证书确认的Jabber完整入门指南

目录

[简介](#)
[哪些Jabber客户端是否是受此更改的影响的？](#)
[这是什么意思Jabber环境？](#)
[哪证书要求？](#)
[什么方法为证书确认是可用的？](#)
[如果证书自已签署的或CA签名的，请验证](#)
[生成 CSR](#)
[I进口证明书到用户设备证书存储？](#)
[在证书的服务器标识](#)
[标识符字段](#)
[XMPP证书](#)
[HTTP证书](#)
[防止标识不匹配](#)
[提供XMPP域给客户端](#)
[相关信息](#)

简介

本文结合几Cisco资源到使用为了实现所有证书确认的需求在思科Jabber的一个完整，统一的入门指南。因为思科Jabber当前要求使用证书确认为了建立安全连接用服务器，这是必要的。此需求需要也许为用户环境要求的许多更改。

> **注意**：此指南是为仅前提部署。因为他们验证公共Certificate Authority (CA)，当前没有为网云服务部署要求的更改。

哪些Jabber客户端是否是受此更改的影响的？

这是列出所有客户端实现证书确认的表：

表 1

桌面客户端	**莫比尔和片剂客户端**
麦金塔版本的9.2 (九月2013) Jabber	IP电话版本的9.5 (十月2013) Jabber
Microsoft (MS) Windows版本的9.2.5 (九月2013) Jabber	IP电话和iPad版本的9.6 (十一月2013) Jabber
	机器人版本的9.6 (十二月2013) Jabber

这是什么意思Jabber环境？

当您安装或升级给在**表**列出的所有客户端**1时**，必须证书确认用服务器使用安全连接。本质上，当Jabber客户端尝试当前时建立安全连接，服务器提交与证书的思科Jabber。思科Jabber然后尝试验证那些证书设备的证书存储。如果客户端不能验证证书，提示您确认您要接受证书，并且在其企业托拉斯存储安置它。

哪证书要求？

这是他们提交对思科Jabber为了建立安全连接前提服务器的列表和证书：

表 2

服务器	**证书**
Cisco Unified Presence	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager IM和在线状态	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager	HTTP (Tomcat)
Cisco Unity Connection	HTTP (Tomcat)
思科WebEx会议服务器	HTTP (Tomcat)

这是注释的一些重点：

- 申请最最近的服务更新(SU) Cisco Unified Presence (CUP)或Cisco Unified Communications Manager (CUCM) IM和在线状态，在您开始证书签署的进程前。
- 需要的证书适用于所有服务器版本。例如， CUP版本8.x和CUCM IM和在线状态版本9.x和以上提交有可扩展消息传送和在线状态协议(XMPP)和HTTP证书的客户端。
- 在集群的每个节点，用户和发行商，管理Tomcat服务，并且能提交有HTTP证书的客户端。计划签署每个节点的证书在集群。
- 为了获取发信号在客户端和CUCM之间的会话初始化协议(SIP)，请使用证书颁发机构代理功能(CAPF)登记。

什么方法为证书确认是可用的？

当前有能使用证明验证的几个方法。

方法 1：用户单击**接受**对所有证书弹出窗口。这也许是更加小的环境的多数理想的解决方案。如果单击**接受**，证书被放置到企业托拉斯存储在设备。在证书在企业托拉斯存储后安置，不再提示用户，当他们登录该本地设备的时Jabber客户端。

方法 2：需要的证书(**表2)**从单个服务器下载(默认情况下，这些是自签名证书)并且安装到企业托拉斯用户设备的存储。如果您的环境不访问证书签字的，私有或公共CA这也许是理想的解决方案。

几个方法可以用于为了推送这些证书对用户，但是一个快速方法将使用使用Microsoft Windows注册：

1. 从其中一台机器，请接受提交闲聊到企业托拉斯存储的所有证书。

2. 为了验证证书存在，输入**Certmgr.msc命令**并且导航对EnterpriseTrust **>证书。**
3. 开放**Regedit**用**运行**命令和导航对**HKCU >软件> Microsoft > SystemCertificates >信任>证书。**
4. 用鼠标右键单击并且导出在注册的Certifates文件夹作为**.reg**文件。
5. 通过组策略对象(GPO)推出此文件对所有用户(或其他首选方法)。

