

Configuración y resolución de problemas de integración segura entre CUCM y CUC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama](#)

[Configurar - Enlace troncal SIP seguro](#)

[Configurar CUC](#)

[1. Agregar certificado SIP](#)

[2. Crear nuevo sistema telefónico o modificar uno predeterminado](#)

[3. Agregar un nuevo grupo de puertos](#)

[4. Editar servidores](#)

[5. Restablecer el grupo de puertos](#)

[6. Agregar puertos de buzón de voz](#)

[7. Descargar certificado raíz de CUC](#)

[Configuración de CUCM](#)

[1. Configuración del perfil de seguridad del troncal SIP para el enlace troncal hacia CUC](#)

[2. Configurar perfil SIP](#)

[3. Crear tronco SIP](#)

[4. Crear un patrón de ruta](#)

[5. Creación de un piloto de buzón de voz](#)

[6. Crear perfil de buzón de voz](#)

[7. Asignar perfil de buzón de voz a los DN](#)

[8. Cargar certificado raíz CUC como CallManager-trust](#)

[Configurar puertos SCCP seguros](#)

[Configurar CUC](#)

[1. Descargue el certificado raíz de CUC](#)

[2. Crear sistema telefónico / Modificar el que existe.](#)

[3. Agregar un nuevo grupo de puertos SCCP](#)

[4. Editar servidores](#)

[5. Agregar puertos SCCP seguros](#)

[Configuración de CUCM](#)

[1. Agregar puertos](#)

[2. Cargar certificado raíz CUC como CallManager-trust](#)

[3. Configurar extensiones de activación/desactivación de información de mensaje en espera \(MWI\)](#)

[4. Crear cabecera de buzón de voz](#)

[5. Crear perfil de buzón de voz](#)

[6. Asignar perfil de buzón de voz a los DN](#)

[7. Crear un grupo de búsqueda de correo de voz](#)

[Verificación](#)

[Verificación de puertos SCCP](#)

[Verificación segura del troncal SIP](#)

[Verificación segura de llamada RTP](#)

[Troubleshoot](#)

[1. Consejos generales para la resolución de problemas](#)

[2. Seguimientos a recopilar](#)

[Problemas comunes](#)

[Caso 1: No se puede establecer una conexión segura \(alerta de CA desconocida\)](#)

[Caso 2: No se puede descargar el archivo CTL desde CUCM TFTP](#)

[Caso 3: Los puertos no se registran](#)

[Defectos](#)

Introducción

Este documento describe la configuración, verificación y resolución de problemas de la conexión segura entre Cisco Unified Communication Manager (CUCM) y el servidor Cisco Unity Connection (CUC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de CUCM.

Refiérase a [Guía de Seguridad de Cisco Unified Communications Manager](#) para obtener más detalles.

Nota: Debe configurarse en modo mixto para que la integración segura funcione correctamente.

El cifrado debe estar habilitado para Unity Connection 11.5(1) SU3 y posteriores.

Comando CLI "utils cuc encryption <enable/disable>"

Componentes Utilizados

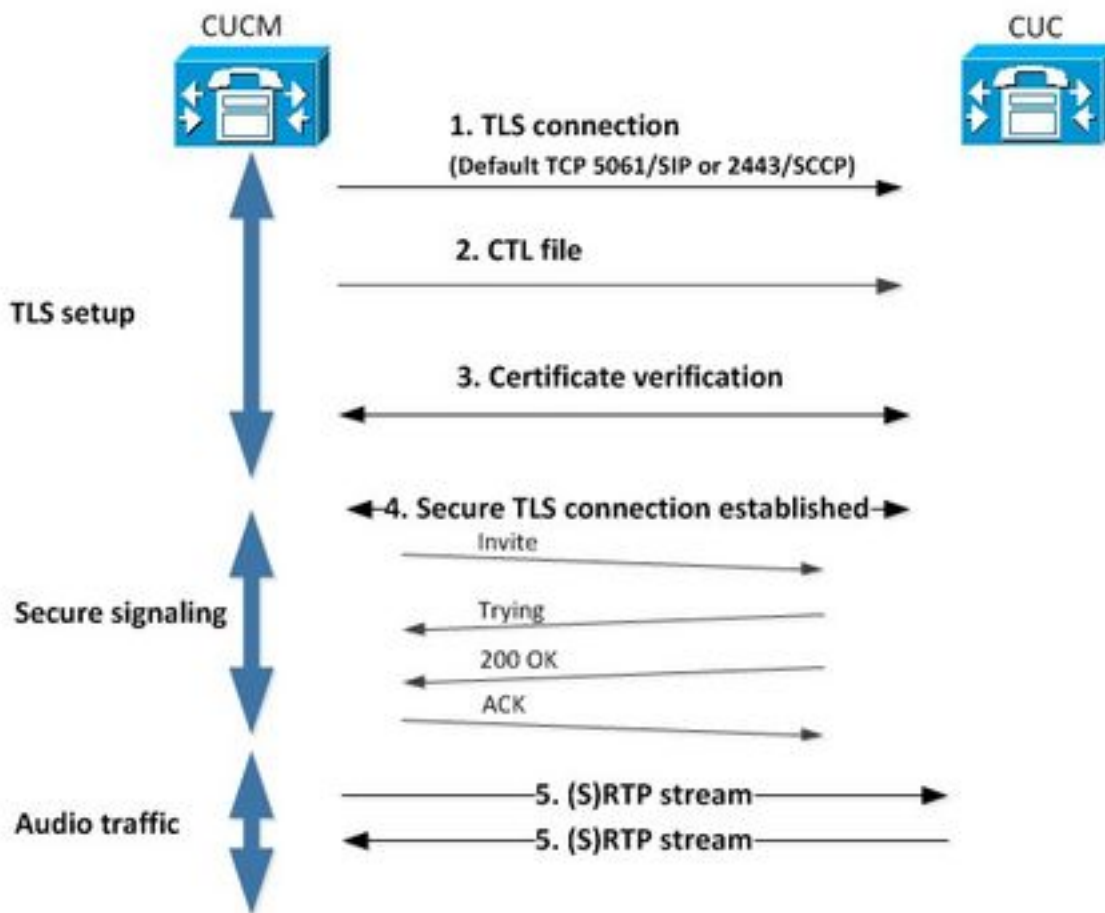
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CUCM, versión 10.5.2.11900-3.
- CUC versión 10.5.2.11900-3.

