



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 *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

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

crypto fips-mode

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

crypto fips-mode

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Global Configuration mode

Command History	Release	Modification
	Release 4.3.1	This command was introduced.

Usage Guidelines Install and activate the **asr9k-k9sec-px.pie** file before using this command.



Note For the configuration to take effect, reload the router by using the reload command in the admin mode.

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 6.7.2, Release 7.1.2, 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 ID	Operation
	crypto	read, write

Example

This example shows how to configure FIPS:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto fips-mode
```