# Configurer CUCM pour la connexion IPsec entre les noeuds

## Contenu



## Introduction

Ce document décrit comment établir la connectivité IPsec entre les noeuds Cisco Unified Communications Manager (CUCM) dans un cluster.

> **Note**: Par défaut, la connexion IPsec entre les noeuds CUCM est désactivée.

## Conditions préalables

### Conditions requises

Cisco vous recommande de connaître le CUCM.

### Components Used

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

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.

# Configuration

Utilisez les informations décrites dans cette section afin de configurer le CUCM et d'établir la connectivité IPsec entre les noeuds dans un cluster.

## Présentation de la configuration

Voici les étapes de cette procédure, chacune d'entre elles étant détaillée dans les sections suivantes :

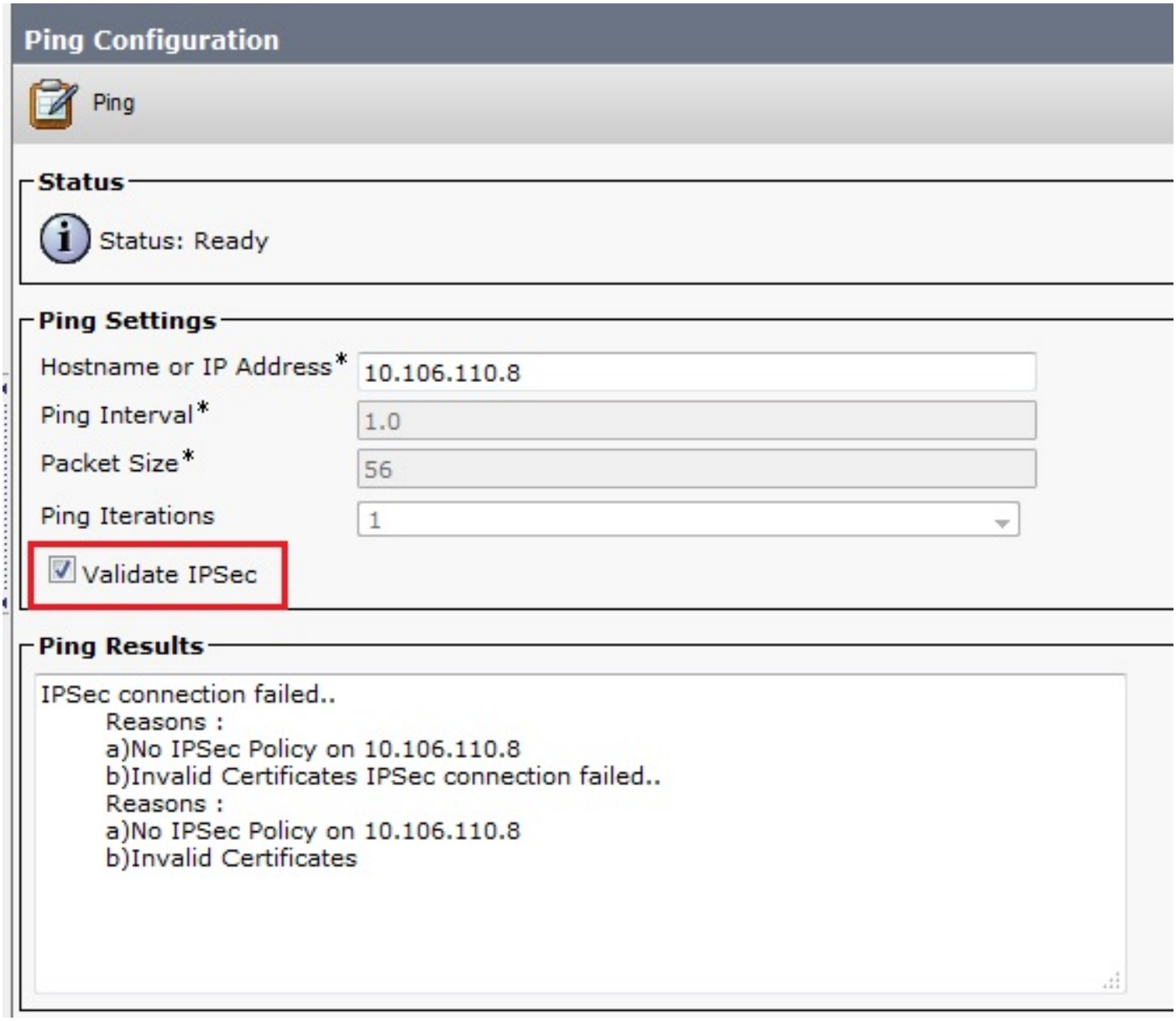
1. Vérifiez la connectivité IPsec entre les noeuds.
2. Vérifiez les certificats IPsec.
3. Téléchargez les certificats racine IPsec à partir du noeud Abonné.
4. Téléchargez le certificat racine IPsec du noeud Abonné vers le noeud Éditeur.
5. Configurez la stratégie IPsec.

