FIPS

- FIPS, on page 1
- Guidelines and Restrictions for FIPS, on page 2
- FIPS Self-Tests, on page 2
- Configuring FIPS, on page 3
- Configuring FIPS in HA Setup, on page 4
- Verifying FIPS Configuration, on page 5

FIPS

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.

With FIPS in enabled state, some passwords and pre-shared keys must have the following minimum lengths:

- For Software-Defined Access Wireless, between the controller and map server, a pre-shared key (for example, the LISP authentication key) is used in authentication of all TCP messages between them. This pre-shared key must be at least 14 characters long.
- The ISAKMP key (for example, the Crypto ISAKMP key) must be at least 14 characters long.

Limitations for FIPS

- The console of APs get disabled when the controller is operating in FIPS mode.
- The weak or legacy cipher like SHA1 is not supported in FIPS mode.
- APs would not reload immediately, if you change the FIPS status.

Note We recommend a minimum RSA key size of 2048 bits under RADSEC when operating in FIPS mode. Otherwise, the RADSEC fails.

Guidelines and Restrictions for FIPS

- In the controller switches, 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.

Note You need to use FIPS compliant SSH clients to access the controller.

- While configuring WLAN ensure that the PSK length must be 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.
- FIPS is not compatible with level-6 encrypted passwords. Additionally, 802.1X authentications will fail if the RADIUS shared secret uses a type-6 encryption key.

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

Ensure that both the active and standby controllers have the same FIPS authorization key.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**fips authorization-key** *key* **Example:** `Device(config)# fips authorization-key 12345678901234567890123456789012`	Enables the FIPS mode. The key length should be of 32 hexadecimal characters. **Note** When FIPS is enabled, you may need to trigger more than one factory reset using the reset button. 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. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

What to do next

You must reboot the controller whenever you enable or disable the FIPS mode.

Configuring FIPS in HA Setup

While bringing up HA pair in FIPS mode, you need to configure both active and standby controllers with the same FIPS authorization key independently before forming HA pair.

If you configure FIPS authorization key after forming HA pair, the FIPS authorization key configuration will not be synced with the standby. Rebooting HA pair at this state causes reload loop. To avoid this, you need to perform the following:

- Break the HA pair.
- Configure the same FIPS authorization key independently on both the members.
- Pair up members.

To configure FIPS in HA setup, perform the following:

1. Power off both the members of the stack.
2. Power on only member1, and wait for the controller to come up and prompt for login from the console.
3. Login successfully with your valid credentials, and execute the following commands:

```
Show fips status
Show fips authorization-key
Show romvar
Show chassis
```

Note Keep the configured FIPS authorization key handy.

4. Configure the FIPS key, if you have not configured one earlier.

```
conf t
fips authorization-key <32 hex char>
```

5. Save and power off the member1.
6. Power on only member2 and wait for the controller to come up and prompt for login from the console.
7. Login successfully with your valid credentials, and execute the following commands:

```
Show fips status
Show fips authorization-key
Show romvar
Show chassis
```

Note Keep the configured FIPS authorization key handy.

8. Configure the FIPS key, if you have not configured one earlier.

Note The key value must be the same in both the members of the stack.

```
conf t
fips authorization-key <32 hex char>
```

9. Save and power off the member2.
10. Power on both the members together, and wait for the stack to form.
11. Monitor any crash or unexpected reload.

Note It is expected that members must not reload due to FIPS issue.

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
```