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

Este diagrama explica brevemente el proceso que ayuda a establecer una conexión segura entre CUCM y CUC:



1. El administrador de llamadas configura una conexión segura de seguridad de la capa de transporte (TLS) al servidor CUC en el puerto 2443 Skinny Call Control Protocol (SCCP) o en el protocolo 5061 Session Initiation Protocol (SIP) en el protocolo utilizado para la integración.

2. El servidor CUC descarga el archivo de lista de confianza de certificados (CTL) del servidor TFTP (proceso único), extrae el certificado de CallManager.pem y lo almacena.

3. El servidor CUCM ofrece el certificado Callmanager.pem que se verifica con el certificado CallManager.pem obtenido en el paso anterior. Además, se está verificando el certificado CUC con un certificado raíz CUC almacenado en CUCM. Tenga en cuenta que el administrador debe cargar el certificado raíz en CUCM.

4. Si la verificación de los certificados se realiza correctamente, se establece una conexión TLS segura. Esta conexión se utiliza para intercambiar señales SCCP o SIP cifradas.

5. El tráfico de audio se puede intercambiar como protocolo de transporte en tiempo real (RTP) o SRTP.

Nota: Cuando establece una comunicación TLS, CUCM y CUC utilizan la autenticación mutua TLS. Consulte RFC5630 para obtener más información.

Configurar - Enlace troncal SIP seguro

Configurar CUC

1. Agregar certificado SIP

Vaya a **Administración de CUC > Integración de telefonía > Seguridad > Certificado SIP > Agregar nuevo**

- Nombre de visualización: <cualquier nombre significativo>
- Nombre del asunto: <cualquier nombre, por ejemplo, **SecureConnection**>

Nota: el nombre del asunto debe coincidir con el nombre del asunto X.509 en el perfil de seguridad del troncal SIP (configurado en el paso 1 de la configuración de CUCM más adelante en este documento).

New SIP Certificate

SIP Certificate Reset Help

New SIP Certificate

Display Name* Secure SIP integration with CUCMv10.5.2

Subject Name* SecureConnection

Save

Fields marked with an asterisk (*) are required.

Nota: El certificado es generado y firmado por el certificado raíz CUC.

2. Crear nuevo sistema telefónico o modificar uno predeterminado

Vaya a **Telephony Integration > Phone System**. Puede utilizar el sistema telefónico que ya existe o crear uno nuevo.

Phone System Basics (PhoneSystem)

Phone System Edit Refresh Help

Save Delete Previous Next

Status

The phone system cannot take calls until a port group is set. Use the Related Links to add a port group.

Phone System

Phone System Name* PhoneSystem

Default TRAP Phone System

3. Agregar un nuevo grupo de puertos

En la página Conceptos básicos del sistema telefónico, en el cuadro desplegable Enlaces relacionados, seleccione Agregar grupo de puertos y seleccione Ir. En la ventana de configuración, introduzca esta información:

- Sistema telefónico:
- Crear desde: tipo de grupo de puertos SIP
- SIP Security Profile: 5061/TLS
- Certificado SIP:
- Modo de seguridad: cifrado
- RTP seguro: activado
- Dirección IPv4 o nombre de host:

Pulse Guardar.

New Port Group

Port Group Reset Help

Save

New Port Group

Phone System Secure SIP integration ▼

Create From Port Group Type SIP ▼
 Port Group ▼

Port Group Description

Display Name* Secure SIP integration-1

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile 5061/TLS ▼

SIP Certificate Secure SIP integration with CUCMv10.5.2 ▼

Security Mode Encrypted ▼

Secure RTP

Primary Server Settings

IPv4 Address or Host Name 10.48.47.110

IPv6 Address or Host Name

Port 5060

Save

4. Editar servidores

Navegue hasta **Editar > Servidores** y agregue el servidor TFTP desde el clúster de CUCM como se muestra en esta imagen.

The image shows two configuration panels. The top panel is titled "SIP Servers" and contains a table with one row: Order 0, IPv4 Address or Host Name 10.48.47.110. Below the table are "Delete Selected" and "Add" buttons. The bottom panel is titled "TFTP Servers" and contains a table with one row: Order 0, IPv4 Address or Host Name 10.48.47.110. Below the table are "Delete Selected" and "Add" buttons.

Nota: Es importante proporcionar una dirección TFTP correcta. El servidor CUC descarga el archivo CTL de este TFTP como se explicó.

5. Restablecer el grupo de puertos

Vuelva a **Port Group Basics** y restablezca el grupo de puertos según lo solicitado por el sistema como se muestra en esta imagen.

The image shows the "Port Group Basics (Secure SIP integration-1)" configuration page. It includes a "Status" section with two warning messages: "The phone system cannot take calls if it has no ports. Use the Related Links to add ports." and "One or more port groups need to be reset." Below this, the "Port Group" section shows "Display Name*" as "Secure SIP integration-1", "Integration Method" as "SIP", and "Reset Status" as "Reset Required". A "Reset" button is visible.

6. Agregar puertos de buzón de voz

En la página **Conceptos básicos de grupos de puertos**, en el cuadro desplegable **Enlaces relacionados**, seleccione **Agregar puertos** y seleccione **Ir**. En la ventana de configuración,

introduzca esta información:

- Habilitado: Activado
- Número de puertos:
- Sistema telefónico:
- Grupo de puertos
- Servidor:
- Comportamiento del puerto:

New Port

Port Reset Help

Status

⚠ Because it has no port groups, PhoneSystem is not listed in the Phone system field.

