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

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

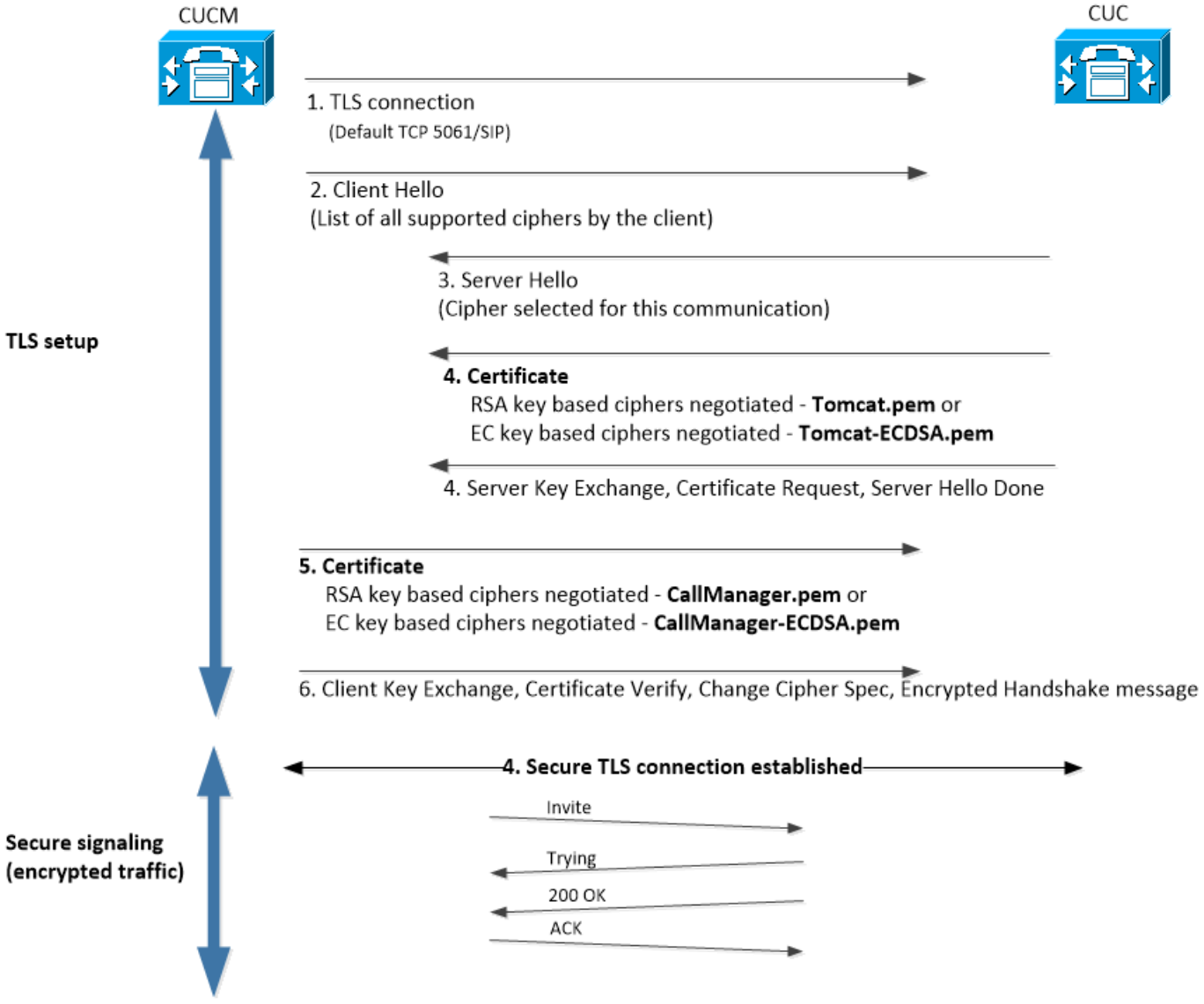
本文档中的信息基于以下软件和硬件版本：

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
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 CallMa
CallManager.pem（CA签名）	Tomcat.pem（自签名）	要上传到CUCM > CallManger-trust的Tomcat.pem	要上传和中间
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。

