# 认证Cisco Unified通信管理器的(CUCM)重新生成进程

## Contents



## Introduction

本文提供一个推荐的逐步程序关于怎样重新生成在Cisco Unified通信管理器(CUCM)版本8.X的证书和更高。此进程不使用退路对版本在8.0功能前并且由功能更新证书。默认情况下安全以为特色是身份信任列表(ITL)，并且Mixed-Mode功能是证书信任列表(CTL)寻址为了避免注册问题。

贡献用肯赖德， Cisco TAC工程师。

## Prerequisites

### Requirements

Cisco 建议您了解以下主题：

- 实时监视工具(RTMT)
- CUCM证书

### Components Used

- CUCM版本8.X和更高

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.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

## 安装RTMT

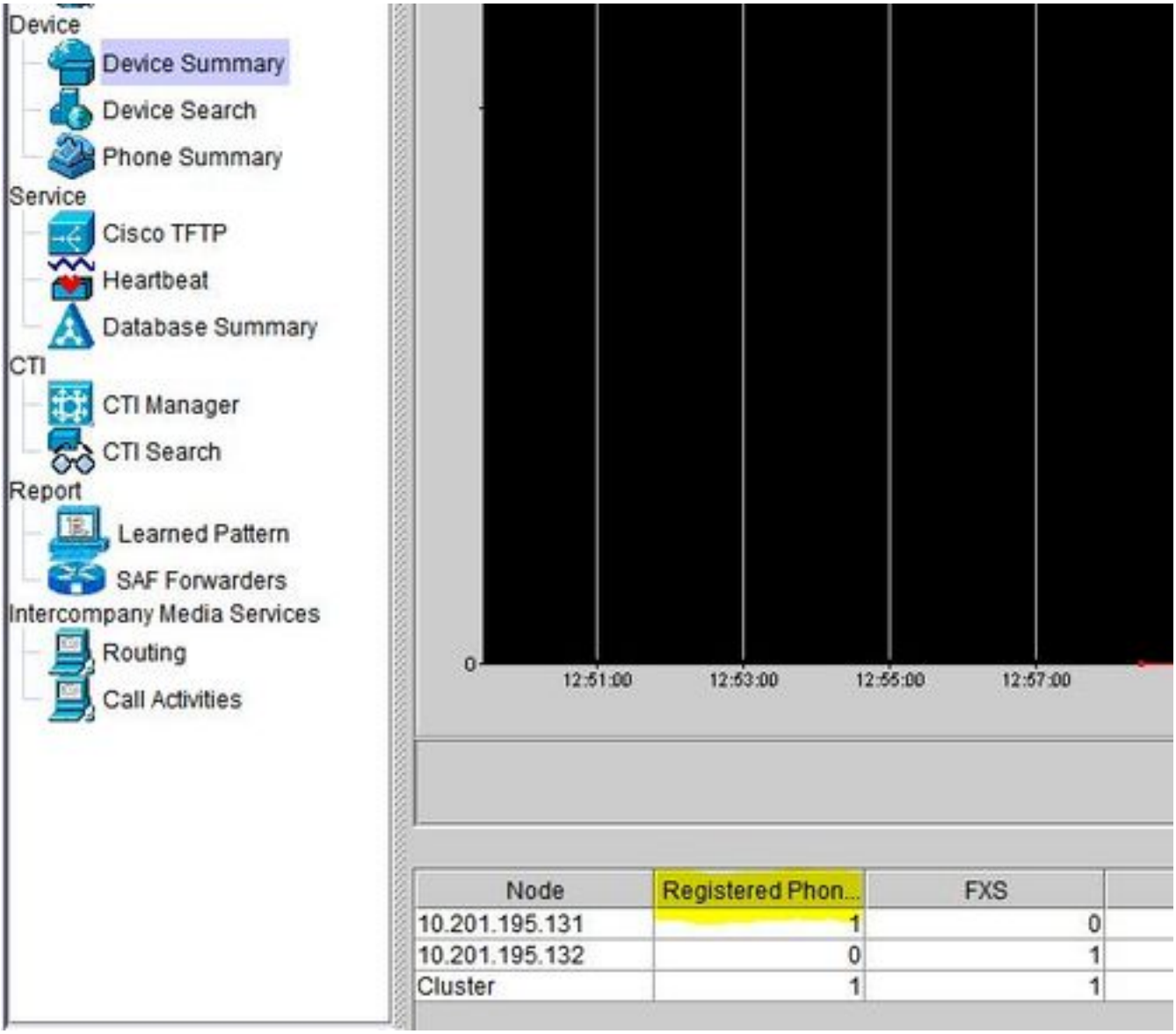
- 从呼叫管理器下载并且安装RTMT工具 连接对呼叫管理器(CM)管理**应用程序>插件>查找 > Cisco Unified实时监视工具- Windows >下载** 安装并且启动