Save

New Phone System Port

Enabled

Number of Ports

Phone System

Port Group

Server

Port Behavior

Answer Calls

Perform Message Notification

Send MWI Requests (may also be disabled by the port group)

Allow TRAP Connections

Save

7. Descargar certificado raíz de CUC

Navegue hasta **Telephony Integrations > Security > Root Certificate**, haga clic con el botón derecho en la URL para guardar el certificado como un archivo denominado <filename>.0 (la extensión del archivo debe ser .0 en lugar de .htm)' y presione save como se muestra en esta imagen.



Configuración de CUCM

1. Configuración del perfil de seguridad del troncal SIP para el enlace troncal hacia CUC

Vaya a **CUCM Administration > System > Security > SIP Trunk Security Profile > Add new**

Asegúrese de que estos campos se rellenan correctamente:

- Modo de seguridad del dispositivo: cifrado
- Nombre del asunto X.509: SecureConnection>
- Aceptar fuera del diálogo: activado
- Aceptar notificación no solicitada: activada
- Aceptar reemplaza el encabezado: activado

Nota: El nombre del asunto X.509 debe coincidir con el campo Nombre del asunto del certificado SIP en el servidor de Cisco Unity Connection (configurado en el paso 1 de la configuración CUC).

SIP Trunk Security Profile Information

Name*	Secure_sip_trunk_profile_for_CUC
Description	
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	SecureConnection
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

2. Configurar perfil SIP

Vaya a **Device > Device Settings > SIP Profile** si necesita aplicar alguna configuración específica. De lo contrario, puede utilizar el perfil SIP estándar.

3. Crear tronco SIP

Vaya a **Device > Trunk > Add new**. Cree un troncal SIP que se utilizará para la integración segura con Unity Connection como se muestra en esta imagen.

Trunk Information

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

En la sección Información del dispositivo de la configuración troncal, introduzca esta información:

- Nombre del dispositivo:
- Agrupación de dispositivos:
- SRTP permitido: activado

Nota: Asegúrese de que el grupo CallManager (en la configuración del conjunto de dispositivos) contenga todos los servidores configurados en CUC (**grupo de puertos > Editar > Servidores**).

Trunk Configuration

Save

Status

Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	SecureSIPtoCUC
Description	Trunk for secure integration with CUC
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
 Consider Traffic on This Trunk Secure* When using both sRTP and TLS
 Route Class Signaling Enabled* Default
 Use Trusted Relay Point* Default
 PSTN Access
 Run On All Active Unified CM Nodes

En la sección Llamadas entrantes de la configuración troncal, ingrese esta información:

- Calling Search Space:
- Redireccionamiento de Entrega de Encabezado de Desviación - Entrante: Activado

Inbound Calls

Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	AllPhones
AAR Calling Search Space	< None >
Prefix DN	

Redirecting Diversion Header Delivery - Inbound

En el campo Oubound Sección Llamadas de configuración troncal, introduzca esta información:

- Redireccionamiento de Entrega de Encabezado de Desviación - Saliente: activado

Outbound Calls

Called Party Transformation CSS

Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS

Use Device Pool Calling Party Transformation CSS

Calling Party Selection*

Calling Line ID Presentation*

Calling Name Presentation*

Calling and Connected Party Info Format*

Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS

Use Device Pool Redirecting Party Transformation CSS

En la sección Información de SIP de la configuración troncal, introduzca esta información:

- dirección de destino:
- Perfil de seguridad del enlace troncal SIP:
- Volver a enrutar el espacio de búsqueda de llamada:
- Espacio de búsqueda de llamadas de consulta fuera del diálogo:
- Perfil SIP:

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	<input type="text" value="10.48.47.124"/>	<input type="text"/>	<input type="text" value="5061"/>

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

DTMF Signaling Method*

Ajuste otros parámetros según sus requisitos.

4. Crear un patrón de ruta

Cree un patrón de ruta que apunte al tronco configurado (**Call Routing > Route/Hunt > Route Pattern**). La extensión ingresada como número de patrón de ruta se puede utilizar como piloto de correo de voz. Ingresar esta información

- Patrón de ruta:
- Gateway/lista de rutas:

Route Pattern Configuration

Save

Status

Status: Ready

Pattern Definition

Route Pattern*	8000
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	SecureSIPtoCUC (Edit)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error

5. Creación de un piloto de buzón de voz

Cree un piloto de correo de voz para la integración (**Funciones avanzadas > Buzón de voz > Piloto de buzón de voz**). Introduzca estos valores:

- Número piloto de buzón de voz:
- Espacio de búsqueda de llamadas: que incluye particiones que contienen el patrón de ruta utilizado como piloto>

Voice Mail Pilot Information

Voice Mail Pilot Number	8000
Calling Search Space	< None >
Description	
<input type="checkbox"/> Make this the default Voice Mail Pilot for the system	

6. Crear perfil de buzón de voz

Cree un perfil de correo de voz para vincular todos los ajustes (**Funciones avanzadas > Buzón de voz > Perfil de buzón de voz**). Introduzca la siguiente información:

- Piloto del correo de voz:
- Máscara de casilla de correo de voz:

Voice Mail Profile Information

Voice Mail Profile Name* Voicemail-profile-8000

Description Secure Voicemail

Voice Mail Pilot** 8000/< None >

Voice Mail Box Mask

Make this the default Voice Mail Profile for the System

7. Asignar perfil de buzón de voz a los DN

Asigne el perfil de buzón de voz a los DN que pretendan utilizar una integración segura. No olvide hacer clic en el botón 'Aplicar configuración' después de cambiar la configuración de DN:

Vaya a: **Call Routing > Directory number** y cambie lo siguiente:

- Voice Mail Profile: Secure_SIP_Integration

Directory Number Configuration

Save Delete Reset Apply Config Add New

Directory Number Settings

Voice Mail Profile Secure_SIP_Integration (Choose <None> to use system default)

Calling Search Space < None >

BLF Presence Group* Standard Presence group

User Hold MOH Audio Source < None >

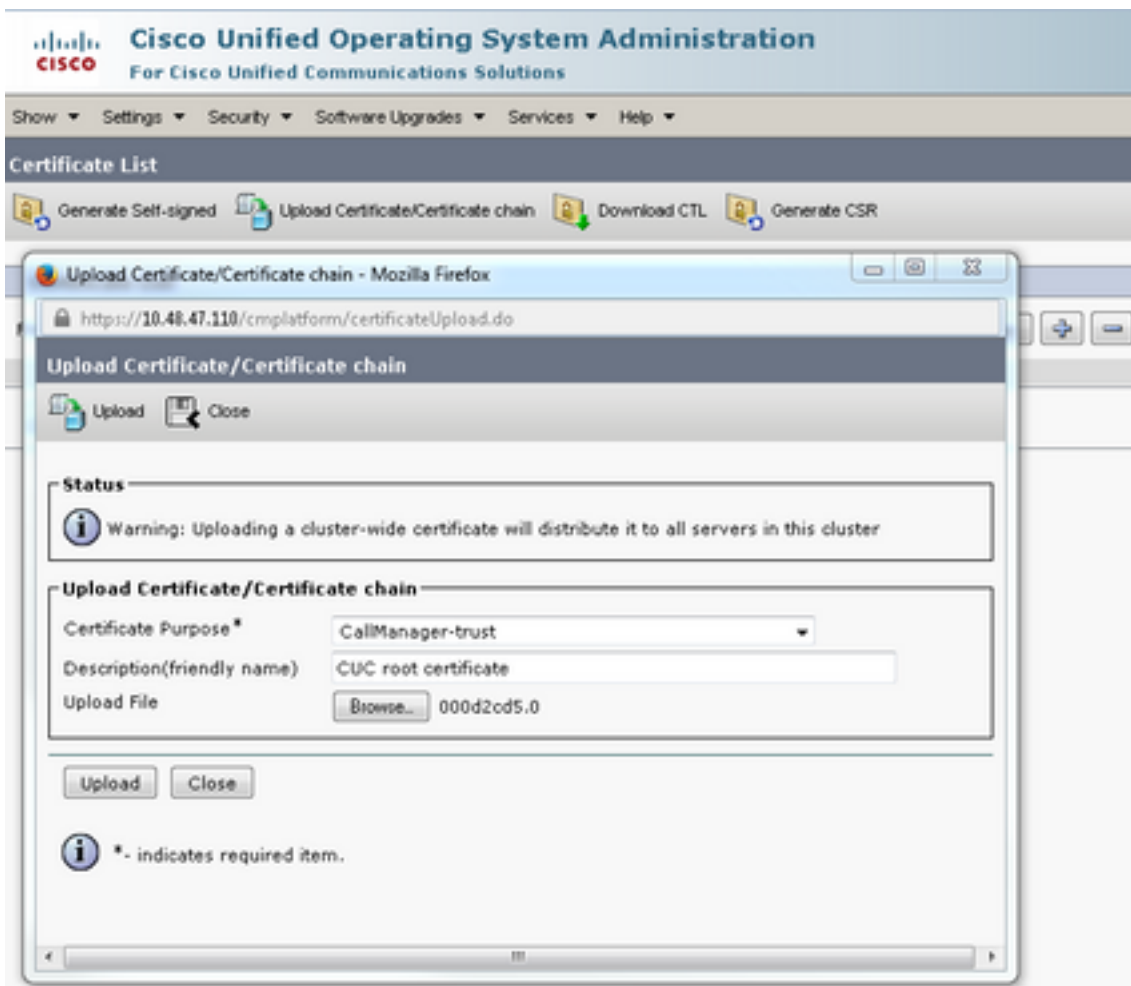
Network Hold MOH Audio Source < None >

Auto Answer* Auto Answer Off

Reject Anonymous Calls

8. Cargar certificado raíz CUC como CallManager-trust

Navegue hasta **Administración del sistema operativo > Seguridad > Administración de certificados > Cargar certificado/Cadena de certificados** y cargue el certificado raíz de CUC como **CallManager-trust** en todos los nodos configurados para comunicarse con el servidor CUC.



Nota: El servicio Cisco CallManager debe reiniciarse después de cargar el certificado para que el certificado tenga efecto.

Configurar puertos SCCP seguros

Configurar CUC


1. Descargue el certificado raíz de CUC


Vaya a Administración de CUC > Integración de telefonía > Seguridad > Certificado raíz. Haga clic con el botón derecho del ratón en la URL para guardar el certificado como un archivo denominado <filename>.0 (la extensión del archivo debe ser .0 en lugar de .htm)' y presione Guardar:

- Sistema telefónico:
- Tipo de grupo de puertos: SCCP
- Prefijo de nombre de dispositivo*: CiscoUM1-VI
- MWI En extensión:
- Extensión MWI Off:

Nota: Esta configuración debe coincidir con la configuración en CUCM.

Status

 The phone system cannot take calls if it has no ports. Use the Related Links to add ports.

 Created Port Group(s)

Port Group

Display Name*

Integration Method

Device Name Prefix*

Reset Status

Message Waiting Indicator Settings

Enable Message Waiting Indicators

MWI On Extension

MWI Off Extension

Delay between Requests milliseconds

Maximum Concurrent Requests

Retries After Successful Attempt

Retry Interval After Successful Attempt milliseconds

Fields marked with an asterisk (*) are required.

4. Editar servidores

Navegue hasta **Editar > Servidores** y agregue el servidor TFTP desde el clúster de CUCM.