## Vérifier la connectivité IPsec

Complétez ces étapes afin de vérifier la connectivité IPsec entre les noeuds :

1. Connectez-vous à la page Operating System (OS) Administration du serveur CUCM.
2. Accédez à **Services > Ping**.
3. Spécifiez l'adresse IP du noeud distant.
4. Cochez la case **Valider IPsec** et cliquez sur **Ping**.

S'il n'y a pas de connectivité IPsec, alors vous voyez des résultats similaires à ceci :



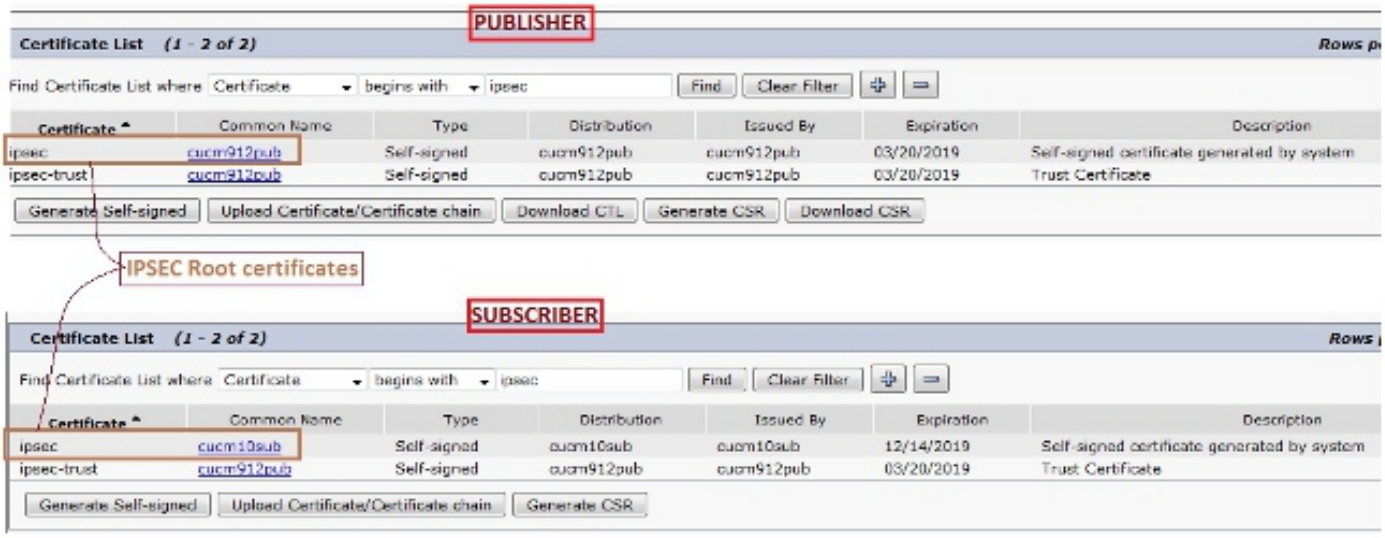

## Vérifier les certificats IPsec

Complétez ces étapes afin de vérifier les certificats IPsec :

1. Connectez-vous à la page OS Administration.
2. Accédez à **Security > Certificate Management**.
3. Recherchez les certificats IPsec (connectez-vous séparément aux noeuds Éditeur et Abonné).

