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:

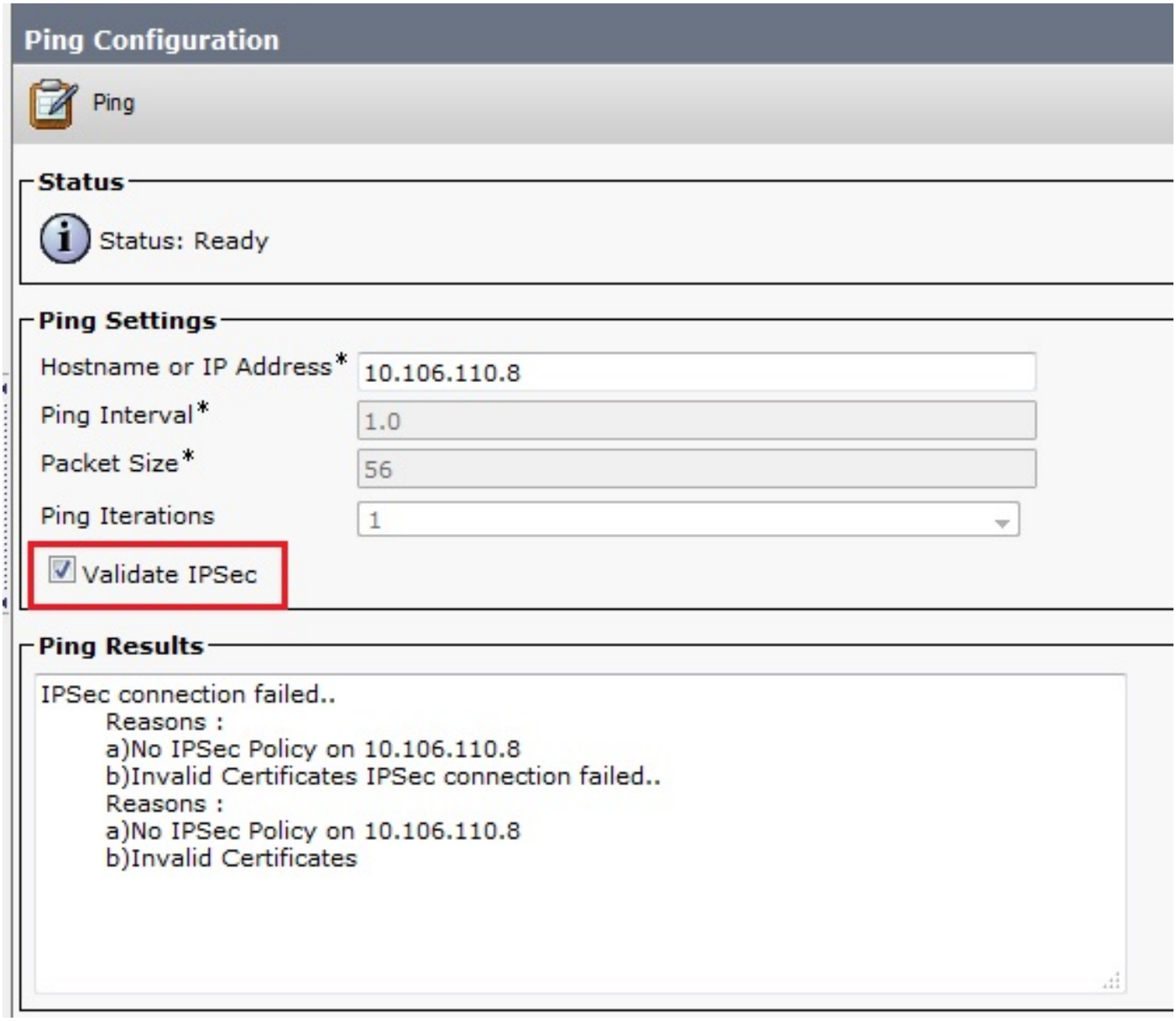
1. Проверьте Подключение IPsec между узлами.
2. Проверьте сертификаты IPsec.
3. Загрузите корневые сертификаты IPsec от узла Абонента.
4. Загрузите корневой сертификат IPsec от узла Абонента до узла Издателя.
5. Настройте политику IPsec.

