

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Les informations de Background](#)

[Configuration](#)

[Diagramme du réseau](#)

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

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

[Partie C. VVB Configuration](#)

[Partie D. CUCM Configuration](#)

[Vérifiez](#)

[Dépannez](#)

[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 par Autorité de certification (CA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- 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 V1.2 de supports de passerelle d'entrée. D'IOS 15.6(1) T et d'IOS XE 3.17S, le TLS 1.2 de support, IOS précédent a utilisé le TLS 1.0.

Support de version 1.2 de TLS de SIP sur le CUBE	Cisco IOS 15.6(1)T Cisco IOS XE 3.17S
--	--

Le support est donné pour des appels de Sip-à-SIP en version 1.2 de Transport Layer Security (TLS).
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.

Composants utilisés

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

- Routeur de Cisco 3945
- CVP 11.6
- Cisco a virtualisé la Voix Broswer (VVB) 11.6
- 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

Les informations de Backgroud

D'UCCE 11.6, SIP/TLS est introduit.

C'est l'écoulement complet d'appel UCCE : **Le public a commuté le réseau de telepone (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.**

Dans ce document, CUCM est utilisé pour simuler le côté PSTN entre le PSTN et le SIP de passerelle d'entrée au-dessus du Protocole TCP (Transmission Control Protocol) est usedBetween l'agent CUCM et l'agent que le téléphone IP SIP/TCP est utilisé toute autre utilisation SIP/TLS (le CA de tronçons de SIP signé)

Configuration

La configuration inclut quatre parts.