   **Note**: Le certificat IPsec du noeud Abonné n'est généralement pas visible à partir du noeud Éditeur ; cependant, vous pouvez voir les certificats IPsec du noeud Éditeur sur tous les noeuds Abonné en tant que certificat IPsec-Trust.

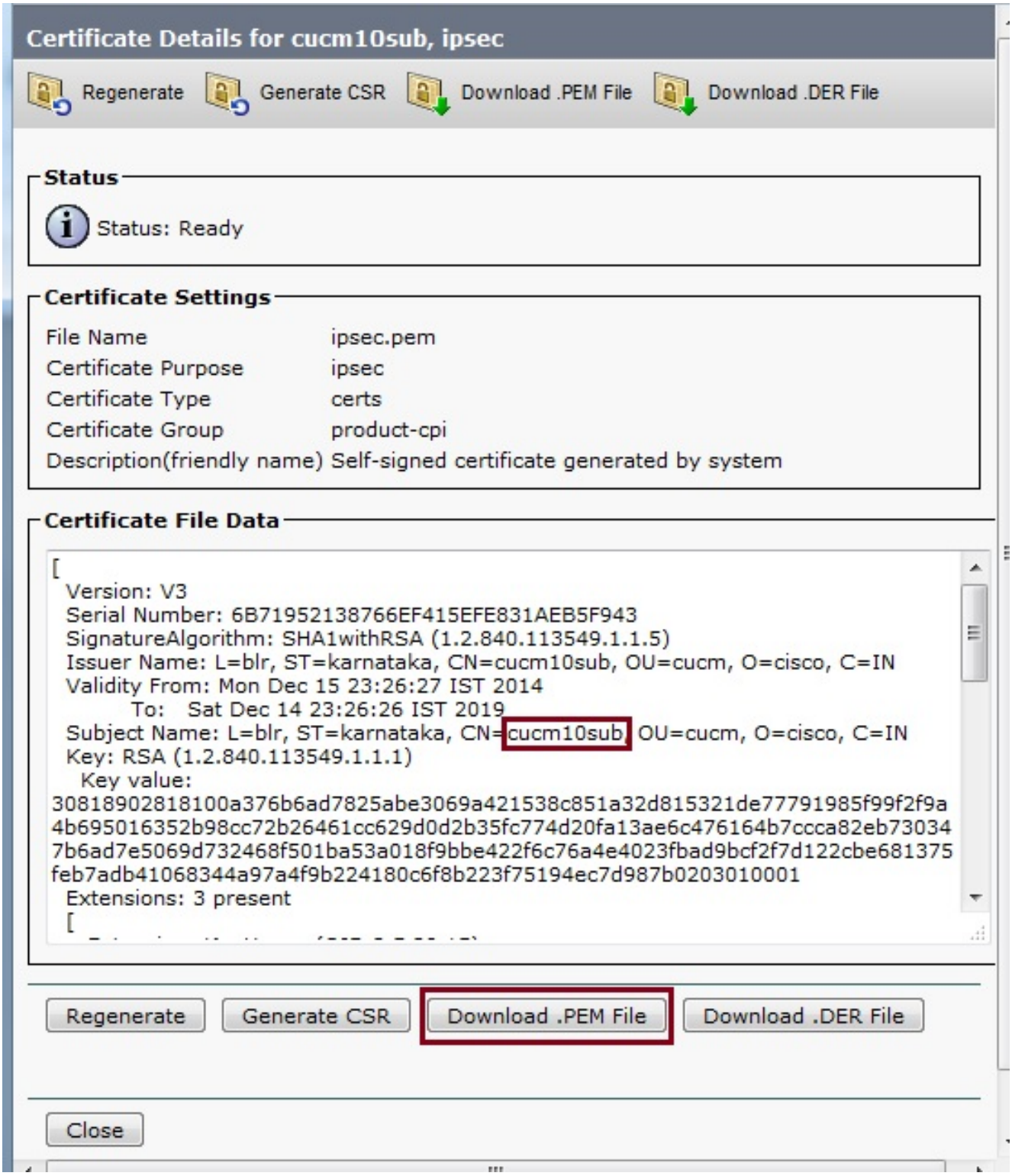
Pour activer la connectivité IPsec, vous devez avoir un certificat IPsec d'un noeud défini comme un certificat **ipsec-trust** sur l'autre noeud :




