

# 从已签名的CA证书创建新证书

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[预检查信息](#)

[配置和重新生成证书](#)

[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故障排除](#)

[CA证书在信任存储中不可用](#)

[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](#)

[不会替换具有相同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。

## 预检查信息

**注意：**有关自签名证书再生的信息，请参阅[证书再生指南](#)。有关CA签名的多SAN证书再生的信息，请参阅[多SAN证书再生指南](#)。

要了解每个证书及其再生的影响，请参阅[自签名再生指南](#)。

每种证书签名请求(CSR)类型具有不同的密钥用途，签名证书中需要这些用途。[安全指南](#)包括一个表，其中包含每种证书类型所需的密钥用法。

要更改主题设置（位置、状态、组织单元等），请运行以下命令：

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

Tomcat证书将在您运行 `set web-security` 命令。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](#)
- [思科社区步骤链接](#)
- [视频](#)

## 配置和重新生成证书

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：**验证集群中是否已禁用SSO(CM Administration > System > SAML Single Sign-On影响。如果SSO已启用，则必须先将其禁用，然后在Tomcat证书重新生成过程完成后将其启用。

在集群的所有节点（CallManager和IM&P）上：

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

步骤2.单击 **Generate CSR > Certificate Purpose: tomcat**.为证书选择所需的设置，然后单击 **Generate**.等待成功消息出现，然后单击 **Close**.

步骤3.下载CSR。点击 **Download CSR** ,选择 **Certificate Purpose: tomcat** , 并点击 **Download** .

步骤4.将CSR发送到证书颁发机构。

步骤5.证书颁发机构返回签名证书链的两个或多个文件。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**. 设置证书的说明并浏览根证书文件。
- 中间证书作为tomcat-trust ( 可选 )。导航至 **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. 设置证书的说明并浏览中间证书文件。

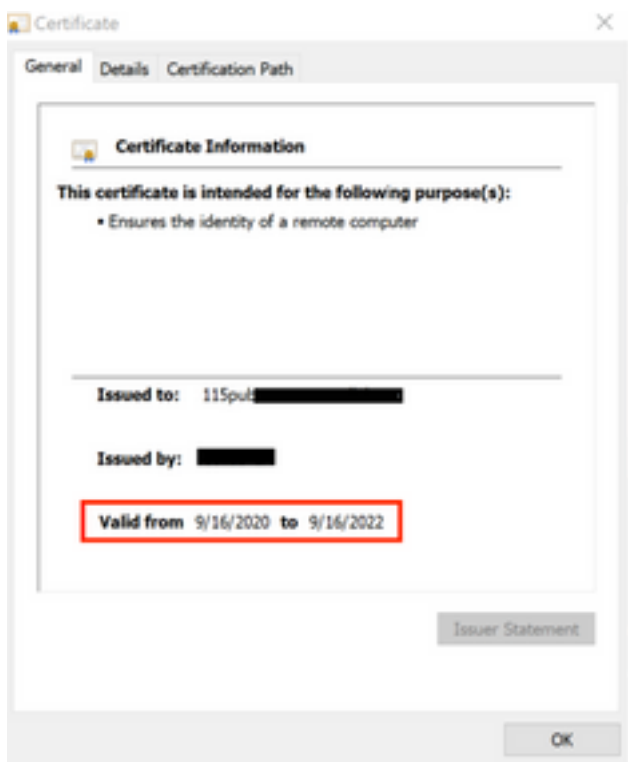
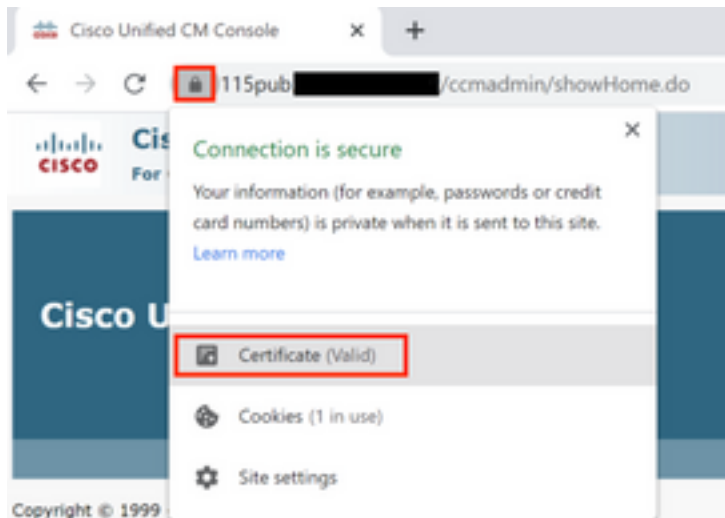
**注意：**某些CA不提供中间证书，如果仅提供根证书，则可省略此步骤。

