

# アクセスポイント(AP)でのセキュアシェル(SSH)の有効化

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[Aironet APでのコマンドラインインターフェイス\(CLI\)へのアクセス](#)

[設定](#)

[CLIでの設定](#)

[手順説明](#)

[GUIでの設定](#)

[手順説明](#)

[確認](#)

[トラブルシューティング](#)

[SSHのディセーブル化](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、セキュアシェル(SSH)ベースのアクセスをイネーブルにするためにアクセスポイント(AP)を設定する方法について説明します。

## 前提条件

### 要件

この設定を行う前に、次の要件が満たされていることを確認します。

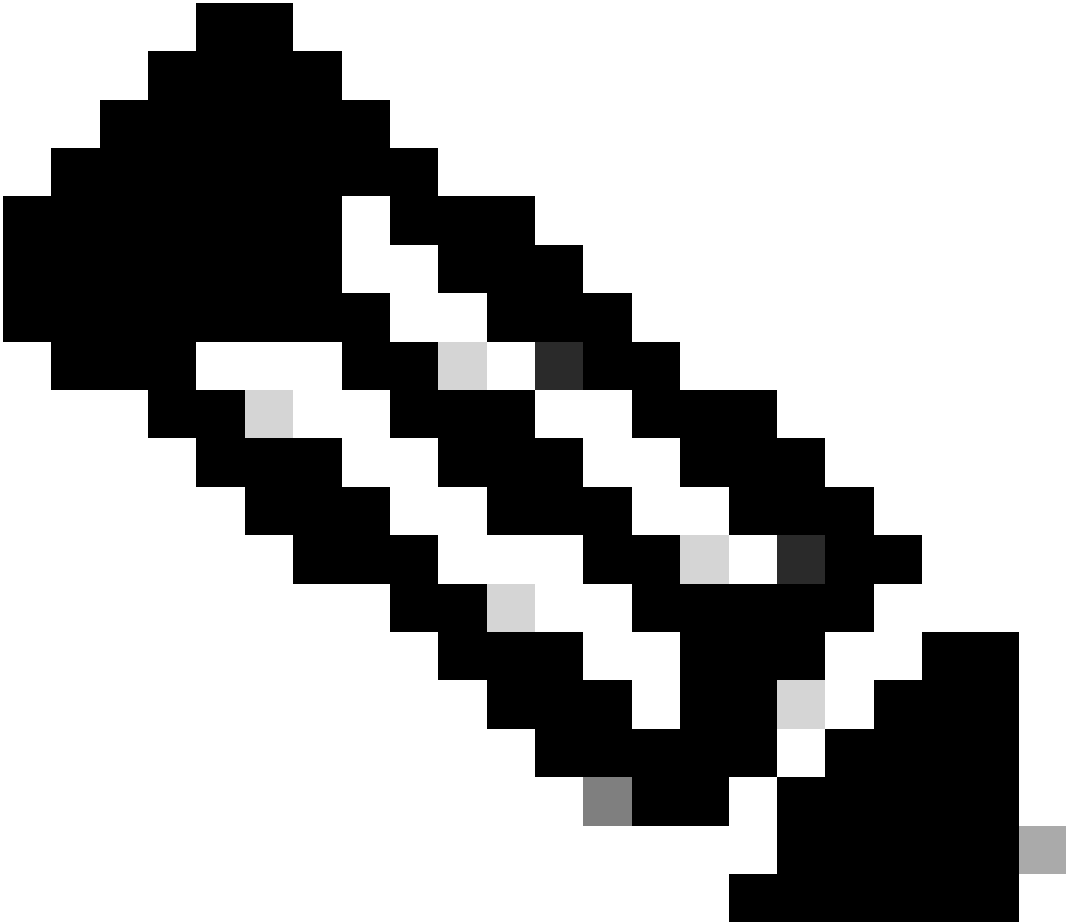
- Cisco Aironet AP の設定方法に関する知識
- SSH および関連するセキュリティの概念に関する基本的な知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS(R) ソフトウェア リリース 12.3(8)JEB が稼働する Aironet 1200 シリーズ AP
- SSH クライアント ユーティリティをインストールした PC またはラップトップ

