配置证书

证书概述

证书用于保护身份并在 IM and Presence Service 和另一个系统之间建立信任关系。您可以使用证书将 IM and Presence Service 连接到 Cisco Unified Communications Manager、Cisco Jabber 客户端或任何外部服务器。没有证书，就无法知道是否使用了流氓DNS服务器，或者您是否被路由到了另一台服务器。

IM and Presence Service 可以使用的证书主要有两类：

- 自签名证书 — 自签名证书由颁发证书的同一服务器签名。在企业内部，您可以使用自签名证书与另一个内部系统连接，不过有一个前提条件：这些连接都不通过不安全的网络传输。例如，IM and Presence Service 可能会为到 Cisco Unified Communications Manager 的内部连接生成自签名证书。
- CA 签名证书 — 这些是由第三方证书颁发机构 (CA) 签名的证书。它们可以由控制服务器/服务证书有效性的公共 CA（例如 Verisign、Entrust 或 Digicert）或服务器（例如 Windows 2003、Linux、Unix、IOS）签名。CA 签名证书比自签名证书更安全，通常用于 WAN 连接。例如，与另一个企业的联合连接或使用 WAN 连接的群集间对等配置将要求 CA 签名证书与外部系统建立信任关系。

CA 签名证书比自签名证书更安全。通常，自签名证书被认为适用于内部连接，但对于任何 WAN 连接或通过公共 Internet 的连接，您应使用 CA 签名证书。

多服务器证书

IM and Presence Service 还支持某些系统服务的多服务器 SAN 证书。为多服务器证书生成证书签名请求 (CSR) 时，一旦将证书上传到任何群集节点，生成的多服务器证书及其关联的签名证书链将自动分发到所有群集节点。

IM and Presence Service 中的证书类型

在 IM and Presence Service 中，不同的系统组件需要不同类型的证书。下表介绍 IM and Presence Service 上的客户端和服务需要的不同证书。

注释 如果证书名称以 -ECDSA 结尾，证书/密钥类型是椭圆曲线 (EC)。否则，为 RSA。

表 *1:* 证书类型和服务

证书类型	服务	证书信任存储库	多服务器支持	备注
tomcat、 tomcat-ECDSA	Cisco 客户端配置文件代理、 Cisco AXL Web 服务、 Cisco Tomcat	tomcat- trust	是	在 IM and Presence Service 的客户端验证过程中显示给 Cisco Jabber 客户端。 导航 Cisco Unified CM IM and Presence 管理用户界面时显示给 Web 浏览器。 关联的信任存储在使用配置的 LDAP 服务器验证用户凭证时用于验证 IM and Presence Service 建立的连接。
ipsec		ipsec-trust	否	在 IPSec 策略启用时使用。
cup、 cup-ECDSA	Cisco SIP Proxy、 Cisco Presence Engine	cup-trust	否	向 Expressway-C 颁发证书，以获取 SIP 联合用户的 IM and Presence。IM and Presence 代理可用作客户端和服务器。 Presence Engine 会将这些证书用于 Exchange/Office 365 通信以获取日历在线状态。Presence Engine 只能用作客户端。

证书类型	服务	证书信任存储库	多服务器支持	备注
cup-xmpp、 cup-xmpp-ECDSA	Cisco XCP 连接管理器、 Cisco XCP Web 连接管理器、 Cisco XCP 目录服务、 Cisco XCP 路由器服务	cup-xmpp-trust	是	创建 XMPP 会话时显示给 Cisco Jabber 客户端、第三方 XMPP 客户端或基于 CAXL 的应用程序。 关联的信任存储在对第三方 XMPP 客户端执行 LDAP 搜索操作时用于验证 Cisco XCP 目录服务建立的连接。 如果“路由通信类型”设置为“路由器-路由器”，Cisco XCP 路由器服务在 IM and Presence Service 服务器之间建立安全连接时将使用关联的信任存储。
cup-xmpp-s2s、 cup-xmpp-s2s-ECDSA	Cisco XCP XMPP 联合连接管理器	cup-xmpp-trust	是	连接外部联合的 XMPP 系统时显示给 XMPP 域间联合。