- CA签名证书作为tomcat。导航至 **Certificate Management > Upload certificate > Certificate Purpose: tomcat**。设置证书的说明并浏览当前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** 部分。

步骤6.要获取应用到服务器的新证书，需要通过CLI重新启动Cisco Tomcat服务（先从Publisher启动，然后逐一启动），请使用命令 `utils service restart Cisco Tomcat`。

验证CUCM现在已使用Tomcat证书。导航到节点的网页并选择 Site Information（锁定图标）在浏览器中，单击 certificate 选项，并验证新证书的日期。



## CallManager证书

**警告：**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，这需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的流程。

**注意：**要确定集群是否处于混合模式，请导航到Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode(0 == Non-Secure;1 == 混合模式)。

对于集群的所有CallManager节点：

步骤1. 导航至 Cisco Unified OS Administration > Security > Certificate Management > Find 并验证CallManager证书的到期日期。

步骤2. 单击 Generate CSR > Certificate Purpose: CallManager. 为证书选择所需的设置，然后单击 Generate. 等待成功消息出现，然后单击 Close.

步骤3. 下载CSR。单击 **Download CSR**. Select **Certificate Purpose: CallManager** and click **Download**.

步骤4. 将CSR发送到 Certificate Authority .

步骤5. 证书颁发机构返回签名证书链的两个或多个文件。按以下顺序上传证书：

- 根CA证书作为CallManager-trust。导航至 Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust. 设置证书的说明并浏览根证书文件。
- 中间证书作为CallManager-trust ( 可选 )。导航至 Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust. 设置证书的说明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。导航至 Certificate Management > Upload certificate > Certificate Purpose: CallManager. 设置证书的说明并浏览当前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。

步骤6. 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[无令牌的](#)。如果集群处于非安全模式，请跳过此步骤并继续服务重新启动。

步骤7. 要使新证书应用到服务器，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：

- 导航至 Cisco Unified CM Administration > System > Enterprise Parameters > Reset. 系统将显示一个弹出窗口，其中显示语句You are about to reset all devices in the system. 此操作无法撤消。Continue? 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

**警告：**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. 导航至 Cisco Unified OS Administration > Security > Certificate Management > Find 并验证ipsec证书的到期日期。

步骤2.单击生成CSR >证书用途：ipsec.为证书选择所需的设置，然后单击Generate。等待显示成功消息，然后单击Close。

步骤3.下载CSR。单击Download CSR。选择Certificate Purpose ipsec并单击Download。

步骤4.将CSR发送到证书颁发机构。

步骤5.证书颁发机构返回签名证书链的两个或多个文件。按以下顺序上传证书：

- 根CA证书作为ipsec-trust。导航到证书管理>上传证书>证书用途：ipsec-trust。设置证书的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。设置证书的说明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.设置证书的说明并浏览当前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</strong>部分。

步骤6.要使新证书应用于服务器，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（发布者）
- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco DRF Local（Publisher和Subscribers）

## CAPF证书

**注意：**要确定集群是否处于混合模式，请转至Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode(0 == Non-Secure;1 == 混合模式)。

**注意:**CAPF服务仅在发布服务器上运行，这是唯一使用的证书。不需要获取由CA签名的用户节点，因为它们未被使用。如果证书在订阅服务器中过期，并且您希望避免过期证书的警报，您可以将订阅服务器CAPF证书重新生成成为自签名。有关详细信息，请参阅[CAPF Certificate as Self-Signed](#)。

