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

Contents

Introduction

本文描述安全的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。

下一代安全性在SIP接口的限制SIP接口使用根据TLS 1.2， SHA-2和AES256协议的套件B密码。它允许根据RSA或ECDSA密码优先级顺序的密码的多种组合。在Unity Connection和Cisco Unified CM之间的通信时，密码和第三方证书被验证在两个末端。下面下一代加密支持的配置。

如果计划使用第三方认证机构签字的然后证书从签字在配置部分结束时的认证开始(请配置-签署EC键基于证书由第三方CA)

Prerequisites

Requirements

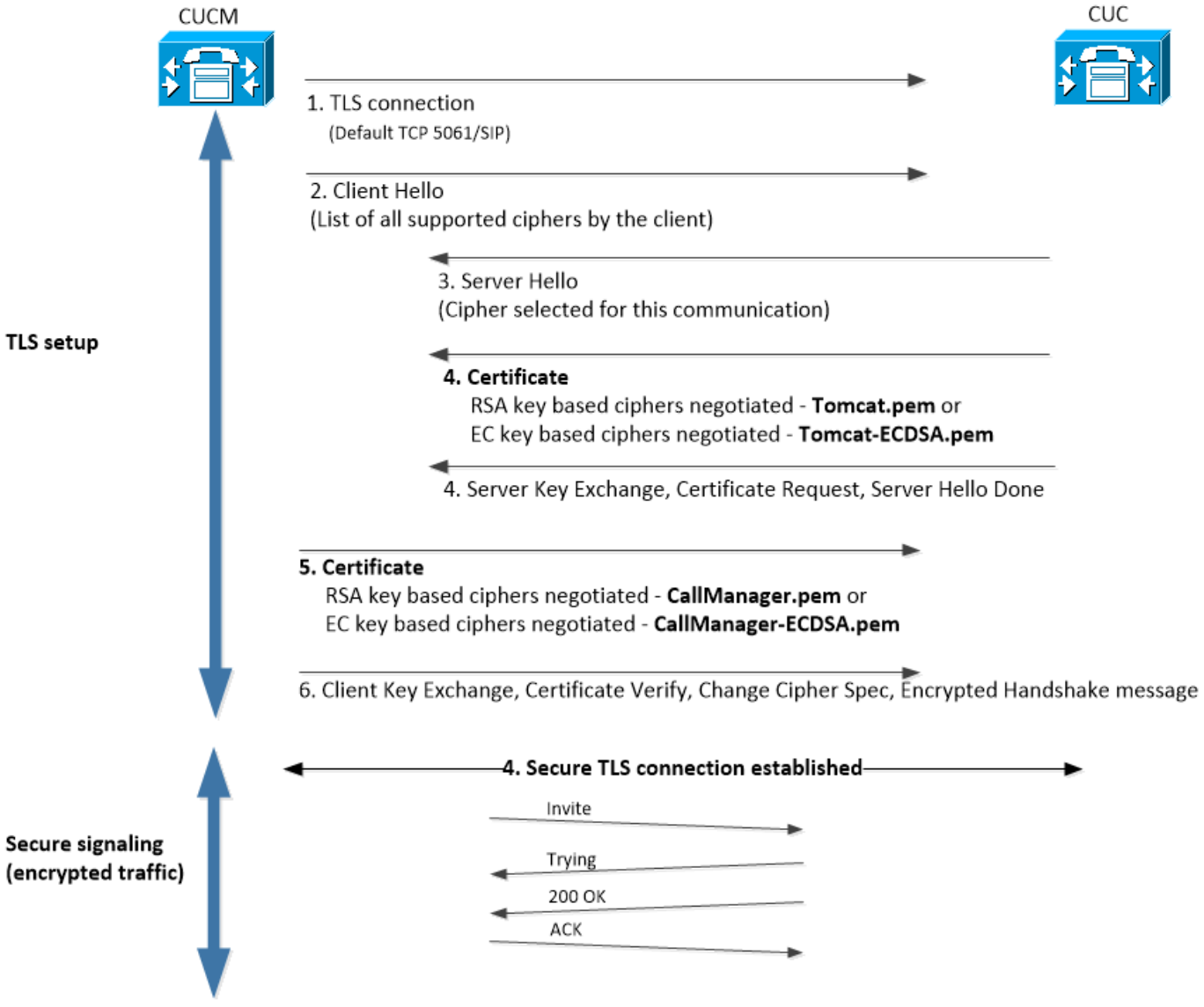
本文档中的信息基于以下软件和硬件版本：

在混合模式的CUCM版本11.0和以上
CUC版本11.0和以上

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

此图表简要地解释进程帮助建立CUCM之间的一个安全连接，并且CUC一次下一代加密支持是启用的：



认证需求

一旦下一代加密支持在Cisco Unity Connection，被启用这些是认证交换需求。

- **RSA密钥协商的基于密码**

使用的CUCM认证	使用的CUC认证	加载的Certs到CUCM	加载的Certs到CUC
CallManager.pem (自已签署的)	Tomcat.pem (自已签署的)	将被加载的Tomcat.pem到CUCM > CallManger信任	无。
CallManager.pem (签字的CA)	Tomcat.pem (签字的CA)	CUC根&将被加载的中间CA证书[*1]到CUCM >呼叫管理器信任	CUCM根&将被加载 CUC >呼叫管理器
CallManager.pem (签字的CA)	Tomcat.pem (自已签署的)	将被加载的Tomcat.pem到CUCM > CallManger信任	CUCM根&将被加载 >呼叫管理器信任。
CallManager.pem (自已签署的)	Tomcat.pem (签字的CA)	CUC根&将被加载的中间CA证书到CUCM >呼叫管理器信任	无。

