

Secure Shell—Configuring SFTP Username and Password

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

- Overview, on page 1
- Configuring SFTP Username and Password, on page 1

Overview

The Secure File Transfer Protocol (SFTP) is a vital component of network security, ensuring secure file transfer capabilities across networked systems.

By leveraging the security framework provided by the Secure Shell (SSH) protocol, SFTP extends the functionality of file operations with robust encryption and authentication mechanisms.

A critical step in deploying SFTP for secure file exchanges involves the configuration of usernames and passwords. This process authenticates users and ensures that only authorized individuals can access and manage files on the Cisco device.

This document is intended to guide network administrators through the process of configuring SFTP usernames and passwords to secure file transfers on Cisco devices.

Configuring SFTP Username and Password

To configure a username and password for SFTP, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configureterminal**
3. **ip sftpusername** *username*

4. **ip sftppassword** *encryption level {0| 7| LINE} password*
5. **exit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip sftpusername** *username* **Example:** `Device(config)# ip sftp username cisco`	Defines the username.
Step 4	**ip sftppassword** *encryption level {0| 7| LINE} password* **Example:** `Device(config)# ip sftp password 0 cisco123`	Defines the password. Specify the encryption level. • 0 – Unencrypted password. • 7 – Encrypted password. • Line – Clear text password.
Step 5	**exit**	Exits global configuration mode and returns to privileged EXEC mode.