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)为使用自己签署的和签名证书。

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

要求所有服务器在UCCX配置里安装与域名系统(DNS)服务器和域名。也要求代理程序、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服务器在安装之上填充。由UCCX版本10.0+安装程序生成的证书包含FQDN，如适当。在您升级对UCCX版本10.0+前，请添加DNS服务器和一个域到UCCX集群。

如果域第一次更改或填充，应该重新生成证书。在您添加域名到服务器配置后，请重新生成所有Tomcat证书，在您安装他们在其他申请，在客户端浏览器，或者在证书签名请求(CSR)前的生成对签字。

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
- 思科精良Tomcat
- Cisco Unified智能中心(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的介绍，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，并且安装证书，能力排除故障证书问题当前是极其重要的。

本文描述使用在包括的UCCX配置环境的自己签署的和签名证书：

- UCCX通知服务
- UCCX网站服务
- UCCX脚本

- coresident精良
- 共存CUIC (实际数据和历史报告)
- MediaSense (基于精良的录音和标记)
- SocialMiner (聊天)

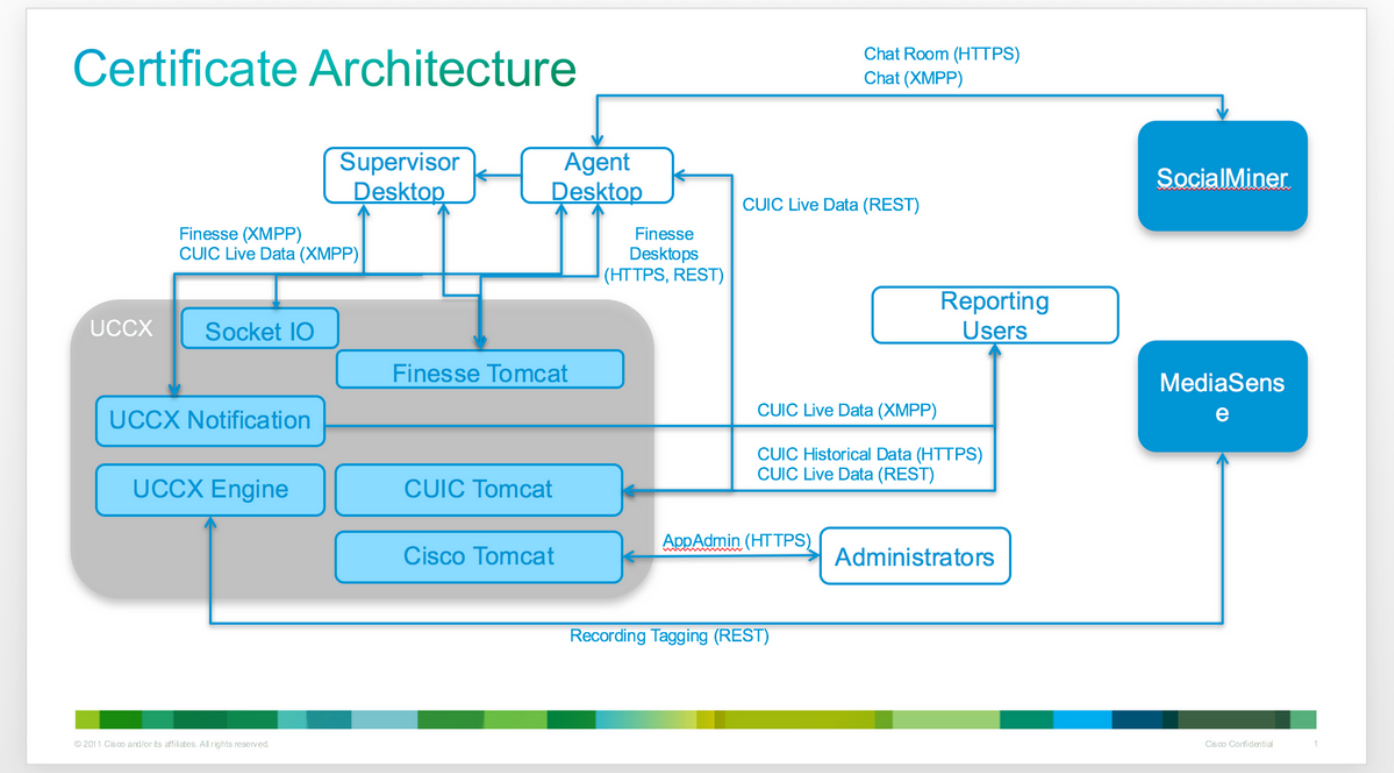
在两应用程序(服务器)在UCCX配置里，以及代理程序和Supervisor客户端桌面必须安装证书，签字或自己签署的。

