Setting Up a Cisco Unified Communications Manager SIP Trunk Integration

This chapter provides instructions for setting up a Cisco Unified Communications Manager SIP trunk integration with Cisco Unity Connection. This document does not apply to the configuration in which Unity Connection is installed as Cisco Business Edition—on the same server with Cisco Unified CM.

Note If you are configuring MWI relay across trunks in a distributed phone system, you must see the Cisco Unified CM documentation for requirements and instructions. Configuring MWI relay across trunks does not involve Unity Connection settings.

Cisco Unified CM Music on Hold (MOH) feature is not available during supervised transfers for the Cisco Unified CM SIP trunk integration.

Pre-requisites

Before starting the SIP integration between Cisco Unified CM and Unity Connection, you need to understand the tasks to be done and the components required for the integration. Below table contains a list of pre-requisites that you must consider to ensure a successful integration.

Pre-requisites	Important Notes
Install the applicable version of Cisco Unified CM.	• For compatible version of Cisco Unified CM, see the *Compatibility Matrix: Cisco Unity Connectio* http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-device-support-tables-list.html
Install the applicable version of Unity Connection with a license that enables the applicable number of voice messaging ports.	• For details on compatible versions of Unity Connection, see the Compatibility Matrix for Cisco Un Connection at http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-device-support-tables-list.html • For details on installation tasks, see the "Installing Cisco Unity Connection" chapter of the *Install, Up 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_15cucium

The supported Phone system for SCCP integration are: • Only IP phones for the Cisco Unified CM extensions. • Both IP phones and SIP phones for the Cisco Unified CM extensions without a media termination point (MTP) on the Cisco Unified CM server.	• A LAN connection in each location is required where you plug the applicable phone into the ne • For multiple Cisco Unified CM clusters, the capability for users to dial an extension on another Unified CM cluster without dialing a trunk access code or prefix.

If Unity Connection uses IPv6 or dual-mode (IPv4 and IPv6) to communicate with Cisco Unified CM, do the following subtasks: 1. Enable IPv6 on the Unity Connection server. 2. In Cisco Unity Connection Administration, on the **System Settings** > **General Configuration** page, select an option for IP Addressing Mode to control where Unity Connection listens for incoming traffic. You can select IPv4, IPv6, or IPv4 and IPv6. The setting defaults to IPv4.	See the "Ethernet IPv6 Configuration Settings" section in the "Settings" chapter of the Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 15 at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15cucosag

Use of Tomcat Certificates for Secure SIP Call

Cisco Unity Connection supports the use of RSA key based Tomcat certificates to configure secure calls in place of SIP certificates. This allows the use of both self signed and third-party CA signed certificates for SIP secure call.

Integration Tasks

Do the tasks mentioned in the following table to integrate Cisco Unified CM with Unity Connection in a standalone or cluster mode through a SIP trunk.

Table 1: Integration Tasks

Integration Scenario	Integration Tasks

Integration between Cisco Unified CM and Unity Connection (Standalone)	• Planning the Voice Messaging Ports in Cisco Unity Connection
	• Configuring Cisco Unified CM for Integration
	  • Creating SIP Trunk Security Profile
	  • Creating SIP Profile
	  • Creating SIP Trunk
	  • Creating Route Pattern
	  • Creating Voice Mail Pilot
	  • Setting Up Voice Mail Profile
	  • Setting Up Voice Mail Server Service Parameters
	• Configuring Unity Connection for Integration
	• Testing the Integration
	• Optional Tasks
	  • (Optional) Setting Up SIP Digest Authentication
	  • (Optional) Creating Application User

Integration Scenario	Integration Tasks

Integration between Cisco Unified CM and Unity Connection (Cluster mode)	• Planning the Voice Messaging Ports in Cisco Unity Connection
	• Configuring Cisco Unified CM for Integration
	  • Creating SIP Trunk Security Profile
	  • Creating SIP Profile
	  • Creating SIP Trunk
	  • Creating Route Pattern
	  • Creating Route List
	  • Creating Route Pattern
	  • Creating Voice Mail Pilot
	  • Setting Up Voice Mail Profile
	  • Setting Up Voice Mail Server Service Parameters
	• Configuring Unity Connection for Integration
	• Testing the Integration
	• Optional Tasks
	  • (Optional) Setting Up SIP Digest Authentication
	  • (Optional) Creating Application User
	  • (Optional) Setting up an AXL Server, on page 15

Note If this is the first integration, the first phone system is automatically selected in the default user template. The users that you add after creating the phone system integration are assigned to this phone system by default. However, for each subsequent integration add the applicable new user templates for the new phone system.For details on adding new user templates, or on selecting a user template when adding a new user, see the User Templates section in "User Attributes" chapter of the System Administration Guide for Cisco Unity Connection, Release 15 available at, https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/administration/guide/b_15cucsag.html

Creating SIP Trunk Security Profile

There must be a c alling search space that is used by all user phones (directory numbers). Otherwise, the integration does not function correctly. For instructions on setting up a calling search space and assigning user phones to it, see the Cisco Unified CM Help.

Step 1 In Cisco Unified CM Administration, on the System menu, navigate to **Security** > **and select** > **SIP Trunk Security Profile**.

Step 2 On the Find and List SIP Trunk Security Profiles page, select **Add New**.

Step 3 On the SIP Trunk Security Profile Configuration page, under SIP Trunk Security Profile Information, enter the following settings.

