

在PCCE 12.6解決方案中交換自簽名證書

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景](#)

[程式](#)

[第1部分：CVP和ADS伺服器之間的證書交換](#)

[步驟 1. 導出CVP伺服器證書](#)

[步驟 2. 將CVP伺服器WSM證書導入ADS伺服器](#)

[步驟 3. 匯出ADS伺服器憑證](#)

[步驟 4. 將ADS伺服器憑證匯入CVP伺服器和報表伺服器](#)

[第2部分：VOS平台應用和ADS伺服器之間的證書交換](#)

[步驟 1. 導出VOS平台應用伺服器證書。](#)

[步驟 2. 將VOS平台應用證書導入到ADS伺服器](#)

[步驟 3. 將CUCM平台應用證書導入CUCM PG伺服器](#)

[第3部分：Rogers、PG和ADS伺服器之間的證書交換](#)

[步驟 1. 從記錄器和PG伺服器匯出IIS憑證](#)

[步驟 2. 從記錄器和PG伺服器導出DFP證書](#)

[步驟 3. 將憑證匯入ADS伺服器](#)

[步驟 4. 將ADS憑證匯入Rogger和PG伺服器](#)

[第4部分：CVP CallStudio Web服務整合](#)

[相關資訊](#)

簡介

本文說明如何在Cisco Packaged Contact Center Enterprise (PCCE)解決方案中交換自簽名證書。

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，所有裝置都透過託管在主要AW伺服器中的單一管理平台(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透過安全HTTP協定來完成。

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是必需的。

程式


這些是導出自簽名證書的元件，以及需要將自簽名證書導入其中的元件。

(i)所有AW/ADS伺服器：這些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AW/ADS和ECE伺服器。

 註：需要IIS和診斷架構門戶(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。憑證必須使用完整網域名稱(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)和其他適用伺服器。


(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：這些伺服器需要來自以下位置的證書：

- Windows平台：所有AW/ADS伺服器IIS證書。

- VOS平台：CUCM發佈伺服器（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客戶端需要執行此操作。

(iv) CVP伺服器：這些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：雲連線伺服器、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：所有ADS伺服器IIS證書、CVP伺服器的VXML證書以及CVP伺服器的Callserver證書
- VOS平台：雲連線伺服器。

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：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如下：

步驟 1. 導出CVP伺服器WSM證書。


步驟 2. 將CVP伺服器WSM證書導入ADS伺服器。

步驟 3. 導出ADS伺服器證書。

步驟 4. 將ADS伺服器導入CVP伺服器和CVP報告伺服器。

步驟 1. 導出CVP伺服器證書

在從CVP伺服器導出證書之前，您需要使用伺服器的FQDN重新生成證書，否則，智慧許可、虛擬代理語音(VAV)以及與SPOG的CVP同步等少數功能可能會出現問題。

 注意：在開始之前，您必須執行以下操作：

1. 以管理員身份開啟命令視窗。
 2. 對於12.6.2，若要辨識金鑰庫密碼，請移至%CVP_HOME%\bin資料夾，然後執行
-


 DecryptKeystoreUtil.bat檔案。

3. 對於12.6.1，要標識金鑰庫口令，請運行命令more

%CVP_HOME%\conf\security.properties。

4. 執行keytool指令時需要此密碼。


5. 從%CVP_HOME%\conf\security\目錄，運行命令copy .keystore backup.keystore。

 附註：您可以使用keytool引數-storepass來簡化本文檔中使用的命令。對於所有CVP伺服器，請提供您辨識的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)列出伺服器中的憑證

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

 注意：CVP伺服器具有以下自簽名證書：wsm_certificate、vxml_certificate和callserver_certificate。如果您使用keytool的引數-v，就可以看到每個憑證的更多詳細資訊。此外，您可以在keytool.exe list指令的結尾新增「>」符號，將輸出傳送到文字檔，例如> test.txt

(ii)刪除舊的自簽名證書

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：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 callserver_certificate
```


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

(iii)使用伺服器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
```

 注意：預設情況下，證書生成時間為兩年。使用-validity XXXX設定證書重新生成的到期日期，否則證書有效期為90天，並且在此時間之前需要由CA簽署。對於大多數認證來說，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以下值：-keyalg RSA和-keysize 2048。CVP keystore命令必須包括-storetype JCEKS引數。如果不這樣做，證書、金鑰或更糟的金鑰庫可能會損壞。

