统一的CCE解决方案：程序获得并上载第三方CA证书(版本11.x)

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[背景信息](#)
[Configure](#)
[步骤1.生成并且下载认证署名请求(CSR)。](#)
[步骤2.获得根，中间(如果applicableStep 5.和从认证机关的应用程序认证。](#)
[步骤3.对服务器的加载证书。](#)
[精良服务器](#)
[CUIC服务器(假设半成品证书当前在证书链)](#)
[实际数据服务器](#)
[实际数据服务器认证依靠](#)
[Verify](#)
[Troubleshoot](#)

Introduction

本文打算详细解释包括的步骤从第三方供应商获得和安装认证机构(CA)认证，生成建立精良，Cisco Unified智力中心(CUIC)之间的HTTPS连接和居住数据(LD)服务器。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Cisco Unified Contact Center Enterprise (UCCE)
- Cisco Live数据(LD)
- Cisco Unified智力中心(CUIC)
- Cisco精良
- 被认可的CA

Components Used

用于本文的信息根据UCCE解决方案11.0(1)版本。

The information in this document was created from the devices in a specific lab environment.All of

the devices used in this document started with a cleared (default) configuration.如果您的网络实际，请切记您了解所有步骤的潜在影响。

背景信息

为了使用HTTPS精良之间的安全通信， CUIC和实际数据服务器，安全证书设置是需要的。默认情况下这些服务器提供使用的自已签署的certifcates或用户能获得和安装Certificate Authority (CA)签名的证书。这些CA certs从一个第三方供应商获得类似VeriSign， Thawte， GeoTrust或可以被生产internaly。

Configure

设置HTTPS通信的认证在精良， CUIC和实际数据服务器要求这些步骤：

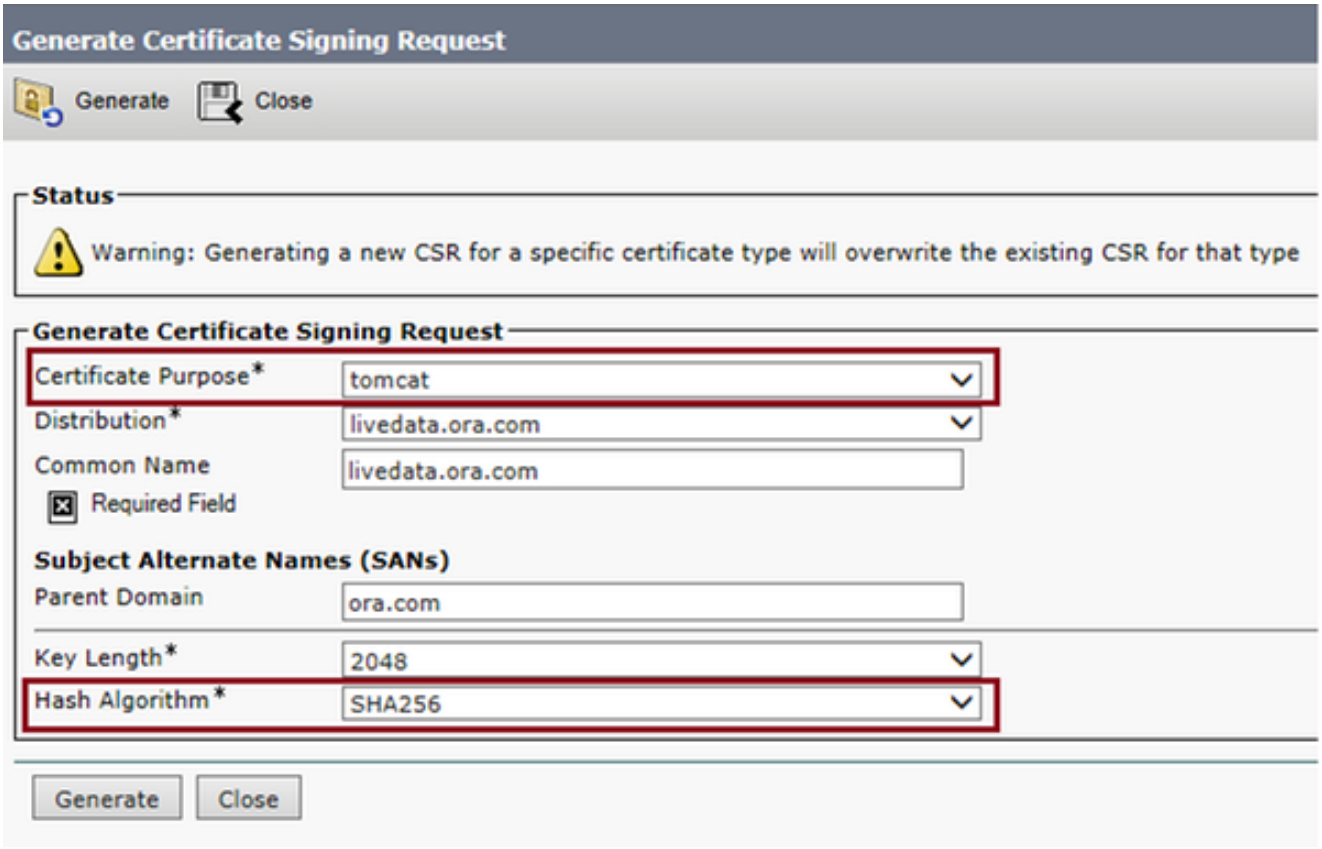
1. 生成并且下载认证署名请求(CSR)。
2. 获得根、中间(如果适用)使用CSR，和从认证机关的应用程序认证。
3. 加载证书到服务器。

