Ejemplo de configuración para la integración segura de SIP entre CUCM y CUC basada en el cifrado de última generación (NGE)

Contenido

Introducción

Este documento describe la configuración y verificación de la conexión SIP segura entre Cisco Unified Communication Manager (CUCM) y el servidor Cisco Unity Connection (CUC) mediante el cifrado Next Generation.

La interfaz de seguridad de última generación sobre SIP restringe la interfaz SIP para utilizar los cifrados Suite B basados en los protocolos TLS 1.2, SHA-2 y AES256. Permite las diversas combinaciones de cifrados en función del orden de prioridad de los cifrados RSA o ECDSA. Durante la comunicación entre Unity Connection y Cisco Unified CM, se verifican los certificados de cifrado y de terceros en ambos extremos. A continuación se muestra la configuración para el soporte de cifrado Next Generation.

Si planea utilizar los certificados firmados por la Autoridad de certificación de terceros, comience con la firma de certificados al final de la sección de configuración (Configurar - Firmar los certificados basados en la clave EC por parte de la CA de terceros)

Prerequisites

Requirements

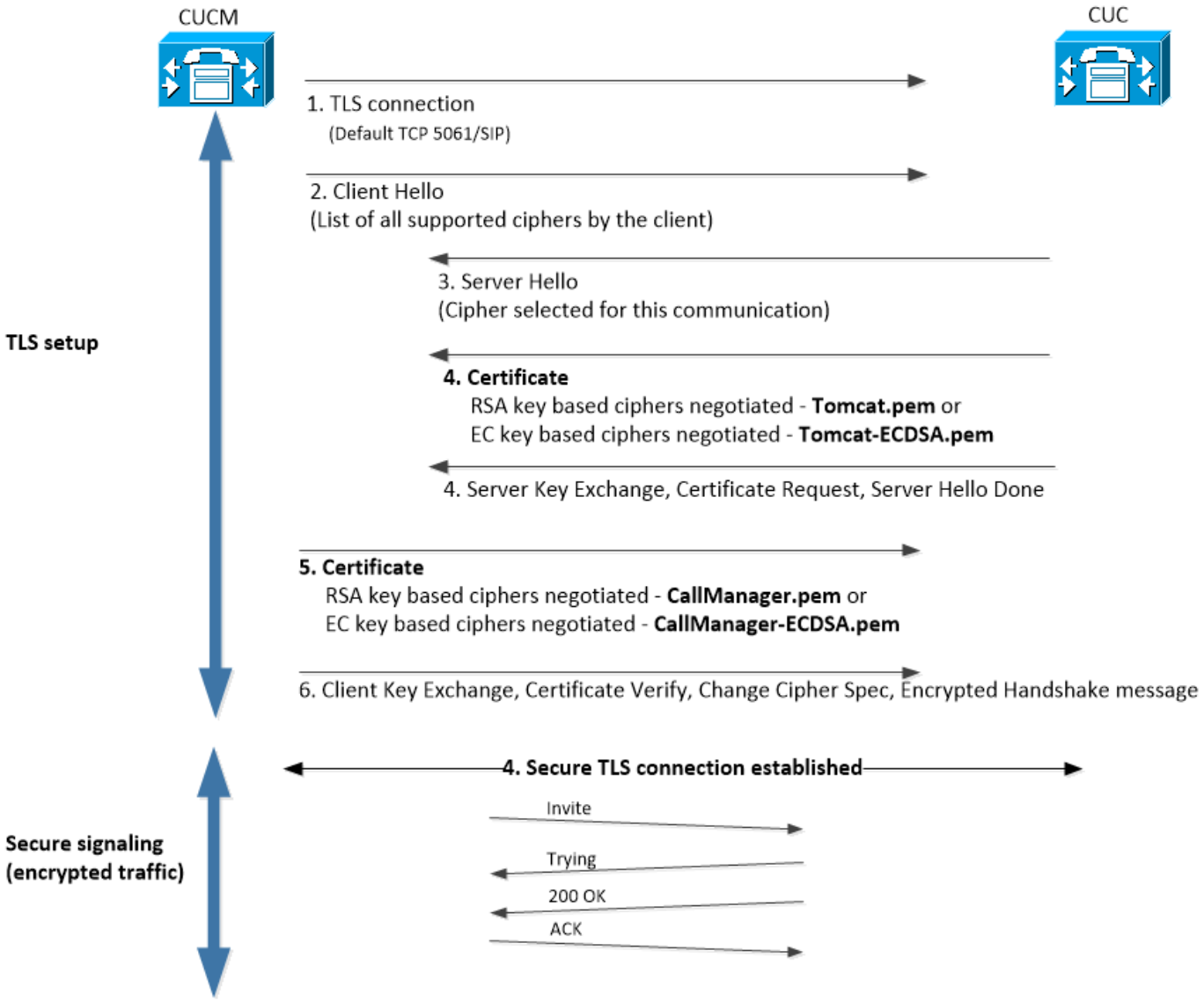
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

CUCM versión 11.0 y posteriores en modo mixto
CUC versión 11.0 y posteriores

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de la red

Este diagrama explica brevemente el proceso que ayuda a establecer una conexión segura entre CUCM y CUC una vez que se habilita el soporte de cifrado de última generación:



Requisitos del certificado

Estos son los requisitos de intercambio de certificados una vez que el soporte de cifrado de última generación esté habilitado en Cisco Unity Connection.

- **Cifrados basados en claves RSA negociados**

certificado CUCM utilizado	certificado CUC utilizado	Certificados para cargar en CUCM	Certificados para cargar en
CallManager.pem (autofirmado)	Tomcat.pem (autofirmado)	Tomcat.pem que se cargará en CUCM > CallManager-trust	Ninguno.
CallManager.pem (CA firmada)	Tomcat.pem (CA firmada)	Certificado de CA intermedia y raíz de CUC[*1] que se cargará en CUCM > CallManager-trust	Certificado de CA intermed raíz de CUCM[*2] que se car en CUC > CallManager-trus
CallManager.pem (CA firmada)	Tomcat.pem (autofirmado)	Tomcat.pem que se cargará en CUCM > CallManager-trust	El certificado de CA interme raíz de CUCM se cargará e CUC > CallManager-trust.
CallManager.pem (autofirmado)	Tomcat.pem (CA firmada)	Certificado de CA intermedia y raíz de CUC que se cargará en CUCM > CallManager-trust	Ninguno.

*1 El certificado de CA intermedia y raíz de CUC se refiere al certificado de CA que firmó el certificado Tomcat de conexión de Unity (Tomcat.pem).

*2 El certificado de CA intermedia y raíz de CUCM se refiere al certificado de CA que firmó el certificado de CUCM CallManager (Callmanager.pem).

