Secure SIP集成的配置示例在根据下一代加密和CUC之间的CUCM (NGE)

目录

简介

本文描述安全SIP连接的配置和验证Cisco Unified Communications管理器(CUCM)和Cisco Unity Connection (CUC)使用下一代加密，服务器之间的。

在SIP接口的下一代安全性限制SIP接口使用根据TLS 1.2， SHA-2和AES256协议的套件B密码器。它允许根据RSA或ECDSA密码器优先级定货的密码器的多种组合。在Unity Connection和Cisco Unified CM之间的通信时，密码器和第三方证书验证在两个末端。下面下一代加密支持的配置。

如果计划使用第三方证书颁发机构签字的然后证书从签字在配置部分结束时的证书开始(请配置-签署EC密钥基于证书由第三方CA)

先决条件

要求

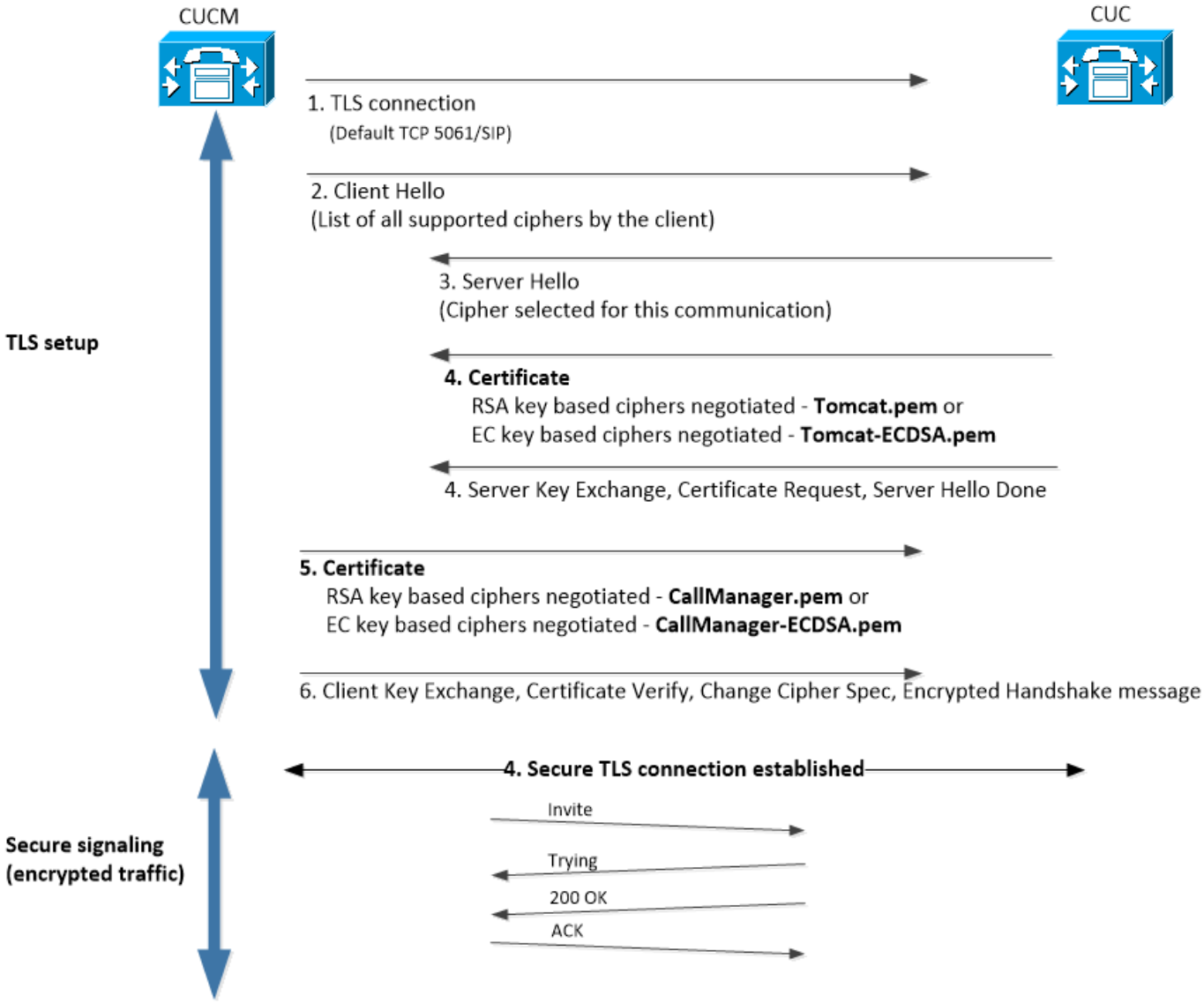
本文档中的信息基于以下软件和硬件版本：

在混合模式的CUCM版本11.x和以上
CUC版本11.x和以上

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

此图表简要地解释帮助建立CUCM之间的一个安全连接，并且CUC下一代加密支持一次启用的进程：



证书需求

一旦下一代加密支持在Cisco Unity Connection，启用这些是证书交换需求。

使用的自签名证书：

- Unity Connection
  没有需要上传任何证书。Unity Connection服务器将自动地下载从在配置和信任指定的TFTP server的ITLfile CallManager.pem期间& CallManagerEC.pem在TLS协商时。

- Cisco Unified CM
  您必须上传Unity连接的Tomcat.pem & TomcatEC.pem到CUCM的CallManager托拉斯存储