---



注：このドキュメントでは、SSHクライアントユーティリティを使用して設定を確認します。SSHを使用してAPにログインするために任意のサードパーティクライアントユーティリティを使用できます。

---

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 表記法

表記法の詳細については、『シスコテクニカルティップスの表記法』を参照してください。

## Aironet APでのコマンドラインインターフェイス(CLI)へのアクセス

Aironet AP でコマンドライン インターフェイス ( CLI ) にアクセスするには、次のいずれかの方法を使用できます。

- コンソール ポート
- Telnet
- SSH

AP にコンソール ポートがあり、AP に物理的にアクセスできる場合、コンソール ポートを使用して AP にログインでき、必要に応じて設定を変更できます。コンソールポートを使用してAPにログインする方法の詳細については、『アクセスポイントの最初の設定』ドキュメントの「1200シリーズアクセスポイントへのローカル接続」セクションを参照してください。

イーサネットを介してのみ AP にアクセスできる場合、AP にログインするには、Telnet プロトコルまたは SSH プロトコルを使用します。

Telnet プロトコルでは通信用にポート 23 が使用されます。Telnet はクリア テキストでデータを送受信します。データ通信はクリアテキストで行われるため、ハッカーはパスワードを改ざんしたり、AP にアクセスしたりすることが簡単にできます。[RFC 854](#)では、Telnetが定義され、他の多くのRFCのオプションを使用してTelnetを拡張しています。

SSH は Berkley の r ツールに代わる安全性の高いプロトコルおよびアプリケーションです。SSH は、レイヤ 2 デバイスまたはレイヤ 3 デバイスに安全なリモート接続を提供するプロトコルです。SSHには、SSHバージョン1とSSHバージョン2の2つのバージョンがあります。このソフトウェア リリースでは、どちらの SSH バージョンもサポートしています。バージョン番号を指定しない場合、AP はデフォルトのバージョン 2 になります。

SSHは、デバイスの認証時に強力な暗号化を提供するため、Telnetよりもリモート接続の方がセキュリティが高くなります。この暗号化は、通信がクリア テキストで実行される Telnet セッションと比べて長所になります。SSH の詳細については、セキュア シェル ( SSH ) に関する FAQ を参照してください。SSH 機能では SSH サーバと SSH 統合クライアントを使用します。

クライアントは次のユーザ認証方式をサポートしています。

- RADIUS
- ローカル認証と認可

---

注：このソフトウェアリリースのSSH機能は、IP Security(IPSec)をサポートしていません。

---

CLI または GUI を使用して SSH 用に AP を設定できます。このドキュメントでは、両方の設定方法を説明します。

## 設定

### CLI での設定

このセクションでは、CLIを使用して機能を設定する方法について説明します。

#### 手順説明

AP で SSH ベースのアクセスを可能にするには、まず、SSH サーバとして AP を設定する必要があります。CLIからAPにSSHサーバを設定するには、次の手順を実行します。

