



FIPS 140-2 Mode Setup

This chapter provides information about FIPS 140-2 mode setup.

- [FIPS 140-2 Setup, on page 1](#)

FIPS 140-2 Setup



Caution

FIPS mode is only supported on releases that have been through FIPS compliance. Be warned that FIPS mode should be disabled before you upgrade to a non-FIPS compliance version of Unified Communications Manager.

For information about which releases are FIPS compliant and to view their certifications, see the *FIPS 140* document at <https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html>.

FIPS, or Federal Information Processing Standard, is a U.S. and Canadian government certification standard that defines requirements that cryptographic modules must follow.

Certain versions of Unified Communications Manager are FIPS 140-2 compliant, in accordance with the U.S. National Institute of Standards (NIST), and can operate in FIPS mode, level 1 compliance.

When you enable FIPS 140-2 mode, Unified Communications Manager reboots, runs certification self-tests at startup, performs the cryptographic modules integrity check, and then regenerates the keying materials. At this point, Unified Communications Manager operates in FIPS 140-2 mode.

FIPS requirements include the following: performance of startup self-tests and restriction to a list of approved cryptographic functions.

FIPS mode uses the following FIPS 140-2 level 1 validated cryptographic modules:

- CiscoSSL 1.0.2n.6.2.194 with FIPS Module CiscoSSL FOM 6_2_0
- CiscoJ 5.2.1
- RSA CryptoJ 6_2_3
- openssh 7.5.9
- NSS

You can perform the following FIPS-related tasks:

- Enable FIPS 140-2 mode
- Disable FIPS 140-2 mode
- Check the status of FIPS 140-2 mode

**Note**

- By default, your system is in non-FIPS mode, you must enable it.

Enable FIPS 140-2 Mode

You can enable FIPS 140-2 through the CLI. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Consider the following information before you enable FIPS 140-2 mode on Unified CM:

- When you switch from non-FIPS to FIPS mode, the MD5 and DES protocols will not be functional.
- In single server clusters, because certificates are regenerated, you need to run the CTL Client or apply the Prepare Cluster for Rollback to pre-8.0 enterprise parameter before you enable FIPS mode. If you do not perform either of these steps, you must manually delete the ITL file after you enable FIPS mode.
- After you enable FIPS mode on a server, please wait until the server reboots and the phones re-register successfully before enabling FIPS on the next server.

**Caution**

Before you enable FIPS mode, we strongly recommend that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

Procedure

Step 1 Start a CLI session.

For more information, see “Start CLI Session” in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Step 2 In the CLI, enter **utils fips enable**

The following prompts appear:

```
Security Warning: The operation will regenerate certificates for1)
CallManager

2) Tomcat
3) IPsec
4) TVS
5) CAPF
6) SSH
Any third party CA signed certificates that have been uploaded for the above
components will need to be re-uploaded. If the system is operating in mixed
mode, then the CTL client needs to be run again to update the CTL file.
```

```

*****
This will change the system to FIPS mode and will reboot.
*****
Do you want to continue (yes/no)?

```

Step 3 Enter yes.

The following message appears:

```

Generating certificates...Setting FIPS mode in operating system.
FIPS mode enabled successfully.
*****
It is highly recommended that after your system restarts
that a system backup is performed.
*****
The system will reboot in a few minutes.

```

Unified CM reboots automatically.

Note Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

Note If you have a single server cluster and applied the **Prepare Cluster for Rollback to pre 8.0** enterprise parameter before you enabled FIPS 140-2 mode, you must disable this enterprise parameter after making sure that all the phones registered successfully to the server.

Note In FIPS mode, Unified CM uses RedHat Openswan (FIPS validated) in place of Racoon (non-FIPS validated). If the security policies in Racoon contain functions that are not FIPS approved, the CLI command will ask you to redefine the security policies with FIPS approved functions and abort. For more information, see topics related to IPsec Management in the *Cisco Unified Communications Operating System Administration Guide*.

Disable FIPS 140-2 Mode

FIPS 140-2 is disabled through the CLI. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Consider the following information before you disable FIPS 140-2 mode on Unified Communications Manager (Unified CM):

- In single or multiple server clusters, we strongly recommend that you run the CTL Client. If the CTL Client is not run on a single server cluster, you must manually delete the ITL File after disabling FIPS mode.
- In multiple server clusters, each server must be disabled separately, because FIPS mode is not disabled cluster-wide but rather on a per-server basis.

To disable FIPS 140-2 mode, perform the following procedure:

Procedure

Step 1 Start a CLI Session.

For more information, see the Starting a CLI Session section in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Step 2 In the CLI, enter **utils fips disable**

Unified CM reboots and is restored to non-FIPS mode.

Note Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

Check FIPS 140-2 Mode Status

To confirm that FIPS 140-2 mode is enabled, check the mode status from the CLI.

To check the status of FIPS 140-2 mode, perform the following procedure:

Procedure

Step 1 Start a CLI Session.

For more information, see the Starting a CLI Session section in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Step 2 In the CLI, enter **utils fips status**

The following message appears to confirm that FIPS 140-2 mode is enabled.

```
admin:utils fips status
The system is operating in FIPS mode. Self test status:

- S T A R T -----
Executing FIPS selftests
runlevel is N 3
Start time: Thu Apr 28 15:59:24 PDT 2011
NSS self tests passed.
Kernel Crypto tests passed.
Operating System OpenSSL self tests passed.
Openswan self tests passed.
OpenSSL self tests passed.
CryptoJ self tests passed...
```

FIPS 140-2 Mode Server Reboot

When a Unified Communications Manager (Unified CM) server reboots in FIPS 140-2 mode, it triggers FIPS startup self-tests in each of the FIPS 140-2 modules after rebooting.



Caution If any of these self-tests fail, the Unified CM server halts.



Note A Unified CM server is automatically rebooted when FIPS is enabled or disabled with the corresponding CLI command. A user can also initiate a reboot.



Caution If the startup self-test failed because of a transient error, restarting the Unified CM server fixes the issue. However, if the startup self-test error persists, it indicates a critical problem in the FIPS module and the only option is to use a recovery CD.
