配置安全TSP

目录

简介

本文描述与安全电话服务提供商(TSP)的Cisco Unified Communications Manager (CUCM)集成。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM版本11.5和以上
- 插件的TSP

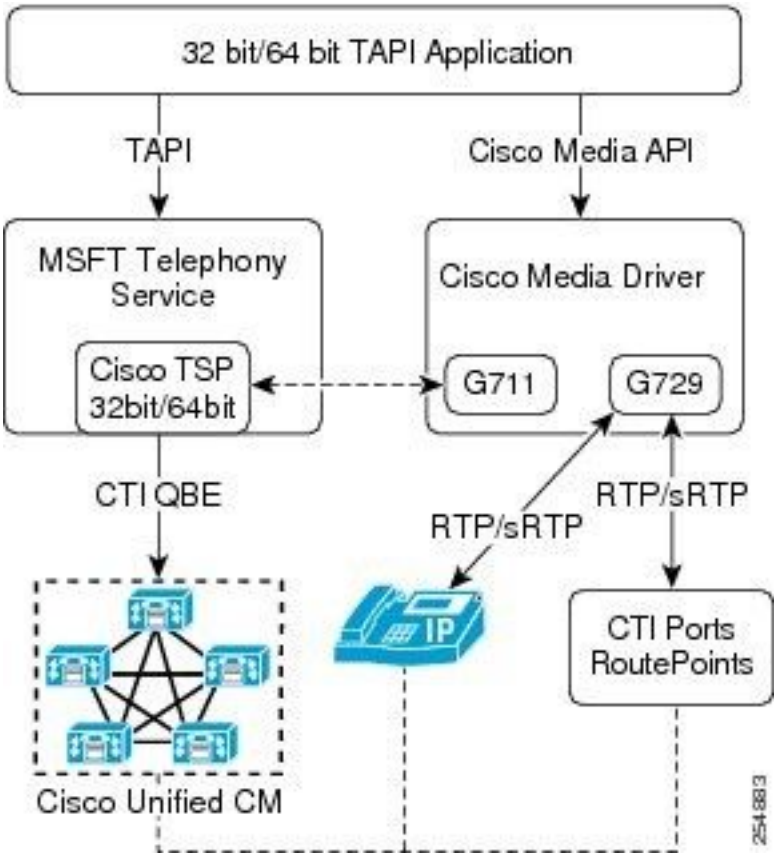
使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Call Manager版本11.5
- 插件的TSP

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。如果您的网络实际，请保证您了解所有命令潜在影响。

背景信息



这些是Cisco TSP组件：

- CiscoTSP dll- TAPI CiscoTSP提供的服务实施
- 在TCP/IP的CTIQBE -思科协议用于的监控和控制设备和线路
- CTI Manager服务-管理CTI资源和连接对设备。显示在第三方应用通过Cisco TSP和JTAPI API

1. 在安全连接时CiscoTSP执行TFTP连接为了获得证书信任列表(CTL)文件。
2. 一独立集群的CTL文件包括ITL恢复、CallManager和认证机关代理功能(CAPF)证书。然后CiscoTSP，与提供的实例ID和认证字符串在CiscoTSP配置里，执行CAPF握手。
3. 如果握手是成功的， CiscoTSP创建与最终用户的CAPF实例的信息的QBE证书。

