

Preguntas Frecuentes sobre Secure Shell (SSH)

Contenido

[Introducción](#)

[¿Cómo configuro el acceso de línea terminal SSH \(también conocido como Telnet inverso\)?](#)

[¿El SSH es compatible con Catalyst 2900?](#)

[Cómo puedo determinar qué plataformas y versiones de código admiten SSH](#)

[Cuando intento eliminar ciertos comandos de mi router, me pide que cree claves RSA para habilitar el SSH. ¿Por qué ocurre esto?](#)

[¿La versión 2 de SSH de Cisco IOS admite el estándar de firma digital \(DSS\)?](#)

[¿El servidor SSH de Cisco IOS soporta el reenvío de agentes?](#)

[¿Qué mecanismos de autenticación de cliente se soportan en el servidor SSH de Cisco IOS?](#)

[¿Qué significa el error Local: ¿Qué significa bytes de comprobación dañados en entrada?](#)

[¿Cisco IOS soporta SSH con el cifrado Blowfish?](#)

[Cuando intento generar claves RSA para el acceso SSH en un router usando el comando `crypto key generate rsa` en el modo de configuración, recibo este error: % Entrada no válida detectada en el marcador '^'. No permite que el router genere las claves RSA para habilitar el acceso SSH para el router. ¿Cómo se resuelve este error?](#)

[¿Las imágenes criptográficas admiten cifrado fuerte para utilizar SSH con cifras como 3DES o AES?](#)

[Estos mensajes se ven en los registros cuando intento configurar SSH en un router: SSH2 13: RSA sign: clave privada no encontrada y SSH2 13: error en la creación de la firma, estado -1.](#)

[¿Cómo se resuelve esto?](#)

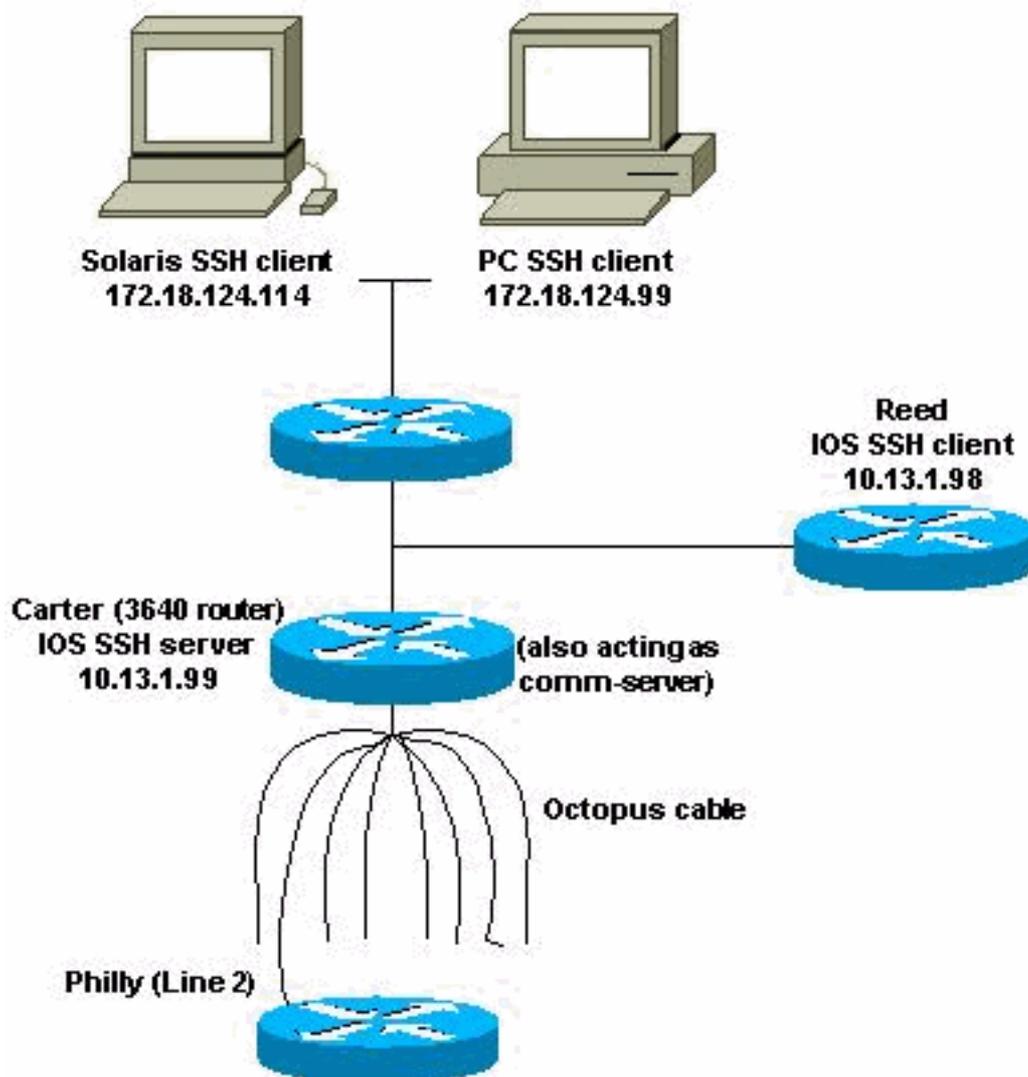
[Información Relacionada](#)

Introducción

Este documento contesta las Preguntas Frecuentes (FAQ) relacionadas con Secure Shell (SSH). El código SSH Cisco IOS[®] es el código original de Cisco.

