UCCX解决方案证书管理指南

目录

简介

本文档介绍如何配置Cisco Unified Contact Center Express(UCCX)以使用自签名和签名证书。

先决条件

要求

在您继续本文档中介绍的配置步骤之前，请确保您有权访问这些应用程序的“操作系统(OS)管理”页面：

- UCCX
- SocialMiner
- MediaSense

管理员还应有权访问代理和Supervisor客户端PC上的证书存储区。

FQDN、DNS和域

UCCX配置中的所有服务器都必须安装域名系统(DNS)服务器和域名。此外，还需要代理、主管和管理员通过完全限定域名(FQDN)访问UCCX配置应用。

UCCX版本10.0+要求在安装时填充域名和DNS服务器。UCCX版本10.0+安装程序生成的证书包含FQDN（视情况而定）。在升级到UCCX版本10.0+之前，将DNS服务器和域添加到UCCX集群。

如果域更改或首次填充，应重新生成证书。将域名添加到服务器配置后，先重新生成所有Tomcat证书，然后再将它们安装在其他应用程序上、客户端浏览器中或生成用于签名的证书签名请求(CSR)。

使用的组件

本文档中描述的信息基于以下硬件和软件组件：

- UCCX Web服务
- UCCX通知服务
- UCCX平台Tomcat
- 思科Finesse Tomcat
- 思科统一情报中心(CUIC)Tomcat
- SocialMiner Tomcat
- MediaSense Web服务

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

随着同驻的Finesse和CUIC的推出、UCCX与SocialMiner在电子邮件和聊天方面的集成，以及使用MediaSense通过Finesse记录、了解和安装证书，对证书问题进行故障排除的能力现在变得至关重要。

本文档介绍在涵盖以下内容的UCCX配置环境中使用自签名证书和签名证书：

- UCCX通知服务
- UCCX Web服务
- UCCX脚本
- 并存Finesse
- 共存CUIC（实时数据和历史报告）
- MediaSense（基于Finesse的录制和标记）
- SocialMiner（聊天）

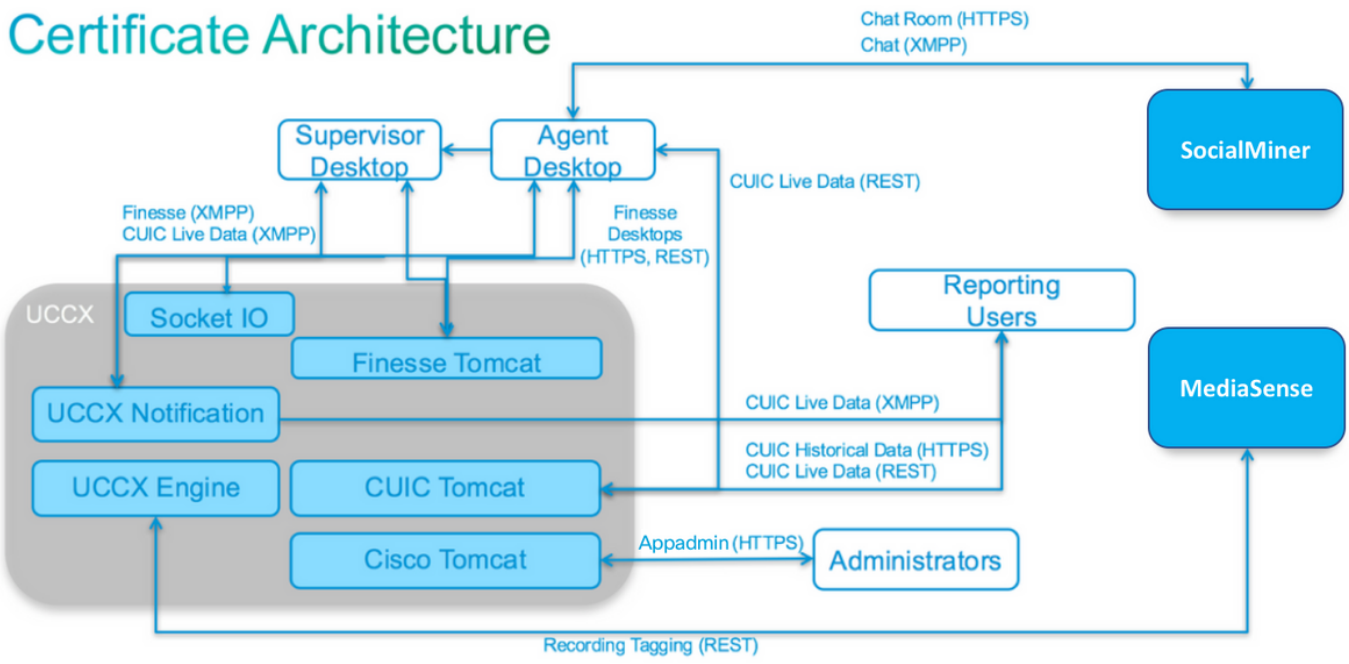
在UCCX配置中，必须在应用（服务器）以及代理和主管客户端桌面上安装证书（签名或自签名）。

