

Configurer la liaison SIP TLS sur Communications Manager avec un certificat signé CA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Étape 1. Utiliser l'autorité de certification publique ou la configuration de l'autorité de certification sur Windows Server 2003](#)

[Étape 2. Vérifier le nom d'hôte et les paramètres](#)

[Étape 3. Générer et télécharger la demande de signature de certificat \(CSR\)](#)

[Étape 4. Signer le CSR avec l'autorité de certification Microsoft Windows 2003](#)

[Étape 5. Obtenir le certificat racine de l'autorité de certification](#)

[Étape 6. Télécharger le certificat racine CA en tant que CallManager Trust](#)

[Étape 7. Télécharger le certificat CSR CallManager en tant que certificat CallManager.](#)

[Étape 8. Créer des profils de sécurité de liaison SIP](#)

[Étape 9. Créer des liaisons SIP](#)

[Étape 10. Créer des modèles de routage](#)

[Vérification](#)

[Dépannage](#)

[Collecter la capture de paquets sur CUCM](#)

[Collecter les traces CUCM](#)

Introduction

Ce document décrit un processus étape par étape pour configurer la liaison TLS (Transport Layer Security) SIP (Session Initiation Protocol) sur Communications Manager avec un certificat signé Autorité de certification (CA).

Après avoir suivi ce document, les messages SIP entre deux clusters seront chiffrés à l'aide de TLS.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître :

- Gestionnaire de communications unifiées de Cisco (version CUCM)

- SIP

Components Used

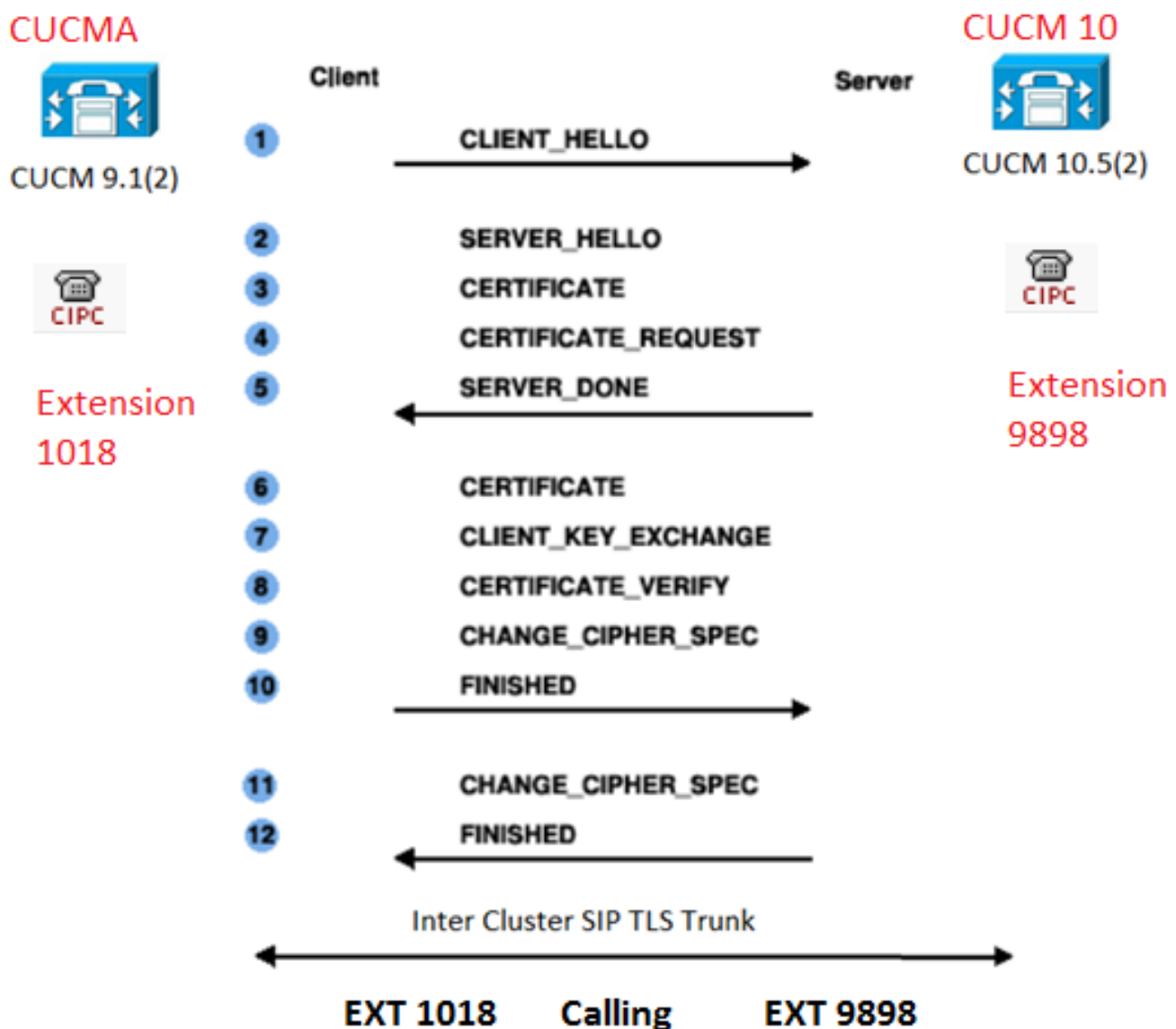
Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- CUCM version 9.1(2)
- CUCM version 10.5(2)
- Microsoft Windows Server 2003 en tant qu'autorité de certification

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.

Informations générales

Comme l'illustre cette image, la connexion SSL à l'aide de certificats.



Étape 1. Utiliser l'autorité de certification publique ou la configuration de l'autorité de certification sur Windows Server 2003

Reportez-vous au lien : [Configurer l'autorité de certification sur le serveur Windows 2003](#)

Étape 2. Vérifier le nom d'hôte et les paramètres

Les certificats sont basés sur des noms. Assurez-vous que les noms sont corrects avant de commencer.

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

Pour modifier le nom d'hôte, reportez-vous au lien : [Modifier le nom d'hôte sur CUCM](#)

Étape 3. Générer et télécharger la demande de signature de certificat (CSR)

CUCM 9.1(2)

Pour générer le CSR, accédez à **OS Admin > Security > Certificate Management > Generate CSR**.


Dans le champ **Nom du certificat**, sélectionnez **CallManager** dans la liste déroulante.

The screenshot shows a web-based dialog box titled "Generate Certificate Signing Request". At the top, there are two buttons: "Generate CSR" (with a lock icon) and "Close" (with a document icon). Below this is a "Status" section containing a yellow warning triangle icon and the text: "Warning: Generating a new CSR will overwrite the existing CSR". The main area of the dialog is titled "Generate Certificate Signing Request" and contains a dropdown menu labeled "Certificate Name*" with "CallManager" selected. At the bottom of the dialog, there are two buttons: "Generate CSR" and "Close".

Pour télécharger le CSR, accédez à **OS Admin > Security > Certificate Management > Download CSR**.

Dans le champ **Nom du certificat**, sélectionnez **CallManager** dans la liste déroulante.

Download Certificate Signing Request

 Download CSR  Close

Status

 Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request



Certificate Name*

CUCM 10.5(2)


Pour générer le CSR, accédez à OS Admin > Security > Certificate Management > Generate CSR.

1. Dans le champ Objet du certificat, sélectionnez CallManager dans la liste déroulante.
2. Dans le champ Longueur de clé, sélectionnez 1024 dans la liste déroulante..
3. Dans le champ Hash Algorithm, sélectionnez SHA1 dans la liste déroulante.