Table 2: Settings for the SIP Trunk Security Profile Configuration Page

Field	Setting
Name	Enter **Unity Connection SIP Trunk Security Profile** or another name.
Description	Enter **SIP trunk security profile for Cisco Unity Connection** or another description.
Device Security Mode	If you cannot enable Cisco Unified CM authentication and encryption, accept the default of **Non Secure**. If you enable Cisco Unified CM authentication or encryption, select **Authenticated** or **Encrypted**. Note the following requirements for the Cisco Unified CM server: • A TFTP server must be configured. • The Cisco Unified CM server must be configured for secure signalling and media. For details see the Default Security Overview section of the "Default Security " chapter in *Security Guide for Cisco Unified Communications Manager release 15* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/15_0/cucm_b_security-guide-release-15.html • The Device Security Mode setting on the Cisco Unified CM server must match the Security Mode setting on the Unity Connection server (Authenticated or Encrypted). **Note** If Next Generation Encryption is enabled on Cisco Unity Connection, "**Encrypted**" must be selected on Cisco Unified CM server.
X.509 Subject Name	If you cannot enable Cisco Unified CM authentication and encryption, leave this field blank. If you enable Cisco Unified CM authentication and encryption, enter **Connection** or another name. This name must match the Subject Name field for the SIP certificate on the Unity Connection server. **Note** X.509 Subject Name must match the FQDN of Unity Connection server.
Accept Out-of-Dialog REFER	Check this check box.
Accept Unsolicited Notification	Check this check box.
Accept Replaces Header	Check this check box.

Step 4 Select **Save**.

Creating SIP Profile

Step 1 On the Device menu, navigate to **Device Settings** > **and select** > **SIP Profile**.

Step 2 On the Find and List SIP Profiles page, select **Find**.

Step 3 To the right of the SIP profile that you want to copy, select **Copy**.

Step 4 On the SIP Profile Configuration page, under SIP Profile Information, enter the following settings.

Table 3: Settings for the SIP Profile Configuration Page

Field	Setting
Name	Enter **Unity Connection SIP Profile** or another name.
Description	Enter **SIP profile for Unity Connection** or another description.

Step 5 If Unity Connection uses IPv6 or dual-stack IPv4 and IPv6 to communicate with Cisco Unified CM, check the Enable ANAT check box. This step is required to ensure proper handling of callers in an IPv6 or dual-stack environment.

Step 6 Select **Save**.

Creating SIP Trunk

Step 1 On the Device menu, select **Trunk**.

Step 2 On the Find and List Trunks page, select **Add New**.

Step 3 On the Trunk Configuration page, in the Trunk Type field, select **SIP Trunk**.

Step 4 In the Device Protocol field, select **SIP** and select **Next**.

Step 5 Under Device Information, enter the following settings.

Table 4: Settings for Device Information on the Trunk Configuration Page

Field	Setting
Device Name	Enter **Unity_Connection_SIP_Trunk** or another name.
Description	Enter **SIP trunk for Unity Connection** or another description.
SRTP Allowed	If you enable Cisco Unified CM authentication and encryption, check this check box.

Step 6 If user phones are contained in a calling search space, under Inbound Calls, enter the following settings. Otherwise, continue to Step 7.

Table 5: Settings for Inbound Calls on the Trunk Configuration Page

Field	Setting
Calling Search Space	Select the name of the calling search space that contains the user phones.
Redirecting Diversion Header Delivery - Inbound	Check this check box.

Step 7 If user phones are contained in a calling search space, under Outbound Calls, enter the following settings.

Field	Setting
Redirecting Diversion Header Delivery - Outbound	Check this check box.
Deliver DN only in connected party	In outgoing SIP messages, Unity Connection inserts the calling party's directory number in the SIP contact header information. This is the default setting.
Deliver URI only in connected party	In outgoing SIP messages, Unity Connection inserts the sending party's directory URI in the SIP contact header. If a directory URI is not available, Unity Connection inserts the directory number instead.
Deliver URI and DN in connected party	In outgoing SIP messages, Unity Connection inserts a blended address that includes the calling party's directory URI and directory number in the SIP contact headers. If a directory URI is not available, Unity Connection includes the directory number only.

Settings Outbound Calls on Trunk Configuration Page

Step 8 Under SIP Information, enter the following settings.

Table 6: Settings for SIP Information on the Trunk Configuration Page

Field	Setting
Destination Address	Enter the IP address of the Unity Connection SIP port to which Cisco Unified CM connects.
Destination Address IPv6	Enter the IPv6 address of the Unity Connection SIP port to which Cisco Unified CM connects. The IPv6 address should be in canonical textual representation format proposed by "RFC 5952" standard for IPv6 Address Text Representation. **Note** IPv6 is supported for SIP integrations between Unity Connection and Cisco Unified CM .
Destination Port	We recommend that you accept the default of **5060**.

Field	Setting
SIP Trunk Security Profile	Select the name of the SIP trunk security profile that you created in the Creating SIP Trunk Security Profile. For example, select "Unity Connection SIP Trunk Security Profile."
Rerouting Calling Search Space	Select the name of the calling search space that is used by user phones.
Out-of-Dialog Refer Calling Search Space	Select the name of the calling search space that is used by user phones.
SIP Profile	Select the name of the SIP profile that you created in the Creating SIP Profile. For example, select "Unity Connection SIP Profile."

Step 9 Adjust any other settings that are needed for your site.

Step 10 Select **Save**.

Creating Route Pattern

Step 1 On the Call Routing menu, navigate to **Route/Hunt** > **and select** > **Route Pattern**.

Step 2 On the Find and List Route Patterns page, select **Add New**.

Step 3 On the Route Pattern Configuration page, enter the following settings.

Table 7: Settings for the Route Pattern Configuration Page

Field	Setting
Route Pattern	Enter the voice mail pilot number for Unity Connection.
Gateway/Route List	Select the name of the SIP trunk that you created in the Creating SIP Trunk. For example, select "Unity_Connection_SIP_Trunk."

Step 4 Select **Save**.

Creating Route Group

Step 1 On the Call Routing menu, navigate to **Route/Hunt** > **and select** > **Route Group**.

Step 2 On the Find and List Route Groups page, select **Add New**.

Step 3 On the Route Group Configuration page, enter the following settings.

Table 8: Settings for the Route Group Configuration Page

Field	Setting
Route Group Name	Enter **SIP_Trunk_Route_Group** or another name.
Distribution Algorithm	Select **Top Down**.

Step 4 Confirm that both SIP trunks appear in the Available Devices field. Otherwise, select **Find**.

Step 5 Select **Add to Route Group**.

Step 6 Under Current Route Group Members, confirm that the SIP trunk that connects to the subscriber server appears first in the list.

You can select the up or down arrows to change the order of the SIP trunks.

Step 7 Select **Save**.