证书前提条件

在 Cisco Unified Communications Manager 上配置以下项目：

- 配置 IM and Presence Service 的 SIP 干线安全性配置文件。
- 配置 IM and Presence Service 的 SIP 干线：
  - 将安全性配置文件与 SIP 干线关联。
  - 通过 IM and Presence Service 证书的主题通用名称 (CN) 配置 SIP 干线。

与 Cisco Unified Communications Manager 交换证书

完成这些任务，以与 Cisco Unified Communications Manager 交换证书。

注释 系统会在安装过程中自动处理 Cisco Unified Communications Manager 与 IM and Presence Service 之间的证书交换。但是，如果您需要手动完成证书交换，请完成以下任务。

过程

	命令或操作	目的
步骤 1	将 Cisco Unified Communications Manager 证书导入到 IM and Presence Service，第 4 页	将证书从 Cisco Unified Communications Manager 导入到 IM and Presence Service。

	命令或操作	目的
步骤 2	从 IM and Presence Service 下载证书，第 5 页	从 IM and Presence Service 下载证书。证书必须导入到 Cisco Unified Communications Manager。
步骤 3	将 IM and Presence 证书导入 Cisco Unified Communications Manager，第 5 页	要完成证书交换，请将 IM and Presence Service 证书导入到 Cisco Unified Communications Manager 的 CallManager 信任存储区中。

将 Cisco Unified Communications Manager 证书导入到 IM and Presence Service

此程序用于将证书从 Cisco Unified Communications Manager 导入到 IM and Presence Service。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**系统** > **安全性** > **证书导入工具**。

步骤 2 从**证书信任存储**菜单中选择 **IM and Presence (IM/P) 服务信任**。

步骤 3 输入 Cisco Unified Communications Manager 节点的 IP 地址、主机名或 FQDN。

步骤 4 输入用来与 Cisco Unified Communications Manager 节点通信的端口号。

步骤 5 单击**提交**。

注释 “证书导入工具”完成导入操作后，它会报告是否已经成功连接到 Cisco Unified Communications Manager，以及是否已成功从 Cisco Unified Communications Manager 下载证书。如果“证书导入工具”报告失败，请参阅在线帮助获取建议操作。您也可以通过选择 **Cisco Unified IM and Presence 操作系统管理** > **安全** > **证书管理**来手动导入证书。

注释 根据协商的 TLS 密码，证书导入工具将下载基于 RSA 的证书或基于 ECDSA 的证书。

步骤 6 重新启动 Cisco SIP Proxy 服务：

a) 在 Cisco Unified IM and Presence 功能配置中，选择 IM and Presence 上的**工具** > **控制中心 - 功能服务**。

b) 从**服务器**下拉列表框中选择 IM and Presence Service 群集节点，然后单击**前往**。

c) 选择 **Cisco SIP Proxy** 并单击**重新启动**。

下一步做什么

从 IM and Presence Service 下载证书，第 5 页

从 IM and Presence Service 下载证书

此程序用于从 IM and Presence Service 下载证书。证书必须导入到 Cisco Unified Communications Manager。

过程

步骤 1 在 **Cisco Unified IM and Presence 操作系统管理**中，选择 IM and Presence 上的**安全性** > **证书管理**。

步骤 2 单击**查找**。

步骤 3 选择 `cup.pem` 文件。

注释 `cup-ECDSA.pem` 也是一个可用的选项。

步骤 4 单击**下载**并将文件保存到本地计算机。

提示 忽略 IM and Presence Service 所显示的与访问 cup.csr 文件有关的任何错误；CA（证书机构）无需签署您与 Cisco Unified Communications Manager 交换的证书。