在发布服务器中：

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

步骤2.单击生成CSR >证书用途：CAPF.为证书选择所需的设置，然后单击Generate。等待显示成功消息，然后单击Close。

步骤3.下载CSR。单击**Download CSR**。选择Certificate Purpose CAPF并单击**Download**。

步骤4.将CSR发送到证书颁发机构。

步骤5.证书颁发机构返回签名证书链的两个或多个文件。按以下顺序上传证书：

- 根CA证书作为CAPF-trust。导航到**证书管理>上传证书>证书用途：CAPF-trust**。设置证书的说明并浏览根证书文件。
- 作为CAPF-trust的中间证书（可选）。导航到**证书管理>上传证书>证书用途：CAPF-trust**。设置证书的说明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CAPF。导航到**证书管理>上传证书>证书用途：CAPF**。设置证书的说明并浏览当前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**。

步骤6.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[无令牌的](#)。如果集群处于非安全模式，请跳过此步骤并继续服务重新启动。

步骤7.要使新证书应用到服务器，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（运行服务的所有节点）
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP（运行服务的所有节点）
- 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>系统>企业参数>重置**。系统将显示一个弹出窗口，其中显示语句 You are about to reset all devices in the system.此操作无法撤消。Continue?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

**警告：**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，这需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的流程。

对于集群的所有TVS节点：

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

步骤2.单击生成CSR >证书用途：TVS.为证书选择所需的设置，然后单击Generate。等待显示成功消息，然后单击Close。

步骤3.下载CSR。单击Download CSR。选择Certificate Purpose TVS，然后单击Download。

步骤4.将CSR发送到证书颁发机构。

步骤5.证书颁发机构返回签名证书链的两个或多个文件。按以下顺序上传证书：

- 根CA证书作为TVS-trust。导航到证书管理>上传证书>证书用途：TVS信任。设置证书的说明并浏览根证书文件。
- 作为TVS-trust的中间证书（可选）。导航到证书管理>上传证书>证书用途：TVS信任。设置证书的说明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.设置证书的说明并浏览当前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。

步骤6.要使新证书应用于服务器，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（运行服务的所有节点）
- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service（运行服务的所有节点）

步骤7.重置所有电话：

- 导航到Cisco Unified CM管理>系统>企业参数>重置。系统将显示一个弹出窗口，其中显示语句You are about to reset all devices in the system.此操作无法撤消。Continue?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。

## 常见上传的证书错误消息故障排除

本节列出了上传CA签名证书时最常见的一些错误消息。

### CA证书在信任存储中不可用

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



信任存储上传。

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

当证书(tomcat、callmanager、ipsec、capf、tvs)的CSR不存在时，会出现此错误。验证之前是否创建了CSR以及是否基于该CSR创建了证书。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的错误是“无法上传/usr/local/platform/upload/certs//tomcat.der文件”。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。可能的原因是：

- 上传了不正确的证书（可能来自其他节点）。
- CA证书是使用不同的CSR生成的。
- CSR已重新生成，它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，有多个在线工具(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:

```
Tj13aW4xMxDTj1DRFAsQ049UHvibGj1IwS2v5j1hwu2VydmiJzAMsQ049U2vy
dmjZQMsQ049Q29uZmindQjhdGhbixEQz1Jb2xsYwSREM9bXg/Y2VydGimaWWh
dGV5ZXZvY2F0aW9uTGZldD9lYXNlP29laWVjdENsYXNzPWN5TERpc3RyaWJ1dGV
blBvaW50MIG7BgEgEFBQcBAQ5BjCBqCBqA1KwYBBQUHMAKGZtsZGFwOi9v
L0NOPUNvbGxhYUyMENBLENOPUFjQ5xDTj1QdWJsaWMMIMjBLZXMjBTZjZaWNI
cyxDTj1TZDQ2aWNIcyxDTj1Db25maWd1cmF0aW9uLERDPWNvbGxhYXNlEQz1teD9j
QUNicmRpZmlyXkRlP2hrc2U/b2JqZWV0Q2xhc3M9Y2VydGimaWWhdGhbikF1dGhw
cm10eTAhBgkrcBqEEAY13FAIEFB4SAFAZQBIAFMAZQBIAHYAZQBIAQOGCSqGSib3
DQEBCWUAA4BAQCFqj2Bc28CMxkunQavdYaUioDrfDpMLSA/77hisqiw55x/bEQs
9LyqftmidCmkMPFGK4t2vMie4oTpKBYAQvbrApG001miW5u+f1lo9PvrygWtYL
D+ve7rMp8sirVo1Tmhe/26in3lbn+Ofwe5NuvCx3wNudLRR3904KcaFCcsVLQ6Aw
PtmvAz/9K2GRhzqacd9fVlJuoWTKDJ2Qsladcgsl5cVFMz3BBf0MjGBNX16jGllQ
yZZbr6Gm4pa4yKq6sUrcOxHylomecYeRheKuSkuPusOoEwW5zj0QMT7P4Ww
ZBpT2TkrQdODAzhjGujP+yBa75OGGTZWVvg1
-----END CERTIFICATE-----
```

