安全外部电话服务配置示例

目录

简介

本文档介绍如何配置安全外部电话服务。此配置可与任何第三方服务配合使用，但为了进行演示，本文档使用远程Cisco Unified Communications Manager(CUCM)服务器。

作者：思科TAC工程师Jose Villalobos。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM
- CUCM证书
- 电话服务

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM 10.5.X/CUCM 11.X
- 瘦客户端控制协议(SCCP)和会话发起协议(SIP)电话向CUCM注册
- 本实验使用主题备用名称(SAN)证书。
- 外部目录将位于SAN证书上。
- 对于本示例中的所有系统，证书颁发机构(CA)将相同，所有证书都是CA符号。
- 域名服务器(DNS)和网络时间协议(NTP)需要进行属性设置和工作。

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，请确保您了解任何更改的潜在影响。

相关产品

本文档也可用于以下硬件和软件版本：

- CUCM 9.X/10.X/11.X

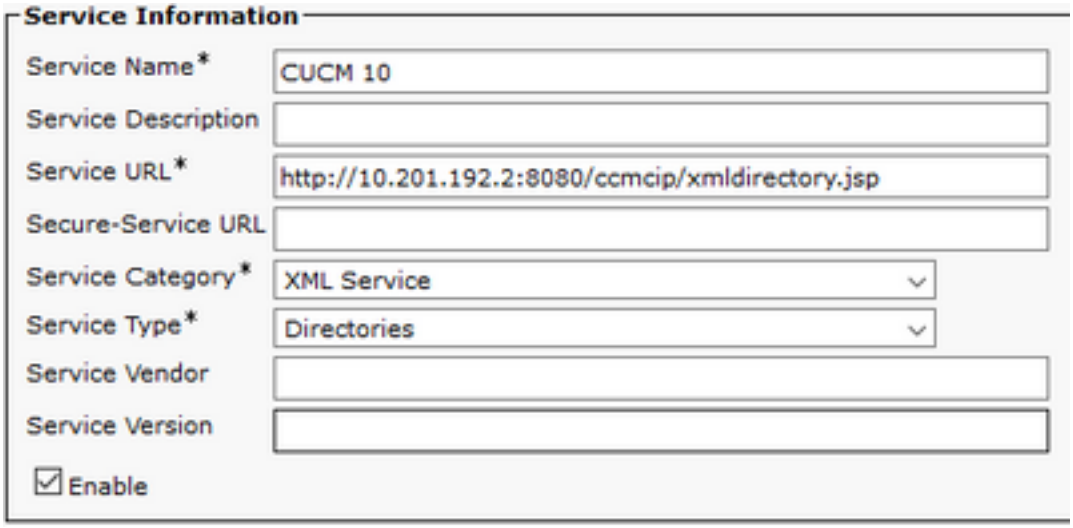
配置步骤

步骤1.在系统上设置服务URL。

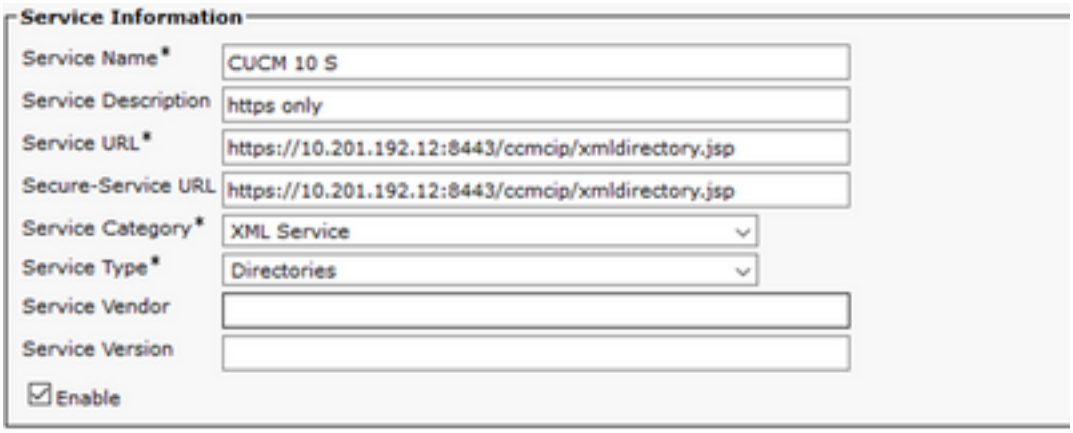
设置超文本传输协议(HTTP)和安全超文本传输协议(HTTPS)作为概念证明。最后一个想法是仅使用安全HTTP流量。