下一步做什么

将 IM and Presence 证书导入 Cisco Unified Communications Manager，第 5 页

将 IM and Presence 证书导入 Cisco Unified Communications Manager

要完成证书交换，请将 IM and Presence Service 证书导入到 Cisco Unified Communications Manager 的 CallManager 信任存储区中。

开始之前

从 IM and Presence Service 下载证书，第 5 页

过程

步骤 1 登录到 Cisco Unified 操作系统管理。

步骤 2 选择**安全性** > **证书管理**

步骤 3 单击**上传证书**。

步骤 4 从“证书名称”菜单中选择 **Callmanager-trust**。

步骤 5 浏览并选择之前从 IM and Presence Service 下载的证书。

步骤 6 单击**上传文件**。

步骤 7 重新启动 Cisco CallManager 服务：

a) 在 Cisco Unified 功能配置中，选择**工具** > **控制中心 - 功能服务**。

b) 从**服务器**下拉列表框中选择一个 Cisco Unified Communications Manager 群集节点并单击**前往**。
c) 选择 **Cisco CallManager** 服务并单击**重新启动**。

在 IM and Presence Service 上安装证书颁发机构 (CA) 根证书链

要在 IM and Presence Service 中使用由第三方证书颁发机构 (CA) 签名的证书，您必须首先在 IM and Presence Service 上安装该 CA 的根证书信任链。

过程

	命令或操作	目的
步骤 1	上传 CA 根证书链，第 6 页	此程序用于将 CA 根证书链从第三方证书颁发机构上传到 IM and Presence Service。
步骤 2	重新启动思科群集间同步代理服务，第 7 页	上传证书后，重新启动思科群集间同步代理服务。
步骤 3	验证 CA 证书已同步到其他群集，第 7 页	确认您的CA证书链已复制到所有对等群集。

上传 CA 根证书链

此程序用于将证书链从签名的证书颁发机构 (CA) 上传到 IM and Presence 数据库发布方节点。链可能包含一连串的多个证书，每个证书签署后续证书：

- 根证书 > 中间 1 证书 > 中间 2 证书

过程

步骤 1 在 IM and Presence 数据库发布方节点上，登录到 Cisco Unified IM and Presence 操作系统管理。
步骤 2 选择**安全性** > **证书管理**。
步骤 3 单击**上传证书/证书链**。
步骤 4 从**证书名称**下拉列表中选择以下选项之一：

- 如果要上传 CA 签名的 tomact 证书，选择 **tomcat-trust**
- 如果要上传 CA 签名的 cup-xmpp 证书或 CA 签名的 cup-xmpp-s2s，选择 **cup-xmpp-trust**

步骤 5 输入签名证书的**说明**。
步骤 6 单击**浏览**找到根证书的文件。
步骤 7 单击**上传文件**。

步骤 8 使用**上传证书/证书链**窗口以相同方式上传每个中间证书。对于每个中间证书，必须输入链中上一个证书的名称。

下一步做什么

重新启动思科群集间同步代理服务，第 7 页

重新启动思科群集间同步代理服务

将根证书和中间证书上传到 IM and Presence 数据库发布方节点后，必须在该节点上重新启动思科群集间同步代理服务。此重新启动可确保 CA 证书立即同步到所有其他群集。

过程

步骤 1 在 Cisco Unified IM and Presence 功能配置中，选择**工具 > 控制中心 - 网络服务**。

步骤 2 从**服务器**下拉列表框中选择要导入证书的 IM and Presence Service 节点，然后单击**前往**。

注释 您可以使用以下命令从命令行界面重新启动思科群集间同步代理服务：`utils service restart Cisco Intercluster Sync Agent`。

步骤 3 选择**思科群集间同步代理**服务并单击**重新启动**。

下一步做什么

验证群集间同步，第 10 页

验证 CA 证书已同步到其他群集

思科群集间同步代理服务重新启动后，必须确保 CA 证书已正确同步到其他群集。在其他每个 IM and Presence 数据库发布方节点上完成以下步骤。

注释 以下程序中的信息也适用于以 `-ECDSA` 结尾的证书。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**诊断 > 系统故障诊断程序**。