- **Cifrados basados en claves EC negociados**

certificado CUCM utilizado	certificado CUC utilizado	Certificados para cargar en CUCM	Certificados para cargar en CUC
CallManager-ECDSA.pem (autofirmado)	Tomcat-ECDSA.pem (firmado automáticamente)	Tomcat-ECDSA.pem para ser cargado en CUCM > CallManager-trust	Ninguno.
CallManager-ECDSA.pem (CA firmada)	Tomcat-ECDSA.pem (CA firmada)	Certificado de CA intermedia y raíz de CUC*1 que se cargará en CUCM > CallManager-trust	Certificado de CA intermedia y raíz de CUCM*2 que se cargará en CUC > CallManager-trust.
CallManager-ECDSA.pem (CA firmada)	Tomcat-ECDSA.pem (firmado automáticamente)	Tomcat-ECDSA.pem para ser cargado en CUCM > CallManager-trust.	El certificado de CA intermedia y raíz de CUCM se cargará en CUC > CallManager-trust.
CallManager-ECDSA.pem (autofirmado)	Tomcat-ECDSA.pem (CA firmada)	Certificado de CA intermedia y raíz de CUC que se cargará en CUCM > CallManager-trust	Ninguno.

*1 El certificado de CA intermedia y raíz de CUC se refiere al certificado de CA que firmó el certificado Tomcat basado en la conexión de Unity EC (Tomcat-ECDSA.pem).

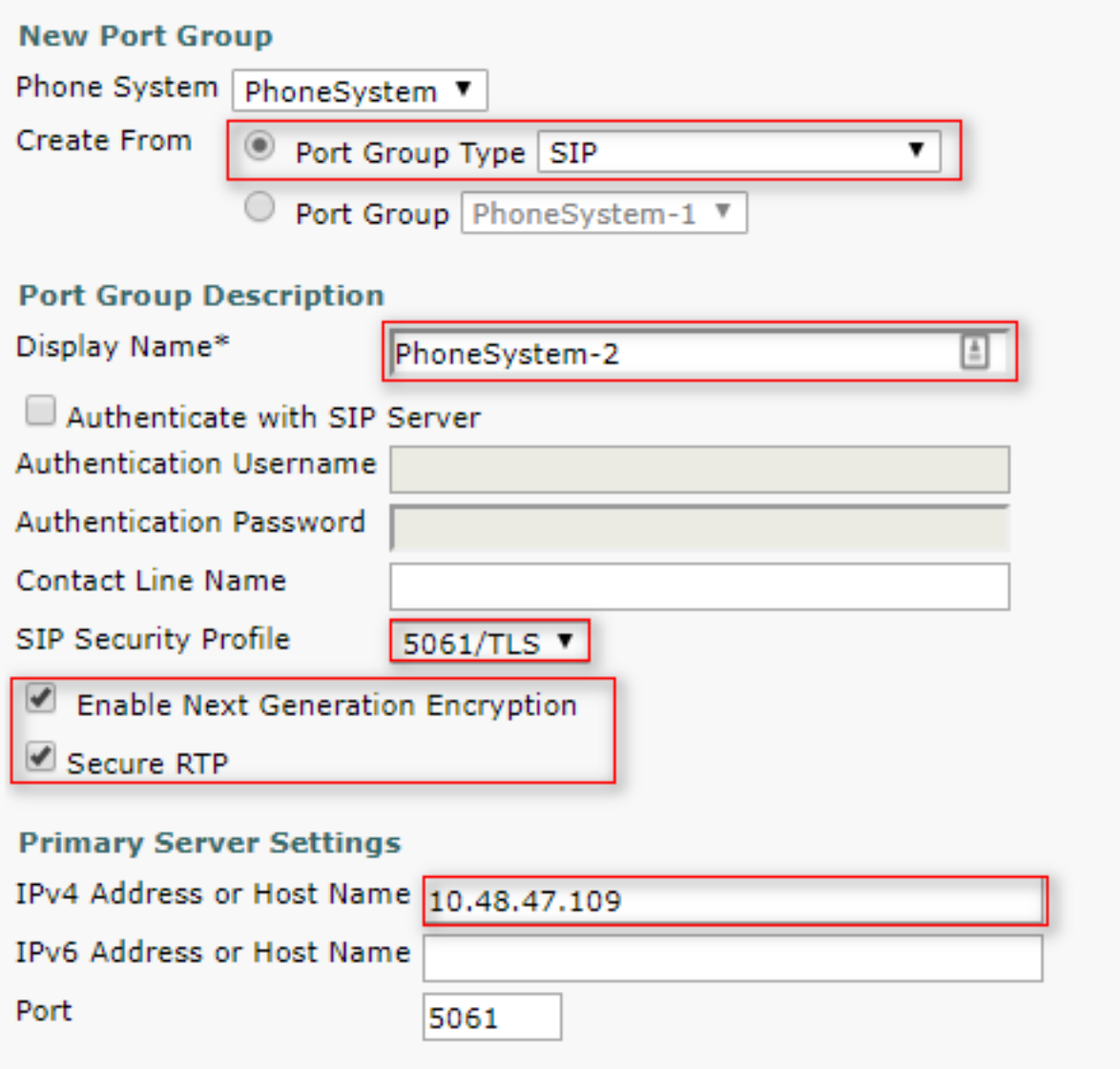
*2 El certificado de CA intermedia y raíz de CUCM se refiere al certificado de CA que firmó el certificado de CUCM CallManager (CallManager-ECDSA.pem).

1. **Nota:** El certificado Tomcat-ECDSA.pem se denomina CallManager-ECDSA.pem en las versiones 11.0.1 de CUC. Desde CUC 11.5.x el certificado se ha cambiado a Tomcat-ECDSA.pem.

