UCCX解决方案证书管理指南

目录

简介

本文描述如何配置Cisco Unified Contact Center Express (UCCX)为使用自已签署和签名证书。

先决条件

要求

在您继续进行在本文描述的配置步骤前，请保证您访问这些应用程序的操作系统(OS)管理页面：

- UCCX
- SocialMiner
- MediaSense

管理员应该也访问在代理程序和Supervisor客户端PC机的证书存储

FQDN、DNS和域

切记在UCCX配置的所有服务器安装有域名系统(DNS)服务器和域名。也切记代理程序、Supervisor和管理员通过完全合格的域名(FQDN)访问UCCX配置应用程序。

UCCX版本10.0+要求域名和DNS服务器在安装之上被填充。是由UCCX版本10.0+安装程序生成的认证包含FQDN，如适当。在您升级到UCCX版本10.0+前，请添加DNS服务器和一个域到UCCX簇。

如果域第一次更改或被填充，应该重新生成认证。在您添加域名到服务器配置后，请重新生成所有Tomcat认证，在您安装他们在其他应用程序上，在客户端浏览器上，或者在证书签名请求(CSR)前的生成签字的。

使用的组件

在本文描述的信息根据这些硬件与软件硬件元件：

- UCCX网站服务
- UCCX通知服务
- UCCX平台Tomcat
- Cisco精良Tomcat
- Cisco Unified智力中心(CUIC) Tomcat
- SocialMiner Tomcat
- MediaSense网站服务

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

使用coresident精良和CUIC的简介，在UCCX和SocialMiner之间的集成电子邮件和聊天的和使用MediaSense为了记录，请通过精良了解，并且安装认证，能力排除认证问题故障当前是极其重要的。

本文在包括的UCCX配置环境里描述使用自已签署和签名证书：

- UCCX通知服务
- UCCX网站服务
- UCCX脚本
- coresident精良
- coresident CUIC (实际数据和历史报告)
- MediaSense (基于精良的记录和标记)
- SocialMiner (聊天)

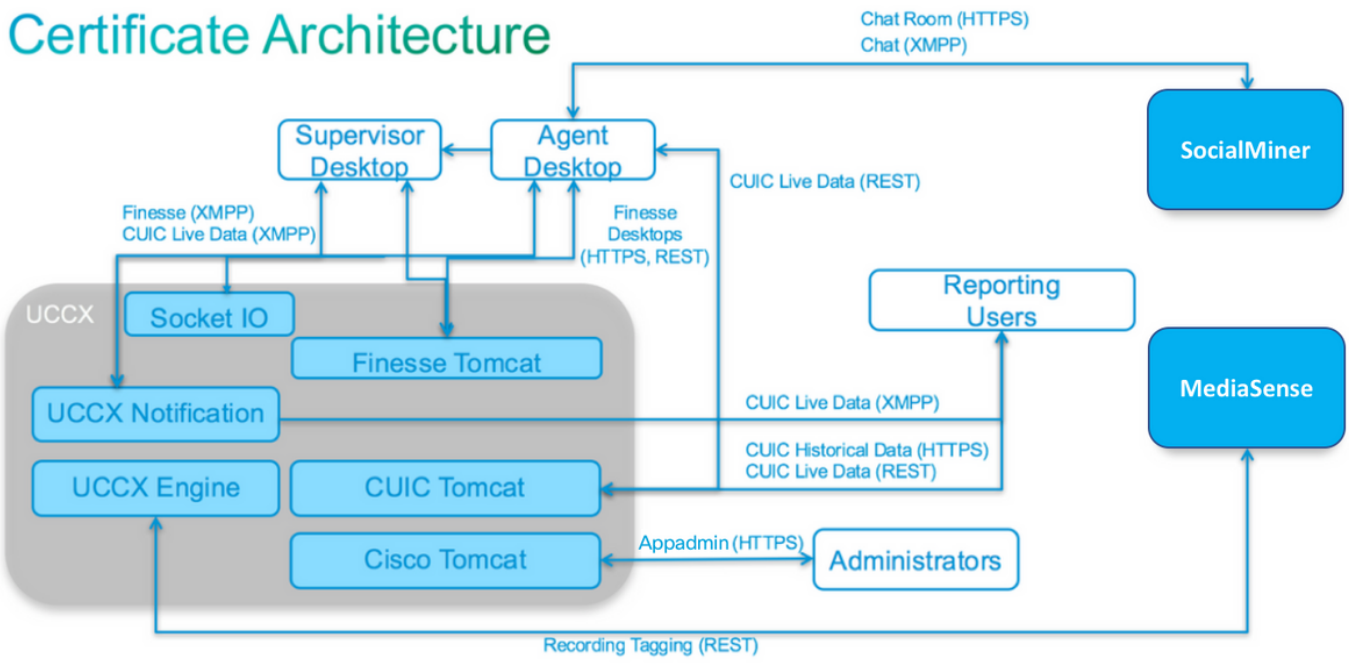
必须在两个应用程序(服务器)在UCCX配置上，以及代理程序和Supervisor客户端桌面上安装认证，签字或自已签署。

