

# 基於下一代加密(NGE)的CUCM和CUC之間安全SIP整合的配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[網路圖表](#)

[證書要求](#)

[協商的基於RSA金鑰的密碼](#)

[協商基於EC金鑰的密碼](#)

[配置 — Cisco Unity Connection\(CUC\)](#)

[1.新增新埠組](#)

[2.新增TFTP伺服器參考](#)

[3.新增語音郵件埠](#)

[4.上傳第三方CA的CUCM根和中間證書](#)

[配置 — Cisco Unified CM\(CUCM\)](#)

[1.建立SIP中繼安全配置檔案](#)

[2.建立安全SIP中繼](#)

[3.配置TLS和SRTP密碼](#)

[4.上傳CUC Tomcat證書 \( 基於RSA和EC \)](#)

[5.建立路由模式](#)

[6.建立語音郵件引導、語音郵件配置檔案並將其分配給DN](#)

[配置 — 由第三方CA對基於EC金鑰的證書進行簽名 \( 可選 \)](#)

[驗證](#)

[安全SIP中繼驗證](#)

[安全RTP呼叫驗證](#)

[相關資訊](#)

---

## 簡介

本檔案介紹使用下一代加密在Cisco Unified Communication Manager(CUCM)和Cisco Unity Connection(CUC)伺服器之間安全SIP連線的配置和驗證。

Next Generation Security over SIP interface限制SIP介面使用基於TLS 1.2、SHA-2和AES256協定的Suite B密碼。它允許根據RSA或ECDSA密碼的優先順序順序進行各種密碼組合。在Unity Connection和Cisco Unified CM之間的通訊期間，密碼和第三方證書均會在兩端進行驗證。以下是下一代加密支援的配置。

如果您計畫使用由第三方證書頒發機構簽名的證書，則從配置部分末尾的證書簽名開始 ( 配置 — 由第三方CA對基於EC金鑰的證書簽名 )