在Unified Communications Operating System(UCOS)10.5中，添加了多服务器证书，以便可以为集群生成单个CSR，而不必为集群中的每个节点签署单个证书。UCCX、MediaSense和SocialMiner明确不支持此类型的证书。

配置

本节介绍如何配置UCCX以使用自签名和签名证书。

配置图



UCCX解决方案架构自UCCX 11.0起有效。HTTPS通信图。

已签名证书

对于UCCX配置，推荐的证书管理方法是利用已签名的证书。这些证书可以由内部证书颁发机构(CA)或已知的第三方CA签署。

在Mozilla Firefox和Internet Explorer等主要浏览器中，默认情况下会安装已知第三方CA的根证书。默认情况下，由这些CA签名的UCCX配置应用的证书是受信任的，因为它们的证书链以浏览器中已安装的根证书结尾。

也可以通过组策略或其他当前配置在客户端浏览器中预安装内部CA的根证书。

您可以根据客户端浏览器中CA的根证书的可用性和预安装情况，选择是由已知第三方CA还是由内部CA签署UCCX配置应用证书。

安装签名的Tomcat应用证书

为UCCX发布服务器和订用服务器、SocialMiner以及MediaSense发布服务器和订用服务器管理应用程序的每个节点完成以下步骤：

1. 导航到**OS Administration**页面，然后选择**Security > Certificate Management**。
2. 点击**生成 CSR**。
3. 从**Certificate List**下拉列表中，选择**tomcat**作为证书名称，然后单击**Generate CSR**。
4. 导航到**安全>证书管理**，然后选择**下载CSR**。
5. 在弹出窗口中，从下拉列表中选择**tomcat**，然后单击**Download CSR**。

如前所述，将新CSR发送到第三方CA或用内部CA签署。此过程应生成以下签名证书：

- CA的根证书
- UCCX发布服务器应用证书
- UCCX用户应用证书
- SocialMiner应用证书
- MediaSense发布器应用证书
- MediaSense用户应用证书

注意：将CSR中的**Distribution**字段保留为服务器的FQDN。

注意：从11.6版本开始，UCCX支持“多服务器(SAN)”证书。但是，SAN应仅包括UCCX节点1和节点2。其他服务器（如SocialMiner）不应包含在UCCX的SAN中。

注意：UCCX仅支持1024和2048位的证书密钥长度。

在每个应用服务器上完成以下步骤，以便将根证书和应用证书上传到节点：

注意：如果上传发布服务器（UCCX或MediaSense）上的根证书和中间证书，应自动将其复制到订阅服务器。如果所有应用证书都通过同一证书链进行签名，则无需将根或中间证书上传到配置中的其他非发布方服务器。

