

在存取點(AP)上啟用安全殼層(SSH)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[訪問Aironet AP上的命令列介面\(CLI\)](#)

[設定](#)

[CLI配置](#)

[逐步說明](#)

[GUI配置](#)

[逐步說明](#)

[驗證](#)

[疑難排解](#)

[停用SSH](#)

[相關資訊](#)

簡介

本文說明如何設定存取點(AP)，以啟用安全殼層(SSH)型存取。

必要條件

需求

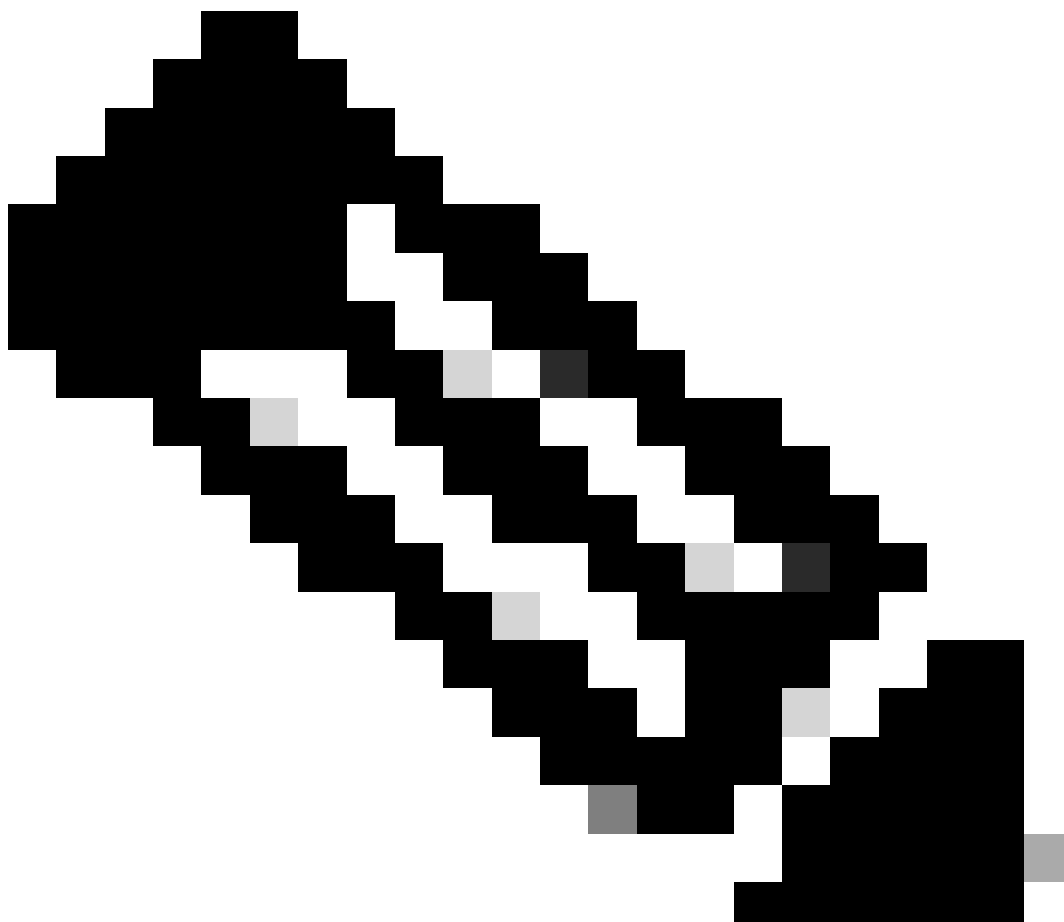
嘗試此組態之前，請確保符合以下要求：

- 瞭解如何配置Cisco Aironet AP
- SSH及相關安全概念的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS®軟體版本12.3(8)JEB的Aironet 1200系列AP
- 具有SSH客戶端實用程式的PC或筆記型電腦



注意：本文檔使用SSH客戶端實用程式來驗證配置。您可以使用任何第三方客戶端實用程式來使用SSH登入AP。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

訪問Aironet AP上的命令列介面(CLI)

可使用以下任何一種方法訪問Aironet AP上的命令列介面(CLI)：

- 控制檯埠
- Telnet

- SSH

如果AP具有控制檯埠，並且您可以實際訪問AP，則可以使用控制檯埠登入AP並在必要時更改配置。有關如何使用控制檯埠登入到AP的資訊，請參閱文檔第一次配置存取點中的本地連線到1200系列存取點部分。

