Ejemplo de configuración para la integración segura del SORBO entre CUCM y CUC basados en el cifrado de la última generación (NGE)

Contenido

Introducción

Este documento describe la configuración y la verificación de la conexión segura del SORBO entre el servidor unificado Cisco del administrador (CUCM) y del Cisco Unity Connection de la comunicación (CUC) usando el cifrado de la última generación.

La Seguridad de la última generación sobre la interfaz del SORBO restringe la interfaz del SORBO para utilizar las cifras de la habitación B basadas en los protocolos 1.2, SHA-2 y AES256 de TLS. Permite las diversas combinaciones de cifras basadas en la orden de la prioridad de las cifras RSA o ECDSA. Durante la comunicación entre el Unity Connection y Cisco unificó el CM, las cifras y los Certificados del otro vendedor se verifican en ambos los extremos. Abajo está la configuración para el soporte de encripción de la última generación.

Si usted planea utilizar los Certificados firmados por las autoridades de certificación del otro

vendedor después comienzan con el certificado que firma en el extremo de la sección de configuración (configuración - firmando los Certificados basados clave EC del otro vendedor CA)

Prerequisites

Requisitos

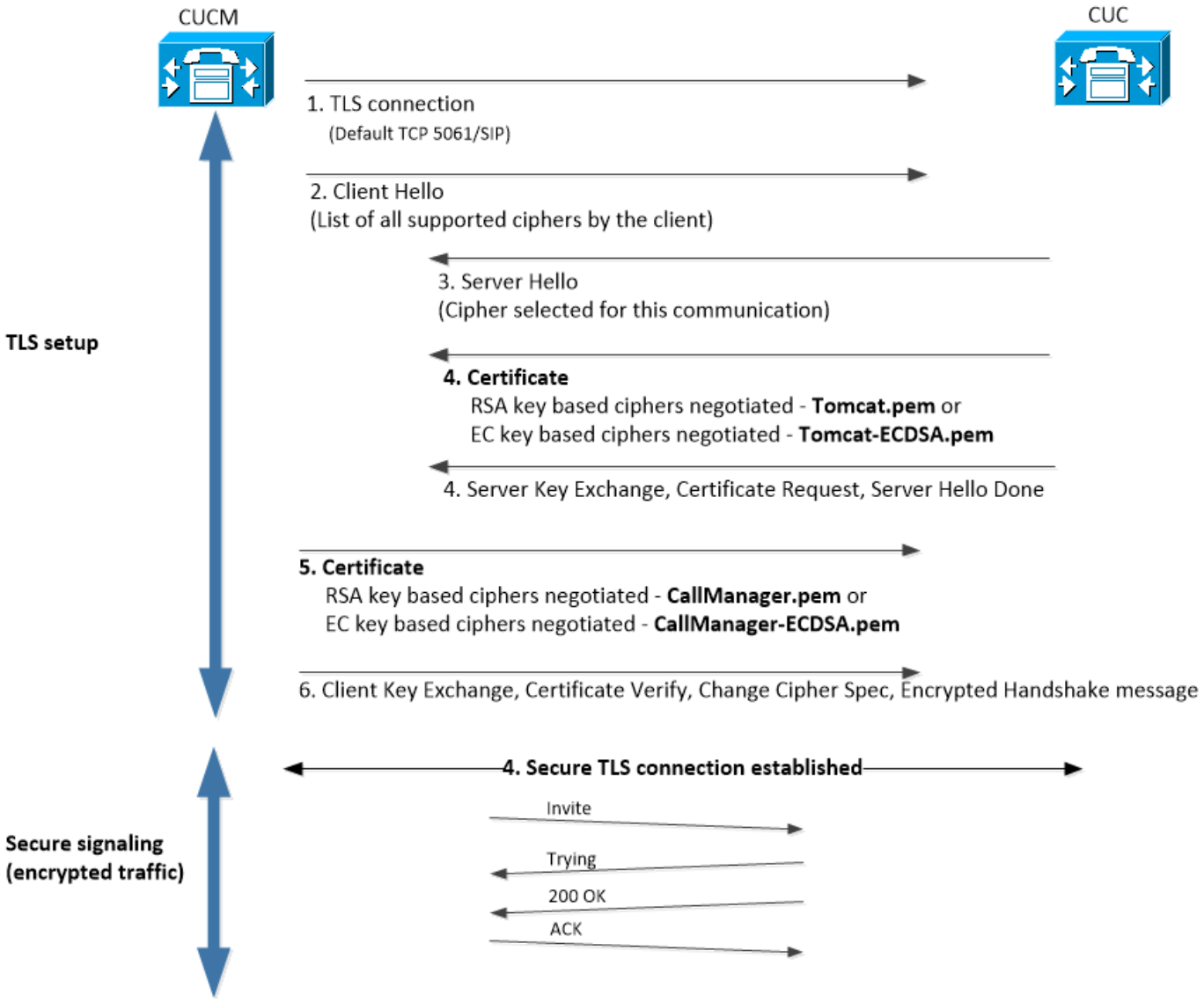
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Versión 11.x y posterior CUCM en el modo mezclado
Versión 11.x y posterior CUC

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Diagrama de la red

Este diagrama explica abreviadamente el proceso que las ayudas establecen una conexión segura entre CUCM y CUC una vez la última generación que se habilita el soporte de encripción:



Requisitos del certificado

Éstos son los requisitos del intercambio del certificado una vez que el soporte de encripción de la última generación se habilita en el Cisco Unity Connection.

Certificados autofirmados usados:

- Unity Connection
  Ninguna necesidad de cargar cualquier certificado. El servidor del Unity Connection descargará automáticamente el ITLfile del servidor TFTP especificado durante la configuración y la confianza CallManager.pem y CallManager-EC.pem durante la negociación de TLS.

