

Configurez l'écoulement complet d'appel UCCE 11.6 avec SIP/TLS (le CA signé)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration de TLS d'A. Ingress Gateway de partie](#)

[Processus de configuration](#)

[Détails de configuration](#)

[Configuration de B. CVP TLS de partie](#)

[Processus de configuration](#)

[Détails de configuration](#)

[Partie C. VVB Configuration](#)

[Détails de configuration](#)

[Partie D. CUCM Configuration](#)

[Détails de configuration](#)

[Vérifier](#)

[Dépanner](#)

[Informations connexes](#)

Introduction

Ce document décrit le processus de configuration pour déployer le Protocole SIP (Session Initiation Protocol) au-dessus du Transport Layer Security (TLS) dans l'écoulement complet d'appel du Cisco Unified Contact Center Enterprise (UCCE) avec les Certificats signés d'Autorité de certification (CA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CUCCE
- Réseau téléphonique public commuté (PSTN)
- [Protocole SIP](#)
- [Infrastructure à clé publique \(PKI\)](#)
- TLS

Composants utilisés

Ces informations dans ce document sont basées sur des ces logiciel et versions de matériel :

- Routeur de Cisco 3945
- Customer Voice Portal de Cisco (CVP) 11.6
- Cisco a virtualisé le navigateur de Voix (VVB) 11.6
- Intelligent Contact Management de Cisco (missile aux performances améliorées) 11.6

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

Dans ce document, Cisco Unified Communications Manager (CUCM) est utilisé au côté de simulatePSTN entre le PSTN et la passerelle d'entrée. Le SIP au-dessus du Protocole TCP (Transmission Control Protocol) est utilisé entre l'agent CUCM et le téléphone IP d'agent. Tout autre SIP d'utilisation de tronçons de SIP au-dessus du TLS (CA signé).

L'écoulement complet d'appel UCCE est le **réseau téléphonique public commuté (PSTN) > passerelle d'entrée > Portail Cisco Unified Customer Voice (CVP) > l'Intelligent Contact Management (missile aux performances améliorées) (étiquette de retour d'agent) > CVP > Cisco Unified Communications Manager (CUCM) > téléphone IP d'agent.**

SIP/TLS est introduit sur la version 11.6 UCCE. Après mise à jour à CVP 11.6, assurez la configuration manuelle de finition de CVP unifié Properties.

UCCE 11.6 utilise le TLS 1.2, assure le TLS 1.2 de supports de passerelle d'entrée.

TLS 1.2 de support IOS 15.6(1) T et IOS XE 3.17S. TLS précédent 1.0 de supports de versions IOS seulement.

Les suites suivantes de chiffrement sont introduites pour le Cisco IOS 15.6(1)T de release :

