CUCM 证书重新生成/续约流程

Contents

Introduction

本文档就重新生成在思科统一通信管理器 (CUCM) 版本 8.x 及更高版本中使用的证书提供了建议的分步程序。为避免发生任何意外中断，本文档还介绍了默认安全功能 (ITL) 和混合模式 (CTL)。例如，如何避免电话注册问题或者不接受配置更改或固件的电话。

> **警告**：始终建议在维护时段完成证书重新生成。

概述

本文档介绍的证书重新生成过程适用于以下服务：

- CallManager
- CAPF（思科证书颁发机构代理功能)
- IPsec
- Tomcat
- TVS（信任验证服务）
- ITLRecovery（仅适用于 CUCM 10.X 及更高版本）
- phone-vpn-trust
- phone-sast-trust

- phone-trust
- phone-ctl-trust

以及以下电话证书：

- LSC（本地重要证书）
- MIC（制造商安装的证书）

Components Used

本文档中显示的所有输出和屏幕截图均基于 CUCM 版本 9.1(2)SU2a，但介绍的程序可用于 CUCM 版本 8.x 及更高版本。如有与版本相关的特定区别，将在相应部分提及。

本文档中的信息基于实验室环境中的设备，启动时均为出厂（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或采取的操作可能造成的影响。

何时重新生成证书

在 CUCM 中，全新安装后使用的大多数证书都是自签名证书，默认情况下颁发期限为五年。请注意，目前无法在 CUCM 上将五年的时间范围修改为更短的时间范围。但是，证书颁发机构 (CA) 几乎可以颁发任何时间范围的证书。

还有一些预先加载并且有效期更长的可信证书（例如 CAPF-trust 和 CallManager-trust）。例如，CUCM 信任库中为特定功能提供“思科制造 CA”证书且有效期直到 2029 年。

应在证书到期前重新生成证书。当证书即将到期时，您会在 RTMT（系统日志查看器）中收到警告，如果进行了相应配置，还会收到一封通知邮件。

下面显示的证书到期通知示例详细说明服务器 CUCM02 上的信任库“tomcat-trust”中的“CUCM01.der”证书将于“5 月 19 日星期一 14:46”到期：

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
SyslogSeverityMatchFound events generated:

SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent

ClusterID :

NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

如果服务证书（未标有“-trust”的证书库）已经过期，仍有可能重新生成这些证书。请注意，过期证书可能会影响 CUCM 功能，具体取决于集群的配置。下一部分将介绍相关注意事项。

证书库对服务的影响

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，可能会严重影响系统的正常功能。下面列出了当任何特定证书无效或过期时，您可能遇到的潜在问题。受到的影响可能因系统设置而不同。

CallManager.pem

- 经过加密/身份验证的电话无法注册。
- TFTP 不受信任（电话不接受签名的配置文件和/或 ITL 文件）。
- 电话服务可能会受到影响。
- 安全会话发起协议 (SIP) 中继或媒体资源（会议网桥、媒体终止点 (MTP)、Xcoder 等）无法注册或工作。
- AXL 请求失败。

Tomcat.pem

- 电话不能访问 CUCM 节点上托管的 HTTP 服务，例如企业目录。
- CUCM 的 Web GUI 问题，例如无法从集群中的其他节点访问服务页面。
- 分机移动性或跨集群分机移动问题。

CAPF.pem

- 电话无法向电话 VPN、802.1x 或电话代理进行身份验证。
- 无法为电话颁发 LSC 证书。
- 加密的配置文件无法工作。

IPSec.pem

- 灾难恢复系统 (DRS)/灾难恢复框架 (DRF) 可能无法正常工作。
- 与通往其他 CUCM 集群的网关 (GW) 之间的 IPsec 隧道无法工作。

TVS（信任验证服务）

- 电话无法对 HTTPS 服务进行身份验证。电话无法对配置文件进行身份验证（这几乎会对 CUCM 上的一切造成影响）。

phone-vpn-trust

- 电话 VPN 无法工作，因为无法对 VPN 的 HTTPS URL 进行身份验证。

  Note:如果不存在这种情况也无需担心。这种情况仅适用于特定配置。

phone-sast-trust

- 以前的 CTL/电子令牌将无法更新或修改 CTL。

  Note:如果不存在这种情况也无需担心。这种情况仅适用于特定配置。

Phone-trust 和 phone-ctl-trust

- 配备 Unity 或 Unity Connection 的可视语音邮件将无法工作。

  Note:如果不存在这种情况也无需担心。这种情况仅适用于特定配置。

LSC 和 MIC

- 电话无法注册，电话无法向电话 VPN、电话代理或 802.1x 进行身份验证。

  Note:在默认情况下，大多数电话型号上都有 MIC。LSC 则默认由 CAPF 签名，有效期为五年。CIPC（思科 IP Communicator）和 Jabber 等软件客户端未安装 MIC。