[*1]CUC根&中间CA证书是指签署Unity Connection Tomcat认证的CA证书(Tomcat.pem)。

[*2]CUCM根&中间CA证书是指签署CUCM呼叫管理器认证的CA证书(Callmanager.pem)。

- **协商的EC键基于密码**

使用的CUCM认证	使用的CUC认证	加载的Certs到CUCM	加载的Certs到CUC
呼叫管理器ECDSA.pem (自已签署的)	TomcatECDSA.pem (自已签署的)	将被加载的TomcatECDSA.pem到CUCM > CallManger信任	无。
呼叫管理器ECDSA.pem (签字的CA)	TomcatECDSA.pem (签字的CA)	CUC根&将被加载的中间CA证书[*1]到CUCM >呼叫管理器信任	CUCM根&将被加载的中间CA证书[*2]到CUC >呼叫管理器信任。
呼叫管理器ECDSA.pem (签字的CA)	TomcatECDSA.pem (自已签署的)	将被加载的TomcatECDSA.pem到CUCM > CallManger信任。	CUCM根&将被加载的中间CA证书到CUC >呼叫管理器信任。
呼叫管理器ECDSA.pem (自已签署的)	TomcatECDSA.pem (签字的CA)	CUC根&将被加载的中间CA证书到CUCM >呼叫管理器信任	无。

[*1] CUC根&中间CA证书是指签署Unity Connection EC基于Tomcat认证的CA证书(TomcatECDSA.pem)。

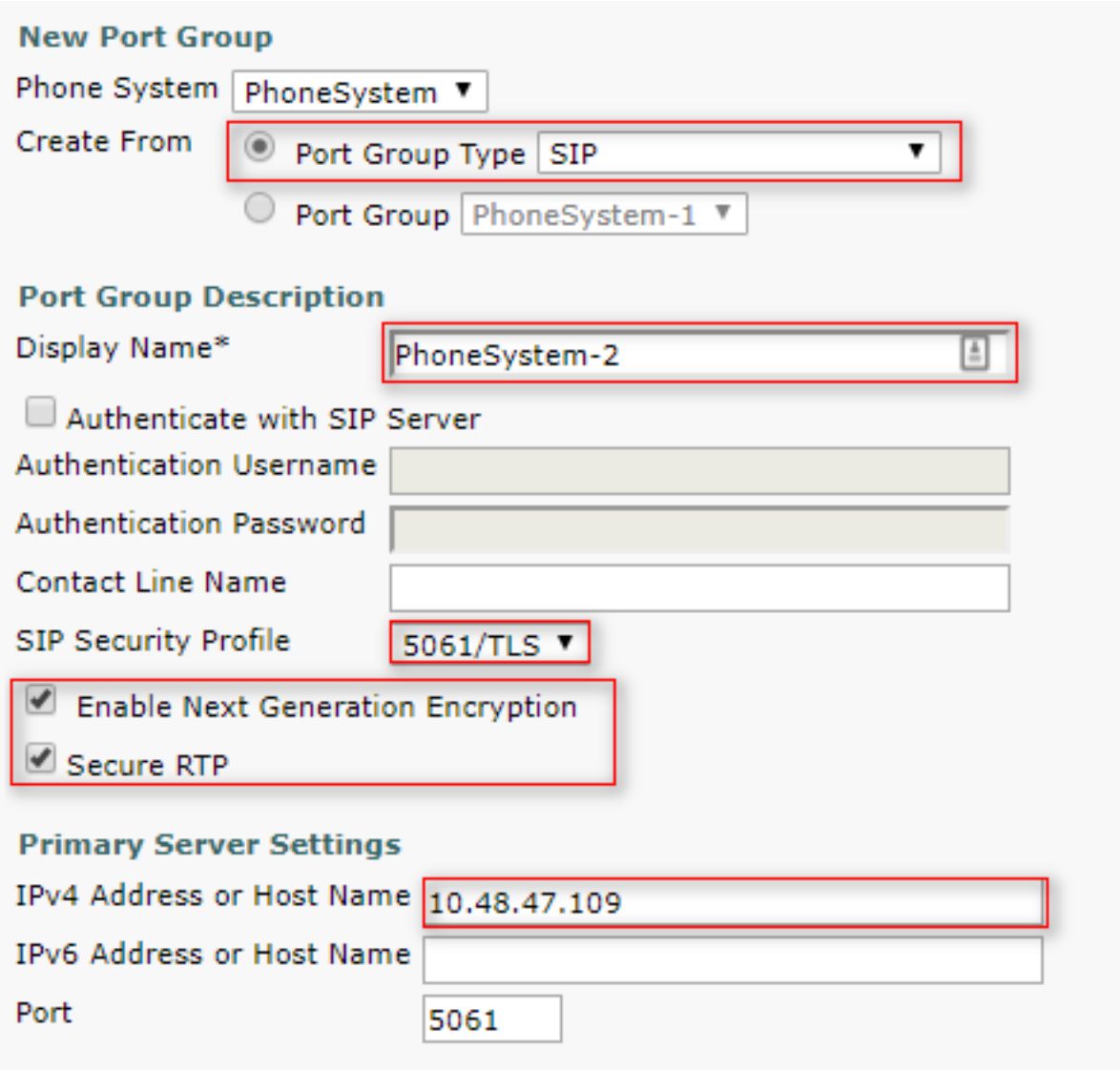
[*2] CUCM根&中间CA证书是指签署CUCM呼叫管理器认证的CA证书(呼叫管理器ECDSA.pem)。

1. **Note**:TomcatECDSA.pem认证称为在CUC的11.0.1版本的呼叫管理器ECDSA.pem。从CUC 11.5.x认证改了名对TomcatECDSA.pem。

配置- Cisco Unity Connection (CUC)