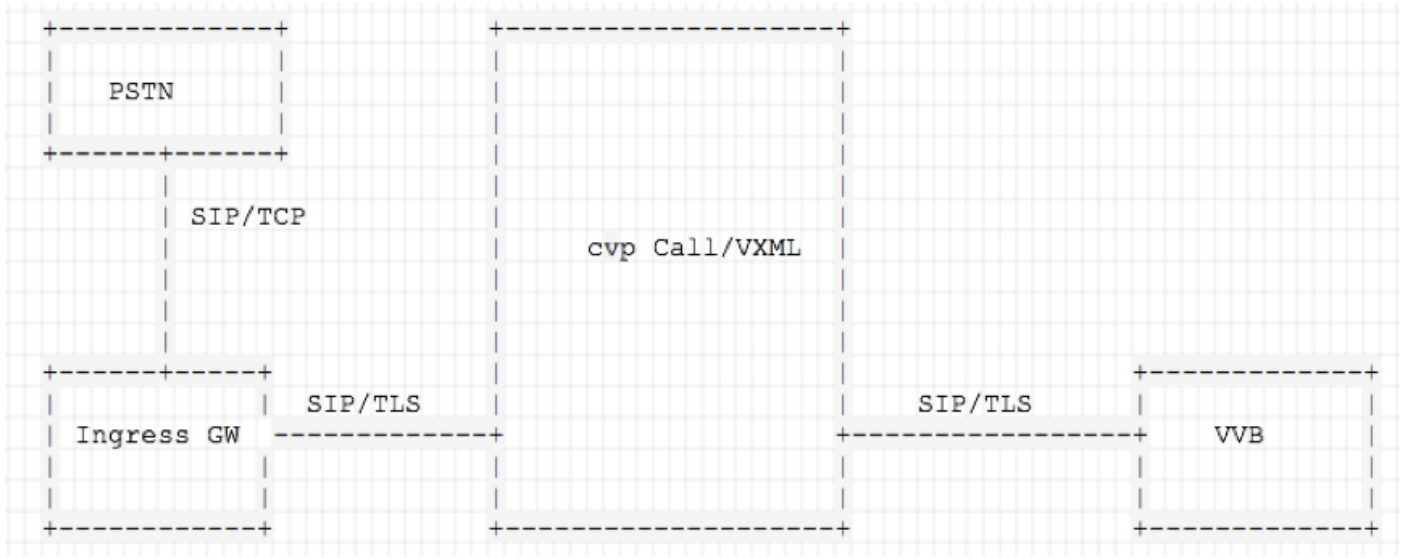
Partie A. Ingress Gateway

Partie B. CVP

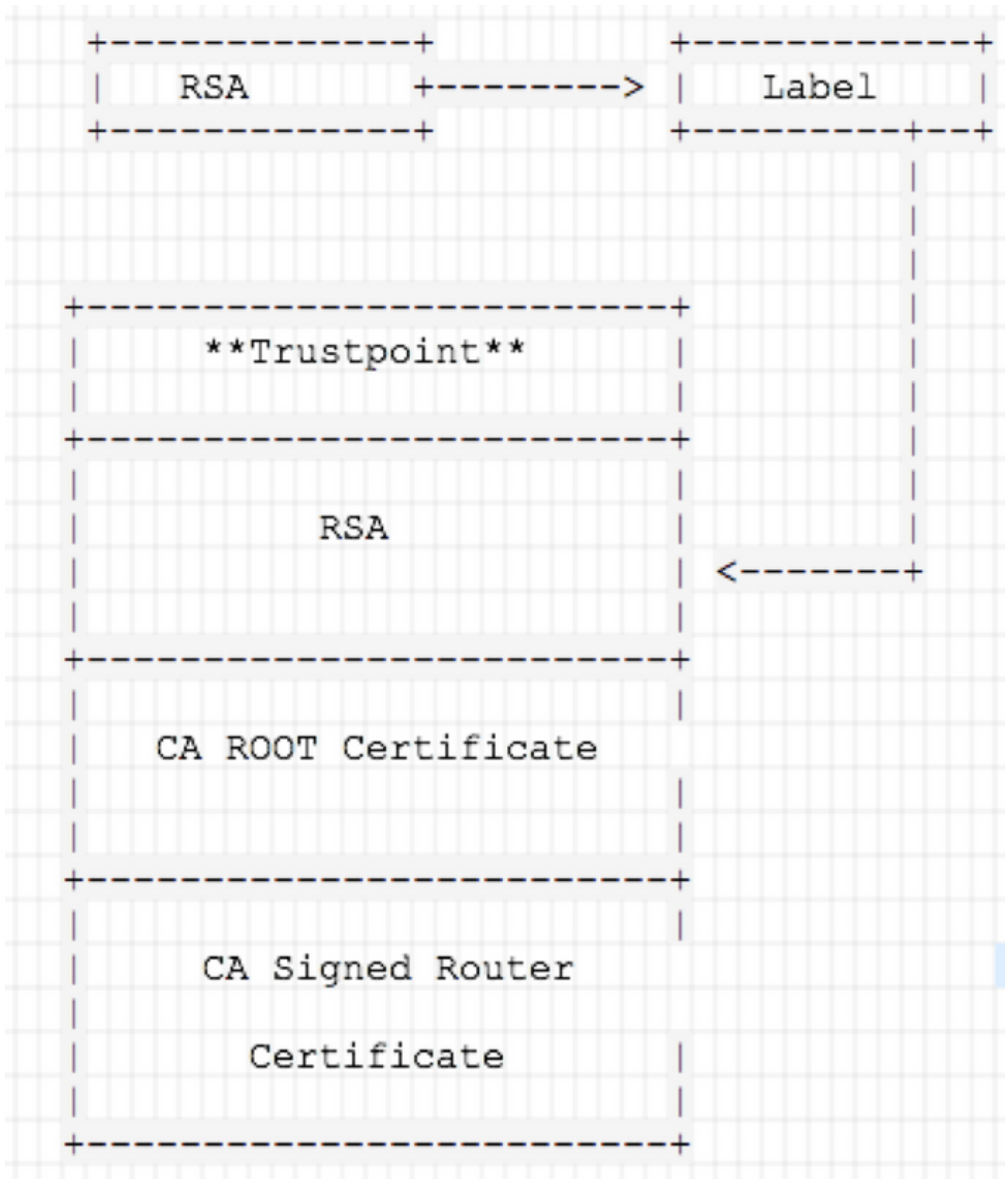
Partie C. VVB

Partie D. CUCM

Diagramme du réseau



Configuration de TLS d'A. Ingress Gateway de partie



Étapes générales :

Étape 1. Créez la clé RSA.