在统一通信操作系统(UCOS) 10.5中，多服务器的认证被添加了，以便单个CSR能为簇生成而不是必须签署每个节点的一个单个认证在簇。此种认证为UCCX、MediaSense和SocialMiner明确地是不支持的。

配置

此部分描述如何配置UCCX为使用自已签署和签名证书。

配置图表



UCCX解决方案体系结构有效自UCCX 11.0。HTTPS通信图表。

签名证书

证书管理推荐的方法UCCX配置的将有效利用签名证书。这些认证可能由一内部Certificate Authority (CA)或著名的第三方CA签字。

默认情况下在主要浏览器，例如Mozilla Firefox和Internet Explorer，安装著名的第三方CA的根证明。UCCX由这些CA签字的配置应用程序的默认情况下认证委托，作为他们的证书链末端在浏览器上已经安装的根证明。

内部CA的根证明在客户端浏览器也许也被事先装配通过组策略或其他当前配置。

您是否能选择安排UCCX配置应用程序认证签字由著名的第三方CA或由根据根证明的可用性和装配前准备工作的内部CA CA的在客户端浏览器。

安装签字的Tomcat应用程序认证

完成UCCX发布服务器和用户、SocialMiner和MediaSense发布服务器和用户管理应用程序的每个节点的这些步骤：

1. 连接对**OS管理页面**并且选择**安全> Certificate Management**。
2. 点击**生成CSR**。
3. 从**认证列表**下拉列表，请选择**Tomcat**作为验证名称并且点击**生成CSR**。
4. 连接对**安全> Certificate Management**并且选择**下载CSR**。
5. 从弹出窗口，从下拉列表请选择**Tomcat**并且点击**下载CSR**。

发送新的CSR到第三方CA或签署它与内部CA，如前所述。此进程应该生产这些签名证书：

- CA的根证明
- UCCX发布人应用程序认证
- UCCX订户应用程序认证
- SocialMiner应用程序认证
- MediaSense发布人应用程序认证
- MediaSense订户应用程序认证

Note:留下**分配**字段在CSR作为服务器的FQDN。请勿更改它到“多服务器(SAN)”，因为多服务器的认证没有用UCCX、MediaSense或者SocialMiner支持。

Note:UCCX只支持认证密钥长度1024和2048位。

完成在每个应用服务器的这些步骤为了加载根证明和应用程序认证到节点：

Note:如果加载在发布人的根和半成品认证(UCCX或MediaSense)，应该自动地复制对订户。如果所有应用程序认证通过同一条证书链，签字没有需要加载在其他上的根或半成品认证，在配置的非发布人服务器。

1. 连接对**OS管理页面**并且选择**安全> Certificate Management**。
2. 点击**加载认证**。
3. 加载根证明并且选择Tomcat**信任**作为证书类型。
4. 单击 **Upload File**。
5. 点击**加载认证**。
6. 加载应用程序认证并且选择**Tomcat**作为证书类型。
7. 单击 **Upload File**。 **Note**:如果辅助CA签署认证，请加载辅助CA的根证明作为Tomcat*信任*认证而不是根证明。如果发出中间证书，除应用程序认证之外，请加载此认证到Tomcat*信任*存储。
8. 一旦完整，请重新启动这些应用程序： Cisco MediaSense发布服务器和用户Cisco SocialMinerCisco UCCX发布服务器和用户

Note:当您使用UCCX、MediaSense和SocialMiner 11.5及以后时，有称为Tomcat ECDSA的

新证书。当您加载一个签字的Tomcat ECDSA认证到服务器，请加载应用程序认证作为Tomcat ECDSA认证--不是Tomcat认证。欲知关于ECDSA的详情，请是指链路的相关信息部分了解和配置ECDSA认证。

