配置CUCM以實現節點之間的IPsec連線

目錄

簡介

本文檔介紹如何在集群內的Cisco Unified Communications Manager(CUCM)節點之間建立IPsec連線。

> **附註**：預設情況下，CUCM節點之間的IPsec連線處於禁用狀態。

必要條件

需求

思科建議您瞭解CUCM。

採用元件

本檔案中的資訊是根據CUCM版本10.5(1)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

使用本節中介紹的資訊配置CUCM並在集群中的節點之間建立IPsec連線。

組態概觀

以下是此過程中涉及的步驟，以下各節詳述了每個步驟：

1. 檢驗節點之間的IPsec連線。

2. 檢查IPsec證書。

3. 從訂閱伺服器節點下載IPsec根證書。

4. 將IPsec根證書從訂閱伺服器節點上傳到發佈伺服器節點。

5. 配置IPsec策略。

檢驗IPsec連線

完成以下步驟，驗證節點之間的IPsec連線：

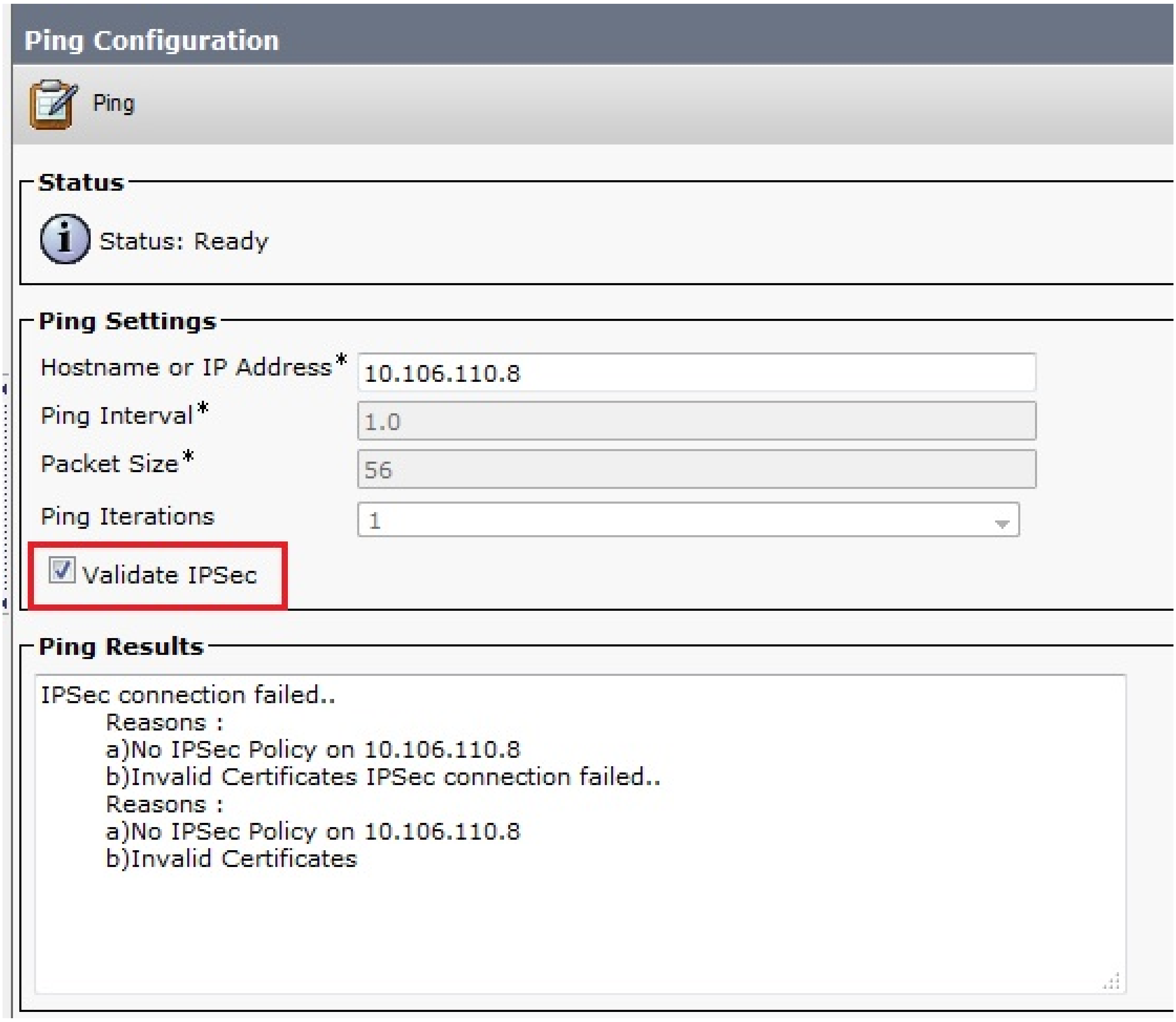
1. 登入到CUCM伺服器的作業系統(OS)管理頁面。

2. 導覽至**Services > Ping**。

3. 指定遠端節點IP地址。

4. 選中**Validate IPsec**覈取方塊並按一下**Ping**。

如果沒有IPsec連線，則會看到類似以下的結果：



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
```

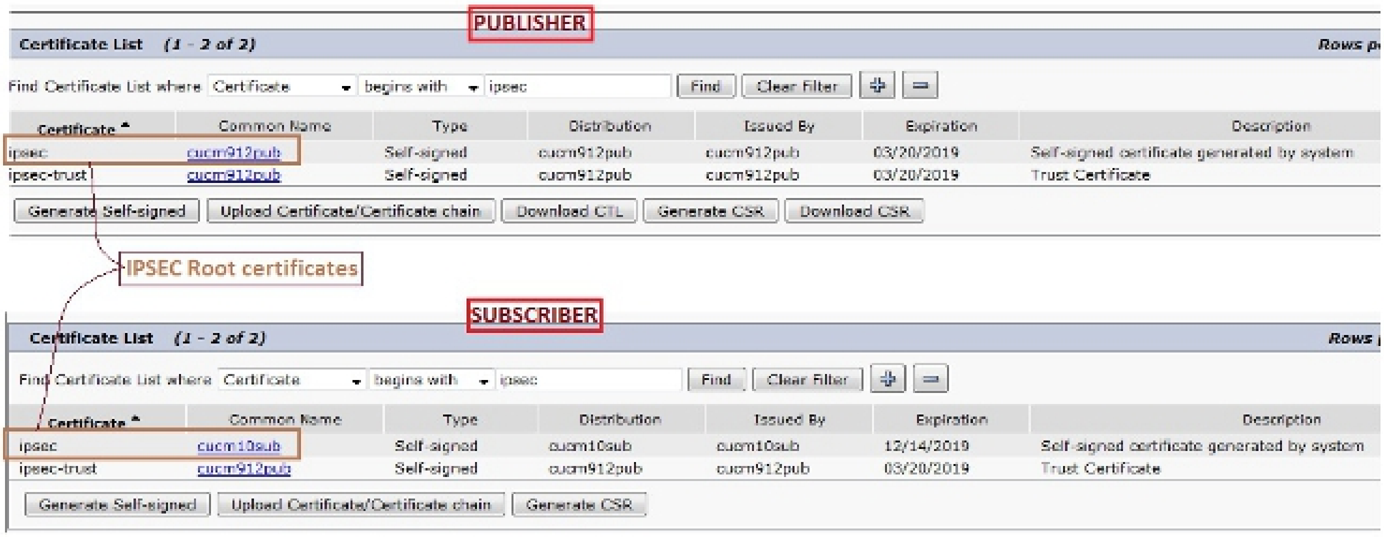
檢查IPsec證書

完成以下步驟即可檢查IPsec憑證：

1. 登入到「作業系統管理」頁。
2. 導覽至**Security > Certificate Management**。
