

基于下一代加密(NGE)的CUCM和CUC之间安全SIP集成配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[网络图](#)

[证书要求](#)

[协商的基于RSA密钥的密码](#)

[基于EC密钥的密码协商](#)

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

[1.添加新端口组](#)

[2.添加TFTP服务器参考](#)

[3.添加语音信箱端口](#)

[4.上传第三方CA的CUCM根和中间证书](#)

[配置 — Cisco Unified CM\(CUCM\)](#)

[1.创建SIP中继安全配置文件](#)

[2.创建安全SIP中继](#)

[3.配置TLS和SRTP密码](#)

[4.上传CUC Tomcat证书 \(基于RSA和EC \)](#)

[5.创建路由模式](#)

[6.创建语音邮件引导、语音邮件配置文件并将其分配给DN](#)

[配置 — 由第三方CA对基于EC密钥的证书进行签名 \(可选 \)](#)

[验证](#)

[安全SIP中继验证](#)

[安全RTP呼叫验证](#)

[相关信息](#)

简介

本文档介绍使用下一代加密的Cisco Unified Communication Manager(CUCM)和Cisco Unity Connection(CUC)服务器之间安全SIP连接的配置和验证。

下一代SIP安全接口限制SIP接口使用基于TLS 1.2、SHA-2和AES256协议的套件B密码。它允许根据RSA或ECDSA密码的优先级顺序进行各种密码组合。在Unity Connection与Cisco Unified CM之间的通信过程中，密码和第三方证书在两端都经过验证。以下是下一代加密支持的配置。