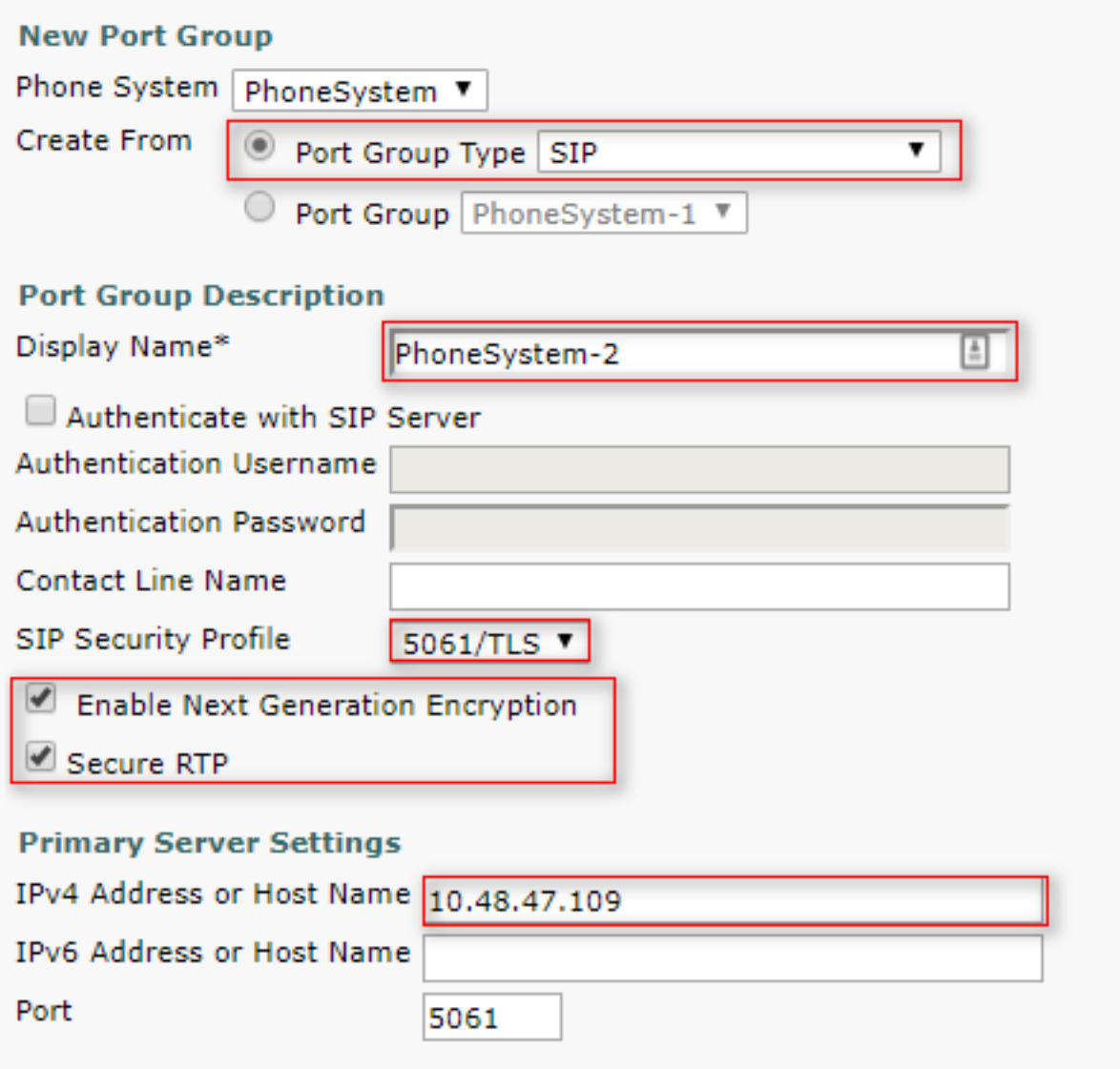
*2 CUCM根和中间CA证书是指签署CUCM CallManager证书(CallManager-ECDSA.pem)的CA证书。

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

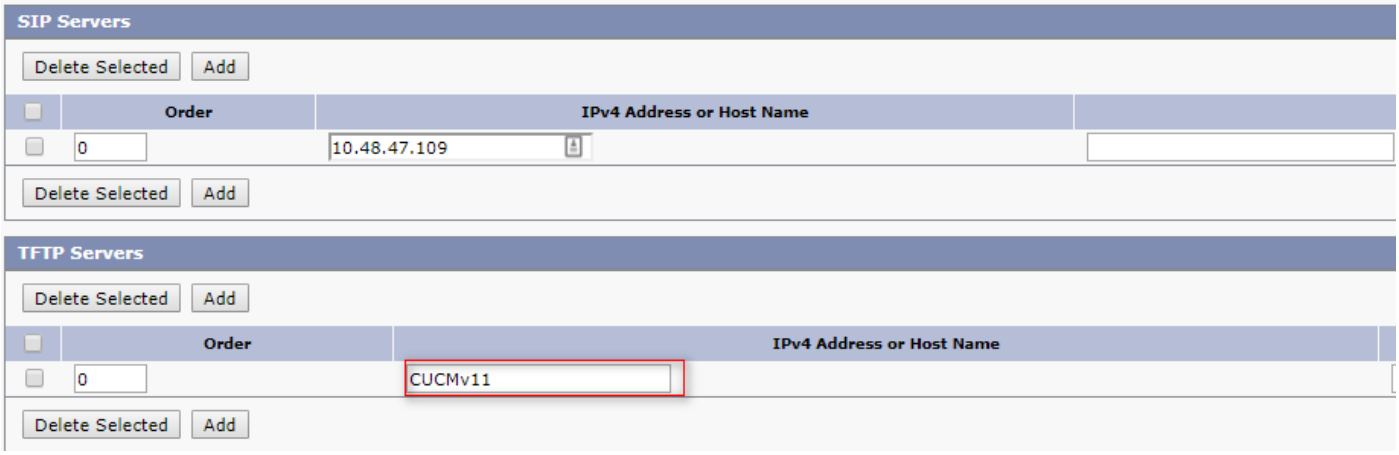
导航至Cisco Unity Connection Administration页面> Telephony integration > Port group，然后点击Add New。确保选中启用下一代加密复选框。



