在PCCE解決方案中交換自簽名證書

目錄

簡介

本檔案介紹如何在Cisco Packaged Contact Center Enterprise(PCCE)解決方案中的主體管理伺服器(ADS/AW)和其他應用伺服器之間交換自簽署憑證。

作者：Anuj Bhatia、Robert Rogier和Ramiro Amaya，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- PCCE版本12.5(1)
- 客戶語音入口網站(CVP)版本12.5(1)

採用元件

本檔案中的資訊是根據以下軟體版本：

- PCCE 12.5(1)
- CVP 12.5(1)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

在12.x的PCCE解決方案中，所有裝置都通過主用AW伺服器中託管的單一窗格(SPOG)進行控制。由於PCCE 12.5(1)版本中的安全管理合規性(SRC)，解決方案中SPOG和其他伺服器之間的所有通訊都通過安全的HTTP協定嚴格完成。

證書用於實現SPOG與其他裝置之間的無縫安全通訊。在自簽名證書環境中，伺服器之間的證書交換成為必需。要啟用12.5(1)版本中的新功能(如智慧許可、Webex體驗管理(WXM)和客戶虛擬助理(CVA))，也需要交換證書。

程式

這些是匯出自簽名證書的元件和需要將自簽名證書匯入其中的元件。

(i)主要AW伺服器：此伺服器需要來自以下位置的證書：

- Windows平台： ICM: 路由器和記錄器（記錄器）{A/B}、外圍網關(PG){A/B}、所有ADS以及電子郵件和聊天(ECE)伺服器。 附註：需要IIS和診斷框架證書。CVP:CVP伺服器、CVP報告伺服器。 附註1:需要來自伺服器的Web服務管理(WSM)證書。附註2:證書必須具有完全限定的域名(FQDN)。
- VOS平台：Cloud Connect、Cisco Virtual Voice Browser(VVB)、Cisco Unified Call Manager(CUCM)、Finesse、Cisco Unified Intelligent Center(CUIC)、Live Data(LD)、Identity Server(IDS)以及其他適用伺服器。

這同樣適用於解決方案中的其他ADS伺服器。

(ii)路由器\記錄器伺服器：此伺服器需要來自以下位置的證書：

- Windows平台： 所有ADS伺服器IIS證書。

(iii)CUCM PG伺服器：此伺服器需要來自以下位置的證書：

- VOS平台：CUCM發佈程式。 附註：從CUCM伺服器下載JTAPI客戶端時需要執行此操作。

(iv)CVP伺服器：此伺服器需要來自的證書

- Windows平台： 所有ADS伺服器IIS證書
- VOS平台：適用於WXM整合的雲連線伺服器、適用於安全SIP和HTTP通訊的VVB伺服器。

(v)CVP報告伺服器：此伺服器需要來自以下位置的證書：

- Windows平台： 所有ADS伺服器IIS證書

(vi)VVB伺服器：此伺服器需要來自以下位置的證書：

- Windows平台：CVP VXML伺服器（安全HTTP）、CVP呼叫伺服器（安全SIP）

在解決方案中，有效交換自簽名證書所需的步驟分為三部分。

第1部分：CVP伺服器和ADS伺服器之間的證書交換。

第2部分：VOS平台應用和ADS伺服器之間的證書交換。

第3部分：Rogers、PG和ADS伺服器之間的證書交換。

第1部分：CVP和ADS伺服器之間的證書交換

成功完成此交換所需的步驟為：

步驟1.匯出CVP伺服器WSM證書。

步驟2.將CVP伺服器WSM證書匯入ADS伺服器。

步驟3.匯出ADS伺服器證書。

步驟4.將ADS伺服器匯入CVP伺服器和CVP報告伺服器。

步驟1.匯出CVP伺服器證書

從CVP伺服器匯出證書之前，您需要使用伺服器的FQDN重新生成證書，否則，智慧許可、CVA以及與SPOG同步的CVP等功能很少會遇到問題。

> **注意**：開始之前，必須執行以下操作：

- 獲取金鑰庫密碼。運行此命令：
  更多%CVP_HOME%\conf\security.properties
- 將%CVP_HOME%\conf\security資料夾複製到另一個資料夾。
- 以管理員身份開啟「命令」視窗以運行命令。