步骤1.生成并且下载认证署名请求(CSR)。

1. 为生成和下载CSR描述的这里步骤是同样为精良， CUIC，并且实际数据切断。

2. 打开**Cisco Unified通信操作系统的管理页面**使用陈述的URL并且签到与在安装过程中被创建的OS管理帐户
   https://FQDN:8443/cmplatform

3. 生成认证署名请求(CSR)如镜像所显示， ：

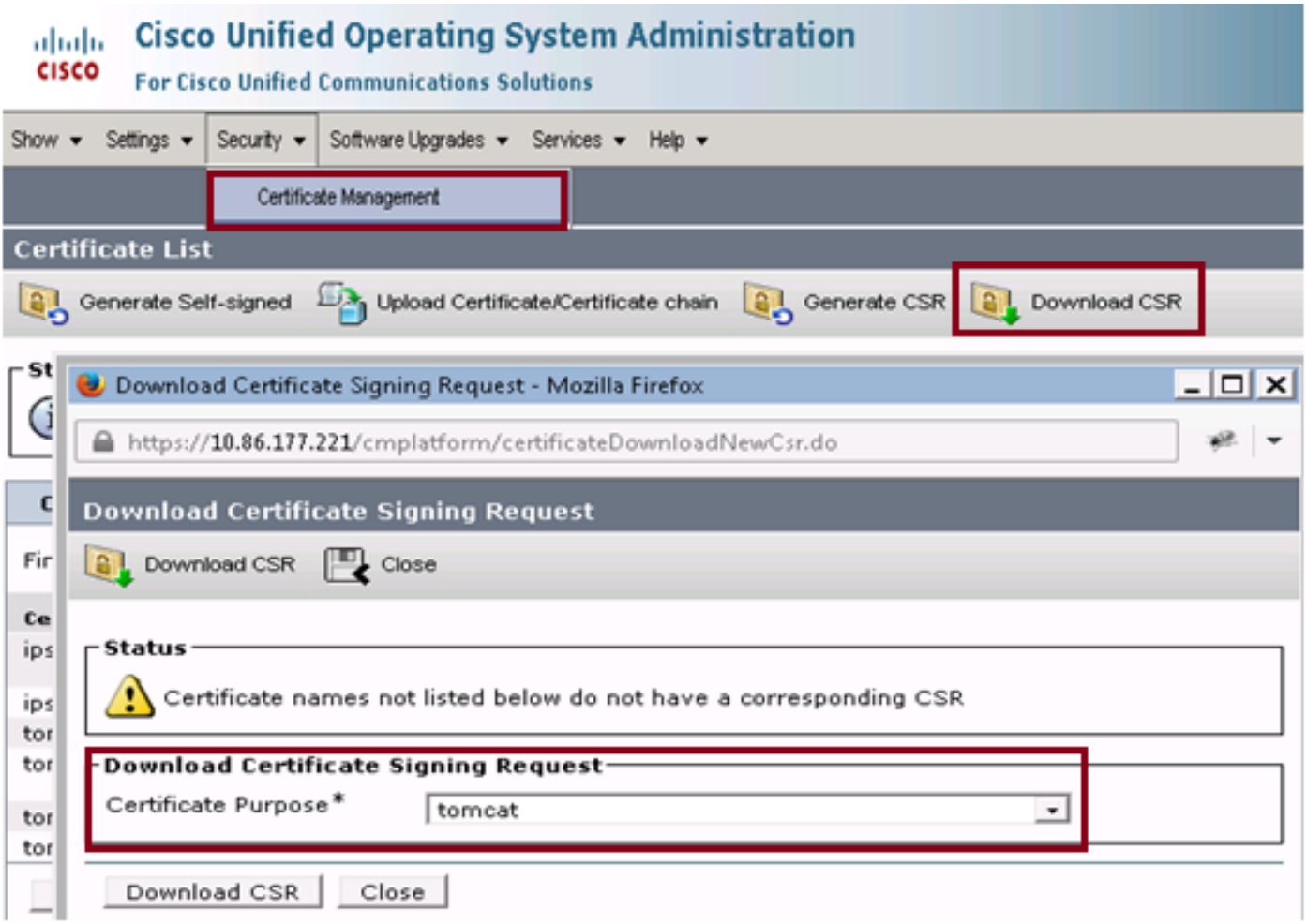


步骤1.连接对**安全> Certificate Management >生成CSR。Step 2.**从认证目的名字下拉列表，请选择Tomcat。步骤3.选择depeding在商业需要的Hash算法和密钥长度。

-密钥长度：2048 \ Hash算法：SHA256是推荐的

步骤4.点击**生成CSR。Note**: 如果事务要求附属的替代名称(SANs)父母Domain字段请充满域名然后请注意在本文的问题地址[“SANs第三方签名的证书的问题在精良”。]

4. 下载认证署名请求(CSR)如镜像所显示， ：