在問題您的姓和名是什麼上指定伺服器的FQDN？

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\keystore -alias wsm_certificate1 -keysize 2048 -keyalg RSA
Enter keystore password:
What is your first and last name?
[Unknown]: cvp.bora.com
What is the name of your organizational unit?
[Unknown]:
```

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]： <指定組織名稱>

您所在城市或地區的名稱是什麼？

[未知]： <指定城市/地區的名稱>

您所在州或省的名稱是什麼？

[未知]： <指定州/省的名稱>

此單位的兩個字母的國家代碼是什麼？

[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
```

指定伺服器FQDN以進行查詢您的姓氏和名字？並繼續執行與CVP伺服器相同的步驟。

對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 callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

重新啟動報表伺服器。

(iv)從CVP和報告伺服器導出wsm_Certificate

a)將每個CVP伺服器的WSM證書導出到一個臨時位置，然後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。

用於導出自簽名證書的命令：

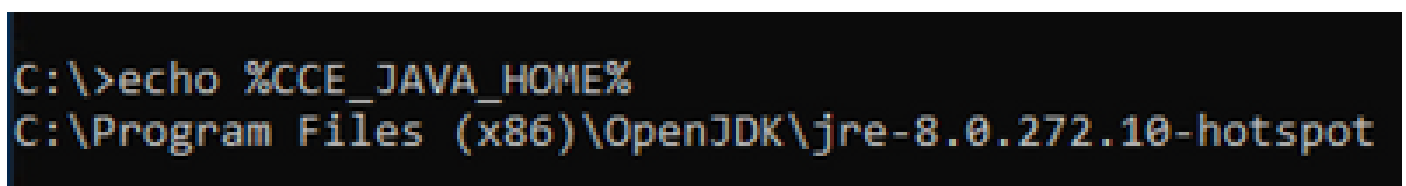
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

