FIPS 140-2 Mode Setup

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

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. It 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). They can operate in FIPS mode, level 1 compliance.

Unified Communications Manager

- Reboots
- Runs certification self-tests at startup
- Performs the cryptographic modules integrity check
- Regenerates the keying materials

when you enable FIPS 140-2 mode. At this point, Unified Communications Manager operates in FIPS 140-2 mode.

FIPS requirements include the following:

- Performance of startup self-tests
- 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

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

- When you switch from non-FIPS to FIPS mode, the MD5 and DES protocols aren't 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.
- In a cluster, all nodes should be either in FIPS or Non FIPS mode. Each node being in different modes is not allowed. For example, Node A in FIPS mode and Node B in Non-FIPS mode is not allowed.
- 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.

Make sure that all cluster nodes are set to FIPS mode or Non-FIPS mode during deployment. You cannot deploy mixed nodes in a cluster. A cluster must be either a FIP or a non-FIPS node.

Procedure

Step 1 Start a CLI session.

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

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

If you enter a password less than 14 characters, the following prompt appear:

```
The cluster security password must be at least 14 characters long before
 security modes such as FIPS, Common Criteria and Enhanced Security modes can be
 enabled. Update the cluster security password using the 'set password user
security' CLI command on all nodes and retry this command.
**********************************************************************************
Executed command unsuccessfully
```