1. 添加新的端口组

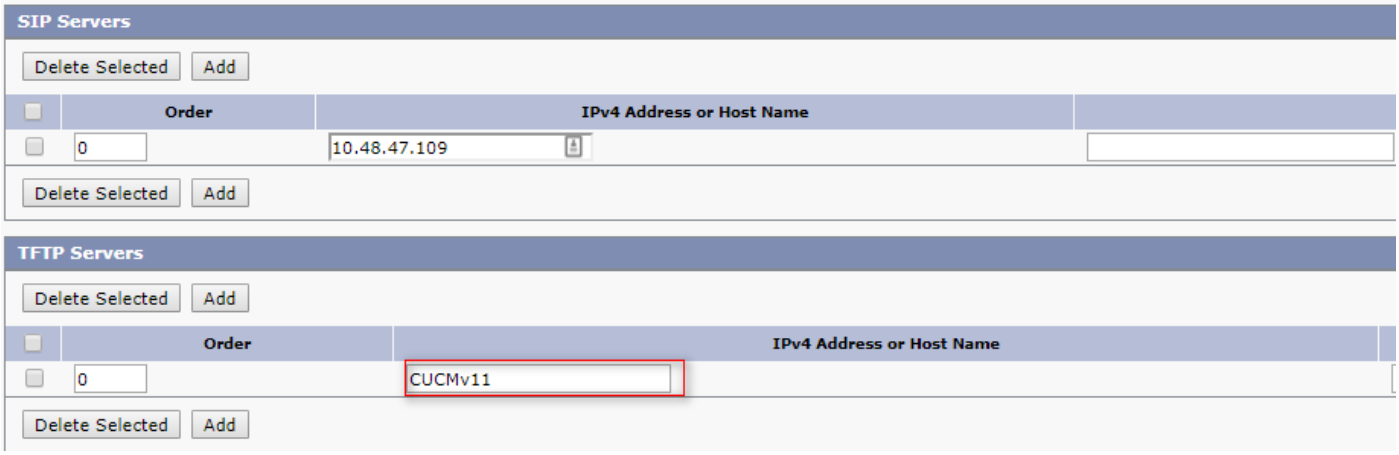
连接对Cisco Unity Connection管理页>电话集成>端口组并且点击新的Add。保证检查Enable (event)下一代加密复选框。



1. **Note**:一旦Enable (event)下一代加密复选框是启用的， Unity连接的Cisco Tomcat认证将使用在SSL握手期间。
    - •万一ECDSA基于密码是然后协商的EC关键基于TomcatECDSA认证用于SSL握手。
    - •万一RSA基于密码是然后协商的RSA密钥基于Tomcat认证用于SSL握手。

2. 添加TFTP server参考

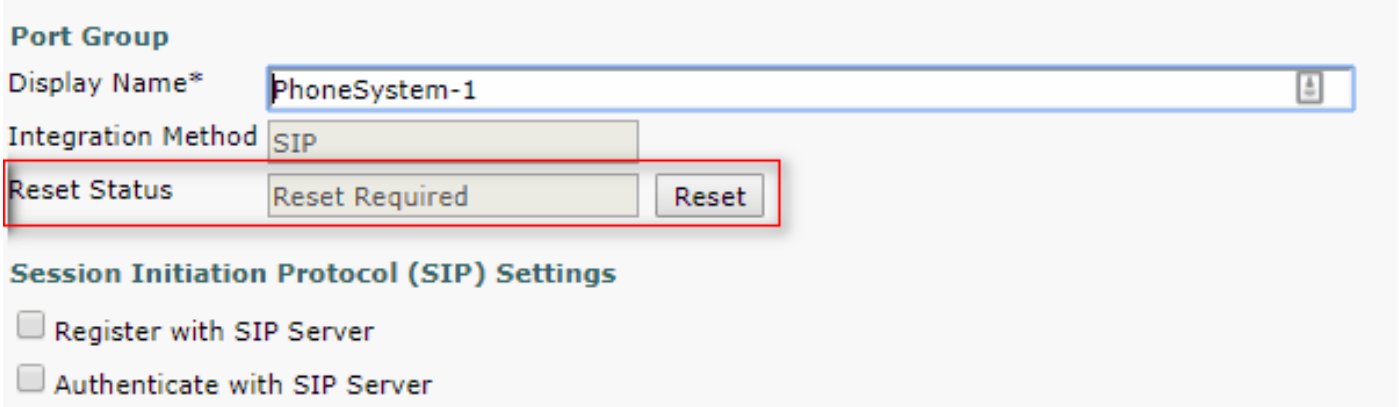
在端口组基础页，请连接编辑>服务器和添加您的CUCM簇TFTP server FQDN。TFTP server的FQDN/主机名必须匹配呼叫管理器认证共同名称(CN)。服务器的IP地址不会工作，并且将导致失败下载ITL文件。因此DNS名一定是可溶解的通过被配置的DNS服务器。



通过连接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从CUCM的TFTP下载ITL文件(ITLfile.tlv)使用关于安全的6972端口(URL的https协议： https://<CUCM-TFTP-FQDN>:6972/ITLFile.tlv)。因为CUC寻找“CCM+TFTP”功能认证从ITL文件， CUCM必须在混合模式。

连接回到电话集成>端口组>端口组基础配置页并且重置您新加的端口组。



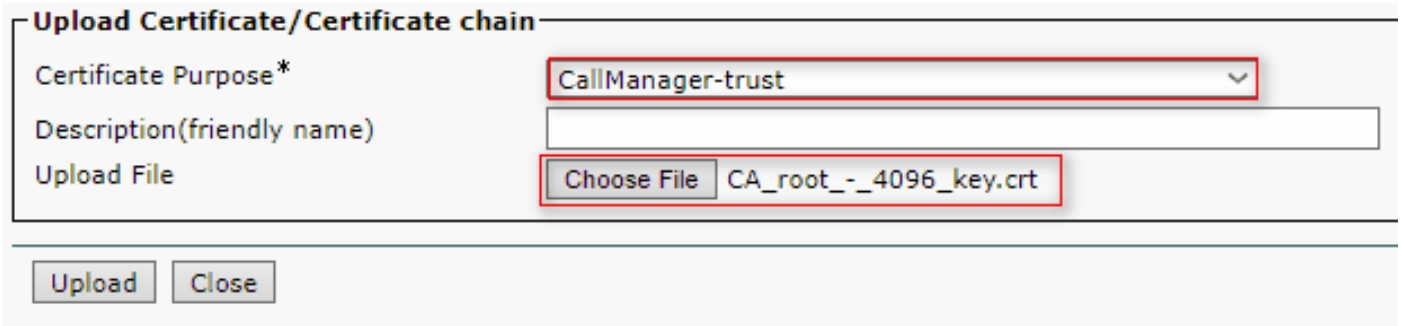
1. **Note**:在重置时候端口组， CUC服务器将通过连接到CUCM服务器更新其本地存储的ITL文件。

