

# ノード間の IPSec 用 CUCM の設定

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[設定の概要](#)

[IPSec 接続を確認して下さい](#)

[IPsec 証明書をチェックして下さい](#)

[サブスクリバから IPsec ルート証明をダウンロードして下さい](#)

[サブスクリバからパブリッシャに IPsec ルート証明をアップロードして下さい](#)

[IPsec ポリシーを設定して下さい](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

この資料にクラスタ内の Cisco Unified Communications Manager ( CUCM ) ノード間の IPSec 接続を確立する方法を記述されています。

注: デフォルトで、CUCM ノード間の IPSec接続は無効になります。

## 前提条件

### 要件

Cisco は CUCM のナレッジがあることを推奨します。

### 使用するコンポーネント

この文書に記載されている情報は CUCM バージョン 10.5(1)に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。稼働中

のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## 設定

情報を使用して下さい CUCM を設定し、クラスタでノード間の IPsec 接続を確立するためにこのセクションに説明がある。

### 設定の概要

それぞれが続くセクションで詳述される、このプロシージャに関連するステップはここにありません:

1. ノード間の IPsec 接続を確認して下さい。
2. IPsec 証明書をチェックして下さい。
3. Subscriber ノードから IPsec ルート証明をダウンロードして下さい。
4. Subscriber ノードからパブリッシャ ノードに IPsec ルート証明をアップロードして下さい。
5. IPsec ポリシーを設定して下さい。


### IPsec 接続を確認して下さい

ノード間の IPsec 接続を確認するためにこれらのステップを完了して下さい:

1. CUCM サーバの Operating System ( OS ) 管理 ページにログイン して下さい。
2. サービス > PING へのナビゲート。
3. 遠隔ノード IP アドレスを規定 して下さい。
4. **検証 IPsec チェックボックス**をチェックし、**PING** をクリックして下さい。


IPsec 接続がない場合、これと同じような結果が表示されます:

## 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

## IPsec 証明書をチェックして下さい

IPsec 証明書をチェックするためにこれらのステップを完了して下さい:

1. OS 管理 ページにログイン して下さい。
2. セキュリティ > Certificate Management へのナビゲート。
3. IPsec 証明書のための検索 (パブリッシャ および サブスクライバ ノードに別々にログイン して下さい)。

注: Subscriber ノード IPsec 証明書は通常パブリッシャ ノードから視認できません; ただし、IPsec 信頼証明書として Subscriber ノードすべてのパブリッシャ ノード IPsec 証明書を表示できます。

IPsec 接続を可能にするために、他のノードの ipsec 信頼証明書として設定 される 1 つのノードからの IPsec 証明書がなければなりません:

**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

**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

*Note: A red box labeled "IPSEC Root certificates" has an arrow pointing to the "ipsec" row in the PUBLISHER table and the "ipsec" row in the SUBSCRIBER table.*

## サブスクライバからのダウンロード IPsec ルート証明

Subscriber ノードから IPsec ルート証明をダウンロードするためにこれらのステップを完了して下さい:

1. Subscriber ノードの OS 管理 ページにログイン して下さい。
2. **セキュリティ > Certificate Management** へのナビゲート。
3. IPsec ルート証明を開き、.pem 形式でダウンロード して下さい:

**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

*Note: A red box labeled "IPSEC Root certificates" has an arrow pointing to the "ipsec" row in the SUBSCRIBER table.*

