配置安全TSP

目录

简介

本文档介绍Cisco Unified Communications Manager(CUCM)与安全电话服务提供商(TSP)的集成。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM版本11.5及更高版本
- TSP插件

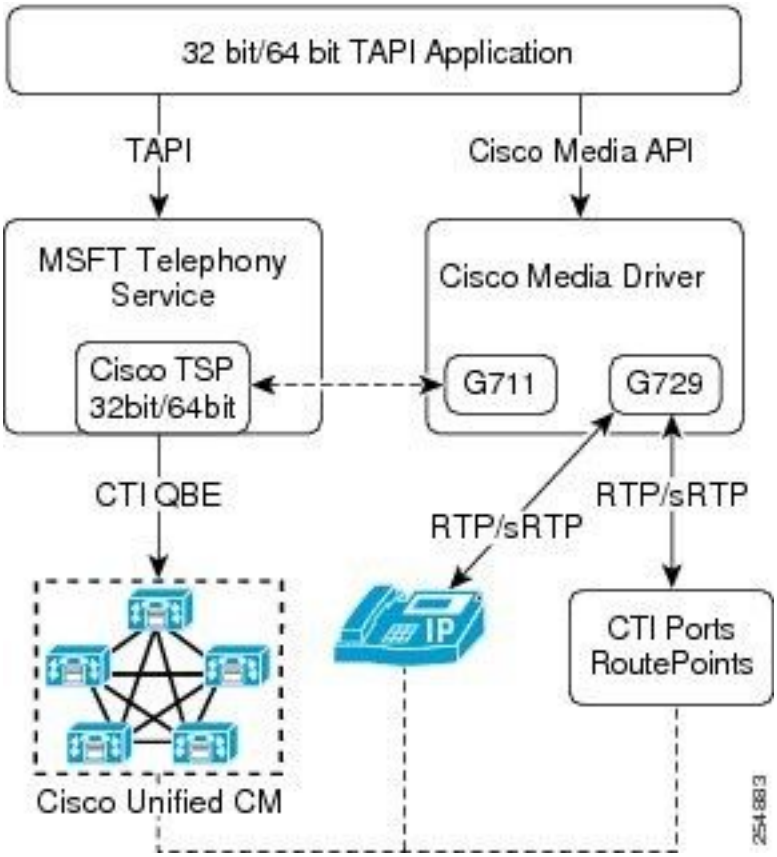
使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科Call Manager版本11.5
- TSP插件

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。

背景信息



以下是思科TSP组件：

- CiscoTSP dll - CiscoTSP提供的TAPI服务实施
- 基于TCP/IP的CTIQBE — 用于监控和控制设备和线路的思科协议
- CTI管理器服务 — 管理CTI资源和设备连接。通过思科TSP和/或JTAPI API接触第三方应用

1. 在安全连接期间，CiscoTSP执行TFTP连接以获取证书信任列表(CTL)文件。
2. 独立群集的CTL文件由ITL恢复、呼叫管理器和证书颁发机构代理功能(CAPF)证书组成。然后，CiscoTSP在CiscoTSP配置中使用提供的实例ID和身份验证字符串进行CAPF握手。
3. 如果握手成功，CiscoTSP将使用最终用户的CAPF实例信息创建QBE证书。