Note:Cisco TSP不与脱机CA一起使用。

配置

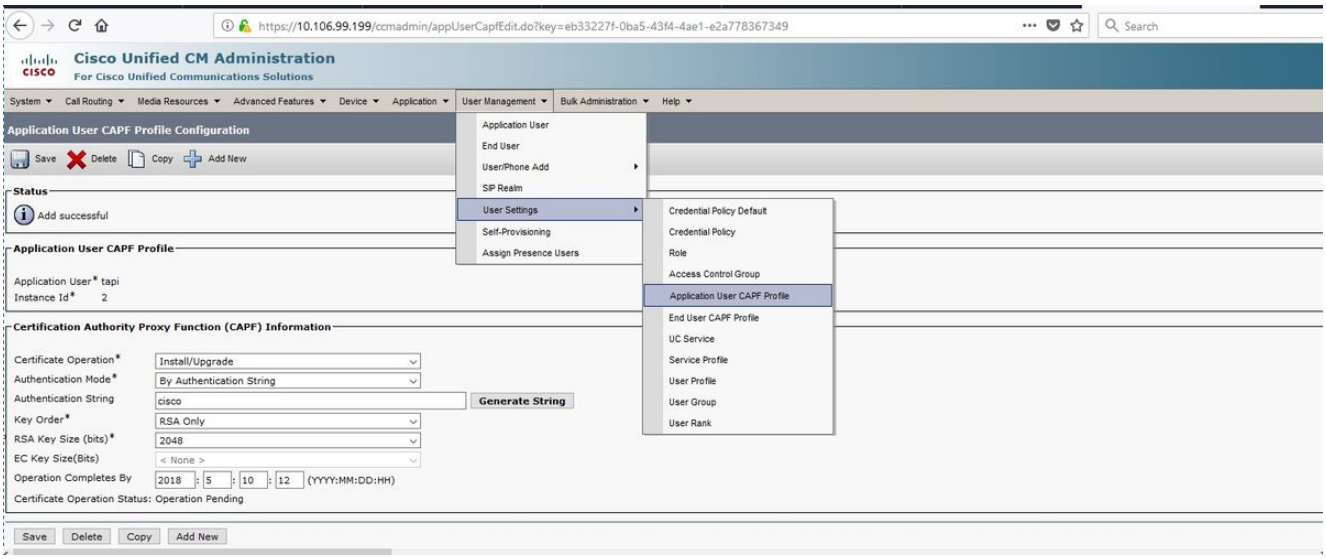
验证

- 验证您执行所有必要的任务为了安装和配置思科CTL客户端。验证在企业参数配置窗口的团星安全模式是1 (混合模式)。
- 为了使用CAPF，您必须启动在第一个节点的思科CAPF服务。
- 由于许多证书的genration也许同时导致呼叫处理中断，思科强烈建议在定期维护窗口期间，您使用CAPF。
- 保证第一个节点是工作和运行在整个证书操作时。
- 保证CTI JTAPI/TAPI应用程序在整个证书操作时是工作。

CUCM

1. 创建应用程序用户： 验证应用程序或最终用户在英文虎报CTI启用的组中存在为了添加应用程序用户或最终用户到英文虎报CTI安全连接用户组，请点击**英文虎报CTI安全连接**链路如镜像所显示，为了添加应用程序用户或最终用户到英文虎报CTI允许SRTP密钥材料用户组的接收，点击**英文虎报CTI允许SRTP密钥材料**链路的**接收**。