使用的第三方CA证书：

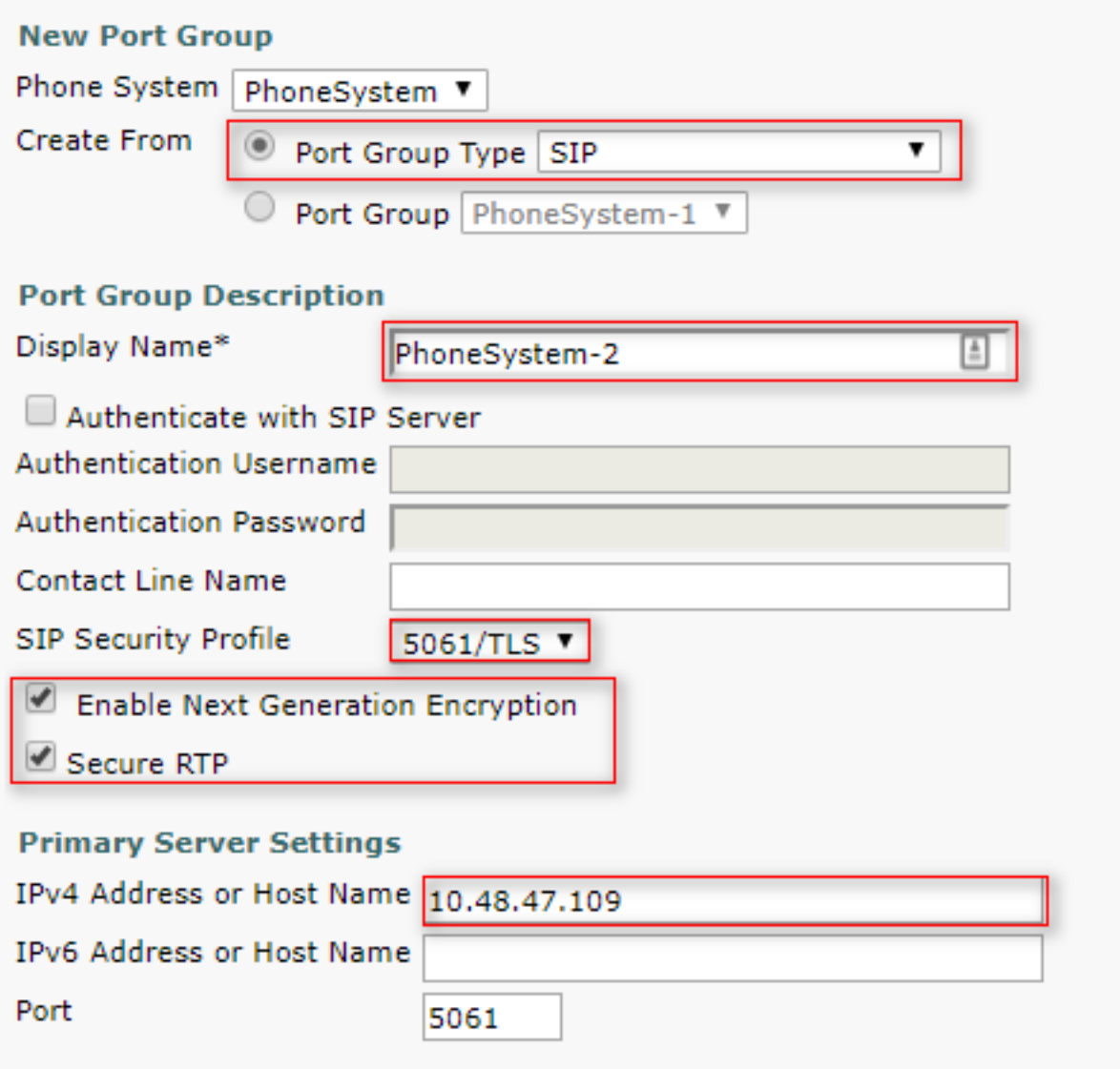
- Unity Connection
  您必须上传根和第三方证书颁发机构的所有半成品证书Unity Connection CallManager托拉斯的。在那顶部，
  连接服务器将自动地下载从在配置和信任指定的TFTP server的ITLfile CallManager.pem期间& CallManagerEC.pem在TLS协商时。

- Cisco Unified CM
  您必须上传根和第三方证书颁发机构的所有半成品证书Unified CM CallManager托拉斯的。

配置- Cisco Unity Connection (CUC)

1. 添加新的端口组

导航给Cisco Unity Connection管理页>电话集成>端口组并且点击新建的Add。确保检查Enable (event)下一代加密复选框。



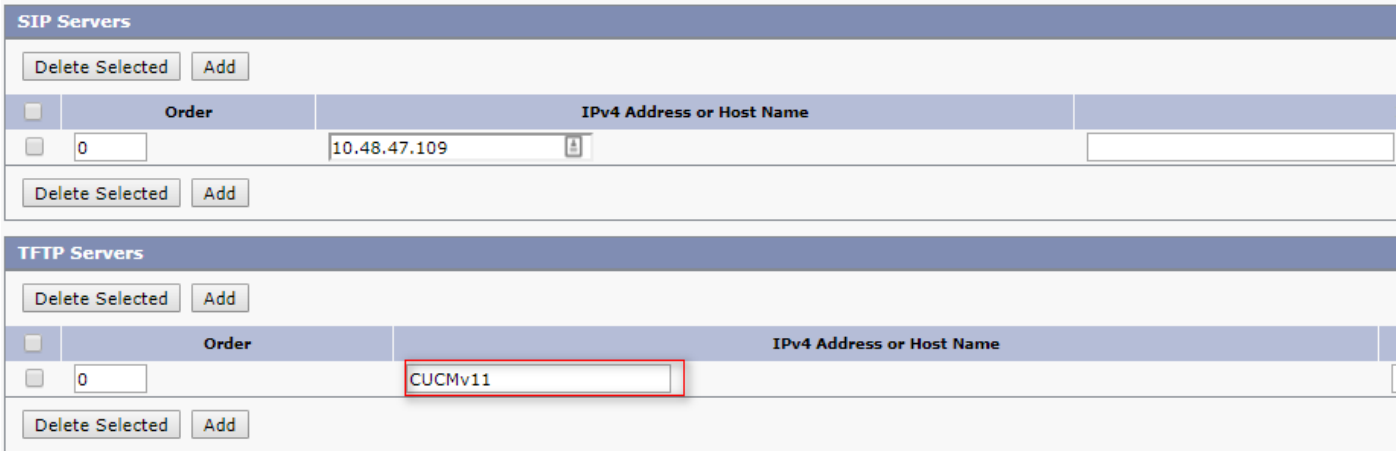
1. **Note**:一旦Enable (event)下一代加密复选框启用， Unity连接的思科Tomcat证书将使用在SSL握手期间。