**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
Signature Algorithm: 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
[
```

Regenerate Generate CSR **Download .PEM File** Download .DER File

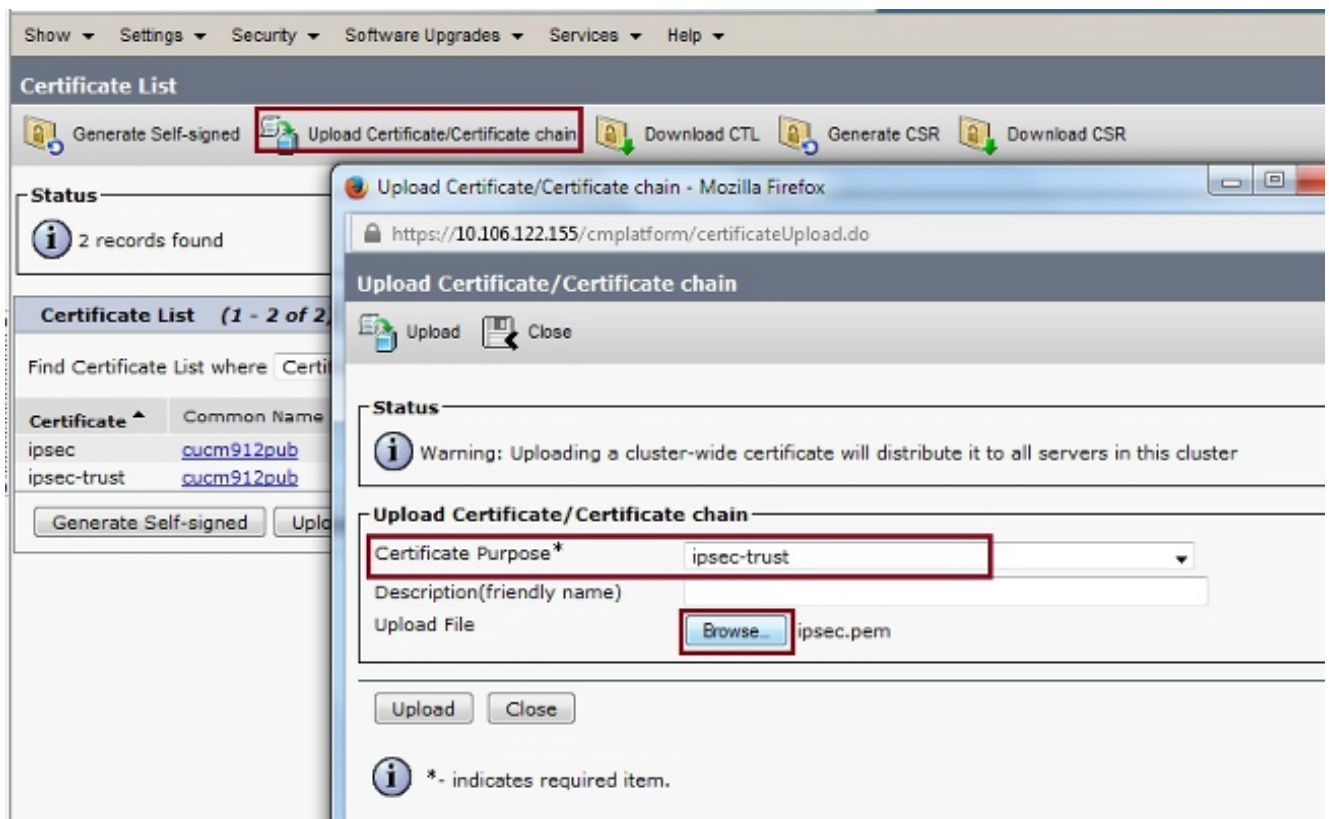
Close

## サブスクライバからパブリッシャに IPsec ルート証明をアップロードして下さい

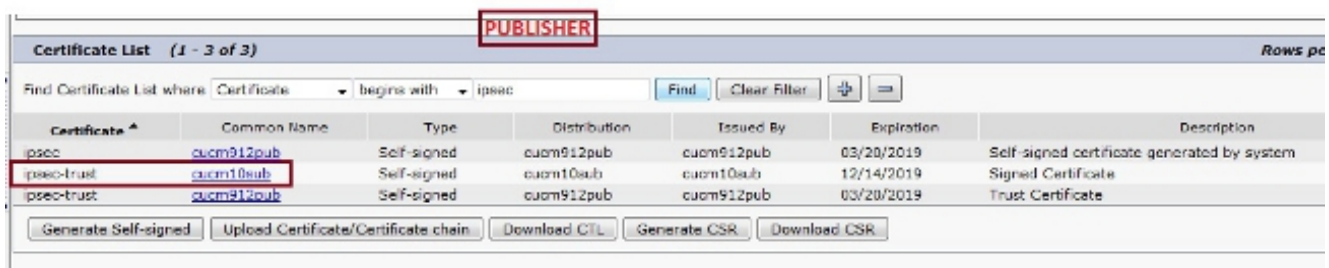
Subscriber ノードからパブリッシャ ノードに IPsec ルート証明をアップロードするためにこれらのステップを完了して下さい:

1. パブリッシャ ノードの OS 管理 ページにログイン して下さい。
2. **セキュリティ > Certificate Management** へのナビゲート。
3. **証明書/証明書 チェーン**を『Upload』 をクリックし、ipsec 信頼証明書として Subscriber ノード IPsec ルート証明をアップロードして下さい:





4. 証明書をアップロードした後、Subscriber ノード IPsec ルート証明が示されているように現われることを確認して下さい:



注: クラスタのマルチノード間の IPsec 接続を可能にするために必要となる場合それらのノードのための IPsec ルート証明をまたダウンロードして下さいパブリッシャ ノードに同じプロシージャによってそれらをアップロードします。

## 設定 IPsec ポリシー

IPsec ポリシーを設定するためにこれらのステップを完了して下さい:

1. パブリッシャおよび Subscriber ノードの OS 管理 ページに別々にログインして下さい。
2. セキュリティ > IPsec構成へのナビゲート。
3. IP および証明書の詳細を設定するためにこの情報を使用して下さい:

\*\*\*\*\*

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

\*\*\*\*\*

Cisco Unified Operating System Administration  
For Cisco Unified Communications Solutions

Show Settings Security Software Upgrades Services Help

IPSEC Policy Configuration **PUBLISHER**

Save

The system is in non-FIPS Mode

IPSEC Policy Details

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

Phase 1 DH Group

Phase One Life Time\* 3600  
Phase One DH\* Group 2

Phase 2 DH Group

Phase Two Life Time\* 3600  
Phase Two DH\* Group 2

IPSEC Policy Configuration

Enable Policy

Save

Cisco Unified Operating System Administration  
For Cisco Unified Communications Solutions

Show Settings Security Software Upgrades Services Help

IPSEC Policy Configuration **SUBSCRIBER**

Save

The system is in non-FIPS Mode

IPSEC Policy Details

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

Phase 1 DH Group

Phase One Life Time\* 3600  
Phase One DH\* Group 2

Phase 2 DH Group

Phase Two Life Time\* 3600  
Phase Two DH\* Group 2

IPSEC Policy Configuration

Enable Policy

Save

## 確認

ことノード間の IPsec 接続が確立されることを設定作業、そして確認するためにこれらのステップを完了して下さい:

1. CUCM サーバの OS 管理にログインして下さい。

2. サービス > PING へのナビゲート。


3. 遠隔ノード IP アドレスを規定して下さい。

4. 検証 IPsec チェックボックスをチェックし、PING をクリックして下さい。

IPsec 接続が確立される場合、これと同じようなメッセージが表示されます:


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

---

## トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- [Cisco Unified Communications オペレーティング システム管理 ガイド、リリース 8.6\(1\) – IPsec 新しいポリシーを設定して下さい](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)