管理PCCE组件证书以用于SPOG

目录

简介

本文档介绍如何将管理工作站(AW)自签名SSL证书交换到客户语音门户(CVP)、Finesse、思科企业聊天和电子邮件(ECE)、思科统一情报中心(CUIC)、思科身份服务(ID)和虚拟化语音浏览器(VB)软件包联络中心企业版(PCCE)单一玻璃板(SPOG)。

作者：Nagarajan Paramasivam和Robert Rogier，Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 套装/统一联系中心企业(PCCE/UCCE)
- VOS平台
- 证书管理
- 证书密钥库

使用的组件

本文档中的信息基于以下组件：

- 管理工作站(CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC、IDS
- VVB
- 思科ECE

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。

PCCE PCCE

新用户界面 — SPOG

Packaged CCE 12.0具有与其他联系中心应用相符的新用户界面。用户界面允许您通过一个应用配置解决方案。登录https://<IP Address>/cceadmin中的新Unified CCE Administration。<IP Address>是A端或B端Unified CCE AW或可选外部HDS的地址。

在此版本中，Unified CCE管理界面允许您配置：

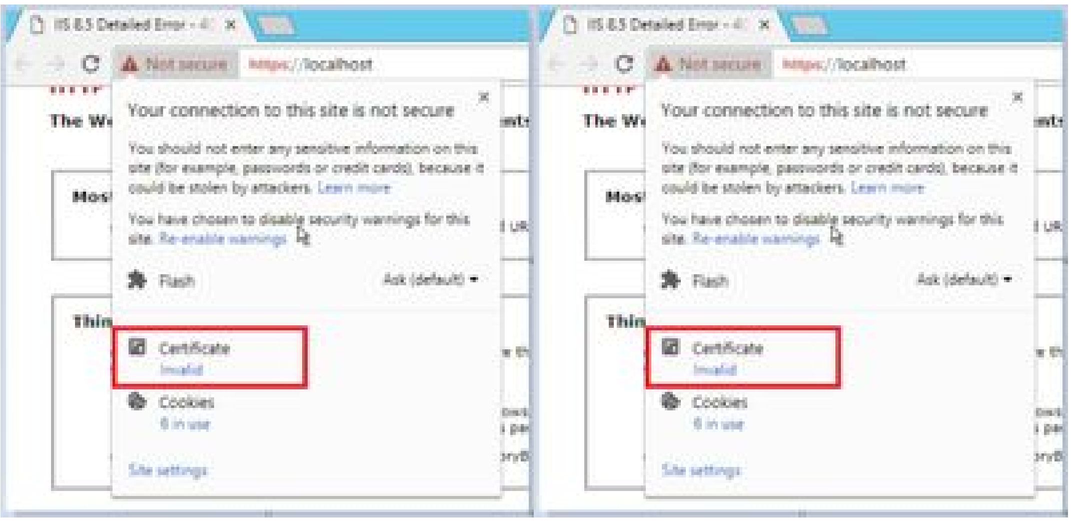
- 营销活动
- 礼貌回叫
- SIP服务器组
- 文件传输程序:仅可通过Principal AW(在2000代理部署中的A侧AW和在4000代理和12000代理部署中配置的AW)传输文件。
- 路由模式：Unified CVP操作控制台中的拨号号码模式现在在Unified CCE管理中称为路由模式。
- 位置：在Unified CCE管理中，路由代码现在是位置前缀，而不是站点ID。
- 设备配置:Unified CCE Administration允许您配置以下设备：CVP服务器、CVP报告服务器、VVB、Finesse、身份服务（单点登录设置）。
- 球队资源:Unified CCE Administration允许您为座席团队定义和关联以下资源：呼叫变量布局、桌面布局、电话簿、工作流程、原因（未就绪、注销、摘要）。
- 电子邮件和聊天

