

Abilitare Secure Shell (SSH) su un access point (AP)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Accedere all'interfaccia della riga di comando \(CLI\) sull'access point Aironet](#)

[Configurazione](#)

[Configurazione dalla CLI](#)

[Istruzioni dettagliate](#)

[Configurazione GUI](#)

[Istruzioni dettagliate](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Disabilitazione SSH](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare un access point (AP) in modo da abilitare l'accesso basato su SSH (Secure Shell).

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

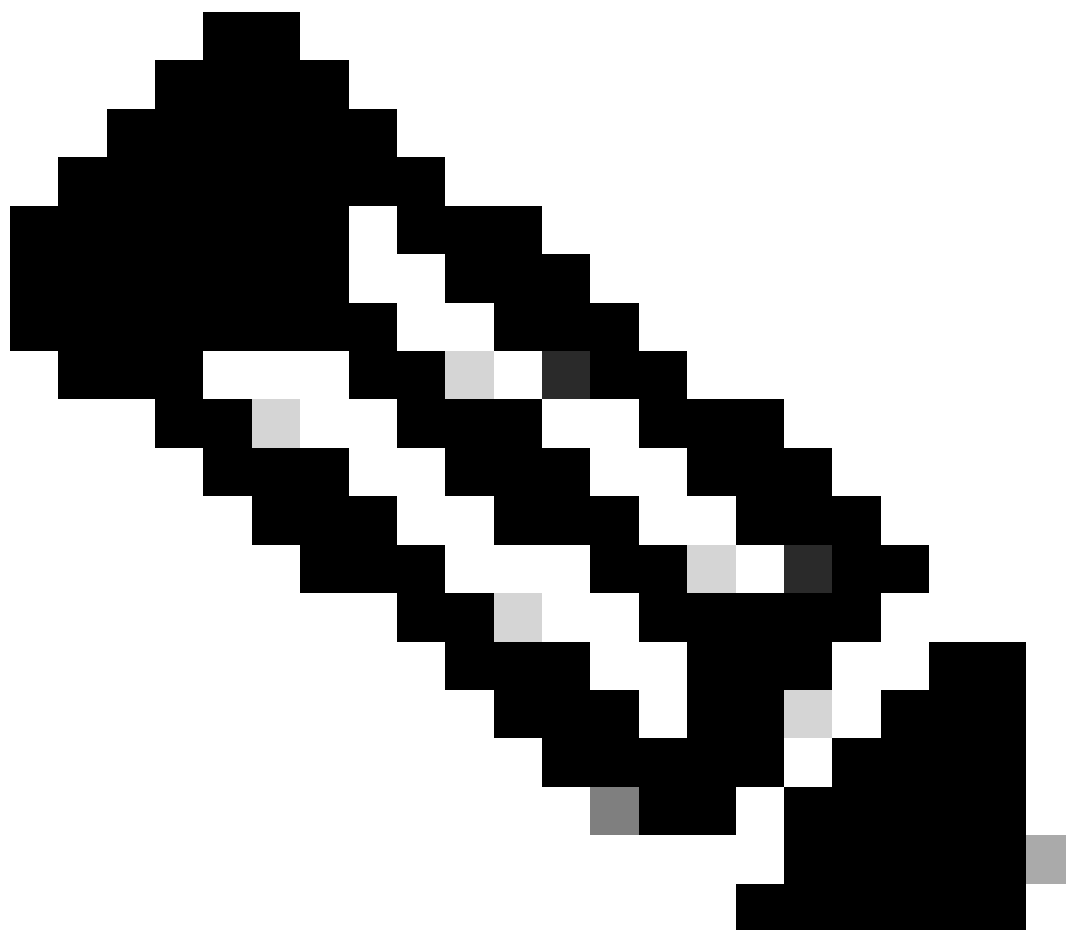
- Informazioni su come configurare i Cisco Aironet AP
- Conoscenze base di SSH e dei concetti di sicurezza correlati

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Aironet serie 1200 AP con software Cisco IOS® versione 12.3(8)JEB