3. 搜尋IPsec證書（分別登入到發佈伺服器和訂閱伺服器節點）。

   附註：通常無法從發佈伺服器節點檢視訂閱伺服器節點IPsec證書；但是，可以將所有訂閱伺服器節點上的發佈伺服器節點IPsec證書視為IPsec-Trust證書。

要啟用IPsec連線，必須將來自一個節點的IPsec證書設定為另一個節點上的**ipsec-trust**證書：



Certificate List (1 - 2 of 2)

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

Certificate List (1 - 2 of 2)

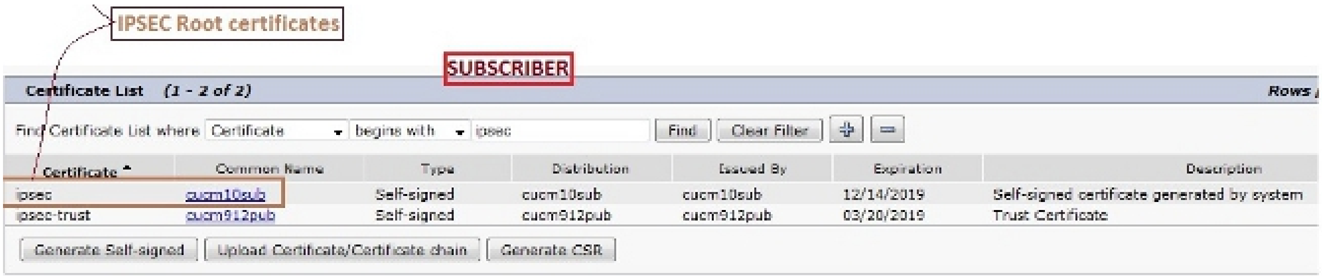
Find Certificate List where Certificate begins with ipsec

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

