Enable Secure Shell (SSH) on an Access Point (AP)

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Access the Command-line Interface (CLI) on the Aironet AP

Configure

- CLI Configuration
  - Step-by-Step Instructions
- GUI Configuration
  - Step-by-Step Instructions

Verify

Troubleshoot

- Disable SSH

Related Information

Introduction

This document describes how to configure an access point (AP) in order to enable Secure Shell (SSH)-based access.

Prerequisites

Requirements

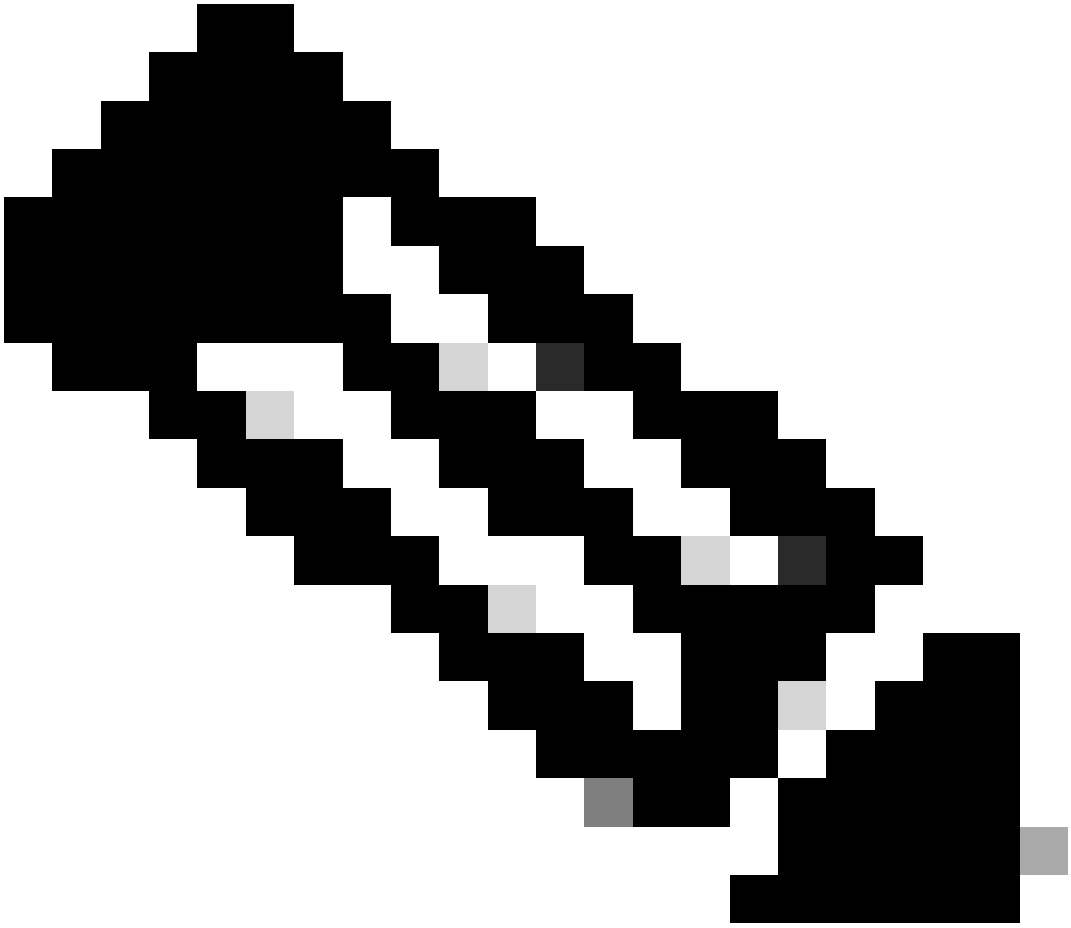
Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure Cisco Aironet APs
- Basic knowledge of SSH and related security concepts

Components Used

The information in this document is based on these software and hardware versions:

- Aironet 1200 Series AP that runs Cisco IOS® Software Release 12.3(8)JEB
- PC or laptop with SSH client utility



Note: This document uses the SSH client utility in order to verify the configuration. You can use any third-party client utility in order to log in to the AP with the use of SSH.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Access the Command-line Interface (CLI) on the Aironet AP

You can use any of these methods in order to access the command-line interface (CLI) on the Aironet AP:

- The console port
- Telnet

- SSH

If the AP has a console port and you have physical access to the AP, you can use the console port in order to log in to the AP and change the configuration if necessary. For information on how to use the console port in order to log in to the AP, refer to the Connecting to the 1200 Series Access Points Locally section of the documentConfigure the Access Point for the First Time.

