI에서 AP에 SSH 서버를 구성하려면 다음 단계를 수행합니다.

1. AP에 대한 호스트 이름 및 도메인 이름을 구성합니다.

```
<#root>
```

```
AP#
```

```
configure terminal
```

```
!--- Enter global configuration mode on the AP.
```

```
AP<config>#
```

```
hostname Test
```

```
!--- This example uses "Test" as the AP host name.
```

```
Test<config>#
```

```
ip domain name domain
```

```
!--- This command configures the AP with the domain name "domain name".
```

## 2. AP에 대한 RSA(Rivest, Shamir, and Adelman) 키를 생성합니다.

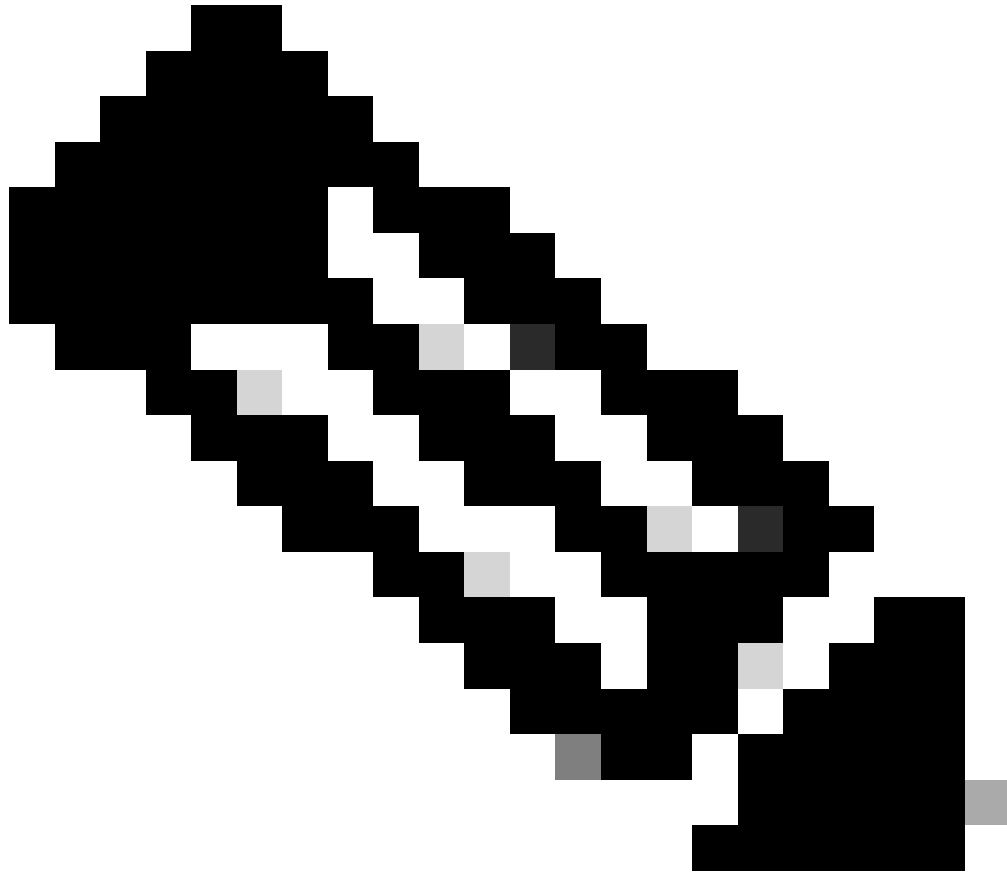
RSA 키를 생성하면 AP에서 SSH가 활성화됩니다. 전역 컨피그레이션 모드에서 다음 명령을 실행합니다.

```
<#root>
```

```
Test<config>#
```

```
crypto key generate rsa rsa_key_size
```

```
!--- This generates an RSA key and enables the SSH server.
```



참고: 권장되는 최소 RSA 키 크기는 1024입니다.

---

### 3. AP에 대한 사용자 인증을 구성합니다.

AP에서 로컬 목록 또는 외부 AAA(authentication, authorization, and accounting) 서버를 사용하도록 사용자 인증을 구성할 수 있습니다. 이 예에서는 사용자를 인증하기 위해 로컬에서 생성된 목록을 사용합니다.

```
<#root>
```

```
Test<config>#
```

```
aaa new-model
```

```
!--- Enable AAA authentication.
```

```
Test<config>#
```

```
aaa authentication login default local none
```

```
!--- Use the local database in order to authenticate users.
```

```
Test<config>#
```

```
username Test password Test123
```

```
!--- Configure a user with the name "Test".
```

```
Test<config>#
```

```
username ABC password xyz123
```

```
!--- Configure a second user with the name "Domain".
```

이 컨피그레이션은 AP에 구성된 로컬 데이터베이스를 사용하여 사용자 기반 인증을 수행하도록 AP를 구성합니다. 이 예에서는 로컬 데이터베이스에서 "Test" 및 "ABC"라는 두 사용자를 구성합니다.

