配置CUCM以实现节点之间的IPsec连接

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[配置概述](#)
[检验IPsec连接](#)
[检查IPsec证书](#)
[从用户下载IPsec根证书](#)
[将IPsec根证书从用户上传到发布服务器](#)
[配置IPsec策略](#)
[验证](#)
[故障排除](#)
[相关信息](#)

简介

本文档介绍如何在集群内的Cisco Unified Communications Manager(CUCM)节点之间建立IPsec连接。

> **注意：**默认情况下，CUCM节点之间的IPsec连接处于禁用状态。

先决条件

要求

Cisco建议您了解CUCM。

使用的组件

本文档中的信息基于CUCM 10.5(1)版。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

使用本节中描述的信息配置CUCM并在集群中的节点之间建立IPsec连接。

配置概述

以下是此过程涉及的步骤，以下各节将详细介绍这些步骤：

1. 检验节点之间的IPsec连接。

2. 检查IPsec证书。

3. 从用户节点下载IPsec根证书。

4. 将IPsec根证书从订阅服务器节点上传到发布服务器节点。

5. 配置IPsec策略。

检验IPsec连接

要验证节点之间的IPsec连接，请完成以下步骤：

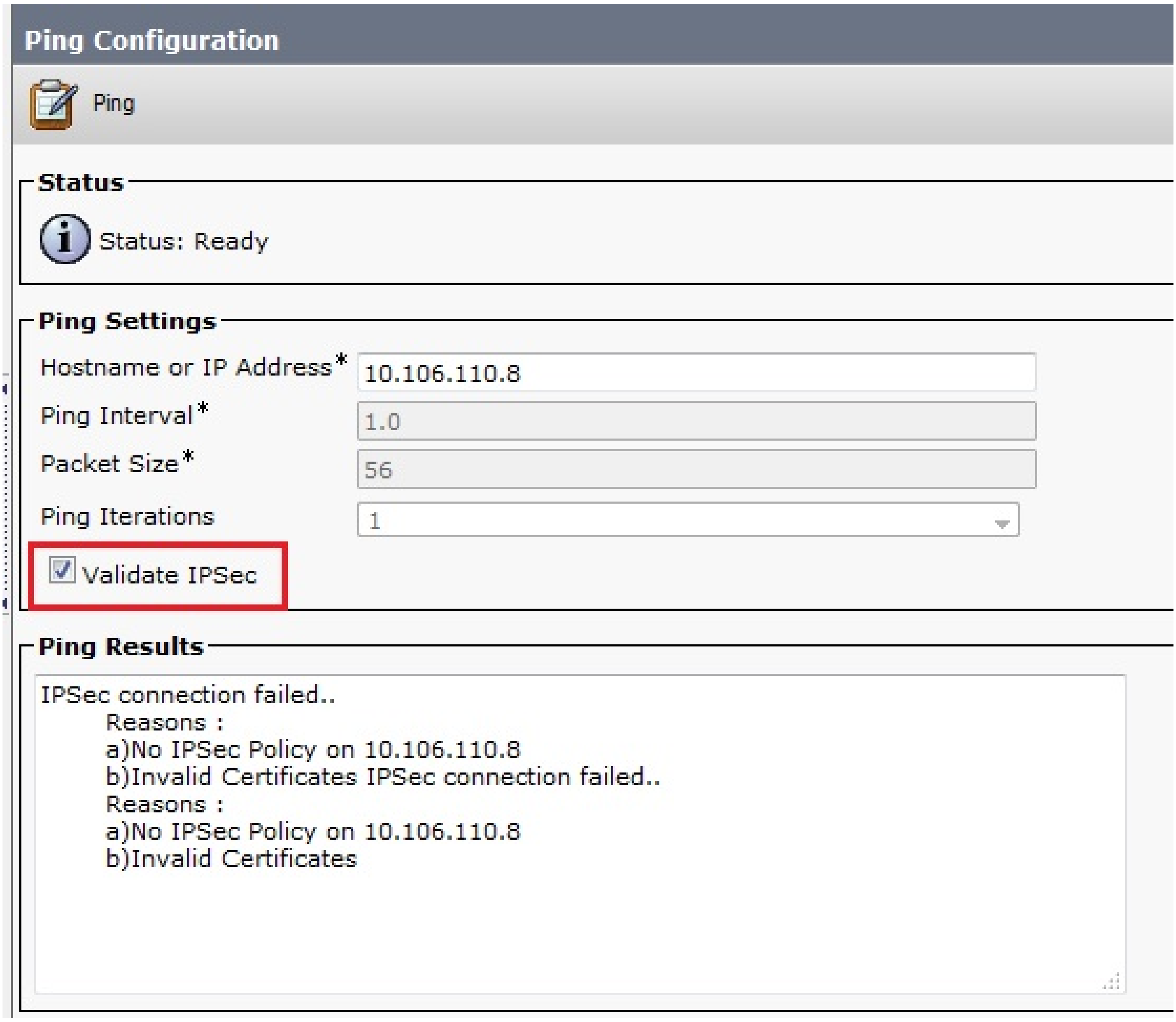
1. 登录到CUCM服务器的“操作系统(OS)管理”(Operating System [OS] Administration)页面。