Creating Route List

Step 1 On the Call Routing menu, navigate to **Route/Hunt** > **and select** > **Route List**.

Step 2 On the Find and List Route Lists page, select **Add New**.

Step 3 On the Route List Configuration page, enter the following settings.

Table 9: Settings for the Route List Configuration Page

Field	Setting
Name	Enter **SIP_Trunk_Route_List** or another name.
Description	Enter **SIP Trunk Route List** or another description.
Cisco Unified Communications Manager Group	Select **Default**.

Step 4 Select **Save**.

Step 5 Confirm that the **Enable This Route List** check box is checked.

Step 6 Under Route List Member Information, select **Add Route Group**.

Step 7 On the Route List Detail Configuration page, in the Route Group field, select the Route Group that you created in the Configuring Unity Connection for Integration and select **Save**.

Step 8 When prompted that the route list settings are saved, select **OK**.

Step 9 On the Route List Configuration page, select **Reset**.

Step 10 When prompted to confirm resetting the route list, select **Reset**.

Step 11 Select **Close**.

Creating Voice Mail Pilot

Step 1 On the Advanced Features menu, navigate to **Voice Mail** > **and select** > **Voice Mail Pilot**.

Step 2 On the Find and List Voice Mail Pilots page, select **Add New**.

Step 3 On the Voice Mail Pilot Configuration page, enter the following voice mail pilot number settings.

Table 10: Settings for the Voice Mail Pilot Configuration Page

Field	Setting
Voice Mail Pilot Number	Enter the voice mail pilot number that users dial to listen to their voice messages. This number must match the route pattern that you entered in the Creating Route Pattern.
Calling Search Space	Select the calling search space that includes partitions containing the user phones and the partition that you set up for the voice mail pilot number.
Description	Enter **Unity Connection Pilot** or another description.
Make This the Default Voice Mail Pilot for the System	Check this check box. When this check box is checked, this voice mail pilot number replaces the current default pilot number.

Step 4 Select **Save**.

Setting Up Voice Mail Profile

Step 1 On the Advanced Features menu, navigate to **Voice Mail** > **and select** > **Voice Mail Profile**.

Step 2 On the Find and List Voice Mail Profiles page, select **Add New**.

Step 3 On the Voice Mail Profile Configuration page, enter the following voice mail profile settings.

Table 11: Settings for the Voice Mail Profile Configuration Page

Field	Setting
Voice Mail Profile Name	Enter **Unity Connection Profile** or another name to identify the voice mail profile.
Description	Enter **Profile for Unity Connection** or another description.
Voice Mail Pilot	Select the voice mail pilot that you defined in the Creating Voice Mail Pilot.

Field	Setting
Voice Mail Box Mask	When multitenant services are not enabled on Cisco Unified CM, leave this field blank. When multitenant services are enabled, each tenant uses its own voice mail profile and must create a mask to identify the extensions (directory numbers) in each partition that is shared with other tenants. For example, one tenant can use a mask 972813XXXX, while another tenant can use the mask 214333XXXX. Each tenant also uses its own translation patterns for MWIs.
Make This the Default Voice Mail Profile for the System	Check this check box to make this voice mail profile the default. When this check box is checked, this voice mail profile replaces the current default voice mail profile.

Step 4 Select **Save**.

Setting Up Voice Mail Server Service Parameters

If you do not want to set up SIP digest authentication, continue to the Configuring Unity Connection for Integration.

Step 1 In Cisco Unified CM Administration, snavigate to **System** > **and select** > **Service Parameters**.

Step 2 On the Service Parameters Configuration page, in the Server field, select the name of the Cisco Unified CM server.

Step 3 In the Service list, select **Cisco CallManager**. The list of parameters appears.

Step 4 Under Clusterwide Parameters (Feature - General), locate the Multiple Tenant MWI Modes parameter.

Step 5 If you use multiple tenant MWI notification, select **True**.

When this parameter is set to True, Cisco Unified CM uses any configured translation patterns to convert voicemail extensions into directory numbers when turning on or off an MWI.

Step 6 If you changed any settings, select **Save**. Then shut down and restart the Cisco Unified CM server.

(Optional) Setting Up SIP Digest Authentication

Step 1 On the System menu, navigate to **Security** > **and sele ct** > **SIP Trunk Security Profile**.

Step 2 On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the Creating SIP Trunk Security Profile.

Step 3 On the SIP Trunk Security Profile Configuration page, check the **Enable Digest Authentication** check box.

Step 4 Select **Save**.

(Optional) Creating Application User

Step 1 On the User Management menu, select **Application User**.

Step 2 On the Find and List Application Users page, select **Add New**.

Step 3 On the Application User Configuration page, enter the following settings.

Table 12: Settings for the Application User Configuration Page

Field	Setting
User ID	Enter the application user identification name. Cisco Unified CM does not permit modifying the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \, , “”, and blank spaces.
Password	Enter the same password that you use for the digest credentials.
Confirm Password	Enter the password again.
Digest Credentials	Enter the name of the digest credentials.
Accept Replaces Header	Leave this check box unchecked.
Available Devices	This list box displays the devices that are available for association with this application user. To associate a device with this application user, select the device and select the Down arrow below this list box. If the device that you want to associate with this application user does not appear in this pane, select one of these buttons to search for other devices: • **Find More Phones**—Select this button to find more phones to associate with this application user. The Find and List Phones window appears to enable a phone search. • **Find More Route Points**—Select this button to find more phones to associate with this application user. The Find and List CTI Route Points window displays to enable a CTI route point search.
Associated CAPF Profiles	In the Associated CAPF Profile pane, the Instance ID for the Application User CAPF Profile displays if you configured an Application User CAPF Profile for the user. To edit the profile, select the Instance ID; then, select Edit Profile. The Application User CAPF Profile Configuration window appears.
Groups	The list box displays the groups to which the application user belongs.
Roles	The list box displays the roles that are assigned to the application user.

Step 4 Select **Save**.

(Optional) Setting up an AXL Server

Do the following configurations if Unity Connection connects to an AXL server.

Step 1 Expand **Telephony Integrations** and select Phone System.