## 必要條件

# 需求

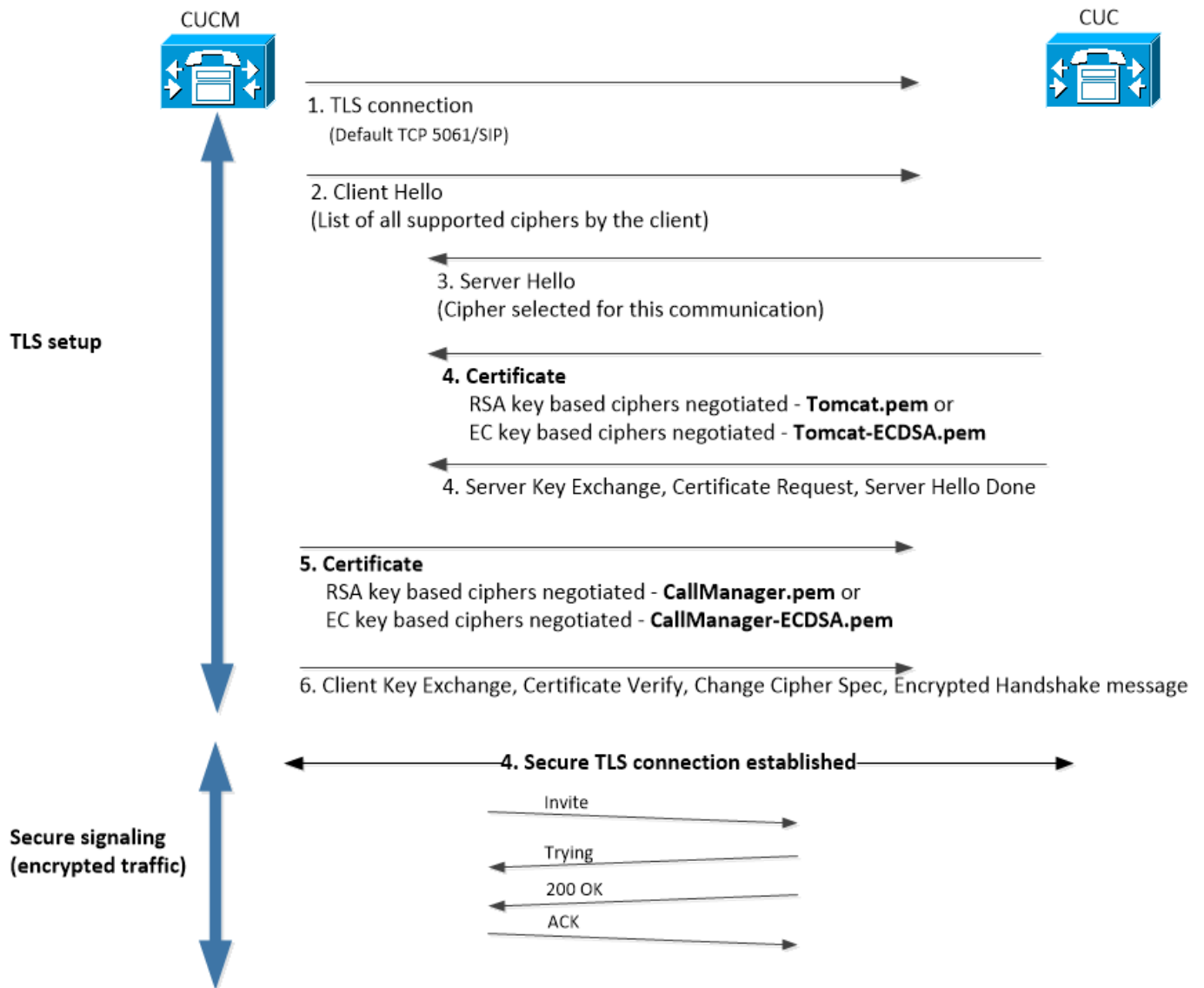
本文中的資訊係根據以下軟體和硬體版本：

混合模式下的CUCM 11.0版及更高版本  
CUC版本11.0及更高版本

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。

# 網路圖表

此圖簡要說明了啟用下一代加密支援後，在CUCM和CUC之間建立安全連線的過程：



# 證書要求

在Cisco Unity Connection上啟用下一代加密支援後，這些是證書交換要求。

**• 協商的基於RSA金鑰的密碼**

使用的CUCM證書	使用的CUC證書	要上傳到CUCM的證書	要上傳到CUC的證書
CallManager.pem ( 自簽名 )	Tomcat.pem ( 自簽名 )	要上傳到CUCM > CallManger-trust的Tomcat.pem	無.
CallManager.pem ( 已簽署CA )	Tomcat.pem ( CA簽名 )	要上傳到CUCM的CUC <sup>根和</sup> 中繼CA證書*1 > CallManager-trust	要上傳到CUC > CallManager-trust的CUCM根和中繼CA證書*1
CallManager.pem ( 已簽署CA )	Tomcat.pem ( 自簽名 )	要上傳到CUCM > CallManger-trust的Tomcat.pem	要上傳到CUC > CallManager-trust的CUCM根和中繼CA證書
CallManager.pem ( 自簽名 )	Tomcat.pem ( CA簽名 )	要上傳到CUCM的CUC根和中繼CA證書> CallManager-trust	無.

\*1 CUC根和中繼CA證書是指簽署Unity connection Tomcat證書(Tomcat.pem)的CA證書。

\*2 CUCM根和中繼CA證書是指簽署CUCM CallManager證書(Callmanager.pem)的CA證書。

**• 協商基於EC金鑰的密碼**

使用的CUCM證書	使用的CUC證書	要上傳到CUCM的證書	要上傳到CUC的證書
CallManager-ECDSA.pem ( 自簽名 )	Tomcat-ECDSA.pem ( 自簽名 )	要上傳到CUCM的Tomcat-ECDSA.pem > CallManger-trust	無.
CallManager-ECDSA.pem ( CA簽名 )	Tomcat-ECDSA.pem ( CA簽名 )	要上傳到CUCM的CUC <sup>根和</sup> 中繼CA證書*1 > CallManager-trust	要上傳到CUC > CallManager-trust的CUCM根和中繼CA證書*2。
CallManager-ECDSA.pem ( CA簽名 )	Tomcat-ECDSA.pem ( 自簽名 )	要上傳到CUCM > CallManger-trust的Tomcat-ECDSA.pem。	要上傳到CUC > CallManager-trust的CUCM根和中繼CA證書。
CallManager-ECDSA.pem ( 自簽名 )	Tomcat-ECDSA.pem ( CA簽名 )	要上傳到CUCM的CUC根和中繼CA證書> CallManager-trust	無.