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:



Проверьте сертификаты IPsec

Выполните эти шаги для проверки сертификатов IPsec:

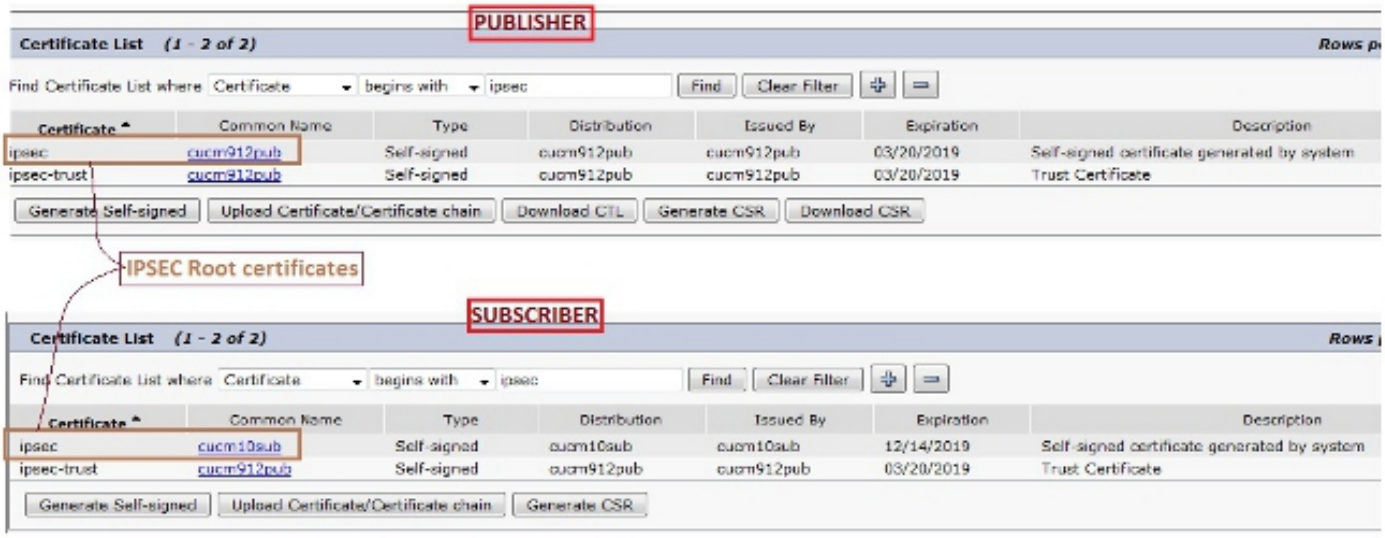
1. Войдите в Страницу администрирования операционной системы.

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 Трастовый Ipsec сертификат.