## Télécharger le certificat racine IPsec depuis l'abonné

Complétez ces étapes afin de télécharger le certificat racine IPsec à partir du noeud Abonné :

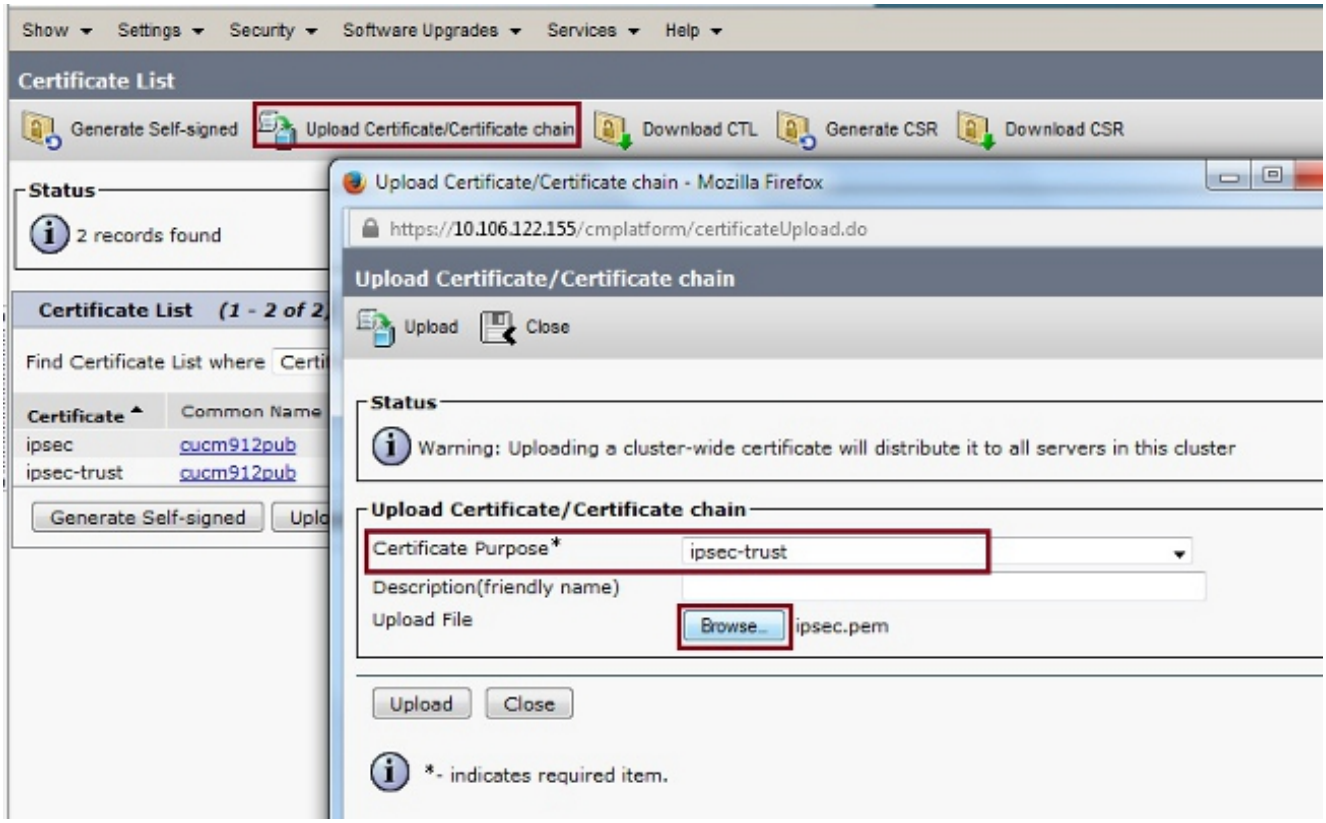
1. Connectez-vous à la page Administration du système d'exploitation du noeud Abonné.
2. Accédez à **Security > Certificate Management**.
3. Ouvrez le certificat racine IPsec et téléchargez-le au format **.pem** :