Step 2 On the Search Phone Systems page, select the display name of the phone system that you created.

Step 3 On the Phone System Basics page, in the Edit menu, select **Cisco Unified Communications Manager AXL Servers**.

Connecting to an AXL server is needed when Unity Connection needs to have access to the Cisco Unified CM database for importing Cisco Unified CM users and for changing certain phone settings for users of Cisco Unity Connection personal call transfer rules.

Note If you plan to import Cisco Unified CM users, confirm that the Primary Extension field on the End User Configuration page for each user is filled in. Otherwise, the search does not find any users to select for importing.

Step 4 On the **Edit AXL Servers** page, under AXL Servers, select **Add New**.

Step 5 Enter the following settings for the AXL server and select Save.

Table 13: Settings for AXL Server

Field	Setting
Order	Enter the order of priority for the AXL server. The lowest number is the primary AXL server, the higher numbers are the secondary servers.
IP Address	Enter the IP address of the AXL server.
Port	Enter the AXL server port that Unity Connection connects to. This setting must match the port that the AXL server uses.

Step 6 Repeat Step 4 and Step 5 for all remaining AXL servers.

Step 7 Under AXL Server Settings, enter the following settings and select Save.

Table 14: Settings for AXL Server

Field	Setting
Username	Enter the username that Unity Connection uses to sign in to the AXL server. **Note** This user must match the user name of a Cisco Unified CM application user who is assigned to the "Standard AXL API Access" role.

Field	Setting
Password	Enter the password for the user that Unity Connection uses to sign in to the AXL server. **Note** This password must match the password of the Cisco Unified CM application user entered in the User Name field.
Cisco Unified Communications Manager Version	Select the applicable setting that accurately describes the following: • The version of Cisco Unified CM that you are integrating with Unity Connection. • Whether the AXL port is enabled for SSL. If you select the non-SSL version, the AXL port must be a non-SSL port (typically port 80). If you select the SSL-enabled version, the AXL port must be an SSL-enabled port (typically port 443 or port 8443).
Enable End User PIN Synchronization for Primary AXL Server	Check this check box to enable PIN synchronization between Unity Connection and Cisco Unified CM for the users having same user ID (alias in Unity Connection). After enabling the feature whenever user updates the PIN on Cisco Unity Connection, the PIN gets synchronized with Cisco Unified CM and vice-versa. Default setting: Check box is not checked. For more information on PIN Synchronization, see the "PIN Generation between Unity Connection and Cisco Unified CM" section of the "User Settings" chapter of the *System Administration Guide for Cisco Unity Connection Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/design/b_15cucsag/b_12xcucsag_appendix_010011.html .
Ignore Certificate Errors	Check the check box to ignore certificate validation errors for AXL Servers. When the check box is unchecked, Unity Connection validates the certificate for the AXL servers. However, before checking the checkbox make sure that the tomcat root certificate of Cisco Unified CM must be uploaded to tomcat trust of Unity Connection server. Default setting: Check box is checked. For more information on certificates, see "Security" chapter of *Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 15* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/os_administration/guide/b_15cucosagx.html.

Step 8 To add a corresponding application server to Cisco Unified CM, sign in to Cisco Unified CM Administration.

Step 9 In Cisco Unified CM Administration, navigate to **System > Application Server** page.

Step 10 On the Find and List Application Servers page, select Find to display all application servers.

Step 11 In the Name column, select the name of the Cisco Unity Connection server.

Step 12 On the Application Server Configuration page, in the Available Application User field, select the Cisco Unified CM application user that you used in Step 7 and select the down arrow to move it to the Selected Application User field.

Step 13 Select **Save**.

Configuring Unity Connection for Integration

Unity Connection uses certificates and security profiles for authentication and encryption of voice messaging ports through SIP trunk integration with Cisco Unified Communications Manager.

Prerequisites

Before beginning the Integration process, you must consider the following points for successful Secure SIP Configuration.

- Cisco Unity Connection must be registered with Smart Licensing that has the Export-Controlled Functionality as allowed. For more information on Cisco Smart Software Licensing, see the Smart Software Licensing Overview section in the Smart Software Licensing chapter of the *System Configuration Guide for Cisco Unified Communications Manager, Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/15/systemConfig/cucm_b_system-configuration-guide-15.html
- Cisco Unity Connection must be running a Restricted version. For more information on the Restricted and Unrestricted Version in Cisco Unity Connection, see Cisco Unity Connection - Restricted and Unrestricted Version section in the Cisco Unity Connection - Restricted and Unrestricted Version chapter of the Security Guide for Cisco Unity Connection Release 15 available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/security/b_15cucsecx.html
- Cisco Unity Connection must be enabled for encryption via CLI command "**utils cuc encryption enable**". For more information on the CLI command, see the Command Line Interface Reference Guide for Cisco Unified Solutions for the latest release, available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

After ensuring that Cisco Unified Communications Manager and Unity Connection are ready for the integration, do the following procedure to set up the integration and to enter the port settings.

Creating an Integration

Step 1 Sign in to Cisco Unity Connection Administration.

Step 2 In Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Phone System**.

Step 3 On the Search Phone Systems page, under Display Name, select the name of the default phone system.

Step 4 On the Phone System Basics page, in the Phone System Name field, enter the descriptive name that you want for the phone system.

Step 5 If you want to use this phone system as the default for TRaP connections so that administrators and users without voicemail boxes can record and playback through the phone in Unity Connection web applications, check the **Default TRAP Switch** check box. If you want to use another phone system as the default for TRaP connections, uncheck this check box.

Step 6 Select **Save**.

Step 7 On the Phone System Basics page, in the Related Links drop-down box, select **Add Port Group** and select **Go**.

Step 8 On the New Port Group page, enter the applicable settings and select **Save**.