## 1. AP のホスト名とドメイン名を設定します。

```
<#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

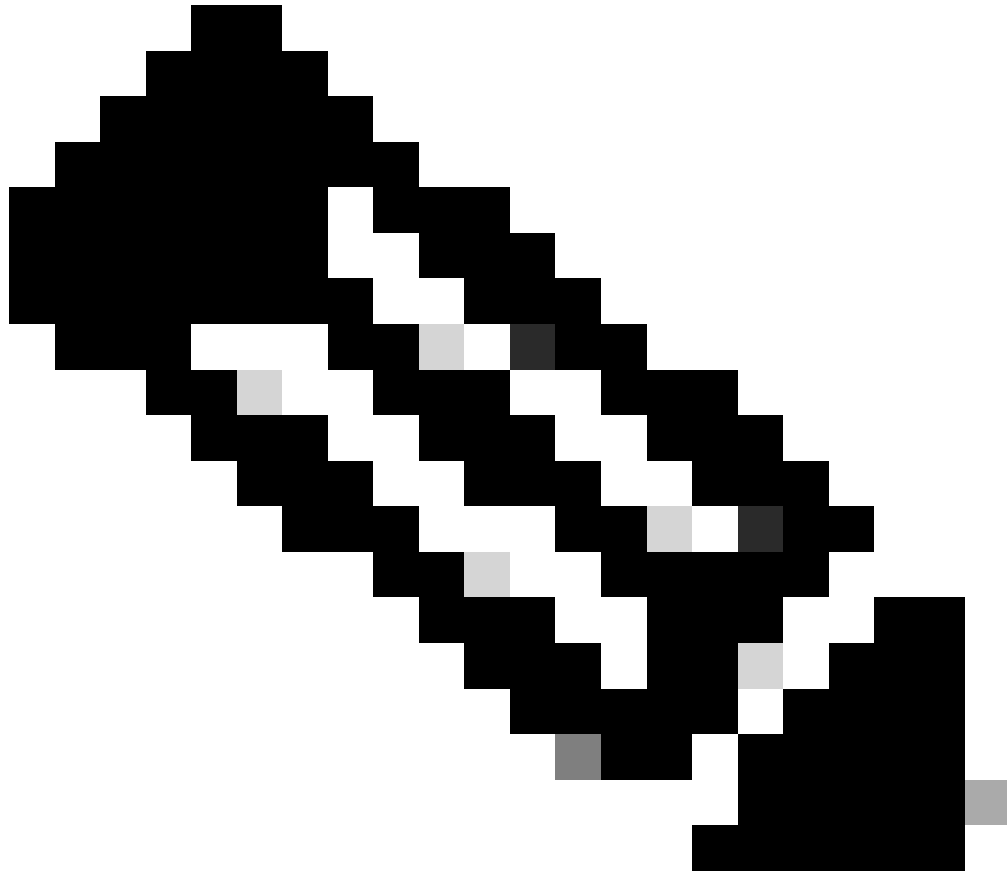
!--- This command configures the AP with the domain name "domain name".
```

## 2. AP の Rivest, Shamir, and Adelman ( RSA ) のキーを生成します。

RSA キーを生成することにより、AP 上で SSH がイネーブルになります。グローバル コンフィギュレーション モードで次のコマンドを発行します。

```
<#root>
Test<config>#
crypto key generate rsa rsa_key_size

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



注：推奨される最小RSAキーサイズは1024です。

---

### 3. AP 上にユーザ認証を設定します。

AP では、ローカル リストまたは外部認証、許可、アカウントिंग ( AAA ) サーバを使用するようにユーザ認証を設定できます。この例では、ローカルで生成されたリストを使用してユーザを認証します。

```
<#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".
```

この設定では、AP 上に設定されたローカル データベースを使用してユーザベースの認証を行うように AP を設定します。この例では、ローカル データベースに 2 人のユーザ、「Test」と「ABC」を設定します。

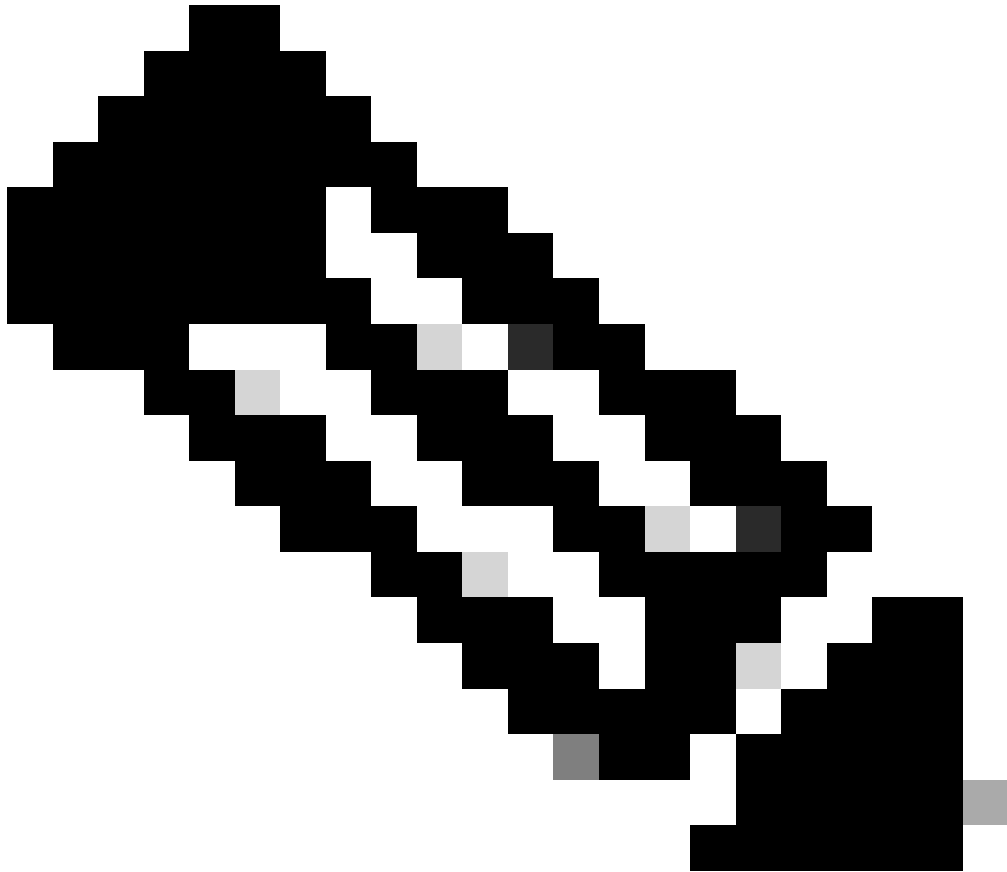
#### 4. SSH パラメータを設定します。

