Configurar o fluxo de chamadas detalhado UCCE 11.6 com SIP/TLS (CA assinou)

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configuração
Diagrama de Rede
Configuração do gateway de ingresso TLS da parte A.
Trabalhos da configuração
Detalhes de configuração
Configuração de B. CVP TLS da parte
Trabalhos da configuração
Detalhes de configuração
Parte C. VVB Configuração
Detalhes de configuração
Parte D. CUCM Configuração
Detalhes de configuração
Verificar
Troubleshooting
Informações Relacionadas

Introdução

Este original descreve o processo de configuração para distribuir o Session Initiation Protocol (SIP) sobre o Transport Layer Security (TLS) no fluxo de chamadas detalhado do Cisco Unified Contact Center Enterprise (UCCE) com os certificados assinados do Certificate Authority (CA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CUCCE
- Rede telefônica pública comutada (PSTN)
- Protocolo SIP
- Public Key Infrastructure (PKI)
- TLS

Componentes Utilizados

Esta informação neste documento é baseada nestes versão de software e hardware:

- Cisco 3945 Router
- Portal da Voz de cliente Cisco (CVP) 11.6
- Cisco virtualizou o navegador de voz (VVB) 11.6
- Cisco Intelligent Contact Management (ICM) 11.6

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 sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Informações de Apoio

Neste original, o gerente das comunicações unificadas de Cisco (CUCM) é usado ao lado do simulatePSTN entre o PSTN e o gateway de ingresso. O SORVO sobre o Transmission Control Protocol (TCP) é usado entre o agente CUCM e o telefone IP do agente. Todo SORVO restante do uso dos pés do SORVO sobre TLS (CA assinado).

O fluxo de chamadas detalhado UCCE é a **rede telefônica pública comutada (PSTN) > gateway de ingresso > Portal Cisco Unified Customer Voice (CVP) > o Intelligent Contact Management (ICM) (etiqueta do retorno do agente) > CVP > gerente das comunicações unificadas de Cisco (CUCM) > telefone IP do agente**.

SIP/TLS é introduzido na versão 11.6 UCCE. Após a elevação a CVP 11.6, assegure a configuração manual do revestimento de propriedades unificadas CVP.

UCCE 11.6 usa TLS 1.2, assegura os apoios TLS 1.2 do gateway de ingresso.

Os IO 15.6(1) T e os IO XE 3.17S apoiam TLS 1.2. Apoios precedentes TLS1.0 das Versões do IOS somente.

As seguintes séries da cifra são introduzidas para o Cisco IOS 15.6(1)T da liberação:

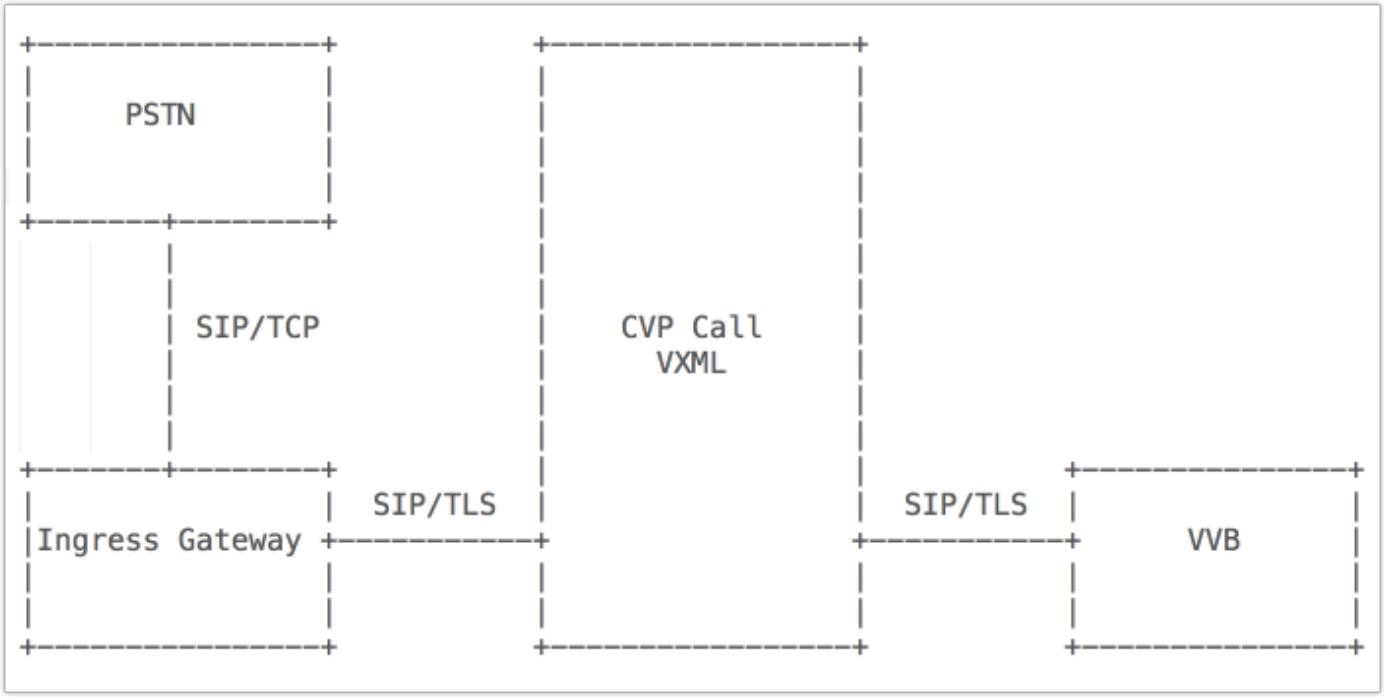
- do TLS_DHE_RSA_WITH_AES_128_CBC_SHA1
- do TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