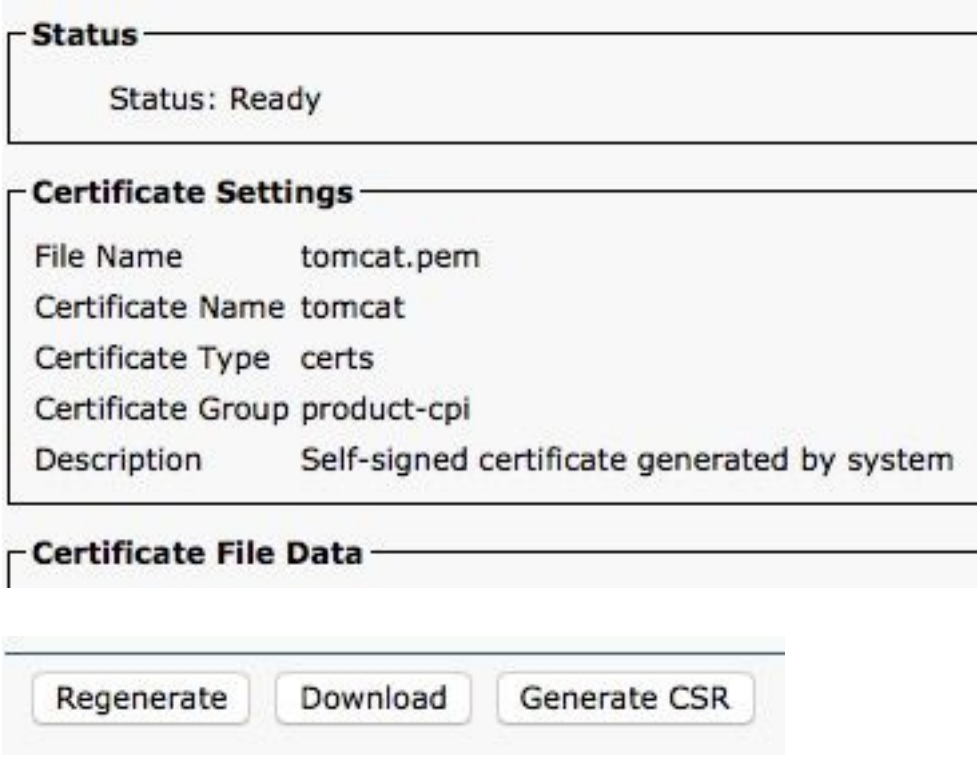
自签名证书

安装在周边服务器上

在UCCX配置使用的所有认证在配置应用程序来事先装配并且是自己签署的。这些自签名证书没有隐含地委托，当提交对客户端浏览器或另一个配置应用程序。虽然推荐签署在UCCX配置的所有认证，您能使用被事先装配的自签名证书。

对于每个应用程序关系，您必须下载适当的认证和加载它到应用程序。完成这些步骤为了获得并上载认证：

1. 访问应用程序**OS管理页面**并且选择**安全> Certificate Management**。
2. 点击适当的认证**.pem**文件并且选择**下载**：



3. 为了加载在适当应用程序的一个认证，请连接对**OS管理页面**并且选择**安全> Certificate Management**。
4. 点击**加载认证/证书链：**

5. 一旦完整，请重新启动这些服务器：

Cisco MediaSense发布服务器和用户Cisco SocialMinerCisco UCCX发布服务器和用户

为了在客户端机器上安装自签名证书，请使用一个组策略或程序包管理器或者在每个代理程序PC浏览器上单个安装他们。

对于Internet Explorer，请安装客户端自签名证书到**可靠的根证书颁发机构**存储。

对于Mozilla Firefox，请完成这些步骤：

1. 连接对**Tools>选项**。
2. 单击 **Advanced** 选项卡。
3. 点击**视图认证**。
4. 连接对**服务器**选项。
5. 点击**添加例外**。

重新生成自签名证书

在自签名证书超时的案件，他们将需要被重新生成，并且从**安装的**配置步骤**在周边服务器上将**需要再被执行。

1. 访问应用程序**OS管理页面**并且选择**安全> Certificate Management**。
2. 点击适当的认证并且选择**重新生成**。
3. 认证被重新生成的服务器必须重新启动。
4. 对于每个应用程序关系，您必须下载适当的认证和加载它到应用程序在配置步骤后从**安装在周边服务器上。**

集成和客户端配置

UCCX对MediaSense

UCCX为两个目的消耗MediaSense网站服务其余Application Programming Interface (API) ：

- 为了预订在Cisco Unified Communications Manager新的记录的通知(CUCM)被调用。
- 为了用代理程序和Contact Service Queue (CSQ)信息标记UCCX代理程序记录。

UCCX消耗MediaSense管理节点的基于API。有最多两在所有MediaSense簇。UCCX不通过其余API连接对MediaSense扩展节点。两个UCCX节点必须消耗MediaSense其余API，因此在两个上UCCX节点请安装两个MediaSense Tomcat认证。

