在UCCE解决方案中交换自签名证书

目录

简介

本文档介绍如何在Unified Contact Center Enterprise(UCCE)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：

- UCCE版本12.5(1)
- 客户语音门户(CVP)版本12.5(1)
- 思科虚拟化语音浏览器(VVB)

使用的组件

本文档中的信息基于以下软件版本：

- UCCE 12.5(1)
- CVP 12.5(1)
- 思科VVB 12.5
- CVP操作控制台(OAMP)
- CVP新OAMP(NOAMP)

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。

背景信息

在UCCE解决方案中，涉及核心应用(如ROGGER、外围设备网关(PG)、管理工作站(AW)/管理数据服务器(ADS)、Finesse、Cisco Unified Intelligence Center(CUIC)等)的新功能配置通过Contact Center Enterprise(CCE)Admin页面完成。对于CVP、Cisco VVB和网关等交互式语音应答(IVR)应用，NOAMP控制新功能的配置。从CCE 12.5(1)，由于安全管理合规性(SRC)，所有与CCE管理员和NOAMP的通信都严格通过安全HTTP协议完成。

为了在自签名证书环境中实现这些应用程序之间的无缝安全通信，服务器之间的证书交换成为一项必需。下一部分详细介绍在以下区域之间交换自签名证书所需的步骤：

- CCE AW服务器和CCE核心应用服务器
- CVP OAMP服务器和CVP组件服务器

步骤

CCE AW服务器和CCE核心应用服务器

这些是导出自签名证书的组件和必须将自签名证书导入其中的组件。

CCE AW服务器：此服务器需要来自以下位置的证书：

- Windows平台：路由器和记录器(ROGGER){A/B}、外围网关(PG){A/B}和所有AW/ADS。

注意：需要IIS和诊断框架门户(DFP)证书。

- VOS平台：Finesse、CUIC、实时数据(LD)、身份服务器(IDS)、云连接和其他适用服务器是资产数据库的一部分。

这一点同样适用于解决方案中的其他AW服务器。

Router\Logger Server：此服务器需要来自以下位置的证书：

- Windows平台：所有AW服务器的IIS证书。

有效交换CCE自签名证书所需的步骤分为以下部分：

1 节.路由器\记录器、PG和AW服务器之间的证书交换。
2 节.VOS平台应用和AW服务器之间的证书交换。

1 节.路由器\记录器、PG和AW服务器之间的证书交换

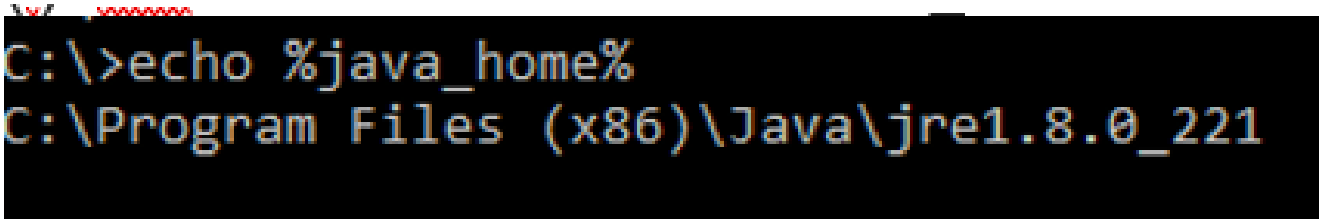
成功完成此交换所需的步骤如下：

步骤1:从路由器\记录器、PG和所有AW服务器导出IIS证书。
第二步：从路由器\记录器、PG和所有AW服务器导出DFP证书。
第三步：将IIS和DFP证书从Router\Logger、PG和AW导入AW服务器。
第四步：从AW服务器将IIS证书导入到Router\Logger和PG。