注意：思科TSP不能与离线CA配合使用。

配置

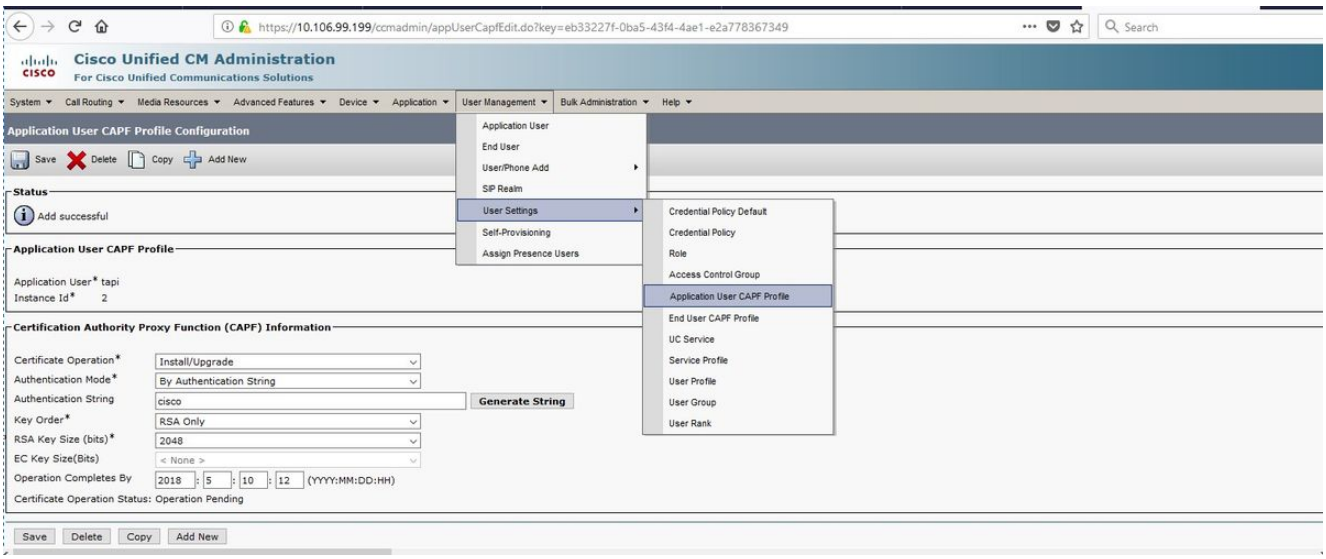
验证

- 验证您执行了安装和配置Cisco CTL客户端所需的所有任务。验证“企业参数配置”窗口中的集群安全模式是1（混合模式）。
- 要使用CAPF，您必须在第一个节点上激活思科CAPF服务。
- 由于同时生成多个证书可能会导致呼叫处理中断，因此思科强烈建议您在计划的维护窗口期间使用CAPF。
- 确保第一个节点在整个证书操作期间正常运行。
- 确保CTI/JTAPI/TAPI应用在整个证书操作期间正常运行。

CUCM

1. 创建应用用户： 验证应用或最终用户是否存在于“标准CTI已启用”组中要将应用用户或最终用户添加到标准CTI安全连接用户组，请单击标准CTI安**全连接链**接要将应用用户或最终用户添加到标准CTI允许接收SRTP密钥材料用户组，请点击**标准CTI允许接收SRTP密钥**材料链接，如图所示。