在尝试通过SPOG管理系统之前，必须在客户语音门户(CVP)、Finesse、思科企业聊天和电子邮件(ECE)、思科统一情报中心(CUIC)、思科身份服务(idS)和虚拟语音浏览器(VVB)之间交换SSL证书和管理工作站(AW)，以建立信任通信。

SSL证书导出

管理工作站(AW)

步骤1.访问AW服务器中的https://localhost URL，并下载服务器SSL证书。



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

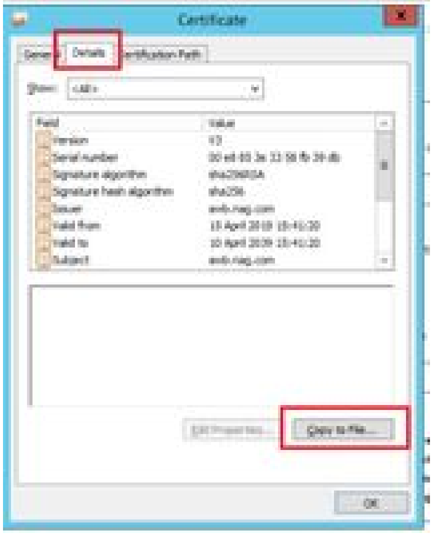
Flash: Ask (default)

Certificate: Invalid

Cookies: 6 in use

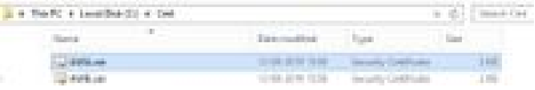
Site settings

步骤2.在证书窗口中，导航至“详细信息”选项卡，然后点击“复制到文件”按钮。



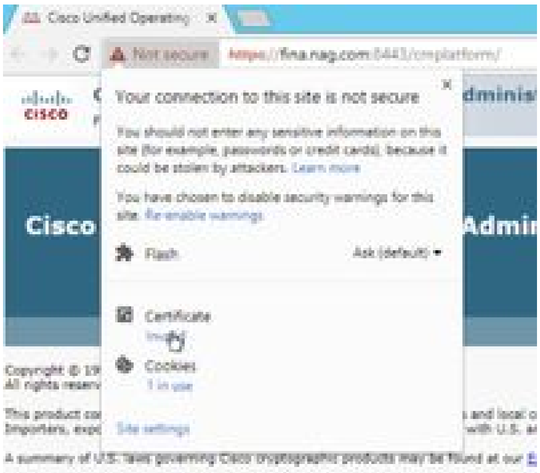
Field	Value
Version	V3
Serial number	00 e8 83 3e 33 58 fb 39 db
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	awb.nag.com
Valid from	15 April 2019 15:41:20
Valid to	10 April 2039 15:41:20
Subject	awb.nag.com

第3步：选择Base-64编码的X.509(CER)并将证书存储在本地存储中。



Finesse

步骤1.访问https://Finesseserver:8443/cmplatform并下载tomcat证书。



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

Flash: Ask (default)

