在PCCE 12.6解决方案中交换自签名证书

目录

简介

本文档介绍如何在Cisco Packaged Contact Center Enterprise (PCCE)解决方案中交换自签名证书。

先决条件

要求

Cisco 建议您了解以下主题：

- PCCE版本12.6(2)
- 客户语音门户(CVP)版本12.6(2)
- 虚拟化语音浏览器(VVB) 12.6(2)
- 管理工作站/管理日期服务器(AW/ADS) 12.6(2)
- 思科统一情报服务器(CUIC)
- 客户协作平台(CCP) 12.6(2)

- 企业聊天和电子邮件(ECE) 12.6(2)

使用的组件

本文档中的信息基于以下软件版本：

- PCCE 12.6(2)
- CVP 12.6(2)

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

在来自12.x的PCCE解决方案中，所有设备均通过托管在主要AW服务器中的单一平台(SPOG)进行控制。由于PCCE 12.5(1)版本的安全管理合规性(SRC)，解决方案中SPOG与其他服务器之间的所有通信都通过安全的HTTP协议严格完成。

证书用于实现SPOG与其他设备之间的无缝安全通信。在自签名证书环境中，服务器之间的证书交换是必需的。

步骤

这些是导出自签名证书的组件和需要将自签名证书导入其中的组件。

(i)所有AW/ADS服务器：这些服务器需要以下证书：

- Windows平台：
  - ICM：路由器和记录器（记录器）{A/B}、外围网关(PG){A/B}、所有AW/ADS和ECE服务器。

注：需要IIS和诊断框架门户(DFP)。

  - CVP：CVP服务器、CVP报告服务器。

    注意：需要来自所有服务器的Web服务管理(WSM)证书。证书必须使用完全限定域名(FQDN)。

- VOS平台：云连接、思科虚拟化语音浏览器(VVB)、思科统一通信管理器(CUCM)、Finesse、思科统一情报中心(CUIC)、实时数据(LD)、身份服务器(IDS)和其他适用服务器。

(ii)路由器\记录器服务器：这些服务器需要来自以下来源的证书：

- Windows平台：所有AW/ADS服务器IIS证书。

(iii) PG服务器：这些服务器需要来自以下来源的证书：

- Windows平台：所有AW/ADS服务器IIS证书。
- VOS平台：CUCM发布服务器（仅限CUCM PG服务器）；云连接和CCP（仅限MR PG服务器）。

注意：从CUCM服务器下载JTAPI客户端需要执行此操作。

(iv) CVP服务器：这些服务器需要从

- Windows平台：所有ADS服务器IIS证书
- VOS平台：云连接服务器、VVB服务器。

(v) CVP报告服务器：此服务器需要来自以下来源的证书：

- Windows平台：所有ADS服务器IIS证书

(vi) VVB服务器：此服务器需要以下证书：

- Windows平台：所有ADS服务器IIS证书、来自CVP服务器的VXML证书以及来自CVP服务器的Callserver证书
- VOS平台：云连接服务器。

在解决方案中，有效交换自签名证书所需的步骤分为三个部分。

第1部分：CVP服务器和ADS服务器之间的证书交换。

第2部分： VOS平台应用和ADS服务器之间的证书交换。

第3部分：路由器、PG和ADS服务器之间的证书交换。

第1部分：CVP和ADS服务器之间的证书交换

成功完成此交换所需的步骤如下：

步骤1:导出CVP服务器WSM证书。

第二步：将CVP服务器WSM证书导入ADS服务器。

第三步：导出ADS服务器证书。

第四步：将ADS服务器导入CVP服务器和CVP报告服务器。

步骤1:导出CVP服务器证书

从CVP服务器导出证书之前，需要使用服务器的FQDN重新生成证书，否则，智能许可、虚拟代理语音(VAV)和CVP与SPOG同步等少数功能可能会出现问题。

注意：开始之前，您必须完成以下操作：
1. 以管理员身份打开命令窗口。

⚠ 2. 对于12.6.2，要标识密钥库密码，请转到%CVP_HOME%\bin文件夹并运行DecryptKeystoreUtil.bat文件。
3. 对于12.6.1，要标识密钥库口令，请运行命令more %CVP_HOME%\conf\security.properties。
4. 运行keytool命令时需要此口令。
5. 从%CVP_HOME%\conf\security\目录，运行命令copy .keystore backup.keystore。

注意：通过使用keytool参数-storepass，您可以简化本文档中使用的命令。对于所有CVP服务器，请提供您确定的密钥工具密码。对于ADS服务器，默认密码为：changeit