Table 15: Settings for the New Port Group Page

Field	Setting
Phone System	Select the name of the phone system that you entered in Step 5.
Create From	Select **Port Group Template** and select **SIP** in the drop-down box.
Display Name	Enter a descriptive name for the port group. You can accept the default name or enter the name that you want.
Authenticate with SIP Server	Check this check box if you want Unity Connection to authenticate with the Cisco Unified CM server.
Authentication User Name	Enter the name that Unity Connection uses to authenticate with the Cisco Unified CM server.
Authentication Password	Enter the password that Unity Connection uses to authenticate with the Cisco Unified CM server.
Contact Line Name	Enter the voice messaging line name (or pilot number) that users use to contact Unity Connection and that Unity Connection uses to register with the Cisco Unified CM server.
SIP Security Profile	Select the SIP security profile that Unity Connection uses.
Enable Next Generation Encryption	**Note** (*Only when a secure TLS port is used*) Check this check box if you want Unity Connection to use RSA key based or EC key based certificates (self signed and third party certificates) to provide Next Generation encryption Support on SIP interface.For more information refer Enabling Next Generation Security over SIP Integration.
Security Mode	*(Only when a secure TLS port is used and Enable Next Generation Encryption check box is unchecked)* Select the applicable security mode: • **Authenticated**—The integrity of call-signaling messages are ensured because they are connected to Cisco Unified CM through an secure TLS port. However, the privacy of call-signaling messages are not ensured because they are sent as clear (unencrypted) text. • **Encrypted**—The integrity and privacy of call-signaling messages are ensured on this port because they are connected to Cisco Unified CM through an secure TLS port, and the call-signaling messages are encrypted. The Security Mode setting on the Unity Connection server must match the Device Security Mode setting on the Cisco Unified CM server.
Secure RTP	*(Only when a secure TLS port is used)* Check this check box so that the media stream (RTP) is encrypted. Uncheck this check box so that the media stream is not encrypted.
SIP Transport Protocol	Select the SIP transport protocol that Unity Connection uses.

Field	Setting
IPv4 Address or Host Name	Enter the IPv4 address (or host name) of the primary Cisco Unified CM server that you are integrating with Unity Connection. You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.
IPv6 Address or Host Name	Enter the IPv6 address (or host name) of the primary Cisco Unified CM server that you are integrating with Unity Connection. The IPv6 address should be in canonical textual representation format proposed by "RFC 5952" standard for IPv6 Address Text Representation. You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank. **Note** IPv6 is supported for SIP integrations with Cisco Unified CM 10.0.
IP Address or Host Name	Enter the IP address (or host name) of the primary Cisco Unified CM server that you are integrating with Cisco Unity Connection.
Port	Enter the TCP port of the primary Cisco Unified CM server that you are integrating with Unity Connection. We recommend that you use the default setting.

Step 9 On the Port Group Basics page, do the following substeps if the Cisco Unified CM cluster has secondary servers, or if you want to add a TFTP server (required for Cisco Unified CM authentication and encryption). Otherwise, skip to Step 11.

a) On the Edit menu, select **Servers**.

b) If you want to add a secondary Cisco Unified CM server, on the Edit Servers page, under SIP Servers, select **Add**. Otherwise, skip to Step 10e.

c) Enter the following settings for the secondary Cisco Unified CM server and select **Save**.

Table 16: Settings for the SIP Servers

Field	Setting
Order	Enter the order of priority for the Cisco Unified CM server. The lowest number is the primary Cisco Unified CM server, the higher numbers are the secondary servers.
IPv4 Address or Host Name	Enter the IPv4 address (or host name) of the secondary Cisco Unified CM server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.

Field	Setting
IPv6 Address or Host Name	Enter the IPv6 address (or host name) of the secondary Cisco Unified CM server. The IPv6 address should be in canonical textual representation format proposed by "RFC 5952" standard for IPv6 Address Text Representation. You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank. **Note** IPv6 is supported for SIP integrations with Cisco Unified CM 10.0.
IP Address or Host Name	Enter the IP address (or host name) of the secondary Cisco Unified CM server.
Port	Enter the IP port of the Cisco Unified CM server that you are integrating with Unity Connection. We recommend that you use the default setting.
TLS Port	Enter the TLS port of the Cisco Unified CM server that you are integrating with Unity Connection. We recommend that you use the default setting.

d) If applicable, repeat Step 10b. and Step 10c. for an additional Cisco Unified CM server in the Cisco Unified CM cluster.

e) If you want to add a TFTP server (required for Cisco Unified CM authentication and encryption), under TFTP Servers, select **Add**. Otherwise, skip to Step 10h.

f) Enter the following settings for the TFTP server and select **Save**.

Table 17: Settings for the TFTP Servers

Field	Setting
Order	Enter the order of priority for the TFTP server. The lowest number is the primary TFTP server, the higher numbers are the secondary servers.
IPv4 Address or Host Name	Enter the IPv4 address (or host name) of the TFTP server. You must enter an IP address or host name in this field, or an IP address or host name in the IPv6 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank.

Field	Setting
IPv6 Address or Host Name	Enter the IPv6 address (or host name) of the TFTP server. The IPv6 address should be in canonical textual representation format proposed by "RFC 5952" standard for IPv6 Address Text Representation. You must enter an IP address or host name in this field, or an IP address or host name in the IPv4 Address or Host Name field (or, if applicable, enter information in both fields). You cannot leave both fields blank. **Note** • IPv6 is supported for SIP integrations with Cisco Unified CM 10.0. • If you select a secured SIP profile from the SIP security profile drop down menu with IPv6 configuration in the **Primary Server Settings,** then make sure that the DNS server should be able to resolve both the IPv6 address and host name correctly.
IP Address or Host Name	Enter the IP address (or host name) of the TFTP server.

g) If applicable, repeat Step 10e. and Step 10f. for an additional TFTP server.
h) On the Edit menu, select **Port Group Basics**.
i) On the Port Group Basics page, select **Reset**.

Step 10 On the Port Group Basics page, in the Related Links drop-down box, select **Add Ports** and select **Go**.

Step 11 On the New Port page, enter the following settings and select **Save**.

Table 18: Settings for the New Port Page

Field	Setting
Enabled	Check this check box.
Number of Ports	Enter the number of voice messaging ports that you want to create in this port group. **Note** For a Unity Connection cluster, you must enter the total number of voice messaging ports that are used by all Unity Connection servers. Each port is later assigned to a specific Unity Connection server.
Phone System	Select the name of the phone system that you entered in Step 5.
Port Group	Select the name of the port group that you added in Step 9.
Server	Select the name Unity Connection server.