2. 导航到**服务> Ping**。

3. 指定远程节点IP地址。

4. 选中**Validate IPsec**复选框并单击**Ping**。

如果没有IPsec连接，则会看到类似以下结果：



Status

Status: Ready

Ping Settings

Hostname or IP Address* 10.106.110.8

Ping Interval* 1.0

Packet Size* 56

Ping Iterations 1

☑ 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
```

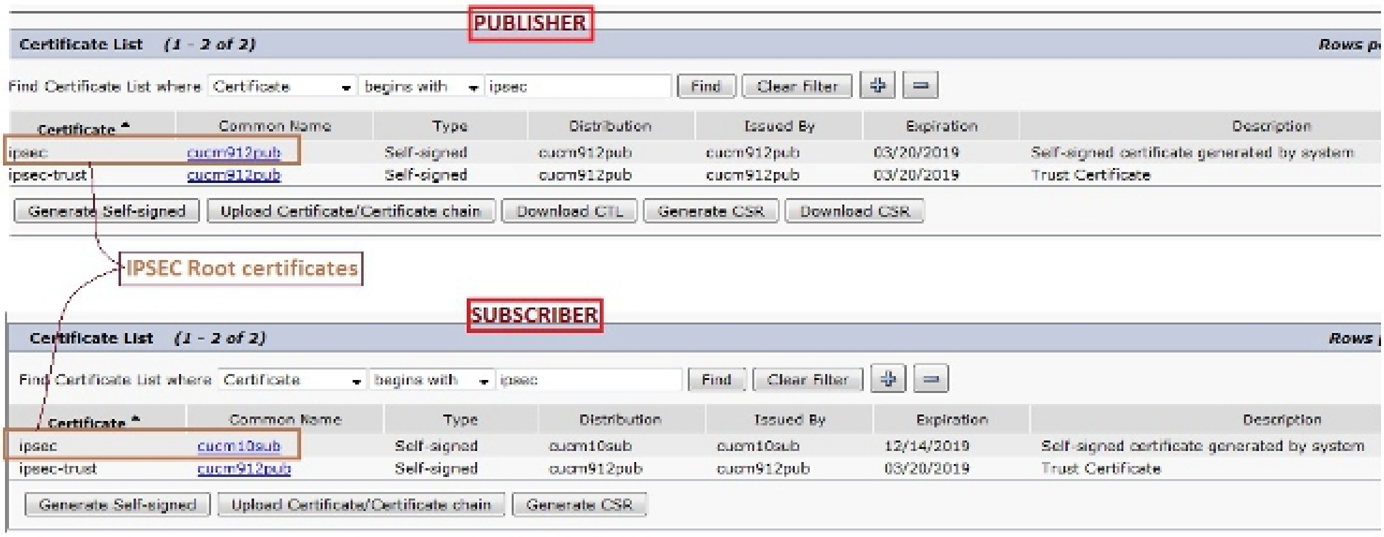
检查IPsec证书

完成以下步骤以检查IPsec证书：

1. 登录操作系统管理页面。
2. 导航到**安全>证书管理**。
3. 搜索IPsec证书（分别登录到发布服务器和订阅服务器节点）。

   注意：用户节点IPsec证书通常无法从发布服务器节点查看；但是，您可以看到所有用户节点上的发布服务器节点IPsec证书作为IPsec-Trust证书。

要启用IPsec连接，您必须将来自一个节点的IPsec证书设置为另一个节点上的**ipsec-trust**证书：


PUBLISHER
Find Certificate List where Certificate begins with ipsec
Find
Clear Filter
Generate Self-signed
Upload Certificate/Certificate chain
Download CTL
Generate CSR
Download CSR
IPSEC Root certificates
SUBSCRIBER
Find Certificate List where Certificate begins with ipsec
Find
Clear Filter
