



# Fabric Security

---

This chapter contains the following sections:

- [About Federal Information Processing Standards \(FIPS\), on page 1](#)
- [Guidelines and Limitations for FIPS, on page 1](#)
- [Configuring FIPS for Cisco APIC Using the GUI, on page 2](#)
- [Configuring FIPS for Cisco APIC Using the NX-OS Style CLI, on page 2](#)
- [Configuring FIPS for Cisco APIC Using REST API, on page 3](#)

## About Federal Information Processing Standards (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 cryptographic algorithms as secure, and it also identifies which algorithms should be used if a cryptographic module is to be called FIPS compliant.

## Guidelines and Limitations for FIPS

The following guidelines and limitations apply to FIPS:

- When FIPS is enabled, FIPS is applied across the Cisco Application Policy Infrastructure Controller (APIC).
- When FIPS is enabled, you must disable FIPS before you downgrade the Cisco APIC to a release that does not support FIPS.
- Make your passwords a minimum of eight characters in length.
- Disable Telnet. Log in using only SSH. Telnet is not supported in 5.3(1) and later releases.
- Delete all SSH Server RSA1 keypairs.
- Secure Shell (SSH) and SNMP are supported.

- 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 for privacy.
- Starting with the 2.3(1) release, FIPS can be configured at the switch level.
- Starting with the 3.1(1) release, when FIPS is enabled, NTP will operate in FIPS mode, Under FIPS mode NTP supports authentication with HMAC-SHA1 and no authentication.
- In the 5.2(3) release and earlier, after enabling FIPS on the Cisco APIC, reload the dual supervisor spine switches twice for FIPS to take effect.
- In the 5.2(4) release and later, after enabling FIPS on the Cisco APIC, reload and then power cycle the dual supervisor spine switches for FIPS to take effect.
- In the 5.2(3) release and earlier, on a dual supervisor spine switch that has FIPS enabled, if all the supervisors are replaced, then the spine switch must be reloaded twice for FIPS to take effect.
- In the 5.2(4) release and later, on a dual supervisor spine switch that has FIPS enabled, if all supervisors are replaced, then the spine switch must be reloaded and then power cycled for FIPS to take effect.
- In the 5.2(3) release and earlier, disable the RADIUS and TACACS+ remote authentication methods. Only the local and LDAP authentication methods are supported in FIPS mode.
- In the 5.2(4) release and later, disable the RADIUS, TACACS+, and RSA remote authentication methods. Only the local, LDAP, OAuth2, and SAML authentication methods are supported in FIPS mode.

## Configuring FIPS for Cisco APIC Using the GUI

When FIPS is enabled, it is applied across the Cisco Application Policy Infrastructure Controller (APIC).

### Procedure

---

- Step 1** On the menu bar, choose **System > System Settings**.
- Step 2** In the **Navigation** pane, choose **Fabric Security**.
- Step 3** In the **Work** pane, in the **Properties** area, choose the desired FIPS mode.
- The options for FIPS mode are **Disable** and **Enable**. The default value is **Disable**.

#### Note

You must reboot to complete the configuration. Anytime you change the mode, you must reboot to complete the configuration.

---

## Configuring FIPS for Cisco APIC Using the NX-OS Style CLI

When FIPS is enabled, it is applied across Cisco Application Policy Infrastructure Controller (APIC).

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	Enter the configuration mode.  <b>Example:</b> <code>apic1# configure</code>	
<b>Step 2</b>	Enable FIPS.  <b>Example:</b> <code>apic1(config)# fips mode enable</code>	You must reboot to complete the configuration. Anytime you change the mode, you must reboot to complete the configuration.  The <b>no fips mode enable</b> command disables FIPS.

## Configuring FIPS for Cisco APIC Using REST API

When FIPS is enabled, it is applied across Cisco APIC.

**Procedure**


---

Configure FIPS for all tenants.

**Example:**

```
https://apic1.cisco.com/api/node/mo/uni/userext.xml
<aaaFabricSec fipsMode="enable" />
```

**Note**

You must reboot to complete the configuration. Anytime you change the mode, you must reboot to complete the configuration.

---