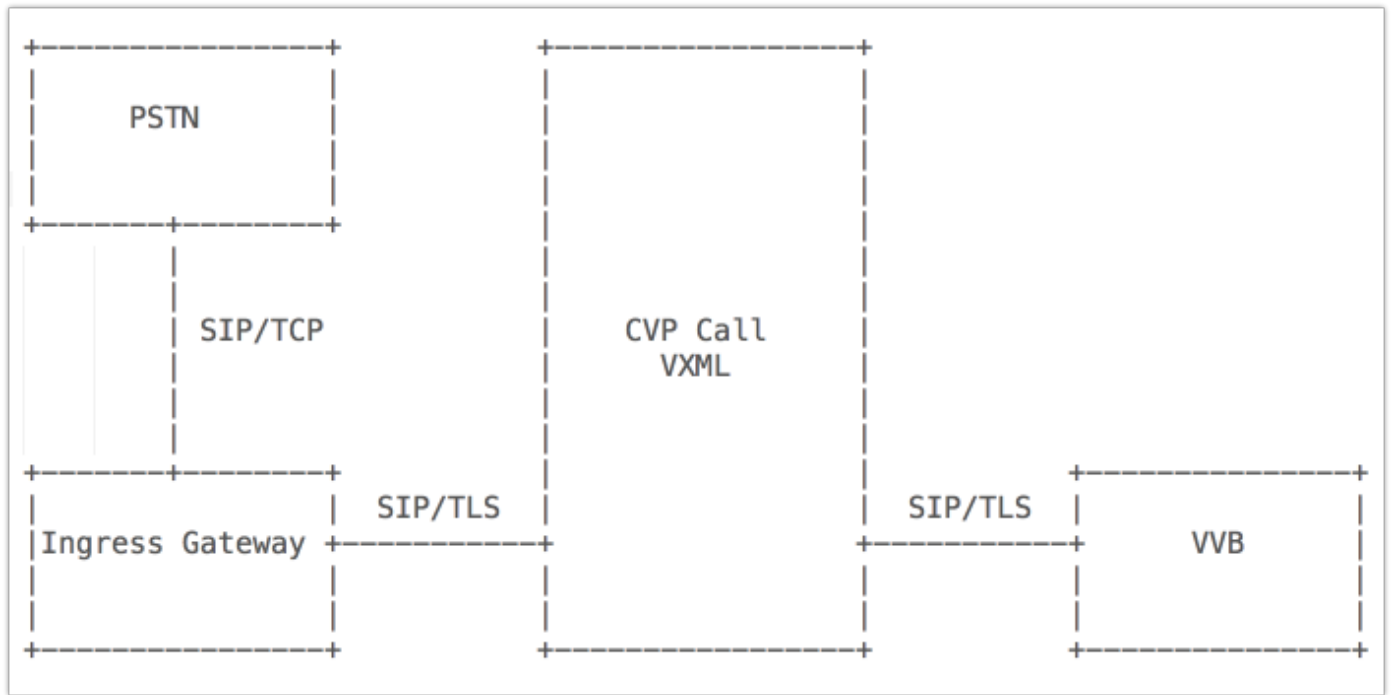
- du TLS_DHE_RSA_WITH_AES_128_CBC_SHA1
- du TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

La caractéristique du permis Securityk9 doit être activée dans la passerelle d'entrée.

VVB doit être mis à jour à 11.6.

Configuration

Diagramme du réseau



La configuration inclut quatre parts.