從訂閱伺服器下載IPsec根證書

完成以下步驟，以便從訂閱伺服器節點下載IPsec根證書：

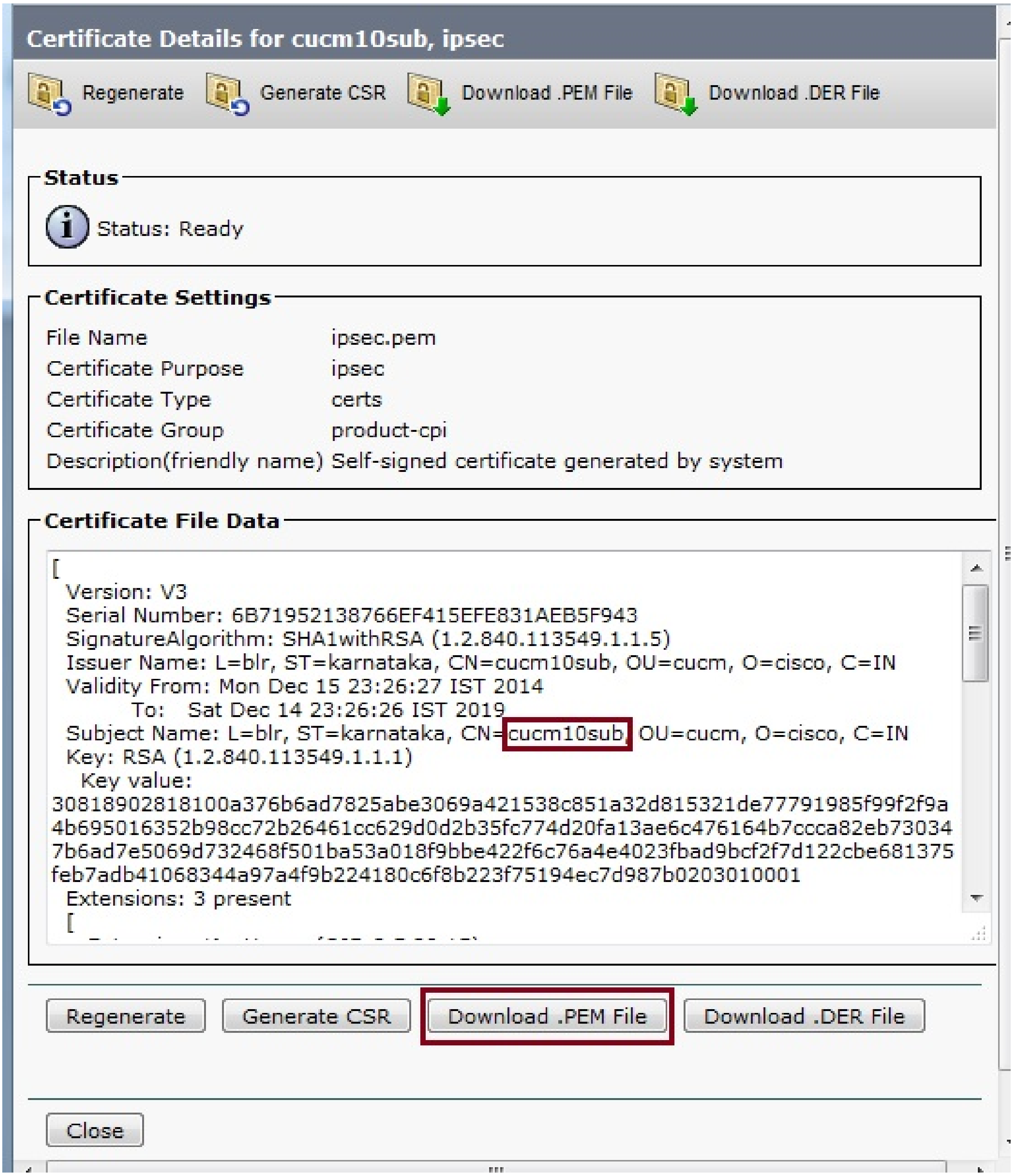
1. 登入到訂閱伺服器節點的OS管理頁。
2. 導覽至**Security > Certificate Management**。
3. 開啟IPsec根證書並以**.pem格式**下載：



Certificate List (1 - 2 of 2)

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



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

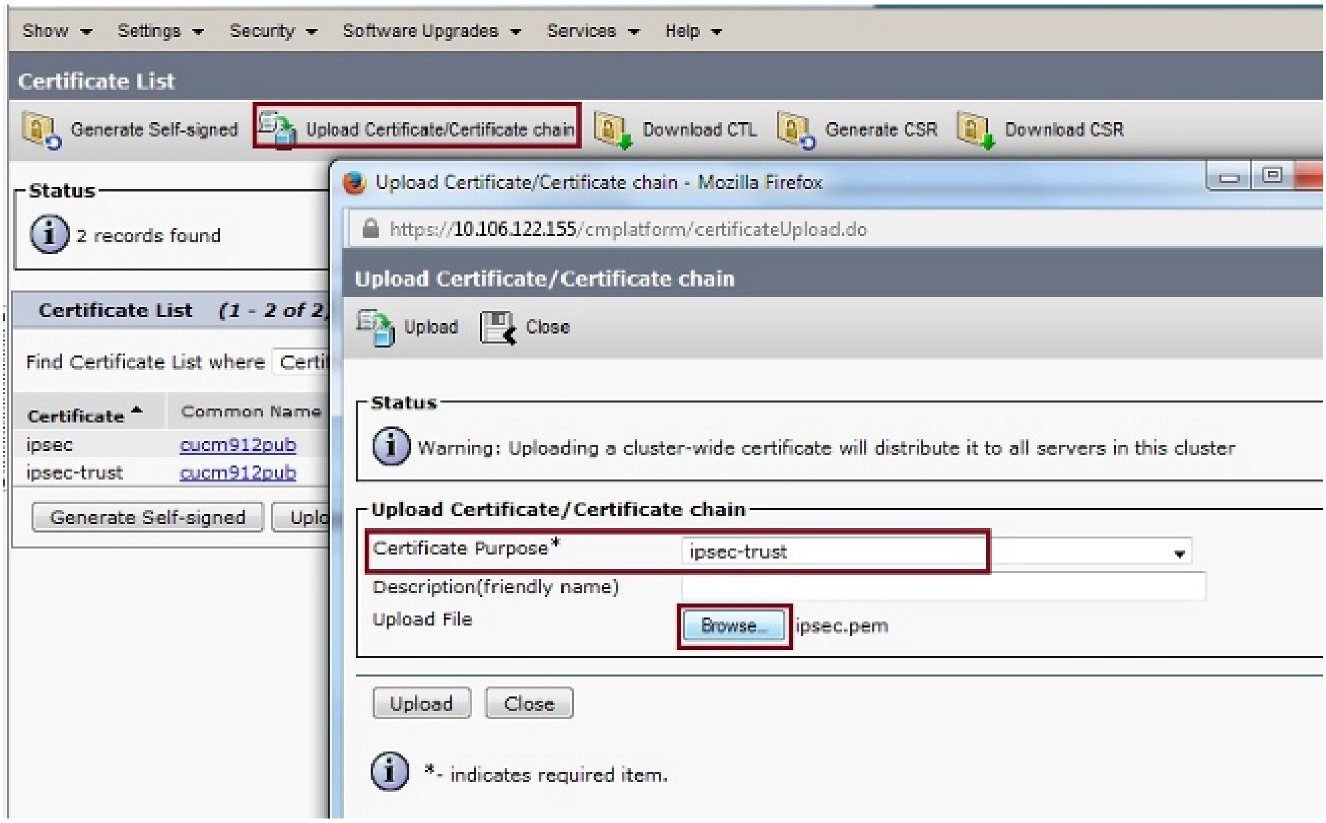
Certificate File Data