Configuración: Cisco Unity Connection (CUC)

1. Agregar un nuevo grupo de puertos

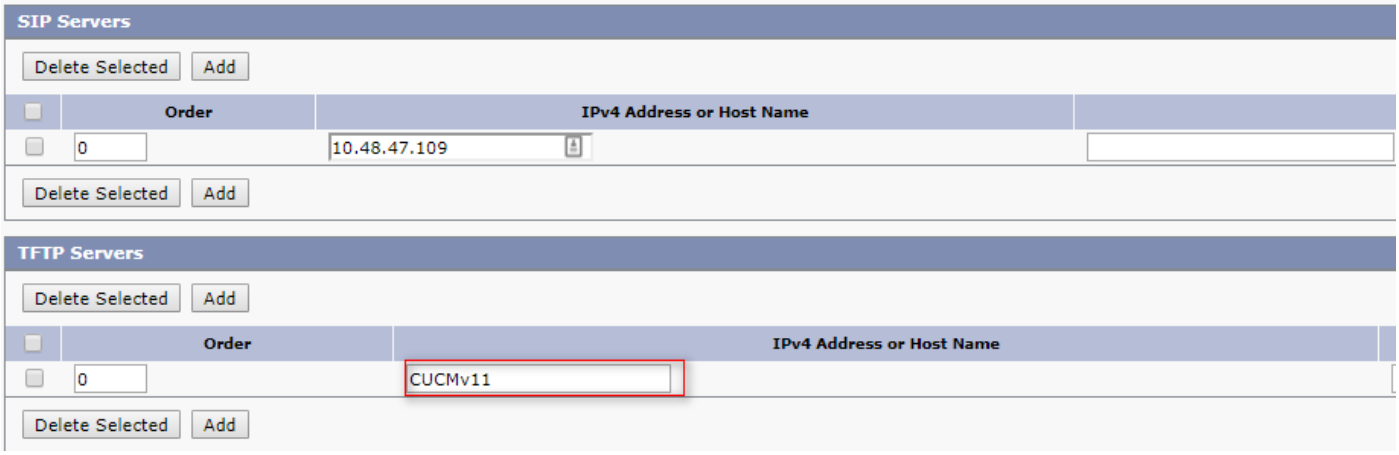
Vaya a la página Cisco Unity Connection Administration > Telephony Integration > Port Group y haga clic en Add New . Asegúrese de marcar la casilla de verificación Enable Next Generation Encryption (Activar cifrado de última generación).



1. **Nota**: El certificado Tomcat de Cisco de Unity Connection se utilizará durante el intercambio de señales SSL una vez que se active la casilla de verificación Habilitar cifrado de última generación.
   · En caso de que se negocie el cifrado basado en ECDSA, el certificado basado en la clave EC tomcat-ECDSA se utiliza en el intercambio de señales SSL.
   · En caso de que se negocie el cifrado basado en RSA, el certificado tomcat basado en la clave RSA se utiliza en el intercambio de señales SSL.

2. Agregar la referencia del servidor TFTP

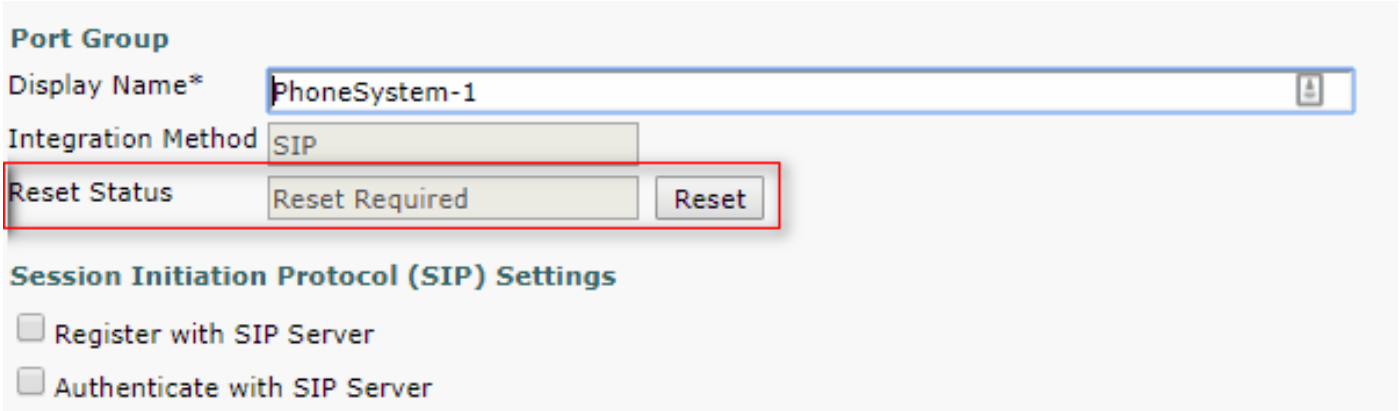
En la página Conceptos básicos del grupo de puertos, navegue hasta Editar > Servidores y agregue FQDN del servidor TFTP de su clúster de CUCM. El FQDN/nombre de host del servidor TFTP debe coincidir con el nombre común (CN) del certificado de CallManager. La dirección IP del servidor no funcionará y dará lugar a un error en la descarga del archivo ITL. Por lo tanto, el nombre DNS debe resolverse a través del servidor DNS configurado.



Reinicie Connection Conversation Manager en cada nodo. Para ello, vaya a Serviciabilidad de Cisco Unity Connection > Herramientas > Administración de servicios. Esto es obligatorio para que la configuración tenga efecto.

1. **Nota:** La conexión de Unity descarga el archivo ITL (ITLfile.tlv) del TFTP de CUCM utilizando el protocolo https en el puerto seguro 6972 (URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv). CUCM debe estar en modo mixto ya que CUC busca el certificado de función "CCM+TFTP" del archivo ITL.

Vuelva a la página Telephony Integration > Port Group > Port Group Basics configuration y restablezca el grupo de puertos recién agregado.



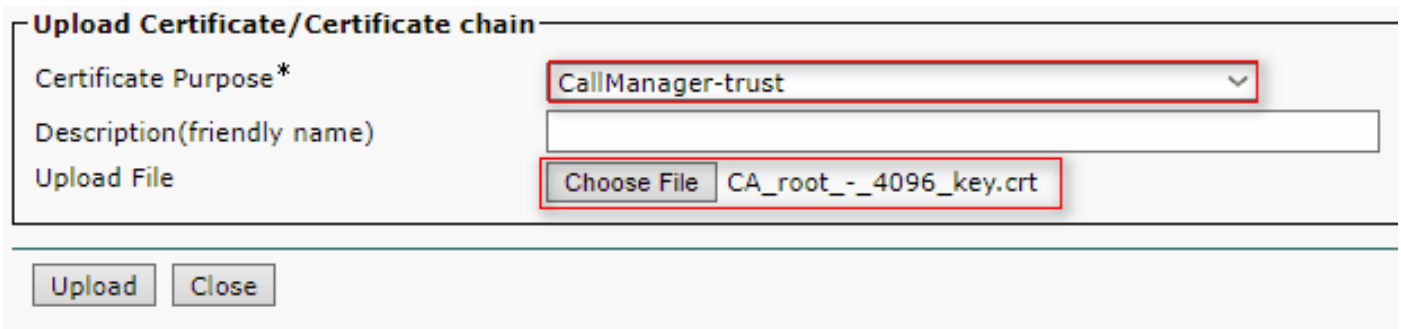
1. **Nota:** Cada vez que se reinicia el grupo de puertos, el servidor CUC actualizará su archivo ITL almacenado localmente conectándose al servidor CUCM.