\*1 CUC根和中繼CA證書是指簽署基於Unity連線EC的Tomcat證書(Tomcat-ECDSA.pem)的CA證書。

\*2 CUCM根和中繼CA證書是指簽署CUCM CallManager證書(CallManager-ECDSA.pem)的CA證書。

1. 附註：Tomcat-ECDSA.pem證書在11.0.1版本的CUC中稱為CallManager-ECDSA.pem。從CUC 11.5.x中，證書已重新命名為Tomcat-ECDSA.pem。

## 配置 — Cisco Unity Connection(CUC)

### 1. 新增新埠組

導航到Cisco Unity Connection Administration頁面>電話整合>埠組，然後點選Add New。確保選中

Enable Next Generation Encryption 覈取方塊。

**New Port Group**

Phone System PhoneSystem ▼

Create From  Port Group Type SIP ▼

Port Group PhoneSystem-1 ▼

**Port Group Description**

Display Name\* PhoneSystem-2

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile 5061/TLS ▼

Enable Next Generation Encryption

Secure RTP

**Primary Server Settings**

IPv4 Address or Host Name 10.48.47.109

IPv6 Address or Host Name

Port 5061

1. **注意：**啟用「啟用下一代加密」覈取方塊後，在SSL握手期間將使用Unity Connection的Cisco Tomcat證書。
  - 在協商基於ECDSA的密碼的情況下，基於EC金鑰的tomcat-ECDSA證書用於SSL握手。
  - 在協商基於RSA的密碼的情況下，基於RSA金鑰的tomcat證書用於SSL握手。

## 2. 新增TFTP伺服器參考

在Port Group Basics頁面上，導航到Edit > Servers並新增CUCM群集的TFTP伺服器的FQDN。TFTP伺服器的FQDN/主機名必須與CallManager證書的公用名(CN)匹配。伺服器的IP地址不起作用，將導致無法下載ITL檔案。因此，DNS名稱必須通過已配置的DNS伺服器進行解析。

SIP Servers			
Delete Selected Add			
<input type="checkbox"/>	Order	IPv4 Address or Host Name	
<input type="checkbox"/>	0	10.48.47.109	
Delete Selected Add			

TFTP Servers			
Delete Selected Add			
<input type="checkbox"/>	Order	IPv4 Address or Host Name	
<input type="checkbox"/>	0	CUCMv11	
Delete Selected Add			

導航到Cisco Unity Connection Serviceability > Tools > Service Management，在每個節點上重新啟動Connection Conversation Manager。要使配置生效，必須執行此操作。

1. 附註：Unity connection使用https協定在安全6972埠(URL: https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv)從CUCM的TFTP下載ITL檔案(ITLfile.tlv)。CUCM必須處於混合模式，因為CUC正在從ITL檔案查詢「CCM+TFTP」功能證書。

導航回電話整合>埠組>埠組基本配置頁，並重置新新增的埠組。

Port Group	
Display Name*	PhoneSystem-1
Integration Method	SIP
Reset Status	Reset Required <input type="button" value="Reset"/>

**Session Initiation Protocol (SIP) Settings**

Register with SIP Server

Authenticate with SIP Server

1. 附註：每次重置埠組時，CUC伺服器都會通過連線到CUCM伺服器更新其本地儲存的ITL檔案。

### 3.新增語音郵件埠

導航回電話整合(Telephony integration)>埠(Port)，然後點選新增新(Add new)將埠新增到新建立的埠組。

### New Phone System Port

Enabled

Number of Ports

Phone System

Port Group

Server

### Port Behavior

Answer Calls

Perform Message Notification

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

Allow TRAP Connections

#### 4.上傳第三方CA的CUCM根和中間證書

如果是第三方證書，您必須在Unity Connection的CallManager-trust上上傳第三方證書頒發機構的根證書和中間證書。僅當第三方CA對您的Call Manager證書簽名時，才需要此功能。通過導航到Cisco Unified OS Administration > Security > Certificate Management並點選Upload Certificate來執行此操作。

### Upload Certificate/Certificate chain

Certificate Purpose\*

Description(friendly name)

Upload File  CA\_root\_-\_4096\_key.crt

## 配置 — Cisco Unified CM(CUCM)

### 1.建立SIP中繼安全配置檔案

導航到CUCM管理>系統>安全> SIP中繼安全配置檔案並新增新配置檔案。X.509使用者名稱必須與CUC伺服器的FQDN匹配。

### SIP Trunk Security Profile Information

Name\*

Description

Device Security Mode

Incoming Transport Type\*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)\*

X.509 Subject Name

Incoming Port\*

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer\*\*

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

- 註:CLI命令「show cert own tomcat/tomcat.pem」可在Unity Connection上顯示基於RSA金鑰的tomcat證書。其CN必須與CUCM上配置的X.509主題名稱相匹配。CN等於Unity伺服器的FQDN/主機名。基於EC金鑰的證書在其Subject Alternate Name(SAN)欄位中包含FQDN/主機名。

