

Configureer de CUCM voor IPsec-verbinding tussen knooppunten

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Overzicht van configuratie](#)

[Controleer de connectiviteit van IPsec](#)

[IPsec-certificaten controleren](#)

[IPsec Root-certificaat downloaden bij Subscriber](#)

[IPsec-wortelcertificaat uploaden van Subscriber naar Publisher](#)

[IPsec-beleid configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u IPsec-connectiviteit kunt instellen tussen de knooppunten van Cisco Unified Communications Manager (CUCM) binnen een cluster.

Opmerking: Standaard is de IPsec-verbinding tussen de CUCM-knooppunten uitgeschakeld.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van CUCM.

Gebruikte componenten

De informatie in dit document is gebaseerd op CUCM versie 10.5(1).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Gebruik de informatie die in deze sectie wordt beschreven om de CUCM te configureren en IPsec-connectiviteit tussen de knooppunten in een cluster te realiseren.

Overzicht van configuratie

Hieronder volgen de stappen die bij deze procedure betrokken zijn. Deze worden allemaal in de volgende paragrafen beschreven:

1. Controleer de IPsec-connectiviteit tussen de knooppunten.
2. Controleer de IPsec-certificaten.
3. Download de IPsec root certificaten van het Subscriber-knooppunt.
4. Upload het IPsec root certificaat van het Subscriber-knooppunt naar het knooppunt van Uitgevers.
5. Configureer het beleid van IPsec.


Controleer de connectiviteit van IPsec

Voltooi deze stappen om de IPsec-connectiviteit tussen de knooppunten te controleren:


1. Log in op de beheerpagina van het besturingssysteem van de CUCM server.
2. Navigeer naar **services > Ping**.
3. Specificeer het IP-adres van het externe knooppunt.
4. Controleer het aanvinkvakje **IPsec valideren** en klik op **Ping**.

Als er geen IPsec-connectiviteit is, ziet u resultaten vergelijkbaar:

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-certificaten controleren

Voltooi de volgende stappen om de IPsec-certificaten te controleren:

1. Log in op de pagina OS-beheer.
2. Blader naar **Security > certificaatbeheer**.
3. Zoeken naar de IPsec-certificaten (los van de knoppen Uitgever en Subscriber).

Opmerking: Het certificaat van Subscriber Node IPsec is gewoonlijk niet zichtbaar voor het knooppunt van Uitgevers. u kunt echter de IPsec-certificaten van het publiceerknooppunt op alle Subscriber-knooppunten zien als een IPsec-trust-certificaat.

Om IPsec-connectiviteit mogelijk te maken, moet u een IPsec-certificaat van één knooppunt hebben ingesteld als een **ipsec-trust**-certificaat voor het andere knooppunt:

PUBLISHER

Certificate List (1 - 2 of 2) Rows p

Find Certificate List where Certificate begins with ipsec Find Clear Filter

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

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR Download CSR

IPSEC Root certificates

SUBSCRIBER

Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec Find Clear Filter

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

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

IPsec Root-certificaat downloaden bij Subscriber

Voltooi deze stappen om het IPsec-wortelcertificaat te downloaden van het Subscriber-knooppunt:

1. Log in op de pagina OS-beheer van het Subscriber-knooppunt.
2. Blader naar **Security > certificaatbeheer**.
3. Open het IPsec-wortelcertificaat en download het in **.pem**-indeling:

IPSEC Root certificates

SUBSCRIBER

Certificate List (1 - 2 of 2) Rows

Find Certificate List where Certificate begins with ipsec Find Clear Filter

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

Generate Self-signed Upload Certificate/Certificate chain Generate CSR

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
  [
```

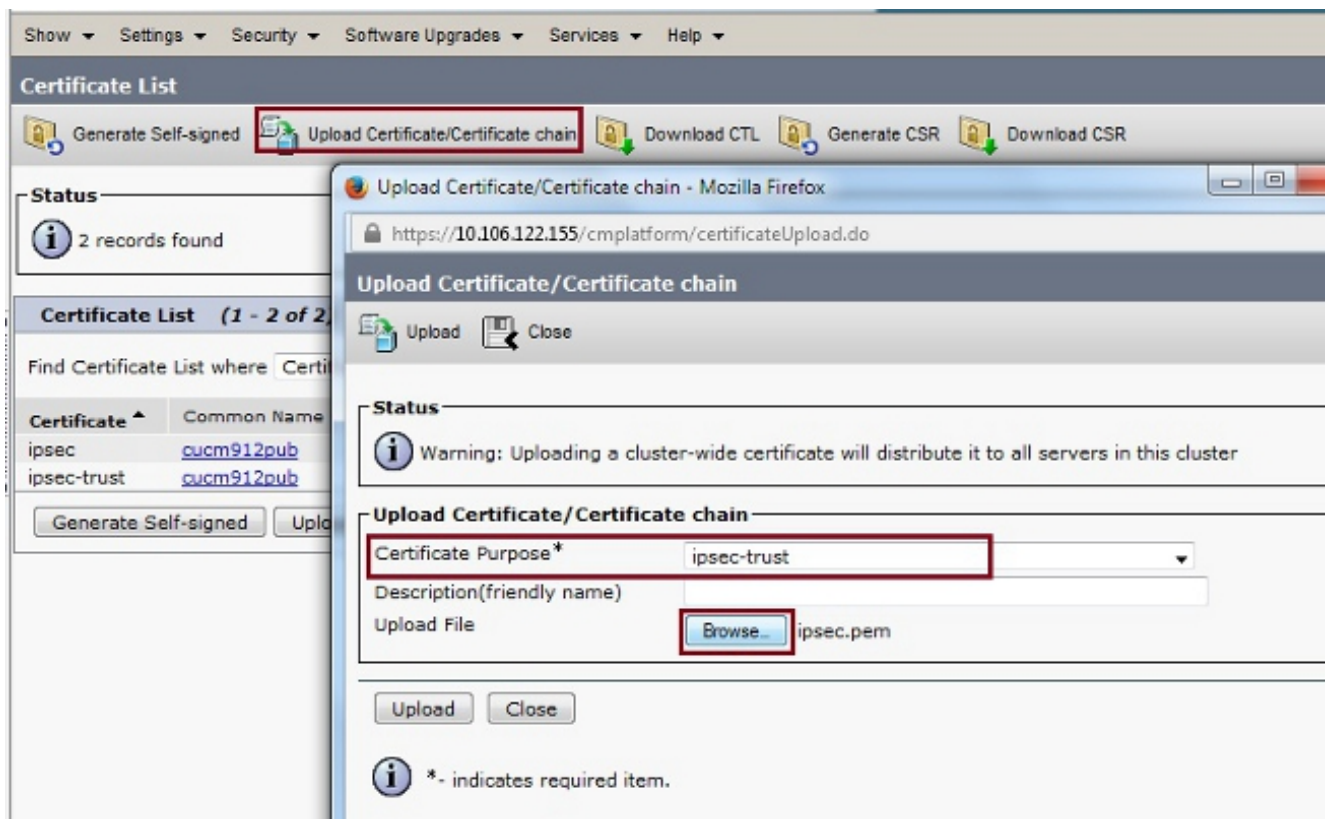
Regenerate Generate CSR **Download .PEM File** Download .DER File

Close

IPsec-wortelcertificaat uploaden van Subscriber naar Publisher

Voltooi deze stappen om het IPsec root certificaat van de Subscriber Node naar het knooppunt van de uitgever te uploaden:

1. Log in op de pagina OS-beheer van het knooppunt Uitgever.
2. Blader naar **Security > certificaatbeheer**.
3. Klik op **Upload certificaatketting/certificaatketting** en uploaden het Subscriber Node IPsec-basiscertificaat als een **ipsec-trust** certificaat:



4. Controleer na het uploaden van het certificaat of het Subscriber Node IPsec root certificaat verschijnt zoals wordt weergegeven:

PUBLISHER

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	cucm10sub	Self-signed	cucm10sub	cucm10sub	12/14/2019	Signed Certificate
ipsec-trust	cucm912pub	Self-signed	cucm912pub	cucm912pub	03/20/2019	Trust Certificate

Opmerking: Als u IPsec-connectiviteit tussen meerdere knooppunten in een cluster moet inschakelen en dan moet u ook de IPsec-wortelcertificaten voor die knooppunten downloaden en via dezelfde procedure naar het knooppunt van Uitgevers uploaden.

IPsec-beleid configureren

Voltooi deze stappen om het IPsec-beleid te configureren:

1. Meld u afzonderlijk aan in de OS-beheerpagina van de uitgever en de Subscriber-knooppunten.
2. Navigeer naar **security > IPSEC-configuratie**.
3. Gebruik deze informatie om de IP- en certificaatgegevens te configureren:

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 side. The page title is "IPSEC Policy Configuration" and it includes a "PUBLISHER" label. The system status is "The system is in non-FIPS Mode". The IPSEC Policy Details section is highlighted with a red box and contains the following fields: 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), and ESP Algorithm (AES 128). Below this, the Phase 1 DH Group and Phase 2 DH Group sections are visible, both with Phase One Life Time set to 3600 and Phase One DH set to Group 2. The IPSEC Policy Configuration section at the bottom has the "Enable Policy" checkbox checked. A "Save" button is located at the bottom left.

The screenshot shows the IPSEC Policy Configuration page for the SUBSCRIBER side. The page title is "IPSEC Policy Configuration" and it includes a "SUBSCRIBER" label. The system status is "The system is in non-FIPS Mode". The IPSEC Policy Details section is highlighted with a red box and contains the following fields: 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), and ESP Algorithm (AES 128). Below this, the Phase 1 DH Group and Phase 2 DH Group sections are visible, both with Phase One Life Time set to 3600 and Phase One DH set to Group 2. The IPSEC Policy Configuration section at the bottom has the "Enable Policy" checkbox checked. A "Save" button is located at the bottom left.

Verifiëren


Voltooi deze stappen om te verifiëren dat uw configuratie werkt en dat de IPsec-connectiviteit tussen de knooppunten is vastgesteld:

1. Log in op de OS-beheerder van de CUCM-server.
2. Navigeer naar **services > Ping**.
3. Specificeer het IP-adres van het externe knooppunt.
4. Controleer het aanvinkvakje **IPsec bevestigen** en klik op **Ping**.


Als de IPsec-connectiviteit is gerealiseerd, ziet u een vergelijkbaar bericht:

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

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Cisco Unified Communications Management Guide, release 8.6\(1\) - Stel een nieuw IPsec-beleid in](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)