- PC o portatile con SSH client utility
-



Nota: per verificare la configurazione, questo documento utilizza l'utility del client SSH. Per accedere all'access point con SSH, è possibile usare qualsiasi utility client di terze parti.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Accedere all'interfaccia della riga di comando (CLI) sull'access point Aironet

Per accedere all'interfaccia della riga di comando (CLI) sull'access point Aironet, è possibile utilizzare uno dei seguenti metodi:

- Porta della console
- Telnet
- SSH

Se l'access point è dotato di una porta console e si dispone di accesso fisico all'access point, è possibile utilizzare la porta console per accedere all'access point e modificare la configurazione, se necessario. Per informazioni su come utilizzare la porta console per accedere al punto di accesso, fare riferimento alla sezione Connessione ai punti di accesso serie 1200 in locale del documento Configurazione del punto di accesso per la prima volta.

Se l'accesso all'access point è possibile solo tramite Ethernet, usare il protocollo Telnet o il protocollo SSH per accedere all'access point.

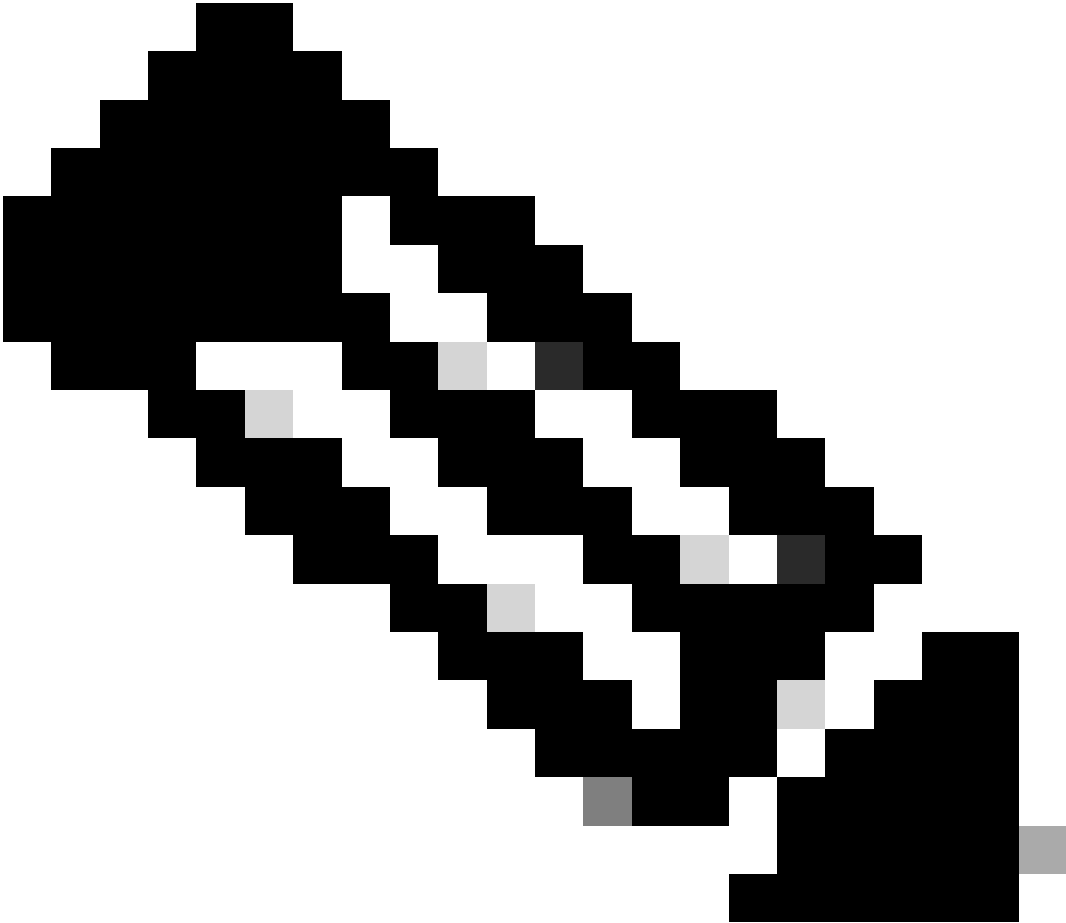
Il protocollo Telnet utilizza la porta 23 per la comunicazione. Telnet trasmette e riceve i dati in formato testo non crittografato. Poiché la comunicazione dei dati avviene in testo non crittografato, un hacker può facilmente compromettere le password e accedere all'access point. La [RFC 854](#) definisce Telnet ed estende Telnet con opzioni di molte altre RFC.

