

Exemplo de configuração para a integração SIP segura entre CUCM e CUC com base na criptografia de última geração (NGE)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Diagrama de Rede](#)

[Requisitos de certificado](#)

[cifras baseadas em chave RSA negociadas](#)

[Cifras com base na chave CE negociadas](#)

[Configurar - Cisco Unity Connection \(CUC\)](#)

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

[2. Adicionar a referência do servidor TFTP](#)

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

[4. Fazer upload da raiz do CUCM e do certificado intermediário da CA de terceiros](#)

[Configurar - Cisco Unified CM \(CUCM\)](#)

[1. Criar um perfil de segurança de tronco SIP](#)

[2. Criar um tronco SIP seguro](#)

[3. Configurar cifras TLS e SRTP](#)

[4. Carregar certificados CUC Tomcat \(com base em RSA e EC\)](#)

[5. Criar padrão de rota](#)

[6. Criar piloto de correio de voz, perfil de correio de voz e atribuí-lo aos DNS](#)

[Configurar - Assinatura de certificados com base na chave EC por CA de terceiros \(opcional\)](#)

[Verificar](#)

[Verificação de tronco SIP seguro](#)

[Verificação de chamada RTP segura](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve a configuração e a verificação da conexão SIP segura entre o servidor do Cisco Unified Communication Manager (CUCM) e do Cisco Unity Connection (CUC) usando a criptografia de próxima geração.

A segurança de próxima geração na interface SIP restringe a interface SIP a usar cifras do Suite B com base nos protocolos TLS 1.2, SHA-2 e AES256. Permite as várias combinações de cifras com base na ordem de prioridade de cifras RSA ou ECDSA. Durante a comunicação entre o Unity Connection e o Cisco Unified CM, tanto cifras quanto certificados de terceiros são verificados em ambas as extremidades. Abaixo está a configuração do suporte à criptografia de última geração.

Se você planeja usar os certificados assinados por uma autoridade de certificação de terceiros, comece com a assinatura do certificado no final da seção de configuração (Configurar - Assinatura dos certificados com base na chave EC por uma autoridade de certificação de terceiros)

Prerequisites

Requirements

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

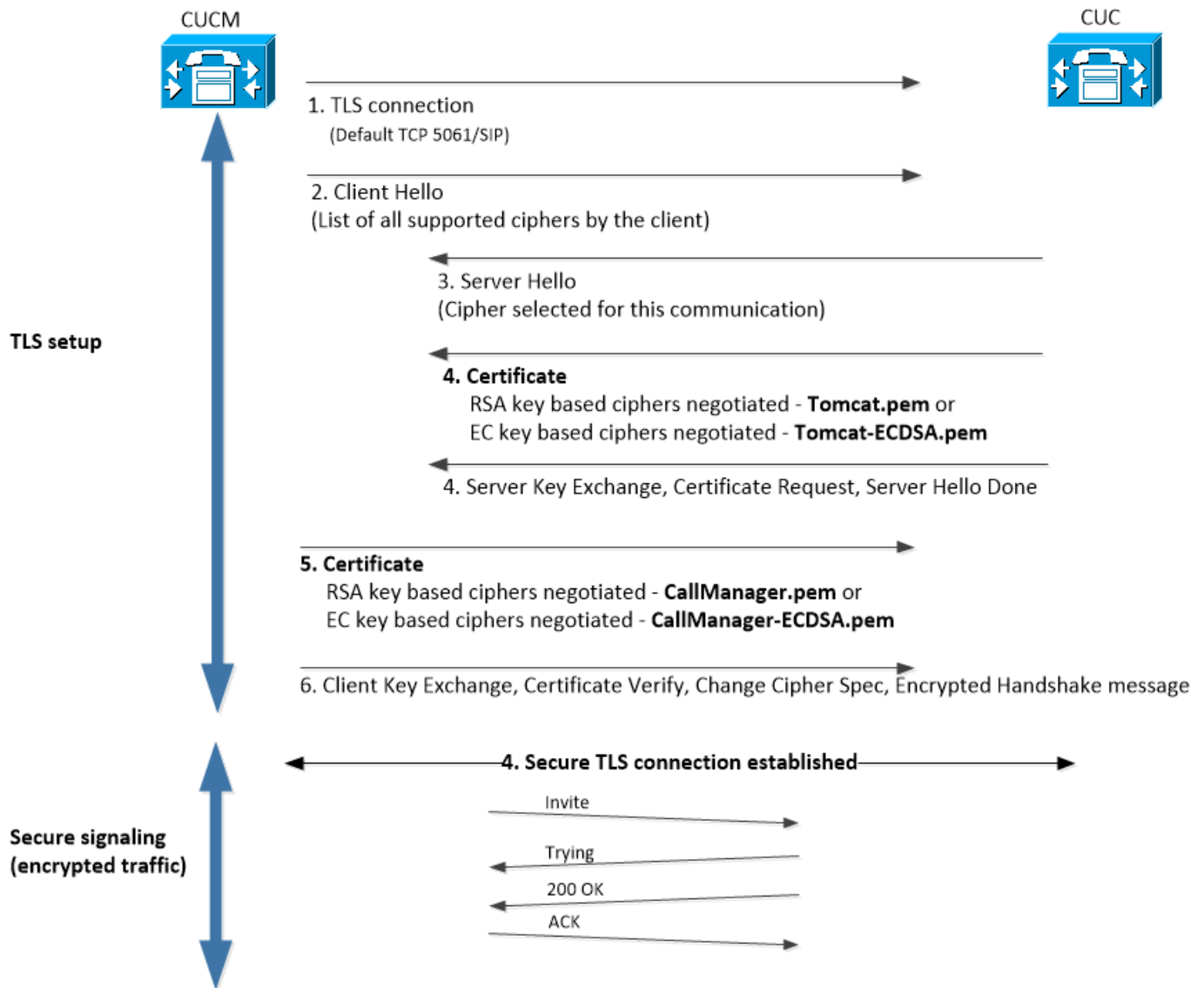
CUCM versão 11.0 e posterior no modo misto