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

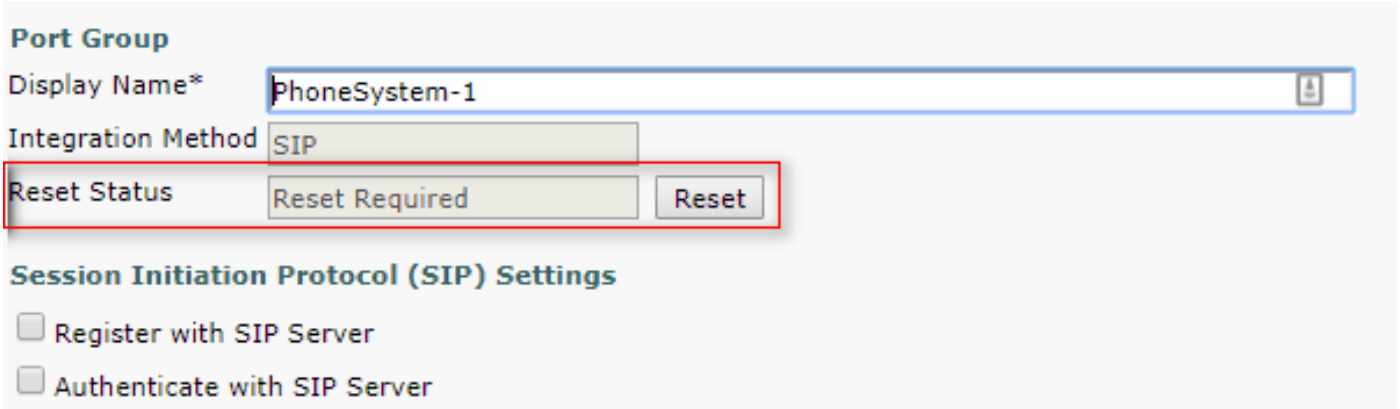
在Port Group Basics页面，导航至Edit > Servers，然后添加CUCM集群的TFTP服务器的FQDN。TFTP服务器的FQDN/主机名必须与CallManager证书的公用名(CN)匹配。服务器的IP地址将无法工作，并且会导致无法下载ITL文件。因此，DNS名称必须可通过配置的DNS服务器解析。



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。



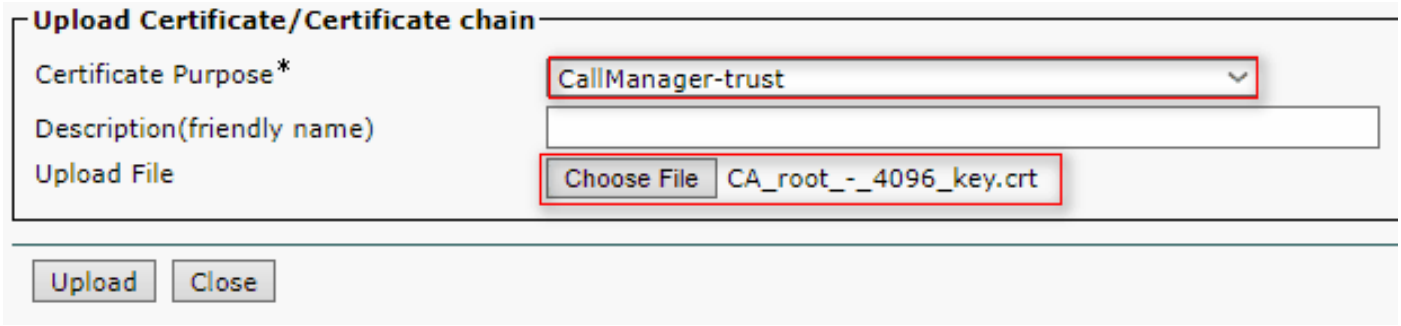
1. **注意**：每次重置端口组时，CUC服务器将通过连接到CUCM服务器更新其本地存储的ITL文件。