要在CVP服务器上重新生成证书，请执行以下步骤：

(i)列出服务器中的证书

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list
```

注意：CVP服务器使用以下自签名证书：wsm_certificate、vxml_certificate、callserver_certificate。如果使用keytool的参数-v，则可以看到每个证书的更详细信息。此外，您可以在keytool.exe list命令末尾添加“>”符号，以便将输出发送到文本文件，例如：> test.txt

(ii)删除旧的自签名证书

CVP服务器：用于删除自签名证书的命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias vxml_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias callserver_certificate
```

CVP报告服务器：用于删除自签名证书的命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias callserver_certificate
```

注意：CVP报告服务器使用以下自签名证书：wsm_certificate、callserver_certificate。

(iii)使用服务器的FQDN生成新的自签名证书

CVP服务器

用于为WSM生成自签名证书的命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

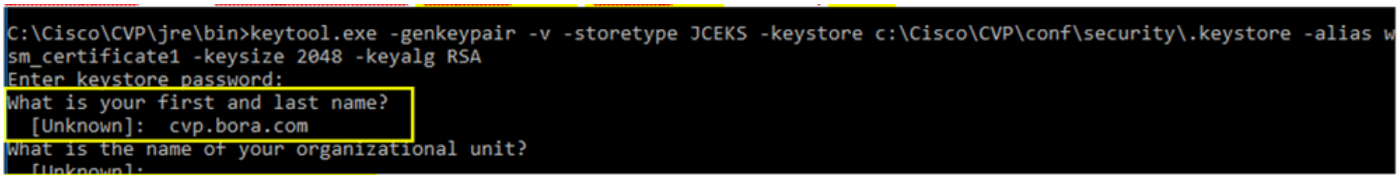
注意：默认情况下，证书的生成时间为两年。使用-validity XXXX设置重新生成证书时的到期日期，否则证书有效期为90天，并且在此时间之前需要由CA签名。对于这些证书中的大多数，3-5年必须是合理的验证时间。

以下是一些标准有效性输入：

一年	365
两年	730
三年	1095
四年	1460
五年	1895
十年	3650

注意：从12.5证书必须是SHA 256、密钥大小2048和加密算法RSA，请使用以下参数设置这些值：-keyalg RSA和-keysize 2048。CVP密钥库命令必须包括-storetype JCEKS参数。如果不执行此操作，证书、密钥或更糟的密钥库可能会损坏。

在问题您的名字和姓氏是什么上指定服务器的FQDN？



完成以下其他问题：

您的组织单位名称是什么？

[未知]：<指定OU>

贵公司的名称是什么？

[未知]：<指定组织的名称>

您的城市或地区名称是什么？

[未知]：<指定城市/地区的名称>

