

从签名CA证书创建新证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[预检信息](#)

[配置并重新生成证书](#)

[Tomcat证书](#)

[CallManager证书](#)

[IPSec证书](#)

[CAPF证书](#)

[TVS证书](#)

[常见上传的证书错误消息疑难解答](#)

[CA证书在信任库不可用](#)

[文件/usr/local/platform/.security/tomcat/keys/tomcat.csr不存在](#)

[CSR公钥和证书公钥不匹配](#)

[CSR使用者备用名称\(SAN\)和证书SAN不匹配](#)

[不替换具有相同CN的信任证书](#)

简介

本文档介绍如何在Cisco Unified Communications Manager (CUCM)中重新生成证书颁发机构 (CA)签名的证书。

先决条件

要求

Cisco 建议您了解以下主题：


- 实时监控工具(RTMT)
- CUCM证书

使用的组件

- CUCM版本10.x、11.x和12.x。

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。

预检信息

 注意：有关重新生成自签名证书的信息，请参阅[证书重新生成指南](#)。有关CA签名的多SAN证书重新生成的信息，请参阅[多SAN证书重新生成指南](#)

要了解每个证书及其重新生成的影响，请参阅[自签名重新生成指南](#)。

每种证书签名请求(CSR)类型具有不同的密钥用途，签名证书中需要使用这些密钥。[安全指南](#)包括一个表，其中提供了每种证书类型所需的密钥用法。

要更改主题设置（位置、状态、组织单位等），请运行此命令：

- `set web-security orgunit orgname locality state [country] [alternatehostname]`

在您运行`set web-security`命令之后，Tomcat证书将自动重新生成。除非重新启动Tomcat服务，否则不会应用新的自签名证书。有关此命令的详细信息，请参阅以下指南：

- [命令行参考指南](#)
- [链接到思科社区步骤](#)
- [视频](#)

配置并重新生成证书

针对每种类型的证书，列出了在由CA签名的CUCM集群中重新生成单节点证书的步骤。如果集群中的所有证书尚未过期，则无需重新生成这些证书。

Tomcat证书

 注意：验证是否在集群中禁用SSO (CM Administration > System > SAML Single Sign-On)。如果已启用SSO，则必须先将其禁用，然后在完成Tomcat证书重新生成过程后将其启用。

在群集的所有节点（CallManager和IM&P）上：


步骤1: 导航到Cisco Unified OS Administration > Security > Certificate Management > Find并验证Tomcat证书的到期日期。

第二步：单击。Generate CSR > Certificate Purpose: tomcat选择所需的证书设置，然后单击Generate。等待系统显示成功消息，然后单击Close。

Generate Certificate Signing Request

Generate Close


Status


 Success: Certificate Signing Request Generated

Generate Certificate Signing Request

Certificate Purpose**	tomcat
Distribution*	115pub [REDACTED]
Common Name*	115pub [REDACTED]
Subject Alternate Names (SANs)	
Parent Domain	[REDACTED]
<hr/>	
Key Type**	RSA
Key Length*	2048
Hash Algorithm*	SHA256

Generate Close

 *- indicates required item.


 **When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

第三步：下载CSR。点击Download CSR，选择Certificate Purpose: tomcat，然后点击Download。

Download Certificate Signing Request

Download CSR Close


Status

 Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Purpose*	tomcat
----------------------	--------


Download CSR Close

 *- indicates required item.


第四步：将CSR发送到证书颁发机构。

第五步：证书颁发机构为签名证书链返回两个或多个文件。按以下顺序上传证书：

- 根CA证书作为tomcat-trust。导航至Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust。设置证书描述并浏览根证书文件。
- 中间证书作为tomcat-trust（可选）。导航到Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust。设置证书描述并浏览中间证书文件。

