

Configurar e solucionar problemas de integração segura entre CUCM e CUC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Diagrama](#)

[Configurar - Tronco SIP seguro](#)

[Configurar CUC](#)

[1. Adicionar certificado SIP](#)

[2. Criar novo sistema de telefone ou modificar o padrão](#)

[3. Adicionar um novo grupo de portas](#)

[4. Editar servidores](#)

[5. Redefina o grupo de portas](#)

[6. Adicionar portas de correio de voz](#)

[7. Fazer download do certificado raiz CUC](#)

[Configurar CUCM](#)

[1. Configurar o perfil de segurança do tronco SIP para o tronco em direção ao CUC](#)

[2. Configurar perfil SIP](#)

[3. Criar tronco SIP](#)

[4. Criar um padrão de rota](#)

[5. Crie um piloto de correio de voz](#)

[6. Criar perfil de correio de voz](#)

[7. Atribuir perfil de correio de voz aos DN's](#)

[8. Carregar certificado raiz CUC como CallManager-trust](#)

[Configurar portas SCCP seguras](#)

[Configurar CUC](#)

[1. Fazer download do certificado raiz CUC](#)

[2. Crie um sistema telefônico/modifique o que existe.](#)

[3. Adicionar um novo grupo de portas SCCP](#)

[4. Editar servidores](#)

[5. Adicionar portas SCCP seguras](#)

[Configurar CUCM](#)

[1. Adicionar portas](#)

[2. Carregar certificado raiz CUC como CallManager-trust](#)

[3. Configurar extensões de ativação/desativação de MWI \(Message Waiting Information, informações de espera de mensagem\)](#)

[4. Criar piloto de correio de voz](#)

[5. Criar perfil de correio de voz](#)

[6. Atribuir perfil de correio de voz aos DN's](#)

[7. Criar um grupo de busca de correio de voz](#)

[Verificar](#)

[Verificação de portas SCCP](#)

[Verificação de tronco SIP seguro](#)

[Verificação de chamada RTP segura](#)

[Troubleshoot](#)

[1. Dicas gerais de solução de problemas](#)

[2. Rastreios para coletar](#)

[Problemas comuns](#)

[Caso 1: Não é possível estabelecer uma conexão segura \(alerta de CA desconhecido\)](#)

[Caso 2: Não é possível baixar o arquivo CTL do CUCM TFTP](#)

[Caso 3: As portas não se registram](#)

[Defeitos](#)

Introduction

Este documento descreve a configuração, verificação e solução de problemas da conexão segura entre o servidor Cisco Unified Communication Manager (CUCM) e o servidor Cisco Unity Connection (CUC).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do CUCM.

Consulte o [Guia de Segurança do Cisco Unified Communications Manager](#) para obter mais detalhes.

Note: Ele deve ser definido para o modo misto para que a integração segura funcione corretamente.

A criptografia deve ser habilitada para Unity Connection 11.5(1) SU3 ou posterior.

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

Componentes Utilizados

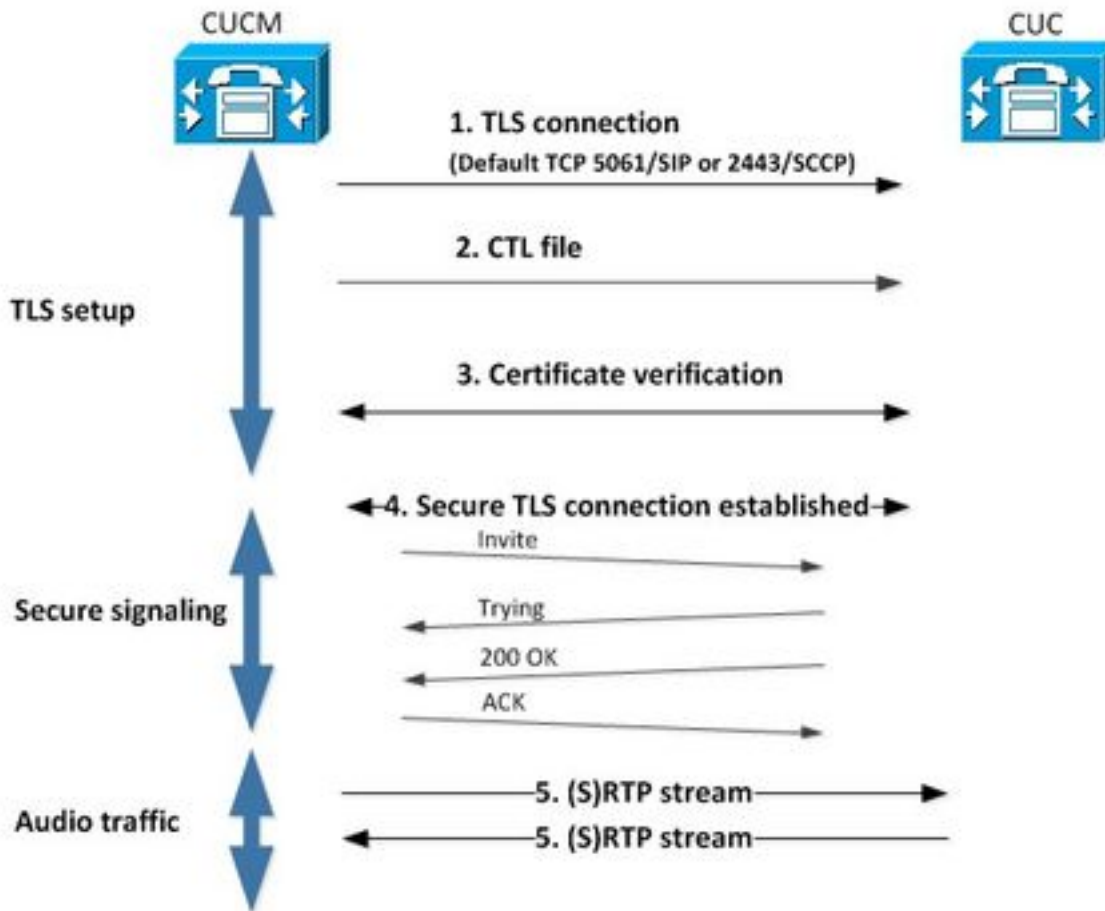
As informações neste documento são baseadas nestas versões de software e hardware:

- CUCM versão 10.5.2.11900-3.
- CUC versão 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 o processo que ajuda a estabelecer uma conexão segura entre o CUCM e o CUC:



1. O Call Manager configura uma conexão TLS (Transport Layer Security) segura para o servidor CUC na porta 2443 Skinny Call Control Protocol (SCCP) ou no SIP (Session Initiation Protocol) 5061 no protocolo usado para integração.

