配置CUCM和CUC之間的安全整合並排除故障

目錄

簡介

本檔案介紹Cisco Unified Communication Manager(CUCM)與Cisco Unity Connection(CUC)伺服器之間安全連線的配置、驗證和故障排除。

必要條件

需求

思科建議您瞭解CUCM。

有關詳細資訊，請參閱思科統一通訊管理器安全指南。

> **附註**：必須將其設定為混合模式，才能使安全整合正常工作。

必須為Unity Connection 11.5(1)SU3及更高版本啟用加密。

CLI命令「utils cuc encryption <enable/disable>」

採用元件

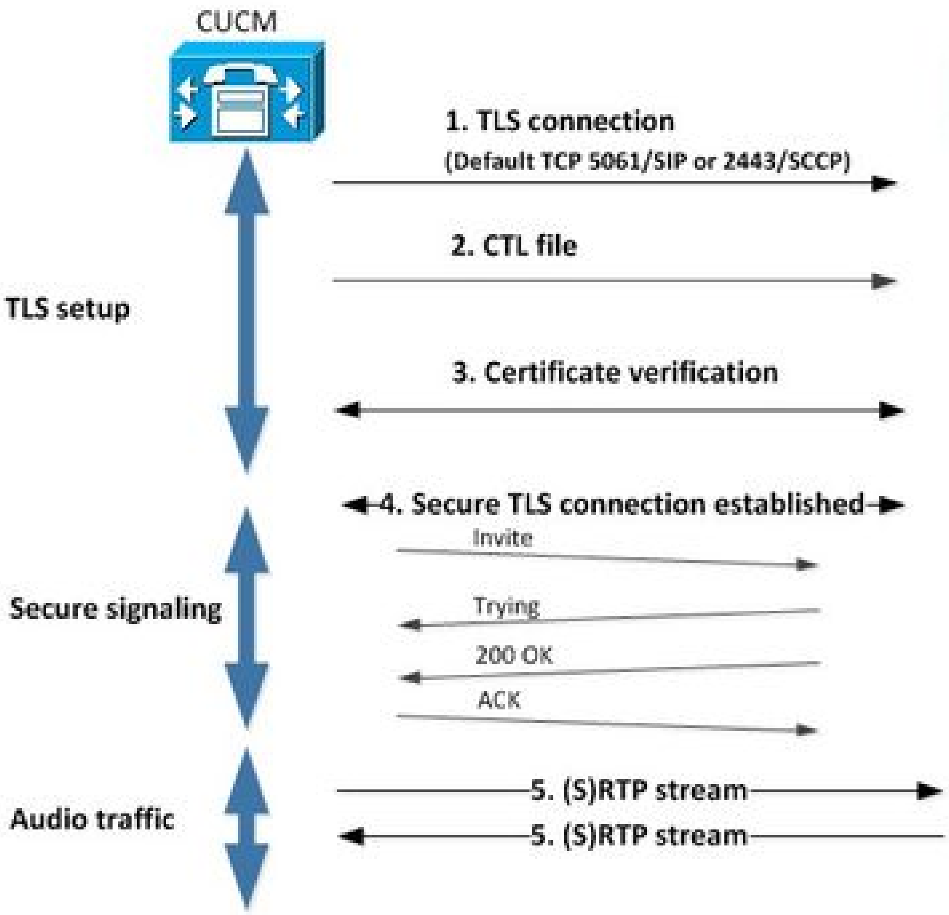
本文中的資訊係根據以下軟體和硬體版本：

- CUCM版本10.5.2.11900-3。
- CUC版本10.5.2.11900-3。

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。

圖表

此圖簡要說明了幫助在CUCM和CUC之間建立安全連線的過程：



1.呼叫管理器在用於整合的協定上，通過埠2443精簡型呼叫控制協定(SCCP)或基於5061會話初始協定(SIP)建立與CUC伺服器的安全傳輸層安全(TLS)連線。

2. CUC伺服器從TFTP伺服器下載證書信任清單(CTL)檔案（一次性進程），提取CallManager.pem證書並儲存它。

3. CUCM伺服器提供Callmanager.pem證書，該證書根據上一步獲得的CallManager.pem證書進行驗證。此外，正在根據CUCM中儲存的CUC根證書驗證CUC證書。請注意，根證書必須由管理員上傳到CUCM。

4.如果證書驗證成功，則建立安全的TLS連線。此連線用於交換加密的SCCP或SIP信令。

5.音訊流量可以交換為即時傳輸協定(RTP)或SRTP。

> **附註**：建立TLS通訊時，CUCM和CUC使用TLS相互驗證。如需詳細資訊，請參閱RFC5630。

配置 — 安全SIP中繼

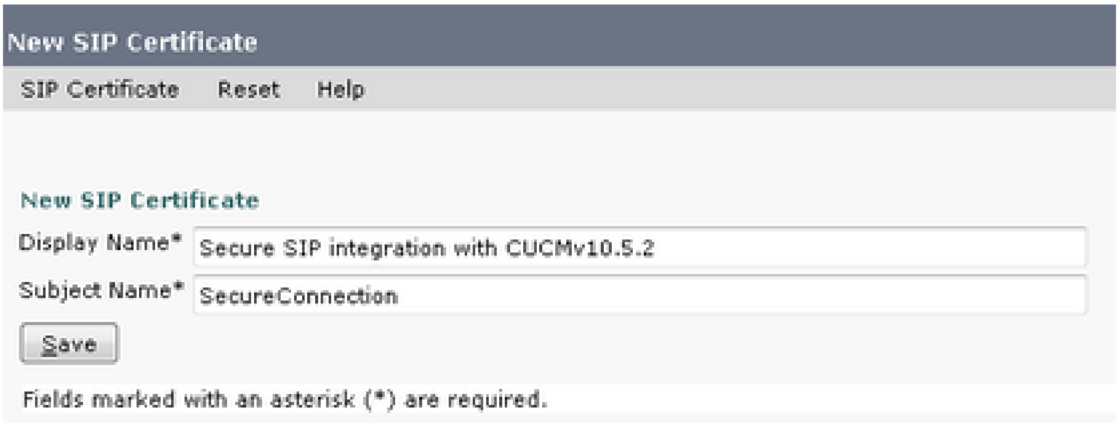
配置CUC

1.新增SIP證書

導覽至**CUC Administration > Telephony Integrations > Security > SIP Certificate > Add new**

- 顯示名稱：<任何有意義的名稱>
- 使用者名稱：<任意名稱，例如**SecureConnection**>

注意：主題名稱必須與SIP中繼安全配置檔案中的X.509主題名稱相匹配（本文檔後面的CUCM配置步驟1中進行了配置）。


New SIP Certificate

New SIP Certificate

Display Name* Secure SIP integration with CUCMv10.5.2

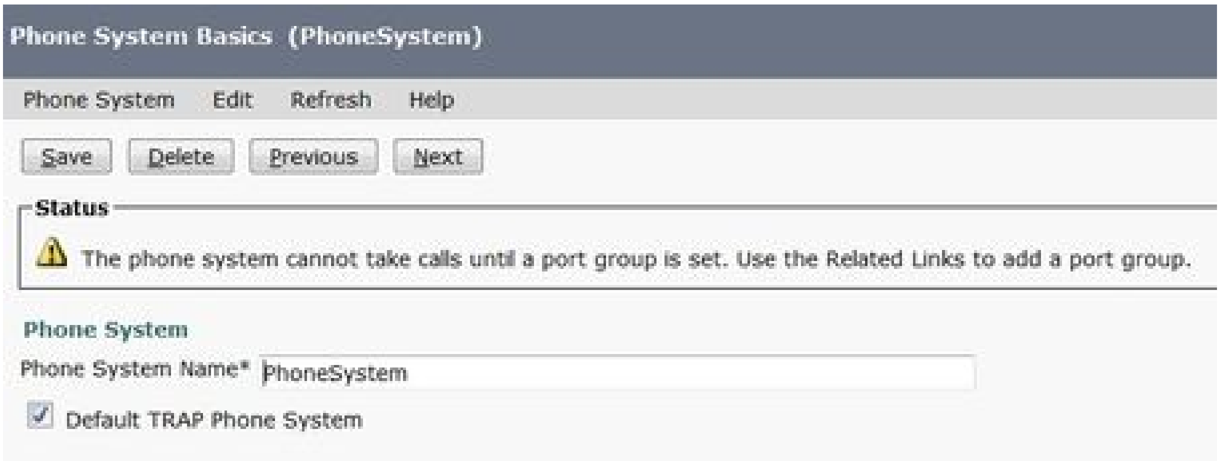
Subject Name* SecureConnection

Fields marked with an asterisk (*) are required.

附註：證書由CUC根證書生成並簽名。

2.建立新電話系統或修改預設電話系統

導覽至**Telephony Integration > Phone System**。您可以使用已經存在的電話系統或建立一個新系統。


Phone System Basics (PhoneSystem)

Status

⚠ The phone system cannot take calls until a port group is set. Use the Related Links to add a port group.

Phone System

Phone System Name* PhoneSystem

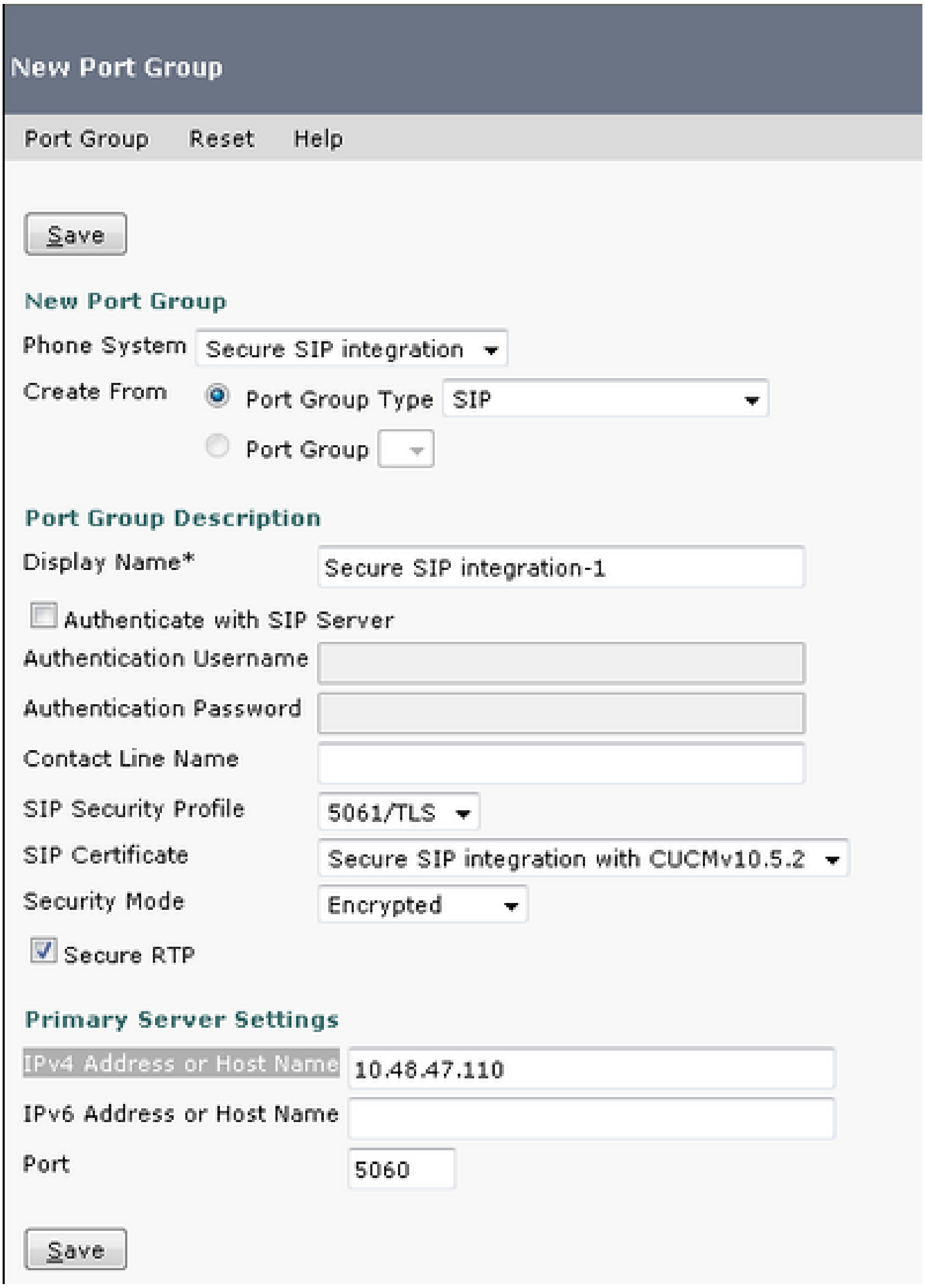
☑ Default TRAP Phone System

3.新增新埠組

在Phone System Basics頁面的Related Links下拉框中，選擇Add Port Group並選擇Go。在組態視窗中，輸入以下資訊：

- 電話系統：
- 建立源： 埠組型別SIP
- SIP安全配置檔案： 5061/TLS
- SIP證書：
- 安全模式： 已加密
- 安全RTP: 已檢查
- IPv4地址或主機名：