加载MediaSense服务器的签字的或自签名证书一系列到UCCX Tomcat*信任*keystore。

MediaSense对精良

MediaSense消耗精良网站服务其余API为了验证MediaSense搜索和作用小配件的代理程序在精良。

在搜索和作用小配件的精良XML布局配置的MediaSense服务器必须消耗精良其余API，因此在该MediaSense节点上请安装两个UCCX Tomcat认证。

加载UCCX服务器的签字的或自签名证书一系列到MediaSense Tomcat*信任*keystore。

UCCX对SocialMiner

UCCX消耗SocialMiner其余和通知API为了管理电子邮件联系和配置。必须消耗SocialMiner其余API和由SocialMiner通知服务通知两个UCCX节点，因此在两个上UCCX节点请安装SocialMiner Tomcat认证。

加载SocialMiner服务器的签字的或自签名证书一系列到UCCX Tomcat*信任*keystore。

UCCX Appadmin客户端证书

UCCX Appadmin客户端证书使用UCCX系统的管理。为了在客户端PC上安装UCCX管理员的UCCX Appadmin认证，请连接对**https://**其中每一个的**<UCCX FQDN>/appadmin/main** UCCX节点并且通过浏览器安装认证。

UCCX平台客户端证书

UCCX网站服务使用聊天联系发运对客户端浏览器的。为了在客户端PC上安装UCCX代理程序和Supervisor的UCCX平台认证，请连接对**https://**其中每一个的**<UCCX FQDN>/appadmin/main** UCCX节点并且通过浏览器安装认证。

通知服务客户端证书

精良、UCCX和CUIC用于CCX通知服务为了发送实时信息到客户端桌面通过可扩展传讯和存在协议(XMPP)。这使用实时精良通信以及CUIC居住数据。

为了在代理程序和Supervisor或者报告用户的PC上安装通知服务客户端证书使用实际数据，连接对**https://**其中每一个的**<UCCX FQDN>:7443/** UCCX节点并且通过浏览器安装认证。

精良客户端证书

精良桌面用于精良客户端证书为了连接到精良Tomcat实例为桌面和coresident精良服务器之间的其余API通信。

为了在客户端PC上安装代理程序和Supervisor的精良认证，连接到**https://**其中每一个的**<UCCX FQDN>:8445/** UCCX节点和通过浏览器提示安装认证。

为了在客户端PC上安装精良管理员的精良认证，连接到**https://**其中每一个的**<UCCX FQDN>:8445/cfadmin** UCCX节点和通过浏览器提示安装认证。

SocialMiner客户端证书

必须在客户端机器上安装SocialMiner Tomcat认证。一旦代理程序接受聊天请求，表示聊天室的聊天小配件重定向对URL。此聊天室由SocialMiner服务器主机并且包含用户或聊天联系。

为了在浏览器上安装SocialMiner认证，在客户端PC上，连接到**https:// <SocialMiner FQDN>/**和通过浏览器提示安装认证。

CUIC客户端证书

应该在代理程序的客户端机器上安装CUIC Tomcat认证， Supervisor，并且报告使用CUIC Web接口历史报告或居住数据的用户报告在CUIC网页内或在桌面的小配件内。

为了在浏览器上安装CUIC Tomcat认证，在客户端PC上，连接到**https:// <UCCX FQDN>:8444/**和通过浏览器提示安装认证。

CUIC居住数据认证(从11.x)

CUIC使用插槽IO服务后端实际数据。应该在代理程序的客户端机器上安装此认证， Supervisor和使用CUIC Web接口Live数据或使用在精良内的实际数据小配件的报告用户。

为了在浏览器上安装插槽IO认证，在客户端PC上，连接到**https:// <UCCX FQDN>:12015/**和通过浏览器提示安装认证。

第三方应用可访问从脚本

如果UCCX脚本设计为了访问第三方服务器的一个安全的位置(例如，请*有URL文件步*骤HTTPS URL或请*做其余呼叫*对HTTPS其余URL)，请加载第三方服务的签字的或自签名证书一系列到UCCX Tomcat*信任*keystore。为了获取此认证，请访问UCCX **OS管理页面**并且选择**加载认证**。