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。

4.上传第三方CA的CUCM根和中间证书

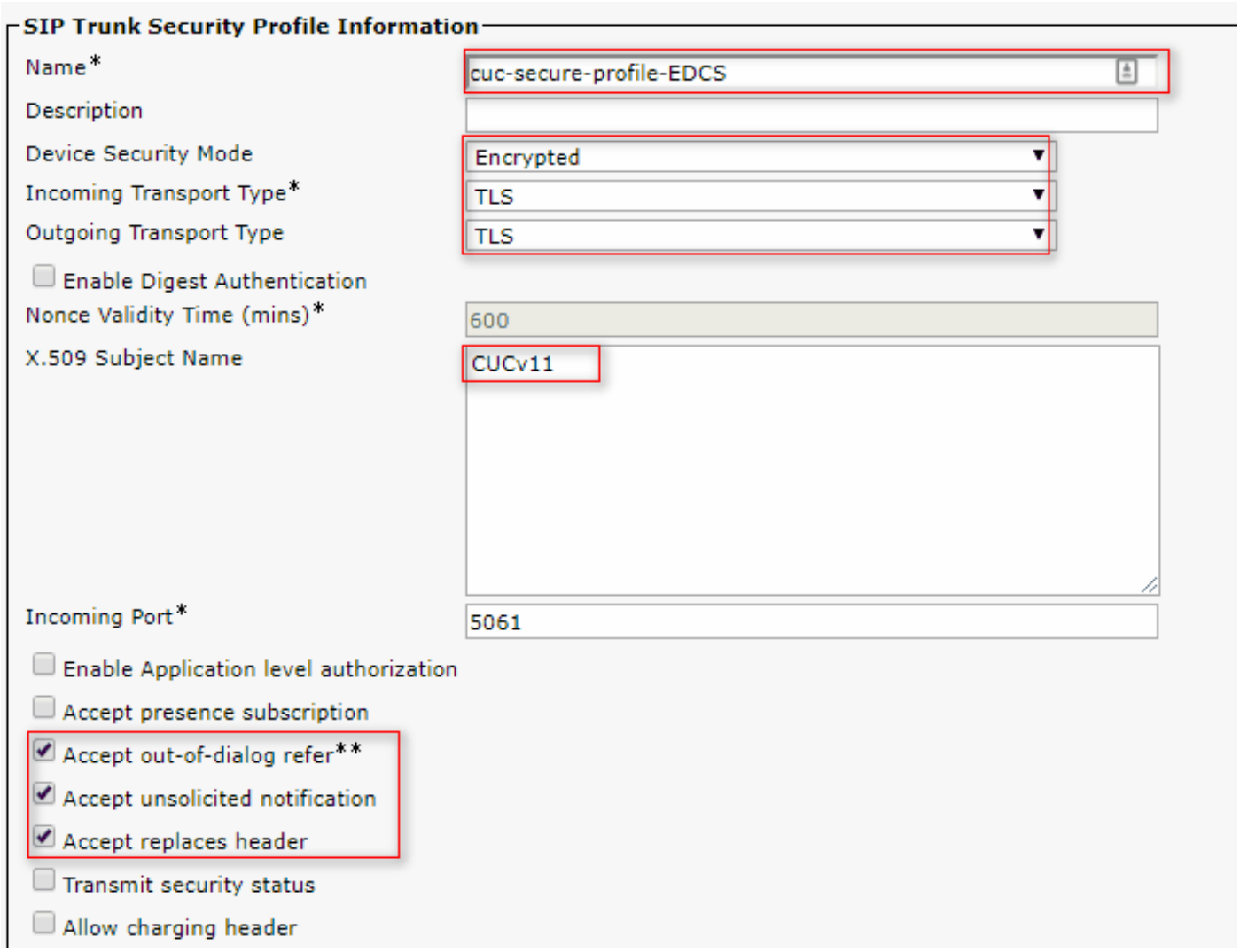
如果是第三方证书，则必须在Unity Connection的CallManager信任上上传第三方证书颁发机构的根证书和中间证书。仅当第3方CA为Call Manager证书签名时，才需要此设置。导航至Cisco Unified OS Administration > Security > Certificate Management，然后点击Upload Certificate，执行此操作。



配置 — Cisco Unified CM(CUCM)

1.创建SIP中继安全配置文件

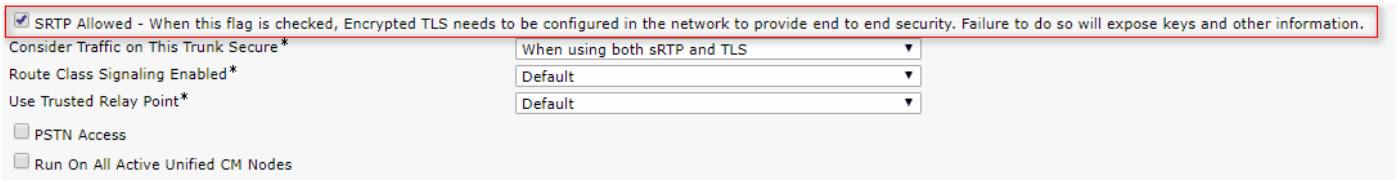
导航至CUCM管理>System >安全> SIP中继安全配置文件并添加新配置文件。X.509主题名称必须与CUC服务器的FQDN匹配。