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR

Certificate List (1 - 2 of 2)

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

Certificate List (1 - 2 of 2)

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

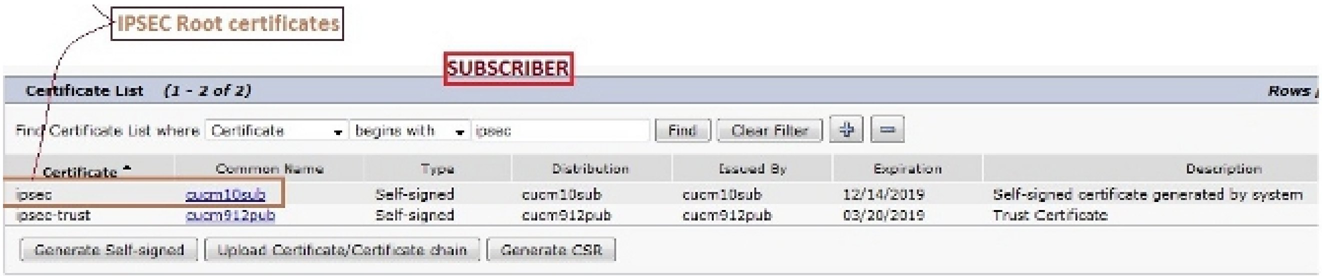
从用户下载IPsec根证书

要从用户节点下载IPsec根证书，请完成以下步骤：

1. 登录订用服务器节点的OS管理页面。

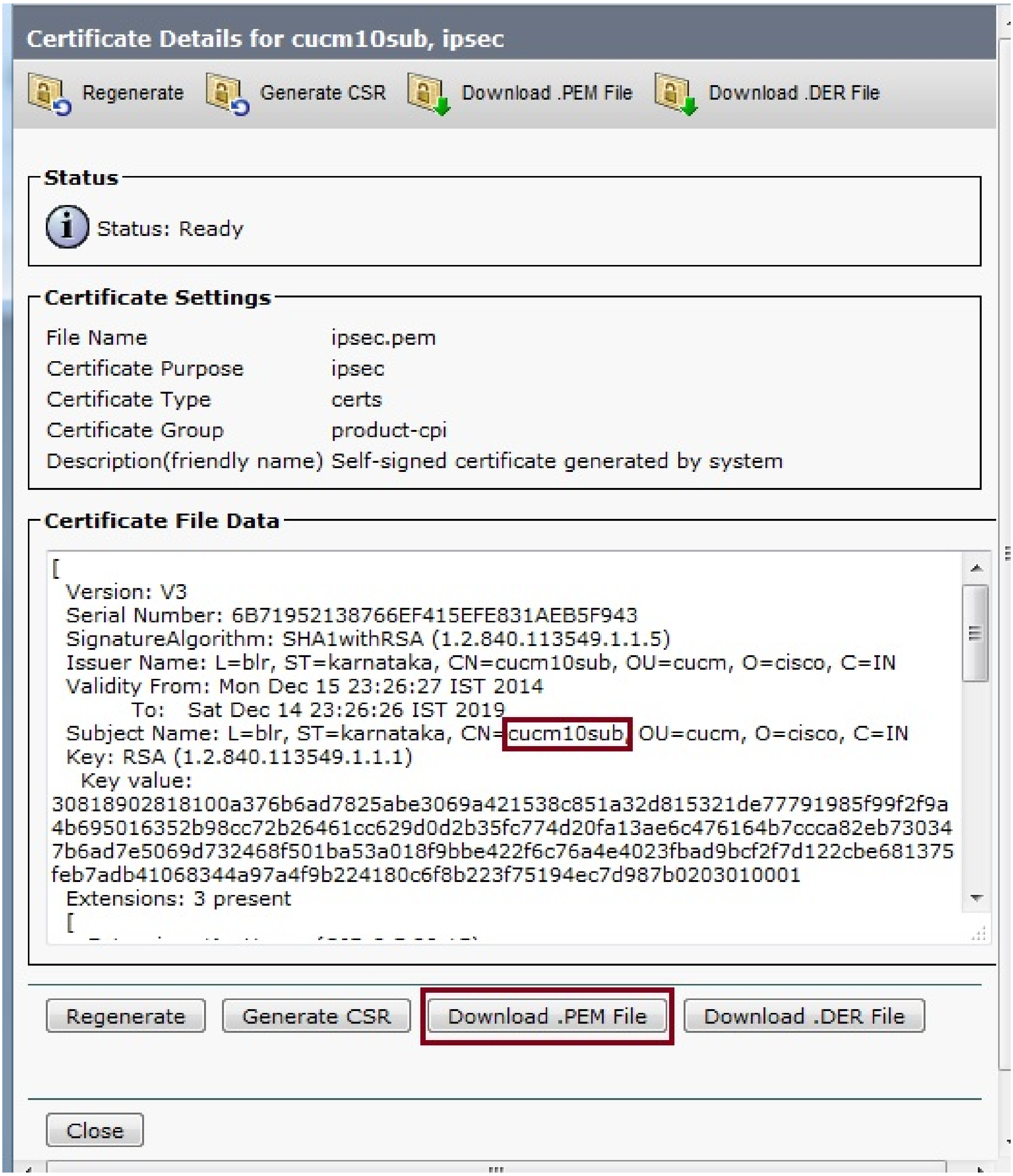
2. 导航到**安全>证书管理**。

3. 打开IPsec根证书并以.pem格**式下载**：


IPSEC Root certificates
SUBSCRIBER
Find Certificate List where Certificate begins with ipsec
Find
Clear Filter
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR

Certificate List (1 - 2 of 2)

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



Status: Ready

File Name ipsec.pem
Certificate Purpose ipsec
Certificate Type certs
Certificate Group product-cpi
Description(friendly name) Self-signed certificate generated by system