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

步驟 2.將CVP伺服器WSM證書導入ADS伺服器

若要在ADS伺服器中匯入憑證，您必須使用keytool（屬於java工具集）。有幾種方法可以讓您找到裝載此工具的Java本位目錄路徑。

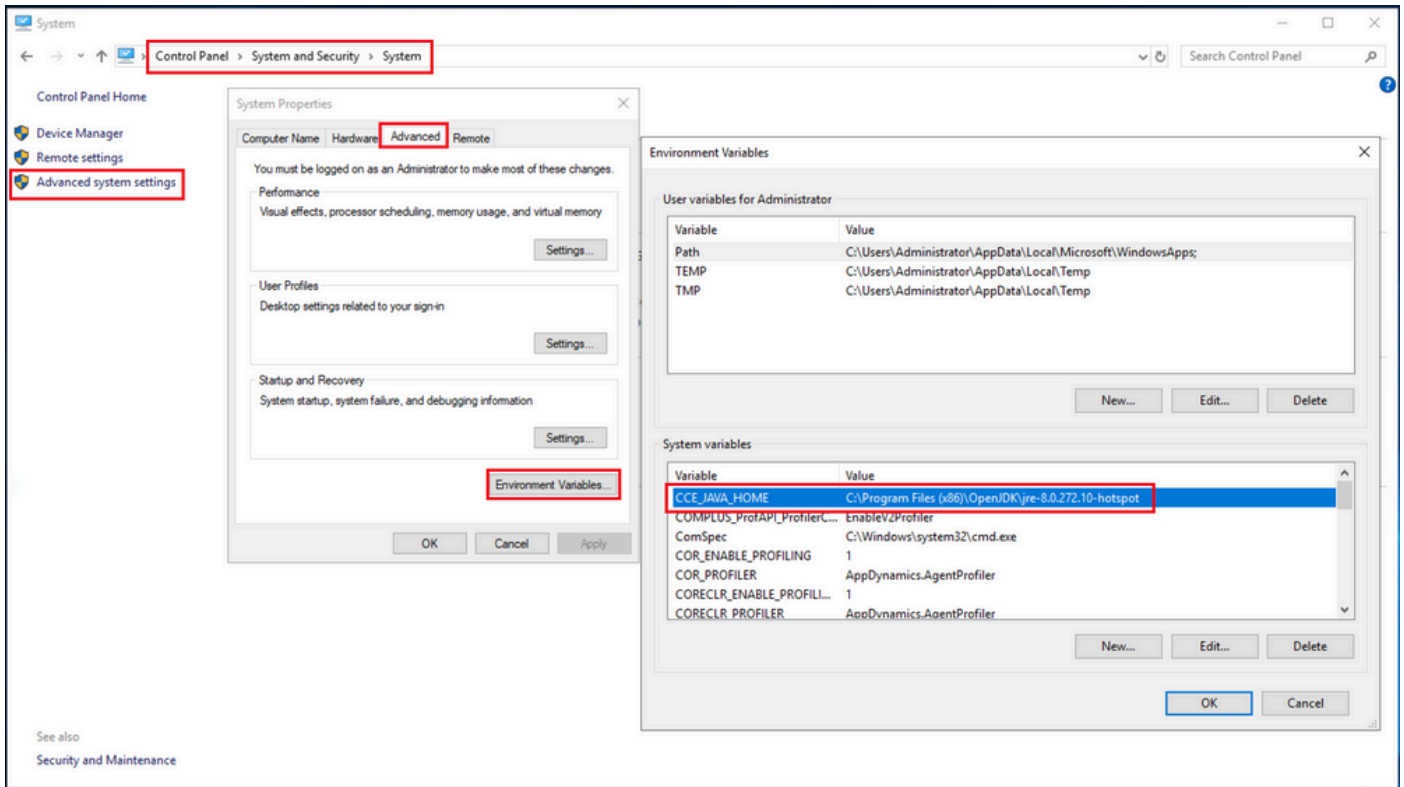
(i) CLI命令> echo %CCE_JAVA_HOME%



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

java本位目錄路徑

(ii)透過進階系統設定手動，如圖所示。



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

用於導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
directory}\ssl\cacerts
```



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

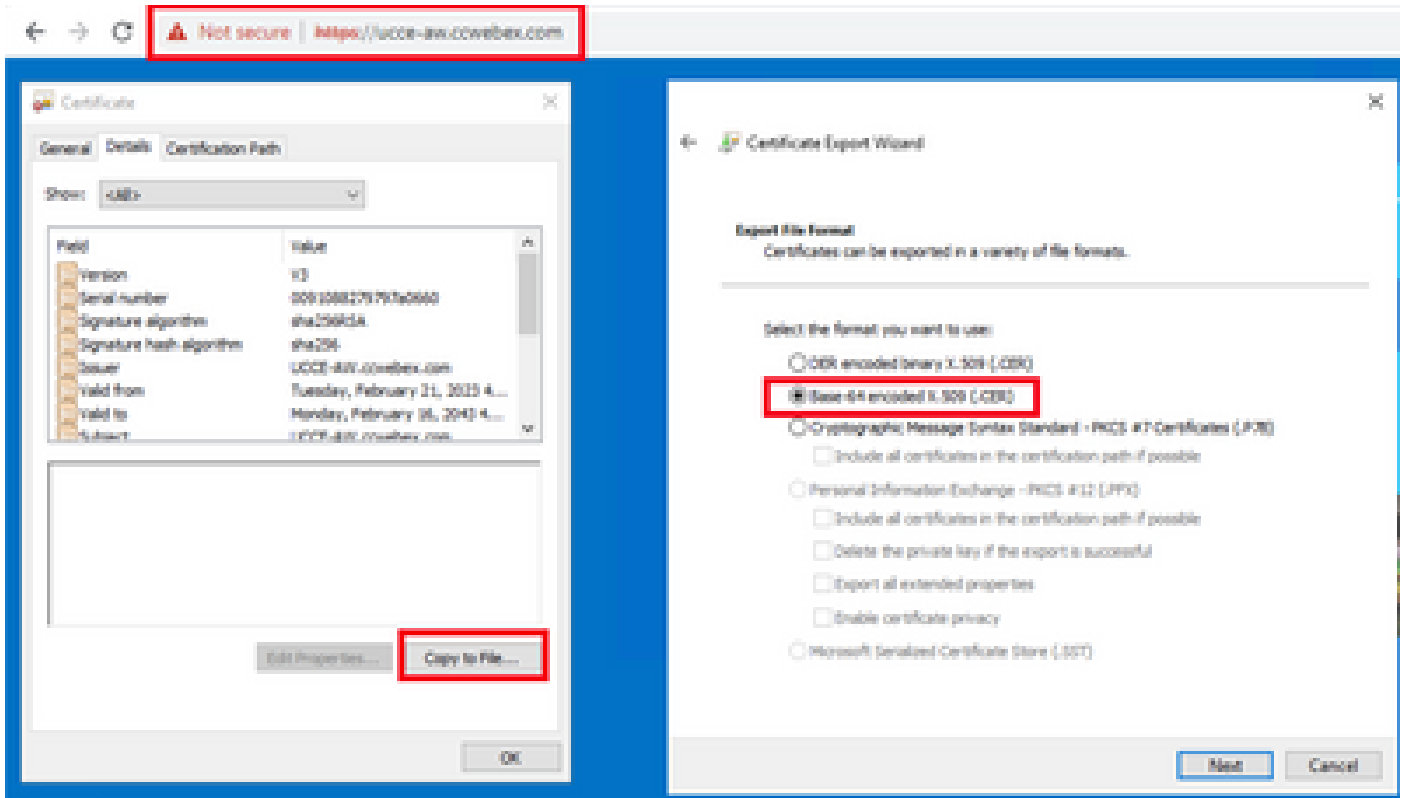
(iii)重新啟動ADS伺服器上的Apache Tomcat服務。

步驟 3.匯出ADS伺服器憑證

以下是導出ADS證書的步驟：

(i)在ADS伺服器上，從瀏覽器導航至伺服器URL：<https://<servername>>。

(ii)將證書儲存到臨時資料夾，例如：c:\temp\certs，並將證書命名為ADS<svr>[ab].cer。



匯出ADS憑證

 註：選擇Base-64 encoded X.509 (.CER)選項。

步驟 4. 將ADS伺服器憑證匯入CVP伺服器和報表伺服器

- (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) 將證書導入到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\ADS{svr}[ab].cer
```

