



Configuration and File System Management

This module describes methods for configuration management and file transfer enhancements.

- [Secure file transfer from the Router, on page 1](#)
- [Auto-Save Configuration, on page 4](#)
- [Auto-Save and Copy Router Configuration Using Public Key Authentication, on page 6](#)

Secure file transfer from the Router

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Secure file transfer from the Router	Release 7.9.1	Your routers are now enabled to transfer files securely to an archive server. It's made possible because the copy command now supports SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol) using the underlying SSH protocol implementation. Secure transfer of files from the router maintains the integrity, confidentiality, and availability of network configurations. This feature modifies the copy command.

You can duplicate files or data in the router from one location to another using the **copy** command. This functionality helps to create a copy of a file, folder, or data set and place it in a specific destination. You can use the copy functionality to back up files, move data between directories, create duplicates of the files for editing or distribution without modifying the original content. It also allows you to retain the original data while making a duplicate that you can further manipulate independently.

Starting with Cisco IOS XR Release 7.9.1, we've enhanced the functionality of the copy command to support secure file transfer from the router. Secure file transfer protects data during transit using the SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol) when sharing files within or across networks. The

SFTP and SCP functionalities in the copy feature use the SSH protocol implementation in the router to secure transfer the files to a remote server.

You can use the following options in the **copy** command for secure file transfer:

- **sftp**: You can transfer the files to a remote location using the **SFTP** file transfer protocol. SFTP is a secure file transfer protocol for transferring large files.
- **scp**: You can transfer the files to a remote location using the **SCP** file transfer protocol. SCP is a secure copy protocol to transfer files between servers.

Starting Cisco IOS XR Software Release 7.10.1, you can use public-key authentication while copying the running configuration.

Prerequisites:

Enable the SSH Server in the router as follows:

```
Router# config
Router(config)# ssh server v2
Router(config)# ssh server vrf default
Router(config)# ssh server netconf vrf default
Router(config)# commit
```

Configuration Example for Secure File Transfer Protocol

You can copy the running configuration file from the router to a remote server using SFTP:

Configuration in the Router

```
Router# copy running-config sftp://root:testpassword@192.0.2.1//var/opt/run_conf_sftp.txt

Destination file name (control-c to cancel): [/var/opt/run_conf_sftp.txt]?
.
215 lines built in 1 second
[OK]Connecting to 192.0.2.1...22
Password:
sftp> put /tmp/tmpsymlink/nvgen-34606-_proc_34606_fd_75 /var/opt/run_conf_sftp.txt

/tmp/tmpsymlink/nvgen-34606-_proc_34606_fd_75

  Transferred 3271 Bytes
  3271 bytes copied in 0 sec (3271000)bytes/sec
sftp> exit
```

Verification in the SFTP Server

```
[root@sftp_server ~]# ls -ltr /var/opt/run_conf_sftp.txt
-rw-r--r-- 1 root root 3271 Mar 21 18:07 /var/opt/run_conf_sftp.txt
```

Configuration Example for Secure Copy Protocol

You can copy the running configuration file from the router to a remote server using SCP:

Configuration in the Router

```
Router# copy running-config scp://root:testpassword@192.0.4.2//var/opt/run_conf_scp.txt

Destination file name (control-c to cancel): [/var/opt/run_conf_scp.txt]?
```

```
.
215 lines built in 1 second
[OK]Connecting to 192.0.4.2...22
Password:

  Transferred 3271 Bytes
  3271 bytes copied in 0 sec (0)bytes/sec
```

Verification in the SCP Server

```
[root@scp_server ~]# ls -ltr /var/opt/run_conf_scp.txt
-rw-r--r-- 1 root root 3271 Mar 21 18:07 /var/opt/run_conf_scp.txt
```

Configuration Example for SCP and SFTP Using Public-Key Authentication

While you're using public-key authentication for copying running configuration from the router to a remote server, you don't need to mention **password** in the command. The following example shows how you can configure public-key authentication while copying configuration using the SCP protocol:

```
Router#copy running-config scp://root@192.0.4.2//var/opt/run_conf_scp.txt
```

Auto-Save Configuration

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
Auto-Save with Secure File-Transfer and Additional Configurable Parameters	Release 7.9.1	<p>Apart from automatically backing up the running configuration after every commit, you can also do the following with Auto-Save:</p> <ul style="list-style-type: none"> • Save running configurations to remote systems using Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP). • Configure wait-time between two subsequent auto-saves. • Append time-stamp to the file name of the saved configuration. • Save the encrypted password. • Specify the maximum number of files that you can auto-save. <p>The feature introduces these changes:</p> <p>CLI: Modified the configuration commit auto-save command by adding the following keywords:</p> <ul style="list-style-type: none"> • filename scp • filename sftp • wait-time • timestamp • password • maximum <p>Yang Data Model:</p> <ul style="list-style-type: none"> • New XPath for Cisco-IOS-XR-config-autosave-cfg • New XPath for Cisco-IOS-XR-um-config-commit-cfg

You can configure the router to automatically take the backup of the running configuration by using **configuration commit auto-save** command. This auto-save feature saves the configuration to the specified location on the router after every **commit** is made. These auto-save files are stored in the form of Linux files.

