

Exemplo de configuração para a integração segura do SORVO entre CUCM e CUC baseados na criptografia da próxima geração (NGE)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Diagrama de Rede](#)

[Exigências do certificado](#)

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

1. [Adicionar um grupo de porta novo](#)
2. [Adicionar a referência do servidor TFTP](#)
3. [Adicionar portas de correio de voz](#)
4. [Transfira arquivos pela rede a raiz CUCM e o certificado do intermediário da terceira parte CA](#)

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

1. [Crie um perfil de segurança do tronco do SORVO](#)
2. [Crie um tronco seguro do SORVO](#)
3. [Configurar cifras TLS e SRTP](#)
4. [Transfira arquivos pela rede Certificados CUC Tomcat \(RSA & o EC baseados\)](#)
5. [Crie a rota padrão](#)
6. [Crie o piloto do correio de voz, perfil do correio de voz e atribua-o aos DN](#)

[Configurar - Assinar a chave EC baseou Certificados pela terceira parte CA \(opcional\)](#)

[Verificar](#)

[Fixe a verificação do tronco do SORVO](#)

[Fixe a verificação do atendimento RTP](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a configuração e a verificação da conexão segura do SORVO entre o server unificado Cisco do gerente (CUCM) e do Cisco Unity Connection de uma comunicação (CUC) usando a criptografia da próxima geração.

A Segurança da próxima geração sobre a relação do SORVO restringe a relação do SORVO para usar as cifras da série B baseadas nos protocolos TLS 1.2, SHA-2 e AES256. Permite as várias combinações de cifras baseadas na ordem da prioridade de cifras RSA ou ECDSA. Durante a comunicação entre a conexão de unidade e o Cisco unificou o CM, cifras e os Certificados da terceira parte são verificados em ambas as extremidades. Está abaixo a configuração para o suporte de criptografia da próxima geração.

Se você planeja se usar os Certificados assinados pela autoridade de certificação da terceira parte a seguir começam com o certificado que assina na extremidade da seção de configuração (configurar - assinando os Certificados baseados chave EC pela terceira parte CA)

Pré-requisitos

Requisitos

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

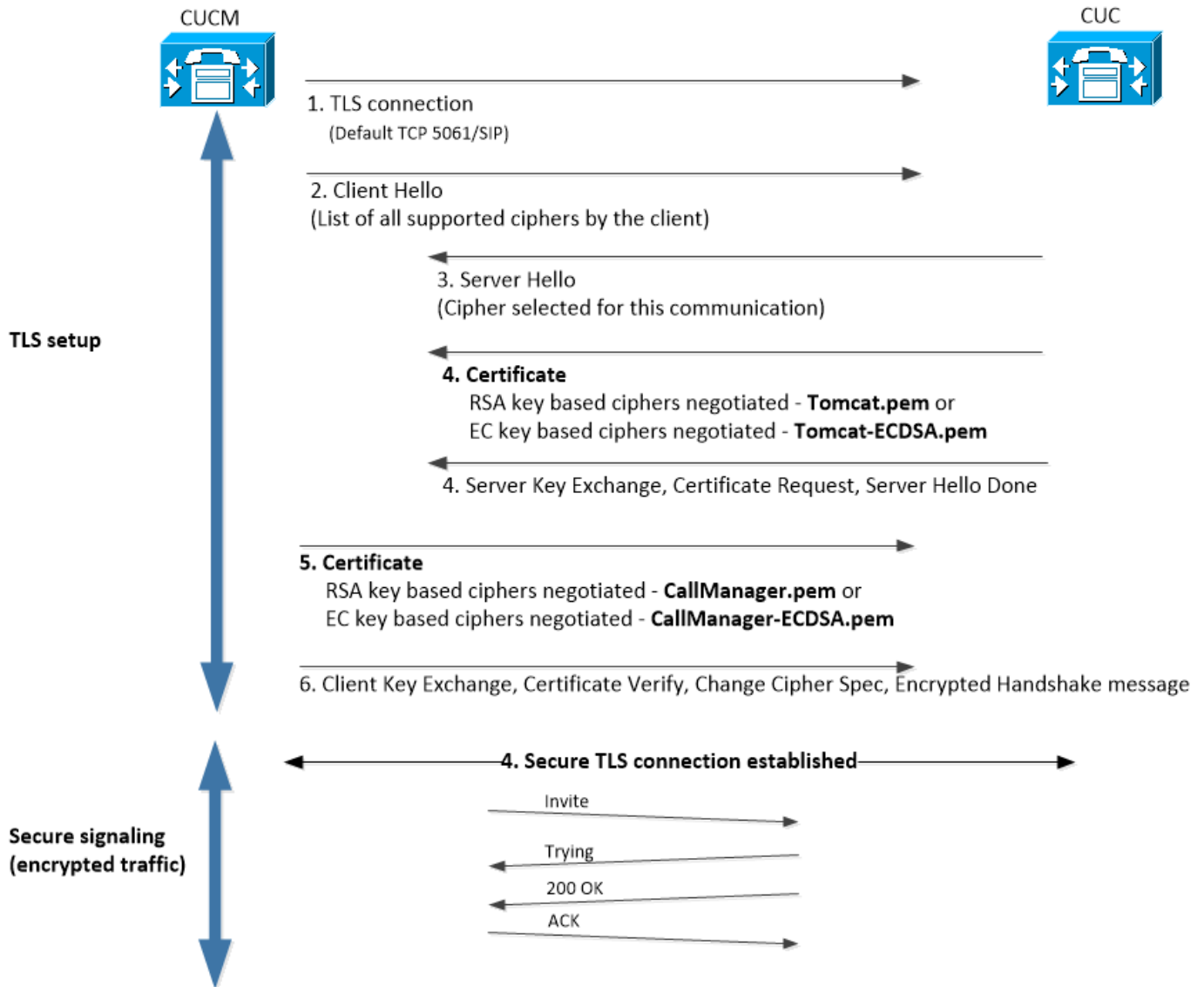
Versão 11.x e mais recente CUCM em modo misturado