Generate Certificate Signing Request

 Generate  Close

Status

 Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*

Distribution*

Common Name*

Subject Alternate Names (SANs)



Parent Domain

Key Length*

Hash Algorithm*

Pour télécharger le CSR, accédez à OS Admin > Security > Certificate Management > Download CSR. Dans le champ Objet du certificat, sélectionnez CallManager dans la liste déroulante.

Download Certificate Signing Request

 Download CSR  Close


Status



Certificate names not listed below do not have a corresponding CSR

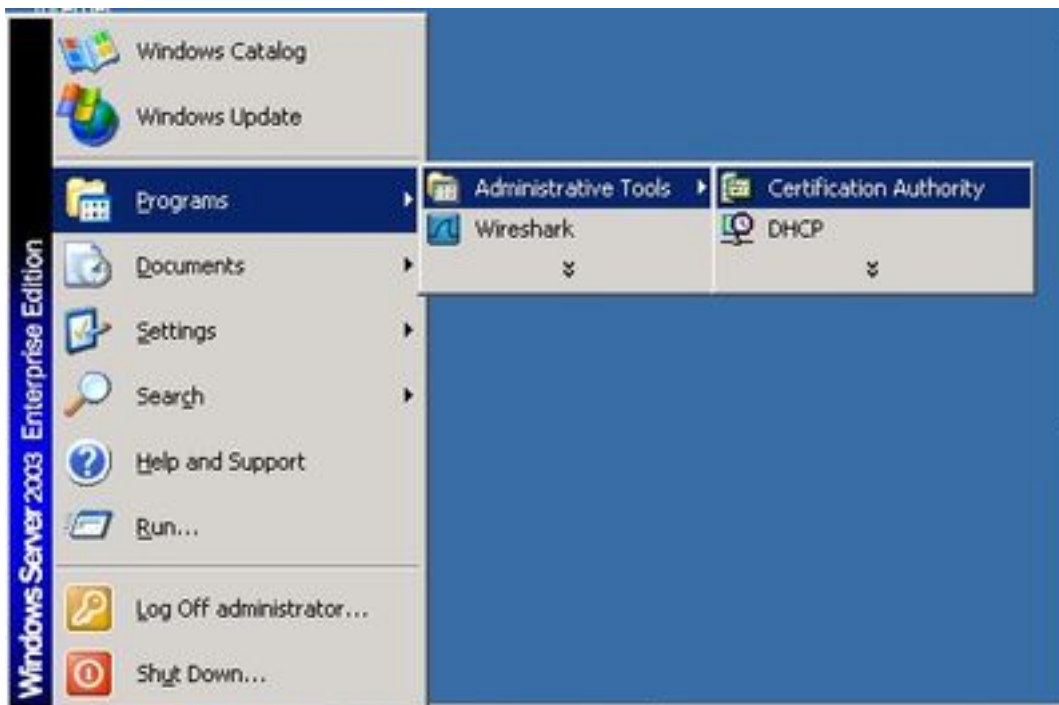
Download Certificate Signing Request

Certificate Purpose*

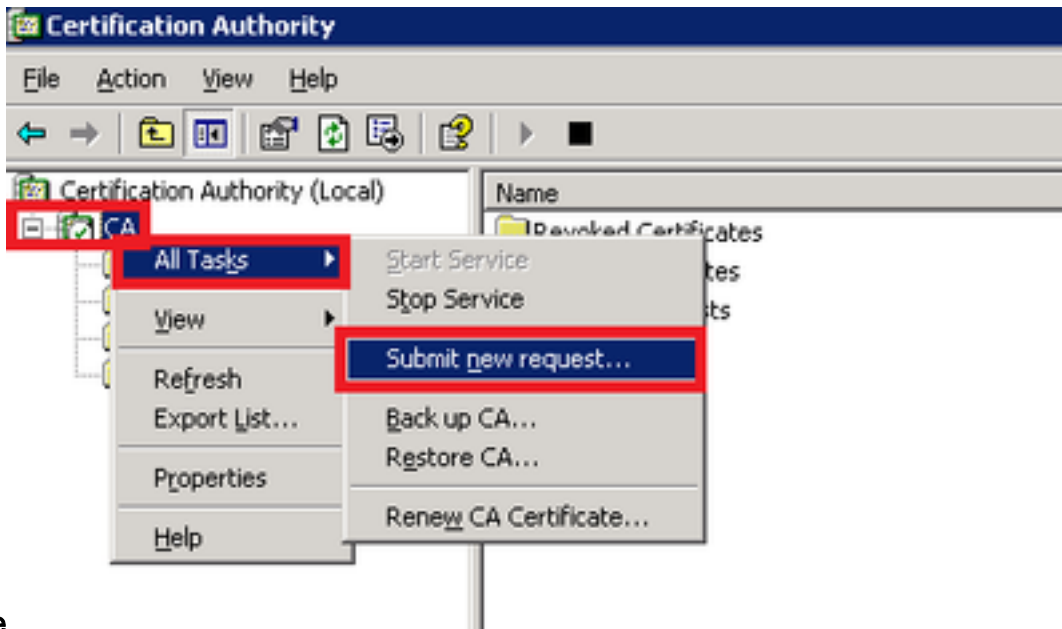
 Download CSR

 Close

Note: Le CSR CallManager est généré avec les clés RSA (Rivest-Shamir-Addleman) 1 024 bits. Étape 4. Signer le CSR avec l'autorité de certification Microsoft Windows 2003. Il s'agit d'une information facultative permettant de signer le CSR avec l'autorité de certification Microsoft Windows 2003.1. Ouvrez l'autorité de



