

在接入点(AP)上启用安全外壳(SSH)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[访问Aironet AP上的命令行界面\(CLI\)](#)

[配置](#)

[CLI 配置](#)

[逐步指导](#)

[GUI 配置](#)

[逐步指导](#)

[验证](#)

[故障排除](#)

[禁用SSH](#)

[相关信息](#)

简介

本文档介绍如何配置接入点(AP)以启用基于Secure Shell (SSH)的访问。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解如何配置Cisco Aironet AP
- 基本了解SSH和相关安全概念

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS®软件版本12.3(8)JEB的Aironet 1200系列AP
- 使用SSH客户端实用程序的PC或笔记本电脑



注意：本文档使用SSH客户端实用程序验证配置。您可以使用SSH使用任何第三方客户端实用程序登录到AP。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

访问Aironet AP上的命令行界面(CLI)

您可以使用以下任何一种方法访问Aironet AP上的命令行界面(CLI)：

- 控制台端口
- Telnet

- SSH

如果AP具有控制台端口，并且您可以实际访问AP，则可以使用控制台端口登录到AP并在必要时更改配置。有关如何使用控制台端口以登录AP的信息，请参阅文档第一次配置接入点的本地连接到1200系列接入点部分。

如果只能通过以太网访问AP，请使用Telnet协议或SSH协议登录AP。

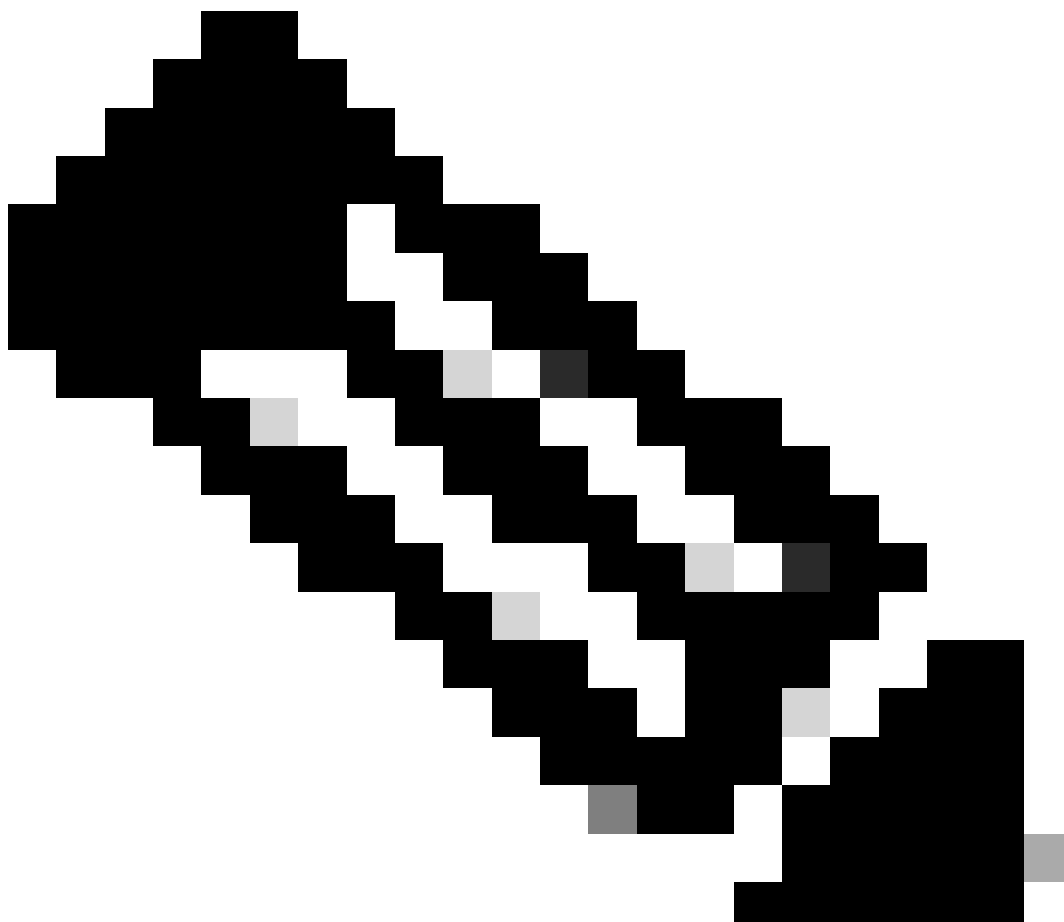
Telnet协议使用端口23进行通信。Telnet以明文形式传输和接收数据。由于数据通信采用明文形式，因此黑客很容易入侵密码和访问AP。[RFC 854](#)对Telnet进行了定义，并通过许多其他的RFC提供的选项对Telnet进行了扩展。

SSH是一种可安全替代Berkley r-tools的应用和协议。SSH是一种提供到第2层或第3层设备的安全远程连接的协议。SSH有两个版本：SSH第1版和SSH第2版。此软件版本支持两个SSH版本。如果不指定版本号，则AP默认为版本2。