Versão 11.x e mais recente CUC

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Diagrama de Rede

Este diagrama explica momentaneamente o processo que as ajudas estabelecem uma conexão segura entre CUCM e CUC o suporte de criptografia da próxima geração é permitido uma vez que:



Exigências do certificado

Estas são as exigências da troca do certificado uma vez que o suporte de criptografia da próxima geração é permitido no Cisco Unity Connection.

Certificados auto-assinados usados:

- **Conexão de unidade**
Nenhuma necessidade de transferir arquivos pela rede algum certificado. O server da conexão de unidade transferirá automaticamente o ITLfile do servidor TFTP especificado durante a configuração e a confiança CallManager.pem & CallManager-EC.pem durante a negociação TLS.
- **Cisco unificou o CM**
Você deve transferir arquivos pela rede o Tomcat.pem & o Tomcat-EC.pem da conexão de unidade na loja da CallManager-confiança em CUCM

Os certificados de CA da terceira usados:

- Conexão de unidade
Você deve transferir arquivos pela rede a raiz e todos os Certificados intermediários da autoridade de certificação da terceira parte na CallManager-confiança da conexão de unidade. Sobre isso, o servidor de conexão transferirá automaticamente o ITLfile do servidor TFTP especificado durante a configuração e a confiança CallManager.pem & CallManager-EC.pem durante a negociação TLS.
- Cisco unificou o CM
Você deve transferir arquivos pela rede a raiz e todos os Certificados intermediários da autoridade de certificação da terceira parte na CallManager-confiança do CM unificado.

Configurar - Cisco Unity Connection (CUC)

1. Adicionar um grupo de porta novo

Navegue à página de administração > à integração de telefonia > ao grupo de porta do Cisco Unity Connection e clique adicionam sobre novo. Certifique-se verificar a caixa de seleção da criptografia da próxima geração da possibilidade.

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

1. **Note:** O certificado de Cisco Tomcat da conexão de unidade estará usado durante a saudação de SSL uma vez que a caixa de seleção da criptografia da próxima geração da possibilidade é permitida.
 - Caso que a cifra baseada ECDSA é negociada então o certificado baseado chave EC Tomcat-ECDSA está usado na saudação de SSL.
 - Caso que a cifra baseada RSA é negociada então o certificado baseado chave RSA TomCat está usado na saudação de SSL.

2. Adicionar a referência do servidor TFTP

No grupo de porta que os princípios paginam, navegam para editar > server e para adicionar o FQDN do servidor TFTP de seu conjunto CUCM. FQDN/Hostname do servidor TFTP deve combinar o Common Name (CN) do certificado do CallManager. O endereço IP de Um ou Mais Servidores Cisco ICM NT do server não trabalhará e conduzirá à falha transferir o arquivo ITL. O nome de DNS deve ser consequentemente pode ser resolvido através do servidor DNS configurado.

The screenshot displays two configuration sections: 'SIP Servers' and 'TFTP Servers'. Each section has a table with columns for 'Order' and 'IPv4 Address or Host Name'. In the 'SIP Servers' table, the first row has '0' in the Order column and '10.48.47.109' in the IPv4 Address or Host Name column. In the 'TFTP Servers' table, the first row has '0' in the Order column and 'CUCMv11' in the IPv4 Address or Host Name column, which is highlighted with a red box.