3. Agregar puertos de buzón de voz

Vuelva a Telephony Integration > Port y haga clic en Add new para agregar puerto al grupo de puertos recién creado.

4. Cargar certificado raíz e intermedio de CUCM de la CA de terceros

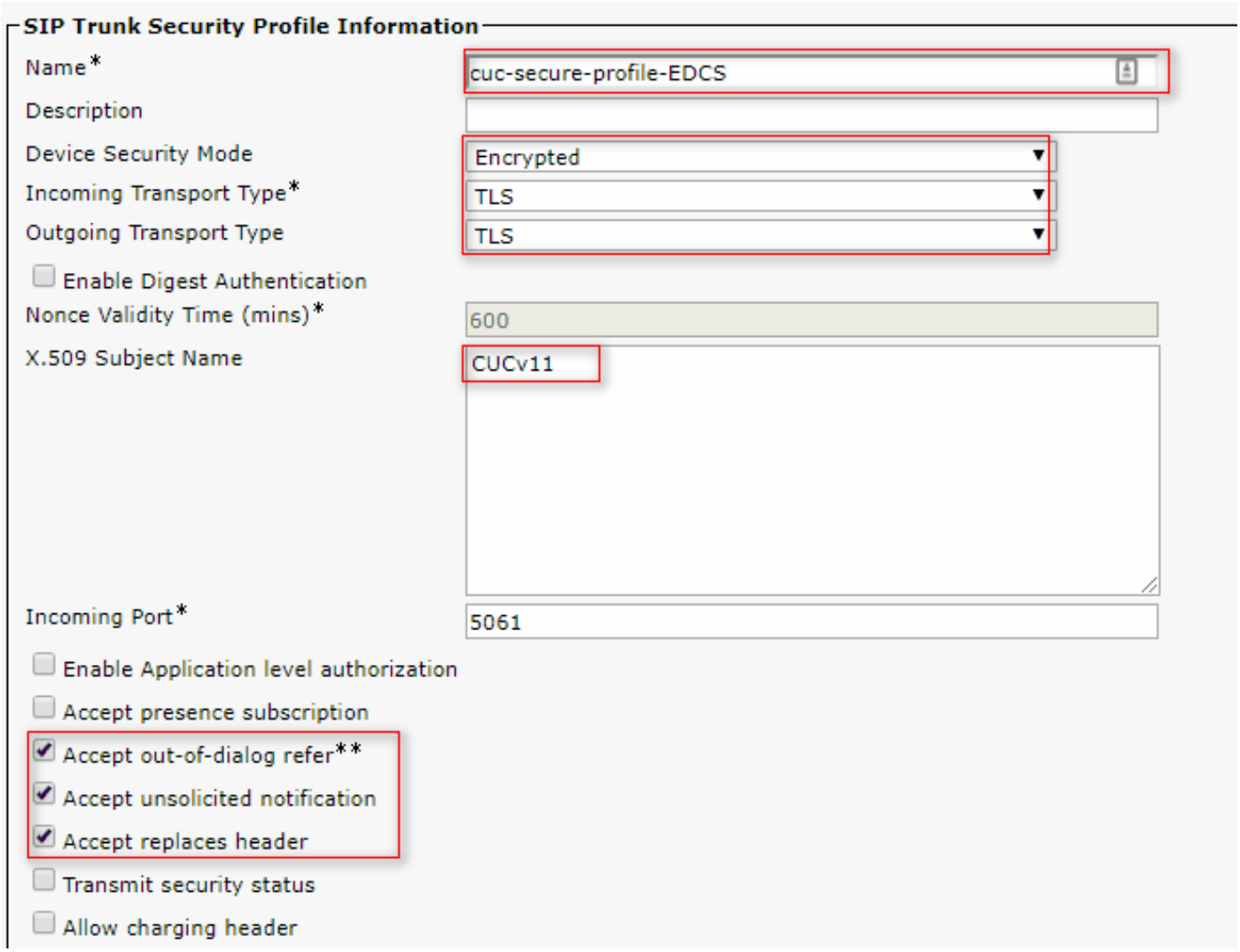
En caso de certificados de terceros, debe cargar el certificado raíz e intermedio de la Autoridad de certificación de terceros en CallManager-trust de Unity Connection. Esto sólo es necesario si la CA de terceros firmó el certificado del Call Manager. Realice esta acción navegando hasta Administración de Cisco Unified OS > Seguridad > Administración de certificados y haga clic en Cargar certificado.



Configurar: Cisco Unified CM (CUCM)

1. Crear un perfil de seguridad de tronco SIP

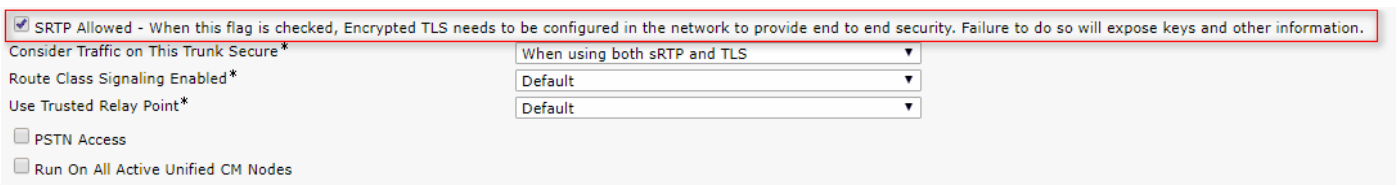
Vaya a CUCM Administration > System > Security > SIP Trunk Security Profile y agregue un nuevo perfil. El nombre del asunto X.509 debe coincidir con el FQDN del servidor CUC.