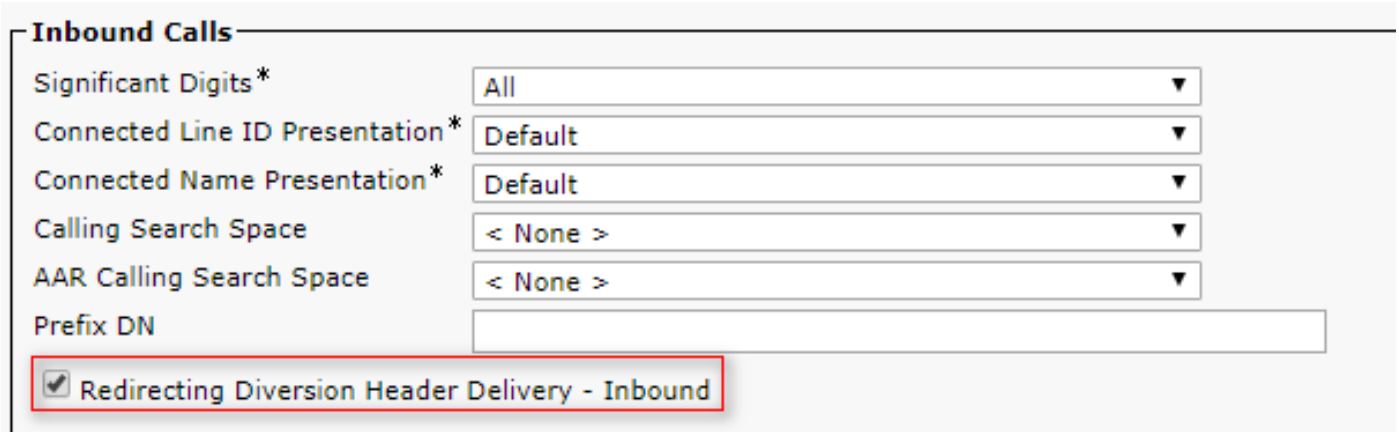


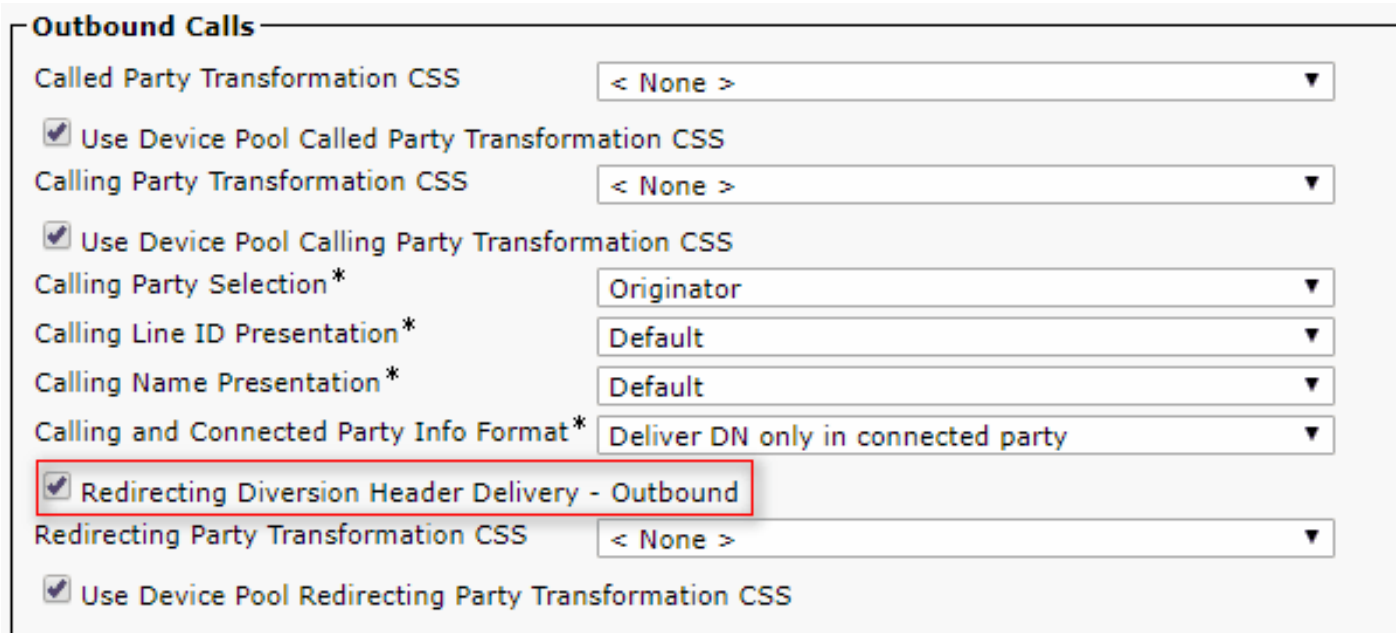
1. **注意**：CLI命令“show cert own tomcat/tomcat.pem”可在Unity Connection上显示基于RSA密钥的tomcat证书。CN必须与CUCM上配置的X.509主题名称匹配。CN等于Unity服务器的FQDN/主机名。基于EC密钥的证书在其使用者备用名称(SAN)字段中包含FQDN/主机名。