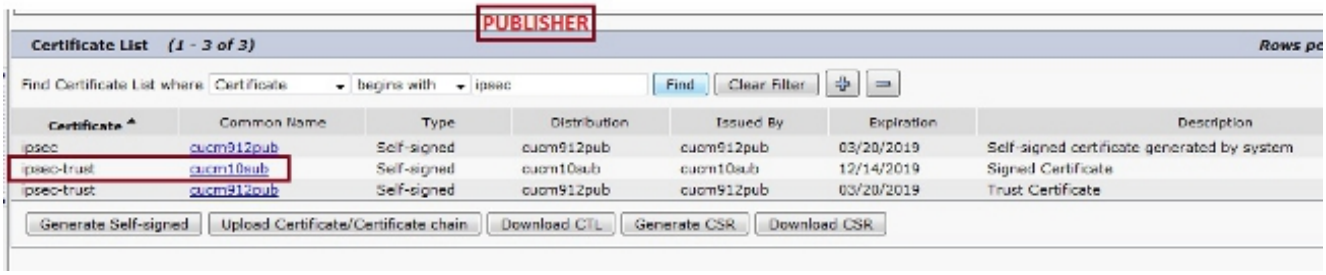

## Télécharger le certificat racine IPsec de l'abonné vers l'éditeur

Complétez ces étapes afin de télécharger le certificat racine IPsec du noeud Abonné au noeud Éditeur :

1. Connectez-vous à la page OS Administration du noeud Publisher.
2. Accédez à **Security > Certificate Management**.
3. Cliquez sur **Upload Certificate/Certificate chain**, et téléchargez le certificat racine IPsec du noeud Abonné en tant que certificat **ipsec-trust** :




4. Après avoir téléchargé le certificat, vérifiez que le certificat racine IPsec du noeud Abonné apparaît comme suit :




**Note**: Si vous devez activer la connectivité IPsec entre plusieurs noeuds dans un cluster, vous devez télécharger les certificats racines IPsec pour ces noeuds également, puis les télécharger vers le noeud Éditeur via la même procédure.

## Configurer la stratégie IPsec

Complétez ces étapes afin de configurer la stratégie IPsec :