您所在省/自治区/直辖市的名称是什么？

[未知]：<指定州/省的名称>

此设备的两个字母的国家/地区代码是什么？

[未知]：<指定两个字母的国家/地区代码>

为接下来的两个输入指定yes。

对vxml_certificate和callserver_certificate执行相同的步骤：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias vxml_certificate -keysize 2048 -keyalg RSA -validity XXXX

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

重新启动CVP呼叫服务器。

CVP报告服务器

用于为WSM生成自签名证书的命令：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

指定用于查询您的姓和名的服务器的FQDN，并继续执行与CVP服务器相同的步骤。

对callserver_certificate执行相同的步骤：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

重新启动报告服务器。

(iv)从CVP和报告服务器导出wsm_Certificate

a)将WSM证书从每个CVP服务器导出到临时位置，并使用所需的名称重命名证书。您可以将其重命名为wsmcsX.crt。将“X”替换为服务器的主机名。例如，wsmcsa.crt、wsmcsb.crt、wsmrepa.crt、wsmrepb.crt。

用于导出自签名证书的命令：

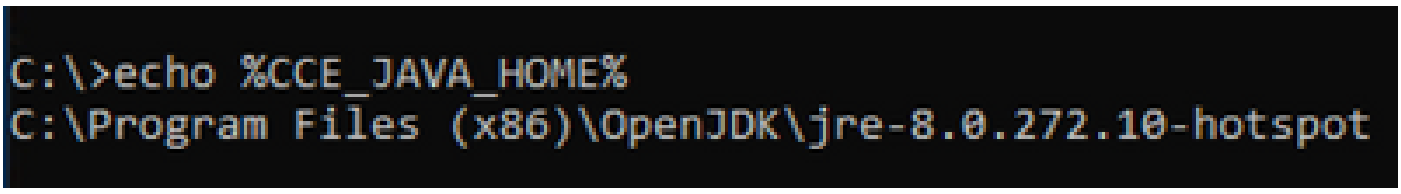
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b)从路径%CVP_HOME%\conf\security\wsm.crt复制证书，将其重命名为wsmcsX.crt，然后将其移到ADS服务器上的临时文件夹。

第二步：将CVP服务器WSM证书导入ADS服务器

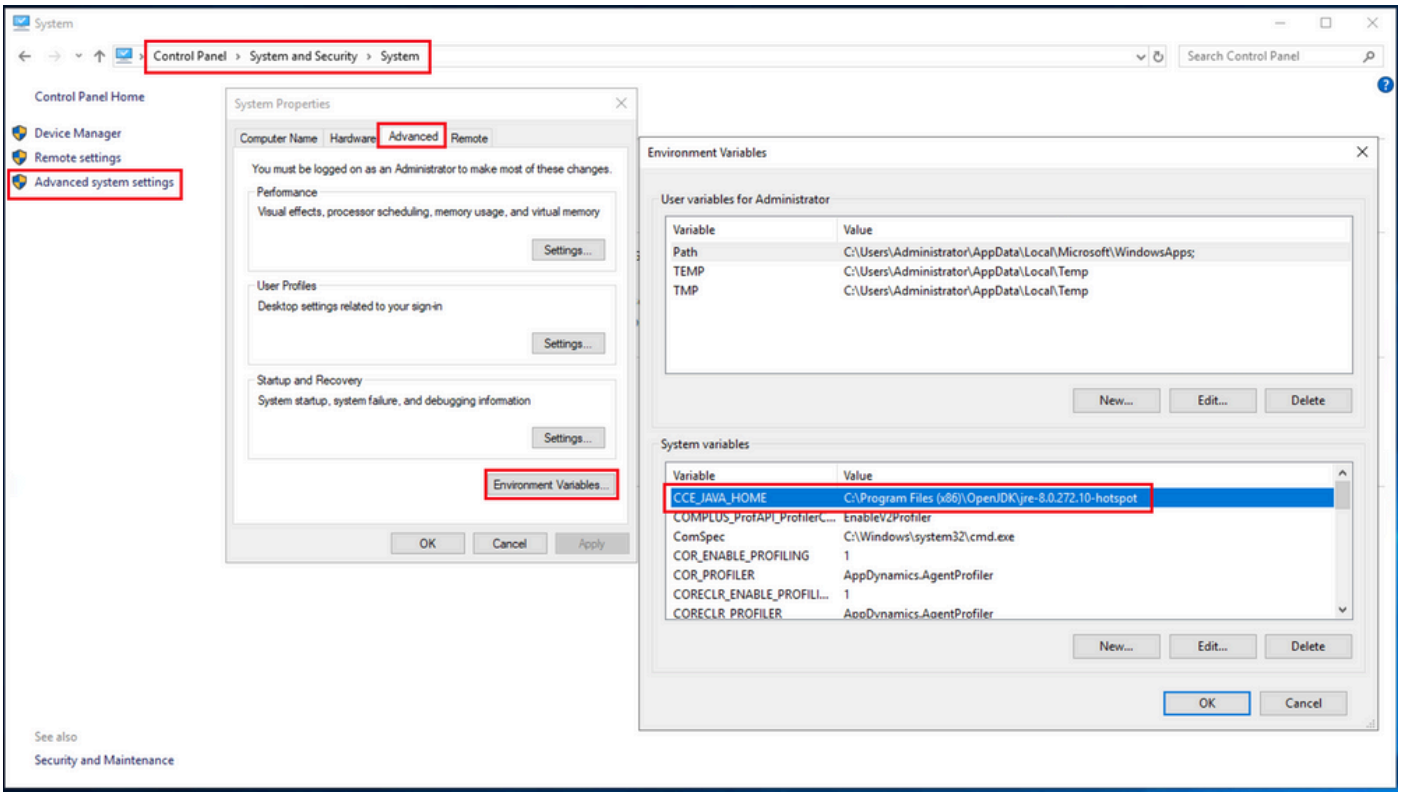
要在ADS服务器中导入证书，您需要使用Java工具集中的keytool。您可以通过两种方法查找托管此工具的java主路径。

(i) CLI命令> echo %CCE_JAVA_HOME%



Java主路径

(ii)通过高级系统设置手动，如图所示。



环境变量

在PCCE 12.6上，OpenJDK的默认路径为C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

导入自签名证书的命令：