If you can only access the AP through the Ethernet, use either the Telnet protocol or the SSH protocol in order to log in to the AP.

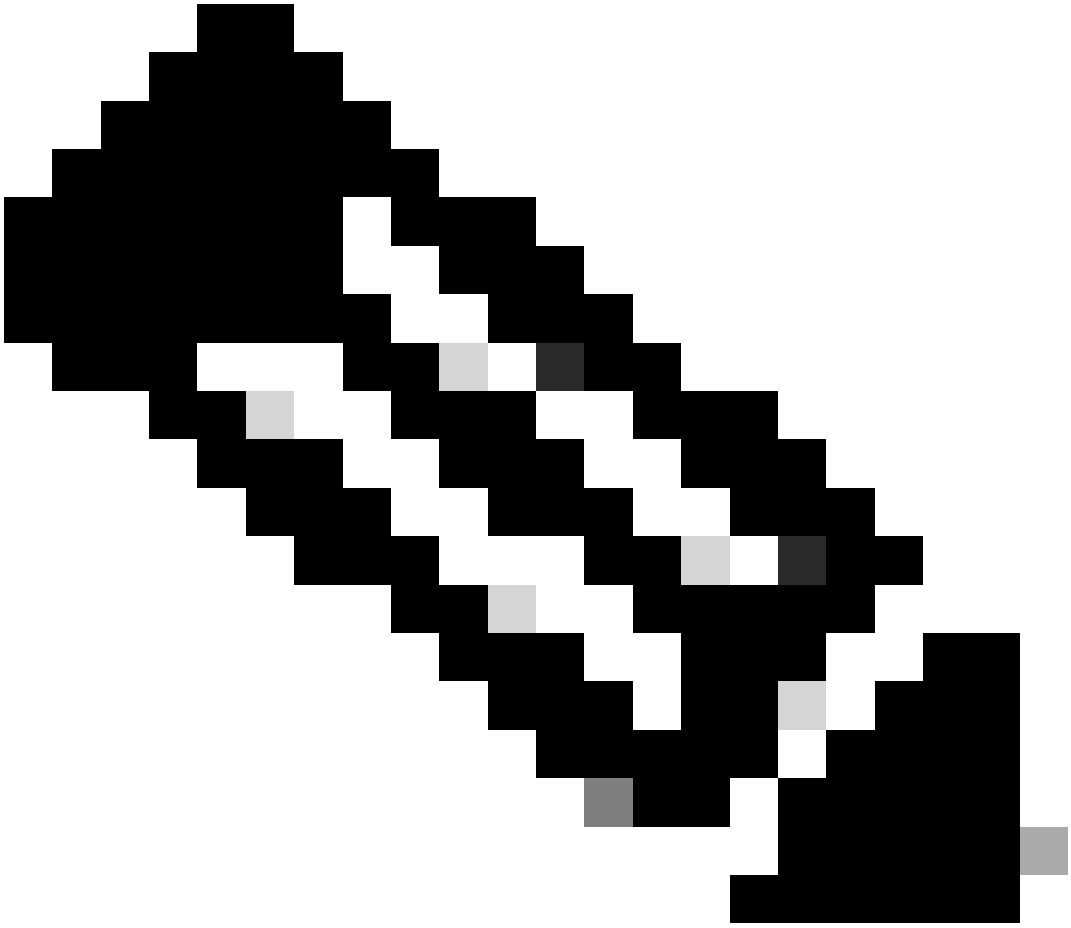
The Telnet protocol uses port 23 for communication. Telnet transmits and receives data in clear text. Because the data communication happens in clear text, a hacker can easily compromise the passwords and access the AP. RFC 854 defines Telnet and extends Telnet with options by many other RFCs.

SSH is an application and protocol that provides a secure replacement to the Berkley r-tools. SSH is a protocol that provides a secure, remote connection to a Layer 2 or a Layer 3 device. There are two versions of SSH: SSH version 1 and SSH version 2. This software release supports both SSH versions. If you do not specify the version number, the AP defaults to version 2.

