

# دقعلل نيب IPsec لاصتال CUCM نيوكت

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [نظرة عامة على التكوين](#)
- [التحقق من اتصال IPsec](#)
- [التحقق من شهادات IPsec](#)
- [تنزيل شهادة جذر IPsec من المشترك](#)
- [تحميل شهادة جذر IPsec من المشترك إلى الناشر](#)
- [تكوين نهج IPsec](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

## المقدمة

يوضح هذا المستند كيفية إنشاء اتصال IPsec بين عقد مدير الاتصالات الموحدة (CUCM) من Cisco داخل مجموعة.

ملاحظة: بشكل افتراضي، يتم تعطيل اتصال IPsec بين عقد CUCM.

## المتطلبات الأساسية

### المتطلبات

cisco يوصي أن يتلقى أنت معرفة من ال CUCM.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 10.5(1) من CUCM.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

# التكوين

أستخدم المعلومات الموضحة في هذا القسم لتكوين CUCM وإنشاء اتصال IPsec بين العقد في نظام مجموعة.

## نظرة عامة على التكوين

وفيما يلي الخطوات التي ينطوي عليها هذا الإجراء، والتي يرد تفصيل كل منها في الأقسام التالية:


1. تحقق من اتصال IPsec بين العقد.
2. تحقق من شهادات IPsec.
3. تنزيل شهادات جذر IPsec من عقدة المشترك.
4. قم بتحميل شهادة جذر IPsec من عقدة المشترك إلى عقدة Publisher.
5. قم بتكوين نهج IPsec.

## التحقق من اتصال IPsec

أكمل الخطوات التالية للتحقق من اتصال IPsec بين العقد:


1. قم بتسجيل الدخول إلى صفحة إدارة نظام التشغيل (OS) لخدوم CUCM.
2. انتقل إلى الخدمات < اختبار الاتصال.
3. حدد عنوان IP للعقدة البعيدة.
4. حدد خانة الاختيار **التحقق من IPsec** وانقر فوق **إختبار الاتصال**.  
في حالة عدم وجود اتصال IPsec، سترى النتائج المماثلة لما يلي:

## 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

## التحقق من شهادات IPsec

أتمت هذا steps in order to فحصت ال IPsec شهادة:

1. قم بتسجيل الدخول إلى صفحة إدارة نظام التشغيل.
2. انتقل إلى التأمين < إدارة الشهادات.

3. ابحث عن شهادات IPsec (قم بتسجيل الدخول إلى عقد الناشر والمشارك بشكل منفصل).

**ملاحظة:** لا يمكن عادة عرض شهادة IPsec لعقدة المشارك من عقدة Publisher؛ ومع ذلك، يمكنك رؤية شهادات IPsec لعقدة Publisher على جميع عقد المشارك كشهادة ثقة IPsec.

لتمكين اتصال IPsec، يجب أن يكون لديك شهادة IPsec من عقدة معينة كشهادة ثقة IPsec على العقدة الأخرى:

**PUBLISHER**

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	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

## تنزيل شهادة جذر IPsec من المشترك

أكمل هذه الخطوات لتنزيل شهادة جذر IPsec من عقدة المشترك:

1. قم بتسجيل الدخول إلى صفحة إدارة نظام التشغيل لعقدة المشترك.
2. انتقل إلى التأمين < إدارة الشهادات.
3. افتح شهادة جذر IPsec وقم بتنزيلها بتنسيق pem.

