

Secure Storage

- Feature history for secure storage, on page 1
- Secure Storage, on page 1
- Enable secure storage, on page 1
- Configuration example to verify the encryption status, on page 2

Feature history for secure storage

This table provides release and platform support 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 name and description	Supported platform
Cisco IOS XE 26.2.1ea	Secure Storage: Secure Storage feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	Secure Storage: This feature protects critical configuration information by encrypting it.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Secure Storage

The Secure Storage feature protects critical configuration information by encrypting it. This includes asymmetric key-pairs, pre-shared secrets, the type 6 password encryption key, and specific credentials. To ensure security, an instance-unique encryption key is stored within the hardware trust anchor, preventing unauthorized access or compromise.

Enable secure storage

Secure storage is disabled by default. Perform this task to enable secure storage.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Enter your password, if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 [**no**] **service private-config-encryption**

Example:

```
Device(config)# service private-config-encryption
```

Enables secure storage on the device.

Use the no form of this command to disable secure storage on the device

Note
When secure storage is disabled, all the user data is stored in plain text in the NVRAM.

Step 4 **end**

Example:

```
Device(config)# end
```

Returns to privileged EXEC mode.

Step 5 **write memory**

Example:

```
Device# write memory
```

Encrypts the private-config file and saves the file in an encrypted format.

Configuration example to verify the encryption status

The following is a sample output to verify if encryption status is enabled.

```
Device# show parser encrypt file status
Feature:            Enabled
File Format:        Cipher text
Encryption Version: ver1
```

In this example, the file format is displayed as *Cipher text*. This indicates that file is encrypted and secure storage is enabled.