



FIPS Commands

This module describes the commands used in enabling the FIPS mode.

For detailed information about FIPS configuration tasks, and examples, see the *Configuring FIPS Mode* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers* and *System Security Configuration Guide for Cisco 8000 Series Routers*.

- [crypto fips-mode](#), on page 2

crypto fips-mode

To configure FIPS, use the **crypto fips-mode** command in the global configuration mode. To remove FIPS configuration, use the **no** form of this command.

crypto fips-mode
no crypto fips-mode

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Global configuration

Command History	Release	Modification
	Release 7.0.12	This command was introduced.

Usage Guidelines



Note You must reload the router for this configuration to take effect.

Use the **show logging** command to display the contents of logging buffers. You can use the **show logging | i fips** command to filter FIPS specific logging messages.

You must configure the session with a FIPS-approved cryptographic algorithm. A session configured with non-approved cryptographic algorithm for FIPS (such as, **MD5** and **HMAC-MD5**) does not work. This is applicable from Cisco IOS XR Software Release 7.2.1 and later, for OSPF, BGP, RSVP, ISIS, or any application using key chain with non-approved cryptographic algorithm, and only for FIPS mode (that is, when **crypto fips-mode** is configured).

Task ID	Task	Operation
	crypto read, write	

Example

This example shows how to configure FIPS:

```
RP/0/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto fips-mode
```