Reinicie o gerente da conversação da conexão em cada nó navegando à utilidade do Cisco Unity Connection > às ferramentas > ao Gerenciamento do serviço. Isto é imperativo para que a configuração tome o efeito.

1. **Note:** O arquivo ITL das transferências da conexão de unidade (ITLfile.tlv) do TFTP de CUCM que usa o protocolo dos https em 6972 seguros move (URL: <https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv>). CUCM deve reagir do modo misturado desde que CUC está procurando o certificado da função "CCM+TFTP" do arquivo ITL.

Navegue de volta aos princípios página de configuração da integração de telefonia > do grupo de porta > do grupo de porta e restaure seu grupo de porta recentemente adicionado.

Port Group

Display Name*

Integration Method

Reset Status

Session Initiation Protocol (SIP) Settings

Register with SIP Server

Authenticate with SIP Server

1. **Note:** Cada vez que o grupo de porta é restaurado, o server CUC atualizará seu arquivo localmente armazenado ITL conectando ao server CUCM.

3. Adicionar portas de correio de voz

Navegue de volta à integração de telefonia > à porta e clique sobre Add novo para adicionar a porta a seu grupo de porta 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. Transfira arquivos pela rede a raiz CUCM e o certificado do intermediário da terceira parte CA

Em caso dos Certificados da terceira parte, você deve transferir arquivos pela rede o certificado da raiz e do intermediário da autoridade de certificação da terceira parte na CallManager-confiança da conexão de unidade. Isto é precisado somente se a 3ª parte CA assinou seu certificado do gerenciador de chamada. Execute esta ação navegando a Cisco unificou o > gerenciamento de certificado do > segurança da administração do OS e clicam sobre o certificado da transferência de arquivo pela rede.

Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust

Description(friendly name)

Upload File Choose File CA_root_-_4096_key.crt

Upload Close

Configurar - Cisco unificou CM (CUCM)

1. Crie um perfil de segurança do tronco do SORVO

Navegue ao > segurança da administração > do sistema CUCM > ao perfil de segurança do tronco do SORVO e adicionar um perfil novo. O nome do sujeito X.509 deve combinar o FQDN do server 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

- Note:** O comando CLI da “CERT mostra para possuir TomCat/tomcat.pem” pode indicar o certificado baseado chave RSA TomCat na conexão de unidade. É CN deve combinar o nome do sujeito X.509 configurado em CUCM. O CN é igual a FQDN/Hostname do servidor de unidade. O certificado baseado chave EC contém o FQDN/hostname em seu campo sujeito do nome alternativo (SAN).

2. Crie um tronco seguro do SORVO

Navegue ao dispositivo > ao tronco > ao clique e adicionar novo e crie um tronco padrão do SORVO que seja usado para a integração segura com conexão de unidade.

SRTTP 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

Redirecting Diversion Header Delivery - Inbound

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

Destination

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 SRTTP

1. **Note:** A negociação entre a conexão de unidade e o gerente das comunicações unificadas de Cisco depende da configuração da cifra TLS com as seguintes circunstâncias: Quando a conexão de unidade atua como o server, a negociação da cifra TLS está baseada na preferência selecionada por Cisco unificou o CM. Caso que a cifra baseada ECDSA é negociada então os Certificados baseados chaves EC Tomcat-ECDSA estão usados na saudação de SSL. Caso que a cifra baseada RSA é negociada então os Certificados baseados chaves RSA TomCat estão usados na saudação de SSL. Quando a conexão de unidade atua como o cliente, a negociação da cifra TLS está baseada na preferência selecionada pela conexão de unidade.

Navegue a Cisco unificou CM > sistemas > parâmetros empresariais e selecionam a opção apropriada da cifra das cifras TLS e SRTP da lista de drop-down.

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 do Cisco Call Manager em cada nó navegando a Cisco unificou a página da utilidade, as ferramentas > os serviços da Centro-característica do controle e Cisco Call Manager seletos sob serviços CM

Navegue à página de administração > às configurações de sistema > às configurações gerais do Cisco Unity Connection e selecione a opção apropriada da cifra das cifras TLS e SRTP da lista de drop-down.

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 gerente da conversação da conexão em cada nó navegando à utilidade do Cisco Unity Connection > às ferramentas > ao Gerenciamento do serviço.