Étape 2. Créez le point de confiance.

Étape 3. Créez une demande de certificat.

Étape 4. Soumettez la demande au CA et avez signé la demande.

Étape 5. Installez le certificat racine.

Étape 6. Installez le certificat signé CA.

Détails de configuration :

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

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

2. Create un point de confiance (le point de confiance A représente un CA de confiance).

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

```
crypto pki trustpoint coll15ca
```

```
enrollment terminal
```

3. Créez une demande de certificat (le CSR qui sera envoyé au CA).

```
crypto ski enroll coll15ca
```

4. Certificat brûlé légèrement par CA (CERT de bit CA de base 64).

5. Installez le certificat racine.

```
crypto pki authenticate coll15ca
```

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

```
crypto pki import coll15ca certificate
```

7. Vérifiez les Certificats ont été installés correctement.

```
show crypto pki certificates
```

8. Configurez la version de TLS sur la passerelle.

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

selon la destination 9. sepecify utilisé par point de confiance.

```
sip-ua
```

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

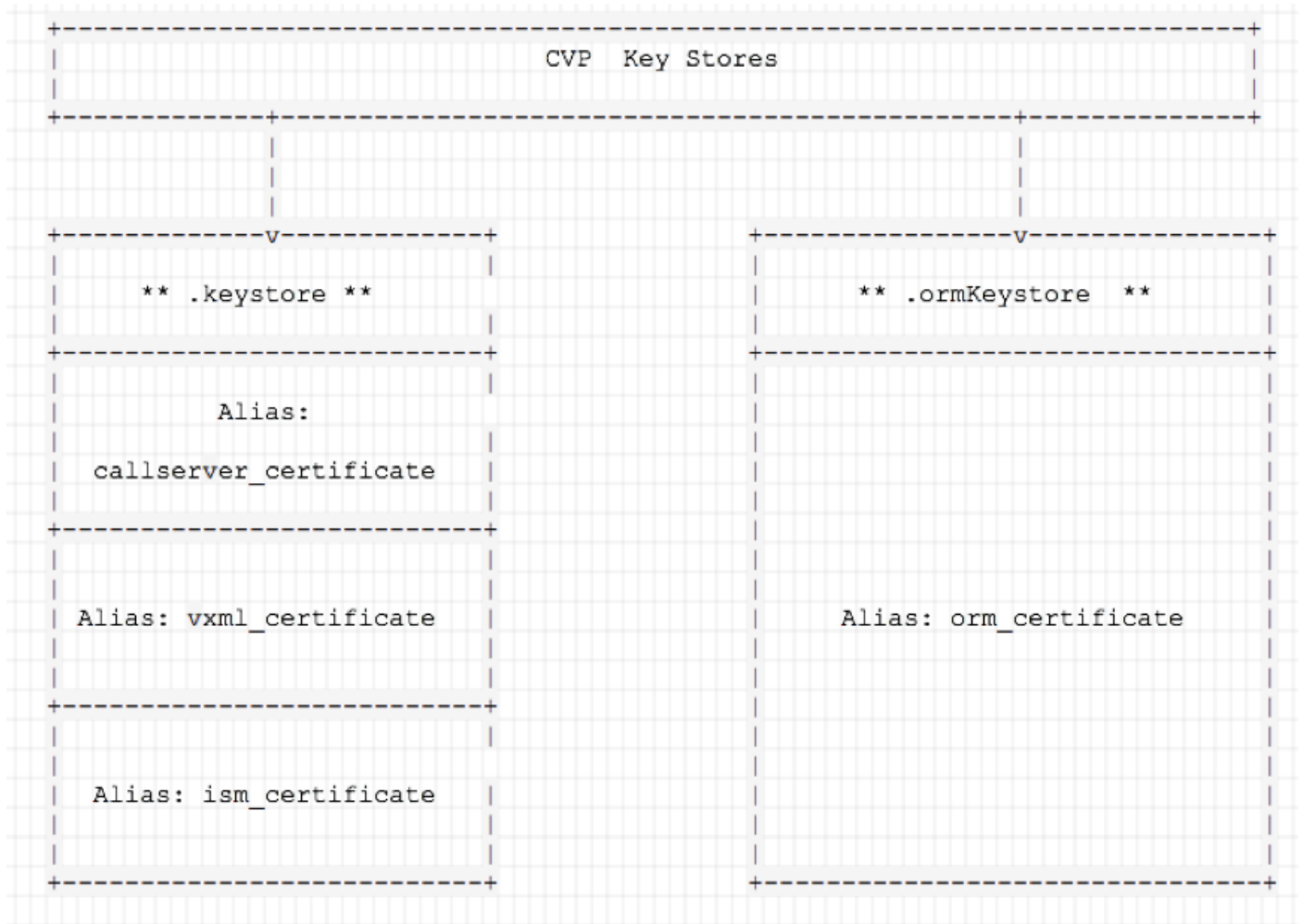
10. Ajustez le cadran-pair qui indiquent CVP pour utiliser le TLS

```
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

CVP a deux keystores, situés à `c:\Cisco\CVP\conf\security`.

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



Étapes générales :

Étape 1. Paramètres systèmes par défaut `Callserver_certificate` d'effacement.

Étape 2. Générez le keypair.

Étape 3. Créez une demande de certificat (CSR).

Étape 4. Soumettez la demande au CA et avez signé la demande.

Étape 5. Installez le certificat racine.

Étape 6. Installez le certificat signé CA.

Détails de configuration :

Quand actionnez le keystore, demande de système d'entrer le mot de passe

Mot de passe de découverte pour le keystore.

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 le keystore, qui est exigé en actionnant le keystore.

1. Paramètres systèmes par défaut `Callserver_certificate` d'effacement.

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

2. Générez le keypair.

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

Étape 3. Créez une demande de certificat (CSR) et l'enregistrez dans le répertoire de racine de C : drive (`c:\callcsr.csr`).

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