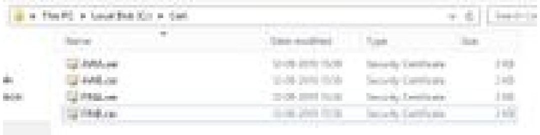
Certificate: Invalid

Cookies: 1 in use

Site settings

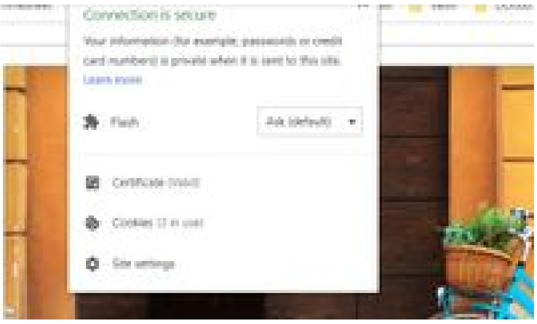
步骤2.在证书窗口中，导航至“详细信息”选项卡，然后点击“复制到文件”按钮。

步骤3.选择Base-64编码的X.509(CER)并将证书存储在本地存储中。



思科ECE

步骤1.访问https://ECEWebServer并下载服务器SSL证书。

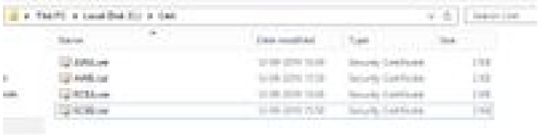


Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

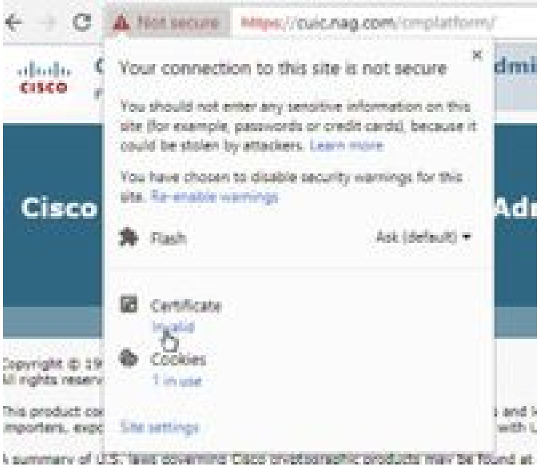
步骤2.在证书窗口中，导航至“详细信息”选项卡，然后点击“复制到文件”按钮。

步骤3.选择Base-64编码的X.509(CER)并将证书存储在本地存储中。



CUIC

步骤1.访问https://CUICServer:8443/cmplatform并下载tomcat证书。



Not secure https://cuic.nag.com/cmplatform/

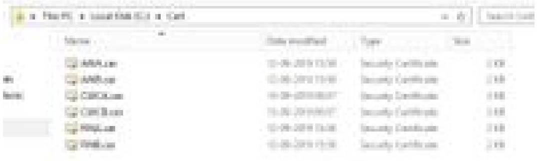
Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

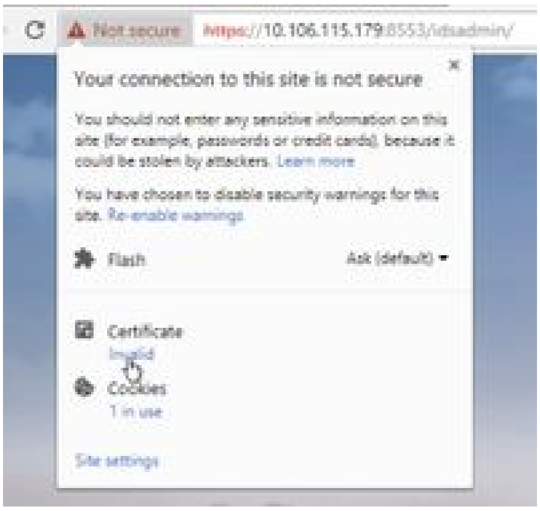
步骤2.在证书窗口中，导航至“详细信息”选项卡，然后点击“复制到文件”按钮。

步骤3.选择Base-64编码的X.509(CER)并将证书存储在本地存储中。



Cisco IDS

步骤1.访问https://IDSServer:8553/idsadmin/并下载tomcat证书。



Not secure https://10.106.115.179:8553/idsadmin/

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

Flash Ask (default)

