



Configuring SSHv2 and Telnet

This chapter describes how to configure Secure Shell Protocol version 2 (SSHv2) and Telnet on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as Cisco CG-OS router).

This chapter includes the following sections:

- [Information About SSHv2 and Telnet, page 5-1](#)
- [Prerequisites, page 5-3](#)
- [Guidelines and Limitations, page 5-3](#)
- [Default Settings, page 5-3](#)
- [Configuring SSHv2, page 5-3](#)
- [Configuring Telnet, page 5-9](#)
- [Verifying the SSHv2 and Telnet Configuration, page 5-11](#)
- [Configuration Example, page 5-11](#)

Information About SSHv2 and Telnet

This section includes the following topics:

- [SSHv2 Server, page 5-1](#)
- [SSHv2 Client, page 5-2](#)
- [SSHv2 Server Keys, page 5-2](#)
- [SSHv2 Authentication Using Digital Certificates, page 5-2](#)
- [Telnet Server, page 5-3](#)

SSHv2 Server

You can use the SSHv2 server to enable an SSH client to make a secure, encrypted connection to the Cisco CG-OS router. SSHv2 uses strong encryption for authentication. The SSHv2 server in the Cisco CG-OS software can interoperate with publicly and commercially available SSHv2 clients.

The user authentication mechanisms supported for SSHv2 are RADIUS, TACACS+, and the use of locally stored usernames and passwords on the Cisco CG-OS router.

SSHv2 Client

The SSHv2 client feature is an application that runs over the SSHv2 protocol to provide device authentication and encryption. The SSHv2 client enables the Cisco CG-OS router to make a secure, encrypted connection to any other device that runs the SSHv2 server. This connection provides an encrypted outbound connection. With authentication and encryption, the SSHv2 client allows for a secure communication over an insecure network.

The SSHv2 client in Cisco CG-OS works with publicly and commercially available SSHv2 servers.

SSHv2 Server Keys

SSHv2 requires server keys for secure communications to the Cisco CG-OS router. You can use SSHv2 server keys for the following SSHv2 options:

- SSHv2 version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography
- SSHv2 version 2 using the Digital System Algorithm (DSA)

Be sure to have an SSHv2 server key-pair with the appropriate version before enabling the SSHv2 service. You can generate the SSHv2 server key-pair according to the SSHv2 client version used. The SSHv2 service accepts two types of key-pairs for use by SSHv2:

- The **dsa** option generates the DSA key-pair for the SSHv2 protocol.
- The **rsa** option generates the RSA key-pair for the SSHv2 protocol.

By default, Cisco CG-OS generates an RSA key using 1024 bits.

SSHv2 supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)

**Caution**

If you delete all of the SSHv2 keys, you cannot start the SSHv2 services.

SSHv2 Authentication Using Digital Certificates

SSHv2 authentication provides X.509 digital certificate support for host authentication. An X.509 digital certificate is a data item that ensures the origin and integrity of a message. It contains encryption keys for secured communications and is signed by a trusted certification authority (CA) to verify the identity of the presenter. The X.509 digital certificate support provides either DSA or RSA algorithms for authentication.

The certificate infrastructure uses the first certificate that supports the Secure Socket Layer (SSL) and is returned by the security infrastructure, either through query or notification. Verification of certificates is successful if the certificates are from any of the trusted CAs.

You can configure your device for either SSHv2 authentication using an X.509 certificate or SSHv2 authentication using a Public Key Certificate, but not both. If either of them is configured and the authentication fails, you are prompted for a password.

For more information on CAs and digital certificates, see [Chapter 6, “Configuring PKI.”](#)

Telnet Server

The Telnet protocol enables TCP/IP connections to a host. Telnet allows a user at one site to establish a TCP connection to a login server at another site and then passes the keystrokes from one device to the other. Telnet can accept either an IP address or a domain name as the remote device address.

By default, the Telnet server is disabled on the Cisco CG-OS router.

Prerequisites

Configure IP on a Layer 3 interface, out-of-band on the mgmt 0 interface, or inband on an Ethernet interface.

Guidelines and Limitations

Cisco CG-OS supports only SSH version 2 (SSHv2).

You can configure the Cisco CG-OS router with either SSHv2 authentication using an X.509 certificate or SSHv2 authentication using a Public Key Certificate, but not both. Regardless of which authentication method is in use, the Cisco CG-OS router prompts the user for a password when authentication fails.

Cisco CG-OS supports a maximum of 60 concurrent SSHv2 and Telnet sessions.

Default Settings

Table 5-1 lists the default settings for SSHv2 and Telnet parameters.

Table 5-1 Default SSHv2 and Telnet Parameters

Parameters	Default
SSHv2 server	Enabled
SSHv2 server key	RSA key generated with 1024 bits
RSA key bits for generation	1024
Telnet server	Disabled
Telnet port number	23

Configuring SSHv2

This section includes the following sections:

- [Generating SSHv2 Server Keys, page 5-4](#)
- [Specifying the SSHv2 Public Keys for User Accounts, page 5-4](#)
- [Starting SSHv2 Sessions, page 5-6](#)
- [Clearing SSHv2 Hosts, page 5-7](#)
- [Disabling the SSHv2 Server, page 5-7](#)

- [Clearing SSHv2 Sessions, page 5-8](#)

Generating SSHv2 Server Keys

You can generate an SSHv2 server key based on your security requirements. The default SSHv2 server key is an RSA key that the Cisco CG-OS router generates using 1024 bits.