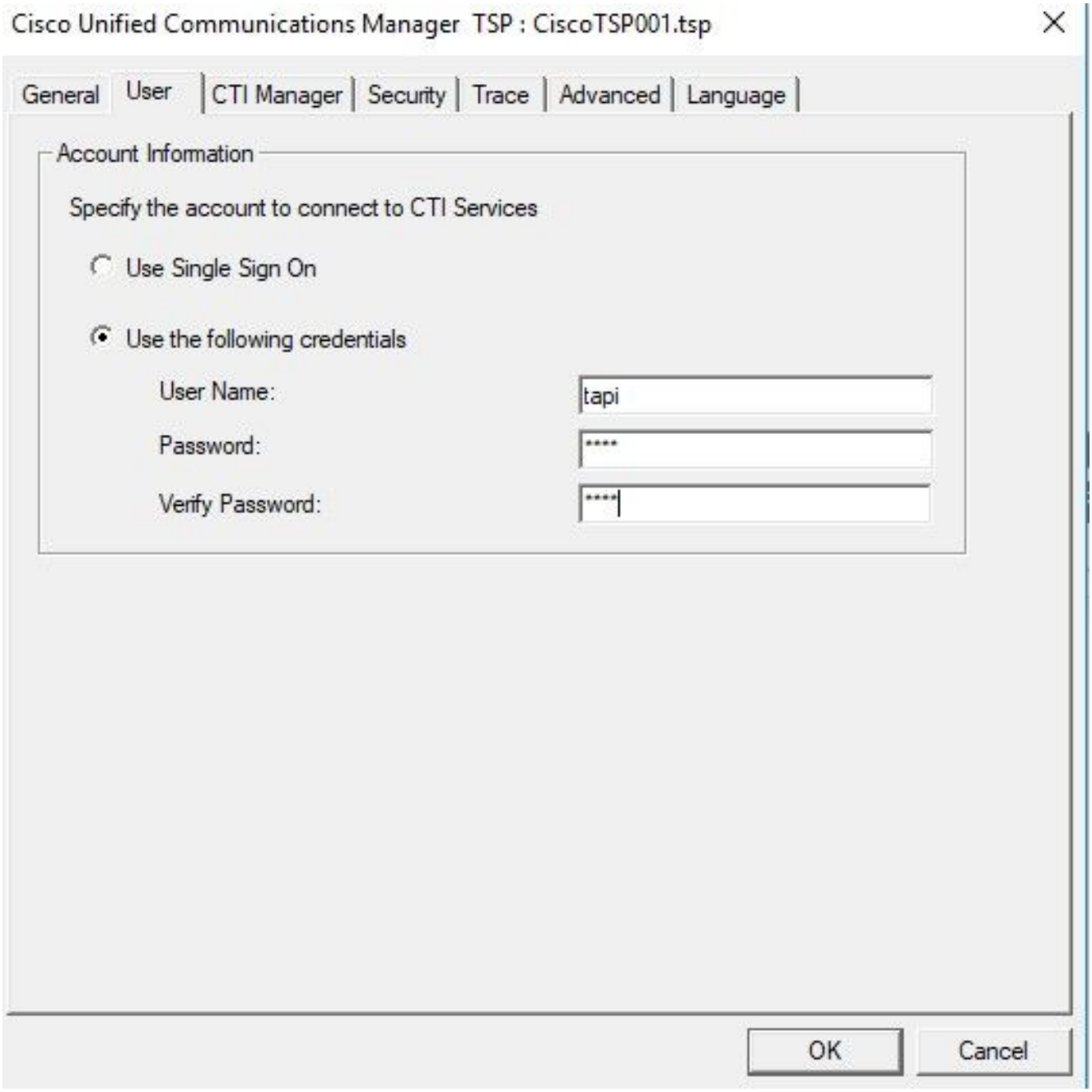
2. 如图所示，为应用用户创建CAPF配置文件。



