

Domande frequenti (SSH) su Secure Shell

Sommario

[Introduzione](#)

[Come configurare l'accesso alla linea terminale SSH \(nota anche come reverse telnet\)?](#)

[Il protocollo SSH è supportato su Catalyst 2900?](#)

[Come posso determinare quali piattaforme e versioni del codice supportano SSH?](#)

[Quando cerco di rimuovere alcuni comandi SSH dal router, continuo a chiedere di creare le chiavi RSA per abilitare SSH. Perché?](#)

[Cisco IOS SSH versione 2 supporta Digital Signature Standard \(DSS\)?](#)

[Il server SSH Cisco IOS supporta l'inoltro di agenti?](#)

[Quali meccanismi di autenticazione client sono supportati sul server SSH Cisco IOS?](#)

[Qual è l'errore Local: Byte di controllo danneggiati in input?](#)

[Cisco IOS supporta SSH con la cifratura Blowfish?](#)

[Quando si cerca di generare le chiavi RSA per l'accesso SSH su un router usando il comando `crypto key generate rsa` in modalità di configurazione, viene visualizzato questo errore: `% Input non valido rilevato in corrispondenza del marcatore '^`. Il router non può generare le chiavi RSA per abilitare l'accesso SSH al router. Come viene risolto questo errore?](#)

[Le immagini crittografiche supportano la crittografia avanzata per l'utilizzo del protocollo SSH con cifrature come 3DES o AES?](#)

[Quando si cerca di configurare SSH su un router, nei log vengono visualizzati i seguenti messaggi: `SSH2 13: Firma RSA: chiave privata non trovata` e `SSH2 13: creazione della firma non riuscita, stato -1`. Come viene risolto?](#)

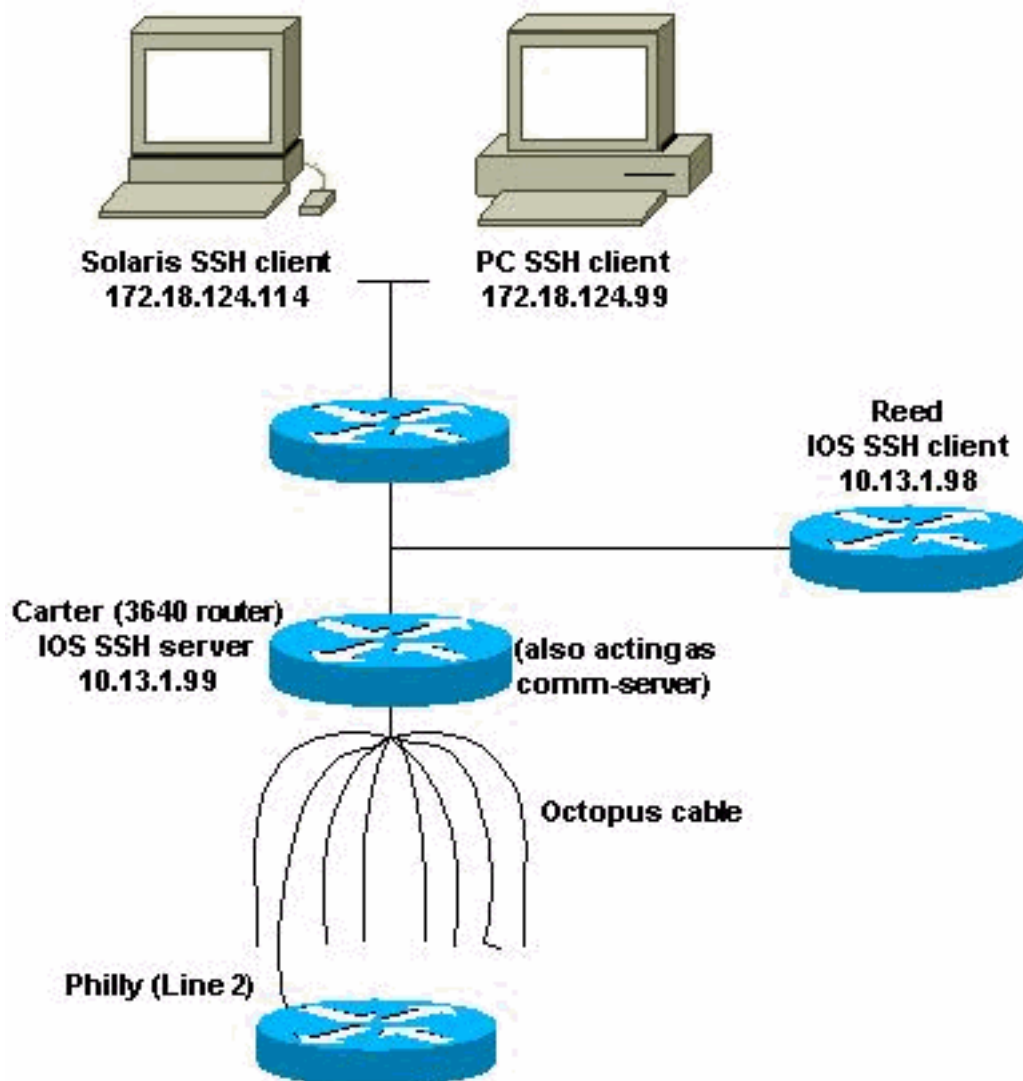
[Informazioni correlate](#)

Introduzione

Questo documento risponde alle domande più frequenti (FAQ) relative a Secure Shell (SSH). Il codice SSH Cisco IOS[®] è il codice originale Cisco.

