配置CUCM和CUC之间的安全集成并对其进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

图解

配置 — 安全SIP中继

- 配置CUC
  - 1.添加SIP证书
  - 2.创建新电话系统或修改默认电话系统
  - 3.添加新端口组
  - 4.编辑服务器
  - 5.重置端口组
  - 6.添加语音邮件端口
  - 7.下载CUC根证书
- 配置CUCM
  - 1.为指向CUC的中继配置SIP中继安全配置文件
  - 2.配置SIP配置文件
  - 3.创建SIP中继
  - 4.创建路由模式
  - 5.创建语音邮件引导
  - 6.创建语音邮件配置文件
  - 7.将语音邮件配置文件分配给DN
  - 8.将CUC根证书上传为CallManager-trust

配置安全SCCP端口

- 配置CUC
  - 1.下载CUC根证书
  - 2.创建电话系统/修改现有的电话系统。
  - 3.添加新的SCCP端口组
  - 4.编辑服务器
  - 5.添加安全SCCP端口
- 配置CUCM
  - 1.添加端口
  - 2.将CUC根证书上传为CallManager-trust
  - 3.配置消息等待信息(MWI)开/关分机
  - 4.创建语音邮件引导
  - 5.创建语音邮件配置文件
  - 6.将语音邮件配置文件分配给DN
  - 7.创建语音邮件寻线组

验证

- SCCP端口验证
- 安全SIP中继验证

安全RTP呼叫验证
故障排除
1.一般故障排除提示
2.要收集的跟踪
常见问题
第 1 种情况：无法建立安全连接（未知CA警报）
第 2 种情况：无法从CUCM TFTP下载CTL文件
实例3：其它WRR加权修改端口未注册
缺陷

简介

本文档介绍Cisco Unified Communication Manager(CUCM)与Cisco Unity Connection(CUC)服务器之间的安全连接的配置、验证和故障排除。

先决条件

要求

Cisco建议您具备CUCM知识。

有关详细信息，请参阅Cisco Unified Communications Manager安全指南。

注意：必须将其设置为混合模式，才能使安全集成正常工作。

必须为Unity Connection 11.5(1)SU3及更高版本启用加密。

CLI命令“utils cuc encryption <enable/disable>”

使用的组件

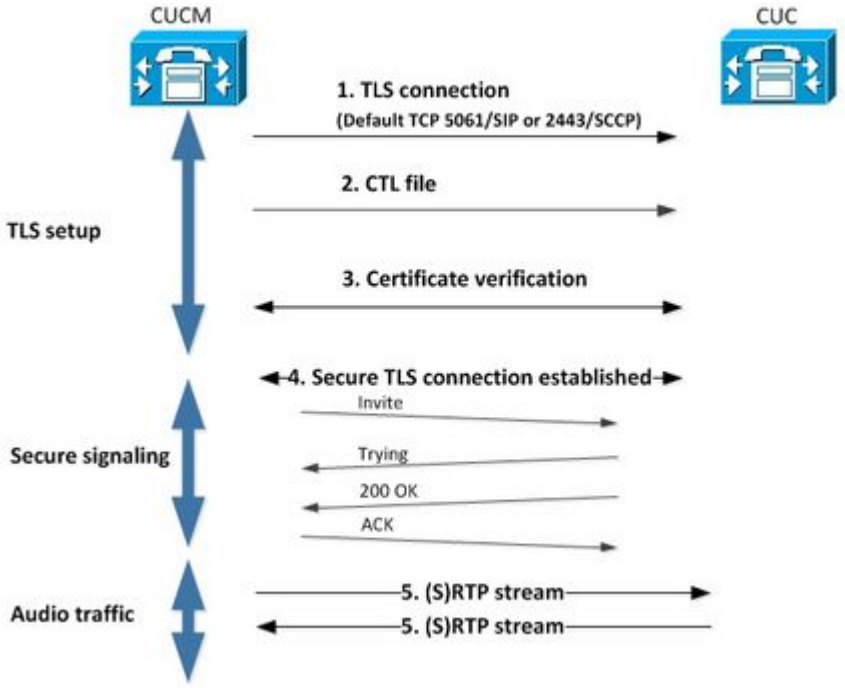
本文档中的信息基于以下软件和硬件版本：

- CUCM 版本 10.5.2.11900-3.
- CUC 10.5.2.11900-3版。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

图解

下图简要说明了帮助在CUCM和CUC之间建立安全连接的过程：



1. Call Manager在用于集成的协议的端口2443 Skinny Call Control Protocol(SCCP)或基于5061 Session Initiation Protocol(SIP)上建立与CUC服务器的安全传输层安全(TLS)连接。

2. CUC服务器从TFTP服务器下载证书信任列表(CTL)文件（一次性进程），提取CallManager.pem证书并存储它。

3. CUCM服务器提供Callmanager.pem证书，该证书根据上一步获得的CallManager.pem证书进行验证。此外，正在根据CUCM中存储的CUC根证书验证CUC证书。请注意，根证书必须由管理员上传到CUCM。

4.如果证书验证成功，则建立安全TLS连接。此连接用于交换加密的SCCP或SIP信令。

5.音频流量可以作为实时传输协议(RTP)或SRTP进行交换。

注意：建立TLS通信时，CUCM和CUC使用TLS相互身份验证。有关详细信息，请参阅

RFC5630。

配置 — 安全SIP中继

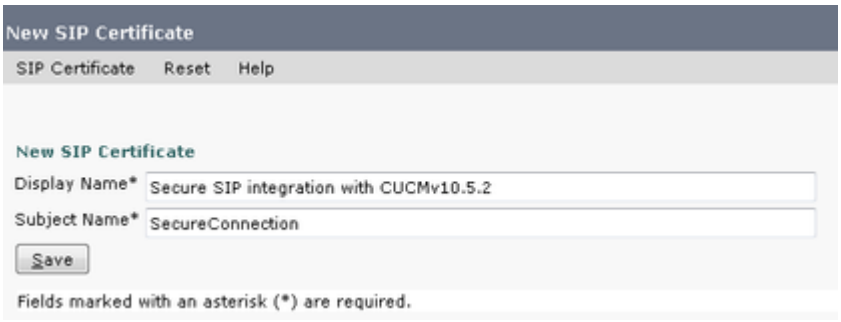
配置CUC

1.添加SIP证书

导航到CUC管理>电话集成>安全> SIP证书>添加新

- 显示姓名：<任何有意义的名称>
- 主题名称:<任何名称，例如SecureConnection>

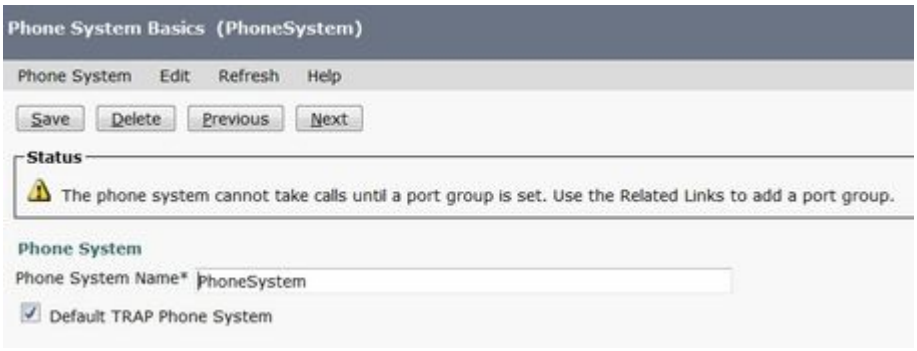
注意：主题名称必须与SIP中继安全配置文件中的X.509主题名称匹配（在本文档后面的CUCM配置步骤1中配置）。



