

Information About Secure Storage

Secure Storage feature allows you to secure critical configuration information by encrypting it. It encrypts VPN, IPSec, and other 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.

By default, this feature is enabled on platforms that come with a hardware trust anchor. This feature is not supported on platforms that do not have hardware trust anchor.

- Supported Platforms, on page 1
- Enabling Secure Storage , on page 4
- Disabling Secure Storage , on page 5
- Verifying the Status of Encryption, on page 6
- Downgrading the Platform Image to an Older Version, on page 6
- Feature Information for Overview of Secure Storage, on page 7

Supported Platforms

Starting from Cisco IOS Release 15.6(3) M1, the following Cisco 880 Series platforms support Secure Storage:

Table 1: Secure Storage Supported Platforms - Cisco Integrated Services Router 880 PID

C881-K9
C887VA-K9
C886VA-K9
C887VAM-K9
C886VAJ-K9
C888-K9

Starting from Cisco IOS Release 15.6(3) M1, the following Cisco 890 Series platforms support Secure Storage:

Table 2: Secure Storage Supported Platforms - Cisco Integrated Services Router 890 PID

C891FW-E-K9

C891F-K9
C891FW-A-K9
C891-24X-K9

Starting from Cisco IOS Release 15.6(3) M1, the following Cisco 800M Series platforms support Secure Storage:

Table 3: Secure Storage Supported Platforms - Cisco Integrated Services Router 800M PID

C841M-4X/K9
C886VA-K9
C841M-8X/K9

Starting from Cisco IOS XE Release 16.6.1, the following ISR 4000 platforms support Secure Storage:

Table 4: Secure Storage Supported Platforms - Cisco Integrated Services Router 4000 PID

ISR4431
ISR4221
ISR4321
ISR4331
ISR4351
ISR4451-X

Starting from Cisco IOS XE Release 16.6.1, the following ASR 1000 platforms support Secure Storage::

Table 5: Secure Storage Supported Platforms - Cisco ASR 1000 Series Aggregation Services Routers PID

ASR1000-RP3
ASR1001-X
ASR1001-HX
ASR1002-HX

Starting from Cisco IOS XE Release 16.9.1, the following Cisco 1000 Series platforms support Secure Storage::

Table 6: Secure Storage Supported Platforms - Cisco 1000 Series PID

C1101-4P
C1111-8P
C1111-4P

C1112-8P
C1113-8P
C1113-8PM
C1116-4P
C1117-4P
C1117-4PM
C1101-4PLTEP
C1111-8PLTEEA
C1111-8PLTELA
C1111-4PLTEEA
C1111-4PLTELA
C1112-8PLTEEA
C1113-8PLTEEA
C1113-8PLTELA
C1113-8PMLTEEA
C1116-4PLTEEA
C1117-4PLTEEA
C1117-4PLTELA
C1117-4PMLTEEA
C1111-8PWY
C1111-4PWX
C1112-8PWE
C1113-8PWA
C1113-8PWB
C1113-8PWE
C1116-4PWE
C1117-4PWE
C1117-4PWA
C1117-4PWZ

C1117-4PMWE
C1111-8PLTEEAWX
C1111-8PLTELAWY
C1112-8PLTEAWE
C1113-8PLTEEAWA
C1113-8PLTEEAWB
C1113-8PLTEEAWE
C1113-8PLTELAWZ
C1116-4PLTEEAWE
C1117-4PMLTEEA
C1117-4PLTEEAWE
C1117-4PLTEEAWA
C1117-4PLTELAWZ
C1117-4PMLTEEAWE
C1101-4PLTEPWX

Enabling Secure Storage

Before you begin

By default, this feature is enabled on a platform. Use this procedure on a platform where it is disabled.

SUMMARY STEPS

1. Config terminal
2. service private-config-encryption
3. do write memory

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Config terminal **Example:** `router#config terminal`	Enters the configuration mode.

	Command or Action	Purpose
Step 2	service private-config-encryption **Example:** `router(config)# service private-config-encryption`	Enables the Secure Storage feature on your platform.
Step 3	do write memory **Example:** `router(config)# do write memory`	Encrypts the private-config file and saves the file in an encrypted format.

Example

The following example shows how to enable Secure Storage:

```
router#config terminal
router(config)# service private-config-encryption
router(config)# do write memory
```

Disabling Secure Storage

Before you begin

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

SUMMARY STEPS

1. Config terminal
2. no service private-config-encryption
3. do write memory

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Config terminal **Example:** `router#config terminal`	Enters the configuration mode.
Step 2	no service private-config-encryption **Example:** `router(config)# no service private-config-encryption`	Disables the Secure Storage feature on your platform.

	Command or Action	Purpose
Step 3	do write memory **Example:** `router(config)# do write memory`	Decrypts the private-config file and saves the file in plane format.

Example

The following example shows how to disable Secure Storage:

```
router#config terminal
router(config)# no service private-config-encryption
router(config)# do write memory
```

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.

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

The following command output indicates that the feature is enabled and the file is encrypted. The file is in 'cipher text' format.

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

Downgrading the Platform Image to an Older Version

Before you downgrade the platform image to an older version where the Secure Storage is not supported, you have to disable the feature in the version where it is supported.

If you do not disable this feature before downgrading to an older image, the private-config file will be in encrypted format. The following Syslog message will be generated to indicate that the file is in encrypted format:

```
%PARSER-4-BADCFG: Unexpected end of configuration file.
```

If the file is in 'plain text', no Syslog message will be generated.

Feature Information for Overview of Secure Storage

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7: Feature Information for Overview of Cisco TrustSec

Feature Name	Releases	Feature Information
Secure Storage	Cisco IOS XE Fuji 16.9.1	The support for Secure Storage is introduced for ASR and ISR platforms.