# Contents

# FIPS commands

## display crypto version

Use **display crypto version** to display the version number of the device algorithm base.

### Syntax

**display crypto version**

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Usage guidelines

Each algorithm base version number represents a set of cryptographic algorithms.

### Examples

# Display the version number of the current device algorithm base.

```
<Sysname> display crypto version
7.1.1.1.1.72
```

**Table 1 Command output**

| Field | Description |
|---|---|
| 7.1.1.1.1.72 | Version number in the **7.1.***X* format.<br>• **7.1**—Comware V700R001.<br>• **X**—Version number of the device algorithm base. |

## display fips status

Use **display fips status** to display the FIPS mode state.

### Syntax

**display fips status**

### Views

Any view

### Predefined user roles

network-admin

network-operator

### Examples

# Display the FIPS mode state.

```
<Sysname> display fips status
FIPS mode is enabled.
```

### Related commands

**`fips mode enable`**

# fips mode enable

Use **`fips mode enable`** to enable FIPS mode.

Use **`undo fips mode enable`** to disable FIPS mode.

### Syntax

**`fips mode enable`**

**`undo fips mode enable`**

### Default

FIPS mode is disabled.

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

After you enable FIPS mode and reboot the device, the device operates in FIPS mode. The FIPS device has strict security requirements, and performs self-tests on cryptography modules to verify that they are operating correctly.

After you execute the **`fips mode enable`** command, the system provides the following methods to enter FIPS mode:

- Automatic reboot

  Select the automatic reboot method. The system automatically performs the following tasks:

  **a.** Create a default FIPS configuration file named **fips-startup.cfg**.

  **b.** Specify the default file as the startup configuration file.

  **c.** Require you to configure the username and password for next login.

  You can press **Ctrl+C** to exit the configuring process so the **`fips mode enable`** command will not be executed.

  The system automatically uses the specified startup configuration file to reboot the device after you configure the administrator's username and password.

- Manual reboot

  This method requires that you manually complete the configurations for entering FIPS mode, and then reboot the device.

  To use manual reboot to enter FIPS mode:

  **a.** Enable the password control feature globally.

  **b.** Set the number of character types a password must contain to 4, and set the minimum number of characters for each type to one character.

  **c.** Set the minimum length of user passwords to 15 characters.

  **d.** Add a local user account for device management, including the following items:

  - A username.
  - A password that must comply with the password control policies.
  - A user role of **network-admin**.

- A service type of **terminal**.

**e.** Delete the FIPS-incompliant local user service types Telnet, HTTP, and FTP.

**f.** Save the configuration file and specify it as the startup configuration file.

**g.** Delete the original startup configuration file in binary format.

**h.** Reboot the device.

After the **fips mode enable** command is executed, the system prompts you to choose a reboot method. If you do not make a choice within 30 seconds, the system uses the manual reboot method by default.

After the **undo fips mode enable** command is executed, the system provides the following methods to exit FIPS mode:

- Automatic reboot

  Select the automatic reboot method. The system automatically creates a default non-FIPS configuration file named **non-fips-startup.cfg**, and specifies the file as the startup configuration file. The system reboots the device by using the default non-FIPS configuration file. After the reboot, you are directly logged into the device.

- Manual reboot

  This method requires that you manually complete the configurations for entering non-FIPS mode, and then reboot the device. After the device reboots, you must enter user information according to the authentication mode to log in to the device.

## Examples

# Enable FIPS mode, and choose the automatic reboot method to enter FIPS mode.

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:y
The system will create a new startup configuration file for FIPS mode. After you set the login username and password for FIPS mode, the device will reboot automatically.
Enter username(1-55 characters): root
Enter password(15-63 characters):
Confirm password:
Waiting for reboot... After reboot, the device will enter FIPS mode.
```

# Enable FIPS mode, and choose the manual reboot method to enter FIPS mode.

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:n
Change the configuration to meet FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter FIPS mode.
```

# Disable FIPS mode, and choose the automatic reboot method to enter non-FIPS mode.

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode and then reboot automatically. Continue? [Y/N]:y
Waiting for reboot... After reboot, the device will enter non-FIPS mode.
```

# Disable FIPS mode, and choose the manual reboot method to enter non-FIPS mode.

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
```

```
The system will create a new startup configuration file for non-FIPS mode, and then reboot
automatically. Continue? [Y/N]:n
Change the configuration to meet non-FIPS mode requirements, save the configuration to
the next-startup configuration file, and then reboot to enter non-FIPS mode.
```

### Related commands

**`display fips status`**

# fips self-test

Use **`fips self-test`** to trigger a self-test on the cryptographic algorithms.

### Syntax

**`fips self-test`**

### Views

System view

### Predefined user roles

network-admin

### Usage guidelines

This command is supported only in FIPS mode. To examine whether the cryptography modules operate correctly, you can use this command to trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test.

A successful self-test requires that all cryptographic algorithms pass the self-test. If the self-test fails, the device where the self-test process exists reboots.

### Examples

# Trigger a self-test on the cryptographic algorithms.

```
<Sysname> system-view
[Sysname] fips self-test
Cryptographic Algorithms Known-Answer Tests are running ...
Slot 1:
Starting Known-Answer tests in the user space.
Known-answer test for 3DES passed.
Known-answer test for SHA1 passed.
Known-answer test for SHA224 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA224 passed.
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for AES passed.
Known-answer test for RSA(signature/verification) passed.
Pairwise conditional test for RSA(signature/verification) passed.
Pairwise conditional test for RSA(encrypt/decrypt) passed.
Pairwise conditional test for DSA(signature/verification) passed.
Pairwise conditional test for ECDSA(signature/verification) passed.
```

```
Known-answer test for ECDH passed.
Known-answer test for random number generator(x931) passed.
Known-answer test for DRBG passed.
Known-Answer tests in the user space passed.
Starting Known-Answer tests in the kernel.
Known-answer test for 3DES passed.
Known-answer test for AES passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for SHA1 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for GCM passed.
Known-answer test for GMAC passed.
Known-Answer tests in the kernel passed.
Cryptographic Algorithms Known-Answer Tests passed.
```