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
- Libreswan
- 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.
- Ensure that the security password length is minimum 14 characters before you upgrade to FIPS, Common Criteria, or Enhanced Security mode on the cluster. Update the password even if the prior version was FIPS enabled.

If you generate a Self-Signed Certificate or Certificate Signing Request (CSR) on FIPS mode, certificates must be encrypted using the SHA256 hashing algorithm and can't select SHA1.

IPsec Requirements

With this release, the Libreswan library support replaces Openswan library support for IPsec. This support has no changes to the existing functionality.

For the certificate-based authentication to function with the Libreswan library, the certificates of both the source and destination must be CA-signed certificates. In addition, same certificate authority (CA) must sign these certificates. The migration to the Libreswan library has the following limitations:

- If you upgrade Unified Communications Manager which has IPsec configured using a certificate-based authentication with self-signed certificate, then the upgrade fails. To perform a successful upgrade, reconfigure the IPsec policy with a CA-signed certificate.
- IPsec stops working if you're using certificate-based authentication and self-signed certificates for setting up IPsec.
- IPsec stops working if you're using certificate-based authentication and CA-signed certificates with different CAs signing source and destination for setting up IPsec.
- In Unified Communications Manager, the IPsec policies with DH group key values 1, 2 or 5 are disabled. However, if you have configured the IPSec policies with DH group key values 1, 2 or 5 and FIPS mode is enabled, the upgrade to Unified Communication Manager is blocked.

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.
- To enable FIPS in a cluster, first enable the Publisher and make sure all the configured services are properly initialized which will take some time to come up. Then enable fips in all other nodes one after the other within the cluster.

Note In FIPS mode, Unified Communications Manager uses Libreswan (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**

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, you should configure the server with a fully qualified domain name (FQDN) which matches the certificate.

When Unified Communications Manager is in FIPS mode, the devices that you set as a backup device must be FIPS compliance. The key exchange algorithm **diffie-hellman-group1-sha1** isn't supported in FIPS mode. If you configure **diffie-hellman-group1-sha1** algorithm in a non-FIPS mode of Unified Communications Manager, this algorithm is automatically removed from SSH Key Exchange when you enable FIPS mode.

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 can't 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 needs to differ by at least 4 characters from the old password's character sequence.

Note When Unified Communications Manager is enabled to operate in Enhanced mode, ensure that you change the user credentials for IPMASysUser and IPMASecureSysUser. Else, the IPMA functionalities won't be in a working state and the 'IPMANotStarted' alarms will be triggered. The CLI sessions will be flooded on the next Cisco Tomcat service restart or IPMA service restart.

You can change the application user password credentials at documented in the "Manage Application User Password Credential Information" section at: Administration Guide for Cisco Unified Communications Manager.

From Cisco Unified CM Administration user interface, navigate to **User Management > Application User** and click **Edit Credential**. From the Authentication Rule drop-down list, select **Enhanced Security Credential Policy** and ensure that you keep the **User Must Change at Next Login check box** unchecked. You can view the Enhanced Security Mode policies as described in the 'Credential Policy Updates' section.

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.

Common Criteria Mode

Common Criteria mode allows both Unified Communications Manager and IM and Presence Service Service to comply with Common Criteria guidelines. Common Criteria mode can be configured with the following set of CLI commands on each cluster node:

- `utils fips_common_criteria enable`
- `utils fips_common_criteria disable`
- `utils fips_common_criteria status`

Common Criteria Configuration Task Flow

- FIPS mode must be running to enable Common Criteria mode. If FIPS isn't already enabled, you'll be prompted to enable it when you try to enable Common Criteria mode. Enabling FIPS does require certificate regeneration. For more information, see Enable FIPS 140-2 Mode, on page 3.
- In Common Criteria mode, Certificate Exchange operation is mandatory between clusters/nodes before configuring IPSec policies for Certificate based IPSec Policy.
- X.509 v3 certificates are required in Common Criteria mode. X.509 v3 certificates enable secure connections when using TLS 1.2 as a communication protocol for the following:
  - Remote audit logging
  - Establishing connection between the FileBeat client and the logstash server.

To configure Unified Communications Manager and IM and Presence Service for Common Criteria mode, perform the following:

Procedure

	Command or Action	Purpose
Step 1	Enable TLS, on page 8	TLS is a prerequisite for configuring Common Criteria mode.
Step 2	Configure Common Criteria Mode, on page 9	Configure Common Criteria mode on all Unified Communications Manager and IM and Presence Service cluster nodes.