在统一通信操作系统(UCOS) 10.5中，多服务器的证书被添加了，以便单个CSR能为集群生成而不是必须签署每个节点的一单个证书在集群。此种证书为UCCX、MediaSense和SocialMiner明确地是不支持的。

配置

此部分描述如何配置UCCX为使用自己签署的和签名证书。

配置图表



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。这些证书可能由一内部Certificate Authority (CA)或著名的第三方CA签字。

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

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配置应用程序证书签字由著名的第三方CA或由根据根证明的可用性和安装

前的内部CA CA的在客户端浏览器。

安装签字的Tomcat应用程序证书

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. 导航对**OS管理页面**并且选择**安全> Certificate Management**。
2. 单击**生成CSR**。
3. 从**证书列表**下拉列表，请选择**Tomcat**作为验证名称并且单击**生成CSR**。
4. 导航对**安全> Certificate Management**并且选择**下载CSR**。
5. 从弹出窗口，请从下拉列表选择**Tomcat**并且点击**下载CSR**。

发送新的CSR对第三方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发行商应用程序证书
- UCCX用户应用程序证书
- SocialMiner应用程序证书
- MediaSense发行商应用程序证书
- MediaSense用户应用程序证书

注意：留下CSR的**分配**字段作为服务器的FQDN。请勿更改它对“多服务器(SAN)”，因为多服务器的证书不支持与UCCX、MediaSense或者SocialMiner。

完成在每个应用服务器的这些步骤为了上传根证明和应用程序证书到节点：

注意：如果上传根和中间证书在发行商(UCCX或MediaSense)，应该自动地复制对用户。如果所有应用程序证书通过同一条证书链，签字没有需要上传根或中间证书在其他上，非发行商服务器在配置里。

1. 导航对**OS管理页面**并且选择**安全> Certificate Management**。
2. 点击**加载证书**。
3. 上传根证明并且选择Tomcat**托拉斯**作为证书类型。
4. 单击 **Upload File**。
5. 点击**加载证书**。
6. 上传应用程序证书并且选择**Tomcat**作为证书类型。
7. 单击 **Upload File**。 **注意**：如果辅助CA签署证书，请上传辅助CA的根证明作为Tomcat*托拉斯*证书而不是根证明。如果中间证书发出，除应用程序证书之外，请上传此证书到Tomcat*托拉斯*存储。
8. 一旦完整，请重新启动这些应用程序： 思科MediaSense发布服务器和用户思科SocialMiner思科UCCX发布服务器和用户

注意：当您使用UCCX、MediaSense和SocialMiner 11.5及以后时，有呼叫Tomcat ECDSA的新证书。当您上传一签字的Tomcat ECDSA证书到服务器时，请上传应用程序证书作为Tomcat ECDSA证书--不是Tomcat证书。欲知关于ECDSA的详情，参考链路的相关信息部分能了解和配置ECDSA证书。

