在PCCE 12.6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)解決方案中交換自簽署憑證。

必要條件

需求

思科建議您瞭解以下主題：

- PCCE版本12.6(2)
- 客戶語音入口網站(CVP)版本12.6(2)
- 虛擬化語音瀏覽器(VVB)12.6(2)
- 管理工作站/管理日期伺服器(AW/ADS)12.6(2)
- Cisco Unified Intelligence server(CUIC)
- 客戶合作平台(CCP)12.6(2)

- 企業版聊天與電子郵件(ECE)12.6(2)

採用元件

本檔案中的資訊是根據以下軟體版本：

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

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

在來自12.x的PCCE解決方案中，所有裝置都通過託管在主要AW伺服器中的單一窗格(SPOG)進行控制。由於PCCE 12.5(1)版本的安全管理合規性(SRC)，解決方案中SPOG和其他伺服器之間的所有通訊都嚴格通過安全的HTTP協定完成。

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，必須在伺服器之間進行證書交換。

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)所有AW/ADS伺服器：這些伺服器需要以下證書：

- 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AW/ADS和ECE伺服器。

註：需要IIS和診斷框架門戶(DFP)。

  - CVP:CVP伺服器、CVP報告伺服器。

注意：需要來自所有伺服器的Web服務管理(WSM)證書。證書必須具有完全限定的域名(FQDN)。

- VOS平台：Cloud Connect、Cisco Virtualized Voice Browser(VVB)、Cisco Unified Communication Manager(CUCM)、Finesse、Cisco Unified Intelligence Center(CUIC)、Live Data(LD)、Identity Server(IDS)以及其他適用伺服器。

(ii)路由器\記錄器伺服器：這些伺服器需要來自以下位置的證書：

- Windows平台：所有AW/ADS伺服器IIS證書。

(iii)PG伺服器：這些伺服器需要證書：

- Windows平台：所有AW/ADS伺服器IIS證書。
- VOS平台：CUCM發佈器（僅限CUCM PG伺服器）；雲連線和CCP（僅限MR PG伺服器）。

注意：從CUCM伺服器下載JTAPI客戶端時需要執行此操作。

(iv)CVP伺服器：這些伺服器需要來自

- Windows平台：所有ADS伺服器IIS證書
- VOS平台：雲連線伺服器、VVB伺服器。

(v)CVP報告伺服器：此服務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：此服務器需要來自以下位置的證書：

- Windows平台：所有ADS伺服器IIS證書、來自CVP伺服器的VXML證書以及來自CVP伺服器的Callserver證書
- VOS平台：雲連線伺服器。

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平台應用程式與ADS伺服器之間的證書交換。

第3部分:路由器、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，需要使用伺服器的FQDN重新生成證書，否則，智慧許可、虛擬代理語音(VAV)以及與SPOG的CVP同步等功能很少會遇到問題。

注意：開始之前，必須執行以下操作：
1.以管理員身份開啟命令視窗。

2.對於12.6.2，要標識金鑰庫密碼，請轉到%CVP_HOME%\bin資料夾並運行DecryptKeystoreUtil.bat檔案。
3.對於12.6.1，要標識金鑰庫密碼，請運行命令，其他%CVP_HOME%\conf\security.properties。
4.運行keytool命令時需要此密碼。
5.從%CVP_HOME%\conf\security\目錄運行命令copy .keystore backup.keystore。

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，請提供您識別的keytool密碼。對於ADS伺服器，預設密碼為：changeit

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
```

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，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服務器：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 -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

CVP報告伺服器：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 -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

注意: 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 -genkeypai
```