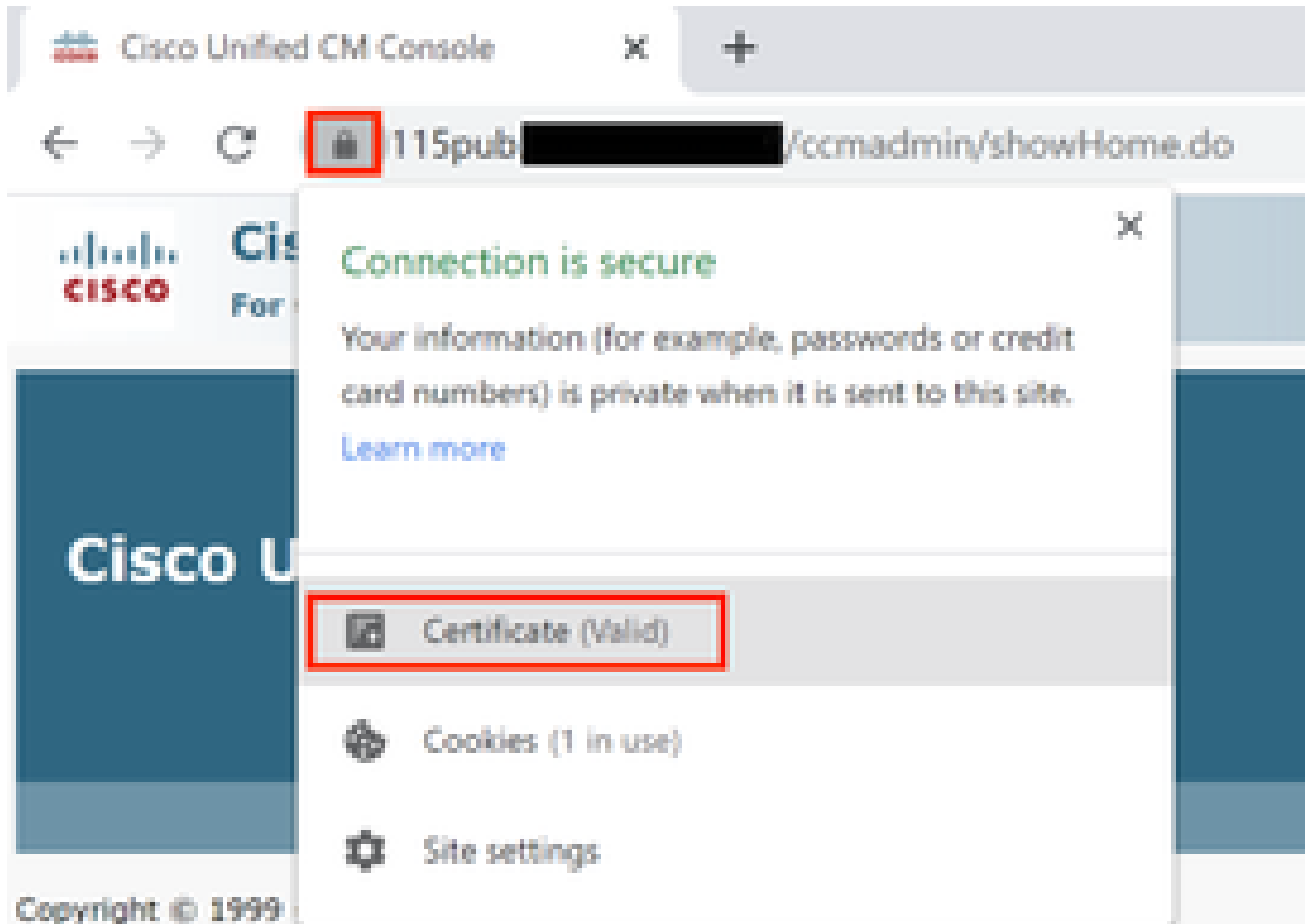
 注意：某些CA不提供中间证书。如果仅提供根证书，则可省略此步骤。

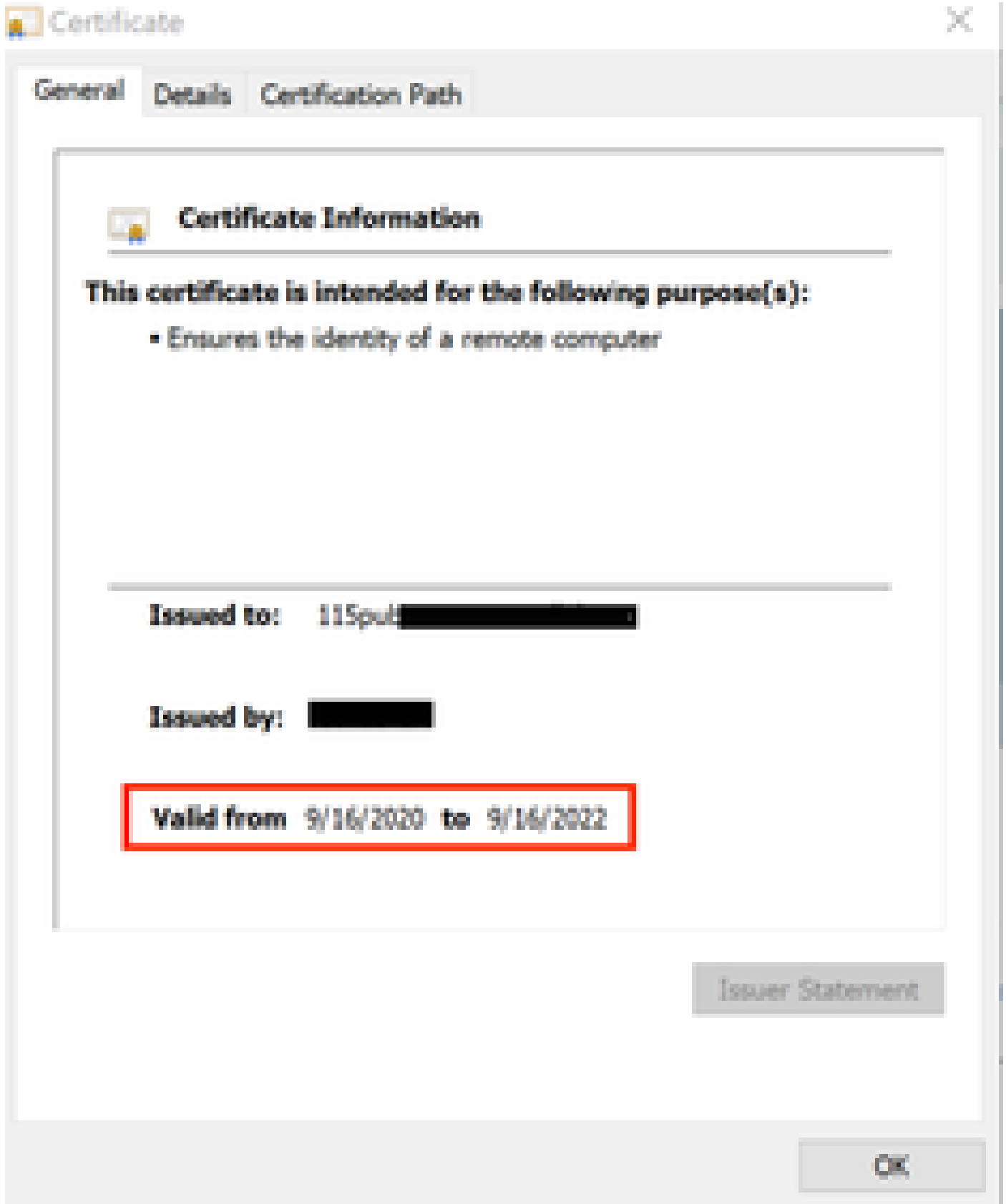
- CA签名的证书作为tomcat。导航到Certificate Management > Upload certificate > Certificate Purpose: tomcat。设置证书描述并浏览当前CUCM节点的CA签名证书文件。

 注意：此时，CUCM会比较CSR和上传的CA签名证书。如果信息匹配，则CSR消失，并且上传新的CA签名证书。如果在证书上传后收到错误消息，请参阅 Upload Certificate Common Error Messages。


第六步：要向服务器应用新证书，需要通过CLI重新启动Cisco Tomcat服务（先从发布服务器启动，然后逐个订阅服务器），请使用命令 `utils service restart Cisco Tomcat`。


要验证CUCM现在使用的Tomcat证书，请导航到节点的网页并在浏览器中选择 Site Information（锁定图标）。单击 `certificate`选项，并验证新证书的尺寸。





CallManager证书

 注意：请勿同时重新生成CallManager和TVS证书。这会导致终端上已安装的ITL出现不可恢复的不匹配，需要从集群中的所有终端中删除ITL。完成CallManager的整个过程，并在电话重新注册后，启动TVS过程。

 **注意：**要确定集群是否处于混合模式，请导航到Cisco 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)。

对于集群的所有CallManager节点：

步骤1:导航 Cisco Unified OS Administration > Security > Certificate Management > Find 到CallManager证书的到期日期。

第二步：单击。Generate CSR > Certificate Purpose: CallManager选择所需的证书设置，然后单击Generate。等待系统显示成功消息，然后单击Close。

第三步：下载CSR。单击。Download CSR. Select Certificate Purpose: CallManager and click Download


第四步：将CSR发送到Certificate Authority。

第五步：证书颁发机构为签名证书链返回两个或多个文件。按以下顺序上传证书：

- CallManager-trust的根CA证书。导航到Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust。设置证书说明并浏览根证书文件。
- 中间证书作为CallManager-trust (可选)。导航到Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust。设置证书描述并浏览中间证书文件。