2. O servidor CUC faz o download do arquivo CTL (Certificate Trust List) do servidor TFTP (processo único), extrai o certificado CallManager.pem e o armazena.

3. O servidor CUCM oferece o certificado Callmanager.pem que é verificado em relação ao certificado CallManager.pem obtido na etapa anterior. Além disso, o certificado CUC está sendo verificado em um certificado raiz CUC armazenado no CUCM. Observe que o certificado raiz deve ser carregado no CUCM pelo administrador.

4. Se a verificação dos certificados for bem-sucedida, uma conexão TLS segura é estabelecida. Essa conexão é usada para trocar a sinalização SCCP ou SIP criptografada.

5. O tráfego de áudio pode ser trocado como Real-time Transport Protocol (RTP) ou SRTP.

Note: Quando você estabelece uma comunicação TLS, o CUCM e o CUC usam autenticação mútua TLS. Consulte RFC5630 para obter mais informações.

Configurar - Tronco SIP seguro

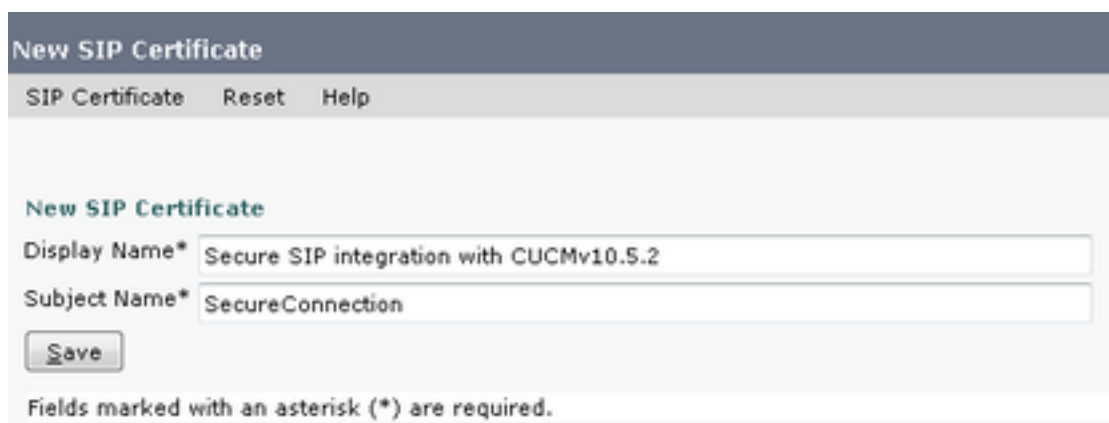
Configurar CUC

1. Adicionar certificado SIP

Navegue até **CUC Administration > Telephony Integrations > Security > SIP Certificate > Add new**

- Nome de exibição: <qualquer nome significativo>
- Nome do assunto: <qualquer nome, por exemplo, **SecureConnection**>

Observação: o nome do assunto deve corresponder ao nome do assunto X.509 no perfil de segurança do tronco SIP (configurado na etapa 1 da configuração do CUCM posteriormente neste documento).



New SIP Certificate

SIP Certificate Reset Help

New SIP Certificate

Display Name* Secure SIP integration with CUCMv10.5.2

Subject Name* SecureConnection

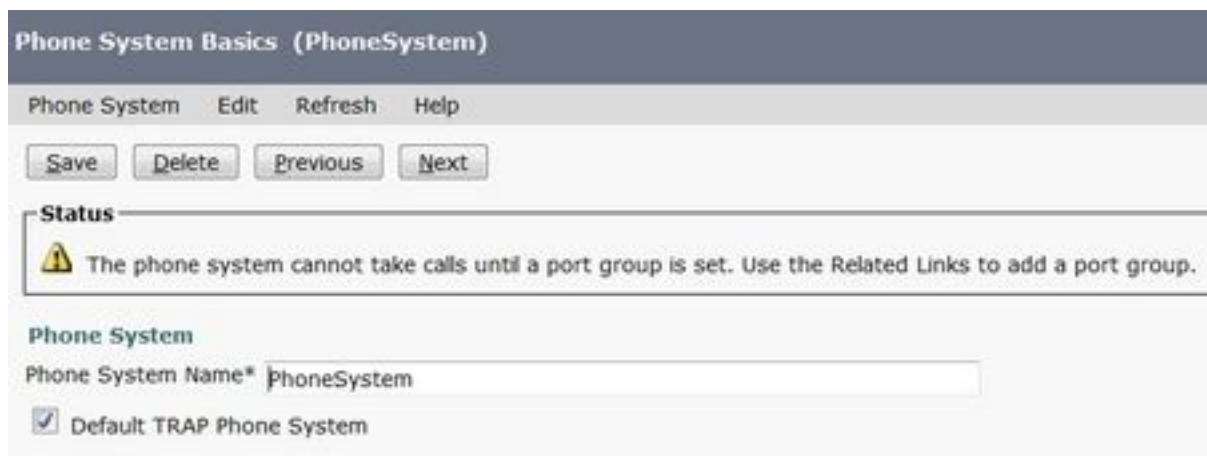
Save

Fields marked with an asterisk (*) are required.

Note: O certificado é gerado e assinado pelo certificado raiz CUC.

2. Criar novo sistema de telefone ou modificar o padrão

Navegue até **Telephony Integration > Phone System**. Você pode usar o sistema telefônico que já existe ou criar um novo.




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. Adicionar um novo grupo de portas

Na página Opções básicas do sistema telefônico, na caixa suspensa Links relacionados, selecione Adicionar grupo de portas e selecione Ir. Na janela de configuração, insira estas informações:

- Sistema telefônico:
- Criar de: Tipo de grupo de portas SIP
- SIP Security Profile: 5061/TLS
- Certificado SIP:
- Modo de segurança: criptografado
- RTP seguro: verificado
- Endereço IPv4 ou nome do host:

Clique em Salvar.