按儲存。



New Port Group

Phone System: Secure SIP integration

Create From: ● Port Group Type: SIP

○ Port Group

Port Group Description

Display Name*: Secure SIP integration-1

□ Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile: 5061/TLS

SIP Certificate: Secure SIP integration with CUCMv10.5.2

Security Mode: Encrypted

☑ Secure RTP

Primary Server Settings

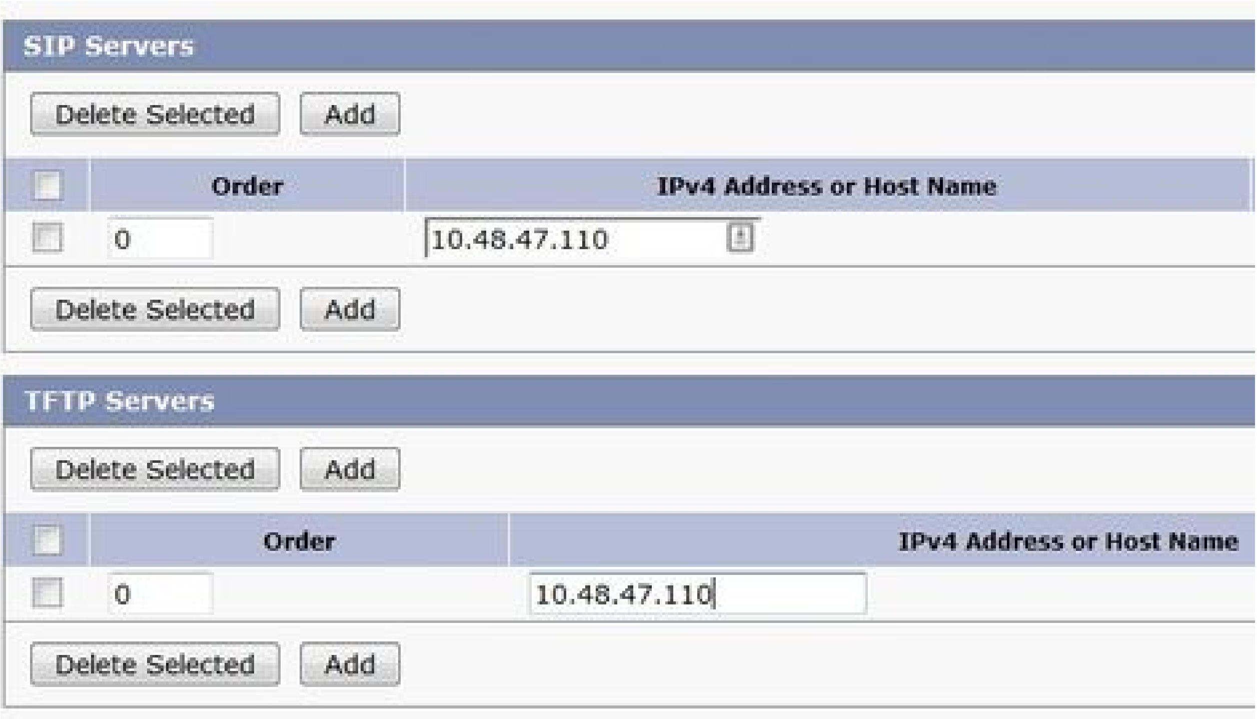
IPv4 Address or Host Name: 10.48.47.110

IPv6 Address or Host Name

Port: 5060

4.編輯伺服器

導覽至**Edit > Servers**，然後從CUCM群集中新增TFTP伺服器，如下圖所示。



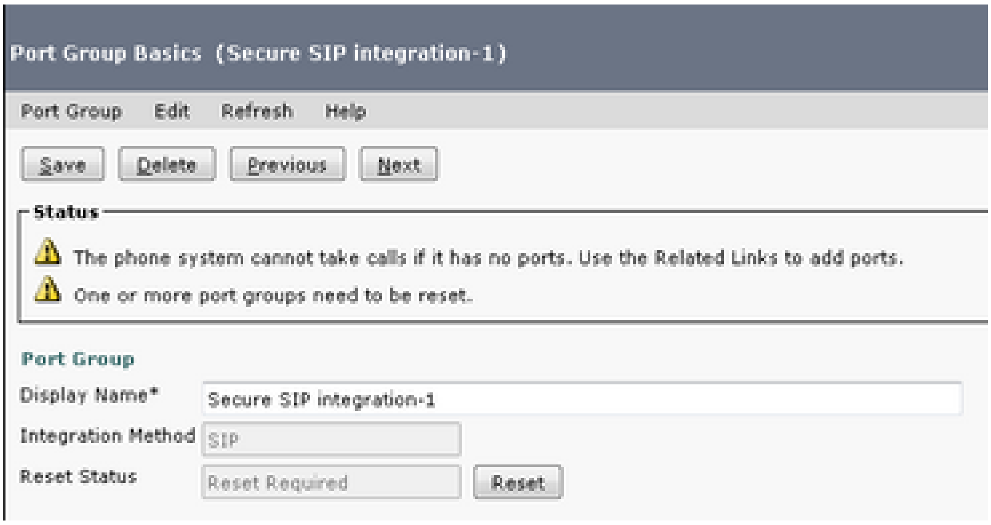
□	Order	IPv4 Address or Host Name
□	0	10.48.47.110

□	Order	IPv4 Address or Host Name
□	0	10.48.47.110

附註：提供正確的TFTP地址非常重要。CUC伺服器按說明從此TFTP下載CTL檔案。

5.重置埠組

按照系統提示返回**Port Group Basics**，重置埠組，如下圖所示。



Status

⚠ The phone system cannot take calls if it has no ports. Use the Related Links to add ports.

⚠ One or more port groups need to be reset.

Port Group

Display Name* Secure SIP integration-1

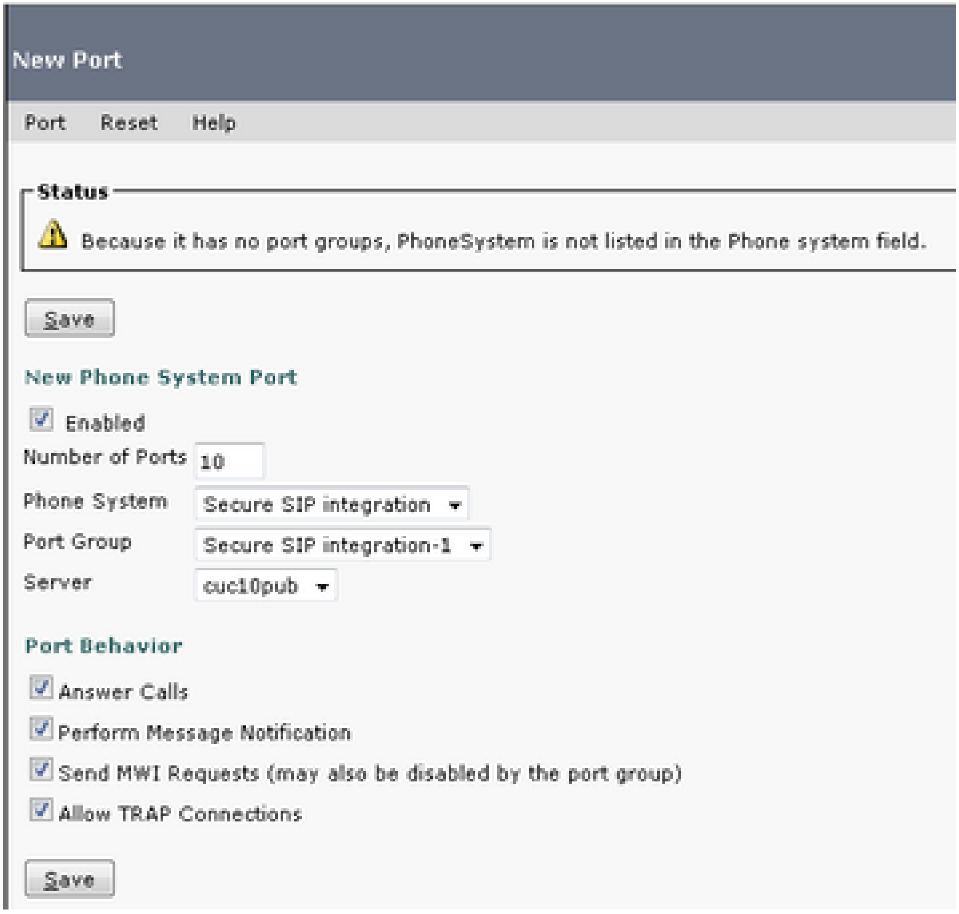
Integration Method SIP

Reset Status Reset Required

6.新增語音郵件埠

在「埠組基本資訊」頁的「相關連結」下拉框中，選擇**Add Ports**並選擇**Go**。在配置視窗中，輸入以下資訊：

- 已啟用:已檢查
- 連線埠數量：
- 電話系統：
- 埠組：
- 伺服器:
- 埠行為：



New Port

Port Reset Help

Status

⚠ Because it has no port groups, PhoneSystem is not listed in the Phone system field.

Save

New Phone System Port

☑ Enabled

Number of Ports: 10

Phone System: Secure SIP integration

Port Group: Secure SIP integration-1

Server: cuc10pub

Port Behavior

☑ Answer Calls

☑ Perform Message Notification

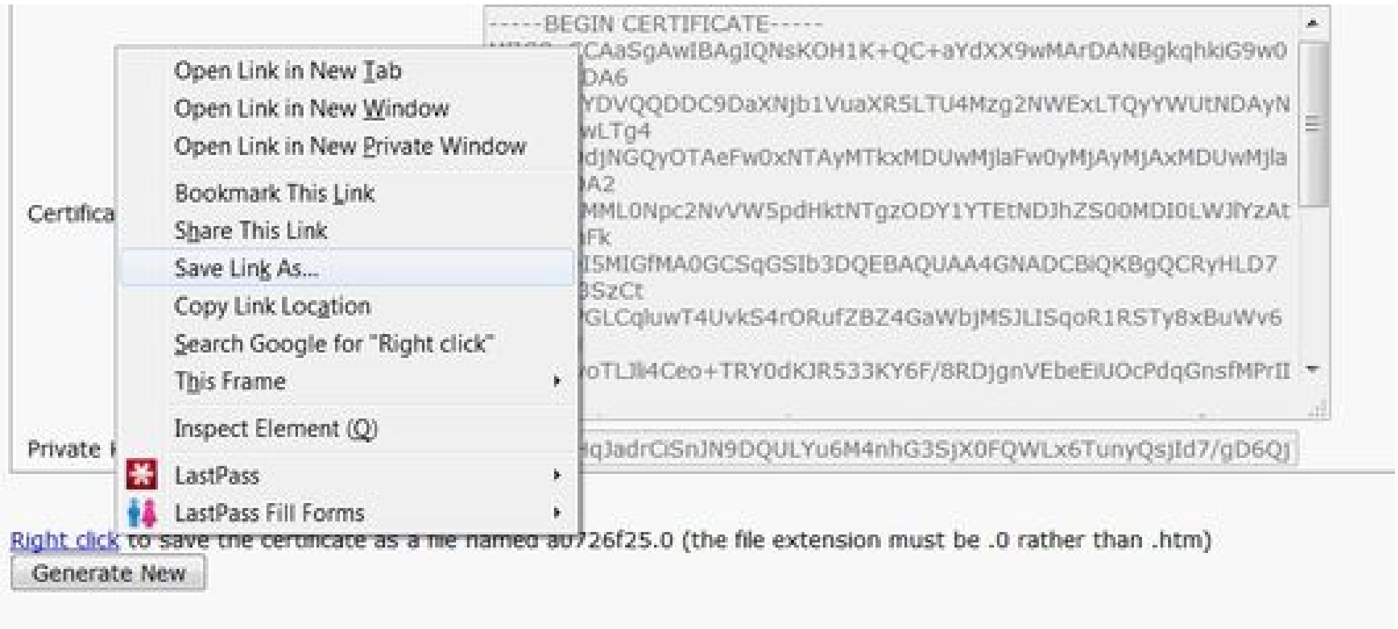
☑ Send MWI Requests (may also be disabled by the port group)

☑ Allow TRAP Connections

Save

7.下載CUC根證書

導覽至**Telephony Integrations > Security > Root Certificate**，按一下右鍵URL以將憑證儲存為名為<filename>.0（檔案副檔名必須是。0而不是.htm）'的檔案，然後按下save，如下圖所示。



Certifica

Private

```
-----BEGIN CERTIFICATE-----
CAaSgAwIBAgIQNsKOH1K+QC+aYdXX9wMArDANBgkqhkiG9w0
DA6
YDVQQDDC9DaXNjb1VuaXR5LTU4Mzg2NWExLTQyYWUtNDAyN
wLTg4
djNGQyOTAeFw0xNTAyMTkxMDUwMjlaFw0yMjAyMjAxMDUwMjla
A2
MML0Npc2NvVW5pdHktNTgzODY1YTEtNDJhZS00MDI0LWJlYzAt
Fk
I5MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCRyHLD7
SzCt
GLCqluwT4UvkS4rORufZBZ4GaWbjMSJLISqoR1RSTy8xBuWv6
oTLJl4Ceo+TRY0dKJR533KY6F/8RDjgnVEbeEiUOcPdqGnsfMPrII
```

qJadrCiSnJN9DQULYu6M4nhG3SjX0FQWLx6TunyQsjId7/gD6Qj

Right click to save the certificate as a file named a0726f25.0 (the file extension must be .0 rather than .htm)

Generate New

配置CUCM

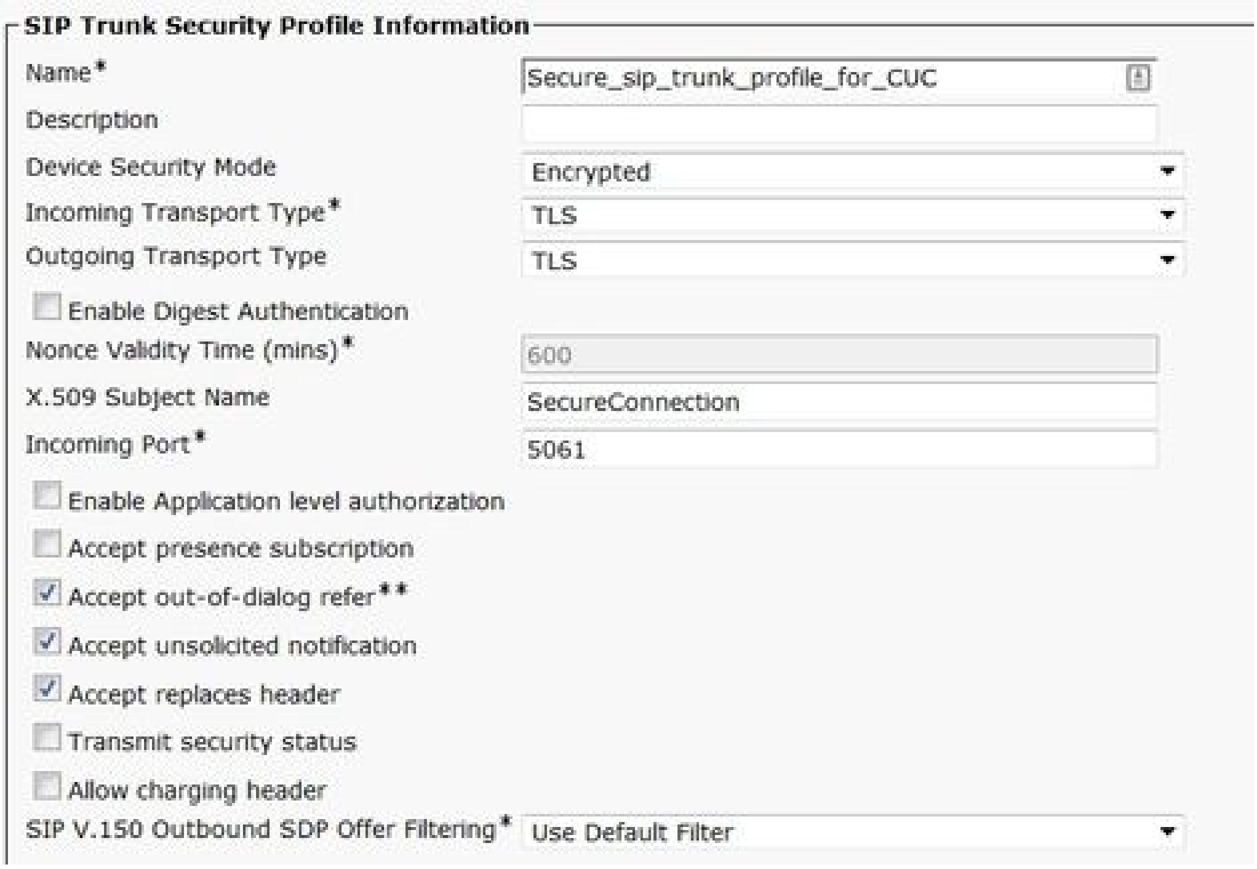
1.為指向CUC的中繼配置SIP中繼安全配置檔案

導航至**CUCM Administration > System > Security > SIP Trunk Security Profile > Add new**