```
- keystore c:\Cisco\CVP\conf\security\ .keystore
```

Étape 4. Signez la demande et l'submit la demande au CA.

(quand vous téléchargez le CERT, choisissez la base 64 encodée)

Étape 5. Installez le certificat racine (CERT enregistré chez `C:\ DC-Root.cer`).

```
C:\Cisco\CVP\jre\bin >keytool.exe - importation - v - trustcacerts - alias racine
```

```
- fichier C:\ DC-Root.cer - storetype JCEKS
```

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

Étape 6. Installez le certificat signé CA (CERT enregistré à `c:\95callserver.cer`).

```
C:\Cisco\CVP\jre\bin >keytool.exe - importation - v - des trustcacerts - alias callserver_certificate -  
fichier c:\95callserver.cer - storetype JCEKS
```

```
- keystore c:\Cisco\CVP\conf\security\ .keystore
```

Étape 7. Vérifiez les détails de certificat dans la mémoire principale.

```
C:\Cisco\CVP\jre\bin >keytool.exe - liste - v - storetype JCEKS
```

```
- keystore c:\Cisco\CVP\conf\Sécurité\ .keystore
```

Partie C. VVB Configuration

TLS d'enable de paramètre de système

Dans cette configuration, le RTP d'utilisations, ainsi n'a pas activé SRTP sur VVB.

The screenshot displays the 'System Parameters Configuration' interface for a Cisco VVB. It features a navigation menu at the top with 'System', 'Applications', 'Subsystems', 'Tools', and 'Help'. Below the menu, there are 'Update' and 'Clear' buttons. The 'Status' section shows 'Status : 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), and 'User Prompts override System Prompts' (Disable).
- Security Parameters:** A table with two columns: 'Parameter Name' and 'Parameter Value'. The entries are: 'TLS(SIP)' (Enable), 'Supported TLS(SIP) Versions' (TLSv1.2), and 'SRTP' (Disable). There is also an unchecked checkbox for 'Allow RTP (Mixed mode)'.

Le certificat signé CA pour VVB, la présente partie est identique comme 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