New Port Group

Port Group Reset Help

New Port Group

Phone System Secure SIP integration ▼

Create From Port Group Type SIP ▼

Port Group ▼

Port Group Description

Display Name*

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

IPv6 Address or Host Name

Port

4. Editar servidores

Navegue para **Editar > Servidores** e adicione o servidor TFTP do cluster CUCM como mostrado

nesta imagem.

The image displays two screenshots of a configuration interface. The top screenshot is titled "SIP Servers" and shows a table with two columns: "Order" and "IPv4 Address or Host Name". The first row contains the value "0" in the "Order" column and "10.48.47.110" in the "IPv4 Address or Host Name" column. Below the table are "Delete Selected" and "Add" buttons. The bottom screenshot is titled "TFTP Servers" and shows a similar table with the same data: "0" in the "Order" column and "10.48.47.110" in the "IPv4 Address or Host Name" column. It also includes "Delete Selected" and "Add" buttons.

Note: É importante fornecer o endereço TFTP correto. O servidor CUC faz o download do arquivo CTL desse TFTP conforme explicado.

5. Redefina o grupo de portas

Volte para o **Port Group Basics** e redefina o grupo de portas conforme solicitado pelo sistema, como mostrado nesta imagem.

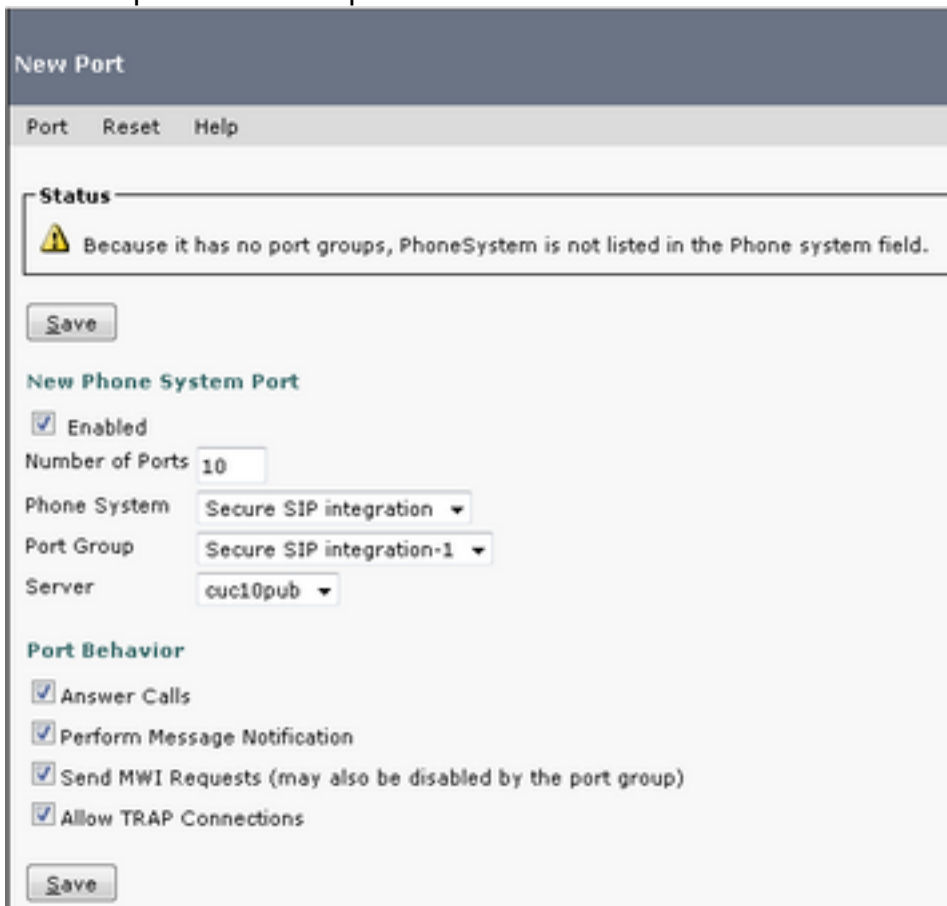
The screenshot shows the "Port Group Basics (Secure SIP integration-1)" configuration page. At the top, there are buttons for "Save", "Delete", "Previous", and "Next". Below this is a "Status" section with two warning icons and the following text: "The phone system cannot take calls if it has no ports. Use the Related Links to add ports." and "One or more port groups need to be reset." The "Port Group" section contains the following fields: "Display Name*" with the value "Secure SIP integration-1", "Integration Method" with the value "SIP", and "Reset Status" with the value "Reset Required" and a "Reset" button.

6. Adicionar portas de correio de voz

Na página Noções básicas do grupo de portas, na caixa suspensa Links relacionados, selecione **Adicionar portas** e selecione **Ir**. Na janela de configuração, insira estas informações:

- Habilitado: Verificado
- Número de portas:
- Sistema telefônico:

- Grupo de porta:
- Servidor:
- Comportamento da porta:



7. Fazer download do certificado raiz CUC

Navegue até **Telephony Integrations > Security > Root Certificate**, clique com o botão direito do mouse na URL para salvar o certificado como um arquivo chamado <filename>.0 (a extensão do arquivo deve ser .0 em vez de .htm)' e pressione save como mostrado nesta imagem.



Configurar CUCM

1. Configurar o perfil de segurança do tronco SIP para o tronco em direção ao CUC

Navegue até **CUCM Administration > System > Security > SIP Trunk Security Profile > Add new**

Certifique-se de que estes campos estejam preenchidos corretamente:

- Modo de segurança do dispositivo: criptografado
- Nome do assunto X.509: SecureConnection>
- Aceitar referência fora do diálogo: marcada
- Aceitar notificação não solicitada: marcada
- Aceitar substituir cabeçalho: marcado

Note: O nome do assunto do X.509 deve corresponder ao campo Nome do assunto no certificado SIP no servidor do Cisco Unity Connection (configurado na etapa 1 da configuração do CUC).