3. 添加语音邮件端口

连接回到电话集成>端口并且点击新的Add添加端口到您新建立的端口组。

4. 加载CUCM第三方CA的根和中间证书

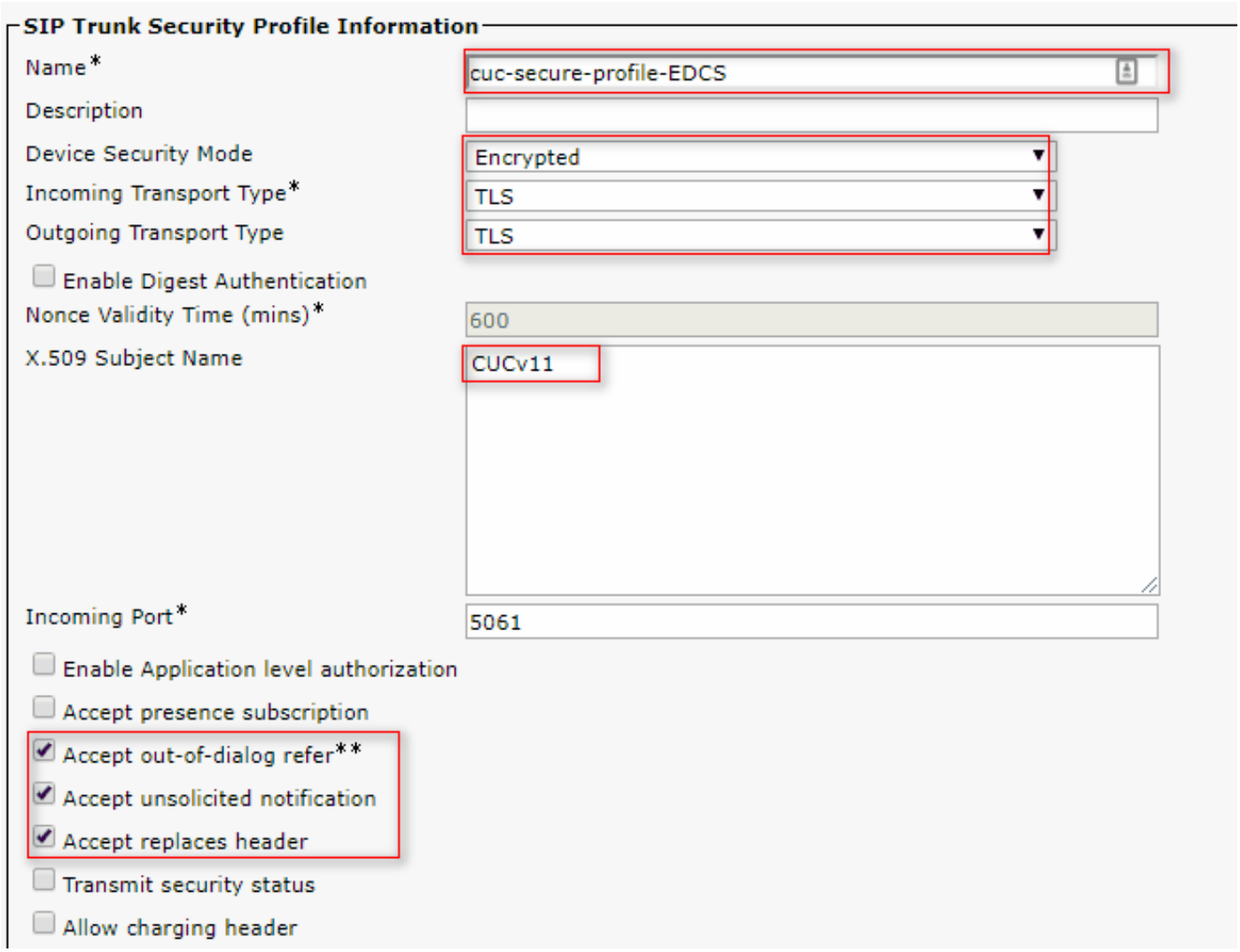
在第三方证书的情况下，您必须加载第三方认证机构的根和中间证书在Unity Connection呼叫管理器信任的。只有当第三方CA签署了您的呼叫管理器认证，这必要。通过连接进行此动作对Cisco Unified OS管理> Security > Certificate Management并且点击加载认证。



配置- Cisco Unified CM (CUCM)

1. 创建SIP Trunk安全配置文件

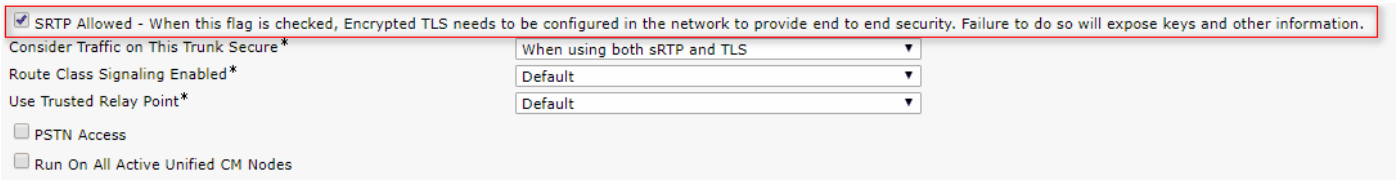
连接对CUCM管理>System > Security > SIP Trunk安全配置文件并且添加新配置文件。 X.509主题名称必须匹配CUC服务器的FQDN。