 **注意：**某些CA不提供中间证书。如果仅提供根证书，则可省略此步骤。

- CA签名证书作为CallManager。导航到Certificate Management > Upload certificate > Certificate Purpose: CallManager。设置证书描述并浏览当前CUCM节点的CA签名证书文件。

 **注意：**此时，CUCM会比较CSR和上传的CA签名证书。如果信息匹配，则CSR消失，并且上传新的CA签名证书。如果在证书上传后收到错误消息，请参阅上传证书常见错误消息部分。


第六步：如果集群处于混合模式，请在服务重新启动之前更新CTL：[令牌](#)或[无令牌](#)。如果集群处于非安全模式，请跳过此步骤，继续执行服务重新启动。

步骤 7.要获取应用到服务器的新证书，必须重新启动所需的服务（仅当服务运行且处于活动状态时）。导航至：


- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager

步骤 8重置所有电话：

- 导航到Cisco Unified CM Administration > System > Enterprise Parameters > Reset。系统将显示一个弹出窗口，其中包含“You are about to reset all devices in the system”语句。此操作无法撤消。是否继续？选择OK，然后单击Reset。

 注意：通过RTMT监控设备注册。所有电话重新注册后，您可以继续下一个证书类型。

IPSec证书

 注意：重新生成IPSec证书时，备份或还原任务不能处于活动状态。

对于集群的所有节点（CallManager和IM&P）：

步骤1:导航到Cisco Unified OS Administration > Security > Certificate Management > Find(仅限)并验证ipsec证书的到期日期。


第二步：单击Generate CSR > Certificate Purpose：ipsec。选择所需的证书设置，然后单击Generate。等待系统显示成功消息，然后单击Close。

第三步：下载CSR。点击下载CSR。选择Certificate Purpose ipsec并单击Download。


第四步：将CSR发送到证书颁发机构。

第五步：证书颁发机构为签名证书链返回两个或多个文件。按以下顺序上传证书：

- 根CA证书为ipsec-trust。导航到证书管理>上传证书>证书用途：ipsec-trust。设置证书说明并浏览根证书文件。
- 中间证书作为ipsec-trust（可选）。导航到证书管理>上传证书>证书用途：tomcat-trust。设置证书描述并浏览中间证书文件。

 注意：某些CA不提供中间证书。如果仅提供根证书，则可省略此步骤。


- CA签名的证书作为ipsec。导航到证书管理>上传证书>证书用途：ipsec。设置证书描述并浏览当前CUCM节点的CA签名证书文件。


 注意：此时，CUCM会比较CSR和上传的CA签名证书。如果信息匹配，则CSR消失，并且上传了新的CA签名证书。如果在证书上传后收到错误消息，请参阅上传证书常见错误消息部分。


第六步：要获取应用到服务器的新证书，必须重新启动所需的服务（仅当服务运行且处于活动状态时）。导航至：

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco DRF Master（发布方）
- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco DRF Local（发布服务器和订用服务器）

CAPF证书

 注意：要确定集群是否处于混合模式，请导航到Cisco 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)。

 注意：CAPF服务仅在发布服务器中运行，并且这是使用的唯一证书。无需获取由CA签名的用户节点，因为这些节点未使用。如果证书在订用服务器中过期，并且您希望避免出现过期证书的警报，则可以将订用服务器CAPF证书重新生成成为自签名。有关详细信息，请参阅[CAPF证书自签名](#)。

在发布服务器中：

步骤1:导航到Cisco Unified OS Administration > Security > Certificate Management > Find，并验证CAPF证书的到期日期。


第二步：单击Generate CSR > Certificate Purpose：CAPF。选择所需的证书设置，然后单击Generate。等待系统显示成功消息，然后单击Close。

第三步：下载CSR。点击下载CSR。选择“证书用途”CAPF并单击下载。


第四步：将CSR发送到证书颁发机构。

第五步：证书颁发机构为签名证书链返回两个或多个文件。按以下顺序上传证书：

- CAPF-trust的根CA证书。导航到证书管理>上传证书>证书用途：CAPF-trust。设置证书说明并浏览根证书文件。
- 中间证书作为CAPF-trust（可选）。导航到证书管理>上传证书>证书用途：CAPF-trust。设置证书描述并浏览中间证书文件。

 注意：某些CA不提供中间证书。如果仅提供根证书，则可省略此步骤。

- CA签名的证书作为CAPF。导航到证书管理>上传证书>证书用途：CAPF。设置证书描述并浏览当前CUCM节点的CA签名证书文件。

 注意：此时，CUCM会比较CSR和上传的CA签名证书。如果信息匹配，则CSR消失，并且上传了新的CA签名证书。如果在证书上传后收到错误消息，请参阅上传证书常见错误消息部分。