与Telnet相比，SSH为远程连接提供了更高的安全性，因为它在设备通过身份验证时提供了强加密。与Telnet会话相比，这种加密的优点是通信采用明文形式。有关SSH的详细信息，请参阅[安全外壳\(SSH\)常见问题](#)。SSH功能具有SSH服务器和SSH集成客户端。

客户端支持以下用户身份验证方法：

- RADIUS
- 本地身份验证和授权。



注意：此软件版本中的SSH功能不支持IP安全(IPSec)。

您可以使用CLI或GUI为SSH配置AP。本文档介绍了这两种配置方法。

配置

CLI 配置

本节提供有关如何使用CLI配置功能的信息。

逐步指导

要在AP上启用基于SSH的访问，必须先将AP配置为SSH服务器。要从CLI在AP上配置SSH服务器，请执行以下步骤：

1. 配置AP的主机名和域名。

```
<#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. 为AP生成Rivest、Shamir和Adelman (RSA)密钥。

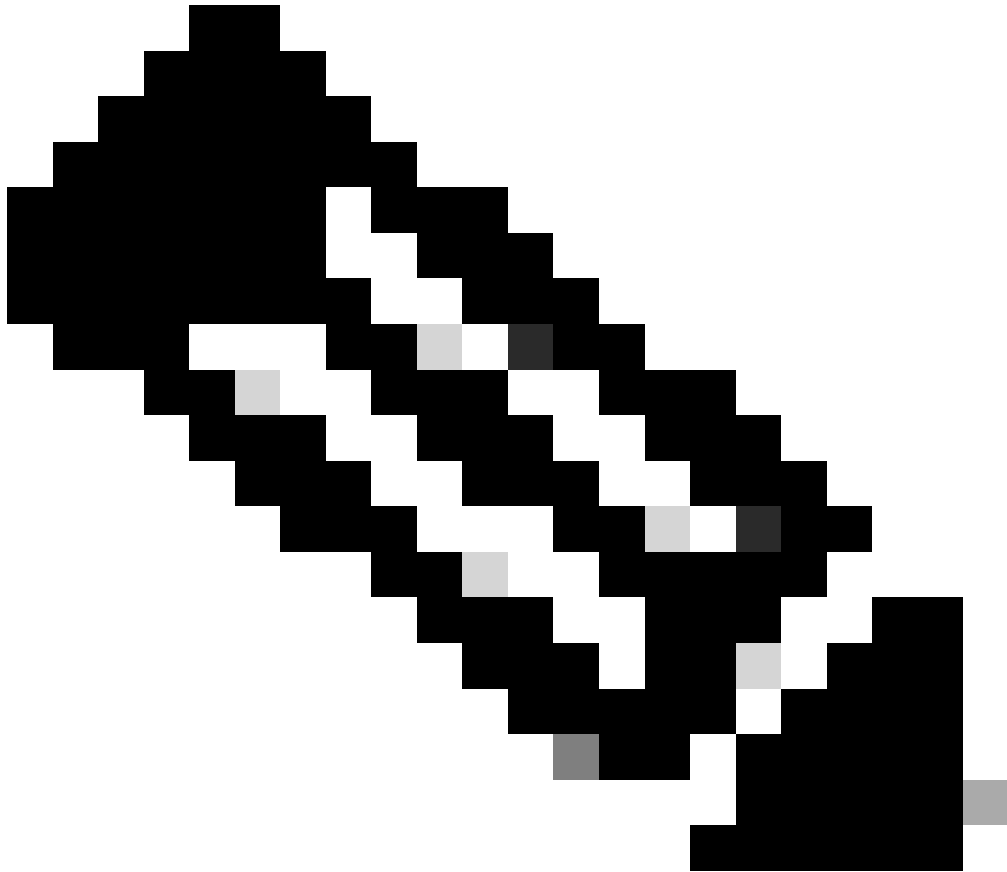
生成RSA密钥会在AP上启用SSH。在全局配置模式下发出以下命令：

```
<#root>
```

```
Test<config>#
```

```
crypto key generate rsa rsa_key_size
```

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



注意：建议的最小RSA密钥大小为1024。

3. 在AP上配置用户身份验证。

在AP上，可以将用户身份验证配置为使用本地列表或外部身份验证、授权和记帐(AAA)服务器。此示例使用本地生成的列表对用户进行身份验证：