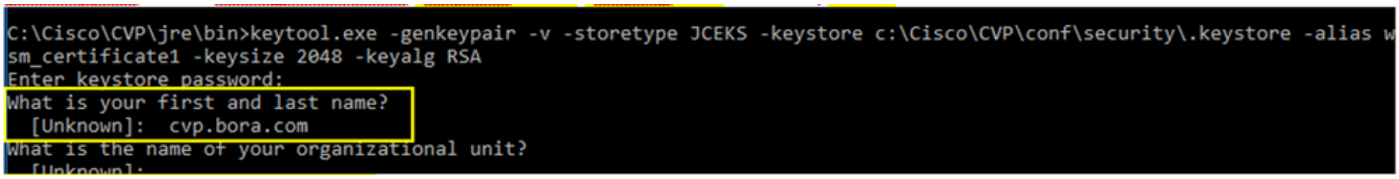
> 註：預設情況下，生成的證書為兩年。使用 — validity XXXX設定重新生成證書時的到期日期，否則證書的有效期為90天，並且需要在此時間之前由CA簽名。對於大多數此類證書，3-5年必須是合理的驗證時間。

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：從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。

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>

您所在州或省份的名稱是什麼？

[未知]: <指定省/市/自治區名稱>

此裝置的國碼（兩個字母）是什麼？

[未知]: <指定雙字母國家/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 -genkeypai
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

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 -genkeypai