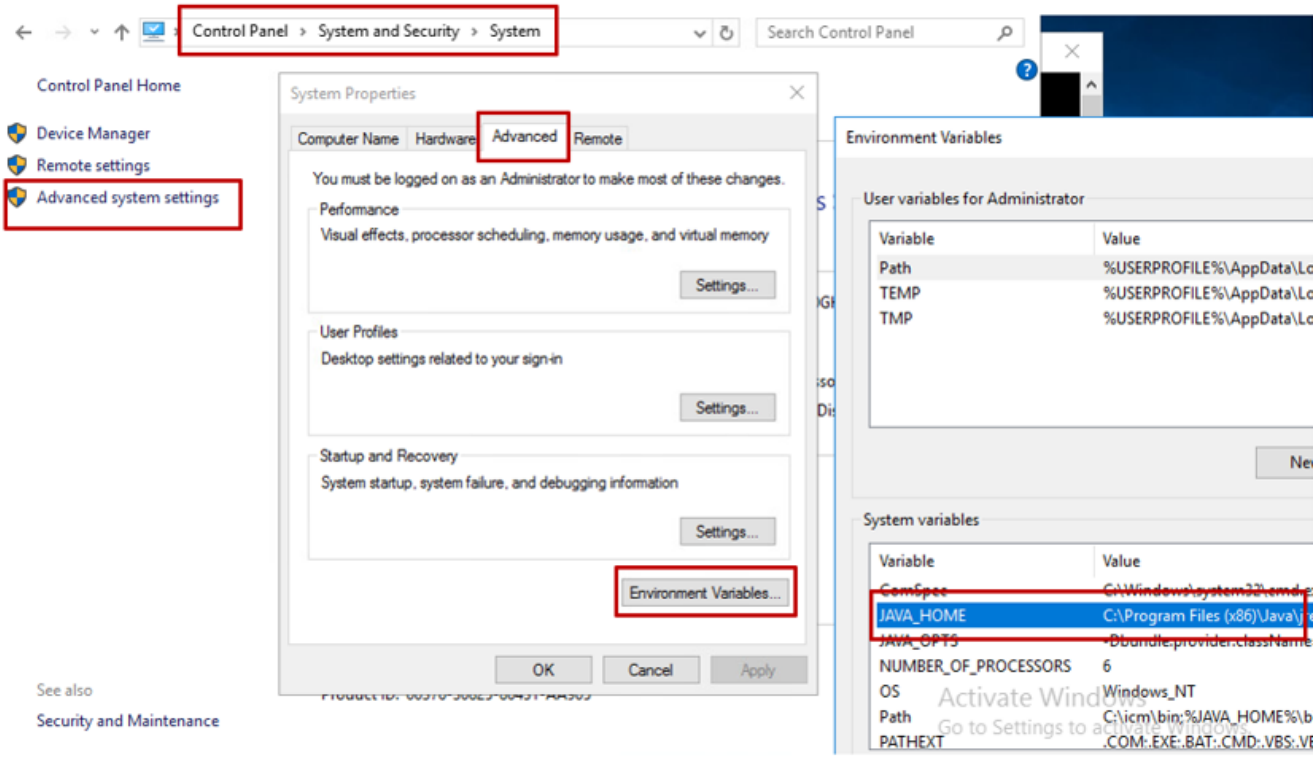
⚠ 注意：开始之前，您必须备份密钥库并以Administrator身份打开命令提示符。