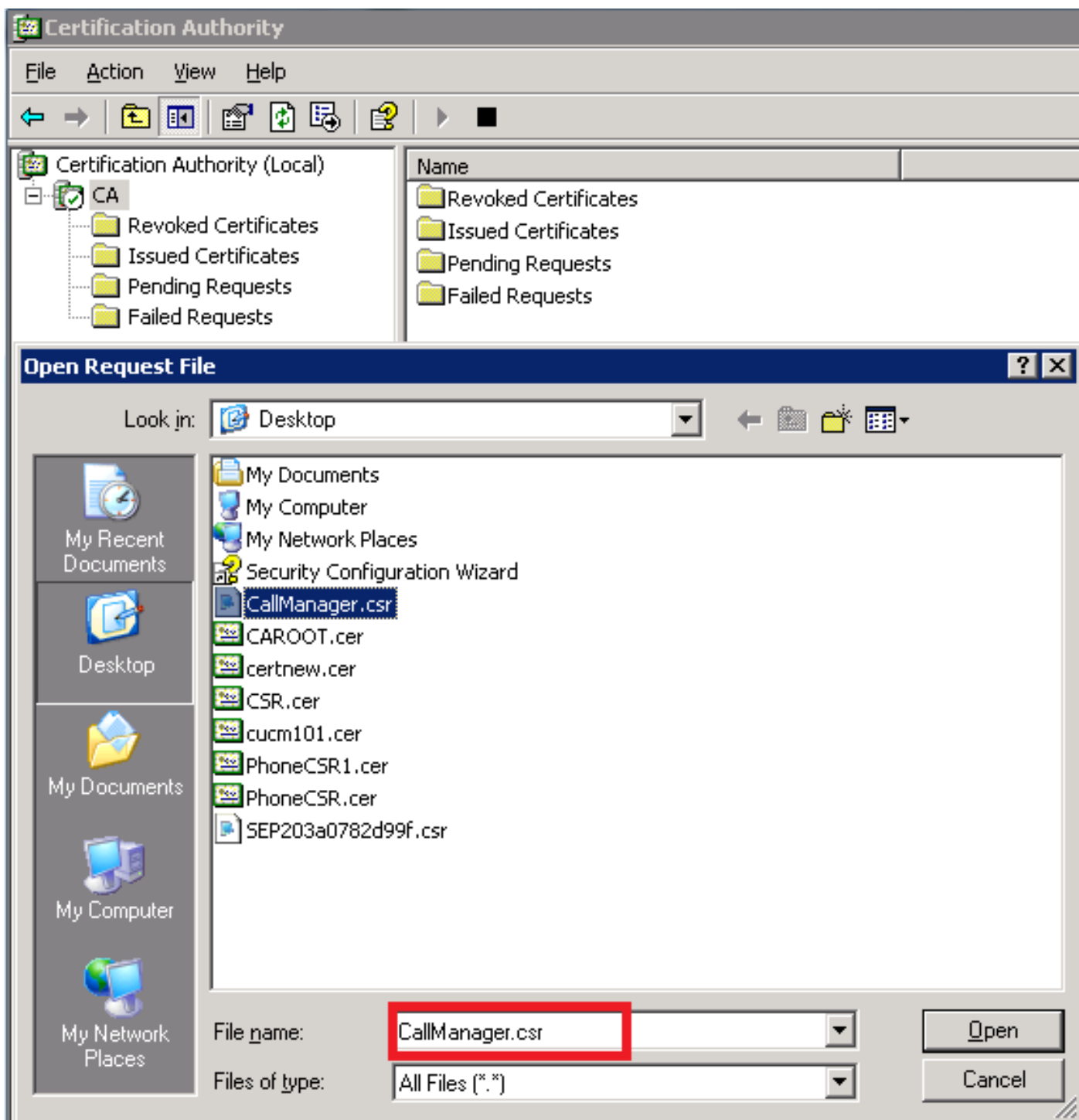
certification. 2. Cliquez avec le bouton droit sur l'icône AC et accédez à Toutes les tâches > Soumettre une nouvelle



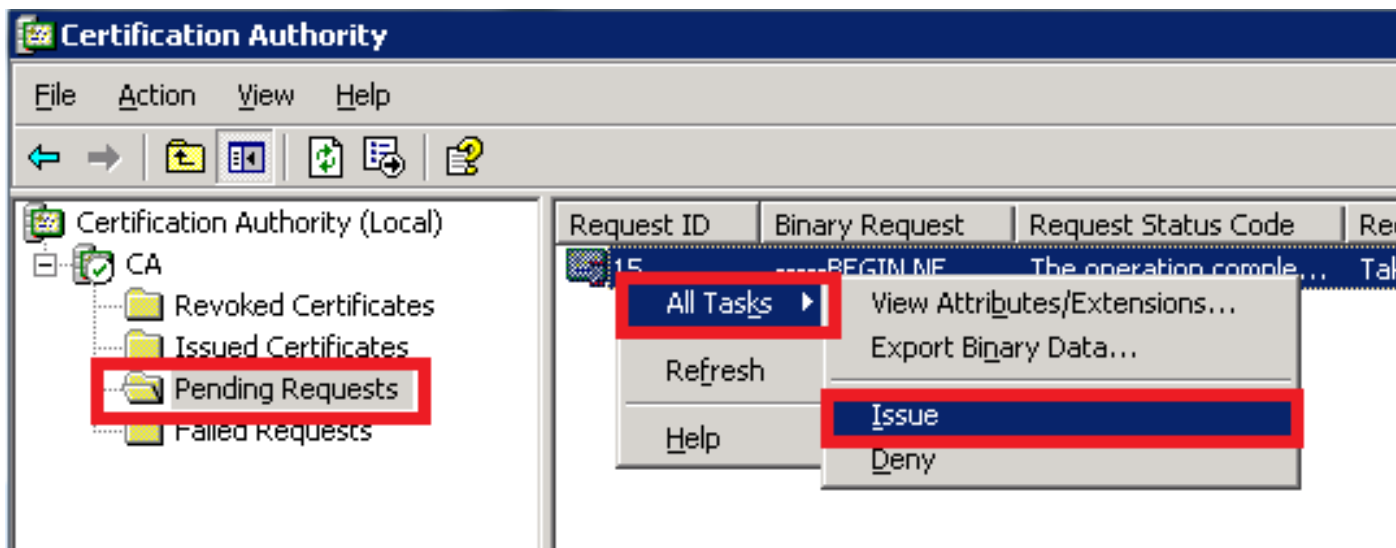
demande

3.

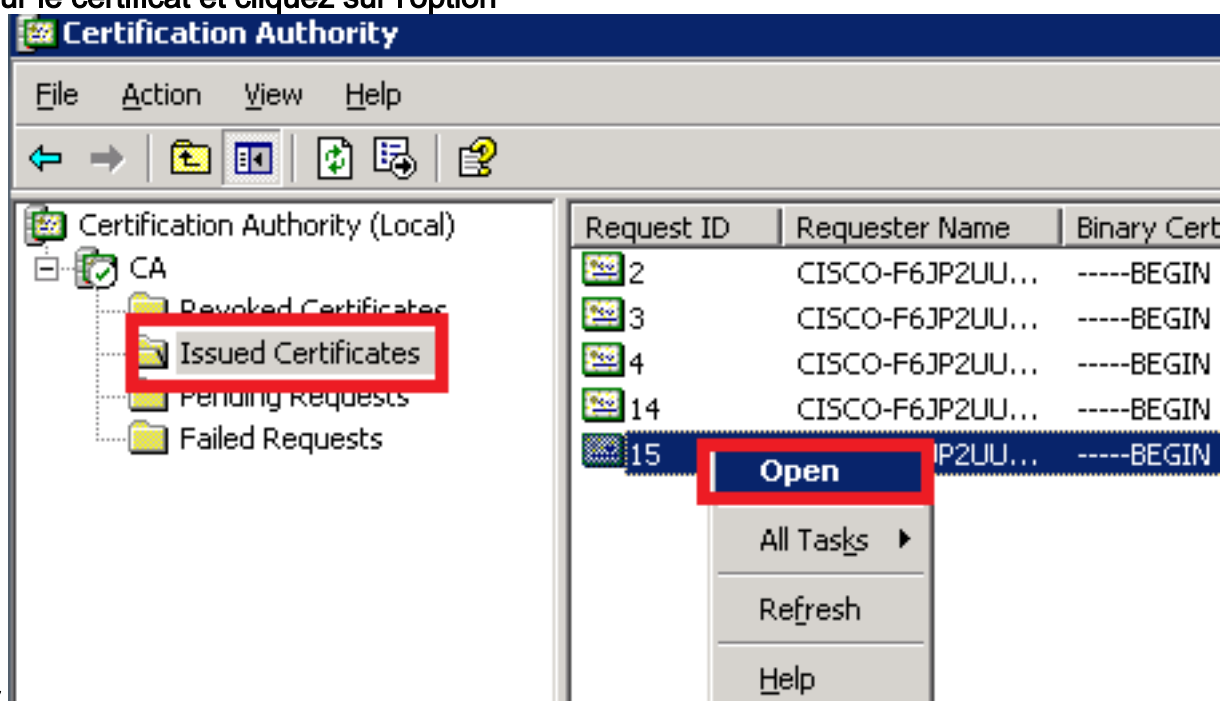
Sélectionnez le CSR et cliquez sur l'option Open (Applicable dans les CSR (CUCM 9.1(2) et CUCM 10.5(2))