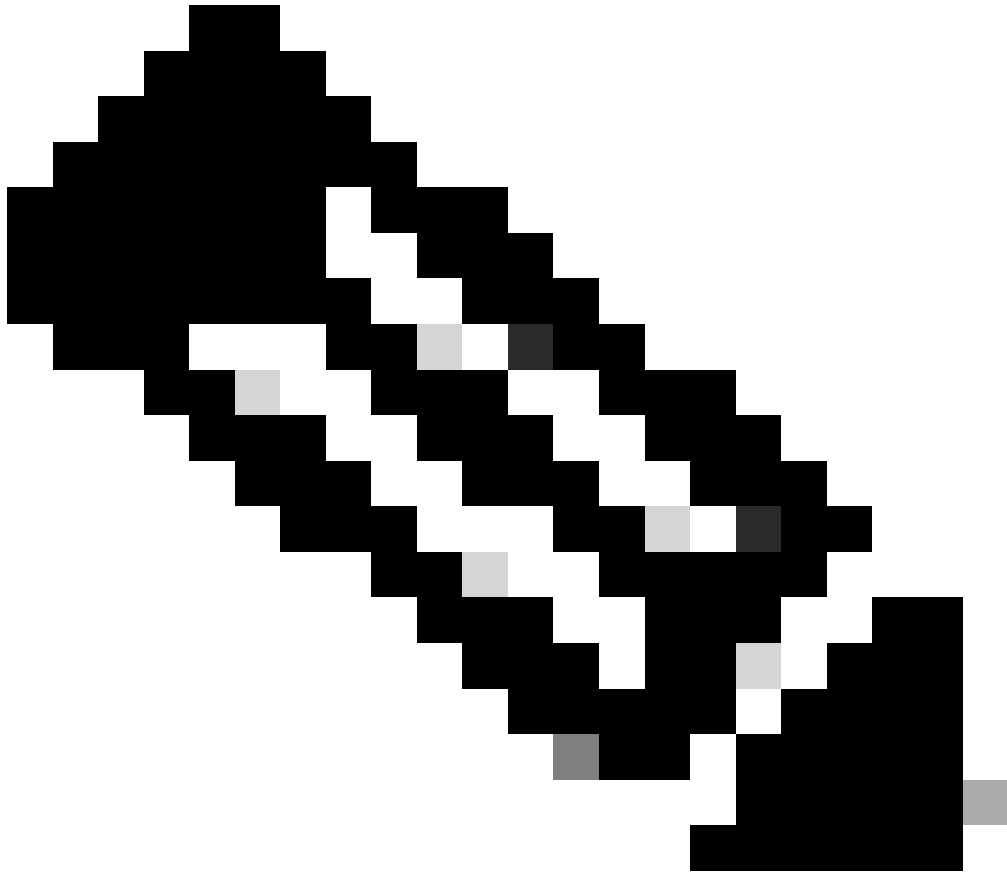
#### 4. SSH 매개변수를 구성합니다.

```
<#root>
```

```
Test<config>#
```

```
ip ssh {[timeout seconds] | [authentication-retries integer]}
```

```
!--- Configure the SSH control variables on the AP.
```



참고: 시간 제한을 초 단위로 지정할 수 있지만 120초를 초과하지 않습니다. 기본값은 120입니다. SSH 협상 단계에 적용되는 사양입니다. 인증 재시도 횟수를 지정할 수도 있지만 인증 재시도 횟수를 5회 초과할 수는 없습니다. 기본값은 3입니다.

---

## GUI 컨피그레이션

AP에서 SSH 기반 액세스를 활성화하기 위해 GUI를 사용할 수도 있습니다.

### 단계별 지침

다음 단계를 완료하십시오.

1. 브라우저를 통해 AP에 로그인합니다.

요약 상태 창이 표시됩니다.

2. 왼쪽의 메뉴에서 서비스를 클릭합니다.

서비스 요약 창이 표시됩니다.



3. Telnet/SSH 매개변수를 활성화하고 구성하려면 Telnet/SSH를 클릭합니다.

서비스: 텔넷/SSH 창이 표시됩니다. 아래로 스크롤하여 Secure Shell Configuration 영역으로 이동합니다. Secure Shell 옆에서 Enable(활성화)을 클릭하고 다음 예와 같이 SSH 매개변수를 입력합니다.

이 예에서는 다음 매개변수를 사용합니다.

- 시스템 이름: 테스트
- 도메인 이름: DOMAIN
- RSA 키 크기: 1024
- 인증 시간 초과: 120
- 인증 재시도 횟수: 3

4. Apply를 클릭하여 변경 사항을 저장합니다.

## 다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

OIT(Output Interpreter Tool)는 특정 show 명령을 지원합니다. OIT를 사용하여 show 명령 출력 분석을 볼 수 있습니다.

---

참고: 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

- `show ip ssh` - AP에서 SSH가 활성화되어 있는지 확인하고 AP에서 실행되는 SSH 버전을 확인할 수 있습니다. 이 출력은 다음과 같은 예를 제공합니다.
- `show ssh` - SSH 서버 연결의 상태를 볼 수 있습니다. 이 출력은 다음과 같은 예를 제공합니다.

이제 서드파티 SSH 소프트웨어를 실행하는 PC를 통해 연결을 시작한 다음 AP에 로그인을 시도합니다. 이 확인에서는 AP IP 주소 10.0.0.2를 사용합니다. 사용자 이름 Test를 구성했으므로 이 이름을 사용하여 SSH를 통해 AP에 액세스합니다.

## 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결합니다.

SSH 컨피그레이션 명령이 잘못된 명령으로 거부된 경우 AP에 대한 RSA 키 쌍을 생성하지 못했습니다.

## SSH 비활성화

AP에서 SSH를 비활성화하려면 AP에서 생성된 RSA 쌍을 삭제해야 합니다. RSA 쌍을 삭제하려면 전역 컨피그레이션 모드에서 `crypto key zeroize rsa` 명령을 실행합니다. RSA 키 쌍을 삭제하면 SSH 서버를 자동으로 비활성화합니다. 이 출력은 다음과 같은 예를 제공합니다.

## 관련 정보

- [SSH\(Secure Shell\) 지원 페이지](#)
- [Cisco 기술 지원 및 다운로드](#)

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.