这完成企业信任认证安装Jabber的，并且不再提示用户。

方法 3：公共或私有CA (**表2)**签署所有需要的证书。这是思科推荐的方法。此方法要求证书签名请求(CSR)为其中每一证书生成，签字，重新上传的对服务器，然后导入给可信的根证书权限用户设备的存储。请参阅**生成CSR**和**我如何有证书用户设备证书存储？**本文的部分欲知更多信息。

注意：一旦公共CA，根证明应该已经在客户端信任存储。

请记住公共CA典型地要求CSR为了依照特定格式。例如，公共CA也许只接受CSR那：

- 是Base64-encoded
- 请勿包含某些字符，例如@&! 在组织、组织单位(OU)，或者其他字段
- 请使用特定比特长度在公共密钥服务器

同样，如果提交从多个节点的CSR，公共CA也许需要信息是一致在所有CSR。

为了防止与您的CSR的问题，请查看从您计划提交CSR的公共CA的格式需求。然后请保证您输入的信息，当您配置您的服务器依照公共CA要求的格式时。

这是您也许遇到的一个可能的需求：

每FQDN:一证书某个公共CA符号仅每完全合格的域名(FQDN)一证书。

例如，为了签署单个CUCM IM和在线状态节点的HTTP和XMPP证书，您也许需要提交每个CSR到不同的公共CA。

如果证书自已签署的或CA签名的，请验证

注意：此示例是为CUCM版本8.x。进程也许变化在服务器之间。

1. 导航对**Cisco Unified OS管理。**
2. 选择**安全> Certificate Management。**
3. 查找并且点击Tomcat**托拉斯证书.pem**文件。
4. 点击**下载**，并且**保存。**
5. 导航到文件，并且重命名它与**.cer**分机。
6. 打开并且查看此文件(微软视窗用户)。
7. 验证字段**发出的。**如果它匹配**发出对**字段，则证书自已签署的(请参见**示例**)。

示例：自已签署的与私有CA签发的证书

自已签署的私有CA签名的

生成 CSR

注意：此示例是为CUCM版本8.x。进程也许变化在服务器之间。

1. 导航对**Cisco Unified OS管理**。
2. 选择**安全> Certificate Management**。
3. 单击**生成CSR**，并且从下拉列表选择**Tomcat**。
4. 单击**生成CSR**，并且点击**Close**。
5. 点击**下载CSR**，并且从下拉列表选择**Tomcat**。
6. 点击**下载CSR**，并且保存文件。
7. 发送您的私有CA服务器或公共CA将签字的**.csr**文件。
   注意：一旦有此CSR文件，进程变化基于您的环境。
8. 单击**加载证书/证书链**在**安全> Certificate Management**为了重新上传下发出到您的服务器的新的签名证书。

I进口证明书到用户设备证书存储？

每服务器证书应该有一个相关的根证明现在用户设备的信任存储。思科Jabber验证服务器提交根证明在信任存储的证书。

请导入根证明到微软视窗证书存储，如果：

- 证书由如果那样不在信任存储已经存在，例如私有CA.，您必须导入私有CA证书到可靠的根证书颁发机构存储的CA签字。
- 证书自已签署的。如果那样，您必须导入自签名证书到企业托拉斯存储。

您能使用所有适当的方法为了进口证明书到微软视窗证书存储，例如：

- 单个请使用证书导入向导为了进口证明书。
- 部署证书给用户用在微软视窗服务器的CertMgr.exe line命令工具。(此选项要求您使用认证管理器工具， CertMgr.exe，不是证书MS管理控制台， CertMgr.msc。)
- 部署证书给有GPO的用户在微软视窗服务器。

注意：关于关于对进口证明书，如何的更多的指导信息参考适当的MS文档。

在证书的服务器标识

作为签署的进程一部分， CA指定在证书的服务器标识。当客户端验证该证书时，检查：

- 委托权限发出证书。
- 提交证书服务器的标识匹配在证书指定的服务器的标识。

注意：公共CA通常需要FQDN作为服务器标识，不是IP地址。

标识符字段

客户端检查服务器证书的这些标识符字段标识匹配：

XMPP证书

- SubjectAltName \ OtherName \ xmppAddr
- SubjectAltName \ OtherName \ srvName
- SubjectAltName \ dnsNames
- 附属的CN