Step 12 On the Search Ports page, select the display name of the first voice messaging port that you created for this phone system integration.

Note By default, the display names for the voice messaging ports are composed of the port group display name followed by incrementing numbers.

Step 13 On the Port Basics page, set the voice messaging port settings as applicable. The fields in the following table are the ones that you can change.

Table 19: Settings for the Voice Messaging Ports

Field	Considerations
Enabled	Check this check box to enable the port. The port is enabled during normal operation. Uncheck this check box to disable the port. When the port is disabled, calls to the port get a ringing tone but are not answered. Typically, the port is disabled only by the installer during testing.
Server	*(For Unity Connection clusters only)* Select the name of the Unity Connection server that you want to handle this port. Assign an equal number of answering and dial-out voice messaging ports to the Cisco Unity Connection servers so that they equally share the voice messaging traffic.
Answer Calls	Check this check box to designate the port for answering calls. These calls can be incoming calls from unidentified callers or from users.
Perform Message Notification	Check this check box to designate the port for notifying users of messages. Assign Perform Message Notification to the least busy ports.
Send MWI Requests	Check this check box to designate the port for turning MWIs on and off. Assign Send MWI Requests to the least busy ports.
Allow TRAP Connections	Check this check box so that users can use the port for recording and playback through the phone in Unity Connection web applications. Assign Allow TRAP Connections to the least busy ports.

Step 14 Select **Save**.

Step 15 Select **Next**.

Step 16 Repeat Step 14 through Step 16 for all remaining voice messaging ports for the phone system.

Step 17 If you use Cisco Unified CM authentication and encryption then generate and upload RSA key based Tomcat certificates. For details, see Settings for RSA Key Based certificates section.

Step 18 If another phone system integration exists, in Cisco Unity Connection Administration, expand **Telephony Integrations**, then select **Trunk**.

Step 19 On the Search Phone System Trunks page, on the Phone System Trunk menu, select **New Phone System Trunk**.

Step 20 On the New Phone System Trunk page, enter the following settings for the phone system trunk and select **Save**.

Table 20: Settings for the Phone System Trunk

Field	Setting
From Phone System	Select the display name of the phone system that you are creating a trunk for.
To Phone System	Select the display name of the previously existing phone system that the trunk connects to.
Trunk Access Code	Enter the extra digits that Unity Connection must dial to transfer calls through the gateway to extensions on the previously existing phone system.

Step 21 Repeat Step 18 and Step 19 for all remaining phone system trunks that you want to create.

Enabling Next Generation Security over SIP Integration

Unity Connection supports Next Generation Security over SIP interface which provides confidentiality, integrity, and authentication through cryptographic algorithms. Next Generation Encryption is more secure as it restricts SIP interface to use Suite B ciphers based on TLS 1.2, SHA-2 and AES256 protocols. In addition to ciphers, Next Generation Encryption also includes third party certificates that must be uploaded on both Unity Connection and Cisco Unified CM. During the communication between Unity Connection and Cisco Unified CM, both ciphers and third party certificates are verified at both the ends. Below is the configuration for Next Generation Encryption support:

Generate and Upload Certificates

Unity Connection uses RSA key based Tomcat certificates and EC key based tomcat-ECDSA certificates (self signed and third party) for next generation security. The settings for each certificate are described in further sections.

Settings for RSA Key Based certificates

Generating RSA Key Based Certificates of Unity Connection

Below are the steps to generate RSA key based certificates of Unity Connection and uploading them on Cisco Unified CM:

Step 1 On Unity Connection, sign in to Cisco Unified Operating System Administration page.

Step 2 Navigate to Security and select **Certificate Management**.

Step 3 If you want to generate self signed certificates of Unity Connection, follow the Step 4 to Step 6. Otherwise skip to Step 7.

Step 4 On Certificate Management page, select **Generate Self Signed**.

Step 5 In the Generate Self-Signed window, select **tomcat** in Certificate Purpose.

Step 6 Select **Generate**.

Step 7 To generate RSA key based third party certificates, select **Generate CSR** on Certificate Management page.

Step 8 In the Generate Certificate Signing Request window, select **tomcat** in Certificate Purpose field.

Step 9 In Parent Domain field, enter the complete FQDN of Unity Connection.

Step 10 Select **Generate**.

Step 11 On Certificate List page, select **Download CSR**. This generates the Unity Connection certificates from third party that is Microsoft CA or Verisign.

Step 12 Save the leaf certificate of Unity Connection and root/chain certificate of certification authority on your system.

Step 13 On Certificate List page, select **Upload Certificate/Certificate** Chain.

Step 14 In the Upload Certificate/Certificate Chain window, select **tomcat** in Certificate Purpose field.

Step 15 Navigate to Upload File, select **Browse** and upload the Unity Connection leaf certificate generated by third party CSR, which you have saved in Step 12.

Step 16 Select **Upload**.

Step 17 On Cisco Unified CM, sign in to Cisco Unified Operating System Administration page.

Step 18 Navigate to Security and select **Certificate Management**.

Step 19 On Certificate List page, select **Upload Certificate/Certificate Chain**.

Step 20 In the Upload Certificate/Certificate Chain window, select **CallManager-trust** in Certificate Purpose field.

Step 21 Navigate to Upload File, select Browse and upload the Unity Connection self signed certificate generated in Step 6. To upload Unity Connection third party certificates, browse to the root/chain certificate of third party Certification Authority saved in Step 12.

Note In case of Unity Connection cluster, generate and upload self signed certificates of both publisher and subscriber in CallManager-trust of Cisco Unified CM.

Step 22 Select **Upload**.

Generating RSA Based Certificates of Cisco Unified CM

Below are the steps to generate RSA based certificates of Cisco Unified CM and uploading them on Unity Connection:

Step 1 On Cisco Unified CM, sign in to Cisco Unified Operating System Administration page.

Step 2 Navigate to Security and select **Certificate Management**.