如果您计划使用由第三方证书颁发机构签名的证书，则从配置部分末尾的证书签名开始（配置 — 由第三方CA签名基于EC密钥的证书）

先决条件

要求

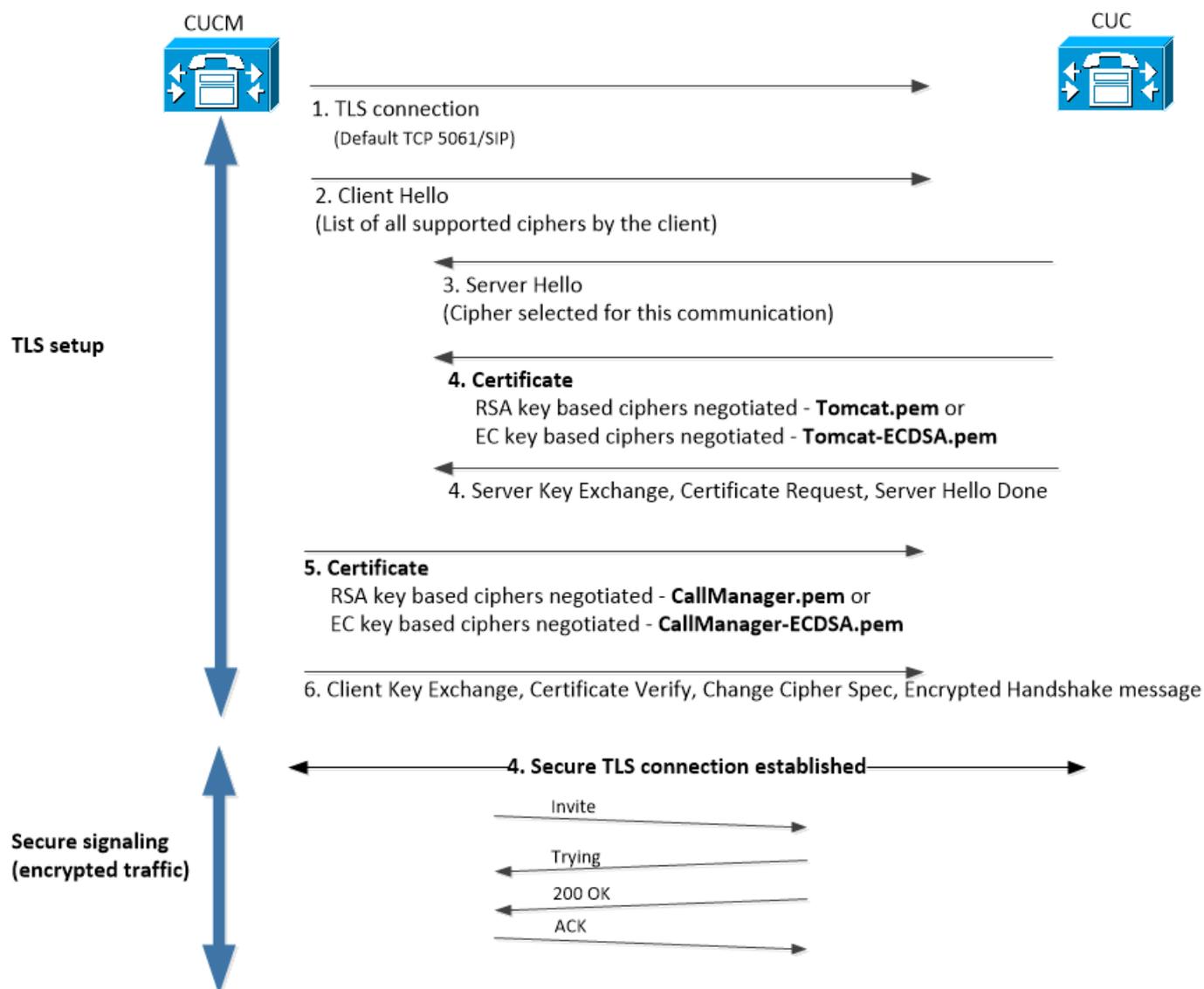
本文档中的信息基于以下软件和硬件版本：

CUCM 11.0版及更高版本（混合模式）
CUC版本11.0及更高版本

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。

网络图

此图简要说明了在启用下一代加密支持后帮助在CUCM和CUC之间建立安全连接的过程：



证书要求

在Cisco Unity Connection上启用下一代加密支持后，这些是证书交换要求。

• 协商的基于RSA密钥的密码

使用的CUCM证书	使用的CUC证书	上传到CUCM的证书	要上传到CUC的证书
CallManager.pem (自签名)	Tomcat.pem (自签名)	要上传到CUCM > CallManger-trust的 Tomcat.pem	无.
CallManager.pem (CA签名)	Tomcat.pem (CA签名)	CUC根和中间CA证书* ¹ 要上传到CUCM > CallManager-trust	CUCM根和中间CA证书
CallManager.pem (CA签名)	Tomcat.pem (自签名)	要上传到CUCM > CallManger-trust的 Tomcat.pem	要上传到CUCM根和中间CA证书
CallManager.pem (自签名)	Tomcat.pem (CA签名)	要上传到CUCM > CallManager-trust的 CUC根和中间CA证书	无.

*¹ CUC根和中间CA证书是指签署Unity connection Tomcat证书(Tomcat.pem)的CA证书。

*² CUCM根和中间CA证书是指签署CUCM CallManager证书(Callmanager.pem)的CA证书。

• 基于EC密钥的密码协商

使用的CUCM证书	使用的CUC证书	上传到CUCM的证书	要上传到CUC的证书
CallManager-ECDSA.pem (自签名)	Tomcat-ECDSA.pem (自签名)	要上传到CUCM > CallManger-trust的 Tomcat-ECDSA.pem	无.
CallManager-ECDSA.pem (CA签名)	Tomcat-ECDSA.pem (CA签名)	CUC根和中间CA证书* ¹ 要上传到CUCM > CallManager-trust	CUCM根和中间CA证书* ² 要上传到CUC > CallManager-trust。
CallManager-ECDSA.pem (CA签名)	Tomcat-ECDSA.pem (自签名)	要上传到CUCM > CallManger-trust的 Tomcat-ECDSA.pem。	要上传到CUC > CallManager-trust的 CUCM根和中间CA证书。
CallManager-ECDSA.pem (自签名)	Tomcat-ECDSA.pem (CA签名)	要上传到CUCM > CallManager-trust的 CUC根和中间CA证书	无.

*¹ CUC根和中间CA证书是指签署基于Unity连接EC的Tomcat证书(Tomcat-ECDSA.pem)的CA证书。

*² CUCM根和中间CA证书是指签署CUCM CallManager证书(CallManager-ECDSA.pem)的CA证书。

1. **注意：**在CUC的11.0.1版本中，Tomcat-ECDSA.pem证书称为CallManager-ECDSA.pem。从CUC 11.5.x，证书已重命名为Tomcat-ECDSA.pem。

配置 — Cisco Unity Connection(CUC)

1.添加新端口组

导航至Cisco Unity Connection Administration页面> Telephony integration > Port group，然后点击Add New。确保选中启用下一代加密复选框。

New Port Group

Phone System

Create From Port Group Type Port Group

Port Group Description

Display Name*

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile

Enable Next Generation Encryption

Secure RTP

Primary Server Settings

IPv4 Address or Host Name

IPv6 Address or Host Name

Port

1. 注意：一旦启用Enable Next Generation Encryption复选框，Unity Connection的Cisco Tomcat证书将在SSL握手期间使用。
 - 在协商基于ECDSA的密码时，SSL握手中使用基于EC密钥的tomcat-ECDSA证书。
 - 如果协商基于RSA的密码，则在SSL握手中使用基于RSA密钥的tomcat证书。