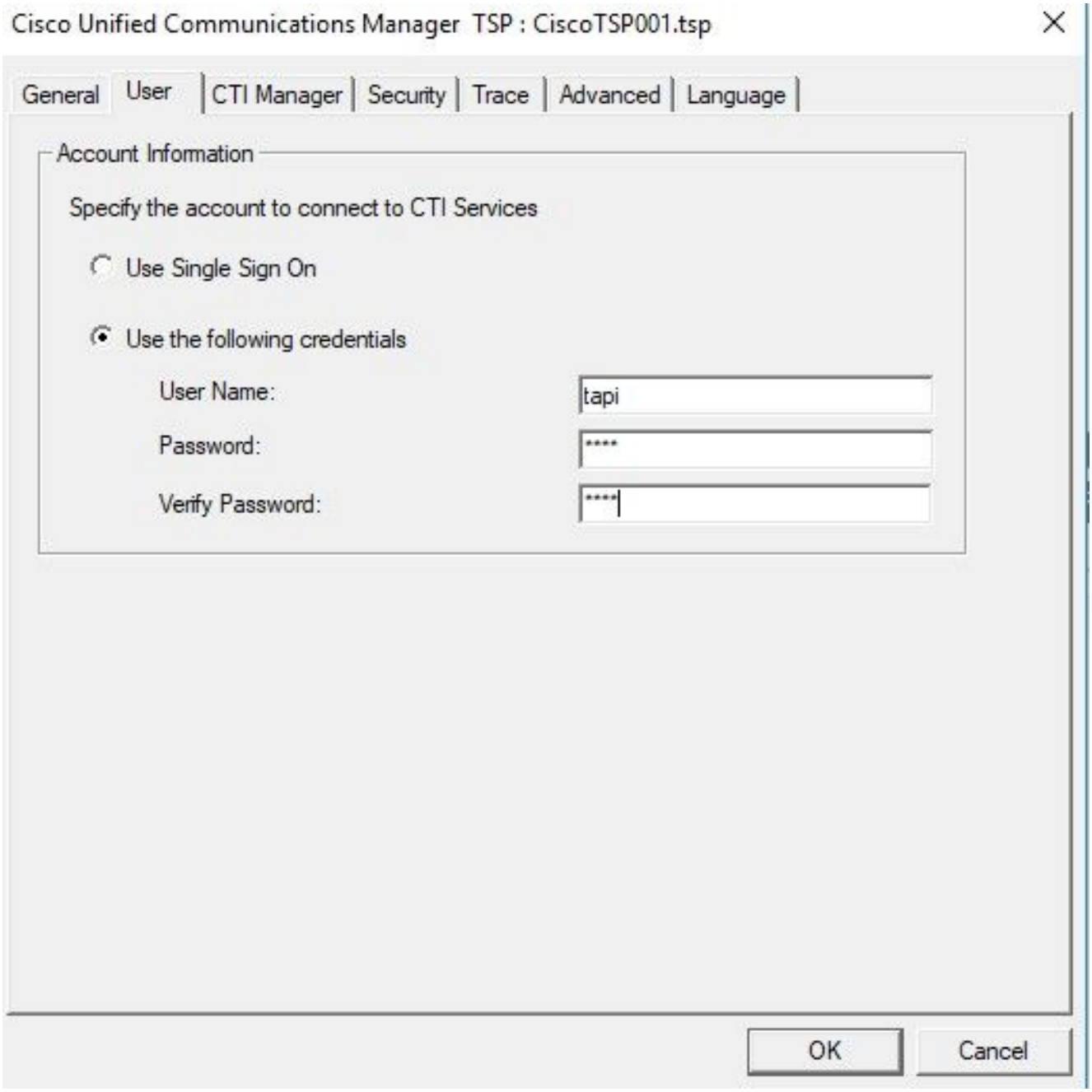
2. 如镜像所显示，创建应用程序用户的CAPF配置文件。



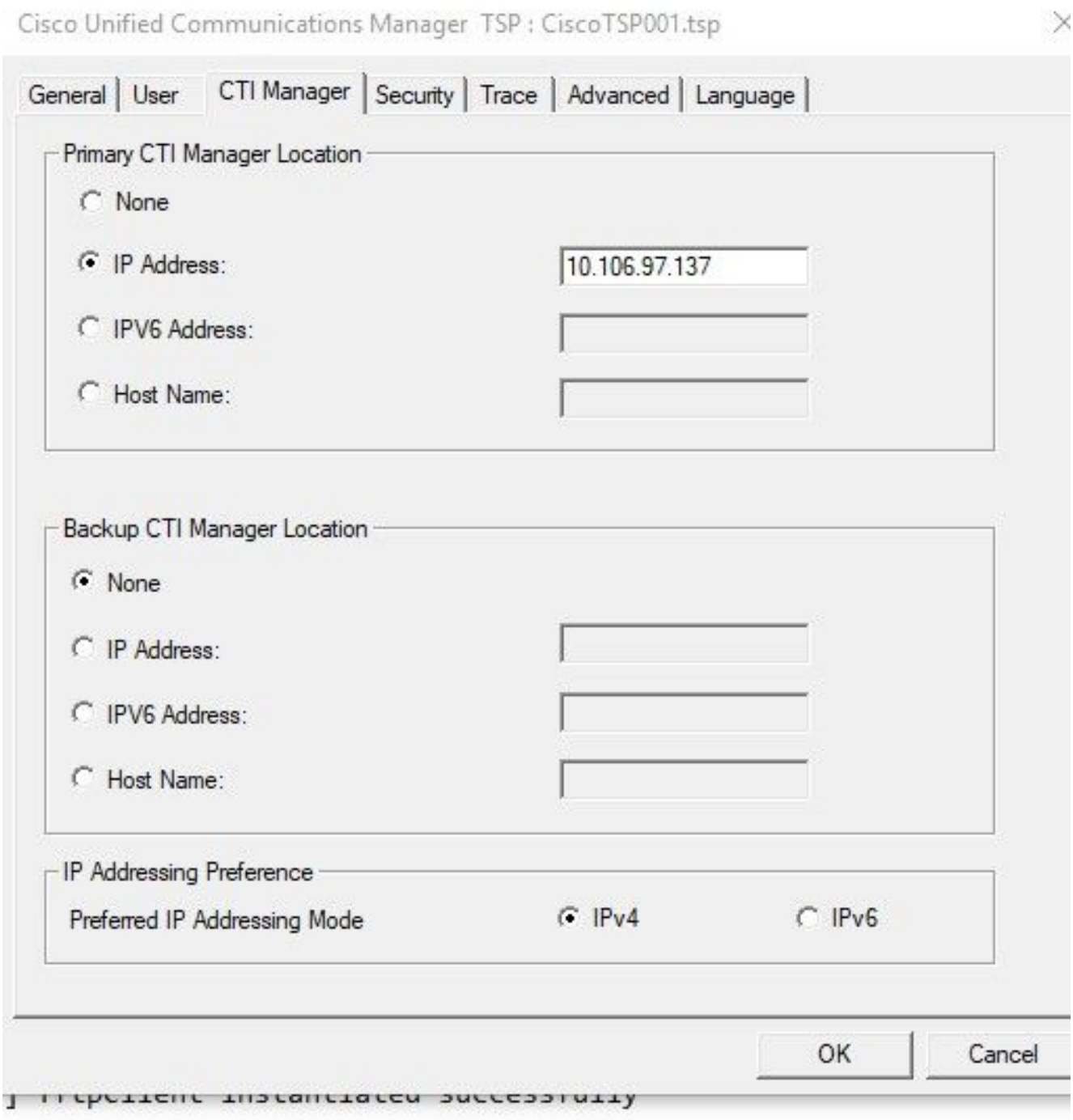
3. 选择用户建立在步骤1. (TAPI)。
4. 给任何编号作为实例ID。
5. 选择在安装升级的证书操作。