步骤 2 在**群集间故障诊断程序**中，查找测试**验证每个启用 TLS 的群集间对等成员是否已成功交换安全证书**并确认该测试已通过。

步骤 3 如果测试显示错误，记下群集间对等成员的 IP 地址；该地址应引用您上传 CA 证书的群集。继续以下步骤以解决该问题。

步骤 4 选择 **Presence** > **群集间**，然后单击与**系统故障诊断程序**页面上标识的群集间对等节点关联的链接。

步骤 5 单击**强制手动同步**。

步骤 6 留出 60 秒时间以便“群集间对等成员状态”面板自动刷新。

步骤 7 验证**证书状态**字段显示“连接是安全的”。

步骤 8 如果证书状态字段没有显示“连接是安全的”，在 IM and Presence 数据库发布方节点上重新启动思科群集间同步代理服务，然后重复步骤 5 至 7。

- 从管理 CLI 运行以下命令以重新启动服务：utils service restart Cisco Intercluster Sync Agent
- 或者，可以从 Cisco Unified IM and Presence 功能配置 GUI 重新启动此服务。

步骤 9 验证**证书状态**现在显示为“连接是安全的”。这意味着群集之间的群集间同步已正确建立，并且您上传的 CA 证书已同步到其他群集。

下一步做什么

将签名证书上传到每个 IM and Presence Service 节点。

将证书上传到 IM and Presence Service

完成这些任务以将证书上传到 IM and Presence Service。您可以上传 CA 签名证书或自签名证书。

开始之前

要使用第三方证书颁发机构 (CA) 签名的 CA 签名证书，您必须先在 IM and Presence Service 上安装 CA 的根证书链。有关详细信息，请参阅在 IM and Presence Service 上安装证书颁发机构 (CA) 根证书链，第 6 页。

过程

	命令或操作	目的
步骤 1	上传证书，第 9 页	将签名的证书上传到 IM and Presence Service。
步骤 2	重新启动 Cisco Tomcat 服务，第 10 页	（仅 Tomcat 证书）。重新启动 Cisco Tomcat 服务。
步骤 3	验证群集间同步，第 10 页	（仅 Tomcat 证书）。对群集内所有受影响的节点重新启动 Cisco Tomcat 服务后，必须验证群集间同步是否正确运行。
步骤 4	在所有节点上重新启动 Cisco XCP 路由器服务，第 11 页	将证书上传到 cup-xmpp 存储区后，在所有群集节点上重新启动 Cisco XMP 路由器。

	命令或操作	目的
步骤 5	重新启动 Cisco XCP XMPP 联合连接管理器服务，第 11 页	（仅 XMPP 联合）。将证书上传到 XMPP 联合的 cup-xmpp 存储区后，重新启动 Cisco XCPXMPP 联合连接管理器服务。
步骤 6	在 XMPP 联合安全证书中启用通配符，第 11 页	（仅 XMPP 联合）。通过 TLS 将证书上传到 XMPP 的 cup-xmpp 存储区后，必须为 XMPP 安全证书启用通配符。必需为群聊执行此操作。

上传证书

此程序用于将证书上传到每个 IM and Presence Service 节点。

注释 思科建议您为群集签名所有必需的 tomcat 证书，然后同时上传这些证书。此过程可缩短恢复群集间通信的时间。

注释 以下程序中的信息也适用于以 `-ECDSA` 结尾的证书。

开始之前

如果证书由 CA 签名，您还必须安装该 CA 的根证书链，否则 CA 签名证书将不受信任。CA 证书正确同步到所有群集后，您可以将适当的签名证书上传到每个 IM and Presence Service 节点。