SIP Servers		
<input type="button" value="Delete Selected"/> <input type="button" value="Add"/>		
<input type="checkbox"/>	Order	IPv4 Address or Host Name
<input type="checkbox"/>	0	10.48.47.110
<input type="button" value="Delete Selected"/> <input type="button" value="Add"/>		
TFTP Servers		
<input type="button" value="Delete Selected"/> <input type="button" value="Add"/>		
<input type="checkbox"/>	Order	IPv4 Address or Host Name
<input type="checkbox"/>	0	10.48.47.110
<input type="button" value="Delete Selected"/> <input type="button" value="Add"/>		


Nota: Es importante proporcionar una dirección TFTP correcta. El servidor CUC descarga el archivo CTL de este TFTP como se explicó.

5. Agregar puertos SCCP seguros

En la página Conceptos básicos de grupos de puertos, en el cuadro desplegable Enlaces relacionados, seleccione **Agregar puertos** y seleccione **Ir**. En la ventana de configuración, introduzca esta información:

- Habilitado: activado
- Número de puertos:
- Sistema telefónico:
- Grupo de puertos
- Servidor:
- Comportamiento del puerto:
- Modo de seguridad: **Cifrado**

Status

 Because it has no port groups, PhoneSystem is not listed in the Phone system field.

New Phone System Port

Enabled

Number of Ports

Phone System

Port Group

Server

Port Behavior

Answer Calls

Perform Message Notification

Send MWI Requests (may also be disabled by the port group)

Allow TRAP Connections

Security Mode

Configuración de CUCM

1. Agregar puertos

Vaya a **CUCM Administration > Advanced Features > Voice Mail Port Configuration > Add New**.

Configure los puertos de correo de voz SCCP como siempre. La única diferencia está en el Modo de seguridad del dispositivo en la configuración del puerto donde debe seleccionarse la opción Puerto de buzón de voz cifrado.

Voice Mail Port Configuration

Save Delete Copy Reset Apply Config Add New

Status

Status: Ready

Device Information

Registration: Registered with Cisco Unified Communications Manager 10.48.46.182
 IPv4 Address: 10.48.46.184
 Device is trusted
 Port Name* CiscoUM1-VI1
 Description VM-sccp-secure-ports
 Device Pool* Default
 Common Device Configuration < None >
 Calling Search Space < None >
 AAR Calling Search Space < None >
 Location* Hub_None
 Device Security Mode* Encrypted Voice Mail Port
 Use Trusted Relay Point* Default
 Geolocation < None >

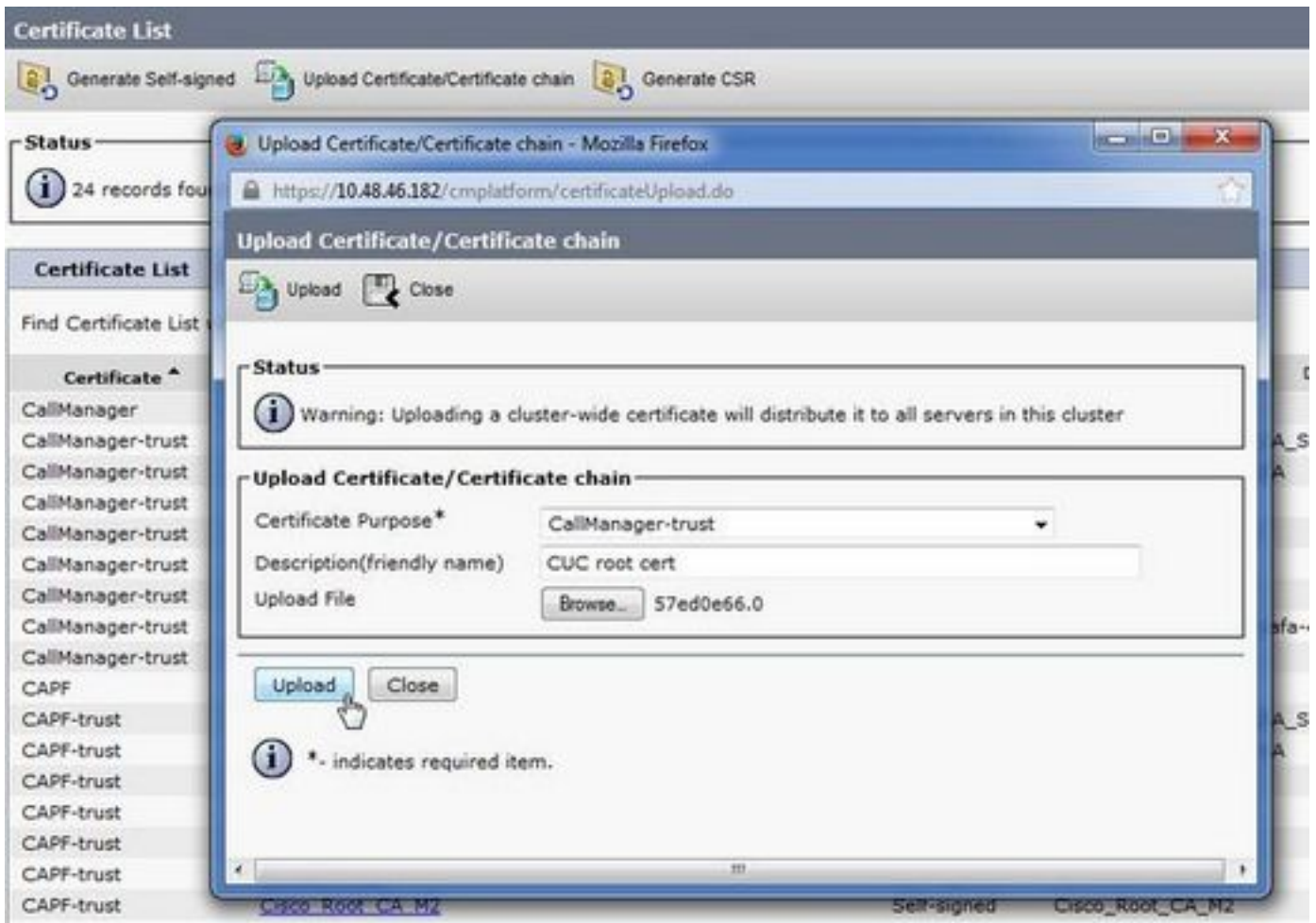
Directory Number Information

Directory Number* 999001
 Partition < None >
 Calling Search Space < None >
 AAR Group < None >
 Internal Caller ID Display VoiceMail
 Internal Caller ID Display (ASCII format) VoiceMail
 External Number Mask