```

為查詢指定伺服器FQDN您的名字和姓氏後，繼續執行與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 -genkeypai
```

重新啟動報表伺服器。

(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」替換為伺服器的主機名。例如， wsmcsa.crt 、 wsmcsb.crt 、 wsmrepa.crt 、 wsmrepb.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 -a
```

b)從路徑%CVP_HOME%\conf\security\wsm.crt複製證書，將其重新命名為wsmcsX.crt，並將其移動到ADS伺服器上的臨時資料夾中。

步驟2.將CVP伺服器WSM證書匯入ADS伺服器

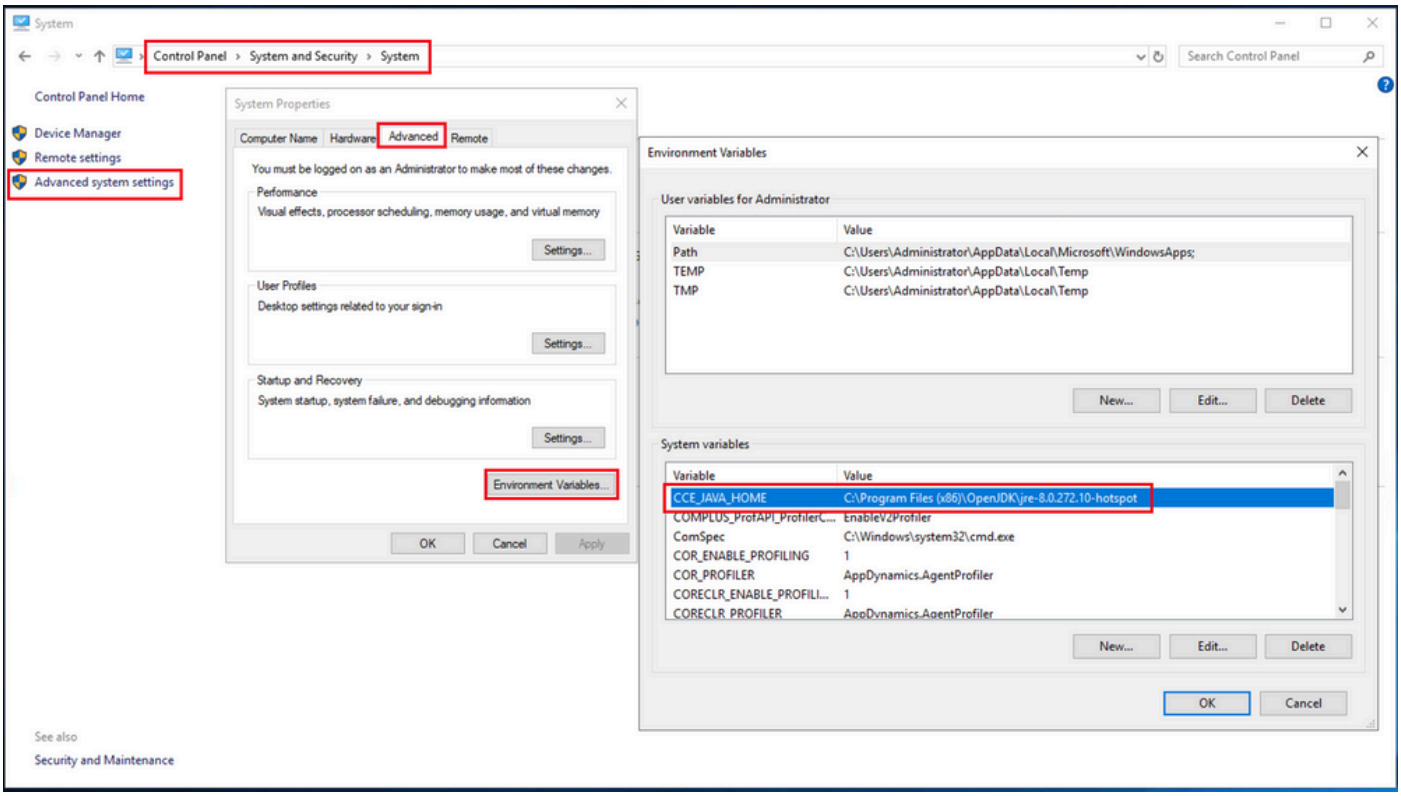
要在ADS伺服器中匯入證書，您需要使用keytool，該工具是java工具集的一部分。可以通過幾種方法找到此工具所在的java home路徑。

(i)CLI命令>echo %CCE_JAVA_HOME%