第六步：如果集群处于混合模式，请在服务重新启动之前更新CTL：[令牌](#)或[无令牌](#)。如果集群处于非安全模式，请跳过此步骤并继续重新启动服务。


步骤 7.要获取应用到服务器的新证书，必须重新启动所需的服务（仅当服务运行且处于活动状态时）。导航至：

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service（服务运行的所有节点。）
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP（服务运行的所有节点。）


- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco Certificate Authority Proxy Function (Publisher)

步骤 8重置所有电话：

- 导航到Cisco Unified CM管理>System >企业参数>重置。系统将显示一个弹出窗口，其中包含“You are about to reset all devices in the system”语句。此操作无法撤消。是否继续？选择确定，然后单击重置。

 注意：通过RTMT监控设备注册。所有电话重新注册后，您可以继续下一个证书类型。

TVS证书

 注意：请勿同时重新生成CallManager和TVS证书。这会导致终端上已安装的ITL出现不可恢复的不匹配，需要从集群中的所有终端中删除ITL。完成CallManager的整个过程，并在电话重新注册后，启动TVS过程。

对于集群的所有TVS节点：

步骤1:导航到Cisco Unified OS Administration > Security > Certificate Management > Find并验证TVS证书的到期日期。


第二步：单击Generate CSR > Certificate Purpose：TVS。选择所需的证书设置，然后单击Generate。等待系统显示成功消息，然后单击Close。

第三步：下载CSR。点击下载CSR。选择证书用途TVS，然后单击下载。

第四步：将CSR发送到证书颁发机构。

第五步：证书颁发机构为签名证书链返回两个或多个文件。按以下顺序上传证书：

- 根CA证书为TVS-trust。导航到证书管理>上传证书>证书用途：TVS-trust。设置证书说明并浏览根证书文件。
- 中间证书作为TVS-trust（可选）。导航到证书管理>上传证书>证书用途：TVS-trust。设置证书描述并浏览中间证书文件。

 注意：某些CA不提供中间证书。如果仅提供根证书，则可省略此步骤。

- CA签名的证书作为TVS。导航到证书管理>上传证书>证书用途：TVS。设置证书描述并浏览当前CUCM节点的CA签名证书文件。

 注意：此时，CUCM会比较CSR和上传的CA签名证书。如果信息匹配，则CSR消失，并且上传新的CA签名证书。如果在证书上传后收到错误消息，请参阅上传证书常见错误消息部分。


第六步：要获取应用到服务器的新证书，必须重新启动所需的服务（仅当服务运行且处于活动状态

时)。导航至：

- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP (服务运行的所有节点。)
- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service (服务运行的所有节点。)

步骤 7.重置所有电话：

- 导航到Cisco Unified CM管理>System >企业参数>重置。系统将显示一个弹出窗口，其中包含“**You are about to reset all devices in the system**”语句。此操作无法撤消。是否继续？选择确定，然后单击重置。

 注意：通过RTMT监控设备注册。所有电话重新注册后，您可以继续使用下一个证书类型。

常见上传的证书错误消息疑难解答

本节列出了上传CA签名证书时的一些最常见的错误消息。

CA证书在信任库不可用

此错误表示根证书或中间证书未上传到CUCM。在上传服务证书之前，验证这两个证书是否已作为信任库上传。

文件/usr/local/platform/.security/tomcat/keys/tomcat.csr不存在

如果证书 (tomcat、callmanager、ipsec、capf和tvs) 的CSR不存在，则会出现此错误。验证之前是否创建了CSR以及证书是否基于该CSR而创建。需要牢记的要点：

- 每个服务器和证书类型只能存在1个CSR。这意味着如果创建了新的CSR，旧的CSR将被替换。
- CUCM不支持通配符证书。
- 如果没有新的CSR，则无法替换当前已存在的服务证书。
- 同一问题的另一个可能错误是“无法上载文件/usr/local/platform/upload/certs//tomcat.der”。这取决于CUCM版本。

CSR公钥和证书公钥不匹配

当CA提供的证书的公钥与CSR文件中发送的公钥不同时，会出现此错误。可能的原因包括：

- 上传了不正确的证书 (可能来自其他节点)。
- CA证书是使用其他CSR生成的。
- CSR已重新生成，并取代了用于获取签名证书的旧CSR。

要验证CSR和证书公钥是否匹配，可在线使用多个工具，例如[SSL](#)。

What to Check

- Check if a Certificate and a Private Key match
- Check if a CSR and a Certificate match