- Cisco unificó el CM
  Usted debe cargar el Tomcat.pem y el Tomcat-EC.pem del Unity Connection en el almacén de la CallManager-confianza en CUCM

Los Certificados de CA de tercera persona usados:

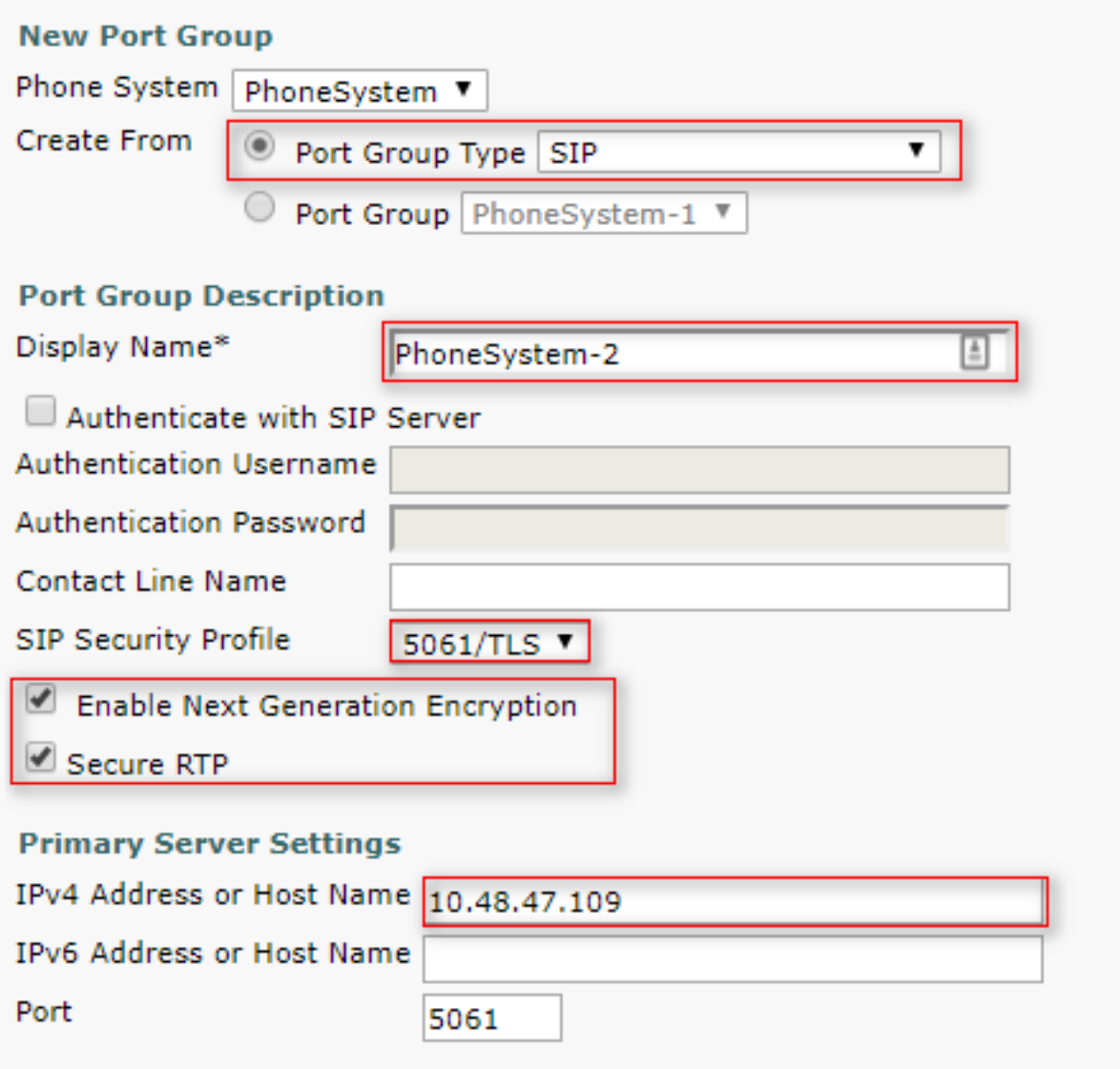
- Unity Connection
  Usted debe cargar la raíz y cualquier Certificados intermedio de las autoridades de certificación del otro vendedor en la CallManager-confianza del Unity Connection. Encima de eso,
  el Servidor de conexión descargará automáticamente el ITLfile del servidor TFTP especificado durante la configuración y la confianza CallManager.pem y CallManager-EC.pem durante la negociación de TLS.

- Cisco unificó el CM
  Usted debe cargar la raíz y cualquier Certificados intermedio de las autoridades de certificación del otro vendedor en la CallManager-confianza del CM unificado.

Configuración - Cisco Unity Connection (CUC)

1. Agregue a un nuevo grupo de puertos

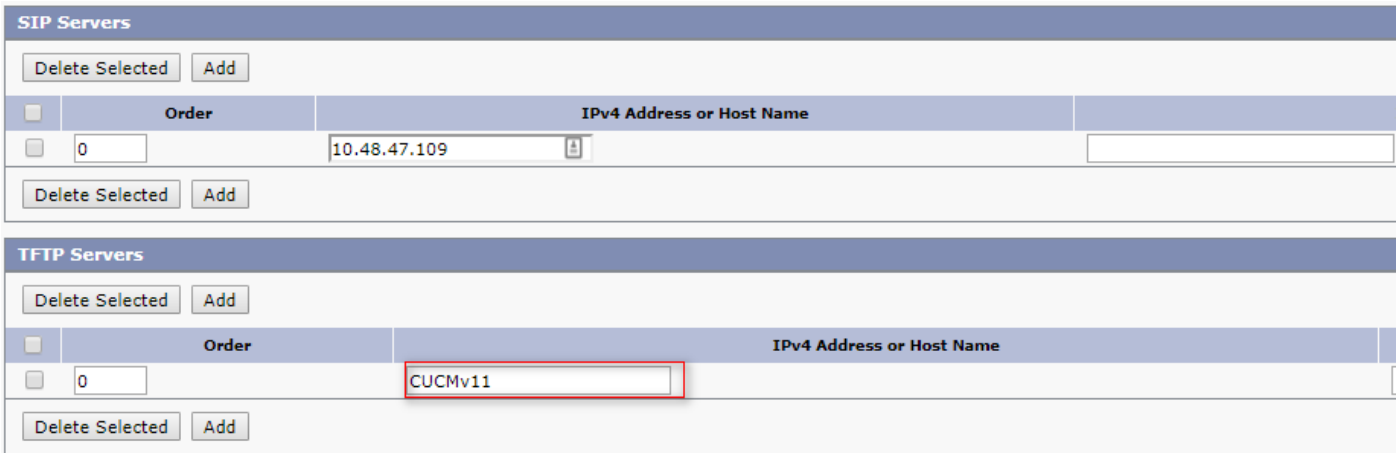
Navegue a la página de administración > a la integración de telefonía > al grupo de puertos del Cisco Unity Connection y haga clic en agregan nuevo. Aseegurese marcar el checkbox del cifrado de la última generación del permiso.