```
[
  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
  [
```

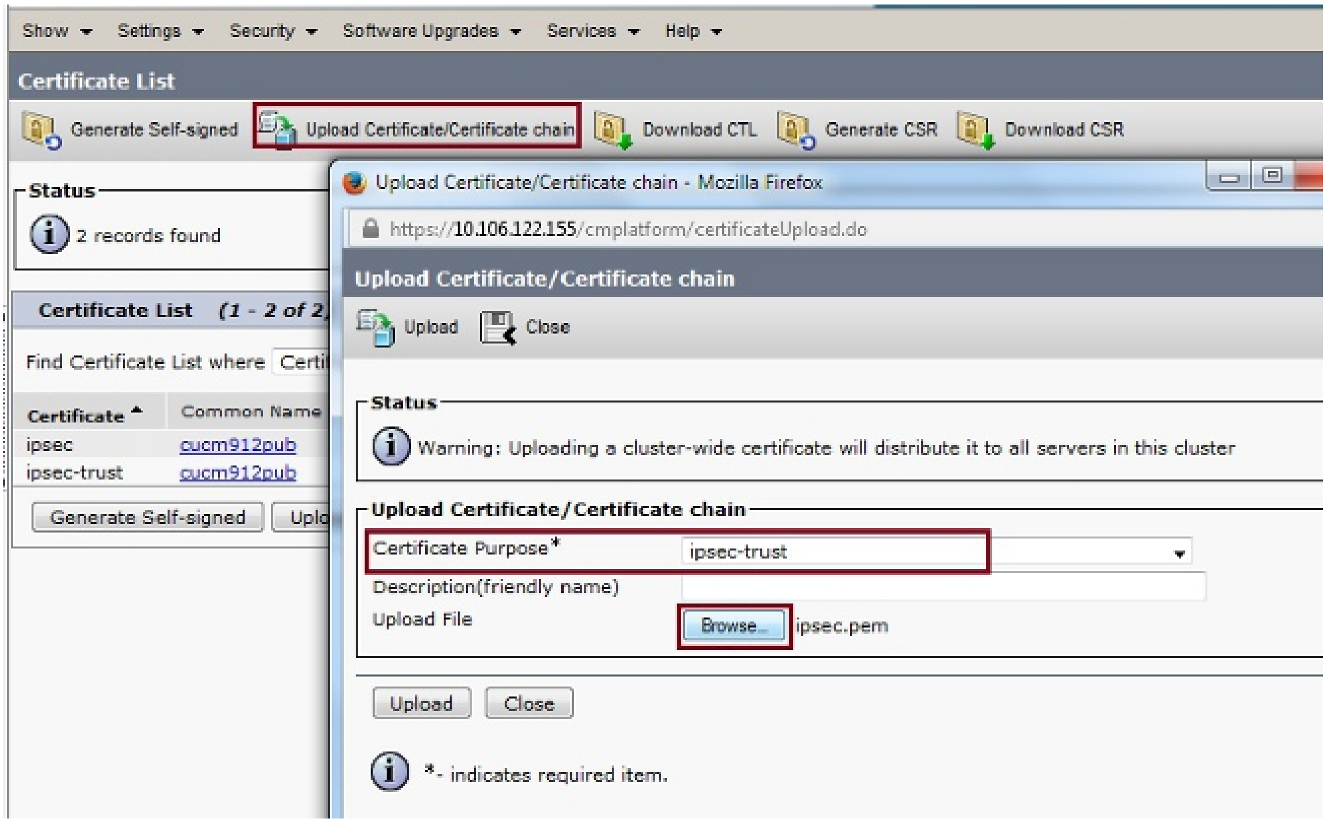
将IPsec根证书从用户上传到发布服务器

要将IPsec根证书从订阅服务器节点上传到发布服务器节点，请完成以下步骤：

1. 登录发布服务器节点的OS Administration页面。

2. 导航到**安全>证书管理。**

3. 单击**Upload Certificate/Certificate chain**，然后上传用户节点IPsec根证书作为**ipsec-trust**证书：


Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Download CTL
Generate CSR
Download CSR
Upload Certificate/Certificate chain - Mozilla Firefox
https://10.106.122.155/cmplatform/certificateUpload.do
Upload
Close

Status

2 records found

Certificate List (1 - 2 of 2

Find Certificate List where Certi