```
<#root>
```

```
Test<config>#
```

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

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



注：タイムアウトは秒単位で指定できますが、120秒を超えることはできません。デフォルトは 120 です。これは、SSHネゴシエーションフェーズに適用される仕様です。認証の再試行回数（5 回以内）も指定できます。デフォルトは 3 です。

---

## GUI での設定

AP 上で SSH ベースのアクセスをイネーブルにするために GUI を使用することもできます。

### 手順説明

次のステップを実行します。

1. ブラウザを使用して AP にログインします。

[Summary Status] ウィンドウが表示されます。

2. 左側のメニューで [Services] をクリックします。

[Services Summary] ウィンドウが表示されます。



3. Telnet/SSH パラメータをイネーブルにして設定するには、[Telnet/SSH] をクリックします。

Services: Telnet/SSHウィンドウが表示されます。[Secure Shell Configuration] 領域までスクロールします。Secure Shell のそばの [Enable] をクリックし、次の例に示すように SSH パラメータを入力します。

この例では、次のパラメータを使用します。

- システム名 : Test
- Domain Name (ドメイン名) : DOMAIN
- RSAキーサイズ : 1024
- 認証タイムアウト : 120
- 認証の再試行回数 : 3

4. [Apply] をクリックして変更を保存します。

## 確認

このセクションでは、設定が正常に動作していることを確認します。

Output Interpreter Tool (登録ユーザ専用) (OIT)では、特定のshowコマンドがサポートされています。OIT を使用して show コマンド出力の解析を表示します。

---

注：シスコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです。

- `show ip ssh` - SSH が AP でイネーブルかどうかを検証し、AP で実行されている SSH のバージョンを確認できます。次に出力例を示します。
- `show ssh` - SSH サーバの接続のステータスを表示できます。次に出力例を示します。

ここで、サードパーティの SSH ソフトウェアを実行する PC を介して接続を開始し、AP への口グインを試行します。この検証では、AP の IP アドレス、10.0.0.2 を使用します。ユーザ名 Test を設定したため、SSH を使用して AP にアクセスするには、この名前を使用してください。

## トラブルシュート

ここでは、設定に関するトラブルシューティングについて説明します。

SSH コンフィギュレーション コマンドが正規のコマンドとして拒否される場合、AP の RSA キーペアを正常に生成していません。

## SSH のディセーブル化

AP 上の SSH をディセーブルにするには、AP で生成された RSA ペアを削除する必要があります。RSA ペアを削除するには、グローバル コンフィギュレーション モードで `crypto key zeroize rsa` コマンドを発行します。RSA キー ペアを削除すると、SSH サーバは自動的にディセーブルになります。次に出カ例を示します。

## 関連情報

- [セキュア シェル \(SSH\) に関するサポート ページ](#)
- [シスコのテクニカルサポートとダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。