2.添加TFTP服务器参考

在Port Group Basics页面，导航至Edit > Servers，然后添加CUCM集群的TFTP服务器的FQDN。TFTP服务器的FQDN/主机名必须与CallManager证书的公用名(CN)匹配。服务器的IP地址将无法工作，并且会导致无法下载ITL文件。因此，DNS名称必须可通过配置的DNS服务器解析。

SIP Servers		
Delete Selected Add		
Order	IPv4 Address or Host Name	
0	10.48.47.109	
Delete Selected Add		

TFTP Servers		
Delete Selected Add		
Order	IPv4 Address or Host Name	
0	CUCMv11	
Delete Selected Add		

导航至Cisco Unity Connection Serviceability > Tools > Service Management，在每个节点上重新启动Connection Conversation Manager。这是配置生效的必需条件。

1. **注意**：Unity Connection使用安全6972端口上的https协议从CUCM的TFTP下载ITL文件 (ITLfile.tlv)(URL:https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv)。CUCM必须处于混合模式，因为CUC正在从ITL文件中查找“CCM+TFTP”功能证书。

导航回Telephony integration > Port group > Port Group Basics配置页面并重置新添加的端口组。

Port Group	
Display Name*	PhoneSystem-1
Integration Method	SIP
Reset Status	Reset Required Reset

Session Initiation Protocol (SIP) Settings

Register with SIP Server

Authenticate with SIP Server

1. **注意**：每次重置端口组时，CUC服务器将通过连接到CUCM服务器更新其本地存储的ITL文件。

3.添加语音信箱端口

导航回Telephony integration > Port，然后点击Add new，将端口添加到新创建的端口组。

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.上传第三方CA的CUCM根和中间证书

如果是第三方证书，则必须在Unity Connection的CallManager信任上上传第三方证书颁发机构的根证书和中间证书。仅当第3方CA为Call Manager证书签名时，才需要此设置。导航至Cisco Unified OS Administration > Security > Certificate Management，然后点击Upload Certificate，执行此操作。

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File

配置 — Cisco Unified CM(CUCM)

1.创建SIP中继安全配置文件

导航至CUCM管理>System >安全> SIP中继安全配置文件并添加新配置文件。X.509主题名称必须与CUC服务器的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

1. 注意：CLI命令“show cert own tomcat/tomcat.pem”可在Unity Connection上显示基于RSA密钥的tomcat证书。CN必须与CUCM上配置的X.509主题名称匹配。CN等于Unity服务器的FQDN/主机名。基于EC密钥的证书在其使用者备用名称(SAN)字段中包含FQDN/主机名。

2.创建安全SIP中继

导航至Device > Trunk > Click and Add new，然后创建标准SIP中继，该中继将用于与Unity Connection的安全集成。

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*

Connected Line ID Presentation*

Connected Name Presentation*

Calling Search Space

AAR Calling Search Space

Prefix DN

Redirecting Diversion Header Delivery - Inbound

Outbound Calls

Called Party Transformation CSS

Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS

Use Device Pool Calling Party Transformation CSS

Calling Party Selection*

Calling Line ID Presentation*

Calling Name Presentation*

Calling and Connected Party Info Format*

Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS

Use Device Pool Redirecting Party Transformation CSS

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	<input type="text" value="10.48.47.123"/>	<input type="text"/>	<input type="text" value="5061"/>

MTP Preferred Originating Codec*

BLF Presence Group*

SIP Trunk Security Profile*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile* [View Details](#)

DTMF Signaling Method*

3.配置TLS和SRTP密码

- 注意：** Unity Connection和Cisco Unified Communications Manager之间的协商取决于TLS密码配置，具有以下条件：当Unity Connection用作服务器时，TLS密码协商基于Cisco Unified CM选择的首选项。在协商基于ECDSA的密码时，SSL握手中使用基于EC密钥的tomcat-ECDSA证书。在协商基于RSA的密码时，SSL握手中使用基于RSA密钥的tomcat证书。当Unity Connection用作客户端时，TLS密码协商基于Unity Connection选择的首选项。

导航至Cisco Unified CM > Systems > Enterprise Parameters，然后从下拉列表中选择适当的密码选项TLS和SRTP密码。

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

导航至Cisco Unified Serviceability页面、Tools > Control Center-Feature Services并在CM Services下选择Cisco Call Manager，重新启动每个节点上的Cisco Call Manager服务

导航至Cisco Unity Connection Administration页面> System Settings > General Configurations，然后从下拉列表中选择适当的密码选项TLS和SRTP密码。

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

导航至Cisco Unity Connection Serviceability > Tools > Service Management，在每个节点上重新启动Connection Conversation Manager。

优先级顺序的TLS密码选项

TLS密码选项

仅最强 — AES-256 SHA-384:RSA首选

仅最强 — AES-256 SHA-384:首选ECDSA

仅中型AES-256 AES-128:RSA首选

按优先级顺序的TLS密码

- TLS_ECDHE_RSA_WITH_AES_256_GCM_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