A característica da licença Securityk9 deve ser permitida no gateway de ingresso.

VVB precisa de ser promovido a 11.6.

Configuração

Diagrama de Rede



A configuração inclui quatro porções.

Configuração do gateway de ingresso TLS da parte A.

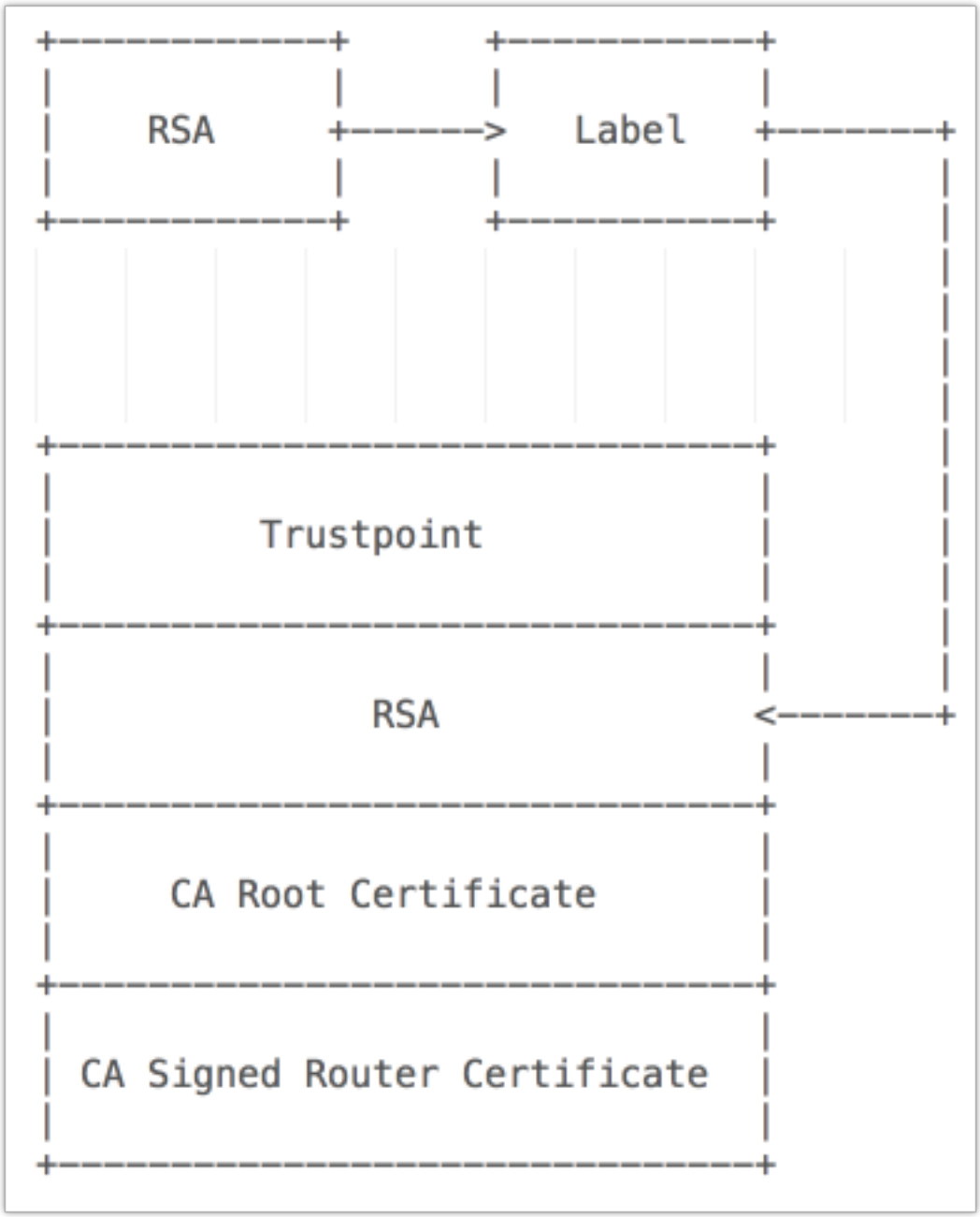
Configuração de B. CVP TLS da parte

Parte C. VVB Configuração

Parte D. CUCM Configuração

Configuração do gateway de ingresso TLS da parte A.

Trabalhos da configuração



Detalhes de configuração

Etapa 1. Gerencia a chave RSA no roteador (chave 1024-bit RSA).

```
crypto key generate rsa modulus 1024 label INGW
```

Etapa 2. Crie um ponto confiável (um ponto confiável representa CA confiado).

```
crypto pki trustpoint col115ca
revocation-check none
serial-number none
ip-address none
fqdn none
rsakeypair INGW
subject-name cn=INGRESSGW, ou=TAC, o=CISCO

crypto pki trustpoint col115ca
```

```
enrollment terminal
```

Etapa 3. Crie um pedido do certificado (CSR) que seja enviado a CA.

```
crypto ski enroll col115ca
```

Etapa 4. Certificado assinado de CA (bit CA CERT da base 64).

Etapa 5. Instale o certificado de raiz.

```
crypto pki authenticate col115ca
```

Etapa 6. Instale o certificado assinado de CA (CERT da base 64).

```
crypto pki import col115ca certificate
```

Etapa 7. Verifique que os Certificados estiveram instalados.

```
show crypto pki certificates
```

Etapa 8. Configurar a versão TLS no gateway.

```
sip-ua
transport tcp tls v1.2
```

Etapa 9. Especifique o conforme o destino usado ponto confiável.

```
sip-ua

crypto signaling remote-addr 10.66.75.49 255.255.255.255 trustpoint col115ca
```

Etapa 10. Ajuste o dial-peer que apontam ao CVP para usar o TLS.