注意：证书由CUC根证书生成并签名。

2.创建新电话系统或修改默认电话系统

导航到电话集成>电话系统。您可以使用已经存在的电话系统或创建新系统。

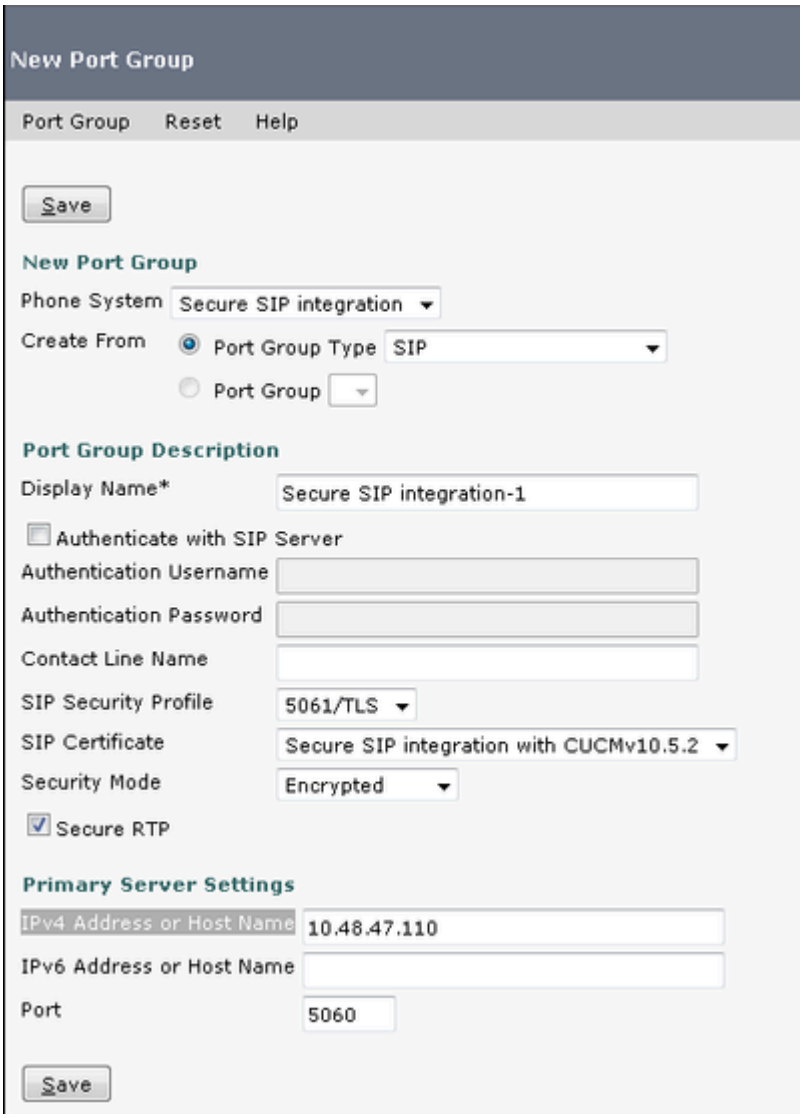


3.添加新端口组

在Phone System Basics页面的Related Links下拉框中，选择Add Port Group并选择Go。在配置窗口中，输入以下信息：

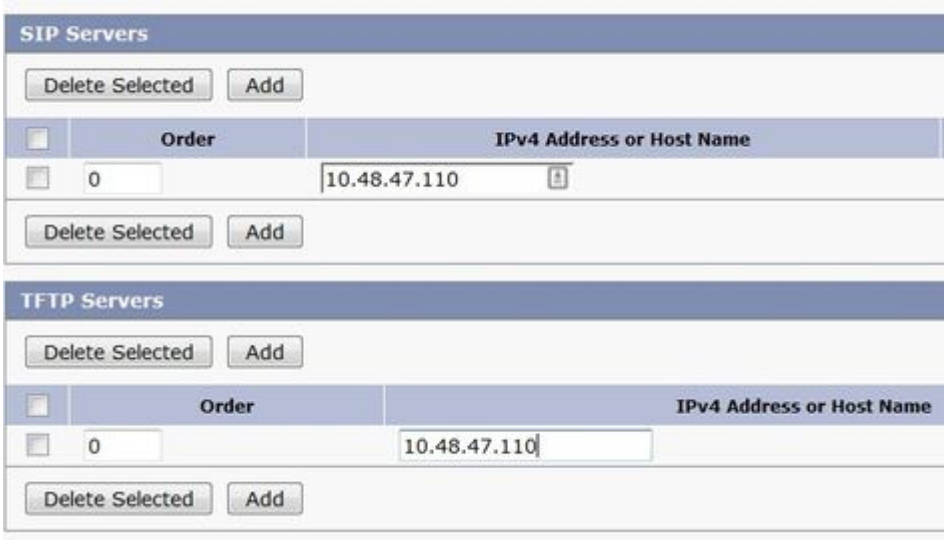
- 电话系统:
- 创建源： 端口组类型SIP
- SIP安全配置文件： 5061/TLS
- SIP证书：
- 安全模式: 已加密
- 安全 RTP: 已选中
- IPv4地址或主机名：

点击Save。



4.编辑服务器

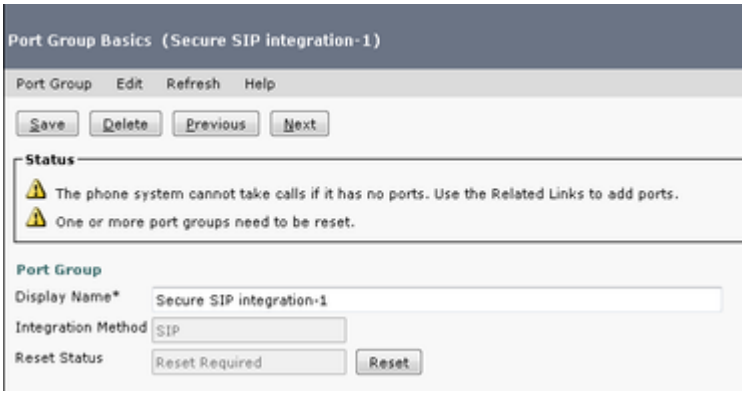
导航到Edit > Servers，然后从CUCM集群添加TFTP服务器，如下图所示。



注意：必须提供正确的TFTP地址。CUC服务器按照说明从此TFTP下载CTL文件。

5.重置端口组

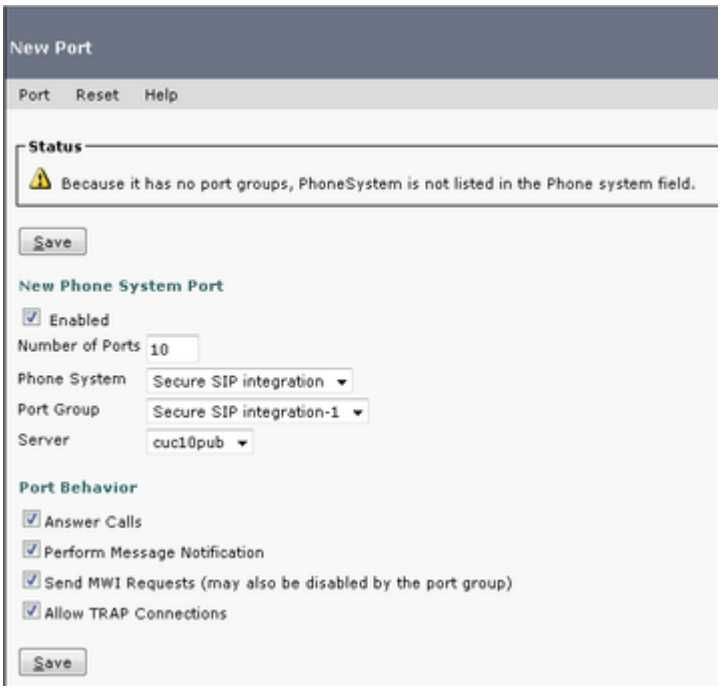
返回Port Group Basics，按照系统提示重置端口组，如下图所示。



6.添加语音邮件端口

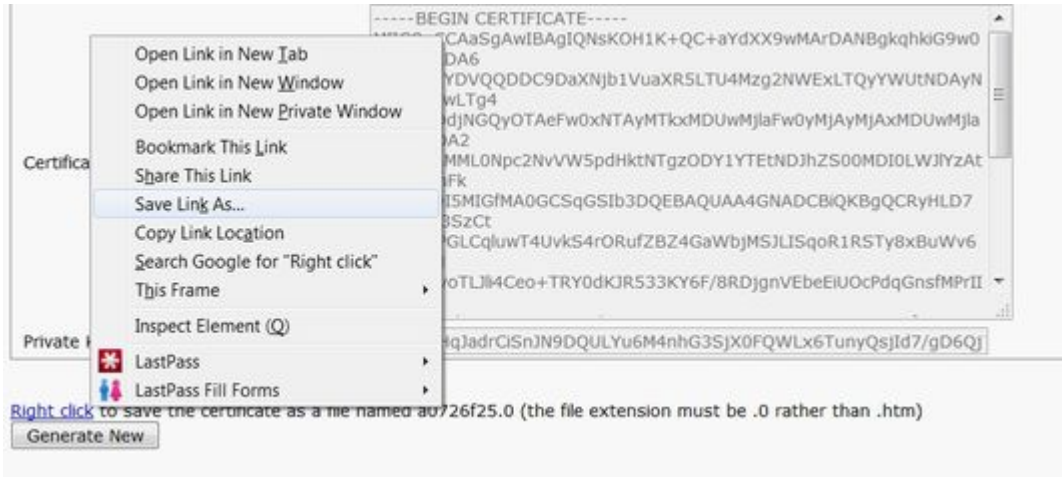
在“端口组基本信息”页的“相关链接”下拉框中，选择添加端口，然后选择转到。在配置窗口中，输入以下信息：

