Secure Storage

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 storager.

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.