Configuration de TLS d'A. Ingress Gateway de partie

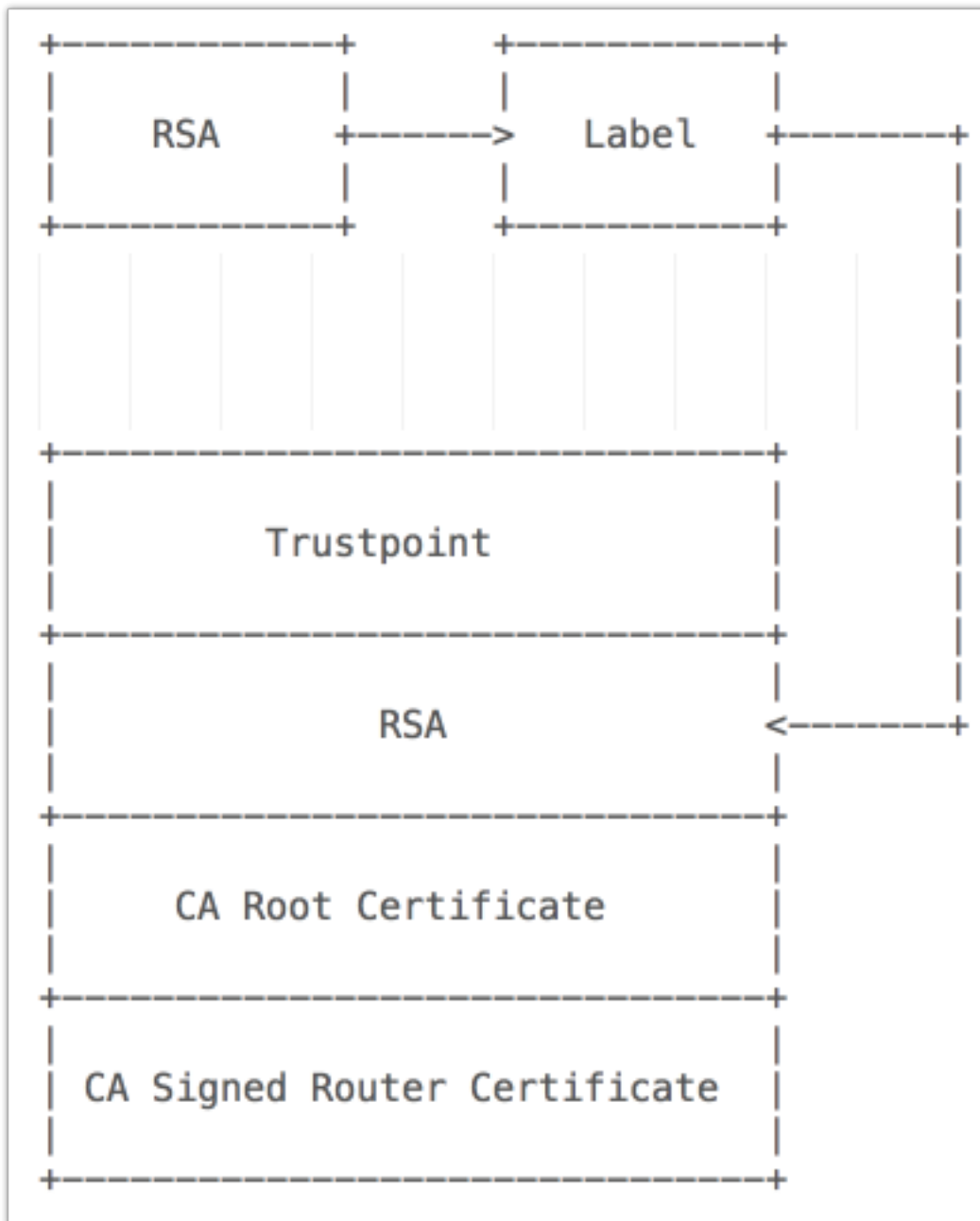
Configuration de B. CVP TLS de partie

Partie C. VVB Configuration

Partie D. CUCM Configuration

Configuration de TLS d'A. Ingress Gateway de partie

Processus de configuration



Détails de configuration

Étape 1. Générez la clé RSA sur le routeur (clé RSA 1024-bit).

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

Étape 2. Créez un point de confiance (un point de confiance représente un CA de confiance).

```
crypto pki trustpoint coll15ca
revocation-check none
serial-number none
ip-address none
fqdn none
rsa keypair INGW
subject-name cn=INGRESSGW, ou=TAC, o=CISCO
```

```
crypto pki trustpoint coll15ca
```

```
enrollment terminal
```

Étape 3. Créez une demande de certificat (CSR) qui sera envoyée au CA.

```
crypto ski enroll coll15ca
```

Étape 4. Certificat signé CA (CERT de bit CA de base 64).

Étape 5. Installez le certificat racine.

```
crypto pki authenticate coll15ca
```

Étape 6. Installez le certificat signé CA (CERT de base 64).

```
crypto pki import coll15ca certificate
```

Étape 7. Vérifiez les Certificats ont été installés.

```
show crypto pki certificates
```

Étape 8. Configurez la version de TLS sur la passerelle.

```
sip-ua
```

```
transport tcp tls v1.2
```

Étape 9. Spécifiez le selon la destination utilisé par point de confiance.

```
sip-ua
```

```
crypto signaling remote-addr 10.66.75.49 255.255.255.255 trustpoint coll15ca
```

Étape 10. Ajustez le cadran-pair qui indiquent CVP pour utiliser le TLS.

