

# 重新生成CUCM IM/P服务自签名证书

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[证书存储利用率](#)

[Cisco Unified Presence \(CUP\)证书](#)

[Cisco Unified Presence -可扩展消息传送和网真协议\(CUP-XMPP\)证书](#)

[Cisco Unified Presence -可扩展消息传送和网真协议-服务器到服务器\(CUP-XMPP-S2S\)证书](#)

[IP安全\(IPSec\)证书](#)

[Tomcat证书](#)

[证书再生过程](#)

[CUP证书](#)

[CUP-XMPP证书](#)

[CUP-XMPP-S2S证书](#)

[IPSec证书](#)

[Tomcat证书](#)

[删除过期的信任证书](#)

[验证](#)

[故障排除](#)

---

简介

本文档介绍如何在CUCM IM/P 8.x及更高版本中重新生成证书的推荐分步过程。

先决条件

要求

思科建议您了解即时消息和在线状态(IM/P)服务证书。

使用的组件

本文档中的信息基于IM/P版本8.x及更高版本。

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。

背景信息

## 证书存储利用率

### Cisco Unified Presence (CUP)证书

用于SIP联合的安全SIP连接、适用于Lync/OCS/LCS的Microsoft远程呼叫控制、思科统一证书管理器(CUCM)与IM/P之间的安全连接等等。

### Cisco Unified Presence - 可扩展消息传送和网真协议(CUP-XMPP)证书

用于在创建XMPP会话时验证XMPP客户端的安全连接。

### Cisco Unified Presence - 可扩展消息传送和网真协议-服务器到服务器(CUP-XMPP-S2S)证书

用于验证与外部联合XMPP系统的XMPP域间联合的安全连接。

### IP安全(IPSec)证书

用于：

- 验证灾难恢复系统(DRS)/灾难恢复框架(DRF)的安全连接
- 验证到集群中的Cisco Unified Communications Manager (CUCM)和IM/P节点的IPsec隧道的安全连接

### Tomcat证书

用于：

- 验证各种Web访问，例如从集群中的其他节点访问服务页面和Jabber访问。
- 验证SAML单点登录(SSO)的安全连接。
- 验证集群间对等体的安全连接。



**注意：**如果在统一通信服务器上使用SSO功能，并且重新生成Cisco Tomcat证书，则必须使用新证书重新配置SSO。在CUCM和ADFS 2.0上配置SSO的链接是：<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html>。



**注意：**CUCM证书重新生成/续订流程的链接为：<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html>。

---

## 证书再生过程

### CUP证书

步骤1:为集群中的每台服务器打开图形用户界面(GUI)。从IM/P发布服务器开始，然后依次打开每个IM/P订用服务器的GUI并导航至Cisco Unified OS Administration > Security > Certificate Management.

第二步：从发布者GUI开始，然后选择Find显示所有证书。选择cup.pem证书。打开后，选择Regenerate，并等到看到成功再关闭弹出

窗口。

第三步：继续后续用户，参考与步骤2中相同的过程。并完成集群中的所有用户。

步骤4.在所有节点上重新生成CUP证书后，必须重新启动服务。



**注意：**如果在线状态冗余组配置已选中Enable High Availability，Uncheck则在服务重新启动之前。可以访问CUCM Pub Administration > System > Presence Redundancy Group在线状态冗余组配置。重新启动服务会导致IM/P暂时中断，必须在生产时间之外完成。

按以下顺序重新启动服务：

· 登录发布服务器的Cisco Unified Serviceability：

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. 思科Restart SIP代理服务。

c. 服务重新启动完成后，继续使用用户和Restart Cisco SIP代理服务。

d. 从发布者开始，然后继续发布订阅者。Restart 思科SIP代理服务(也来自Cisco Unified Serviceability > Tools > Control Center - Feature Services)。

· 登录发布服务器的Cisco Unified Serviceability：

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco Presence引擎服务。

c. 服务重新启动完成后，继续在用户Restart 上使用Cisco Presence EngineService。



**注意：**如果为SIP联合配置，Restart Cisco XCP SIP联合连接管理器服务(位于Cisco Unified Serviceability > Tools > Control Center - Feature Services)。从发布服务器开始，然后继续发布订阅服务器。

## CUP-XMPP证书



**注意：**由于Jabber使用CUCM和IM/P Tomcat以及CUP-XMPP服务器证书来验证Tomcat和CUP-XMPP服务的连接，因此，这些CUCM和IM/P证书在大多数情况下都是CA签名的。假设Jabber设备没有根证书和中间证书(该证书是CUP-XMPP证书的一部分安装在其证书信任库中)，在这种情况下，Jabber客户端会显示不可信证书的安全警告弹出窗口。如果尚未安装在Jabber设备信任存储的证书中，则必须通过组策略、MDM、邮件等将根证书和任何中间证书推送到Jabber设备，具体取决于Jabber客户端。