1. 了解Java主路径以确保承载Java密钥工具的位置。您可以通过几种方法查找Java主路径。

   第 1 项.CLI命令： echo %JAVA_HOME%



   第 2 项.通过高级系统设置手动设置，如图所示。

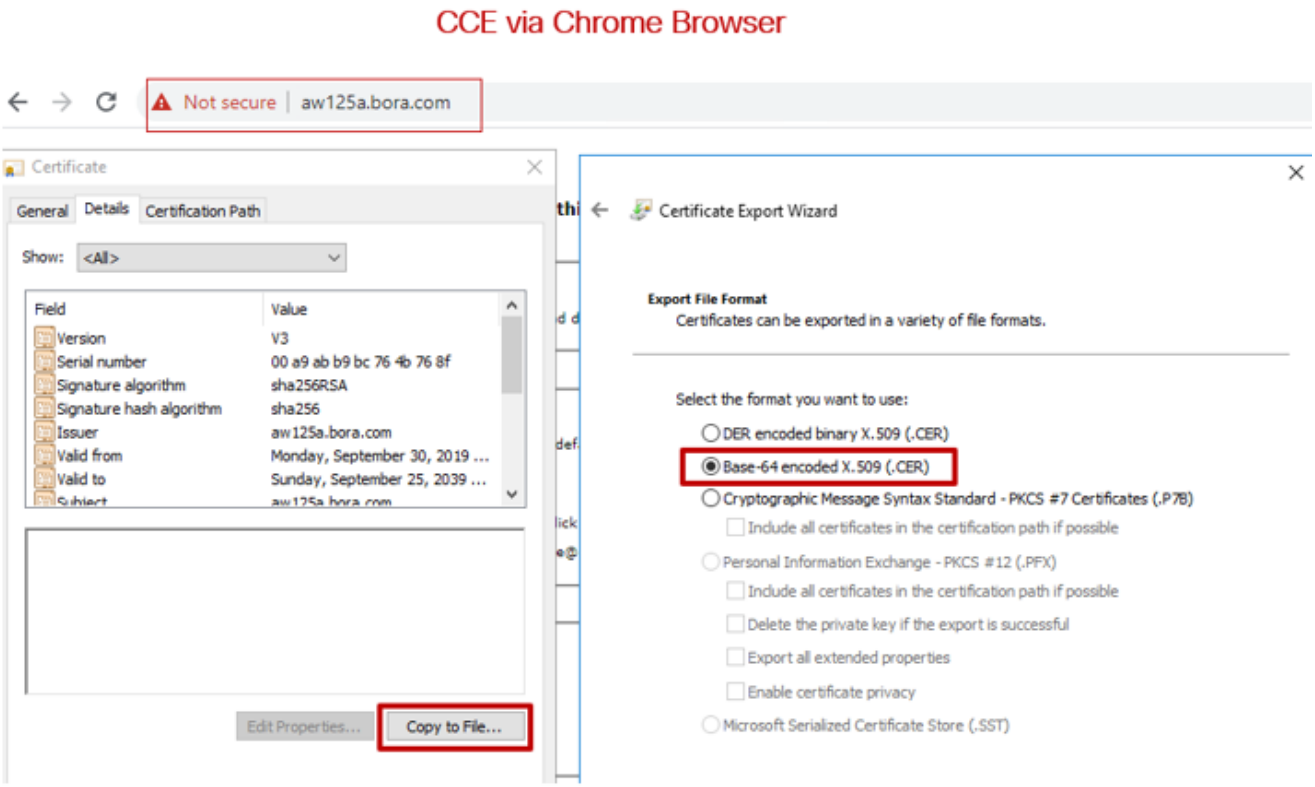


   ✎ 注：在UCCE 12.5上，默认路径为C:\Program Files (x86)\Java\jre1.8.0_221\bin。但是，如果您已使用12.5(1a)安装程序或安装了12.5 ES55（必备OpenJDK ES），则使用%CCE_JAVA_HOME%，而不是%JAVA_HOME%，因为数据存储路径已随OpenJDK一起更改。有关CCE和CVP中的OpenJDK迁移的详细信息，请参阅以下文档：在CCE 12.5(1)中安装和迁移到OpenJDK和在CVP 12.5(1)中安装和迁移到OpenJDK。