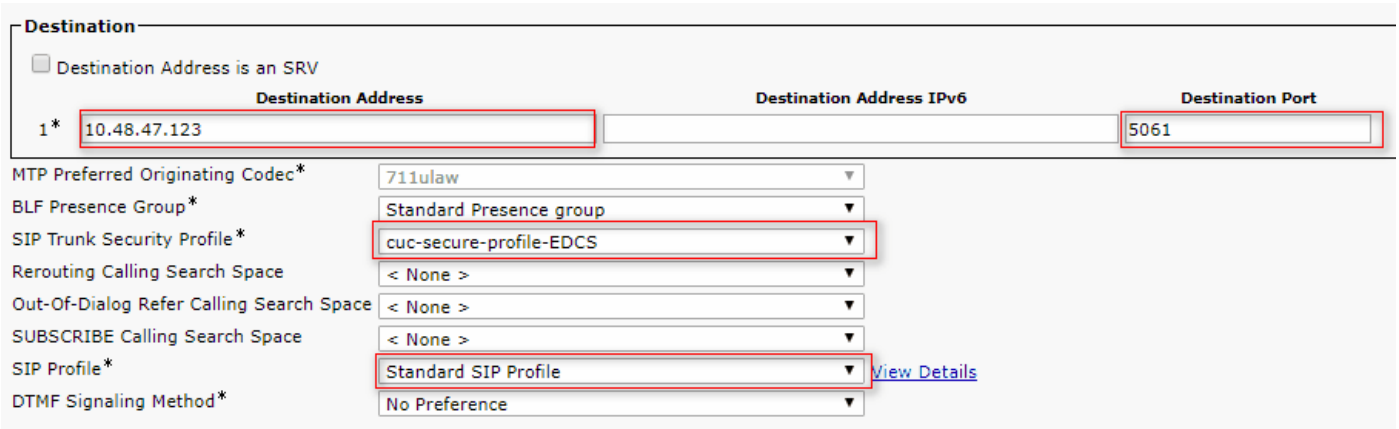
2.创建安全SIP中继

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。





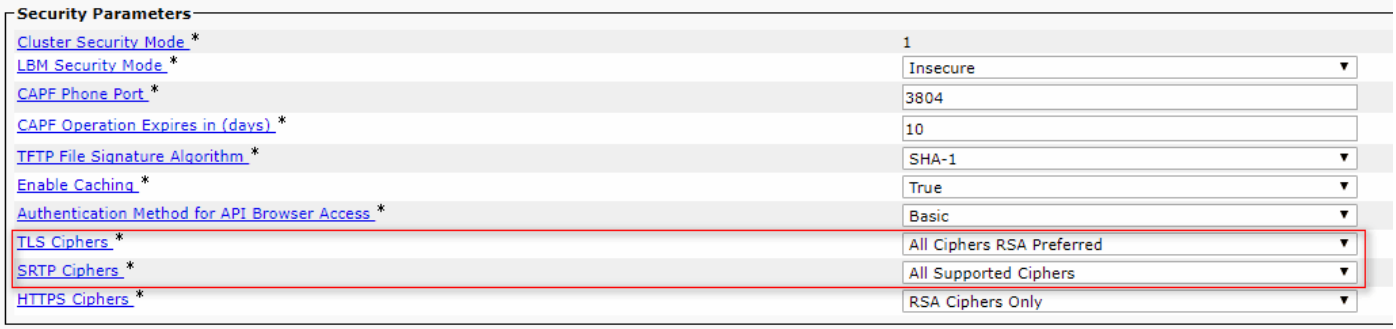




3.配置TLS和SRTP密码

1. **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。



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。

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	按优先级顺序的TLS密码
仅最强 — AES-256 SHA-384:RSA首选	• 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
仅最强 — AES-256 SHA-384:首选ECDSA	• 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:RSA首选	

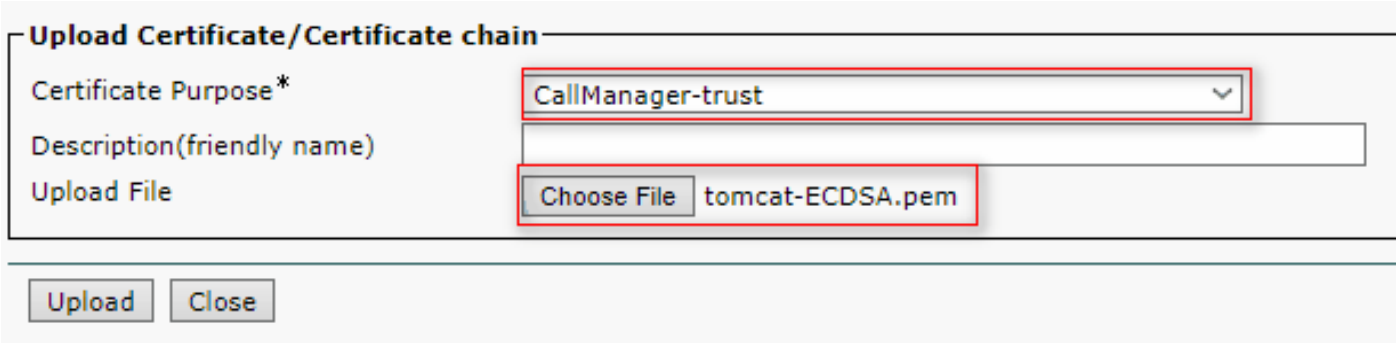
仅中型AES-256 AES-128:首选ECDSA	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
所有密码RSA首选（默认）	• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • 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

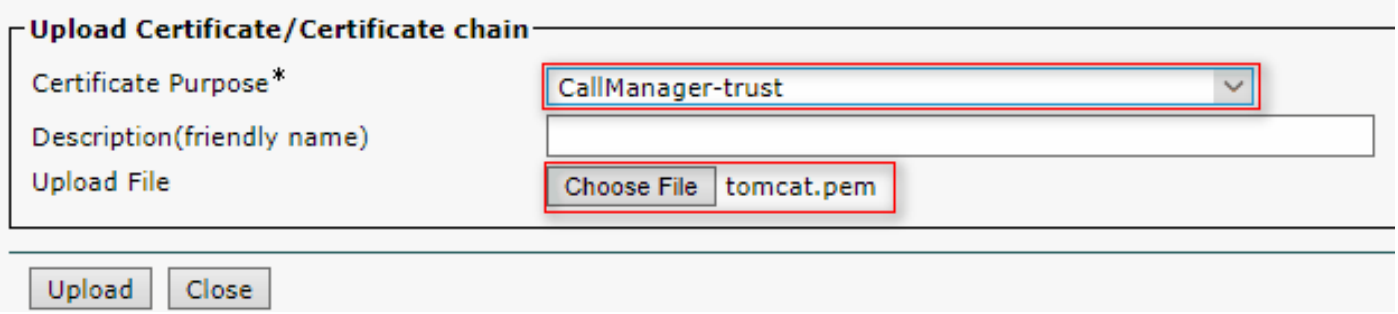
按优先级顺序的SRTP密码选项

SRTP密码选项	按优先级顺序排列的SRTP
所有支持的AES-256、AES-128密码	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1_32
AEAD AES-256、AES-28基于GCM的密码	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
仅AEAD AES256基于GCM的密码	• AEAD_AES_256_GCM