## 2.建立安全SIP中繼

導航到Device > Trunk > Click and Add new並建立用於與Unity Connection安全整合的標準SIP中繼

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\*

Route Class Signaling Enabled\*

Use Trusted Relay Point\*

PSTN Access

Run On All Active Unified CM Nodes

### Inbound Calls

Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Inbound	

### Outbound Calls

Called Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Called Party Transformation CSS	
Calling Party Transformation CSS	< None >
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> Redirecting Diversion Header Delivery - Outbound	
Redirecting Party Transformation CSS	< None >
<input checked="" type="checkbox"/> Use Device Pool Redirecting Party Transformation CSS	

### Destination

<input type="checkbox"/> Destination Address is an SRV			
	Destination Address	Destination Address IPv6	Destination Port
1*	10.48.47.123		5061
MTP Preferred Originating Codec*	711ulaw		
BLF Presence Group*	Standard Presence group		
SIP Trunk Security Profile*	cuc-secure-profile-EDCS		
Rerouting Calling Search Space	< None >		
Out-Of-Dialog Refer Calling Search Space	< None >		
SUBSCRIBE Calling Search Space	< None >		
SIP Profile*	Standard SIP Profile	<a href="#">View Details</a>	
DTMF Signaling Method*	No Preference		

## 3. 配置TLS和SRTP密碼

1. 附註： Unity Connection和Cisco Unified Communications Manager之間的協商取決於具有以下條件的TLS密碼配置： 當Unity Connection充當伺服器時，TLS密碼協商基於Cisco Unified CM選擇的首選項。在協商基於ECDSA的密碼時，基於EC金鑰的tomcat-ECDSA證書用於SSL握手。在協商基於RSA的密碼時，基於RSA金鑰的tomcat證書將用於SSL握手。當Unity Connection充當客戶端時，TLS密碼協商基於Unity Connection選擇的首選項。

導航到Cisco Unified CM > Systems > Enterprise Parameters，然後從TLS和SRTP密碼下拉選單中選擇相應的密碼選項。



Security Parameters	
Cluster Security Mode *	1
LBM Security Mode *	Insecure
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
TFTP File Signature Algorithm *	SHA-1
Enable Caching *	True
Authentication Method for API Browser Access *	Basic
TLS Ciphers *	All Ciphers RSA Preferred
SRTP Ciphers *	All Supported Ciphers
HTTPS Ciphers *	RSA Ciphers Only

導航到Cisco Unified Serviceability頁面Tools > Control Center-Feature Services並選擇CM Services下的Cisco Call Manager，在每個節點上重新啟動Cisco Call Manager服務

導航到Cisco Unity Connection Administration頁面>系統設定>常規配置，然後從TLS和SRTP密碼下拉選單中選擇相應的密碼選項。

### Edit General Configuration

Time Zone: (GMT+01:00) Europe/Warsaw

System Default Language: English(United States)

System Default TTS Language: English(United States)

Recording Format: G.711 mu-law

Maximum Greeting Length: 90

Target Decibel Level for Recordings and Messages: -26

Default Partition: cucv11 Partition

Default Search Scope: cucv11 Search Space

When a recipient cannot be found: Send a non-delivery receipt

IP Addressing Mode: IPv4

**TLS Ciphers: All Ciphers RSA Preferred**

**SRTP Ciphers: All supported AES-256, AES-128 ciphers**

HTTPS Ciphers: RSA Ciphers Only

導航到Cisco Unity Connection Serviceability > Tools > Service Management，在每個節點上重新啟動Connection Conversation Manager。

具有優先順序順序的TLS密碼選項

#### TLS密碼選項

最強 — 僅AES-256 SHA-384:RSA首選

僅限Strong-AES-256 SHA-384:ECDSA首選

僅限中型AES-256 AES-128:RSA首選

僅限中型AES-256 AES-128:ECDSA首選

#### 按優先順序順序排列的TLS密碼

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GC M\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

84

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

所有密碼RSA首選 ( 預設 )

首選所有密碼ECDSA

按優先順序排列的SRTP密碼選項

SRTP密碼選項

按優先順序排列的SRTP

- AEAD\_AES\_256\_GCM
- AEAD\_AES\_128\_GCM
- AES\_CM\_128\_HMAC\_SHA1\_32
- AEAD\_AES\_256\_GCM
- AEAD\_AES\_128\_GCM
- AEAD\_AES\_256\_GCM

所有支援的AES-256、AES-128密碼

AEAD AES-256、AES-28 GCM型密碼

僅基於AEAD AES256 GCM的密碼

#### 4.上傳CUC Tomcat證書 ( 基於RSA和EC )

導航到OS Administration > Security > Certificate Management , 並將兩個CUC Tomcat證書 ( 基於RSA和EC ) 上傳到CallManager-trust儲存區。