- 启用:已选中
- 端口数量:
- 电话系统:
- 端口组:
- 服务器：
- 端口行为：



7.下载CUC根证书

导航到Telephony Integrations > Security > Root Certificate，右键点击URL，将证书另存为名为<filename>.0（文件扩展名必须是。0而不是.htm）'，然后按此图所示点击save。



配置CUCM

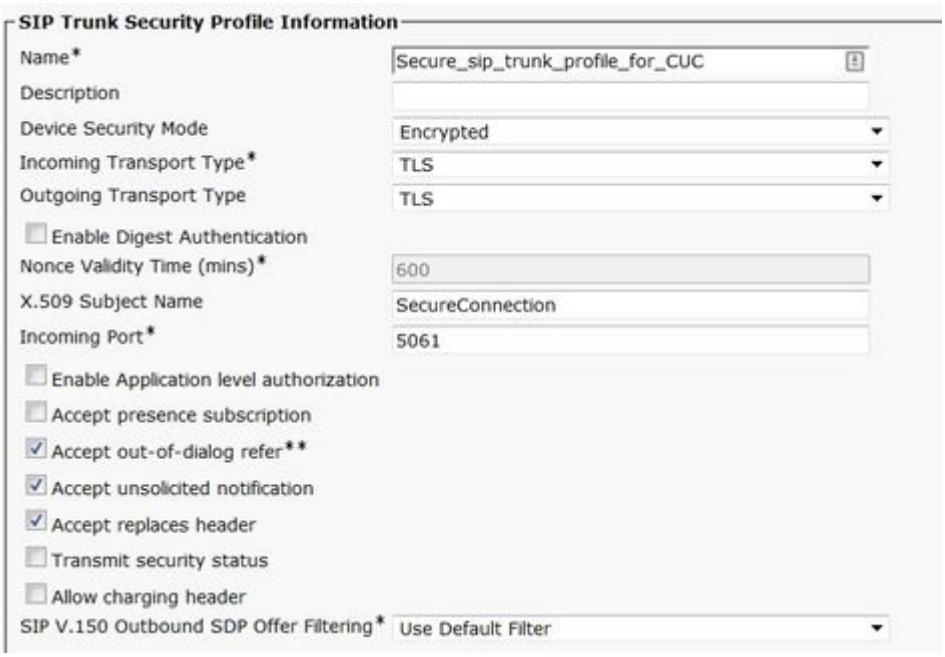
1.为指向CUC的中继配置SIP中继安全配置文件

导航到CUCM Administration > System > Security > SIP Trunk Security Profile > Add new

确保正确填写以下字段：

- 设备安全模式: 已加密
- X.509使用者名称： SecureConnection>
- 接受对话外 REFER: 已选中
- 接受未经请求的通知: 已选中
- 接受更换报头: 已选中

注意：X.509主题名称必须与Cisco Unity Connection服务器（在CUC配置的第1步中配置）上SIP证书中的Subject Name字段匹配。



2.配置SIP配置文件

如果需要应用任何特定设置，请导航到Device > Device Settings > SIP Profile。否则，您可以使用标准SIP配置文件。

3.创建SIP中继

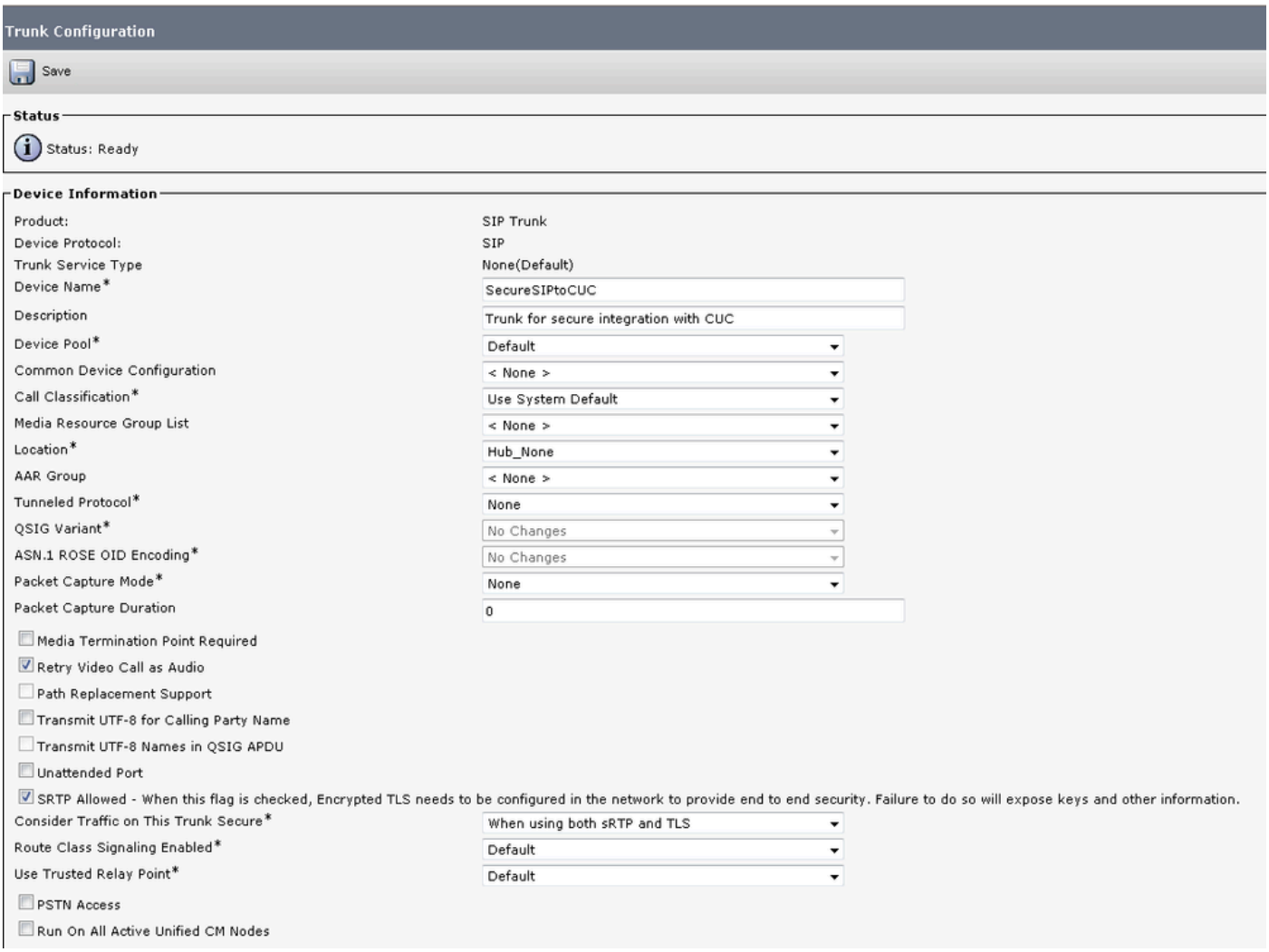
转至Device > Trunk > Add new。创建用于与Unity Connection安全集成的SIP中继，如下图所示。