**注意：**如果CUP-XMPP证书是自签名证书，并且如果CUP-XMPP证书未安装在Jabber设备证书的信任库中，则Jabber客户端会显示不可信证书的安全警告弹出窗口。如果尚未安装，则必须通过组策略、MDM、邮件等将自签名CUP-XMPP证书推送到Jabber设备，具体取决于Jabber客户端。

步骤1:为集群中的每台服务器打开GUI。从IM/P发布服务器开始，然后依次打开每个IM/P用户服务器的GUI并导航到Cisco Unified OS Administration > Security > Certificate Management。

第二步：从发布者GUI开始，然后选择Find显示所有证书。从证 cup-xmpp.pem 书的type列中，确定证书是自签名还是CA签名。如果证 cup-xmpp.pem 书是第三方签名（类型为CA签名）的分发多SAN，请在生成多SAN CUP-XMPP CSR并提交CA以获取CA签名的CUP-XMPP证书时查看此链接；[使用CA签名的多服务器主体备用名进行统一通信集群设置配置示例](#)。

如果证 cup-xmpp.pem 书是第三方签名的（键入CA签名）分发单节点（分发名称等于证书的公用名称），请在生成单节点CUP-XMPP CSR并提交CA以获取CA签名的CUP-XMPP证书时查看此链接；[Jabber完成证书验证操作指南](#)。如果证cup-xmpp.pem 书是自签名的，请继续进行步骤3。

第三步：选择Find以显示所有证书，然后选择cup-xmpp.pem证书。打开后，选择Regenerate，并等到看到成功再关闭弹出窗口。

第四步：继续后续用户；请参阅步骤2中的相同过程，并为集群中的所有用户完成该过程。

第五步：在所有节点上重新生成CUP-XMPP证书后，必须在IM/P节点上重新启动Cisco XCP路由器服务。



**注意：**如果在线状态冗余组配置已选中Enable High Availability，Uncheck则在服务重新启动之前会进行此操作。可以访问CUCM Pub Administration > System > Presence Redundancy Group在线状态冗余组配置。重新启动服务会导致IM/P临时中断，必须在生产时间之外完成。

· 登录发布服务器的Cisco Unified Serviceability：

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart Cisco XCP路由器服务。

c.服务重新启动完成后，在用户上继续使用RestartCisco XCP路由器服务。

#### CUP-XMPP-S2S证书

步骤1: 为集群中的每台服务器打开GUI。从IM/P发布服务器开始，然后依次打开通向每个IM/P用户服务器的GUI并导航到Cisco Unified OS Administration > Security > Certificate Management。

第二步：从发布者GUI开始，选择 Find显示所有证书，并选择cup-xmpp-s2s.pem证书。打开后，选择Regenerate，并等到看到成功再关闭弹出窗口。

第三步：继续后续用户，并参考步骤2中的相同步骤，完成集群中所有用户的操作。

第四步：在所有节点上重新生成CUP-XMPP-S2S证书后，必须按照上述顺序重新启动服务。



**注意：**如果在线状态冗余组配置已选中Enable High Availability，Uncheck则在重新启动这些服务之前会进行此操作。可以在CUCM Pub Administration > System > Presence Redundancy Group上访问在线状态冗余组配置。重新启动服务会导致IM/P暂时中断，必须在生产时间之外完成。

· 登录发布服务器的Cisco Unified Serviceability：

- a. Cisco Unified Serviceability > Tools > Control Center - Network Services.
- b. Restart Cisco XCP路由器服务。
- c. 服务重新启动完成后，继续在用户Restart 上使用Cisco XCP路由器服务。

· 登录发布服务器的Cisco Unified Serviceability：

- a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.
- b. Restart Cisco XCP XMPP联合连接管理器服务。
- c. 服务重新启动完成后，继续在用户Restart 上使用Cisco XCP XMPP联合连接管理器服务。

## IPSec证书



**注意：**CUCM发布方中的证 ipsec.pem 书必须有效且存在于IPSec信任库中的所有用户（CUCM和IM/P节点）中。发布服务器中不存在用户的证 ipsec.pem 书，因为标准部署中存在IPSec信任存储。要验证有效性，请将CUCM-PUB的 ipsec.pem 证书中的序列号与用户中的IPSec-trust进行比较。他们必须匹配。