SSH è un'applicazione e un protocollo che sostituisce in modo sicuro gli r-tool Berkley. SSH è un protocollo che permette di connettersi in modo sicuro e remoto a un dispositivo di livello 2 o 3. SSH è disponibile in due versioni: SSH versione 1 e SSH versione 2. Questa versione del software supporta entrambe le versioni SSH. Se non si specifica il numero di versione, l'access point utilizza per impostazione predefinita la versione 2.

SSH offre una maggiore sicurezza per le connessioni remote rispetto a Telnet, in quanto fornisce una crittografia avanzata quando un dispositivo viene autenticato. Questa crittografia è un vantaggio rispetto a una sessione Telnet, in cui la comunicazione avviene in testo non crittografato. Per ulteriori informazioni sul protocollo SSH, consultare le [domande frequenti su Secure Shell \(SSH\)](#). La funzionalità SSH ha un server SSH e un client integrato SSH.

Il client supporta i seguenti metodi di autenticazione utente:

- RAGGIO
- Autenticazione e autorizzazione locali.



Nota: la funzione SSH in questa versione del software non supporta IPsec (IP Security).

È possibile configurare gli AP per SSH usando la CLI o la GUI. Questo documento spiega entrambi i metodi di configurazione.

Configurazione

Configurazione dalla CLI

Questa sezione fornisce le informazioni su come configurare le funzionalità con l'uso di CLI.

Istruzioni dettagliate

Per abilitare l'accesso basato su SSH sull'access point, è necessario prima configurare l'access point come server SSH. Per configurare un server SSH sull'access point dalla CLI, attenersi alla seguente procedura:

1. Configurare un nome host e un nome di dominio per l'access point.

```
<#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

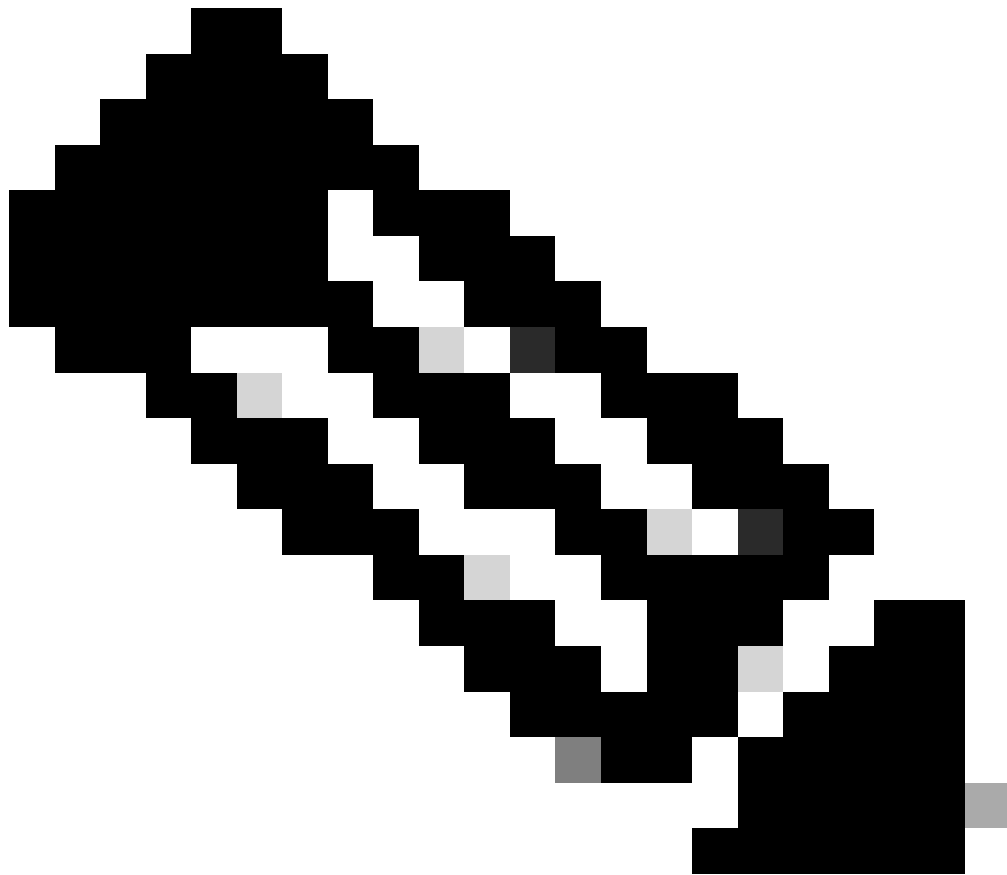
!--- This command configures the AP with the domain name "domain name".
```