The screenshot shows the configuration page for a SIP Trunk Security Profile. The title is "SIP Trunk Security Profile Information". The fields are as follows:

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

Navegue até **Device > Device Settings > SIP Profile** se precisar aplicar qualquer configuração específica. Caso contrário, você pode usar o perfil SIP padrão.

3. Criar tronco SIP

Vá para **Dispositivo > Tronco > Adicionar novo**. Crie um tronco SIP que será usado para a integração segura com o Unity Connection, como mostrado nesta imagem.

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

Na seção Informações do dispositivo da configuração de tronco, insira estas informações:

- Nome de dispositivo:
- Conjunto de dispositivos:
- SRTP permitido: verificado

Note: Verifique se o grupo do CallManager (na configuração do pool de dispositivos) contém todos os servidores configurados no CUC (**Grupo de portas > 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
<input type="checkbox"/> Media Termination Point Required	
<input checked="" type="checkbox"/> Retry Video Call as Audio	
<input type="checkbox"/> Path Replacement Support	
<input type="checkbox"/> Transmit UTF-8 for Calling Party Name	
<input type="checkbox"/> Transmit UTF-8 Names in QSIG APDU	
<input type="checkbox"/> Unattended Port	
<input checked="" type="checkbox"/> 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
<input type="checkbox"/> PSTN Access	
<input type="checkbox"/> Run On All Active Unified CM Nodes	

Na seção Chamadas de Entrada da configuração de tronco, insira estas informações:

- Espaço de pesquisa de chamada:
- Redirecionando entrega do cabeçalho de desvio - Entrada: marcada

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

Na saída Seção Chamadas da configuração do tronco, insira estas informações:

- Redirecionando a entrega do cabeçalho de desvio - Saída: verificado

Outbound Calls

Called Party Transformation CSS < None >

Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS < None >

Use Device Pool Calling Party Transformation CSS

Calling Party Selection* Originator

Calling Line ID Presentation* Default

Calling Name Presentation* Default

Calling and Connected Party Info Format* Deliver DN only in connected party

Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS < None >

Use Device Pool Redirecting Party Transformation CSS

Na seção SIP Information da configuração do tronco, insira estas informações:

- endereço de destino:
- Perfil de segurança do tronco SIP:
- Novo Roteamento do Espaço de Pesquisa de Chamada:
- Espaço de pesquisa de chamada fora de caixa de diálogo:
- Perfil SIP:

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.48.47.124		5061

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Secure_sip_trunk_profile_for_CUC

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile [View Details](#)

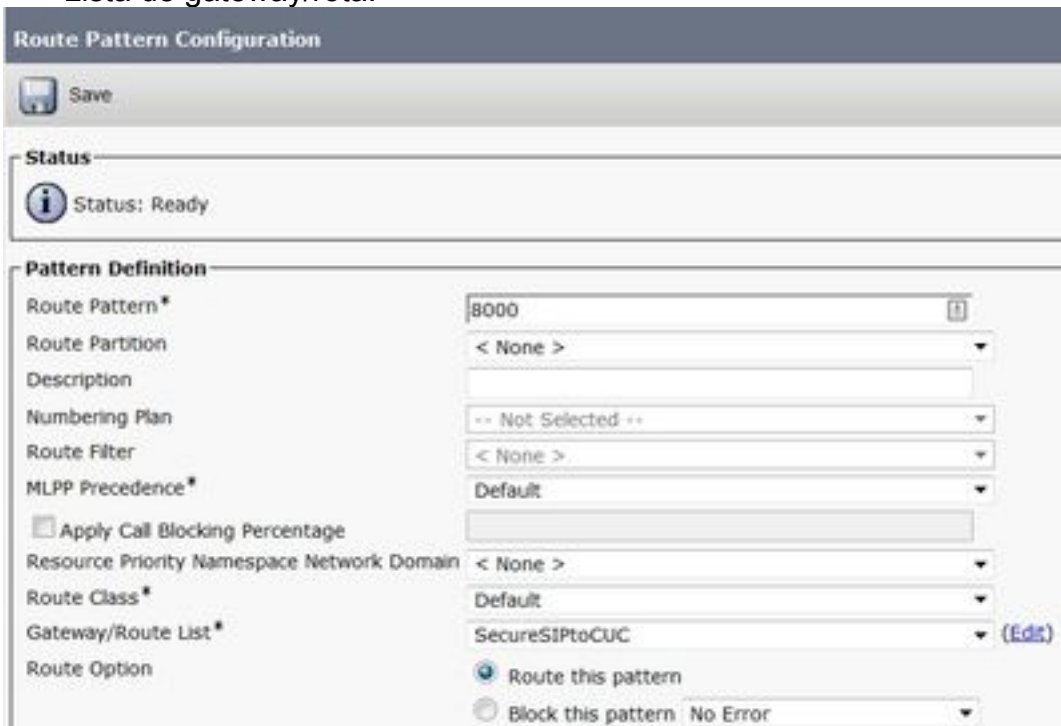
DTMF Signaling Method* No Preference

Ajuste outras configurações de acordo com seus requisitos.

4. Criar um padrão de rota

Crie um padrão de rota que aponte para o tronco configurado (**Roteamento de chamada > Rota/busca > Padrão de rota**). A extensão inserida como um número de padrão de rota pode ser usada como um piloto de correio de voz. Insira esta informação:

- Padrão de rota:
- Lista de gateway/rota:



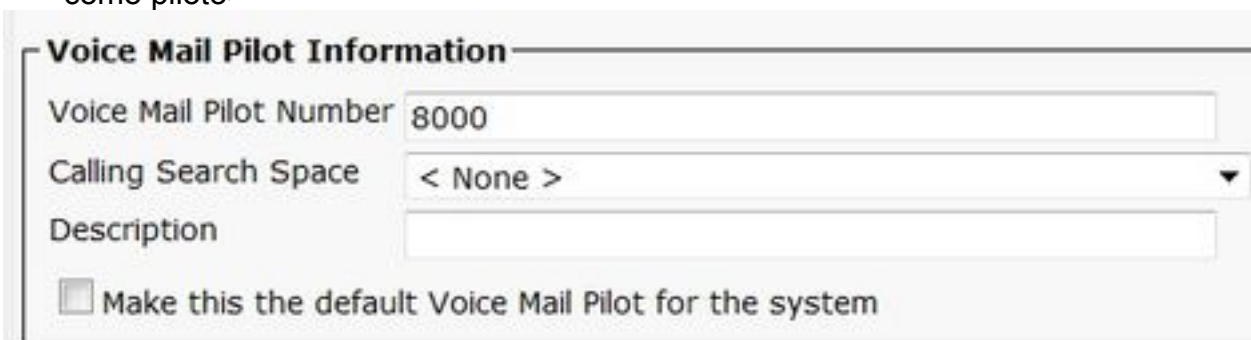
The screenshot shows the 'Route Pattern Configuration' window. At the top, there is a 'Save' button. Below it, the 'Status' section shows 'Status: Ready'. The main area is 'Pattern Definition', which includes the following fields and values:

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 (Eds)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error

5. Crie um piloto de correio de voz

Crie um piloto de correio de voz para a integração (**Recursos avançados > Correio de voz > Piloto de correio de voz**). Insira estes valores:

- Número piloto do correio de voz:
- Espaço de pesquisa de chamada: que inclui partições que contêm o padrão de rota usado como piloto>



The screenshot shows the 'Voice Mail Pilot Information' form. It contains the following fields and values:

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

6. Criar perfil de correio de voz

Crie um perfil de correio de voz para vincular todas as configurações (**Recursos avançados > Correio de voz > Perfil de correio de voz**). Insira as seguintes informações:

- Piloto de correio de voz:
- Máscara da caixa de correio 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. Atribuir perfil de correio de voz aos DNs

Atribua o perfil de correio de voz aos DNs destinados a usar uma integração segura. Não se esqueça de clicar no botão 'Aplicar configuração' após alterar as configurações de DN:

Navegue até: **Roteamento de chamada > Número do diretório** e altere o seguinte:

- 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 >

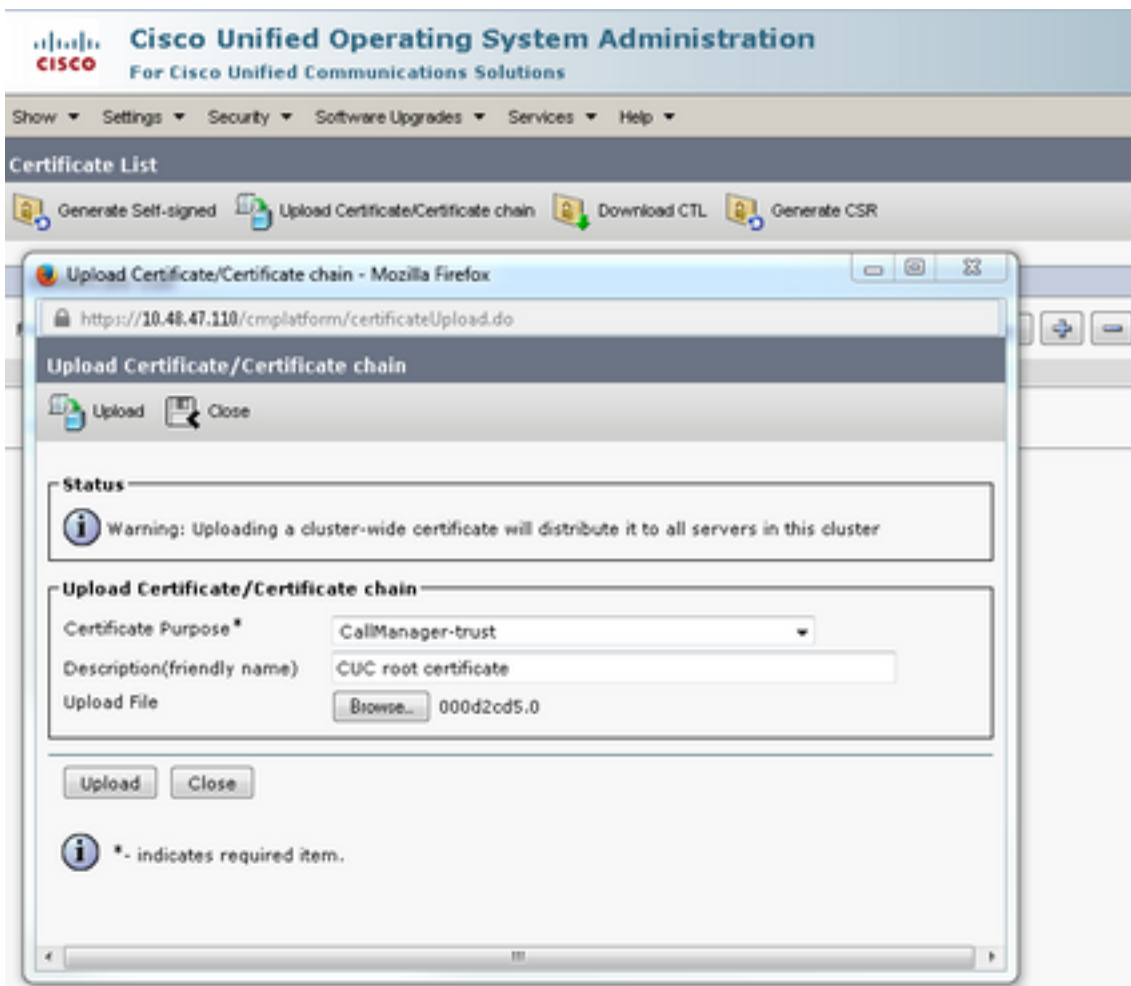
Network Hold MOH Audio Source < None >

Auto Answer* Auto Answer Off

Reject Anonymous Calls

8. Carregar certificado raiz CUC como CallManager-trust

Navegue até **OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain** e carregue o certificado raiz CUC como **CallManager-trust** em todos os nós configurados para se comunicar com o servidor CUC.



Observação: o serviço Cisco CallManager precisa ser reiniciado após o upload do certificado para que o certificado tenha efeito.