```
cd %CCE_JAVA_HOME%\bin
keytool.exe -import -file C:\Temp\certs\wsmcsX.crt -alias {fqdn_of_CVP} -keystore {ICM install directory}\ssl\cacerts
```

注意：对部署中的每个CVP重复这些命令，并在其他ADS服务器上执行相同任务

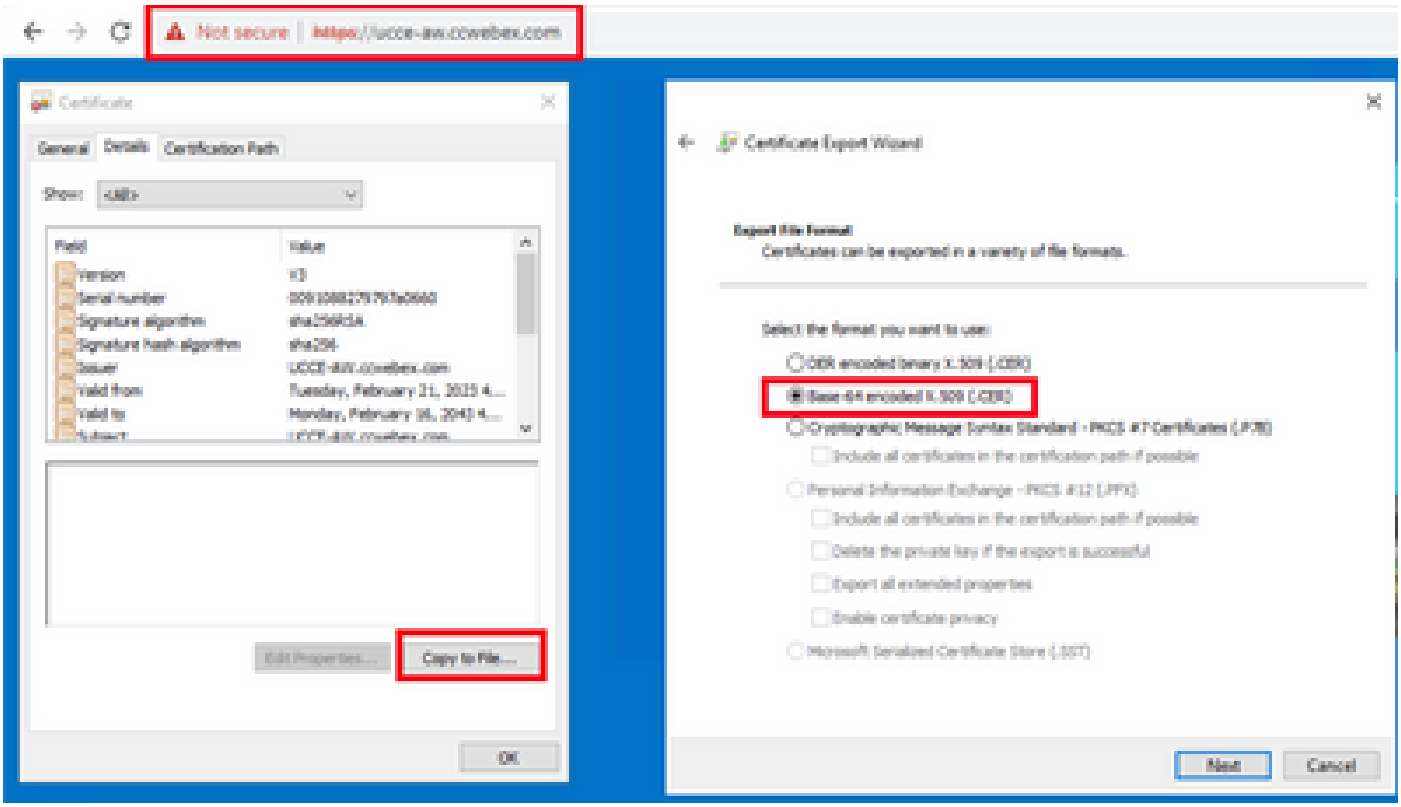
(iii)在ADS服务器上重新启动Apache Tomcat服务。

第三步：导出ADS服务器证书

以下是导出ADS证书的步骤：

(i)在ADS服务器上，从浏览器导航至服务器URL：https://<servername>。

(ii)将证书保存到临时文件夹(例如c：\temp\certs)中，并将证书命名为ADS<svr>[ab].cer。



导出ADS证书

注意：选择选项Base-64 encoded X.509 (.CER)。

第四步：将ADS服务器证书导入CVP服务器和报告服务器

(i)将证书复制到%CVP_HOME%\conf\security目录中的CVP服务器和CVP报告服务器。

(ii)将证书导入到CVP服务器和CVP报告服务器。

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -trustcacerts -alias {fqdn_of_ads} -file %CVP_HOME%\conf\security\ADS{svr}[ab].cer
```