过程

步骤 1 在 **Cisco Unified IM and Presence 操作系统管理**中选择**安全性** > **证书管理**。

步骤 2 单击**上传证书/证书链**。

步骤 3 选择**证书用途**。例如，**tomcat**。

步骤 4 输入签名证书的说明。

步骤 5 单击**浏览**找到要上传的文件。

步骤 6 单击**上传文件**。

步骤 7 对每个 IM and Presence Service 节点重复操作。

下一步做什么

重新启动 Cisco Tomcat 服务。

重新启动 Cisco Tomcat 服务

将 tomcat 证书上传到每个 IM and Presence Service 节点后，必须在每个节点上重新启动 Cisco Tomcat 服务。

过程

步骤 1 登录到管理 CLI。

步骤 2 运行以下命令：`utils service restart Cisco Tomcat`。

步骤 3 对每个节点重复操作。

下一步做什么

验证群集间同步正常运行。

验证群集间同步

对群集内所有受影响的节点重新启动 Cisco Tomcat 服务后，必须验证群集间同步是否正确运行。在其他群集中的每个 IM and Presence 数据库发布方节点上完成以下步骤。

过程

步骤 1 在 **Cisco Unified CM IM and Presence 管理**中，选择**诊断** > **系统故障诊断程序**。

步骤 2 在**群集间故障诊断程序**中，查找测试**验证每个启用 TLS 的群集间对等成员是否已成功交换安全证书**并确认该测试已通过。

步骤 3 如果测试显示错误，记下群集间对等成员的 IP 地址；该地址应引用您上传 CA 证书的群集。继续以下步骤以解决该问题。

步骤 4 选择 **Presence** > **群集间**，然后单击与“系统故障诊断程序”页面上标识的群集间对等节点关联的链接。

步骤 5 单击**强制手动同步**。

步骤 6 选中**同时重新同步对等成员的 Tomcat 证书**复选框，然后单击**确定**。

步骤 7 留出 60 秒时间以便“群集间对等成员状态”面板自动刷新。

步骤 8 验证**证书状态**字段显示“连接是安全的”。

步骤 9 如果**证书状态**字段没有显示“连接是安全的”，在 IM and Presence 数据库发布方节点上重新启动思科群集间同步代理服务，然后重复步骤 5 至 8。

- 从管理 CLI 运行以下命令以重新启动服务：utils service restart Cisco Intercluster Sync Agent。
- 或者，可以从 Cisco Unified IM and Presence 功能配置 GUI 重新启动此服务。

步骤 10 验证证书状态现在显示为“连接是安全的”。这意味着此群集与证书上传的群集之间的群集间同步现已重新建立。

在所有节点上重新启动 Cisco XCP 路由器服务

将 cup-xmpp 和/或 cup-xmpp-ECDSA 证书上传到每个 IM and Presence Service 节点后，必须在每个节点上重新启动 Cisco XCP 路由器服务。

注释 您也可以从 Cisco Unified IM and Presence 功能配置 GUI 重新启动 Cisco XCP 路由器服务。

过程

步骤 1 登录到管理 CLI。

步骤 2 运行以下命令：utils service restart Cisco XCP Router。

步骤 3 对每个节点重复操作。

重新启动 Cisco XCP XMPP 联合连接管理器服务

将 cup-xmpp-s2s 和/或 cup-xmpp-s2s-ECDSA 证书上传到每个 IM and Presence Service 联合节点后，您必须在每个联合节点上重新启动 Cisco XCP XMPP 联合连接管理器服务。

过程

步骤 1 登录到管理 CLI。

步骤 2 运行以下命令：utils service restart Cisco XCP XMPP Federation Connection Manager。

步骤 3 对每个联合节点重复此过程。

在 XMPP 联合安全证书中启用通配符

要支持 XMPP 联合合作伙伴之间在 TLS 上进行群聊，您必须为 XMPP 安全证书启用通配符。

默认情况下，XMPP 联合安全证书 `cup-xmpp-s2s` 和 `cup-xmpp-s2s-ECDSA` 中包含 IM and Presence Service 部署托管的所有域。这些在证书中作为主题备选名称 (SAN) 条目添加。您必须为同一证书内所有托管的域提供通配符。因此，XMPP 安全证书中必须包含 SAN 条目 “*.example.com”，而不是 SAN 条目 “example.com”。之所以需要通配符，是因为群聊服务器别名是 IM and Presence Service 系统上其中一个托管域的子域。例如：“conference.example.com”。