4. Tous les CSR ouverts s'affichent dans le dossier Demandes en attente. Cliquez avec le bouton droit sur chaque CSR et accédez à Toutes les tâches > Émettre afin d'émettre les certificats. (Applicable dans les CSR [CUCM 9.1(2) et CUCM 10.5(2)])



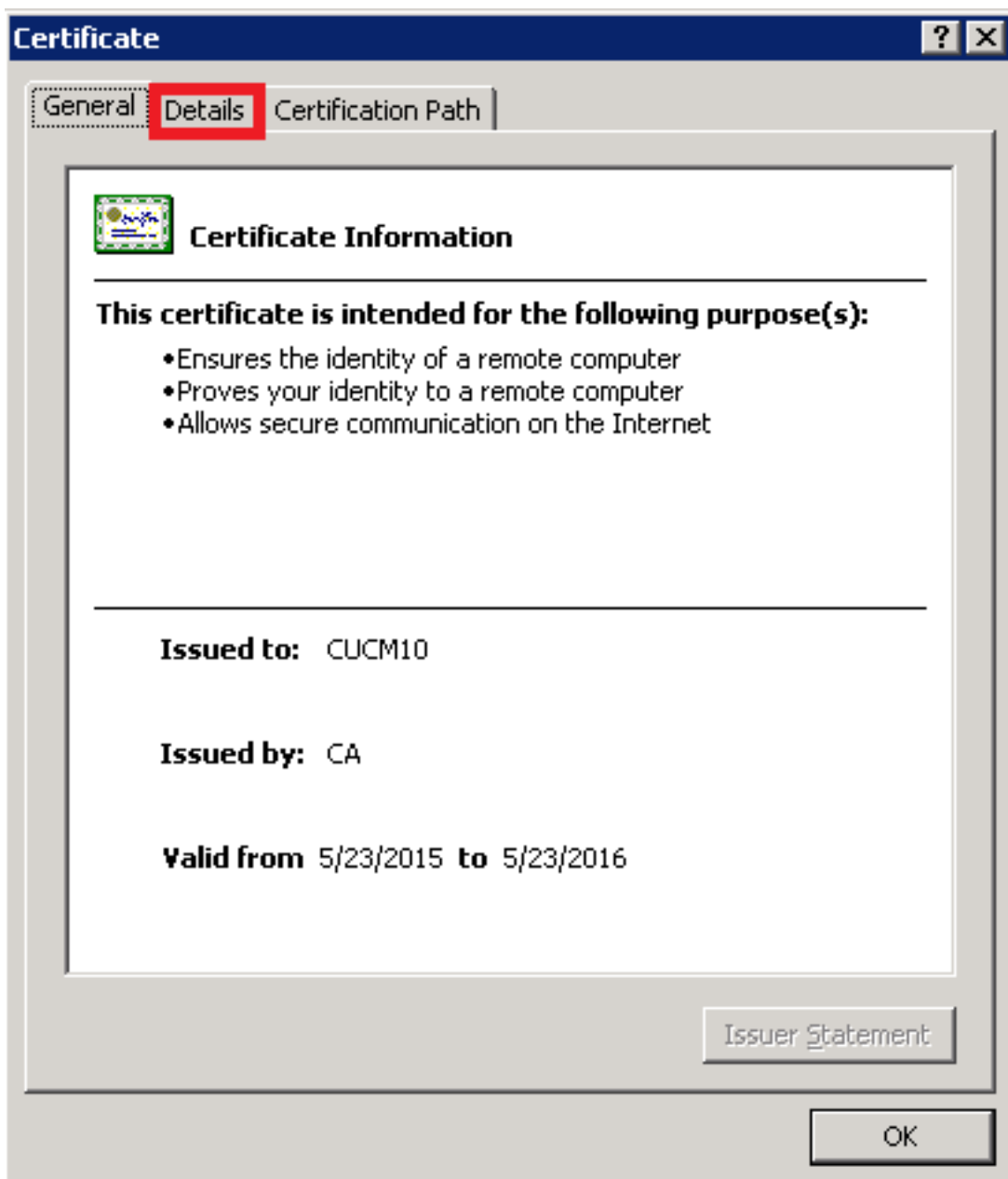
5. Afin de télécharger le certificat, choisissez le dossier Certificats émis. Cliquez avec le bouton droit sur le certificat et cliquez sur l'option



Ouvrir.

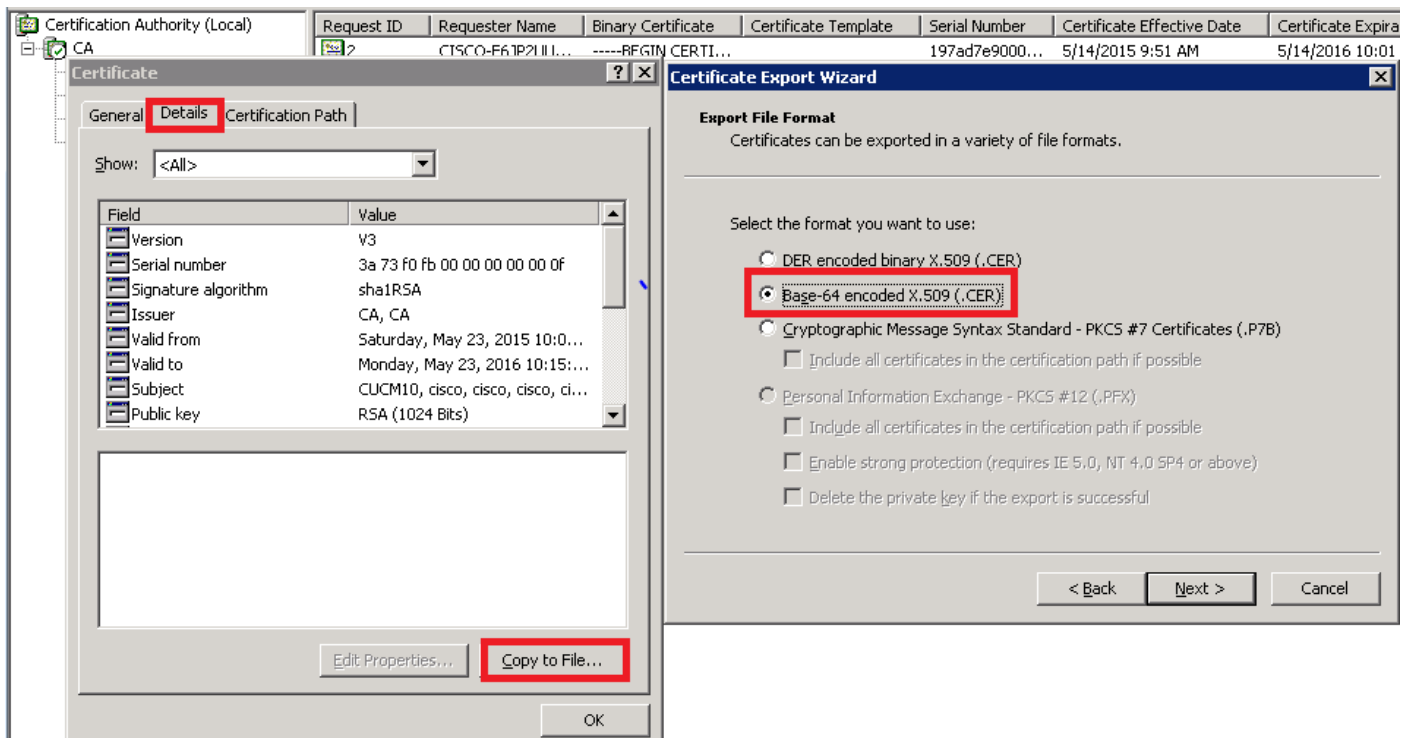
détails du certificat s'affichent. Pour télécharger le certificat, sélectionnez l'onglet Détails et cliquez sur le bouton Copier dans un