导航至**Device> Device Settings> Phone service> Add new**

仅 HTTP



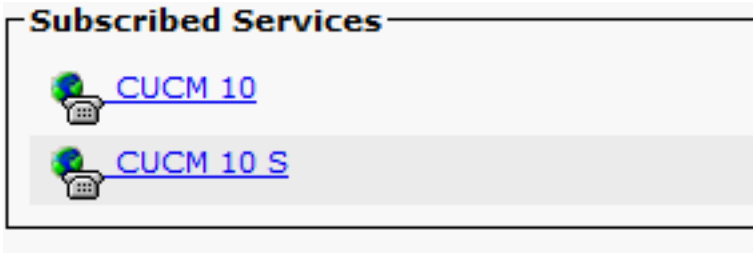
仅 HTTPS



> **警告**：如果添加了企业订用**的检查，**则可跳过步骤2。但是，此更改会重置所有电话，因此请确保您了解潜在影响。

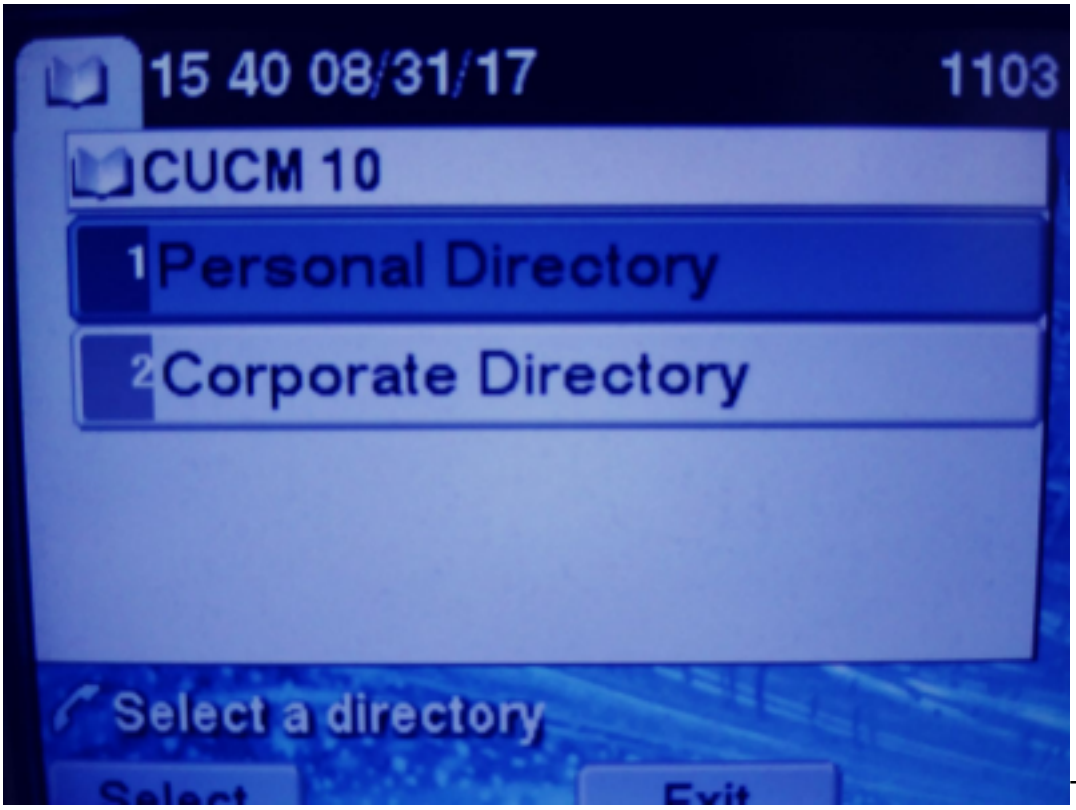
步骤2.将电话订用到服务。

Natigate to **Device>Phone>Subscriber/Unsubscribe service。**



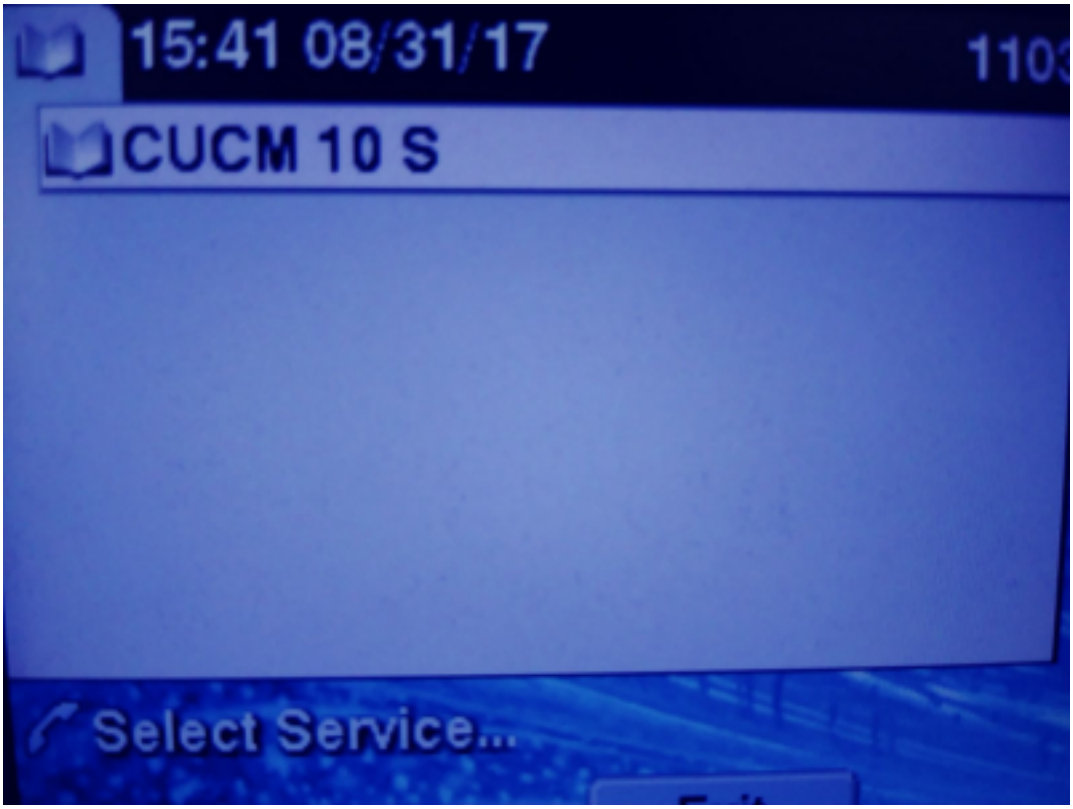
此时，如果应用程序提供HTTP，您必须能够访问服务，但https仍未打开。

HTTP



TTP

HTTPS



HTTPS将显示“**未**找到主**机**”错误，因为事实，TVS服务无法对电话进行身份验证。