•万一ECDSA基于密码器是然后协商的EC关键基于Tomcat ECDSA证书用于SSL握手。

•万一RSA基于密码器是然后协商的RSA密钥基于Tomcat证书用于SSL握手。

2. 添加TFTP server参考

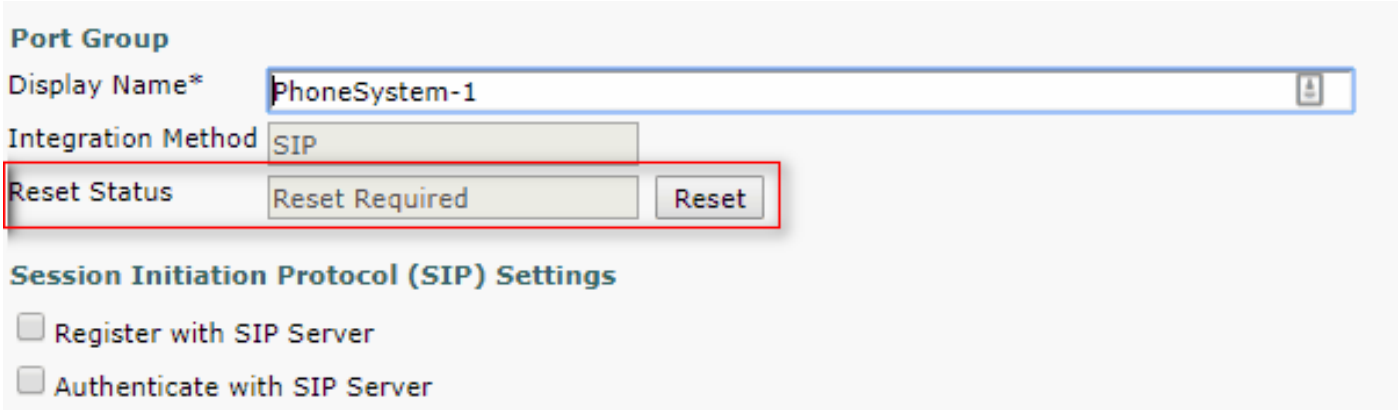
在端口组基础页，请导航编辑>服务器和添加您的CUCM集群TFTP server FQDN。TFTP server的FQDN/主机名必须匹配CallManager证书共同名称(CN)。服务器的IP地址不会工作，并且将导致失败下载ITL文件。因此DNS名一定是可解决通过已配置的DNS服务器。



通过导航重新启动连接每个节点的会话管理器对Cisco Unity Connection维护性> Tools > Service管理。这对于配置是必需生效。

1. **Note**:Unity Connection下载ITL文件(ITLfile.tlv)从CUCM的TFTP使用在安全6972端口(URL的https协议： https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv)。因为CUC寻找“CCM+TFTP”功能证书从ITL文件， CUCM必须在混合模式。

导航回到电话集成>端口组>端口组基础配置页并且重置您新加的端口组。



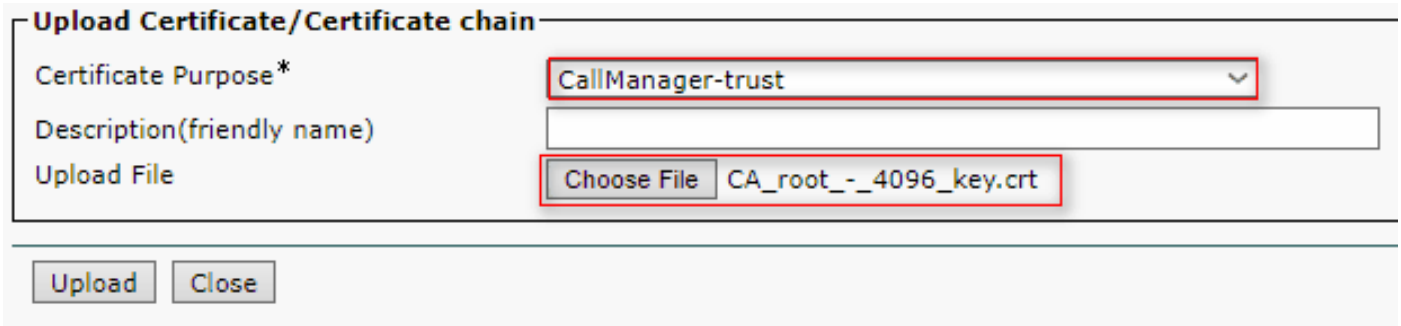
1. **Note**:在端口组重置时候， CUC服务器将通过连接对CUCM服务器更新其本地存储的ITL文件。