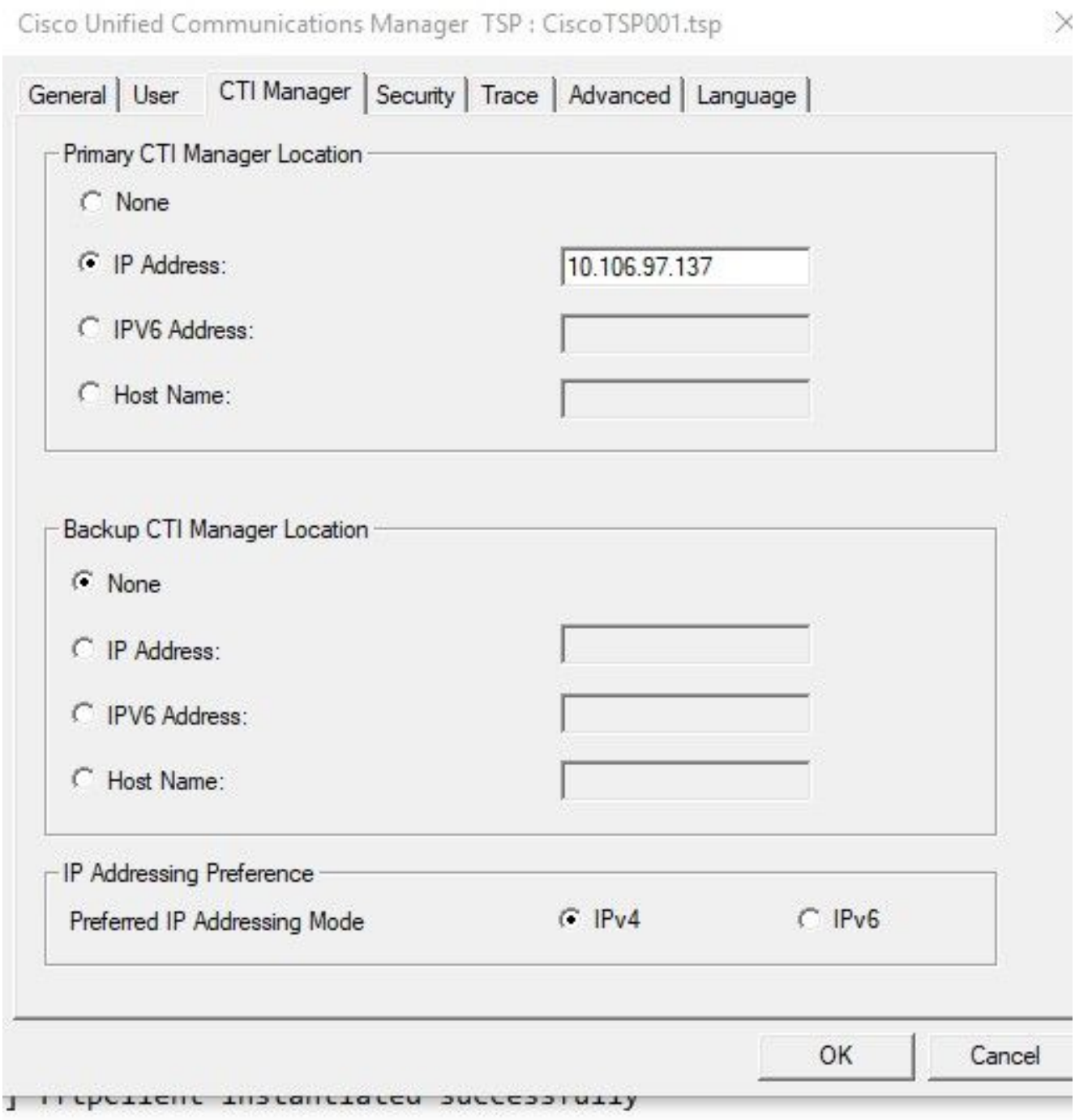
3. 选择在步骤1.(tapi)中创建的用户。
4. 提供任意编号作为实例ID。
5. 选择证书操作在安装升级中。