2. Generare una chiave Rivest, Shamir e Adelman (RSA) per l'access point.

La generazione di una chiave RSA abilita il protocollo SSH sull'access point. Utilizzare questo comando in modalità di configurazione globale:

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

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



Nota: la dimensione minima consigliata per la chiave RSA è 1024.

3. Configurare l'autenticazione utente sull'access point.

Nell'access point è possibile configurare l'autenticazione dell'utente per l'utilizzo dell'elenco locale o di un server di autenticazione, autorizzazione e accounting (AAA) esterno. In questo esempio viene utilizzato un elenco generato localmente per autenticare gli utenti:

```
<#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".

Questa configurazione configura l'access point per eseguire l'autenticazione basata sull'utente con l'uso di un database locale configurato sull'access point. Nell'esempio vengono configurati due utenti nel database locale, "Test" e "ABC".

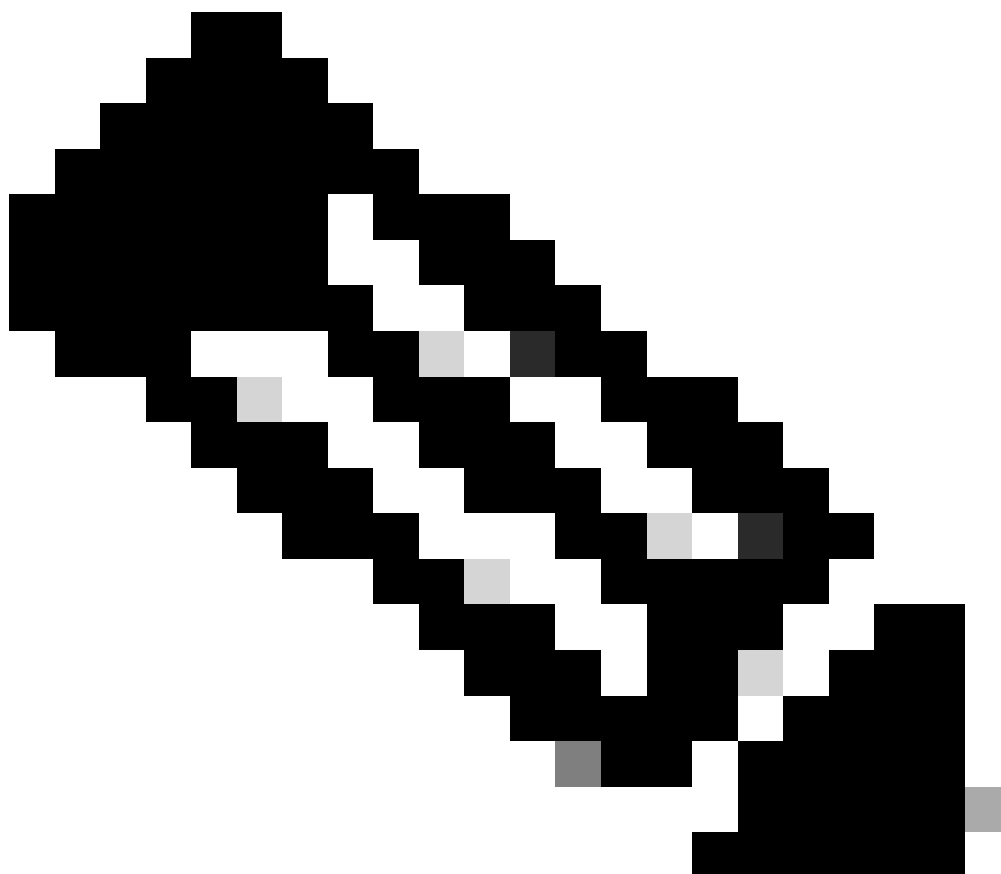
4. Configurare i parametri SSH.

<#root>

Test<config>#

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

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



Nota: è possibile specificare il timeout in secondi, ma non superare i 120 secondi. Il valore predefinito è 120. Questa è la specifica che si applica alla fase di negoziazione SSH. È inoltre possibile specificare il numero di tentativi di autenticazione, ma non superare i cinque. Il valore predefinito è tre.

Configurazione GUI

È possibile anche usare la GUI per abilitare l'accesso basato su SSH sull'access point.

Istruzioni dettagliate

Attenersi alla seguente procedura:

1. Accedere all'access point tramite il browser.

Viene visualizzata la finestra Stato riepilogo.

2. Fare clic su Services (Servizi) nel menu a sinistra.

Viene visualizzata la finestra Riepilogo servizi.

3. Per abilitare e configurare i parametri Telnet/SSH, fare clic su Telnet/SSH.