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

### 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
[
```

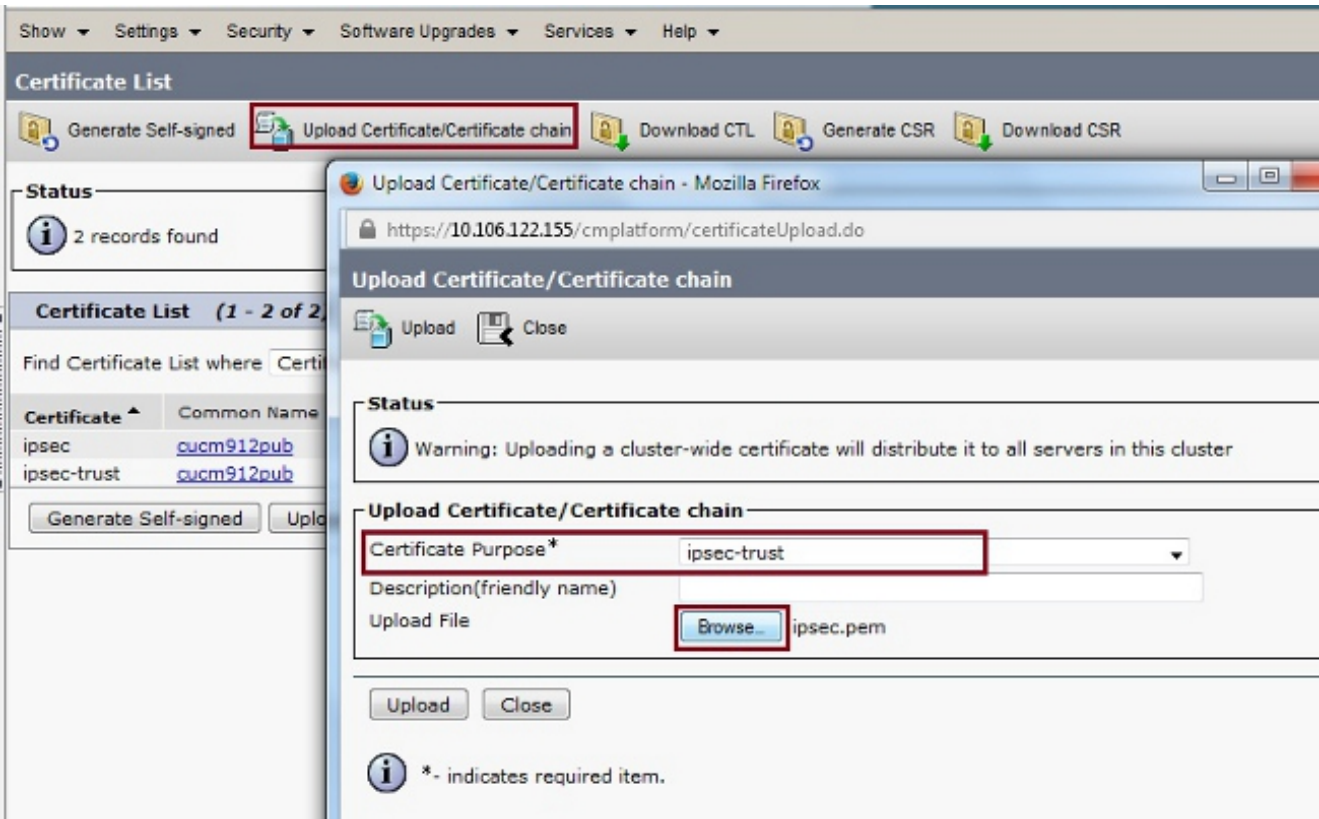
Regenerate Generate CSR Download .PEM File Download .DER File

Close

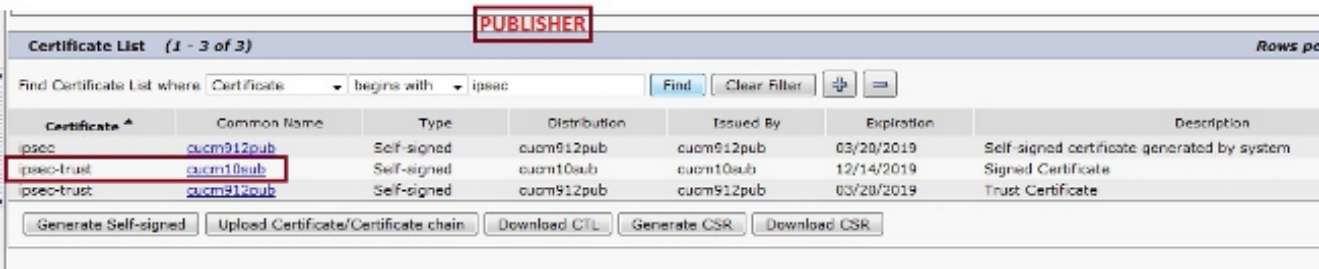
## تحميل شهادة جذر IPsec من المشترك إلى الناشر

أكمل هذه الخطوات لتحميل شهادة جذر IPsec من عقدة المشترك إلى عقدة الناشر:

1. قم بتسجيل الدخول إلى صفحة إدارة نظام التشغيل لعقدة Publisher.
2. انتقل إلى التأمين < إدارة الشهادات.
3. انقر فوق تحميل الشهادة/سلسلة الشهادات، وتحميل شهادة جذر IPsec لعقدة المشترك كشهادة ثقة IPSec.



4. بعد تحميل الشهادة، تحقق من ظهور شهادة جذر عقدة المشترك IPsec كما هو موضح:



ملاحظة: إذا كنت مطلوبا لتمكين اتصال IPsec بين عقد متعددة في مجموعة، فيجب عليك تنزيل شهادات جذر IPsec لهذه العقد أيضا وتحميلها إلى عقدة Publisher عبر الإجراء نفسه.

## تكوين نهج IPsec

أكمل الخطوات التالية لتكوين سياسة IPsec:

1. قم بتسجيل الدخول إلى صفحة إدارة نظام التشغيل الخاصة بـ Publisher وعقد المشترك بشكل منفصل.

2. انتقل إلى الأمان < تكوين IPsec.

3. أستخدم هذه المعلومات لتكوين تفاصيل IP والشهادة:

\*\*\*\*\*

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\* 10.106.122.159  
 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

**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


## التحقق من الصحة

أكمل هذه الخطوات للتحقق من عمل التكوين الخاص بك ومن إنشاء اتصال IPsec بين العقد:


1. قم بتسجيل الدخول إلى إدارة نظام التشغيل لخدّام CUCM.
2. انتقل إلى الخدمات < اختبار الاتصال.
3. حدد عنوان IP للعقدة البعيدة.
4. حدد خانة الاختيار التحقق من صحة IPsec وانقر فوق اختبار الاتصال.  
إذا تم إنشاء اتصال IPsec، سترى رسالة مماثلة لما يلي:

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

## استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

## معلومات ذات صلة

- [دليل إدارة نظام تشغيل الاتصالات الموحدة من Cisco، الإصدار 8.6\(1\) - إعداد سياسة IPsec جديدة](#)
- [الدعم التقني والمستندات - Cisco Systems](#)



ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س مل ا ذه Cisco ت مچرت  
م ل اع ل اء ان ا ع مچ ي ف ن م دخت س مل ل م عد و ت ح م م دقت ل ة يرش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ى ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س مل ا