If you enter a password more than 14 characters, the following prompts appear:

```
Security Warning: The operation will regenerate certificates for

1)CallManager
2)Tomcat
3)IPsec
4)TVS
5)CAPF
6)SSH
7)ITLRecovery
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.
If there are other servers in the cluster, please wait and do not change
the FIPS Settings on any other node until the FIPS operation on this node
is complete and the system is back up and running.

If the enterprise parameter 'TFTP File Signature Algorithm' is configured
with the value 'SHA-1' which is not FIPS compliant in the current version of the
Unified Communications Manager, though the signing operation
will continue to succeed, it is recommended the parameter value be changed to
SHA-512 in order to be fully FIPS. Configuring SHA-512 as the signing algorithm
may reqiure all the phones that are provisioned in the cluster to be capable of
verifying SHA-512 signed configuration file, otherwise the phone registration
may fail. Please refer to the Cisco Unified Communications Manager Security Guide
for more details.
**********************************************************************************
This will change the system to FIPS mode and will reboot.
**********************************************************************************

WARNING: Once you continue do not press Ctrl+C. Canceling this operation after
it
starts will leave the system in an inconsistent state; rebooting the system and
running "utils fips status" will be required to recover.
**********************************************************************************
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 Communications Manager reboots automatically.

Note
- Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.
- 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 Communications Manager uses RedHat Openswan (FIPS validated) in place of Racoon (non-FIPS validated). If the security policies in Racoon contain functions that aren't FIPS approved, CLI command asks you to redefine security policies with FIPS approved functions and abort. For more information, see topics related to IPsec Management in the Administration Guide for Cisco Unified Communications Manager.

Disable FIPS 140-2 Mode

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

- In single or multiple server clusters, we recommend you to 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 Communications Manager reboots and is restored to non-FIPS mode.

Note Certificates and SSH key are regenerated automatically.

Check FIPS 140-2 Mode Status

To confirm if the 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

FIPS startup self-tests in each of the FIPS 140-2 modules are triggered after rebooting when Unified Communications Manager server reboots in FIPS 140-2 mode.

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

Note Unified Communications Manager server is automatically rebooted when FIPS is enabled or disabled with the corresponding CLI command. You can also initiate a reboot.

Caution If the startup self-test failed because of a transient error, restarting the 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.

Enhanced Security Mode

Enhanced Security Mode runs on a FIPS-enabled system. Both Unified Communications Manager and the IM and Presence Service can be enabled to operate in Enhanced Security Mode, which enables the system with the following security and risk management controls:

- Stricter credential policy is implemented for user passwords and password changes.
- Contact search authentication feature becomes enabled by default.
- If the protocol for remote audit logging is set to TCP or UDP, the default protocol is changed to TCP. If the protocol for remote audit logging is set to TLS, the default protocol remains TLS. In Common Criteria Mode, strict hostname verification is implemented. Hence, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

Credential Policy Updates

When Enhanced Security Mode is enabled, a stricter credential policy takes effect for new user passwords and password changes. After Enhanced Security Mode is enabled, administrators can use the **set password ***** series of CLI commands to modify any of these requirements:

- Password Length should be between 14 to 127 characters.
- Password should have at least 1 lowercase, 1 uppercase, 1 digit and 1 special character.
- Any of the previous 24 passwords cannot be reused.
- Minimum age of the password is 1 day and Maximum age of the password is 60 days.
- Any newly generated password's character sequence will need to differ by at least 4 characters from the old password's character sequence.

Configure Enhanced Security Mode

Enable FIPS before you enable Enhanced Security Mode.

Use this procedure on all Unified Communications Manager or IM and Presence Service cluster nodes to configure Enhanced Security Mode.

Note You must ensure that services in the IM and Presence Service publishers are in the 'STARTED' state ("Cisco IM and Presence Data Monitor" service and SyncAgent), when you are changing the password on the Unified Communications Manager publisher after enabling the Enhanced Security Mode.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run **utils EnhancedSecurityMode status** command to confirm whether Enhanced Security Mode is enabled.

Step 3 Run one of the following commands on a Unified Communications Manager cluster node:

- To enable Enhanced Security Mode, run **utils EnhancedSecurityMode enable** command.

- To disable Enhanced Security Mode, run **utils EnhancedSecurityMode disable** command.

Step 4 After enabling Enhanced Security Mode, change the password in the Cisco Unified CM Administration user interface with a new password containing 14 characters.

Perform the following after enabling Enhanced Security Mode on Unified Communications Manager publisher:

a. Enable Enhanced Security Mode on Unified Communications Manager subscribers.

b. Enable Enhanced Security Mode on IM and Presence Service publisher.

c. Enable Enhanced Security Mode on IM and Presence Service subscribers.

Note Do not run either **utils EnhancedSecurityMode enable** or **utils EnhancedSecurityMode disable** CLI commands on all nodes simultaneously.

FIPS Mode Restrictions

Feature	Restrictions
SNMP v3	FIPS mode does not support SNMP v3 with MD5 or DES. If you have SNMP v3 configured while FIPS mode is enabled, you must configure **SHA** as the Authentication Protocol and **AES128** as the Privacy Protocol.
Certificate Remote Enrolment	FIPS mode does not support Certificate Remote Enrolment.
SFTP Server	By Default, the JSCH library was using ssh-rsa for SFTP connection but the FIPS mode doesn't support ssh-rsa. Due to a recent update of CentOS, the JSCH library supports both **ssh-rsa** (SHA1withRSA) or **rsa-sha2-256** (SHA256withRSA) depending on the FIPS value after modifications. That is, **Note** • FIPS mode only supports **rsa-sha2-256**. • Non-FIPS mode supports both **ssh-rsa** and **rsa-sha2-256**. The **rsa-sha2-256** (SHA256WithRSA) support is available only from OpenSSH 6.8 version onwards. In FIPS mode, only the SFTP servers running with OpenSSH 6.8 version onwards supports the **rsa-sha2-256** (SHA256WithRSA)

Feature	Restrictions
IPSec Policy	In Common Criteria (CC) mode, Certificate Exchange operation is recommended first between clusters/nodes before configuring IPSec policies for Certificate based IPSec Policy. Certificate based IPSec Policy will not work when moving from Non-FIPS to FIPS / Common Criteria mode or vice-versa. Perform the following when you should move from Non-FIPS mode to FIPS / CC Mode or vice-versa. If you have a certificate based IPSec policy and its in enabled state then: **1.** Disable the IPSec policy before moving to FIPS/CC mode or vice versa. **2.** Re-certify the certificate and exchange the new certificate after moving to FIPS/CC mode or vice versa. **3.** Enable IPSec policy. **Note** When you enable/disable the FIPS CC mode server that is having IPSec configuration, multiple Pluto Cores are visible (`utils core active list`). However, this doesn't have impact on any functionality.