Viene visualizzata la finestra Services: Telnet/SSH. Scorrere verso il basso fino all'area di configurazione Secure Shell. Fare clic su Enable accanto a Secure Shell e immettere i parametri SSH, come mostrato nell'esempio:

In questo esempio vengono utilizzati i seguenti parametri:

- Nome sistema: Test
- Nome dominio: DOMAIN
- Dimensione chiave RSA: 1024
- Timeout autenticazione: 120
- Tentativi di autenticazione: 3

4. Per salvare le modifiche, fare clic su Apply (Applica).

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (OIT) supporta alcuni comandi show. Usare OIT per visualizzare un'analisi dell'output del comando show.



Nota: solo gli utenti Cisco registrati possono accedere alle informazioni e agli strumenti Cisco interni.

-
- `show IP ssh`: verifica se SSH è abilitato sull'access point e consente di controllare la versione di SSH in esecuzione sull'access point. Questo output offre un esempio:
 - `show ssh`: consente di visualizzare lo stato delle connessioni del server SSH. Questo output offre un esempio:

A questo punto, avviare una connessione tramite un PC con software SSH di terze parti e tentare di accedere all'access point. Per questa verifica viene utilizzato l'indirizzo IP dell'access point, 10.0.0.2. Poiché è stato configurato il nome utente Test, utilizzare questo nome per accedere all'access point tramite SSH:

Risoluzione dei problemi

Consultare questa sezione per risolvere i problemi di configurazione.

Se i comandi della configurazione SSH sono rifiutati come non validi, la coppia di chiavi RSA per l'access point non è stata generata correttamente.

Disabilitazione SSH

Per disabilitare SSH su un access point, è necessario eliminare la coppia RSA generata sull'access point. Per eliminare la coppia RSA, usare il comando `crypto key zeroize rsa` in modalità di configurazione globale. Quando si elimina la coppia di chiavi RSA, il server SSH viene disabilitato automaticamente. Questo output offre un esempio:

Informazioni correlate

- [Pagina di supporto Secure Shell \(SSH\)](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).