对其他ADS服务器证书执行相同步骤。

(iii)重新启动CVP服务器和报告服务器

第2部分：VOS平台应用与ADS服务器之间的证书交换

成功完成此交换所需的步骤如下：

步骤1:导出VOS平台应用服务器证书。

第二步：将VOS平台应用证书导入ADS服务器。

第三步：将CUCM平台应用证书导入CUCM PG服务器。

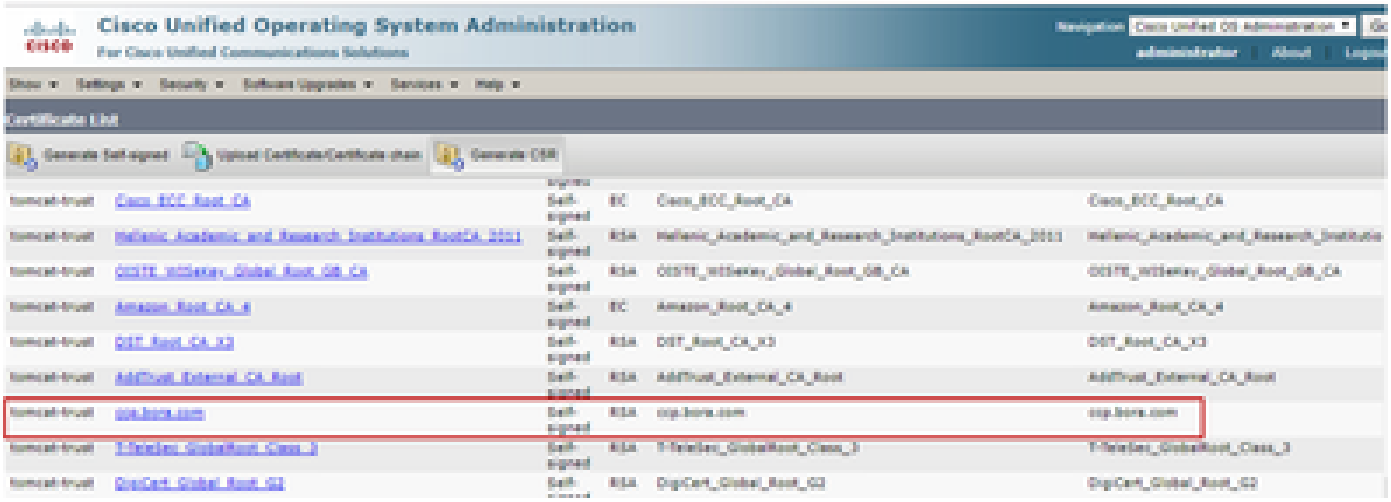
此过程适用于所有VOS应用，例如：

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- 云连接

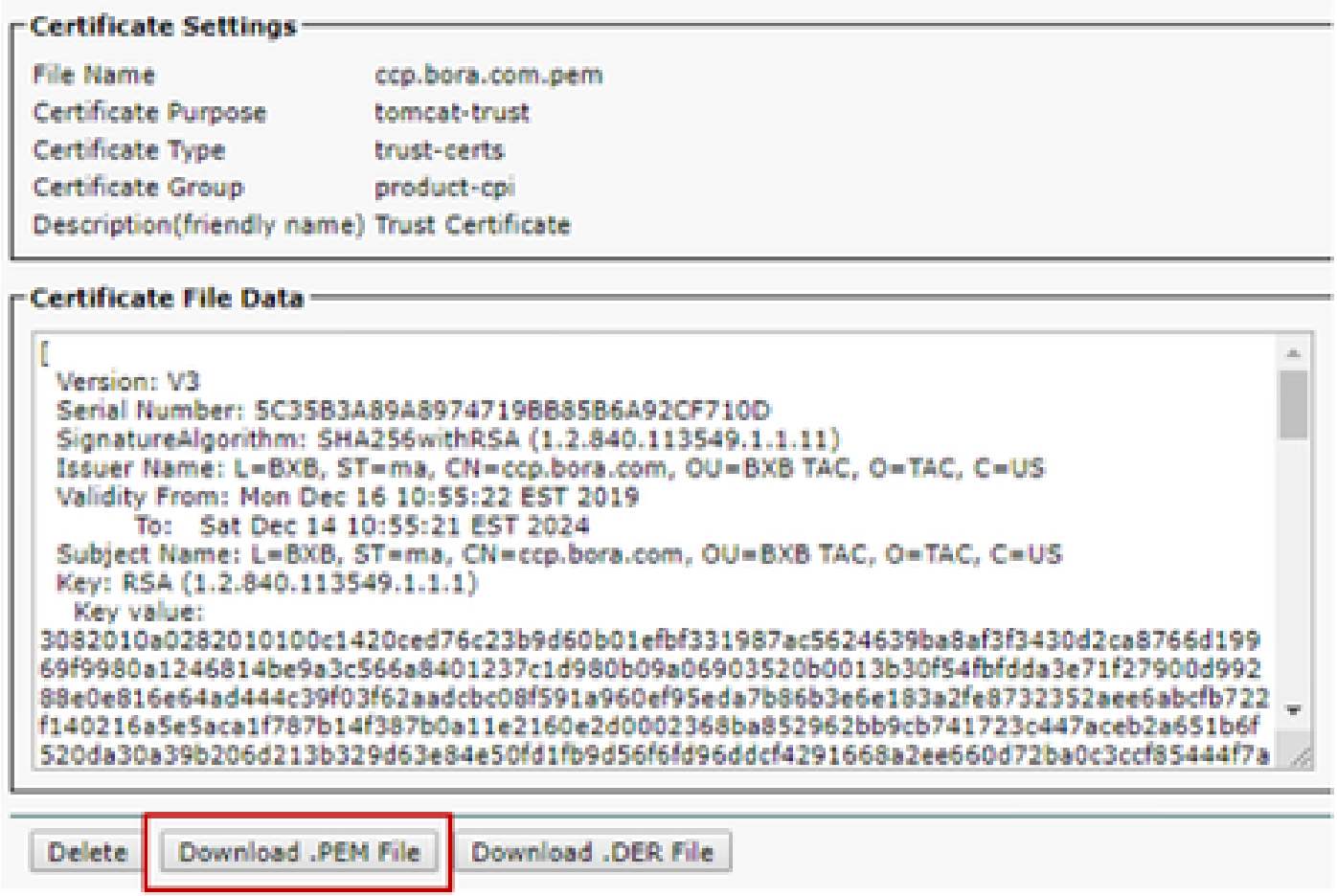
步骤1:导出VOS平台应用服务器证书。

(i)导航至Cisco Unified Communications Operating System Administration页面：https://FQDN:8443/cmplatform。

(ii)导航到安全>证书管理，并在tomcat-trust文件夹中查找应用程序主服务器证书。



(iii)选择证书并点击下载.PEM文件，将其保存在ADS服务器上的临时文件夹中。



注意：对用户执行相同的步骤。

第二步：将VOS平台应用证书导入ADS服务器

运行密钥工具的路径：%CCE_JAVA_HOME%\bin

导入自签名证书的命令：

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias
{fqdn_of_VOS>} -keystore {ICM install directory}\ssl\cacerts
```

在ADS服务器上重新启动Apache Tomcat服务。

注意：在其他ADS服务器上执行相同任务

第三步：将CUCM平台应用证书导入CUCM PG服务器

运行密钥工具的路径：%CCE_JAVA_HOME%\bin

导入自签名证书的命令：

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\cucmapplicationX.cer -alias
{fqdn_of_cucm>} -keystore {ICM install directory}\ssl\cacerts
```