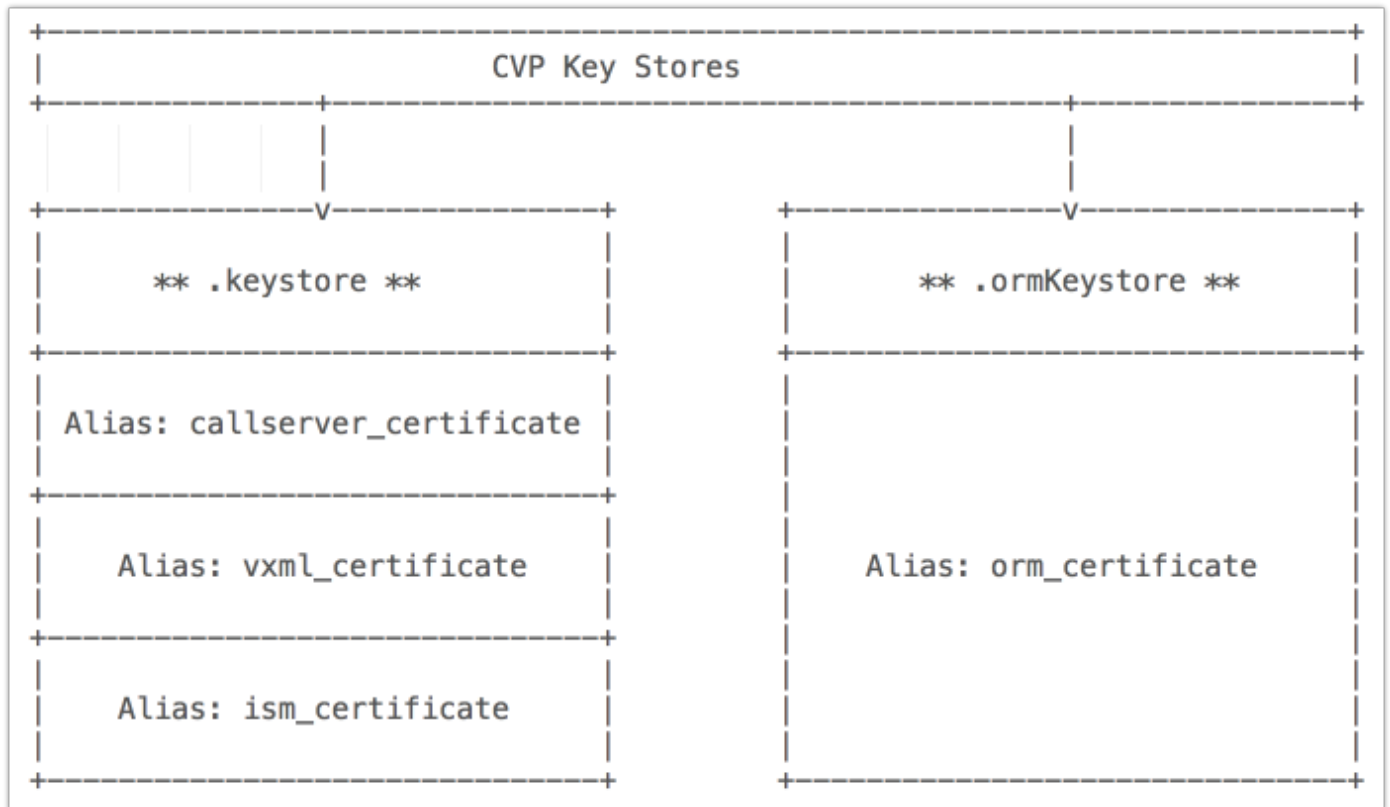
```
dial-peer voice 7205 voip
  description to CVP
  destination-pattern 700.$
  session protocol sipv2
  session target ipv4:10.66.75.49
  session transport tcp tls
  dtmf-relay rtp-nte
  codec g711ulaw
```

Configuration de B. CVP TLS de partie

Processus de configuration

CVP a deux mémoires principales, situées à `c:\Cisco\CVP\conf\security`.

Suivant les indications de l'image, ces deux mémoires principales tiennent différents Certificats.



Détails de configuration

Étape 1. Naviguez vers le serveur d'appel de `c:\Cisco\CVP\conf\security.properties` in CVP afin de trouver ce mot de passe. Ce fichier contient le mot de passe pour la mémoire principale, qui est exigée en actionnant la mémoire principale.

Étape 2. Paramètres systèmes par défaut Callserver_certificate d'effacement.

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

Étape 3. Générez le 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
```

Étape 4. Créez un CSR et sauvegardez-le dans le répertoire de racine de C : drive (`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
```

Étape 5. Signez la demande et soumettez la demande au CA (quand vous téléchargez le CERT, choisissez la base 64 encodée).

Étape 6. Installez le certificat racine (CERT enregistré chez `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
```

Étape 7. Installez le certificat signé CA (CERT enregistré à 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
```

Étape 8. Vérifiez les détails de certificat dans la mémoire principale.

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

Partie C. VVB Configuration

Détails de configuration

Étape 1. TLS d'enable de paramètre de système

Cet exemple utilise le RTP, ainsi SRTP sur VVB n'est pas activé.