1. **Note**: El certificado de Cisco Tomcat del Unity Connection será utilizado durante el contacto SSL una vez que se habilita el checkbox del cifrado de la última generación del permiso.
   • En caso de que la cifra basada ECDSA entonces se negocie el certificado basado dominante EC Tomcat-ECDSA se utiliza en el contacto SSL.
   • En caso de que la cifra basada RSA entonces se negocie el certificado basado dominante del tomcat RSA se utiliza en el contacto SSL.

2. Agregue la referencia del servidor TFTP

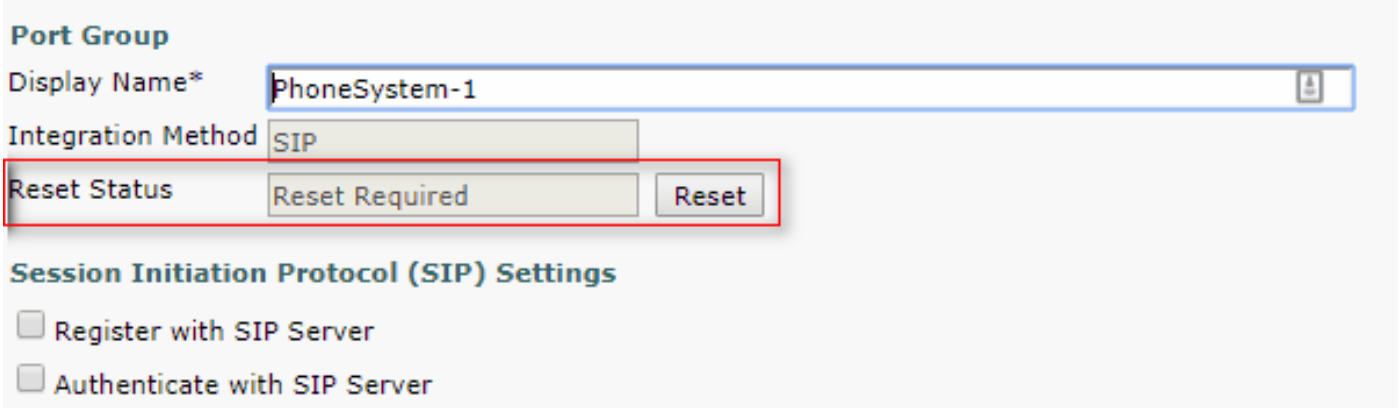
En el grupo de puertos que los fundamentos paginan, que navegue para editar > los servidores y para agregar el FQDN del servidor TFTP de su cluster CUCM. FQDN/Hostname del servidor TFTP debe hacer juego el Common Name (CN) del certificado del CallManager. La dirección IP del servidor no trabajará y dará lugar al error descargar el archivo ITL. El nombre DNS debe ser por lo tanto resolvable vía el servidor DNS configurado.



Recomience al administrador de la conversación de la conexión en cada nodo navegando a la utilidad del Cisco Unity Connection > a las herramientas > a la Administración del servicio. Esto es obligatorio para que la configuración tome el efecto.

1. **Note**: El archivo ITL de las descargas del Unity Connection (ITLfile.tlv) del TFTP CUCM usando el protocolo del https en 6972 seguros vira hacia el lado de babor (URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv). CUCM debe estar en el modo mezclado puesto que CUC está buscando el certificado de la función “CCM+TFTP” del archivo ITL.

Navegue de nuevo a los fundamentos página de configuración de la integración de telefonía > del grupo de puertos > del grupo de puertos y reajuste a su grupo de puertos nuevamente agregado.



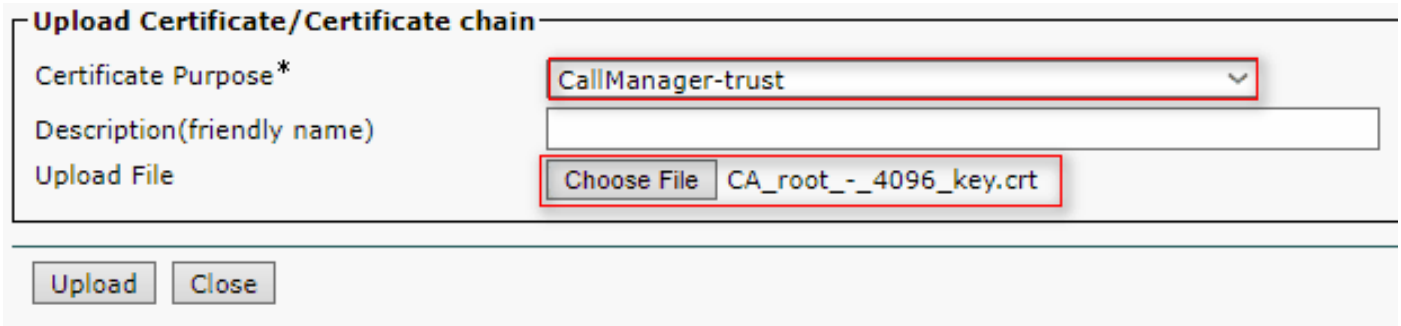
1. **Note**: Cada vez que reajustan al grupo de puertos, el servidor CUC pondrá al día su archivo localmente salvado ITL conectando con el servidor CUCM.

3. Agregue los puertos de correo de voz

Navegue de nuevo a la integración de telefonía > al puerto y haga clic en agregan nuevo para agregar el puerto a su grupo de puertos creado recientemente.