Step 3 If you want to generate self signed certificates of Cisco Unified CM, follow Step 4 to Step 6. Otherwise skip to Step 7.

Step 4 On Certificate Management page, select **Generate Self Signed**.

Step 5 In the Generate New Self Signed Certificate window, select **CallManager** in **Certificate Purpose** field.

Step 6 Select **Generate**.

Step 7 To generate RSA key based third party certificates, select **Generate CSR** on Certificate Management page.

Step 8 In the Generate Certificate Signing Request window, select **CallManager** in Certificate Purpose field.

Step 9 In Parent Domain field, enter the complete FQDN of Cisco Unified CM.

Step 10 Select **Generate**.

Step 11 On Certificate List page, select **Download CSR**. This generates the Cisco Unified CM certificates from third party that is Microsoft CA or Verisign.

Step 12 Save the leaf certificate of Cisco Unified CM and root/chain certificate of certification authority on your system.

Step 13 On Certificate List page, select **Upload Certificate/Certificate Chain**.

Step 14 In the Upload Certificate/Certificate Chain window, select **CallManager** in Certificate Purpose field.

Step 15 Navigate to Upload File, select Browse and upload the Cisco Unified CM leaf certificate generated by third party CSR, which you have saved in Step 12.

Step 16 Select **Upload**.

Note You do not need to upload the CallManager certificate manually on Unity Connection as the certificates are downloaded automatically on port-group reset. However, in case of third party certificates, you must upload the root certificate of the third party Certification Authority on **CallManager-trust** of Unity Connection.

Settings for EC Key Based certificates

Generating EC Key Based Certificates of Unity Connection

Below are the steps to generate EC key based certificates of Unity Connection and uploading them on Cisco Unified CM:

Step 1 On Unity Connection, sign in to Cisco Unified Operating System Administration page.

Step 2 Navigate to Security and select Certificate Management.

Step 3 If you want to generate self signed certificates of Unity Connection, follow the Step 4 to Step 6. Otherwise skip to Step 7.

Step 4 On Certificate Management page, select Generate Self Signed.

Step 5 In the Generate New Self Signed Certificate window, select tomcat-ECDSA in Certificate Purpose field.

Step 6 Select Generate.

Step 7 To generate EC key based third party certificates, select Generate CSR on Certificate Management page.

Step 8 In the Generate Certificate Signing Request window, select tomcat-ECDSA in Certificate Purpose field.

Step 9 In Parent Domain field, enter the complete FQDN of Unity Connection.

Step 10 Select Generate.

Step 11 On Certificate List page, select Download CSR. This generates the Unity Connection ECDSA certificates from third party that is Microsoft CA or Verisign.

Step 12 Save the leaf certificate of Unity Connection and root/chain certificate of certification authority on your system.

Step 13 On Find and List Certificates page, select Upload Certificate/Certificate Chain.

Step 14 In the Upload Certificate/Certificate Chain window, select tomcat-ECDSA in Certificate Purpose field.

Step 15 Navigate to Upload File, select Browse and upload the Unity Connection leaf certificate generated by third party CSR, which you have saved in Step 12.

Step 16 Select Upload.

Step 17 On Cisco Unified CM, sign in to Cisco Unified Operating System Administration page.

Step 18 Navigate to Security and select Certificate Management.

Step 19 On Certificate List page, select Upload Certificate/Certificate Chain.

Step 20 In the Upload Certificate/Certificate Chain window, select CallManager-trust in Certificate Purpose field.

Step 21 Navigate to Upload File, select Browse and upload the Unity Connection self signed certificate generated in Step 6. To upload Unity Connection third party certificates, browse to the root/chain certificate of third party Certification Authority saved in Step 12.

Note In case of Unity Connection cluster, generate and upload self signed certificates of both publisher and subscriber in CallManager-trust of Cisco Unified CM.

Step 22 Select Upload.

Generating EC Key Based Certificates of Cisco Unified CM

Below are the steps to generate EC key based certificates of Cisco Unified CM and uploading them on Unity Connection:

Step 1 On Cisco Unified CM, sign in to Cisco Unified Operating System Administration page.

Step 2 Navigate to Security and select Certificate Management.

Step 3 If you want to generate self signed certificates of Cisco Unified CM, follow Step 4 to Step 6. Otherwise skip to Step 7.

Step 4 On Certificate Management page, select Generate Self Signed.

Step 5 In the Generate New Self Signed Certificate window, select CallManager-ECDSA in Certificate Purpose field.

Step 6 Select Generate.

Step 7 To generate EC key based third party certificates, select Generate CSR on Certificate Management page.

Step 8 In the Generate Certificate Signing Request window, select CallManager-ECDSA in Certificate Purpose field.

Step 9 In Parent Domain field, enter the complete FQDN of Cisco Unified CM.

Step 10 Select Generate.

Step 11 On Certificate List page, select Download CSR. This generates the Cisco Unified CM certificates from third party that is Microsoft CA or Verisign.

Step 12 Save the leaf certificate of Cisco Unified CM and root/chain certificate of certification authority on your system.

Step 13 On Certificate List page, select Upload Certificate/Certificate Chain.

Step 14 In the Upload Certificate/Certificate Chain window, select CallManager-ECDSA in Certificate Purpose field.

Step 15 Navigate to Upload File, select Browse and upload the Cisco Unified CM leaf certificate generated by third party CSR, which you have saved in Step 12.

Step 16 Select **Upload**.

Note You do not need to upload the CallManager certificate manually on Unity Connection as the certificates are downloaded automatically on port-group reset. However, in case of third party certificates, you must upload the root certificate of the third party Certification Authority on **CallManager-trust** of Unity Connection.

Security Mode Settings

Step 1 Sign in Cisco Unity Connection Administration.

Step 2 In Cisco Unity Connection Administration, expand **Telephony Integrations** and select **Port Group**.

Step 3 On the Search Port Groups page, select the applicable port group.

Step 4 Verify that the **Enable Next Generation Encryption** check box is checked.

Step 5 Sign in to Cisco Unified CM Administration.

Step 6 Navigate to **System** > **Security** and select **SIP Trunk Security Profile**.