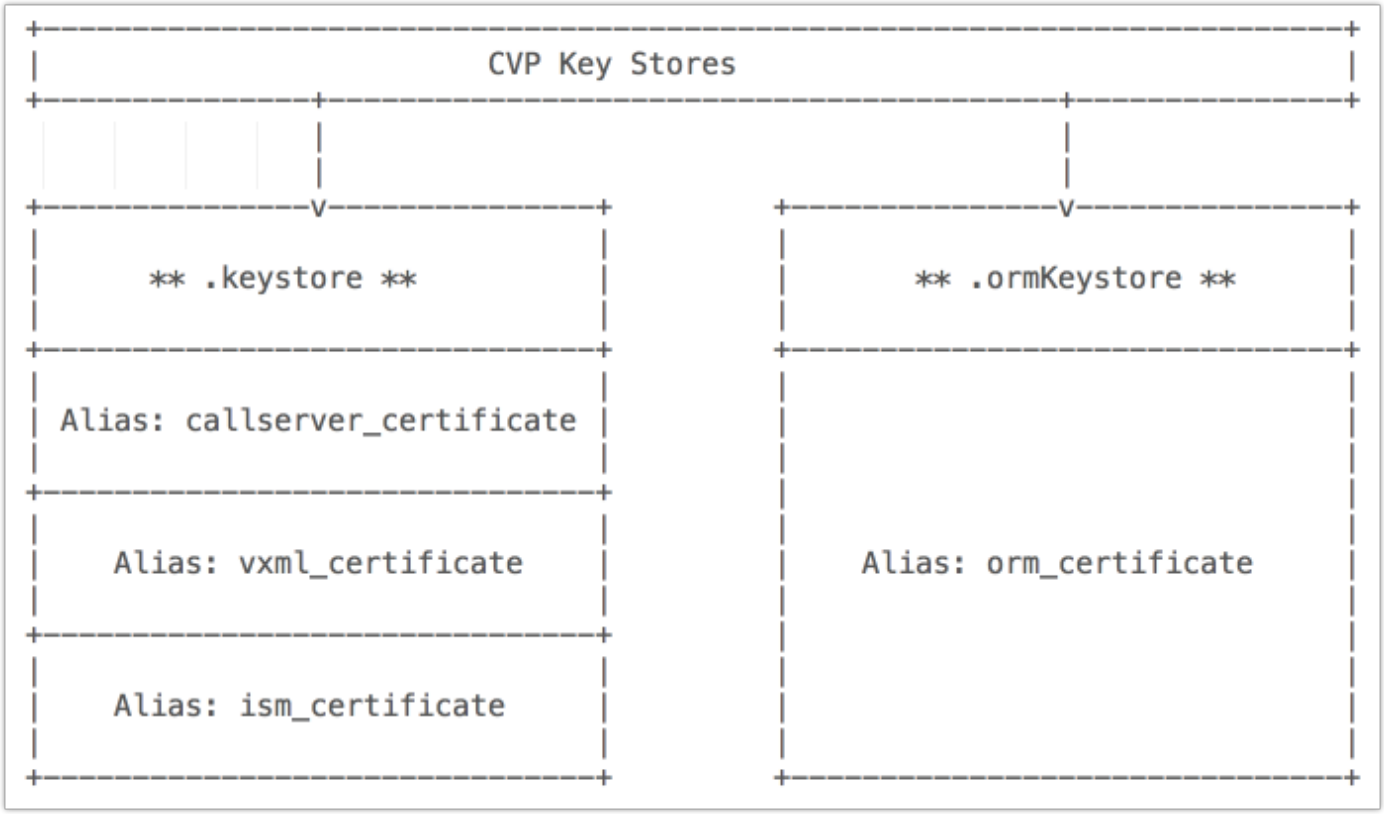
```
dial-peer voice 7205 voip
  description to CVP
  destination-pattern 700.$
  session protocol sipv2
  session target ipv4:10.66.75.49
  session transport tcp tls
  dtmf-relay rtp-nte
  codec g711ulaw
```

Peça a configuração de B. CVP TLS

Trabalhos da configuração

O CVP tem duas lojas chaves, situadas em **c:\Cisco\CVP\conf\security**.

Segundo as indicações da imagem, estas duas lojas chaves guardam Certificados diferentes.



Detalhes de configuração

Etapa 1. Navegue ao server do atendimento de **c:\Cisco\CVP\conf\security.propertiesin** CVP a fim encontrar esta senha. Este arquivo contém a senha para a loja chave, que é exigida ao operar a loja chave.

Etapa 2. Padrão de sistema Callserver_certificate da supressão.

```
C:\Cisco\CVP\jre\bin>keytool.exe -delete -alias orm_certificate -storetype JCEKS -keystore
c:\Cisco\CVP\conf\security\.keystore
```

Etapa 3. Gerencia o keypair.

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -alias callserver_certificate -v -k eysize 1024 -
keyalg RSA -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\.keystore
```

Etapa 4. Crie um CSR e salvar o no C: conduza a pasta raiz (**c:\callcsr.csr**).

```
C:\Cisco\CVP\jre\bin>keytool.exe -certreq  -alias callserver_certificate -file c:\callcsr.csr  -
storetype JCEKS
-keystore c:\Cisco\CVP\conf\security\.keystore
```

Etapa 5. Assine o pedido e submeta o pedido a CA (quando você transfere o CERT, escolhem Base64 codificado).

Etapa 6. Instale o certificado de raiz (CERT armazenado em **C:\DC - Root.cer).**

```
C:\Cisco\CVP\jre\bin>keytool.exe -import -v -trustcacerts -alias root -file  C:\ DC-Root.cer   -
```

```
storetype JCEKS -keystore C:\Cisco\CVP\conf\security\.Keystore
```

Etapa 7. Instale o certificado assinado de CA (CERT armazenado em c:\95callserver.cer).