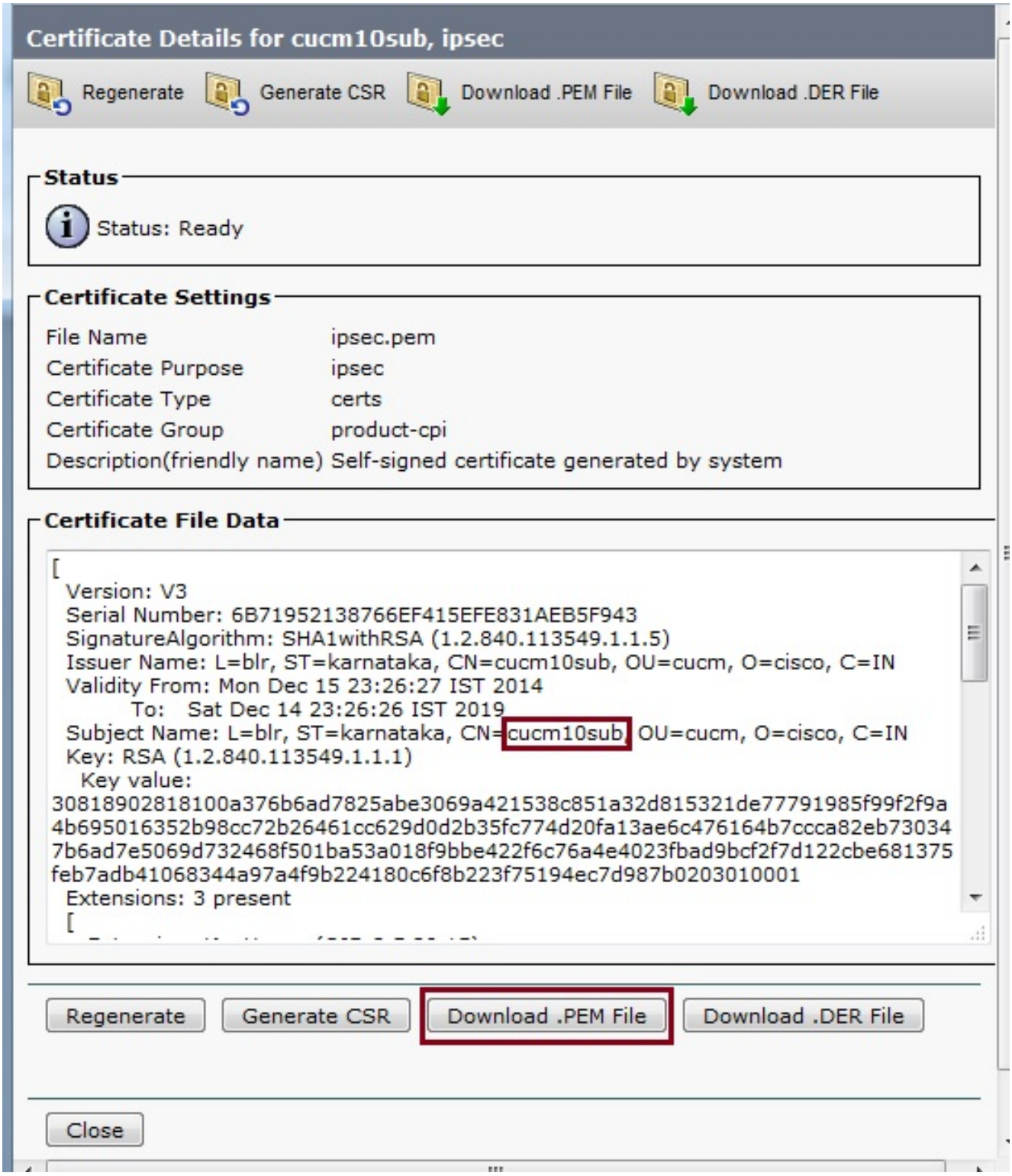
Для включения Подключения IPsec у вас должен быть сертификат IPsec от одного набора узлов как **трастовый ipsec** сертификат на другом узле:



Корневой сертификат IPsec загрузки от абонента

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

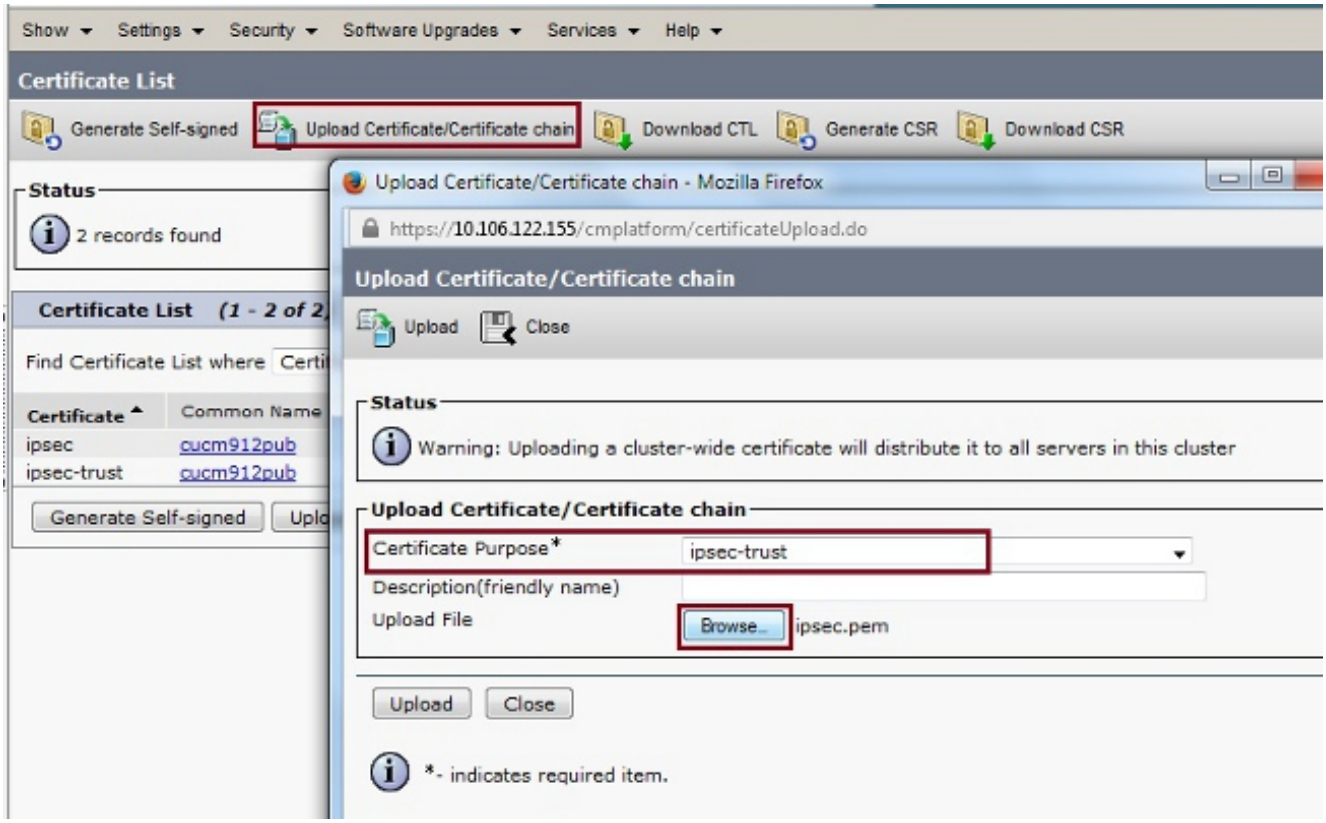
1. Войдите в Страницу администрирования операционной системы узла Абонента.
2. Перейдите к **Безопасности> Управление сертификатами**.
3. Откройте корневой сертификат IPsec и загрузите его в формате **.pem**:



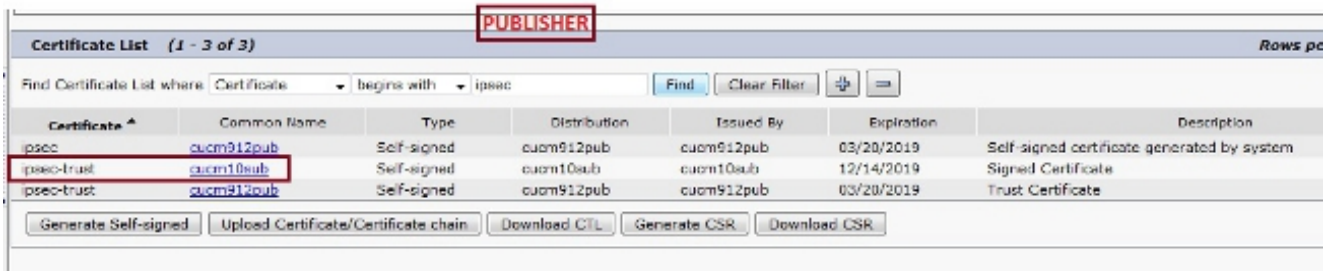
Корневой сертификат IPsec загрузки от абонента к издателю

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 корневой сертификат IPsec узла Абонента появляется как показано:



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

Настройте политику IPsec

Выполните эти шаги для настройки политики IPsec:

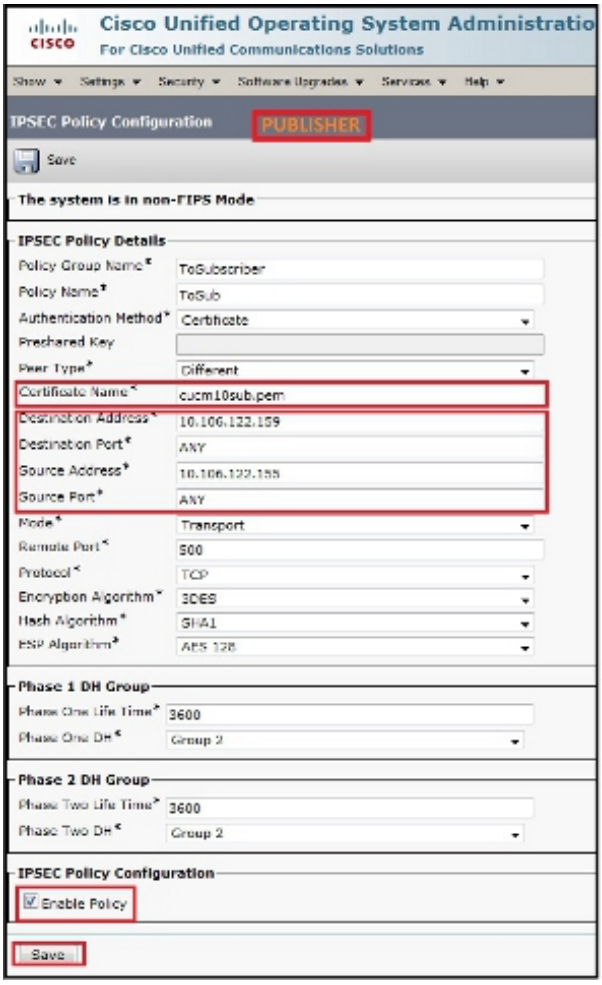
1. Войдите в Страницу администрирования операционной системы Издателя и узлов Абонента отдельно.

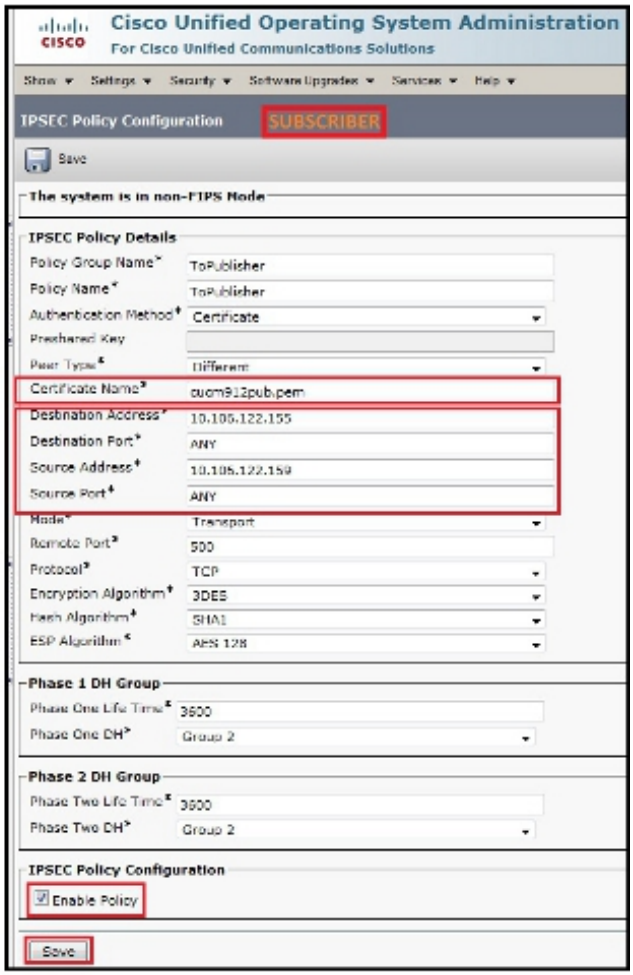
2. Перейдите к **Безопасности> Конфигурация IPSec**.

