Federal Information Processing Standard

Federal Information Processing Standard

Federal Information Processing Standard (FIPS) 140-2 is a security standard used to validate cryptographic modules. The cryptographic modules are produced by the private sector for use by the U.S. government and other regulated industries (such as financial and healthcare institutions) that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information.

Note Cisco TrustSec (CTS) is not supported when the controller is in FIPS mode.

For more information about FIPS, see

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html.

Guidelines and Restrictions for FIPS

- In the controller, a legacy key is used to support the legacy APs. However, in FIPS mode, the crypto engine detects the legacy key as a weak key and rejects it by showing the following error message: "**% Error in generating keys: could not generate test signature.**" We recommend that you ignore such error messages that are displayed during the bootup of the controller (when operating in FIPS mode).
- SSH clients using SHA1 will not be able to access the controller when you enable FIPS. You need to use FIPS compliant SSH clients to access the controller.
- While configuring WLAN ensure that the SSID name contain a minimum of 15 characters. If not, the APs will not be able to join the controller after changing tags.
- TrustSec is not supported.

- PAC key configuration is not supported.
- APs would not reload immediately, if you change the FIPS status.
- With FIPS in enabled state, some passwords and pre-shared keys must have the minimum lengths, for example the ISAKMP key (Crypto ISAKMP key) must be at least 14 characters long.:
- We recommend a minimum RSA key size of 2048 bits under RADSEC when operating in FIPS mode. Otherwise, the RADSEC fails.

FIPS Self-Tests

A cryptographic module must perform power-up self-tests and conditional self-tests to ensure that it is functional.

Power-up self-tests run automatically after the device powers up. A device goes into FIPS mode only after all self-tests are successfully completed. If any self-test fails, the device logs a system message and moves into an error state. Also, if the power-up self test fails, the device fails to boot.

Using a known-answer test (KAT), a cryptographic algorithm is run on data for which the correct output is already known, and then the calculated output is compared to the previously generated output. If the calculated output does not equal the known answer, the known-answer test fails.

Power-up self-tests include the following:

- Software integrity
- Algorithm tests

Conditional self-tests must be run when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

The device uses a cryptographic algorithm known-answer test (KAT) to test FIPS mode for each FIPS 140-2-approved cryptographic function (encryption, decryption, authentication, and random number generation) implemented on the device. The device applies the algorithm to data for which the correct output is already known. It then compares the calculated output to the previously generated output. If the calculated output does not equal the known answer, the KAT fails.

Conditional self-tests run automatically when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

Conditional self-tests include the following:

- Pair-wise consistency test—This test is run when a public or private key-pair is generated.
- Continuous random number generator test—This test is run when a random number is generated.
- Bypass
- Software load

Configuring FIPS

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**fips authorization-key** [*option*] *key* **Example:** `Device(config)# fips authorization-key 0 12345678901234567890123456789012`	Enables the FIPS mode. The options are as follows: • **0**: Specifies that an UNENCRYPTED password will follow. • **7**: Specifies that an ENCRYPTED password will follow. • **LINE**: Use the cleartext 128-bits (16 octet) key. The *key* length should be of 32 hexadecimal characters. To disable FIPS mode on the device, use the **no** form of this command.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

What to do next

You must reboot the controller whenever you enable or disable the FIPS mode using the **reload** command.

After the system reloads, all the APs are FIPS enabled except the internal AP (Internal AP is the AP acting as the EWC). Therefore, reload the internal AP using the **wireless ewc-ap ap reload** command.

After the internal AP reload, the standby controller becomes the new active controller, and all APs are FIPS enabled.

Verifying FIPS Configuration

You can verify FIPS configuration using the following commands:

Use the following **show** command to display the installed authorization key:

```
Device# show fips authorization-key
```

```
FIPS: Stored key (16) : 12345678901234567890123456789012
```

Use the following **show** command to display the status of FIPS on the device:

```
Device# show fips status

Chassis is running in fips mode
```