Application/TSP

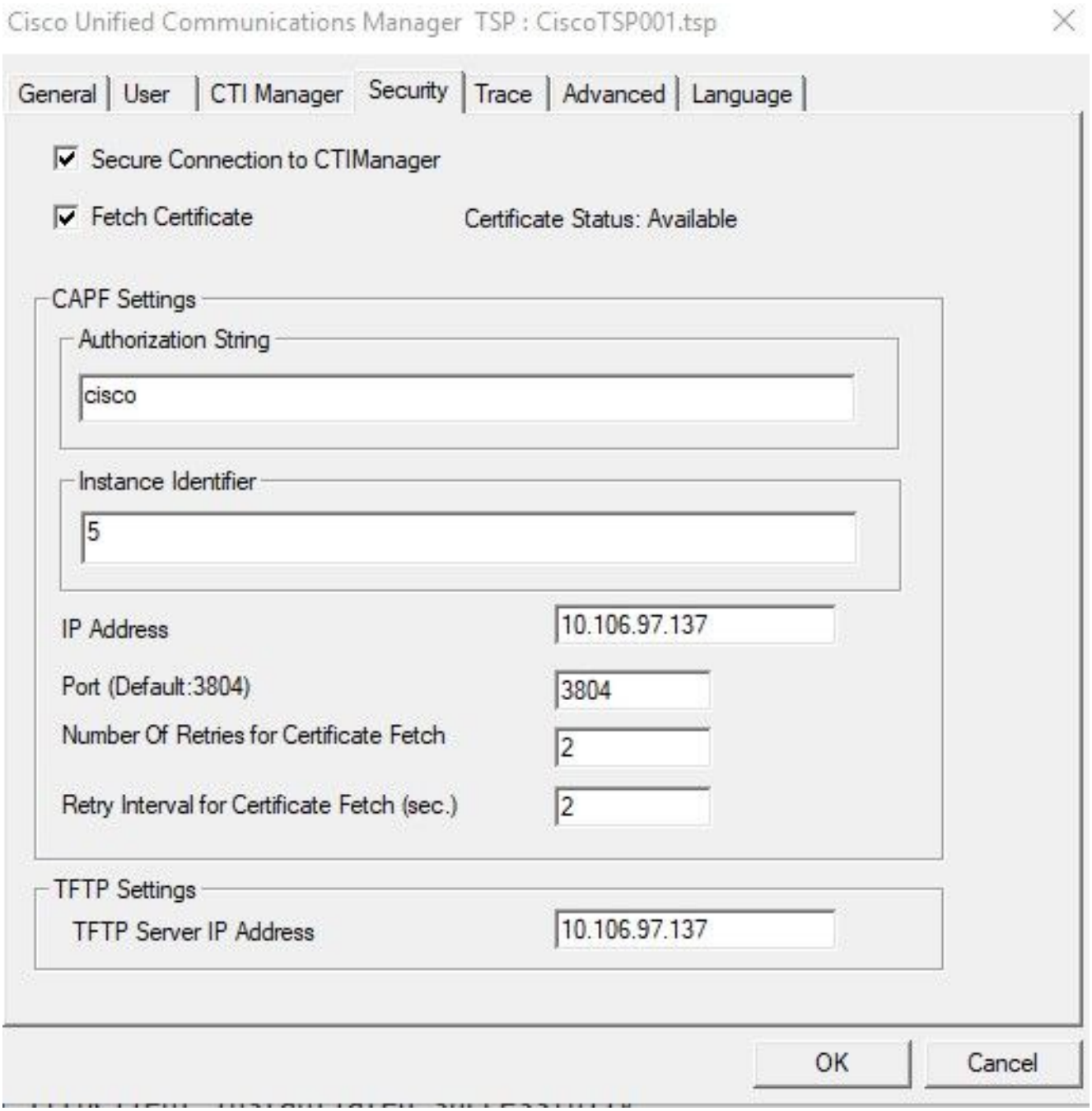
1. 下载并且安装从CUCM的TAPI插件(请导航对**应用程序>插件**)。
2. 添加应用程序用户详细信息如配置在CUCM如镜像所显示。