確保正確填寫以下欄位：

- 裝置安全模式： 已加密
- X.509使用者名稱： SecureConnection>
- 接受對話之外的內容請參閱： 已檢查
- 接受未經請求的通知： 已檢查
- 接受替換報頭： 已檢查

附註：X.509使用者名稱必須與Cisco Unity Connection伺服器（在CUC配置步驟1中配置）上SIP證書中的Subject Name欄位匹配。



SIP Trunk Security Profile Information

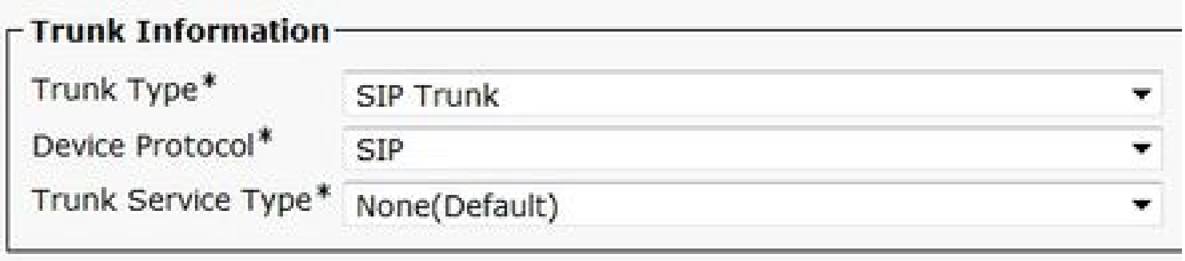
Name*	Secure_sip_trunk_profile_for_CUC
Description	
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	SecureConnection
Incoming Port*	5061
□ Enable Application level authorization	
□ Accept presence subscription	
☑ Accept out-of-dialog refer**	
☑ Accept unsolicited notification	
☑ Accept replaces header	
□ Transmit security status	
□ Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

2.配置SIP配置檔案

如果您需要應用任何特定設定，請導航到**Device > Device Settings > SIP Profile**。否則，您可以使用標準SIP配置檔案。

3.建立SIP中繼

轉至**Device > Trunk > Add new**。建立將用於與Unity Connection安全整合的SIP中繼，如下圖所示。



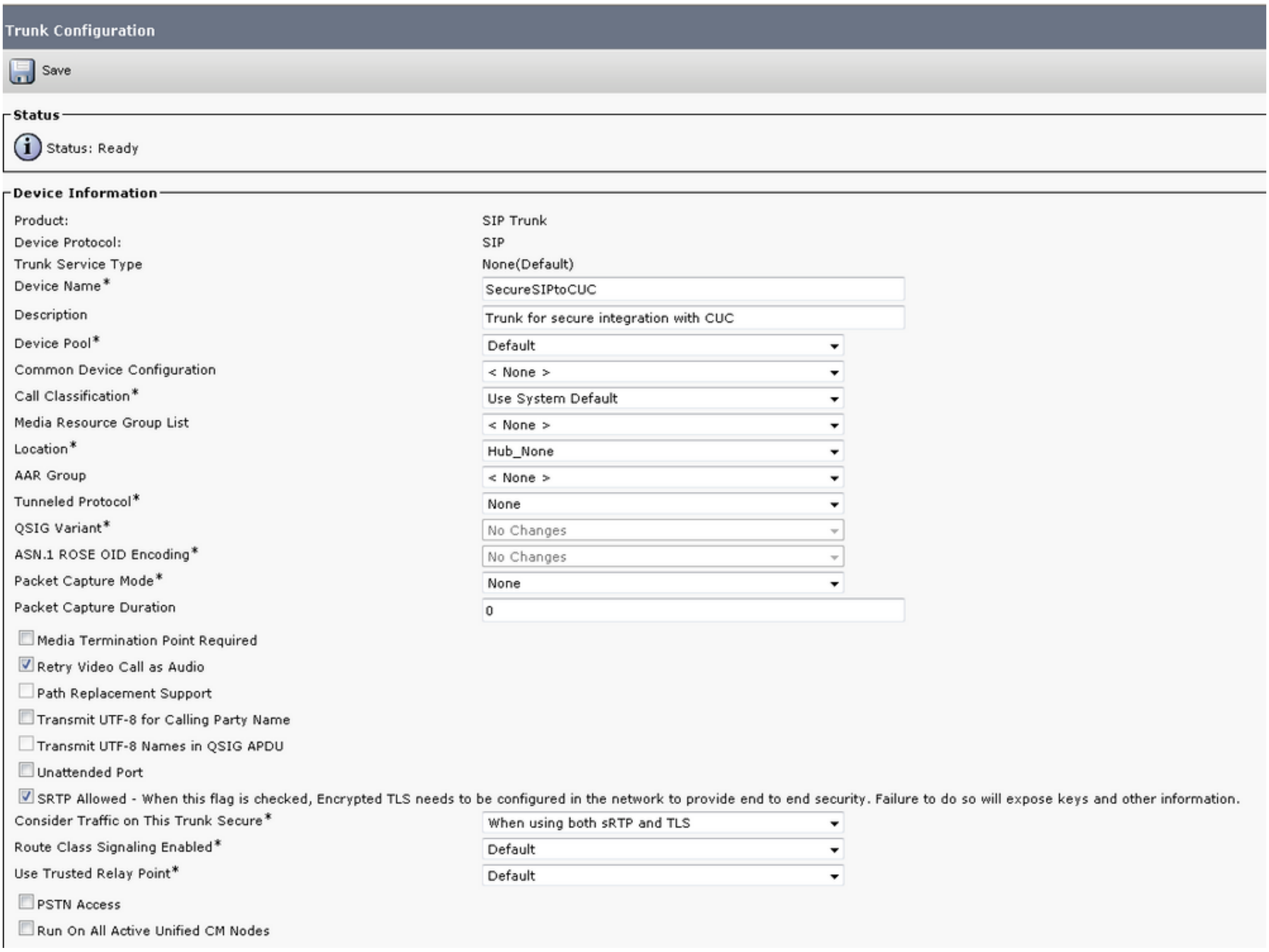
Trunk Information

Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

在Trunk配置的Device Information部分中，輸入以下資訊：

- 裝置名稱：
- 裝置池：
- 允許的SRTP:　　　已檢查

附註：確保CallManager組（在裝置池配置中）包含在CUC中配置的所有伺服器(**埠組>編輯>伺服器**)。



Trunk Configuration

Save

Status

Status: Ready

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	SecureSIPtoCUC
Description	Trunk for secure integration with CUC
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0

□ Media Termination Point Required

☑ Retry Video Call as Audio

□ Path Replacement Support

□ Transmit UTF-8 for Calling Party Name

□ Transmit UTF-8 Names in QSIG APDU

□ Unattended Port

☑ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

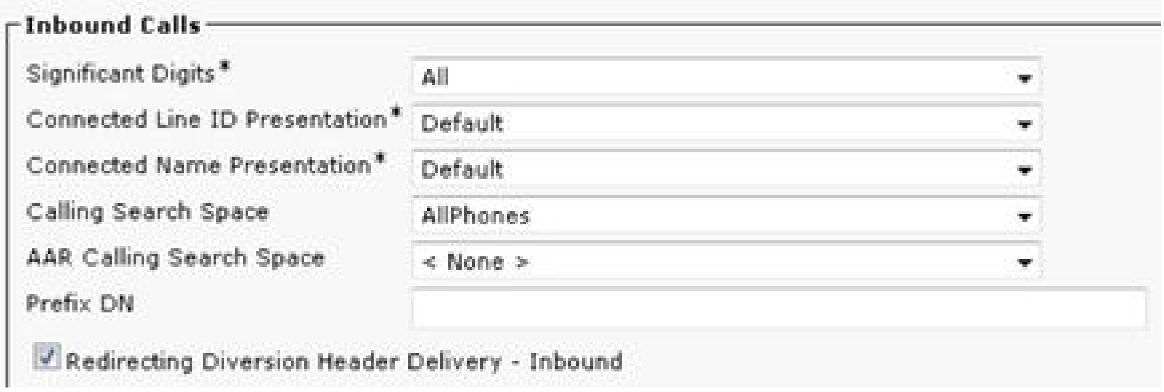
Consider Traffic on This Trunk Secure*	When using both sRTP and TLS
Route Class Signaling Enabled*	Default
Use Trusted Relay Point*	Default

□ PSTN Access

□ Run On All Active Unified CM Nodes

在TRUNK配置的Inbound Calls部分，輸入以下資訊：

- 呼叫搜尋空間：
- 重定向轉接轉接標頭傳送 — 傳入：　已檢查



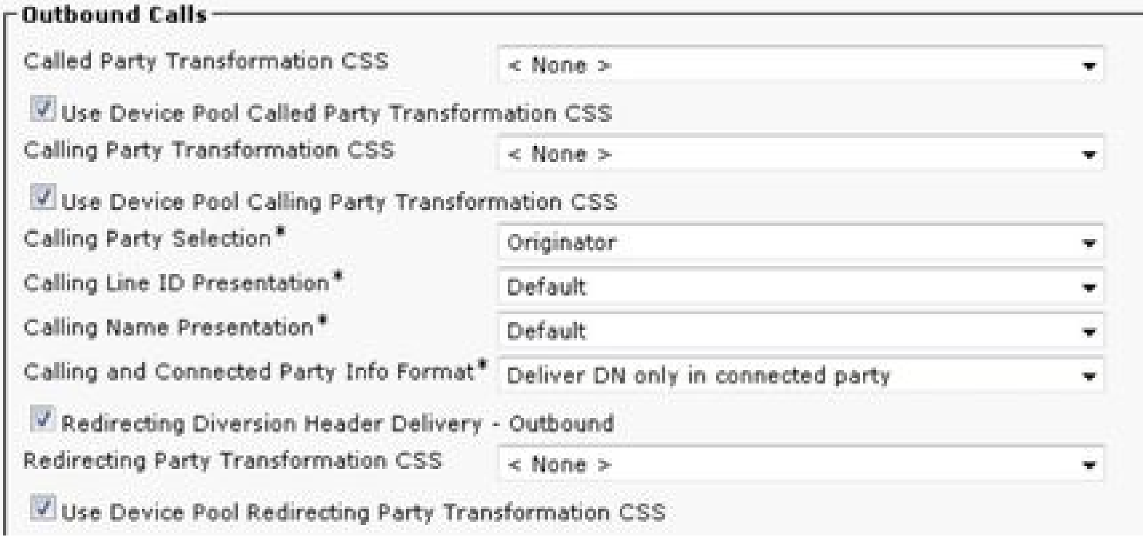
Inbound Calls

Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	AllPhones
AAR Calling Search Space	< None >
Prefix DN	

☑ Redirecting Diversion Header Delivery - Inbound

《外界》 Calls（呼叫）部分，輸入以下資訊：

- 重定向轉接轉接標頭傳送 — 出站：已檢查

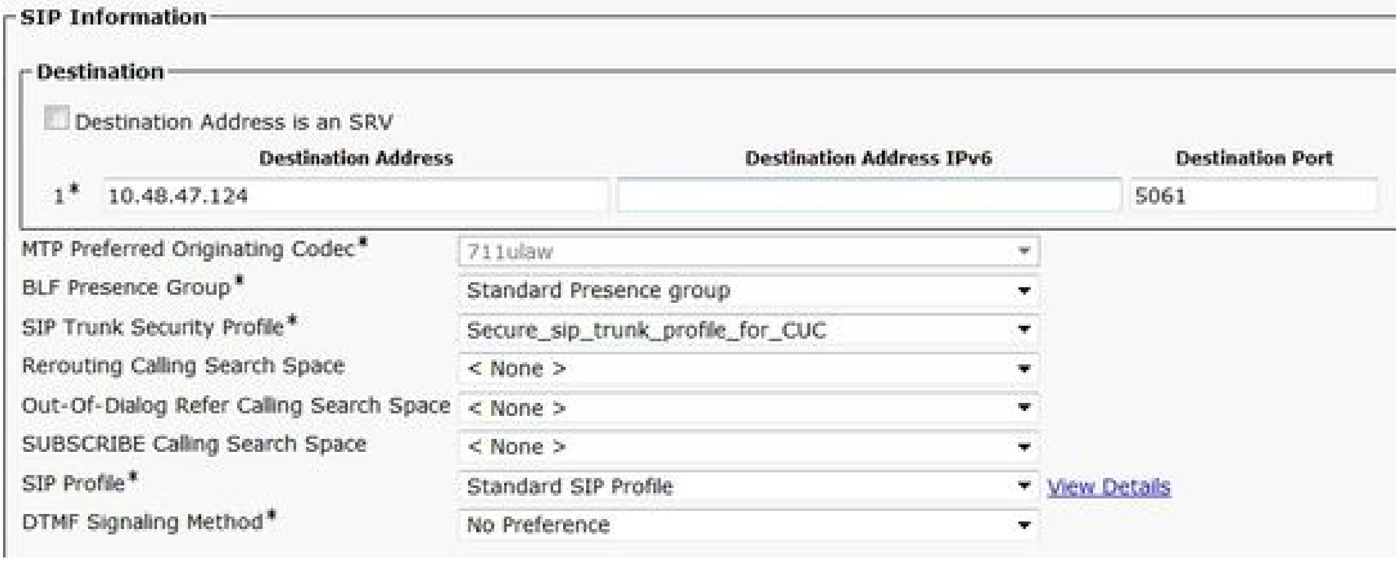


Outbound Calls

Called Party Transformation CSS	< None >
☑ Use Device Pool Called Party Transformation CSS	
Calling Party Transformation CSS	< None >
☑ Use Device Pool Calling Party Transformation CSS	
Calling Party Selection*	Originator
Calling Line ID Presentation*	Default
Calling Name Presentation*	Default
Calling and Connected Party Info Format*	Deliver DN only in connected party
☑ Redirecting Diversion Header Delivery - Outbound	
Redirecting Party Transformation CSS	< None >
☑ Use Device Pool Redirecting Party Transformation CSS	

