

程序包CCE解决方案：程序获得并上载第三方CA证书

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[程序](#)

[生成并且下载CSR](#)

[获得根、中间\(如果适用\)和从CA的应用程序认证](#)

[加载证书到服务器](#)

[精良服务器](#)

[CUIC服务器](#)

[认证依靠](#)

[加载CUIC在精良主要服务器的服务器根证明](#)

[加载精良根/中间证书在CUIC主要服务器](#)

简介

本文描述包括的步骤为了从第三方供应商获得和安装认证机构(CA)认证，生成为了建立精良和Cisco Unified智力中心(CUIC)服务器之间的HTTPS连接。

为了使用HTTPS精良和CUIC服务器之间的安全通信，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署名的认证或用户能获得和安装CA证书。这些CA证书从一个第三方供应商获得类似VeriSign，Thawte，GeoTrust或可以被生产内部地。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

- Cisco程序包联系中心企业(PCCE)
- CUIC
- Cisco精良
- CA证书

[使用的组件](#)

用于本文的信息根据PCCE解决方案11.0 (1)版本。

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。如果您的网络实际，请切记您了解所有步骤的潜在影响。

程序

为了设置HTTPS通信的证书在精良和CUIC服务器，请遵从这些步骤：

- 生成并且下载认证签名请求(CSR)
- 获得根、中间(如果适用)和从CA的应用程序认证与使用CSR
- 加载证书到服务器

生成并且下载CSR

1. 被描述的步骤这里将为了生成和下载CSR。这些步骤是相同的为精良和CUIC服务器。
2. 打开与URL的Cisco Unified通信操作系统的管理页面并且签到与在安装过程时被创建的操作系统(OS)管理帐户。主要服务器/cmplatform <https://hostname>
3. 生成认证签名请求。
 - a. 连接对**安全 > Certificate Management > 生成CSR**。
 - b. 从认证Purpose*下拉列表，请选择Tomcat。
 - c. 选择Hash算法作为SHA256。
 - d. 如镜像所显示，点击生成。

Generate Certificate Signing Request

Generate Close

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose* tomcat

Distribution* livedata.ora.com

Common Name livedata.ora.com

Required Field

Subject Alternate Names (SANs)