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
```

*****





Проверка

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

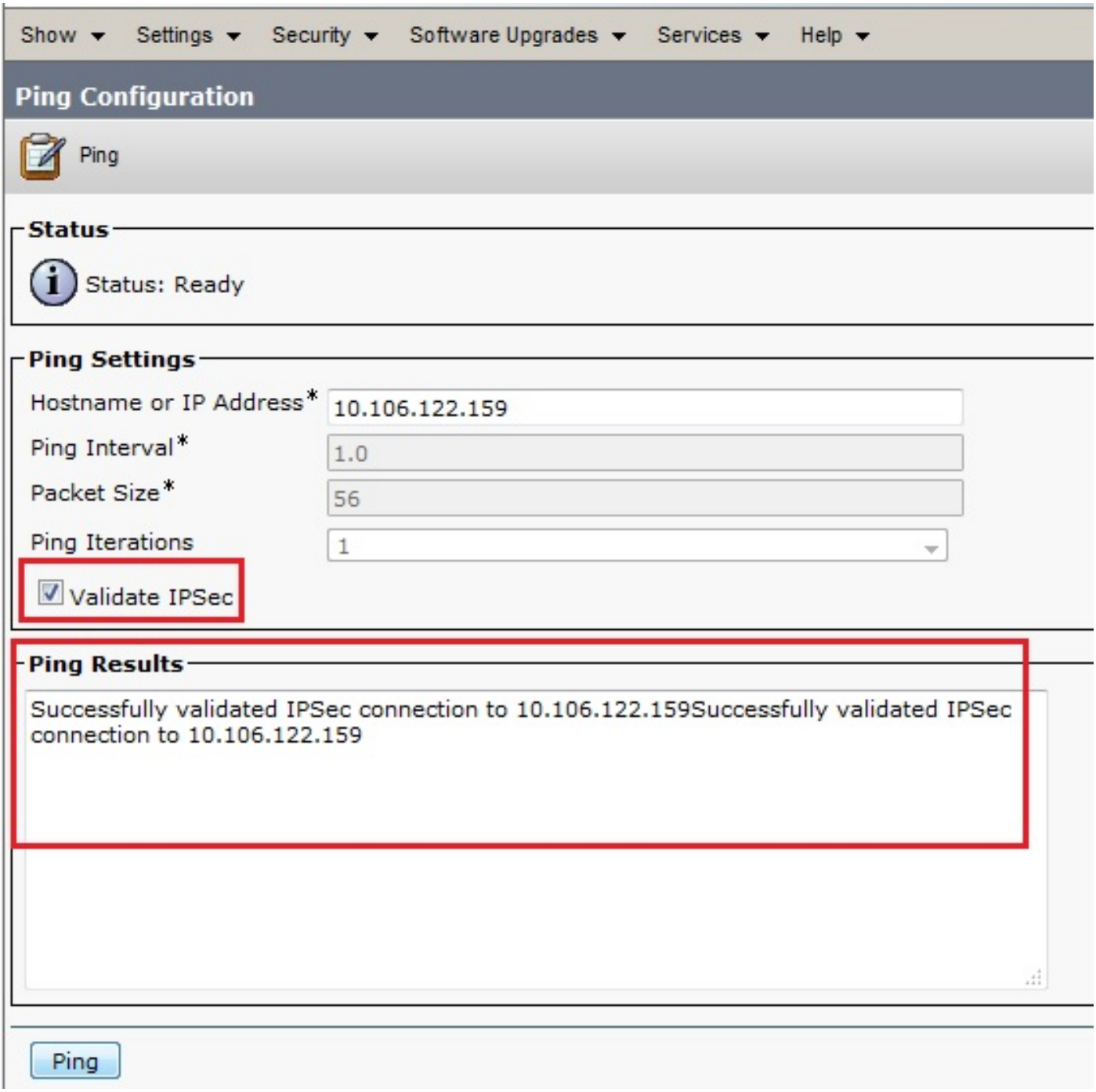
1. Войдите в администрирование ОС сервера CUCM.

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:



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