Enable TLS

TLS 1.2 version or TLS version 1.1 is a requirement for Common Criteria mode. Secure connections using TLS version 1.0 are not permitted after enabling Common Criteria mode.

- During establishment of a TLS connection, the `extendedKeyUsage` extension of the peer certificate is checked for proper values.
  - The peer certificate should have `serverAuth` as `extendedKeyUsage` extension if the peer is a server.
  - The peer certificate should have `clientAuth` as `extendedKeyUsage` extension if the peer is a client.

If the `extendedKeyUsage` extension does not exist in the peer certificate or is not set properly, the connection is closed.

To support TLS version 1.2, perform the following:

Procedure

Step 1 Install Soap UI version 5.2.1.

Step 2 If you are running on the Microsoft Windows platform:

a) Navigate to `C:\Program Files\SmartBear\SoapUI-5.2.1\bin`.

b) Edit the `SoapUI-5.2.1.vmoptions` file to add `-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3` and save the file.

Step 3 If you are running on Linux, edit the `bin/soaup.sh` file to add `JAVA_OPTS="$JAVA_OPTS -Dsoapui.https.protocols=SSLv3,TLSv1.2"` and save the file.

Step 4 If you are running OSX:

a) Navigate to `/Applications/SoapUI-{VERSION}.app/Contents`.

b) Edit the `vmoptions.txt` file to add `-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3` and save the file.

Step 5 Restart the SoapUI tool and proceed with AXL testing

Configure Common Criteria Mode

Use this procedure to configure Common Criteria mode for Unified Communications Manager and IM and Presence Service Service.

Procedure

Step 1 Log in to the Command Line Interface prompt.

Step 2 Run `utils fips_common_criteria status` command to verify whether the system is operating in Common Criteria mode.

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

- To enable the Common Criteria mode, run `utils fips_common_criteria enable`.
- To disable the Common Criteria mode, run `utils fips_common_criteria disable`.

  When Common Criteria mode is disabled, a prompt is displayed to set the minimum TLS version.

Note Do not run these commands on all nodes simultaneously.

Step 4 To enable Common Criteria Mode across a single cluster, repeat this procedure on all Unified Communications Manager and IM and Presence Service cluster nodes.

Note
- CTL client does not connect to Unified Communications Manager node when server is in the Common Criteria mode, as CTL client does not support TLS 1.1 and TLS 1.2 protocols.
- Only phone models that support TLS 1.1 or TLS 1.2 such as DX series and 88XX series phones are supported in Common Criteria mode. Phone models that support only TLSv1.0 such as 7975 and 9971 are not supported in the Common Criteria mode.
- Temporarly allow TLS 1.0 when using the CTL Client and then move the Cluster to Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2.
- Migrate to Tokenless CTL by using the CLI Command **utils ctl set-cluster mixed-mode** in Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2.

Step 5 To enable the Common Criteria mode in a multi cluster setup where ICSA is already configured between the nodes, enable Common Criteria mode in each of the nodes in the following order:

a. Unified Communications Manager - Cluster 1 (Publisher)

b. IM and Presence Service - Cluster 1 (Publisher)

c. IM and Presence Service - Cluster 1 (Subscriber or subscribers)

d. Unified Communications Manager - Cluster 2 (Publisher)

e. IM and Presence Service - Cluster 2 (Publisher)

f. IM and Presence Service - Cluster 2 (Subscriber or subscribers)

Step 6 In case of a cert sync failure, see.

CiscoSSH Support

Unified Communications Manager supports CiscoSSH. When you enable FIPS mode on your system, CiscoSSH is enabled automatically with no extra configuration required.

CiscoSSH Support

CiscoSSH supports the following key exchange algorithms:

- **Diffie-Hellman-Group14-SHA1**
- **Diffie-Hellman-Group-Exchange-SHA256**
- **Diffie-Hellman-Group-Exchange-SHA1**

CiscoSSH supports the following ciphers with the Unified Communications Manager server:

- **AES-128-CTR**
- **AES-192-CTR**

- **AES-256-CTR**
- **AES-128-GCM@openssh.com**
- **AES-256-GCM@openssh.com**
- **AES-128-CBC** (supported for Release 12.0(1) and up)
- **AES-192-CBC** (supported for Release 12.0(1) and up)
- **AES-256-CBC** (supported for Release 12.0(1) and up)

CiscoSSH supports the following ciphers for clients:

- **AES-128-CTR**
- **AES-192-CTR**
- **AES-256-CTR**
- **AES-128-GCM@openssh.com**
- **AES-256-GCM@openssh.com**
- **AES-128-CBC**
- **AES-192-CBC**
- **AES-256-CBC**

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)