Parent Domain ora.com

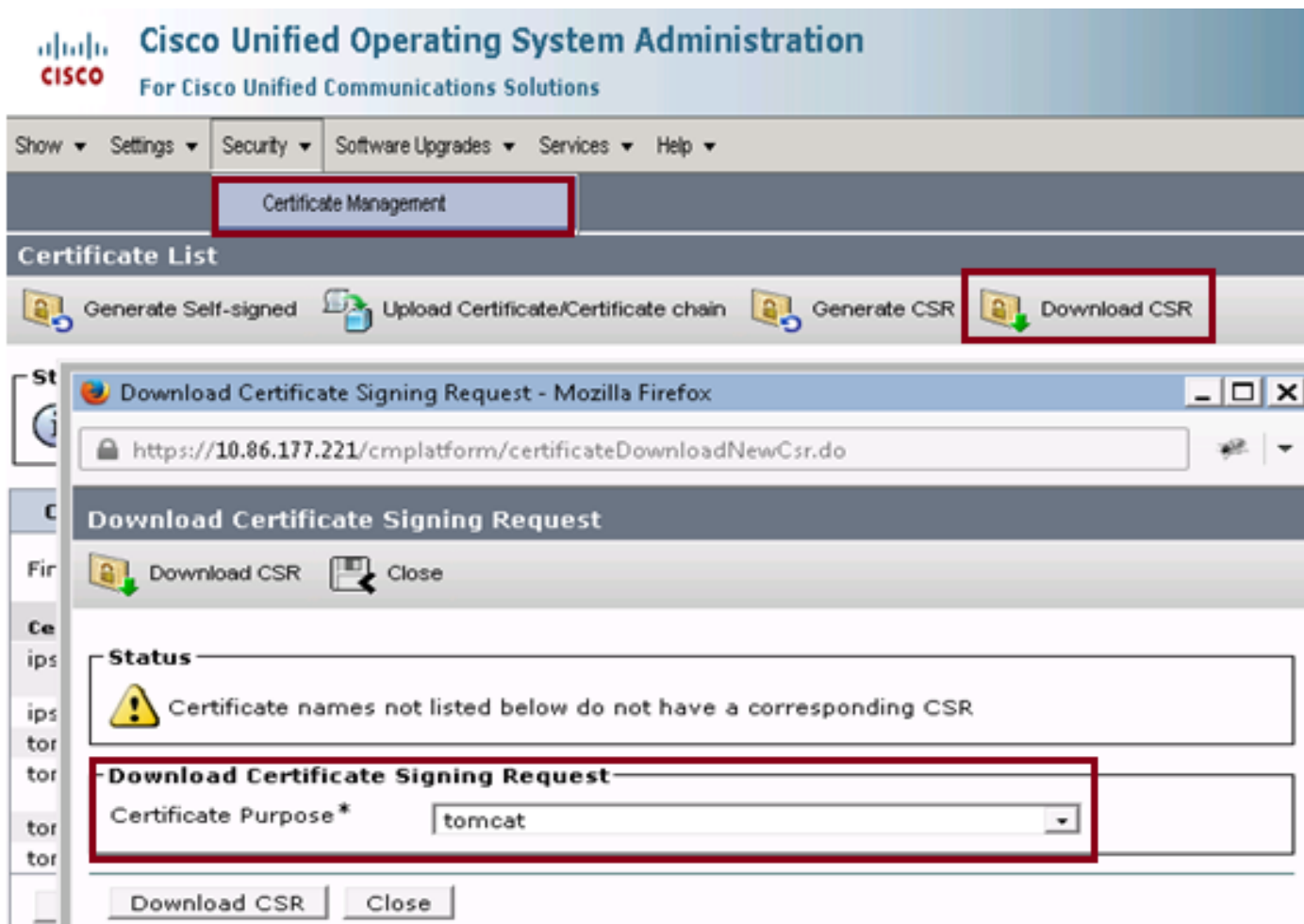
Key Length* 2048

Hash Algorithm* SHA256

Generate Close

4. 下载CSR。

- a. 连接对安全> Certificate Management > 下载CSR。
- b. 从认证Purpose*下拉列表，请选择Tomcat。
- c. 如镜像所显示，点击下载CSR。



Note: 执行在附属服务器的这些步骤与URL附属服务器/cmplatform https://hostname为了得到CA的CSR。

获得根、中间(如果适用)和从CA的应用程序认证

1. 提供主要的和附属服务器的CSR信息给第三方CA类似VeriSign、Thawte，GeoTrust等。
2. 从CA，您必须接受这些主要的和附属服务器的证书链：
 - 精良服务器：根、中间和应用程序认证
 - CUIC服务器：根和应用程序认证

对服务器的加载证书

此部分在精良和CUIC服务器描述关于怎样正确地加载证书链。

精良服务器

1. 加载主要的精良服务器根认证：

- a. 在主要服务器的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。
- b. 从认证目的下拉列表，请选择Tomcat信任。
- c. 在上传文件字段，请点击访问并且访问根证明文件。
- d. 单击 Upload File。

2. 加载主要的精良服务器中间证书：

- a. 从认证目的下拉列表，请选择Tomcat信任。
- b. 在被归档的根证明，请输入在上一步被加载根证明的名字。这是生成的.pem文件，当安装了根/公共认证。

为了查看此文件，连接对证书管理>查找。在认证列表中，.pem文件名是列出的Tomcat信任。

- c. 在上传文件字段，请点击访问并且访问中间证书文件。
- d. 单击 Upload File。

Note:当Tomcat信任存储被复制在主要的和附属服务器之间，不是需要的加载主要的精良服务器根或中间证书到附属精良服务器。

3. 加载主要的精良服务器应用认证：

- a. 从认证目的下拉列表，请选择Tomcat。
- b. 在根证明字段，请输入在上一步被加载中间证书的名字。包括.pem扩展名(例如，TEST SSL CA.pem)。
- c. 在上传文件字段，请点击访问并且访问应用程序证书文件。
- d. 单击 Upload File。

4. 加载附属精良服务器根和中间证书：

- a. 遵从同样步骤按照在附属服务器的第1步和第2步所述的其证书。

Note:当Tomcat信任存储被复制在主要的和附属服务器之间，不是需要的加载附属精良服务器根或中间证书到主要的精良服务器。

5. 加载附属精良服务器应用认证：

- a. 遵从同样步骤按照在附属服务器的第3步所述的其自己的证书。

6. 重新启动服务器：

- a. 访问在主要的和附属精良服务器的CLI并且运行命令**utils系统重新启动**为了重新启动服务器。

CUIC服务器

1. 加载CUIC主要的服务器根(公共)认证：

- a. 在主要服务器的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。
- b. 从认证目的下拉列表，请选择Tomcat信任。
- c. 在上传文件字段，请点击访问并且访问根证明文件。
- d. 单击 **Upload File**。