在TRUNK配置的Device Information部分，输入以下信息：

- 设备名称：
- 设备池:
- 允许的SRTP:　　已选中

注意：确保CallManager组（在设备池配置中）包含在CUC中配置的所有服务器(Port group > Edit > Servers)。



在TRUNK配置的Inbound Calls部分，输入以下信息：

- 呼叫搜索空间：
- 重定向转移标头传送 — 入站：　已选中



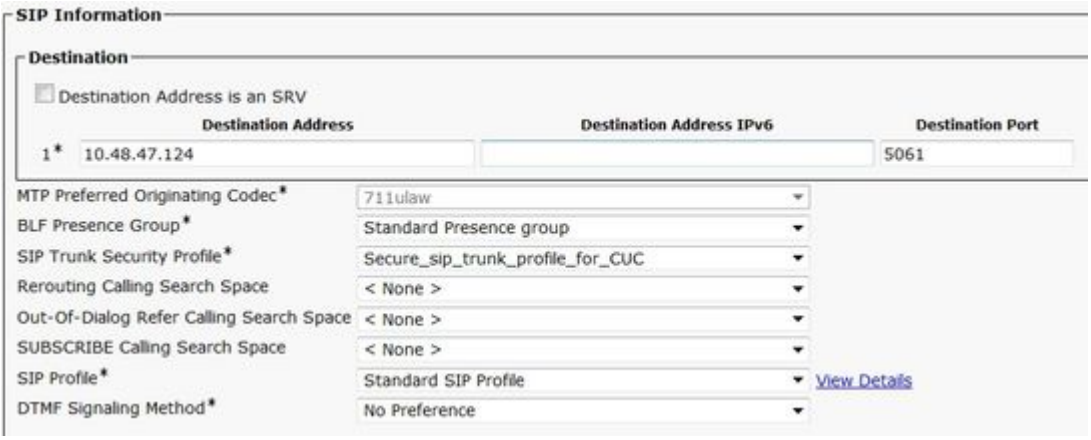
在TRUNK配置的Outbound Calls部分，输入以下信息：

- 重定向转移标头传送 — 出站：已选中



在中继配置的SIP信息部分，输入以下信息：

- 目的地址：
- SIP 干线安全性配置文件:
- 重新路由呼叫搜索空间：
- 对话框外部引用呼叫搜索空间：
- Sip 配置文件:

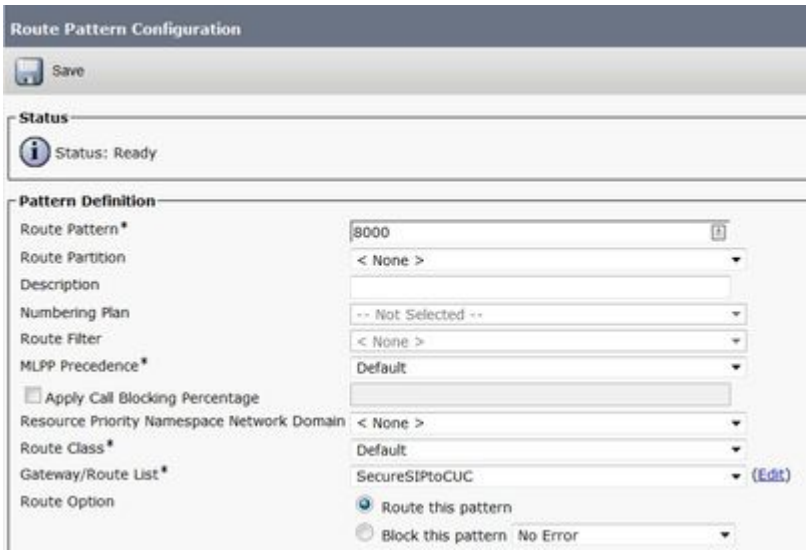


根据您的要求调整其他设置。

4.创建路由模式

创建指向已配置中继的路由模式(Call Routing > Route/Hunt > Route Pattern)。 作为路由模式编号输入的分机可用作语音邮件引导。输入此信息：

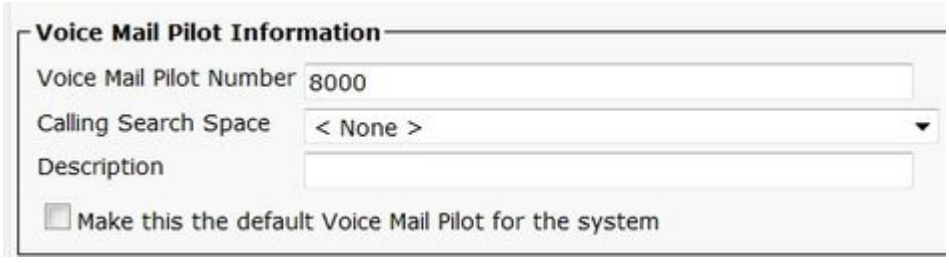
- 路由模式:
- 网关/路由列表：



5.创建语音邮件引导

为集成创建语音邮件引导(Advanced Features > Voice Mail > Voice Mail Pilot)。 输入以下值：

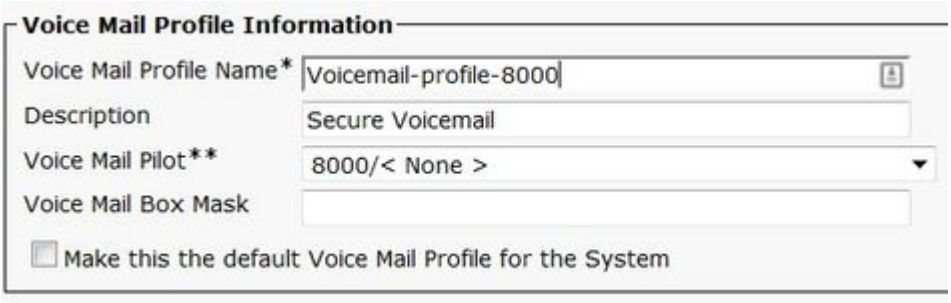
- 语音邮件引导号：
- 呼叫搜索空间： 包括包含用作引导的路由模式的分区>



6.创建语音邮件配置文件

创建语音邮件配置文件以将所有设置链接在一起(Advanced Features > Voice Mail > Voice Mail Profile)。 输入此信息：

- 语音邮件引导:
- 语音信箱掩码：

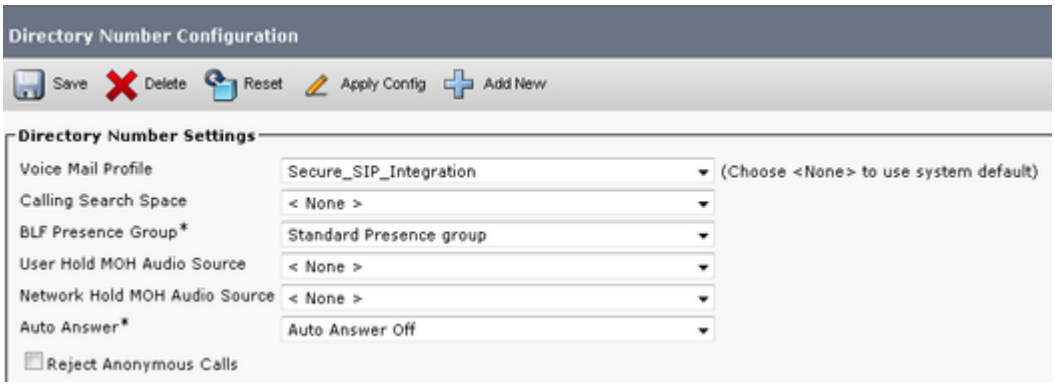


7.将语音邮件配置文件分配给DN

将语音邮件配置文件分配到旨在使用安全集成的DN。更改DN设置后，不要忘记点击“Apply Config”（应用配置）按钮：

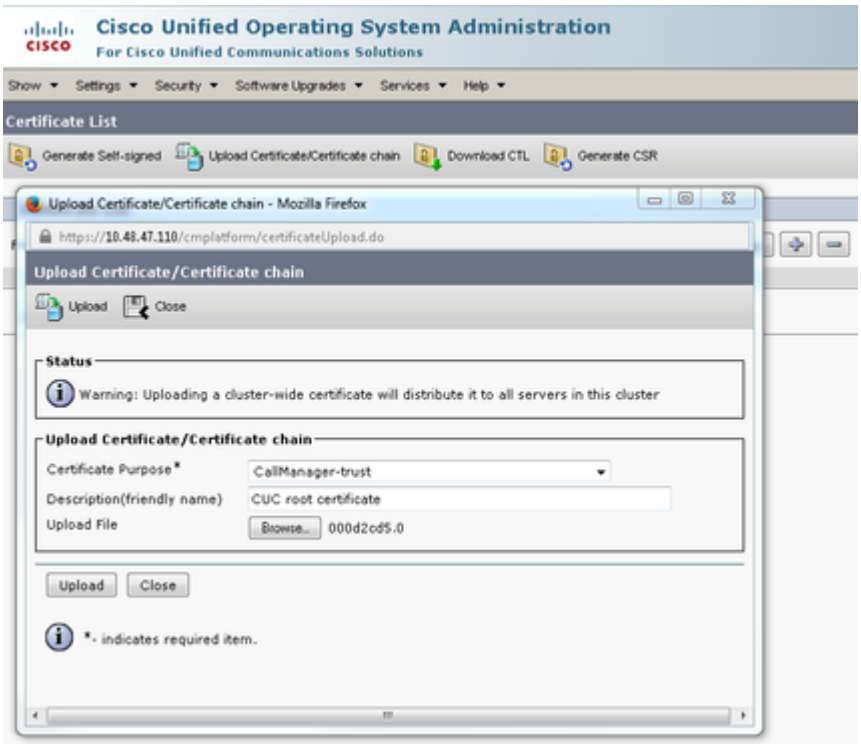
导航至：呼叫路由(Call Routing)>目录号码(Directory number)并更改：