```
C:\>echo %CCE_JAVA_HOME%
C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot
```

java home path

(ii)手動通過高級系統設置，如下圖所示。



環境變數

在PCCE 12.6上，OpenJDK的預設路徑為C:\Program Files(x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

用於匯入自簽名證書的命令：

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

注意：對部署中的每個CVP重複這些命令，並在其他ADS伺服器上執行相同任務

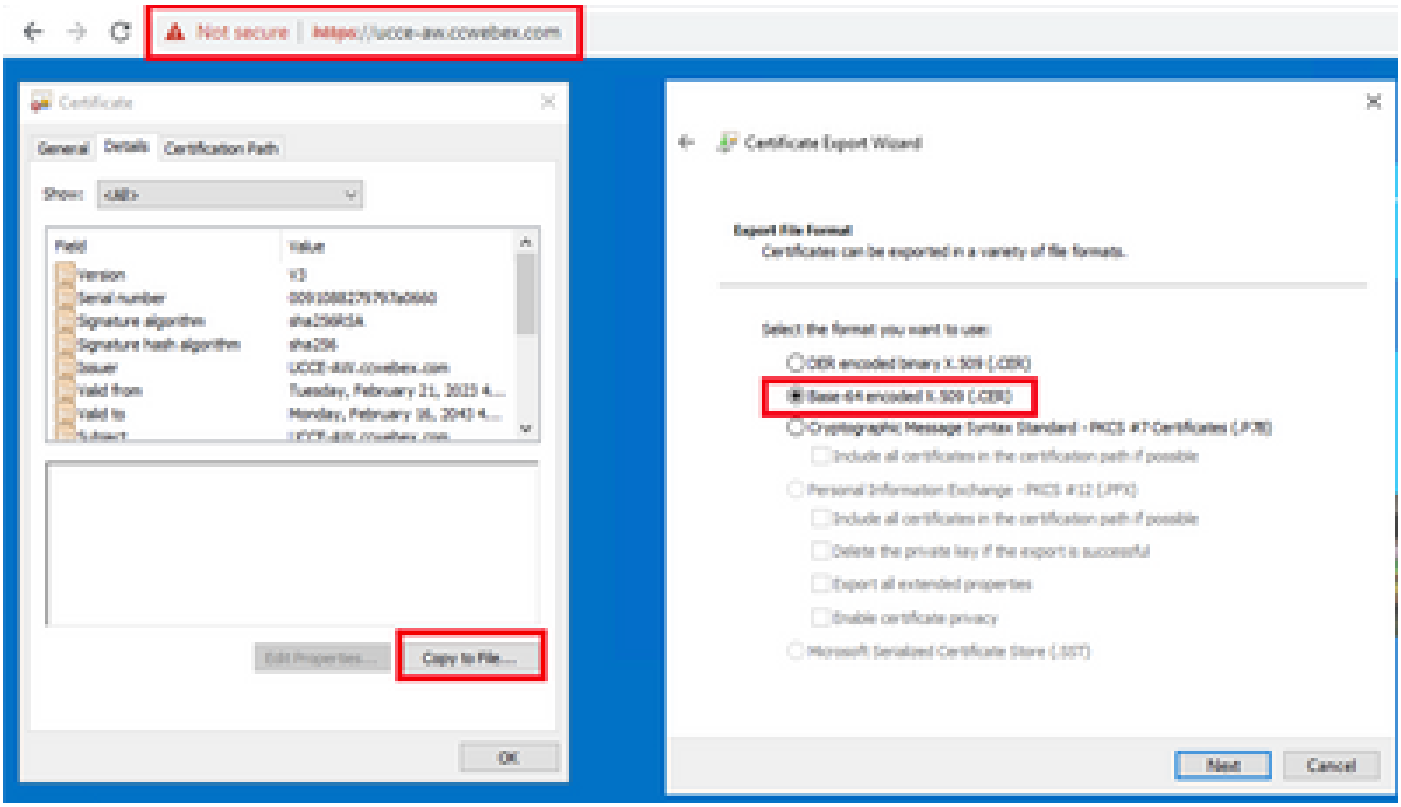
(iii)在ADS伺服器上重新啟動Apache Tomcat服務。

步驟3.匯出ADS伺服器證書

以下是匯出ADS證書的步驟：

(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，並將憑證命名為ADS<svr>[ab].cer。



匯出ADS證書

註：選擇Base-64 encoded X.509(.CER)選項。

步驟4.將ADS伺服器證書匯入CVP伺服器和報告伺服器

(i)將證書複製到%CVP_HOME%\conf\security目錄中的CVP伺服器和CVP報告伺服器。

(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 -t
```