CUC versão 11.0 e posterior

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

Diagrama de Rede

Este diagrama explica brevemente o processo que ajuda a estabelecer uma conexão segura entre o CUCM e o CUC quando o suporte à criptografia de última geração estiver ativado:



Requisitos de certificado

Esses são os requisitos de troca de certificado quando o suporte à criptografia de última geração é ativado no Cisco Unity Connection.

• cifras baseadas em chave RSA negociadas

certificado CUCM usado	certificado CUC usado	Certificados a serem carregados no CUCM	Certificados a serem carregados no CUC
CallManager.pem (autoassinado)	Tomcat.pem (autoassinado)	Tomcat.pem a ser carregado no CUCM > CallManager-trust	Nenhum.
CallManager.pem (CA assinado)	Tomcat.pem (CA assinado)	Certificado CA raiz e intermediário do CUC ^{*1} a ser carregado no CUCM > CallManager-trust	Certificado CA raiz e intermediário do CUCM ^{*2} a ser carregado no CUC > CallManager-trust.
CallManager.pem (CA assinado)	Tomcat.pem (autoassinado)	Tomcat.pem a ser carregado no CUCM > CallManager-trust	Certificado CA raiz e intermediário do CUCM a ser carregado no CUC > CallManager-trust.
CallManager.pem	Tomcat.pem (CA	Certificado CA raiz e	Nenhum.

(autoassinado) assinado) intermediário do CUC a ser carregado no CUCM > CallManager-trust

*1 O certificado CA raiz e intermediário do CUC refere-se ao certificado CA que assinou o certificado Tomcat de conexão Unity (Tomcat.pem).

*2 Certificado CA raiz e intermediário do CUCM refere-se ao certificado CA que assinou o certificado do CUCM CallManager (Callmanager.pem).

• **Cifras com base na chave CE negociadas**

certificado CUCM usado	certificado CUC usado	Certificados a serem carregados no CUCM	Certificados a serem carregados no CUC
CallManager-ECDSA.pem (autoassinado)	Tomcat-ECDSA.pem (autoassinado)	Tomcat-ECDSA.pem a ser carregado no CUCM > CallManager-trust	Nenhum.
CallManager-ECDSA.pem (CA assinado)	Tomcat-ECDSA.pem (CA assinado)	Certificado CA raiz e intermediário do CUC*1 a ser carregado no CUCM > CallManager-trust	Certificado CA raiz e intermediário do CUCM*2 a ser carregado no CUC > CallManager-trust.
CallManager-ECDSA.pem (CA assinado)	Tomcat-ECDSA.pem (autoassinado)	Tomcat-ECDSA.pem a ser carregado no CUCM > CallManager-trust.	Certificado CA raiz e intermediário do CUCM a ser carregado no CUC > CallManager-trust.
CallManager-ECDSA.pem (autoassinado)	Tomcat-ECDSA.pem (CA assinado)	Certificado CA raiz e intermediário do CUC a ser carregado no CUCM > CallManager-trust	Nenhum.