## 监控与RTMT的终端

- 启动RTMT并且输入IP地址或完全合格的域名(FQDN)，用户名和密码然后访问工具 选择**语音/视频选项**选择**设备汇总** 此部分识别注册的终端总数，并且多少对每个节点监控，当终端重置在下个认证的重新生成之前时保证注册

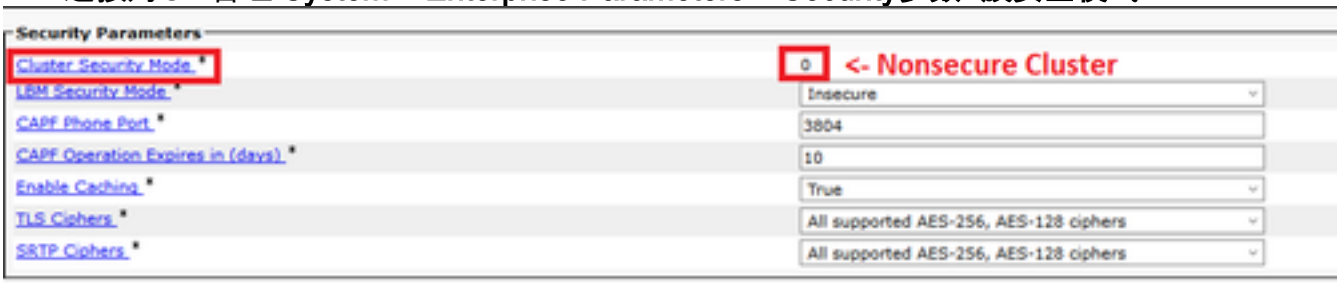
  **提示**：一些证书的重新生成进程能影响终端。在正常工作时间之后考虑一个行动方案由于需求重新启动服务和重新启动电话。监控电话注册通过RTMT是高度推荐的。

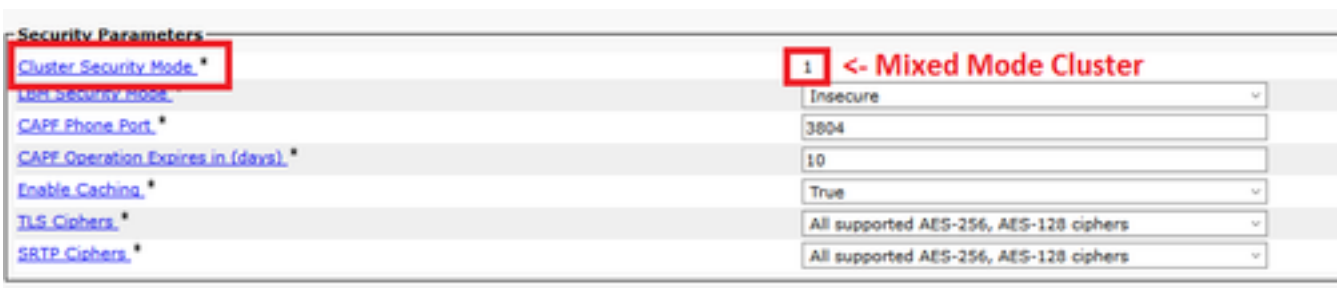
  **警告：**与当前ITL不匹配的终端能在此进程以后有注册问题。 ITL的删除在终端的是一个典型的最佳实践解决方案，在重新生成进程完成后，并且其他电话注册。