步骤1.连接对**安全> Certificate Management >下载CSR**。
Step 2.从验证名称下拉列表，请选择Tomcat。
步骤3.点击**下载CSR**。

Note:

> **Note**:执行在附属服务器的上述的步骤使用URL **https://FQDN:8443/cmplatform**得到认证机关的CSR

步骤2.获得根，中间(如果applicableStep 5.和从认证机关的应用程序认证。

1. 提供主要的和附属服务器认证署名请求(CSR)信息给第三方Certifcate权限类似VeriSign、Thawte， GeoTrust等。

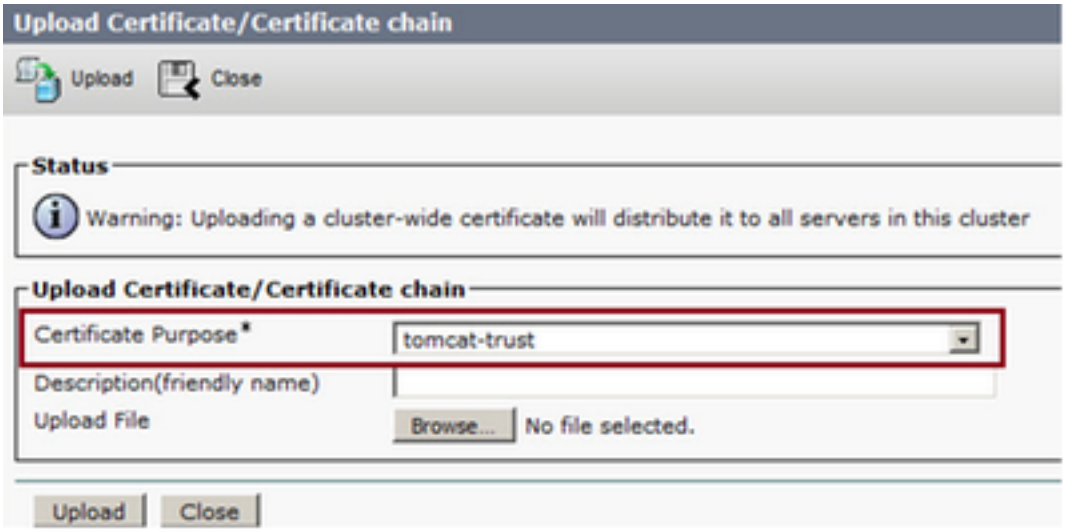
2. 从certifcate权限一个应该接受主要的和secondory服务器的以下证书链。

- **精良服务器：根源，中间(可选)和应用程序认证**
- **CUIC服务器：根源，中间(可选)和应用程序认证**
- **生活数据服务：根源，中间(可选)和应用程序认证**

