

Настройте CUCM для IP - безопасного соединения между узлами

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Обзор конфигурации](#)

[Проверьте подключение IPsec](#)

[Проверьте сертификаты IPsec](#)

[Корневой сертификат IPsec загрузки от абонента](#)

[Корневой сертификат IPsec загрузки от абонента к издателю](#)

[Настройте политику IPsec](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает, как установить Подключение IPsec между узлами Cisco Unified Communications Manager (CUCM) в кластере.

Примечание: По умолчанию IP - безопасное соединение между узлами CUCM отключено.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с CUCM.

Используемые компоненты

Сведения в этом документе основываются на Версии 10.5 (1) CUCM.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Используйте информацию, которая описана в этом разделе, чтобы настроить CUCM и установить Подключение IPsec между узлами в кластере.

Обзор конфигурации

Вот шаги, которые вовлечены в эту процедуру, каждый из которых детализирован в разделах, которые придерживаются:

1. Проверьте Подключение IPsec между узлами.
2. Проверьте сертификаты IPsec.
3. Загрузите корневые сертификаты IPsec от узла Абонента.
4. Загрузите корневой сертификат IPsec от узла Абонента до узла Издателя.
5. Настройте политику IPsec.


Проверьте подключение IPsec

Выполните эти шаги для проверки Подключения IPsec между узлами:


1. Войдите в Страницу администратора Операционной системы (OS) сервера CUCM.
2. Перейдите к **Сервисам > Эхо-запрос**.
3. Задайте удаленный IP-адрес узла.
4. Проверьте флажок **Validate IPsec** и нажмите **Ping**.

Если нет никакого Подключения IPsec, то вы видите результаты, подобные этому:

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

Проверьте сертификаты IPsec

Выполните эти шаги для проверки сертификатов IPsec:

1. Войдите в Страницу администрирования операционной системы.
2. Перейдите к **Безопасности**> **Управление сертификатами**.
3. Ищите сертификаты IPsec (войдите в узлы Издателя и подписчика отдельно).

Примечание: Сертификат IPsec узла Абонента не обычно доступен для просмотра от узла Издателя; однако, вы видите сертификаты IPsec узла Издателя на всех узлах Абонента как Тростовой Ipsec сертификат.

Для включения Подключения IPsec у вас должен быть сертификат IPsec от одного набора узлов как **тростовой ipsec** сертификат на другом узле:

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

Корневой сертификат IPsec загрузки от абонента

Выполните эти шаги для загрузки корневого сертификата IPsec от узла Абонента:

1. Войдите в Страницу администрирования операционной системы узла Абонента.
2. Перейдите к **Безопасности**> **Управление сертификатами**.
3. Откройте корневой сертификат IPsec и загрузите его в формате **.pem**:

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
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
[
```

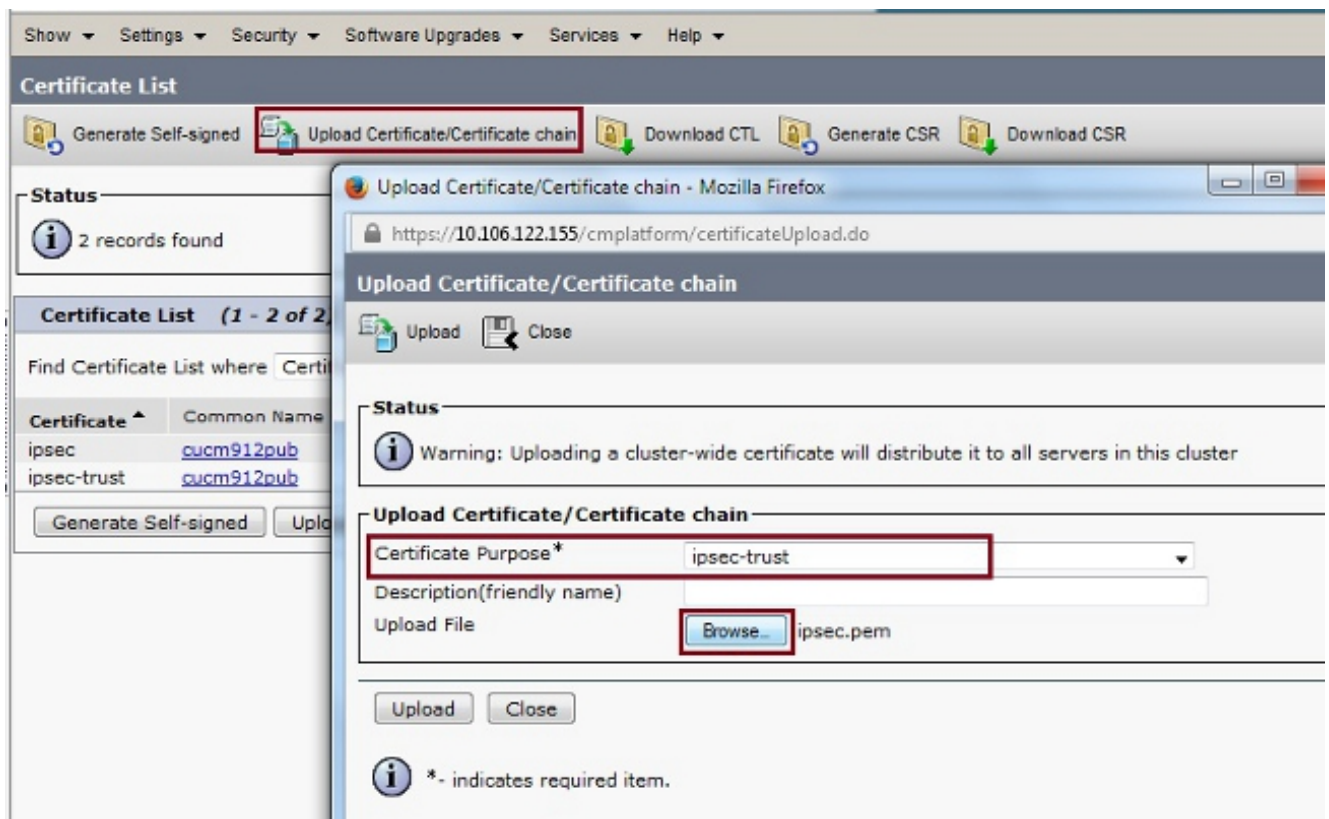
Regenerate Generate CSR **Download .PEM File** Download .DER File

Close

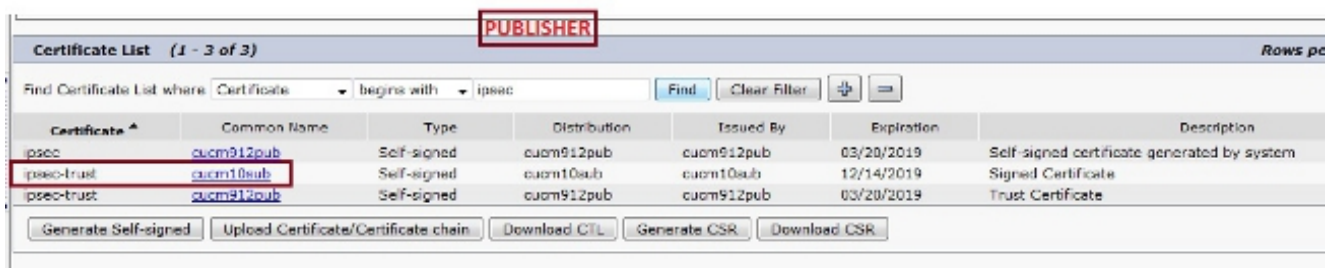
Корневой сертификат IPsec загрузки от абонента к издателю

Выполните эти шаги для загрузки корневого сертификата IPsec от узла Абонента до узла Издателя:

1. Войдите в Страницу администрирования операционной системы узла Издателя.
2. Перейдите к **Безопасности > Управление сертификатами**.
3. Нажмите **Upload Certificate/Certificate** и загрузите корневой сертификат IPsec узла Абонента как **трастовый ipsec** сертификат:



4. После того, как вы загрузите сертификат, проверите, что корневым сертификатом IPsec узла Абонента является как показано:



Примечание: Если вы обязаны включить Подключение IPsec между несколькими узлами в кластере, то необходимо загрузить корневые сертификаты IPsec для тех узлов также, и загрузать их к узлу Издателя с помощью той же процедуры.

Настройте политику IPsec

Выполните эти шаги для настройки политики IPsec:

1. Войдите в Страницу администрирования операционной системы Издателя и узлов Абонента отдельно.
2. Перейдите к **Безопасности** > **Конфигурация IPsec**.
3. Используйте эту информацию для настройки IP и сведений о сертификате:

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

Проверка


Выполните эти шаги, чтобы проверить, что ваша конфигурация работает и что установлено Подключение IPsec между узлами:

1. Войдите в администрирование ОС сервера CUCM.
2. Перейдите к **Сервисам**> Эхо-запрос.
3. Задайте удаленный IP-адрес узла.
4. Проверьте флажок **Validate IPsec** и нажмите **Ping**.


Если Подключение IPsec было установлено, то вы видите сообщение, подобное этому:

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

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- [Руководство по администрированию операционной системы унифицированной связи Cisco, выпуск 8.6 \(1\) – установленный новая политика IPsec](#)
- [Cisco Systems – техническая поддержка и документация](#)