- 语音邮件配置文件: 安全_SIP_集成



8.将CUC根证书上传为CallManager-trust

导航到OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain，然后以CallManager-trust形式在配置为与CUC服务器通信的所有节点上上上传CUC根证书。



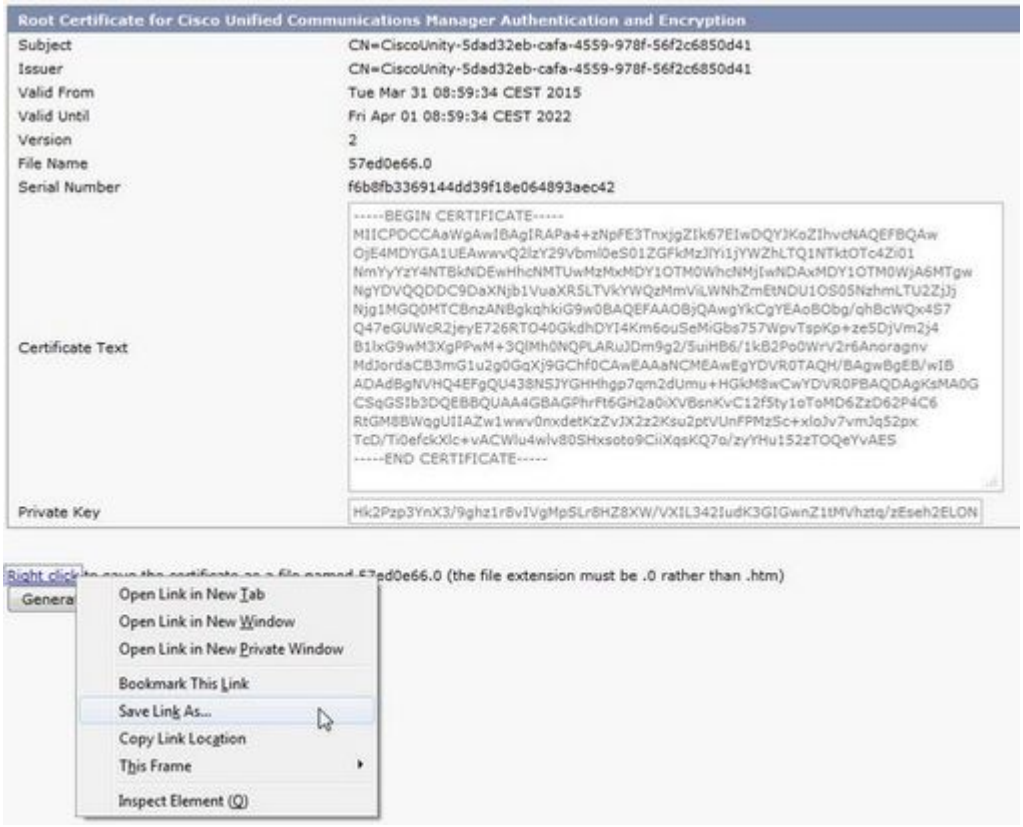
注意：上传证书后，需要重新启动Cisco CallManager服务以使证书生效。

配置安全SCCP端口

配置CUC

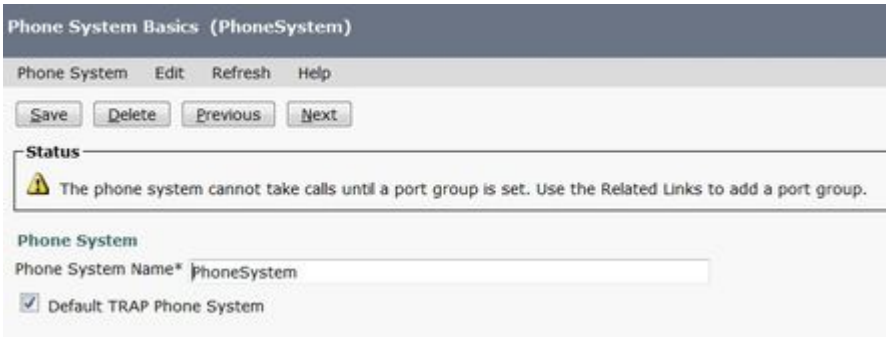
1.下载CUC根证书

导航到CUC管理>电话集成>安全>根证书。右键点击URL，将证书另存为名为<filename>.0（文件扩展名必须是。0而不是.htm）的文件，然后点击Save:



2.创建电话系统/修改现有的电话系统。

导航到电话集成>电话系统。您可以使用已经存在的电话系统或创建新系统。



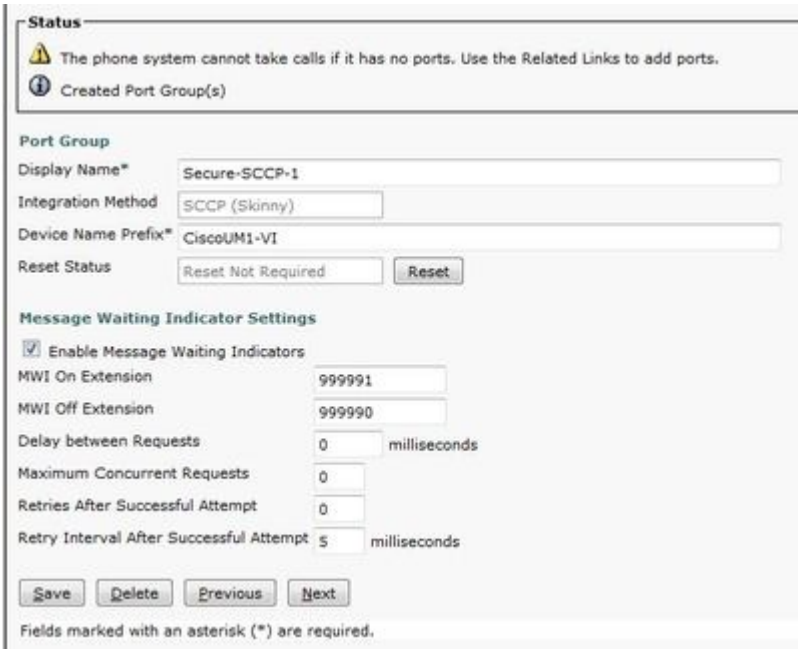
3.添加新的SCCP端口组

在Phone System Basics页面的Related Links下拉框中，选择Add Port Group，然后选择Go。在配置窗口中，输入以下信息：

- 电话系统:
- 端口组类型： SCCP
- 设备名称前缀*: CiscoUM1-VI
- MWI On分机：

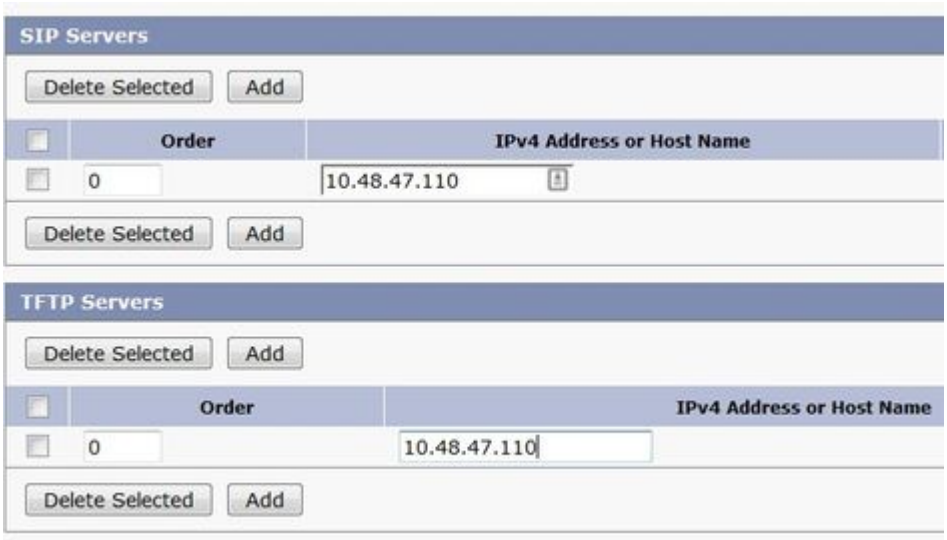
- MWI关闭分机：

注意：此配置必须与CUCM上的配置匹配。



4.编辑服务器

导航到Edit > Servers，然后从CUCM集群添加TFTP服务器。

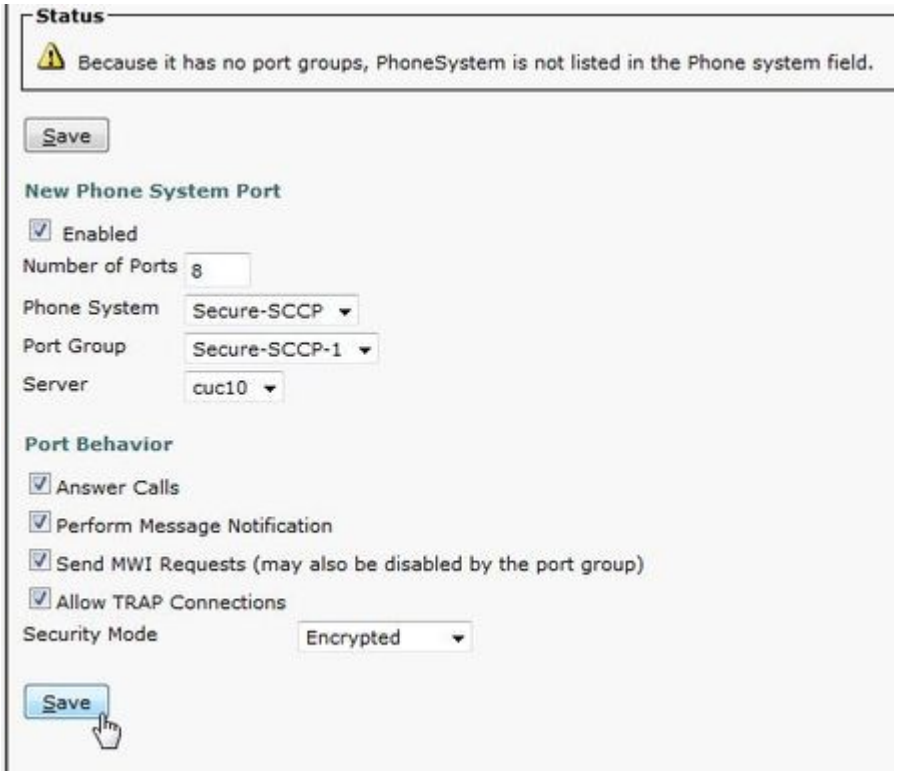


注意：必须提供正确的TFTP地址。CUC服务器按照说明从此TFTP下载CTL文件。

5.添加安全SCCP端口

在“端口组基本信息”页的“相关链接”下拉框中，选择添加端口，然后选择转到。在配置窗口中，输入以下信息：

- 启用:已选中
- 端口数量:
- 电话系统:
- 端口组:
- 服务器：
- 端口行为：
- 安全模式:　　已加密

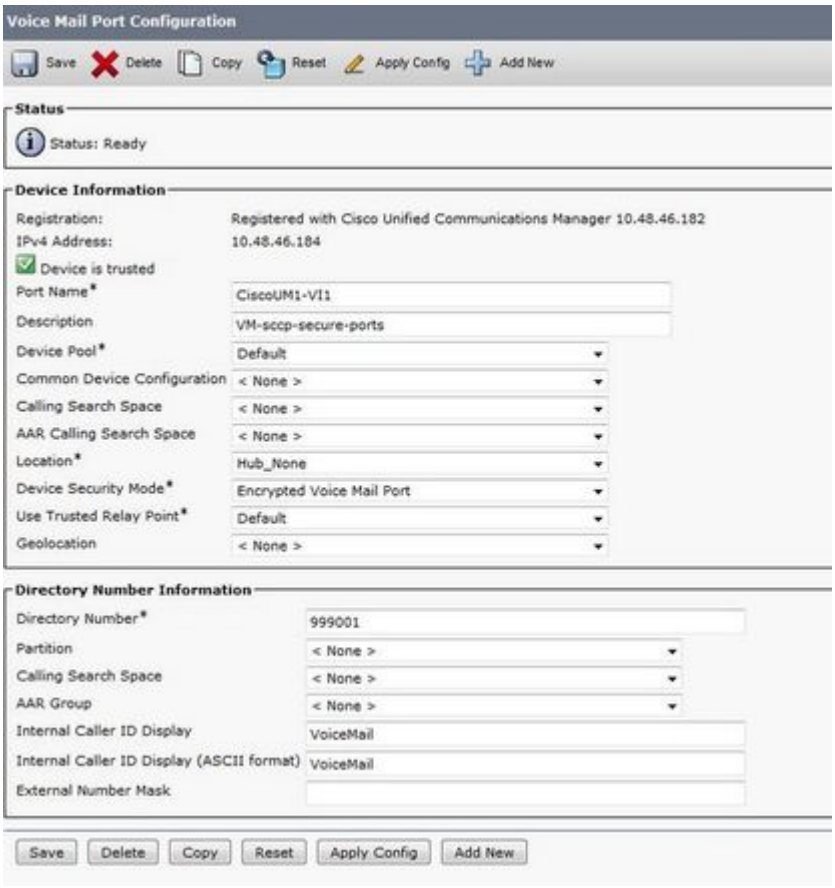


配置CUCM

1.添加端口

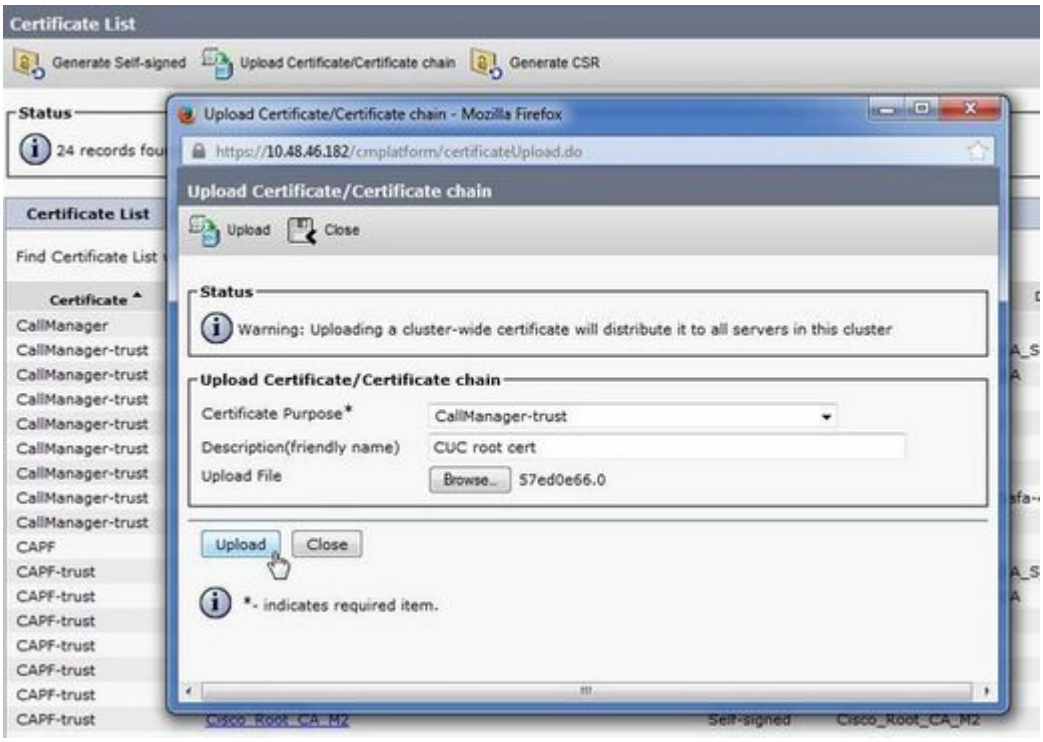
依次导航至 CUCM Administration > Advanced features > Voice Mail Port Configuration > Add New。