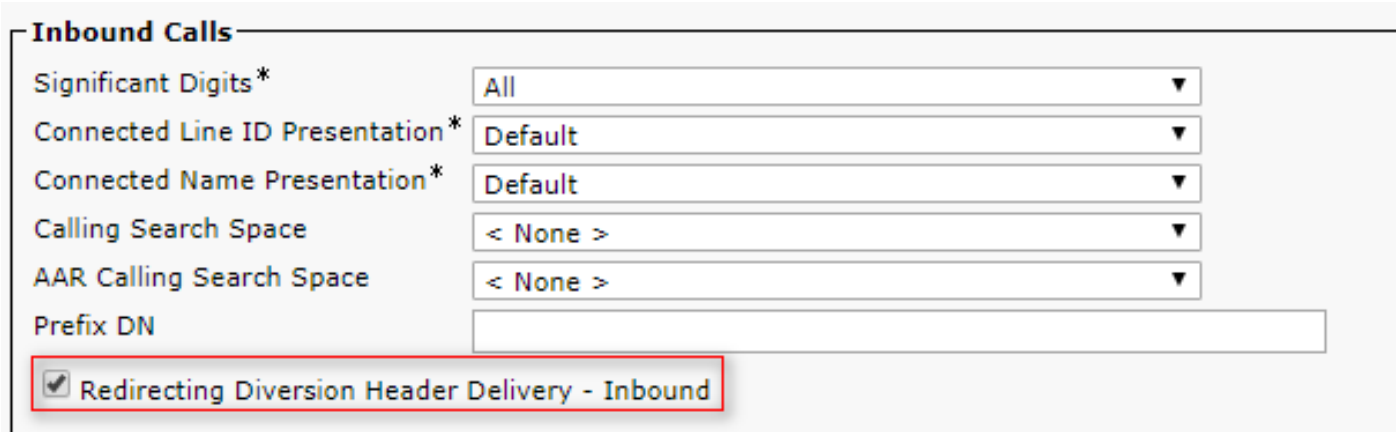


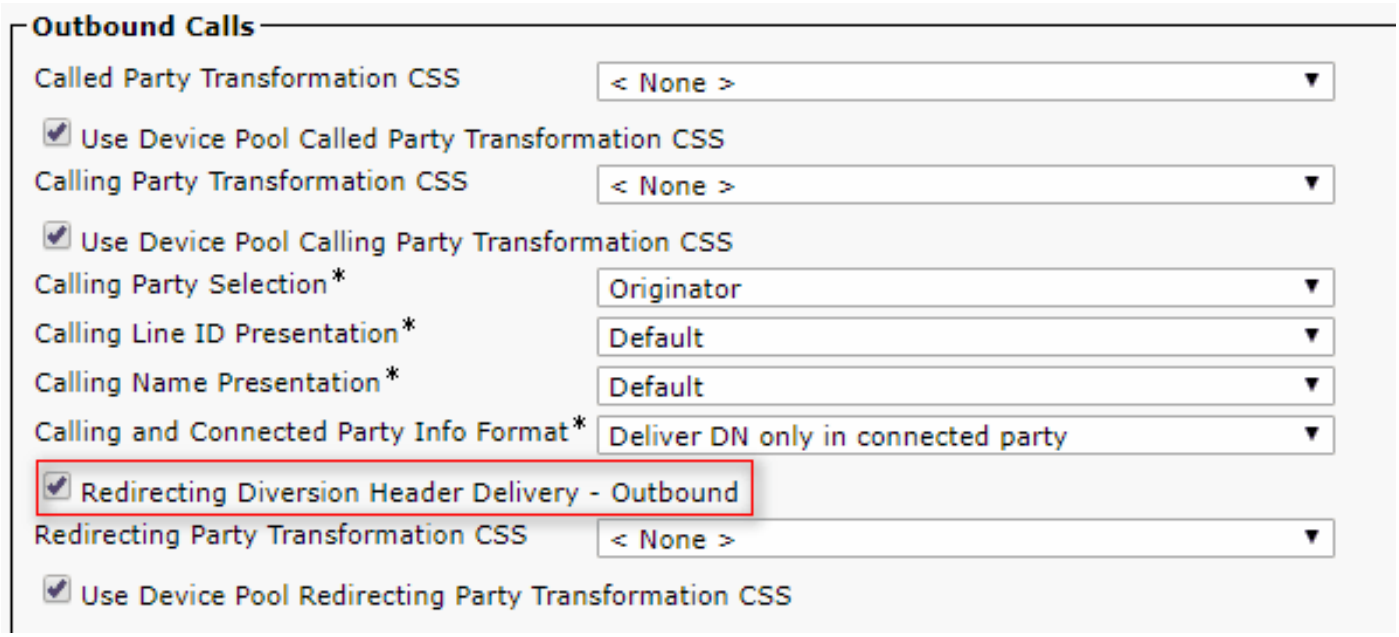
1. **Note**: CLI命令“请显示cert拥有Tomcat/tomcat.pem”能显示在Unity Connection的RSA密钥基于Tomcat认证。它是CN必须匹配在CUCM配置的X.509主题名称。CN与Unity服务器的FQDN/主机名是相等的。EC键基于认证包含FQDN/hostname -在其附属的替代名称(SAN)字段。

