

在UCCE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](#)

[背景資訊](#)

[程式](#)

[CCE AW伺服器 and CCE 核心應用伺服器](#)

[第1部分。路由器\記錄器、PG和AW伺服器之間的證書交換](#)

[第2部分。VOS平台應用程式和AW伺服器之間的證書交換](#)

[CVP OAMP伺服器和CVP元件伺服器](#)

[第1部分。CVP OAMP伺服器與CVP伺服器及報告伺服器之間的證書交換](#)

[第2部分。CVP OAMP伺服器和VOS平台應用程式之間的證書交換](#)

[第3部分。CVP伺服器和VVB伺服器之間的證書交換](#)

[CVP Call Studio Web服務整合](#)

[相關資訊](#)

簡介

本文檔介紹如何在Unified Contact Center Enterprise(UCCE)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：

- UCCE版本12.5(1)
- 客戶語音入口網站(CVP)版本12.5(1)
- Cisco Virtualized Voice Browser(VVB)

採用元件

本檔案中的資訊是根據以下軟體版本：

- UCCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12.5
- CVP營運主控台(OAMP)
- CVP新OAMP(NOAMP)

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。

背景資訊

在UCCE解決方案中，涉及核心應用程式(如ROGGER、外圍裝置網關(PG)、管理工作站(AW)/管理資料伺服器(ADS)、Finesse、Cisco Unified Intelligence Center(CUIC)等)的新功能的配置通過聯絡中心企業版(CCE)管理頁面完成。對於CVP、Cisco VVB和網關等互動式語音響應(IVR)應用，NOAMP控制新功能的配置。從CCE 12.5(1)開始，由於安全管理合規性(SRC)，所有與CCE管理員和NOAMP的通訊都嚴格通過安全HTTP協定完成。

為了在自簽名證書環境中實現這些應用程式之間的無縫安全通訊，伺服器之間的證書交換成為一項必需。下一節詳細說明了交換自簽名證書所需的步驟：

- CCE AW伺服器和CCE核心應用伺服器
- CVP OAMP伺服器和CVP元件伺服器

程式

CCE AW伺服器和CCE核心應用伺服器

這些是匯出自簽名證書的元件和必須將自簽名證書匯入其中的元件。

CCE AW伺服器：此伺服器需要來自以下位置的證書：

- Windows平台：路由器和記錄器(ROGGER){A/B}、外圍裝置網關(PG){A/B}和所有AW/ADS。

 注意：需要IIS和診斷框架門戶(DFP)證書。

- VOS平台：Finesse、CUIC、即時資料(LD)、身份伺服器(IDS)、Cloud Connect和其他適用的伺服器是清單資料庫的一部分。

這同樣適用於解決方案中的其他AW伺服器。

Router\Logger Server：此伺服器需要來自以下位置的證書：

- Windows平台：所有AW伺服器的IIS證書。

有效交換CCE自簽名證書所需的步驟分為以下部分：

第1部分。Router\Logger、PG和AW Server之間的證書交換。

第2部分。VOS平台應用程式和AW伺服器之間的證書交換。

第1部分。路由器\記錄器、PG和AW伺服器之間的證書交換

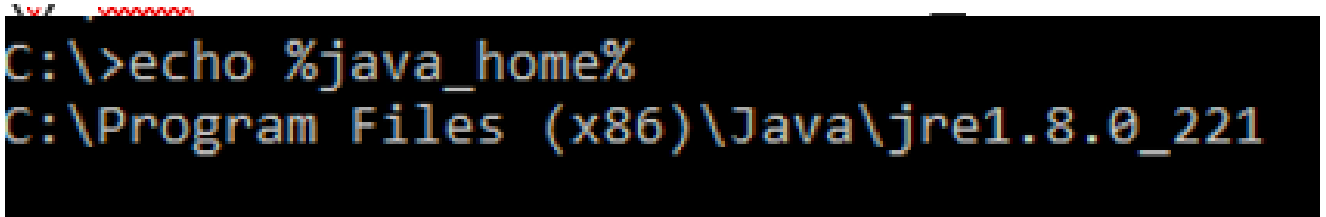
成功完成此交換所需的步驟為：

- 步驟 1.從Router\Logger、PG和所有AW伺服器匯出IIS證書。
- 步驟 2.從Router\Logger、PG和所有AW伺服器匯出DFP證書。
- 步驟 3.將IIS和DFP證書從路由器\記錄器、PG和AW匯入AW伺服器。
- 步驟 4.從AW伺服器將IIS證書匯入Router\Logger和PG。