**注意：**DRS在源代理和本地代理之间使用基于安全套接字层(SSL)的通信，以对CUCM集群节点（CUCM和IM/P节点）之间的数据进行身份验证和加密。DRS将IPSec证书用于其公钥/私钥加密。请注意，如果您从Certificate Management页面删除IPSEC信任存储(hostname.pem)文件，则DRS不会按预期工作。如果手动删除IPSEC信任文件，则必须确保将IPSEC证书上传到IPSEC信任库。有关详细信息，请参阅《CUCM安全指南》中的证书管理帮助页面。

步骤1:为集群中的每台服务器打开GUI。从IM/P发布服务器开始，然后依次打开通向每个IM/P用户服务器的GUI并导航到Cisco Unified OS Administration > Security > Certificate Management。

第二步：从发布者GUI开始，选择Find显示所有证书。Choose ipsec.pem 该证书。打开后，选择Regenerate，并等到看到成功再关闭弹出窗口。

第三步：继续后续用户，并参考步骤2中的相同步骤，完成集群中所有用户的操作。

第四步：在所有节点重新生成IPSEC证书之后，再生Restart这些服务。导航到发布服务器的Cisco Unified Serviceability；Cisco Unified Serviceability > Tools > Control Center - Network Services。

- a. 在Cisco DRF主要服务上选择Restart。
- b. 服务重新启动完成后，在发布服务器上选择Restart of Cisco DRF Local service，然后继续操作Restart(在每个用户上)Cisco DRF Local service。

## Tomcat证书



**注意：**由于Jabber使用CUCM Tomcat和IM/P Tomcat及CUP-XMPP服务器证书来验证Tomcat和CUP-XMPP服务的连接，因此这些CUCM和IM/P证书在大多数情况下都使用CA签名。假设Jabber设备没有根证书和属于其证书信任库中Tomcat证书一部分的任何中间证书。在这种情况下，Jabber客户端会显示不可信证书的安全警告弹出窗口。如果尚未安装在Jabber设备的证书信任库中，则必须通过组策略、MDM、邮件等将根证书和任何中间证书推送到Jabber设备，具体取决于Jabber客户端。

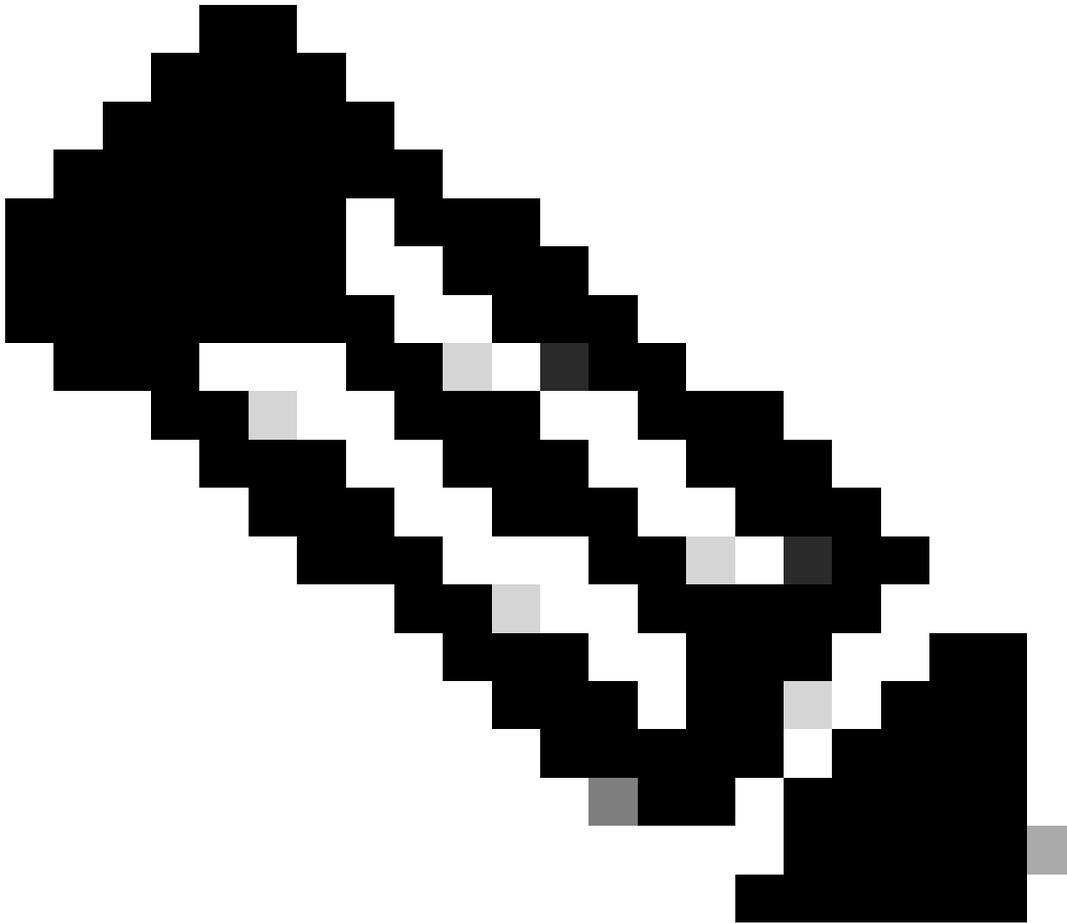
 **注意：**如果Tomcat证书是自签名证书，且未在Jabber设备的证书信任存储中安装Tomcat证书，则Jabber客户端会显示不受信任证书的安全警告弹出窗口。如果尚未安装在Jabber设备的证书信任库中，则必须通过组策略、MDM、邮件等将自签名CUP-XMPP证书推送到Jabber设备，具体取决于Jabber客户端。