## 如果您的簇在Mixed-Mode或不安全的模式，请识别

- 连接对CM管理 System > Enterprise Parameters > Security参数>簇安全模式




## 由证书存储的影响

在整个 CUCM 集群中更新所有证书对于确保系统的出色功能非常重要。如果证书过期或无效他们也许极大影响系统的正常功能。无效或过期的特定证书的服务列表显示得这里。受到的影响可能因系统设置而不同。

### CallManager.pem

- 被加密的/验证的电话不注册
- 简单文件传输协议(TFTP)没有委托(电话不接受签字的配置文件和ITL文件)
- 电话服务也许受影响
- 安全的会话初始化协议(SIP)建立中继或媒体资源(会议网桥，媒介终接点(MTP)， Xcoders，等等)不注册也不工作。
- AXL 请求失败。

### Tomcat.pem

- 电话不能访问在CUCM节点主机的HTTPs服务，例如公共目录
- CUCM能有多种Web问题，例如无法从在簇的其他节点访问服务页
- 扩展移动性(EM)或扩展移动性交叉簇发出
- 单一登录(SSO)

### CAPF.pem

- 电话不为电话VPN， 802.1x或者电话代理验证
- 不能发行电话的局部重要的认证(LSC)证书。
- 被加密的配置文件不工作

### IPSec.pem

- 灾难恢复系统(DR) /Disaster恢复框架(DRF)也许不正常运行
- 对网关(GW)的IPSec隧道对其他CUCM簇不工作

### TVS（信任验证服务）

信任验证服务(TV)默认情况下是安全主要组件。TV enable (event)验证应用服务器的Cisco Unified IP电话，例如EM服务、目录和MIDlet，当HTTPS设立。

TV提供功能如下：

- 可扩展性- Cisco Unified IP电话资源没有由证书的编号影响委托
- 灵活性-信任认证添加或删除在系统自动地被反射
- 安全默认情况下-非媒体和信号安全功能是默认安装的一部分，并且不要求用户干涉

### ITL和CTL

- ITL在簇和认证机关代理功能(CAPF)包含呼叫管理器的TFTP认证角色，所有TV证书，当运行了
- CTL包含系统管理员安全令牌的(SAST)条目， Cisco CallManager，并且是的Cisco Tftp服务在同样服务器、CAPF， TFTP服务器和可适应的安全工具(ASA)防火墙运作了。TV没有被参考