在中繼配置的SIP資訊部分，輸入以下資訊：

- 目的地位址:
- SIP中繼安全配置檔案：
- 重新路由呼叫搜尋空間：
- 對話中斷引用呼叫搜尋空間：
- SIP配置檔案：



SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.48.47.124		5061

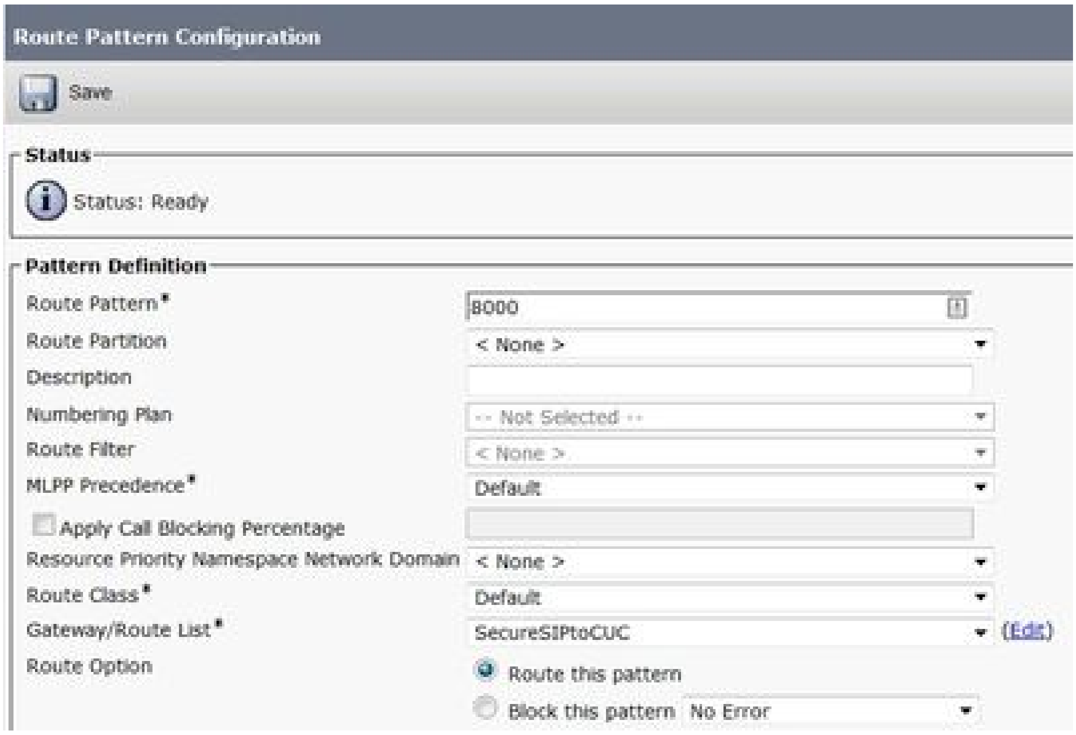
MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Secure_sip_trunk_profile_for_CUC
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	No Preference

根據您的要求調整其他設定。

4.建立路由模式

建立指向已配置中繼的路由模式(**Call Routing > Route/Hunt > Route Pattern**)。 作為路由模式編號輸入的分機可用作語音郵件引導。輸入以下資訊：

- 路由模式：
- 網關/路由清單：



Route Pattern Configuration

Save

Status

Status: Ready

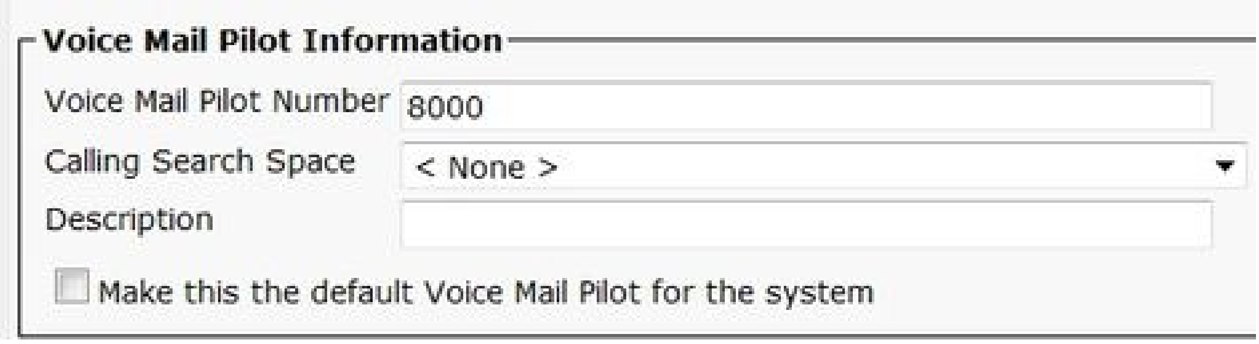
Pattern Definition

Route Pattern*	8000
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
□ Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	SecureSIPtoCUC (Edit)
Route Option	● Route this pattern ○ Block this pattern No Error

5.建立語音郵件引導

為整合建立語音郵件引導(**高級功能>語音郵件>語音郵件引導**)。 輸入以下值：

- 語音郵件引導號碼：
- 呼叫搜尋空間： 其中包括包含用作引導的路由模式的分割槽>



Voice Mail Pilot Information

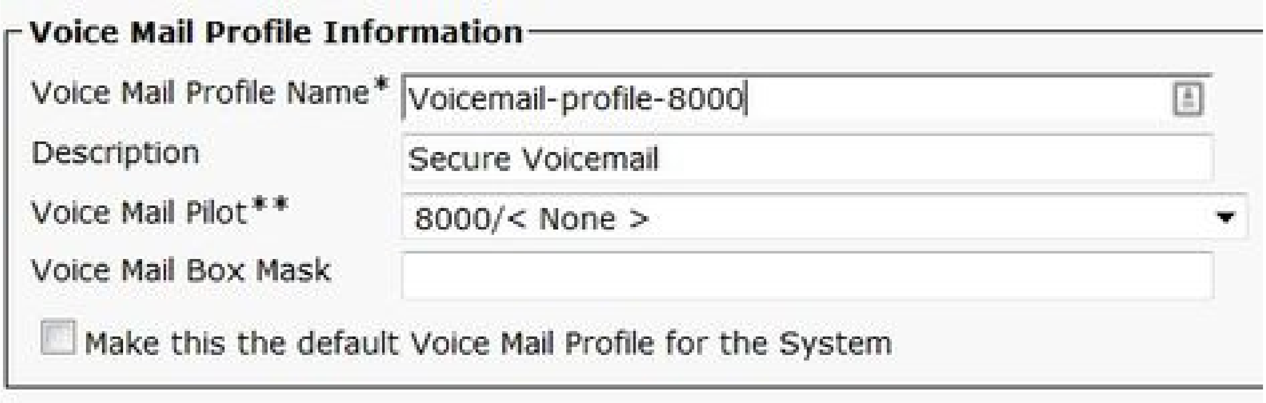
Voice Mail Pilot Number	8000
Calling Search Space	< None >
Description	

□ Make this the default Voice Mail Pilot for the system

6.建立語音郵件配置檔案

建立語音郵件配置檔案以將所有設定連結在一起(「**高級功能」>「語音郵件」>「語音郵件配置檔案**」)。 輸入以下資訊：

- 語音郵件引導：
- 語音信箱掩碼：



Voice Mail Profile Information

Voice Mail Profile Name*	Voicemail-profile-8000
Description	Secure Voicemail
Voice Mail Pilot**	8000/< None >
Voice Mail Box Mask	

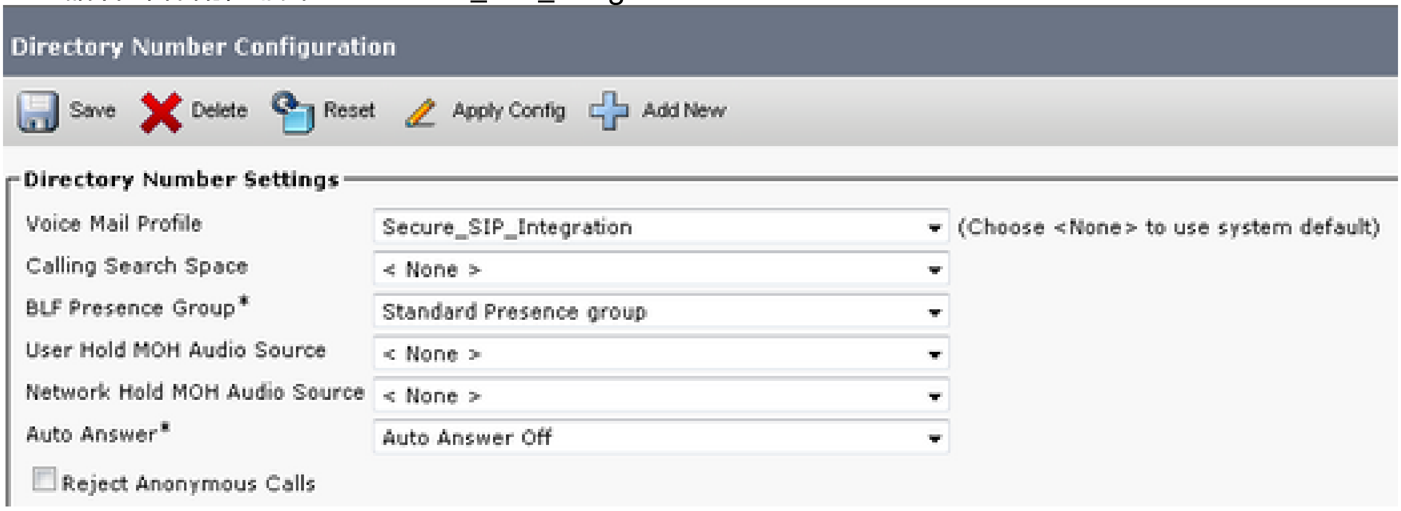
□ Make this the default Voice Mail Profile for the System

7.將語音郵件配置檔案分配給DN

將語音郵件配置檔案分配給使用安全整合的DN。更改DN設定後不要忘記按一下「Apply Config」按鈕：

導覽至：**呼叫Routing > Directory number並**更改以下內容：

- 語音郵件配置檔案： Secure_SIP_Integration



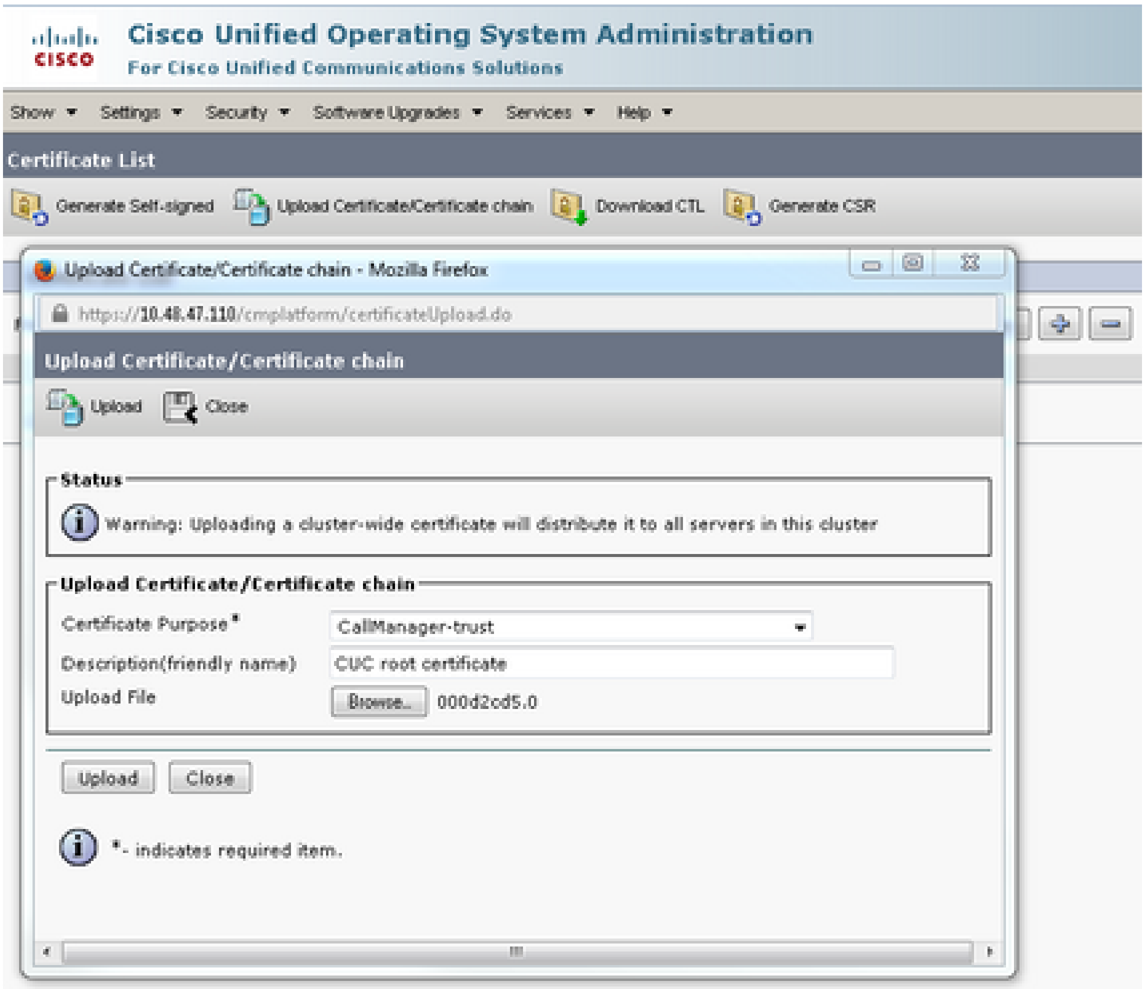
Directory Number Settings

Voice Mail Profile	Secure_SIP_Integration	(Choose <None> to use system default)
Calling Search Space	< None >	
BLF Presence Group*	Standard Presence group	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	
Auto Answer*	Auto Answer Off	

□ Reject Anonymous Calls

8.將CUC根證書上傳為CallManager-trust

導航到**OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain**，然後以**CallManager-trust**方式上傳所有配置為與CUC伺服器通訊的節點上的CUC根證書。


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Download CTL
Generate CSR
Upload Certificate/Certificate chain - Mozilla Firefox
http://10.48.47.110/cmplatform/certificateUpload.do
Upload Certificate/Certificate chain
Upload
Close
Browse...
Upload
Close

Status

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

Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust

Description(friendly name) CUC root certificate

Upload File 000d2cd5.0

*- indicates required item.