如果只能透過乙太網訪問AP，請使用Telnet協定或SSH協定登入AP。

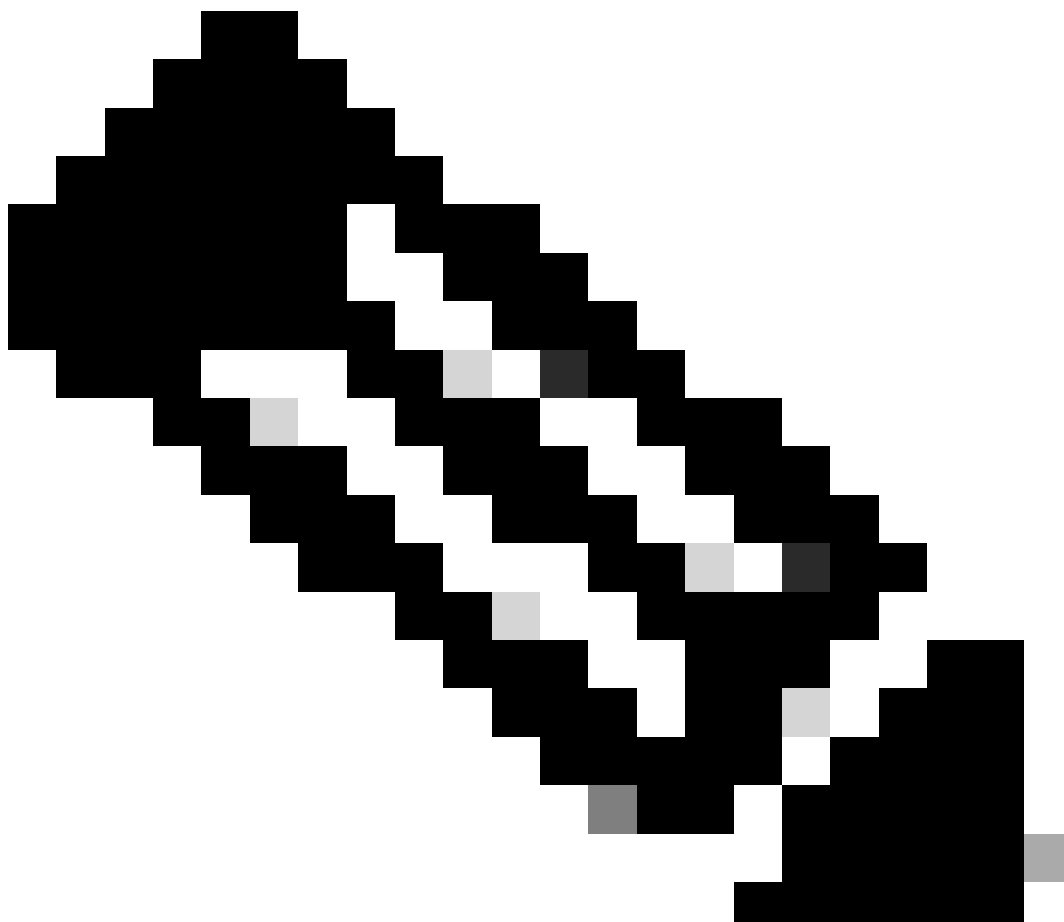
Telnet通訊協定使用連線埠23進行通訊。Telnet以明文形式傳輸和接收資料。由於資料通訊採用明文形式，因此駭客很容易便會入侵密碼和訪問AP。[RFC 854](#) 對Telnet進行了定義，並透過許多其他的RFC的選項擴展Telnet。

SSH是一種應用和協定，可為Berkley r-tools提供安全的替代方案。SSH是一種提供到第2層或第3層裝置的安全遠端連線的協定。SSH有兩個版本：SSH版本1和SSH版本2。此軟體版本支援兩個SSH版本。如果未指定版本號，則AP預設為版本2。

與Telnet相比，SSH為遠端連線提供了更高的安全性，因為它在裝置透過身份驗證時提供了強加密。與Telnet會話相比，這種加密是一種優勢，在該會話中，通訊以明文形式進行。有關SSH的詳細資訊，請參閱[安全外殼\(SSH\)常見問題](#)。SSH功能具有SSH伺服器和SSH整合客戶端。

客戶端支援以下使用者身份驗證方法：

- RADIUS
- 本地身份驗證和授權。



注意：此軟體版本中的SSH功能不支援IP Security (IPSec)。

可以使用CLI或GUI為SSH配置AP。本檔案將說明兩種組態方法。

設定

CLI配置

本部分提供有關如何使用CLI配置功能的資訊。

逐步說明

要在AP上啟用基於SSH的訪問，必須先將AP配置為SSH伺服器。要從CLI在AP上配置SSH伺服器，請執行以下步驟：

1. 配置AP的主機名和域名。

```
<#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. 為AP生成Rivest、Shamir和Adelman (RSA)金鑰。

生成RSA金鑰可在AP上啟用SSH。在全局配置模式下發出以下命令：

```
<#root>
```

```
Test<config>#
```

```
crypto key generate rsa rsa_key_size
```

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

註：建議的最小RSA金鑰大小為1024。

3. 在AP上配置使用者身份驗證。

在AP上，可以將使用者身份驗證配置為使用本地清單或外部身份驗證、授權和記帳(AAA)伺服器。此範例使用本機產生的清單對使用者進行驗證：