 The certificate and CSR do NOT match!

 Certificate Hash:  
684ad486131856ce0015d4b3e615e1ed  
3b3bef6b8f590a493921661a4c4f62e9

 CSR Hash:  
635f45c1ebcd876526a3133d1ee73d9a8  
4544876fdbcb8dc3a4d8fed377dcc635

### Enter your CSR:

```
q+hjgokSx+ogqVavFSNRdqTh0Grls1ga0pJ5sGxOOLCqAtQhEARNcGyanZtrK
gSjTQHfBJ5tD2vDyD3wg5iyhwNilqkMUI3IRD5qcSD/rfLGLS8hB9y5HQtaDA3
1hwJ5Q4RkX2188ESCL1B3bAozEgZ05Vw4r51P8r09e/CTWsxZtBfLgYtvcDGk
OGrdW2xLueUVZu29jWtMLD70CNXCMi9XypLj6uuyMuf0BFh+s0PIMr7gal3b
hXkS4ZjoFIMkXYBWSPDwexH7XFD+HQaPeM4Y50N4YqhxAgMBAAAGbzBtBkqkhdG
9w0BCQ4xYDBeMBOGA1UjdjQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAJALBgWwHQBE
BAMCBLAwMAYDR0RBR0xw4iOY3Vjb55j2xsYwubXCFTEhNKB1Y15jdWNIcmNv
bGxhYU50eDANBgkqhkiG9w0BAQsFAAOCQAEEAhhBgli76T59rWxOjjs7hsj36vf
ubcW7HGfRnyx6/pI9UydanRkXDXQtzZWwC9iOQA3/fpcjyz+8LdHtR1FnnwBwCV
YcAs9oNIWZsmU1+clbTH1H5g8FFoHAdg+FR3+1AE7GNfGK0CA0RlpRihZPGzQ6dO
6ZTRSfQ45LbcWxe4EZO5xjEQW7Zrkjfwby1GQYg3CuXCETy3UunMCZnwjmnXkKg0
n7B1nNdx7Ybgfz1eY+ZozPHWgbu2HwChuh1boAMUpkwiFebQZn9H+R7drgBAZR
IeXEYWL739M7B7veNmHoOnR6SkwvHybb7iqQjnhXcSy9R05052vUthkj7Hw==
-----END CERTIFICATE REQUEST-----
```

同一问题的另一个可能的错误是“无法上传/usr/local/platform/upload/certs/tomcat.der文件”。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。这会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（以64为基数）。在线提供不同的解码器，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:C5:21:9D: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:C4:00:00:00:00:00:2D(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)	D8:22:33:92:5D:F7:70:2A:05:28:9D:2D:57:C0:F7:EC
SANS	sub-ms.domain.com, domain.com, sub.domain.com, pub.domain.com, imp.domain.com, *.xx.xx.xx

3.一旦您确定SAN不匹配，有两种方法可以解决此问题：

1. 请求您的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. 如果创建多SAN证书，则有些CA不接受公用名中的“—ms”。创建“—ms”时，可以将其从CSR中删除。

