

Secure Operation in FIPS Mode on NFVIS

Table 1: Feature History

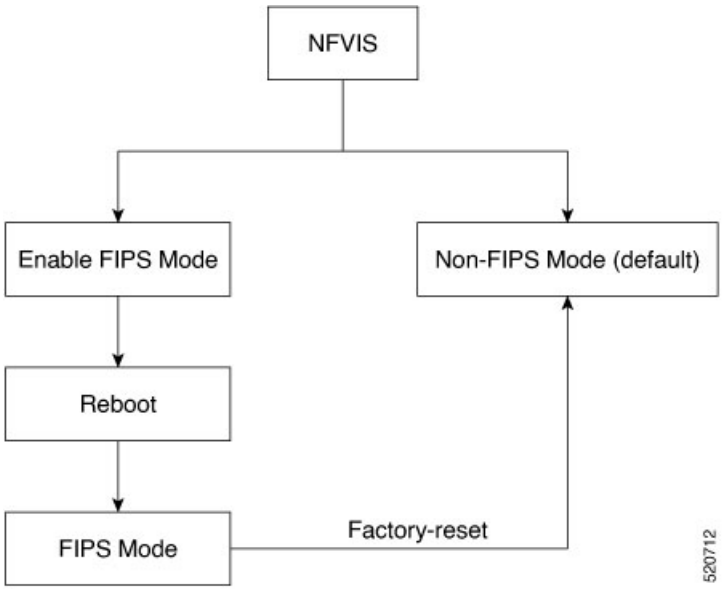
Feature Name	Release Information	Description
Secure Operation in FIPS Mode on NFVIS	NFVIS 4.2.1	The Federal Information Processing Standards (FIPS) Publication 140-2 are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.

The Federal Information Processing Standards (FIPS) Publication 140-2 are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors. In FIPS mode, the device tries to prevent the use of non-FIPS compatible algorithms, but you must ensure that you configure the device to use only FIPS approved algorithms. Some functionality may silently fail in FIPS mode if it attempts to use non-FIPS compliant algorithms.

- Configuring FIPS Mode, on page 1
- FIPS Operational Status, on page 4

Configuring FIPS Mode

NFVIS supports both FIPS and non-FIPS mode of operation. NFVIS is FIPS 140-2 compliant for SSH, TLS and SNMP protocols.



To enable FIPS mode:

```
config terminal
security fips
commit
```

Only after NFVIS reboot after the configuration FIPS mode is enabled.

FIPS mode can be disabled only with factory reset. If you try to disable FIPS mode with the no form of the command:

```
config terminal
no security fips
commit
Aborted: This command can only be removed while factory reset
```

The following is an example, where FIPS mode is successfully configured, but not enabled:

```
nfvis# show security
security fips-status CONFIGURED_REBOOT_TO_ENABLE
```

To verify the status of the FIPS mode after reboot:

```
nfvis# show security
security fips-status ENABLED
```

FIPS mode configuration is terminated when:

- SNMP v1 or v2 is configured.

  The following is an example of FIPS mode configuration failure when SNMP v1 or v2 is configured:

  ```
  config terminal
  security fips
  commit
  Aborted: SNMP version 1 and/or SNMP version 2 is configure. Please unconfigure SNMPv1
  and SNMPv2 and then try again
  ```

- SNMP v3 is configured with auth protocol MD5.

  The following is an example of FIPS mode configuration failure when SNMP v3 is configured with auth protocol md5:

```
config terminal
security fips
commit
Aborted: SNMP version 3 MD5 auth-protocol configured other secure protocol and try again
```



Note After FIPS mode is enabled, SNMP v1or v2 and SNMP v3 with auth protocol MD5 cannot be configured.

```
snmp group test_v1 snmp 1 noAuthNoPriv read test write test
commit
Aborted: Cannot configure SNMP group-version 1 because fips-status is ENABLED
```

```
config terminal
snmp user test_md5_v3
    user-version  3
    user-group test_v3
    auth-protocol md5
    auth-key 46:97:c3:b0:ba:45:fd:5e:be:99:44:c5:64:c9:bc:44
    commit
Aborted: 'snmp user test_md5_v3_passhd auth-protocol': Cannot configure SNMP user-version
3 with auth-protocol MD5 because fips-status is CONFIGURED_REBOOT_TO_ENABLE
nfvis(config-user-test_md5_v3_passhd)#
```