CTL

# 认证重新生成进程

## Tomcat认证

如果第三方证书是在使用中的，请识别。

1. 连接到在您的簇的每个服务器(在您的Web浏览器独立的选项)从发布人开始，跟随由每个订户。 连接对**Cisco Unified OS管理> Security > Certificate Management >查找**
   如果Tomcat陈述系统，生成的自签证书请从说明列观察。如果Tomcat是第三方签字，请跟随提供的链路并且在Tomcat重新生成以后执行那些步骤第三方签名的证书- DOC-6119
2. 选择**查找**为了显示所有证书 选择**Tomcat pem**认证一旦开放请选择**重新生成**并且等待，直到您看到成功上推然后close上推或者返回并且选择**查找/列表**
3. 继续每个随后的订户，遵从在第2步的同一个程序并且完成在您的簇的所有订户
4. 在所有节点重新生成了Tomcat认证后，请重新启动在所有节点的Tomcat服务。开始从发布人然后跟随由订户。 为了重新启动您需要开始每个节点的一次CLI会话和执行命令**utils服务重新启动Cisco Tomcat的**Tomcat

```
admin:
admin:utils service restart Cisco Tomcat
 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

## IPSEC认证

**Note**:CUCM/Instant消息传送和存在(在version10.X前的IM&P)在CUCM发布人和IM&P发布人的DRF主代理运行。 DRF在各自订户的本地服务运行。 版本10.X和以上， DRF在CUCM发布人的主代理运行只有和DRF本地服务在CUCM订户和IM&P发布服务器和用户。

**Note**:灾难恢复系统使用主代理和数据的本地座席认证的和加密的之间安全套接字层SSL基于通信在CUCM簇结之间的。DR利用其公共/Private密钥加密的IPSec证书。注意，如果从证书管理页删除IPSEC truststore (hostname.pem)文件，然后DR不会运转得正如所料。如果手工删除IPSEC信任文件，则您必须保证您加载IPSEC认证到IPSEC truststore。欲了解更详细的信息，请参见证书管理Help页在Cisco Unified通信管理器安全指南。

1. 连接到在您的簇的每个服务器(在您的Web浏览器独立的选项)从发布人开始，跟随由每个订户。 连接对**Cisco Unified OS管理> Security > Certificate Management >查找**
   选择**IPSEC pem**认证。一旦开放请选择**重新生成**并且等待，直到您看到成功上推然后close上推或者返回并且选择**查找/列表**
2. 继续随后的订户;遵从在step1的同一个程序并且完成在您的簇的所有订户
3. 在所有节点重新生成了IPSEC认证然后后重新启动服务。
   连接对发布人的**Cisco Unified维护性 Cisco Unified维护性> Tools > Control Center -网络服务**
   选择在**Cisco DRF主服务的重新启动**一旦服务重新启动完成，请选择在**Cisco DRF本地服务的重新启动**在发布人然后继续订户并且选择在**Cisco DRF本地服务的重新启动**

在发布人的IPSEC.pem认证一定是有效的，并且一定是存在所有订户作为IPSEC truststores。订户

IPSEC.pem认证不会是存在发布人作为在标准的配置的IPSEC truststore。为了验证正确性在IPSEC.pem认证的序列号从PUB与在Sub的IPSEC-信任比较。他们必须配比。

## CAPF认证

**警告：**请保证您识别，如果您的簇在Mixed-Mode，在您进行前。 **如果您的簇在MIX模式或不安全的模式下，请**参考部分**识别。**

1. 连接对**Cisco Unified CM管理>System >企业参数**。
   检查部分安全参数并且验证簇安全模式是否设置到0或1。如果值，如果0然后簇在不安全的模式下。如果它是1然后簇在mixed-mode，并且您将需要在服务之前重新启动更新CTL文件。 请参阅下面令牌和Tokenless链路。
2. 连接到在您的簇的每个服务器(在您的Web浏览器单独的选项)从发布人开始，然后每个订户。
   连接对**Cisco Unified OS管理> Security > Certificate Management >查找**
   选择**CAPF pem**认证。一旦开放请选择**重新生成**并且等待，直到您看到成功上推然后close上推或者返回并且选择**查找/列表**
3. 继续随后的订户;遵从在第2步的同一个程序并且完成在您的簇的所有订户 如果簇在仅Mixed-Mode，并且CAPF是被重新生成的–请更新CTL，在您进行进一步令牌-前Tokenless如果簇在混合模式那么呼叫管理器服务也将需要在其他服务之前重新启动被重新启动
4. 在所有节点重新生成了CAPF认证后，请重新启动服务
