



FIPS

- [Federal Information Processing Standard \(FIPS\), on page 1](#)

Federal Information Processing Standard (FIPS)

A Federal Information Processing Standard (FIPS) is a security standard that

- defines requirements for cryptographic modules intended to secure sensitive but unclassified (SBU) information
- is mandated for use by U.S. government agencies and adopted by many regulated industries such as finance and healthcare, and
- establishes assurance levels to validate the strength and reliability of cryptographic implementations.

Sensitive but unclassified (SBU) information: Data that, while not classified for national security, still requires protection due to its sensitive nature and potential impact if disclosed.

Additional reference information

Federal Information Processing Standard (FIPS) 140-2 is a well-known FIPS standard specifying security requirements for cryptographic modules protecting SBU information. These cryptographic modules are produced by the private sector for use in government and regulated environments.

With FIPS in the 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 (such as the LISP authentication key) used for authenticating TCP messages must be at least 14 characters long.
- The ISAKMP key (for example, the Crypto ISAKMP key) must also be at least 14 characters long.

Guidelines and restrictions for FIPS

- Controller switches use a legacy key to support legacy APs. In FIPS mode, the crypto engine identifies the key as weak and displays this error message: **% Error in generating keys: could not generate test signature.** Ignore error messages during controller startup in FIPS mode.

- When you enable FIPS, SSH clients that use SHA1 cannot access the controller.
- You need to use FIPS-compliant SSH clients to access the controller.
- You cannot use TrustSec in FIPS mode.
- You cannot configure PAC keys in FIPS mode.
- You cannot use level-6 encrypted passwords in FIPS mode. Also, 802.1X authentications fail if the RADIUS shared secret uses a type-6 encryption key.
- 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.
- 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 FIPS self-test is a cryptographic module validation mechanism that

- verifies functionality and integrity during device power-up
- performs conditional checks whenever security functions are invoked, and
- ensures FIPS 140-2 compliance by enforcing automated self-testing procedures.

Power-up self-tests

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

The module uses a known-answer test (KAT), in which a cryptographic algorithm runs on data for which the correct output is already known, and then the calculated output is compared to this expected value. If the calculated output does not equal the known answer, the known-answer test fails.

Power-up self-tests include:

- Software integrity: Validates the integrity of module software as it loads.
- Algorithm tests: Verifies correct operation of cryptographic algorithms using KATs.

Conditional self-tests

Conditional self-tests are performed each time an applicable security function or operation is accessed, unlike power-up self-tests that run only at startup.

The device uses a cryptographic algorithm known-answer test (KAT) on each FIPS 140-2-approved function, which includes encryption, decryption, authentication, and random number generation. The algorithm is applied to a set of data with a known correct output, and the calculated output is compared to this known value. If the calculated output is different, the KAT fails.

Conditional self-tests run automatically whenever their associated security function or operation is invoked. They include the following:

- Pair-wise consistency test: Runs when a public or private key-pair is generated to confirm the correct relationship.
- Continuous random number generator test: Runs each time a random number is generated to check the quality of randomness.
- Bypass: Evaluates bypass operations if performed.
- Software load: Validates integrity when new software is loaded.

Examples

- When a device boots, it performs power-up self-tests to confirm its cryptographic algorithms work as intended before entering FIPS mode.
- Whenever the device generates a new cryptographic key pair, a pair-wise consistency test is executed.
- If a random number is generated, the system runs a continuous random number generator test, verifying the output for compliance.

Configure FIPS (CLI)

Enable or disable FIPS mode on controllers for compliance and security.

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

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device
# configure terminal
```

Step 2 Enable FIPS mode.

Example:

```
Device
(config)#
fips authorization-key key
```

The key length must be 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 Return to privileged EXEC mode.

Example:

```
Device
(config)#
end
```

Enable or disable FIPS mode. Reboot the controller to apply changes. After the controller reboots, access points also reboot once they rejoin.

What to do next

Reboot the controller each time you enable or disable FIPS mode.

How FIPS configuration works in high availability setups

Set up a high availability (HA) pair in FIPS mode by configuring both controllers with the same FIPS authorization key before forming the HA pair.

If you configure the key after forming the HA pair, it will not sync to the standby. This may cause reload loops when you reboot.

- Break the HA pair if you configured the FIPS key after pairing.
- Configure the same FIPS authorization key on both members independently.
- Form the HA pair again.

Summary

In this process, you configure FIPS in an HA setup by setting the same FIPS authorization key on both members before forming the HA pair.

- You must perform the configuration steps on both controllers.
- Configure and pair both controllers (member1 and member2) in HA mode.

Matching FIPS authorization keys on both controllers in the HA pair prevent synchronization issues and reload loops.

Workflow

These stages describe the steps to configure FIPS in an HA setup.

1. Turn off both members of the stack.
2. Power on only member1 and wait for the controller to start. Log in from the console when prompted.
3. Log in to member1 with valid credentials and use the following commands to verify FIPS status and configuration:
 - Use the **show fips status** command

- Use the **show fips authorization-key** command
- Use the **show romvar** command
- Use the **show chassis** command



Note Keep the configured FIPS authorization key available.

4. Configure the FIPS key on member1 if you have not already configured it.
 - conf t
 - fips authorization-key <thirty-two hexadecimal characters>
5. Save your changes and power off member1.
6. Power on only member2 and wait for the controller to start. Log in from the console when prompted.
7. Log in to member2 with valid credentials and use the following commands to verify FIPS status and configuration:
 - Use the **show fips status** command
 - Use the **show fips authorization-key** command
 - Use the **show romvar** command
 - Use the **show chassis** command



Note Keep the configured FIPS authorization key available.

8. Configure the FIPS key on member2 if you have not already configured it.



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

- conf t
 - fips authorization-key <thirty-two hexadecimal characters>
9. Save your changes and power off member2.
 10. Power on both members together and wait for the stack to form.
 11. Monitor the system for any crash or unexpected reload events.



Note The members are not expected to reload because of FIPS issues.

Result

Both controllers in the HA pair operate in synchronized FIPS mode. Correct configuration prevents synchronization issues and reload loops caused by mismatched or improperly applied FIPS authorization keys.

Verify FIPS configuration

You can verify FIPS configuration using these commands:

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

```
Device# show fips authorization-key  
FIPS: Stored key (16) : 12345678901234567890123456789012
```

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

```
Device# show fips status  
Chassis is running in fips mode
```