> **附註**：您可以使用keytool引數 — storepass簡化本文檔中使用的命令。對於所有CVP伺服器，請貼上從指定的security.properties檔案獲取的密碼。對於ADS伺服器，請鍵入密碼：**更改**

要在CVP伺服器上重新生成證書，請執行以下步驟：

(i)列出伺服器中的證書

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

> **附註**：CVP伺服器具有以下自簽名證書：wsm_certificate 、 vxml_certificate 、 callserver_certificate。如果使用keytool的引數 — v，則可以看到每個證書的更多詳細資訊。此外，您還可以在keytool.exe list命令末尾新增「>」符號，以將輸出傳送到文本檔案，例如： > test.txt

(ii)刪除舊的自簽證書

CVP伺服器：用於刪除自簽名證書的命令：

```
%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報告伺服器：刪除自簽名證書的命令：

```
%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
```

附註：CVP報告伺服器具有以下自簽名證書wsm_certificate和callserver_certificate。

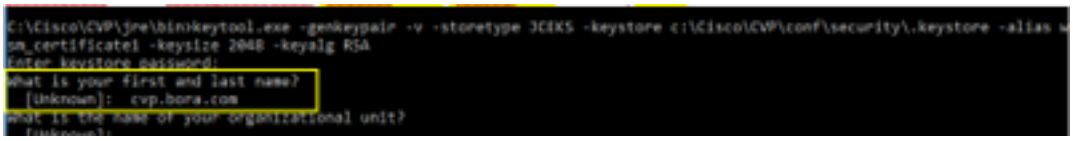
(iii)使用伺服器的FQDN生成新的自簽名證書

CVP伺服器

用於為WSM生成自簽名證書的命令：

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

指定伺服器的FQDN，在問**題中您的名字和姓是什麼**?



請完成以下其他問題：

您的組織單位名稱是什麼？

[未知]:<指定OU>

貴公司的名稱是什麼？

[未知]:<指定組織的名稱>

您的城市或地區名稱是什麼？

[未知]:<指定城市/地區名稱>

您所在州或省的名稱是什麼？

[未知]:<指定州/省的名稱>

此裝置的國碼（兩個字母）是什麼？

[未知]:<指定兩個字母的國家/地區代碼>

為接下來的兩個輸入指定**yes**。

對vxml_certificate和callserver_certificate執行相同的步驟：