2. cacerts 从文件夹备份文{JAVA_HOME}\lib\security件。您可以将其复制到其他位置。

步骤1:从路由器\记录器、PG和所有AW服务器导出IIS证书。

1. 在浏览器的AW服务器上，导航至服务器（ROGGER、PG、其他AW服务器）URL:https://{servername}。

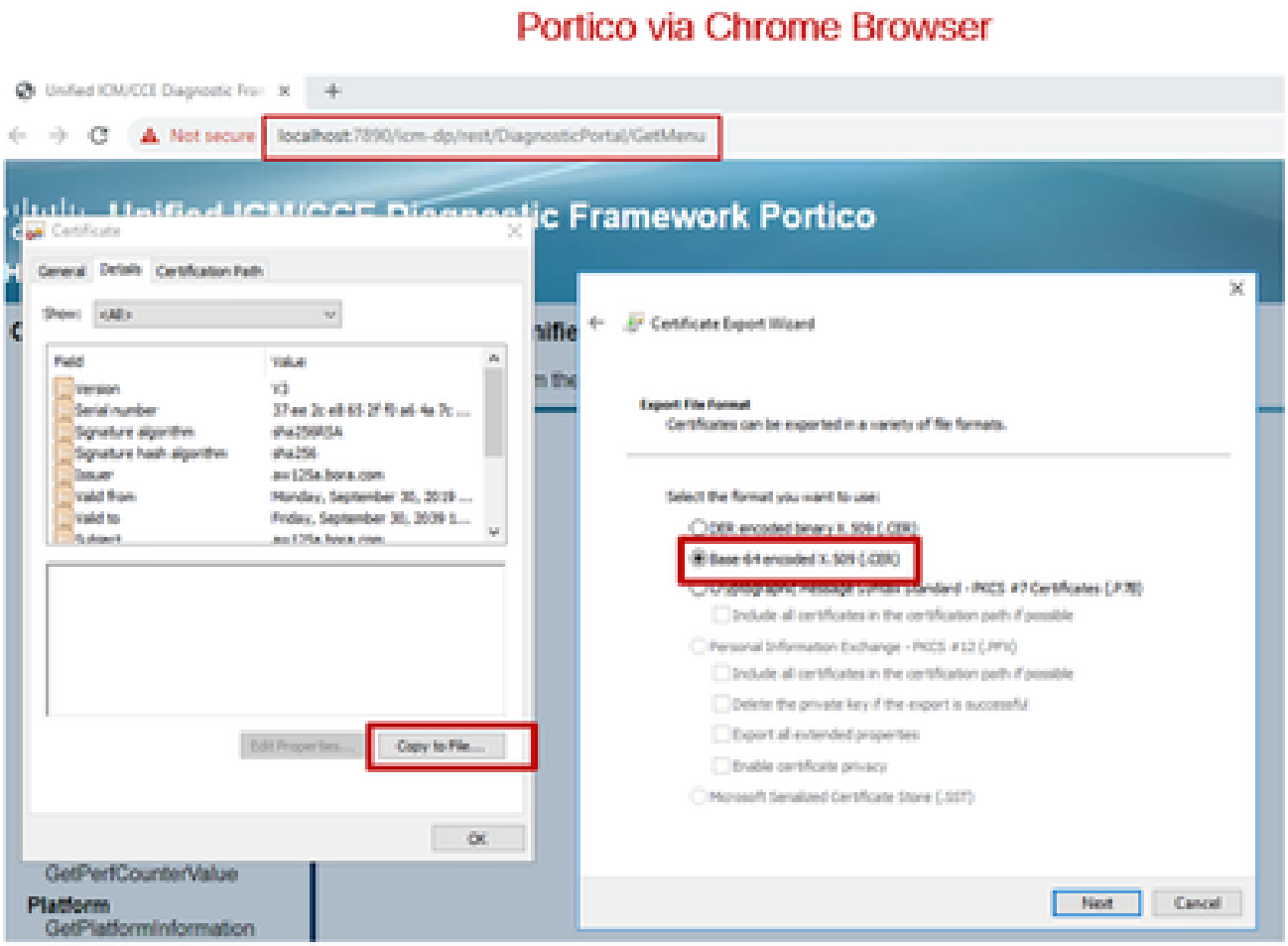


2. 例如，将证书保存到临时文件夹c:\temp\certs，并将证书命名为ICM{svr}[ab].cer。

注：选择选项Base-64 encoded X.509(.CER)。

第二步：从路由器\记录器、PG和所有AW服务器导出DFP证书。

1. 在AW服务器上，打开浏览器，然后导航到服务器（路由器、记录器或ROGER、PG和AW）DFP URL:https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion。