Save Delete Copy Reset Apply Config Add New

2. Cargar certificado raíz CUC como CallManager-trust

Navegue hasta **Administración del sistema operativo > Seguridad > Administración de certificados > Cargar certificado/Cadena de certificados** y cargue el certificado raíz de CUC como **CallManager-trust** en todos los nodos configurados para comunicarse con el servidor CUC.



Nota: El servicio Cisco CallManager debe reiniciarse después de cargar el certificado para que el certificado tenga efecto.

3. Configurar extensiones de activación/desactivación de información de mensaje en espera (MWI)

Navegue hasta **Administración de CUCM > Funciones avanzadas > Configuración de puerto de buzón de voz** y configure **Extensiones de encendido/apagado de MWI**. Los números MWI deben coincidir con la configuración CUC.

Message Waiting Information	
Message Waiting Number*	999991
Partition	< None >
Description	MWI on
Message Waiting Indicator*	<input checked="" type="radio"/> On <input type="radio"/> Off
Calling Search Space	< None >

Message Waiting Information

Message Waiting Number* 999990

Partition < None >

Description MWI off

Message Waiting Indicator* On Off

Calling Search Space < None >

Save

4. Crear cabecera de buzón de voz

Cree un piloto de correo de voz para la integración (**Funciones avanzadas > Buzón de voz > Piloto de buzón de voz**). Introduzca estos valores:

- Número piloto de buzón de voz:
- Espacio de búsqueda de llamadas: que incluye particiones que contienen el patrón de ruta utilizado como piloto>

Voice Mail Pilot Information

Voice Mail Pilot Number 8000

Calling Search Space < None >

Description

Make this the default Voice Mail Pilot for the system

5. Crear perfil de buzón de voz

Cree un perfil de correo de voz para vincular todos los ajustes (**Funciones avanzadas > Buzón de voz > Perfil de buzón de voz**). Ingresar esta información

- Piloto del correo de voz:
- Máscara de casilla de correo de voz:

Voice Mail Profile Information

Voice Mail Profile Name* Voicemail-profile-8000

Description Secure Voicemail

Voice Mail Pilot** 8000/< None >

Voice Mail Box Mask

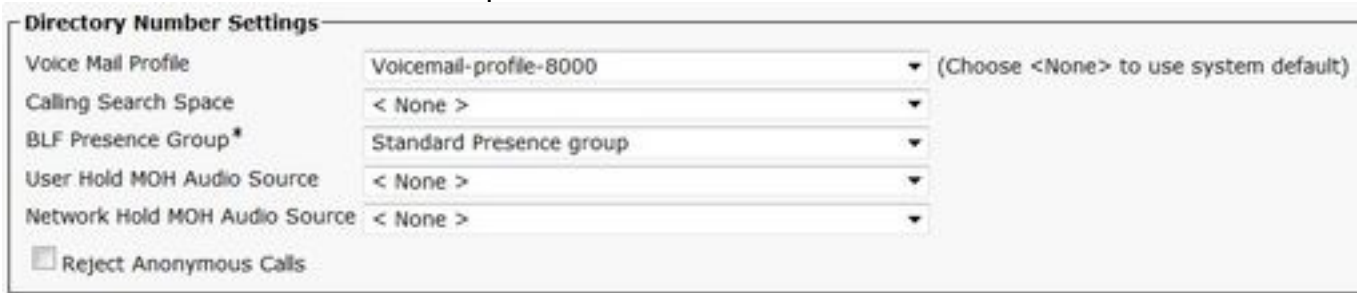
Make this the default Voice Mail Profile for the System

6. Asignar perfil de buzón de voz a los DN

Asigne el perfil de correo de voz a los DN que pretendan utilizar una integración segura. Haga clic en el botón **Aplicar configuración** después de cambiar la configuración DN:

Vaya a **Call Routing > Directory number** y cambie a:

- Voice Mail Profile: Voicemail-profile-8000



Directory Number Settings

Voice Mail Profile	Voicemail-profile-8000	(Choose <None> to use system default)
Calling Search Space	< None >	
BLF Presence Group*	Standard Presence group	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	

Reject Anonymous Calls

7. Crear un grupo de búsqueda de correo de voz

a) Agregar un nuevo grupo de línea (Call Routing > Route/Hunt > Line group)



Line Group Information

Line Group Name*	voicemail-1g
RNA Reversion Timeout*	10
Distribution Algorithm*	Longest Idle Time

b) Agregar una nueva lista de salto de correo de voz (Call Routing > Route/Hunt > Hunt List)