BEFORE YOU BEGIN

Ensure that you have met the prerequisites for SSHv2 summarized under [Prerequisites](#).

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>no feature ssh</code>	Disables SSHv2. By default, SSHv2 is enabled on the Cisco CG-OS router.
Step 3	<code>ssh key {dsa [force] rsa [bits [force]]}</code>	Generates the SSHv2 server key. dsa —generates the DSA key-pair for the SSHv2 protocol. rsa —generates the RSA key-pair for the SSHv2 protocol. (Optional) The <i>bits</i> argument is the number of bits used to generate the key. The range is from 768 to 2048 and the default value is 1024. (Optional) Use the force keyword to replace an existing key.
Step 4	<code>feature ssh</code>	Enables SSHv2.
Step 5	<code>show ssh key</code>	(Optional) Displays the SSHv2 server keys.
Step 6	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to generate a SSHv2 server key on the Cisco CG-OS router.

```
router# configure terminal
router(config)# no feature ssh
router(config)# ssh key rsa 2048
router(config)# feature ssh
router(config)# copy running-config startup-config
```

Specifying the SSHv2 Public Keys for User Accounts

You can configure an SSHv2 public key to log in using an SSHv2 client without being prompted for a password. You can specify the SSHv2 public key in one of these formats:

- OpenSSH format
- IETF SECSH format

Specifying the SSHv2 Public Keys in OpenSSH Format

You can specify the SSHv2 public keys in OpenSSH format for user accounts.

BEFORE YOU BEGIN

Generate an SSHv2 public key in OpenSSH format.

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>username <i>username</i> sshkey <i>ssh-key</i></code>	Configures the SSHv2 public key in OpenSSH format.
Step 3	<code>show user-account</code>	(Optional) Displays the user account configuration.
Step 4	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to specify SSHv2 public keys for user accounts.

```
router# configure terminal
router(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK30iW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+1VKRXFY/G+1JNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
router(config)# copy running-config startup-config
```

Specifying the SSHv2 Public Keys in IETF SECSH Format

You can specify the SSHv2 public keys in IETF SECSH format for user accounts.

BEFORE YOU BEGIN

Generate an SSHv2 public key in IETF SCHSH format.

DETAILED STEPS

	Command	Purpose
Step 1	<code>copy server-file bootflash:filename</code>	Downloads the file containing the SSHv2 key in IETF SECSH format from a server. The server can be FTP, secure copy (SCP), secure FTP (SFTP), or TFTP. Note Only a network-admin or vdc-admin can perform this task.
Step 2	<code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>username username sshkey file bootflash:filename</code>	Configures the SSHv2 public key in IETF SECSH format.
Step 4	<code>show user-account</code>	(Optional) Displays the user account configuration.
Step 5	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to specify the SSHv2 public keys in IETF SECSH format.

```
router# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub
router(config)# configure terminal
router(config)# username User1 sshkey file bootflash:secsh_file.pub
router(config)# copy running-config startup-config
```

Starting SSHv2 Sessions

You can start SSHv2 sessions using IPv4 or IPv6 to connect to remote devices from the Cisco CG-OS router.

**Note**

Cisco CG-OS supports a maximum of 60 concurrent SSHv2 and Telnet sessions.

BEFORE YOU BEGIN

Obtain the hostname for the remote device and, if needed, the username on the remote device.

Enable the SSHv2 server on the remote device.

DETAILED STEPS

	Command	Purpose
Step 1	<code>ssh [username@]{ipv4-address hostname}</code>	Creates an SSHv2 IPv4 session to a remote device using IPv4.
	<code>ssh6 [username@]{ipv6-address hostname}</code>	Creates an SSHv2 IPv6 session to a remote device using IPv6.

EXAMPLE

This example shows how to create an SSHv2 IPv4 session to a remote device.

```
router# ssh 10.10.1.1
```

This example shows how to how to create an SSHv2 IPv6 session to a remote device.

```
router# ssh6 HostA
```

Clearing SSHv2 Hosts

When you download a file from a server using SCP or SFTP, or when you start an SSHv2 session from the Cisco CG-OS router to a remote host, you establish a trusted SSHv2 relationship with that server. You can clear the list of trusted SSHv2 servers for your user account.

Command	Purpose
clear ssh hosts	Clears the SSHv2 host sessions.

Disabling the SSHv2 Server

By default, the SSHv2 server is enabled on the Cisco CG-OS router. You can disable the SSHv2 server to prevent SSHv2 access to the Cisco CG-OS router.

Command	Purpose
no feature ssh	Disables SSH.