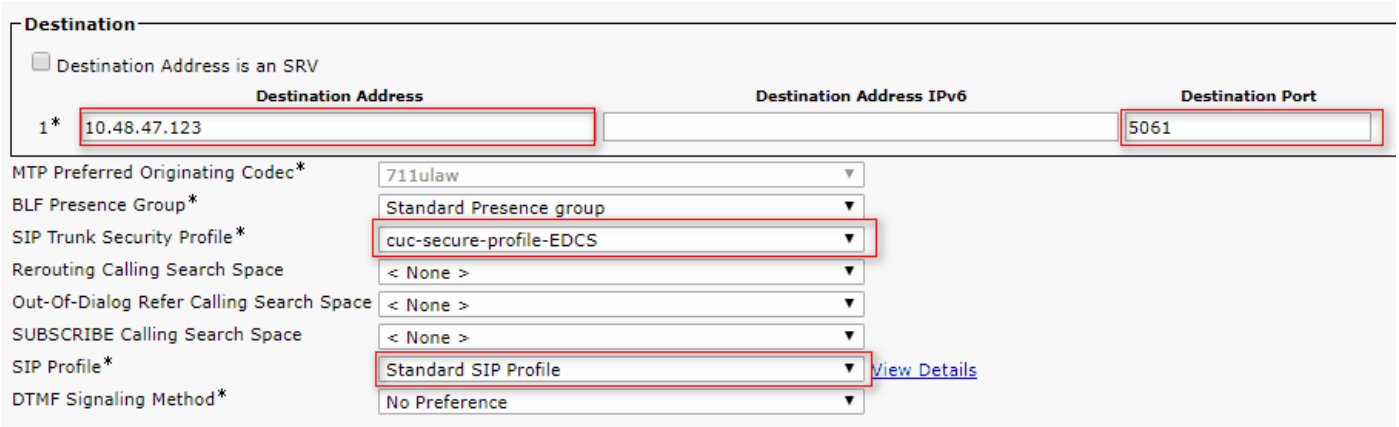
2. 创建安全的SIP Trunk

连接对设备> Trunk >点击并且添加新并且创建将使用安全的集成与Unity Connection的一个标准的SIP Trunk。





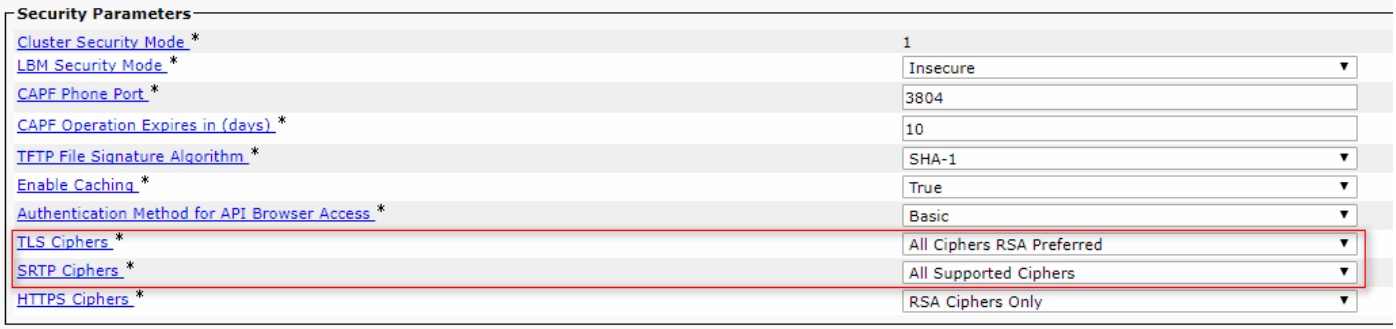




3. 配置TLS和SRTP密码

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

连接对Cisco Unified CM >系统>企业参数并且选择适当的密码选项从从下拉列表的TLS和SRTP密码。



通过连接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

连接对Cisco Unity Connection管理页>System设置>General配置并且选择适当的密码选项从从下拉列表的TLS和SRTP密码。

通过连接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选项

TLS密码选项	TLS密码按优先级顺序
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

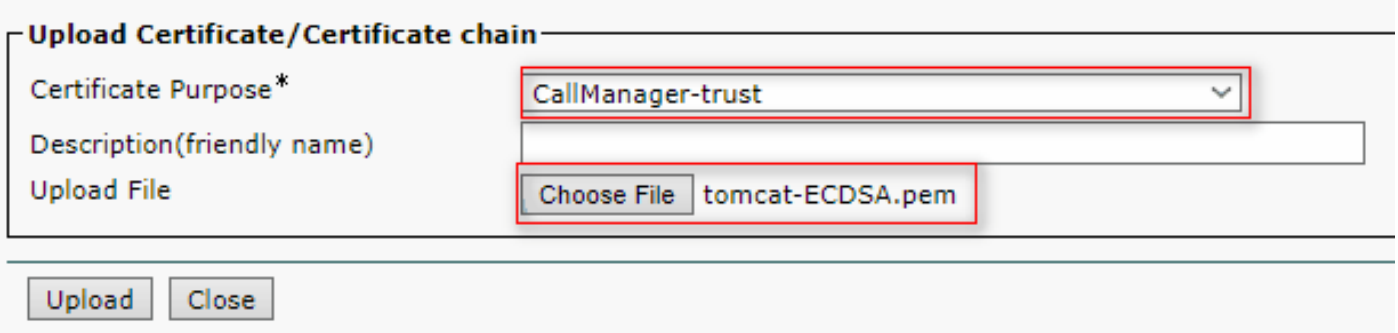
首选的所有密码RSA (默认值)	84 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256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

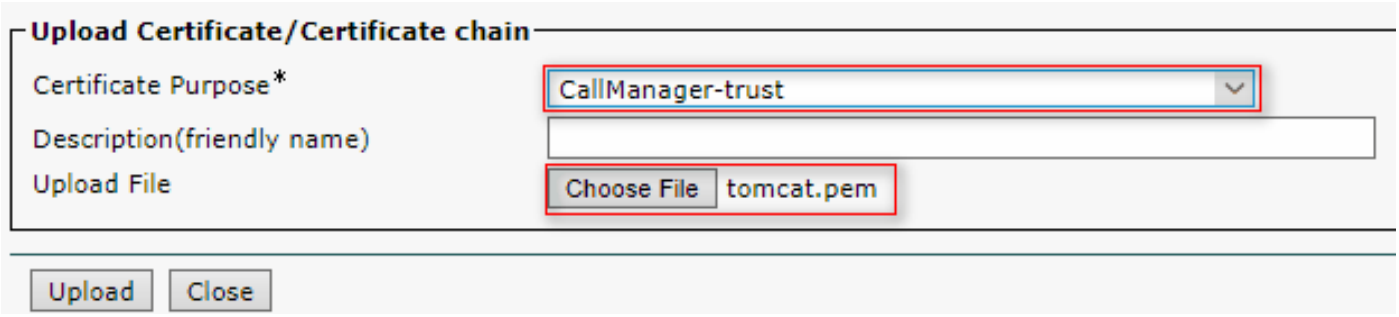
SRTP密码选项按优先级顺序

SRTP密码选项	SRTP按优先级顺序
所有支持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 GCM根据密码	• AEAD_AES_256_GCM • AEAD_AES_128_GCM
AEAD AES256 GCM根据仅密码	• AEAD_AES_256_GCM