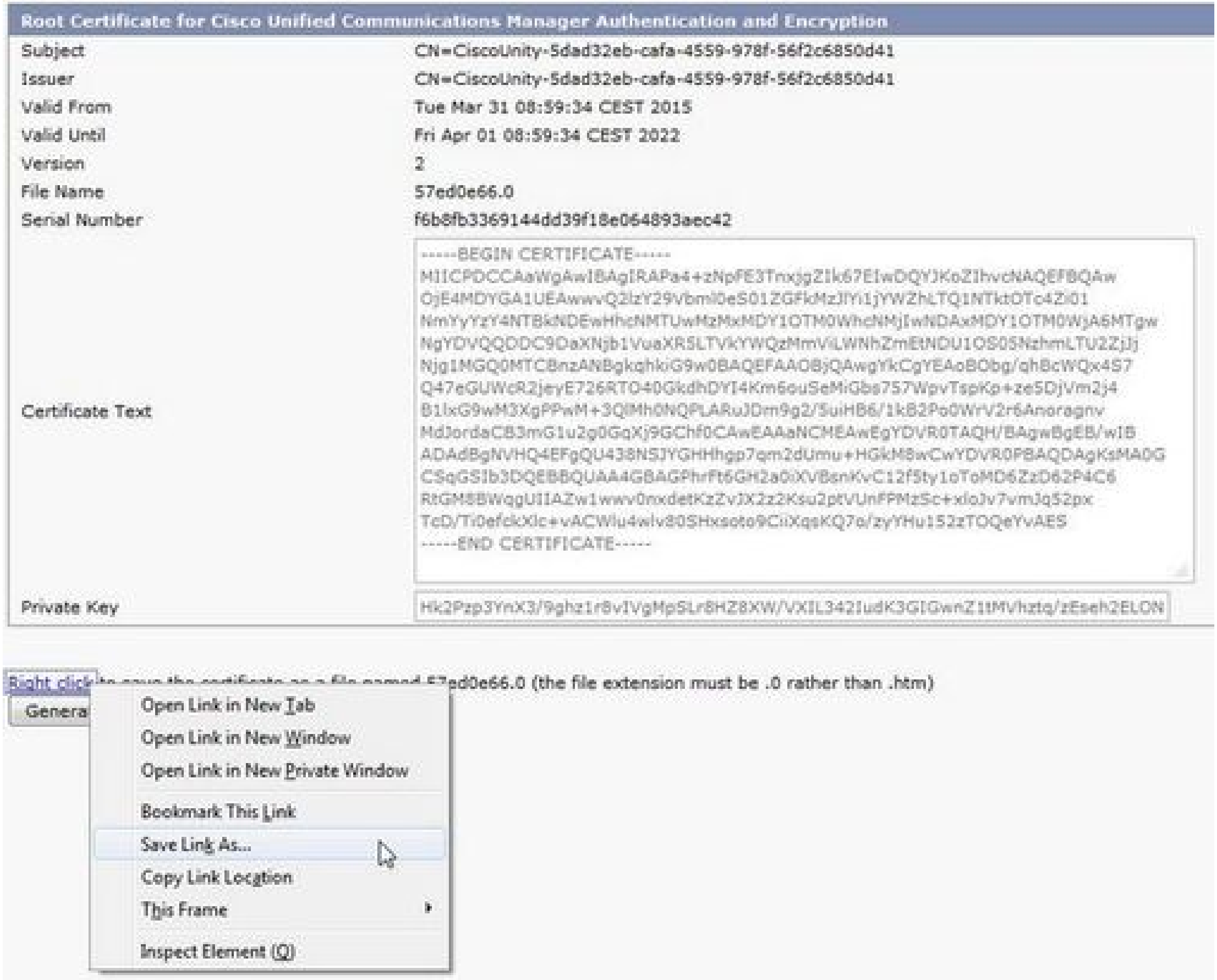
註意：上傳證書後，需要重新啟動Cisco CallManager服務以使證書生效。

配置安全SCCP埠

配置CUC

1.下載CUC根證書

導航到**CUC管理>電話整合>安全>根證書。按一下右鍵URL以將證書另存為名為<filename>.0（副檔名必須是。0而不是.htm）'的檔案，然後按下Save**:



Root Certificate for Cisco Unified Communications Manager Authentication and Encryption

Subject	CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41
Issuer	CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41
Valid From	Tue Mar 31 08:59:34 CEST 2015
Valid Until	Fri Apr 01 08:59:34 CEST 2022
Version	2
File Name	57ed0e66.0
Serial Number	f6b8fb3369144dd39f18e064893aec42

Certificate Text

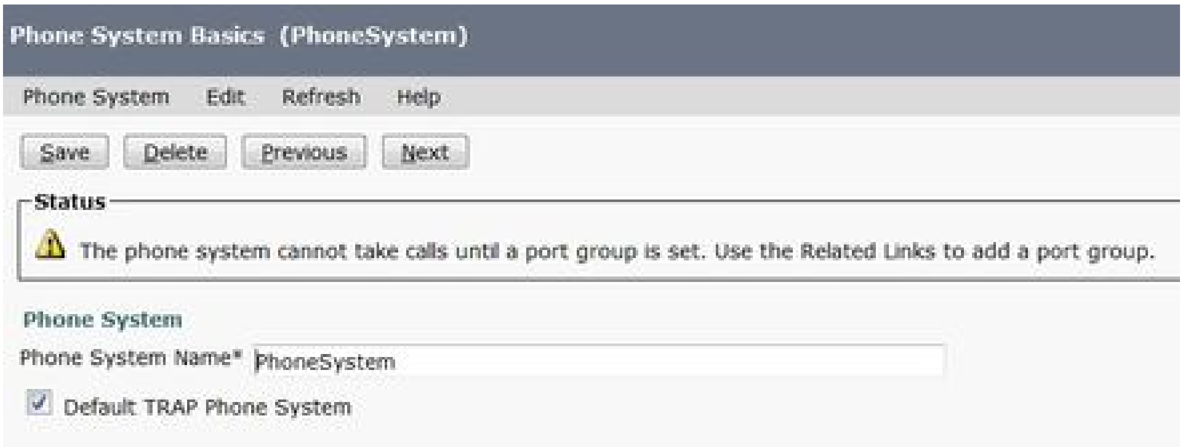
```
-----BEGIN CERTIFICATE-----
MIICPDCCAaWgAwIBAgIRAPa4+zNpFE3TnxjgZIk67EIwDQYJKoZIhvcNAQEFBQAw
OjE4MDYGA1UEAwwvQ2lzY29Vbml0eS01ZGFkMzJlYi1jYWZhLTQ1NTktOTc4Zi01
NmYyYzY4NTBkNDEwHhcNMTUwMzMxMDY1OTM0WhcNMjIwNDAxMDY1OTM0WjA6MTgw
NgYDVQQDDC9DaXNjb1VuaXR5LTVkYWQzMmViLWNhZmEtNDU1OS05NzhmLTU2ZjJj
Njg1MGQ0MTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoBObg/qhBcWQx4S7
Q47eGUWcR2jeyE726RTO40GkdhDYI4Km6ouSeMiGbs757WpvTspKp+ze5DjVm2j4
B1lxG9wM3XgPPwM+3QlMh0NQPLARuJDm9g2/5uiHB6/1kB2Po0WrV2r6Anoragnv
MdJordaCB3mG1u2g0GqXj9GChf0CAwEAAaNCMEAwEgYDVR0TAQH/BAgwBgEB/wIB
ADAdBgNVHQ4EFgQU438NSJYGHHhgp7qm2dUmu+HGkM8wCwYDVR0PBAQDAgKsMA0G
CSqGSIb3DQEBBQUAA4GBAGPhrFt6GH2a0iXVBsnKvC12f5ty1oToMD6ZzD62P4C6
RtGM8BWqgUIIAZw1wwv0nxdetKzZvJX2z2Ksu2ptVUnFPMzSc+xloJv7vmJq52px
TcD/Ti0efckXlc+vACWlu4wlv80SHxsoto9CiXqsKQ7o/zyYHu152zTOQeYvAES
-----END CERTIFICATE-----
```

Private Key Hk2Pzp3YnX3/9ghz1r8vIVgMpSLr8HZ8XW/VXIL342IudK3GIGwnZ1tMVhztq/zEseh2ELON

Right click to save the certificate as a file named 57ed0e66.0 (the file extension must be .0 rather than .htm)

2.建立電話系統/修改現有的電話系統。

導航到**電話整合>電話**系統。您可以使用已經存在的電話系統或建立一個新系統。



Phone System Basics (PhoneSystem)

Status

⚠ The phone system cannot take calls until a port group is set. Use the Related Links to add a port group.

Phone System

Phone System Name* PhoneSystem

☑ Default TRAP Phone System

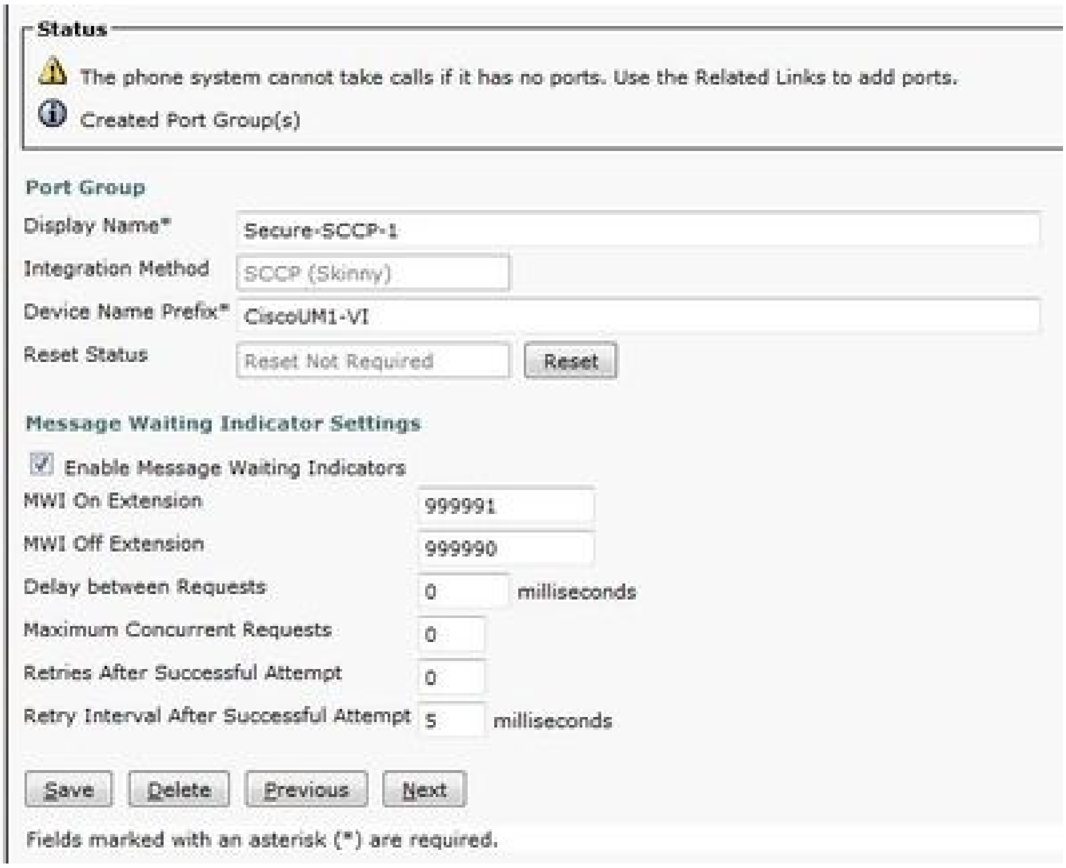
3.新增新的SCCP埠組

在Phone System Basics頁面的Related Links下拉框中，選擇**Add Port Group**並選擇**Go**。在組態視窗中，輸入以下資訊：

- 電話系統：

- 埠組型別：　　　SCCP
- 裝置名稱字首*:　CiscoUM1-VI
- MWI On分機：
- MWI關閉分機：

附註：此配置必須與CUCM上的配置匹配。



Status

⚠ The phone system cannot take calls if it has no ports. Use the Related Links to add ports.

ⓘ Created Port Group(s)

Port Group

Display Name*	Secure-SCCP-1
Integration Method	SCCP (Skinny)
Device Name Prefix*	CiscoUM1-VI
Reset Status	Reset Not Required

Message Waiting Indicator Settings

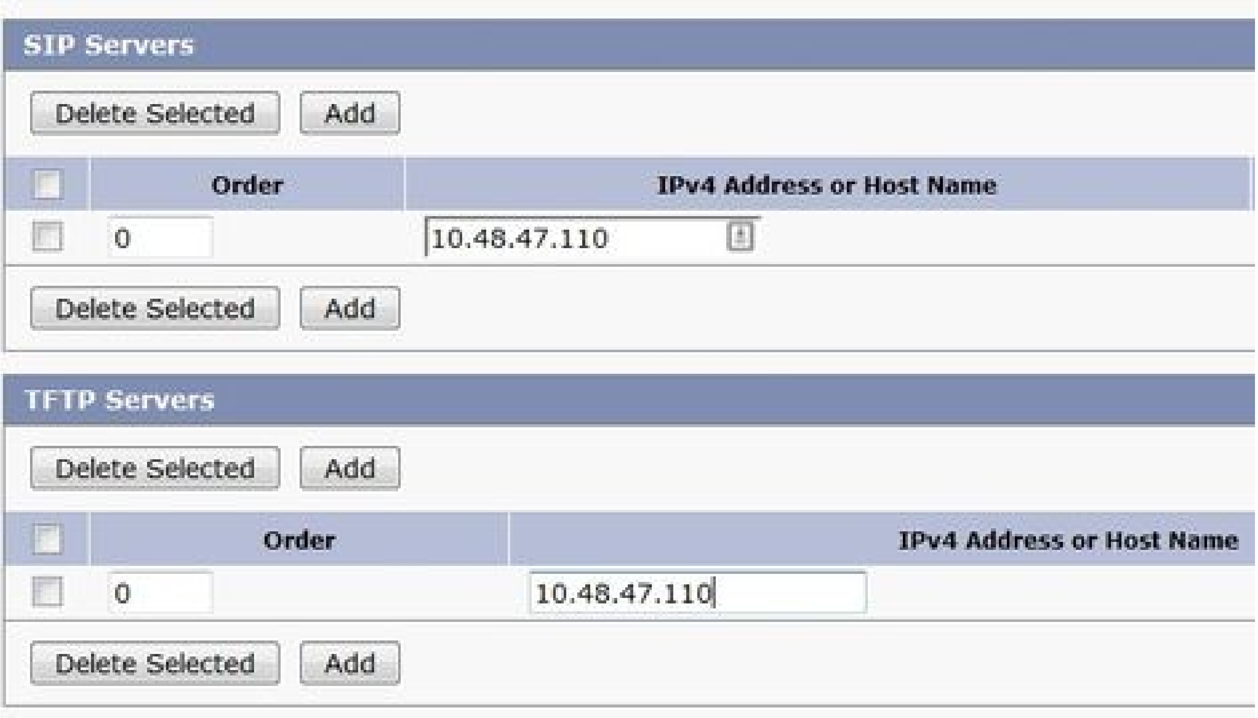
☑ Enable Message Waiting Indicators

MWI On Extension	999991
MWI Off Extension	999990
Delay between Requests	0 milliseconds
Maximum Concurrent Requests	0
Retries After Successful Attempt	0
Retry Interval After Successful Attempt	5 milliseconds

Fields marked with an asterisk (*) are required.

