# Configuring FIPS

This chapter describes how to configure the Federal Information Processing Standards (FIPS) mode on Cisco NX-OS devices.

This chapter includes the following sections:



## Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information"chapter or the Feature History table in this chapter.

## Information About FIPS

The FIPS 140-2 Publication, *Security Requirements for Cryptographic Modules*, details the U.S. government requirements for cryptographic modules. FIPS 140-2 specifies that a cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary.

FIPS specifies certain cryptographic algorithms as secure, and it identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.

# FIPS Self-Tests

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

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.

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.

The Cisco TrustSec manager also runs a bypass test to ensure that encrypted text is never sent as plain text.

**Note** A bypass test failure on CTS-enabled ports causes only those corresponding ports to be shut down. The bypass test might fail because of packet drops caused by data path congestion. In such cases, we recommend that you try bringing up the port again.

# FIPS Error State

When the system is booted up in FIPS mode, the FIPS power-up self-tests run on the supervisor and line card modules. If any of these bootup tests fail, the whole system is moved to the FIPS error state. In this state, as per the FIPS requirement, all cryptographic keys are deleted, and all line cards are shut down. This mode is exclusively meant for debugging purposes.

Once the switch is in the FIPS error state, any reload of a line card moves it to the failure state. To move the switch back to FIPS mode, it has to be rebooted. However, once the switch is in FIPS mode, any power-up self-test failure on a subsequent line card reload or insertion affects only that line card, and only the corresponding line card is moved to the failure state.

# RADIUS Keywrap

RADIUS keywrap support is an extension of the RADIUS protocol. It provides a FIPS-certifiable means for the Cisco Access Control Server (ACS) to authenticate RADIUS messages and distribute session keys.

RADIUS keywrap increases RADIUS protocol security by using the Advanced Encryption Standard (AES) keywrap algorithm to transfer keys while an HMAC-SHA1 algorithm is used to protect packet integrity. It

specifies that the key encryption key (KEK) and the hash key must be different from each other, should not be based on a password, and must be cryptographically independent of the RADIUS shared secret used in calculating the response authenticator.

**Note** The proxy and message authenticator are not supported for RADIUS keywrap.

When FIPS mode is enabled, RADIUS keywrap is enabled automatically. As a result, keywrap attributes are added to any RADIUS request that contains EAP attributes but is not meant for protected access credential (PAC) provisioning. The attributes are sent to the Cisco ACS, which distributes the EAP-TLS session key to an IEEE 802.1X EAP authenticator. The session key is encrypted using AES, and the RADIUS message is authenticated using HMAC-SHA-1.

**Note** Cisco ACS Release 5.2 supports the RADIUS keywrap feature.

## Virtualization Support for FIPS

You can configure FIPS mode and run FIPS self-tests only in the default virtual device context (VDC). For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

# Prerequisites for FIPS

FIPS has the following prerequisites:

- Disable Telnet. Users should log in using Secure Shell (SSH) only.
- Disable SNMPv1 and v2. Any existing user accounts on the device that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Delete all SSH server RSA1 key-pairs.
- Enable HMAC-SHA1 message integrity checking (MIC) for use during the Cisco TrustSec Security Association Protocol (SAP) negotiation. To do so, enter the **sap hash-algorithm HMAC-SHA-1** command from the cts-manual or cts-dot1x mode. Note that this command is not supported for F1 Series or F2 Series modules.

# Guidelines and Limitations for FIPS

FIPS has the following configuration guidelines and limitations:

- The RADIUS keywrap feature works only with Cisco ACS Release 5.2 or later releases.
- The user authentication mechanisms supported for SSH are usernames and passwords, public keys, and X.509 certificates.
- Your passwords should have a minimum of eight alphanumeric characters.

- The F1 Series and F2 Series modules do not support FIPS mode. However, you can deploy an F1 Series or F2 Series module in a Cisco NX-OS device that is operating in FIPS mode.
- The F1 Series and F2 Series modules do not support the cts-dot1x mode or the cts-manual mode.
- Digital image signing is supported on Cisco Nexus 7000 Series switches that contain the Supervisor 2 module.
- The M2 Series modules do not support FIPS mode. However, you can deploy an M2 Series module in a Cisco NX-OS device that is operating in FIPS mode.