4. 加载CUC Tomcat证书(基于的RSA & EC)

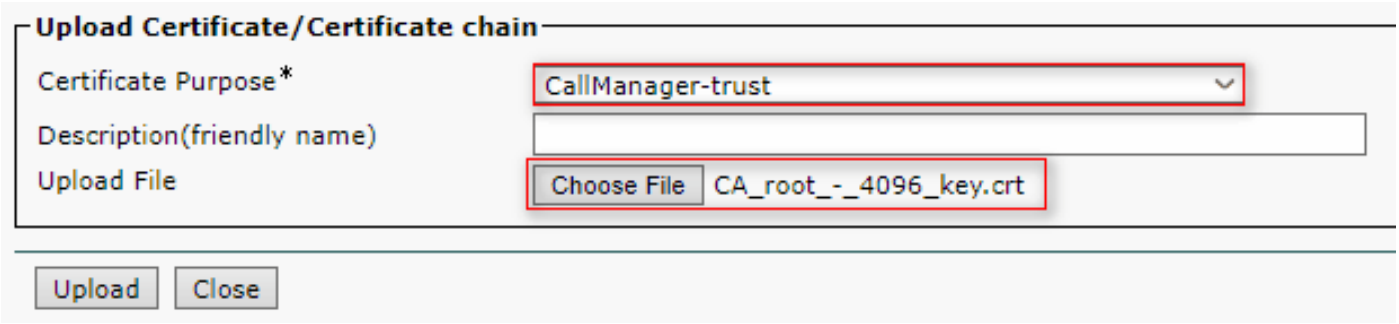
连接对OS管理> Security > Certificate Management并且加载两CUC Tomcat证书(基于的RSA & EC)到呼叫管理器信任存储。





1. **Note**: 如果ECDSA密码只，协商加载两Unity Tomcat证书不是必须的。在这样案件EC基于Tomcat认证是足够。

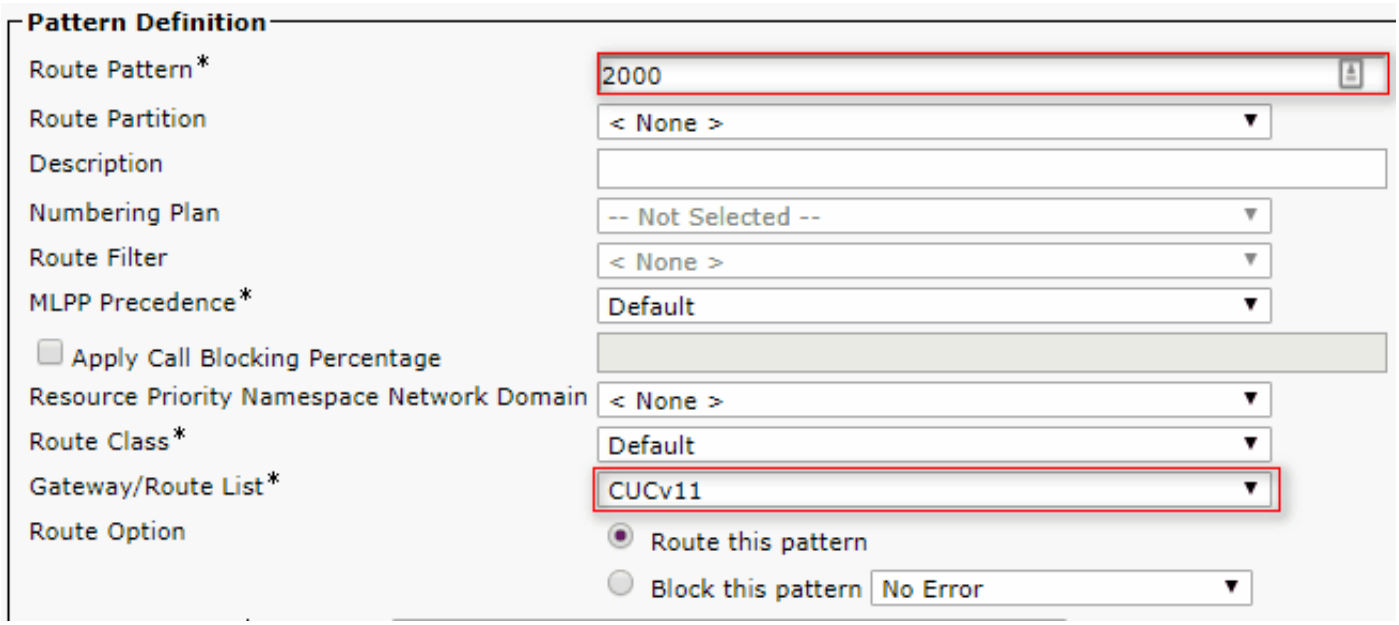
在第三方证书的情况下，您必须加载第三方认证机构的根和中间证书。只有当第三方CA签署了您的Unity Tomcat认证，这必要。



重新启动在所有节点的Cisco Call Manager进程应用更改。

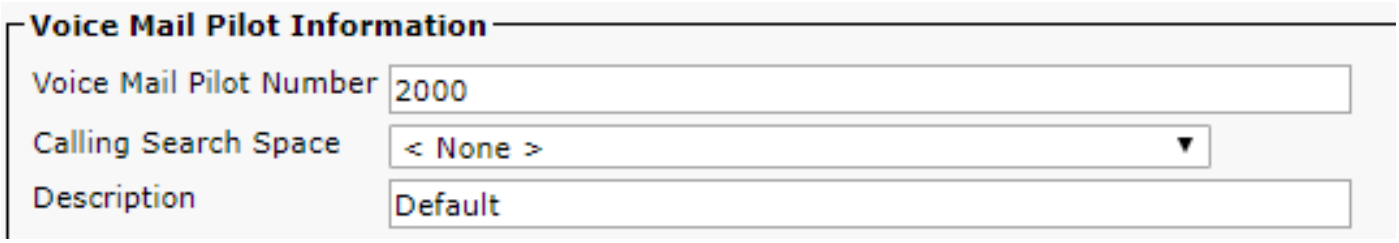
5. 创建路由模式

配置对被配置的Trunk的点通过连接对呼叫路由>路由/搜索>路由模式的一个路由模式。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。