应用/TSP

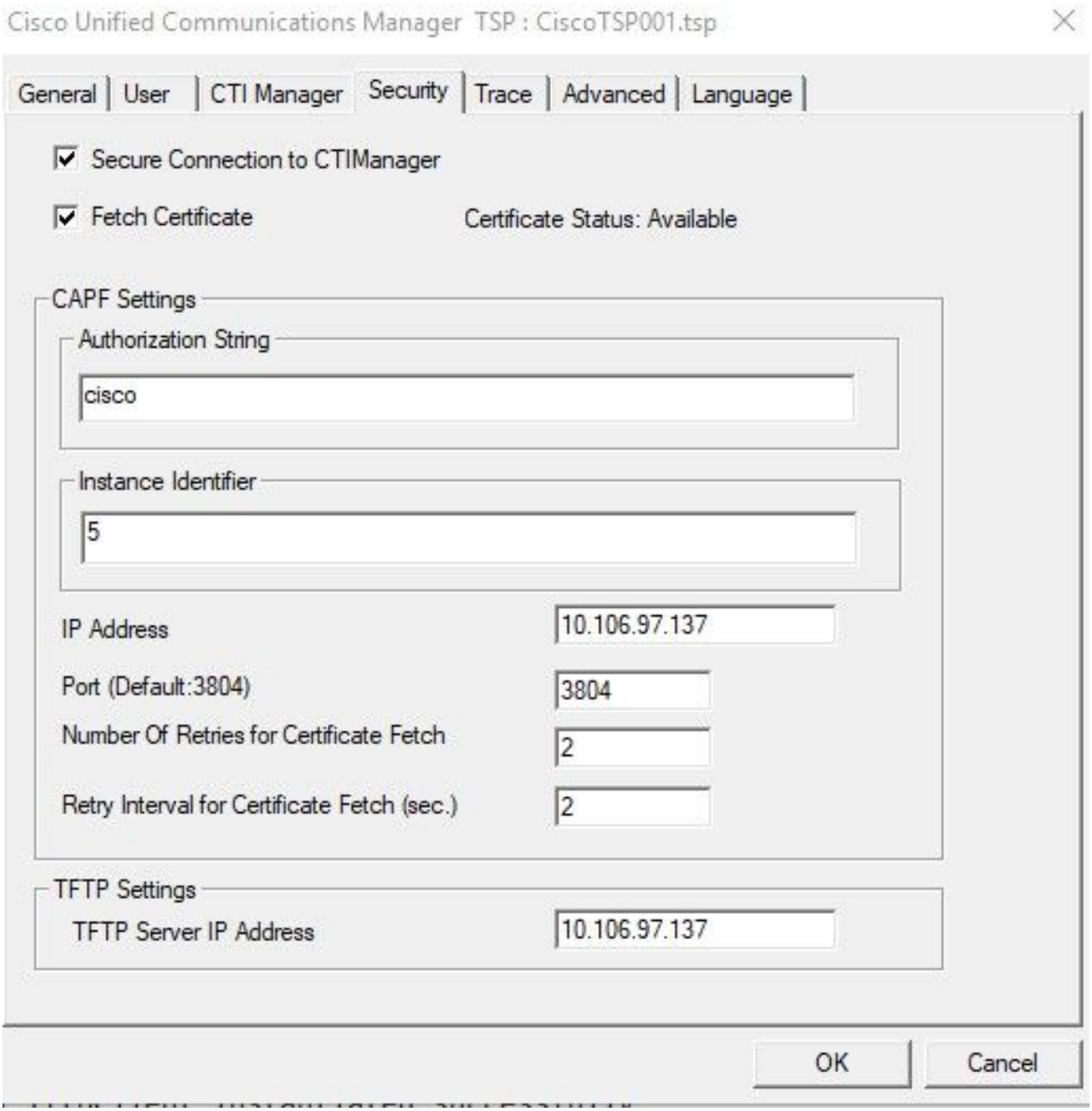
1. 从CUCM下载并安装TAPI插件(导航至“应用”**>“插件”**)。
2. 按照图中所示，添加在CUCM上配置的应用用户详细信息。



3. 输入CTI管理器详细信息，如图所示。



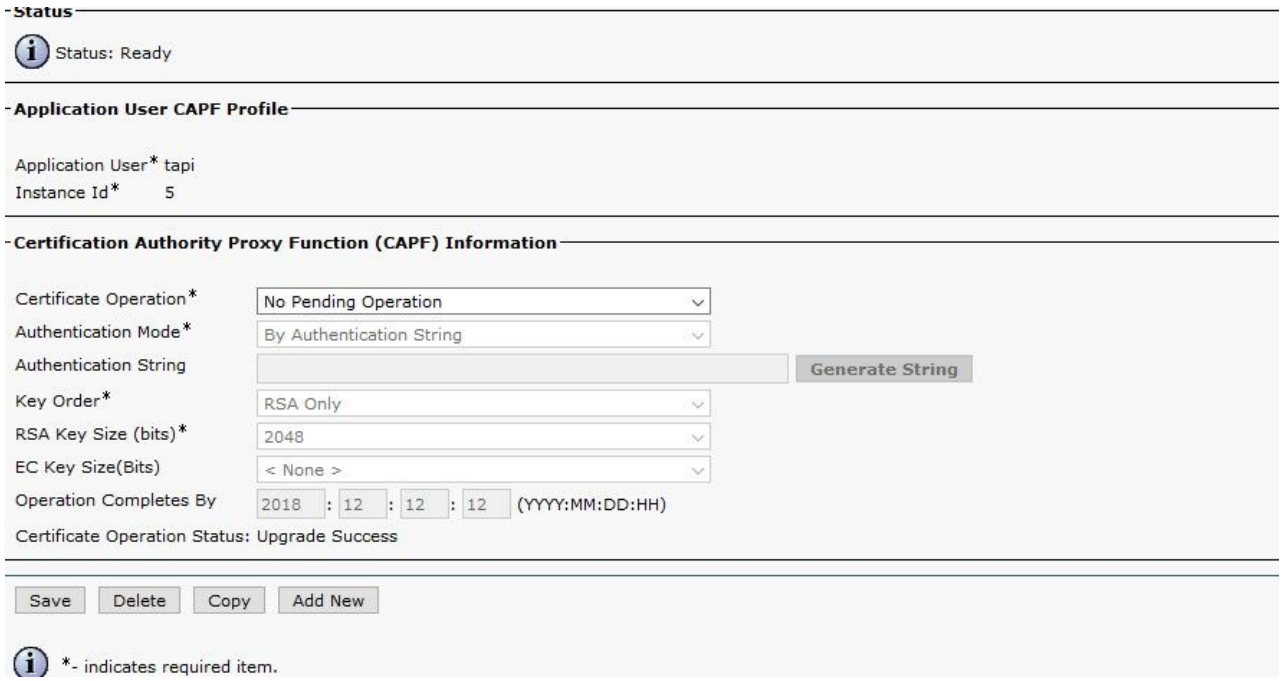
4. 输入与CUCM相同的授权字符串，并在必须下载证书时**第1次点击**获取证书，如图所示。