Configurar portas SCCP seguras

Configurar CUC

1. Fazer download do certificado raiz CUC

Navegue até **CUC Administration > Telephony Integration > Security > Root Certificate**. Clique com o botão direito do mouse na URL para salvar o certificado como um arquivo chamado <filename>.0 (a extensão do arquivo deve ser .0 em vez de .htm) e pressione **Salvar**:

Root Certificate for Cisco Unified Communications Manager Authentication and Encryption	
Subject	CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41
Issuer	CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41
Valid From	Tue Mar 31 08:59:34 CEST 2015
Valid Until	Fri Apr 01 08:59:34 CEST 2022
Version	2
File Name	57ed0e66.0
Serial Number	f6b8fb3369144dd39f18e064893aec42
Certificate Text	<pre>-----BEGIN CERTIFICATE----- MIICPDCCAaWgAwIBAgIRAPa++zNpFE3TnxjgZ1k67E1wDQYJKoZIhvcNAQEFBQAw OjE4MDYGA1UEAwwvQ2lzY29Vbml0eS01ZGFkMzJlYy1jYWZlLTQ1NTktOTc4Zj01 NmYyYzY4NTBkNDEwHhcNMTUwMzY1OTM0WWhcNMjEwNDAxMDY1OTM0WjA6MTgw NgYDVQDDC9D0aXNjb1VuaXR5LTk5Y29Vbml0eS01ZGFkMzJlYy1jYWZlLTQ1NTkt OjE4MDYGA1UEAwwvQ2lzY29Vbml0eS01ZGFkMzJlYy1jYWZlLTQ1NTktOTc4Zj01 Njg1MGQ0MTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoBOBg/qh8cWQx457 Q47eGUWcR2jeyE726RTO40GkdhDYI4Km6ouSeMiGbs757WpvtspKp+zeSDjVm2j4 B1lxG9wM3XgPPwM+3QIMh0NQLARuJdm9g2/5uiHB6/1k82Po0Wrv2r6Anoragrv Md3ordaCB3mG1u2g0GqXj9GChf0CAwEAANCMEEAwEgYDVR0TAQH/BAgwBgEB/wIB ADAdBgNVHQ4EFgQU438N5JYGHhgp7qm2dUmu+HGkM8wCwYDVR0PBAQDAGKsMA0G CSqGSIb3DQEBBQUAA4GBAGPhrFt6GH2a0iXV8bnKvC12f5ty1eTeMD6ZzD62P4C6 RtGM88WqGU1IAZw1www0nxdetKzZvJX2z2Ksu2ptVUnFPMzSc+xloJv7vmJq52px TcD/Ti0efckXlc+vACWlu4wlv20SHxsoto9CiiXqsKQ7e/zyYHu152zTOQeYvAES -----END CERTIFICATE-----</pre>
Private Key	Hk2Pzp3YnX3/9ghz1r8v1VgMpSLr8HZ8XW/VXIL342IudK3G1GwnZ1IMvhztq/zEseh2ELON

Right click to save the certificate as a file named 57ed0e66.0 (the file extension must be .0 rather than .htm)

2. Crie um sistema telefônico/modifique o que existe.

Navegue até **Telephony Integration > Phone system**. Você pode usar o sistema telefônico que já existe ou criar um novo.

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*

Default TRAP Phone System


3. Adicionar um novo grupo de portas SCCP


Na página Opções básicas do sistema telefônico, na caixa suspensa Links relacionados, selecione **Adicionar grupo de portas** e selecione **Ir**. Na janela de configuração, insira estas informações:

- Sistema telefônico:
- Tipo de grupo de portas: SCCP
- Prefixo do nome do dispositivo*: CiscoUM1-VI
- MWI no ramal:
- Ramal MWI desligado:

Note: Essa configuração deve corresponder à configuração no 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 até **Edit > Servers** e adicione o servidor TFTP do cluster 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"/>		


Note: É importante fornecer o endereço TFTP correto. O servidor CUC faz o download do arquivo CTL desse TFTP conforme explicado.

5. Adicionar portas SCCP seguras

Na página Noções básicas do grupo de portas, na caixa suspensa Links relacionados, selecione **Adicionar portas** e selecione **Ir**. Na janela de configuração, insira estas informações:

- Habilitado: verificado
- Número de portas:
- Sistema telefônico:
- Grupo de porta:
- Servidor:
- Comportamento da porta:
- Modo de segurança: **criptografado**

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

Configurar CUCM

1. Adicionar portas

Navegar para **Administração do CUCM > Recursos avançados > Configuração de porta de correio de voz > Adicionar novo.**

Configure as portas de correio de voz SCCP como de costume. A única diferença está no modo de segurança do dispositivo na configuração de porta em que a opção Porta de correio de voz criptografado precisa ser selecionada.