Enter your Certificate:

```
Tj|13aW4xMxDT|1DRFAQ049UHVbGj|Thw52v5jTlwU2VydMjZOMsQ049U2Vy
dm|jZOMsQ049Q29uZmindJhdGlvbixQ21jB2xYWkREM9bXg/r2VydGlmawWvh
dGv5Zi2vY2f0awWjuTGlddD9mXNIP29awvjdENSY0NzPWNSTERpc3RyaWw1dGlv
bllBvaW50MIG7BgggBgEFBQcBAQSBnjCBqrCBqAYKwYBBQUHMAKGZicsZGFwO18v
LONOPUNvbGxhYmYyMENBLENDPUFjQ5xDTj1QdVjsawWMMjBLZXklMjBTZjZaWml
cyxDTj1T2ZjZaWmlcyxDTj1Db25maWwd1cmF0awW9uLERDPWNvbGxhYmYEQz1teD9j
QUwlcncRz2mJmYXRP2jnc2urbzjgZWNOQ2xhc3M9Y2VydGlmawWnhdGwbf1dGlv
cm00eTAhBgkrBgEEAYl3FAIEFB4SAFA2QBIAPMAZQByAHYA2QByMA0GC5qGSib3
DQEBCwUAA4BAQCFqj2BkZ8CMxkunQavdYauleOdfDpMLSA7fhisqiw55x/bEQs
9LyqfmiddCmkoMPyGk4I2vMle4oTpKBYAQvbrApGD01mWv5u+flie9PvrygWtYl
D+ve7rMp8irVo1Tmhe/26in3lbn+Qfwe5NuvCx3wNu/dLRR3904KcaPCxvLQ6Aw
PtnWz/Kk2GRHzqacd9fvUJuoWTKDjZQsladcgsl5cvFMz3BBf0MjGBNX16jGllQ
yZZbr6Gm4pa4yIKjsUrcXhYslomecYeRheKu5kuPusDoEWvWszj0QMT7P4/Ww
z8pT2TkrQdQDAZjGujP+yBa75QGGTZWVng1
-----END CERTIFICATE-----
```

 The certificate and CSR do NOT match!

- Certificate Hash:
684ad486131856ce0015d4b3e615e1ed
3b3bef6b8f590a493921661a4c4f62e9
- CSR Hash:
635f45c1ebcd876526a3133d1ee73d9a8
4544876fdbc8dc3a4d8fed377dcc635

Enter your CSR:

```
q+hj|gokSx+ogqYavFSNRdqTh0Girts1ga0pJ5sGxOOLCqAtQhEARNecGyanZzrk
g5|TQHfBJSD2vD7yD3wag5yhfwvliqkMUI3RD5qcsDHYfLLGLs8hB9ySHqaDA3
1hwJ5Q4RXZ188ESclIB3BA0ZegZ05vW4r05fB09e/cTWsXZIBLQytVCDGk
O0rdW2xLwaUv2u2jyWTmLD79hCN/XOM9XyPjJb6wlyMUf0DFh+s0F1M7ga05b
hXx54Zj0FIM0XYBWSFPDwexH7x7D+HQaPeM4YS0N4YqhxAgMBAAQgbzBtBqkqhkG
9w0BCQ4xYDBeMBOGA1UdjQQWMBQGccsGAQUFBwMBBgggBgEFBQcDAjALBgNVHQ8E
BAMCBLAwMAyDR0RBCKw4IQY3Vjb55jB2xYWludXCFTEwKXBl1Y5jdWNLmNv
bGxhY3teDANBgkqhkiG9w0BAQsIAA0CAQEAAh8gll76T59rWXOFjsg7hsj36vf
ubcw7HGPrNy6/pl9UyduN8XKDXQTizZWwC9KOA3/Fpcjyz+8LdH0r1FnnwBWCV
YcA9soNIWZsmU1+cibTH1HSg8FFoHADg+FR3+1AE7GNfGk0CA0RipRihZPGzQ6dO
62TRSfQ45Lubcwxe4EZO5jEQW7Zrkjfwby1GQKyg3CuXCETy3UunMCZnWjmnXkG0
n7B1nNdX7Ybgf21HrY+ZozPHWgbu2HwChuH1bOAMUpkwiPebQZn9H+R7drjBAZR
leXEYWL739M7BTveNmHoOnR65skwHfYbb7iq0jnhKxSy9R0S052vUhkj7Hw==
-----END CERTIFICATE REQUEST-----
```