Étapes générales :

1. Le CA téléchargé a signé le certificat de callmanager dans le serveur CUCM.
2. créez le profil de Sécurité de joncteur réseau de SIP.
3. Créez le joncteur réseau de SIP entre le serveur CUCM et CVP.

Détails de configuration :

Étape 1. Le CA téléchargé a signé le certificat de callmanager dans le serveur CUCM.


1. CUCM utilise le certificat de callmanager pour SIP/TLS.
2. Générez le CSR pour le certificat de callmanager, assurez-vous que la longueur principale est 1024.

3. A signé ce certificat de Callmanager par CA.
4. Certificat de CallManager-confiance d'importation (certificat de CA de racine).
5. Certificat de callmanager d'importation (certificat signé CA).
6. Services et services TFTP de callmanager de reprise.

Generate Certificate Signing Request

Generate Close

-Status-

 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

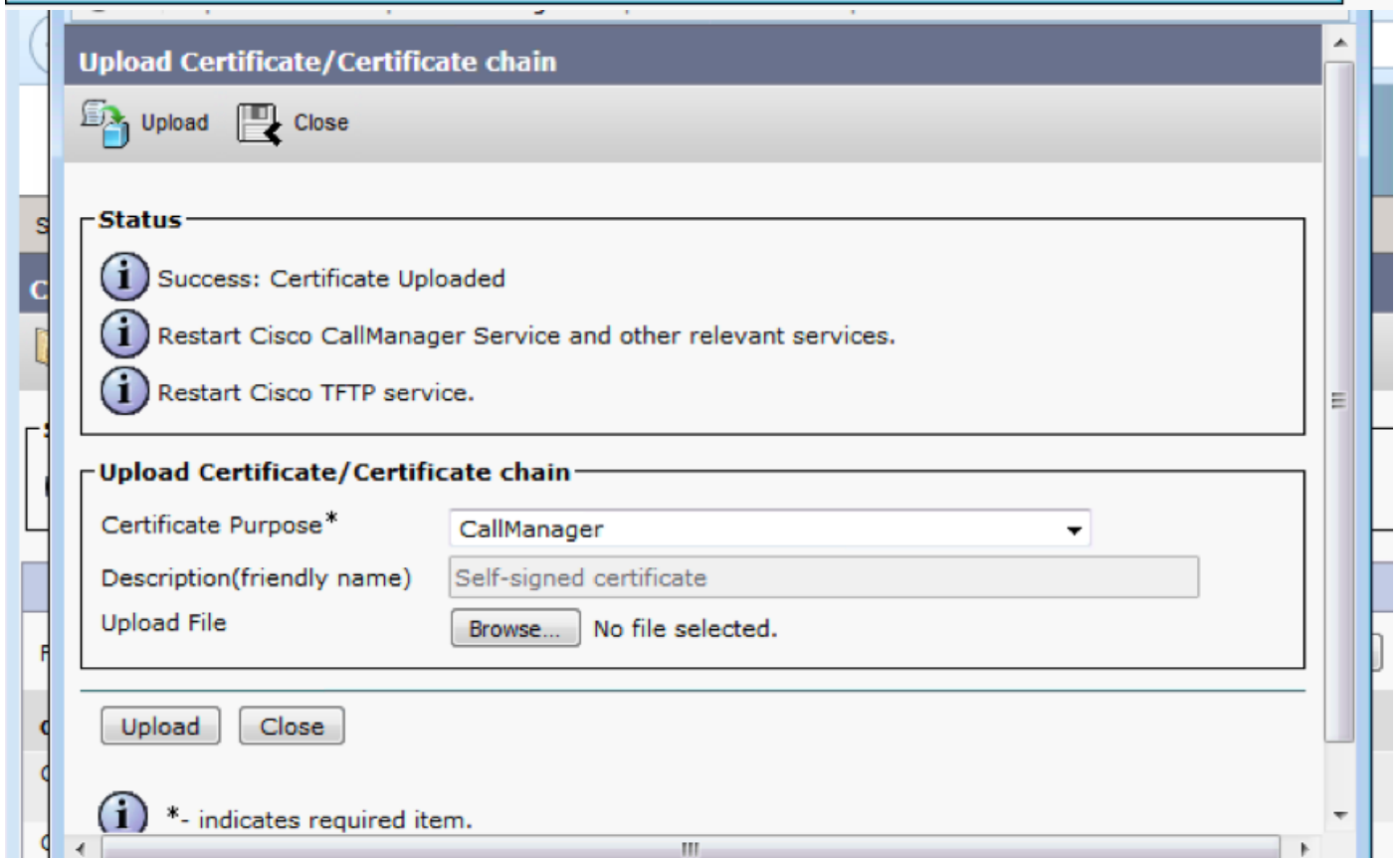