步骤3.对服务器的加载证书。

此部分在精良描述关于怎样正确地加载证书链， CUIC和居住数据服务器。

精良服务器

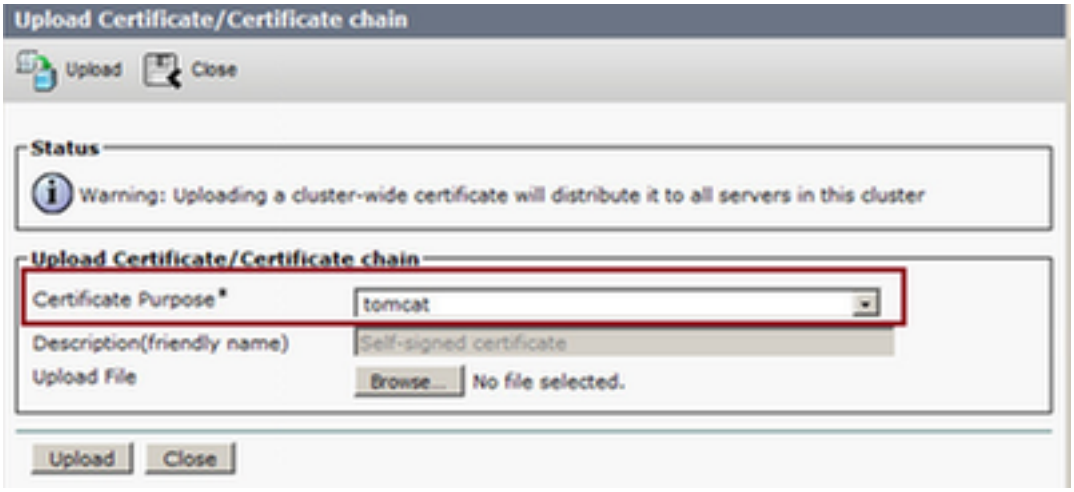


1. 在这些步骤帮助下加载在主要的精良服务器的根证明：

   Step 1.在主要服务器Cisco Unified通信操作系统的管理页面，请连接对**安全> Certificate Management >加载认证。**
   Step 2.从验证名称下拉列表，请选择Tomcat信任。
   第3.步。在上传文件字段，请点击访问并且访问对根证明文件。
   步骤4.点击上传文件。

2. 在这些步骤帮助下加载在主要的Fineese服务器的中间证书：

   步骤1.如step1所显示，在加载半成品certififcate的步骤同根证明一样。
   Step 2.在主要服务器Cisco Unified通信操作系统的管理页面，请连接对**安全> Certificate Management >加载认证。**
   第3.步。从验证名称下拉列表，请选择Tomcat信任。
   第4.步。在上传文件字段，请点击访问并且访问对中间证书文件。
   步骤5.点击**加载**。**Note**:当Tomcat信任存储被复制在主要的和附属服务器之间不是需要的加载根或中间证书到附属精良服务器。
3. 如镜像所显示，加载主要的精良服务器应用认证：



Step 1.从验证名称下拉列表，请选择Tomcat。**Step 2.**在上传文件字段，请点击**访问**并且访问到应用程序证书文件。
步骤3.点击**加载**加载文件。

4. 加载附属Fineese服务器应用认证。
   在此步骤请按照同一个进程按照在附属服务器的第3步所述的其自己的应用程序认证。

5. 现在您能重新启动服务器。
   访问在主要的和附属精良服务器的CLI并且输入命令**utils系统重新启动**重新启动服务器。

CUIC服务器(假设半成品证书当前在证书链)

1. 加载在主要的CUIC服务器的根证明。

   Step 1.在主要服务器Cisco Unified通信操作系统的管理页面，请连接到**安全> Certificate Management >加载认证/证书链**。
   Step 2.从验证名称下拉列表，请选择Tomcat信任。
   第3.步。在上传文件字段，请点击访问并且访问对根证明文件。
   步骤4.点击上传文件。**Note**:当Tomcat信任存储被复制在主要的和附属服务器之间不是需要的加载根证明到第二CUIC服务器。

2. 加载主要的CUIC服务器应用认证。

   Step 1.从验证名称下拉列表，请选择Tomcat。
   Step 2.在上传文件字段，请点击访问并且访问到应用程序证书文件。
   步骤3.点击上传文件。
3. 加载附属CUIC服务器应用认证。
   按照同一个进程如在附属服务器的第(2)步所述的其自己的应用程序认证

4. 重新启动服务器
   访问在主要的和附属CUIC服务器的CLI并且输入命令**"utils系统重新启动"**重新启动服务器。
   Note:如果CA权限提供包括半成品证书那么的证书链在精良服务器部分提及的步骤是可适用的对CUIC服务。

实际数据服务器

1. 步骤在实际数据服务器包括加载证书与精良或CUIC服务器是相同的根据证书链。

2. 在主要的实际数据服务器的加载根证明。

   Step 1.在主要服务器Cisco Unified通信操作系统的管理页面，请连接对**安全> Certificate Management >加载认证**。
   Step 2.从验证名称下拉列表，请选择Tomcat信任。
   第3.步。在上传文件字段，请点击**访问**并且访问对根证明文件。
   步骤4.点击**加载**。