```
C:\Cisco\CVP\jre\bin>keytool.exe -import -v -trustcacerts  -alias callserver_certificate -file
c:\95callserver.cer  -sto retype JCEKS -keystore c:\Cisco\CVP\conf\security\.keystore
```

Etapa 8. Verifique os detalhes certificados na loja chave.

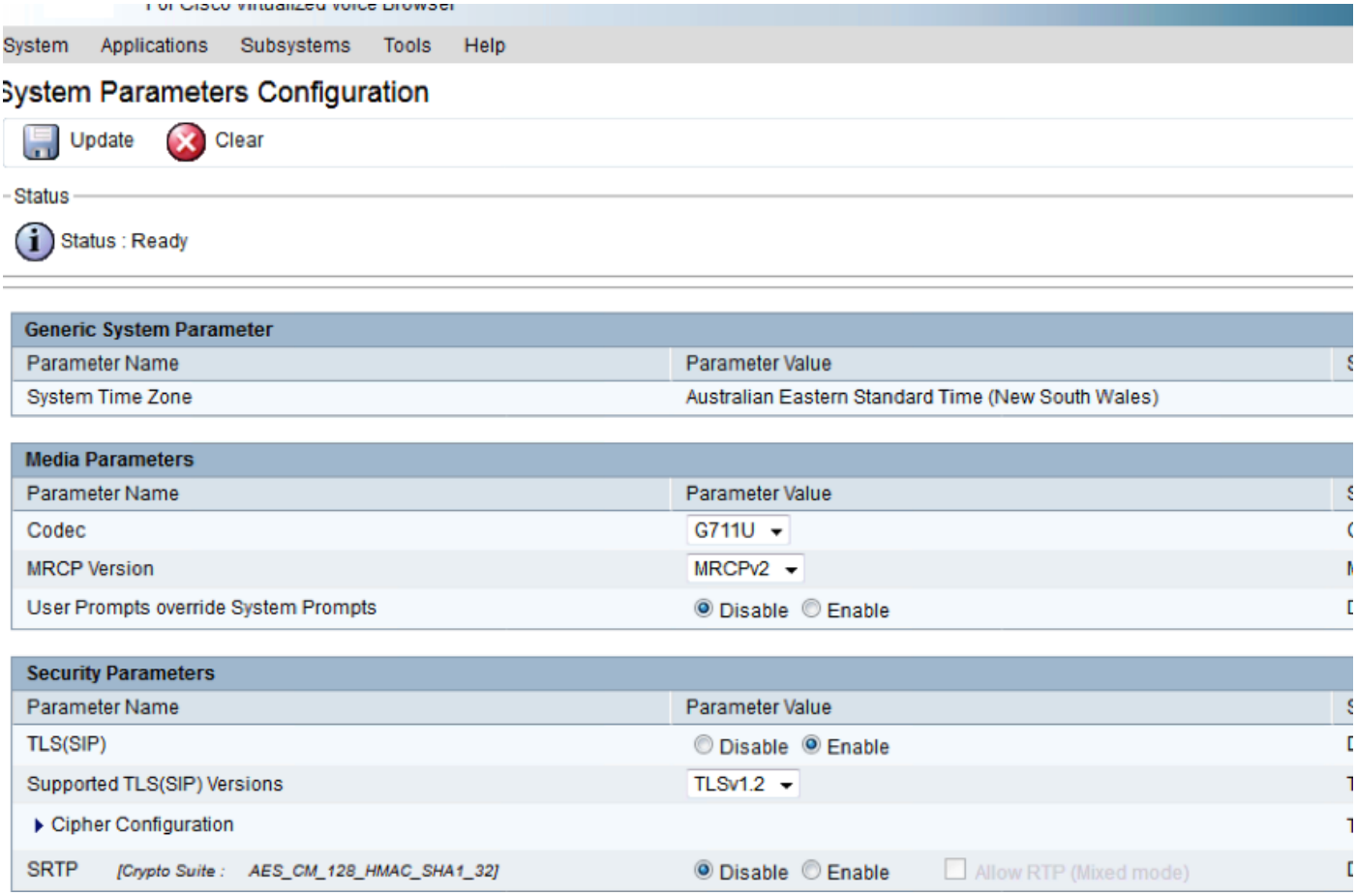
```
C:\Cisco\CVP\jre\bin>keytool.exe -list -v -storetype JCEKS -keystore c:\Cisco\CV
P\conf\security\.keystore
```

Peça C. VVB Configuração

Detalhes de configuração

Etapa 1. Permita o TLS do parâmetro de sistema

Este exemplo usa o RTP, assim que o SRTP em VVB não é permitido.



Etapa 2. Gerencia e importe o certificado assinado de CA para VVB, esta parte é o mesmos como certificado CUCM TomCat

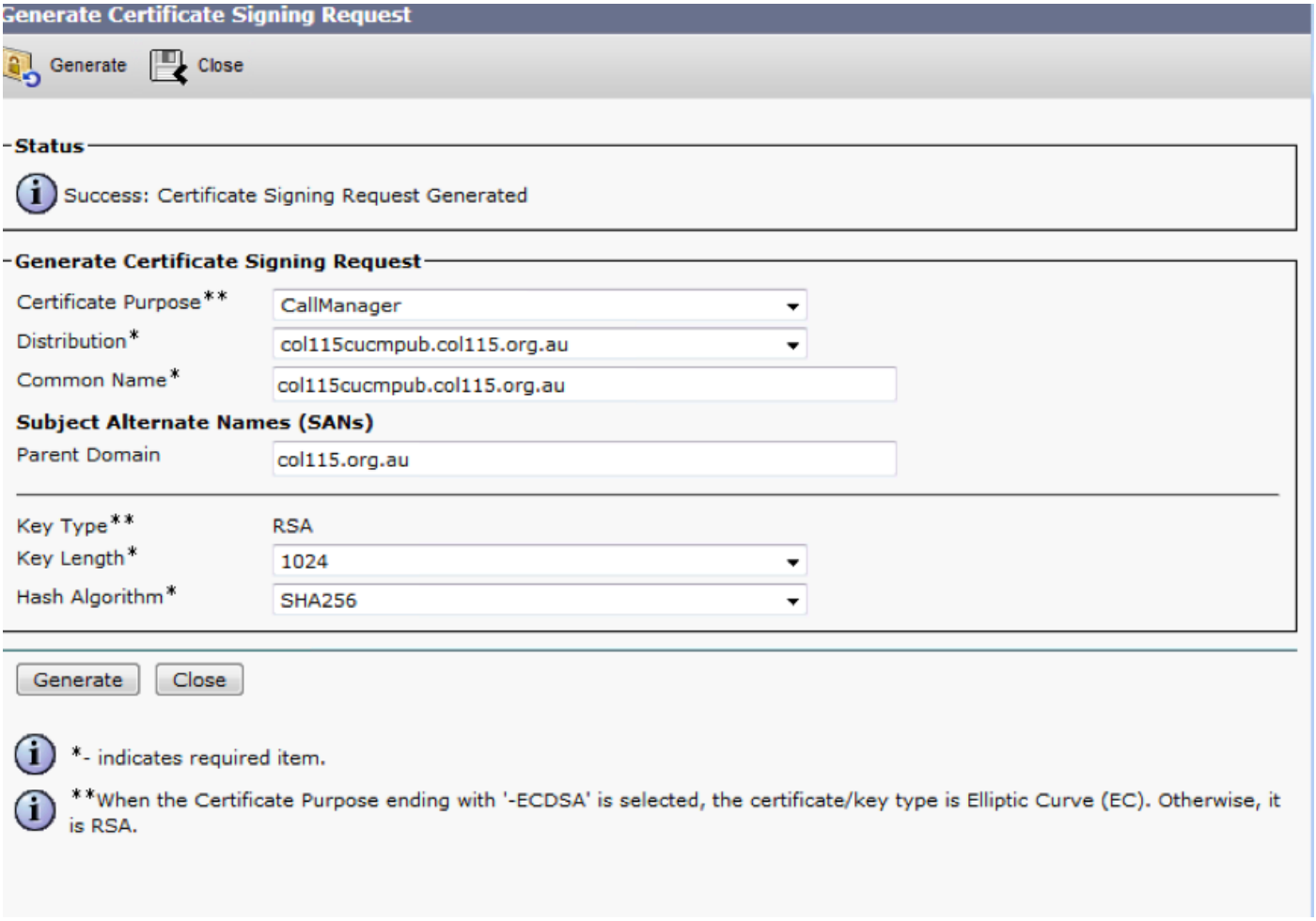
