

Configurez le CUCM pour la connexion d'IPsec entre les Noeuds

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Aperçu de configuration](#)

[Vérifiez la Connectivité d'IPsec](#)

[Certificats d'IPsec de contrôle](#)

[Certificat racine d'IPsec de téléchargement d'abonné](#)

[Certificat racine d'IPsec de téléchargement d'abonné à Publisher](#)

[Configurez la stratégie d'IPsec](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit comment établir la Connectivité d'IPsec entre les Noeuds de Cisco Unified Communications Manager (CUCM) dans une batterie.

Remarque: Par défaut, la connexion d'IPsec entre les Noeuds CUCM est désactivée.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du CUCM.

[Composants utilisés](#)

Les informations dans ce document sont basées sur la version 10.5(1) CUCM.

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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Utilisez les informations qui sont décrites dans cette section afin de configurer le CUCM et établir la Connectivité d'IPsec entre les Noeuds dans une batterie.

Aperçu de configuration

Voici les étapes qui sont impliquées dans cette procédure, qui est détaillée dans les sections qui suivent :

1. Vérifiez la Connectivité d'IPsec entre les Noeuds.
2. Vérifiez les Certificats d'IPsec.
3. Téléchargez les certificats racine d'IPsec du noeud d'abonné.
4. Téléchargez le certificat racine d'IPsec du noeud d'abonné au noeud de Publisher.
5. Configurez la stratégie d'IPsec.


Vérifiez la Connectivité d'IPsec

Terminez-vous ces étapes afin de vérifier la Connectivité d'IPsec entre les Noeuds :


1. Connectez-vous dans la page du système d'exploitation de gestion (de SYSTÈME D'EXPLOITATION) du serveur CUCM.
2. Naviguez vers des **services > le ping**.
3. Spécifiez l'adresse IP de noeud distant.
4. Cochez la case d'**IPsec de validation** et cliquez sur le **ping**.

S'il n'y a aucune Connectivité d'IPsec, alors vous voyez des résultats semblables à ceci :

Ping Configuration

 Ping

Status

 Status: Ready

Ping Settings

Hostname or IP Address*

Ping Interval*

Packet Size*

Ping Iterations

Validate IPsec

Ping Results

IPsec connection failed..
Reasons :
a)No IPsec Policy on 10.106.110.8
b)Invalid Certificates IPsec connection failed..
Reasons :
a)No IPsec Policy on 10.106.110.8
b)Invalid Certificates

Certificats d'IPsec de contrôle

Terminez-vous ces étapes afin de vérifier les Certificats d'IPsec :

1. Connectez-vous dans la page de gestion de SYSTÈME D'EXPLOITATION.
2. Naviguez vers la **Gestion de Sécurité > de certificat**.
3. Recherchez les Certificats d'IPsec (log dans les Noeuds de Publisher et d'abonné séparément).

Remarque: Le certificat d'IPsec de noeud d'abonné n'est pas habituellement visualisable du noeud de Publisher ; cependant, vous pouvez voir les Certificats d'IPsec de noeud de Publisher sur tous les Noeuds d'abonné comme certificat d'IPsec-confiance.

Afin d'activer la Connectivité d'IPsec, vous devez avoir un certificat d'IPsec d'un noeud réglé comme certificat d'ipsec-**confiance** sur l'autre noeud :

PUBLISHER

Certificate List (1 - 2 of 2) Rows p

Find Certificate List where Certificate begins with ipsec

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

IPSEC Root certificates

SUBSCRIBER

Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec

Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm10sub	Self-signed	cucm10sub	cucm10sub	12/14/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Certificat racine d'IPsec de téléchargement d'abonné

Terminez-vous ces étapes afin de télécharger le certificat racine d'IPsec du noeud d'abonné :

1. Connectez-vous dans la page de gestion de SYSTÈME D'EXPLOITATION du noeud d'abonné.
2. Naviguez vers la **Gestion de Sécurité > de certificat**.
3. Ouvrez le certificat racine d'IPsec et téléchargez-le dans le format **.pem** :

SUBSCRIBER





Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec


Certificate	Common Name	Type	Distribution	Issued By	Expiration	Description
ipsec	cucm10sub	Self-signed	cucm10sub	cucm10sub	12/14/2019	Self-signed certificate generated by system
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

IPSEC Root certificates

Certificate Details for cucm10sub, ipsec

 Regenerate
  Generate CSR
  Download .PEM File
  Download .DER File

Status

 Status: Ready

Certificate Settings

File Name	ipsec.pem
Certificate Purpose	ipsec
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```