```
%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
```

重新啟動CVP呼叫伺服器。

CVP報告伺服器

用於為WSM生成自簽名證書的命令：

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

為查詢指定伺服器FQDN，**您的名字和姓是什麼？**並遵循與CVP伺服器相同的步驟。

對callserver_certificate執行相同步驟：

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

重新啟動報表伺服器。

> **附註**：預設情況下，自簽名證書生成長達兩年。使用 — validity XXXX設定重新生成證書時的到期日期，否則證書的有效期為90天。對於大多數此類證書，3-5年必須是合理的驗證時間。

以下是一些標準有效性輸入：

一年	365
兩年	730
三年	1095
四年	1460
五年	1895
十年	3650

> **注意**：在12.5證書中，必須是**SHA 256**、金鑰大小**2048**和加密演算法**RSA**，請使用以下引數設定這些值：-keyalg RSA和 — keysize 2048。CVP金鑰庫命令必須包括 — storetype JCEKS引數。如果不這樣做，則證書、金鑰或更糟的金鑰庫可能會損壞。

(iv)從CVP和報告伺服器匯出wsm_Certificate

a)將WSM證書從每個CVP伺服器匯出到臨時位置，並使用所需的名稱重新命名證書。您可以將其重新命名為wsmcsX.crt。將「X」替換為唯一數字或字母。即wsmcsa.crt、wsmcsb.crt。

用於匯出自簽名證書的命令：

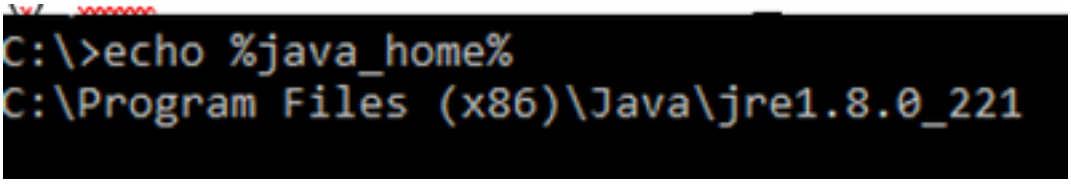
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b)從路徑**C:\Cisco\CVP\conf\security\wsm.crt**複製憑證，並將其重新命名為**wsmcsX.crt**，並將其移到ADS伺服器上的臨時資料夾。

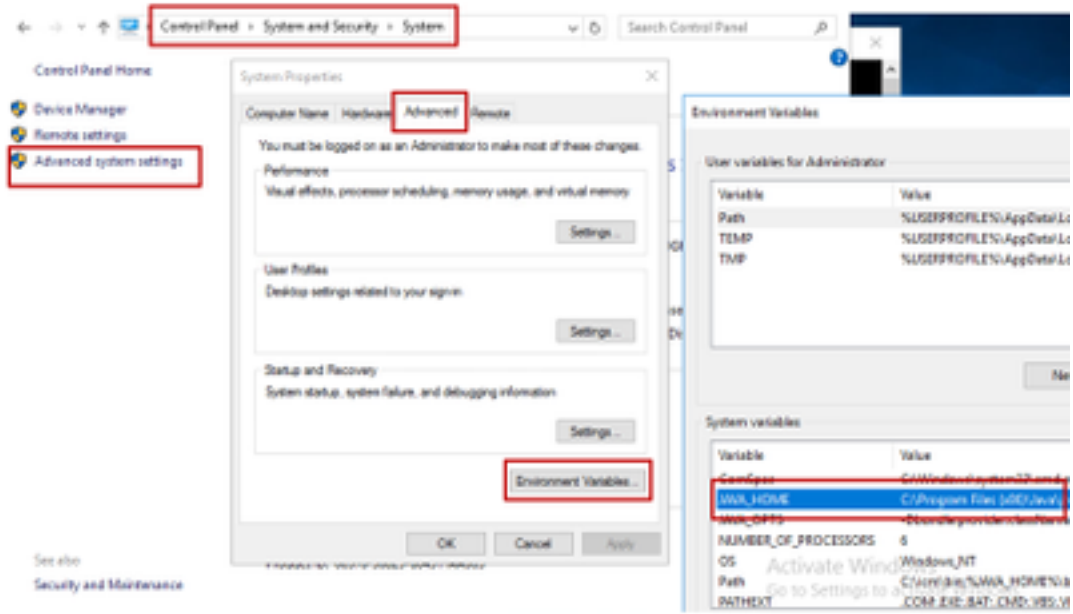
步驟2.將CVP伺服器WSM證書匯入ADS伺服器

要在ADS伺服器中匯入證書，您需要使用keytool，該工具是java工具集的一部分。可以通過幾種方法找到此工具所在的java home路徑。

(i)CLI命令> **echo %JAVA_HOME%**



(ii)手動通過**高級系統設置**，如下圖所示。



在PCCE 12.5上，預設路徑為**C:\Program Files(x86)\Java\jre1.8.0_221\bin**

用於匯入自簽名證書的命令：

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_cvp} -file c:\temp\certs\wsmcsX.crt
```