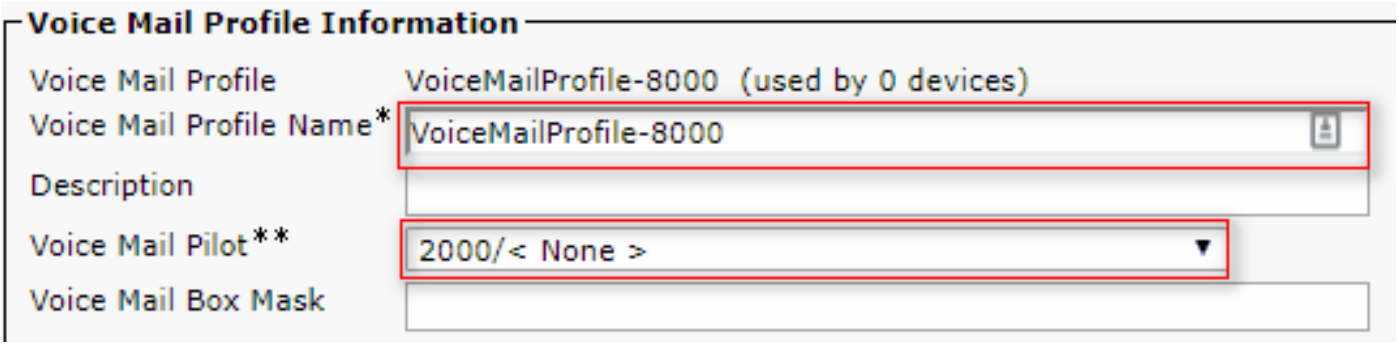


6. 创建语音邮件试验，语音邮件配置文件并且分配它到Dns

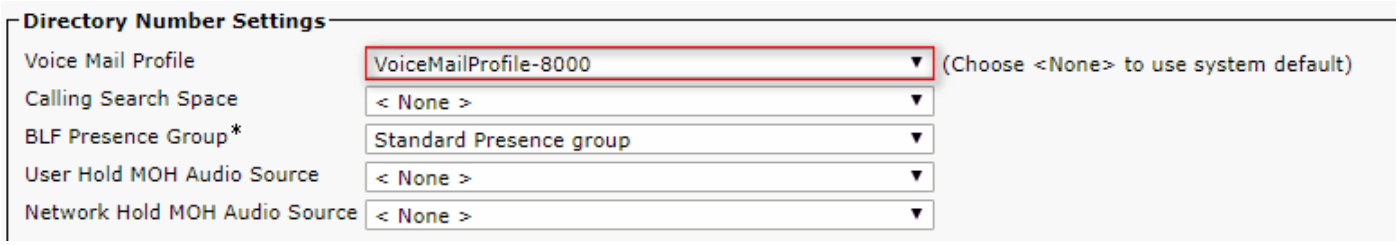
通过去创建集成的一语音邮件引导高级特性>Voice邮件>Voice邮件试验。



创建一个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的集成Dns呼叫路由>目录号



配置-签署EC键由第三方CA根据证书(可选)

证书也许由在设置安全的集成前的第三方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. 生成认证署名请求(CSR) CUC TomcatECDSA的并且安排认证签字由第三方CA
2. CA提供必须加载和跟随的身份认证(CA签名的证书)和CA证书(CA根证明) ：
   加载CA根证明到Tomcat信任存储
   加载身份认证到Tomcat EDCS存储
3. 重新启动CUC的会话管理器

Cisco Unified CM

1. 生成CUCM呼叫管理器ECDSA的CSR并且安排认证签字由第三方CA
2. CA提供必须加载和跟随的身份认证(CA签名的证书)和CA证书(CA根证明) ：
   加载CA根证明到呼叫管理器信任存储
   加载身份认证到呼叫管理器EDCS存储
3. 重新启动Cisco在每个节点的CCM和TFTP服务

同一个进程将用于签署RSA密钥CSR为CUC Tomcat认证和呼叫管理器认证生成并且被加载到各自Tomcat存储和呼叫管理器存储的基于证书。

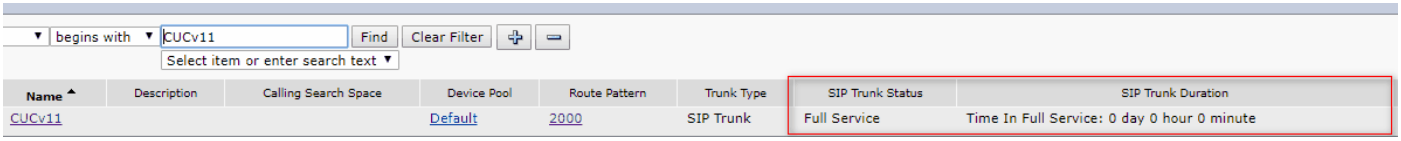
Verify

Use this section to confirm that your configuration works properly.

获取SIP Trunk验证

按在电话的语音邮件按钮呼叫语音邮件。如果用户的扩展名在Unity Connection系统，没有被配置您应该听到开始的问候。

或者，您能enable (event) SIP监控SIP中继线状态的选项Keepalive。此选项在SIP配置文件可以被启用分配到SIP Trunk。一旦这是启用的您能通过设备> Trunk监控饮者中继线状态如下所示：



安全的RTP呼叫验证

验证挂锁图标是否是存在呼叫对Unity Connection。意味着RTP流被加密(设备安全配置文件一定是安全为了它能工作)如此镜像所显示，

Related Information

- SIP Cisco Unity Connection Release 11.x集成指南