3. 添加语音邮件端口

导航回到电话集成>波尔特并且点击Add新建的添加端口到您新建立的端口组。

4. 上传CUCM第三方CA的根和中间证书

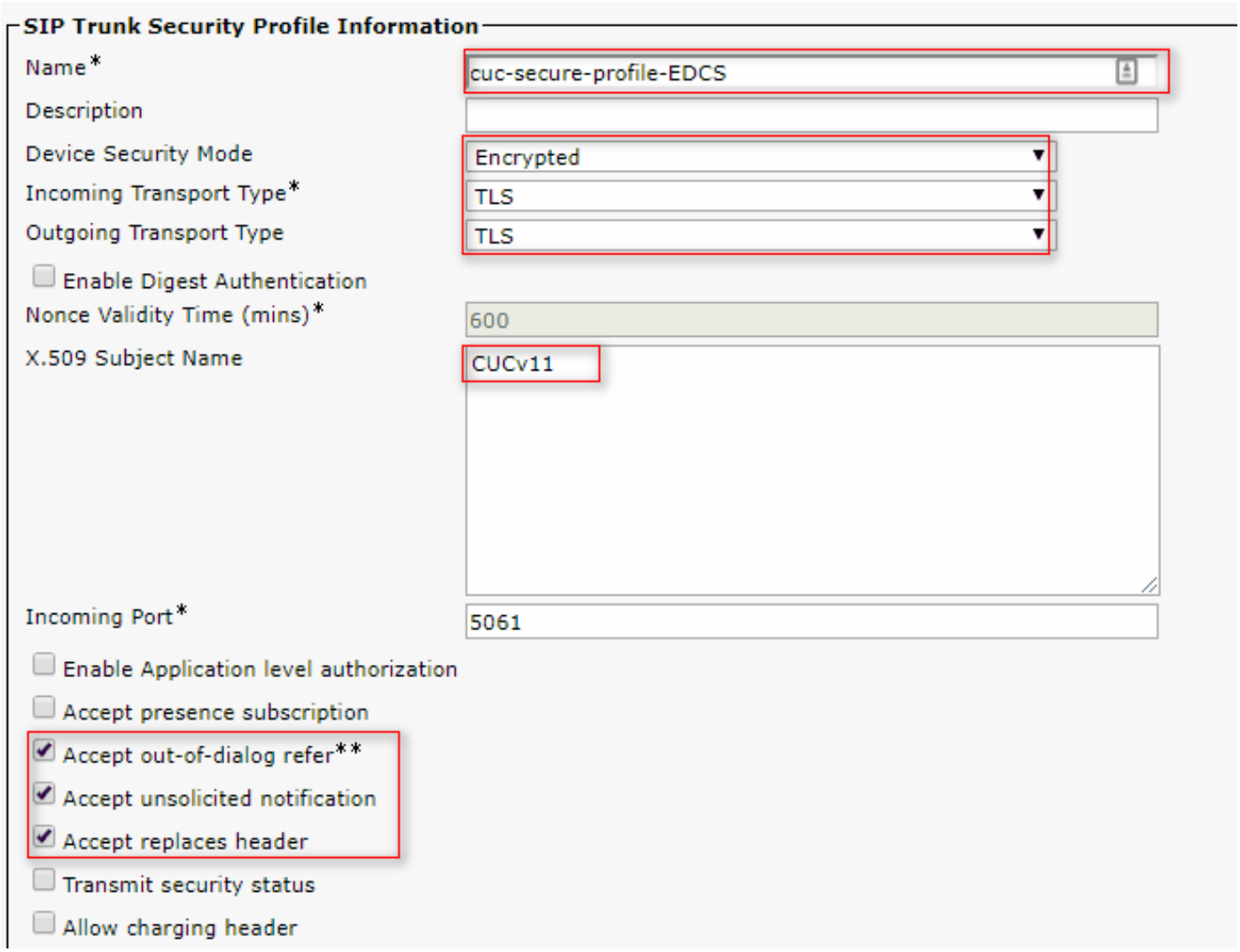
在第三方证书的情况下，您必须上传第三方证书颁发机构的根和中间证书Unity Connection CallManager托拉斯的。只有当第三方CA签署了您的CallManager证书，这必要。通过导航进行此操作对Cisco Unified OS管理> Security > Certificate Management并且点击加载证书。



配置- Cisco Unified CM (CUCM)

1. 创建SIP中继安全配置文件

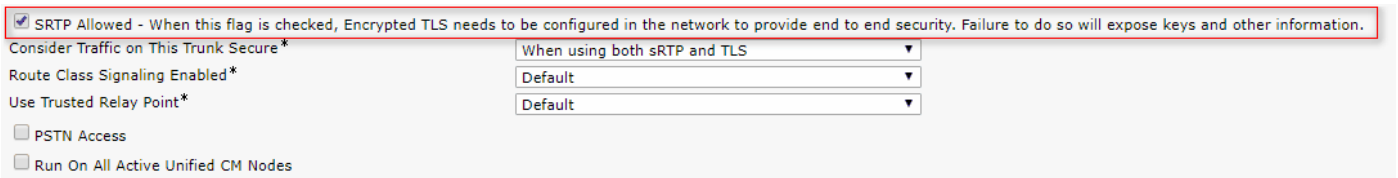
导航对CUCM管理>System > Security > SIP中继安全配置文件并且添加新配置文件。 X.509主题名称必须匹配CUC服务器的FQDN。