4.編輯伺服器

導航到**Edit > Servers**，然後從CUCM群集新增TFTP伺服器。



SIP Servers

□	Order	IPv4 Address or Host Name
□	0	10.48.47.110

TFTP Servers

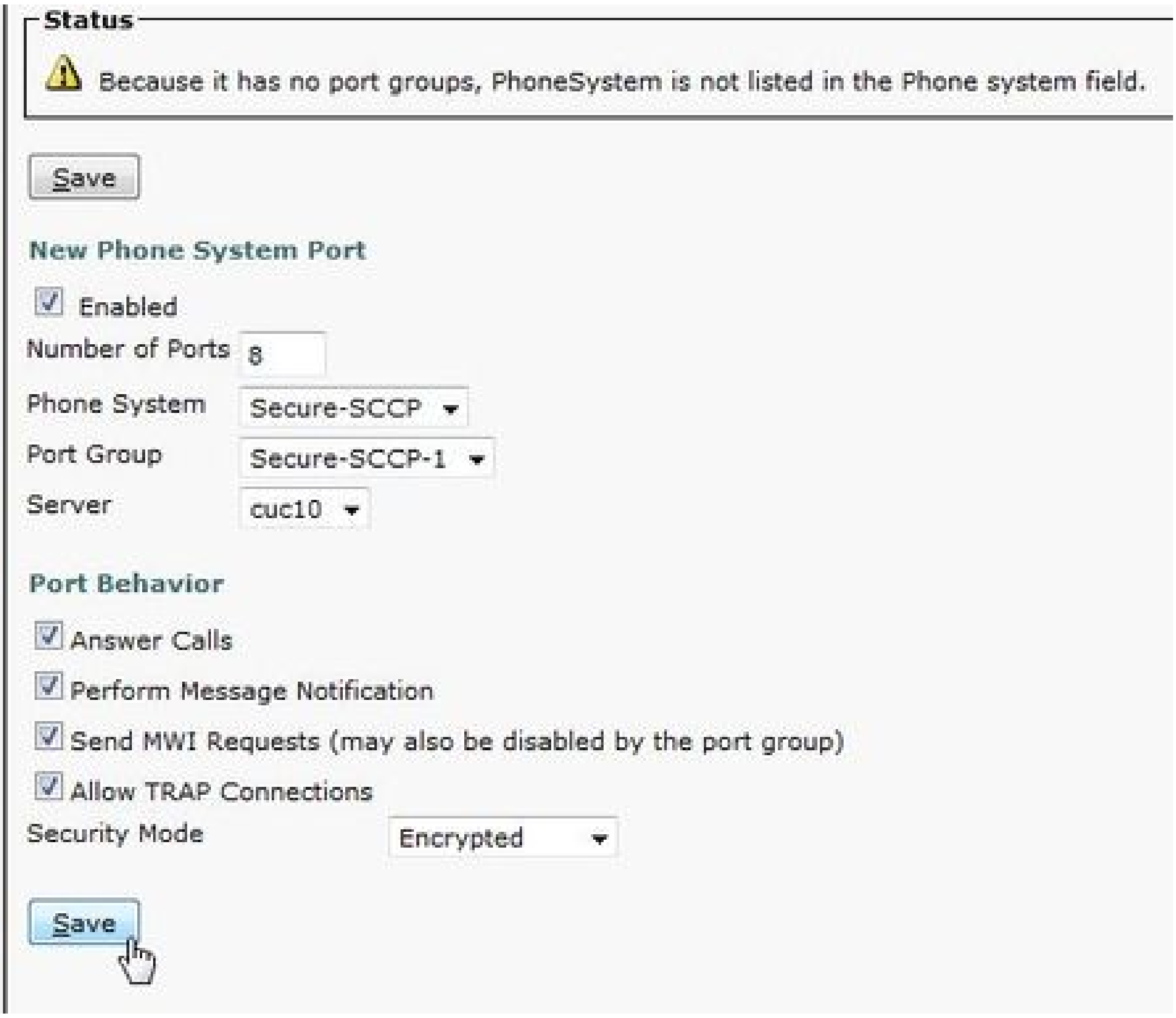
□	Order	IPv4 Address or Host Name
□	0	10.48.47.110

附註：提供正確的TFTP地址非常重要。CUC伺服器按說明從此TFTP下載CTL檔案。

5.新增安全SCCP埠

在「埠組基本資訊」頁的「相關連結」下拉框中，選擇**Add Ports**，然後選擇**Go**。在配置視窗中，輸入以下資訊：

- 已啟用:已檢查
- 連線埠數量：
- 電話系統：
- 埠組：
- 伺服器:
- 埠行為：
- 安全模式：　　**已加密**



Status

⚠ Because it has no port groups, PhoneSystem is not listed in the Phone system field.

New Phone System Port

☑ Enabled

Number of Ports 8

Phone System Secure-SCCP

Port Group Secure-SCCP-1

Server cuc10

Port Behavior

☑ Answer Calls

☑ Perform Message Notification

☑ Send MWI Requests (may also be disabled by the port group)

☑ Allow TRAP Connections

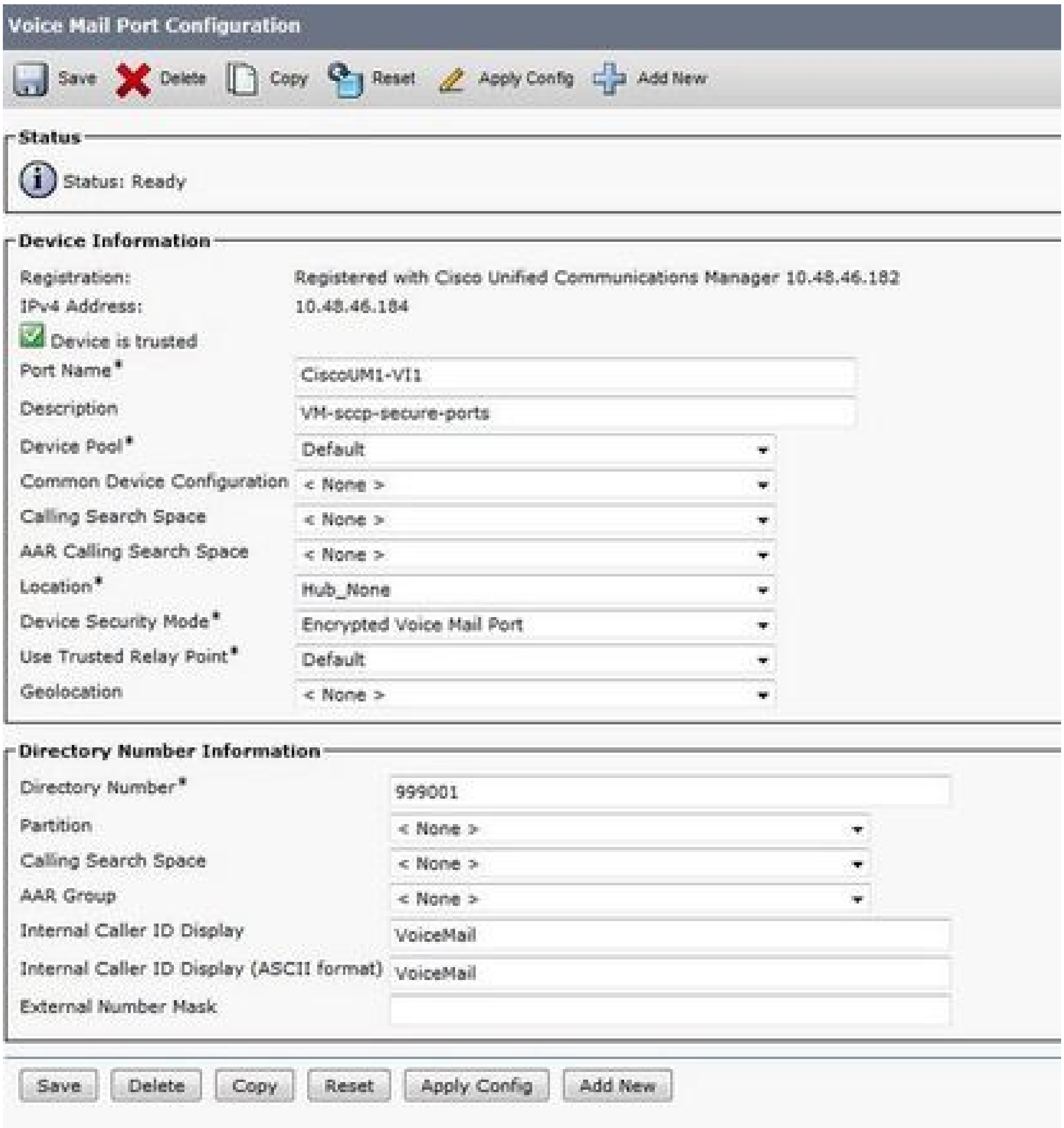
Security Mode Encrypted

配置CUCM

1.新增埠

導航至 **CUCM管理>高級功能>語音郵件埠配置>新增新。**

照常配置SCCP語音郵件埠。唯一的區別是裝置安全模式下的埠配置需要選擇Encrypted Voice Mail Port選項。



Status

Status: Ready

Device Information

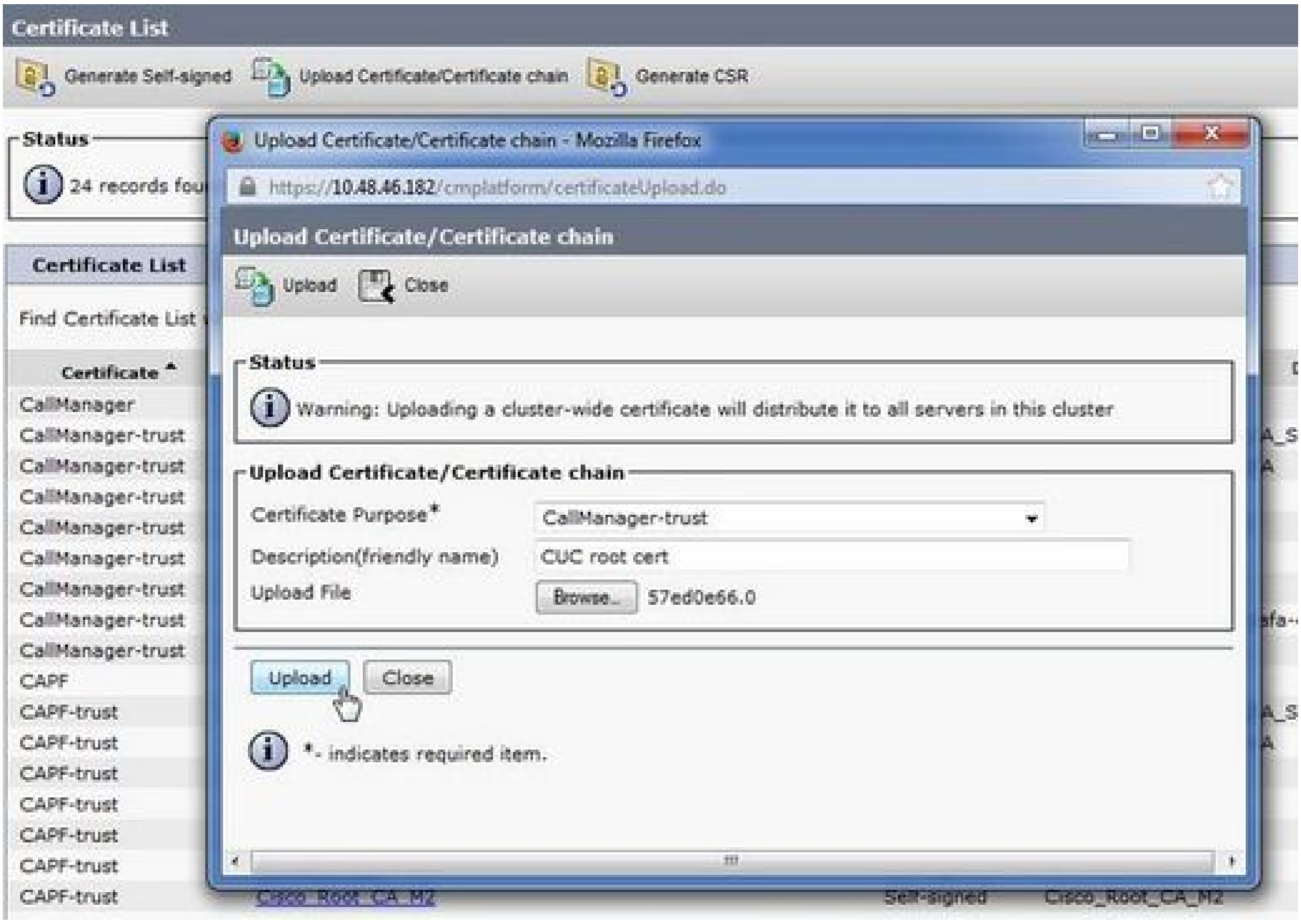
Registration:	Registered with Cisco Unified Communications Manager 10.48.46.182
IPv4 Address:	10.48.46.184
☑ Device is trusted	
Port Name*	CiscoUM1-VI1
Description	VM-sccp-secure-ports
Device Pool*	Default
Common Device Configuration	< None >
Calling Search Space	< None >
AAR Calling Search Space	< None >
Location*	Hub_None
Device Security Mode*	Encrypted Voice Mail Port
Use Trusted Relay Point*	Default
Geolocation	< None >

Directory Number Information

Directory Number*	999001
Partition	< None >
Calling Search Space	< None >
AAR Group	< None >
Internal Caller ID Display	VoiceMail
Internal Caller ID Display (ASCII format)	VoiceMail
External Number Mask	

2.將CUC根證書上傳為CallManager-trust

導航到OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain，然後以CallManager-trust在配置為與CUC伺服器通訊的所有節點上上上傳CUC根證書。


Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Upload Certificate/Certificate chain - Mozilla Firefox
https://10.48.46.182/cmplatform/certificateUpload.do
Upload
Close
Browse...
Upload
Close

Status

24 records fou

Certificate List

Find Certificate List

Certificate ▲
CallManager
CallManager-trust
CallManager-trust
CallManager-trust
CallManager-trust
CallManager-trust
CallManager-trust
CallManager-trust
CallManager-trust
CAPF
CAPF-trust
CAPF-trust
CAPF-trust
CAPF-trust
CAPF-trust
CAPF-trust
CAPF-trust

Cisco_Root_CA_M2 Self-signed Cisco_Root_CA_M2

Upload Certificate/Certificate chain

Status

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

Upload Certificate/Certificate chain

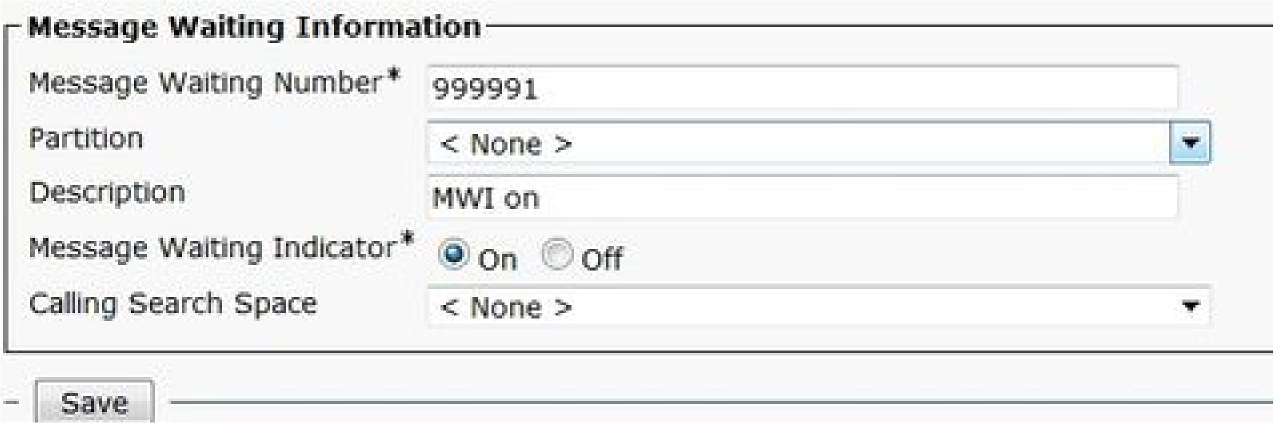
Certificate Purpose*	CallManager-trust
Description(friendly name)	CUC root cert
Upload File	57ed0e66.0

*- indicates required item.