1. 导航到**OS Administration**页面，然后选择**Security > Certificate Management**。
2. 单击**Upload Certificate**。
3. 上传根证书并选择**tomcat-trust**作为证书类型。
4. 单击 **Upload File**。
5. 单击**Upload Certificate**。
6. 上传应用证书并选择**tomcat**作为证书类型。
7. 单击 **Upload File**。 **注意：**如果从属CA签署证书，请上传从属CA的根证书作为*tomcat-trust*证书而不是根证书。如果颁发中间证书，请将此证书除了应用证书外上传到*tomcat-trust*存储。
8. 完成后，重新启动这些应用程序： Cisco MediaSense发布服务器和订用服务器思科SocialMinerCisco UCCX发布服务器和订用服务器

注意：当您使用UCCX、MediaSense和SocialMiner 11.5及更高版本时，有一个名为tomcat-ECDSA的新证书。将签名的tomcat-ECDSA证书上传到服务器时，将应用证书作为tomcat-ECDSA证书（而不是tomcat证书）上传。有关ECDSA的详细信息，请参阅相关信息部分，以获取了解和配置ECDSA证书的链接。

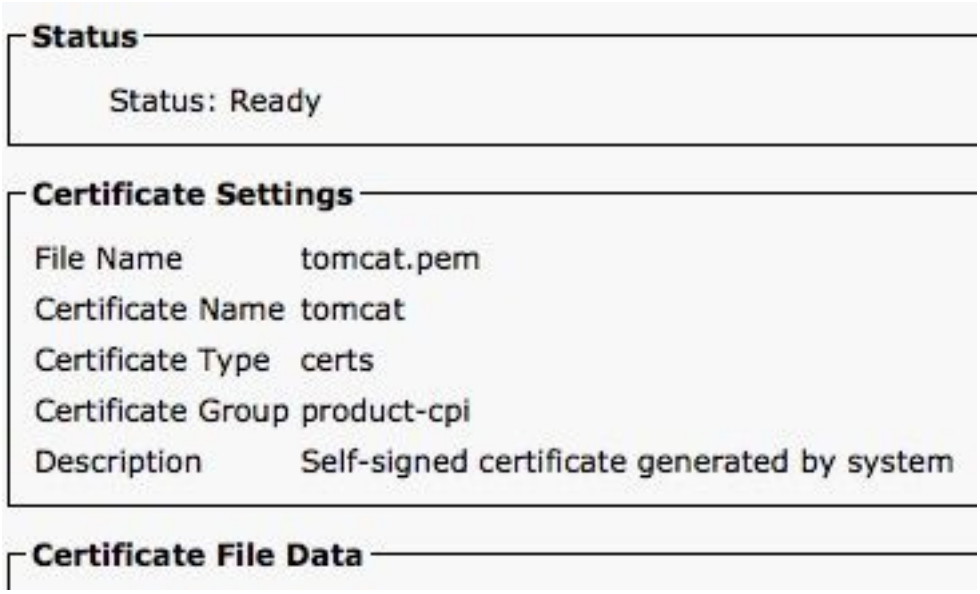
自签名证书

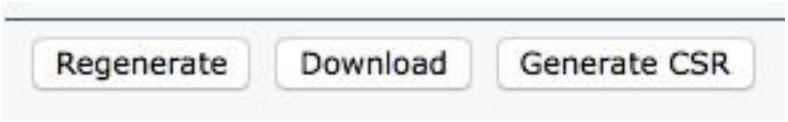
在外围服务器上安装

UCCX配置中使用的所有证书都预先安装在配置应用程序上，并且是自签名证书。这些自签名证书在提供给客户端浏览器或其他配置应用程序时并不隐式信任。虽然建议对UCCX配置中的所有证书进行签名，但您可以使用预安装的自签名证书。

