FIPS Compliance in Cisco Unity Connection

- FIPS Compliance in Cisco Unity Connection, on page 1
- Introduction, on page 1
- Running CLI Commands for FIPS, on page 2
- Regenerating Certificates for FIPS, on page 3
- Configuring Additional Settings When Using FIPS Mode, on page 5
- Configuring Voicemail PIN For Touchtone Conversation Users To Sign-In, on page 6
- FIPS Mode Restrictions, on page 7

FIPS Compliance in Cisco Unity Connection

Introduction

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

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 Cisco Unity Connection.

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

Certain versions of Unity Connection 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. For more information on 'FIPS 140-2' setup, see Security Guide for Cisco Unified Communications Manager for release 15.

(Applicable for Releases before 15 SU2) FIPS mode uses the following FIPS 140-2 level 1 validated cryptographic modules:

- CiscoSSL 1.1.1n.7.2.390 with FIPS Module CiscoSSL FOM 7.2a
- CiscoSSH -1.9.29
- RSA CryptoJ 6_2_3

- BC FIPS -1.0.2.3.jar
- BCTLS FIPS - 1.0.12.3.jar
- BCPKIX FIPS -1.0.5.jar
- Strongswan - 5.9.8
- NSS -3.67

(Applicable for Release 15 SU2 and later) FIPS mode uses the following FIPS 140-2 level 1 validated cryptographic modules:

- CiscoSSL 1.1.1w.7.2.555 with FIPS Module CiscoSSL FOM 7.2a
- CiscoSSH -1.14.56
- RSA CryptoJ 6_2_3
- BC FIPS - 2.0.0.jar
- BCTLS FIPS - 2.0.19.jar
- BCPKIX FIPS - 2.0.6.jar
- BCUTIL FIPS - 2.0.1.jar
- Strongswan - 5.9.8
- NSS -3.67

Note For information on Unity Connection upgrades, see Upgrade Types section of the "Upgrading Cisco Unity Connection" chapter of the *Install, Upgrade and Maintenance Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html

Note If you are upgrading from any release of Unity Connection 12.5 in FIPS mode to Unity Connection 15 and later, make sure to install COP File **ciscocm.ciscossl7_upgrade_CSCwa48315_CSCwa77974_v1.0.k4.cop.sha512** on both nodes of cluster before upgrade. For information on Unity Connection upgrades, see Upgrade Considerations with FIPS Mode section of the "Upgrading Cisco Unity Connection" chapter of the *Install, Upgrade and Maintenance Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html

Running CLI Commands for FIPS

To enable the FIPS feature in Cisco Unity Connection, you use the utils fips enable CLI command. In addition to this, the following CLI commands are also available:

- utils fips disable- Use to disable the FIPS feature.

- utils fips status- Use to check the status of FIPS compliance.

For more information on the utils fips <option> CLI commands, see the applicable *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.

Caution *(Applicable for Releases before 15 SU2)* After enabling or disabling the FIPS mode, the Cisco Unity Connection server restarts automatically.

Caution If the Cisco Unity Connection server is in a cluster, do not change the FIPS settings on any other node until the FIPS operation on the current node is complete and the system is back up and running.

Note Before enabling the FIPS mode on the Unity Connection server, ensure that the security password length is minimum of 14 characters. In case of upgrading Unity Connection, password needs to be updated if the prior version was FIPS enabled.

All the new certificates are signed using SHA-256 hashing algorithm in FIPS mode. When you generate a self-signed certificate or Certificate Signing Request, you can choose only SHA-256 as the hashing algorithm.

Regenerating Certificates for FIPS

Regenerating Root Certificates

Cisco Unity Connection servers with pre-existing telephony integrations must have the root certificate manually regenerated after enabling or disabling the FIPS mode. If the telephony integration uses an Authenticated or Encrypted Security mode, the regenerated root certificate must be re-uploaded to any corresponding Cisco Unified Communications Manager servers. For fresh installations, regenerating the root certificate can be avoided by enabling FIPS mode before adding the telephony integration.

Note In case of clusters, perform the following steps on all nodes.