對其他ADS伺服器證書執行相同步驟。

(iii)重新啟動CVP伺服器和報告伺服器

第2部分：VOS平台應用程式與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。

步驟3.將CUCM平台應用證書匯入CUCM PG伺服器。

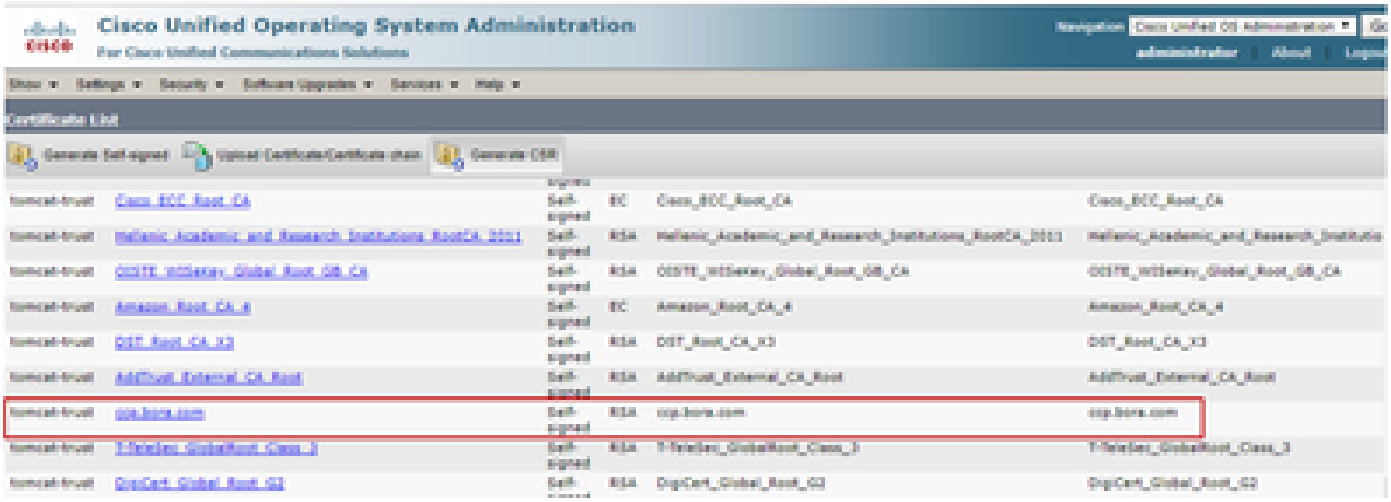
此過程適用於所有VOS應用程式，例如：

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

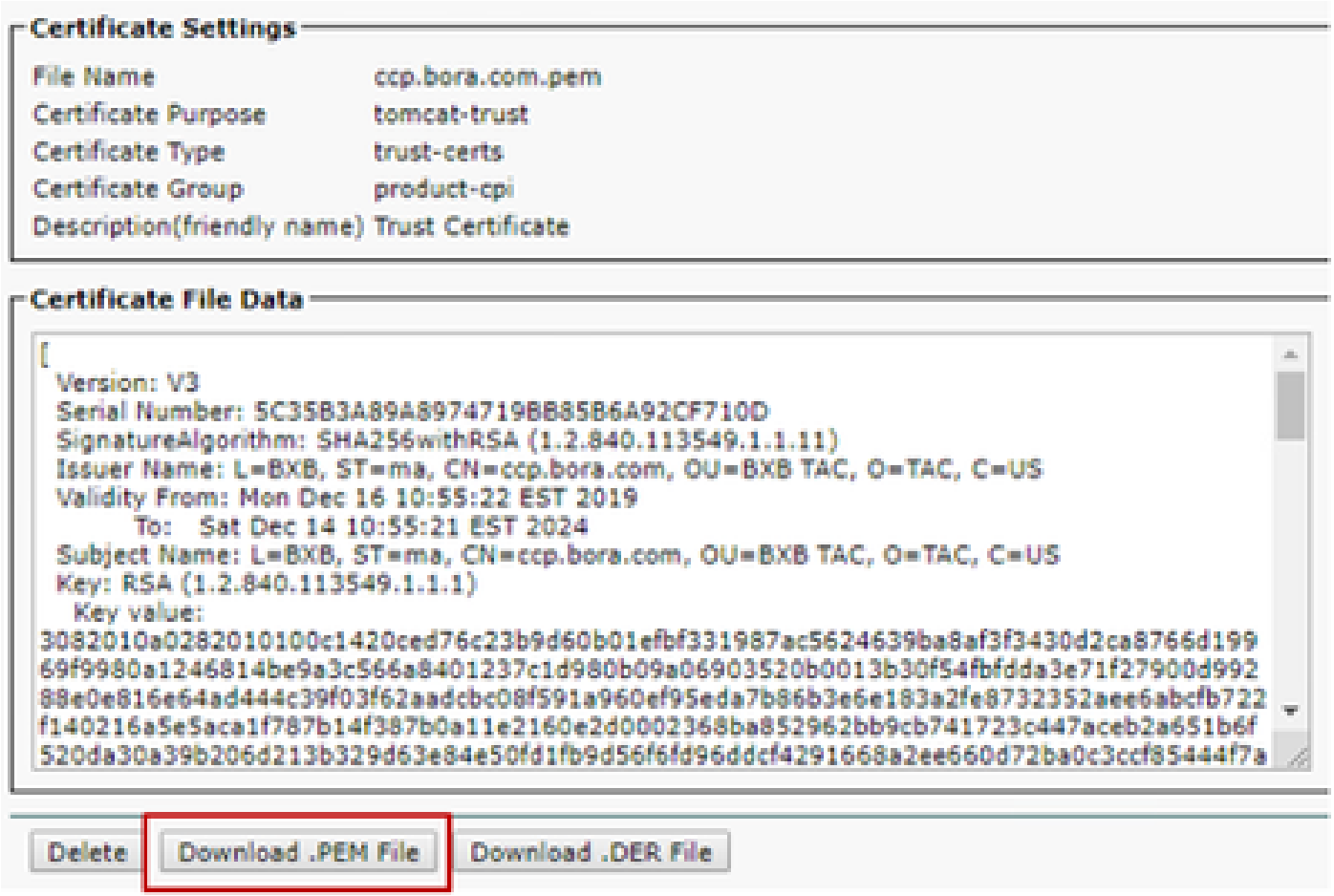
步驟1.匯出VOS平台應用伺服器證書。

(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。



註：對訂戶執行相同步驟。

步驟2.將VOS平台應用證書匯入ADS伺服器

運行金鑰工具的路徑： %CCE_JAVA_HOME%\bin

用於匯入自簽名證書的命令：

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias {fqdn_of_VOS>} -
```

在ADS伺服器上重新啟動Apache Tomcat服務。

注意：在其他ADS伺服器上執行相同任務

步驟3.將CUCM平台應用證書匯入CUCM PG伺服器

運行金鑰工具的路徑： %CCE_JAVA_HOME%\bin

用於匯入自簽名證書的命令：

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\cucmapplicationX.cer -alias {fqdn_of_cucm>}
```