Backup and Restore for FIPS Mode

If you backup NFVIS configurations when FIPS mode is enabled, then upon restore, FIPS mode is configured but needs a manual reboot to enable FIPS mode.

```
Backup configuration
nfvis#
nfvis# show running-config security
security fips
nfvis# show security
security fips-status ENABLED
nfvis#

After restore
nfvis#
nfvis# show running-config security
security fips
nfvis# show security fips-status
security fips-status CONFIGURED_REBOOT_TO_ENABLE
nfvis#

After reboot
nfvis#
nfvis# show running-config security
security fips
nfvis# show security
security fips-status ENABLED
nfvis#
```

When you backup NFVIS configurations with FIPS mode disabled, but the system where you restore the configurations has FIPS mode enabled, upon restore, the NFVIS configurations disable FIPS mode but the system has to reboot for FIPS mode to be in DISABLED state.

Backup configurations

```
nfvis# show running-config security fips
% No entries found.
nfvis# show security fips-status
security fips-status DISABLED
nfvis#
```

Restore system configurations

```
nfvis#
nfvis# show running-config security
security fips
nfvis# show security
security fips-status ENABLED
nfvis#
```

After restore

```
nfvis# show running-config security
% No entries found.
nfvis# show security
security fips-status UNCONFIGURED_REBOOT_TO_DISABLE
nfvis#
```

After reboot

```
nfvis# show running-config security fips
% No entries found.
nfvis# show security fips-status
security fips-status DISABLED
nfvis#
```

FIPS Operational Status

The following is a list of operational states when you try to enable FIPS mode:

- DISABLED
- CONFIGURED-REBOOT-TO-ENABLE
- ENABLED
- UNCONFIGURED-REBOOT-TO-DISABLE
- FAILED

The following table lists the possible operational state transitions for FIPS mode:

From	To	Description
DISABLED	CONFIGURED-REBOOT-TO-ENABLE	If the Oper data of fips-state leafs was previously set to DISABLED and if the **security fips** configuration is pushed
DISABLED	FAILED	If there is an error while pushing the **security fips** configuration

From	To	Description
CONFIGURED-REBOOT-TO-ENABLE	ENABLED	If the fips-mode configuration is successful before and the Oper data was set to CONFIGURED-REBOOT-TO-ENABLE, then after reboot set the Oper data to ENABLED
CONFIGURED-REBOOT-TO-ENABLE	FAILED	If the Oper data of fips-state leafs was previously set to CONFIGURED-REBOOT-TO-ENABLE and there was an error while removing fips-mode configuration
CONFIGURED-REBOOT-TO-ENABLE	DISABLED	If the fips-mode is unconfigured while restoring from a backup package or factory-reset and the current fips-status is CONFIGURED-REBOOT-TO-ENABLE
ENABLED	DISABLED	After factory-reset (of any type)
ENABLED	FAILED	If there is an error while disabling the FIPS mode
ENABLED	UNCONFIGURED-REBOOT-TO-DISABLE	If the fips-mode is unconfigured while restoring from a backup package and the current fips-status is ENABLED
FAILED	CONFIGURED-REBOOT-TO-ENABLE	If the Oper date of fips-state leafs was previously set to FAILED and now configuring fips-mode
FAILED	DISABLED	If the Oper date of fips-state leafs was previously set to FAILED and now issued factory-reset
UNCONFIGURED-REBOOT-TO-DISABLE	DISABLED	If the Oper data of fips-state leafs was previously set to UNCONFIGURED-REBOOT-TO-DISABLE and then NFVIS is rebooted
UNCONFIGURED-REBOOT-TO-DISABLE	CONFIGURED-REBOOT-TO-ENABLE	If the Oper data of fips-state leafs was previously set to UNCONFIGURED-REBOOT-TO-DISABLE and fips-mode config is successful
UNCONFIGURED-REBOOT-TO-DISABLE	FAILED	If the Oper data of fips-state leafs was previously set to UNCONFIGURED-REBOOT-TO-DISABLE and if the fips-mode config was unsuccessful