注释 要查看任意节点上的 cup-xmpp-s2s 或 cup-xmpp-s2s-ECDSA 证书，选择 **Cisco Unified IM and Presence 操作系统管理** > **安全性** > **证书管理**，然后单击 **cup-xmpp-s2s** 或 **cup-xmpp-s2s-ECDSA** 链接。

过程

步骤 1 选择**系统** > **安全设置**。

步骤 2 选中**在 XMPP 联合安全证书中启用通配符**。

步骤 3 单击**保存**。

下一步做什么

您必须在正在运行 Cisco XMPP Federation Connection Manager 服务且已启用 XMPP 联合的群集中所有节点上重新生成 XMPP 联合安全证书。必须在所有 IM and Presence Service 群集上启用此安全设置，以支持基于 TLS 的 XMPP 联合群聊。

生成 CSR

此程序用于生成证书签名请求 (CSR)。您需要将 CSR 提交到第三方 CA，以便他们可以为您提供 CA 签名的证书。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**生成 CSR** 按键。屏幕将弹出**生成证书签署请求**窗口。

步骤 3 从**证书用途**下拉列表中，选择正在生成的证书的类型。

步骤 4 从**分发**下拉列表中，选择 IM and Presence 服务器。对于多服务器证书，选择**多服务器 (SAN)**。

步骤 5 输入**密钥长度**和**哈希算法**。

步骤 6 填写剩余的字段并单击**生成**。

步骤 7 将 CSR 下载到本地计算机：

a) 单击**下载 CSR**。
b) 从**证书目的**下拉列表中选择证书名称。
c) **下载 CSR**

下一步做什么

将 CSR 提交至第三方证书颁发机构，以便他们可以签发 CA 签名的证书。

证书签名请求密钥使用情况扩展

下表显示了 Unified Communications Manager 和 IM and Presence Service CA 证书的证书签名请求 (CSR) 的密钥使用扩展。

表 *2: Cisco Unified Communications Manager CSR* 密钥使用扩展

	多服务器	扩展密钥使用			密钥使用				
		服务器身份验证 **(1.3.6.1.5.5.7.3.1)**	客户端验证 **(1.3.6.1.5.5.7.3.2)**	**IP** 安全端系统 **(1.3.6.1.5.5.7.3.5)**	数字签名	密钥加密	数据加密	密钥证书签名	密钥协议
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		
CAPF（仅发布方）	N	Y			Y	Y		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
TVS	Y	Y	Y		Y	Y	Y		

表 *3: IM and Presence Service CSR* 密钥使用扩展

	多服务器	扩展密钥使用			密钥使用				
		服务器身份验证 **(1.3.6.1.5.5.7.3.1)**	客户端验证 **(1.3.6.1.5.5.7.3.2)**	**IP** 安全端系统 **(1.3.6.1.5.5.7.3.5)**	数字签名	密钥加密	数据加密	密钥证书签名	密钥协议
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		Y
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

生成自签证书

此程序用于生成证书自签名证书。

过程

步骤 1 从 Cisco Unified 操作系统管理中，选择**安全** > **证书管理**。

步骤 2 单击**生成自签名证书**。屏幕将弹出**生成新的自签名证书**窗口。

步骤 3 从**证书用途**下拉列表中，选择正在生成的证书的类型。

步骤 4 从**分发**下拉列表中，输入服务器的名称。

步骤 5 选择适当的**密钥长度**。

步骤 6 从**哈希算法**中选择加密算法。例如，SHA256。

步骤 7 单击**生成**。

从 IM and Presence Service 删除自签名信任证书

为支持相同群集中不同节点配置功能交叉导航，IM and Presence Service 与 Cisco Unified Communications Manager 间的 Cisco Tomcat 服务信任存储区将自动同步。