   连接对发布人的**Cisco Unified维护性 Cisco Unified维护性> Tools > Control Center -功能服务**
   从发布人开始并且选择在**Cisco认证机关代理功能服务的重新启动只有**其中运行
5. 连接对**Cisco Unified维护性> Tools > Control Center -网络服务** 从发布人开始然后继续订户，选择在**Cisco信任验证服务的重新启动**连接对**Cisco Unified维护性> Tools > Control Center -以服务为特色**从发布人开始然后继续订户，重新启动**Cisco Tftp服务只有**其中运行。
6. 重新启动所有电话 **Cisco Unified CM管理>System >企业参数**选择**重置**您然后将看到与语句的上推**您将重置在系统的所有设备。此动作不可能被取消。Continue?请**选择得**好**然后选择**重置**

电话当前将重置。通过RTMT工具监控他们的动作保证重置是成功的，并且设备注册回到CUCM。 在您进行对下个认证前，请等待电话注册完成。电话注册的此进程能用一些时间。请建议，有坏ITLs在重新生成进程之前也许不注册回到簇的设备。

## 呼叫管理器认证

**警告：**请保证您识别，如果您的簇在Mixed-Mode，在您进行前。**如果您的簇在MIX模式或不安全的模式下，请**参考部分**识别。**

**警告：**同时请勿重新生成CallManager.PEM和TVS.PEM证书。 这将导致不可恢复的不匹配在将要求删除ITL从在簇的所有终端的终端的安装的ITL。

1. 连接对**Cisco Unified CM管理>System >企业参数**。 检查部分安全参数并且验证簇安全模式是否设置到0或1。如果值，如果0然后簇在不安全的模式下。如果它是1然后簇在mixed-mode，并且您将需要在服务之前重新启动更新CTL文件。 请参阅下面令牌和Tokenless链路。
2. 连接到在您的簇的每个服务器(在您的Web浏览器单独的选项)从发布人开始，然后每个订户。
   连接对**Cisco Unified OS管理> Security > Certificate Management >查找**
   选择**呼叫管理器pem**认证。一旦开放请选择**重新生成**并且等待，直到您看到成功上推然后close上推或者返回并且选择**查找/列表**
3. 继续随后的订户;遵从在第2步的同一个程序并且完成在您的簇的所有订户。 如果簇在仅Mixed-

Mode，并且CAPF是被重新生成的–请更新CTL，在您进行进一步令牌-前Tokenless

4. 日志到发布人的Cisco Unified维护性里 连接对**Cisco Unified维护性> Tools > Control Center -以服务为特色**从发布人开始然后继续订户，重新启动**Cisco CallManager服务**其中运行。
5. 连接对**Cisco Unified维护性> Tools > Control Center -以服务为特色**
   从发布人开始然后继续订户，重新启动**Cisco CtiManager服务只有**其中运行
6. 连接对**Cisco Unified维护性> Tools > Control Center -网络服务**
   从发布人开始然后继续订户，重新启动**Cisco信任验证服务**
7. 连接对**Cisco Unified维护性> Tools > Control Center -以服务为特色**
   从发布人开始然后继续订户，重新启动**Cisco Tftp服务只有**其中运行
8. 重新启动所有电话 **Cisco Unified CM管理>System >企业参数**选择**重置**您然后将看到与语句的上推**您将重置在系统的所有设备。此动作不可能被取消。Continue?请**选择得**好**然后选择**重置**

电话当前将重置。通过RTMT工具监控他们的动作保证重置是成功的，并且设备注册回到CUCM。 在您进行对下个认证前，请等待电话注册完成。电话注册的此进程能用一些时间。请建议，有坏ITLs在重新生成进程之前也许不注册回到簇的设备。

## TV认证

**警告：** 同时请勿重新生成CallManager.PEM和TVS.PEM证书。 这将导致不可恢复的不匹配在将要求删除ITL从在簇的所有终端的终端的安装的ITL。

**Note**:TV代表呼叫管理器验证证书。重新生成此认证为时。

1. 连接到在您的簇的每个服务器(在您的Web浏览器独立的选项)从发布人开始，然后每个订户。 连接对**Cisco Unified OS管理> Security > Certificate Management >查找**
   选择**TV pem**认证。一旦开放请选择**重新生成**并且等待，直到您看到成功上推然后close上推或者返回并且选择**查找/列表**
2. 继续随后的订户;遵从在step1的同一个程序并且完成在您的簇的所有订户 在所有节点重新生成了TV认证后，请重新启动服务： 日志到发布人的**Cisco Unified维护性里** 连接对**Cisco Unified维护性> Tools > Control Center -网络服务**在发布人请选择在**Cisco信任验证服务的重新启动**。一旦服务重新启动完成，请继续订户并且重新启动**Cisco信任验证服务**