*1 O certificado CA raiz e intermediário do CUC refere-se ao certificado CA que assinou o certificado Tomcat baseado em EC da conexão Unity (Tomcat-ECDSA.pem).

*2 certificado CA raiz e intermediário CUCM refere-se ao certificado CA que assinou o certificado CUCM CallManager (CallManager-ECDSA.pem).

1. **Note:** O certificado Tomcat-ECDSA.pem é chamado CallManager-ECDSA.pem nas versões 11.0.1 do CUC. Do CUC 11.5.x, o certificado foi renomeado para Tomcat-ECDSA.pem.

Configurar - Cisco Unity Connection (CUC)

1. Adicionar um novo grupo de portas

Navegue até a página Cisco Unity Connection Administration > Telephony integration > Port group e clique em Add New. Marque a caixa de seleção Ativar criptografia de próxima geração.

New Port Group

Phone System

Create From Port Group Type Port Group

Port Group Description

Display Name*

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile

Enable Next Generation Encryption

Secure RTP

Primary Server Settings

IPv4 Address or Host Name

IPv6 Address or Host Name

Port

- Nota:** O certificado Cisco Tomcat do Unity Connection será usado durante o handshake SSL quando a caixa de seleção Enable Next Generation Encryption estiver ativada.
 Caso a cifra baseada em ECDSA seja negociada, o certificado tomcat-ECDSA baseado na chave EC será usado no handshake SSL.
 Caso a cifra baseada em RSA seja negociada, o certificado tomcat baseado em chave RSA é usado no handshake SSL.

2. Adicionar a referência do servidor TFTP

Na página Noções básicas do grupo de portas, navegue para Editar > Servidores e adicione FQDN do servidor TFTP do cluster do CUCM. O FQDN/nome de host do servidor TFTP deve corresponder ao nome comum (CN) do certificado do CallManager. O endereço IP do servidor não funcionará e resultará em falha ao baixar o arquivo ITL. O nome DNS deve, portanto, ser resolvido via servidor DNS configurado.

SIP Servers			
Delete Selected Add			
<input type="checkbox"/>	Order	IPv4 Address or Host Name	
<input type="checkbox"/>	0	10.48.47.109	
Delete Selected Add			

TFTP Servers			
Delete Selected Add			
<input type="checkbox"/>	Order	IPv4 Address or Host Name	
<input type="checkbox"/>	0	CUCMv11	
Delete Selected Add			

Reinicie o Connection Conversation Manager em cada nó navegando até Cisco Unity Connection Serviceability > Tools > Service Management. Isso é obrigatório para que a configuração tenha efeito.

- Note:** A conexão Unity faz o download do arquivo ITL (ITLfile.tlv) do TFTP do CUCM usando o protocolo https na porta 6972 segura (URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv). O CUCM deve estar no modo misto, pois o CUC está procurando o certificado de função "CCM+TFTP" do arquivo ITL.

Navegue até a página de configuração Telephony integration > Port group > Port Group Basics e redefina seu grupo de portas recém-adicionado.

Port Group	
Display Name*	PhoneSystem-1
Integration Method	SIP
Reset Status	Reset Required <input type="button" value="Reset"/>

Session Initiation Protocol (SIP) Settings

Register with SIP Server

Authenticate with SIP Server

- Note:** Toda vez que o grupo de portas é redefinido, o servidor CUC atualiza seu arquivo ITL armazenado localmente conectando-se ao servidor CUCM.

3. Adicionar portas de correio de voz

Volte para Telephony integration > Port e clique em Add new para adicionar porta ao seu grupo de portas recém-criado.

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

4. Fazer upload da raiz do CUCM e do certificado intermediário da CA de terceiros

No caso de certificados de terceiros, você deve carregar os certificados Raiz e Intermediário da Autoridade de Certificação de terceiros no CallManager-trust do Unity Connection. Isso só é necessário se a CA de terceiros assinou seu certificado do Call Manager. Execute esta ação navegando até Cisco Unified OS Administration > Security > Certificate Management e clique em Carregar certificado.