配置UCCX引擎为了搜索平台Tomcat keystore第三方证书链，当提交与这些认证由第三方应用，当他们通过脚本步骤时访问安全的位置。

默认情况下，因为Tomcat keystore不包含根证明必须加载整个证书链到平台Tomcat keystore，可访问通过**OS管理页面**。

在您完成这些动作后，请重新启动Cisco UCCX引擎。

验证

为了验证正确地安装所有认证，您能测试在此部分描述的功能。如果认证错误没出现，并且所有功能正常运行，正确地安装认证。

- 配置精良，以便通过工作流自动地记录一个代理程序。在呼叫由代理程序后处理，请使用MediaSense搜索和作用应用程序为了查找呼叫。验证呼叫有代理程序、一CSQ和小组标记附加对记录中间数据在MediaSense。
- 通过SocialMiner配置代理程序Web聊天。通过Web表注入聊天联系。验证代理程序接收标语接受聊天联系并且验证聊天联系一次被接受，适当聊天表负荷，并且代理程序能收到和传送聊天信息。
- 尝试通过精良登录代理程序。验证认证警告没出现，并且网页不提示输入认证的安装到浏览器。验证代理程序能适当地更改状态和一次新的呼叫到UCCX正确地被提交到代理程序。
- 在您配置在代理程序和Supervisor精良桌面布局后的实际数据小配件，请登录代理程序、Supervisor和一个报告的用户。验证实际数据小配件适当地装载，初始数据被填充到小配件，并且数据刷新，当基础数据更改。
- 尝试从浏览器连接到在两个UCCX节点的Appadmin URL。验证认证警告没出现，当提示与登录页。

故障排除

问题-无效用户id/密码

UCCX精良代理程序无法登录与错误“**无效用户id/密码**”。

原因

统一的CCX投掷例外“SSLHandshakeException “并且不能建立与统一的CM的连接。

解决方案

- 验证统一的CM Tomcat认证没有超时。
- 保证您在统一的CM加载的所有认证有作为重要被标记的任何一个这些扩展名：
  X509v3密钥用法(OID - 2.5.29.15)
  X509v3基本约束(OID - 2.5.29.19)
  如果标记任何其他扩展名如重要，通信失效在统一的CCX和统一的CM之间由于统一的CM证书验证的故障。

问题- CSR SAN和认证SAN不配比

CA签名证书的加载显示错误“CSR SAN和认证SAN不匹配”。

原因

CA也许已经添加了在证书主题代替名字(SAN)字段的另一个父域。默认情况下， CSR将有这些SAN：

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

CA也许返回与另一个SAN的一个认证被添加到认证：www.hostname.example.com。认证在这种情况下将有额外SAN ：

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

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

这导致SAN不匹配错误。

解决方案

在UCCX ‘请生成证书签名请求’页的‘附属的替代名称(SAN)’部分，生成与一个空父域字段的CSR。这样CSR没有生成与SAN属性， CA能格式化SAN，并且将没有SAN属性不匹配，当您加载认证到UCCX。注意父域字段默认为UCCX服务器的域，因此必须明确地取消值，当配置时CSR的设置。

问题- NET ： ：ERR_CERT_COMMON_NAME_INVALID

当您访问所有UCCX、MediaSense或者SocialMiner网页时，您收到错误消息。

“您的连接不是专用的。

攻击者也许设法窃取您的从<Server_FQDN>的信息(例如，密码、消息或者信用卡)。NET ：：ERR_CERT_COMMON_NAME_INVALID

此服务器不可能证明，它是<Server_FQDN>;其安全证书是从[missing_subjectAltName]。这可能由拦截您的连接的配置错误或攻击者造成”。

原因

镀铬物版本58介绍了报道的一个新的安全功能网站的认证不安全，如果其共同名称(CN)也没有包括作为SAN。

解决方案

- 您能连接到**先进>继续对<Server_FQDN> (不安全)**为了继续到站点和接受验证错误。
- 您能一共避免错误与CA签名证书。当您生成CSR时，服务器的FQDN包括作为SAN。CA能签署CSR，并且，在您加载签名证书回到服务器后，服务器证明将有在SAN字段的FQDN，以便不会提交错误。

更多信息

请参阅部分“取消配比在认证的公用名称的技术支持”在反对和删除在镀铬物58。

认证缺陷

- Cisco Bug ID CSCvb46250 - UCCX ：Tomcat ECDSA对精良实际数据的认证影响
- Cisco Bug ID CSCvb58580 -无法登录到与Tomcat和Tomcat ECDSA的SocialMiner由RSA CA签了字
- Cisco Bug ID CSCvd56174 - UCCX ：精良代理程序登录故障由于SSLHandshakeException
- Cisco Bug ID CSCuv89545 -精良木材堵塞弱点

相关信息

- 了解在UCCX解决方案的ECDSA认证
- UCCX的SHA 256技术支持
- UCCX签字的和自签名证书配置示例
- 技术支持和文档 - Cisco Systems