4. Cargue la raíz CUCM y el certificado del intermedio del otro vendedor CA

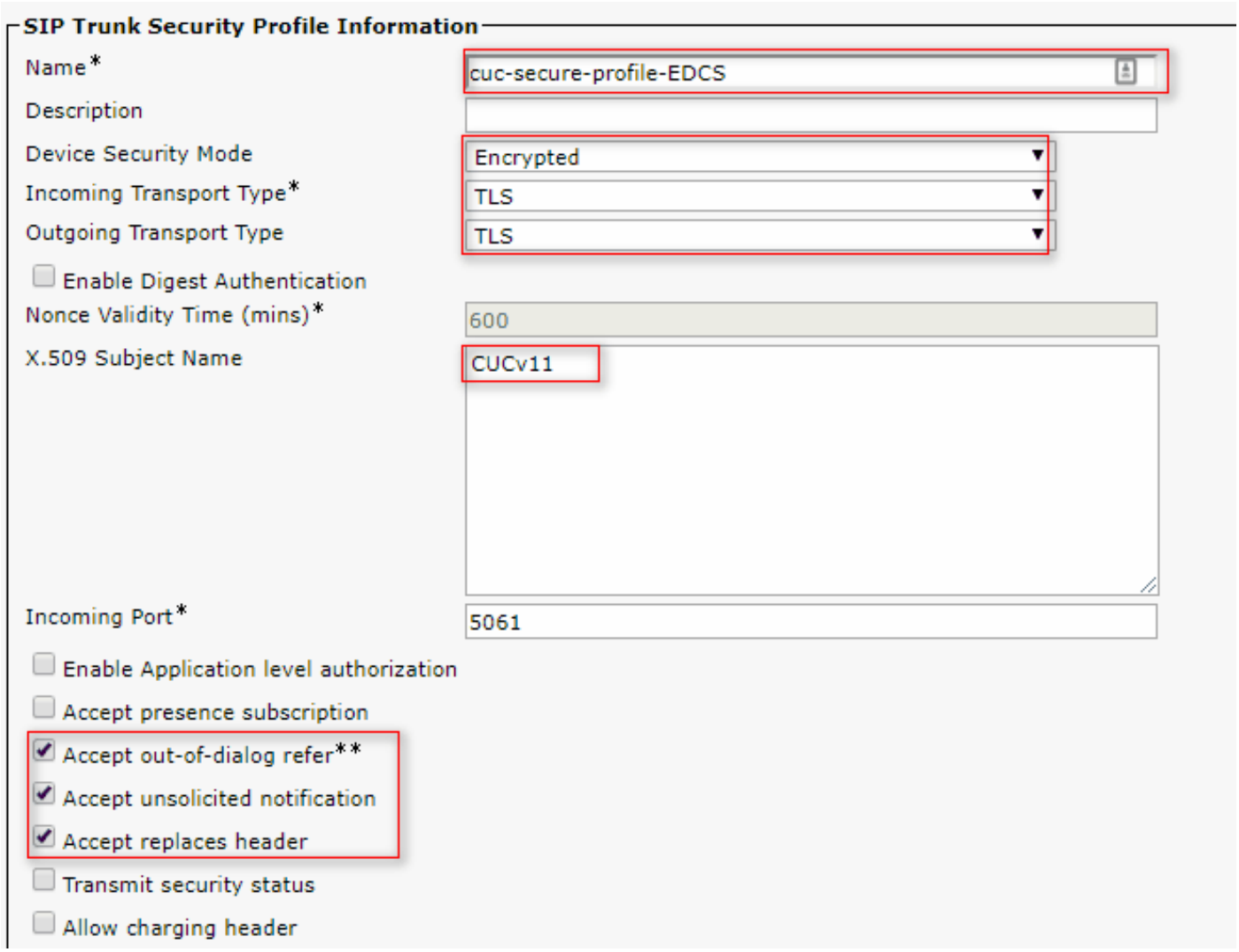
En caso de los Certificados del otro vendedor, usted debe cargar el certificado de la raíz y del intermedio de las autoridades de certificación del otro vendedor en la CallManager-confianza del Unity Connection. Se necesita esto solamente si las de otras compañías CA firmaron su certificado del administrador de llamada. Realice esta acción navegando a Cisco unificó el Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración OS y hacen clic en el certificado de la carga.



Configuración - Cisco unificó CM (CUCM)

1. Cree un perfil de seguridad del trunk del SORBO

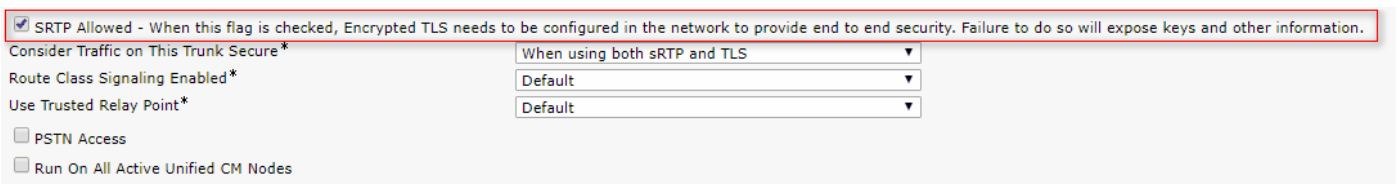
Navegue al > Security (Seguridad) de la administración > del sistema CUCM > al perfil de seguridad del trunk del SORBO y agregue un nuevo perfil. El asunto X.509 debe hacer juego el FQDN del servidor CUC.