4.上传CUC Tomcat证书（基于RSA和EC）

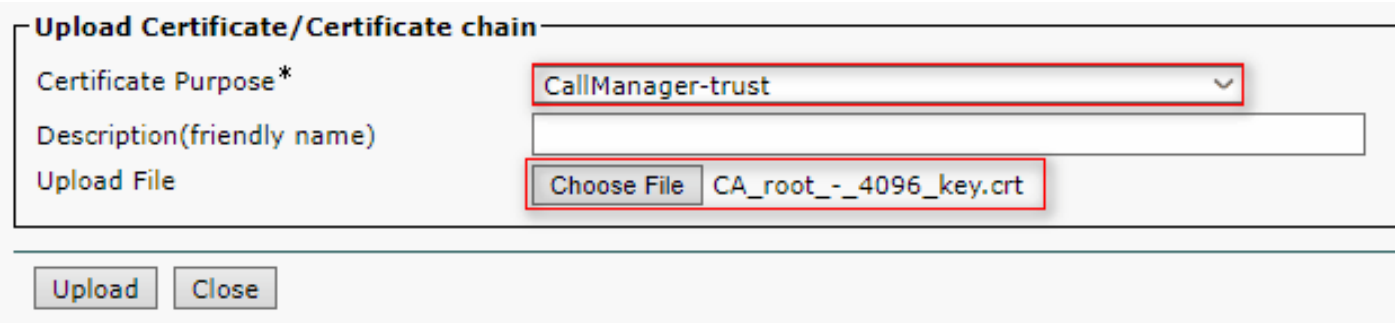
导航到OS Administration > Security > Certificate Management，并将两个CUC Tomcat证书（基于RSA和EC）上传到CallManager信任存储中。





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。

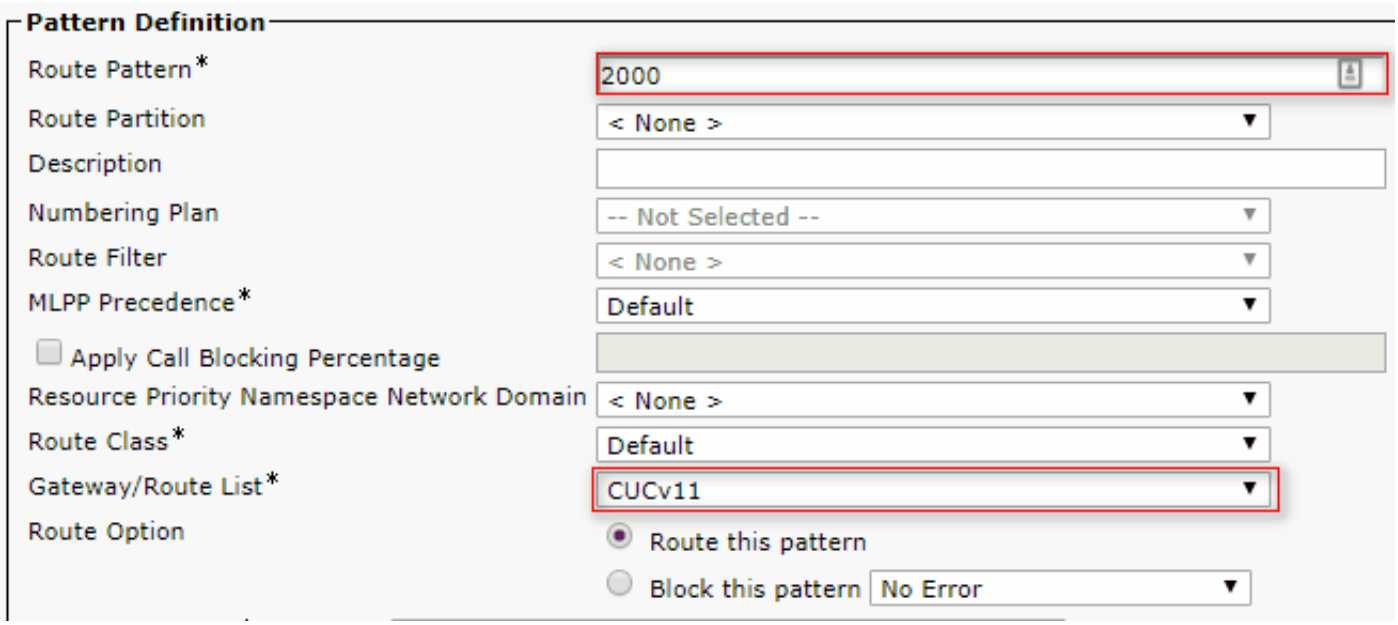
如果有第三方证书，您必须上传第三方证书颁发机构的根证书和中间证书。仅当第三方CA为您的Unity Tomcat证书签名时，才需要此设置。