2. 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。

注：选择选项Base-64 encoded X.509(.CER)。

第三步：将IIS和DFP证书从Router\Logger、PG和AW导入AW服务器。

注意：示例命令使用默认的密钥库密码changeit。如果您已修改系统上的密码，则必须更改此项。

命令将IIS自签名证书导入AW服务器。运行keytool的路径为：%JAVA_HOME%\bin。

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com
```

注意：导入导出到所有AW服务器的所有服务器证书。

用于将DFP自签名证书导入AW服务器的命令：

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_DFP -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com
```

注意：导入导出到所有AW服务器的所有服务器证书。

在AW服务器上重新启动Apache Tomcat服务。

第四步：从AW服务器将IIS证书导入到Router\Logger和PG。

用于将AW IIS自签名证书导入路由器\记录器和PG服务器的命令：

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myawa.domain.com_
```

注意：导入导出到A端和B端的Router\Logger和PG服务器的所有AW IIS服务器证书。

在Router\Logger和PG服务器上重新启动Apache Tomcat服务。

2 节.VOS平台应用程序和AW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AW服务器。

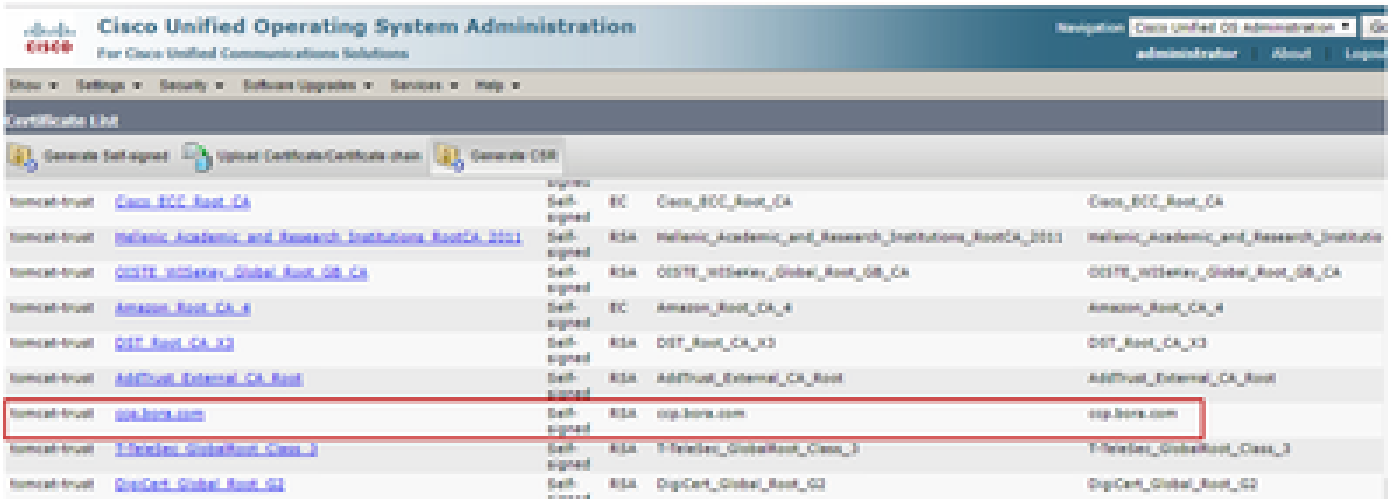
此过程适用于所有VOS应用，例如：

- Finesse
- CUIC\LD\IDS
- 云连接

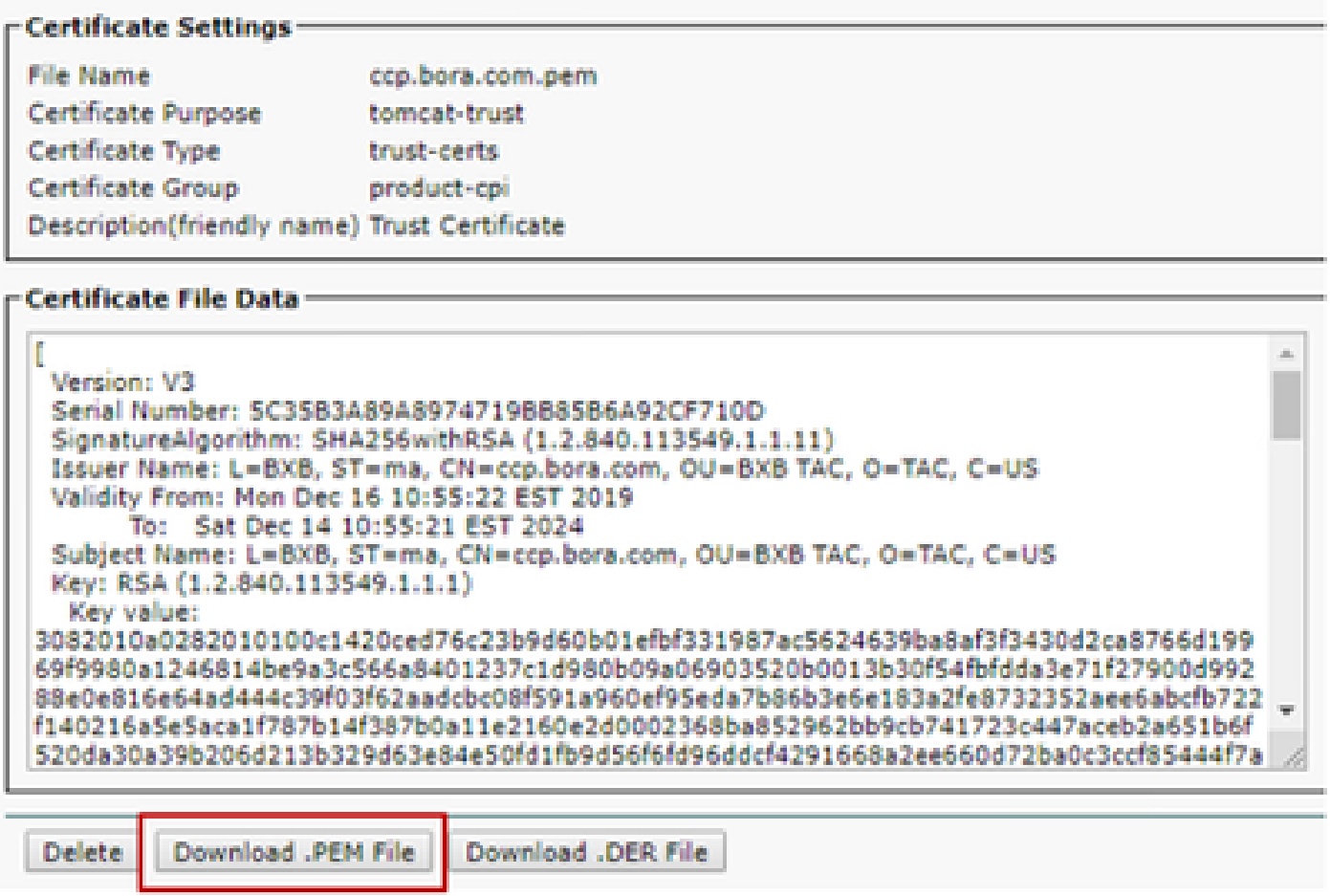
步骤1:导出VOS平台应用服务器证书。

i.导航至Cisco Unified Communications Operating System Administration页面 :https://{FQDN}:8443/cmplatform。

ii.导航至Security > Certificate Management，并在tomcat-trust文件夹中查找应用程序的主服务器证书。



iii.选择证书并单击Download .PEM File，以便将其保存在AW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平台应用导入AW服务器。

运行密钥工具的路径： {JAVA_HOME}\bin

用于导入自签名证书的命令：

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_vos} -file c:\tem
```