6. Les

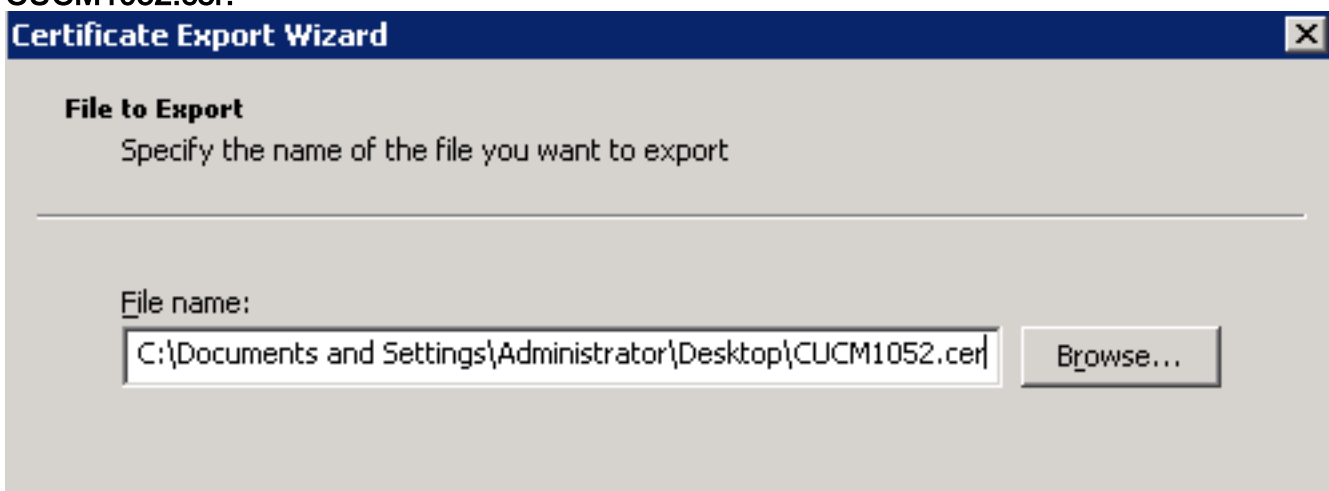


fichier...

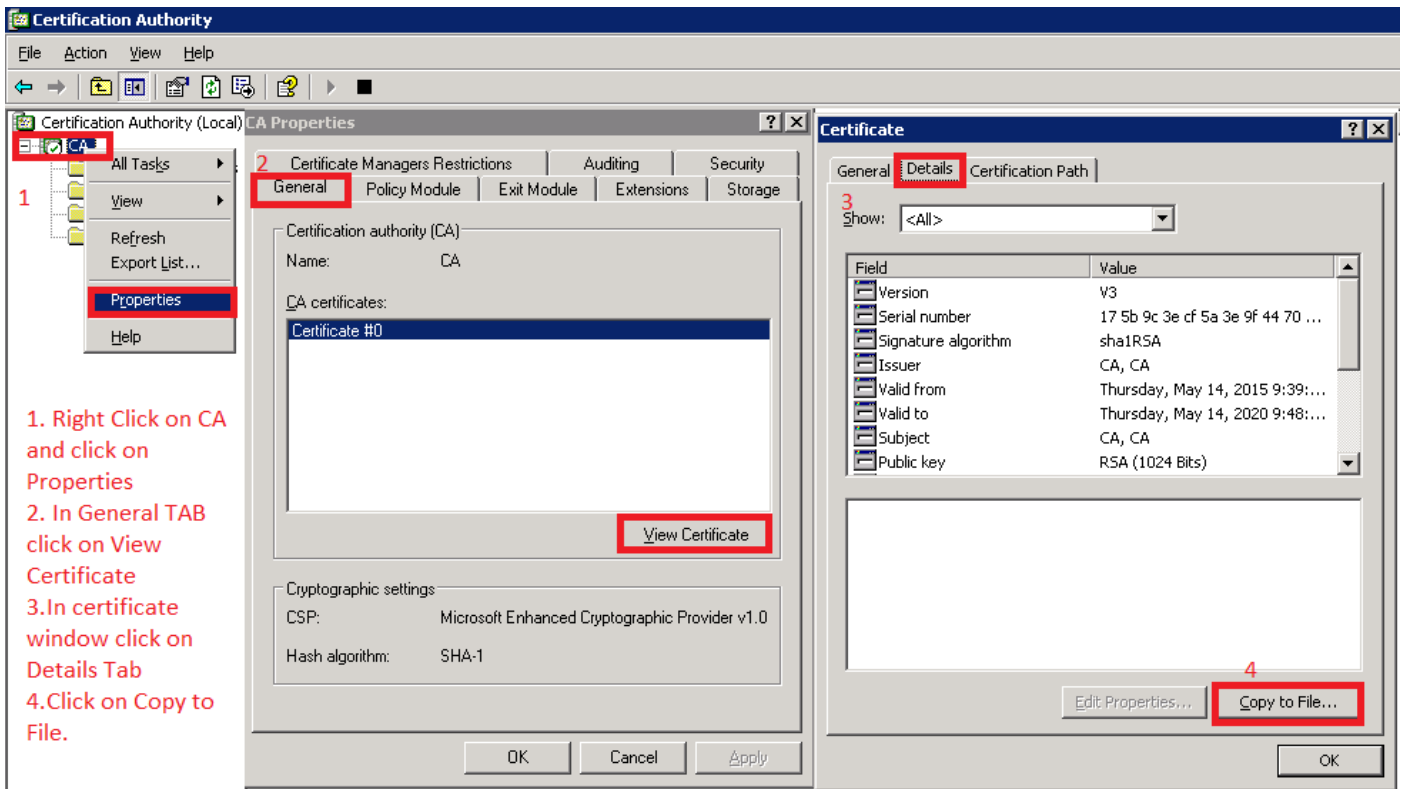
7. Dans la fenêtre Assistant Exportation de certificat, cliquez sur la case d'option X.509(.CER) codée en Base-64.