SSH provides more security for remote connections than Telnet because it provides strong encryption when a device is authenticated. This encryption is an advantage over a Telnet session, in which the communication happens in clear text. For more information on SSH, refer to Secure Shell (SSH) FAQ. The SSH feature has an SSH server and an SSH integrated client.

The client supports these user authentication methods:

- RADIUS
- Local authentication and authorization.



Note: The SSH feature in this software release does not support IP Security (IPSec).

You can configure APs for SSH with the use of either the CLI or GUI. This document explains both methods of configuration.

Configure

CLI Configuration

This section provides the information on how to configure the features with the use of CLI.

Step-by-Step Instructions

In order to enable SSH-based access on the AP, you first must configure the AP as an SSH server. Do these steps in order to configure an SSH server on the AP from CLI:

1. Configure a host name and domain name for the AP.

```
<#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

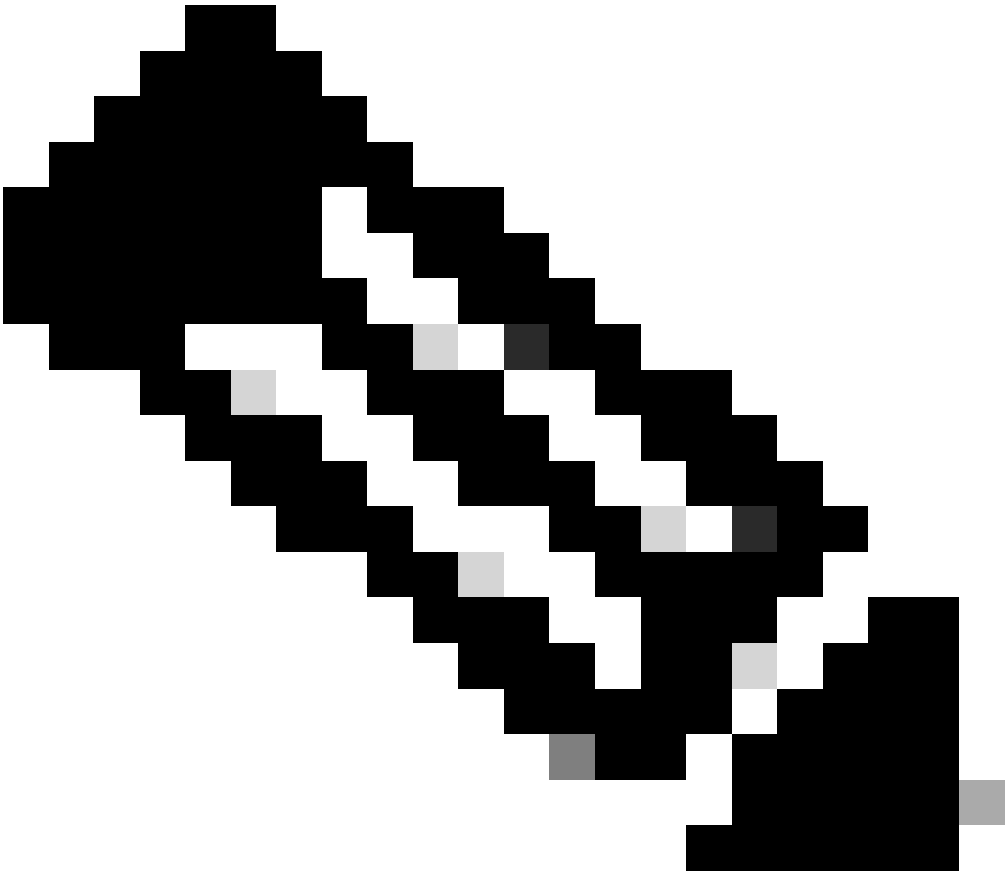
!--- This command configures the AP with the domain name "domain name".
```

2. Generate a Rivest, Shamir, and Adelman (RSA) key for your AP.

   Generation of an RSA key enables SSH on the AP. Issue this command in global configuration mode:

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

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



Note: The recommended minimum RSA key size is 1024.

