



Configuring Secure Storage

- [Information About Secure Storage, on page 1](#)
- [Enabling Secure Storage , on page 1](#)
- [Disabling Secure Storage , on page 2](#)
- [Verifying the Status of Encryption, on page 2](#)
- [Feature History for Secure Storage, on page 3](#)

Information About Secure Storage

Secure Storage feature allows you to secure critical configuration information by encrypting it. It encrypts asymmetric key-pairs, pre-shared secrets, the type 6 password encryption key and certain credentials. An instance-unique encryption key is stored in the hardware trust anchor to prevent it from being compromised.

Enabling Secure Storage

Before you begin

By default, this feature is disabled.

Procedure

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | configure terminal Example: Device# <code>configure terminal</code> | Enters the global configuration mode. |
| Step 2 | service private-config-encryption Example: DEvice(config)# <code>service private-config-encryption</code> | Enables the Secure Storage feature on your device. |
| Step 3 | end Example: | Returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| | Device(config)# end | |
| Step 4 | write memory Example: Device# write memory | Encrypts the private-config file and saves the file in an encrypted format. |

Disabling Secure Storage

Before you begin

To disable Secure Storage feature on a device, perform this task:

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters the global configuration mode. |
| Step 2 | no service private-config-encryption Example: Device(config)# no service private-config-encryption | Disables the Secure Storage feature on your device. When secure storage is disabled, all the user data is stored in plain text in the NVRAM. |
| Step 3 | end Example: Device(config)# end | Returns to privileged EXEC mode. |
| Step 4 | write memory Example: Device# write memory | Decrypts the private-config file and saves the file in plane format. |

Verifying the Status of Encryption

Use the **show parser encrypt file status** command to verify the status of encryption. The following command output indicates that the feature is available but the file is not encrypted. The file is in 'plain text' format.

```
Device#show parser encrypt file status
Feature: Enabled
File Format: Plain Text
Encryption Version: Ver1
```

Feature History for Secure Storage

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|--------------------------|----------------|---|
| Cisco IOS XE Fuji 16.9.2 | Secure Storage | Secure Storage feature allows you to secure critical configuration information by encrypting it. It encrypts asymmetric key-pairs, pre-shared secrets, the type 6 password encryption key and certain credentials. An instance-unique encryption key is stored in the hardware trust anchor to prevent it from being compromised. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.