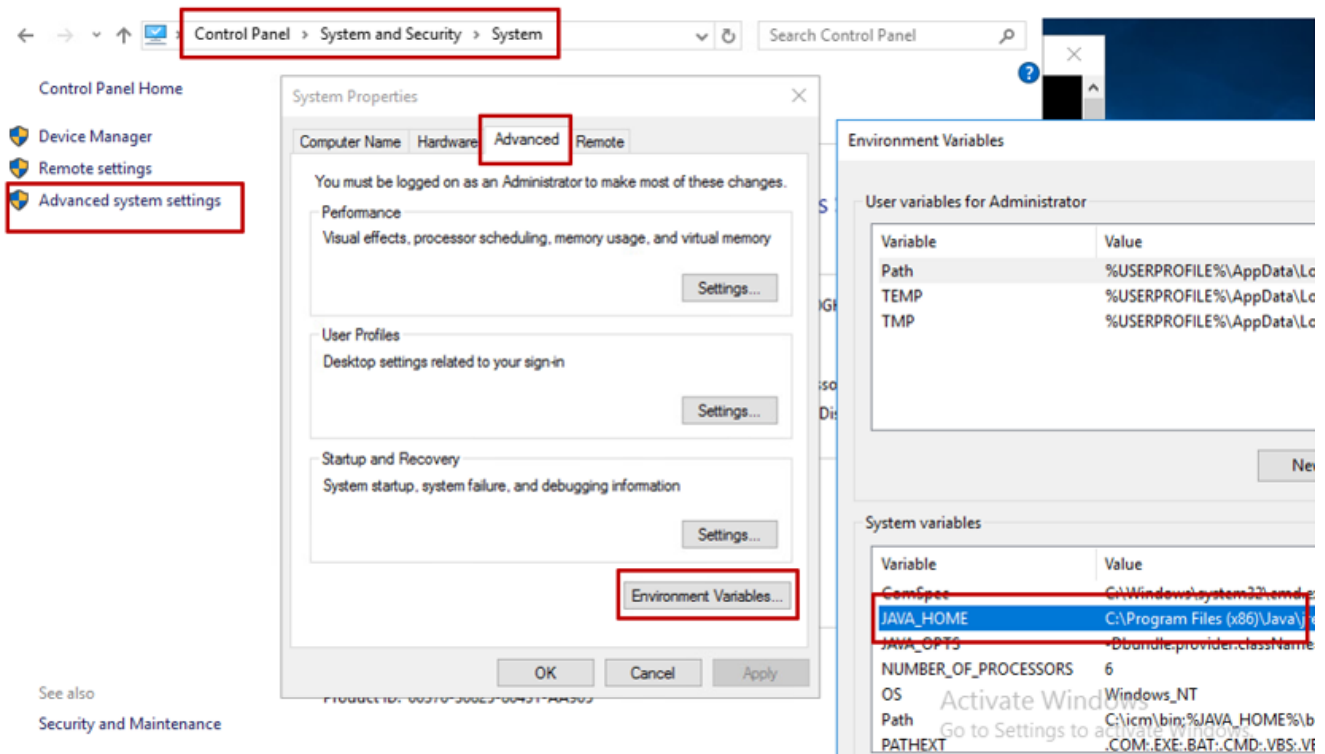
 注意：開始之前，必須備份金鑰庫並以管理員身份開啟命令提示符。


1. 瞭解Java主目錄路徑，以確保Java金鑰工具位於何處。可以通過幾種方法找到Java主路徑。

選項1.CLI命令：`echo %JAVA_HOME%`



選項2.手動通過「Advanced system (高級)」設定，如下圖所示。



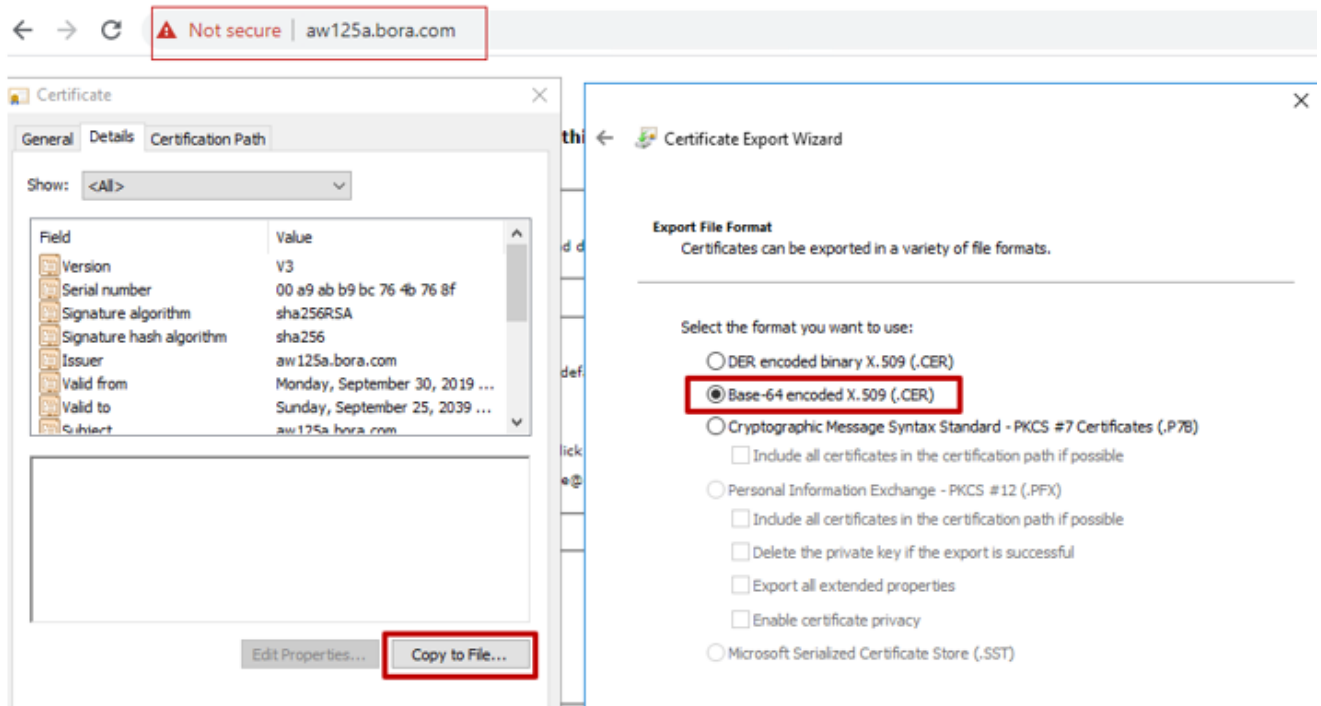
 註：在UCCE 12.5上，預設路徑為C:\Program Files (x86)\Java\jre1.8.0_221\bin。但是，如果您已使用12.5(1a)安裝程式或安裝了12.5 ES55 (必需OpenJDK ES)，則使用%`CCE_JAVA_HOME`%，而不是使用%`JAVA_HOME`%，因為使用OpenJDK更改了資料儲存路徑。有關CCE和CVP中OpenJDK遷移的詳細資訊，請參閱以下文檔：[在CCE 12.5\(1\)中安裝和遷移到OpenJDK](#)和[在CVP 12.5\(1\)中安裝和遷移到OpenJDK](#)。