The screenshot displays the 'System Parameters Configuration' interface. At the top, there are 'Update' and 'Clear' buttons. Below that, the status is 'Ready'. The configuration is organized into three main sections:

- Generic System Parameter:** A table with two columns: 'Parameter Name' and 'Parameter Value'. The entry is 'System Time Zone' with the value 'Australian Eastern Standard Time (New South Wales)'.
- Media Parameters:** A table with two columns: 'Parameter Name' and 'Parameter Value'. The entries are:
 - Codec: G711U
 - MRCP Version: MRCPv2
 - User Prompts override System Prompts: Disable Enable
- Security Parameters:** A table with two columns: 'Parameter Name' and 'Parameter Value'. The entries are:
 - TLS(SIP): Disable Enable
 - Supported TLS(SIP) Versions: TLSv1.2
 - Cipher Configuration: (expanded section)
 - SRTP: Disable Enable Allow RTP (Mixed mode)

Étape 2. Générez et importez le certificat signé CA pour VVB, la présente partie est les mêmes que certificat de chat CUCM

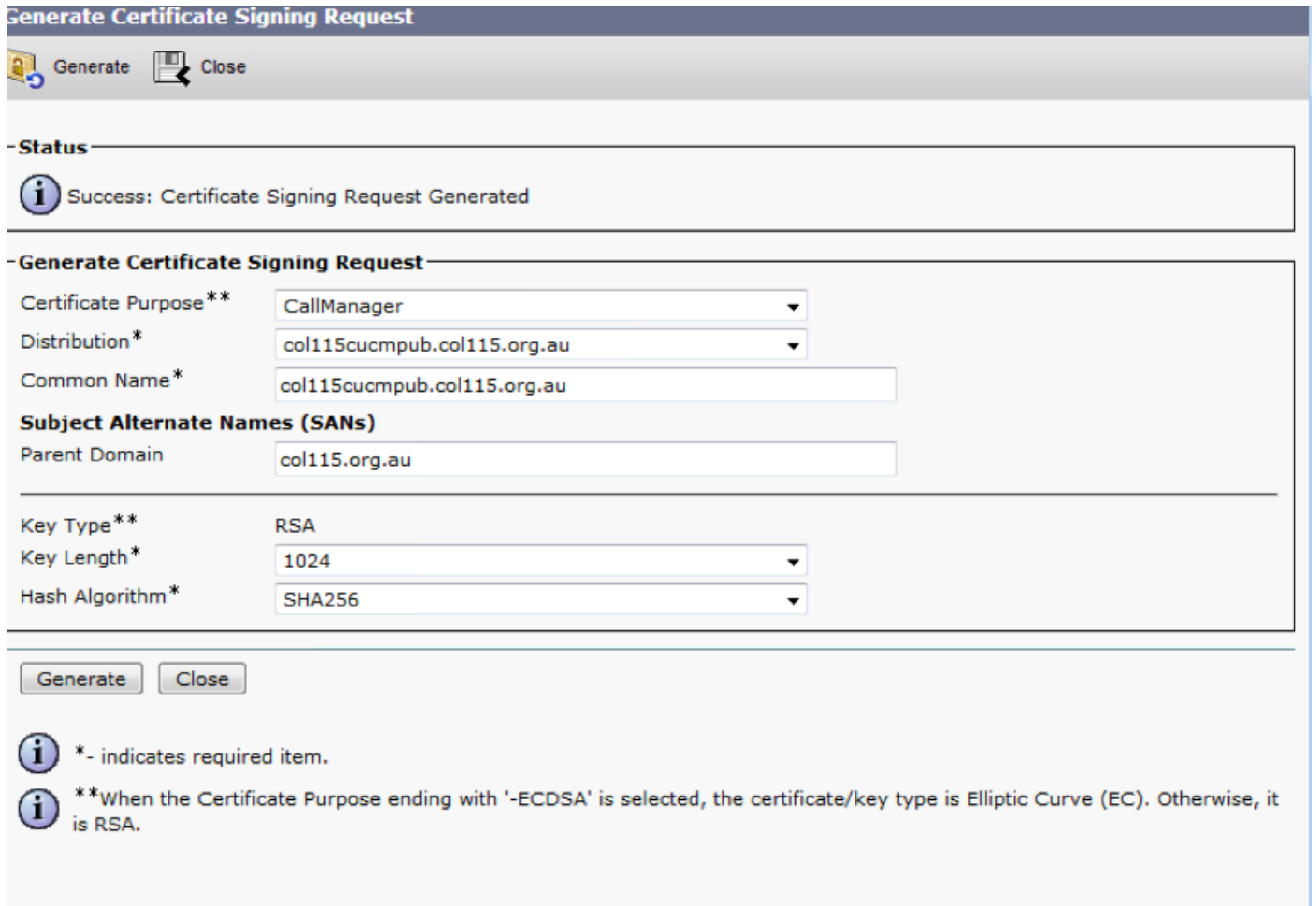
- Générez le CSR et signé par CA.
- Confiance de Tomcat d'importation (CERT de racine CA).
- Importation Tomcat (CERT signé par CA).