在PG伺服器上重新啟動Apache Tomcat服務。

注意：在其他CUCM PG伺服器上執行相同任務

第3部分：路由器、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：

步驟1.從羅傑和PG伺服器匯出IIS證書

步驟2.從Rogger和PG伺服器匯出DFP證書

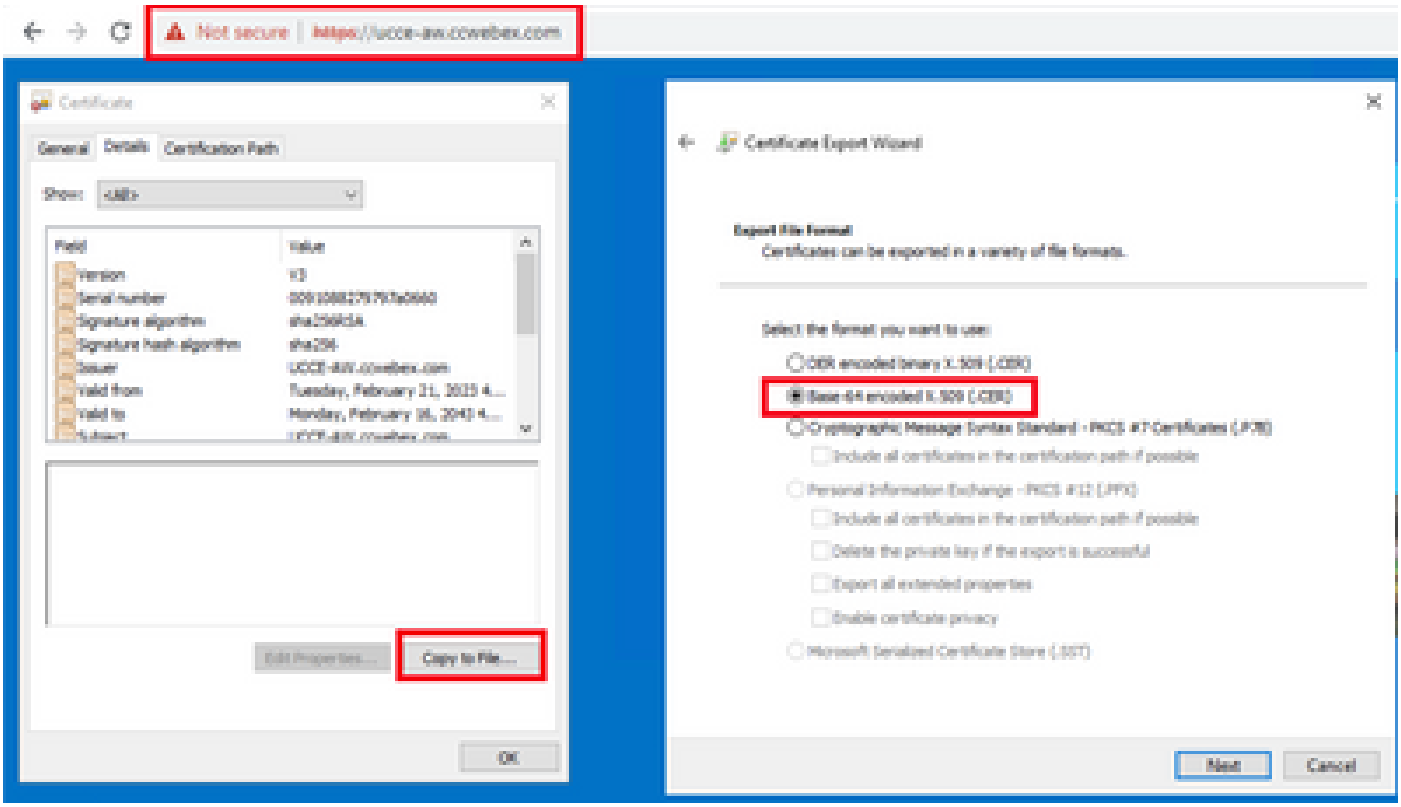
步驟3.將證書匯入到ADS伺服器

步驟4.將ADS證書匯入到路由器和PG伺服器

步驟1.從羅傑和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中，例如c:\temp\certs，並將憑證命名為ICM<svr>[ab].cer