```
<#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.
```

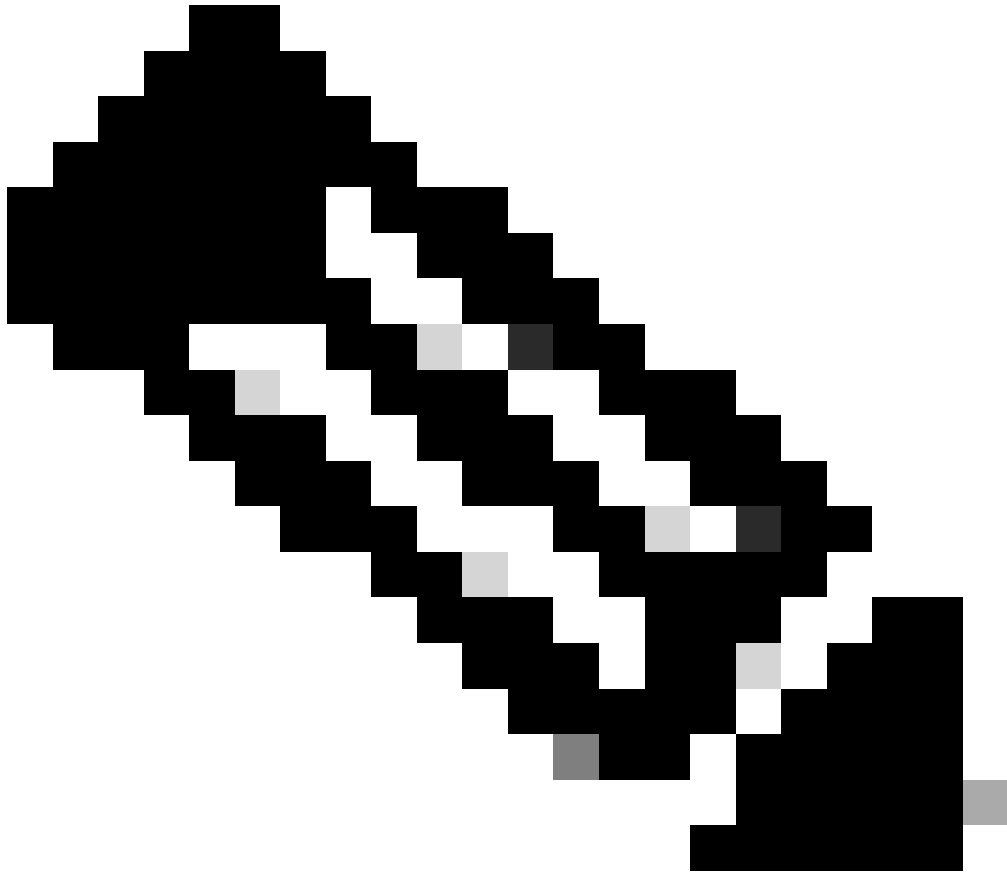
```
Test<config>#  
username Test password Test123  
  
!--- Configure a user with the name "Test".
```

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

此配置將AP配置為使用在AP上配置的本地資料庫來執行基於使用者的身份驗證。該示例在本地資料庫中配置兩個使用者，即「Test」和「ABC」。

4. 配置SSH引數。

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



注意：您可以指定逾時（秒），但不得超過120秒。預設值為120。這是適用於SSH協商階段的規範。您也可以指定驗證重試次數，但驗證重試次數不能超過五次。預設值為3。

GUI配置

還可以使用GUI在AP上啟用基於SSH的訪問。

逐步說明

請完成以下步驟：

1. 透過瀏覽器登入到AP。
「彙總狀態」視窗會出現。
2. 在左側的選單中按一下Services。
將顯示「服務摘要」窗口。

3. 按一下Telnet/SSH以啟用和配置Telnet/SSH引數。

系統隨即會顯示「服務：Telnet/SSH」窗口。向下滾動到Secure Shell Configuration區域。按一下Secure Shell旁邊的Enable，然後輸入SSH引數，如以下示例所示：

此範例使用下列引數：

- 系統名稱：測試
- 網域名稱：網域
- RSA金鑰大小：1024
- 身份驗證超時：120
- 驗證重試次數：3

4. 按一下Apply 以儲存更改。

驗證

使用本節內容，確認您的組態是否正常運作。

命令輸出解釋程式工具(OIT)支援某些 show 命令。使用OIT檢視對show命令輸出的分析。

附註：只有完成註冊的思科使用者能存取思科內部工具與資訊。

- `show ip ssh`— 驗證是否在AP上啟用SSH，並允許您檢查AP上運行的SSH版本。此輸出提供範例：
- `show ssh` -可用於檢視SSH伺服器連線的狀態。此輸出提供範例：

現在，透過運行第三方SSH軟體的PC啟動連線，然後嘗試登入到AP。此驗證使用AP IP地址10.0.0.2。由於您已配置使用者名稱Test，因此請使用此名稱，以便透過SSH訪問AP：

疑難排解

使用本節內容，對組態進行疑難排解。

如果您的SSH配置命令被拒絕為非法命令，您尚未成功為AP生成RSA金鑰對。

停用SSH

要在AP上停用SSH，必須刪除AP上生成的RSA對。要刪除RSA對，請在全局配置模式下發出crypto key zeroize rsa命令。刪除RSA金鑰對時，會自動停用SSH伺服器。此輸出提供範例：

相關資訊

- [安全殼層\(SSH\)支援頁面](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。