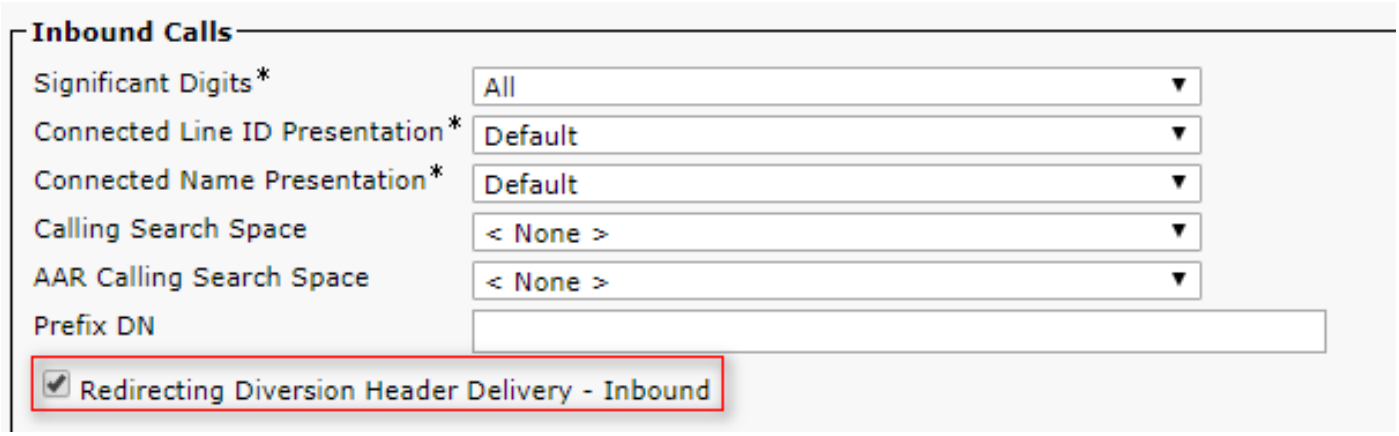


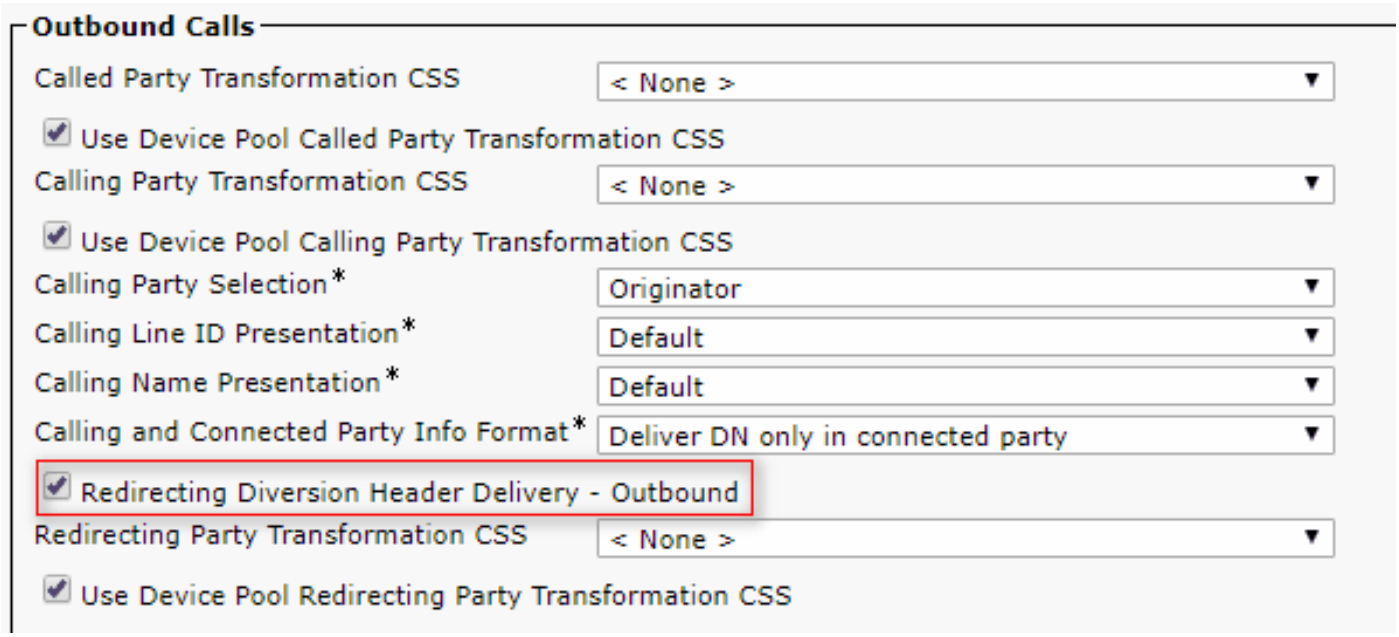
1. **Note**: El comando CLI “CERT de la demostración poseer el tomcat/tomcat.pem” puede visualizar el certificado basado clave del tomcat RSA en el Unity Connection. Es CN debe hacer juego el asunto X.509 configurado en CUCM. El CN es igual a FQDN/Hostname del servidor de Unity. El certificado basado clave EC contiene el FQDN/hostname en su campo sujeto del nombre alterno (SAN).

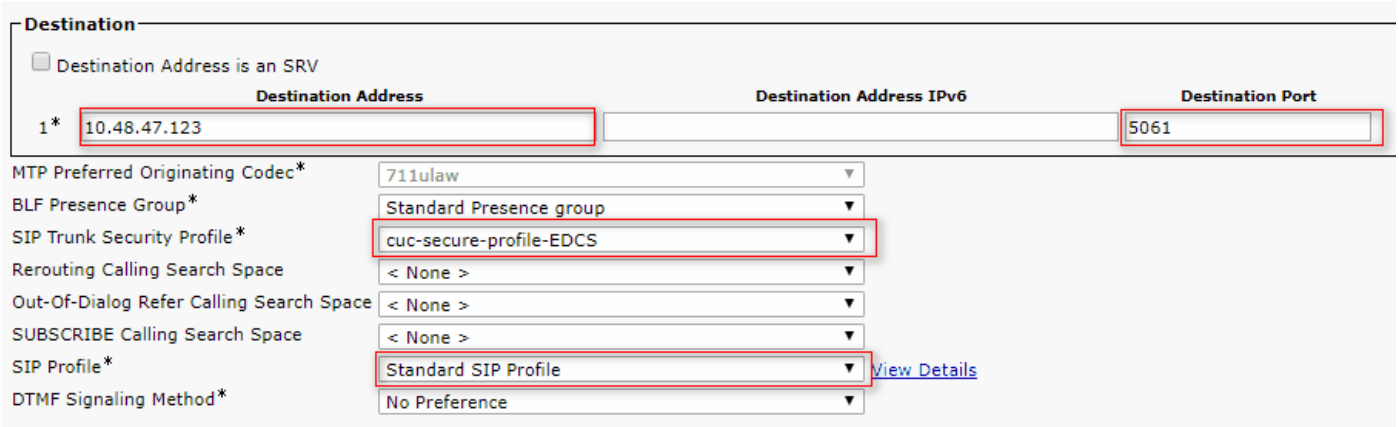
2. Cree un trunk seguro del SORBO

Navegue al dispositivo > al trunk > al tecleo y agregue nuevo y cree un trunk estándar del SORBO que sea utilizado para la integración segura con el Unity Connection.