```
[
  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
  [
```

將IPsec根證書從訂閱伺服器上載到發佈伺服器

完成以下步驟，將IPsec根證書從訂閱伺服器節點上傳到發佈伺服器節點：

1. 登入到發佈伺服器節點的「作業系統管理」頁。
2. 導覽至**Security > Certificate Management**。
3. 點選**Upload Certificate/Certificate chain**，然後上傳使用者節點IPsec根證書作為**ipsec-trust**證書：



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

Generate Self-signed | Uplo

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

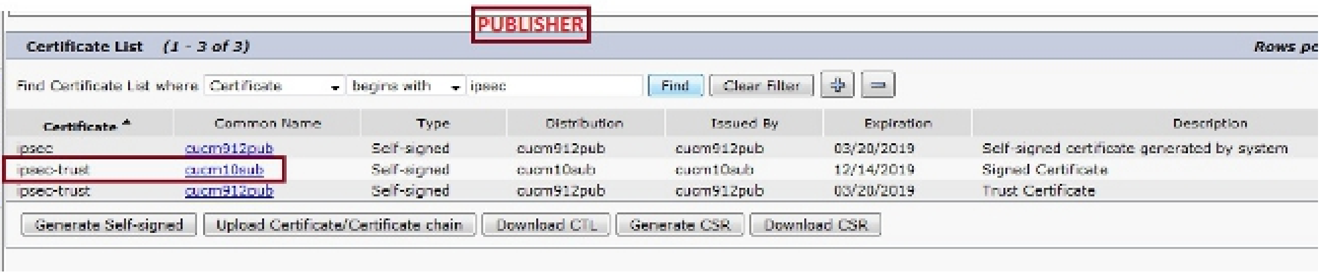
Description(friendly name):

Upload File: Browse... ipsec.pem

Upload | Close

*- indicates required item.

4. 上傳憑證後，確認訂閱者節點IPsec根憑證是否按以下方式顯示：



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

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

附註：如果需要啟用群集中多個節點之間的IPsec連線，則必須同時下載這些節點的IPsec根證書，並通過相同過程將其上傳到Publisher節點。

配置IPsec策略

完成以下步驟以配置IPsec策略：

1. 分別登入到發佈伺服器和訂閱伺服器節點的「作業系統管理」頁。

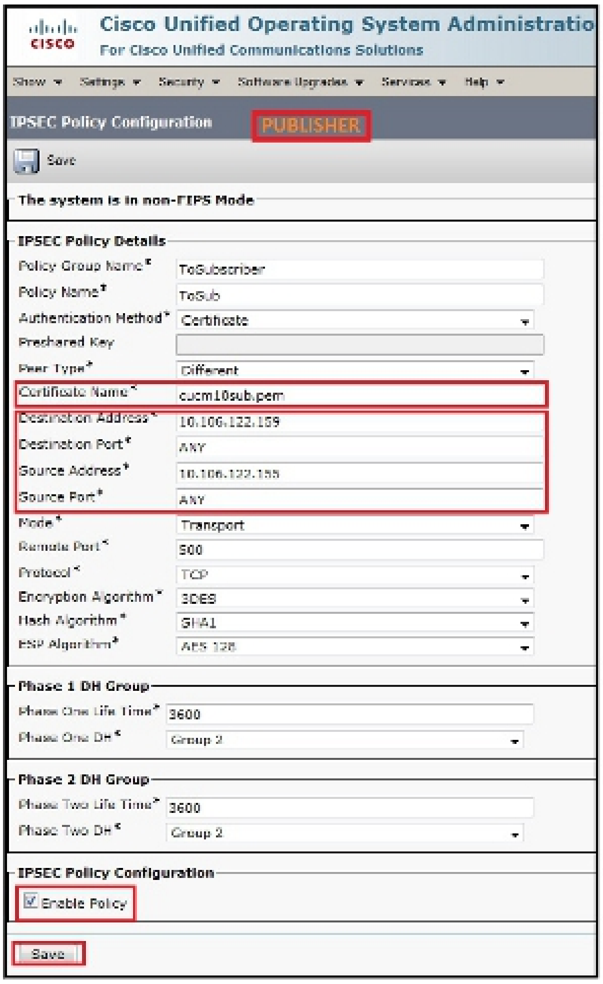
2. 導航到**Security > IPSEC Configuration**。

3. 使用以下資訊設定IP和憑證詳細資訊：