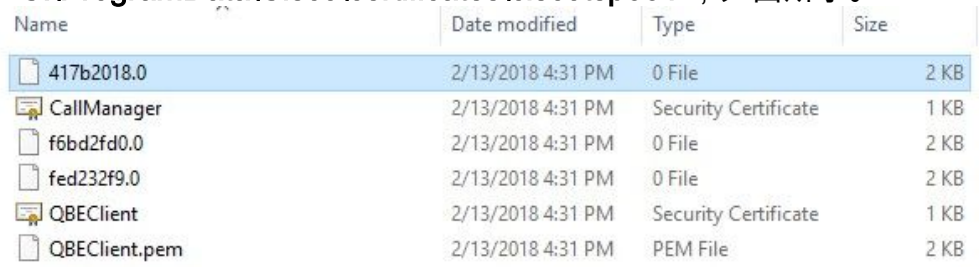
验证

使用本部分可确认配置能否正常运行。

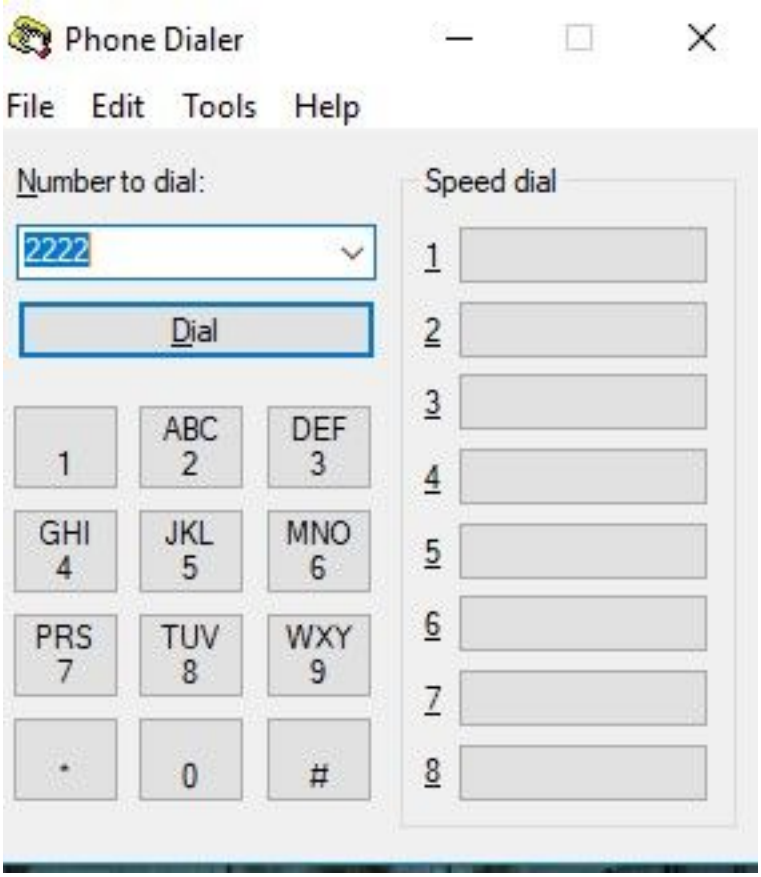
- 在应用用户CAPF配置文件中，必须成功安装本地有效证书(LSC)。如图所示，证书操作状态不得为操作挂起。