8. Nommez le fichier avec précision. Cet exemple utilise le format CUCM1052.cer.

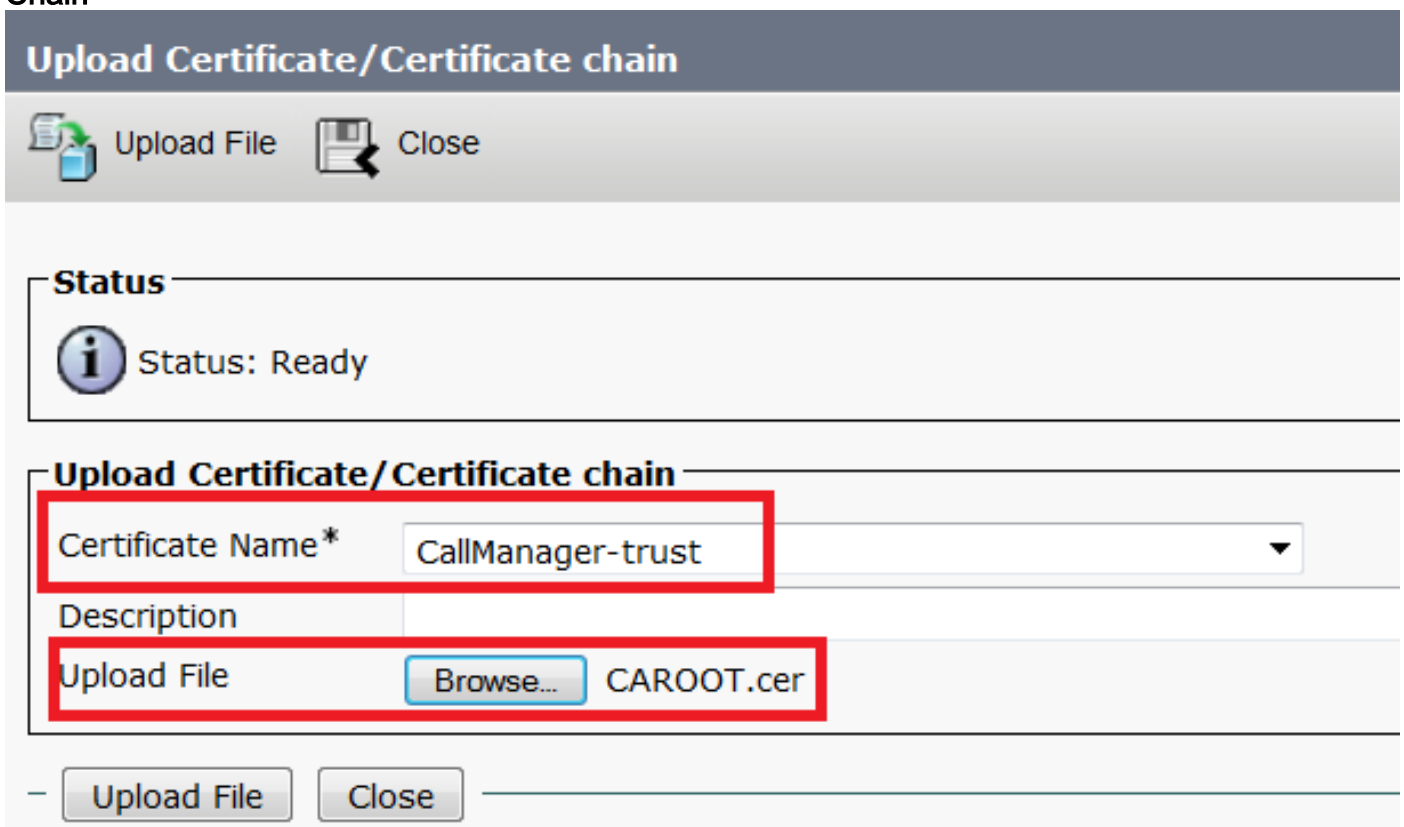


Pour CUCM 9.1(2), suivez la même procédure. Étape 5. Obtenir le certificat racine de l'autorité de certification. Ouvrez la fenêtre Autorité de certification. Afin de télécharger la racine-CA1. Cliquez avec le bouton droit sur l'icône CA et cliquez sur l'option Propriétés. 2. Dans l'onglet Général, cliquez sur Afficher le certificat. 3. Dans la fenêtre Certificat, cliquez sur l'ONGLET Détails. 4. Cliquez sur Copier dans le fichier...



1. Right Click on CA and click on Properties
2. In General TAB click on View Certificate
3. In certificate window click on Details Tab
4. Click on Copy to File.

Étape 6. Télécharger le certificat racine CA en tant que CallManager Trust Afin de télécharger le certificat racine CA, connectez-vous à OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain



Note: Exécutez ces étapes sur les CUCM (CUCM 9.1(2) et CUCM 10.5(2))
 Étape 7. Télécharger le certificat CSR CallManager en tant que certificat CallManager. Afin de télécharger le CSR CallManager du panneau AC, connectez-vous à OS Admin > Security > Certificate Management > Upload Certificate/Certificate Chain

Upload Certificate/Certificate chain



Upload File



Close

Status



Status: Ready

Upload Certificate/Certificate chain

Certificate Name*

CallManager

Description

Self-signed certificate

Upload File

Browse...

CUCM9.cer

Upload File

Close

Note: Exécutez ces étapes sur les CUCM (CUCM 9.1(2) et CUCM 10.5(2))
de liaison SIP CUCM 9.1(2) Étape 8. Créer des profils de sécurité

Afin de créer le profil de sécurité de liaison SIP, accédez à System > Security > SIP Trunk Security Profile. Copiez le profil de liaison SIP non sécurisé existant et donnez-lui un nouveau nom. Dans l'exemple, le profil de liaison SIP non sécurisé a été renommé avec le profil de liaison SIP sécurisé
TLS.

SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile TLS	
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	CUCM10	This Name should be CN of CUCM 10.5(2)
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		
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter ▼	

Dans X.509 Subject Name, utilisez le Common Name (CN) du CUCM 10.5(2) (certificat signé CA) comme indiqué dans cette image.

Certificate Settings

Locally Uploaded	23/05/15
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Certificate Signed by CA

Certificate File Data

```
[
Version: V3
Serial Number: 398B1DA600000000000E
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CA, DC=CA
Validity From: Sat May 23 17:50:42 IST 2015
             To:  Mon May 23 18:00:42 IST 2016
Subject Name: CN=CUCM10, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100bcf093aa206190fe76abe13e3bd3ec45cc8b2afeee86e8393f568e1c9aa0c5fdf3f044eebc
f2d999ed8ac3592220fef3f9dcf2d2e7e939a4b26896152ebb250e407cb65d9e04bf71e8c345633786041e
5c806405160ac42a7133d7d644294226b850810fffd001e5bf2b39829b1fb27f126624e5011f151f0ef07c7
eccb734710203010001
Extensions: 6 present
]
```

CUCM 10.5(2)Accédez à System > Security > SIP Trunk Security Profile.Copiez le profil de liaison SIP non sécurisé existant et donnez-lui un nouveau nom. Dans l'exemple, le profil de liaison SIP non sécurisé a été renommé avec le profil de liaison SIP sécurisé TLS.