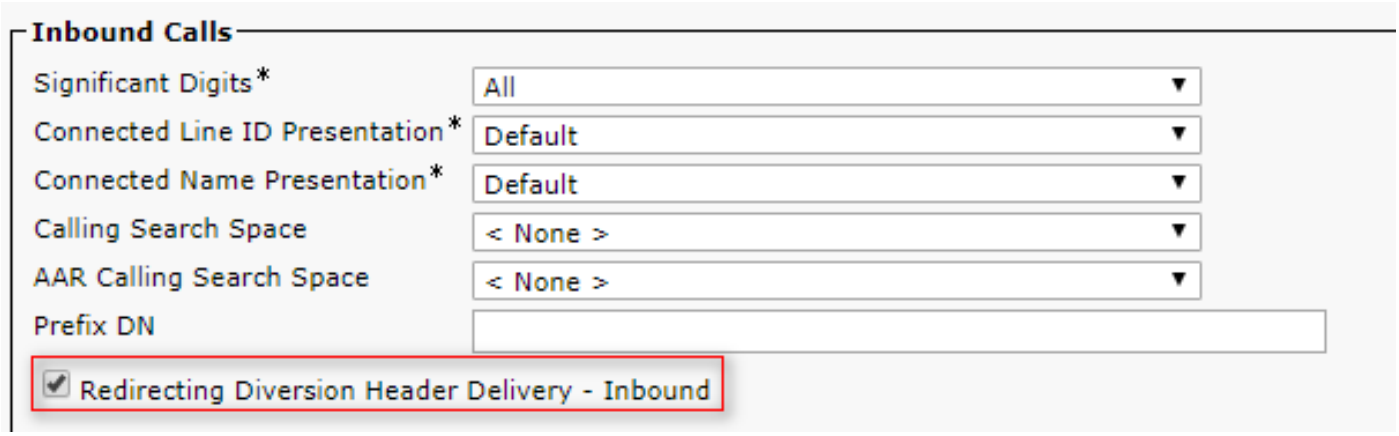


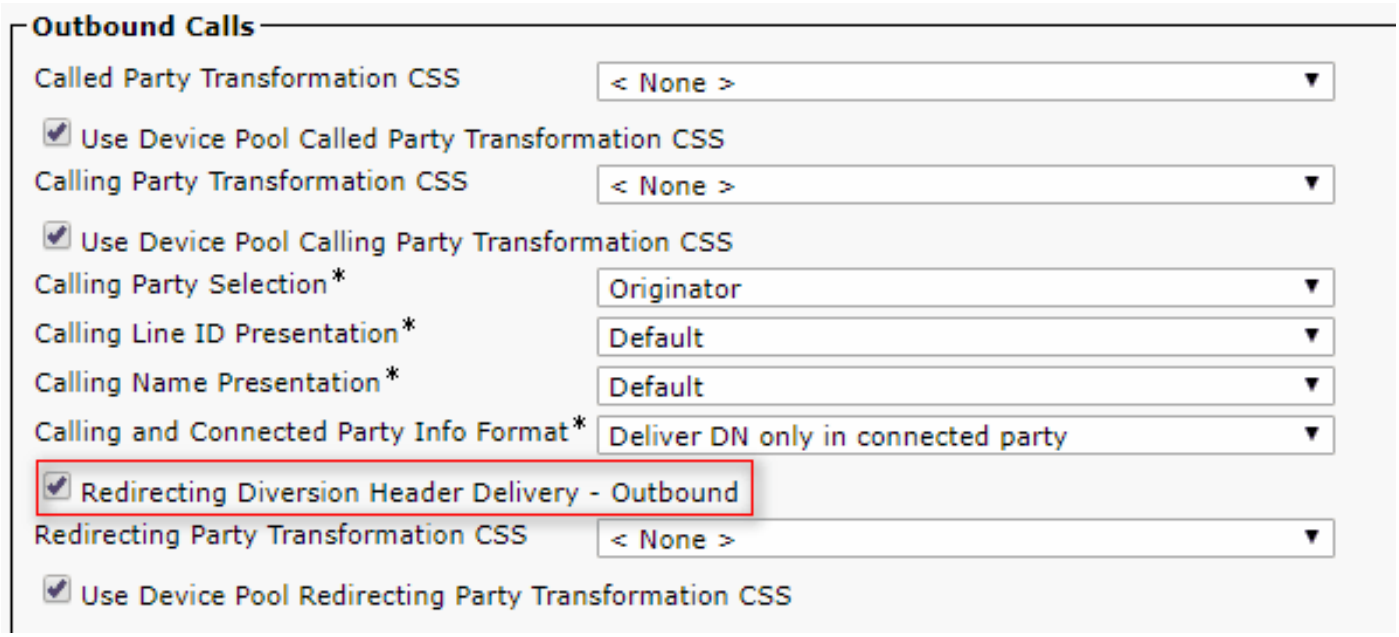
1. **Note**: CLI命令“请显示cert拥有Tomcat/tomcat.pem”能显示在Unity Connection的RSA密钥基于Tomcat证书。它是CN必须匹配在CUCM配置的X.509主题名称。CN与Unity服务器的FQDN/主机名是相等的。EC密钥基于证书在其附属的替代名称(SAN)字段包含FQDN/hostname -。