- 来自CUCM的所有证书都下载到Windows计算机上。路径：**C:\ProgramData\Cisco\certificates\ciscotsp001** ，如图所示。



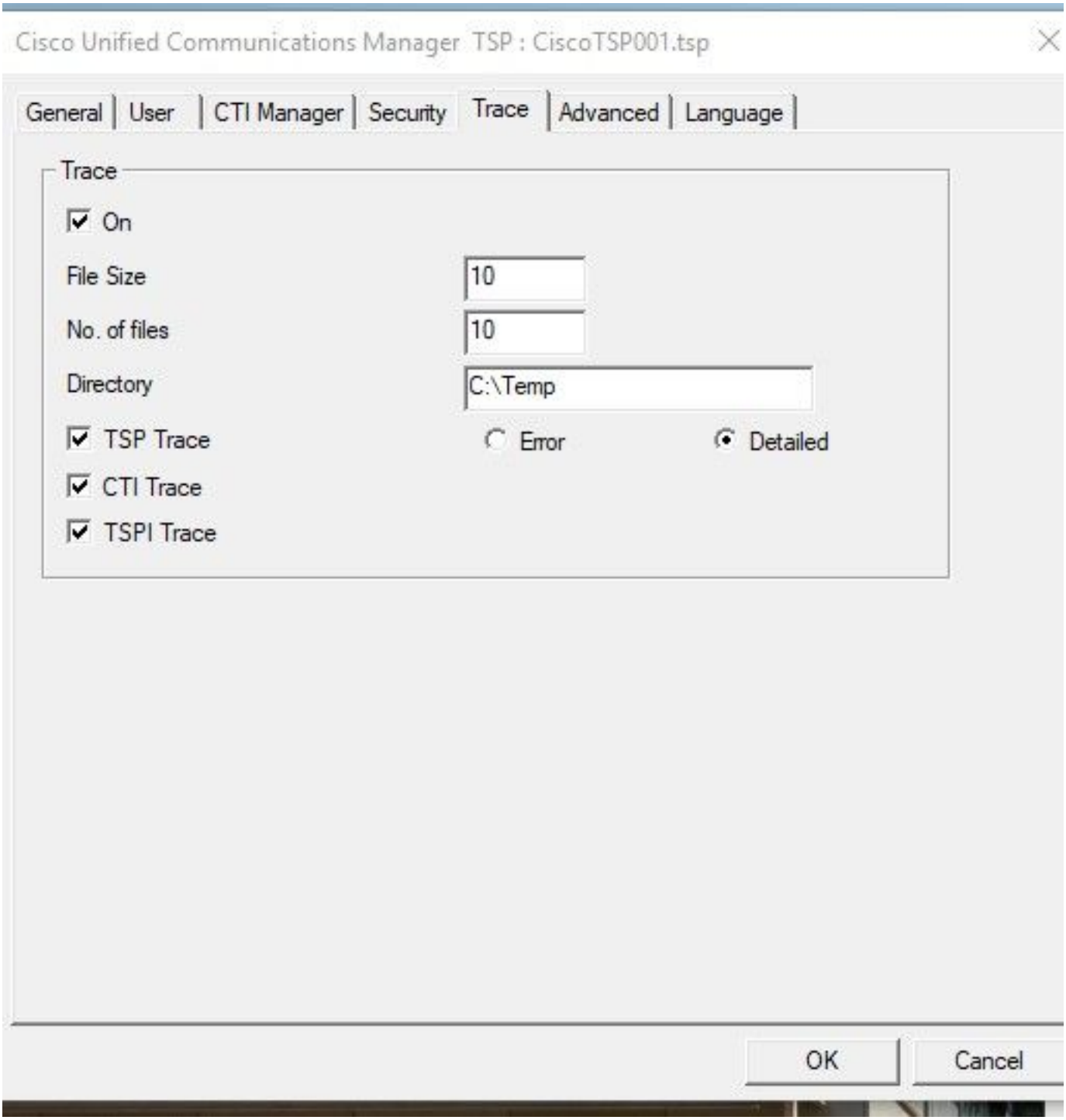
- 您还可以使用Windows内置电话拨号器验证CTI集成是否正常工作。如果CTI集成成功，您可以看到由用户控制的电话的扩展，如图所示。