1. Sign in to Cisco Unity Connection Administration.
2. Select Telephony Integrations> Security> Root Certificate.
3. On the View Root Certificate page, click Generate New.
4. If the telephony integration uses an Authenticated or Encrypted Security mode, continue with steps 5-10, otherwise skip to step 12.
5. On the View Root Certificate page, right-click the Right-click to Save the Root Certificate as a File link.
6. Select Save As to browse to the location to save the Cisco Unity Connection root certificate as a.pem file.

Note The certificate must be saved as a file with the extension.pem rather than.htm, else Cisco Unified CM will not recognize the certificate.

7. Copy the Cisco Unity Connection root certificate to all Cisco Unified CM servers by performing the following substeps:
   a. On the Cisco Unified CM server, sign in to Cisco Unified Operating System Administration.
   b. Select the Certificate Management option from the Security menu.
   c. Select Upload Certificate/Certificate Chain on the Certificate List page.
   d. On the Upload Certificate/Certificate Chain page, select the CallManager-trust option from the Certificate Name drop-down.
   e. Enter Cisco Unity Connection Root Certificate in the Root Certificate field.
   f. Click Browse in the Upload File field to locate and select the Cisco Unity Connection root certificate that was saved in Step 5.
   g. Click Upload File.
   h. Click Close.
8. On the Cisco Unified CM server, sign in to Cisco Unified Serviceability.
9. Select Service Management from the Tools menu.
10. On the Control Center - Feature Services page, restart the Cisco CallManager service.
11. Repeat steps 5-10 on all remaining Cisco Unified CM servers in the Cisco Unified CM cluster.
12. Restart the Unity Connection Conversation Manager Service by following these steps:
    a. Sign in to Cisco Unity Connection Serviceability.
    b. Select Service Management from the Tools menu.
    c. Select Stop for the Unity Connection Conversation Manager service in the Critical Services section.
    d. When the Status area displays a message that the Unity Connection Conversation Manager service is successfully stopped, select Start for the service.
13. New and pre-existing telephony integration ports are now correctly registered with Cisco Unified CM.

FIPS is supported for both SCCP and SIP integrations between Cisco Unified Communications Manager and Cisco Unity Connection.

For more information on managing certificates, see the "Manage Certificates and Certificate Trust Lists" section in the "Security" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15cucosagx.html

Regenerating Tomcat Certificates

Unity Connection supports only RSA key based Tomcat certificates to configure secure calls using SIP Integration.This allows the use of self signed as well as third-party CA signed certificate for SIP secure call. Cisco Unity Connection servers with pre-existing telephony integrations must have the Tomcat certificate manually regenerated after enabling or disabling the FIPS mode. If the telephony integration uses an Authenticated or Encrypted Security mode, the regenerated tomcat certificate must be re-uploaded to any corresponding Cisco Unified Communications Manager servers. For fresh installations, regenerating the tomcat certificate can be avoided by enabling FIPS mode before adding the telephony integration.

To learn how to regenerate certificates, see section Generating RSA Key Based Certificates of chapter "Setting Up a Cisco Unified Communications Manager SIP Trunk Integration" in *Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/integration/cucm_sip/b_15cucintcucmsip.html.

Note Verify that the value entered in **X.509 Subject Name** field on SIP Trunk Security Profile Configuration page of Cisco Unified Communication Manager is the FQDN of the Unity Connection server.

Configuring Additional Settings When Using FIPS Mode

In order to maintain FIPS compliance, additional configurations are mandatory for the following features:

- Networking: Intrasite, Intersite, VPIM
- Unified Messaging: Unified Messaging Services.

Configure Networking When Using FIPS Mode

Networking from Cisco Unity Connection to another server must be secured by an IPsec policy. This includes intersite links, intrasite links, and VPIM locations. The remote server is responsible for assuring its own FIPS compliance.

Note

- Secure Messages are not sent in a FIPS compliant manner unless an IPsec Policy is configured.
- When upgrading from any lower version to 15 SU2 or later, it is mandatory to upgrade all nodes in the networking to ensure smooth operation and avoid replication issues.