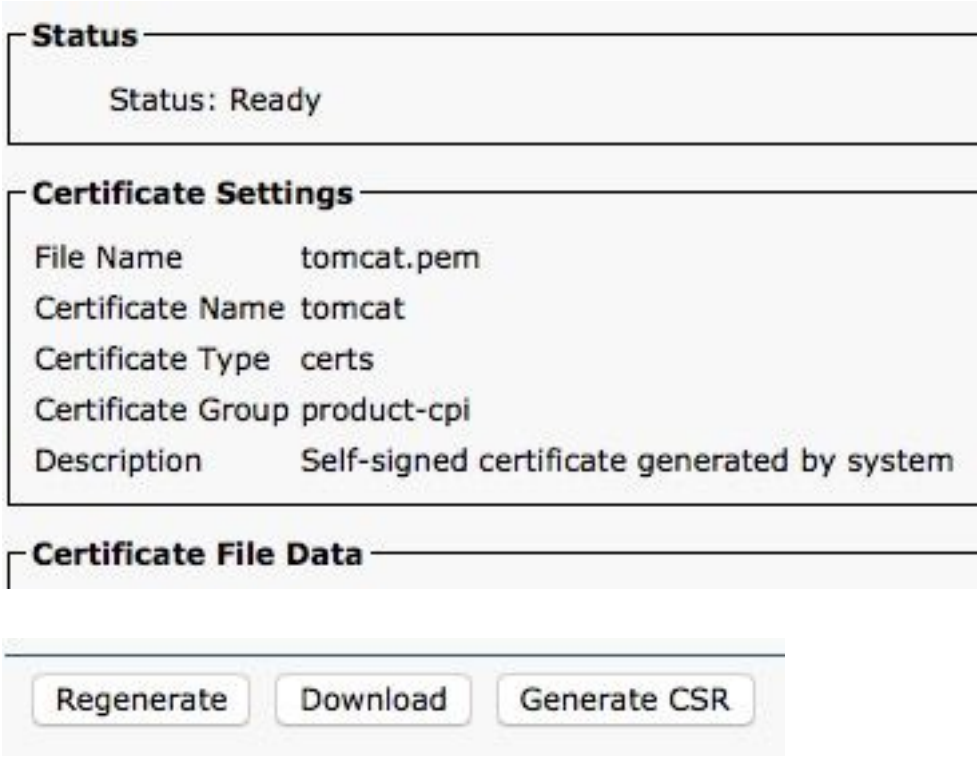
自签名证书

在UCCX配置里使用的所有证书在配置应用程序来事先装配并且自己签署的。这些自签名证书不是隐含地委托，当提交对客户端浏览器或另一配置应用程序。虽然在UCCX配置里推荐签署所有证书，您能使用被事先装配的自签名证书。

对于每应用程序关系，您必须下载适当的证书和上传它到应用程序。完成这些步骤为了获得并上载证书：

1. 访问应用程序**OS管理页面**并且选择**安全> Certificate Management**。

2. 点击适当的证书**.pem**文件并且选择**下载**：



3. 为了上传在适当应用程序的一证书，请导航对**OS管理页面**并且选择**安全> Certificate Management**。
4. 点击**加载证书/证书链：**

5. 一旦完整，请重新启动这些服务器：

思科MediaSense发布服务器和用户思科SocialMiner思科UCCX发布服务器和用户

为了安装在客户端机器的自签名证书，使用组策略或包管理器或者单个安装他们在每个代理程序PC浏览器。

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. 导航对**Tools>选项**。
2. 单击 **Advanced** 选项卡。

3. 点击**视图证书**。
4. 导航对**服务器**选项卡。
5. 单击**添加例外**。

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) ：

- 为了订阅到在Cisco Unified Communications Manager新的录音的通知(CUCM)被调用。
- 为了用代理程序和Contact Service Queue (CSQ)信息标记UCCX代理程序录音。

UCCX消耗在MediaSense管理节点的其余API。有最多两在所有MediaSense集群。UCCX不通过其余API连接对MediaSense扩展节点。两UCCX节点必须消耗MediaSense其余API，因此请安装在两个的两MediaSense Tomcat证书UCCX节点。

上传MediaSense服务器的签字的或自签名证书一系列对UCCX Tomcat*托拉斯*keystore。

MediaSense对精良

MediaSense消耗精良网站服务其余API为了验证MediaSense搜索的代理程序和播放在精良的小配件。

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，因此请安装在该MediaSense节点的两UCCX Tomcat证书。

上传UCCX服务器的签字的或自签名证书一系列对MediaSense Tomcat*托拉斯*keystore。

UCCX对SocialMiner

UCCX消耗SocialMiner其余和通知API为了管理电子邮件联系方式和配置。必须消耗SocialMiner其余API和由SocialMiner通知服务通知两个UCCX节点，因此请安装在两个的SocialMiner Tomcat证书UCCX节点。

上传SocialMiner服务器的签字的或自签名证书一系列对UCCX Tomcat*托拉斯*keystore。

UCCX Appadmin客户端证书

UCCX Appadmin客户端证书使用UCCX系统的管理。为了安装UCCX管理员的UCCX Appadmin证书，客户端PC的，请导航对**https://**其中每一的**<UCCX FQDN>/appadmin/main** UCCX节点并且通过浏览器安装证书。

UCCX平台客户端证书

UCCX网站服务使用聊天联系方式交付对客户端浏览器的。为了安装UCCX代理程序和Supervisor的UCCX平台证书，在客户端PC，请导航对**https://**其中每一的**<UCCX FQDN>/appadmin/main** UCCX节点并且通过浏览器安装证书。

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消息传送和在线状态协议(XMPP)。这使用实时精良通信以及CUIC居住数据。

为了安装在使用Live数据，导航对**https://**其中每一的**<UCCX FQDN>:7443/** UCCX节点并且通过浏览器安装证书代理程序和Supervisor或者报告用户的PC的通知服务客户端证书。

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实例为其余桌面和coresident精良服务器之间的API通信。

为了安装代理程序和Supervisor的精良证书，在客户端PC，请导航对**https://**其中每一的**<UCCX FQDN>:8445/** UCCX节点并且通过浏览器提示符安装证书。