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 >

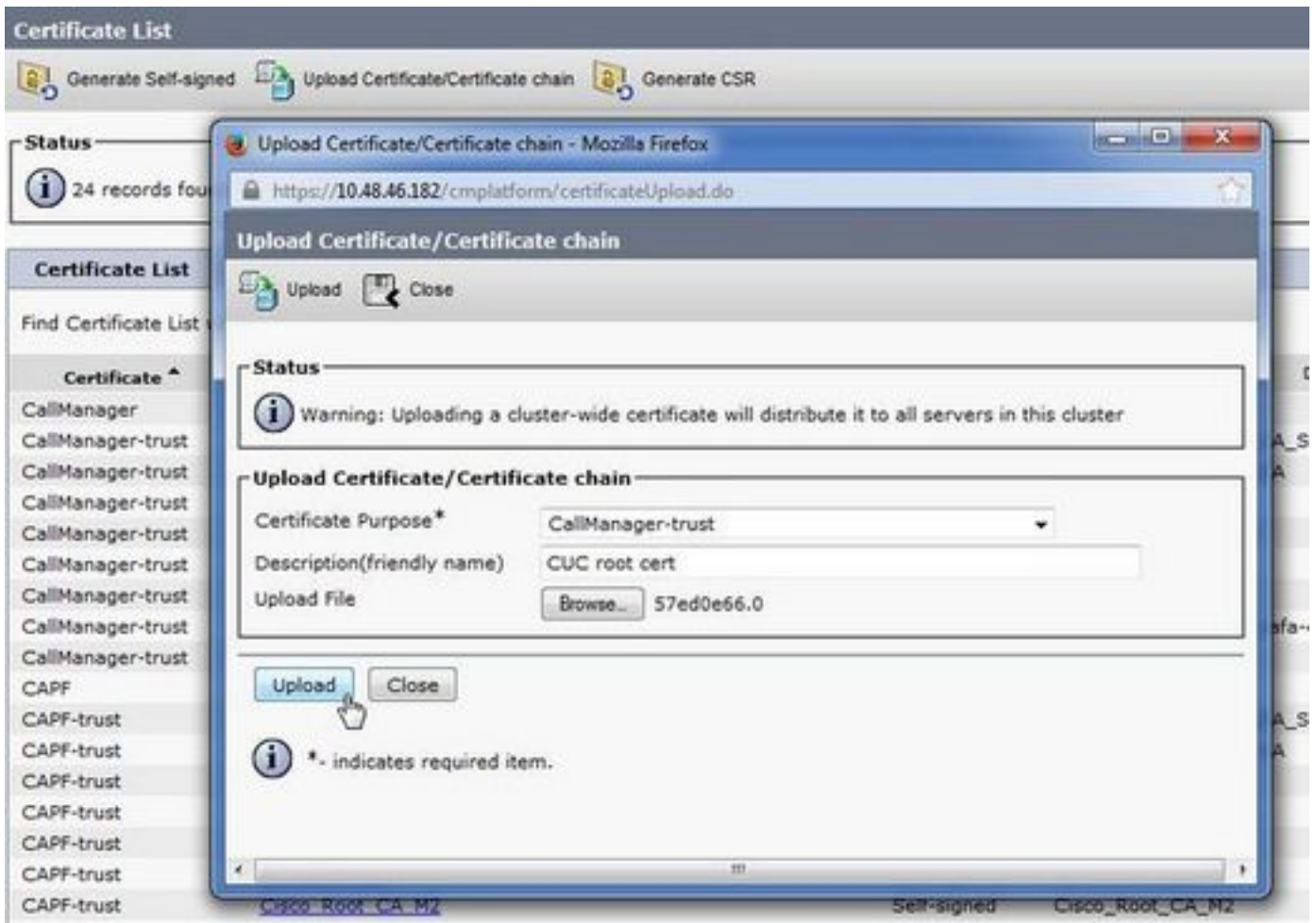
Directory Number Information

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. Carregar certificado raiz CUC como CallManager-trust

Navegue até **OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain** e carregue o certificado raiz CUC como **CallManager-trust** em todos os nós configurados para se comunicar com o servidor CUC.



Observação: o serviço Cisco CallManager precisa ser reiniciado após o upload do certificado para que o certificado tenha efeito.

3. Configurar extensões de ativação/desativação de MWI (Message Waiting Information, informações de espera de mensagem)

Navegue até **CUCM Administration > Advanced Features > Voice Mail Port Configuration** e configure **MWI On/Off Extensions**. Os números MWI devem corresponder à configuração do 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 >

4. Criar piloto de correio de voz

Crie um piloto de correio de voz para a integração (**Recursos avançados > Correio de voz > Piloto de correio de voz**). Insira estes valores:

- Número piloto do correio de voz:
- Espaço de pesquisa de chamada: que inclui partições que contêm o padrão de rota usado 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. Criar perfil de correio de voz

Crie um perfil de correio de voz para vincular todas as configurações (**Recursos avançados > Correio de voz > Perfil de correio de voz**). Insira esta informação:

- Piloto de correio de voz:
- Máscara da caixa de correio 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

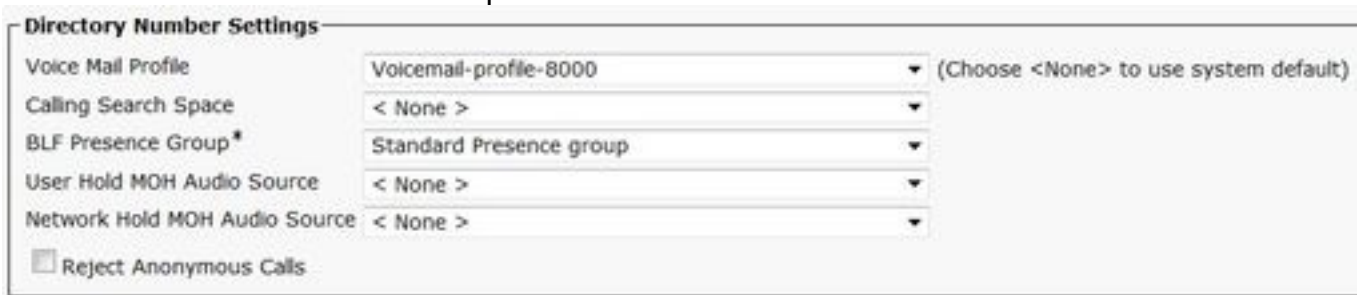
Make this the default Voice Mail Profile for the System

6. Atribuir perfil de correio de voz aos DN's

Atribua o perfil de correio de voz aos DN's que pretendem usar uma integração segura. Clique no botão **Apply Config** depois que as configurações de DN forem alteradas:

Navegue até **Roteamento de chamada > Número do diretório** e altere para:

- Voice Mail Profile: Voicemail-profile-8000



The screenshot shows the 'Directory Number Settings' configuration page. It includes several dropdown menus and a checkbox:

- 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. Criar um grupo de busca de correio de voz

a) Adicionar um novo grupo de linhas (Roteamento de chamadas > Rota/busca > Grupo de linhas)



The screenshot shows the 'Line Group Information' configuration page with the following fields:

- Line Group Name*:** voicemail-ig
- RNA Reversion Timeout*:** 10
- Distribution Algorithm*:** Longest Idle Time

b) Adicionar uma nova lista de busca de correio de voz (Roteamento de chamada > Rota/busca > Lista de busca)



The screenshot shows the 'Hunt List Information' configuration page with the following fields and checkboxes:

- Device is trusted**
- Name*:** voicemail-hi
- Description:** (empty field)
- Cisco Unified Communications Manager Group*:** Default
- Enable this Hunt List (change effective on Save; no reset required)**
- For Voice Mail Usage**

c) Adicionar um novo piloto de busca (Roteamento de chamada > Rota/busca > piloto de busca)

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

Route this pattern

Block this pattern No Error

Verificar

Verificação de portas SCCP

Navegue até **CUCM Administration > Advance Features > Voice Mail > Voice Mail Ports** e verifique o registro da porta.