步骤1:为集群中的每台服务器打开GUI。从IM/P发布服务器开始，然后依次打开每个IM/P用户服务器的GUI并导航到Cisco Unified OS Administration > Security > Certificate Management。

第二步：从发布服务器GUI开始，然后选择Find 以显示所有证书。

· 从tomcat.pem证书的“类型”列中，确定证书是自签名还是CA签名。

· 如果tomcat.pem证书是第三方签名（类型CA签名）的分发多SAN，请查看此链接了解如何生成多SAN Tomcat CSR并提交到CA以获取CA签名的Tomcat证书，[统一通信集群使用CA签名的多服务器主体备用名配置示例](#)



**注意：**多SAN Tomcat CSR在CUCM发布服务器上生成，并分发给集群中的所有CUCM和IM/P节点。

---

· 如果证 tomcat.pem 书是第三方签名的（键入CA签名）分发单节点（分发名称等于证书的公用名称），请查看此链接以生成单节点 CUP-XMPP CSR，并将其提交给CA以获取CA签名的CUP-XMPP证书，[Jabber完成证书验证操作指南](#)

· 如果证 tomcat.pem 书是自签名的，请继续进行步骤3

第三步：选择Find以显示所有证书：

- 选择tomcat.pem证书。
- 打开后，选择Regenerate，并等到看到成功弹出窗口再关闭弹出窗口。

第四步：继续使用每个后续订用服务器，参阅步骤2中的过程，并完成集群中的所有订用服务器。

第五步：所有节点重新生成Tomcat证书后，Restart将在所有节点上使用Tomcat服务。从发布者开始，然后是订阅者。

· 为了Restart实现Tomcat服务，您必须为每个节点打开一个CLI会话并运行该命令，直到服务重新启动Cisco Tomcat，如图所示：

```
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: █
```

## 删除过期的信任证书



**注意：**可以适时删除以-trust结尾的信任证书。可以删除的信任证书是那些不再需要、已过期或已过期的证书。请勿删除五个身份证书：cup.pem、cup-xmpp.pem、cup-xmpp-s2s.pem、ipsec.pem和tomcat.pem证书。如图所示，服务重新启动旨在清除这些服务中这些旧证书的任何内存信息。