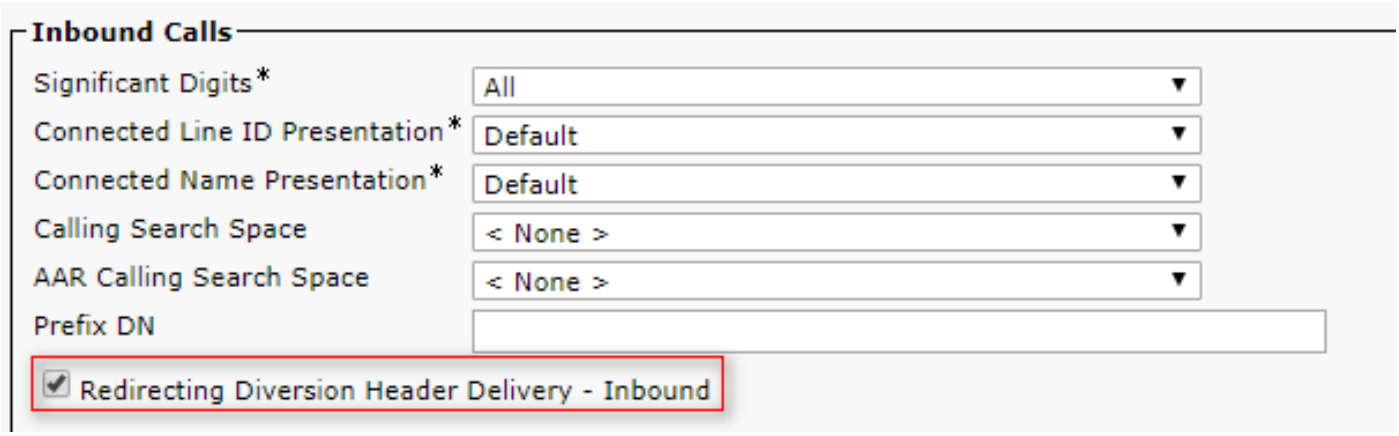


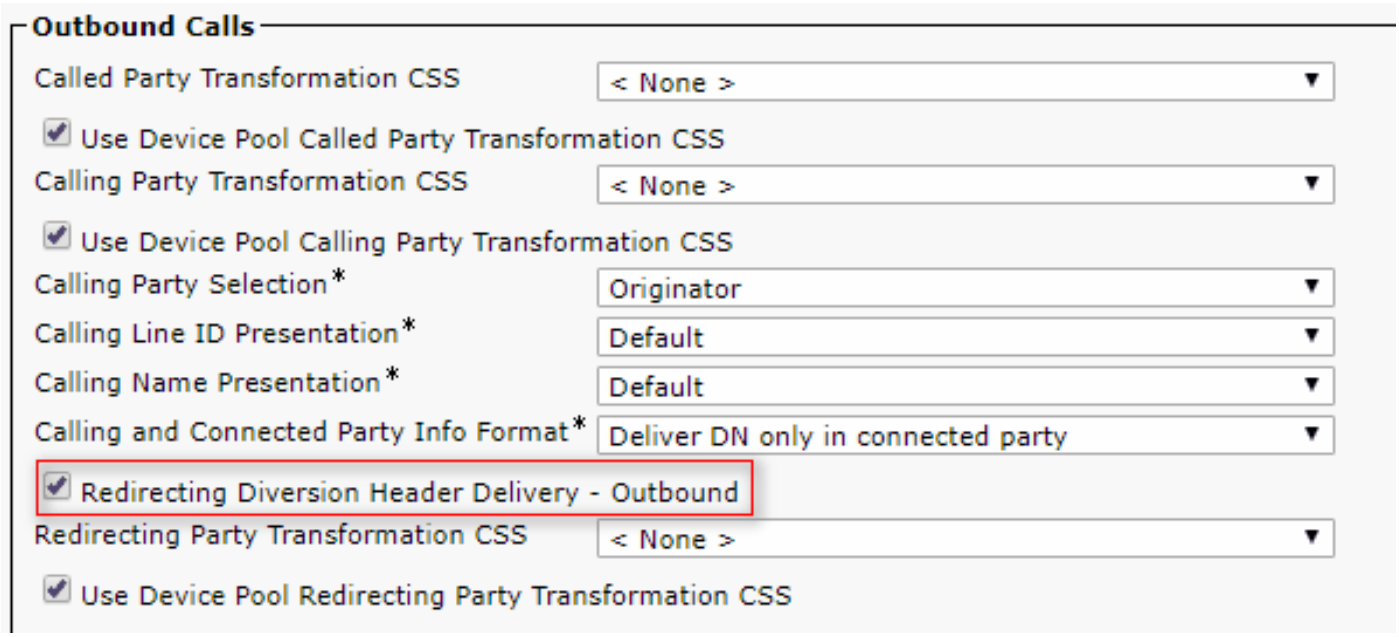
1. **Nota**: El comando CLI "show cert own tomcat/tomcat.pem" puede mostrar el certificado tomcat basado en la clave RSA en Unity Connection. Su CN debe coincidir con el nombre de asunto X.509 configurado en CUCM. El CN es igual a FQDN/nombre de host del servidor Unity. El certificado basado en la clave EC contiene el FQDN/nombre de host en el campo Nombre alternativo del sujeto (SAN).

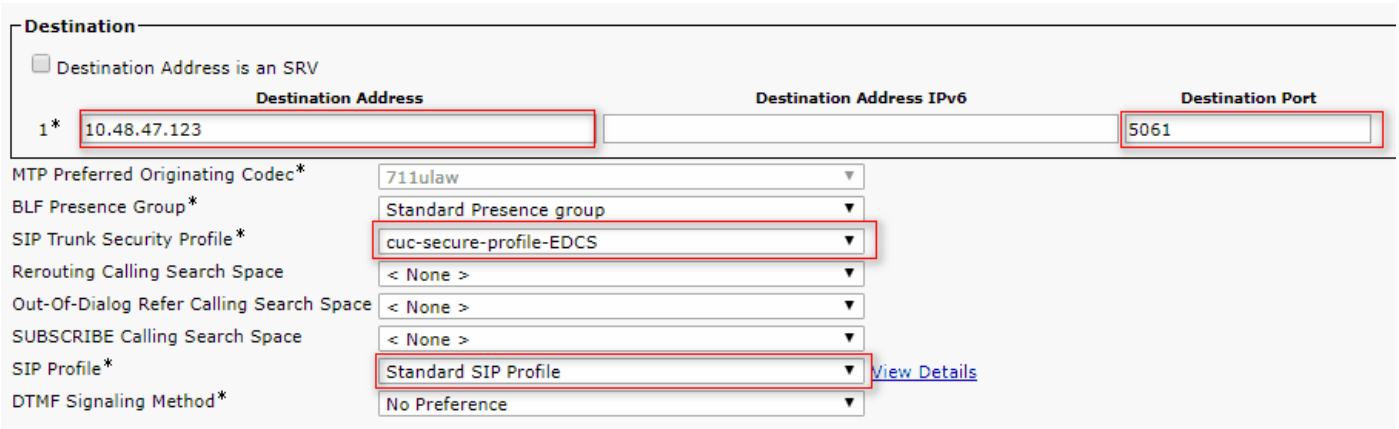
2. Cree un enlace troncal SIP seguro

Vaya a Dispositivo > Troncal > Haga clic y agregue nuevo y cree un troncal SIP estándar que se utilizará para la integración segura con Unity Connection.