3. 加载在主要的实际数据服务器的中间证书。

   步骤1.如step1所显示，在加载半成品certififcate的步骤同根证明一样。
   Step 2.在主要服务器Cisco Unified通信操作系统的管理页面，请连接对**安全> Certificate Management >加载认证**。

第3.步。从验证名称下拉列表，请选择Tomcat信任。
第4.步。在上传文件字段，请点击**访问**并且访问对中间证书文件。
步骤5.点击**加载**。
Note:当Tomcat信任存储被复制在主要的和附属服务器之间不是需要的加载根或中间证书到附属实际数据服务器。

4. 加载主要的实际数据服务器应用认证**。**

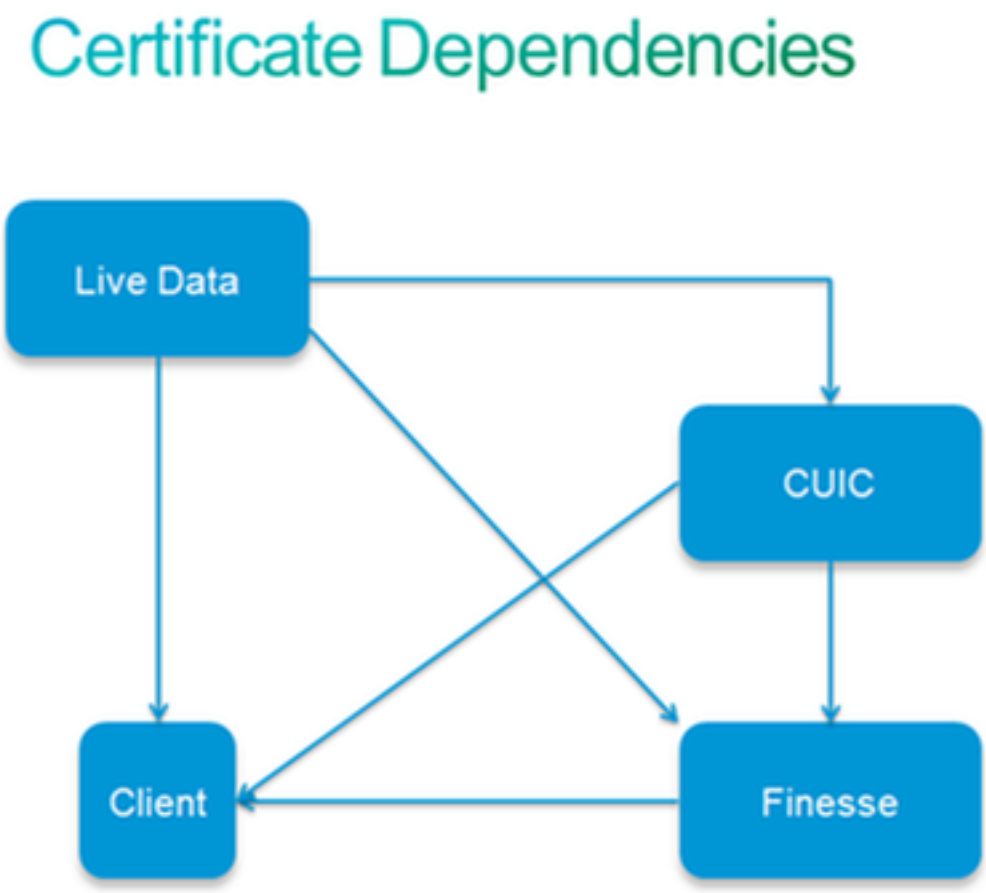
   Step 1.从验证名称下拉列表，请选择Tomcat。
   Step 2.在上传文件字段，请点击**访问**并且访问到应用程序证书文件。
   步骤3.点击**加载**。

5. 加载附属实际数据服务器应用认证。
   遵从同样步骤如上所述在(4)在其自己的应用程序认证的secondory服务器。

6. 重新启动服务器
   访问在主要的和附属精良服务器的CLI并且输入命令**"utils系统重新启动"**重新启动服务器。

居住数据服务器认证依靠

如镜像所显示，作为实际数据服务器与CUIC和精良服务器呼应，那里是在这些服务器之间的认证依靠：



关于第三方CA证书一系列根和中间证书是同样为在组织的所有服务器。结果为了Live数据服务器能适当地工作，您必须保证精良和CUIC服务器有在那里Tomcat信任容器和中间证书适当地装载的根。

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

目前没有针对此配置的故障排除信息。