同一问题的另一个可能错误是“无法上载文件/usr/local/platform/upload/certs//tomcat.der”。这取决于CUCM版本。

CSR使用者备用名称(SAN)和证书SAN不匹配

CSR和证书之间的SAN必须相同。这将阻止对不允许的域进行认证。要验证SAN不匹配，请执行以下步骤：

1. 解码CSR和证书（基础代码64）。有多种不同的解码器可供在线使用，例如[Decoder](#)。

2. 比较SAN条目并检验所有条目是否匹配。顺序并不重要，但CSR中的所有条目在证书中必须相同。

例如，CA签名的证书添加了两个额外的SAN条目，即证书的公用名和一个额外的IP地址。

CSR Summary	
Subject domain.com	
RDN	Value
Common Name (CN)	pub-ms.domain.com
Organizational Unit (OU)	Collaboration
Organization (O)	Cisco
Locality (L)	CUCM
State (ST)	CDMX
Country (C)	MX
Properties domain.com	
Property	Value
Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX
Key Size	2048 bits
Fingerprint (SHA-1)	C3:87:05:C8:79:FE:88:4A:86:96:77:0A:C5:88:63:27:55:3C:A4:84
Fingerprint (MD5)	CE:5C:9D:59:3F:8E:E3:26:C5:23:90:A2:F1:CA:68:86
SANS	domain.com, sub.domain.com, pub.domain.com, imp.domain.com

Certificate Summary	
Subject	
RDN	Value
Common Name (CN)	pub-ms.domain.com
Organizational Unit (OU)	Collaboration
Organization (O)	Cisco
Locality (L)	CUCM
State (ST)	CDMX
Country (C)	MX
Properties	
Property	Value
Issuer	CN = Collab CA,DC = collab,DC = mx
Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX
Valid From	17 Sep 2020, 1:24 a.m.
Valid To	17 Sep 2022, 1:24 a.m.
Serial Number	69:00:00:00:2D:5A:92:EB:EA:9A:85:65:C4:00:00:00:00:2D(2341578246081205845683969935281333940237893677)
CA Cert	No
Key Size	2048 bits
Fingerprint (SHA-1)	4E:15:F7:F3:9C:37:A9:8D:52:1A:6C:6D:4D:7D:AF:FE:08:EB:8D:0F
Fingerprint (MD5)	D8:22:33:92:50:F7:70:2A:05:28:90:2D:57:C0:FF:EC
SANS	pub-ms.domain.com, domain.com, sub.domain.com, pub.domain.com, imp.domain.com, 10.xx.xx.xx

3. 一旦您发现SAN不匹配，有两种方法可以解决此问题：

1. 请您的CA管理员颁发一个证书，该证书与CSR中发送的SAN条目完全相同。
2. 在CUCM中创建符合CA要求的CSR。

修改由CUCM创建的CSR的步骤：

1. 如果CA删除域，则可以在CUCM中创建没有域的CSR。创建CSR时，删除默认填充的域。
2. 如果创建了多SAN证书，则有些CA不接受公用名中的-ms。创建CSR时，可以从CSR中删除-ms。

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose [Ⓜ] tomcat

Distribution [Ⓜ] Multi-server(SAN)

Common Name [Ⓜ] 115pub.ms

Subject Alternate Names (SANs)

Auto-populated Domains

115imp.
115pub.
115sub.

Parent Domain

Other Domains

Key Type [Ⓜ] RSA

Key Length [Ⓜ] 2048

Hash Algorithm [Ⓜ] SHA256

Generate Close

3. 要添加除CUCM自动完成的名称之外的其他名称，请执行以下操作：

1. 如果使用多SAN证书，则可以添加更多FQDN。（不接受IP地址。）

Generate Certificate Signing Request

G Generate X Close

Status
⚠ Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose [*]	<input type="text" value="tomcat"/>
Distribution [*]	<input type="text" value="Multi-server(SAN)"/>
Common Name [*]	<input type="text" value="115pub-ms-██████████"/>
Subject Alternate Names (SANs)	
Auto-populated Domains	<input type="text" value="115imp.██████████"/> <input type="text" value="115pub.██████████"/> <input type="text" value="115sub.██████████"/>
Parent Domain	<input type="text"/>
Other Domains	<input type="text" value="extrahostname.domain.com"/> Choose File For more inform
	+ Add

Key Type [*]	<input type="text" value="RSA"/>
Key Length [*]	<input type="text" value="2048"/>
Hash Algorithm [*]	<input type="text" value="SHA256"/>