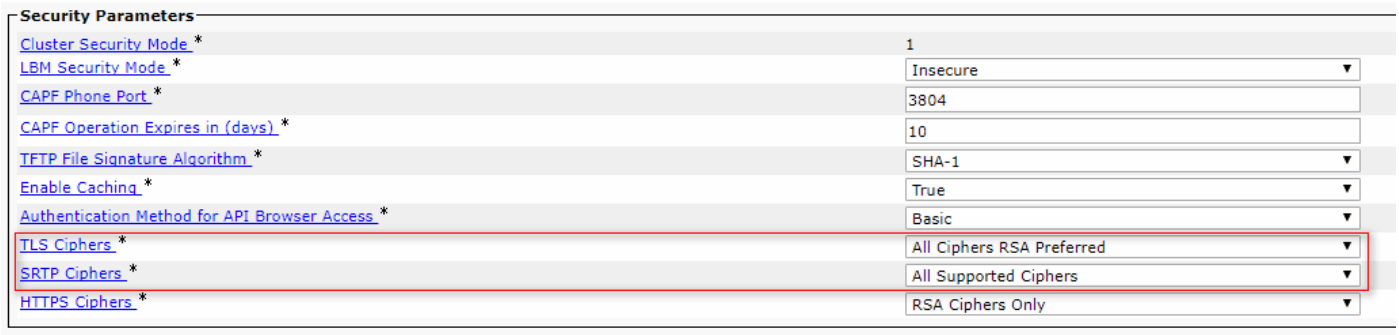


3. Configure las cifras de TLS y SRTP

1. **Note**: La negociación entre el Unity Connection y el administrador de las Comunicaciones unificadas de Cisco depende de la configuración de la cifra de TLS con las condiciones siguientes: Cuando el Unity Connection actúa como servidor, la negociación de la cifra de TLS se basa en la preferencia seleccionada por Cisco unificó el CM.En caso de que la cifra basada ECDSA entonces se negocie los Certificados basados dominantes EC Tomcat-ECDSA se utilizan en el contacto SSL.En caso de que la cifra basada RSA entonces se negocie los Certificados basados dominantes del tomcat RSA se utilizan en el contacto SSL.Cuando el Unity Connection actúa como cliente, la negociación de la cifra de TLS se

basa en la preferencia seleccionada por el Unity Connection.

Navegue a Cisco unificó CM > los sistemas > los parámetros Enterprise y seleccionan la opción apropiada de la cifra de las cifras de TLS y SRTP de la lista desplegable.



Recomience el servicio del Cisco Call Manager en cada nodo navegando a Cisco unificó la página de la utilidad, las herramientas > los servicios de la Centro-característica del control y Cisco Call Manager selecto bajo servicios CM

Navegue a la página de administración > a los ajustes de sistema > a las Configuraciones generales del Cisco Unity Connection y seleccione la opción apropiada de la cifra de las cifras de TLS y SRTP de la lista desplegable.

Recomience al administrador de la conversación de la conexión en cada nodo navegando a la utilidad del Cisco Unity Connection > a las herramientas > a la Administración del servicio.

Opciones de la cifra de TLS con la orden de la prioridad

Opciones de la cifra de TLS	Cifras de TLS en la orden de la prioridad
El SHA-384 más fuerte del AES-256 solamente: RSA preferido	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH
SHA-384 Strongest-AES-256 solamente: ECDSA preferido	

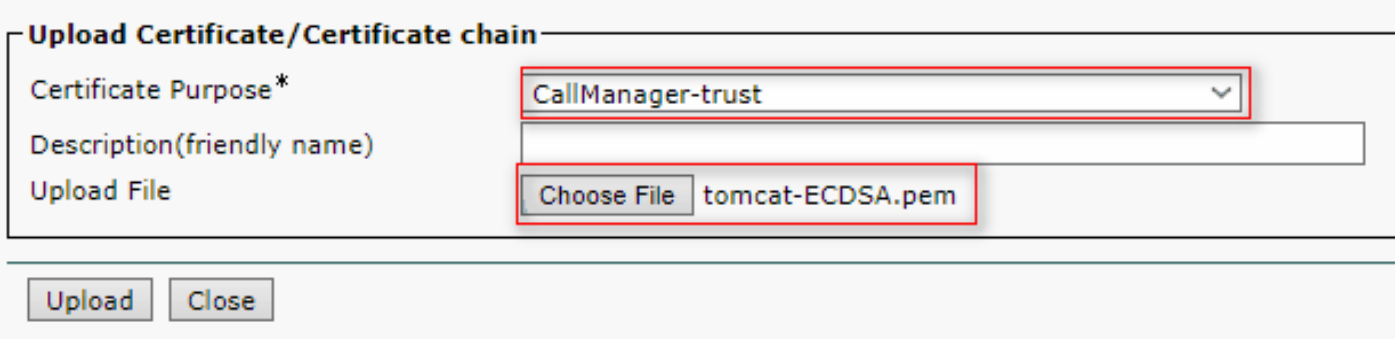
AES-128 Medium-AES-256 solamente: RSA preferido	4 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM _SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384
AES-128 Medium-AES-256 solamente: ECDSA preferido	• 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_ECDHE_RSA_WITH_AES_256_GCM_SH 4 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384
Todas las cifras RSA preferidas (valor por defecto)	• TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ A384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SH 4
Todas las cifras ECDSA preferidas	• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ A256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SH 6 • TLS_RSA_WITH_AES_128_CBC_SHA

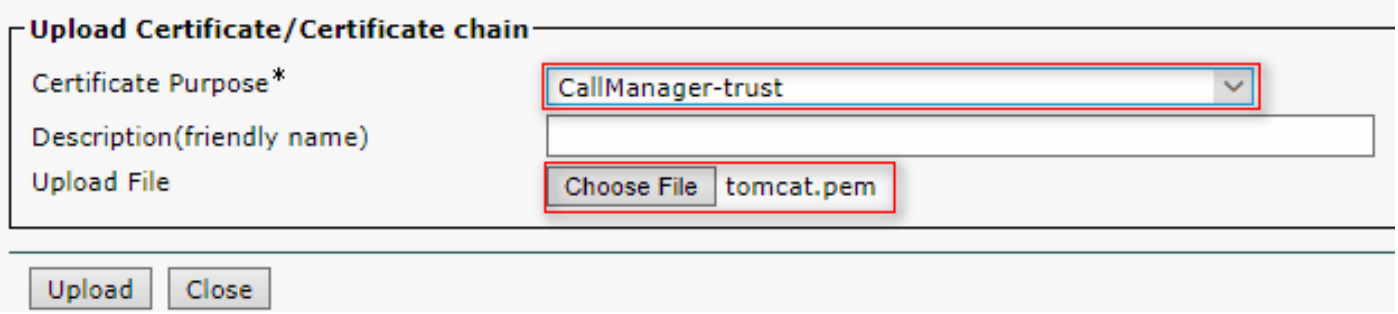
Opciones de la cifra SRTP en la orden de la prioridad

Opción de la cifra SRTP	SRTP en la orden de la prioridad
Todo el soportado AES-256, cifras del AES-128	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1 _32
AEAD AES-256, AES-28 GCM-basó las cifras	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
AEAD AES256 GCM-basó las cifras solamente	• AEAD_AES_256_GCM