HTTP证书

- SubjectAltName \ dnsNames
- 附属的CN

注意：主题CN字段能包含通配符(*)作为最左边的字符;例如， *.cisco.com。您的CUCM、CUP和Cisco Unity Connection服务器也许不支持通配符证书。(参考的增强Cisco Bug ID CSCta14114)。

防止标识不匹配

当Jabber客户端尝试连接到一个服务器用IP地址时，并且服务器证书识别有FQDN的服务器，客户端不能识别服务器作为委托并且提示用户。因此，如果您的服务器证书识别有FQDN的服务器，您必须指定服务器名作为FQDN在您的服务器的许多地方。

表3列出需要指定服务器名的所有地方，当在证书看起来，它是否是IP地址或FQDN。

表 3

服务器	**位置(设置必须匹配证书)**
思科Jabber客户端	洛金服务器地址(为客户端有所不同，通常在**连接设置下)** **所有节点名(**系统>集群结构)** ****小心**：确保，如果更改此对FQDN，您能通过DNS解决此或服务器留在开始的状态! TFTP服务器(**应用程序>思科Jabber >设置)**
CUP (版本8.x和以下)	主要的和附属Cisco Call Manager Cisco IP电话(CCMCIP) (**应用程序>思科Jabber > CCMCIP配置文件)** 语音邮件主机名(**应用程序>思科Jabber >语音邮件服务器)** 邮件库名称**(应用程序>思科Jabber >邮件库)** 会议主机名(**应用程序>思科Jabber >会议服务器)** (仅会议地点) XMPP域(请参阅**提供XMPP域对客户端**部分)
CUCM IM和在线状态(版本9.x和以上)	**所有节点名**(系统>集群结构**)** ****小心**：确保，如果更改此对FQDN，您能通过DNS解决此或服务器留在开始的状态! TFTP服务器(**应用程序>传统客户端>设置)** 主要的和附属CCMCIP **(应用程序>传统客户端> CCMCIP配置文件)** XMPP域(请参阅**提供XMPP域对客户端**部分)
CUCM (版本8.x和以下)	服务器名(**System > Server)** 服务器名**(System > Server)**
CUCM (版本9.x和以上)	IM和Presence Server (**用户管理>用户设置> UC Service> IM和在线状态)** 语音邮件主机名**(用户管理>用户设置> UC Service>语音邮件)** 邮件库名称**(用户管理>用户设置> UC Service>邮件库)** 会议主机名(**(用户管理>用户设置> UC Service>会议)** (仅会议地点)

Cisco Unity Connection (所有版本) **崔凡吉莱没有需要**

提供XMPP域给客户端

客户端识别与XMPP域的XMPP证书，而不是与FQDN。XMPP证书必须包含XMPP域在标识符字段。

当客户端尝试连接到Presence Server时， Presence Server提供XMPP域给客户端。客户端能然后验证Presence Server的标识XMPP证书。

完成这些步骤为了以保证Presence Server提供XMPP域给客户端的那：

1. 打开您的Presence Server的管理界面， **Cisco Unified CM IM和在线状态管理界面**或者**Cisco Unified Presence管理界面**。
2. 导航对**系统> Security >设置**。
3. 找出**XMPP证书**设置部分。
4. 指定在**域名的**Presence Server域**XMPP服务器对服务器证书主题替代方案Name字段的**。
5. 检查**使用域名XMPP证书主题替代方案名称**复选框。
6. 单击 **Save**。
7. 在您保存此更改后，您必须重新生成在服务器的**CUPxmpp**证书。
8. 重新启动**XCP路由器**为了更改能生效。

警告：XCP路由器影响服务的重新启动。

证书确认当前完成!

相关信息

- 思科Jabber 9.2.5版本注释
- 思科Jabber ：必须服务器证书验证TechNote
- 技术支持和文档 - Cisco Systems