3. 如镜像所显示，输入CTI Manager详细信息。



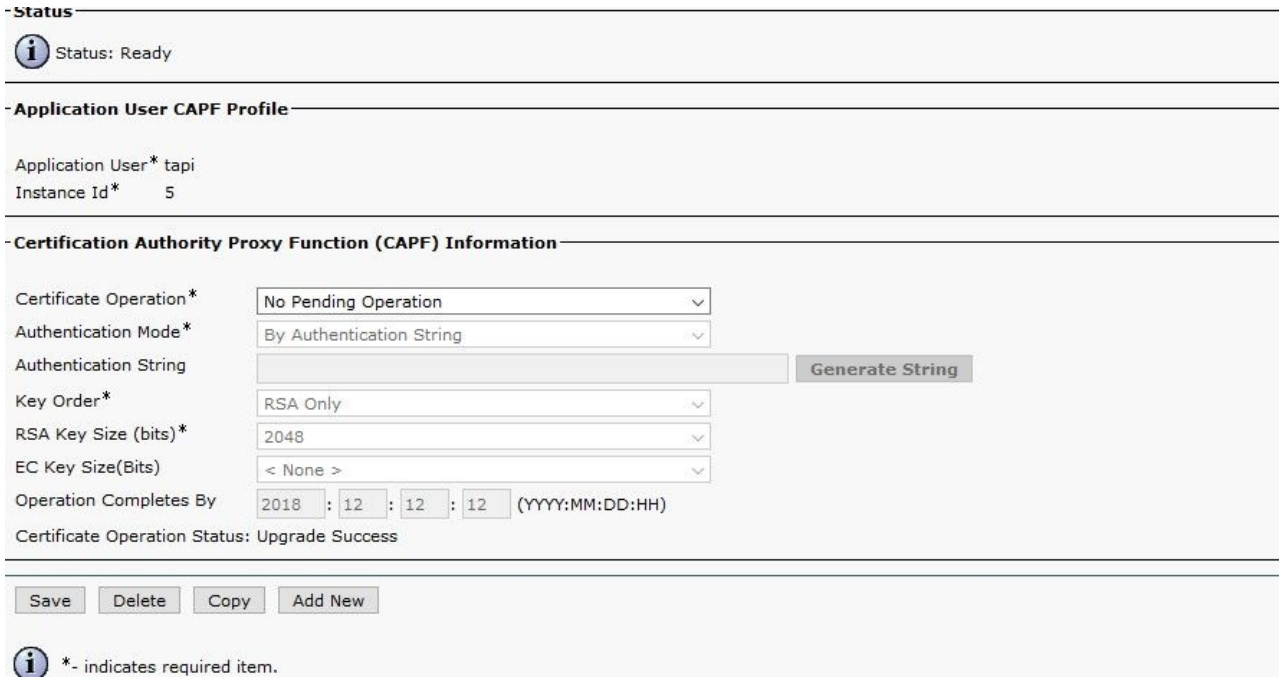
4. 输入授权字符串同CUCM一样并且单击第1次的**取指令证书，**证书必须下载，如镜像所显示。