4. Certificados de la carga CUC Tomcat (RSA y EC basados)

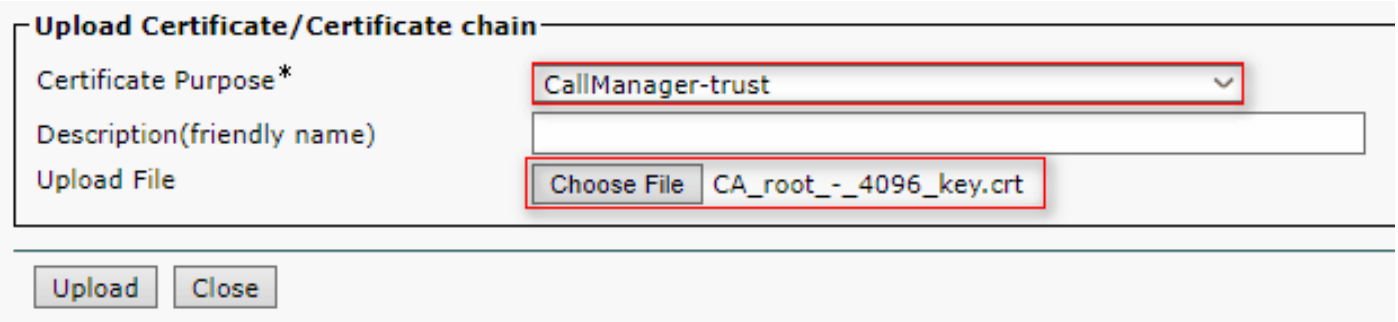
Navegue al Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración OS y cargue ambos Certificados CUC Tomcat (RSA y EC basados) en el almacén de la CallManager-confianza.





1. **Note**: Cargar ambos Certificados de Tomcat del Unity no es obligatorio si las cifras ECDSA se negocian solamente. En tal certificado basado EC de Tomcat del caso es bastante.

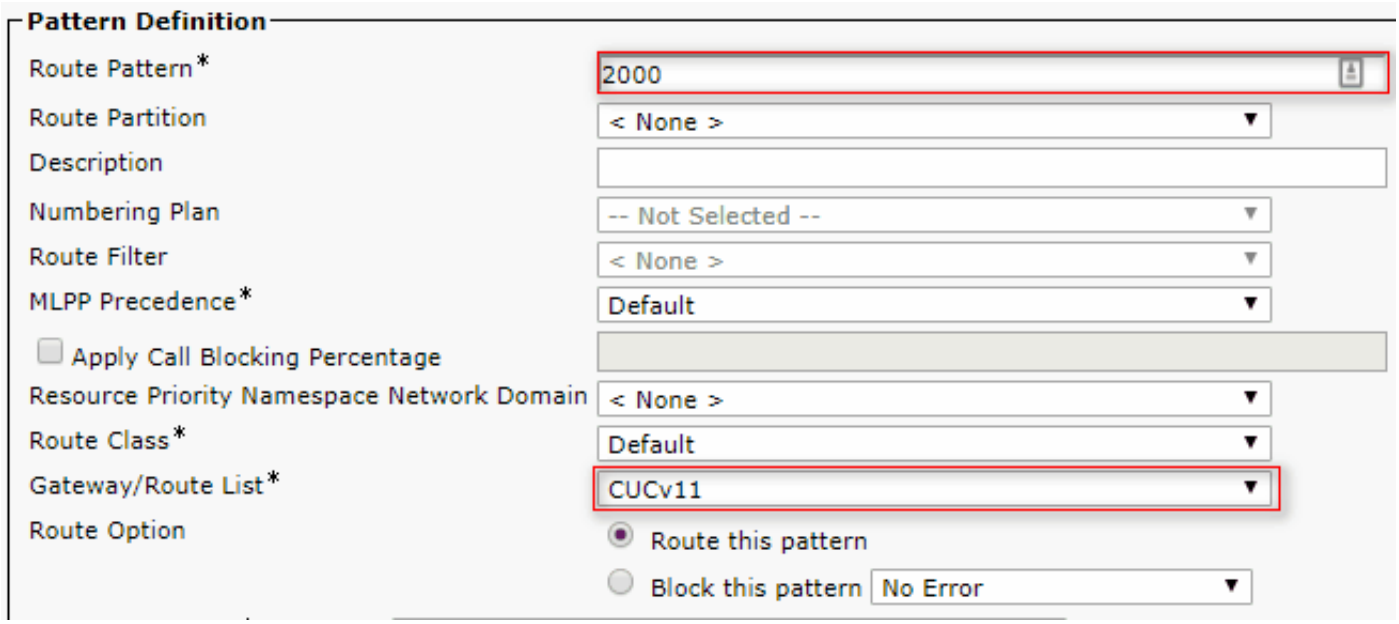
En caso de los Certificados del otro vendedor, usted debe cargar la raíz y el certificado del intermedio de las autoridades de certificación del otro vendedor. Se necesita esto solamente si las de otras compañías CA firmaron su certificado de Tomcat del Unity.



Recomience el proceso del Cisco Call Manager en todos los Nodos para aplicar los cambios.

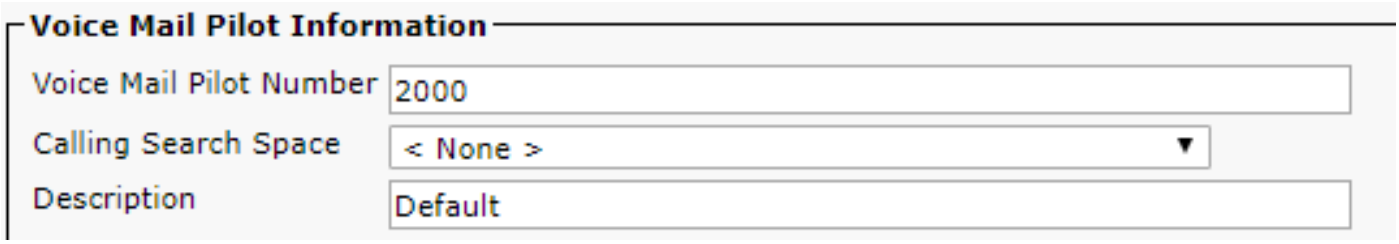
5. Cree al patrón de ruta

Configure a un patrón de ruta que las puntas al trunk configurado navegando al ruteo de llamadas > a la ruta/a la caza > al patrón de ruta. La extensión ingresada como número del patrón de ruta se puede utilizar como piloto del voicemail.