如果您用CA签名证书替换了初始自签名信任证书，则初始自签名信任证书将保留在服务信任库中。您可以执行此程序以删除 IM and Presence Service 和 Cisco Unified Communications Manager 节点上的自签名证书。

开始之前

重要事项 如果您添加了 CA 签名的证书，请确保等待 30 分钟让思科群集间同步代理服务在给定 IM and Presence Service 节点上执行其定期清理任务。

过程

步骤 1 在 Cisco Unified IM and Presence 操作系统管理中选择**安全性** > **证书管理**。

步骤 2 单击**查找**。

此时将显示**证书列表**。

注释 证书名称由两部分组成，服务名称和证书类型。例如，tomcat-trust 中 tomcat 是服务，而 trust 是证书类型。

您可删除的自签信任证书包括：

- Tomcat 和 Tomcat-ECDSA — tomcat-trust
- Cup-xmpp 和 Cup-xmpp-ECDSA — cup-xmpp-trust
- Cup-xmpp-s2s 和 Cup-xmpp-s2s-ECDSA — cup-xmpp-trust

- Cup 和 Cup-ECDSA — cup-trust
- Ipsec — ipsec-trust

步骤 3 单击指向您希望删除的自签信任证书的链接。

重要事项 确保您已为与服务信任存储区相关联的服务配置 CA 签署的证书。

此时将显示一个新窗口，其中将显示证书的详细信息。

步骤 4 单击**删除**。

注释 仅在您有权限删除该证书时，**删除**按键才会显示。

步骤 5 为群集中和任何跨群集对等机上的各个 IM and Presence Service 节点重复上述程序，以确保跨部署完全删除不需要的自签信任证书。

下一步做什么

如果服务是 Tomcat，则您必须在 Cisco Unified Communications Manager 节点上检查 IM and Presence Service 节点的自签 tomcat 信任证书。请参阅从 Cisco Unified Communications Manager 删除自签 Tomcat 信任证书，第 15 页。

从 Cisco Unified Communications Manager 删除自签 Tomcat 信任证书

Cisco Unified Communications Manager 服务信任存储区中有一个针对群集中各个节点的自签 tomcat 信任证书。这些是您可从 Cisco Unified Communications Manager 节点中删除的唯一证书。

注释 以下程序中的信息也适用于 -EC 证书。

开始之前

确保您已使用 CA 签署证书配置群集的 IM and Presence Service 节点，并等待 30 分钟让证书传播到 Cisco Unified Communications Manager 节点。

过程

步骤 1 在 **Cisco Unified 操作系统管理**中选择**安全性** > **证书管理**。

此时将显示**证书列表**窗口。

步骤 2 要筛选搜索结果，请从下拉列表选择**证书**和**始于**，然后在空字段输入 tomcat 信任。单击**查找**。

证书列表窗口将展开并列出 tomcat 信任证书。

步骤 3 识别名称中包含 IM and Presence Service 节点主机名或 FQDN 的链接。这些是与此服务和 IM and Presence Service 节点相关的自签证书。

步骤 4 单击指向 IM and Presence Service 节点上自签 tomcat 信任证书的链接。

此时将显示一个新窗口，其中将显示 tomcat 信任证书的详细信息。

步骤 5 确保“Issuer Name CN=”与“Subject Name CN=”值相匹配，从而在“证书详细信息”内确认。

步骤 6 如果您确认这是一个自签证书，并确定 CA 签名证书已经传播到 Cisco Unified Communications Manager 节点，请单击**删除**。