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平台應用和ADS伺服器之間的證書交換

成功完成此交換所需的步驟如下：

- 步驟 1. 導出VOS平台應用伺服器證書。
- 步驟 2. 將VOS平台應用證書導入ADS伺服器。

步驟 3.將CUCM平台應用證書導入CUCM PG伺服器。

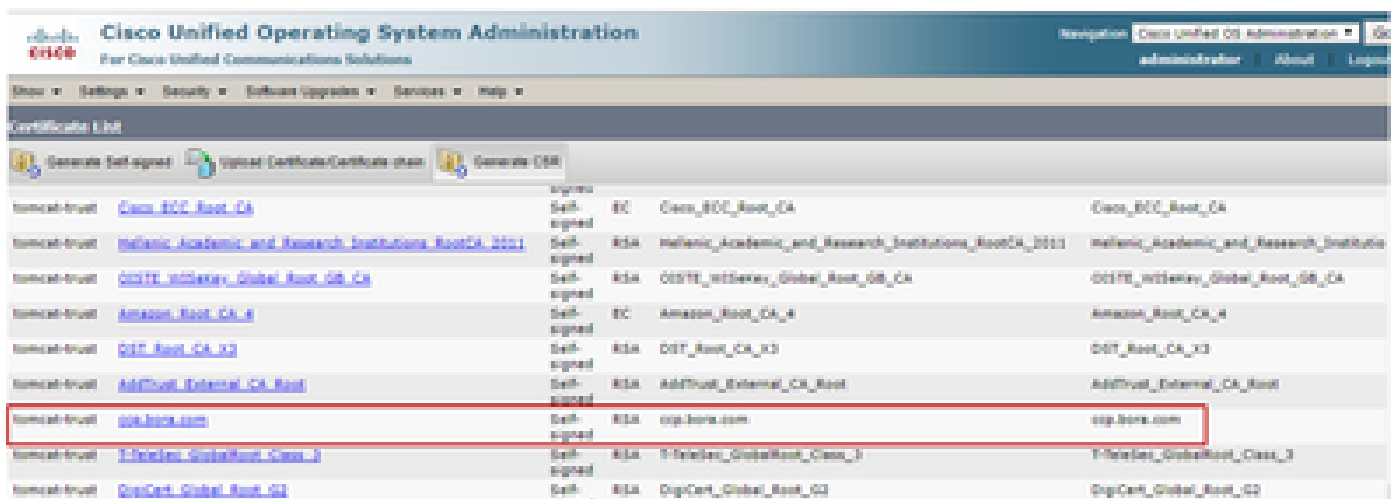
此程式適用於所有VOS應用程式，例如：

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

步驟 1.導出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)導航到安全>證書管理，然後在tomcat-trust資料夾中查詢應用程式主伺服器證書。