3. 从发布人开始然后继续订户，重新启动**Cisco Tftp服务只有**其中运行。
4. 重新启动所有电话 **Cisco Unified CM管理>System >企业参数**选择**重置**您然后将看到与语句的上推**您将重置在系统的所有设备。此动作不可能被取消。Continue?请**选择得**好**然后选择**重置**

电话当前将重置。通过RTMT工具监控他们的动作保证重置是成功的，并且设备注册回到CUCM。 在您进行对下个认证前，请等待电话注册完成。电话注册的此进程能用一些时间。请建议，有坏ITLs在重新生成进程之前也许不注册回到簇的设备。

## ITLRecovery认证

**Note**:ITLRecovery认证，当设备丢失他们的委托的状态时，使用。(当CTL供应商是活跃的)时，认证出现于ITL和CTL。
如果设备丢失他们的信任状态，您能使用命令**utils itl重置localkey**不安全的簇和命令**utils ctl重置localkey** MIX模式簇。读您的CallManager版本熟悉如何使用ITLRecovery认证和要求的进程安全指南恢复委托的状态。
如果簇被升级了到支持一个密钥长度的2048和簇服务器证明的版本被重新生成了到2048，并且ITLRecovery当前未被重新生成并且是1024个密钥长度， ITL恢复命令将发生故障，并且ITLRecovery方法不能使用。

1. 连接到在您的簇的每个服务器(在您的Web浏览器单独的选项)从发布人开始，然后每个订户。 连接对**Cisco Unified OS管理> Security > Certificate Management >查找** 选择**ITLRecovery pem**认证。一旦开放请选择**重新生成**并且等待，直到您看到成功上推然后close上推或者返回并且选择**查找/列表**
2. 继续随后的订户;遵从在第2步的同一个程序并且完成在您的簇的所有订户
3. 在所有节点重新生成了ITLRecovery认证后，服务将需要按顺序被重新启动如下： 如果是在混合模式–，在您进行令牌- Tokenless前，请更新CTL日志到发布人的**Cisco Unified维护性里** 连接对**Cisco Unified维护性> Tools > Control Center -网络服务**在发布人请选择在**Cisco信任验证服务的重新启动**。 一旦服务重新启动完成，请继续订户并且重新启动**Cisco信任验证服务**
4. 重新启动所有电话 **Cisco Unified CM管理>System >企业参数**选择**重置**您然后将看到与语句的上推**您将重置在系统的所有设备。此动作不可能被取消。Continue?请**选择得**好**然后选择**重置**
5. 当他们重置时，电话当前将加载新的ITL/CTL。

# 删除过期的信任认证

**Note**:识别需要被删除，不再要求的信任认证，或者到期了。 请勿删除包括CallManager.pem、tomcat.pem、ipsec.pem、CAPF.pem和TVS.pem的五基本证书。信任认证可以被删除，若适合。 下面服务的重新启动在传统证书的内存信息在那些服务内设计清除其中任一。

1. 连接对**Cisco Unified维护性> Tools > Control Center -网络服务** 从丢弃下来请选择CUCM发布人选择**终止认证修改提示**为在您的簇的每个呼叫管理器节点重复如果有一个IMP服务器 从下拉菜单请选择您的IMP服务器一次一个并且选择**终止平台管理网站服务和Cisco簇之间同步代理程序**
2. 连接对**Cisco Unified OS管理> Security > Certificate Management >查找** 查找过期的信任认证。(您能由到期过滤的版本10.X和以上。Fr版本在您将需要识别特定证书手工或通过RTMT戒备的10.0以下，如果接受)同一个信任认证能出现于多个节点。必须从每个节点单个删除它。选择信任认证被删除(从属于您的版本您或者将获得上推或您将连接对在同样页的认证) 选择**删除**(您将获得从您开始将永久删除此认证…*)的*上推选择得**好**
3. 重复能将被删除的每个信任认证的进程
4. 在完成，直接地与被删除的证书有关的服务将需要被重新启动。您不需要重新启动在此部分的电话。 呼叫管理器和CAPF将是终端影响。 Tomcat信任：重新启动Tomcat服务通过line命令(请参阅Tomcat部分)CAPF信任：重新启动Cisco认证机关代理功能(请参阅CAPF部分)不重新启动终端呼叫管理器信任：呼叫管理服器务/CtiManager (请参阅呼叫管理器部分)不重新启动终端 影响终端和原因重新启动IPSEC信任：DRF Master/DRF本地(请参阅IPSEC部分)TV (自己签署的)没有信任认证
5. 在step1以前终止的重新启动服务

# Verify

当前没有可用于此配置的验证过程。

# Troubleshoot

目前没有针对此配置的故障排除信息。