创建 DRS 备份

建议您在执行任何此类重大更改之前先创建一份 DRS 备份。CUCM DRF 备份将备份集群中的所有证书。所有 DRS 备份/恢复程序都可以在思科的思科统一通信管理器灾难恢复系统管理指南中找到。

> **警告：** 请注意思科漏洞 ID CSCtn50405 - CUCM DRF 备份不备份证书。

确定集群是否处于混合模式

要确定您运行的是不是 CTL/安全/混合模式集群，请依次选择**思科 Unified CM 管理 > 系统 > 企业参数 > 集群安全模式（0 == 非安全；1 == 混合模式）**。

如果集群处于混合模式

如果您运行的 CUCM 集群处于混合模式，这意味着需要在所有证书更改后再更新 CTL 文件。思科的安全指南文档中介绍了有关如何执行此操作的程序。不过，请确保您至少有一个混合模式功能的原始初始化 eToken，并且知道 eToken 密码。

> **Note**:CTL 更新不会像 ITL 文件的更新那样自动完成，而是需要由管理员使用 CTL 客户端或 CLI 命令手动完成。

在 CUCM 10.X 及更高版本中，您可以通过两种方式将集群设置为混合模式：

- CLI 命令 - 如果使用此方法，则会使用发布方服务器的 CallManager.pem 证书签署 CTL 文件。

```
admin:show ctl
The checksum value of the CTL file:
0c05655de63fe2a042cf252d96c6d609(MD5)
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1156
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
```

```
ST=Malopolska;C=PL
6 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 694 E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
A5 A3 8C 9C (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

- CLI 客户端 - 如果使用此方法，则会使用其中一个硬件 eToken 签署 CTL 文件。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Note: 您可以通过采用无令牌 CTL 的 CUCM 混合模式变换使用的方法。

根据您用于保护集群安全的方法，需要使用相应的 CTL 更新程序。重新运行 CTL 客户端，或从 CLI 输入 **utils ctl update CTLfile** 命令。

验证集群的默认安全设置

避免 ITL 问题很重要，因为 ITL 问题可能导致许多功能发生故障，或者导致电话拒绝遵守任何配置更改。 可以通过以下两种方法避免 ITL 问题。

使用“准备集群以便回滚到 8.0 前的版本”功能

此功能会在所有服务器上“清空”ITL，因此电话会信任所有 TFTP 服务器。当此参数设置为 True 时，电话服务（例如分机移动性）将无法工作。但是，用户仍能继续拨打和接听基本的电话呼叫。

Note: 更改此参数会导致所有电话重置。

设置此功能后，需要重新启动所有 TFTP 服务器（以便提供新的 ITL），还需要重置所有电话以强制其请求新的“空”ITL。一旦完成证书更改并重新启动所有必要的服务，即可将此功能重新设置为“False”，重新启动 TFTP 服务，并重置电话（以便电话可以获取有效的 ITL 文件）。然后，所有功能将继续如以前一样正常工作。

按特定顺序重新生成证书

以下程序可以从受信任的可用 TFTP 服务器为另一台 TFTP 服务器提供有效的/更新后的 ITL 文件。

1. 在主 TFTP 服务器上停止 TFTP 服务。
2. （根据需要）对主 TFTP 服务器上的证书做出更改。
3. 重置电话（以便从辅助 TFTP 服务器获取新的 ITL 文件）- 根据要重新生成的具体证书，此操作可能会自动完成。
4. 电话返回后，启动主 TFTP 服务器的 TFTP 服务。
5. 在辅助 TFTP 服务器上进行证书更改。
6. 重置电话（以便从主 TFTP 服务器获取新的 ITL 文件）。

> **警告**：请勿同时在两台 TFTP 服务器上编辑证书。这会让电话没有可信任的 TFTP 服务器，而需要本地管理员从所有电话上手动删除 ITL。

在 CUCM 中删除并重新生成证书

只能重新生成服务证书（未标有“-trust”的证书库）。信任库（标有“-trust”的证书库）中的证书无法重新生成，因此需要将其删除。

> **警告**：请注意思科漏洞 ID 的 CSCut58407 - 删除 CAPF/CallManager/TVS-trust 时，不应重新启动设备。

完成所有证书修改后，需要重新启动各自的服务以接受更改。重新生成/删除证书后部分将对此进行介绍。

> **警告**： 请注意思科漏洞 ID CSCto86463 - 删除的证书重新出现，无法从 CUCM 删除证书。在此问题中，已删除的证书不断在删除后重新出现。请按照缺陷解决方法操作。

通过 CLI 重新生成证书

> **警告**：重新生成证书会触发集群中的 ITL 文件自动更新，进而触发集群范围的电话软重置，以便让电话触发其本地 ITL 的更新。这种情况主要见于 CAPF 和 CallManager 证书重新生成时，但是在 CUCM 中的其他证书库（例如 Tomcat）重新生成时也有可能发生。

重新生成 CAPF

CAPF 证书在重新生成后会自动将自身上传到 CAPF-trust 和 CallManager-trust。此外，CAPF 始终有一个唯一的“使用者名称”标题，因此以前使用的 CAPF 证书将保留并用于身份验证。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)
```

```
Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

> **Note**: 如果 CAPF 证书过期，使用 LSC 的电话将无法注册到 CUCM，因为 CUCM 会拒绝其证书。不过，您仍然可以使用新的 CAPF 证书为电话生成新的 LSC。当您重新启动电话时，它会下载配置，然后联系 CAPF 以更新 LSC。更新 LSC 后，电话即可正常注册。只要新的 CAPF 证书在 ITL 文件中并且电话已下载和信任签署它的证书 (callmanager.pem)，此方法就可以奏效。

重新生成 CallManager

CallManager 在重新生成后会自动将自身上传到 CallManager-trust。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

重新生成 IPsec

Ipsec 证书在重新生成后会自动将自身上传到 ipsec-trust。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

重新生成 Tomcat

Tomcat 证书在重新生成后会自动将自身上传到 tomcat-trust。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

重新生成 TVS

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)
```

```
Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

预计发生的情况

通过 CLI 重新生成证书时，系统会要求您验证此更改。键入 yes，然后按 Enter。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

通过 CLI 删除证书

删除 CAPF-trust 证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015
```

```
[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

删除 CallManager-trust 证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

删除 ipsec-trust 证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
```

```
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

删除 Tomcat-trust 证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

删除 TVS-trust 证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
```

```
This etoken was used to sign the CTL file.
```