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File CA_root_-_4096_key.crt

Configurar - Cisco Unified CM (CUCM)

1. Criar um perfil de segurança de tronco SIP

Navegue até CUCM Administration > System > Security > SIP Trunk Security Profile e adicione um novo perfil. O nome do assunto X.509 deve corresponder ao FQDN do servidor CUC.

SIP Trunk Security Profile Information

Name* cuc-secure-profile-EDCS

Description

Device Security Mode Encrypted

Incoming Transport Type* TLS

Outgoing Transport Type TLS

Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name CUCv11

Incoming Port* 5061

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

1. **Observação:** o comando CLI "show cert own tomcat/tomcat.pem" pode exibir o certificado tomcat baseado na chave RSA no Unity Connection. É CN que deve corresponder ao nome do assunto X.509 configurado no CUCM. O CN é igual a FQDN/Nome de host do servidor Unity. O certificado baseado na chave EC contém o FQDN/nome do host no campo Nome alternativo do assunto (SAN).

2. Criar um tronco SIP seguro

Navegue até Device > Trunk > Click and Add new e crie um tronco SIP padrão que será usado para a integração segura com o Unity Connection.

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

Inbound Calls

Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Inbound	

Outbound Calls

Called Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Called Party Transformation CSS	
Calling Party Transformation CSS	< None >
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Outbound	
Redirecting Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Redirecting Party Transformation CSS	

Destination

<input type="checkbox"/> Destination Address is an SRV			
	Destination Address	Destination Address IPv6	Destination Port
1*	10.48.47.123		5061
MTP Preferred Originating Codec*	711ulaw		
BLF Presence Group*	Standard Presence group		
SIP Trunk Security Profile*	cuc-secure-profile-EDCS		
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		

3. Configurar cifras TLS e SRTP

- Note:** A negociação entre o Unity Connection e o Cisco Unified Communications Manager depende da configuração da cifra TLS com as seguintes condições: Quando o Unity Connection atua como servidor, a negociação de cifra TLS é baseada na preferência selecionada pelo Cisco Unified CM. Caso a cifra baseada em ECDSA seja negociada, os certificados EC baseado em chave tomcat-ECDSA serão usados no handshake SSL. Caso a cifra baseada em RSA seja negociada, os certificados tomcat baseados em chave RSA são usados no handshake SSL. Quando o Unity Connection atua como cliente, a negociação de cifra TLS é baseada na preferência selecionada pelo Unity Connection.

Navegue até Cisco Unified CM > Systems > Enterprise Parameters e selecione a opção de cifra apropriada na lista suspensa TLS e SRTP Ciphers.

Security Parameters	
Cluster Security Mode *	1
LBM Security Mode *	Insecure
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
TFTP File Signature Algorithm *	SHA-1
Enable Caching *	True
Authentication Method for API Browser Access *	Basic
TLS Ciphers *	All Ciphers RSA Preferred
SRTP Ciphers *	All Supported Ciphers
HTTPS Ciphers *	RSA Ciphers Only

Reinicie o serviço Cisco Call Manager em cada nó navegando até a página Cisco Unified Serviceability, Ferramentas > Control Center-Feature Services e selecione Cisco Call Manager em Serviços CM

Navegue até a página Cisco Unity Connection Administration > System Settings > General Configurations e selecione a opção de cifra apropriada na lista suspensa TLS e SRTP Ciphers.

Edit General Configuration

Time Zone: (GMT+01:00) Europe/Warsaw

System Default Language: English(United States)

System Default TTS Language: English(United States)

Recording Format: G.711 mu-law

Maximum Greeting Length: 90

Target Decibel Level for Recordings and Messages: -26

Default Partition: cucv11 Partition

Default Search Scope: cucv11 Search Space

When a recipient cannot be found: Send a non-delivery receipt

IP Addressing Mode: IPv4

TLS Ciphers: All Ciphers RSA Preferred

SRTP Ciphers: All supported AES-256, AES-128 ciphers

HTTPS Ciphers: RSA Ciphers Only

Reinicie o Connection Conversation Manager em cada nó navegando até Cisco Unity Connection Serviceability > Tools > Service Management.

