



Configure secure storage

A secure storage feature is a security mechanism that

- encrypts critical configuration information, such as VPN and IPSec key pairs, pre-shared secrets, and credentials,
- stores an instance-unique encryption key in the hardware trust anchor to prevent compromise, and
- enables protection for type 6 password encryption keys and certain credentials.

By default, this feature is enabled on platforms with a hardware trust anchor. Platforms without a hardware trust anchor do not support secure storage.

- [Enable secure storage , on page 1](#)
- [Disable secure storage , on page 2](#)
- [Verify the status of encryption, on page 3](#)
- [Verify the platform identity, on page 3](#)

Enable secure storage

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

Procedure

	Command or Action	Purpose
Step 1	Config terminal Example: router#config terminal	Enters the configuration mode.
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:	Encrypts the private-config file and saves the file in an encrypted format.

	Command or Action	Purpose
	router(config)# do write memory	

Example

The following example shows how to enable Secure Storage:

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

Disable secure storage

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.
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
```

Verify 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
```

Verify the platform identity

Use the **show platform sudi certificate** command to display the SUDI certificate in standard PEM format. The command output helps you verify the platform identity.

In the command output, the first certificate is the Cisco Root CA 2048 and the second is the Cisco subordinate CA (ACT2 SUDI CA). The third is the SUDI certificate.

```
router#show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiuGAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDAXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDAXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWlSEWdovyD0My5jOAmahBKeN8hF570YQXJ
FcjPfto1YYmUQ6iEqDGYeJu5Tm8sUxJsZr2tKys7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpdSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6ke0la06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdFhbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
olEwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBvrbW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyC81WhJdTsD9i7rp77rMKSSh0T8lasz
Bvt9YaretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX41Id
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
```