通过 Web GUI 重新生成证书

重新生成 CAPF

CAPF 证书在重新生成后会自动将自身上传到 CAPF-trust 和 CallManager-trust。此外，CAPF 证书始终有一个唯一的“使用者名称”标题，因此以前使用的 CAPF 证书将保留并用于身份验证。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

重新生成 CallManager

CAPF 证书在重新生成后会自动将自身上传到 CallManager-trust。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
```

```
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

重新生成 IPsec

Ipsec 证书在重新生成后会自动将自身上传到 ipsec-trust。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

重新生成 Tomcat

Tomcat 证书在重新生成后会自动将自身上传到 tomcat-trust。

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

重新生成 TVS

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

通过 Web GUI 删除证书

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

重新生成/删除证书后

在证书库中删除或重新生成证书后，需要重新启动各自的服务以接受更改。

证书库	要重新启动的服务	如何
Tomcat	Tomcat	CLI ：实用服务重新启动思科 Tomcat Web Gui ： 思科统一功能配置 > 工具 > 控制中心 - 功能
CallManager	CallManager；TFTP;CtiManager	

		> (选择服务器) > 选择“思科 CallManager”> 重新启动 Web Gui ： 思科统一功能配置 > 工具 > 控制中心 - 功能 务 > (选择服务器) > 选择“思科 Tftp”> 重新启动 Web Gui ： Cisco Unified维护性> Tools > Control Cen 功能Services> (请选择服务器) >选择"Cisco CTIManage >重新启动
CAPF	CAPF (仅在发布方服务器上)	Web Gui ： 思科统一功能配置 > 工具 > 控制中心 - 功能 务 > (选择服务器) > 选择“思科证书颁发机构代理功能” 新启动
TVS	信任验证服务 (在各自的服务器上)	Web Gui ：思科统一功能配置 > 工具 > 控制中心 - 网络 > (选择服务器) > 选择“思科信任验证服务”> 重新启动
ipsec	本地思科 DRF (在所有节点上) ；主思科 DRF (在发布方服务器上)	CLI ：实用服务重新启动本地思科 DRF CLI ：实用服务重新启动主思科 DRF

通过电话安装/更新 LSC

如果已重新生成 CAPF 证书，则需要以新 CAPF 证书签名的 LSC 来更新集群中所有电话的 LSC 证书。

1. 依次选择 **CUCM 功能配置 > 服务激活**。在发布方服务器上，激活思科 CTL 提供程序和思科证书颁发机构代理功能。
2. 从 CUCM CCMAdmin，依次选择**设备 > 电话**。选择要在其中调配 LSC 的 IP 电话。
3. 在“证书操作”下的设备配置页面中，依次选择**安装/升级 > 通过 Null 字符串**。
4. 在 CCMAdmin 中保存电话配置，然后选择**应用配置**。

如果电话安装 LSC 时遇到问题，请在电话上完成以下操作：

当电话重置时，转到物理电话，然后依次选择**设置 > (6) 安全配置 > (4) LSC > **#** (此操作可解锁 GUI，让我们得以继续下一步操作) > **更新** (在您执行上一步操作前，不会显示更新) > **提交**。

请勿将任何证书分配给电话，除非它是无线电话 (7921/25)。为了对自身进行身份验证，无线电话使用第三方证书颁发机构 (CA)。

结论

倘若您遇到问题或需要有关此程序的帮助，请联系思科技术支持中心 (TAC) 寻求帮助。在此情况下，请确保 DRF 备份可用，因为如果 TAC 无法通过其他方法恢复服务，它将用作恢复服务的最后手段。