在AW服务器上重新启动Apache Tomcat服务。

注意：在其他AW服务器上执行相同的任务。

CVP OAMP服务器和CVP组件服务器

这些是导出自签名证书的组件和必须将自签名证书导入其中的组件。

i. CVP OAMP服务器：此服务器需要来自以下位置的证书：

- Windows平台：来自CVP服务器和报告服务器的Web服务管理器(WSM)证书。
- VOS平台：适用于客户虚拟代理(CVA)集成的思科VVB，适用于Webex体验管理(WXM)集成的云连接服务器。

ii. CVP服务器：此服务器需要来自以下位置的证书：

- Windows平台：OAMP服务器的WSM证书。
- VOS平台：适用于WXM集成的云连接服务器和Cisco VVB服务器。

iii. CVP报告服务器：此服务器需要以下证书：

- Windows平台：OAMP服务器的WSM证书。

iv. Cisco VVB服务器：此服务器需要来自以下位置的证书：

- Windows平台：CVP服务器的VXML证书和CVP服务器的Callserver证书。

以下三节介绍了在CVP环境中有效交换自签名证书所需的步骤。

1 节.CVP OAMP服务器与CVP服务器及报告服务器之间的证书交换。
2 节.CVP OAMP服务器和VOS平台应用之间的证书交换。
3 节.CVP服务器和VVB服务器之间的证书交换。

1 节.CVP OAMP服务器与CVP服务器及报告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CVP服务器、报告服务器和OAMP服务器导出WSM证书。
第二步：将WSM证书从CVP服务器和报告服务器导入OAMP服务器。
第三步：将CVP OAMP服务器WSM证书导入CVP服务器和报告服务器。

⚠ 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.要识别密钥库密码，请运行命令more %CVP_HOME%\conf\security.properties。
3.运行keytool命令时需要此密码。