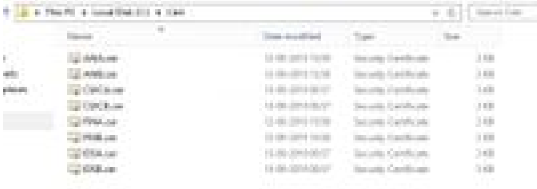
Certificate Invalid

Cookies 1 in use

Site settings

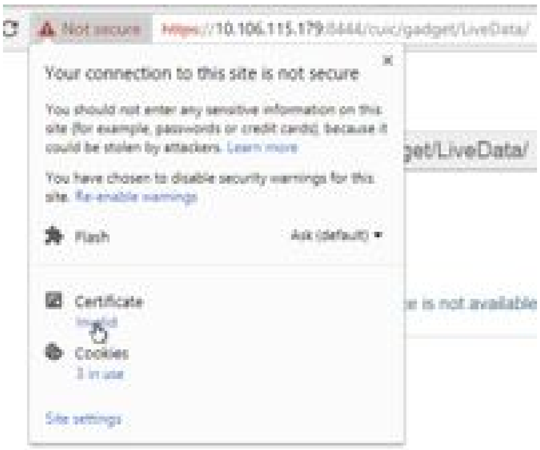
步骤2.在证书窗口中，导航至“详细信息”选项卡，然后点击“复制到文件”按钮。

步骤3.选择Base-64编码的X.509(CER)并将证书存储在本地存储中。



实时数据

步骤1.访问https://LiveDataServer:8444/cuic/gadget/LiveData/并下载tomcat证书。



Not secure https://10.106.115.179:8444/cuic/gadget/LiveData/

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

Flash Ask (default)

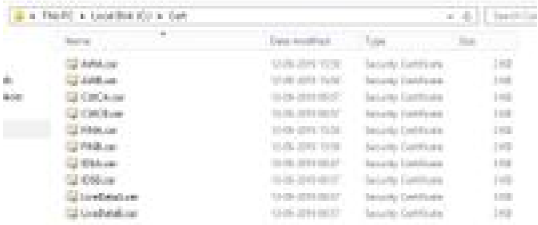
Certificate Invalid

Cookies 3 in use

Site settings

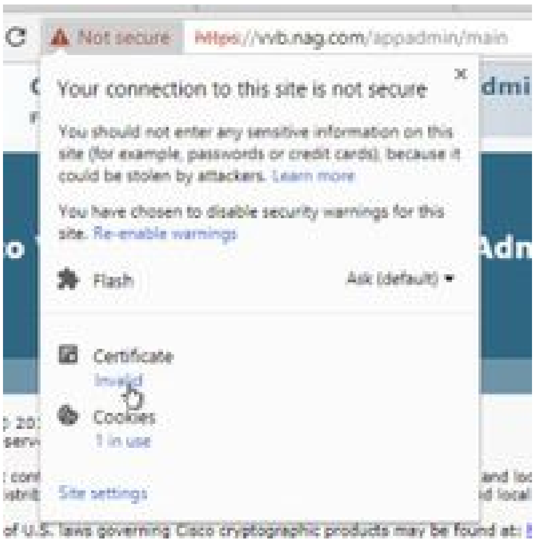
步骤2.在证书窗口中，导航至“详细信息”选项卡，然后点击“复制到文件”按钮。

步骤3.选择Base-64编码的X.509(CER)并将证书存储在本地存储中。



VVB

步骤1.访问https://VVBServer/appadmin/main并下载tomcat证书。



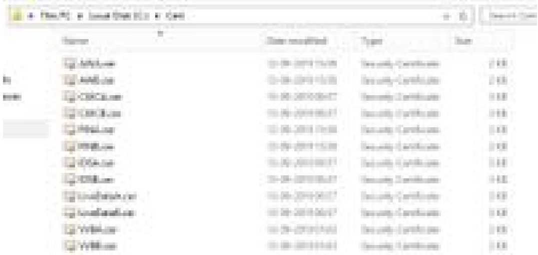
Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to disable security warnings for this site. Re-enable warnings