照常配置SCCP语音邮件端口。唯一的区别在于在端口配置下的设备安全模式下，需要选择Encrypted Voice Mail Port选项。



2.将CUC根证书上传为CallManager-trust

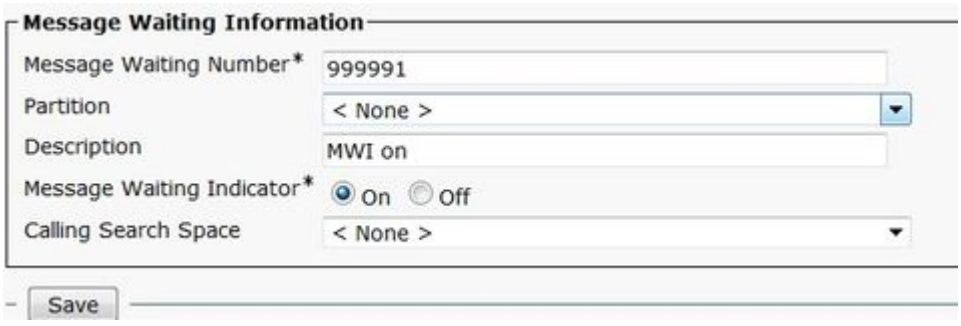
导航到OS Administration > Security > Certificate Management > Upload Certificate/Certificate Chain，然后以CallManager-trust形式在配置为与CUC服务器通信的所有节点上上上传CUC根证书。

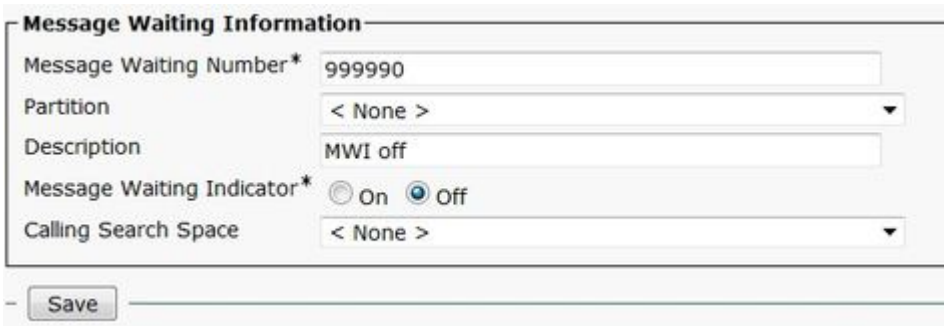


注意：上传证书后，需要重新启动Cisco CallManager服务以使证书生效。

3. 配置消息等待信息(MWI)开/关分机

导航到CUCM Administration > Advanced Features > Voice Mail Port Configuration并配置MWI开/关分机。MWI编号必须与CUC配置匹配。

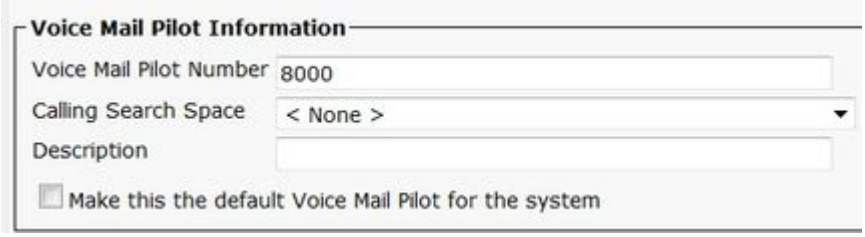




4.创建语音邮件引导

为集成创建语音邮件引导(Advanced Features > Voice Mail > Voice Mail Pilot)。 输入以下值：

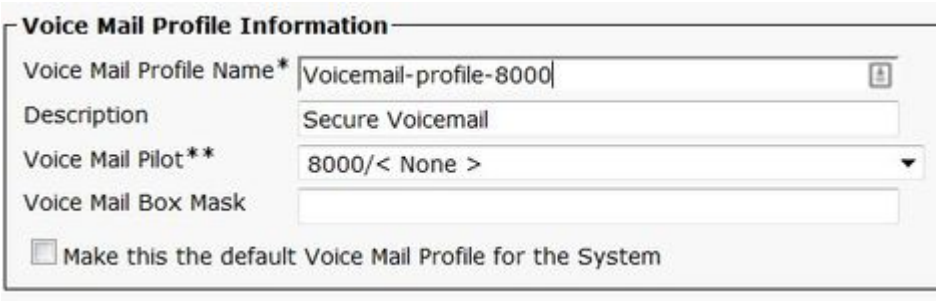
- 语音邮件引导号：
- 呼叫搜索空间： 包括包含用作引导的路由模式的分区>



5.创建语音邮件配置文件

创建语音邮件配置文件以将所有设置链接在一起(Advanced Features > Voice Mail > Voice Mail Profile)。 输入此信息：

- 语音邮件引导:
- 语音信箱掩码：

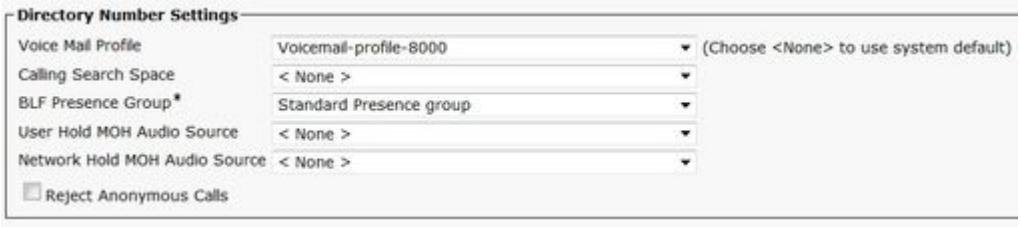


6.将语音邮件配置文件分配给DN

将语音邮件配置文件分配给打算使用安全集成的DN。更改DN设置后，单击Apply Config按钮：

导航到呼叫路由>目录号码，然后更改为：

- 语音邮件配置文件: 语音邮件配置文件–8000

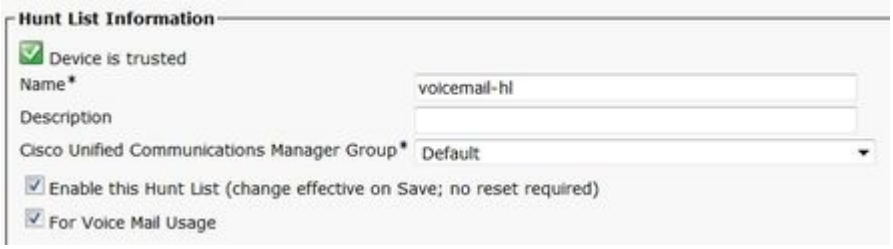


7. 创建语音邮件寻线组

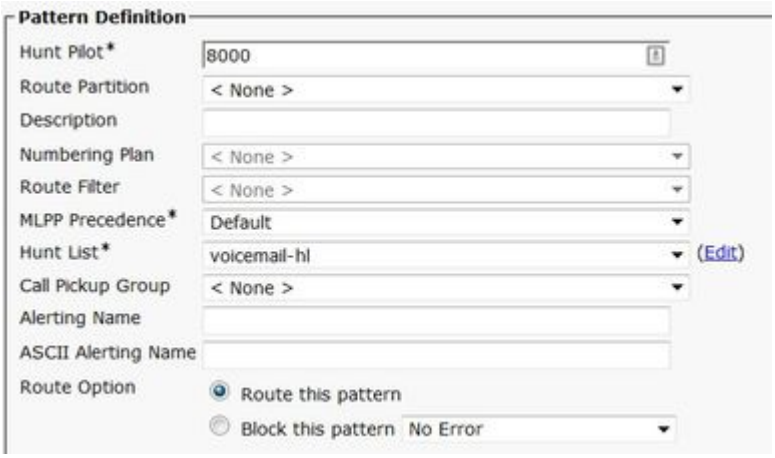
a)添加新的线路组(呼叫路由>路由/寻线>线路组)



b)添加新的语音邮件寻线列表(呼叫路由>路由/寻线>寻线列表)