- Gerencia o CSR e assinado por CA.
- Importe a confiança de Tomcat (CERT da raiz de CA).
- Importe Tomcat (CERT assinado CA).

Peça D. CUCM Configuração

Detalhes de configuração

Etapa 1. Transfira arquivos pela rede o certificado assinado CA do callmanager no server CUCM. CUCM usa o certificado do callmanager para SIP/TLS.

Etapa 2. Gerencia o CSR para o certificado do callmanager, certifique-se que o comprimento chave é 1024.



Etapa 3. Forneça o CSR a CA e recupere o certificado do callmanager.

Etapa 4. Certificado CA raiz de importação e o certificado recentemente assinado do callmanager.

Etapa 5. Callmanager e serviços TFTP do reinício.

Etapa 6. Configurar o perfil de segurança do tronco do SORVO. Navegue ao **> segurança do sistema > ao perfil de segurança do tronco do SORVO**

Assegure-se de que o nome do sujeito X.509 seja mesmo como é usado no certificado de servidor do atendimento CVP, segundo as indicações das imagens.

Name*: Secure SIP Trunk Profile-CVP

Description: Secure SIP Trunk Profile authenticated by null String

Device Security Mode: Encrypted

Incoming Transport Type*: TLS

Outgoing Transport Type: TLS

☐ Enable Digest Authentication

Nonce Validity Time (mins)*: 600

X.509 Subject Name: col115cvpcall02

Incoming Port*: 5061

☐ Enable Application level authorization

☐ Accept presence subscription

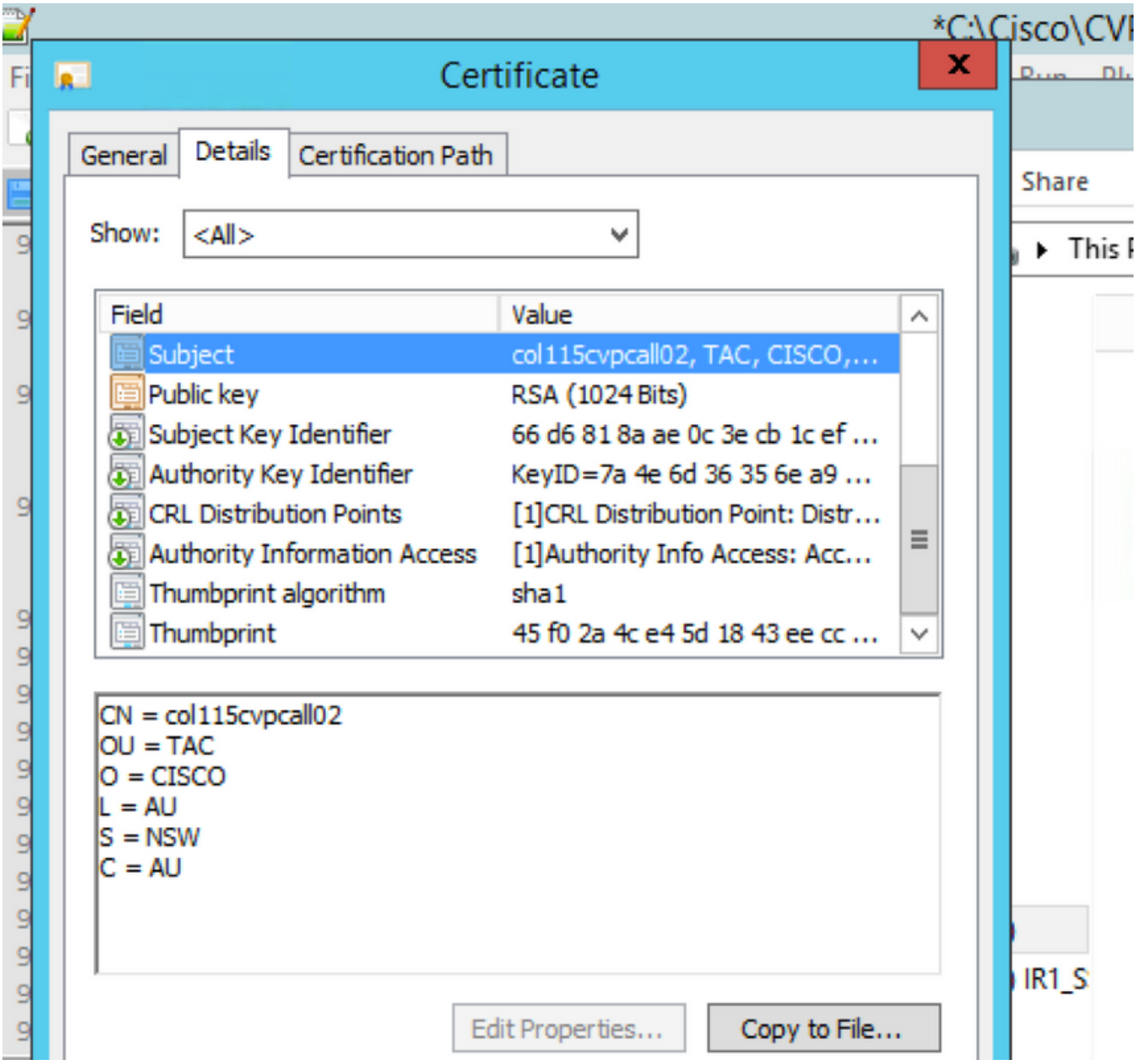
☐ Accept out-of-dialog refer**

☐ Accept unsolicited notification

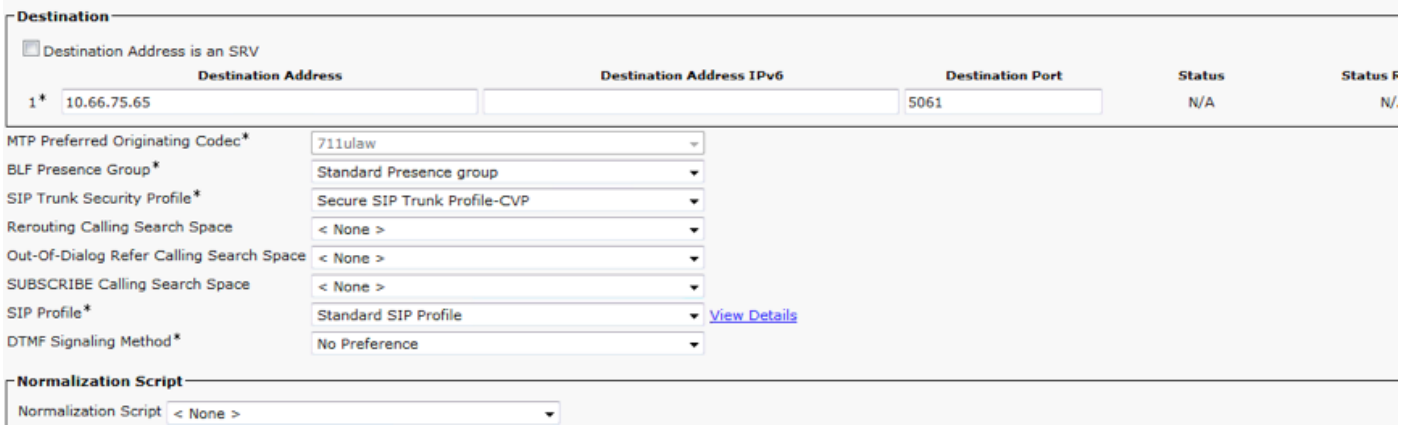
☐ Accept replaces header

☑ Transmit security status

☐ Allow charging header



Etapa 7. Crie o tronco do SORVO e atribua-o a um perfil de segurança.



Verificar

Verifique os Certificados instalados no gateway de ingresso.

```
show crypto pki certificates
```

Verifique detalhes certificados na loja da chave CVP.

```
C:\Cisco\CVP\jre\bin>keytool.exe -list -v -storetype JCEKS -keystore c:\Cisco\CV
P\conf\security\.keystore
```

Troubleshooting

Comandos Debug relativos ao TLS.

```
debug ssl openssl errors

debug ssl openssl msg

debug ssl openssl states
```

Informações Relacionadas

- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/cvp11_6/configuration/guide/ccvp_b_configuration-guide-for-cisco-unified.pdf
- Suporte Técnico e Documentação - Cisco Systems