步骤2.在证书窗口中，导航至“详细信息”选项卡，然后点击“复制到文件”按钮。

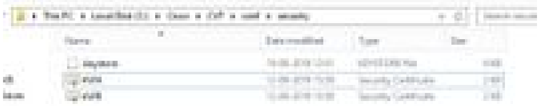
步骤3.选择Base-64编码的X.509(CER)并将证书存储在本地存储中。



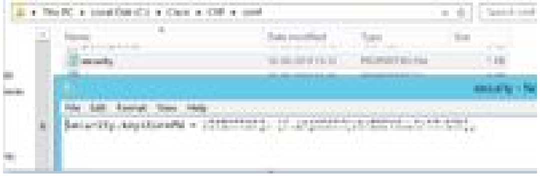
SSL证书导入到密钥库

CVP呼叫服务器和报告服务器

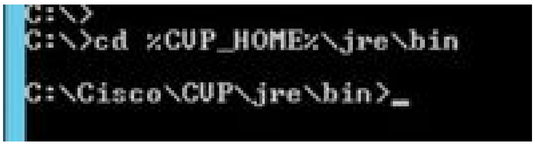
步骤1.登录CVP服务器，并将AW CCE管理员证书复制到**C:\cisco\cvp\conf\security**。



步骤2.导航到**%CVP_HOME%\conf\**并打开security.properties以复制密钥库密码。



步骤3.以管理员身份打开命令提示符并运**行命令cd %CVP_HOME%\jre\bin**。



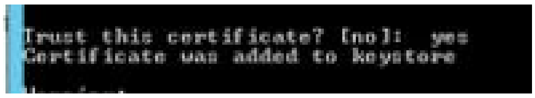
```
C:\>
C:\>cd %CVP_HOME%\jre\bin

C:\Cisco\CVP\jre\bin>_
```

步骤4.使用此命令将AW证书导入CVP服务器。

keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias awa.nag.com -file C:\Cisco\CVP\conf\security\AWA.cer

步骤5.在密码提示符下，粘贴从security.properties复制的密码。

步骤6.键入**yes**以信任证书，并确保您获得**证书已添加到密钥库。**



```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

步骤7.导入成功后，系统会提示警告。这是由专有格式密钥库造成的，您可以忽略它。

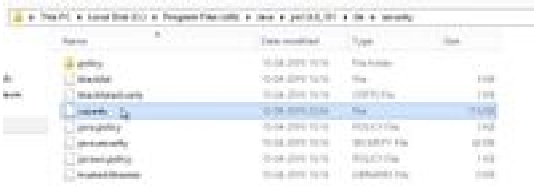
警告：

JCEKS密钥库使用专有格式。建议迁移到PKCS12，该格式是使用“keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore -deststoretype pkcs12”的行业标准格式。

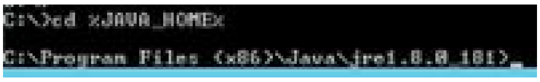
管理工作站

步骤1.以管理员身份登录AW服务器并打开命令提示符。

步骤2.导航至C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist。



步骤3.键入命令**cd %JAVA_HOME%**并输入。



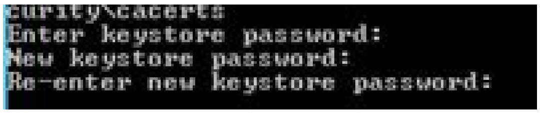
```
C:\>cd %JAVA_HOME%

C:\Program Files (x86)\Java\jre1.8.0_181>_
```

步骤4.使用此命令将Finesse证书导入AW服务器。

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias fina.nag.com-keystore .\lib\security\cacerts

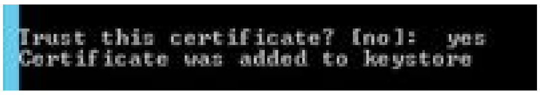
步骤5.首次使用此密钥工具时，请使用密码**changeit**以更改证书存储的密码。

步骤6.输入密钥库的新密码，然后重新输入以确认密码。



```
curity\cacerts
Enter keystore password:
New keystore password:
Re-enter new keystore password:
```

步骤7.键入**yes**以信任证书，并确保您获得结果Certificate was added to keystore。