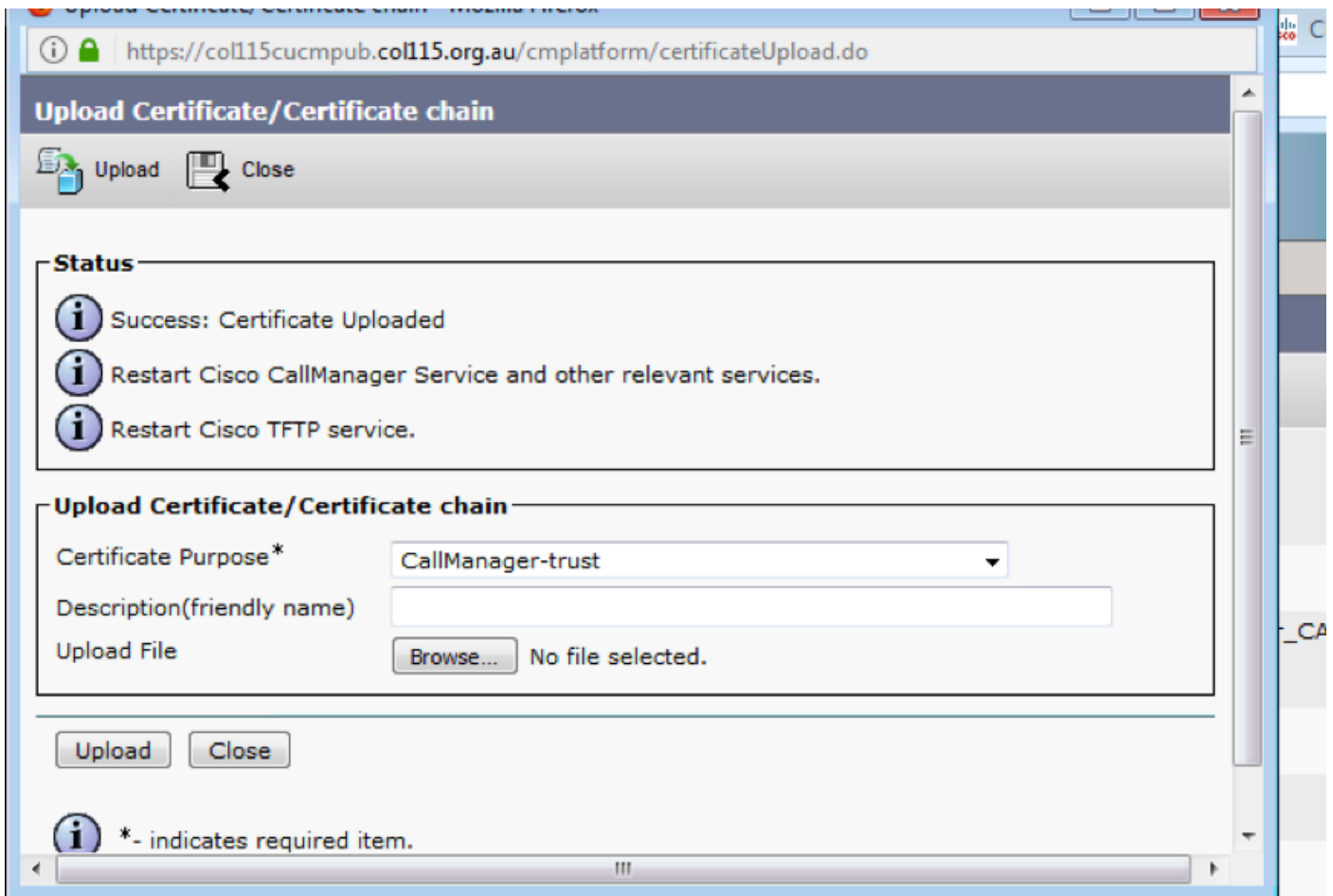
Key Length* 1024

Hash Algorithm* SHA256

Generate Close

 *- indicates required item.

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



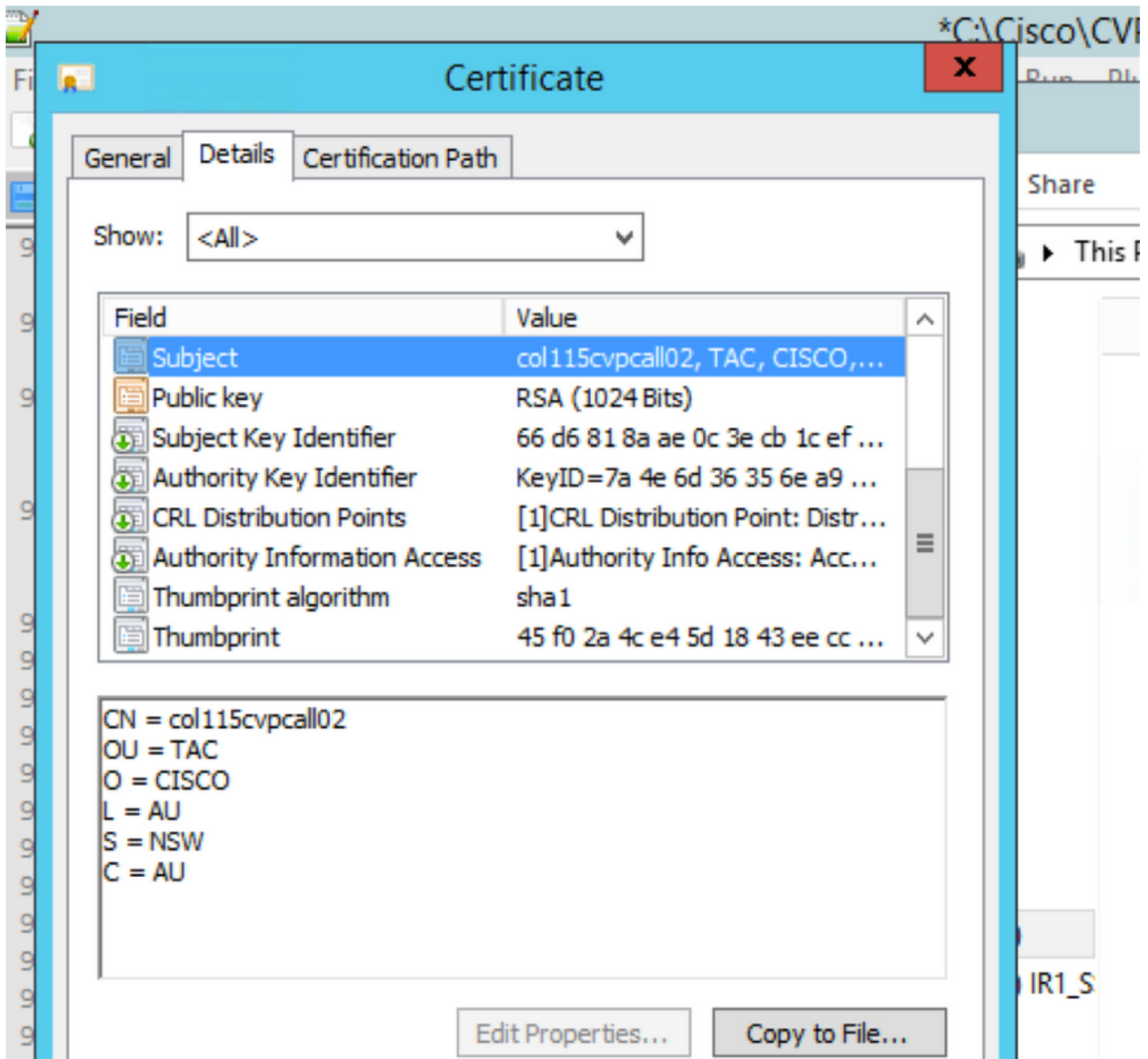
Étape 2. Configurez le profil de Sécurité de joncteur réseau de SIP.

Naviguez **profil de Sécurité** vers le **systeme > la Sécurité > de SIP joncteur réseau**

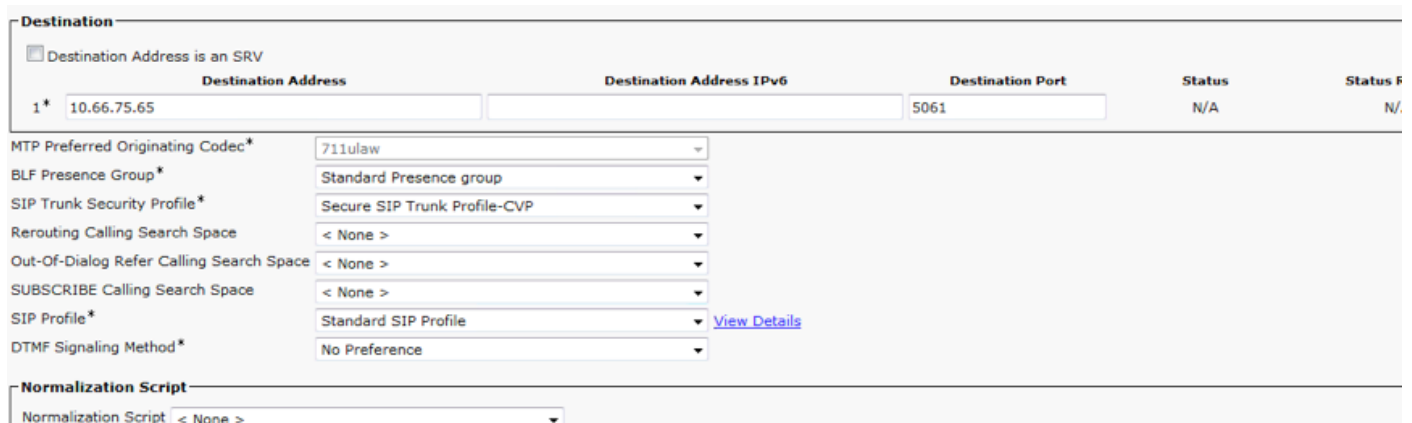
Assurez que le nom du sujet X.509 correspond il est utilisé sur le certificat de serveur d'appel

CVP, suivant les indications de l'image.

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 3. Créez le joncteur réseau de SIP et allouez le profil de Sécurité de joncteur réseau de SIP.



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 - liste - v - storetype JCEKS
```

```
- keystore c:\Cisco\CV P \ conf \ Sécurité \ .keystore
```

Dépannez

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](#)