3. Configure user authentication on the AP.

   On the AP, you can configure user authentication to use either the local list or an external authentication, authorization, and accounting (AAA) server. This example uses a locally generated list in order to authenticate the users:

```
<#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".
```

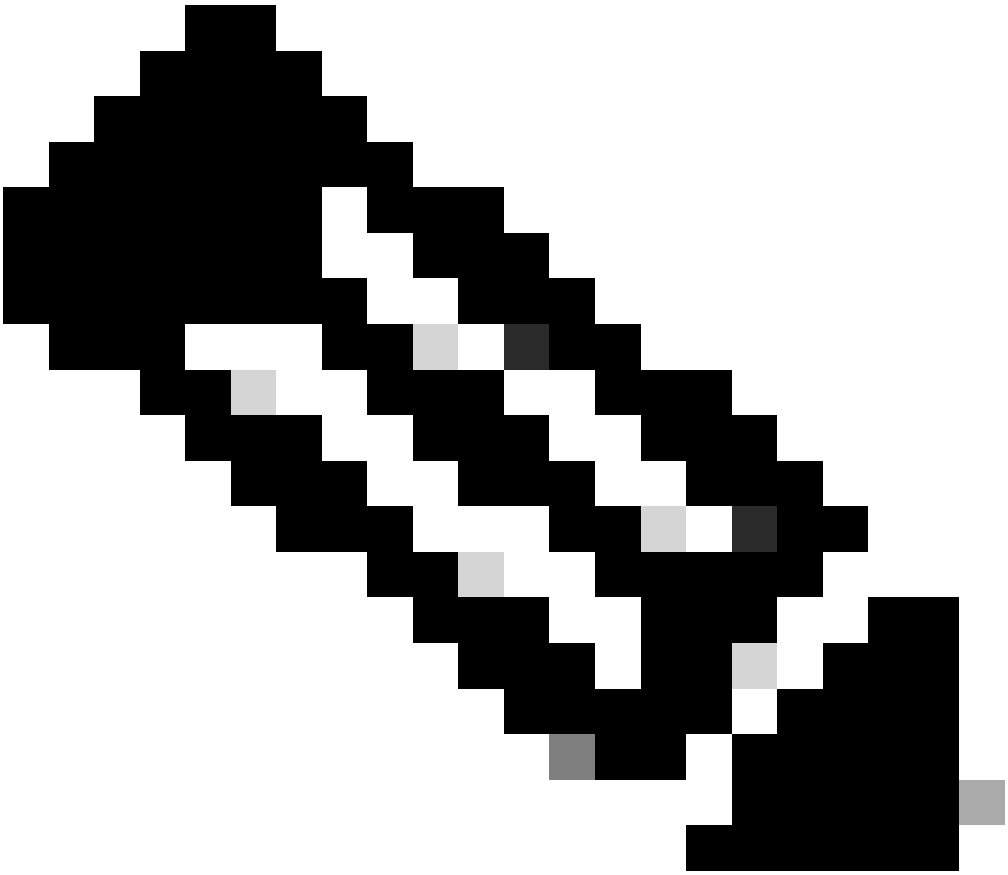
This configuration configures the AP to perform user-based authentication with the use of a local database that is configured on the AP. The example configures two users in the local database, "Test" and "ABC".

