

# ノード間の IPsec 用 CUCM の設定

## 内容

[概要](#)

[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接続の確認](#)

[IPsec証明書の確認](#)

[サブスクリバからのIPsecルート証明書のダウンロード](#)

[サブスクリバからパブリッシャへのIPsecルート証明書のアップロード](#)

[IPsecポリシーの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、クラスタ内のCisco Unified Communications Manager(CUCM)ノード間でIPsec接続を確立する方法について説明します。

注：デフォルトでは、CUCMノード間のIPsec接続は無効になっています。

## 前提条件

### 要件

CUCMに関する知識があることが推奨されます。

### 使用するコンポーネント

このドキュメントの情報は、CUCMバージョン10.5(1)に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。

。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 設定

このセクションで説明されている情報を使用して、CUCMを設定し、クラスタ内のノード間でIPSec接続を確立します。

### 設定の概要

次に、この手順に含まれる手順を示します。各手順については、以降のセクションで詳しく説明します。


1. ノード間のIPSec接続を確認します。
2. IPSec証明書を確認します。
3. サブスクライバノードからIPsecルート証明書をダウンロードします。
4. サブスクライバノードからパブリッシャノードにIPsecルート証明書をアップロードします。  
。
5. IPsecポリシーを設定します。

### IPSec接続の確認

ノード間のIPSec接続を確認するには、次の手順を実行します。


1. CUCMサーバの[Operating System (OS) Administration]ページにログインします。
  2. [Services] > [Ping] に移動します。
  3. リモートノードのIPアドレスを指定します。
  4. [Validate IPsec] チェックボックスをオンにして、[Ping] をクリックします。
- IPSec接続がない場合は、次の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証明書の確認

IPsec証明書を確認するには、次の手順を実行します。

1. [OS Administration]ページにログインします。
2. [Security] > [Certificate Management] に移動します。
3. IPsec証明書を検索します (パブリッシャノードとサブスクライバノードに別々にログインします)。

注：通常、サブスクライバノードのIPsec証明書はパブリッシャノードからは表示できません。ただし、パブリッシャノードのIPsec証明書は、すべてのサブスクライバノードでIPsec-Trust証明書として表示されます。

IPsec接続を有効にするには、一方のノードのIPsec証明書を他方のノードのipsec-trust証明書として設定する必要があります。

**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" points to the "ipsec" row in both screenshots.*

## サブスクライバからのIPsecルート証明書のダウンロード

サブスクライバノードからIPsecルート証明書をダウンロードするには、次の手順を実行します。

1. サブスクライバノードの[OS Administration]ページにログインします。
2. [Security] > [Certificate Management] に移動します。
3. IPsecルート証明書を開き、.pem形式でダウンロードします。