```
<#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.
```

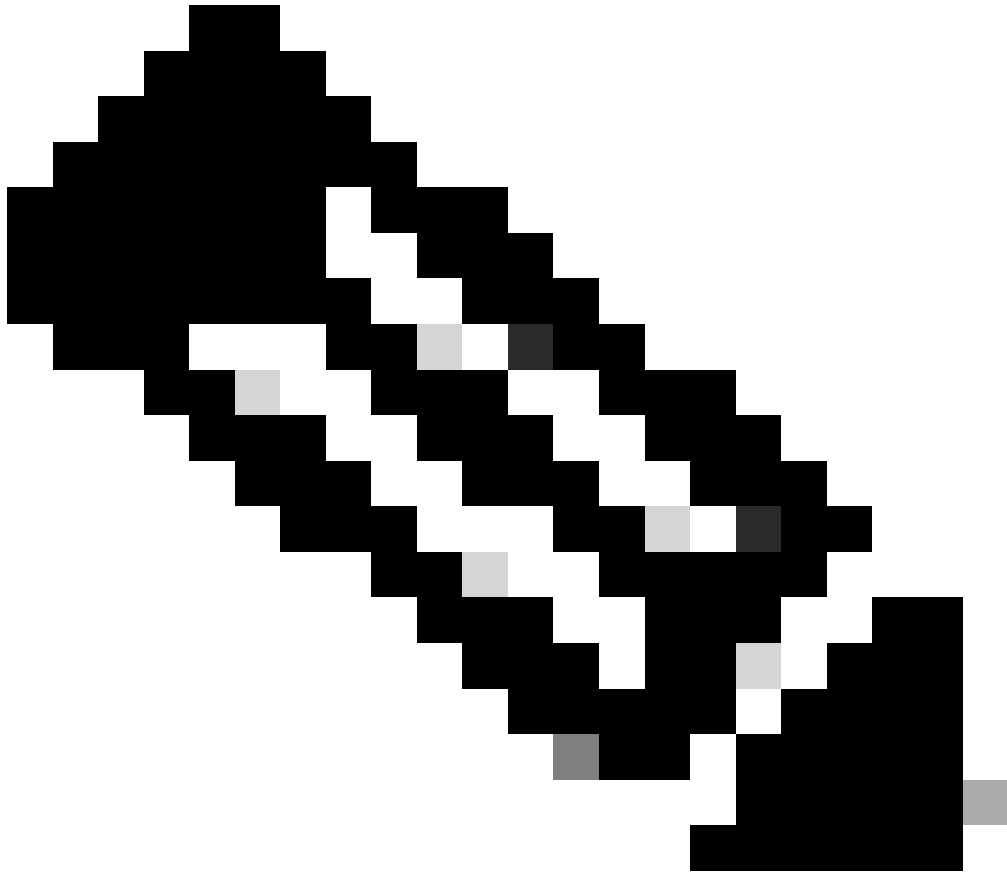
```
Test<config>#  
username Test password Test123  
  
!--- Configure a user with the name "Test".
```

```
Test<config>#  
username ABC password xyz123  
  
!--- Configure a second user with the name "Domain".
```

此配置将AP配置为使用在AP上配置的本地数据库执行基于用户的身份验证。该示例在本地数据库中配置两个用户，即“Test”和“ABC”。

4. 配置SSH参数

```
<#root>  
Test<config>#  
ip ssh {[timeout seconds] | [authentication-retries integer]}  
  
!--- Configure the SSH control variables on the AP.
```



注意：您可以指定超时（以秒为单位），但不能超过120秒。默认值为 120。此规范适用于SSH协商阶段。您还可以指定身份验证重试次数，但不要超过五次身份验证重试。默认值为3。

GUI 配置

也可以使用GUI在AP上启用基于SSH的访问。

逐步指导

请完成以下步骤：

1. 通过浏览器登录AP。

此时将显示“汇总状态”窗口。

2. 在左侧的菜单中单击Services。

系统随即会显示“服务摘要”窗口。

3. 单击Telnet/SSH以启用和配置Telnet/SSH参数。

系统随即会显示“服务：Telnet/SSH”窗口。向下滚动到Secure Shell Configuration区域。单击Secure Shell旁的Enable，然后输入SSH参数，如此示例所示：

本示例使用以下参数：

- 系统名称：Test
- 域名：域
- RSA密钥大小：1024
- 身份验证超时：120
- 身份验证重试次数：3

4. 单击 Apply 以保存更改。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序工具(OIT)支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

注意：只有思科注册用户才能访问思科内部工具和信息。

- `show ip ssh`— 验证AP上是否启用了SSH，并允许您检查AP上运行的SSH的版本。此输出提供一个示例：
- `show ssh` —允许您查看SSH服务器连接的状态。此输出提供一个示例：

现在，通过运行第三方SSH软件的PC启动连接，然后尝试登录到AP。此验证使用AP IP地址10.0.0.2。由于您已配置用户名Test，因此请使用此名称通过SSH访问AP：

故障排除

使用本部分可排除配置故障。

如果您的SSH配置命令被拒绝为非法命令，则您尚未成功生成AP的RSA密钥对。

禁用SSH

要在AP上禁用SSH，必须删除AP上生成的RSA对。要删除RSA对，请在全局配置模式下发出crypto key zeroize rsa命令。删除RSA密钥对时，将自动禁用SSH服务器。此输出提供一个示例：

相关信息

- [安全外壳\(SSH\)支持页](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。