Partie D. CUCM Configuration

Détails de configuration

Étape 1. Le téléchargement CA a signé le certificat de callmanager dans le serveur CUCM. CUCM utilise le certificat de callmanager pour SIP/TLS.

Étape 2. Générez le CSR pour le certificat de callmanager, assurez-vous que la longueur principale est 1024.



Generate Certificate Signing Request

Generate Close

-Status-

i Success: Certificate Signing Request Generated

-Generate Certificate Signing Request-

Certificate Purpose** CallManager

Distribution* col115cucmpub.col115.org.au

Common Name* col115cucmpub.col115.org.au

Subject Alternate Names (SANs)

Parent Domain col115.org.au

Key Type** RSA

Key Length* 1024

Hash Algorithm* SHA256

Generate Close

i *- indicates required item.

i **When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Étape 3. Fournissez le CSR au CA et récupérez le certificat de callmanager.

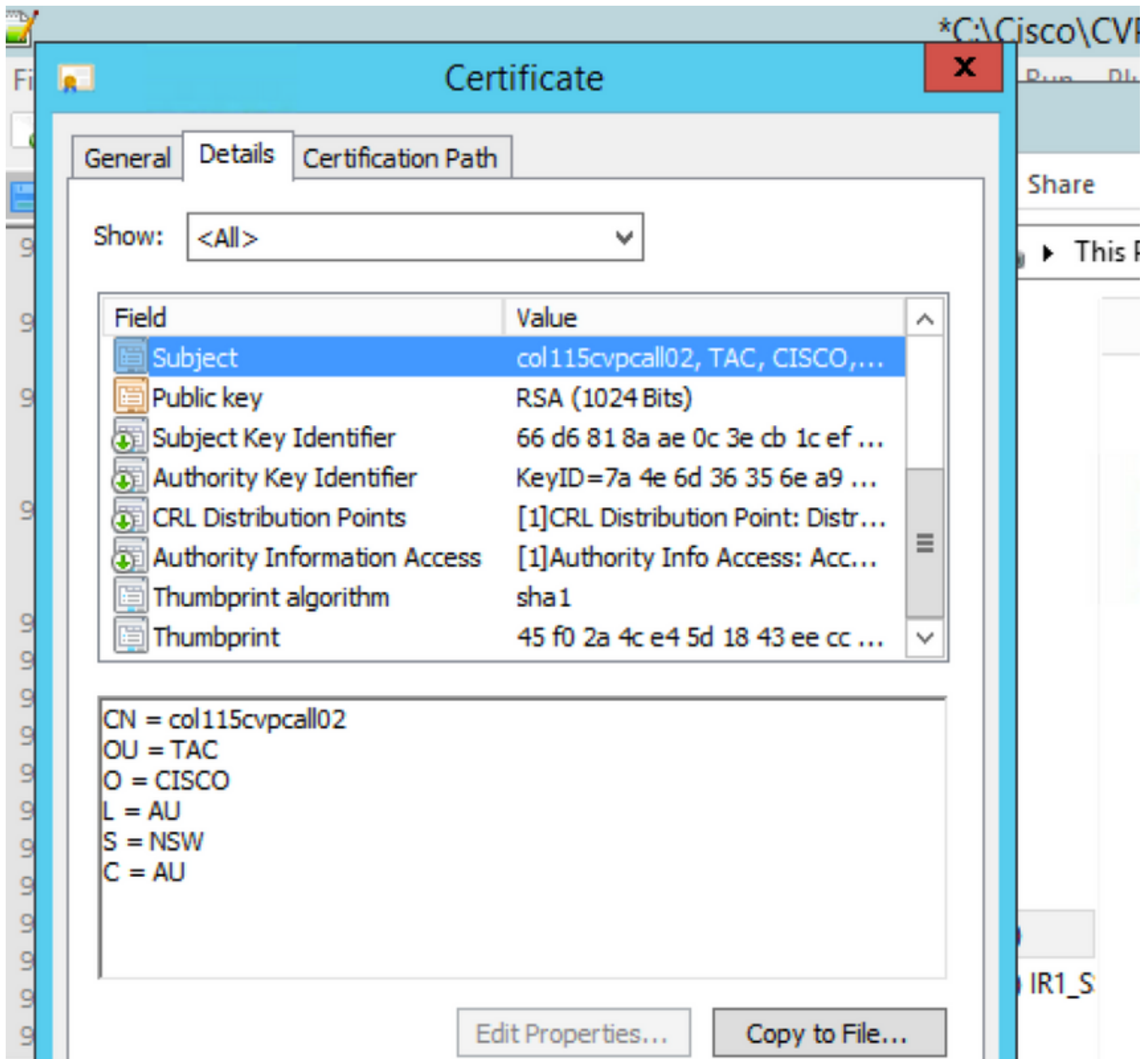
Étape 4. Importez le certificat de CA de racine et le certificat récemment signé de callmanager.