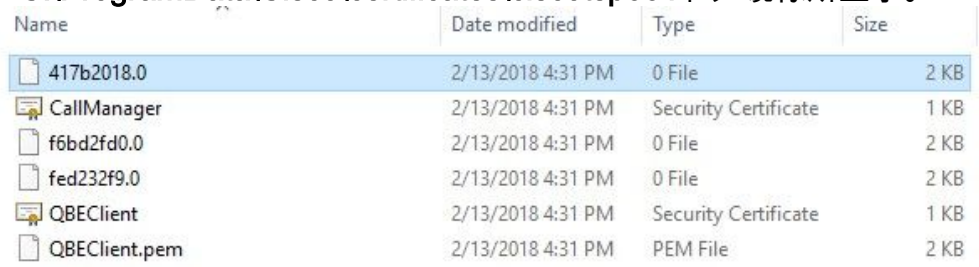
验证

使用本部分可确认配置能否正常运行。

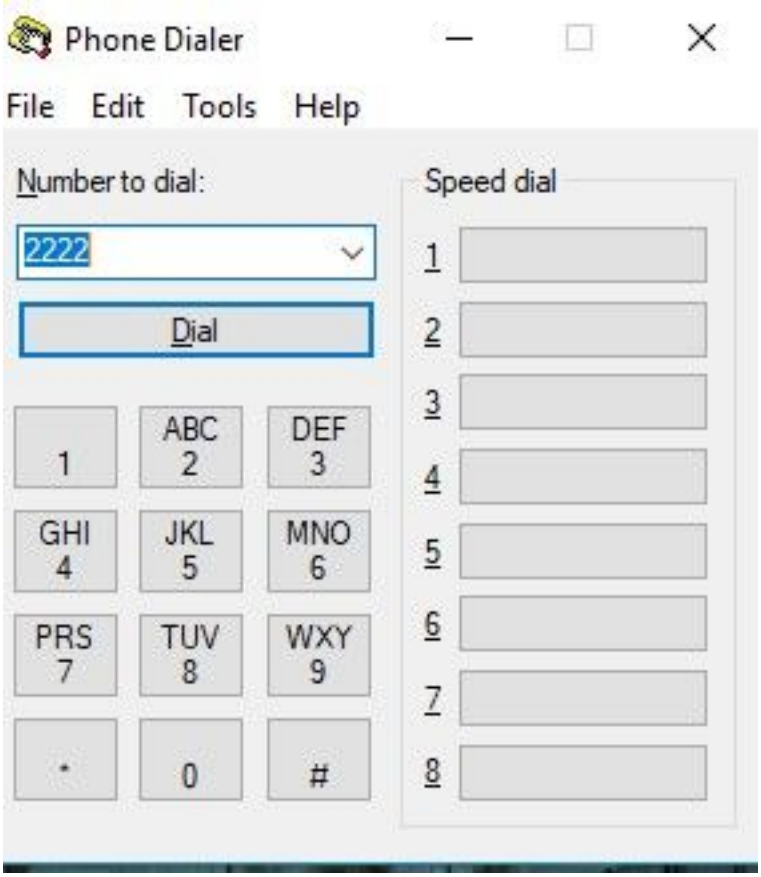
- 在应用程序用户CAPF配置文件，必须顺利地安装局部重要的证书(LSC)。证书操作状态不能是操作待定，如镜像所显示。



- 从CUCM的所有证书在Windows机器下载。路径：C:\ProgramData\Cisco\certificates\ciscotsp001和如镜像所显示。