Certificate	Common Name
ipsec	cucm912pub
ipsec-trust	cucm912pub

Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

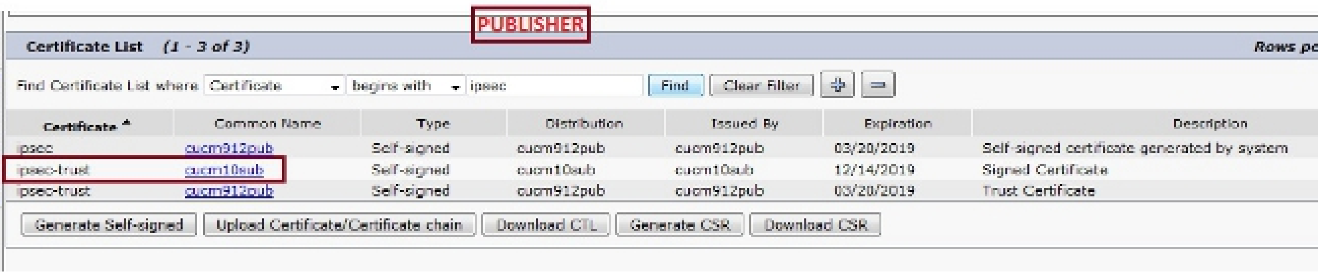
Certificate Purpose* ipsec-trust

Description(friendly name)

Upload File Browse... ipsec.pem

*- indicates required item.

4. 上传证书后，验证用户节点IPsec根证书是否如下所示：



Certificate List (1 - 3 of 3)

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

注意：如果需要在集群中的多个节点之间启用IPsec连接，则必须同时下载这些节点的IPsec根证书，并通过相同过程将其上传到发布方节点。

配置IPsec策略

要配置IPsec策略，请完成以下步骤：

1. 分别登录到发布服务器和订阅服务器节点的OS Administration页面。

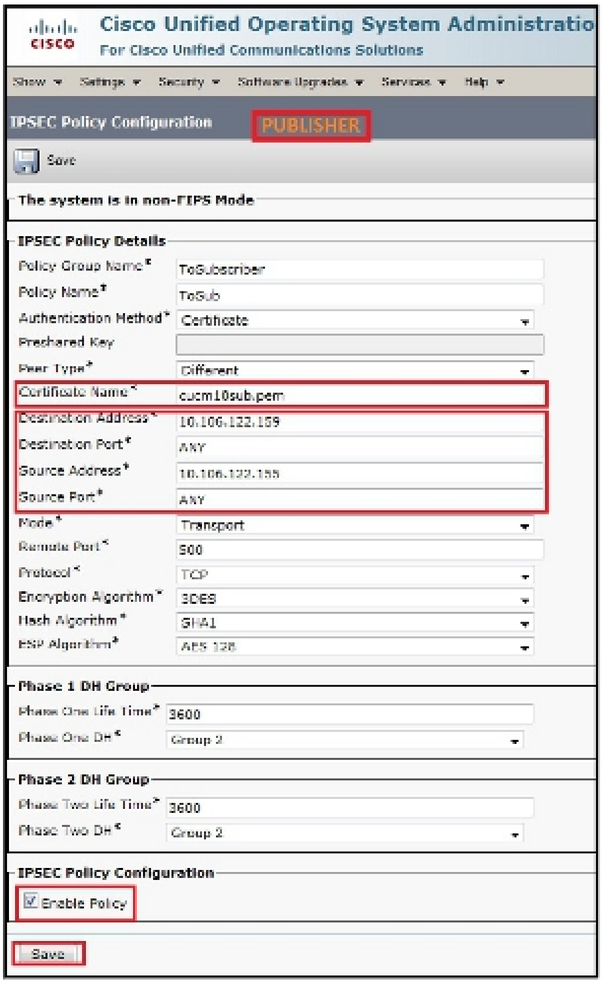
2. 导航到**安全> IPSEC配置**。

3. 使用此信息配置IP和证书详细信息：