tomcat-trust	Self-signed	EC	Self-signed	Self-signed
Cisco_EOC_Root_CA	Self-signed	EC	Cisco_EOC_Root_CA	Cisco_EOC_Root_CA
Malonic_Academic_and_Research_Institutions_RootCA_2011	Self-signed	RSA	Malonic_Academic_and_Research_Institutions_RootCA_2011	Malonic_Academic_and_Research_Institutions
OCITE_wiSentry_Global_Root_CA	Self-signed	RSA	OCITE_wiSentry_Global_Root_CA	OCITE_wiSentry_Global_Root_CA
Amazon_Root_CA_4	Self-signed	EC	Amazon_Root_CA_4	Amazon_Root_CA_4
D4T_Root_CA_X3	Self-signed	RSA	D4T_Root_CA_X3	D4T_Root_CA_X3
AddTrust_External_CA_Root	Self-signed	RSA	AddTrust_External_CA_Root	AddTrust_External_CA_Root
osp.here.com	Self-signed	RSA	osp.here.com	osp.here.com
T-TeleSec_GlobalRoot_Class_3	Self-signed	RSA	T-TeleSec_GlobalRoot_Class_3	T-TeleSec_GlobalRoot_Class_3
DigCert_Global_Root_G2	Self-signed	RSA	DigCert_Global_Root_G2	DigCert_Global_Root_G2

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

Certificate Settings

File Name	ccp.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly name)	Trust Certificate

Certificate File Data

```
[
Version: V3
Serial Number: 5C35B3A89A89747198B85B6A92CF710D
Signature Algorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
Validity From: Mon Dec 16 10:55:22 EST 2019
To: Sat Dec 14 10:55:21 EST 2024
Subject Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199
69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992
88e0e816e64ad444c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
```

Delete Download .PEM File Download .DER File

 注意：對訂戶執行相同的步驟。


步驟 2.將VOS平台應用證書導入到ADS伺服器

運行金鑰工具的路徑： %CCE_JAVA_HOME%\bin

用於導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>} -keystore {ICM install directory}\ssl\cacerts
```

重新啟動ADS伺服器上的Apache Tomcat服務。

 註：在其他ADS伺服器上執行相同任務

步驟 3.將CUCM平台應用證書導入CUCM PG伺服器

運行金鑰工具的路徑： %CCE_JAVA_HOME%\bin

用於導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>} -keystore {ICM install directory}\ssl\cacerts
```