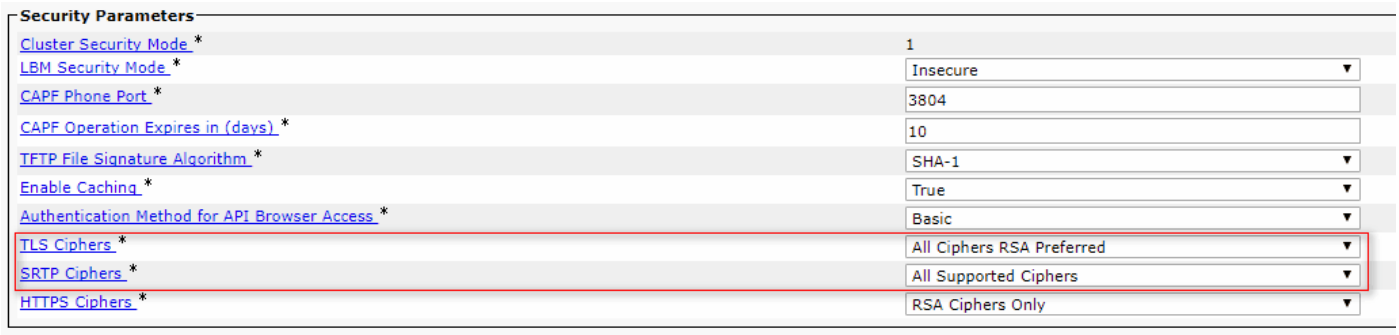


3. Configuración de los cifrados TLS y SRTP

1. **Nota:** La negociación entre Unity Connection y Cisco Unified Communications Manager depende de la configuración del cifrado TLS con las siguientes condiciones: Cuando Unity Connection actúa como servidor, la negociación del cifrado TLS se basa en la preferencia seleccionada por Cisco Unified CM.En caso de que se negocie el cifrado basado en ECDSA, los certificados basados en la clave EC tomcat-ECDSA se utilizan en el intercambio de señales SSL.En caso de que se negocie el cifrado basado en RSA, los certificados tomcat basados en la clave RSA se utilizan en el intercambio de señales SSL.Cuando Unity Connection actúa como cliente, la negociación del cifrado TLS se basa en la preferencia

seleccionada por Unity Connection.

Vaya a Cisco Unified CM > Systems > Enterprise Parameters y seleccione la opción de cifrado correspondiente en la lista desplegable TLS y SRTP Ciphers.



Reinicie el servicio Cisco Call Manager en cada nodo navegando a la página Cisco Unified Serviceability, Tools > Control Center-Feature Services y seleccione Cisco Call Manager en CM Services

Vaya a la página de administración de Cisco Unity Connection > Configuración del sistema > Configuraciones generales y seleccione la opción de cifrado adecuada en la lista desplegable Cifradores TLS y SRTP.

Reinicie Connection Conversation Manager en cada nodo. Para ello, vaya a Serviciabilidad de Cisco Unity Connection > Herramientas > Administración de servicios.

Opciones del cifrado TLS con orden de prioridad

Opciones del cifrado TLS	Cifrados TLS en orden de prioridad
Strongest- AES-256 SHA-384 únicamente: Preferido por RSA	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Strongest-AES-256 SHA-384 únicamente: Preferido por ECDSA	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH

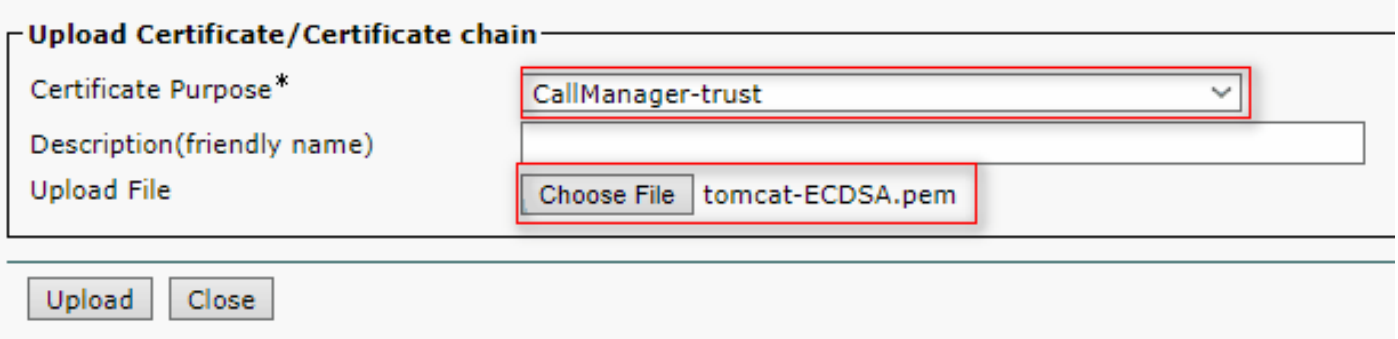
AES-256 AES-128 Solo: Preferido por RSA	4 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM _SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384
AES-256 AES-128 Solo: Preferido por ECDSA	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6
Todos los cifradores RSA preferidos (predeterminado)	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_RSA_WITH_AES_128_CBC_SHA
Todos los filtros preferidos por ECDSA	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_RSA_WITH_AES_128_CBC_SHA

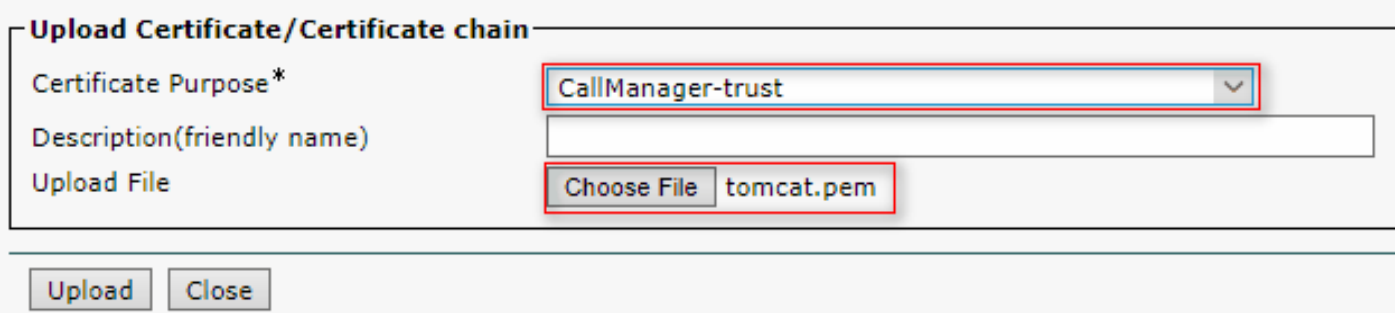
Opciones de cifrado SRTP en orden de prioridad