Hunt List Information

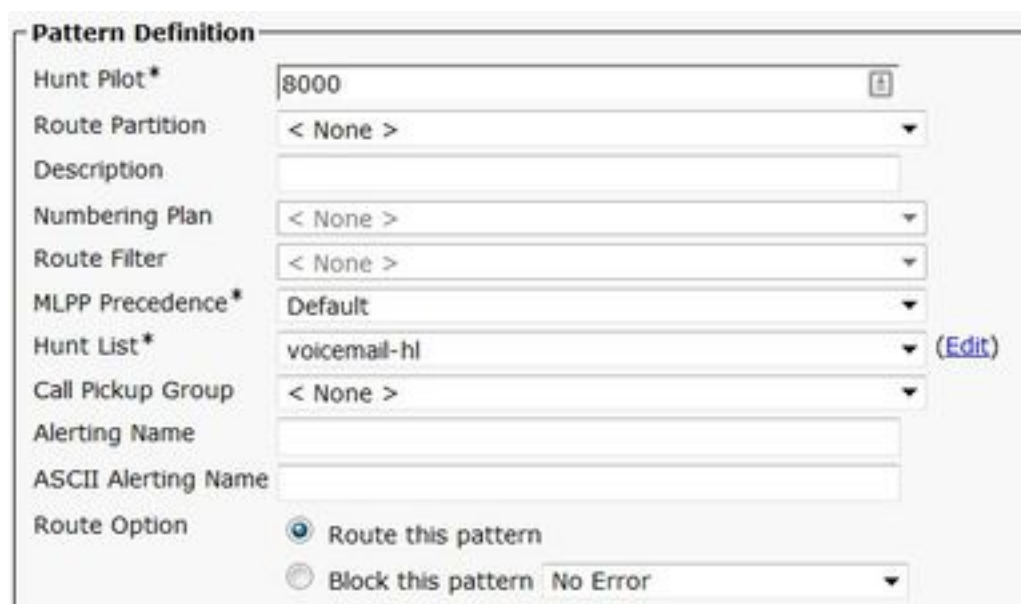
Device is trusted

Name*	voicemail-hl
Description	
Cisco Unified Communications Manager Group*	Default

Enable this Hunt List (change effective on Save; no reset required)

For Voice Mail Usage

c) Agregar un nuevo cabecera de grupo de salto (Call Routing > Route/Hunt > Hunt Pilot)



Pattern Definition

Hunt Pilot*	8000
Route Partition	< None >
Description	
Numbering Plan	< None >
Route Filter	< None >
MLPP Precedence*	Default
Hunt List*	voicemail-hl (Edit)
Call Pickup Group	< None >
Alerting Name	
ASCII Alerting Name	
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error

Verificación

Verificación de puertos SCCP

Navigate hasta **Administración de CUCM > Funciones avanzadas > Buzón de voz > Puertos de buzón de voz** y verifique el registro del puerto.

Device Name	Description	Device Pool	Device Security Mode	Calling Search Space	Extension	Partition	Status	SIP Address	Class
ClassSIP_V01	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999001		Registered with 10.45.46.182	10.45.46.184	
ClassSIP_V02	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999002		Registered with 10.45.46.182	10.45.46.184	
ClassSIP_V03	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999003		Registered with 10.45.46.182	10.45.46.184	
ClassSIP_V04	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999004		Registered with 10.45.46.182	10.45.46.184	
ClassSIP_V05	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999005		Registered with 10.45.46.182	10.45.46.184	
ClassSIP_V06	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999006		Registered with 10.45.46.182	10.45.46.184	
ClassSIP_V07	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999007		Registered with 10.45.46.182	10.45.46.184	
ClassSIP_V08	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999008		Registered with 10.45.46.182	10.45.46.184	

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

Verificación segura del troncal SIP

Presione el botón **Buzón de voz** del teléfono para llamar al correo 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 que esto esté habilitado, puede monitorear el estado del tronco Sip a través de **Device > Trunk** como se muestra en esta imagen.

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
SecureSIPtoCUC		Default						SIP Trunk	No Service	Time not in Full Service: 0 day 0 hour 0 minute

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.



Troubleshoot

1. Consejos generales para la resolución de problemas

Siga estos pasos para resolver problemas de integración segura:

- Verifique la Configuración.
- Asegúrese de que todos los servicios relacionados se estén ejecutando. (CUCM - CallManager, TFTP, CUC - Administrador de conversaciones)
- Asegúrese de que los puertos necesarios para la comunicación segura entre servidores estén abiertos en la red (puerto TCP 2443 para la integración SCCP y TCP 5061 para la integración SIP).
- Si todo esto es correcto, continúe con la colección de seguimientos.

2. Seguimientos a recopilar

Recopile estos seguimientos para resolver problemas de integración segura.

- Captura de paquetes de CUCM y CUC
- Seguimientos de CallManager
- Seguimientos de Cisco Conversation Manager

Consulte estos recursos para obtener información adicional sobre:

Cómo realizar una captura de paquetes en CUCM:

<http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-50/112040-packet-capture-cucm-00.html>

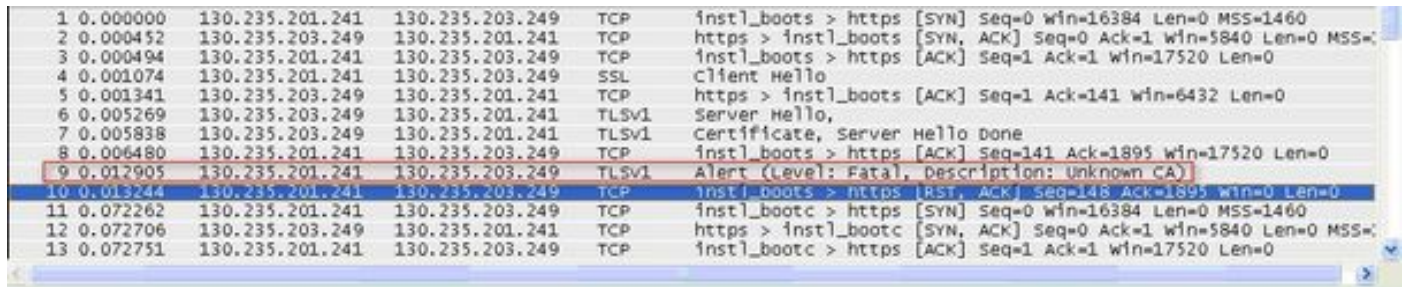
Cómo habilitar seguimientos en el servidor CUC:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsg/10xcuctsg010.html

Problemas comunes

Caso 1: No se puede establecer una conexión segura (alerta de CA desconocida)

Después de que la captura de paquetes se recopile de cualquiera de los servidores, se establece la sesión TLS.