Étape 5. Callmanager et services TFTP de reprise.

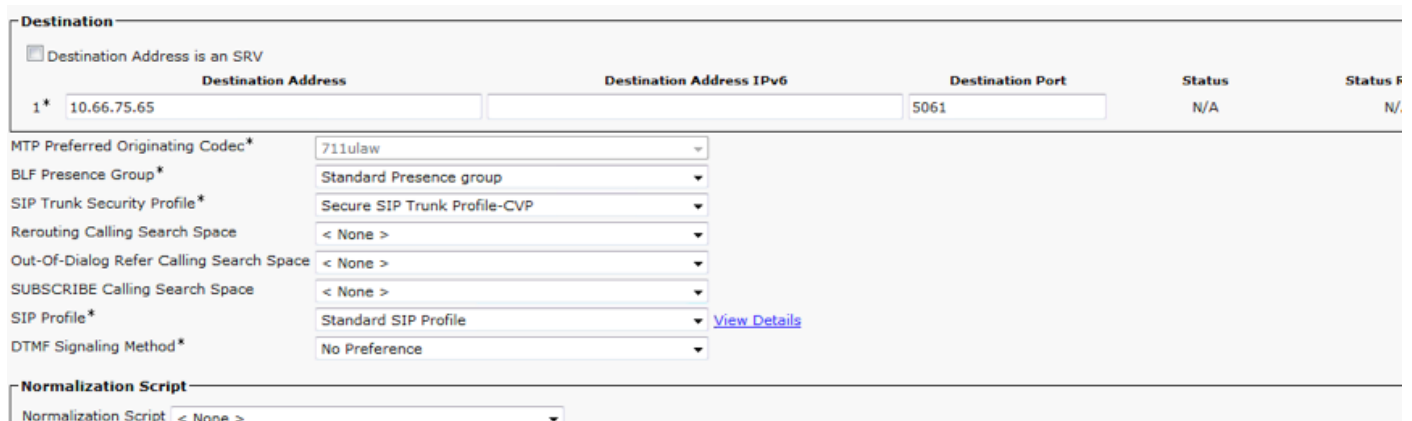
Étape 6. Configurez le profil de Sécurité de joncteur réseau de SIP. Naviguez **profil de Sécurité** vers le **système > la Sécurité > de SIP joncteur réseau**

Assurez que le nom du sujet X.509 correspond il est utilisé sur le certificat de serveur d'appel CVP, suivant les indications des images.

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
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	col115cvpcall02
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input checked="" type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	



Étape 7. Créez le joncteur réseau de SIP et allouez-le à un profil de Sécurité.



Vérifiez

Vérifiez les Certificats installés dans la passerelle d'entrée.

```
show crypto pki certificates
```

Vérifiez les détails de certificat dans la mémoire de clé CVP.

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

Dépanner

Commandes de debug liées au TLS.

```
debug ssl openssl errors
```

```
debug ssl openssl msg
```

```
debug ssl openssl states
```

Informations connexes

- 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
- [Support et documentation techniques - Cisco Systems](#)