```
*****

PUBLISHER : 10.106.122.155 & cucm912pub.pem
SUBSCRIBER: 10.106.122.15 & cucm10sub.pem

*****
```


Cisco Unified Operating System Administratio
For Cisco Unified Communications Solutions
Show
Settings
Security
Software Upgrades
Services
Help
Save

IPSEC Policy Configuration PUBLISHER

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

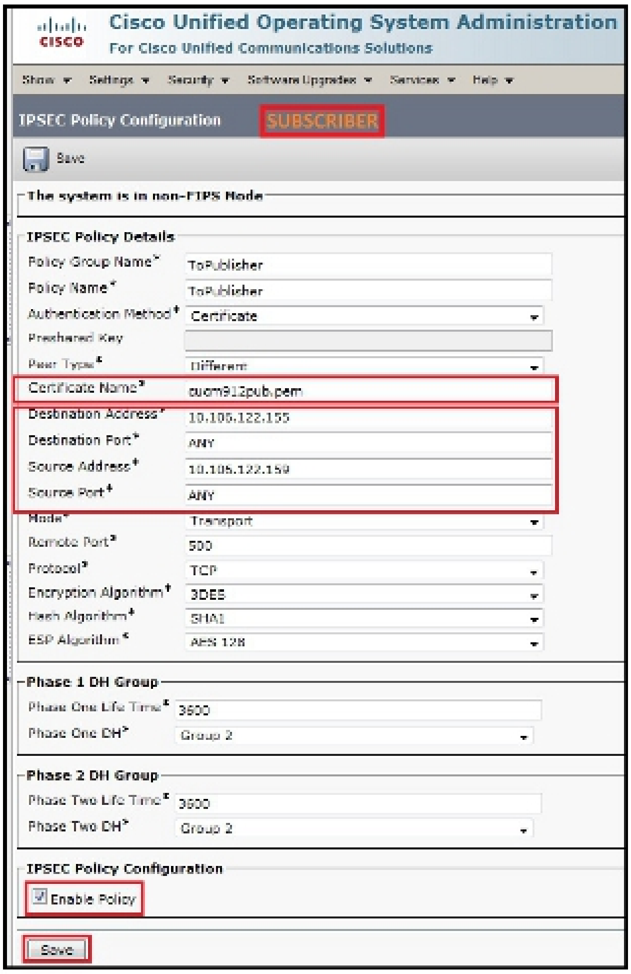
Phase 2 DH Group

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
Save

IPSEC Policy Configuration SUBSCRIBER

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

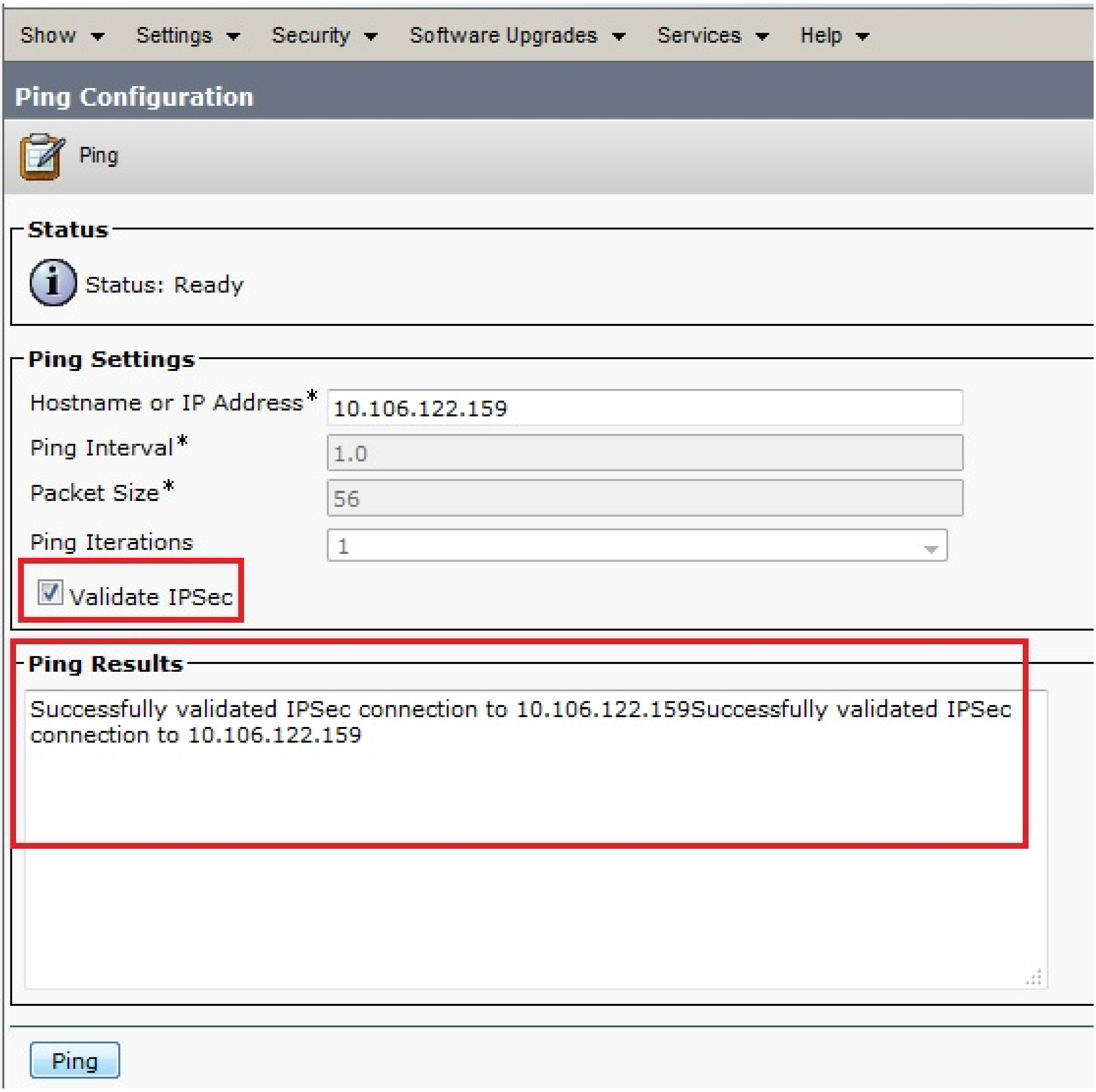
Save

验证

完成以下步骤以验证您的配置是否有效，以及节点之间是否建立了IPsec连接：

1. 登录到CUCM服务器的操作系统管理。
2. 导航到**服务> Ping**。
3. 指定远程节点IP地址。
4. 选中**Validate IPsec**复选框并单击**Ping**。

如果已建立IPsec连接，则会看到类似以下内容的消息：



Ping Configuration

Status

Status: Ready

Ping Settings

Hostname or IP Address* 10.106.122.159

Ping Interval* 1.0

Packet Size* 56

Ping Iterations 1

☑ Validate IPSec

Ping Results

Successfully validated IPSec connection to 10.106.122.159Successfully validated IPSec connection to 10.106.122.159

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科统一通信操作系统管理指南，版本8.6(1) — 设置新的IPsec策略
- 技术支持和文档 - Cisco Systems