



Secure Shell Version 1 Integrated Client

This feature module describes the Secure Shell Version 1 Integrated Client feature. It includes information on the benefits of the new feature, supported platforms, related documents, and so forth.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 3
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 4
- Configuration Examples, page 4
- Command Reference, page 4

Feature Overview

Secure Shell (SSH) is an application and a protocol that provides a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley **rexec** and **rsh** tools. There are currently two versions of SSH available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The Secure Shell Version 1 Integrated Client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco router to make a secure, encrypted connection to another Cisco router or to any other device running the SSH Version 1 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in Cisco IOS software works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), Triple DES (3DES), and password authentication. User authentication is performed like that in the telnet session to the router. The user authentication mechanisms supported for SSH are RADIUS, TACACS+ and the use of locally stored user names and passwords.

**Note**

Hereafter, unless otherwise noted, the term “SSH” will denote “SSH Version 1” only.

The SSH client functionality is available only when the SSH server is enabled.

Benefits

Additional Security

The SSH client enables the initiation of secure sessions from a router to any other SSH server, including another router, that can provide secure, encrypted communication over insecure networks. The SSH client also supports user ID and password authentication using standard authentication methods: local authentication, RADIUS, and TACACS+.

DES and 3DES Encryption

The SSH client supports DES and 3DES encryption.

Restrictions

The SSH client is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available. These are the same ciphers that are supported in the SSH server feature in IOS.

**Caution**

Cisco IOS software with encryption (including, but not limited to, 56-bit data encryption feature sets) is subject to United States government export controls and has a limited distribution. Software images to be installed outside the United States may require an export license. Customer orders might be denied or subject to delay because of United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

Related Features and Technologies

The SSH client feature is related to the following existing features and technologies:

- Secure Shell Version 1 Support feature
- Authentication, Authorization, and Accounting (AAA)
- IP Security (IPSec)

Information about the Secure Shell Version 1 Support feature information is available in the *Secure Shell Version 1 Support* feature module for Cisco IOS Release 12.1(1)T. Information about AAA and IPSec is available in the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference*.

Related Documents

For information related to the Secure Shell Version 1 Integrated Client feature, refer to the following documents:

- *Cisco IOS Security Configuration Guide*, Cisco IOS Release 12.1
- *Cisco IOS Security Command Reference*, Cisco IOS Release 12.1
- *Secure Shell Version 1 Support*, Cisco IOS Release 12.1(1)T

Supported Platforms

- Cisco 1700 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 7200 series
- Cisco 7500 series
- Ciscoubr920 series

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on Cisco Connection Online (CCO) at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

The SSH client functionality is available only when the SSH server is enabled. The instructions for configuring and enabling the Cisco IOS SSH server are available in the *Secure Shell Version 1 Support* feature module for Cisco IOS Release 12.1(1)T.

The SSH client requires you to have an IPSec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(3)T loaded on your Cisco network device.

Configuration Tasks

None. The Secure Shell Version 1 Integrated Client feature runs in user EXEC mode and has no specific configuration on the router. Refer to the “Prerequisites” section for more information on what is required to run the SSH Version 1 Integrated Client feature.

Configuration Examples

None. The Secure Shell Version 1 Integrated Client feature runs in user EXEC mode and has no specific configuration on the router. Refer to the “Command Reference” section for examples of the **ssh** command.

Command Reference

This section documents the new **ssh** command. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

ssh

To start an encrypted session with a remote networking device, use the **ssh** user EXEC command.

```
ssh [-l userid] [-c {des | 3des}] [-o numberofpasswdprompts n] [-p portnum] {ipaddr | hostname}
    [command]
```

Syntax Description		
-l <i>userid</i>	(Optional) Specifies the user ID to use when logging in as on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.	
-c { des 3des }	(Optional) Specifies the crypto algorithm, DES or 3DES, to use for encrypting data. To use SSH, you must have an encryption image must be running on the router. Cisco software images that include encryption have the designators “56i” (DES) or “k2” (3DES).	
-o numberofpasswdprompts <i>n</i>	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the -o numberofpasswdprompts keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.	
-p <i>portnum</i>	(Optional) Indicates the desired port number for the remote host. The default port number is 22.	
<i>ipaddr</i> <i>hostname</i>	Specifies the IP address or host name of the remote networking device.	
<i>command</i>	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.	

Defaults Disabled.

Command Modes User EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Usage Guidelines The **ssh** command enables a Cisco router to make a secure, encrypted connection to another Cisco router or device running an SSH Version 1 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

**Note**

SSH is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.

The **ssh** command requires that you first enable the SSH server on the router. The SSH client is available only when the SSH server is enabled.

Examples

The following example illustrates initiating a secure session between the local router and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users who are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local router and will then close the session.

```
ssh -l adminHQ HQhost "show users"
```

The following example illustrates initiating a secure session between the local router and the edge router HQedge to run the **show ip route** command. In this example, the edge router prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge router will return the result of the **show ip route** command to the local router.

```
ssh -l adminHQ HQedge "show ip route"
```

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge router. The SSH server running on HQedge authenticates the session for the admin7 user on the HQedge router using standard authentication methods. The HQedge router must have SSH enabled for this to work.

```
ssh -l admin7 -c 3des -o numberofpasswdprompts 5 HQedge
```

Related Commands

Command	Description
ip ssh	Configures SSH server control parameters on the router.
show ip ssh	Displays the SSH connections on the router.