Find and List Voice Mail Ports

Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

Status

0 records found

Voice Mail Port (1 - 8 of 8)

Find Voice Mail Port where Device Name Regime with Find Clear Filter Use

Device Name	Description	Device Pool	Device Security Mode	Calling Search Space	Extension	Partition	Status	IP Address	Clear
CiscoSIP-001	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port	999001	999001	Registered with 10.48.46.182	10.48.46.184		
CiscoSIP-002	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port	999002	999002	Registered with 10.48.46.182	10.48.46.184		
CiscoSIP-003	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port	999003	999003	Registered with 10.48.46.182	10.48.46.184		
CiscoSIP-004	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port	999004	999004	Registered with 10.48.46.182	10.48.46.184		
CiscoSIP-005	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port	999005	999005	Registered with 10.48.46.182	10.48.46.184		
CiscoSIP-006	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port	999006	999006	Registered with 10.48.46.182	10.48.46.184		
CiscoSIP-007	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port	999007	999007	Registered with 10.48.46.182	10.48.46.184		
CiscoSIP-008	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port	999008	999008	Registered with 10.48.46.182	10.48.46.184		

Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

Pressione o botão **Correio de Voz** no telefone para chamar o correio de voz. Você deve ouvir a saudação de abertura se o ramal do usuário não estiver configurado no sistema do Unity Connection.

Verificação de tronco SIP seguro

Pressione o botão **Correio de Voz** no telefone para chamar o correio de voz. Você deve ouvir a saudação de abertura se o ramal do usuário não estiver configurado no sistema do Unity Connection.

Como alternativa, você pode habilitar o keepalive das OPÇÕES SIP para monitorar o status do tronco SIP. Essa opção pode ser ativada no perfil SIP atribuído ao tronco SIP. Depois que isso estiver ativado, você poderá monitorar o status do tronco Sip por meio de **Dispositivo > Tronco**, como mostrado nesta imagem.

Trunks (1 - 1 of 1)										
Find Trunks where: Device Name begins with [] Find Clear Filter [] []										
Select item or enter search text []										
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

Verificação de chamada RTP segura

Verifique se o ícone de cadeado está presente em chamadas para o Unity Connection. Significa que o fluxo de RTP é criptografado (o perfil de segurança do dispositivo deve ser seguro para que funcione) como mostrado nesta imagem.



Troubleshoot

1. Dicas gerais de solução de problemas

Siga estas etapas para solucionar problemas da integração segura:

- Verificar a configuração.
- Verifique se todos os serviços relacionados estão em execução. (CUCM - CallManager, TFTP, CUC - Gerenciador de conversação)
- Certifique-se de que as portas necessárias para comunicação segura entre servidores estejam abertas na rede (porta TCP 2443 para integração SCCP e TCP 5061 para integração SIP).
- Se tudo isso estiver correto, continue com a coleta de rastreamentos.

2. Rastreios para coletar

Colete esses rastreamentos para solucionar problemas da integração segura.

- Captura de pacote do CUCM e CUC
- Rastreamentos do CallManager

- Rastreamentos do Cisco Conversation Manager

Consulte estes recursos para obter informações adicionais sobre:

Como fazer uma captura de pacote no CUCM:

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

Como ativar rastreamentos no servidor CUC:

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

Problemas comuns

Caso 1: Não é possível estabelecer uma conexão segura (alerta de CA desconhecido)

Depois que a captura de pacote é coletada de um dos servidores, a Sessão TLS é estabelecida.

```

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

```

O cliente emitiu um alerta com um erro fatal de CA desconhecida para o servidor, apenas porque o cliente não pôde verificar o certificado enviado pelo servidor.

Há duas possibilidades:

1) O CUCM envia o alerta CA desconhecida

- Verifique se o certificado raiz atual do CUC está carregado no servidor que se comunica com o servidor CUC.
- Verifique se o serviço CallManager foi reiniciado no servidor correspondente.

2) O CUC envia o alerta CA desconhecida

- Verifique se o endereço IP TFTP foi inserido corretamente na configuração **Port Group > Edit > Servers** no servidor CUC.
- Verifique se o servidor TFTP do CUCM está acessível a partir do servidor do Connection.
- Verifique se o arquivo CTL no CUCM TFTP está atual (compare a saída de "show ctl" com os certificados conforme visto na página do OS Admin). Execute novamente o CTLClient, se não estiver.
- Reinicialize o servidor CUC OU exclua e recrie o grupo de portas para fazer o download do arquivo CTL do TFTP do CUCM.

Caso 2: Não é possível baixar o arquivo CTL do CUCM TFTP

Esse erro é visto nos rastreamentos do Gerenciador de conversas:

```
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:
```

Solução:

1. Verifique duas vezes se o servidor TFTP está correto no **grupo Porta > Editar > Configuração de servidores**.
2. Verifique se o cluster CUCM está no modo seguro.
3. Verifique se o arquivo CTL existe no TFTP do CUCM.

Caso 3: As portas não se registram

Esse erro é visto nos rastreamentos do Gerenciador de conversas:

```
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-xxxxxxxxxxxx.tlv]
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM IP Address>' in CTL File
```

Solução:

1. Isso provavelmente se deve à incompatibilidade no checksum md5 do arquivo CTL no CUCM e CUC como resultado da regeneração de

certificados. Reinicie o servidor CUC para atualizar o arquivo CTL.

Informações internas da Cisco

Como alternativa, você pode remover o arquivo CTL da raiz da seguinte maneira:

Exclua o arquivo CTL da pasta /tmp/ e redefina o grupo de portas. Você pode fazer uma soma de verificação md5 no arquivo

e compare antes de excluí-lo:

```
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 fev 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
```

Além disso, você pode consultar este guia de solução de problemas:

Defeitos

[CSCum48958](#) - CUCM 10.0 (o comprimento do endereço ip está incorreto)

[CSCtn87264](#) - Falha na conexão TLS para portas SIP seguras

[CSCur10758](#) - Não é possível limpar os certificados revogados do Unity Connection

[CSCur10534](#) - Unity Connection 10.5 TLS/PKI Inter-op Redundante CUCM

[CSCve47775](#) - Solicitação de recurso para um método para atualizar e revisar o arquivo CTLF do CUCM no CUC