註意：上傳證書後，需要重新啟動Cisco CallManager服務以使證書生效。

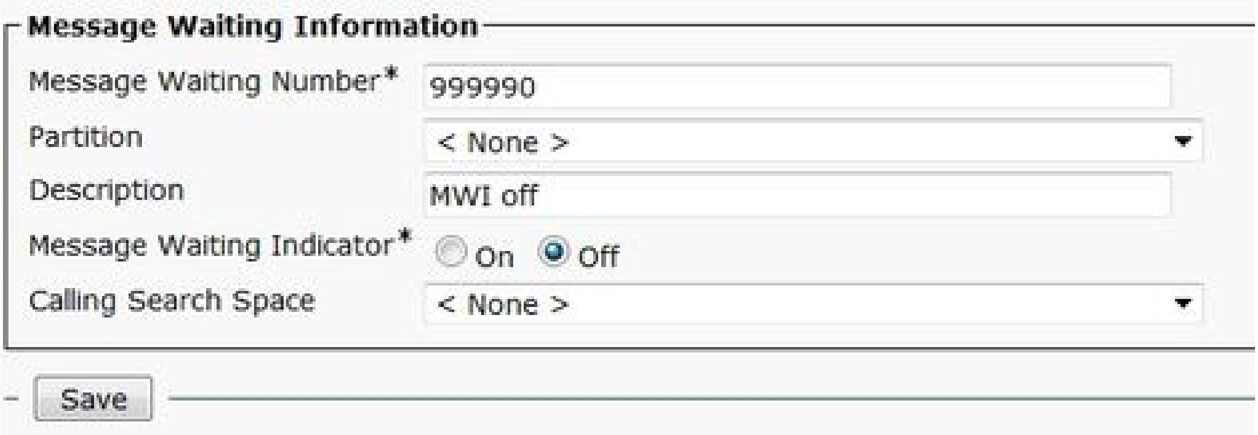
3. 配置消息等待資訊(MWI)開/關擴展

導航到**CUCM Administration > Advanced Features > Voice Mail Port Configuration**，然後配置**MWI開/關擴展。**MWI編號必須與CUC配置匹配。



Message Waiting Information

Message Waiting Number*	999991
Partition	< None >
Description	MWI on
Message Waiting Indicator*	● On ○ Off
Calling Search Space	< None >



Message Waiting Information

Message Waiting Number* 999990

Partition < None >

Description MWI off

Message Waiting Indicator* ○ On ● Off

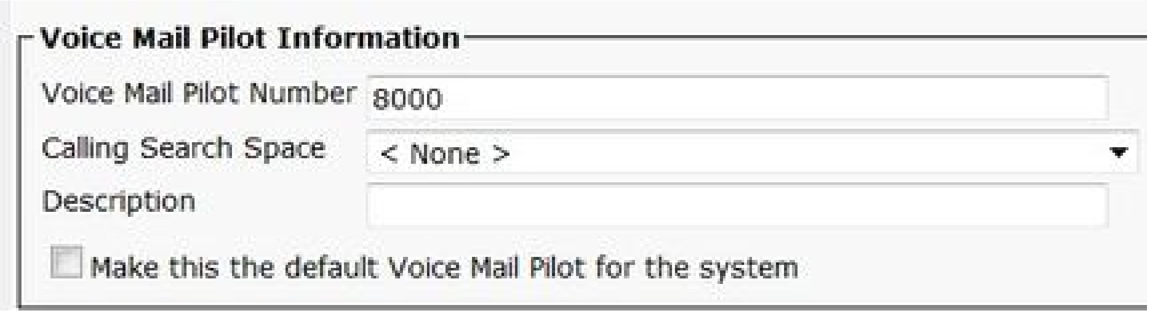
Calling Search Space < None >

Save

4.創建語音郵件引導

為整合建立語音郵件引導(**高級功能>語音郵件>語音郵件引導**)。 輸入以下值：

- 語音郵件引導號碼：
- 呼叫搜尋空間：　　其中包括包含用作引導的路由模式的分割槽>



Voice Mail Pilot Information

Voice Mail Pilot Number 8000

Calling Search Space < None >

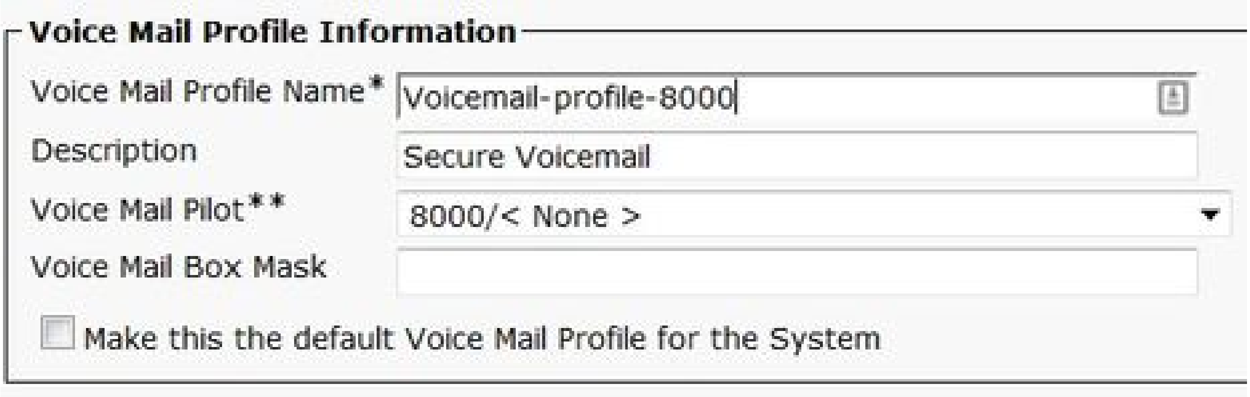
Description

□ Make this the default Voice Mail Pilot for the system

5.建立語音郵件配置檔案

建立語音郵件配置檔案以將所有設定連結在一起(「**高級功能」>「語音郵件」>「語音郵件配置檔案**」)。 輸入以下資訊：

- 語音郵件引導：
- 語音信箱掩碼：



Voice Mail Profile Information

Voice Mail Profile Name* Voicemail-profile-8000

Description Secure Voicemail

Voice Mail Pilot** 8000/< None >

Voice Mail Box Mask

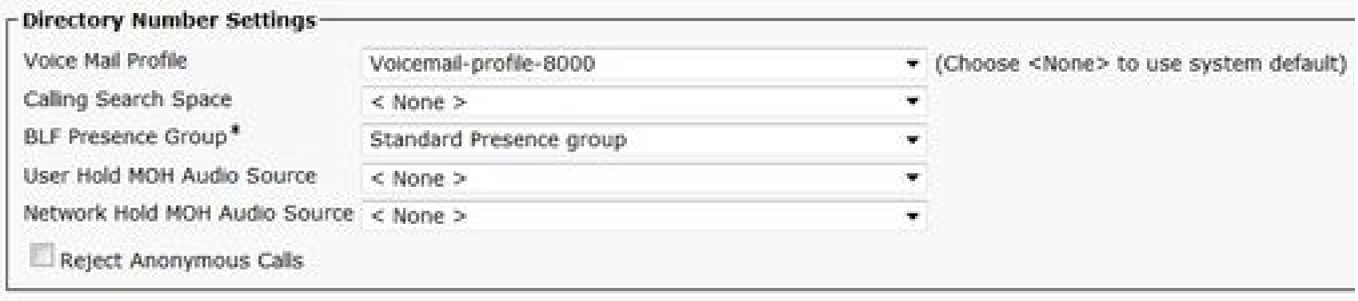
□ Make this the default Voice Mail Profile for the System

6.將語音郵件配置檔案分配給DN

將語音郵件配置檔案分配到打算使用安全整合的DN。更改DN設定後，按一下**Apply Config**按鈕：

導航到**Call Routing > Directory number**，然後更改為：

- 語音郵件配置檔案： Voicemail-profile-8000



Directory Number Settings

Voice Mail Profile: Voicemail-profile-8000 ▾ (Choose <None> to use system default)

Calling Search Space: < None > ▾

BLF Presence Group*: Standard Presence group ▾

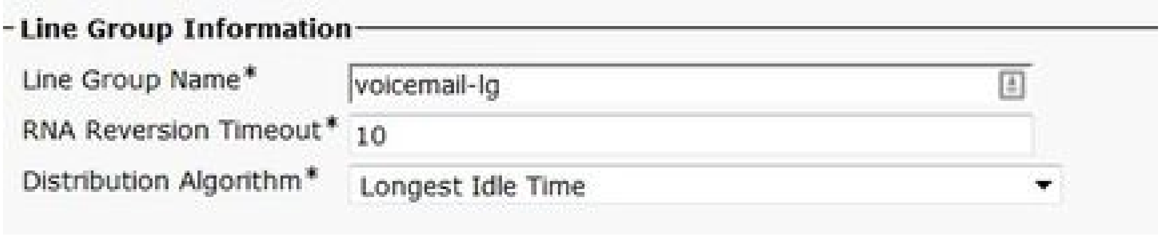
User Hold MOH Audio Source: < None > ▾

Network Hold MOH Audio Source: < None > ▾

□ Reject Anonymous Calls

7. 建立語音郵件搜尋組

a)新增新的**線路組**(**呼叫路由>路由/尋線>線路組**)



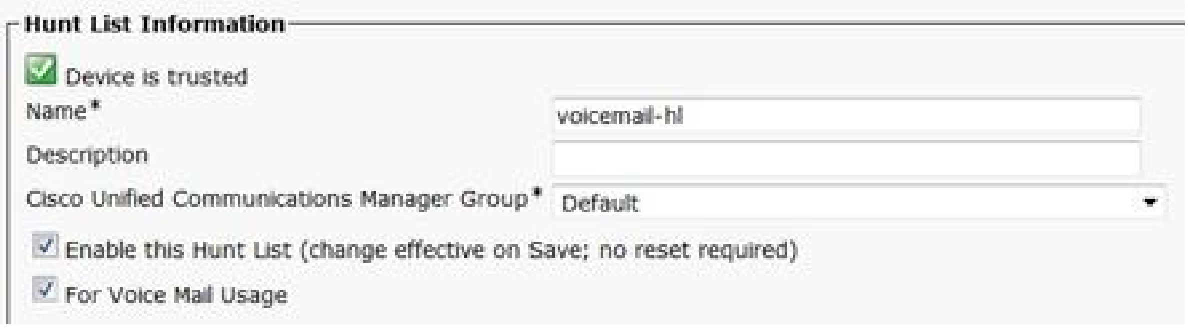
Line Group Information

Line Group Name*: voicemail-lg

RNA Reversion Timeout*: 10

Distribution Algorithm*: Longest Idle Time ▾

b)新增新的語音郵件尋**線清單**(**呼叫路由>路由/尋線>尋線清單**)



Hunt List Information

☑ Device is trusted

Name*: voicemail-hl

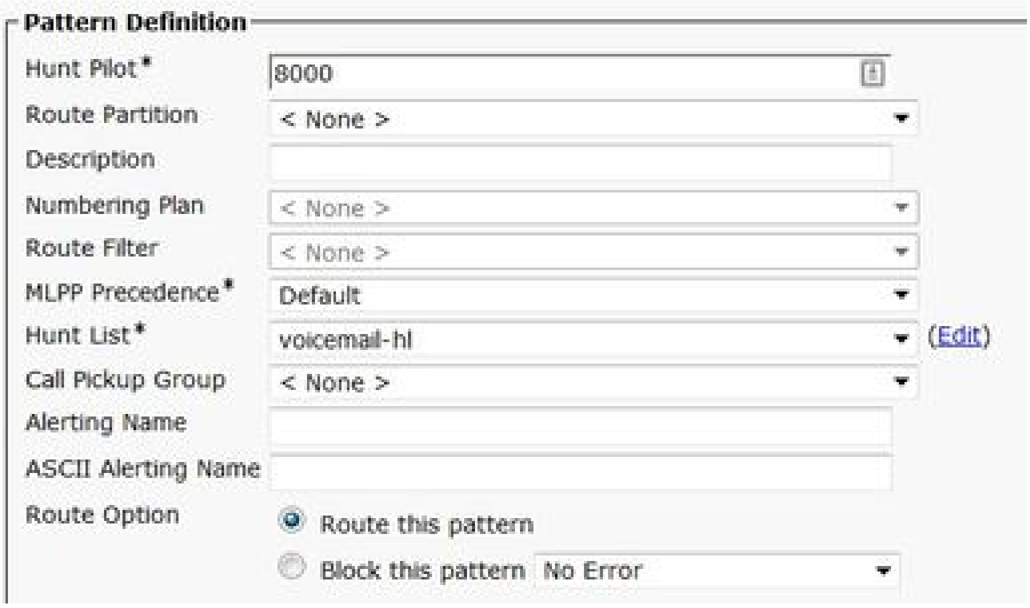
Description:

Cisco Unified Communications Manager Group*: Default ▾

☑ Enable this Hunt List (change effective on Save; no reset required)

☑ For Voice Mail Usage

c)新增新的**尋線引導**(**呼叫路由>路由/尋線>尋線引導**)



Pattern Definition

Hunt Pilot*: 8000

Route Partition: < None > ▾

Description:

Numbering Plan: < None > ▾

Route Filter: < None > ▾

MLPP Precedence*: Default ▾

Hunt List*: voicemail-hl ▾ (Edit)

Call Pickup Group: < None > ▾

Alerting Name:

ASCII Alerting Name:

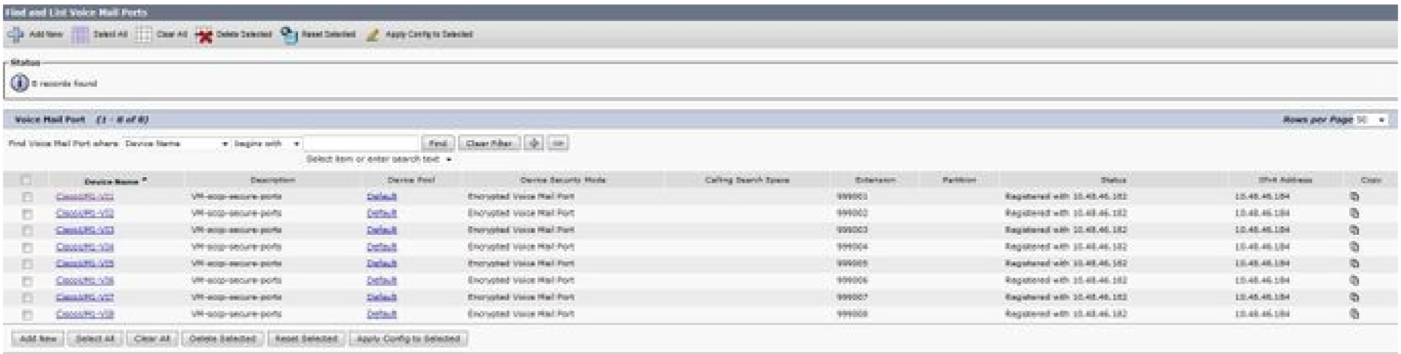
Route Option: ● Route this pattern

○ Block this pattern No Error ▾

驗證

SCCP連線埠驗證

導航到**CUCM Administration > Advanced Features > Voice Mail > Voice Mail Ports**，然後驗證埠註冊。



Find and List Voice Mail Ports

Status: 8 records found

Voice Mail Port (1 - 8 of 8) — Rows per Page 50

Find Voice Mail Port where Device Name begins with — Select item or enter search text

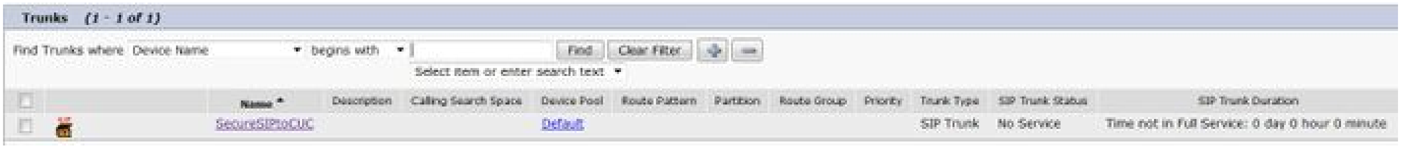
□	Device Name	Description	Device Pool	Device Security Mode	Calling Search Space	Extension	Partition	Status	IPv4 Address	Copy
□	CiscoUM1-VI1	VM-sccp-secure-ports	Default	Encrypted Voice Mail Port		999001		Registered with 10.48.46.182	10.48.46.184	
□	CiscoUM1-VI2	VM-sccp-secure-ports	Default	Encrypted Voice Mail Port		999002		Registered with 10.48.46.182	10.48.46.184	
□	CiscoUM1-VI3	VM-sccp-secure-ports	Default	Encrypted Voice Mail Port		999003		Registered with 10.48.46.182	10.48.46.184	
□	CiscoUM1-VI4	VM-sccp-secure-ports	Default	Encrypted Voice Mail Port		999004		Registered with 10.48.46.182	10.48.46.184	
□	CiscoUM1-VI5	VM-sccp-secure-ports	Default	Encrypted Voice Mail Port		999005		Registered with 10.48.46.182	10.48.46.184	
□	CiscoUM1-VI6	VM-sccp-secure-ports	Default	Encrypted Voice Mail Port		999006		Registered with 10.48.46.182	10.48.46.184	
□	CiscoUM1-VI7	VM-sccp-secure-ports	Default	Encrypted Voice Mail Port		999007		Registered with 10.48.46.182	10.48.46.184	
□	CiscoUM1-VI8	VM-sccp-secure-ports	Default	Encrypted Voice Mail Port		999008		Registered with 10.48.46.182	10.48.46.184	

按電話上的**Voice Mail**按鍵以呼叫語音郵件。如果使用者的分機未在Unity Connection系統上配置，您應該聽到開場問候語。

安全SIP中繼驗證

按電話上的**Voice Mail**按鍵以呼叫語音郵件。如果未在Unity Connection系統上配置使用者分機，您應該會聽到開始問候語。

或者，您可以啟用SIP OPTION保持連線以監控SIP中繼狀態。可以在分配給SIP中繼的SIP配置檔案中啟用此選項。啟用此功能後，您可以透過**Device > Trunk**監控Sip中繼狀態，如下圖所示。



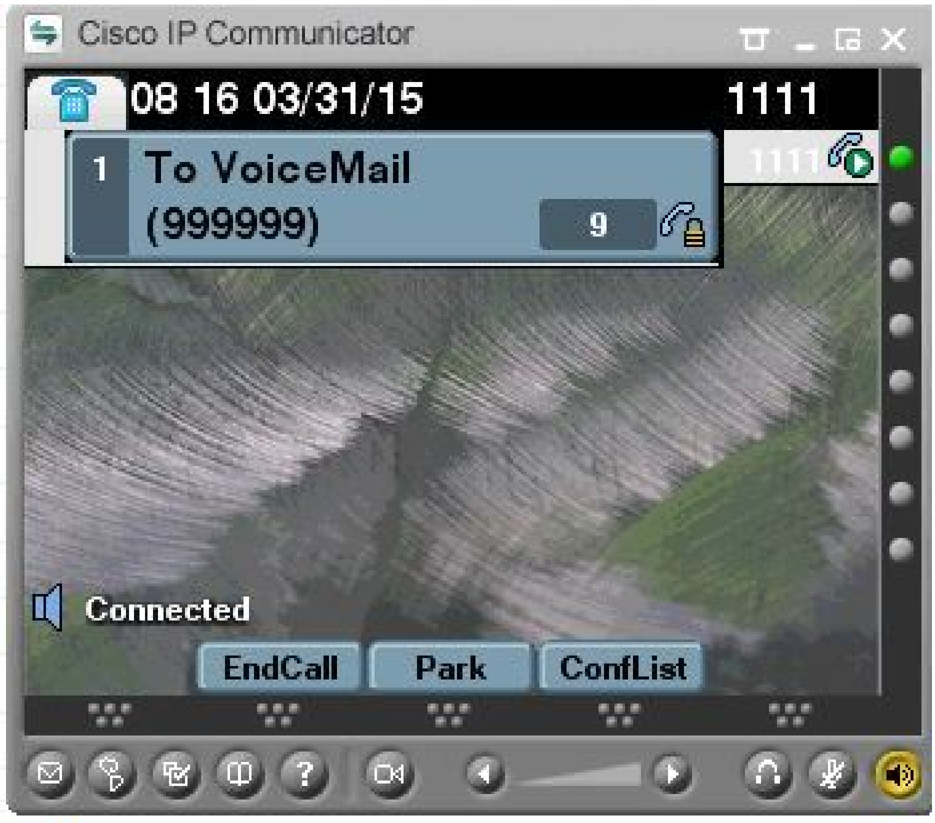
Trunks (1 - 1 of 1)

Find Trunks where Device Name begins with — Select item or enter search text

□		Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
□		SecureSIPtoCUC			Default					SIP Trunk	No Service	Time not in Full Service: 0 day 0 hour 0 minute

安全RTP呼叫驗證

驗證對Unity Connection的呼叫中是否出現掛鎖圖示。它表示RTP流已加密（裝置安全配置檔案必須安全才能運行），如下圖所示。



疑難排解

1.一般故障排除提示

請按照以下步驟操作，對安全整合進行故障排除：

- 驗證設定.
- 確保所有相關服務都在運行。（CUCM - CallManager、TFTP、CUC — 對話管理器）
- 確保在網路中開啟伺服器間安全通訊所需的埠（TCP埠2443用於SCCP整合，TCP 5061用於SIP整合）。
- 如果所有這些都是正確的，則繼續收集跟蹤。

2.要收集的跟蹤

收集這些跟蹤以排除安全整合故障。

- 從CUCM和CUC捕獲資料包
- CallManager跟蹤
- 思科對話管理器跟蹤

請參閱以下資源以瞭解其他資訊：

如何在CUCM上執行資料包捕獲：

http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-50/112040-packet-capture-cucm-00.html

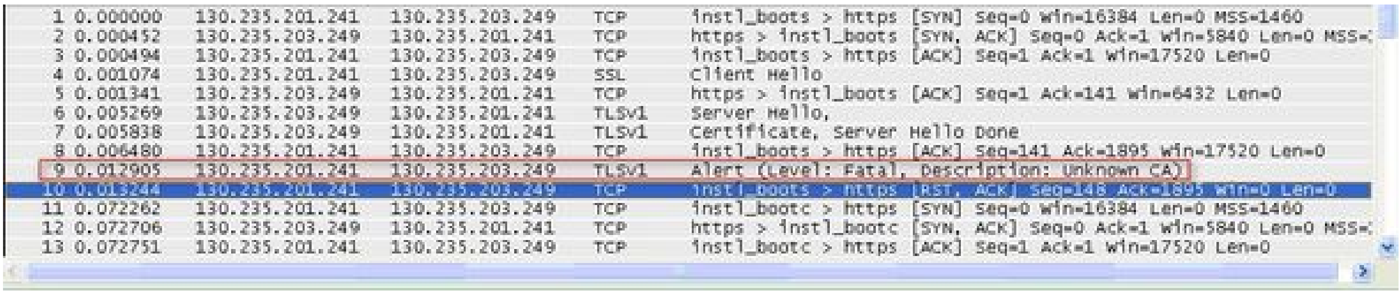
如何在CUC伺服器上啟用跟蹤：

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx/10xcuctsg010.html

常見問題

案例1:無法建立安全連線（未知CA警報）

從任一伺服器收集資料包捕獲後，建立TLS會話。



```
 1 0.000000   130.235.201.241   130.235.203.249   TCP     instl_boots > https [SYN] Seq=0 Win=16384 Len=0 MSS=1460
 2 0.000452   130.235.203.249   130.235.201.241   TCP     https > instl_boots [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
 3 0.000494   130.235.201.241   130.235.203.249   TCP     instl_boots > https [ACK] Seq=1 Ack=1 Win=17520 Len=0
 4 0.001074   130.235.201.241   130.235.203.249   SSL     Client Hello
 5 0.001341   130.235.203.249   130.235.201.241   TCP     https > instl_boots [ACK] Seq=1 Ack=141 Win=6432 Len=0
 6 0.005269   130.235.203.249   130.235.201.241   TLSv1   Server Hello,
 7 0.005838   130.235.203.249   130.235.201.241   TLSv1   Certificate, Server Hello Done
 8 0.006480   130.235.201.241   130.235.203.249   TCP     instl_boots > https [ACK] Seq=141 Ack=1895 Win=17520 Len=0
 9 0.012905   130.235.201.241   130.235.203.249   TLSv1   Alert (Level: Fatal, Description: Unknown CA)
10 0.013244   130.235.201.241   130.235.203.249   TCP     instl_boots > https [RST, ACK] Seq=148 Ack=1895 Win=0 Len=0
11 0.072262   130.235.201.241   130.235.203.249   TCP     instl_bootc > https [SYN] Seq=0 Win=16384 Len=0 MSS=1460
12 0.072706   130.235.203.249   130.235.201.241   TCP     https > instl_bootc [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
13 0.072751   130.235.201.241   130.235.203.249   TCP     instl_bootc > https [ACK] Seq=1 Ack=1 Win=17520 Len=0
```

客戶端向伺服器發出警報，通知中含有未知的CA錯誤，原因僅僅是客戶端無法驗證伺服器傳送的證書。

可能發生兩種情況：

1)CUCM傳送警報 未知CA

- 驗證當前CUC根證書是否上載到與CUC伺服器通訊的伺服器上。
- 確保在相應的伺服器上重新啟動CallManager服務。

2)CUC傳送警報Unknown CA

- 驗證CUC伺服器上的**Port Group > Edit > Servers** 配置中是否正確輸入了TFTP IP地址。
- 驗證是否可從連線伺服器訪問CUCM TFTP伺服器。
- 確保CUCM TFTP上的CTL檔案為當前檔案（將「show ctl」的輸出與OS Admin頁面上顯示的證書進行比較）。 如果沒有運行，請重新運行CTLClient。
- 重新啟動CUC伺服器，或者刪除並重新建立埠組，以便從CUCM TFTP重新下載CTL檔案。

案例2:無法從CUCM TFTP下載CTL檔案

在對話管理器跟蹤中出現此錯誤：

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving
server certificates.
MiuGeneral,25,Error executing tftp command 'tftp://10.48.47.189:69/CTLFile.tlv' res=68 (file not
found on server)
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving
server certificates.
Arbiter,-1,Created port PhoneSystem-1-001 objectId='7c2e86b8-2d86-4403-840e-16397b3c626b' as
ID=1
MiuGeneral,25,Port group object 'b1c966e5-27fb-4eba-a362-56a5fe9c2be7' exists
MiuGeneral,25,FAILED SetInService=true parent port group is out of service:
```

解決方案：

1.在**Port group > Edit > Servers**配置中再次檢查TFTP伺服器是否正確。

2.驗證CUCM群集是否處於安全模式。

3.檢驗CUCM TFTP上是否存在CTL檔案。

案例3:連線埠未註冊

在對話管理器跟蹤中出現此錯誤：

```
MiuSkinny,23,Failed to retrieve Certificate for CCM Server <CUCM IP Address>
MiuSkinny,23,Failed to extract any CCM Certificates - Registration cannot proceed. Starting
retry timer -> 5000 msec
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxx.tlv]
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM
IP Address>' in CTL File
```

解決方案：

1.這很可能是由於CUCM和CUC上的CTL檔案的md5校驗和不匹配，這是由於憑證。重新啟動CUC伺服器以刷新CTL檔案。

思科內部資訊

或者，也可以按如下方式從根目錄刪除CTL檔案：

從/tmp/資料夾中刪除CTL檔案並重置埠組。您可以對檔案執行md5總和檢查碼並在刪除之前進行比較：

```
    CUCM:   [root@vfrscucm1 trust-certs]# md5sum /usr/local/cm/tftp/CTLFile.tlv

            e5bf2ab934a42f4d8e6547dfd8cc82e8 /usr/local/cm/tftp/CTLFile.tlv

    CUC:    [root@vstscuc1 tmp]# cd /tmp

            [root@vstscuc1 tmp]# ls -al *tlv

             -rw-rw-r— 1 cucsmgr customervice 6120 2月5日15:29 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

            [root@vstscuc1 tmp]# md5sum a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

            e5bf2ab934a42f4d8e6547dfd8cc82e8 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

此外，您還可以參閱本故障排除指南：

缺陷

CSCum48958 - CUCM 10.0（IP地址長度不正確）

CSCtn87264 — 安全SIP埠的TLS連線失敗

CSCur10758 -無法清除吊銷的證書Unity Connection

CSCur10534 - Unity Connection 10.5 TLS/PKI互操作冗餘CUCM

CSCve47775 -用於更新和檢查CUC上的CUCM CTLFile方法的功能請求