附註：對部署中的每個CVP重複命令並在其他ADS伺服器上執行相同任務

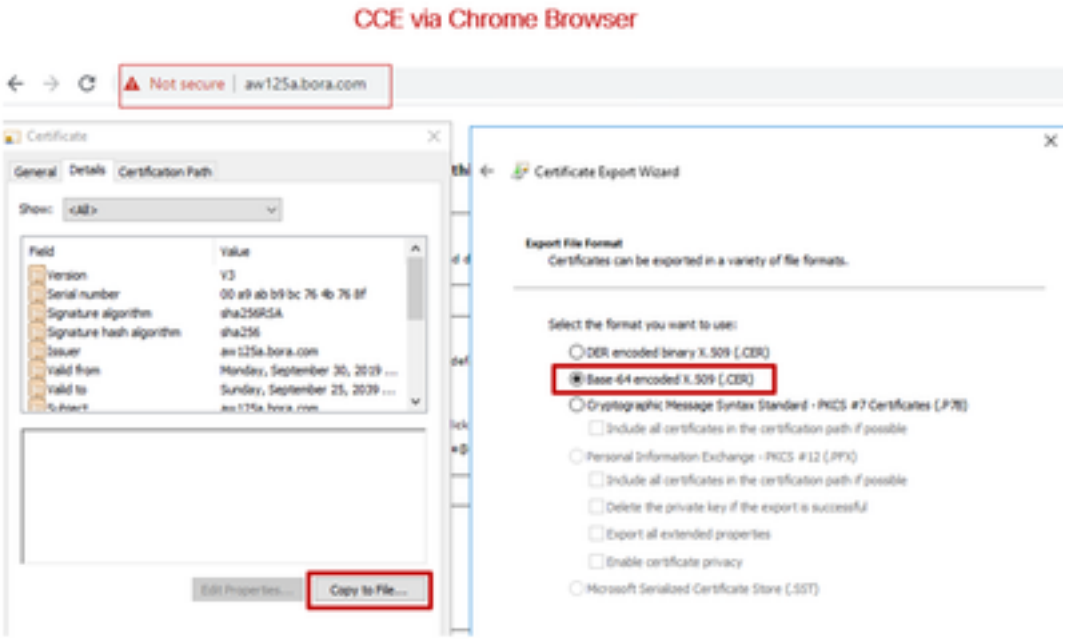
d)在ADS伺服器上重新啟動Apache Tomcat服務。

步驟3.匯出ADS伺服器證書

對於CVP報告伺服器，您必須匯出ADS證書並將其匯入報告伺服器。以下是步驟：

(i)在瀏覽器的ADS伺服器上，導航到伺服器url: **https://{servername}**

(ii)將憑證儲存到臨時資料夾中，例如：**c:\temp\certs**並將證書命**名為ADS{svr}[ab].cer**



附註：選擇Base-64 encoded X.509(.CER)選項。

步驟4.將ADS伺服器匯入CVP伺服器和報告伺服器

(i)將證書複製到C:\Cisco\CVP\conf\security目錄中的CVP伺服器和CVP報告服**務器。**

(ii)將證書匯入到CVP伺服器和CVP報告伺服器。

```
%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\ICM{svr}[ab].cer
```