1. Connectez-vous séparément à la page OS Administration des noeuds Publisher et Subscriber.

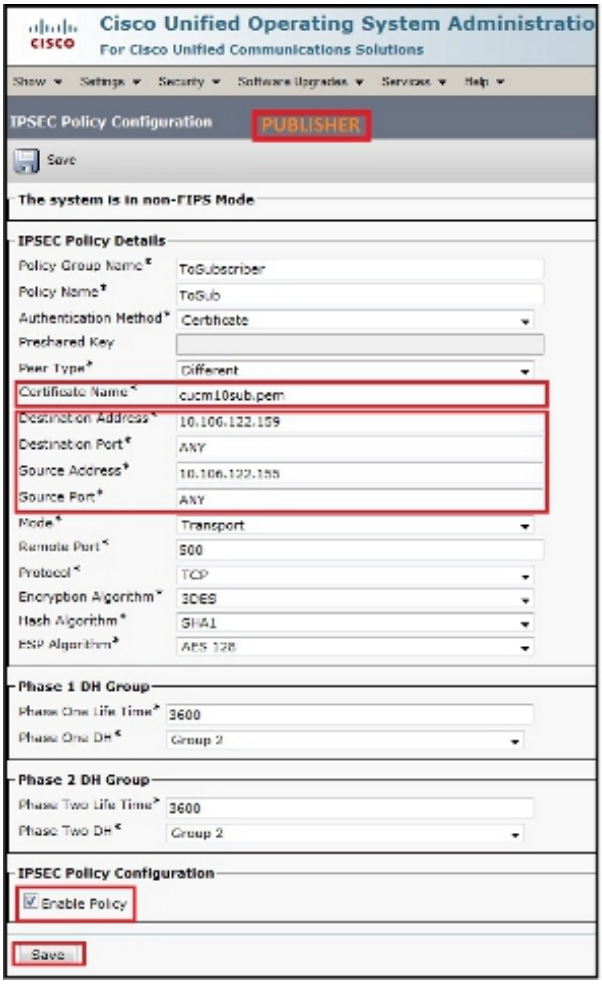
2. Accédez à **Security > IPSEC Configuration**.

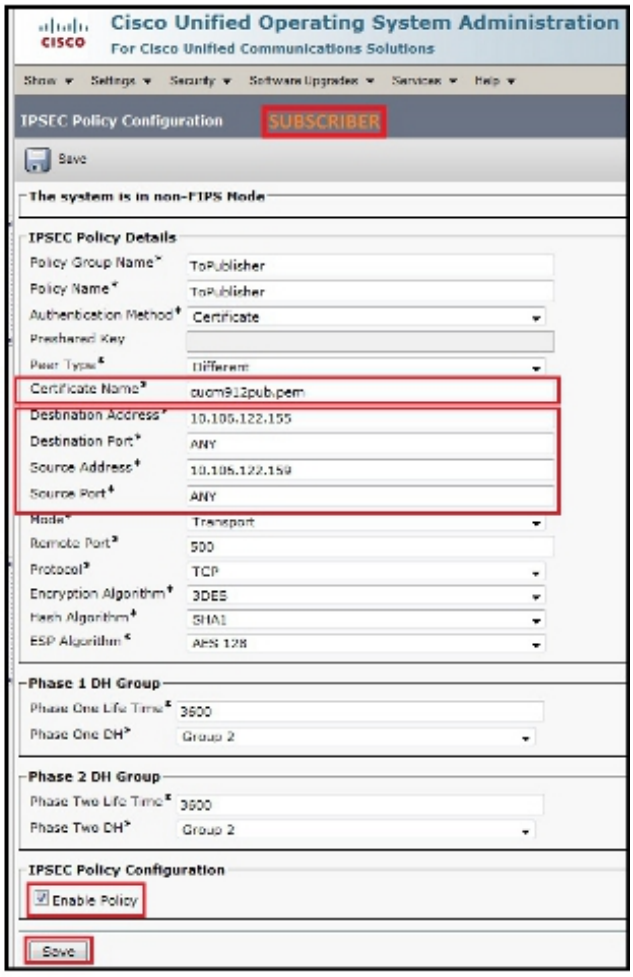
3. Utilisez ces informations afin de configurer l'IP et les détails du certificat :