```
*****

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 ▾

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

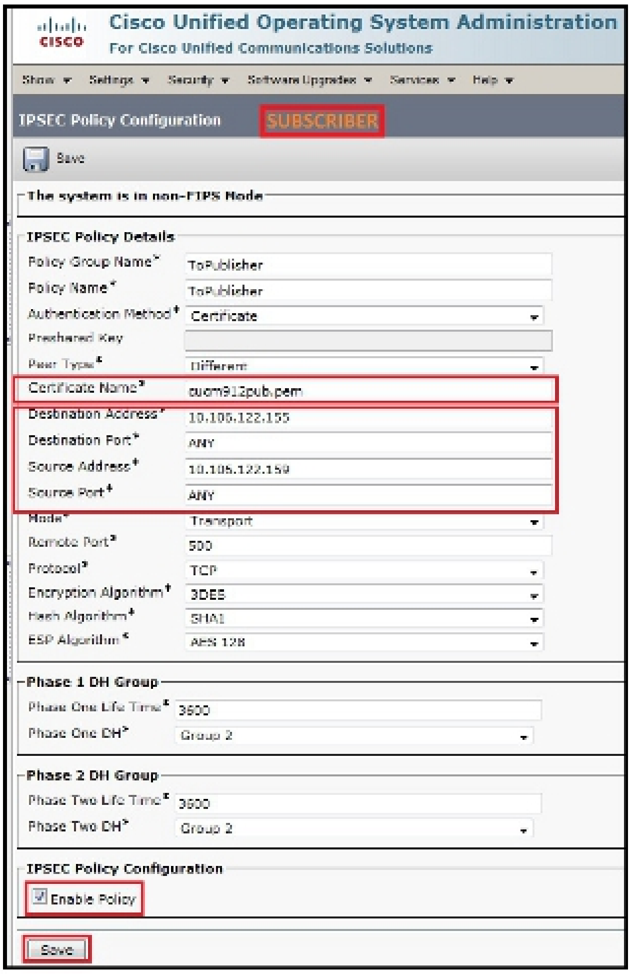
Phase 2 DH Group

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

驗證

完成以下步驟，驗證您的配置是否有效，以及節點之間是否建立了IPsec連線：

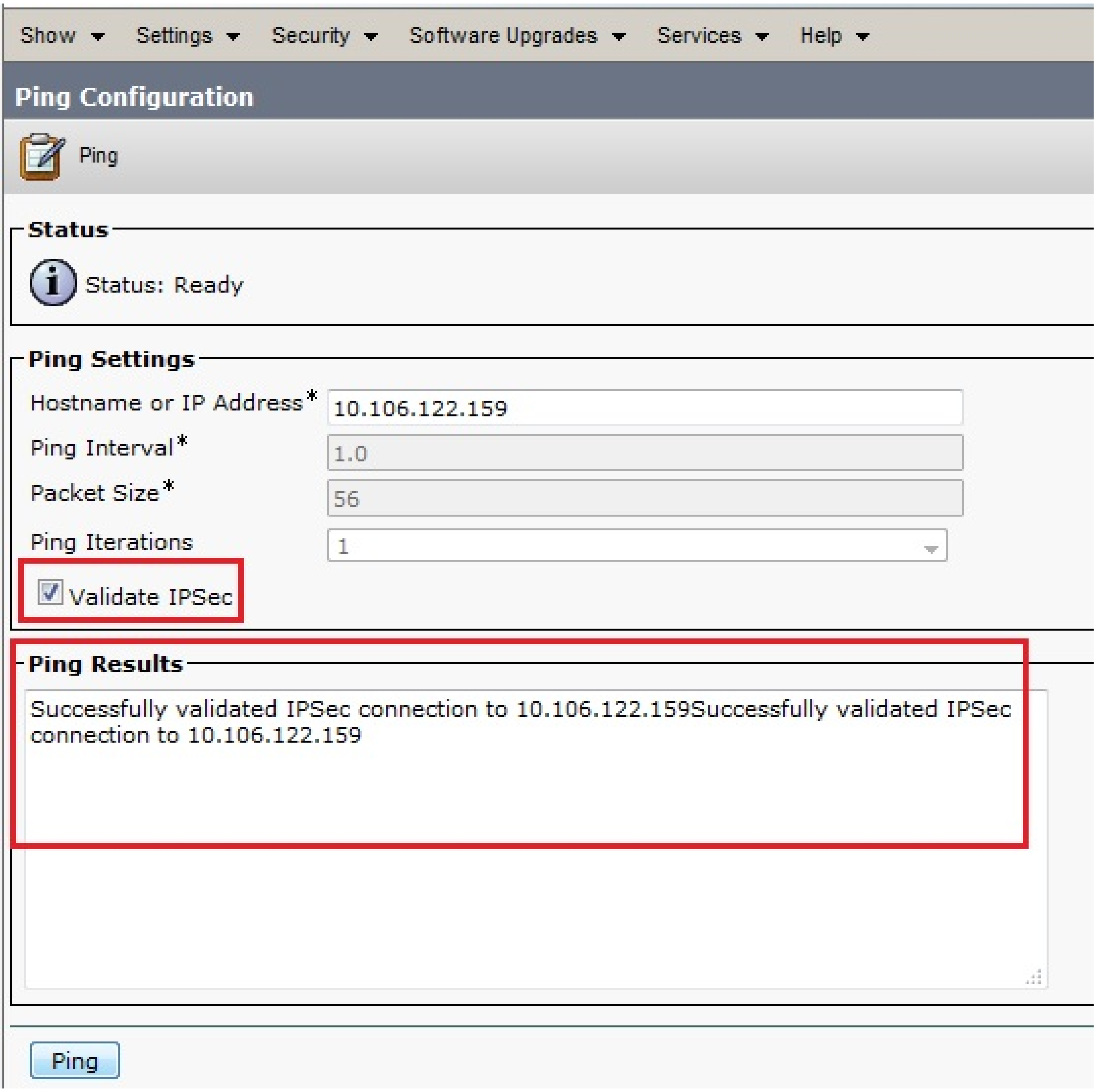
1. 登入到CUCM伺服器的作業系統管理。

2. 導覽至**Services > Ping**。

3. 指定遠端節點IP地址。

4. 選中**Validate IPsec**覈取方塊，然後按一下**Ping**。

如果已建立IPsec連線，則您會看到類似以下的訊息：



Ping Configuration

Ping

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

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 思科統一通訊作業系統管理指南8.6(1)版 — 設定新的IPsec策略
- 技術支援與文件 - Cisco Systems