Note:当Tomcat信任存储被复制在主要的和附属服务器之间，不是需要的加载主要的CUIC服务器根认证到第二CUIC服务器。

2. 加载CUIC主要的服务器应用(主要的)认证：

- a. 从认证目的下拉列表，请选择Tomcat。
- b. 在根证明字段，请输入在上一步被加载根证明的名字。

这是生成的.pem文件，当安装了根/公共认证。为了查看此文件，连接对证书管理>查找。

在认证列表.pem文件名是列出的Tomcat信任。包括该.pem扩展名(例如，TEST SSL CA.pem)。

- c. 在上传文件字段，请点击访问并且访问应用程序(主要的)证书文件。
- d. 单击 **Upload File**。

3. 加载CUIC附属服务器根(公共)认证：

- a. 在第二CUIC服务器上，请遵从同样步骤按照其根证明的第1.步所述。

Note:当Tomcat信任存储被复制在主要的和附属服务器之间，不是需要的加载第二CUIC服务器根认证到主要的CUIC服务器。

4. 加载CUIC附属服务器应用(主要的)认证：

- a. 按照同一个进程如在附属服务器的第2.步所述的其自己的认证。

5. 重新启动服务器：

- a. 访问在主要的和附属CUIC服务器的CLI并且运行命令**utils系统重新启动**为了重新启动服务器。

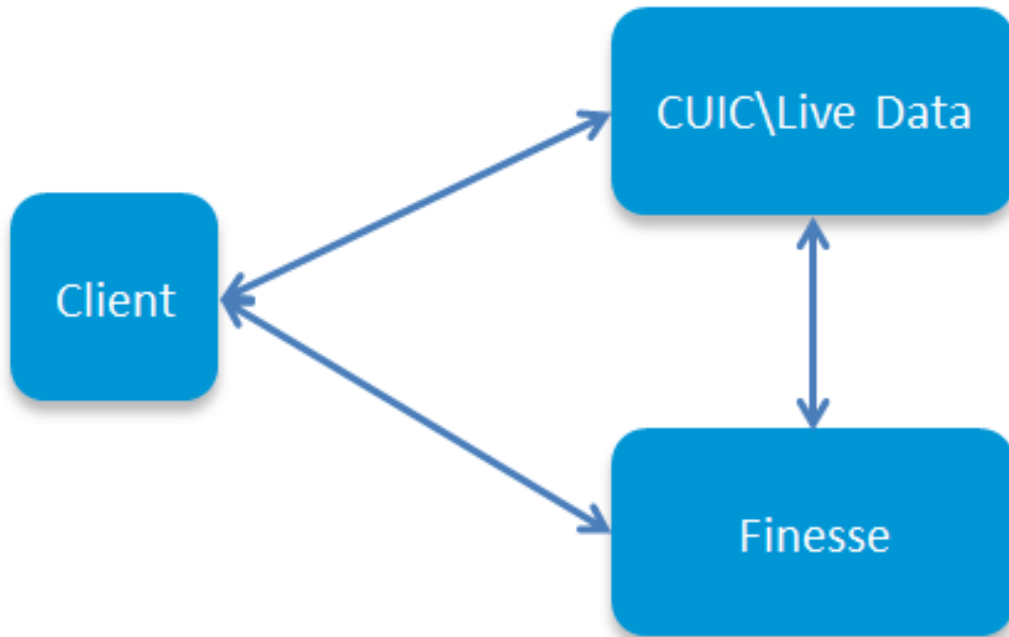
Note:为了避免认证例外警告，您必须访问有使用的服务器完全合格的域名(FQDN)。

认证依靠

因为精良代理程序和Supervisor为报告目的使用CUIC小配件，您必须加载这些服务器根证明，按被提及的顺序这里维护HTTPS通信的认证依靠这些服务器之间和如镜像所显示。

- 加载CUIC在精良主要服务器的服务器根证明
- 加载精良根\中间证书在CUIC主要服务器

Certificate Dependencies



加载CUIC在精良主要服务器的服务器根证明

1. 在主要的精良服务器上，开放与URL的Cisco Unified通信操作系统的管理页面和签到与在安装过程中被创建的OS管理帐户：

主要的精良服务器/cmplatform <https://hostname>

2. 加载主要的CUIC根证明。
 - a. 连接对**安全**> **Certificate Management** >加载认证。
 - b. 从认证目的下拉列表，请选择Tomcat信任。
 - c. 在上传文件字段，请点击访问并且访问根证明文件。
 - d. 单击 **Upload File**。
3. 加载附属CUIC根证明。
 - a. 连接对**安全**> **Certificate Management** >加载认证。
 - b. 从认证目的下拉列表，请选择Tomcat信任。

c. 在上传文件字段，请点击**访问并且访问根证明文件**。

d. 单击 **Upload File**。

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CUIC根证明到附属精良服务器。

4. 访问在主要的和附属精良服务器的CLI并且运行命令**utils系统重新启动**为了重新启动服务器。

加载精良根/中间证书在CUIC主要服务器

1. 在主要的CUIC服务器上，开放与URL的**Cisco Unified通信操作系统的管理页面**和签到与在安装过程时被创建的OS管理帐户：

主要的CUIC服务器/cmplatform https://hostname

2. 加载主要的精良根证明：

a. 连接对**安全> Certificate Management >加载认证**。

b. 从认证目的下拉列表，请选择**Tomcat信任**。

c. 在上传文件字段，请点击**访问并且访问根证明文件**。

d. 单击 **Upload File**。

3. Upload主要的精良中间证书：

a. 从认证目的下拉列表，请选择**Tomcat信任**。

b. 在被归档的根证明，请输入在上一步被加载根证明的名字。

c. 在上传文件字段，请点击**访问并且访问中间证书文件**。

d. 单击 **Upload File**。

4. 执行同一附属精良根\半成品证书的第2步和第3.步在主要的实际数据服务器。

Note:当Tomcat信任存储被复制在主要的和附属服务器之间，不是需要的加载精良根/Intermediate认证到第二CUIC服务器。

5. 访问在主要的和附属CUIC服务器的CLI并且运行命令**utils系统重新启动**为了重新启动服务器。