Configuring Secure Storage

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.

SUMMARY STEPS

1. **configure terminal**
2. **service private-config-encryption**
3. **end**
4. **write memory**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# `**`configure terminal`**	Enters the global configuration mode.

	Command or Action	**Purpose**
Step 2	**service private-config-encryption** **Example:** Device(config)# **service private-config-encryption**	Enables the Secure Storage feature on your device.
Step 3	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode.
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:

SUMMARY STEPS

1. **configure terminal**
2. **no service private-config-encryption**
3. **end**
4. **write memory**

DETAILED STEPS

	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.

	Command or Action	**Purpose**
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 Information for Secure Storage

Release	**Modification**
Cisco IOS XE Fuji 16.9.1	This feature was introduced.