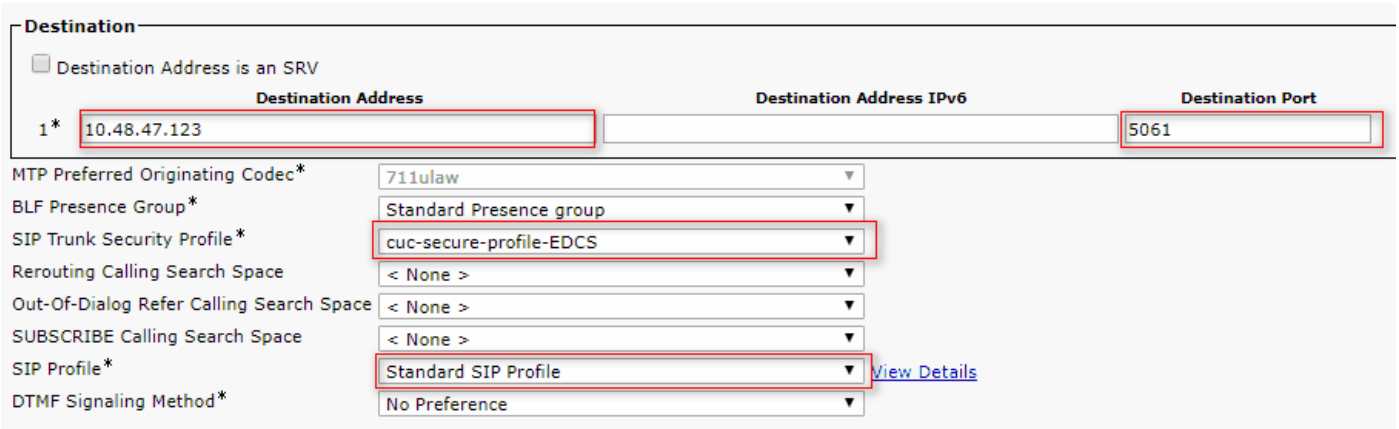
2. 创建安全SIP中继

导航到设备>中继>点击并且添加新并且创建将使用安全集成与Unity Connection的标准SIP中继。





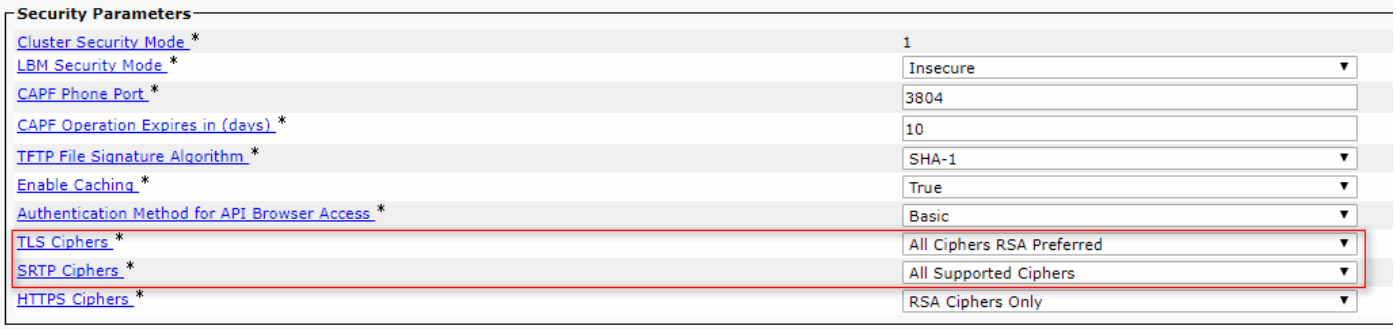




3. 配置TLS和SRTP密码器

1. **Note**：在Unity Connection和Cisco Unified Communications Manager之间的协商取决于TLS密码器配置以以下条件： 当Unity Connection作为服务器时， TLS密码器协商根据Cisco Unified CM选择的首选。万一ECDSA基于密码器是然后协商的EC关键基于Tomcat ECDSA证书用于SSL握手。万一RSA基于密码器是然后协商的RSA密钥基于Tomcat证书用于SSL握手。当Unity Connection作为客户端时， TLS密码器协商根据Unity Connection选择的首选。

导航对Cisco Unified CM >系统>企业参数并且选择从TLS和SRTP密码器的适当的密码器选项从下拉列表。



通过导航重新启动在每个节点的Cisco Call Manager服务对Cisco Unified维护性页 ， Tools>控制中心功能服务并且选择Cisco Call Manager在CM服务下

导航对Cisco Unity Connection管理页>System设置>General配置并且选择从TLS和SRTP密码器的适当的密码器选项从下拉列表。

通过导航重新启动连接每个节点的会话管理器对Cisco Unity Connection维护性> Tools > Service管理。

TLS与优先级顺序的密码器选项

TLS密码器选项	在优先级命令的TLS密码器
仅最严格的AES-256 SHA-384 ：首选的RSA	• TLS_ECDHE_RSA_WITH_AES_256_GC M_SHA38 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384
Strongest-AES-256仅SHA-384 ：首选的ECDSA	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA 84 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Medium-AES-256仅AES-128 ：首选的RSA	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM _SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Medium-AES-256仅AES-128 ：首选的ECDSA	• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA 56 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA

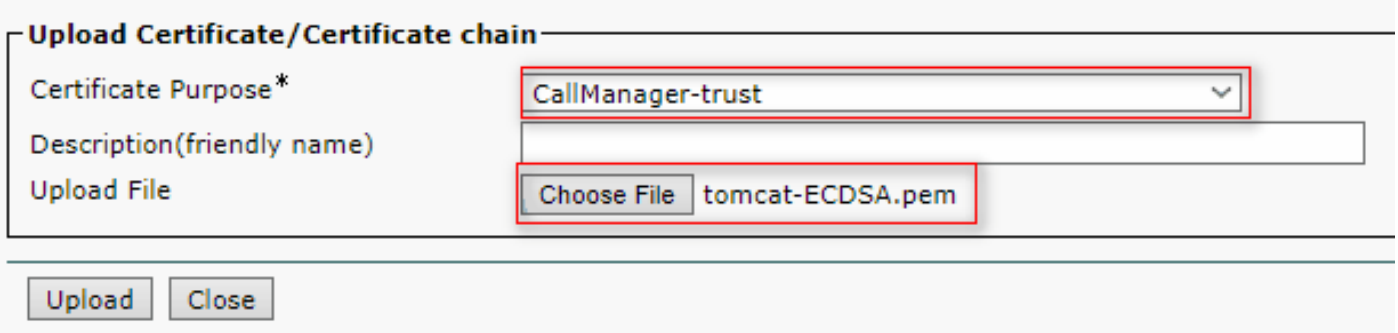
首选的所有密码器RSA (默认)	84 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA
ECDSA首选的所有密码器	• 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_RSA_WITH_AES_128_CBC_SHA

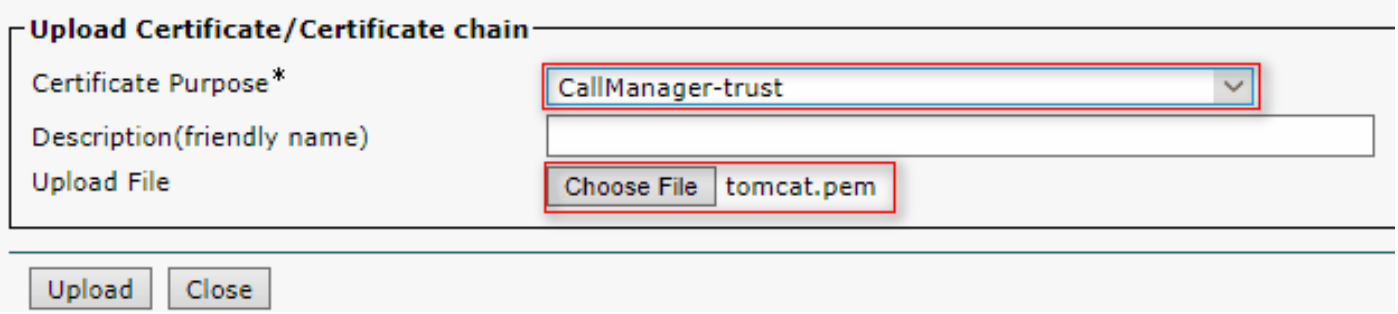
SRTP密码器选项按优先级顺序

SRTP密码器选项	在优先级命令的SRTP
所有支持AES-256， AES-128密码器	• AEAD_AES_256_GCM • AEAD_AES_128_GCM • AES_CM_128_HMAC_SHA1_32
AEAD AES-256， AES-28 GCM根据密码器	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
AEAD AES256 GCM根据仅密码器	• AEAD_AES_256_GCM