1	0.000000	130.235.201.241	130.235.203.249	TCP	instl_boots > https [SYN] Seq=0 win=16384 Len=0 MSS=1460
2	0.000452	130.235.203.249	130.235.201.241	TCP	https > instl_boots [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
3	0.000494	130.235.201.241	130.235.203.249	TCP	instl_boots > https [ACK] Seq=1 Ack=1 win=17520 Len=0
4	0.001074	130.235.201.241	130.235.203.249	SSL	Client Hello
5	0.001341	130.235.203.249	130.235.201.241	TCP	https > instl_boots [ACK] Seq=1 Ack=141 Win=6432 Len=0
6	0.005269	130.235.203.249	130.235.201.241	TLSv1	Server Hello,
7	0.005838	130.235.203.249	130.235.201.241	TLSv1	Certificate, Server Hello Done
8	0.006480	130.235.201.241	130.235.203.249	TCP	instl_boots > https [ACK] Seq=141 Ack=1895 Win=17520 Len=0
9	0.012905	130.235.201.241	130.235.203.249	TLSv1	Alert (Level: Fatal, Description: unknown CA)
10	0.013244	130.235.201.241	130.235.203.249	TCP	instl_boots > https [RST, ACK] Seq=148 Ack=1895 Win=0 Len=0
11	0.072262	130.235.201.241	130.235.203.249	TCP	instl_bootc > https [SYN] Seq=0 win=16384 Len=0 MSS=1460
12	0.072706	130.235.203.249	130.235.201.241	TCP	https > instl_bootc [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
13	0.072751	130.235.201.241	130.235.203.249	TCP	instl_bootc > https [ACK] Seq=1 Ack=1 win=17520 Len=0

El cliente emitió una alerta con un error fatal de CA desconocida al servidor, sólo porque el cliente no pudo verificar el certificado enviado por el servidor.

Hay dos posibilidades:

1) CUCM envía la alerta CA desconocida

- Verifique que el certificado raíz de CUC actual se carga en el servidor que se comunica con el servidor CUC.
- Asegúrese de que el servicio CallManager se reinicie en el servidor correspondiente.

2) CUC envía la alerta CA desconocida

- Verifique que la dirección IP TFTP se ingresa correctamente en la configuración **Port Group > Edit > Servers** en el servidor CUC.
- Verifique que el servidor TFTP de CUCM esté accesible desde el servidor Connection.
- Asegúrese de que el archivo CTL en CUCM TFTP esté actualizado (compare el resultado de "show ctl" con los certificados tal como se ven en la página de administración del sistema operativo). Vuelva a ejecutar CTLClient si no lo es.
- Reinicie el servidor CUC O elimine y vuelva a crear el grupo de puertos para volver a descargar el archivo CTL del TFTP de CUCM.

Caso 2: No se puede descargar el archivo CTL desde CUCM TFTP

Este error se ve en los seguimientos del administrador de conversaciones:

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving server certificates.
MiuGeneral,25,Error executing tftp command 'tftp://10.48.47.189:69/CTLFile.tlv' res=68 (file not found on server)
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving server certificates.
Arbiter,-1,Created port PhoneSystem-1-001 objectId='7c2e86b8-2d86-4403-840e-16397b3c626b' as ID=1
```

```
MiuGeneral,25,Port group object 'b1c966e5-27fb-4eba-a362-56a5fe9c2be7' exists
MiuGeneral,25,FAILED SetInService=true parent port group is out of service:
```

Solución:

1. Verifique dos veces que el servidor TFTP sea correcto en la configuración **Port group > Edit > Servers**.
2. Verifique que el clúster de CUCM esté en modo seguro.
3. Verifique que el archivo CTL exista en CUCM TFTP.

Caso 3: Los puertos no se registran

Este error se ve en los seguimientos del administrador de conversaciones:

```
MiuSkinny,23,Failed to retrieve Certificate for CCM Server <CUCM IP Address>
MiuSkinny,23,Failed to extract any CCM Certificates - Registration cannot proceed. Starting
retry timer -> 5000 msec
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxxx.tlv]
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM
IP Address>' in CTL File
```

Solución:

1. Esto se debe probablemente a una discordancia en la suma de comprobación md5 del archivo CTL en CUCM y CUC como resultado de la regeneración de certificados. Reinicie el servidor CUC para actualizar el archivo CTL.

Información interna de Cisco

Alternativamente, puede quitar el archivo CTL de la raíz como se muestra a continuación:

Elimine el archivo CTL de la carpeta /tmp/ y restablezca el grupo de puertos. Puede realizar una suma de comprobación md5 en el archivo

y comparar antes de eliminarlo:

```
CUCM: [root@vfrscucm1 trust-certs]# md5sum /usr/local/cm/tftp/CTLFile.tlv
e5bf2ab934a42f4d8e6547dfd8cc82e8 /usr/local/cm/tftp/CTLFile.tlv
```

```
CUC: [root@vstscuc1 tmp]# cd /tmp
```

```
[root@vstscuc1 tmp]# ls -al *tlv
```

```
-rw-rw-r--. 1 cucsmgr cuservice 6120 Feb 5 15:29 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

```
[root@vstscuc1 tmp]# md5sum a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

e5bf2ab934a42f4d8e6547dfd8cc82e8 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

Además, puede consultar esta guía de resolución de problemas:

Defectos

[CSCum48958](#) - CUCM 10.0 (la longitud de la dirección IP es incorrecta)

[CSCtn87264](#) - La conexión TLS falla para los puertos SIP seguros

[CSCur10758](#) - No se pueden purgar los certificados revocados Unity Connection

[CSCur10534](#) - CUCM redundante entre operaciones de Unity Connection 10.5 TLS/PKI

[CSCve47775](#) - Solicitud de función para un método para actualizar y revisar el CTLFile de CUCM en el CUC