# Fabric Security

This chapter contains the following sections:



## 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.
- 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.
- Disable remote authentication through RADIUS/TACACS+. Only local and LDAP users can be authenticated.
- After enabling FIPS on the Cisco APIC, reload the dual supervisor spine switches twice for FIPS to take effect.
- On a dual supervisor spine switch that has FIPS enabled, if a supervisor is replaced, then the spine switch must be reloaded twice for FIPS to take effect on the new supervisor.
- 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.

# Configuring FIPS for Cisco APIC Using the GUI

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

**Procedure**

**Step 1** On the menu bar, choose **Admin** > **AAA**.

**Step 2** In the **Navigation** pane, expand **AAA** > **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 NX-OS Style CLI

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

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure**<br>**Example:**<br>`apic1# configure` | Enters configuration mode. |
| **Step 2** | **fips mode enable**<br>**Example:** | Enables FIP. The **no fips mode enable** command disables FIPS. |

| | Command or Action | Purpose |
|---|---|---|
| | `apic1(config)# fips mode enable` | 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 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.