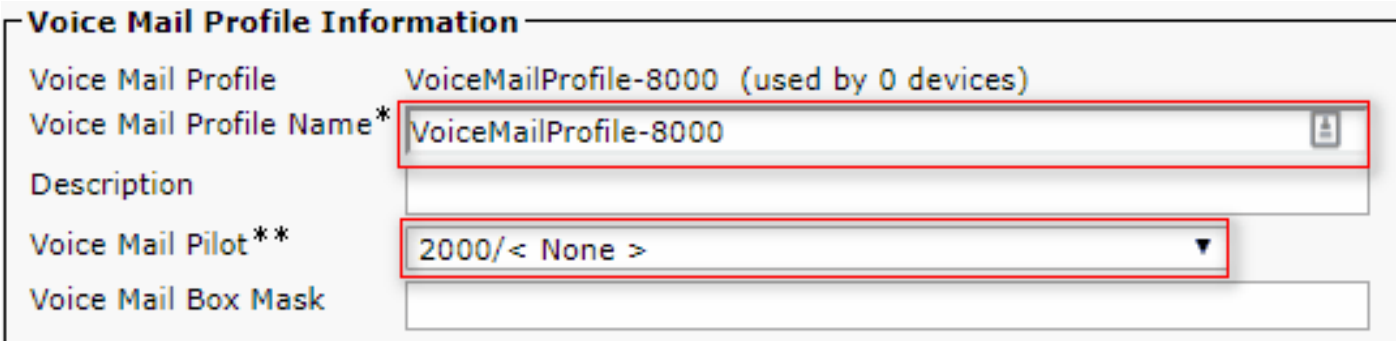


6. Cree al piloto del voicemail, perfil del voicemail y asígnelo a los DN

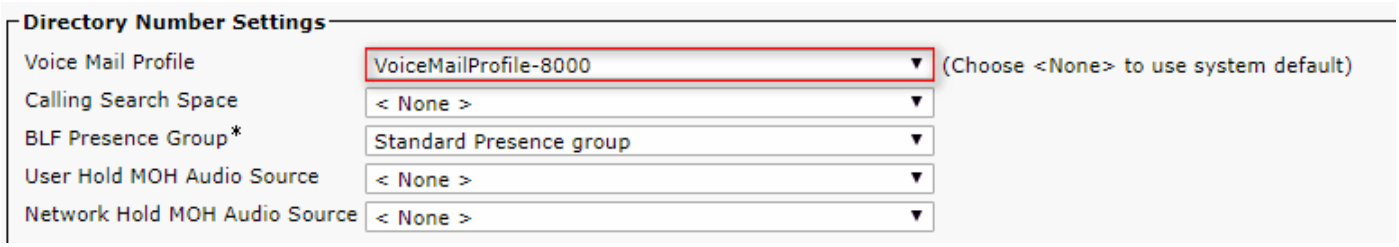
Cree a un correo de voz piloto para la integración yendo a las funciones avanzadas > al correo de voz > al correo de voz piloto.



Cree un perfil del correo de voz para conectar todas las funciones avanzadas > correo de voz > perfil del correo de voz de las configuraciones junto



Asigne el perfil del correo de voz creado recientemente a los DN previstos para utilizar la integración segura yendo al ruteo de llamadas > al número de directorio



Configuración - La firma de la clave EC basó los Certificados del otro vendedor CA (opcional)

Los Certificados se pudieron firmar por otro vendedor CA antes de configurar la integración segura entre los sistemas. Siga los pasos siguientes para firmar los Certificados en ambos sistemas.

Cisco Unity Connection

1. Genere el pedido de firma de certificado (CSR) para CUC Tomcat-ECDSA y haga que el certificado sea firmado por el otro vendedor CA
2. CA proporciona el certificado de identidad (certificado firmado de CA) y el certificado de CA (certificado raíz de CA) que se deben cargar como siguen:
   Cargue el certificado raíz de CA en el almacén de la Tomcat-confianza
   Cargue el certificado de identidad en el almacén Tomcat-EDCS
3. Recomience al administrador de la conversación en CUC

Cisco unificó el CM

1. Genere el CSR para el CallManager-ECDSA CUCM y haga que el certificado sea firmado por el otro vendedor CA
2. CA proporciona el certificado de identidad (certificado firmado de CA) y el certificado de CA (certificado raíz de CA) que se deben cargar como siguen:
   Cargue el certificado raíz de CA en el almacén de la CallManager-confianza
   Cargue el certificado de identidad en el almacén CallManager-EDCS
3. Recomience Cisco CCM y los servicios TFTP en cada nodo

El mismo proceso será utilizado para firmar los Certificados basados clave RSA donde el CSR se genera para el certificado CUC Tomcat y el certificado del CallManager y está cargado en el tomcat el almacén y el almacén del callmanager respectivamente.

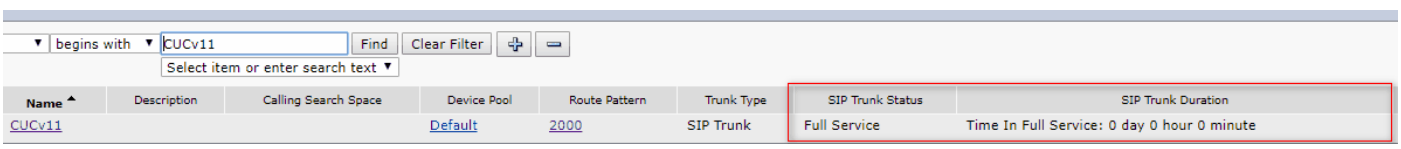
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Asegure la verificación del trunk del SORBO

Presione el botón del correo de voz en el teléfono para llamar el correo de voz. Usted debe oír el saludo inicial si la extensión del usuario no se configura en el sistema del Unity Connection.

Alternativamente, usted puede permitir al keepalive de las opciones del SORBO para monitorear el estado del tronco del SORBO. Esta opción se puede habilitar en el perfil del SORBO asignado al trunk del SORBO. Una vez que se habilita esto usted puede monitorear el estado del tronco del sorbo vía el dispositivo > el trunk como se muestra abajo:



Verificación segura de la llamada RTP

Verifique si el icono del candado esté presente en las llamadas al Unity Connection. Significa que secuencia RTP está cifrado (el perfil de seguridad del dispositivo debe ser seguro para que trabaje) tal y como se muestra en de esta imagen

Información Relacionada

- Guía de integración del SORBO para la versión 11.x del Cisco Unity Connection