Starting Cisco IOS XR Software Release 7.9.1, the auto-save feature is enhanced to provide a set of functionalities. Use the following keywords to achieve the same:

- **scp and sftp** - You can save the running configuration backup files to remote location using **scp** and **sftp** file transfer protocols. SCP is a secure copy protocol to transfer files between servers. Whereas SFTP is a secure file transfer protocol for transferring large files.
- **password** - You can save encrypted passwords for the remote and non-remote URLs.
- **maximum** - You can mention maximum number of files that can be saved automatically. Once the maximum number of auto-saved file is reached, the newer auto-save files starts replacing the older auto-save files. The default value of **maximum** is 1. You can save upto 4294967295 files.
- **timestamp** - Using this keyword, the time-stamp can be appended to the auto-saved configuration file name. The **timestamp** uses the time and timezone configured on the router. The saved file displays timestamp in <day> <month> <date> <hours> <minutes> <seconds> <milliseconds> format. Here is an example of auto-saved file with time-stamp - : *test_123.autosave.1.ts.Tue_Jan_31_15-15-51_805_IST*
- **wait-time** - You can specify how long to wait before next auto-save happens in terms of days, months or hours after the commit is made. The default value of **wait-time** is zero.

Restriction for Auto-Save Configuration

The auto-save configuration is only available on the local paths, scp, and sftp paths.

Configure Auto-Save

Use the **configuration commit auto-save** command to auto save the configuration.

```
Router#configure
Router(config)#configuration commit auto-save
Router(config-cfg-autosave)#commit
```

You can also configure options such as **password**, **timestamp**, **maximum**, and **wait-time** with the **configuration commit auto-save** command. The location to save the file-name must be specified in <protocol>://<user>@<host>:<port>/<url-path>/<file-name> format.

When filename is accessed through VRF, you can specify filename in **filename** <protocol>://<user>@<host>:<port>;<vrf name>/<url-path>/<file-name> format.

When you are using public key authentication, you don't need to mention **password**.

```
Router(config-cfg-autosave)#configuration commit auto-save filename
sftp://user1@server1://test-folder/test_123
Router(config-cfg-autosave)#password clear encryption-default cisco
Router(config-cfg-autosave)#timestamp
Router(config-cfg-autosave)#maximum 10
Router(config-cfg-autosave)#wait-time days 0 hours 0 minutes 0 seconds 5
Router(config-cfg-autosave)#commit
```

Running Configuration

```
Router#show running-config configuration commit auto-save
configuration commit auto-save
 filename sftp://user1@server1://test-folder/test_123
 password encrypted encryption-default <password for above user>
 timestamp
 maximum 10
 wait-time days 0 hours 0 minutes 0 seconds 5
!
```

Auto-Save and Copy Router Configuration Using Public Key Authentication

Table 3: Feature History Table

Feature Name	Release Information	Feature Description
Auto-Save and Copy Router Configuration Using Public Key Authentication	Release 7.10.1	<p>Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native])</p> <p>You can now experience passwordless authentication while automatically saving running configurations and securely copying them on the router. The feature uses public key-based authentication, a secure logging method using a secure shell (SSH), which provides increased data security. This feature offers automatic authentication and single sign-on benefits, which also aids in a secure automation process.</p> <p>This feature modifies configuration commit auto-save and copy command to support password-less authentication.</p>

From Cisco IOS XR Software Release 7.10.1, you don't need to remember and enter the **password** as you can use public key-based authentication while doing the following:

- Automatically saving your running configuration
- Copying the configuration from a source (such as a network server) to a destination (such as a flash disk)

Password is automatically verified when you have enabled SSH connection using public key-based authentication. Using public key-based authentication avoids several problems such as password disclosure and password leakage.

Public key is mathematically related to private key. The private key is secret, whereas the public key is available on the servers. You can copy the public key to the SSH server from the SSH client. Then, when you try to secure the running configuration, the SSH server tries to authenticate by generating a challenge using the public key. Only the private key can answer this challenge. As the keys are related, log-in is successful.

Prerequisites for Auto-Save and Copy Router Configuration Using Public Key Authentication

Ensure you have enabled public key-based authentication of SSH clients, using the following steps:

- Generate RSA key pair on the router configured as the SSH client. Use the **crypto key generate authentication-ssh rsa** command to generate the RSA key pair.
- Use the **show crypto key mypubkey authentication-ssh rsa** command to view the details of the RSA key. The key value starts with *ssh-rsa* in this output.
- Copy the RSA public key from the SSH client to the SSH server.

For more detailed information on how to enable SSH connection using public-key based authentication, see *Public Key Based Authentication of SSH Clients* in System Security Configuration Guide for Cisco NCS 5500 Series Routers.

