CHAPTER 5

FIPS Compliance in Cisco Unity Connection 8.6

Cisco Unity Connection 8.6 supports the FIPS mode that complies with the Federal Information Processing Standards 140-2 (FIPS) requirements.

FIPS mode is not supported in Cisco Unified Communications Manager Business Edition (CUCMBE). Though the **utils fips <option>** Command Line Interface (CLI) command is visible for administrator, but it is not functional.

Recommendations to enable FIPS mode for Connection are:

- If you are performing a fresh installation of Cisco Unity Connection 8.6 and planning to use the FIPS mode, you must enable FIPS before configuring the Connection server and adding a telephony integration.
- If you are performing an upgrade to Cisco Unity Connection 8.6, make sure to follow the steps for regenerating certificates before using any pre-existing telephony integrations. To learn how to regenerate certificates, see the Regenerating Certificates for FIPS section.

See the following sections:

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/en/US/products/ps6509/prod_maintenance_guides_list.html.

Caution After enabling or disabling the FIPS mode, the Cisco Unity Connection server will automatically restart.

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.

Regenerating Certificates for FIPS

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.

Perform the following steps whenever you enable or disable the FIPS mode:

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.

Caution 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 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 Connection Conversation Manager service in the Critical Services section.

d. When the Status area displays a message that the 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* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/os_administration/guide/8xcucosag060.html#wp1053189.

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

See the following sections:

- Configure Networking When Using FIPS Mode, page 5-26
- Configure Unified Messaging When Using FIPS Mode, page 5-26
- Configure IPsec Policies When Using FIPS Mode, page 5-26
- Unsupported Features When Using FIPS Mode, page 5-26

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.

Configure Unified Messaging When Using FIPS Mode

Unified Messaging Services require the following configuration:

- Configure IPsec policy between Cisco Unity Connection and Microsoft Exchange or Cisco Unified MeetingPlace
- Set the Web-Based Authentication Mode setting to Basic on the Edit Unified Messaging Service page in Connection Administration

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

Configure IPsec Policies When 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 http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/os_administration/guide/8xcucosagx.html.

For information on setting up IPsec policies for Microsoft Exchange servers, consult the relevant Microsoft IPsec documentation.

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)

Configuring Voicemail PIN For Touchtone Conversation Users To Sign In

Enabling FIPS in Cisco Unity Connection 8.6 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 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 Connection, the PIN is hashed by using an SHA-1 algorithm, which is much harder to decrypt and is FIPS compliant.

In version 8.5 and earlier, when a user calls Connection and enters the ID and PIN, Connection checks the database to determine whether the user's PIN was hashed with MD5 or SHA-1 algorithm. Connection hashes the PIN that the user entered, and compares it with the hashed PIN in the Connection database. If the PINs match, the user is logged in.

The following sections explains how to configure voicemail PIN in Connection while FIPS is enabled:

- Hashing All Voicemail PIN with SHA-1 Algorithm in Cisco Unity Connection 8.6(1) And Later Versions, page 5-27
- Replacing MD5-hashed Voicemail PIN with SHA-1 Algorithm in Cisco Unity 5.x Or Earlier Versions, page 5-27

Hashing All Voicemail PIN with SHA-1 Algorithm in Cisco Unity Connection 8.6(1) And Later Versions

In version 8.6 and later, 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. Connection hashes all the voicemail PINs with SHA-1 and compares it with the hashed PIN in the 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.

Replacing MD5-hashed Voicemail PIN with SHA-1 Algorithm in Cisco Unity 5.x Or Earlier Versions

For Connection user accounts that were originally created in Cisco Unity 5.x or earlier, the voicemail PIN that might have been hashed with MD5 algorithm must be replaced with SHA-1 algorithm. Consider the following points while replacing the MD5-hashed passwords with SHA-1-hashed passwords:

- Use the latest version of the User Data Dump utility to determine how many users still have MD5-hashed PINs. For each user, the Pin_Hash_Type column contains either MD5 or SHA-1. To download the latest version of the utility and to view the Help, see the User Data Dump page on the Cisco Unity Tools website at http://ciscounitytools.com/Applications/CxN/UserDataDump/UserDataDump.html.

Note The earlier versions of the User Data Dump utility do not include the Pin_Hash_Type column.

- Check the User Must Change at Next Sign-In check box on the Password Settings page in Connection Administration before you enable FIPS. This encourages users to sign in to Connection and change their voicemail PINs.
- Run the Bulk Password Edit utility if you still have users who have not changed their voicemail PINs. The Bulk Password Edit utility lets you selectively change PINs to random values and exports data on the changes to a .csv file. The export file includes the name, alias, email address, and new

PIN for each user who's PIN was changed. You can use the .csv file to send an email to each user with the new PIN. The utility is available on the Cisco Unity Tools website at http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html.