對其他ADS伺服器執行相同步驟。

(iii)重新啟動CVP伺服器和報告伺服器

第2部分：VOS平台應用和ADS伺服器之間的證書交換

成功完成此交換所需的步驟為：

步驟1.匯出VOS平台應用伺服器證書。

步驟2.將VOS平台應用證書匯入ADS伺服器。

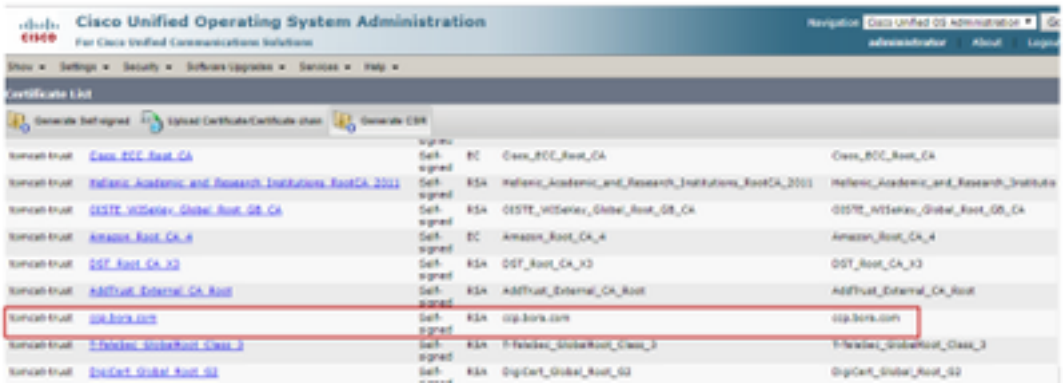
此過程適用於所有VOS應用程式，例如：

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- 雲端連線

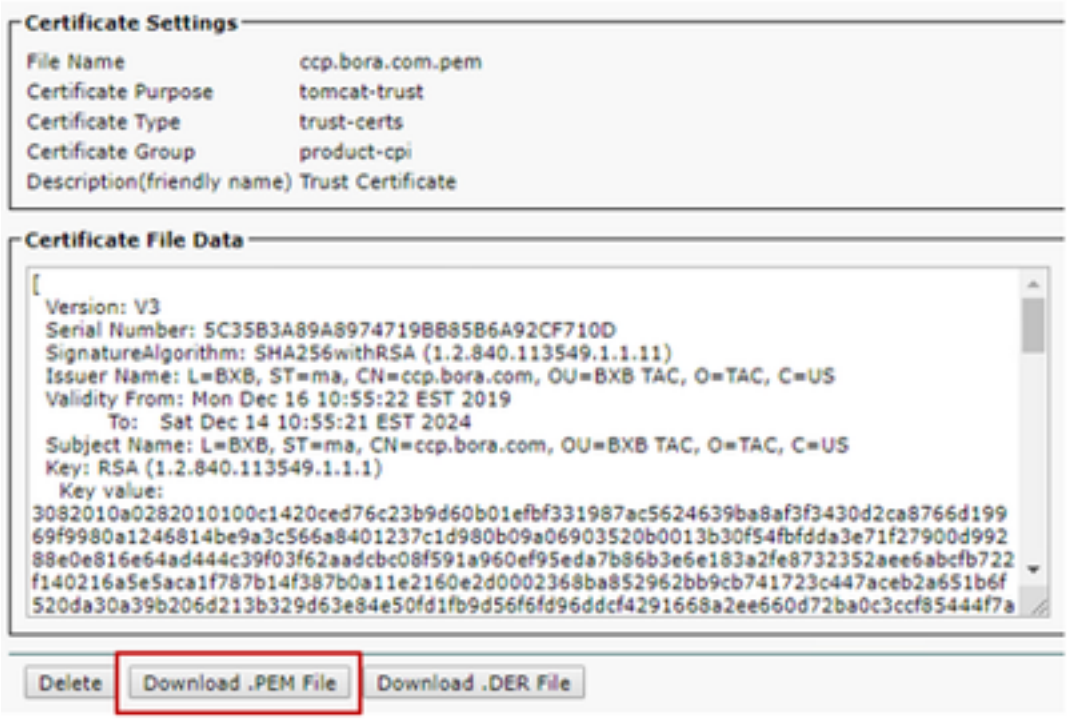
步驟1.匯出VOS平台應用伺服器證書。

(i)導航至Cisco Unified Communications Operating System Administration頁面：https://FQDN:8443/cmplatform

(ii)導航到**Security > Certificate Management**，然後在**tomcat-trust資料夾中查詢應用程式主伺服器證書**。