步骤3.将外部服务证书上传到CUCM。

仅将外部服务作**为Tomcat信任上传**。确保服务在所有节点上重置。

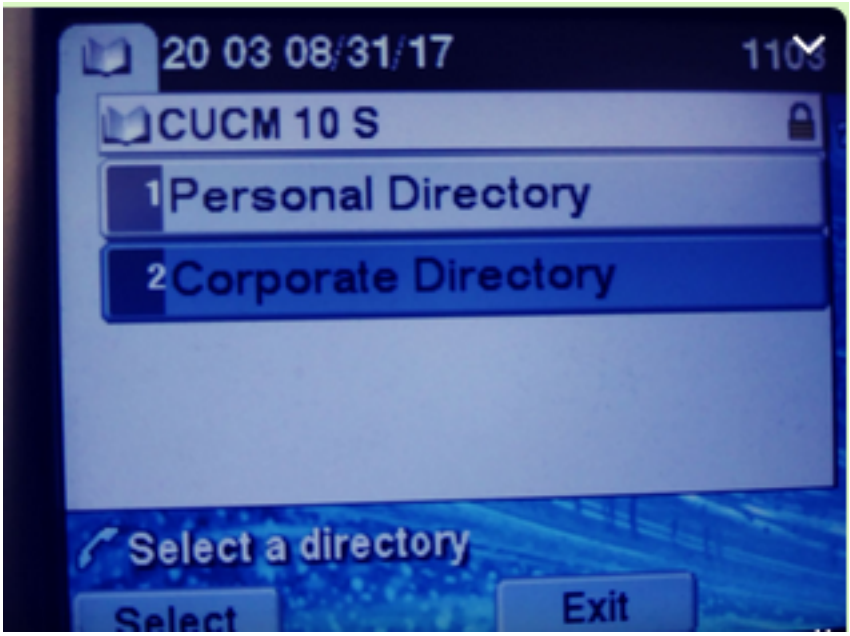
此类证书不存储在电话上，而是电话必须与TVS服务进行检查，以查看它是否建立了HTTPS连接。

导航至**OS admin> Certificate> Certificate upload。**

从SSH重置所有节点上的CUCM Tomcat服务。

```
admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
arted properly, execute the same command again.
Service Manager is running
```

完成这些步骤后，电话必须能够访问HTTPS服务而无问题



常见问题解答(FAQ)