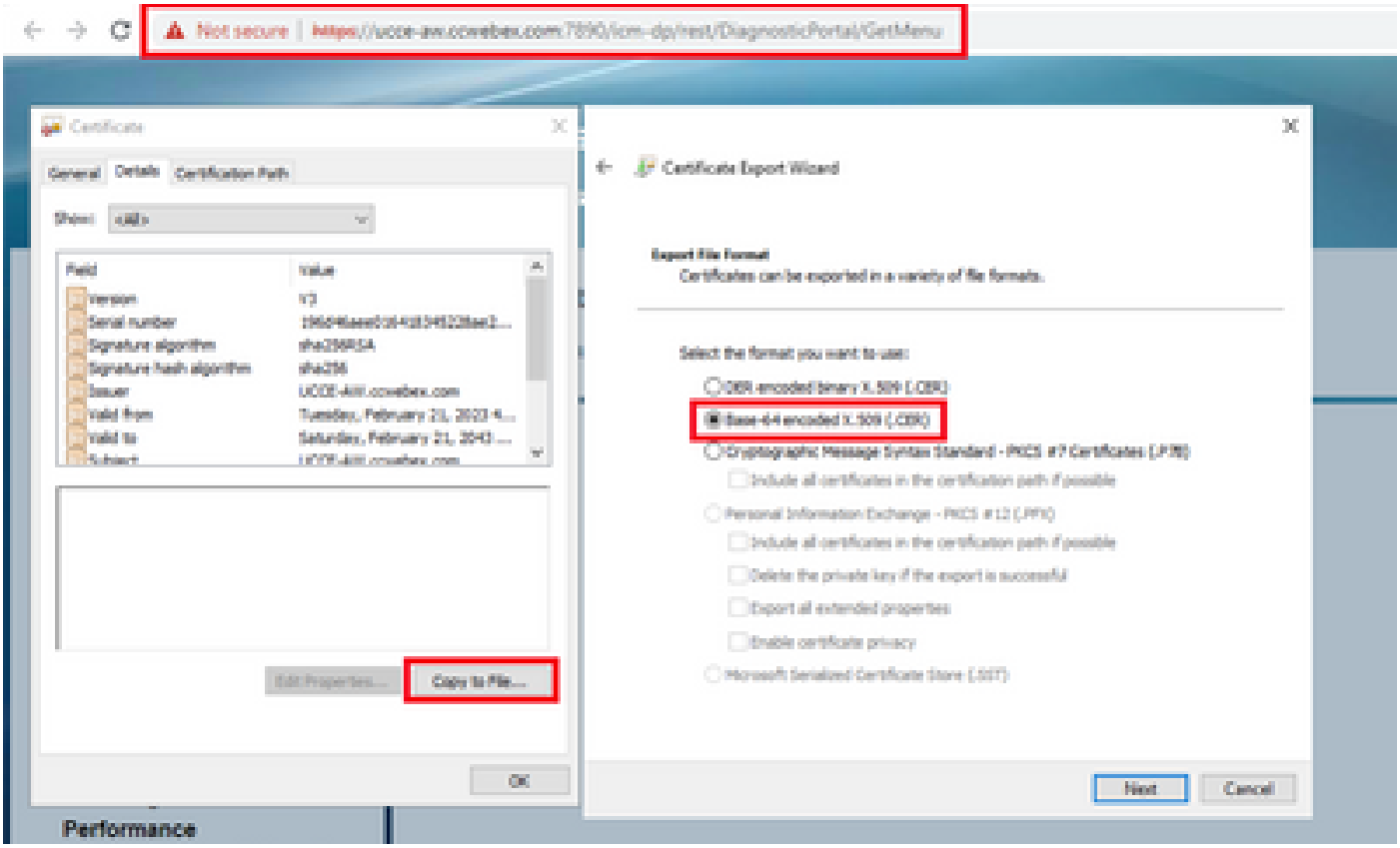
匯出IIS證書

註：選擇Base-64 encoded X.509(.CER)選項。

步驟2.從Rogger和PG伺服器匯出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



匯出DFP證書

註：選擇Base-64 encoded X.509(.CER)選項。

步驟3.將證書匯入到ADS伺服器

命令將IIS自簽名證書匯入ADS伺服器。運行金鑰工具的路徑： %CCE_JAVA_HOME%\bin

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\temp\certs\ICM<svr>[ab].cer -alias {fqdn_of_server}_II
```

注意：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

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp<svr>[ab].cer -alias {fqdn_of_server}_DF
```

注意：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。

步驟4.將ADS證書匯入到路由器和PG伺服器

命令將IIS自簽名證書匯入到路由器和PG伺服器。運行金鑰工具的路徑:
%CCE_JAVA_HOME%\bin。

```
%CCE_JAVA_HOME%\bin\keytool -keystore ..\lib\security\cacerts  -import -storepass changeit -alias {fqdn
```

注意：匯入匯出到所有Rogger和PG伺服器的所有ADS伺服器IIS證書。

在Rogger和PG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版本12.6(2)使用手冊 — Web服務整合[Cisco Unified Customer Voice Portal] - Cisco

相關資訊

- CVP配置指南 — 安全
- UCCE安全指南
- PCCE管理指南
- Exchange PCCE自簽名證書 — PCCE 12.5
- Exchange UCCE自簽名證書 — UCCE 12.5
- Exchange UCCE自簽名證書 — UCCE 12.6
- 實施CA簽名的證書 — CCE 12.6
- 使用客服中心上傳程式工具交換憑證
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。