

Configuring FIPS

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

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

Note From Cisco MDS NX-OS Release 8.3(1) and later, FIPS is compliant on Cisco MDS devices. On Cisco MDS NX-OS Release 7.x and earlier, FIPS feature is supported, but it is not FIPS compliant (certification process is with the U.S. government). For current FIPS compliance, refer to the *Table 1 Current FIPS Compliance Reviews* section in the Cisco FIPS 140 document.

This chapter includes the following sections:

- Configuration Guidelines, on page 1
- Enabling FIPS Mode, on page 2
- Displaying FIPS Status, on page 3
- FIPS Self-Tests, on page 3

Configuration Guidelines

Follow these guidelines before enabling FIPS mode:

- Make your passwords a minimum of eight characters in length.
- Keep Telnet disabled. Users should log in using SSH only.
- Disable remote authentication through RADIUS/TACACS+. Only users local to the switch can be authenticated.
- Disable SNMP v1 and v2. Any existing user accounts on the switch that have been configured for SNMPv3 should be configured only with SHA for authentication and AES/3DES for privacy.
- Disable VRRP.

Note This step is applicable to Cisco NX-OS software release 8.3(1) or older versions.

- Do not configure FIPS and IPsec together on a switch. With FIPS enabled, if you configure IKE, then FCIP links will not come up.
- Delete all SSH Server RSA1 keypairs.
- If FIPS is enabled and you upgrade from Cisco MDS NX-OS Release 8.1(x) to Cisco MDS NX-OS Release 8.2(1) or later release, then you cannot disable FIPS in the upgraded 8.2(x) release.
- Fibre Channel Security Protocol (FCSP) and Network Time Protocol (NTP) are not FIPS compliant in Cisco MDS devices. This is because both protocols are not cryptographically secure and don't meet FIPS 140-2 standards. Using non-FIPS compliant components like FCSP and NTP with MD5 in Cisco MDS devices can potentially lead to vulnerabilities.
- For Cisco MDS NX-OS 8.5(1) and later releases, SSH clients may no longer use ssh-rsa key exchange when the switch is in FIPS mode as ssh-rsa uses an insecure SHA1 signature. SSH clients must use `rsa-sha2-256` for RSA key exchange instead. Older NX-OS SSH server versions were not strict in enforcing this restriction.

Enabling FIPS Mode

To enable FIPS mode, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `switch# configure terminal`	Enters configuration mode.
Step 2	**no ssh keytypes all** **Example:** `switch(config)# no ssh keytypes all`	Disables ssh-dss key type. The ssh-dss algorithm is not compliant with FIPS standards. Disable it before enabling FIPS mode.
Step 3	**fips mode enable** **Example:** `switch(config)# fips mode enable`	Enables FIPS mode.
Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the switch configuration.
Step 5	**reload**	Reloads the switch.

	Command or Action	Purpose

	Example:
	`switch(config)# reload`
	`This command will reboot the system.`
	`(y/n)?  [n] y`
		The switch must be rebooted after saving the configuration to enable FIPS mode.

Step 6	**no fips mode enable** **Example:** `switch(config)# no fips mode enable`	(Optional) Disables FIPS mode. The switch must be rebooted after saving the configuration to disable FIPS mode.

Displaying FIPS Status

To view FIPS status, enter the **show fips status** command. The following example displays the output of the above command where FIPS mode is enabled.

```
switch(config)# show fips status
FIPS mode is enabled
```

FIPS Self-Tests

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

Note FIPS power-up self-tests automatically run when FIPS mode is enabled by entering the fips mode enable command. A switch is in FIPS mode only after all self-tests are successfully completed. If any of the self-tests fail, then the switch is rebooted.

Power-up self-tests run immediately after FIPS mode is enabled. A cryptographic algorithm test using a known answer must be run for all cryptographic functions for each FIPS 140-3-approved cryptographic algorithm implemented on the Cisco MDS 9000 Family.

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.

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.

Conditional self-tests include the following:

- Pair-wise consistency test—This test is run when a public-private keypair is generated.
- Continuous random number generator test—This test is run when a random number is generated.

Both of these tests automatically run when a switch is in FIPS mode.