Next Generation Security

Overview

Cisco Unity Connection supports Next Generation Security that provides confidentiality, integrity, and authentication through Suite B cryptographic algorithm. Suite B algorithm includes various components, such as AES encryption and ECDSA ciphers to meet security and scalability requirements of an organization.

Next Generation Security	Supported Version
Authentication Signature Algorithm	RSA (1024/2048/3092/4096) ECDSA (256/384/512)
Message Integrity	SHA-256 SHA-384 SHA-512
Encryption	AES-GCM (128/256) mode
Key Agreement	ECDH (256/384)

Note

- Unity Connection supports TLS 1.2 for Next Generation Security.
- Next Generation Security does not support RSA 1024 key when FIPS is enabled.

Unity Connection supports Next Generation Security over the following interfaces:

- HTTPS
- SIP
- SRTP

Note In addition to the above interfaces, Unity Connection supports Next Generation Security over SMTP interface as well with default cipher settings.

Next Generation Security Over HTTPS Interface

Next Generation Security over HTTPS Interface restricts web applications deployed over tomcat or jetty to use Suite B ciphers for inbound connections with Unity Connection. User must enable SSL to activate Next generation Security over Jetty or Web interface. For more information on enabling SSL over Connection Jetty, see the applicable *Command Line Interface Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configuring Next Generation Security Over HTTPS Interface

To configure Next Generation Security over HTTPS interface:

Step 1 Sign in to Cisco Unity Connection Administration page, expand **System Settings** > **General Configurations** and select **HTTPS Ciphers**.

Step 2 Select any one of the following:

- **All Supported EC and RSA Ciphers**: When this option is selected, Unity Connection server negotiates with both EC based and RSA based ciphers.
- **RSA Ciphers Only**: When this option is selected, Unity Connection server negotiates with RSA based ciphers only.

Below table lists the HTTPS Cipher options in priority order of RSA or ECDSA ciphers:

Table 1: HTTPS Cipher options with Priority order

HTTPS Cipher Options	HTTPS Ciphers in Priority Order
All Supported EC and RSA Ciphers	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA • SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

HTTPS Cipher Options	HTTPS Ciphers in Priority Order
RSA Ciphers Only	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA • SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

Step 3 Select **Save** to apply the changes.

Note After modifying the HTTPS cipher, make sure to restart tomcat service for the changes to take effect. In addition, you must also disable and enable jetty over SSL using the utils cuc jetty ssl {disable/enable} command, if jetty SSL is enabled.

Next Generation Security Over SIP Interface

Next Generation Security over SIP interface restricts SIP interface to use Suite B ciphers based on TLS 1.2, SHA-2 and AES256 protocols. It allows the various combinations of ciphers based on the priority order of RSA or ECDSA ciphers.

To specify the ciphers that should be used to enable Next Generation Security over SIP interface, navigate to **System Settings** > **General Configuration** and select the cipher from the **TLS Ciphers** drop-down list.

Note Next Generation Security over SIP interface uses only Encryption security mode.

For more information on configuring ciphers and third party certificates over SRTP interface, see "Enabling Next Generation Security over SIP Integration" section of "Setting Up a Cisco Unified Communications Manager SIP Trunk Integration" chapter of *Cisco Unified Communications Manager Cisco Unified Communication 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.

Next Generation Security Over SRTP Interface

Next Generation Security over SRTP interface restricts SRTP interface to use Suite B ciphers based on SHA-2 and AES256 protocols.

To specify the ciphers that should be used to enable Next Generation Security over SRTP interface, navigate to **System Settings** > **General Configuration** and select the cipher from the **SRTP Ciphers** drop-down list.

For more information on configuring ciphers and third party certificates over SRTP interface, see "Enabling Next Generation Security over SIP Integration" section of "Setting Up a Cisco Unified Communications Manager SIP Trunk Integration" chapter of *Cisco Unified Communications Manager Cisco Unified*

Communication 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.