Opción de cifrado SRTP	SRTP en orden de prioridad
Todos los cifrado AES-256 y AES-128 admitidos	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1 _32
cifrado AEAD AES-256, AES-28 basado en GCM	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
Solo cifrado basado en GCM AEAD AES256	• AEAD_AES_256_GCM

4. Cargar certificados de Tomcat CUC (basados en RSA y EC)

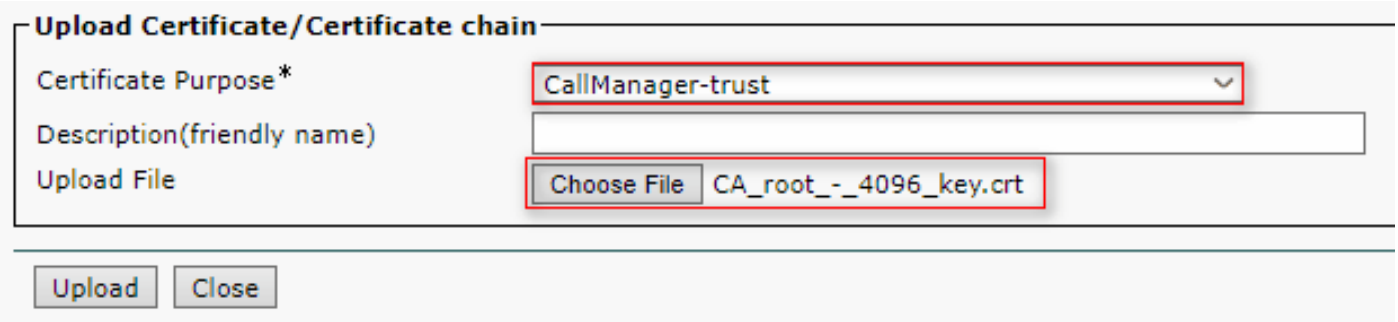
Vaya a OS Administration > Security > Certificate Management y cargue ambos certificados CUC Tomcat (basados en RSA y EC) en el almacén de confianza de CallManager.





1. **Nota**: La carga de ambos certificados de Unity Tomcat no es obligatoria si sólo se negocian los cifrados ECDSA. En tal caso, el certificado Tomcat basado en EC es suficiente.

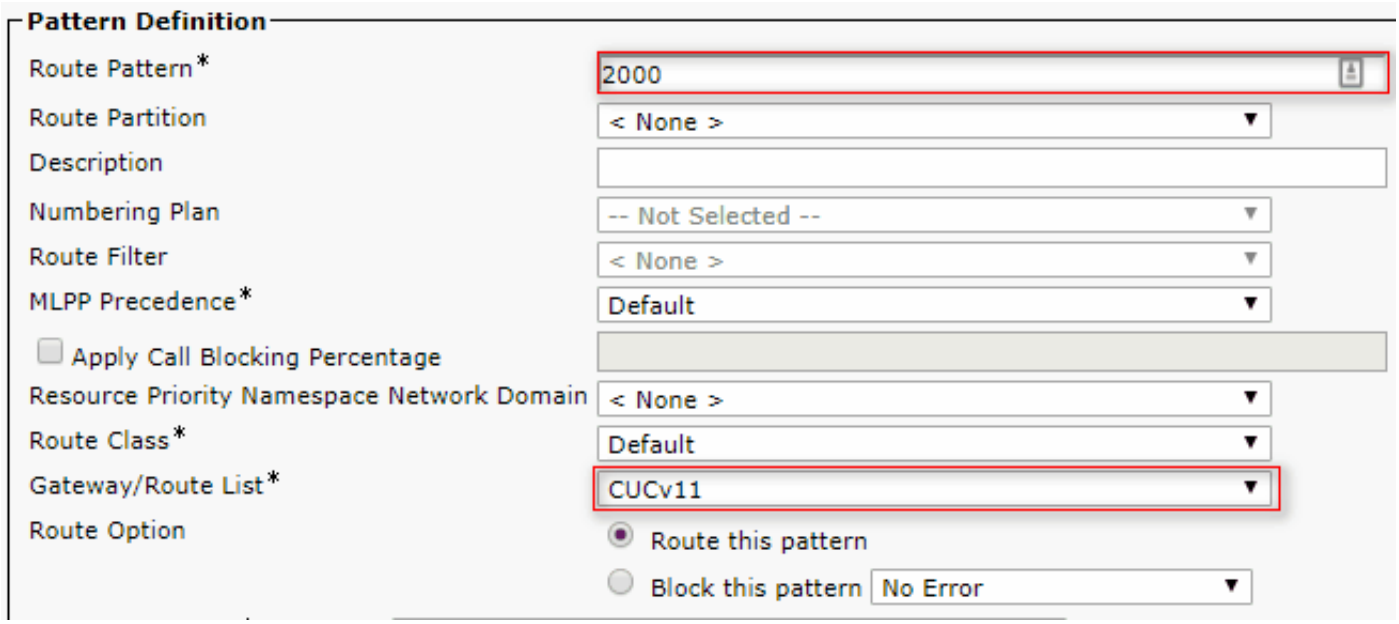
En caso de certificados de terceros, debe cargar el certificado raíz e intermedio de la Autoridad de certificación de terceros. Esto sólo es necesario si la CA de terceros firmó su certificado de Unity Tomcat.



Reinicie el proceso Cisco Call Manager en todos los nodos para aplicar los cambios.

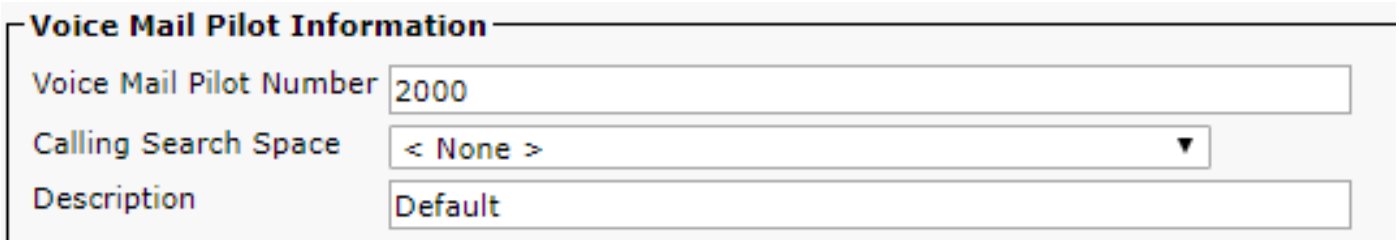
5. Crear patrón de ruta

Configure un patrón de ruta que apunte al tronco configurado navegando a Call Routing > Route/Hunt > Route Pattern . La extensión ingresada como número de patrón de ruta se puede utilizar como piloto de correo de voz.

