FIPS 140-2 mode setup

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

FIPS 140-2 setup

Warning Cisco Unified CM 8.6(1) is the only version at this time that has been through FIPS 140-2 Level 1 compliance. FIPS mode is only supported on releases that have been through FIPS compliance. Be warned that FIPS mode should be disabled prior to upgrading to a non-FIPS compliance version of Cisco Unified CM.

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

Cisco Unified CM 8.6(1) is 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, Cisco Unified CM reboots, runs certification self-tests at startup, performs the cryptographic modules integrity check, and then regenerates the keying materials. At this point, Cisco Unified CM operates in FIPS 140-2 mode.

Cisco Unified CM 8.6(1) meets FIPS requirements, including the following: it performs startup self-tests and a restricts to a list of approved cryptographic functions.

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

- Openssl 0.9.8l with FIPS Module 1.2
- RSA CryptoJ 4.1
- Red Hat Openssl

- Red Hat Openswan
- NSS

In Cisco Unified CM, 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, Cisco Unified CM is in non-FIPS mode. The administrator must enable FIPS mode.

Enable FIPS 140-2 mode

Warning Cisco Unified CM 8.6(1) is the only version at this time that has been through FIPS 140-2 Level 1 compliance. FIPS mode is only supported on releases that have been through FIPS compliance. Be warned that FIPS mode should be disabled prior to upgrading to a non-FIPS compliance version of Cisco Unified CM.

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

Consider the following information before you enable FIPS 140-2 mode on Cisco Unified Communications Manager:

- In single server clusters, because certificates get regenerated, you need to run the CTL Client or apply the "Prepare Cluster for Rollback to pre 8.0" enterprise parameter before enabling FIPS mode. If either of these steps is not performed, the administrator must manually delete the ITL File after enabling FIPS mode.
- After FIPS mode is enabled 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.

To enable FIPS 140-2 Mode, perform the following procedure:

Procedure

Step 1 Start a CLI session.
For more information, see Starting a CLI Session in the *Command Line Interface Reference Guide for Cisco Unifed 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.
```

Cisco Unified Communications Manager 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 prior to enabling FIPS 140-2 mode, disable this enterprise parameter after making sure that all the phones registered successfully to the server.

Note In FIPS mode, Cisco Unified Communications Manager 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 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 Unifed Communications Solutions*.

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

- 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, the administrator must manually delete the ITL File after disabling FIPS mode.
- In multiple server clusters, each server must be disabled separately, because FIPS mode is disabled not cluster-wide but rather 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 Unifed Communications Solutions*.

Step 2 In the CLI, enter **utils fips disable**
Cisco Unified Communications Manager 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 1402 mode is enabled, you can check the 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 Unifed 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 Cisco Unified Communications Manager server reboots in FIPS 140-2 mode, it will trigger FIPS startup self-tests in each of the FIPS 140-2 modules after rebooting.

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

Note A Cisco Unified Communications Manager 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 Cisco Unified Communications Manager 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.