Come configurare l'accesso alla linea terminale SSH (nota anche come reverse telnet)?

Questa funzionalità è stata introdotta per la prima volta in alcune piattaforme del software Cisco IOS versione 12.2.2.T.



```
Router(config)#line line-number [ending-line-number]
Router(config-line)#no exec
Router(config-line)#login {local | authentication listname
Router(config-line)#rotary group
Router(config-line)#transport input {all | ssh}
Router(config-line)#exit
Router(config)#ip ssh port portnum rotary group
```

```
!--- Line 1 SSH Port Number 2001 line 1 no exec login authentication default rotary 1 transport
input ssh !--- Line 2 SSH Port Number 2002 line 2 no exec login authentication default rotary 2
transport input ssh !--- Line 3 SSH Port Number 2003 line 3 no exec login authentication default
rotary 3 transport input ssh ip ssh port 2001 rotary 1 3
```

Riferimento per i comandi

```
ip ssh port
ip ssh port portnum rotary group
no ip ssh port portnum rotary group
```

- portnum: per specificare la porta a cui deve connettersi SSH, ad esempio 2001.
- rotary group - Specifica il rotary definito che deve cercare un nome valido.

Il protocollo SSH è supportato su Catalyst 2900?

No.

Come posso determinare quali piattaforme e versioni del codice supportano SSH?

Vedere [Feature Navigator](#) (solo utenti [registrati](#)) e specificare la funzione SSH.

Quando cerco di rimuovere alcuni comandi SSH dal router, continuo a chiedere di creare le chiavi RSA per abilitare SSH. Perché?

Di seguito è riportato un esempio di questo problema:

```
804#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
804(config)#no ip ssh time-out 120
Please create RSA keys to enable SSH.
804(config)#no ip ssh authen
Please create RSA keys to enable SSH.
804(config)
```

Si è verificato un errore Cisco con ID [CSCdv70159](#) (solo utenti [registrati](#)).

Cisco IOS SSH versione 2 supporta Digital Signature Standard (DSS)?

Cisco IOS SSH versione 2 non supporta DSS.

Il server SSH Cisco IOS supporta l'inoltro di agenti?

Cisco IOS SSH non supporta l'inoltro agente. Interagisce con tutte le implementazioni SSH commerciali.

Quali meccanismi di autenticazione client sono supportati sul server SSH Cisco IOS?

Cisco IOS SSH versione 2 (SSHv2) supporta metodi di autenticazione interattivi da tastiera e basati su password. Oltre a questi metodi di autenticazione, la funzione Miglioramenti SSHv2 per le chiavi RSA (disponibile nel software Cisco IOS versione 15.0(1)M e successive) supporta l'autenticazione con chiave pubblica basata su RSA per il client e il server. Per ulteriori informazioni sui meccanismi di autenticazione supportati dal server SSH Cisco IOS, fare riferimento al [supporto Secure Shell versione 2](#).

Qual è l'errore `Local: Byte di controllo danneggiati in media input?`

Checkbyte danneggiati indica che il pacchetto SSH ricevuto non ha superato il controllo di integrità. Questo problema è in genere causato da una decrittografia non corretta. Ciò è dovuto anche all'utilizzo di una chiave non corretta. La chiave errata è causata dal rifiuto di un pacchetto SSH crittografato. È stato scartato un pacchetto crittografato che avrebbe dovuto essere inviato oppure un pacchetto crittografato ricevuto che avrebbe dovuto essere decrittografato.

Cisco IOS supporta SSH con la cifratura Blowfish?

Cisco IOS non supporta SSH con cifratura Blowfish. Quando un client SSH invia una crittografia non supportata, il router visualizza i messaggi di debug menzionati in [SSH-Sends Unsupported \(Blowfish\)](#).

Quando si prova a generare le chiavi RSA per l'accesso SSH su un router con il comando `crypto key generate rsa` in modalità di configurazione, viene visualizzato questo errore: `% Input non valido rilevato in corrispondenza del marcatore '^'..` Il router non può generare le chiavi RSA per abilitare l'accesso SSH al router. Come viene risolto questo errore?

Questo errore viene visualizzato quando l'immagine utilizzata sul router non supporta il comando `crypto key generate rsa`. Questo comando è supportato solo nelle immagini di sicurezza. Per risolvere questo errore, utilizzare l'immagine di sicurezza della serie appropriata del router Cisco IOS in uso.

Le immagini crittografiche supportano la crittografia avanzata per l'utilizzo del protocollo SSH con cifrature come 3DES o AES?

Sì. Solo le immagini crittografate supportano la crittografia avanzata. Per utilizzare il protocollo SSH con cifrari come 3DES o AES, è necessario avere immagini Crypto sul dispositivo Cisco.

Quando si cerca di configurare SSH su un router, nei log vengono visualizzati i seguenti messaggi: `SSH2 13: _Firma RSA: chiave privata non trovata` e `SSH2 13: creazione della firma non riuscita, stato -1`. Come viene risolta?

I messaggi di registro sono stati visualizzati a causa degli ID bug Cisco CSCsa83601 (solo utenti [registrati](#)) e [CSCtc41114](#) (solo utenti [registrati](#)). Per ulteriori informazioni, fare riferimento a questi bug.

Informazioni correlate

- [Pagina di supporto SSH](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)