交换证书后，HTTPS仍然失败，“找不到主机”。

— 检查电话注册的节点，并确保在节点上看到第三方证书。

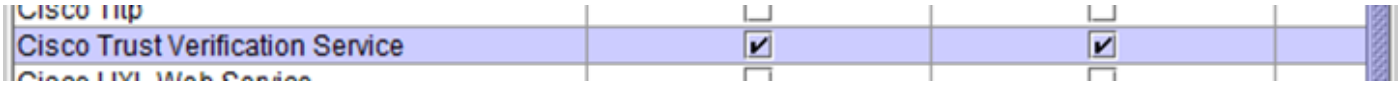
— 重置特定节点上的tomcat。

— 检查DNS，确保证书的公用名(CN)可以解析。

故障排除

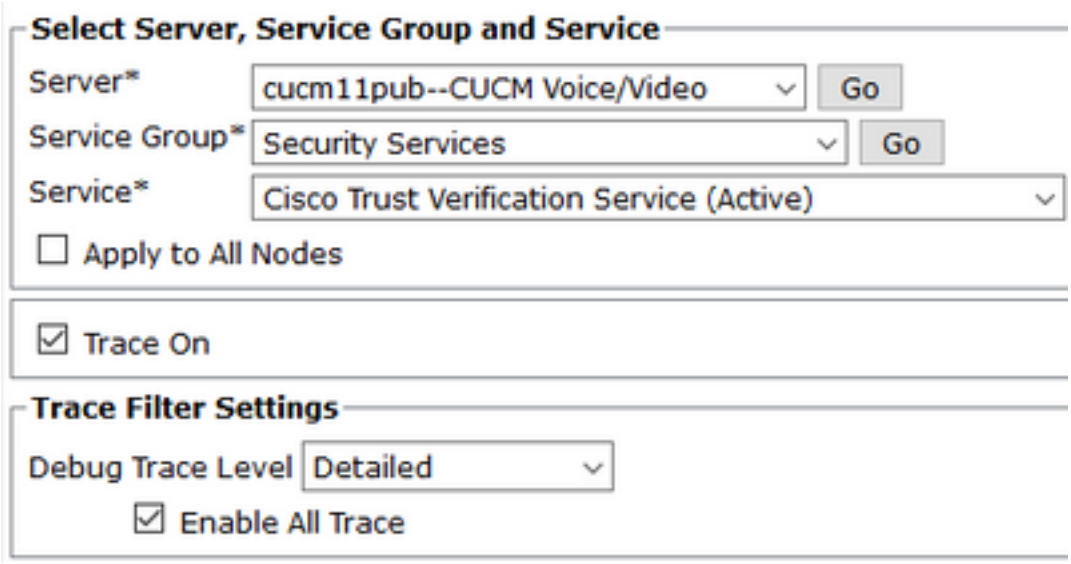
收集CUCM TVS日志必须提供良好信息

导航至**RTMT>System>Trace & log Central > Collect log files**



注意：从所有节点收集日志并确保TVS日志设置为详细。

TVS日志设置为详细



跟踪示例

```
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificate</table><tableid>46</tableid><action>I</action>
<user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>1504203457</cdrtim
e><pkid>e6148ee3-3eb5-e955-fa56-
2baa538a88fb</pkid><servername>cucm11pub</servername><subjectname>CN=10.201.192.12,OU=RCH,O=Cisc
o,L=RCH,ST=Tx,C=US</subjectname><issuername>CN=pablogon-
CA,DC=rcdncollab,DC=com</issuername><serialnumber>3d00000008230ded92f687ec03000000000008</serial
number><certificate></certificate><ipv4address>10.201.192.13</ipv4address><ipv6address></ipv6add
ress><timetolive>NULL</timetolive><tkcertificatedistribution>1</tkcertificatedistribution><ifx_r
eplcheck>6460504654345273346</ifx_replcheck></new></msg>
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificate" has been changed
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Looking up the
roles for
11:17:38.291 |   debug Pkid : fead9987-66b5-498f-4e41-c695c54fac98
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - DBChange Notification
received
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificatetrustrolemap</table><tableid>50</tableid><actio
n>I</action><user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>150420
3457</cdrtime><pkid>5ae6e1d2-63a2-4590-bf40-1954bfa79a2d</pkid><fkcertificate>e6148ee3-3eb5-
e955-fa56-
2baa538a88fb</fkcertificate><tktrustrole>7</tktrustrole><ifx_replcheck>6460504654345273346</ifx_
replcheck></new></msg>
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificatetrustrolemap" has been changed
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:46.811 |   debug updateLocalDBCache : Refreshing the local DB certificate cache
11:34:00.131 |   debug Return value after polling is 1
11:34:00.131 |   debug FD_ISSET i=0, SockServ=14

11:34:00.131 |   debug Accepted TCP connection from socket 0x00000014
```