重新启动PG服务器上的Apache Tomcat服务。

注意：在其他CUCM PG服务器上执行相同任务

第3部分：路由器、PG和ADS服务器之间的证书交换

成功完成此交换所需的步骤如下：

步骤1:从路由器和PG服务器导出IIS证书

第二步：从路由器和PG服务器导出DFP证书

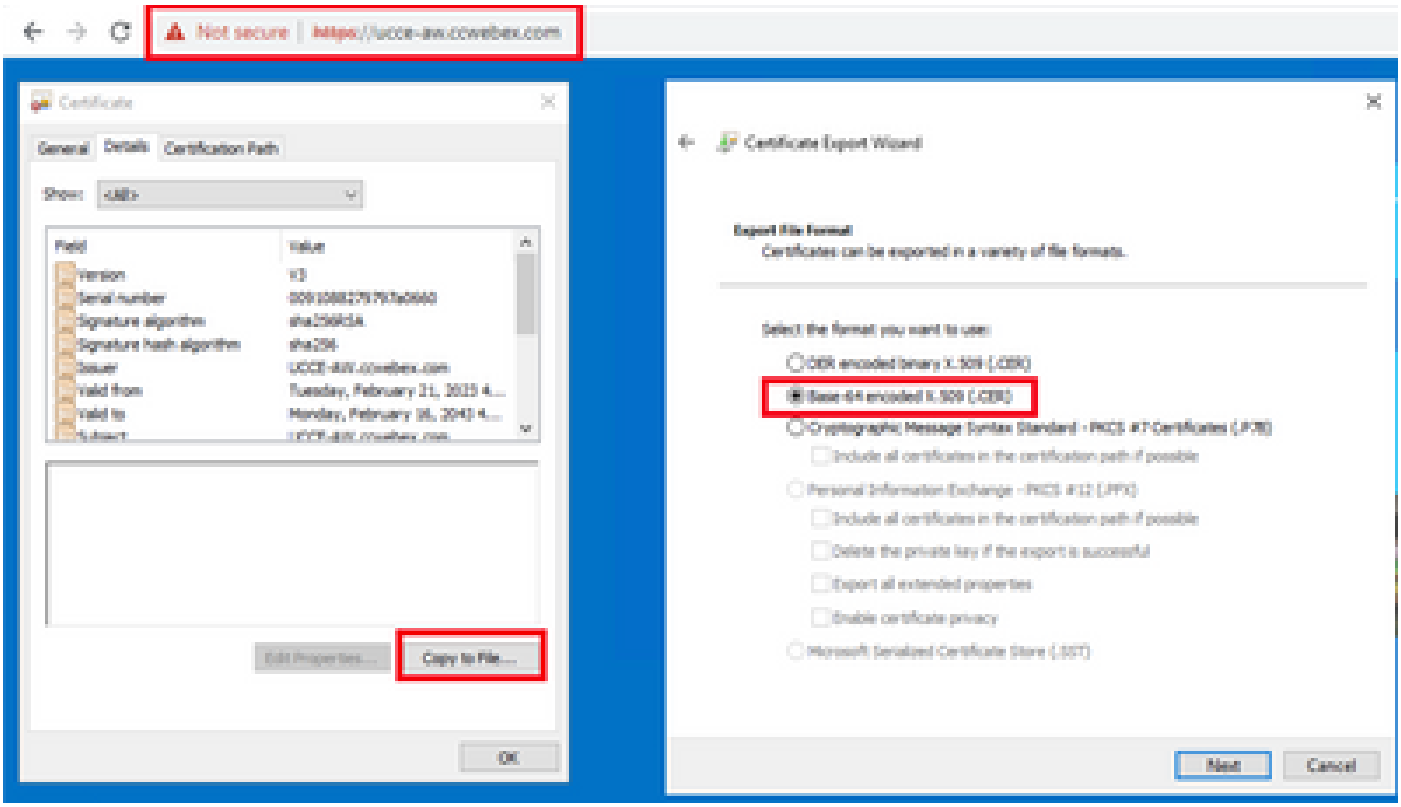
第三步：将证书导入ADS服务器

第四步：将ADS证书导入到路由器和PG服务器

步骤1:从路由器和PG服务器导出IIS证书

(i)在ADS服务器上，从浏览器导航至服务器(Rogers ， PG) url：https://{servername}

(ii)将证书保存到临时文件夹(例如c：\temp\certs)中，并将证书命名为ICM<svr>[ab].cer



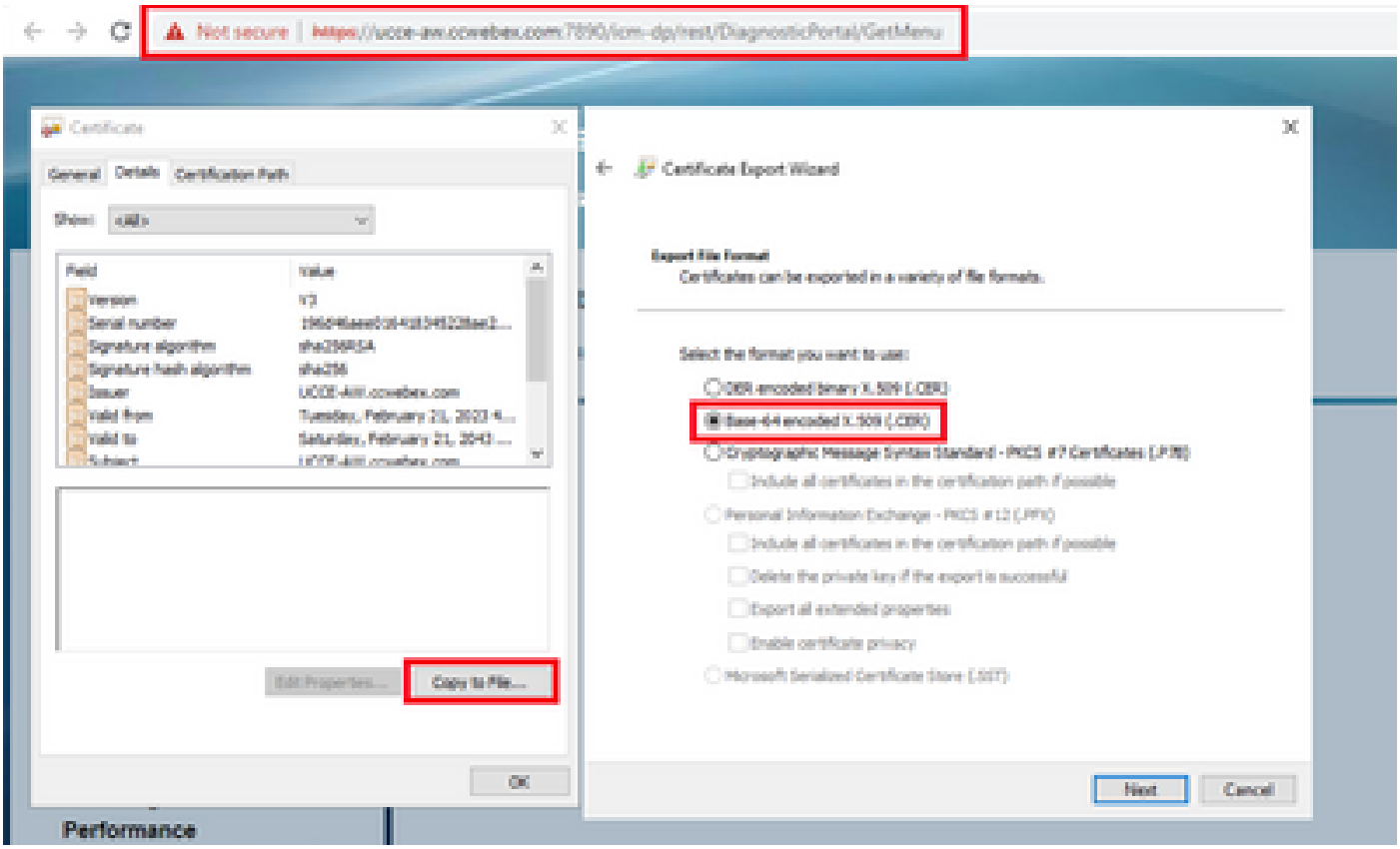
导出IIS证书

注意：选择选项Base-64 encoded X.509 (.CER)。

第二步：从路由器和PG服务器导出DFP证书

(i)在ADS服务器上，从浏览器导航至服务器(Rogers， PGs) DFP
url：https://{servername}：7890/icm-dp/rest/DiagnosticPortal/GetProductVersion

(ii)将证书保存到文件夹示例c：\temp\certs，并将证书命名为dfp{svr}[ab].cer



导出DFP证书

注意：选择选项Base-64 encoded X.509 (.CER)。

第三步：将证书导入ADS服务器

用于将IIS自签名证书导入ADS服务器的命令。运行密钥工具的路径： %CCE_JAVA_HOME%\bin

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\temp\certs\ICM<svr>[ab].cer -alias
{fqdn_of_server}_IIS -keystore {ICM install directory}\ssl\cacerts
```

注意：导入导出到所有ADS服务器的所有服务器证书。