SIP Trunk Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile TLS
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	CUCMA This Name should be CN of CUCM 9.1(2)
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	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

Dans X.509 Subject Name, utilisez le CN du CUCM 9.1(2) (certificat signé CA) comme indiqué

File Name CallManager.pem
Certificate Name CallManager
Certificate Type certs
Certificate Group product-cm
Description Certificate Signed by CA

Certificate File Data

```
[
  Version: V3
  Serial Number: 120325222815121423728642
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=CA, DC=CA
  Validity From: Thu May 14 09:51:09 IST 2015
    To: Sat May 14 10:01:09 IST 2016
  Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
30818902818100916c34c9700ebe4fc463671926fa29d5c98896df275ff305f80ee0c7e9dbf6e90e74cd5c44b5b26:
be0207bf5446944aef901ee5c3daefdb2cf4cbc870f8e1da5c678bc1629702b2f2bbb8e45de83579f4141ee5c53d:
ab8a7af5149194cce07b7ddc101ce0e860dad7fd01cc613fe3f1250203010001
  Extensions: 6 present
  [
    Extension: ExtKeyUsageSyntax (OID.2.5.29.37)
    Critical: false
    Usage oids: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.5,
  ]
]
```

Les deux profils de sécurité de liaison SIP définissent un port entrant de 5061, dans lequel chaque cluster écoute sur le port TCP 5061 les nouveaux appels TLS SIP entrants. **Étape 9. Créer des liaisons SIP**
 Une fois les profils de sécurité créés, créez les liaisons SIP et modifiez le paramètre de configuration ci-dessous sur la liaison SIP. **CUCM 9.1(2)**

1. Dans la fenêtre Configuration de liaison SIP, cochez la case SRTP Allowed du paramètre de configuration.

Cela sécurise le protocole RTP (Real-time Transport Protocol) à utiliser pour les appels sur cette liaison. Cette case ne doit être cochée que lorsque vous utilisez SIP TLS, car les clés du protocole SRTP (Secure Real-time Transport Protocol) sont échangées dans le corps du message SIP. La signalisation SIP doit être sécurisée par TLS, sinon toute personne avec la signalisation SIP non sécurisée pourrait déchiffrer le flux SRTP correspondant sur la liaison.

Trunk Configuration

Save Delete Reset Add New

Status
 Status: Ready

Device Information

Product: SIP Trunk
 Device Protocol: SIP
 Trunk Service Type: None(Default)
 Device Name*: CUCM10
 Description:
 Device Pool*: Default
 Common Device Configuration: < None >
 Call Classification*: Use System Default
 Media Resource Group List: < None >
 Location*: Hub_None
 AAR Group: < None >
 Tunneled Protocol*: None
 QSIG Variant*: No Changes
 ASN.1 ROSE OID Encoding*: No Changes
 Packet Capture Mode*: None
 Packet Capture Duration: 0

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 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

2. Dans la section Informations SIP de la fenêtre Configuration de liaison SIP, ajoutez l'adresse de destination, le port de destination et le profil de sécurité de liaison SIP.

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.106.95.200		5061

MTP Preferred Originating Codec*: 711ulaw
 BLF Presence Group*: Standard Presence group
 SIP Trunk Security Profile*: Secure SIP Trunk Profile TLS
 Rerouting Calling Search Space: < None >
 Out-Of-Dialog Refer Calling Search Space: < None >
 SUBSCRIBE Calling Search Space: < None >
 SIP Profile*: Standard SIP Profile
 DTMF Signaling Method*: No Preference

CUCM 10.5(2)

1. Dans la fenêtre Configuration de liaison SIP, cochez la case SRTP Allowed du paramètre de configuration.

Cela permet d'utiliser SRTP pour les appels sur cette liaison. Cette case ne doit être cochée que lorsque vous utilisez SIP TLS, car les clés de SRTP sont échangées dans le corps du message SIP. La signalisation SIP doit être sécurisée par le TLS, car toute personne disposant d'une signalisation SIP non sécurisée peut déchiffrer le flux RTP sécurisé correspondant sur le trunk.

Trunk Configuration

Save Delete Reset Add New

SIP Trunk Status

Service Status: Unknown - OPTIONS Ping not enabled
Duration: Unknown

Device Information

Product: SIP Trunk
Device Protocol: SIP
Trunk Service Type: None(Default)
Device Name*: CUCMA
Description:
Device Pool*: HQ
Common Device Configuration: < None >
Call Classification*: Use System Default
Media Resource Group List: < None >
Location*: Hub_None
AAR Group: < None >
Tunneled Protocol*: None
QSIG Variant*: No Changes
ASN.1 ROSE OID Encoding*: No Changes
Packet Capture Mode*: None
Packet Capture Duration: 0

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 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

2. Dans la section Informations SIP de la fenêtre Configuration de liaison SIP, ajoutez l'adresse IP de destination, le port de destination et le profil de sécurité

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.106.95.203		5061

MTP Preferred Originating Codec*: 711ulaw
BLF Presence Group*: Standard Presence group
SIP Trunk Security Profile*: Secure SIP Trunk Profile TLS
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

Étape 10. Créer des modèles de routage La méthode la plus simple consiste à créer un modèle de route sur chaque cluster, en pointant directement vers la ligne principale SIP. Les groupes de routage et les listes de routage peuvent également être utilisés. CUCM 9.1(2) pointe vers le modèle de route 9898 via la ligne principale SIP TLS vers le CUCM 10.5(2)

Trunks (1 - 1 of 1)											Rows per Page 50			
Find Trunks where Device Name begins with											Find	Clear Filter	+	-
Select item or enter search text														
Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Security Profile					
CUCM10			Default	9898				SIP Trunk	Secure SIP Trunk Profile TLS					
Add New											Select All	Clear All	Delete Selected	Reset Selected

Le CUCM 10.5(2) pointe vers le modèle de route 1018 via la liaison SIP TLS jusqu'au CUCM 9.1(2)

Trunks (1 - 1 of 1)											Rows per Page 50			
Find Trunks where Device Name begins with											Find	Clear Filter	+	-
Select item or enter search text														
Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration	SIP Trunk Security Profile			
CUCMA		HQ		1018				SIP Trunk	Unknown - OPTIONS Ping not enabled		Secure SIP Trunk Profile TLS			
Add New											Select All	Clear All	Delete Selected	Reset Selected

Vérification Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage L'appel TLS SIP peut être débogué à l'aide de ces étapes. Collecter la capture de paquets sur CUCMAfin de vérifier la connectivité entre CUCM 9.1(2) et CUCM 10.5(2), prenez une capture de paquets sur les serveurs CUCM et observez le trafic TLS SIP. Le trafic TLS SIP est transmis sur le port TCP 5061, considéré comme sip-tls. Dans l'exemple suivant, une session CLI SSH est établie pour CUCM 9.1(2). Capture de paquets CLI à l'écran Cette interface de ligne de commande imprime le résultat à l'écran pour le trafic TLS SIP.

```
admin:utils network capture host ip 10.106.95.200
```

```
Executing command with options:
```

```
interface=eth0
```

```
ip=10.106.95.200
```

```
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack 3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
```

```
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp 6072188 2864697196>
```

```
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249 <nop,nop,timestamp 6072201 2864697196>
```

2. Captures CLI dans un fichier Cette interface de ligne de commande effectue la capture de paquets en fonction de l'hôte et crée un fichier nommé paquets.

```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
```

Redémarrez la liaison SIP sur CUCM 9.1(2) et passez l'appel du poste 1018 (CUCM 9.1(2)) au poste 9898 (CUCM 10.5(2)) Afin de télécharger le fichier à partir de l'interface de ligne de commande, exécutez cette commande :

```
admin:file get activelog platform/cli/packets.cap
```

La capture est effectuée au format .cap standard. Cet exemple utilise Wireshark pour ouvrir le fichier packet.cap, mais n'importe quel outil d'affichage de capture de paquets peut être utilisé.