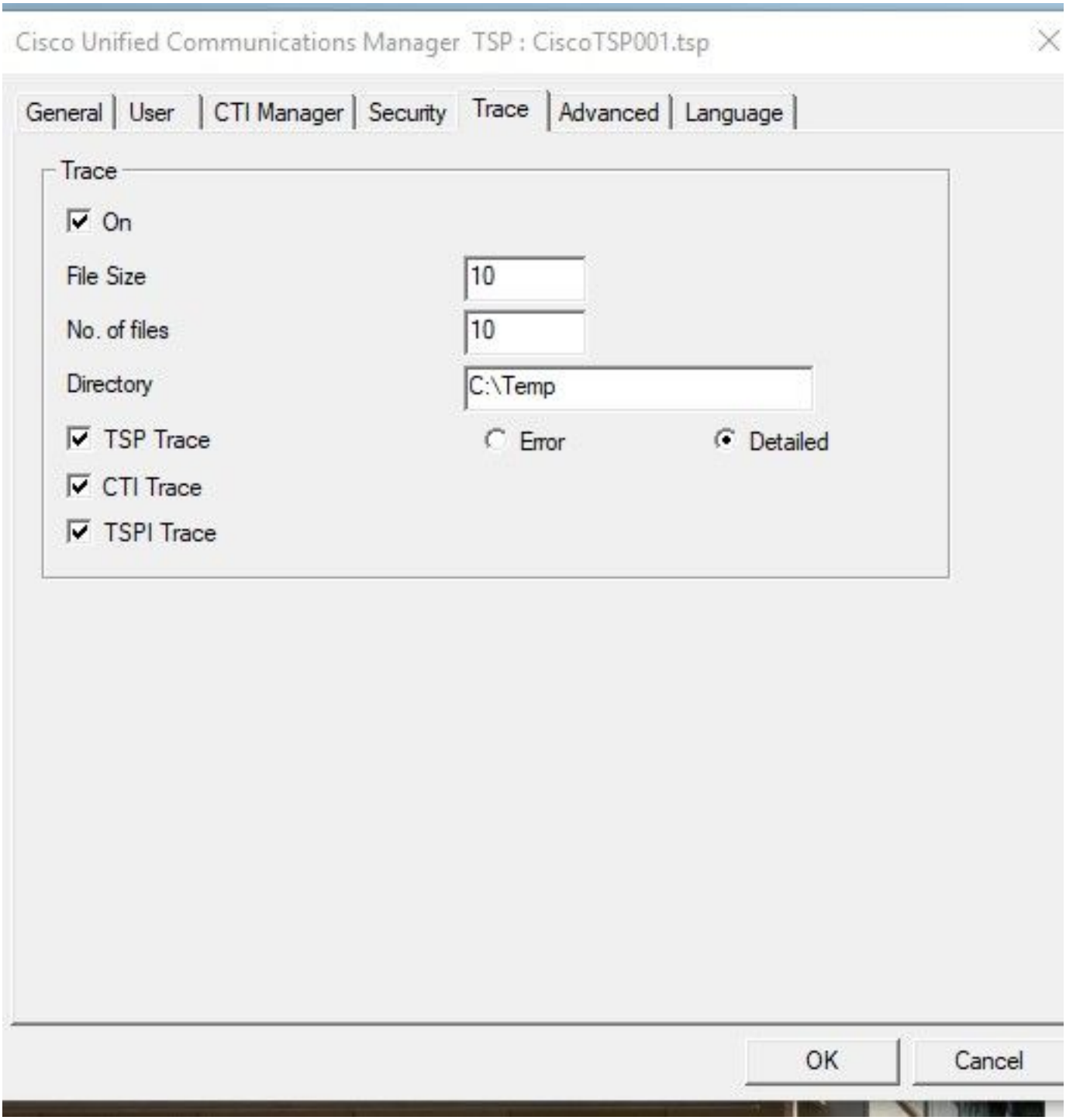
- 如果CTI集成是与使用的工作正常windows内藏的电话拨号程序，您能也验证。如果CTI集成是成功的，您能看到用户控制的电话的分机，如镜像所显示。



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。

- 从应用程序(TSP)侧，您需要设置跟踪到详细如镜像所显示，并且默认trace位置是**C:\Temp**。



- 从CUCM侧，您需要这些跟踪：TV跟踪TFTP跟踪跟踪的CAPF

从TSP的示例Trace

- 首先， TSP联系方式TFTP server为了获得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
```

- 一独立集群的CTL文件包括ITLrecovery， CallManager和CAPF证书。然后CiscoTSP，与提供的实例ID和认证字符串在CiscoTSP配置里，执行CAPF握手。如果握手是成功的，CiscoTSP创建与最终用户的CAPF实例的信息的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
```

- 与成功的CAPF的安全套接字协议层(SSL)握手：

```
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 ...
```

- QBE客户端证书创建与应用程序用户详细信息：

```
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
```