*****

```
PUBLISHER : 10.106.122.155 & cucm912pub.pem
SUBSCRIBER: 10.106.122.15 & cucm10sub.pem

*****
```



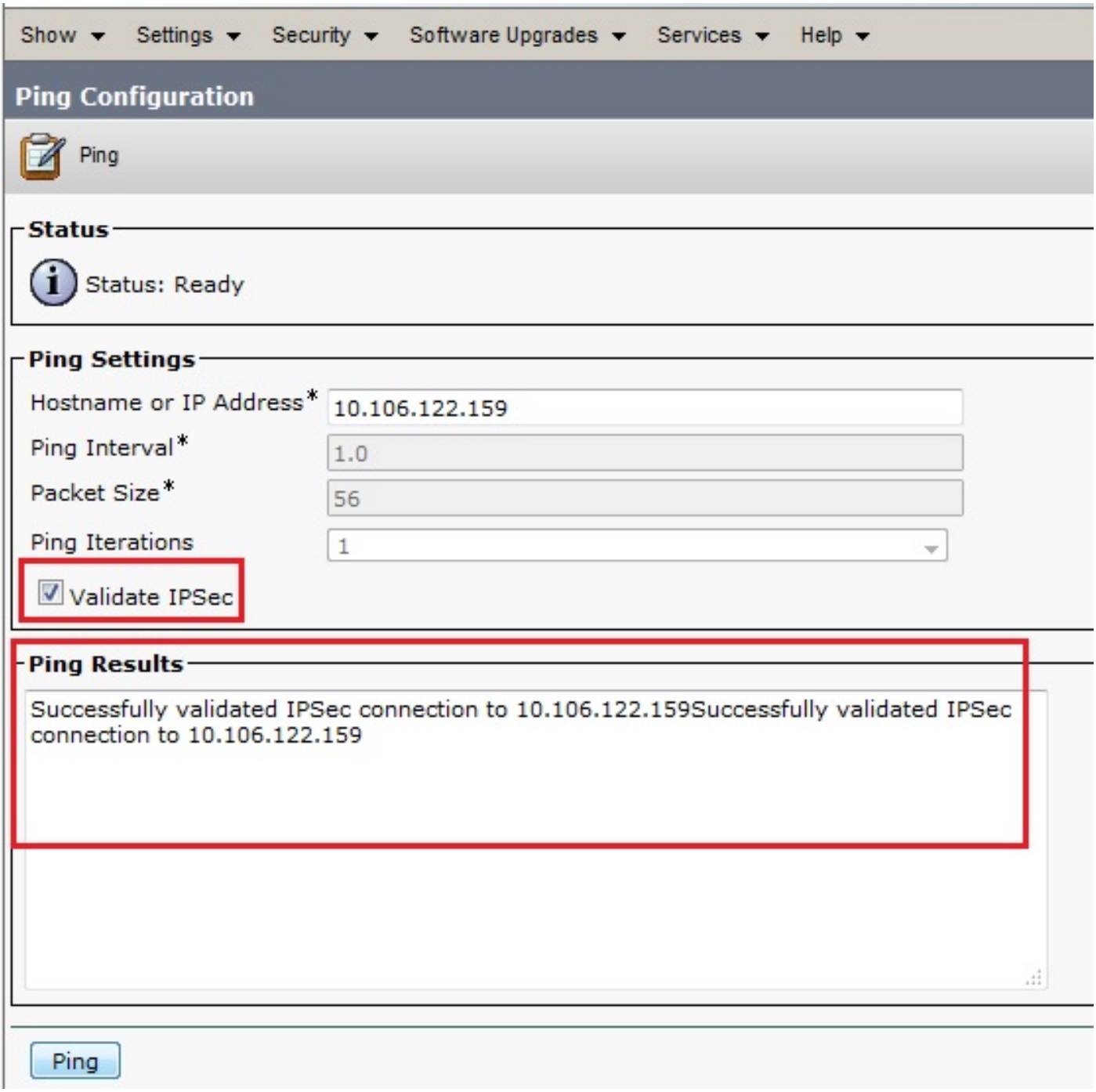




# Vérification

Complétez ces étapes afin de vérifier que votre configuration fonctionne et que la connectivité IPsec entre les noeuds est établie :

1. Connectez-vous à l'administration du système d'exploitation du serveur CUCM.
2. Accédez à **Services > Ping**.
3. Spécifiez l'adresse IP du noeud distant.
4. Cochez la case **Valider IPsec** et cliquez sur **Ping**.

Si la connectivité IPsec a été établie, un message semblable à celui-ci s'affiche :




## Dépannage

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

## Informations connexes

- Guide d'administration du système d'exploitation Cisco Unified Communications, version 8.6(1) - Configuration d'une nouvelle stratégie IPsec
- Support et documentation techniques - Cisco Systems