注释 **删除**按键仅针对您拥有删除权限的证书显示。

步骤 7 为群集中 IM and Presence Service 节点重复步骤 4、5 和 6。

证书监控任务流程

完成以下任务可将系统配置为自动监控证书状态和到期时间。

- 证书即将到期时通过电子邮件通知您。
- 吊销到期的证书。

过程

	命令或操作	目的
步骤 1	配置证书监控通知，第 16 页	配置自动证书监控。当证书即将到期时，系统会定期检查证书状态并向您发送电子邮件。
步骤 2	配置通过 OCSP 吊销证书，第 17 页	配置OCSP，以便系统自动吊销到期的证书。

配置证书监控通知

为 Unified Communications Manager 或 IM and Presence Service 配置自动证书监控。当证书即将到期时，系统会定期检查证书状态并向您发送电子邮件。

注释 **Cisco 证书到期监控**网络服务必须运行。此服务默认启用，但您也可以在 Cisco Unified 功能配置中手动确认该服务是否在运行，方法是选择**工具** > **控制中心 - 网络服务**，然后验证 **Cisco 证书到期监控服务**状态是否是**正在运行**。

过程

步骤 1 登录到 Cisco Unified 操作系统管理（适用于 Unified Communications Manager 证书监控）或 Cisco Unified IM and Presence 管理（适用于 IM and Presence Service 证书监控）。

步骤 2 选择**安全性** > **证书监控**。

步骤 3 在**通知开始时间**字段中输入一个数值。此值表示证书到期前系统开始通知您即将到期的天数。

步骤 4 在**通知频率**字段中，输入通知的频率。

步骤 5 可选。选中**启用电子邮件通知**复选框以让系统发送证书即将到期的电子邮件通知。

步骤 6 选中**启用 LSC 监控**复选框以在证书状态检查种包含 LSC 证书。

步骤 7 在**电子邮件 ID** 字段中，输入您希望系统将通知发送到的电子邮件地址。您可以输入多个电子邮件地址，用分号分隔。

步骤 8 单击**保存**。

注释 默认情况下，证书监控服务每24小时运行一次。当重新启动证书监控服务时，它将启动服务，然后计算下一个计划，仅在24个小时后运行。即使证书接近七天的到期日期，间隔也不会改变。当证书已经过期或将在一天内过期时，服务会每 1 小时运行一次。

下一步做什么

配置在线证书状态协议 (OCSP)，以便系统自动吊销到期的证书。有关详细信息，请参阅 配置通过 OCSP 吊销证书，第 17 页

配置通过 OCSP 吊销证书

启用在线证书状态协议 (OCSP) 定期检查证书状态并自动吊销到期的证书。

开始之前

确保您的系统具有是 OCSP 检查所需的证书。您可以使用通过 OCSP 响应属性配置的根证书或中间 CA 证书，也可以使用已上传到 tomcat-trust 的指定 OCSP 签名证书。

过程

步骤 1 登录到 Cisco Unified 操作系统管理（适用于 Unified Communications Manager 证书吊销）或 Cisco Unified IM and Presence 管理（适用于 IM and Presence Service 证书吊销）。

步骤 2 选择**安全性** > **证书吊销**。

步骤 3 选中**启用 OCSP** 复选框，然后执行以下任务之一：

- 如果要为 OCSP 检查指定 OCSP 响应器，选择**使用配置的 OCSP URI** 按键并在 **OCSP 配置的 URI** 字段中输入响应器的 URI。
- 如果采用 OCSP 响应器 URI 配置证书，选择**使用来自证书的 OCSP URI** 按键。

步骤 4 选中**启用吊销检查**复选框。

步骤 5 使用吊销检查的间隔时间填写**检查间隔**字段。

步骤 6 单击**保存**。

步骤 7 可选。如果您有 CTI、IPsec 或 LDAP 链接，除上述步骤之外，还必须完成以下操作，以便为这些长期连接启用 OCSP 吊销支持：

a) 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

b) 在**证书撤消和过期**下，将**证书有效性检查**参数设置为**真**。

c) 配置**有效性检查频率**参数的值。

注释 **证书吊销**窗口中**启用吊销检查**参数的时间间隔值优先于**有效性检查频率**企业参数的值。

d) 单击**保存**。