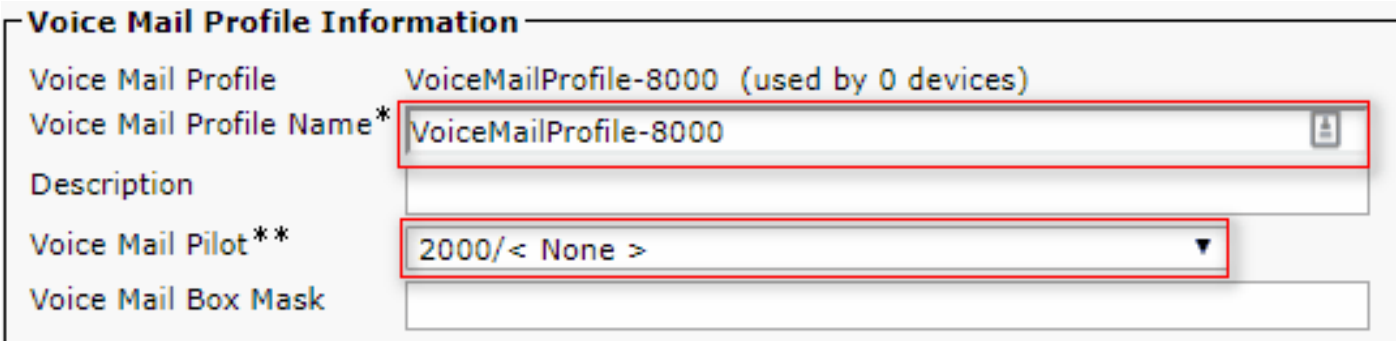


6. Cree el Piloto de buzón de voz, el Perfil de buzón de voz y asígnelo a los DN

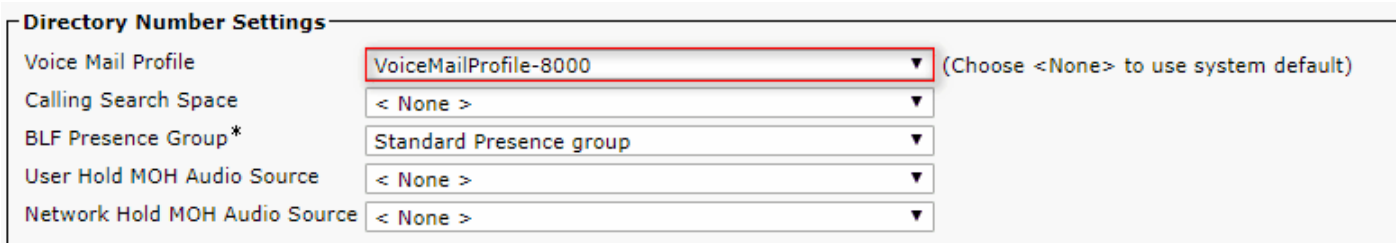
Cree un programa piloto de correo de voz para la integración en Advanced Features > Voice Mail > Voice Mail Pilot.



Cree un perfil de correo de voz para vincular todos los ajustes con Advanced Features > Voice Mail > Voice Mail Profile



Asigne el perfil de correo de voz recién creado a los DNs que pretenden utilizar la integración segura dirigiéndose a Call Routing > Directory number



Configurar: firma de certificados basados en claves EC por parte de CA de terceros (opcional)

Los certificados pueden estar firmados por una CA de terceros antes de configurar la integración segura entre los sistemas. Siga los pasos siguientes para firmar los certificados en ambos sistemas.

Cisco Unity Connection

1. Generar solicitud de firma de certificado (CSR) para CUC Tomcat-ECDSA y tener el certificado firmado por CA de terceros
2. CA proporciona el certificado de identidad (certificado firmado por la CA) y el certificado de la CA (certificado raíz de la CA) que se deben cargar como se indica a continuación:
   Cargar el certificado raíz de la CA en el almacén de tomcat-trust
   Cargar certificado de identidad en el almacén de tomcat-EDCS
3. Reiniciar el administrador de conversaciones en CUC

Cisco Unified CM

1. Generar CSR para CUCM CallManager-ECDSA y tener el certificado firmado por CA de terceros
2. CA proporciona el certificado de identidad (certificado firmado por la CA) y el certificado de la CA (certificado raíz de la CA) que se deben cargar como se indica a continuación:
   Cargar el certificado raíz de la CA en el almacén de confianza del CallManager
   Cargar certificado de identidad en el almacén callmanager-EDCS
3. Reiniciar los servicios Cisco CCM y TFTP en cada nodo

El mismo proceso se utilizará para firmar certificados basados en claves RSA donde se genera CSR para el certificado de Tomcat de CUC y el certificado de CallManager y se carga en el almacén de tomcat y el almacén de callmanager respectivamente.

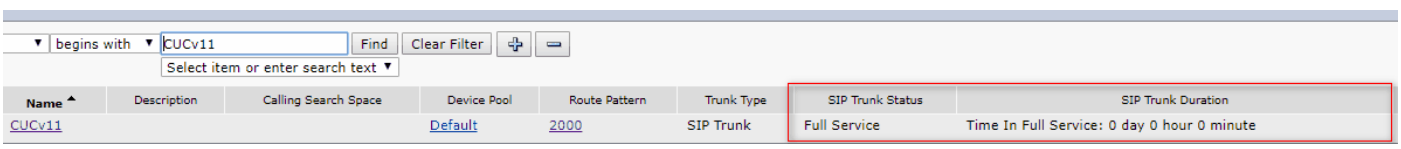
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Verificación segura del troncal SIP

Pulse el botón Buzón de voz del teléfono para llamar al buzón de voz. Debería escuchar el saludo de apertura si la extensión del usuario no está configurada en el sistema Unity Connection.

De manera alternativa, puede habilitar el keepalive de las opciones SIP para supervisar el estado del troncal SIP. Esta opción se puede habilitar en el perfil SIP asignado al troncal SIP. Una vez habilitado, puede supervisar el estado del tronco Sip a través de Device > Trunk como se muestra a continuación:



Verificación segura de llamada RTP

Verifique si el icono de candado está presente en las llamadas a Unity Connection. Significa que la secuencia RTP está cifrada (el perfil de seguridad del dispositivo debe ser seguro para que funcione), como se muestra en esta imagen

Información Relacionada

- Guía de integración SIP para Cisco Unity Connection versión 11.x