4. Configure the SSH parameters.

```
<#root>

Test<config>#
ip ssh {[timeout seconds] | [authentication-retries integer]}

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



Note: You can specify the timeout in seconds, but do not exceed 120 seconds. The default is 120. This the specification that applies to the SSH negotiation phase. You can also specify the number of authentication retries, but do not exceed five authentication retries. The default is three.

GUI Configuration

You can also use the GUI in order to enable SSH-based access on the AP.

Step-by-Step Instructions

Complete these steps:

1. Log in to the AP through the browser.

   The Summary Status window displays.

2. Click **Services** in the menu on the left.

   The Services Summary window displays.

3. Click **Telnet/SSH** in order to enable and configure the Telnet/SSH parameters.

   The Services: Telnet/SSH window displays. Scroll down to the Secure Shell Configuration area. Click **Enable** beside Secure Shell, and enter the SSH parameters as this example shows, using these parameters:

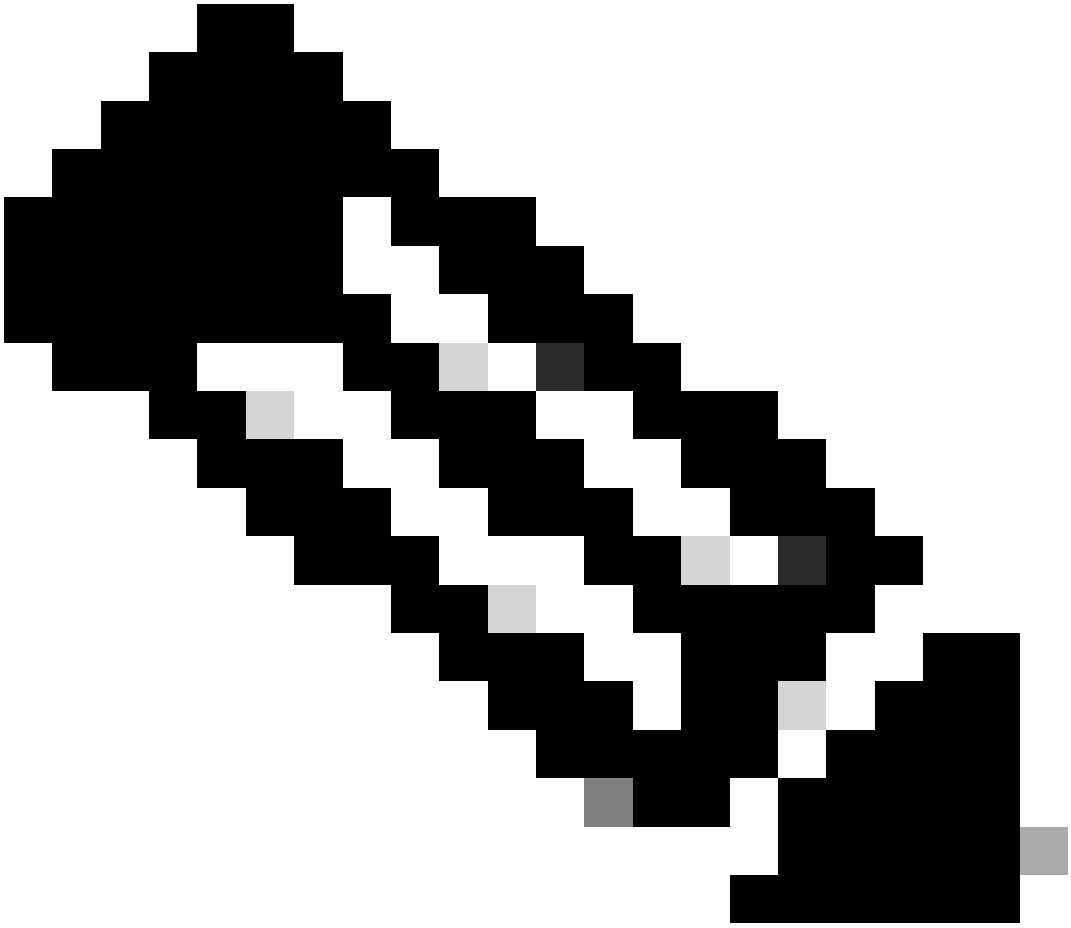
   - System Name: Test
   - Domain Name: DOMAIN
   - RSA Key Size: 1024
   - Authentication Timeout: 120
   - Authentication Retries: 3

4. Click **Apply** in order to save the changes.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.



Note: Only registered Cisco users can access internal Cisco tools and information.

- **show ip ssh**—Verifies if SSH is enabled on the AP and enables you to check the version of SSH that runs on the AP. This output provides an example.
- **show ssh**—Enables you to view the status of your SSH server connections. This output provides an example.

Now, initiate a connection through a PC that runs third-party SSH software and then make an attempt to log in to the AP. This verification uses the AP IP address, 10.0.0.2. Because you have configured the user name Test, use this name in order to access the AP through SSH:

Troubleshoot

Use this section to troubleshoot your configuration.

If your SSH configuration commands are rejected as illegal commands, you have not successfully generated an RSA key pair for your AP.

Disable SSH

In order to disable SSH on an AP, you must delete the RSA pair that is generated on the AP. In order to delete the RSA pair, issue the **crypto key zeroize rsa** command in global configuration mode. When you delete the RSA key pair, you automatically disable the SSH server. This output provides an example.

Related Information

- **Secure Shell (SSH) Support Page**
- **Cisco Technical Support & Downloads**