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager-trust

Description(friendly name)

Upload File Choose File tomcat-ECDSA.pem

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager-trust

Description(friendly name)

Upload File Choose File tomcat.pem

Upload Close

1. 注意：如果僅協商ECDSA密碼，則無需同時上傳兩個Unity Tomcat證書。在這種情況下，基於EC的Tomcat證書就足夠了。

如果是第三方證書，您必須上傳第三方證書頒發機構的根證書和中間證書。僅當第三方CA在您的Unity Tomcat證書上簽名時，才需要此功能。

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager-trust

Description(friendly name)

Upload File Choose File CA\_root\_-\_4096\_key.crt

Upload Close

在所有節點上重新啟動Cisco Call Manager進程以應用更改。

## 5. 建立路由模式

導航到Call Routing > Route/Hunt > Route Pattern，配置指向已配置中繼的路由模式。作為路由模式編號輸入的分機可用作語音郵件引導。

**Pattern Definition**

Route Pattern\* 2000

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\* CUCv11

Route Option  Route this pattern  Block this pattern No Error

## 6. 建立語音郵件引導、語音郵件配置檔案並將其分配給DN

通過轉至高級功能>語音郵件>語音郵件引導，為整合建立語音郵件引導。

Voice Mail Pilot Information	
Voice Mail Pilot Number	2000
Calling Search Space	< None >
Description	Default

建立語音郵件配置檔案以將所有設定連結到「高級功能」>「語音郵件」>「語音郵件配置檔案」

Voice Mail Profile Information	
Voice Mail Profile	VoiceMailProfile-8000 (used by 0 devices)
Voice Mail Profile Name*	VoiceMailProfile-8000
Description	
Voice Mail Pilot**	2000/< None >
Voice Mail Box Mask	

通過轉至Call Routing > Directory number，將新建立的語音郵件配置檔案分配給要用於安全整合的DN

Directory Number Settings	
Voice Mail Profile	VoiceMailProfile-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 >

## 配置 — 由第三方CA對基於EC金鑰的證書進行簽名（可選）

在設定系統之間的安全整合之前，證書可以由第三方CA簽署。按照以下步驟在兩個系統上簽署證書。

### Cisco Unity Connection

1. 為CUC Tomcat-ECDSA生成證書簽名請求(CSR)，並由第三方CA簽名證書
2. CA提供必須上傳的身份證書（CA簽名證書）和CA證書（CA根證書），如下所示：  
將CA根證書上傳到tomcat-trust儲存區  
將身份證書上傳到tomcat-EDCS儲存區
3. 在CUC上重新啟動對話管理器

### Cisco Unified CM

1. 生成CUCM CallManager-ECDSA的CSR，並由第三方CA簽署證書
2. CA提供必須上傳的身份證書（CA簽名證書）和CA證書（CA根證書），如下所示：  
將CA根證書上傳到callmanager-trust儲存  
將身份證書上傳到callmanager-EDCS儲存區
3. 在每個節點上重新啟動Cisco CCM和TFTP服務

同一過程將用於簽署基於RSA金鑰的證書，其中，為CUC Tomcat證書和CallManager證書生成CSR，並分別上傳到tomcat儲存和callmanager儲存中。

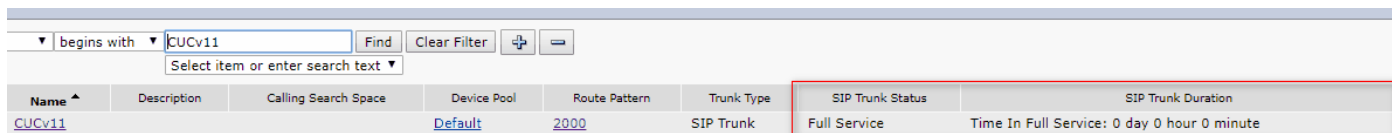
## 驗證

使用本節內容，確認您的組態是否正常運作。

### 安全SIP中繼驗證

按電話上的「語音郵件」按鈕呼叫語音郵件。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。

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，您可以通過Device > Trunk監控Sip中繼狀態，如下所示：



Name	Description	Calling Search Space	Device Pool	Route Pattern	Trunk Type	SIP Trunk Status	SIP Trunk Duration
CUCv11			Default	2000	SIP Trunk	Full Service	Time 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



## 相關資訊

- [適用於Cisco Unity連線版本11.x的SIP整合指南](#)