在所有节点上重新启动Cisco Call Manager进程以应用更改。

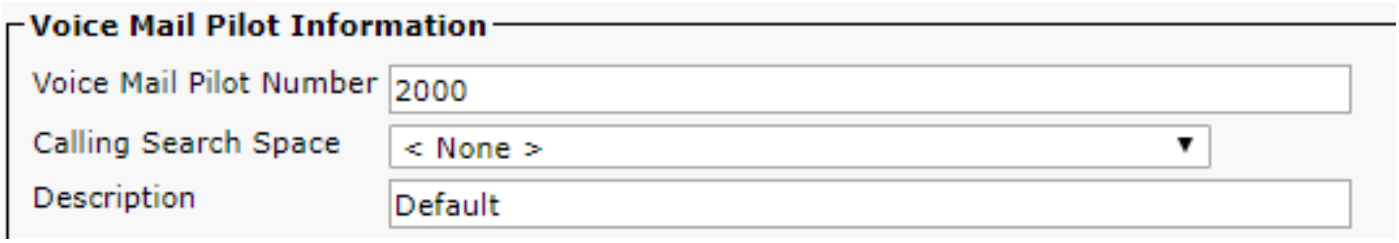
5.创建路由模式

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。

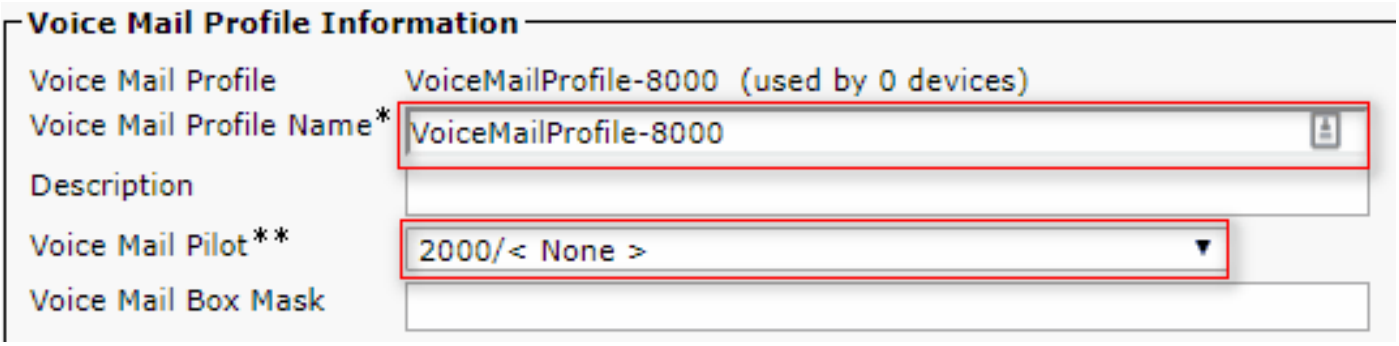


6.创建语音邮件引导、语音邮件配置文件并将其分配给DN

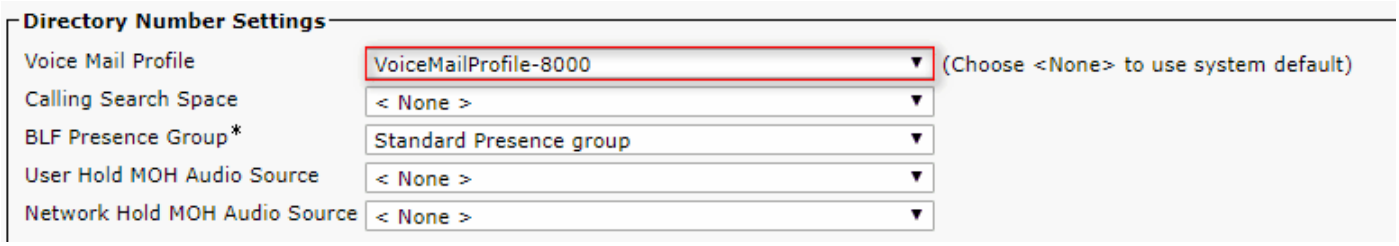
通过转至Advanced Features > Voice Mail > Voice Mail Pilot为集成创建语音邮件引导。



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



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



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。

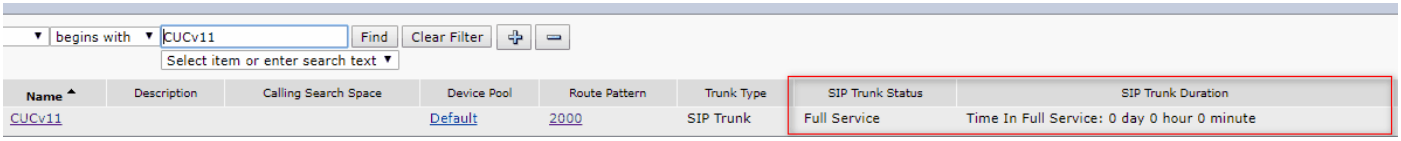
验证

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：



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