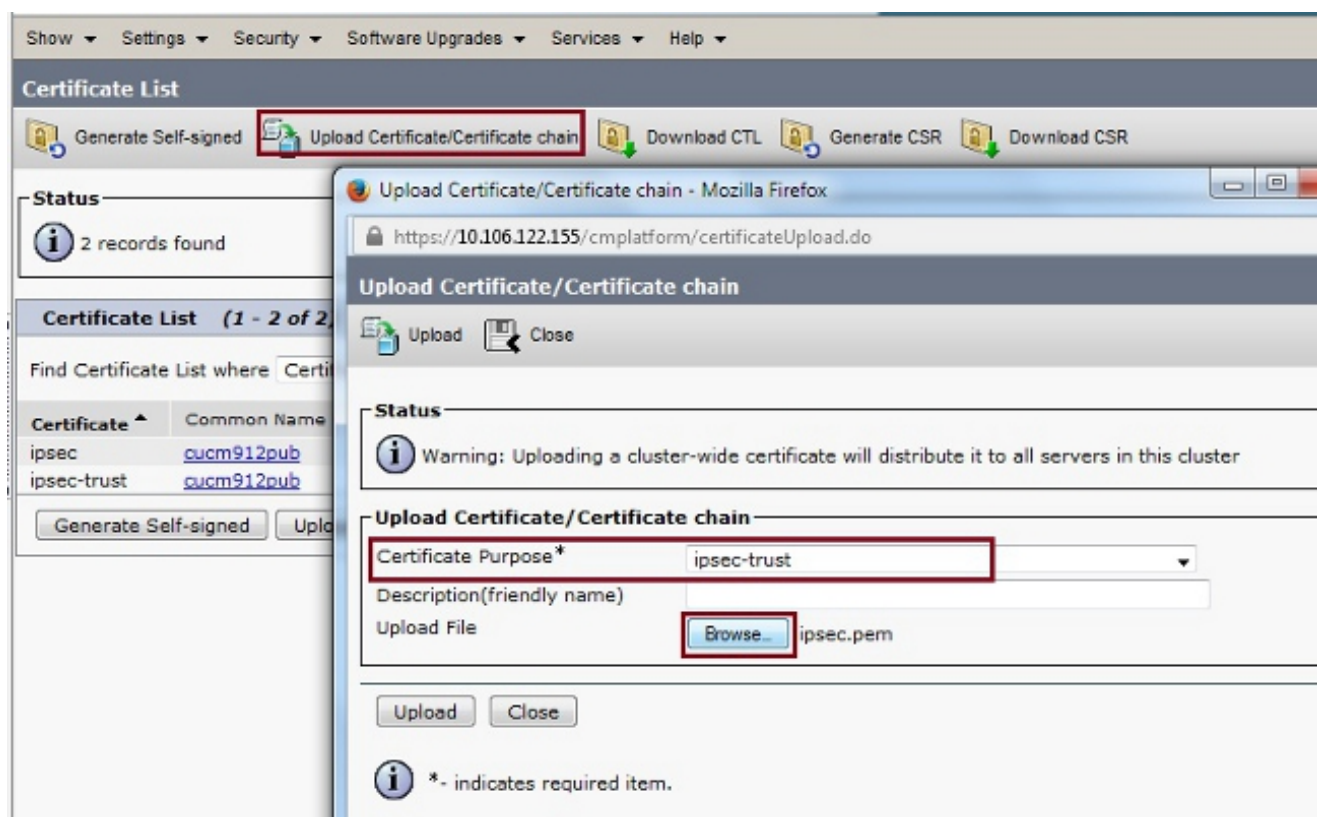
[
  Version: V3
  Serial Number: 6B71952138766EF415EFE831AEB5F943
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=blr, ST=karnataka, CN=cucm10sub, OU=cucm, O=cisco, C=IN
  Validity From: Mon Dec 15 23:26:27 IST 2014
  To: Sat Dec 14 23:26:26 IST 2019
  Subject Name: L=blr, ST=karnataka, CN=cucm10sub, OU=cucm, O=cisco, C=IN
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
  30818902818100a376b6ad7825abe3069a421538c851a32d815321de77791985f99f2f9a
  4b695016352b98cc72b26461cc629d0d2b35fc774d20fa13ae6c476164b7ccca82eb73034
  7b6ad7e5069d732468f501ba53a018f9bbe422f6c76a4e4023fbad9bcf2f7d122cbe681375
  feb7adb41068344a97a4f9b224180c6f8b223f75194ec7d987b0203010001
  Extensions: 3 present
  [
  ]
  ]
  
```

Certificat racine d'IPsec de téléchargement d'abonné à Publisher

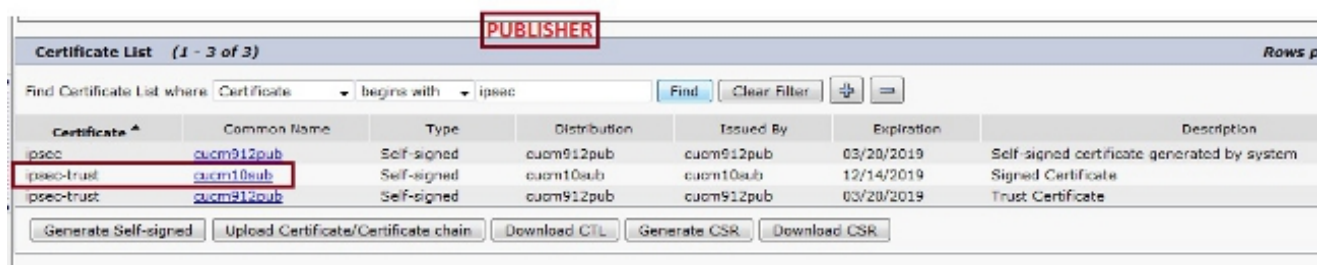
Terminez-vous ces étapes afin de télécharger le certificat racine d'IPsec du noeud d'abonné au noeud de Publisher :

1. Connectez-vous dans la page de gestion de SYSTÈME D'EXPLOITATION du noeud de Publisher.
2. Naviguez vers la **Gestion de Sécurité > de certificat**.
3. Cliquez sur Upload la **chaîne de certificat/certificat**, et téléchargez le certificat racine d'IPsec

de noeud d'abonné comme certificat d'ipsec-confiance :



- Après que vous téléchargez le certificat, vérifiez que le certificat racine d'IPsec de noeud d'abonné apparaît comme affiché :



Remarque: Si vous êtes requis d'activer la Connectivité d'IPsec entre les plusieurs noeuds dans une batterie, alors vous devez télécharger les certificats racine d'IPsec pour ces Noeuds aussi bien, et les téléchargez au noeud de Publisher par l'intermédiaire de la même procédure.

Configurez la stratégie d'IPsec

Terminez-vous ces étapes afin de configurer la stratégie d'IPsec :

- Connectez-vous dans la page de gestion de SYSTÈME D'EXPLOITATION de Publisher et des Noeuds d'abonné séparément.
- Naviguez vers la **Sécurité > la configuration IPsec**.

3. Employez ces informations afin de configurer l'IP et délivrer un certificat des détails :

PUBLISHER : 10.106.122.155 & cucm912pub.pem

SUBSCRIBER: 10.106.122.15 & cucm10sub.pem

The screenshot shows the IPSEC Policy Configuration page for the PUBLISHER node. The system is in non-FIPS Mode. The IPSEC Policy Details section is highlighted with a red box, showing the following configuration:

Policy Group Name*	ToSubscriber
Policy Name*	ToSub
Authentication Method*	Certificate
Preshared Key	
Peer Type*	Different