⚠ 4.从目录%CVP_HOME%\conf\security\，运行命令，copy **.keystore backup.keystore**。

步骤1:从CVP服务器、报告服务器和OAMP服务器导出WSM证书。

i.将WSM证书从每台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wsmX.crt。将X替换为服务器的主机名。例如wsmcsa.crt、 wsmcsb.crt、 wsmrepa.crt、 wsmrepb.crtwsmoamp.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 -a
```

ii.从每台服务器的路径复制证书C:\Cisco\CVP\conf\security\wsm.crt，并根据服务器类型将其重命名wsmX.crt。

第二步：将WSM证书从CVP服务器和报告服务器导入OAMP服务器。

i.将WSM证书从每个CVP服务器和报告服务器(wsmX.crt)复制到%CVP_HOME%\conf\securityOAMP服务器上的目录。

ii.使用以下命令导入这些证书：

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

iii.重新启动服务器。

第三步：将WSM证书从CVP OAMP服务器导入CVP服务器和报告服务器。

i.将OAMP服务器WSM证书(wsmoampX.crt)复制到%CVP_HOME%\conf\security所有CVP服务器和报告服务器上的目录。

ii.使用命令导入证书：

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

iii.重新启动服务器。

2 节.CVP OAMP服务器和VOS平台应用之间的证书交换

成功完成此交换所需的步骤如下：

步骤1:从VOS平台导出应用证书。

第二步：将VOS应用证书导入OAMP服务器。

此过程适用于VOS应用，例如：

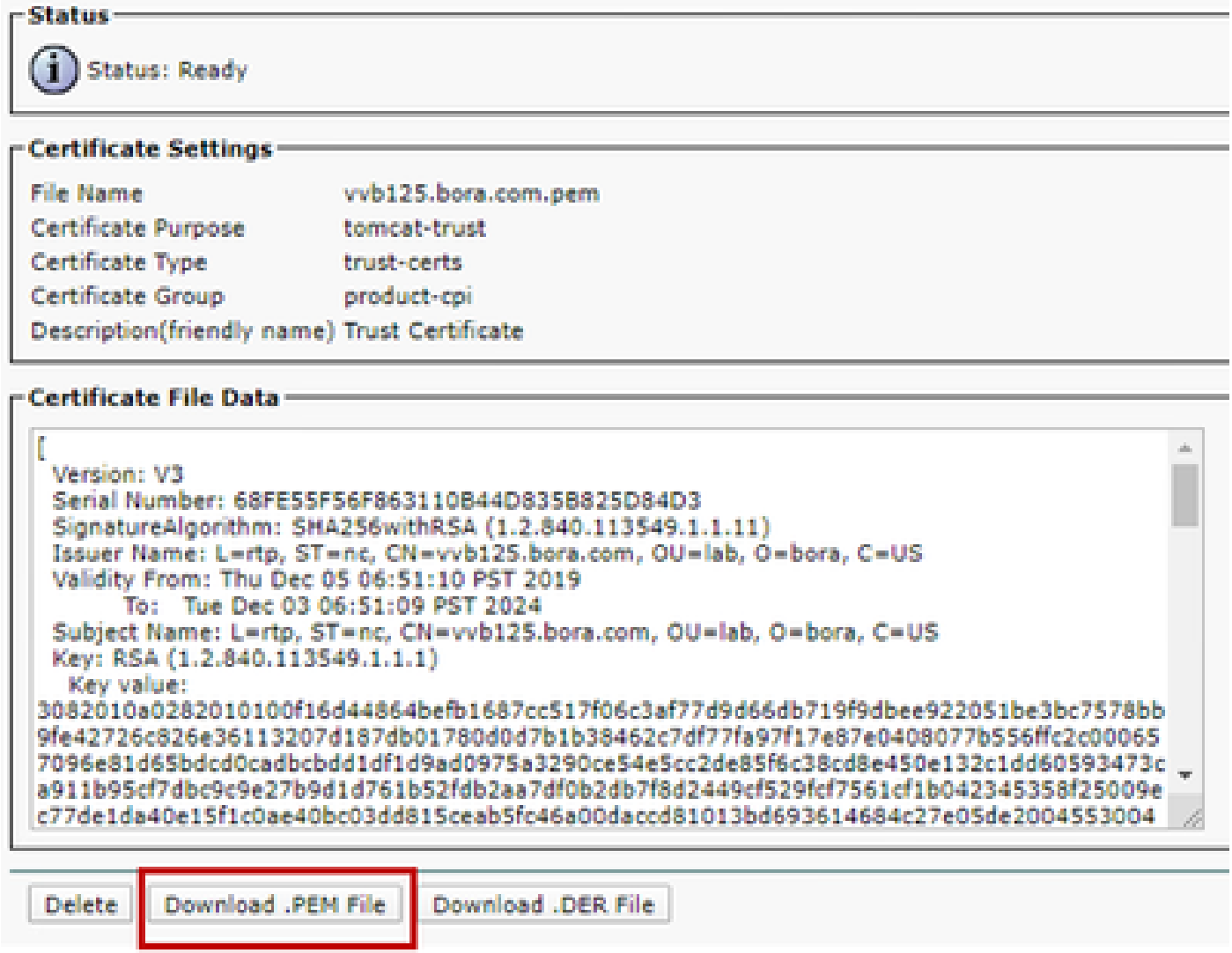
- CUCM
- VVB
- 云连接

步骤1:从VOS平台导出应用证书。

i.导航至Cisco Unified Communications Operating System Administration页面 :https://{FQDN}:8443/cmplatform。

ii.导航至Security > Certificate Management，并在tomcat-trust文件夹中查找应用程序的主服务器证书。

iii.选择证书并单击Download .PEM File，以便将其保存在OAMP服务器上的临时文件夹中。



第二步：将VOS应用证书导入OAMP服务器。

i.将VOS证书复制到%CVP_HOME%\conf\securityOAMP服务器上的目录。

ii.使用命令导入证书：

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

iii.重新启动服务器。

3 节.CVP服务器和VVB服务器之间的证书交换

这是确保CVP与其他联系中心组件之间的SIP通信安全的可选步骤。 有关详细信息, 请参阅 CVP配置指南： [CVP配置指南 — 安全](#).

CVP Call Studio 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12.5(1)- 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管理员指南 — 安全
- 交换PCCE自签名证书 — PCCE 12.5
- Exchange UCCE自签名证书 — UCCE 12.5
- 交换PCCE自签名证书 — PCCE 12.6
- 实施CA签名证书 — CCE 12.6
- CCE OpenJDK迁移
- CVP OpenJDK迁移
- 证书交换实用程序
- 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）。