(iii)選擇證書並按一下download .PEM file（下載.PEM檔案），將其儲存在ADS伺服器上的臨時資料夾中。



附註：對使用者執行相同步驟。

步驟2.將VOS平台應用程式匯入ADS伺服器

運行Key工具的路徑：**C:\Program檔案(x86)\Java\jre1.8.0_221\bin**

用於匯入自簽名證書的命令：

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_vos}  -file c:\temp\certs\vosapplicationX.cer
```

在ADS伺服器上重新啟動Apache Tomcat服務。

附註：在其他ADS伺服器上執行相同任務

第3部分：Rogers、PG和ADS伺服器之間的證書交換

成功完成此交換所需的步驟為：

第1步：從羅傑和PG伺服器匯出IIS證書

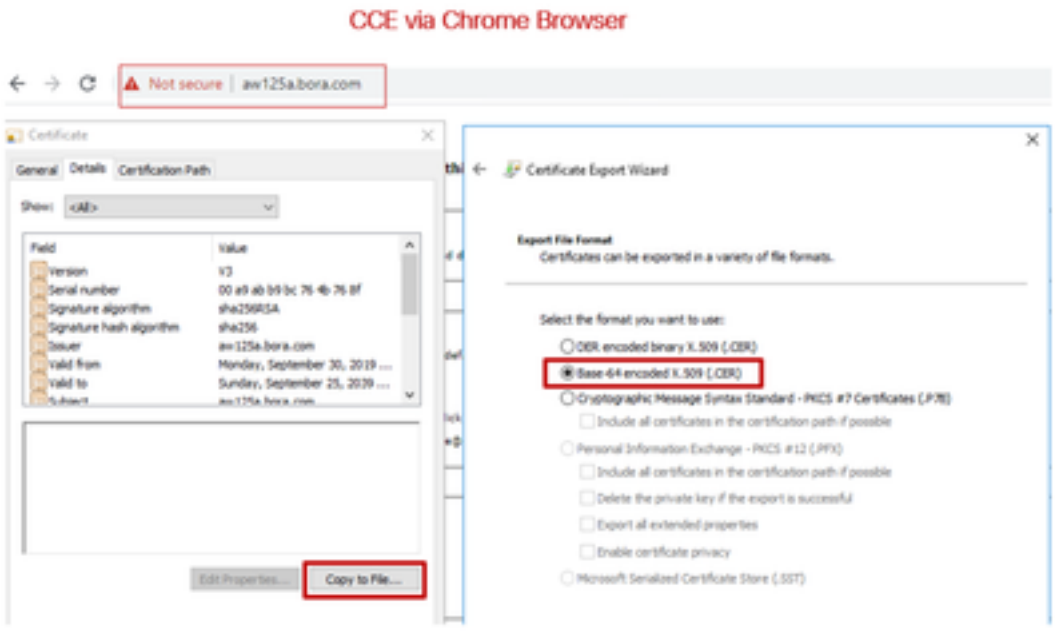
第2步：從記錄器和PG伺服器匯出診斷框架門戶(DFP)證書

步驟3:將證書匯入到ADS伺服器

步驟1.從Rogger和PG伺服器匯出IIS證書

(i)在瀏覽器的ADS伺服器上，導航到伺服器(Rogers， PG)url: **https://{servername}**

(ii)將憑證儲存到臨時資料夾，例如**c:\temp\certs，並將憑證命名為ICM{svr}[ab].cer**

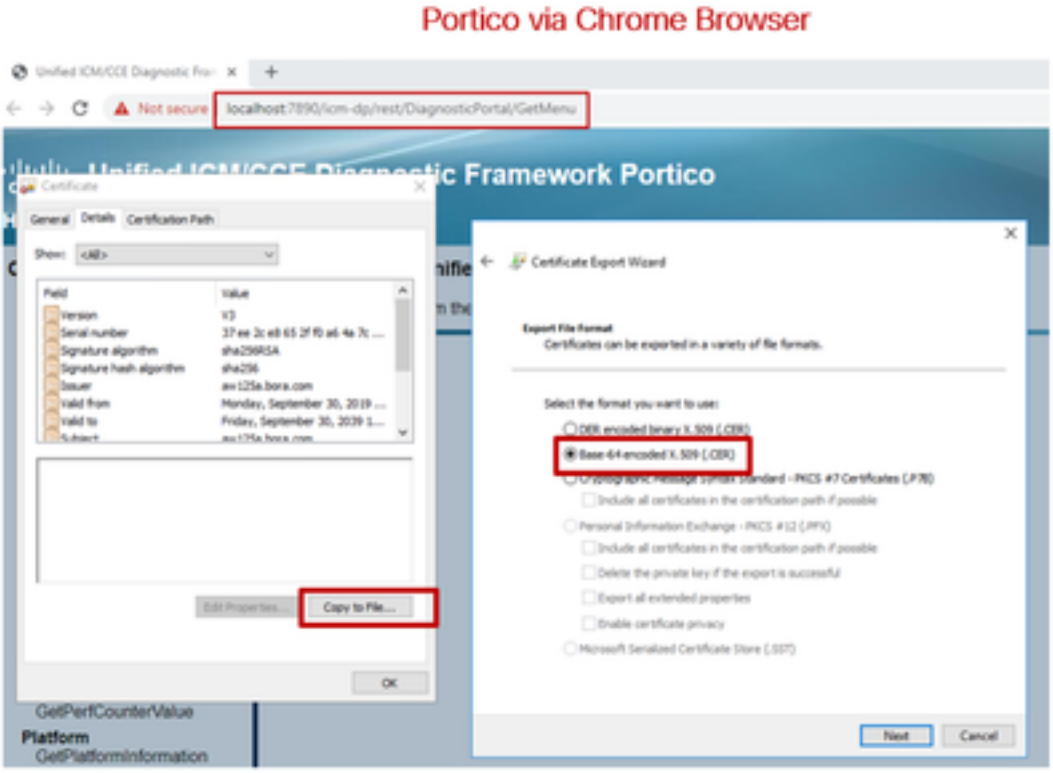


附註：選擇Base-64 encoded X.509(.CER)選項。

步驟2.從記錄器和PG伺服器匯出診斷框架Portico(DFP)證書

(i)在瀏覽器的ADS伺服器上，導航到伺服器(Rogers， PGs)DFP url : *https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion*

(ii)將證書儲存到資料夾示例c:\temp\certs，並將證書命名為dfp{svr}[ab].cer



附註：選擇Base-64 encoded X.509(.CER)選項。

步驟3.將證書匯入ADS伺服器

命令將IIS自簽名證書匯入ADS伺服器。運行Key工具的路徑：**C:\Program檔案(x86)\Java\jre1.8.0_221\bin。**

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}[ab].cer

Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -
import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer
```