Configure Unified Messaging When Using FIPS Mode

Unified Messaging Services require the following configuration:

- Configure IPsec policy between Cisco Unity Connection and Microsoft Exchange.
- Set the Web-Based Authentication Mode setting to Basic on the Edit Unified Messaging Service page in Unity Connection Administration. NTLM web authentication mode is not supported in FIPS mode.

Caution The IPsec policy between servers is required to protect the plain text nature of Basic web authentication.

Configure IPsec Policies Using FIPS Mode

For information on setting up IPsec policies, see the "IPSEC Management" section in the "Security" chapter of the *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection*

at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15cucosagx.html.

For information on the impact of IPsec policies with Unity Connection, see "Upgrading Cisco Unity Connection" chapter of *Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html

.

Unsupported Features When Using FIPS Mode

The following Cisco Unity Connection features are not supported when FIPS mode is enabled:

- SpeechView Transcription Service.
- SIP Digest Authentication (configured for SIP Telephony Integrations).
- SIP NTLM Authentication (configured for SIP Telephony Integration).
- Video Messaging.

Configuring Voicemail PIN For Touchtone Conversation Users To Sign-In

Enabling FIPS in Cisco Unity Connection prevents a touchtone conversation user from signing in to play or send voice messages or to change user settings if both of the following options are true:

- The user was created in Cisco Unity 5.x or earlier, and migrated to Connection.
- The Unity Connection user still has a voicemail PIN that was assigned in Cisco Unity 5.x or earlier.

A touchtone conversation user signs in by entering an ID (usually the user's extension) and a voicemail PIN. The ID and PIN are assigned when the user is created. Either an administrator or the user can change the PIN. To prevent administrators from accessing PINs in Connection Administration, PINs are hashed. In Cisco Unity 5.x and earlier, Cisco Unity hashed the PIN by using an MD5 hashing algorithm, which is not FIPS compliant. In Cisco Unity 7.x and later, and in Unity Connection, the PIN is hashed by using an SHA-1 algorithm, which is much harder to decrypt and is FIPS compliant.

Hashing All Voicemail PIN with SHA-1 Algorithm in Unity Connection

When FIPS is enabled, Cisco Unity Connection no longer checks the database to determine whether the user's voicemail PIN was hashed with MD5 or SHA-1 algorithm. Unity Connection hashes all the voicemail PINs with SHA-1 and compares it with the hashed PIN in the Unity Connection database. The user is not allowed to sign in if the MD5 hashed voicemail PIN entered by user does not match with the SHA-1 hashed voicemail PIN in the database.

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.
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).
SSH Host Key Algorithms	Deprecated Algorithm: • **ssh-rsa** (SHAlwithRSA) New Supported Algorithm: • **rsa-sha2-256** • **rsa-sha2-512** **Note** Before upgrading, we recommend you to refer the Upgrade Types section of the "Upgrading Cisco Unity Connection" chapter of the *Install, Upgrade and Maintenance Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html.

Feature	Restrictions
IPSec Policy	Certificate based IPSec Policy will not work when moving from Non-FIPS to FIPS or vice-versa. Perform the following when you move from Non-FIPS mode to FIPS 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 or vice versa. **2.** Re-certify the certificate and exchange the new certificate after moving to FIPS mode or vice versa. **3.** Enable IPSec policy.
Signature Algorithms *(Applicable for Release 15 SU2 and later)*	• In FIPS mode, Networking supports only **rsa-sha2-256** (SHA256withRSA) as signature algorithm. **Note** It is mandatory to upgrade all nodes in the Networking to Release 15 SU2 or later to ensure smooth operation and avoid replication issues. • In non-FIPS mode, Networking supports both **rsa-sha2-256** and **ssh-rsa** (SHA1withRSA) as signature algorithms. After the upgrade, **ssh-rsa** will be enabled by default. It is recommended to use **rsa-sha2-256** which is more secure. After upgrade to 15 SU2 or later, to enable **rsa-sha2-256**, execute the CLI command given below on Publisher Node of all the Clusters connected in Networking. `run cuc dbquery unitydirdb update tbl_configuration set valuebool = 1 where fullname = 'System.Security.EnableSha256'` **Note** It is recommended to upgrade all nodes in the Networking to Release 15 SU2 or later to ensure smooth operation and avoid replication issues.