故障排除

本部分提供了可用于对配置进行故障排除的信息。

- 从应用(TSP)端，您需要将跟踪设置为详细，默认跟踪位置为**C:\Temp**，如图所示。



- 从CUCM端，您需要以下跟踪：TVS跟踪TFTP跟踪CAPF跟踪

TSP的跟踪示例

- 首先，TSP与TFTP服务器进行联系，以获取CTL文件：

```
16:31:04.075 |   CSSLHelper::GetCTLFromTFTP CTLFileName = CTLCAPFA6A63C5.tlv

16:31:04.075 |-->TftpClient::TftpClient()

16:31:04.075 |   TftpClient::TftpClient() [] TftpClient instantiated successfully
```

- 独立群集的CTL文件由ITLrecovery、call manager和CAPF证书组成。然后，CiscoTSP在CiscoTSP配置中使用提供的实例ID和身份验证字符串进行CAPF握手。如果握手成功，CiscoTSP将使用最终用户的CAPF实例信息创建QBE证书：

```
16:31:04.151 |   CSSLHelper::GetCTLFromTFTP fullname =
C:\ProgramData\Cisco\certificates\ciscotsp001/., fileName = .

16:31:04.151 |   CSSLHelper::GetCTLFromTFTP fullname =
C:\ProgramData\Cisco\certificates\ciscotsp001/.., fileName = ..

16:31:04.151 |   CSSLHelper::GetCTLFromTFTP fullname =
C:\ProgramData\Cisco\certificates\ciscotsp001/417b2018.0, fileName = 417b2018.0

16:31:04.154 |   CSSLHelper::GetCTLFromTFTP CERT SUBJECTNAME =
/C=IN/O=cisco/OU=tac/CN=ITLRECOVERY_cucm11-pub/ST=Karnataka/L=BGL

16:31:04.154 |   CSSLHelper::GetCTLFromTFTP fullname =
C:\ProgramData\Cisco\certificates\ciscotsp001/f6bd2fd0.0, fileName = f6bd2fd0.0

16:31:04.156 |   CSSLHelper::GetCTLFromTFTP CERT SUBJECTNAME = /C=IN/O=cisco/OU=tac/CN=cucm11-
pub/ST=Karnataka/L=BGL

16:31:04.156 |   CSSLHelper::GetCTLFromTFTP fullname =
C:\ProgramData\Cisco\certificates\ciscotsp001/fed232f9.0, fileName = fed232f9.0

16:31:04.158 |   CSSLHelper::GetCTLFromTFTP CERT SUBJECTNAME = /C=IN/O=cisco/OU=tac/CN=CAPF-
c5d37298/ST=Karnataka/L=BGL
```

- 安全套接字层(SSL)与CAPF握手成功：

```
16:31:04.177 |   CSSLHelper::startSSLConnectThread() SSLConnect thread created:
threadHandle=1184 threadId=12504

16:31:04.177 |<--CSSLHelper::startSSLConnectThread()

16:31:04.183 |-->CSSLHelper::SSLConnectThreadEntry()

16:31:04.232 |   CSSLHelper::SSLConnectThreadEntry() Handshake: Finished



16:31:04.232 |   CSSLHelper::SSLConnectThreadEntry() SSL connection using AES128-SHA



16:31:04.232 |   CSSLHelper::SSLConnectThreadEntry() SSLConnect thread exiting ...
```

- 使用应用用户详细信息创建的QBE客户端证书：

```
16:31:05.295 |   CAPFclient::openFile() CAPF client: open file
C:\ProgramData\Cisco\certificates\ciscotsp001/QBEClient.cer mode w+b

16:31:05.295 |<--CAPFclient::openFile()

16:31:05.296 |-->CAPFclient::openFile()

16:31:05.299 |   CAPFclient::openFile() CAPF client: open file
C:\ProgramData\Cisco\certificates\ciscotsp001/QBEClient.pem mode w+b
```