附註： 匯入匯出到所有ADS伺服器的所有伺服器證書。

用於將診斷自簽名證書匯入到ADS伺服器的命令

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_server}_DFP -file c:\temp\certs\ dfp{svr}[ab].cer

Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -
import -storepass changeit -alias myrgra.domain.com_DFP -file c:\temp\certs\dfprgra.cer
```

附註：匯入匯出到所有ADS伺服器的所有伺服器證書。

在ADS伺服器上重新啟動Apache Tomcat服務。

第4部分：CVP CallStudio WEB服務整合

有關如何為Web服務元素和Rest_Client元素建立安全通訊的詳細資訊

請參閱Cisco Unified CVP VXML伺服器和Cisco Unified Call Studio 12.5(1)版 — Web服務整合 [Cisco Unified Customer Voice Portal] - Cisco使用手冊

相關資訊

- CVP配置指南：CVP配置指南 — 安全
- UCCE配置指南：UCCE配置指南 — 安全
- PCCE管理指南：PCE管理員指南 — 安全
- UCCE自簽名證書：Exchange UCCE自簽名證書
- 在CCE 12.5(1)中安裝和遷移到OpenJDK:CCE OpenJDK遷移
- 在CVP 12.5(1)中安裝和遷移到OpenJDK:CVP OpenJDK遷移