4. 加载CUC Tomcat证书(基于的RSA & EC)

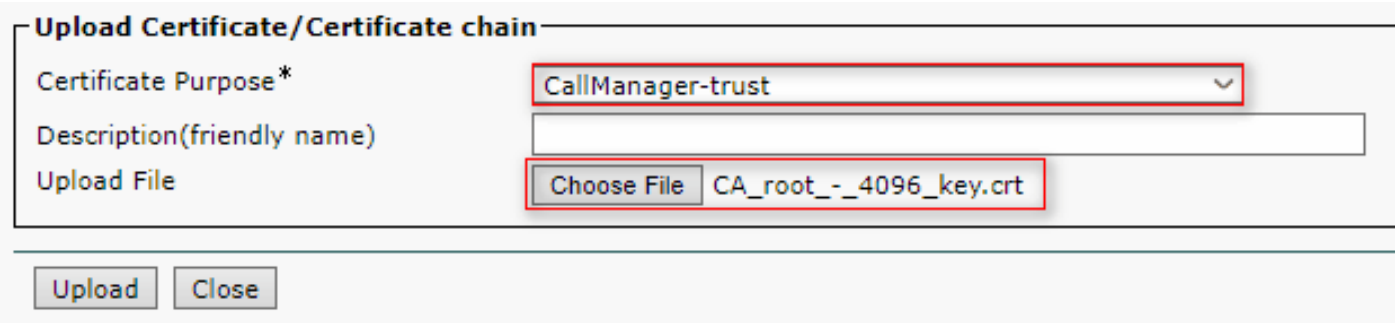
导航对OS管理> Security > Certificate Management并且上传两CUC Tomcat证书(基于的RSA & EC)到CallManager托拉斯存储。





1. **Note**: 如果ECDSA密码器只，协商上传两Unity Tomcat证书不是必须。在这样案件EC基于Tomcat证书是足够。

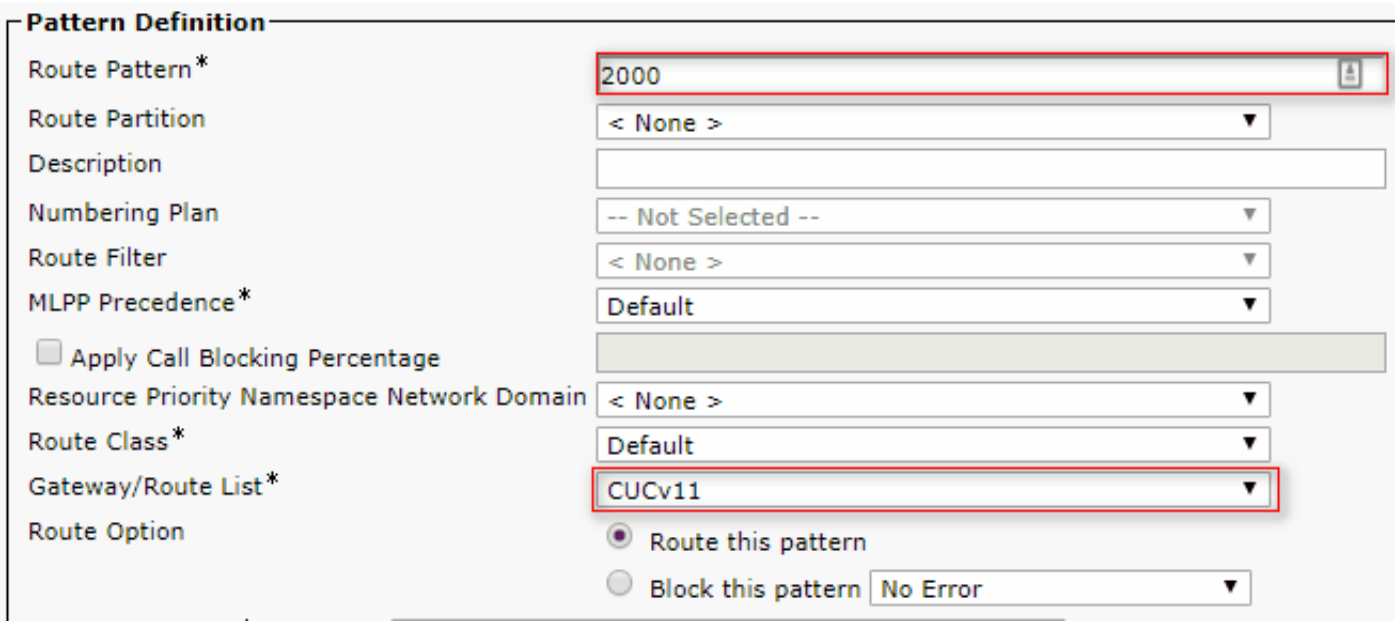
在第三方证书的情况下，您必须上传第三方证书颁发机构的根和中间证书。只有当第三方CA签署了您的Unity Tomcat证书，这必要。