用于将诊断自签名证书导入到ADS服务器的命令

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp<svr>[ab].cer -alias
{fqdn_of_server}_DFP -keystore {ICM install directory}\ssl\cacerts
```

注意：导入导出到所有ADS服务器的所有服务器证书。

在ADS服务器上重新启动Apache Tomcat服务。

第四步：将ADS证书导入到路由器和PG服务器

用于将IIS自签名证书导入到日志程序和PG服务器的命令。运行密钥工具的路径：%CCE_JAVA_HOME%\bin。

```
%CCE_JAVA_HOME%\bin\keytool -keystore ..\lib\security\cacerts  -import -storepass changeit -
alias {fqdn_of_server}_IIS -file c:\temp\certs\ICM{svr}[ab].cer
```

注意：导入导出到所有Rogger和PG服务器的所有ADS服务器IIS证书。

在路由器和PG服务器上重新启动Apache Tomcat服务。

第4部分：CVP CallStudio Web服务集成

有关如何为Web服务元素和Rest_Client元素建立安全通信的详细信息

请参阅Cisco Unified CVP VXML服务器和Cisco Unified Call Studio版本12.6(2)用户指南- Web服务集成[Cisco Unified Customer Voice Portal] - Cisco

相关信息

- CVP配置指南-安全
- UCCE安全指南
- PCCE管理指南
- Exchange PCCE自签名证书- PCCE 12.5
- Exchange UCCE自签名证书- UCCE 12.5
- Exchange UCCE自签名证书- UCCE 12.6
- 实施CA签名证书- CCE 12.6
- 使用联系中心上传工具交换证书
- 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）。