Time	Source	Destination	Protocol	Length	Info
18:46:11.313121	10.106.95.203	10.106.95.200	TCP	74	33135 > sip-tls [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1
18:46:11.313230	10.106.95.200	10.106.95.203	TCP	74	sip-tls > 33135 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460
18:46:11.313706	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=156761672
18:46:11.333114	10.106.95.203	10.106.95.200	TLSv1	124	Client Hello
18:46:11.333168	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1 Ack=59 Win=14592 Len=0 TSval=988679
18:46:11.429700	10.106.95.200	10.106.95.203	TLSv1	1514	Server Hello
18:46:11.429872	10.106.95.200	10.106.95.203	TLSv1	260	Certificate, Certificate Request, Server Hello Done
18:46:11.430111	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1449 Win=8832 Len=0 TSval=15676
18:46:11.430454	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1643 Win=11648 Len=0 TSval=1567
18:46:11.450926	10.106.95.203	10.106.95.200	TCP	1514	[TCP segment of a reassembled PDU]
18:46:11.450969	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1507 Win=17408 Len=0 TSval=98
18:46:11.451030	10.106.95.203	10.106.95.200	TLSv1	507	Certificate, Client Key Exchange, Certificate Verify, Change Ciph
18:46:11.451081	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1948 Win=20352 Len=0 TSval=98
18:46:11.461558	10.106.95.200	10.106.95.203	TLSv1	1200	New Session Ticket, Change Cipher Spec, Finished
18:46:11.463062	10.106.95.203	10.106.95.200	TLSv1	1161	Application Data
18:46:11.502380	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=2777 Ack=3043 Win=23168 Len=0 TSval=98
18:46:11.784432	10.106.95.200	10.106.95.203	TLSv1	440	Application Data
18:46:11.824821	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=3151 Win=17536 Len=0 TSval=15
18:46:12.187974	10.106.95.200	10.106.95.203	TLSv1	1024	Application Data
18:46:12.188452	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=4109 Win=20352 Len=0 TSval=15
18:46:15.288860	10.106.95.200	10.106.95.203	TLSv1	1466	Application Data
18:46:15.289237	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=3043 Ack=5509 Win=23296 Len=0 TSval=15
18:46:15.402901	10.106.95.203	10.106.95.200	TLSv1	770	Application Data

1. La synchronisation du protocole de contrôle de transmission (TCP) (SYN) pour établir la

communication TCP entre CUCM 9.1(2)(Client) et CUCM 10.5(2)(Serveur).

2. CUCM 9.1(2) envoie le message Hello du client pour démarrer la session TLS.
3. CUCM 10.5(2) envoie le message Hello du serveur, le certificat du serveur et la demande de certificat pour démarrer le processus d'échange de certificat.
4. Certificat que le client CUCM 9.1(2) envoie pour terminer l'échange de certificat.
5. Les données d'application qui sont des signaux SIP chiffrés indiquent que la session TLS a été établie.

Vérifiez en outre si les certificats corrects sont échangés. Après Server Hello, le serveur CUCM 10.5(2) envoie son certificat au client CUCM 9.1(2).

No.	Time	Source	Destination	Protocol	Length	Info
4	2015-05-23 18:46:11.333114	10.106.95.203	10.106.95.200	TLSv1	124	Client Hello
5	2015-05-23 18:46:11.333168	10.106.95.200	10.106.95.203	TCP	66	sip-tls > 33135 [ACK] Seq=1 Ack=59 Win=14592 Len=0 TSval=988679
6	2015-05-23 18:46:11.429700	10.106.95.200	10.106.95.203	TLSv1	1514	Server Hello
7	2015-05-23 18:46:11.429872	10.106.95.200	10.106.95.203	TLSv1	260	Certificate, Certificate Request, Server Hello Done
8	2015-05-23 18:46:11.430111	10.106.95.203	10.106.95.200	TCP	66	33135 > sip-tls [ACK] Seq=59 Ack=1449 Win=8832 Len=0 TSval=15676

Secure Sockets Layer

- TLsv1 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 1560
- Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1556
 - Certificates Length: 1553
- Certificates (1553 bytes)
 - Certificate Length: 902
 - Certificate (id-at-commonName=CUCM10,id-at-organizationalUnitName=cisco,id-at-organizationName=cisco,id-at-localityName=cisco,id-at-stateOrProvinceName=)
 - signedCertificate
 - version: v3 (2)
 - serialNumber : 0x398b1da6000000000000e
 - signature (shaWithRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - extensions: 6 items

Le numéro de série et les informations d'objet du serveur CUCM 10.5(2) sont présentés au client CUCM 9.1(2). Le numéro de série, l'objet, l'émetteur et les dates de validité sont tous comparés aux informations de la page Gestion des certificats d'administration du système d'exploitation. Le serveur CUCM 10.5(2) présente son propre certificat pour vérification, maintenant il vérifie le certificat du client CUCM 9.1(2). La vérification se fait dans les deux directions.

Filter:	Source	Destination	Protocol	Length	Info
	10.106.95.203	10.106.95.200	TCP	66	sip-tls > 33135 [ACK] Seq=59 Ack=1043 Win=11048 Len=0 TSval=1007010644 TSecr=988679
	18:46:11.450926	10.106.95.203	TCP	1514	[TCP segment of a reassembled PDU]
	18:46:11.450969	10.106.95.200	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1507 Win=17408 Len=0 TSval=988797 TSecr=15676
	18:46:11.451030	10.106.95.203	TLSv1	507	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Finished
	18:46:11.451081	10.106.95.200	TCP	66	sip-tls > 33135 [ACK] Seq=1643 Ack=1948 Win=20352 Len=0 TSval=988797 TSecr=15676

Secure Sockets Layer

- TLsv1 Record Layer: Handshake Protocol: Certificate
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 1559
- Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 1555
 - Certificates Length: 1552
- Certificates (1552 bytes)
 - Certificate Length: 901
 - Certificate (id-at-commonName=CUCMA,id-at-organizationalUnitName=cisco,id-at-organizationName=cisco,id-at-localityName=cisco,id-at-stateOrProvinceName=)
 - signedCertificate
 - version: v3 (2)
 - serialNumber : 0x197ad7e90000000000002
 - signature (shaWithRSAEncryption)
 - issuer: rdnSequence (0)
 - validity
 - subject: rdnSequence (0)
 - subjectPublicKeyInfo
 - extensions: 6 items

En cas d'incompatibilité entre les certificats de la capture de paquets et les certificats de la page Web d'administration du système d'exploitation, les certificats corrects ne sont pas téléchargés. Les certificats corrects doivent être téléchargés sur la page OS Admin Cert. Collecter les traces CUCM Les traces CUCM peuvent également être utiles pour déterminer quels messages sont échangés entre les serveurs CUCM 9.1(2) et CUCM 10.5(2) et si la session SSL est correctement établie. Dans l'exemple, les traces de CUCM 9.1(2) ont été collectées. Flux d'appels : Ext 1018 > CUCM 9.1(2) > SIP TLS TRUNK > CUCM 10.5(2) > Ext 9898++ Analyse de chiffres 04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",

```
cn="1018",plv="5", pss="", TodFilteredPss="", dd="9898",dac="0")
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
|CallingPartyNumber=1018
|DialingPartition=
|DialingPattern=9898
|FullyQualifiedCalledPartyNumber=9898
```

++ SIP TLS est utilisé sur le port 5061 pour cet appel.

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPtcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

++ Le message SDL (Signal Distribution Layer) SIPCertificateInd fournit des détails sur le CN d'objet et les informations de connexion.

```
04530218.000 |19:59:21.323 |SdlSig |SIPCertificateInd |wait
|SIPHandler(1,100,72,1) |SIPtcp(1,100,64,1)
|1,100,17,11.3^*** |[T:N-H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --
remoteIP=10.106.95.200 --remotePort = 5061 --X509SubjectName
/C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --SubjectAltname =
04530219.000 |19:59:21.324 |SdlSig |SIPCertificateInd
|restart0 |SIPD(1,100,74,16)
|SIPHandler(1,100,72,1) |1,100,17,11.3^*** |[R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```