Opções de Cifra TLS com ordem de prioridade

Opções de Cifra TLS

Mais forte - AES-256 SHA-384 apenas: RSA preferencial

Strongest-AES-256 SHA-384 apenas: ECDSA preferencial

AES-256 AES-128 Médio apenas: RSA preferencial

Cifras TLS em ordem de prioridade

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

AES-256 AES-128 Médio apenas: ECDSA preferencial

Todos os clientes RSA preferidos (padrão)

Todos os clientes preferidos do ECDSA

Opções de cifra SRTP em ordem de prioridade

Opção de cifra SRTP

Todos com suporte para AES-256, cifras AES-128

AEAD AES-256, cifras baseadas em AES-28 GCM

Somente cifras baseadas em AEAD AES256 GCM

- 4
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

SRTP em pedido prioritário

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_32
- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AEAD_AES_256_GCM

4. Carregar certificados CUC Tomcat (com base em RSA e EC)

Navegue até Administração do SO > Segurança > Gerenciamento de certificado e carregue os certificados CUC Tomcat (com base em RSA e EC) no armazenamento confiável do

CallManager.

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File tomcat-ECDSA.pem

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File tomcat.pem

1. **Observação:** o upload de ambos os certificados Unity Tomcat não é obrigatório se cifras ECDSA forem negociadas apenas. Nesse caso, o certificado Tomcat baseado na CE é suficiente.

No caso de certificados de terceiros, você deve carregar o certificado raiz e o certificado intermediário da Autoridade de Certificação de terceiros. Isso só é necessário se a CA de terceiros assinou seu certificado Unity Tomcat.

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File CA_root_-_4096_key.crt

Reinicie o processo do Cisco Call Manager em todos os nós para aplicar as alterações.

5. Criar padrão de rota

Configure um padrão de rota que aponte para o tronco configurado navegando para 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.

Pattern Definition

Route Pattern*	2000
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*	CUCv11
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error

6. Criar piloto de correio de voz, perfil de correio de voz e atribuí-lo aos DNS

Crie um piloto de correio de voz para a integração indo para Advanced Features > Voice Mail > Voice Mail Pilot.

Voice Mail Pilot Information

Voice Mail Pilot Number	2000
Calling Search Space	< None >
Description	Default

Crie um perfil de correio de voz para vincular todas as configurações a recursos avançados > Correio de voz > Perfil de correio de voz

Voice Mail Profile Information

Voice Mail Profile	VoiceMailProfile-8000 (used by 0 devices)
Voice Mail Profile Name*	VoiceMailProfile-8000
Description	
Voice Mail Pilot**	2000/< None >
Voice Mail Box Mask	

Atribua o perfil de correio de voz recém-criado aos DNS destinados a usar a integração segura indo a Call Routing > Directory number

Directory Number Settings

Voice Mail Profile	VoiceMailProfile-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 >	

Configurar - Assinatura de certificados com base na chave EC por CA de terceiros (opcional)

Os certificados podem ser assinados por uma CA de terceiros antes de configurar a integração segura entre os sistemas. Siga as etapas a seguir para assinar os certificados em ambos os sistemas.

Cisco Unity Connection

1. Gerar solicitação de assinatura de certificado (CSR) para CUC Tomcat-ECDSA e ter o certificado assinado por CA de terceiros
2. A AC fornece o certificado de identidade (certificado assinado pela AC) e o certificado CA (certificado raiz da AC) que devem ser carregados da seguinte forma:
Carregar certificado raiz de CA no repositório tomcat-trust
Carregar certificado de identidade no repositório tomcat-EDCS
3. Reiniciar o Gerenciador de conversação no CUC

Cisco Unified CM

1. Gerar CSR para CUCM CallManager-ECDSA e ter o certificado assinado por CA de terceiros
2. A AC fornece o certificado de identidade (certificado assinado pela AC) e o certificado CA (certificado raiz da AC) que devem ser carregados da seguinte forma:
Carregar certificado raiz de CA no arquivo callmanager-trust
Carregar certificado de identidade no arquivo callmanager-EDCS
3. Reiniciar os serviços Cisco CCM e TFTP em cada nó

O mesmo processo será usado para assinar certificados baseados em chave RSA, em que CSR é gerado para certificado CUC Tomcat e certificado CallManager e carregado no armazenamento tomcat e no armazenamento callmanager respectivamente.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verificação de tronco SIP seguro

Pressione o botão Voice Mail 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, conforme mostrado abaixo:

Name ^	Description	Calling Search Space	Device Pool	Route Pattern	Trunk Type	SIP Trunk Status	SIP Trunk Duration
CUCv11			Default	2000	SIP Trunk	Full Service	Time 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



Informações Relacionadas

- [Guia de integração do SIP para Cisco Unity Connection versão 11.x](#)