# Default Settings for FIPS

This table lists the default settings for FIPS parameters.

***Table 1: Default FIPS Parameters***

| Parameters | Default |
|---|---|
| FIPS mode | Disabled |

# Configuring FIPS

This section describes how to configure FIPS mode on Cisco NX-OS devices.

## Enabling FIPS Mode

Beginning with Cisco NX-OS Release 5.1, you can enable FIPS mode on the device.

### Before you begin

Ensure that you are in the default VDC.

### SUMMARY STEPS

1. **configure terminal**
2. **fips mode enable**
3. **exit**
4. (Optional) **show fips status**
5. **copy running-config startup-config**
6. **reload**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **fips mode enable**<br>**Example:**<br>`switch(config)# fips mode enable` | Enables FIPS mode.<br>**Note** **fips mode enable** could be typed only when All LC s are online or else it leads to LC failure. |
| **Step 3** | **exit**<br>**Example:**<br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |
| **Step 4** | (Optional) **show fips status**<br>**Example:**<br>`switch# show fips status`<br>`FIPS mode is enabled` | Displays the status of FIPS mode. |
| **Step 5** | Required: **copy running-config startup-config**<br>**Example:**<br>`switch# copy running-config startup-config` | Copies the running configuration to the startup configuration. |
| **Step 6** | Required: **reload**<br>**Example:**<br>`switch# reload` | Reloads the Cisco NX-OS device.<br>**Note** After you enable FIPS, a reboot is required for the system to operate in FIPS mode. |

#### Related Topics

Disabling FIPS Mode, on page 5

# Disabling FIPS Mode

You can disable FIPS mode on the device.

#### Before you begin

Ensure that you are in the default VDC.

### SUMMARY STEPS

1. **configure terminal**
2. **no fips mode enable**
3. **exit**
4. (Optional) **show fips status**

5. **copy running-config startup-config**
6. **reload**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`switch# configure terminal`<br>`switch(config)#` | Enters global configuration mode. |
| **Step 2** | **no fips mode enable**<br>**Example:**<br>`switch(config)# no fips mode enable` | Disables FIPS mode. |
| **Step 3** | **exit**<br>**Example:**<br>`switch(config)# exit`<br>`switch#` | Exits configuration mode. |
| **Step 4** | (Optional) **show fips status**<br>**Example:**<br>`switch# show fips status`<br>`FIPS mode is disabled` | Displays the status of FIPS mode. |
| **Step 5** | Required: **copy running-config startup-config**<br>**Example:**<br>`switch# copy running-config startup-config` | Copies the running configuration to the startup configuration. |
| **Step 6** | Required: **reload**<br>**Example:**<br>`switch# reload` | Reloads the Cisco NX-OS device. |

**Related Topics**

Enabling FIPS Mode, on page 4

# Verifying the FIPS Configuration

To display FIPS configuration information, perform one of the following tasks:

| Command | Purpose |
|---|---|
| **show fips status** | Displays the status of the FIPS feature. |

For detailed information about the fields in the output from this command, see the *Cisco Nexus 7000 Series NX-OS Security Command Reference*.

# Configuration Example for FIPS

The following example shows how to enable FIPS mode:

```
config terminal
fips mode enable
show fips status
exit
copy running-config startup-config
reload
```

# Additional References for FIPS

This section includes additional information related to implementing FIPS.

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco NX-OS licensing | *Cisco NX-OS Licensing Guide* |
| Command reference | *Cisco Nexus 7000 Series NX-OS Security Command Reference* |
| VDC configuration | *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide* |

### Standards

| Standards | Title |
|---|---|
| FIPS 140-2 | Security Requirements for Cryptographic Modules |

# Feature History for FIPS

This table lists the release history for this feature.

***Table 2: Feature History for FIPS***

| Feature Name | Releases | Feature Information |
|---|---|---|
| FIPS | 6.1(1) | Added support for digital image signing on switches that contain the Supervisor 2 module. |
| FIPS | 6.1(1) | Updated FIPS guidelines for M2 Series modules. |

| Feature Name | Releases | Feature Information |
|---|---|---|
| FIPS | 6.0(1) | Updated FIPS guidelines for F2 Series modules. |
| FIPS | 5.1(1) | This feature was introduced. |