**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" points to the "ipsec" row.*

**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

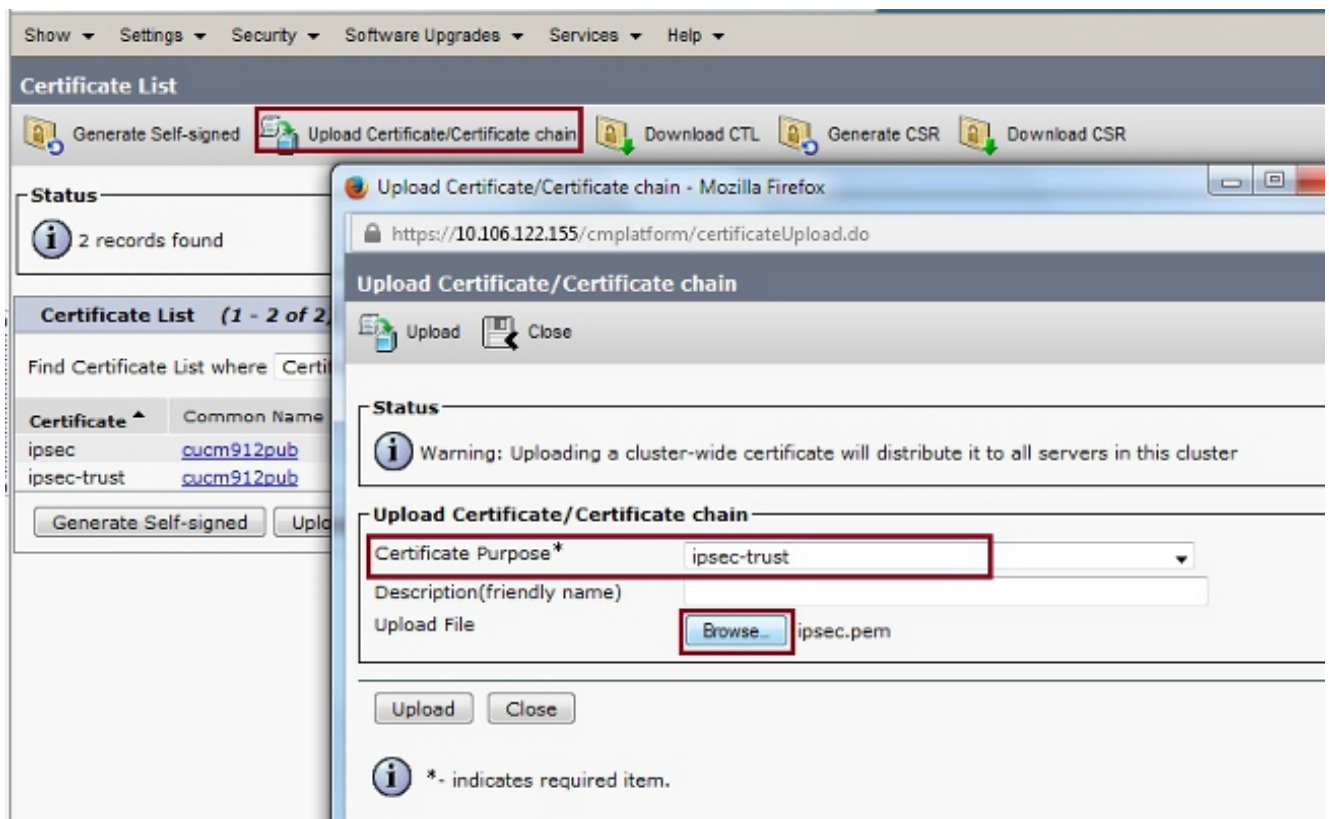
Close

## サブスクリバからパブリッシャへのIPsecルート証明書のアップロード

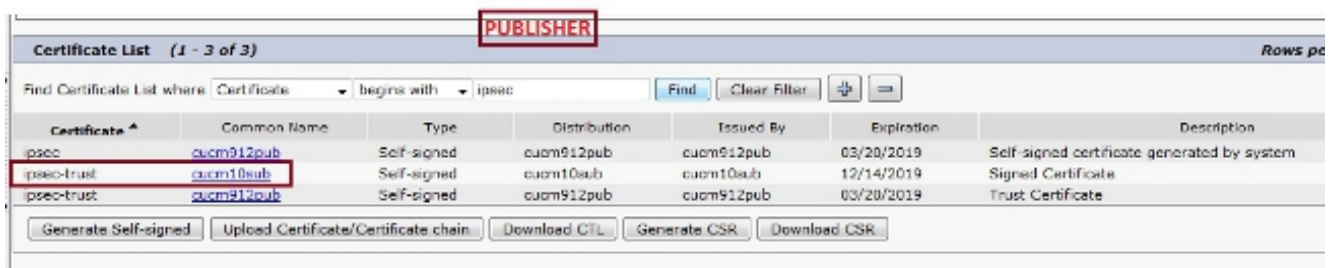
サブスクリバノードからパブリッシャノードにIPsecルート証明書をアップロードするには、次の手順を実行します。

1. パブリッシャノードの[OS Administration]ページにログインします。
2. [Security] > [Certificate Management] に移動します。
3. [Upload Certificate/Certificate chain] をクリックし、サブスクリバノードIPsecルート証明書をipsec-trust証明書としてアップロードします。





4. 証明書をアップロードした後、サブスクリバノードIPsecルート証明書が次のように表示されることを確認します。



注：クラスタ内の複数のノード間でIPsec接続を有効にする必要がある場合は、これらのノードのIPsecルート証明書もダウンロードし、同じ手順でパブリッシャノードにアップロードする必要があります。

## IPSecポリシーの設定

IPSecポリシーを設定するには、次の手順を実行します。

1. パブリッシャとサブスクリバノードのOS Administrationページに個別にログインします。
2. [Security] > [IPSEC Configuration] に移動します。
3. IPと証明書の詳細を設定するには、次の情報を使用します。

\*\*\*\*\*

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

次の手順を実行して、設定が機能していること、およびノード間のIPSec接続が確立されていることを確認します。

1. CUCMサーバのOS Administrationにログインします。
  2. [Services] > [Ping] に移動します。
  3. リモートノードのIPアドレスを指定します。
  4. [Validate IPsec] チェックボックスをオンにして、[Ping] をクリックします。
- IPSec接続が確立されると、次のようなメッセージが表示されます。

## Ping Configuration



Ping

### Status



Status: Ready

### Ping Settings

Hostname or IP Address\*

Ping Interval\*

Packet Size\*

Ping Iterations

Validate IPsec

### Ping Results

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

Ping

## トラブルシューティング

現在、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 Operating System Administration Guide, Release 8.6\(1\) - Set Up a New IPsec Policy』](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)