FIPS

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.

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.

- 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. 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. After the controller is rebooted, the APs, as soon as they rejoin the controller, also reboot.

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.

Monitoring FIPS

Use the following commands to view information about FIPS:

Command	Purpose
show fips authorization-key	Displays the installed authorization key.
show fips status	Displays the status of FIPS on the device.

CC

Information About Common Criteria

Common Criteria (CC) is a testing standard that verifies if the device provides security functionalities as claimed by the product developers. The CC certificate is recognised officially in 24 countries.

CC covers a set of requirements, tests, and evaluation methodology that assures that the Target of Evaluation (ToE) complies to a specific protection profile. In our case, the ToE must comply with the following protection profiles:

- Collaborative Protection Profile for Network Devices (NDcPP) v2 dated May 5, 2017
- Wireless Local Area Network (WLAN) Access Systems Extended Package version 1 May 29, 2015

For more information about CC, see

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

Configuring Common Criteria

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless wlancc** **Example:** `Device(config)# wireless wlancc`	Configures the Common Criteria mode for the controller. **Note** Reboot the controller after enabling the common criteria mode.
Step 3	**ap dtls-cipher** *ciphersuite* **Example:** `Device(config)# ap dtls-cipher DHE-RSA-AES256-SHA256`	Configures the cipher suite supported by DTLS. **Note** Reboot the controller to activate the selected cipher suite.
Step 4	**ap dtls-version** {**dtls_1_0** | **dtls_1_2**} **Example:**	Configure DTLS version 1.0 or 1.2.

	Command or Action	Purpose
	`Device(config)# ap dtls-version dtls_1_2`	**Note** Save the configuration and reload the controller for the changes to take effect.

Step 5	**end**
	Example:
	`Device(config)# end`
		Exits the configuration mode and enters the privileged EXEC mode.

Verifying CC Configuration

Use the following **show** command to display the wireless certification configurations:

```
Device# show wireless certification config
Wireless Certification Configurations

WLANCC                                      : Configured
AP DTLS Cipher Suite                        : DHE-RSA-AES128-SHA
                                              DHE-RSA-AES256-SHA
                                              DHE-RSA-AES256-SHA256
                                              ECDHE-ECDSA-AES128-GCM-SHA256
                                              ECDHE-ECDSA-AES256-GCM-SHA384
AP DTLS Version                             : DTLS v1.2
```

Check Points for CC Mode Operation

You need to be aware of the following for CC mode operation:

Table 1: Check Points for CC Mode Operation

Features	Description
Link encryption	Data link encryption is not supported for C91xx wireless mobility express platform.
Link encryption	For non-C91xx wireless mobility express platfoms - Enabling Data link encryption (using ECDHE keypair) would make AP flap continually.
LDAP	Secure LDAP does not support strong ciphers and is not part of CC certification.
Mobility	Mobility between Cisco Catalyst 9800 Series Wireless controllers is possible with LSC as wireless management trustpoint (having RSA based keys).
Mobility	Mobility between AireOS WLC and Cisco Catalyst 9800 Series Wireless controllers is supported (using SUDI and MIC certificates for wireless management trustpoint).

Features	Description
Mobility	Mobility between AireOS WLC and Cisco Catalyst 9800 Series Wireless controllers is not supported (if using LSC certficates for wireless management trustpoint).
CC mode	The **show wireless certification config** command displays the configured values for WLANCC, or AP-dtls-ciphersuite, or AP-dtls-version, and needs reload after re-configuring these parameters.
CC mode	The AES128-SHA option is not supported for AP-dtls-ciphersuite when Cisco Catalyst 9800 Series Wireless Controller is operating in CC mode.
CC mode	The AES128-SHA option is supported for AP-dtls-ciphersuite when Cisco Catalyst 9800 Series Wireless Controller is operating in FIPS mode.
CC mode	If you want your Cisco Catalyst 9800 Series Wireless Controller to operate in CC mode (you need to enable both FIPS mode and CC mode).
LSC	To secure communication between Cisco Catalyst 9800 Series Wireless Controller and LSC server, you need to deploy ESTCA as LSC server (which uses TLS to secure related communication).
LSC	Cisco Catalyst 9800 Series Wireless Controllers do not support HTTPS to secure its communication with the LSC server.
LSC	During LSC provisioning, APs generate EC based keys only when related Cisco Catalyst 9800 Series Wireless Controller is operating in CC mode.
LSC	During LSC provisioning, APs generate RSA based keys when related Cisco Catalyst 9800 Series Wireless Controller is operating in FIPS mode.
LSC	During LSC provisioning, APs generate RSA based keys when related Cisco Catalyst 9800 Series Wireless Controlle is operating in non-FIPS or non-CC mode.
Password Obfuscation	You can use the following commands for password obfuscation: • **key config-key password-encrypt** • **service password-encryption** • **password encryption aes** • **passwd key obfuscate**

Features	Description
CC mode	APs reload immediately, if you change the **wlancc** status.
FIPS mode	APs do not reload immediately, if you change the FIPS status.
Cisco 1562 AP	To assist Cisco 1562 APs join the Cisco Catalyst 9800 Series wireless controller, you need to have the ethernet MAC of the AP in the username list.
AP serial number authorization	Serial number authorization is possible only when Cisco Catalyst 9800 Series wireless controller is in FIPS and CC mode, and with LSC based trustpoints/certficates only (not with SUDI trustpoint).
Display	FIPS suitability displays **Suitable only** if the controller is in CC mode and LSC certificate is compatible. Both wireless management and Certs CN should match the hostname of the controller and length of RSA Key (> 2048) (or) EC keys being used.
RADSEC	RSA key size must contain a minimum of 2048 bits (of certificate under RADSEC) when operating in FIPS or CC mode, else RADSEC fails.