**Note**

To reenable SSHv2, you must first generate an SSHv2 server key. (See [Generating SSHv2 Server Keys, page 5-4.](#))

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	no feature ssh	Disables the SSHv2 server. Feature is enabled by default.
Step 3	show ssh server	(Optional) Displays the SSHv2 server configuration.
Step 4	copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to disable SSHv2 on the Cisco CG-OS router.

```
router# configure terminal
router(config)# no feature ssh
router(config)# copy running-config startup-config
```

Deleting SSHv2 Server Keys

BEFORE YOU BEGIN

Disable the SSHv2 server. (See [Disabling the SSHv2 Server](#), page 5-7.)

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	no feature ssh	Disables the SSHv2 server.
Step 3	no ssh key [dsa rsa]	Deletes the SSHv2 server key. The default is to delete all the SSHv2 keys.
Step 4	show ssh key	(Optional) Displays the SSHv2 server key configuration.
Step 5	copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to delete SSHv2 server keys.

```
router# configure terminal
router(config)# no feature ssh
router(config)# no ssh key rsa
router(config)# copy running-config startup-config
```

Clearing SSHv2 Sessions

You can clear SSHv2 sessions from the Cisco CG-OS router.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	<code>show users</code>	Displays user session information.
Step 2	<code>clear line vty-line</code>	Clears a user SSHv2 session. <i>vtty-line</i> —virtual terminal line.

EXAMPLE

```
router# configure terminal
router(config)# show users
router(config)# clear line pts/12
```

Configuring Telnet

This section includes the following topics:

- [Enabling the Telnet Server, page 5-9](#)
- [Starting Telnet Sessions to Remote Devices, page 5-10](#)
- [Clearing Telnet Sessions, page 5-10](#)

Enabling the Telnet Server

You can enable the Telnet server on the Cisco CG-OS router. By default, the Telnet server is disabled.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>feature telnet</code>	Enables the Telnet server. The default is disabled.
Step 3	<code>show telnet server</code>	(Optional) Displays the Telnet server configuration.
Step 4	<code>copy running-config startup-config</code>	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to enable Telnet on the Cisco CG-OS router.

```
router# configure terminal
router(config)# feature telnet
```

```
router(config)# copy running-config startup-config
```

Starting Telnet Sessions to Remote Devices

You can start Telnet sessions to connect to remote devices from the Cisco CG-OS router. You can start Telnet sessions by using either IPv4 or IPv6.



Note

Cisco CG-OS supports a maximum of 60 concurrent SSHv2 and Telnet sessions.

BEFORE YOU BEGIN

Obtain the hostname or IP address for the remote device and, if needed, the username on the remote device.

Enable the Telnet server on the Cisco CG-OS router. (See [Enabling the Telnet Server, page 5-9](#).)

Enable the Telnet server on the remote device.

DETAILED STEPS

	Command	Purpose
Step 1	telnet { <i>ipv4-address</i> <i>host-name</i> } [<i>port-number</i>]	Starts a Telnet session to a remote device using IPv4. The default port number is 23. The range is from 1 to 65535.
	telnet6 { <i>ipv6-address</i> <i>host-name</i> } [<i>port-number</i>]	Starts a Telnet session to a remote device using IPv6. The default port number is 23. The range is from 1 to 65535.

EXAMPLE

This example shows how to configure a Telnet session to a remote device that is using IPv4.

```
router# telnet 10.10.1.1
```

This example shows how to configure a Telnet session to a remote device that is using IPv6.

```
router# telnet 2001:0DB8::ABCD:1 management
```

Clearing Telnet Sessions

You can clear Telnet sessions from the Cisco CG-OS router.

BEFORE YOU BEGIN

Telnet server must be enabled on the Cisco CG-OS router.

DETAILED STEPS

	Command	Purpose
Step 1	<code>show users</code>	Displays user session information.
Step 2	<code>clear line vty-line</code>	Clears a user Telnet session.

EXAMPLE

This example shows how to clear a Telnet session.

```
router# show users
router(config)# clear line pts/12
```

Verifying the SSHv2 and Telnet Configuration

To display the SSHv2 and Telnet configuration information, enter any or all of the following commands:

Command	Purpose
<code>show ssh key [dsa rsa]</code>	Displays SSHv2 server key-pair information.
<code>show running-config security [all]</code>	Displays the SSHv2 and user account configuration in the running configuration. The all keyword displays the default values for the SSHv2 and user accounts.
<code>show ssh server</code>	Displays the SSHv2 server configuration.
<code>show telnet server</code>	Displays the Telnet server configuration.

Configuration Example

```
configure terminal
no feature ssh
ssh key rsa
  generating rsa key(1024 bits).....
  generated rsa key
feature ssh
show ssh key
rsa Keys generated: Tues Jan 29 00:10:39 2013

ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+Mzm99n2U0
ChzZG4svRwmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K361r39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhPhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
*****
could not retrieve dsa key information
*****
```

■ Configuration Example

```
username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+1JNqJP/eLowb7ubO+1VKRXY/G+1JNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmsiH
3UD/vKyziEh5S4Tplx8=

copy running-config startup-config
```