¿Cómo configuro el acceso de línea terminal SSH (también conocido como Telnet inverso)?

Esto se introdujo por primera vez en algunas plataformas de Cisco IOS Software Release 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
```

Referencia de Comandos

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

- portnum - Especifica el puerto al que SSH necesita conectarse, como 2001.
- rotary group (grupo rotativo): especifica la rotativa definida que debe buscar un nombre válido.

¿El SSH es compatible con Catalyst 2900?

No.

Cómo puedo determinar qué plataformas y versiones de código admiten SSH

Consulte el Navegador de funciones (sólo para clientes registrados) y especifique la función SSH.

Cuando intento eliminar ciertos comandos de mi router, me pide que cree claves RSA para habilitar el SSH. ¿Por qué ocurre esto?

Aquí se muestra un ejemplo de este 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)
```

Ha encontrado el ID de bug de Cisco [CSCdv70159](#) ([sólo](#) clientes registrados) .

¿La versión 2 de SSH de Cisco IOS admite el estándar de firma digital (DSS)?

Cisco IOS SSH versión 2 no admite DSS.

¿El servidor SSH de Cisco IOS soporta el reenvío de agentes?

Cisco IOS SSH no soporta el reenvío de agentes. Interactúa con todas las instrumentaciones comerciales SSH.

¿Qué mecanismos de autenticación de cliente se soportan en el servidor SSH de Cisco IOS?

Cisco IOS SSH versión 2 (SSHv2) admite métodos de autenticación basados en contraseña e interactivos por teclado. Además de estos métodos de autenticación, la función SSHv2 Enhancements for RSA Keys (disponible en Cisco IOS Software Release 15.0(1)M y posteriores) soporta la autenticación de clave pública basada en RSA para el cliente y el servidor. Para obtener información adicional sobre los mecanismos de autenticación soportados por el servidor SSH de Cisco IOS, refiérase a [Soporte de la Versión 2 de Secure Shell](#).

¿Qué significa el error Local: ¿Qué significa bytes de comprobación dañados en entrada?

Bytes de verificación dañados significa que el paquete SSH recibido falló en su verificación de integridad. Esto suele deberse a un descifrado incorrecto. También ocurre por la utilización de una clave incorrecta. La clave incorrecta es causada por la pérdida de un paquete SSH encriptación. Ha descartado un paquete encriptación que debería haber sido enviado o ha descartado un paquete encriptación recibido que debería haber sido descifrado.

¿Cisco IOS soporta SSH con el cifrado Blowfish?

Cisco IOS no soporta SSH con el cifrado Blowfish. Cuando un cliente SSH envía este tipo de cifrado no admitido, el router muestra los mensajes de depuración mencionados en [SSH Client Envía Cipher No Soportado \(Blowfish\)](#).

Cuando intento generar claves RSA para el acceso SSH en un router usando el comando `crypto key generate rsa` en el modo config, recibo este error: `% Se ha detectado una entrada no válida en el marcador '^'..` No permite que el router genere las claves RSA para habilitar el acceso SSH para el router. ¿Cómo se resuelve este error?

Este error aparece cuando la imagen utilizada en el router no soporta el comando `crypto key generate rsa`. Este comando se soporta solamente en las imágenes de seguridad. Para resolver este error, utilice la imagen de seguridad de la serie apropiada del router Cisco IOS utilizado.

¿Las imágenes criptográficas admiten cifrado fuerte para utilizar SSH con cifras como 3DES o AES?

Yes. Sólo las imágenes criptográficas admiten cifrado fuerte. Para utilizar SSH con cifras como 3DES o AES, debe tener imágenes Crypto en su dispositivo Cisco.

Estos mensajes se ven en los registros cuando intento configurar SSH en un router: `SSH2 13: RSA_sign: clave privada no encontrada` y `SSH2 13: error en la creación de la firma, estado -1`. ¿Cómo se resuelve esto?

Estos mensajes de registro se ven debido a las ID de bug Cisco CSCsa83601 ([sólo](#) clientes registrados) y [CSCtc41114](#) (clientes registrados solamente). Consulte estos errores para obtener más información.

Información Relacionada

- [Página de soporte de SSH](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)