

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:

- About FIPS, on page 1
- Prerequisites for FIPS, on page 2
- Guidelines and limitations for FIPS, on page 3
- Default settings for FIPS, on page 3
- Configuring FIPS, on page 3
- FIPS configuration verification commands, on page 5
- Create 2048 bit RSA key, on page 5
- Configuration example for FIPS, on page 6
- Additional references for FIPS, on page 6

About FIPS

The FIPS 140–2 Publication, *Security Requirements for Cryptographic Modules*, describes U.S. government requirements for cryptographic modules. According to FIPS 140–2, a cryptographic module is a set of hardware, software, firmware, or a combination of these components that implements cryptographic functions and is contained within a defined boundary. These modules provide cryptographic algorithms and, optionally, key generation.

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.

Generate the "crypto key generate rsa label test exportable modulus" with a minimum modulus size of 2048. A key size less than 2048 is categorized as a “FIPS Self-Test” or results in a "FIPS Error State".

The device uses a cryptographic algorithm known-answer test (KAT) for each FIPS 140- 3 -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, and then compares the calculated output to this known answer. If the calculated output does not match the known answer, the KAT fails.

Conditional self-tests include these tests:

- Pair-wise consistency test: This test runs when a public or private key-pair is generated.
- Continuous random number generator test: This test runs 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, the system deletes all cryptographic keys and shuts down all line cards as required by FIPS. This mode is exclusively meant for debugging purposes.

After 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, a power-up self-test failure during a line card reload or insertion affects only that line card, and only the corresponding line card is moved to the failure state.

Prerequisites for FIPS

FIPS has the following prerequisites:

- Disable Telnet. Users should log in using Secure Shell (SSH) only.
- 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 Cisco TrustSec Security Association Protocol (SAP) negotiation. Enter the **sap hash-algorithm HMAC-SHA-1** command in `cts-manual` or `cts-dot1x` mode.

Guidelines and limitations for FIPS

Use this reference to review the guidelines and limitations for FIPS.

FIPS has these configuration guidelines and limitations:

- The user authentication mechanisms supported for SSH are usernames and passwords, public keys, and X.509 certificates.
- Passwords must consist of at least eight alphanumeric characters.
- You must disable Radius and TACACS when FIPS mode is on, because OpenSSL enforces this requirement in FIPS mode.
- When RadSec is enabled, Radius doesn't need to be disabled when FIPS is enabled.
- When the **fips mode enable** command is executed after an ASCII reload, you need to reload the Cisco NX-OS switch after executing the **copy running-config startup-config** command.

Default settings for FIPS

Use this reference to review the 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.

Enable FIPS mode

Before you begin

Ensure that you are in the default VDC.

Procedure

Step 1 Enter global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Enable FIPS mode.

Example:

```
switch(config)# fips mode enable
```

Note
fips mode enable can be entered only when all LCs are online or else it leads to LC failure.

Step 3 Exit configuration mode.

Example:

```
switch(config)# exit
switch#
```

Step 4 (Optional) Display the status of FIPS mode.

Example:

```
switch# show fips status
FIPS mode is enabled
```

Step 5 Required: Copy the running configuration to the startup configuration.

Example:

```
switch# copy running-config startup-config
```

Step 6 Required: Reload the Cisco NX-OS device.

Example:

```
switch# reload
```

Note
After you enable FIPS, a reboot is required for the system to operate in FIPS mode.

Disable FIPS

You can disable FIPS mode on the device using the CLI.

Before you begin

Ensure that you are in the default VDC.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
switch# configure terminal
switch(config)#
```

Step 2 Disable FIPS mode.

Example:

```
switch(config)# no fips mode enable
```

Step 3 Exit the configuration mode.

Example:

```
switch(config)# exit
switch#
```

Step 4 (Optional) Display the status of FIPS mode.

Example:

```
switch# show fips status
FIPS mode is disabled
```

Step 5 Copy the running configuration to the startup configuration.

Example:

```
switch# copy running-config startup-config
```

Step 6 Reload the Cisco NX-OS device.

Example:

```
switch# reload
```

FIPS configuration verification commands

Use this reference to verify the FIPS configuration.

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

Table 2: Table 1

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 9000 Series NX-OS Security Command Reference* .

Create 2048 bit RSA key

Steps to create a 2048 bit RSA key:

- Enter global configuration mode.

```
N9k-Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

- Disable the SSH feature to allow removal or regeneration of SSH keys safely.

```
N9k-Switch(config)#no feature ssh
XML interface to system may become unavailable since ssh is disabled
```

- Remove the existing RSA SSH key from the device configuration and generate a new RSA SSH key with a 2048-bit length to enhance security.

```
N9k-Switch(config)#no ssh key rsa
N9k-Switch(config)#ssh key rsa 2048
New SSH Key has a bitcount of 2048:
```

- Verify the configured SSH keys and their details.

```
N9k-Switch#show ssh key
**************************************
rsa Keys generated:Wed Apr 28 13:05:18 2021
ssh-rsa  AAAAB3NzaC1yc2EAAAADAQABAAABAQDHpxEgZ9LwmbOEpJeJtLwqedmTLkZV7Setxb9D4xgO
rsa Keys generated:Wed Apr 28 13:05:18 2021
ssh-rsa  AAAAB3NzaC1yc2EAAAADAQABAAABAQDHpxEgZ9LwmbOEpJeJtLwqedmTLkZV7Setxb9D4xgO
p2o2f6wt/48bPp/vLDGsxTF2PtLRtRSSDFNSQmkw9bg+MXvTpgNivdxWLjxtwo3YpYwPkBiReVmyrFgE
UuBmV/sDfhJpHXLoH9lR2+y0L5w1OG3cJxMe30TI37O3M8fZPjrAtHgkUubfEpiTbcyEw+aIHf+chyoR
eDJxcEdnlboiTDFR0/+jMUUM/vMtxd5x5DH3AO7htA/i8lvskrReR1CpX1sOOdcshmS57EEuEzR9cs+w
KSftQh6vLD802207T6+J7/+cXMVNQEbq0mCSzeTmOsuIQe8u9ZC24pgYzZ19
bitcount:2048
fingerprint:
SHA256:Am9861AIq5MzfSPQr4ZXGe0f5M9crnhk7HVZBXhMVBo
**************************************
could not retrieve dsa key information
**************************************
could not retrieve ecdsa key information
**************************************
```

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

Table 3: Table 1

Related Topic	Document Title
Cisco NX-OS licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 9000 Series NX-OS Security Command Reference*

Standards

Table 4: Table 3

Standards	Title
FIPS 140-2	Security Requirements for Cryptographic Modules