重新啟動PG伺服器上的Apache Tomcat服務。

 註：在其他CUCM PG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如下：

步驟 1. 從記錄器和PG伺服器匯出IIS憑證

步驟 2. 從記錄器和PG伺服器導出DFP證書

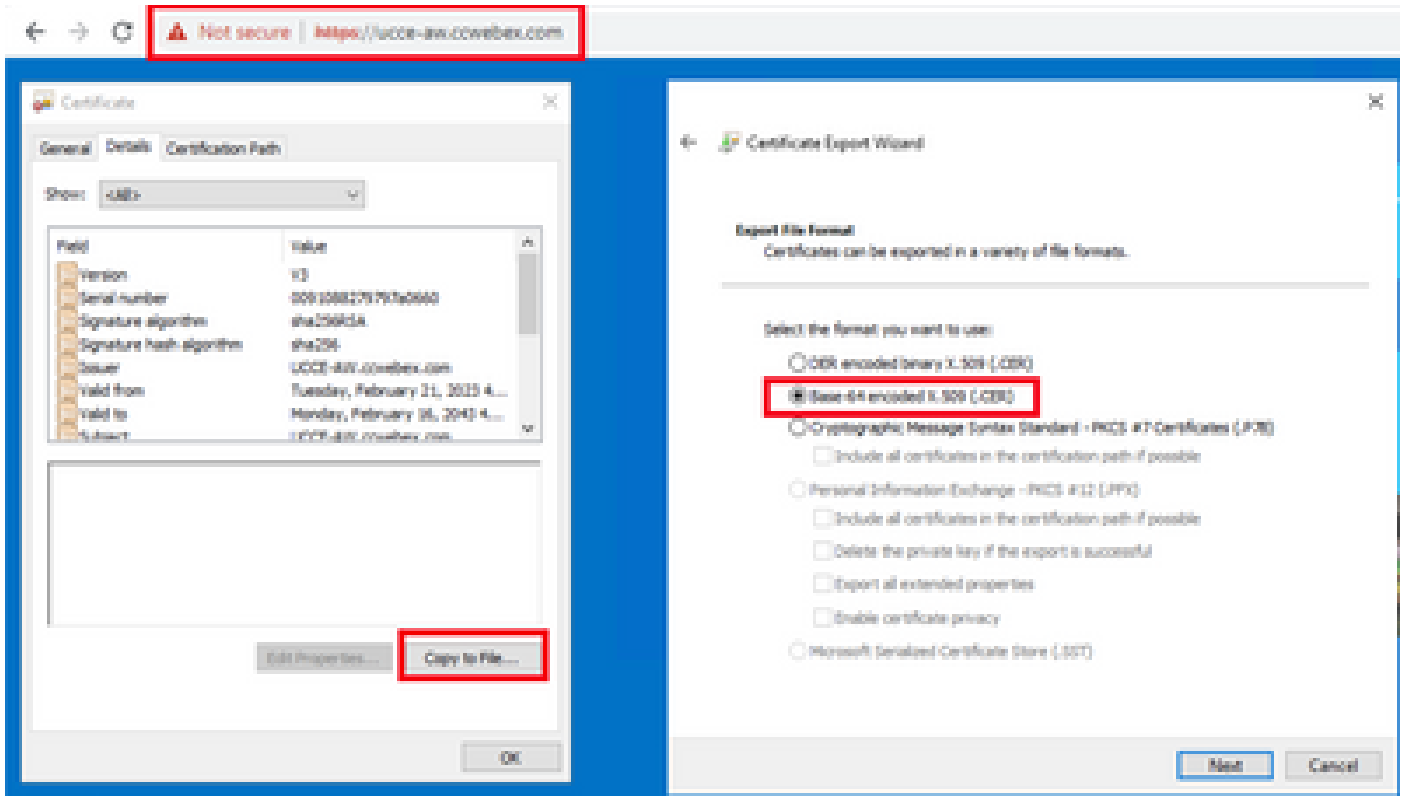
步驟 3. 將憑證匯入ADS伺服器

步驟 4. 將ADS憑證匯入Rogger和PG伺服器


步驟 1. 從記錄器和PG伺服器匯出IIS憑證

(i) 在ADS伺服器上，從瀏覽器導航至伺服器(Rogers , PG) url： <https://{servername}>

(ii) 將證書儲存到臨時資料夾(例如c：\temp\certs)，並將證書命名為ICM<svr>[ab].cer



匯出IIS憑證

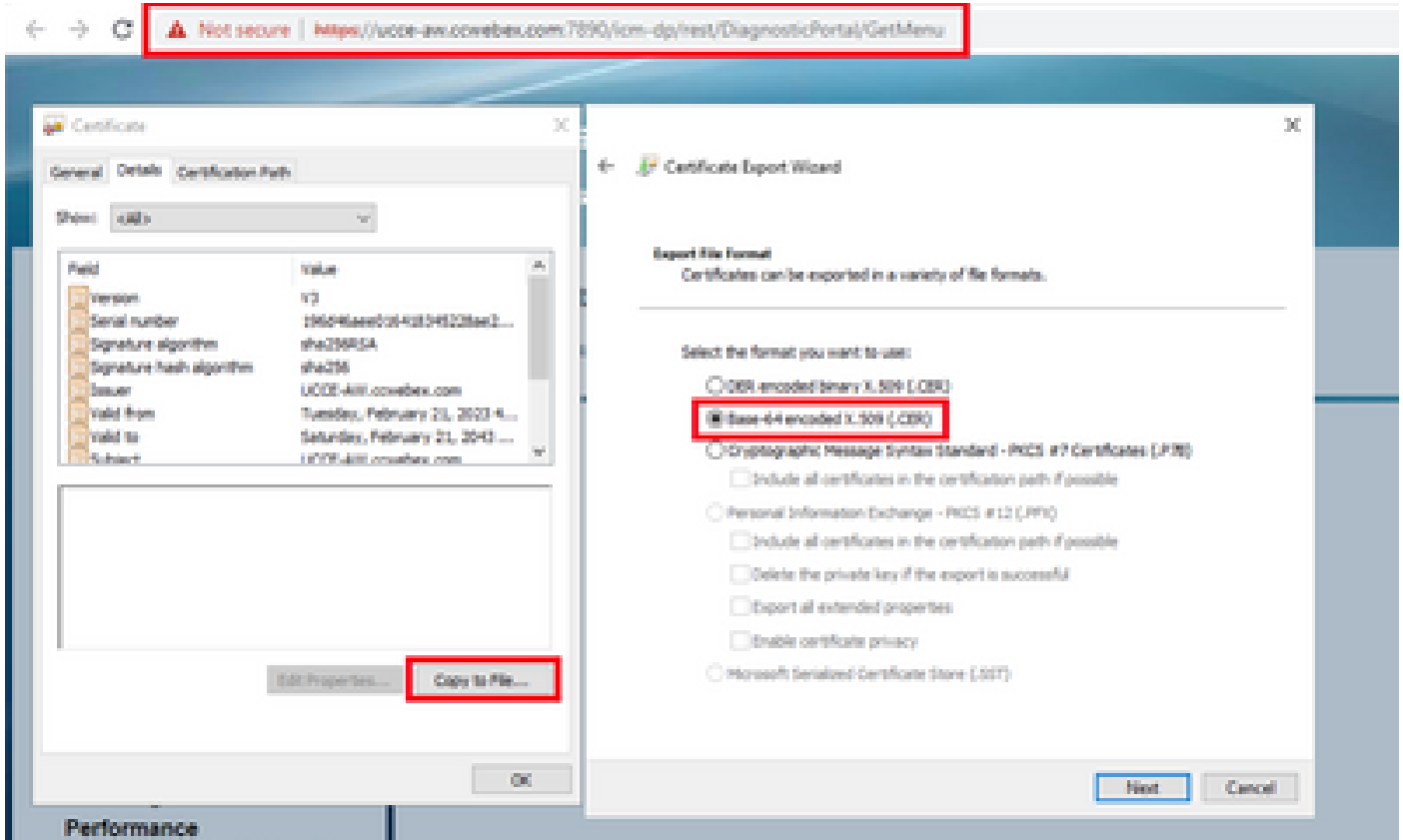
 註：選擇Base-64 encoded X.509 (.CER)選項。

步驟 2. 從記錄器和PG伺服器導出DFP證書

(i) 在ADS伺服器上，從瀏覽器瀏覽至伺服器(Rogers、PG) DFP

URL : `https://{servername} : 7890/icm-dp/rest/DiagnosticPortal/GetProductVersion`

(ii) 將憑證儲存到資料夾範例 `c : \temp\certs`，並將憑證命名為 `dfp{svr}[ab].cer`



匯出DFP憑證

註：選擇Base-64 encoded X.509 (.CER)選項。

步驟 3.將憑證匯入ADS伺服器

命令將IIS自簽名證書導入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}_IIS -keystore {ICM install directory}\ssl\cacerts
```

注意：導入導出到所有ADS伺服器的所有伺服器證書。

用於將診斷自簽名證書導入到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}_DFP -keystore {ICM install directory}\ssl\cacerts
```

注意：導入導出到所有ADS伺服器的所有伺服器證書。

重新啟動ADS伺服器上的Apache Tomcat服務。

步驟 4.將ADS憑證匯入Rogger和PG伺服器

用於將IIS自簽名證書導入到羅傑和PG伺服器的命令。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_of_server}_IIS -file c:\temp\certs\ICM{svr}[ab].cer
```



注意：導入導出到所有Rogger和PG伺服器的所有ADS伺服器IIS證書。

重新啟動Rogger和PG伺服器上的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簽名證書- CCE 12.6](#)
- [使用聯絡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）。