Generate
Close

b.如果证书是单节点，请使用set web-security命令。此命令甚至适用于多SAN证书。（可以添加任何类型的域，也允许IP地址。）

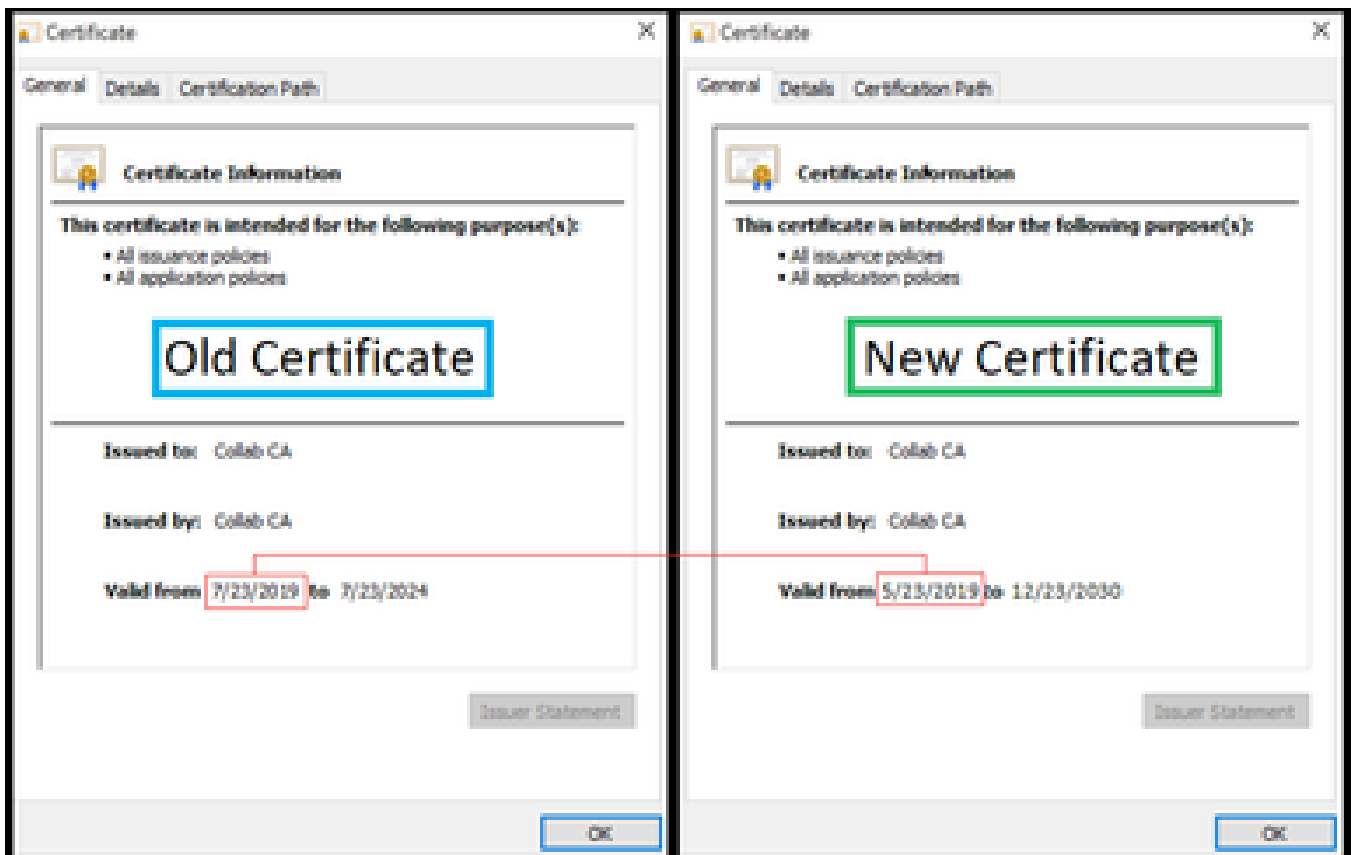
有关详细信息，请参阅[命令行参考指南](#)。

不替换具有相同CN的信任证书

CUCM设计为仅存储一个具有相同公用名称和相同证书类型的证书。这意味着，如果数据库中已经存在tomcat-trust证书，并且需要用具有相同CN的最近证书替换，则CUCM会删除旧证书并用新证书替换。

在某些情况下，CUCM不会替换旧证书：

1. 上传的证书已过期：CUCM不允许上传已过期的证书。
2. 旧证书的FROM日期比新证书的FROM日期更新。CUCM保留最新的证书，而较早的FROM日期被归类为较早的日期。对于此情况，必须删除不需要的证书，然后上传新证书。



关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。