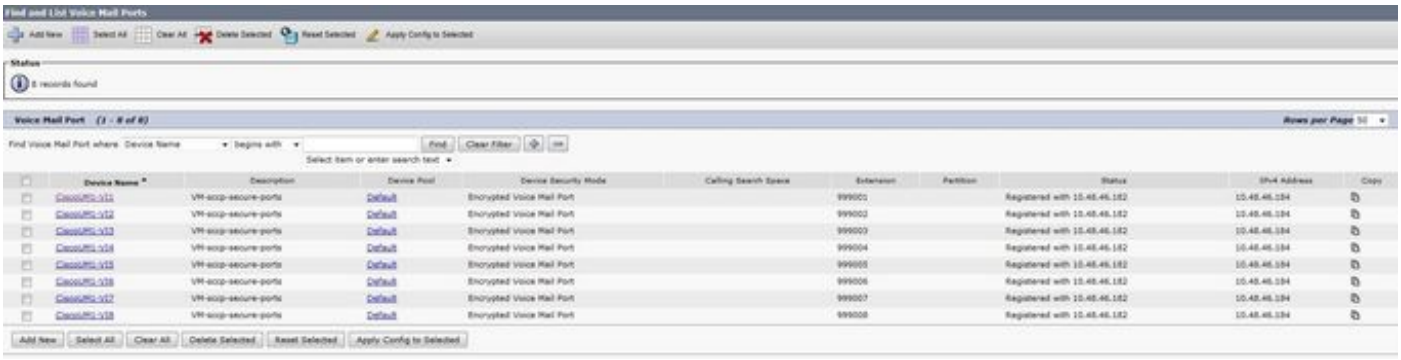
c)添加新的寻线引导(呼叫路由>路由/寻线>寻线引导)



验证

SCCP端口验证

导航到CUCM Administration > Advance Features > Voice Mail > Voice Mail Ports并验证端口注册。



按电话上的Voice Mail按键以呼叫语音邮件。如果用户的分机未在Unity Connection系统上配置，您将听到开场问候语。

安全SIP中继验证

按电话上的Voice Mail按键以呼叫语音邮件。如果Unity Connection系统中未配置用户的分机，您将听到开场问候语。

或者，您可以启用SIP OPTION保持连接以监控SIP中继状态。此选项可以在分配给SIP中继的SIP配置文件中启用。启用此选项后，您可以通过Device > Trunk监控SIP中继状态，如下图所示。



安全RTP呼叫验证

验证对Unity Connection的呼叫中是否显示挂锁图标。这意味着RTP流已加密（设备安全配置文件必须安全才能运行），如图所示。



故障排除

1.一般故障排除提示

使用以下步骤排除安全集成的故障：

- 验证配置。
- 确保所有相关服务都在运行。(CUCM - CallManager、TFTP、CUC - Conversation Manager)
- 确保服务器之间安全通信所需的端口在网络中处于打开状态（TCP端口2443用于SCCP集成，TCP 5061用于SIP集成）。
- 如果所有这些都正确，则继续收集跟踪。

2.要收集的跟踪

收集这些跟踪以排除安全集成故障。

- 从CUCM和CUC捕获数据包
- CallManager跟踪
- Cisco Conversation Manager跟踪

有关以下内容的其他信息，请参阅以下资源：

如何在CUCM上捕获数据包：

http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-50/112040-packet-capture-cucm-00.html

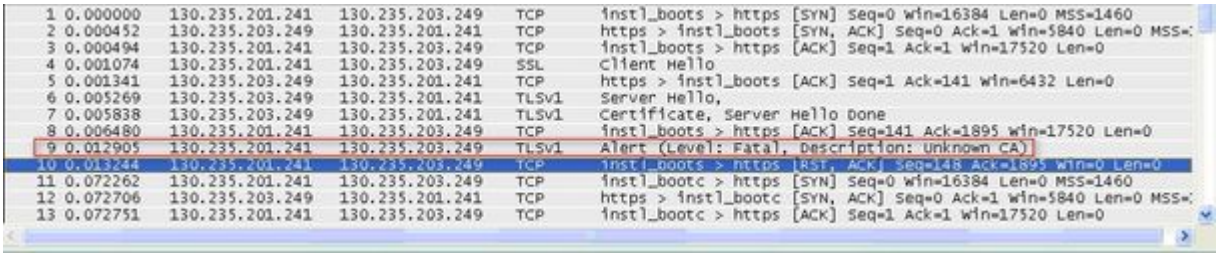
如何在CUC服务器上启用跟踪：

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx/10

常见问题

第 1 种情况：无法建立安全连接（未知CA警报）

从任一服务器收集数据包捕获后，建立TLS会话。



1	0.000000	130.235.201.241	130.235.203.249	TCP	1nstl_boots > https [SYN] Seq=0 Win=16384 Len=0 MSS=1460
2	0.000452	130.235.203.249	130.235.201.241	TCP	https > 1nstl_boots [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
3	0.000494	130.235.201.241	130.235.203.249	TCP	1nstl_boots > https [ACK] Seq=1 Ack=1 Win=17520 Len=0
4	0.001074	130.235.201.241	130.235.203.249	SSL	Client Hello
5	0.001341	130.235.203.249	130.235.201.241	TCP	https > 1nstl_boots [ACK] Seq=1 Ack=141 Win=6432 Len=0
6	0.005269	130.235.203.249	130.235.201.241	TLSv1	Server Hello,
7	0.005838	130.235.203.249	130.235.201.241	TLSv1	Certificate, Server Hello Done
8	0.006480	130.235.201.241	130.235.203.249	TCP	1nstl_boots > https [ACK] Seq=141 Ack=1895 Win=17520 Len=0
9	0.012905	130.235.201.241	130.235.203.249	TLSv1	Alert (Level: Fatal, Description: Unknown CA)
10	0.013244	130.235.201.241	130.235.203.249	TCP	1nstl_boots > https [RST, ACK] Seq=148 Ack=1895 Win=0 Len=0
11	0.072262	130.235.201.241	130.235.203.249	TCP	1nstl_bootc > https [SYN] Seq=0 Win=16384 Len=0 MSS=1460
12	0.072706	130.235.203.249	130.235.201.241	TCP	https > 1nstl_bootc [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=
13	0.072751	130.235.201.241	130.235.203.249	TCP	1nstl_bootc > https [ACK] Seq=1 Ack=1 Win=17520 Len=0

客户端向服务器发出警报，其中显示Unknown CA错误，原因仅仅是客户端无法验证服务器发送的证书。

有两个可能性：

1)CUCM发送警报Unknown CA

- 验证当前CUC根证书已上传到与CUC服务器通信的服务器上。
- 确保在相应的服务器上重新启动CallManager服务。

2)CUC发送警报Unknown CA

- 验证CUC服务器上的Port Group > Edit > Servers配置中是否正确输入了TFTP IP地址。
- 验证可以从连接服务器访问CUCM TFTP服务器。
- 确保CUCM TFTP上的CTL文件是最新的（将“show ctl”的输出与证书进行比较，如操作系统管

理页面所示）。 如果不运行CTLClient，请重新运行CTLClient。
- 重新启动CUC服务器，或者删除并重新创建端口组以从CUCM TFTP重新下载CTL文件。

第 2 种情况：无法从CUCM TFTP下载CTL文件

此错误出现在对话管理器跟踪中：

<#root>

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving server ce
MiuGeneral,25,Error executing tftp command

'tftp://10.48.47.189:69/CTLFile.tlv' res=68 (file not found on server)


MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true),

error retrieving server certificates.


Arbiter,-1,Created port PhoneSystem-1-001 objectId='7c2e86b8-2d86-4403-840e-16397b3c626b' as ID=1
MiuGeneral,25,Port group object 'b1c966e5-27fb-4eba-a362-56a5fe9c2be7' exists
MiuGeneral,25,FAILED SetInService=true parent port group is out of service:
```

解决方案：

1.在Port group > Edit > Servers配置中仔细检查TFTP服务器是否正确。

2.验证CUCM集群是否处于安全模式。

3.检验CUCM TFTP上是否存在CTL文件。

实例3：其它WRR加权修改端口未注册

此错误出现在对话管理器跟踪中：

```
MiuSkinny,23,Failed to retrieve Certificate for CCM Server <CUCM IP Address>
MiuSkinny,23,Failed to extract any CCM Certificates - Registration cannot proceed. Starting retry timer
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxx.tlv]
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM IP Add
```

解决方案：

1.这很可能是由于CUCM和CUC上的CTL文件的md5校验和不匹配，这是由于

证书.重新启动CUC服务器以刷新CTL文件。

缺陷

CSCum48958 - CUCM 10.0（IP地址长度不正确）

CSCtn87264 -安全SIP端口的TLS连接失败

CSCur10758 -无法清除已吊销的证书Unity Connection

CSCur10534 - Unity Connection 10.5 TLS/PKI互操作冗余CUCM

CSCve47775 -用于在CUC上更新和检查CUCM的CTLFile方法的功能请求

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。