Step 7 On the Find and List SIP Trunk Security Profiles page, select the SIP trunk security profile that you created in the Creating SIP Trunk Security Profile.

Step 8 On the SIP Trunk Security Profile Configuration page, verify that the value entered in **X.509 Subject Name** is the FQDN of the corresponding Unity Connection server.

Step 9 Configure TLS Ciphers as mentioned in sectionTLS Ciphers Configuration.

TLS Ciphers Configuration

Below are the steps to configure TLS Cipher option in Unity Connection and Cisco Unified CM:

Step 1 Sign in to Cisco Unified CM Administration page, navigate to **Systems** > **Enterprise Parameters**.

Step 2 Select the appropriate cipher option from the **TLS Ciphers**drop-down list under **Security Parameters**.

Step 3 From the Navigation pane on right corner of the screen, select **Cisco Unified Serviceability** and select **Go**.

Step 4 On Cisco Unified Serviceability page, navigate to **Tools** > **Control Centre-Feature Services** and select **Cisco Call Manager** under CM Services.

Step 5 Select **Restart**.

Note In case of Cisco Unified CM cluster, the Cisco Call Manager service needs to be restarted on both publisher and subscriber server.

Step 6 Sign in to Cisco Unity Connection Administration page, expand **System Settings** and select **General Configurations**.

Step 7 Select the appropriate cipher from the **TLS Ciphers** drop-down list.

Step 8 From the Navigation pane on right corner of the screen, select **Cisco Unity Connection Serviceability** and select **Go**.

Step 9 Go to **Tools** > **Service Management** and stop **Connection Conversation Manager**. Once the Connection Conversation Manager service is stopped, start it again.

Note In case of Unity Connection cluster, **Connection Conversation Manager** needs to be restarted on both publisher and subscriber.

Step 10 Generate and upload RSA and EC key based certificates as mentioned in section Generate and Upload Certificates.

Below table lists the TLS Cipher options in priority order of the RSA or ECDSA ciphers.

Table 21: TLS Cipher options with Priority order

TLS Cipher Options	TLS Ciphers in Priority Order
Strongest- AES-256 SHA-384 Only: RSA Preferred	• TLS_ECDHE_RSA_WITH_AES_ • TLS_ECDHE_ECDSA_WITH_A
Strongest-AES-256 SHA-384 Only: ECDSA Preferred	• TLS_ECDHE_ECDSA_WITH_A • TLS_ECDHE_RSA_WITH_AES_
Medium-AES-256 AES-128 Only: RSA Preferred	• TLS_ECDHE_RSA_WITH_AES_ • TLS_ECDHE_ECDSA_WITH_A • TLS_ECDHE_RSA_WITH_AES_ • TLS_ECDHE_ECDSA_WITH_A
Medium-AES-256 AES-128 Only: ECDSA Preferred	• TLS_ECDHE_ECDSA_WITH_A • TLS_ECDHE_RSA_WITH_AES_ • TLS_ECDHE_ECDSA_WITH_A • TLS_ECDHE_RSA_WITH_AES_

TLS Cipher Options	TLS Ciphers in Priority Order
All Ciphers RSA Preferred (Default)	• TLS_ECDHE_RSA_WITH_AES_256 • TLS_ECDHE_ECDSA_WITH_AES_ • TLS_ECDHE_RSA_WITH_AES_128 • TLS_ECDHE_ECDSA_WITH_AES_ • TLS_RSA_WITH_AES_128_CBC_S
All Ciphers ECDSA Preferred	• TLS_ECDHE_ECDSA_WITH_AES_ • TLS_ECDHE_RSA_WITH_AES_256 • TLS_ECDHE_ECDSA_WITH_AES_ • TLS_ECDHE_RSA_WITH_AES_128 • TLS_RSA_WITH_AES_128_CBC_S

The negotiation between Unity Connection and Cisco Unified Communications Manager depends on the TLS cipher configuration with the following conditions:

- When Unity Connection acts as server, TLS cipher negotiation is based on the preference selected by Cisco Unified CM.
  - In case ECDSA based cipher is negotiated then EC key based tomcat-ECDSA certificates are used in SSL handshake.
  - In case RSA based cipher is negotiated then RSA key based tomcat certificates are used in SSL handshake.
- When Unity Connection acts as client, TLS cipher negotiation is based on the preference selected by Unity Connection.

SRTP Ciphers Configuration

If you want to enable Next Generation Security over RTP interface, configure SRTP Ciphers as mentioned below:

Step 1 Sign in to Cisco Unified CM Administration page, navigate to **Systems** > **Enterprise Parameters**.

Step 2 Select the appropriate cipher option from the **SRTP Ciphers**drop-down list under **Security Parameters**.

Step 3 From the Navigation pane on right corner of the screen, select **Cisco Unified Serviceability** and select **Go**.

Step 4 On Cisco Unified Serviceability page, navigate to **Tools** > **Control Centre-Feature Services** and select **Cisco Call Manager** under CM Services.

Step 5 Select **Restart**.

Note In case of Cisco Unified CM cluster, the Cisco Call Manager service needs to be restarted on both publisher and subscriber server.

Step 6 Sign in to Cisco Unity Connection Administration page, expand **System Settings** and select **General Configurations**.

Step 7 Select the appropriate cipher from the **SRTP Ciphers** drop-down list.

Step 8 From the Navigation pane on right corner of the screen, select **Cisco Unity Connection Serviceability** and select **Go**.

Step 9 Go to **Tools** > **Service Management** and stop **Connection Conversation Manager**. Once the Connection Conversation Manager service is stopped, start it again.

Note In case of Unity Connection cluster, **Connection Conversation Manager** needs to be restarted on both publisher and subscriber.

Below table lists the SRTP Cipher options in priority order of the RSA or ECDSA ciphers.

Table 22: SRTP Cipher Options in Priority order

SRTP Cipher Option	SRTP in Priority Order
All supported AES-256, AES-128 ciphers	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1_32 • AES_CM_128_HMAC_SHA1_80
AEAD AES-256, AES-28 GCM-based ciphers	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
AEAD AES256 GCM-based ciphers only	AEAD_AES_256_GCM