仅中型AES-256 AES-128:首选ECDSA

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- 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

所有密码RSA首选 (默认)

- 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_RSA_WITH_AES_256_GCM_SHA384

首选所有密码ECDSA

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

按优先级顺序的SRTP密码选项

SRTP密码选项

按优先级顺序排列的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

所有支持的AES-256、AES-128密码

AEAD AES-256、AES-128基于GCM的密码

仅AEAD AES256基于GCM的密码

4.上传CUC Tomcat证书 (基于RSA和EC)

导航到OS Administration > Security > Certificate Management , 并将两个CUC Tomcat证书 (基于RSA和EC) 上传到CallManager信任存储中。

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload 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：如果仅协商ECDSA密码，则不必上载两个Unity Tomcat证书。在这种情况下，基于EC的Tomcat证书已足够。

如果有第三方证书，您必须上传第三方证书颁发机构的根证书和中间证书。仅当第三方CA为您的Unity Tomcat证书签名时，才需要此设置。

Upload Certificate/Certificate chain

Certificate Purpose* CallManager-trust

Description(friendly name)

Upload File Choose File CA_root_-_4096_key.crt

Upload Close

在所有节点上重新启动Cisco Call Manager进程以应用更改。

5.创建路由模式

通过导航至Call Routing > Route/Hunt > Route Pattern，配置指向已配置中继的路由模式。输入为路由模式号码的分机可用作语音邮件引导。

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.创建语音邮件引导、语音邮件配置文件并将其分配给DN

通过转至Advanced Features > Voice Mail > Voice Mail Pilot为集成创建语音邮件引导。

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

创建语音邮件配置文件，以将所有设置链接到Advanced Features > Voice Mail > Voice Mail Profile

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	

通过转到呼叫路由(Call Routing)>目录号码(Directory number)，将新创建的语音邮件配置文件分配给旨在使用安全集成的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对基于EC密钥的证书进行签名 (可选)

证书可能由第三方CA签名，然后再设置系统之间的安全集成。按照以下步骤在两个系统上签名证书。

Cisco Unity Connection

1. 为CUC Tomcat-ECDSA生成证书签名请求(CSR)，并且由第三方CA签名
2. CA提供身份证书 (CA签名证书) 和CA证书 (CA根证书)，必须按如下方式上传：
 - 将CA根证书上传到tomcat-trust存储
 - 将身份证书上传到tomcat-EDCS存储
3. 在CUC上重新启动对话管理器

Cisco Unified CM

1. 为CUCM CallManager-ECDSA生成CSR，并且由第三方CA签名
2. CA提供身份证书 (CA签名证书) 和CA证书 (CA根证书)，必须按如下方式上传：
 - 将CA根证书上传到callmanager-trust存储
 - 将身份证书上传到callmanager-EDCS存储
3. 在每个节点上重新启动Cisco CCM和TFTP服务

同一过程将用于对基于RSA密钥的证书进行签名，其中CSR为CUC Tomcat证书和CallManager证书生成，并分别上传到tomcat存储和callmanager存储。

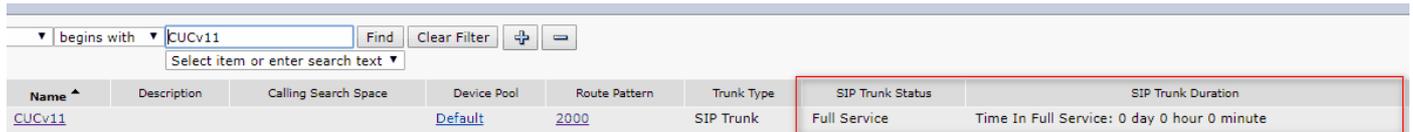
验证

使用本部分可确认配置能否正常运行。

安全SIP中继验证

按电话上的“语音邮件”按钮以呼叫语音邮件。如果Unity Connection系统上未配置用户分机，您应该听到开场问候语。

或者，您可以启用SIP OPTIONS keepalive以监控SIP中继状态。此选项可在分配给SIP中继的SIP配置文件中启用。启用此功能后，您可以通过Device > Trunk监控Sip中继状态，如下所示：



The screenshot shows a table with columns: Name, Description, Calling Search Space, Device Pool, Route Pattern, Trunk Type, SIP Trunk Status, and SIP Trunk Duration. The row for CUCv11 is highlighted with a red border. The SIP Trunk Status is 'Full Service' and the SIP Trunk Duration is 'Time In Full Service: 0 day 0 hour 0 minute'.

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呼叫验证

验证Unity Connection的呼叫中是否存在挂锁图标。这意味着RTP流已加密（设备安全配置文件必须是安全的，才能正常工作），如此图所示



相关信息

- [Cisco Unity Connection版本11.x的SIP集成指南](#)