O TLS calcula opções com ordem da prioridade

Opções da cifra TLS

O SHA-384 o mais forte do AES-256 somente: RSA preferido

SHA-384 Strongest-AES-256 somente: ECDSA preferido

AES-128 Medium-AES-256 somente: RSA preferido

AES-128 Medium-AES-256 somente: ECDSA preferido

Todas as cifras RSA preferidas (padrão)

Todas as cifras ECDSA preferidas

Cifras TLS na ordem da prioridade

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA4
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA4
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA6
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_A256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA4
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_A256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA6
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA4
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA6
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_A256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_A384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA4
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_A256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA6
- TLS_RSA_WITH_AES_128_CBC_SHA

Opções da cifra SRTP na ordem da prioridade

Opção da cifra SRTP

Todos apoiaram o AES-256, cifras do AES-128

SRTP na ordem da prioridade

- 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

O AES-256 AEAD, AES-28 GCM-baseou cifras
 AEAD AES256 GCM-baseou cifras somente

4. Certificados da transferência de arquivo pela rede CUC Tomcat (RSA & EC baseados)

Navegue ao > gerenciamento de certificado do > segurança da administração do OS e transfira arquivos pela rede ambos os Certificados CUC Tomcat (RSA & EC baseados) na loja da CallManager-confiança.

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. **Note:** Transferir arquivos pela rede ambos os Certificados de Tomcat do Unity não é imperativo se as cifras ECDSA são negociadas somente. Em tal certificado baseado EC de Tomcat do caso é bastante.

Em caso dos Certificados da terceira parte, você deve transferir arquivos pela rede a raiz e o certificado do intermediário da autoridade de certificação da terceira parte. Isto é precisado somente se a 3ª parte CA assinou seu certificado de Tomcat do Unity.

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 mudanças.

5. Crie a rota padrão

Configurar uma rota padrão que pontos ao tronco configurado navegando ao roteamento de chamada > à rota/caça > à rota padrão. A extensão incorporada como um número da rota padrão pode ser usada como um piloto do 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. Crie o piloto do correio de voz, perfil do correio de voz e atribua-o aos DN

Crie um correio de voz piloto para a integração indo aos recursos avançados > ao correio de voz > ao correio de voz piloto.

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

Crie um perfil de correio de voz a fim ligar junto os todos os recursos avançados > correio de voz > perfil de correio de voz dos ajustes

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 DN pretendidos usar a integração segura indo ao roteamento de chamada > ao número de diretório

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 - Assinar a chave EC baseou Certificados pela terceira parte CA (opcional)

Os Certificados puderam ser assinados por uma terceira parte CA antes de estabelecer a integração segura entre os sistemas. Siga as seguintes etapas para assinar os Certificados em ambos os sistemas.

Cisco Unity Connection

1. Gerencia a solicitação de assinatura de certificado (CSR) para CUC Tomcat-ECDSA e tenha o certificado assinado pela terceira parte CA
2. CA fornece o certificado de identidade (certificado assinado de CA) e o certificado de CA (certificado de raiz de CA) que devem ser transferidos arquivos pela rede como seguem:
Transfira arquivos pela rede o certificado de raiz de CA na loja da Tomcat-confiança
Transfira arquivos pela rede o certificado de identidade na loja Tomcat-EDCS
3. Reinicie o gerente da conversaç o em CUC

Cisco unificou o CM

1. Gerencia o CSR para o CallManager-ECDSA CUCM e tenha o certificado assinado pela terceira parte CA
2. CA fornece o certificado de identidade (certificado assinado de CA) e o certificado de CA (certificado de raiz de CA) que devem ser transferidos arquivos pela rede como seguem:
Transfira arquivos pela rede o certificado de raiz de CA na loja da CallManager-confiança
Transfira arquivos pela rede o certificado de identidade na loja CallManager-EDCS
3. Reinicie Cisco CCM e servi os TFTP em cada n o

O mesmo processo ser  usado para assinar os Certificados baseados chave RSA onde o CSR   gerado para o certificado CUC Tomcat e o certificado do CallManager e transferido arquivos pela rede TomCat na loja e na loja do callmanager respectivamente.

Verificar

Use esta se o para confirmar se a sua configura o funciona corretamente.

Fixe a verifica o do tronco do SORVO

Pressione o bot o do correio de voz no telefone para chamar o correio de voz. Voc  deve ouvir a sauda o inicial se a extens o do usu rio n o   configurada no sistema da conex o de unidade.

Alternativamente, voc  pode permitir o keepalive das op es do SORVO de monitorar o status de tronco do SORVO. Esta op o pode ser permitida no perfil do SORVO atribuído ao tronco do SORVO. Uma vez que isto   permitido voc  pode monitorar o status de tronco do sorvo atrav s

do dispositivo > do tronco como 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 segura do atendimento RTP

Verifique se o ícone do cadeado esta presente em atendimentos à conexão de unidade. Significa que córrego RTP está cifrado (o perfil de segurança do dispositivo deve ser seguro para que trabalhe) segundo as indicações desta imagem



Informações Relacionadas

- [Guia de integração do SORVO para a liberação 11.x do Cisco Unity Connection](#)