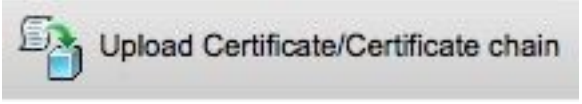
对于每个应用关系，您必须下载相应的证书并将其上传到应用。要获取和上传证书，请完成以下步骤：

1. 访问应用**OS Administration**页，然后选择**Security > Certificate Management**。
2. 点击适当的证**书.pem**文件并选择**下载**:





3. 要在相应应用上上传证书，请导航到**OS Administration**页面并选择**Security > Certificate Management**。
4. 单击**Upload Certificate / Certificate Chain:**



5. 完成后，重新启动这些服务器：

Cisco MediaSense发布服务器和订用服务器思科SocialMinerCisco UCCX发布服务器和订用服

务器

要在客户端计算机上安装自签名证书，请使用组策略或软件包管理器，或在每个代理PC的浏览器中单独安装它们。

对于Internet Explorer，将客户端自签名证书安装到**受信任的根证书颁发机构**存储中。

对于Mozilla Firefox，请完成以下步骤：

1. 导航到**工具>选项**。
2. 单击 **Advanced 选项卡。**
3. 单击**View Certificates**。
4. 导航到**Servers**选项卡。
5. 单击**Add Exception**。

重新生成自签名证书

如果自签名证书过期，需要重新生成这些证书，并重新执行**在外围服务器上安装**中的配置步骤。

1. 访问应用 **操作系统管理** 页面并选择 **安全>证书管理**.
2. 点击适当的证书并选择**Regenerate**。
3. 必须重新启动其证书重新生成的服务器。
4. 对于每个应用关系，您必须下载适当的证书，并按照安装外围设备服务器中的配置步骤**将其上传到应用。**

集成和客户端配置

UCCX到MediaSense

UCCX使用MediaSense Web服务REST应用编程接口(API)有两个用途：

- 订用在Cisco Unified Communications Manager(CUCM)上调用的新录音通知。
- 使用座席和联系服务队列(CSQ)信息标记UCCX座席的记录。

UCCX使用MediaSense管理节点上的REST API。任何MediaSense集群中最多有两台。UCCX不通过REST API连接到MediaSense扩展节点。两个UCCX节点必须使用MediaSense REST API，因此要在两个UCCX节点上安装两个MediaSense Tomcat证书。

将MediaSense服务器的签名或自签名证书链上传到UCCX *tomcat-trust密钥*库。

MediaSense到Finesse

MediaSense使用Finesse Web服务REST API对Finesse上的MediaSense搜索和播放小工具的代理进行身份验证。

在Finesse XML布局上为搜索和播放小工具配置的MediaSense服务器必须使用Finesse REST API，因此请在这个MediaSense节点上安装两个UCCX Tomcat证书。

将UCCX服务器的签名或自签名证书链上传到MediaSense *tomcat-trust密钥*库。

UCCX到SocialMiner

UCCX使用SocialMiner REST和通知API来管理电子邮件联系人和配置。两个UCCX节点必须使用SocialMiner REST API并由SocialMiner通知服务通知，因此要在两个UCCX节点上安装SocialMiner Tomcat证书。

将SocialMiner服务器的签名或自签名证书链上传到UCCX *tomcat-trust密钥*库。

UCCX AppAdmin客户端证书

UCCX AppAdmin客户端证书用于管理UCCX系统。要为UCCX管理员安装UCCX AppAdmin证书，请在客户端PC上，导航到每个UCCX节点的**https://<UCCX FQDN>/appadmin/main**，然后通过浏览器安装证书。

UCCX平台客户端证书

UCCX Web服务用于将聊天联系人传送到客户端浏览器。要安装UCCX代理和主管的UCCX平台证书，请在客户端PC上，导航到每个UCCX节点的**https://<UCCX FQDN>/appadmin/main**，然后通过浏览器安装证书。