Certificate Name*	cucm10sub.pem
Destination Address*	10.106.122.159
Destination Port*	ANY
Source Address*	10.106.122.155
Source Port*	ANY
Mode*	Transport
Remote Port*	500
Protocol*	TCP
Encryption Algorithm*	3DES
Hash Algorithm*	SHA1
ESP Algorithm*	AES 128

Below the IPSEC Policy Details, the Phase 1 and Phase 2 DH Groups are configured with Phase One Life Time of 3600 and Phase One DH of Group 2. The IPSEC Policy Configuration section at the bottom has the Enable Policy checkbox selected, and the Save button is visible.

The screenshot shows the IPSEC Policy Configuration page for the SUBSCRIBER node. The system is in non-FIPS Mode. The IPSEC Policy Details section is highlighted with a red box, showing the following configuration:

Policy Group Name*	ToPublisher
Policy Name*	ToPublisher
Authentication Method*	Certificate
Preshared Key	
Peer Type*	Different
Certificate Name*	cucm912pub.pem
Destination Address*	10.106.122.155
Destination Port*	ANY
Source Address*	10.106.122.159
Source Port*	ANY
Mode*	Transport
Remote Port*	500
Protocol*	TCP
Encryption Algorithm*	3DES
Hash Algorithm*	SHA1
ESP Algorithm*	AES 128

Below the IPSEC Policy Details, the Phase 1 and Phase 2 DH Groups are configured with Phase One Life Time of 3600 and Phase One DH of Group 2. The IPSEC Policy Configuration section at the bottom has the Enable Policy checkbox selected, and the Save button is visible.

Vérifiez


Terminez-vous ces étapes afin de vérifier que vos travaux de configuration et que la Connectivité d'IPsec entre les Noeuds est établie :

1. Connectez-vous dans la gestion de SYSTÈME D'EXPLOITATION du serveur CUCM.
2. Naviguez vers des **services > le ping**.
3. Spécifiez l'adresse IP de noeud distant.
4. Cochez la case d'**IPsec de validation** et cliquez sur le **ping**.


Si la Connectivité d'IPsec a été établie, alors vous voyez un message semblable à ceci :

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Ping Configuration

 Ping

Status

 Status: Ready

Ping Settings

Hostname or IP Address*

Ping Interval*

Packet Size*

Ping Iterations

Validate IPsec

Ping Results

Successfully validated IPsec connection to 10.106.122.159
Successfully validated IPsec connection to 10.106.122.159

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

[Informations connexes](#)

- [Guide d'administration du système d'exploitation de Cisco Unified Communications, version 8.6\(1\) – Installez une nouvelle stratégie d'IPsec](#)
- [Support et documentation techniques - Cisco Systems](#)