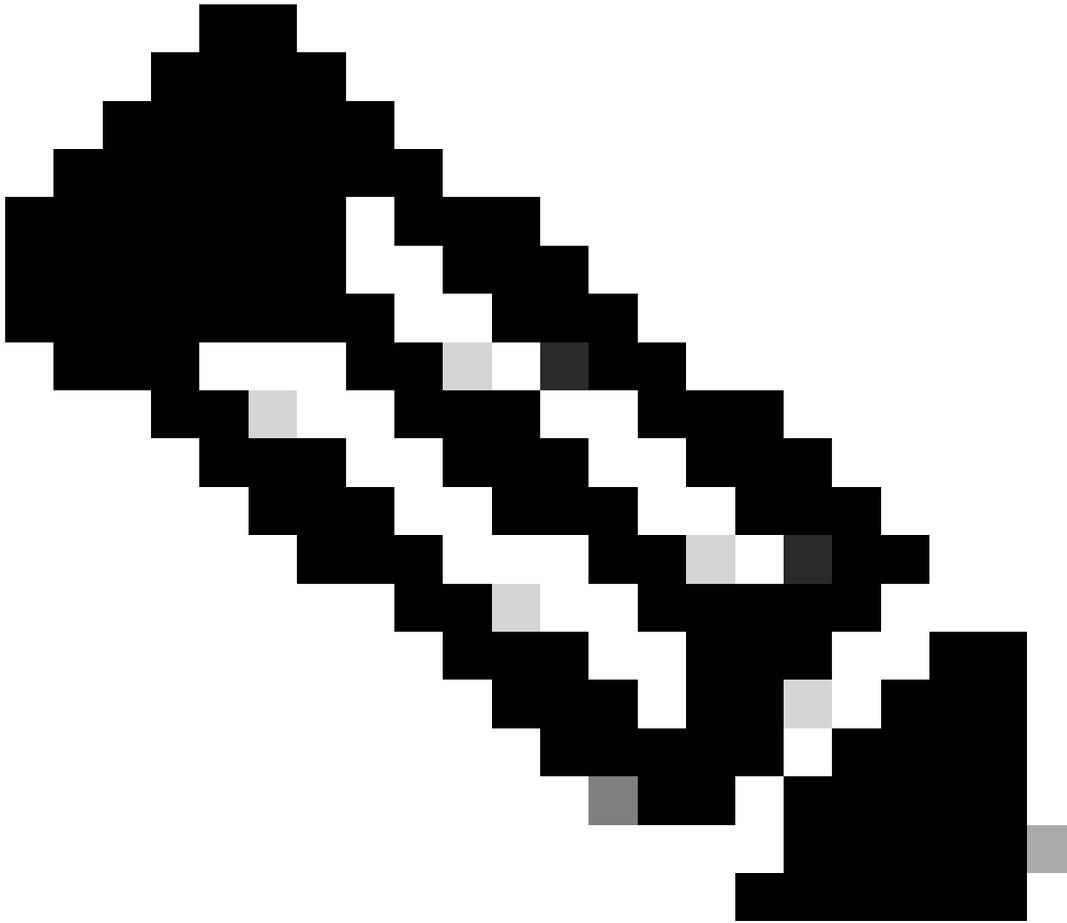
**注意：**如果在线状态冗余组配置已选中Enable High Availability，则Uncheck在服务为Stopped/Started 或Restarted之前需要启用此功能。可以访问CUCM Pub Administration > System > Presence Redundancy Group在线状态冗余组配置。如图所示，重新启动某些服务会导致IM/P暂时中断，必须在生产时间之外完成。

---

步骤1:导航至：Cisco Unified Serviceability > Tools > Control Center - Network Services

· 从下拉菜单中，选择您的IM/P发布者，然后从Cisco Certificate Expiry Monitor中选择Stop，然后在Cisco Intercluster Sync Agent中选择Stop。

· 对集群中的每个IM/P节点重复这些服务的Stop。



**注意：**如果必须删除Tomcat-trust证书，请导航到CUCM发布者的Cisco Unified Serviceability > Tools > Control Center - Network Services。

- 
- 从下拉列表中，选择CUCM发布者。
  - 从Cisco Certificate Expiry Monitor选择Stop，然后在Cisco Certificate Change Notification中选择Stop。
  - 对集群中的每个CUCM节点重复此操作。

**第二步：**导航到Cisco Unified OS Administration > Security > Certificate Management > Find。

- 查找过期的信任证书(对于10.x版及更高版本，您可以按到期进行过滤。从10.0之前的版本，您必须手动或通过RTMT警报 ( 如果收到 ) 识别特定证书。

- 同一信任证书可以出现在多个节点中，必须从每个节点中逐个删除。
- 选择要删除的信任证书（根据版本，系统会显示弹出窗口或导航至同一页面上的证书）。
- 选择Delete（您将永久删除此证书.....”作为开头的弹出窗口）。
- 点击 OK.

第三步：对要删除的每个信任证书重复此过程。

第四步：完成后，必须重新启动与已删除的证书直接相关的服务。

- CUP-trust：Cisco SIP代理、Cisco Presence引擎，如果针对SIP联合进行配置，则使用Cisco XCP SIP联合连接管理器（请参阅CUP证书部分）
- CUP-XMPP-trust：思科XCP路由器（请参阅CUP-XMPP证书部分）
- CUP-XMPP-S2S-trust：思科XCP路由器和思科XCP XMPP联合连接管理器
- IPSec-trust：DRF源/DRF本地（请参阅IPSec证书部分）
- Tomcat-trust：通过命令行重新启动Tomcat服务（请参阅Tomcat certificate部分）

第五步：重新启动服务已在步骤1中停止。

## 验证

当前没有可用于此配置的验证过程。

## 故障排除

目前没有针对此配置的故障排除信息。

## 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）。