通知服务客户端证书

Finesse、UCCX和CUIC使用CCX通知服务通过可扩展消息传送和在线状态协议(XMPP)将实时信息发送到客户端桌面。 用于实时Finesse通信以及CUIC Live Data。

要在使用Live Data的代理和主管或报告用户的PC上安装通知服务客户端证书，请针对每个UCCX节点导航至**https://<UCCX FQDN>:7443/** ，然后通过浏览器安装证书。

Finesse客户端证书

Finesse客户端证书由Finesse桌面用于连接到Finesse Tomcat实例，以便在桌面和共存Finesse服务器之间进行REST API通信。

要安装代理和主管的Finesse证书，请在客户端PC上，为每个UCCX节点导航到**https://<UCCX FQDN>:8445/**，并通过浏览器提示安装证书。

要为Finesse管理员安装Finesse证书，请在客户端PC上，导航到每个UCCX节点的**https://<UCCX FQDN>:8445/cfadmin**，并通过浏览器提示符安装证书。

SocialMiner客户端证书

客户端计算机上必须安装SocialMiner Tomcat证书。座席接受聊天请求后，“聊天”小工具将重定向到代表聊天室的URL。此聊天室由SocialMiner服务器托管，包含客户或聊天联系人。

要在浏览器中安装SocialMiner证书，请在客户端PC上导航到**https://<SocialMiner FQDN>/**，然后通过浏览器提示安装证书。

CUIC客户端证书

CUIC Tomcat证书应安装在客户端计算机上，供在CUIC网页或桌面小工具内使用CUIC Web界面进行历史报告或实时数据报告的座席、主管和报告用户使用。

要在浏览器中安装CUIC Tomcat证书，请在客户端PC上导航至**https://<UCCX FQDN>:8444/**，然后通过浏览器提示符安装证书。

CUIC实时数据证书（自11.x起）

CUIC对后端Live数据使用套接字IO服务。对于使用Live Data的CUIC Web界面或在Finesse中使用Live Data小工具的代理、主管和报告用户，应在客户端计算机上安装此证书。

要在浏览器中安装套接字IO证书，请在客户端PC上导航到**https://<UCCX FQDN>:12015/**，然后通过浏览器提示安装证书。

可从脚本访问的第三方应用程序

如果UCCX脚本旨在访问第三方服务器上的安全位置(例如，*Get URL Document*步骤到HTTPS URL或*Make Rest Call*到HTTPS REST URL)，请将第三方服务的签名或自签名证书链上传到UCCX *tomcat-trust* keystore。要获取此证书，请访问UCCX **OS Administration**页面并选择**Upload Certificate**。

配置UCCX引擎是为了在第三方应用通过脚本步骤访问安全位置时，在第三方应用提供这些证书时，搜索平台Tomcat密钥库中的第三方证书链。

必须将整个证书链上传到平台Tomcat密钥库(可通过**OS Administration**页面访问)，因为Tomcat密钥库默认不包含根证书。

完成这些操作后，请重新启动Cisco UCCX引擎。

验证

为了验证所有证书是否都已正确安装，您可以测试本节中介绍的功能。如果未出现证书错误且所有功能均正常运行，则证书安装正确。

- 配置Finesse，使其通过工作流自动记录代理。座席处理呼叫后，请使用MediaSense搜索和播放应用程序查找呼叫。验证呼叫中是否已将座席、CSQ和组标记附加到MediaSense中的录制元数据。
- 通过SocialMiner配置座席Web聊天。通过Web表单插入聊天联系人。确认座席收到接受聊天联系人的标语，并确认接受聊天联系人后，聊天表单加载正确，座席可以接收和发送聊天消息。
- 尝试通过Finesse登录代理。确认未显示证书警告，网页未提示将证书安装到浏览器中。确认座席可以正确更改状态，并且向UCCX发出的新呼叫已正确呈现给座席。
- 在座席和Supervisor Finesse桌面布局中配置实时数据小工具后，请登录座席、主管和报告用户。验证实时数据小工具已正确加载，初始数据已填充到小工具中，并且当基础数据更改时数据刷新。
- 尝试从浏览器连接到两个UCCX节点上的AppAdmin URL。验证当提示登录页时是否未显示证书警告。