重新启动在所有节点的Cisco Call Manager进程应用更改。

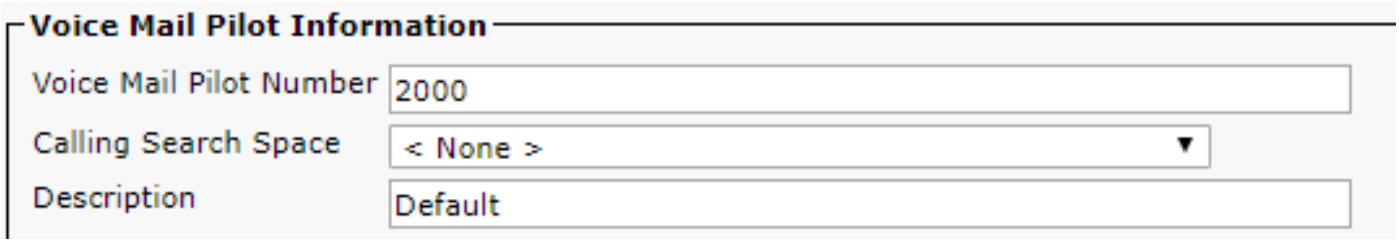
5. 创建路由模式

配置点到已配置的中继通过导航对呼叫路由>路由/寻线>路由模式的路由模式。作为路由模式编号被输入的扩展名可以使用作为语音邮件试验。

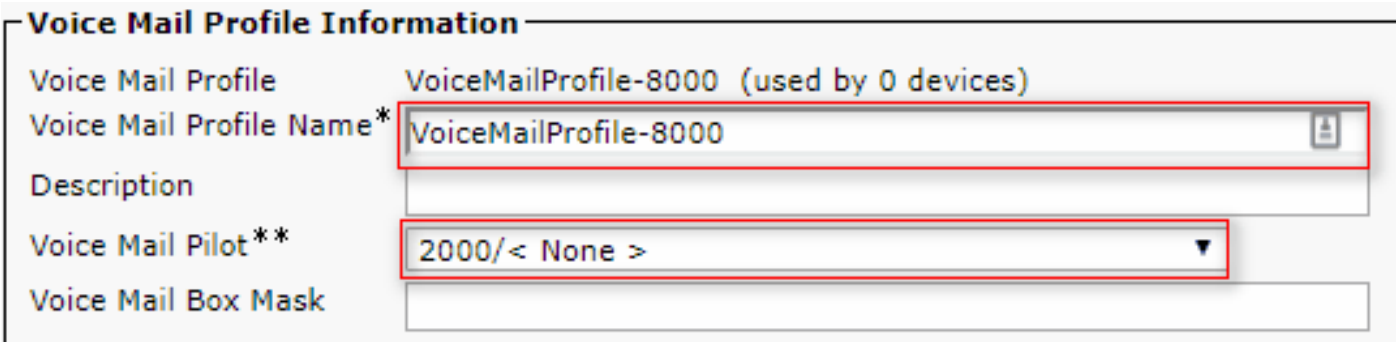


6. 创建语音邮件试验，语音邮件配置文件并且分配它到Dns

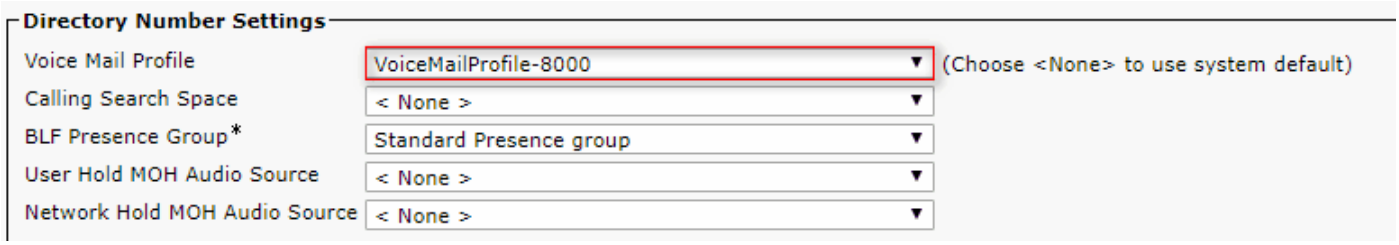
通过去创建集成的一语音邮件引导高级特性>Voice邮件>Voice邮件试验。



创建语音邮件配置文件为了一起连接所有设置高级特性>Voice邮件>Voice邮件配置文件



分配新建立的语音邮件配置文件到去打算的使用安全集成Dns呼叫路由>目录号



配置-签署EC密钥由第三方CA根据证书(可选)

证书也许由在设置安全集成前的第三方CA签字在系统之间。遵从以下步骤签署在两个系统的证书。

Cisco Unity Connection

1. 生成证书签名请求(CSR) CUC的Tomcat ECDSA并且安排证书签字由第三方CA
2. CA提供必须上传和跟随的身份证书(CA签名证书)和CA证书(CA根证明) ：
   上传CA根证明到Tomcat托拉斯存储
   上传身份证书到Tomcat EDCS存储
3. 重新启动CUC的会话管理器

Cisco Unified CM

1. 生成CUCM的CallManager ECDSA CSR并且安排证书签字由第三方CA
2. CA提供必须上传和跟随的身份证书(CA签名证书)和CA证书(CA根证明) ：
   上传CA根证明到CallManager托拉斯存储
   上传身份证书到CallManager EDCS存储
3. 重新启动思科在每个节点的CCM和TFTP服务

同一进程将用于签署RSA密钥CSR为CUC Tomcat证书和CallManager证书生成并且上传到Tomcat各自存储和CallManager存储的基于证书。

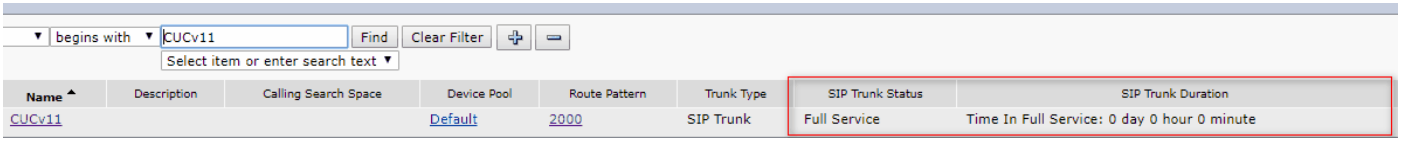
验证

使用本部分可确认配置能否正常运行。

获取SIP中继验证

按在电话的语音邮件按钮呼叫语音邮件。如果用户的分机在Unity Connection系统，没有配置您应该听到开始的问候。

或者，您能使SIP选项Keepalive监控SIP中继线状态。此选项在SIP配置文件可以启用分配到SIP中继。一旦这启用您能通过设备>中继监控Sip中继线状态如下所示：



安全RTP呼叫验证

验证挂锁图标是否是存在呼叫对Unity Connection。含义RTP数据流加密(设备安全性配置文件一定是安全为了它能工作)如此镜像所显示，

相关信息

- [Cisco Unity Connection版本的11.x SIP集成指南]