**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 [REDACTED]

**Subject Alternate Names (SANs)**

Auto-populated Domains

115imp [REDACTED]  
115pub [REDACTED]  
115sub [REDACTED]

Parent Domain

Other Domains

---

Key Type\*\* RSA

Key Length\* 2048

Hash Algorithm\* SHA256

Generate Close

3.添加除CUCM自动完成的名称之外的备用名称：

1. 如果使用多SAN证书，则可以添加更多FQDN。（不接受IP地址。）

The screenshot shows a 'Generate Certificate Signing Request' dialog box. At the top, there are 'Generate' and 'Close' buttons. Below that is a 'Status' section with a warning icon and the text: 'Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type'. The main section is titled 'Generate Certificate Signing Request' and contains several fields: 'Certificate Purpose\*\*' (tomcat), 'Distribution\*' (Multi-server(SAN)), 'Common Name\*' (115pub-ms), and 'Subject Alternate Names (SANs)'. Under 'Subject Alternate Names (SANs)', there is a section for 'Auto-populated Domains' with three entries: 115imp, 115pub, and 115sub. Below that is a section for 'Other Domains' with a text input field containing 'extrahostname.domain.com' and an 'Add' button. To the right of the 'Other Domains' field is a 'Choose File' button and the text 'For more inform'. At the bottom of the dialog, there are fields for 'Key Type\*\*' (RSA), 'Key Length\*' (2048), and 'Hash Algorithm\*' (SHA256). At the very bottom, there are 'Generate' and 'Close' buttons.

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。）

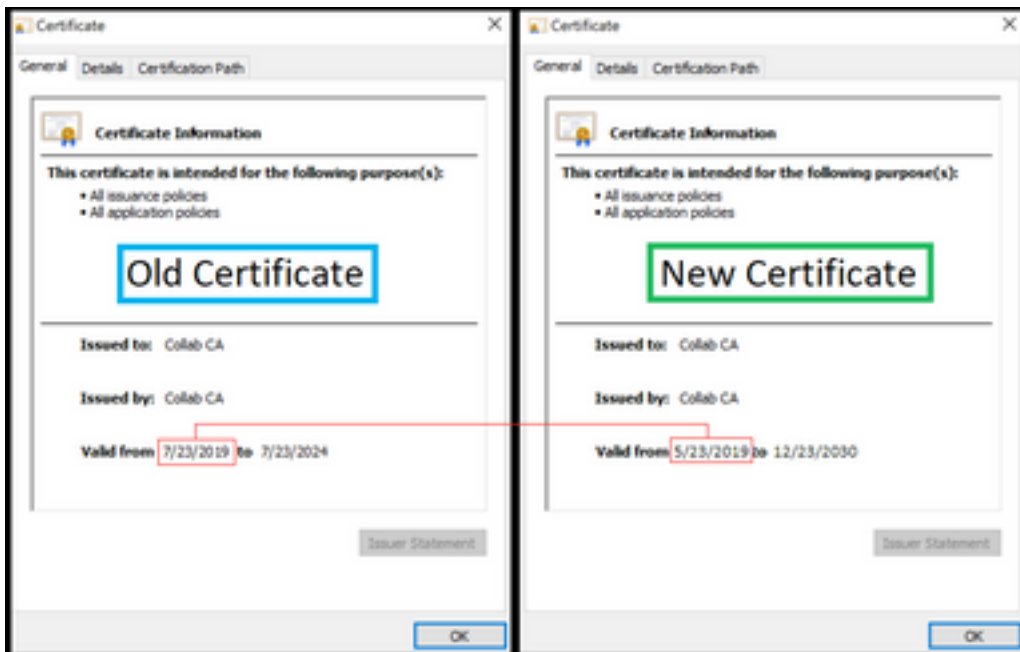
有关详细信息，请参阅[命令行参考指南](#)。

## 不会替换具有相同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tomcat-trust证书已存在于数据库中，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不允许上传过期的证书。
2. 旧证书的“FROM”日期比新证书更近。CUCM保留最新的证书，并且使用较旧的“FROM”日期目录将其标记为较旧的。对于此情况，需要删除不需要的证书，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）。