故障排除

问题 — 用户ID/密码无效

UCCX Finesse代理无法登录，错误为“**用户ID/密码无效**”。

原因

Unified CCX抛出异常“SSLHandshakeException”，且无法与Unified CM建立连接。

解决方案

- 验证Unified CM Tomcat证书未过期。
- 确保您在Unified CM中上传的任何证书都具有以下任一标记为关键的分机：
  X509v3密钥用法(OID - 2.5.29.15)
  X509v3基本限制(OID - 2.5.29.19)
  如果将任何其他扩展标记为重要，由于Unified CM证书验证失败，Unified CCX和Unified CM之间的通信将失败。

问题 — CSR SAN和证书SAN不匹配

CA签名证书的上传显示错误“CSR SAN和证书SAN不匹配”。

原因

CA可能已在证书使用者备用名称(SAN)字段中添加另一个父域。默认情况下，CSR具有以下SAN:

```
SubjectAltName [
  example.com(dNSName)
  hostname.example.com(dNSName)
]
```

CA可能会返回一个证书，其中另一个SAN已添加到证书中：www.hostname.example.com。在这种情况下，证书将具有额外的SAN:

```
SubjectAltName [
  example.com(dNSName)
  hostname.example.com(dNSName)

  www.hostname.example.com(dNSName)
]
```

这会导致SAN不匹配错误。

解决方案

在UCCX“生成证书签名请求”(Generate Certificate Signing Request)页面的“使用者备用名称(SANs)”(Subject Alternate Name(SANs))部分，生成父域字段为空的CSR。这样，不会使用SAN属性生成CSR，CA可以格式化SAN，并且当您向UCCX上传证书时，不会出现SAN属性不匹配的情况。请注意，“父域”字段默认为UCCX服务器的域，因此在配置CSR的设置时必须明确删除该值。

问题- NET::ERR_CERT_COMMON_NAME_INVALID

当您访问任何UCCX、MediaSense或SocialMiner网页时，会收到错误消息。

“您的连接不是专用的。

攻击者可能试图从<Server_FQDN>窃取您的信息（例如，密码、消息或信用卡）。
NET::ERR_CERT_COMMON_NAME_INVALID

此服务器无法证明它是<Server_FQDN>;其安全证书来自[missing_subjectAltName]。这可能是由配置错误或攻击者拦截您的连接造成的。”

原因

Chrome版本58引入了一项新的安全功能，它报告如果网站的公共名称(CN)未作为SAN包含则其证书不安全。

解决方案

- 您可以导航到**Advanced > Proceed to <Server_FQDN>(unsafe)**以继续访问站点并接受证书错误。
- 使用CA签名证书可以完全避免此错误。生成CSR时，服务器的FQDN包含为SAN。CA可以签署CSR，在将已签名的证书上传回服务器后，服务器的证书将在SAN字段中具有FQDN，因此不会显示错误。

更多信息

请参见Chrome 58的“弃用和删除”中的“删除对证书中公用名匹配的支持”部分。

证书缺陷

- Cisco Bug ID CSCvb46250 - UCCX:Tomcat ECDSA证书对Finesse实时数据的影响
- Cisco Bug ID CSCvb58580 — 无法使用RSA CA签名的tomcat和tomcat-ECDSA登录SocialMiner
- 思科漏洞ID CSCvd56174 - UCCX:由于SSLHandshakeException，Finesse代理登录失败
- Cisco Bug ID CSCuv89545 - Finesse Logjam漏洞

相关信息

- **了解UCCX解决方案中的ECDSA证书**
- **SHA 256支持UCCX**
- **UCCX签名和自签名证书配置示例**
- **技术支持和文档 - Cisco Systems**

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）。