```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

注意：第1步到第7步应与所有其他Finesse节点和所有CUIC节点重复

步骤8.如果密钥库密码输入错误或执行了步骤而未重置，则预期会出现此异常。

信任此证书？[no] ： 是

证书已添加到密钥库

键具错误：java.io.FileNotFoundException:.\lib\security\cacerts （系统找不到指定的路径）

输入密钥库密码：
键具错误：java.io.IO异常：密钥库被篡改，或密码不正确

步骤9.要更改密钥库密码，请使用此命令，然后使用新密码从步骤4再次重新启动该过程。

keytool -storepasswd -keystore .\lib\security\cacerts

步骤10.成功导入后，使用此命令从密钥库查看证书。

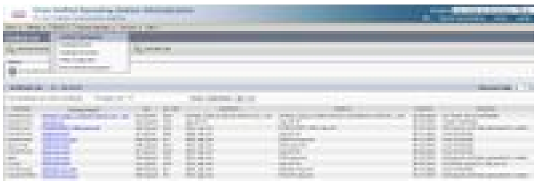
keytool -list -keystore .\lib\security\cacerts -alias fina.nag.com

keytool -list -keystore .\lib\security\cacerts -alias cuic.nag.com

Finesse、CUIC、Cisco idS和VVB

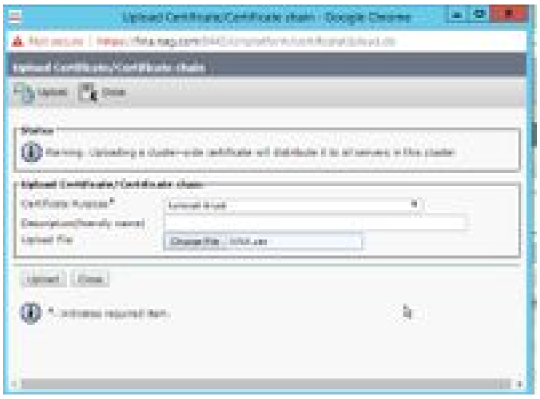
步骤1.登录到Finesse服务器OS管理页，并在tomcat信任中上传AW SSL证书。

步骤2.导航至OS Administration **> Security > Certificate Management。**



步骤3.点击Upload Certificate\Certificate Chain（上传证书\证书链），然后从下拉列表中选择tomcat-trust。

步骤4.浏览本地存储中的证书存储，然后点击Upload按钮。



步骤5.重复上述步骤，将所有AW服务器证书上传到Finesse群集。

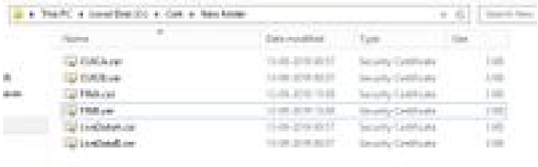
tomcat-trust

步骤6.重新启动tomcat服务，使证书更改生效。

步骤7.在CUIC、IDS和VVB中，按照2到4的步骤操作并上传AW证书。

Finesse和CUIC/LiveData之间的证书交换

步骤1.将Finesse、CUIC和LiveData证书保留在单独的文件夹中。



2.FinesseCUIC和LiveData OS管理页。

步骤3.导航至OS Administration **> Security > Certificate Management。**

步骤4.点击Upload Certificate\Certificate Chain（上传证书\证书链）并从下拉列表中选择tomcat-trust。

步骤5.浏览本地存储中的证书存储并选择Einer servers certificate，如下所示，然后点击Upload按钮。

在Finesse服务器中 — CUIC和LiveData作为Tomcat信任

在CUIC服务器中 — Finesse和LiveData作为tomcat信任

在LiveData Server - CUIC和Finesse作为Tomcat信任

> **注意：**无需将tomcat-trust证书上传到辅助节点，此操作会自动复制。

步骤6.在每个节点上重新启动tomcat服务，使证书更改生效。