为了安装精良管理员的精良证书，客户端PC的，请导航对**https://**其中每一的**<UCCX FQDN>:8445/cfadmin** UCCX节点并且通过浏览器提示符安装证书。

SocialMiner客户端证书

在客户端机器必须安装SocialMiner Tomcat证书。一旦代理程序接受聊天请求，代表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客户或聊天联系方式。

为了安装在浏览器的SocialMiner证书，在客户端PC，请导航对**https:// <SocialMiner FQDN>/**并且通过浏览器提示符安装证书。

CUIC客户端证书

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

为了安装在浏览器的CUIC Tomcat证书，在客户端PC，请导航对**https:// <UCCX FQDN>:8444/**并且通过浏览器提示符安装证书。

CUIC居住数据证书(从11.x)

CUIC使用Socket IO服务后端处理Live数据。在代理程序的客户端机器应该安装此证书， Supervisor和使用CUIC Web接口Live数据或使用在精良内的Live数据小配件的报告用户。

为了安装在浏览器的Socket IO证书，在客户端PC，请导航对**https:// <UCCX FQDN>:12015/**并且通过浏览器提示符安装证书。

第三方应用可访问从脚本

如果UCCX脚本设计为了访问一个第三方服务器的一个安全位置(例如，请*有URL文档步*骤HTTPS URL或请*做其余呼叫*对HTTPS其余URL)，请上传第三方服务的签字的或自签名证书一系列对UCCX Tomcat*托拉斯*keystore。为了获取此证书，访问UCCX **OS管理页面**和选择**加载证书**。

UCCX引擎配置为了搜索平台Tomcat keystore第三方证书链，当提交与这些证书由第三方应用，当他们通过脚本步骤时访问安全位置。

默认情况下，因为Tomcat keystore不包含根证明必须上传整个证书链到平台Tomcat keystore，可

访问通过**OS管理页面**。

在您完成这些操作后，请重新启动思科UCCX引擎。

验证

为了验证所有证书正确地安装，您能测试在此部分描述的功能。如果证书错误没出现，并且所有功能正常运行，证书正确地安装。

- 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搜索并且播放应用程序为了查找呼叫。验证呼叫有代理程序、一CSQ和团队标记附加对录音元数据在MediaSense。
- 通过SocialMiner配置代理程序Web聊天。通过Web表注入聊天联系方式。验证代理程序接收标语接受聊天联系方式并且验证聊天联系方式一次接受，适当聊天表负载，并且代理程序能收到和传送聊天信息。
- 尝试通过精良登陆代理程序。验证证书警告没出现，并且网页不提示输入证书的安装到浏览器。验证代理程序能适当地更改状态，并且一新的呼叫到UCCX里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Live数据小配件，请登陆代理程序、Supervisor和一个报告的用户。验证Live数据小配件适当地装载，初始数据填充到小配件，并且数据刷新，当基础数据更改。
- 尝试从浏览器连接到在两UCCX节点的Appadmin URL。验证证书警告没出现，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

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

解决方案

- 验证Unified CM Tomcat证书没有超时。
- 保证您在Unified CM上传的所有证书有作为关键被标记的任何一个这些扩展：
  X509v3密钥用法(OID - 2.5.29.15)
  X509v3基本限制条件(OID - 2.5.29.19)
  如果标记其他扩展如关键，通信失效在Unified CCX和Unified CM之间由于Unified CM证书验证的失败。

问题- CSR SAN和证书SAN不配比

CA签名证书的加载显示错误“CSR SAN和证书SAN不匹配”。

原因

CA也许已经添加了另一个父域在证书主题代替名称(SAN)字段。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的一证书被添加到证书：www.hostname.example.com。证书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，当您上传证书对UCCX。注意父域字段默认为UCCX服务器的域，因此必须明确地删除值，当CSR的设置配置时。

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。

“您的连接不私有。

攻击者也许尝试窃取您的从<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误配置或攻击者造成”。

原因

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

解决方案

- 您能导航到**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，在您上传签名证书回到服务器后，服务器证明在SAN字段将有FQDN，以便不会提交错误。

更多信息

请参阅部分“取消匹配在证书的公用名称的支持”在反对和删除在镀铬物58。

证书缺陷

- Cisco Bug ID CSCvb46250 - UCCX ：Tomcat ECDSA在精良Live数据的证书影响
- Cisco Bug ID CSCvb58580 -无法登陆到与两Tomcat的SocialMiner和Tomcat ECDSA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 -精良木材堵塞漏洞

相关信息

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