2. cacerts 從檔案夾備份文{`JAVA_HOME`}\lib\security。您可以將其複製到其他位置。

步驟 1.從Router\Logger、PG和所有AW伺服器匯出IIS證書。

1. 在瀏覽器的AW伺服器上，導航到伺服器 (ROgger、PG和其他AW伺服器) URL:https://{servername}。

CCE via Chrome Browser



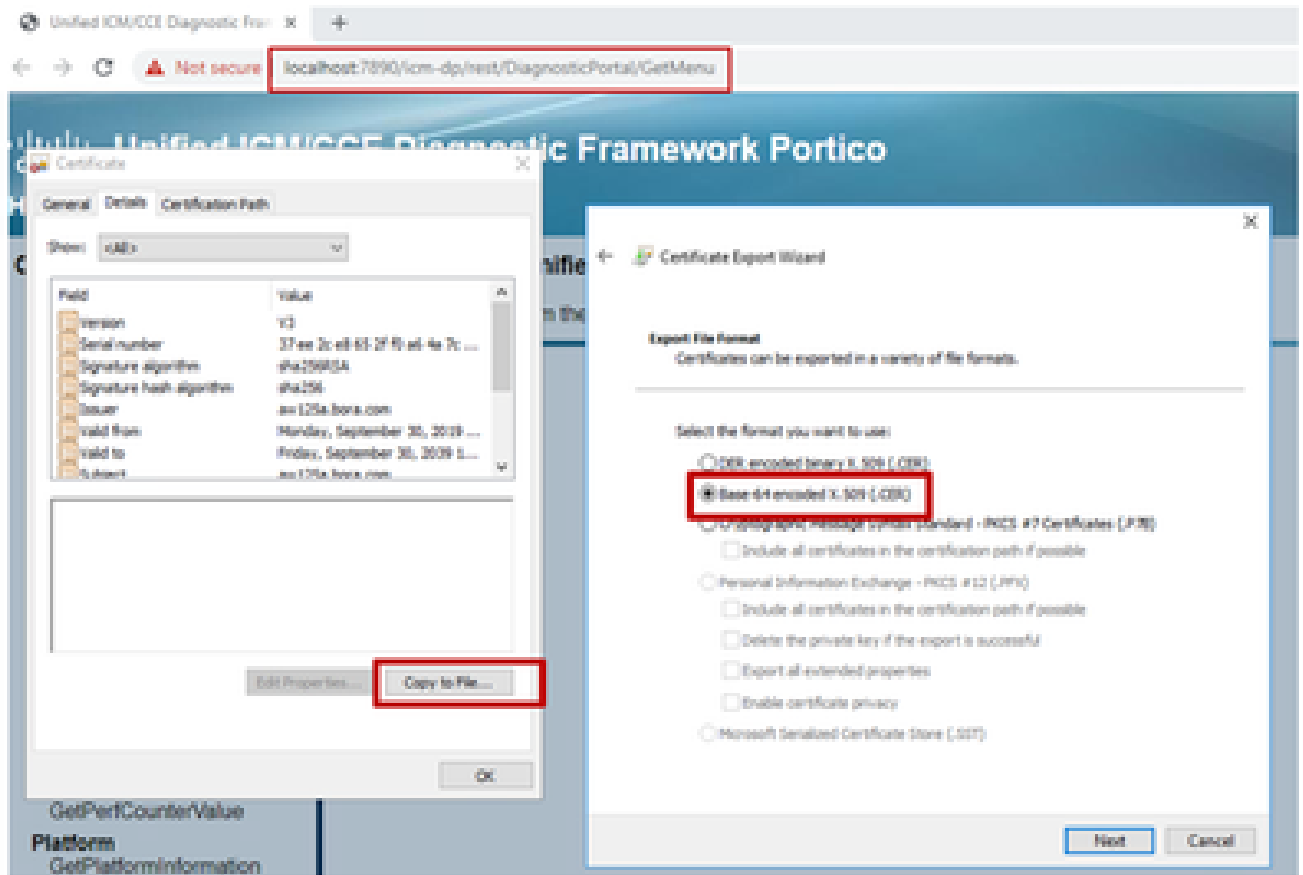
2. 例如，將證書儲存到臨時資料夾c:\temp\certs，並將證書命名為ICM{svr}[ab].cer。

 註：選擇Base-64 encoded X.509(.CER)選項。

步驟 2.從Router\Logger、PG和所有AW伺服器匯出DFP證書。

1. 在AW伺服器上，開啟瀏覽器，然後導航到伺服器 (路由器、記錄器或ROGER、PGs、AWs) DFP URL:https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion。


Portico via Chrome Browser



2. 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`。

 註：選擇 Base-64 encoded X.509(.CER) 選項。

步驟 3. 將 IIS 和 DFP 證書從路由器記錄器、PG 和 AW 匯入 AW 伺服器。

 注意：示例命令使用預設金鑰庫口令 `changeit`。如果您已修改系統上的密碼，則必須更改此設定。

命令將 IIS 自簽名證書匯入 AW 伺服器。運行 `keytool` 的路徑為：`%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：匯入匯出到所有 AW 伺服器的所有伺服器證書。

用於將 DFP 自簽名證書匯入 AW 伺服器的命令：

```
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：匯入匯出到所有AW伺服器的所有伺服器證書。

在AW伺服器上重新啟動Apache Tomcat服務。

步驟 4.從AW伺服器將IIS證書匯入Router\Logger和PG。

用於將AW IIS自簽名證書匯入到Router\Logger和PG伺服器的命令：

```
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：匯入匯出到A端和B端的Router\Logger和PG伺服器的所有AW IIS伺服器證書。

在路由器\記錄器和PG伺服器上重新啟動Apache Tomcat服務。

第2部分。VOS平台應用程式和AW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平台應用程式證書匯入AW伺服器。

此過程適用於所有VOS應用程式，例如：

- Finesse
- CUIC\LD\IDS
- 雲端連線

步驟 1.匯出VOS平台應用伺服器證書。

i.導航到Cisco Unified Communications作業系統管理頁面: <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的主伺服器證書。

tomcat-trust	Issuer	Signature	Key	Key Usage	Key Algorithm	Key Size	Key Type
tomcat-trust	Cisco_EOC_Root_CA	Self-signed	EC		Cisco_EOC_Root_CA		Cisco_EOC_Root_CA
tomcat-trust	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Self-signed	RSA		Hellenic_Academic_and_Research_Institutions_RootCA_2011		Hellenic_Academic_and_Research_Institutions
tomcat-trust	GlobalSign_Global_Root_CA	Self-signed	RSA		GlobalSign_Global_Root_CA		GlobalSign_Global_Root_CA
tomcat-trust	Amazon_Root_CA_4	Self-signed	EC		Amazon_Root_CA_4		Amazon_Root_CA_4
tomcat-trust	DigiNotar_Global_Root_CA_X3	Self-signed	RSA		DigiNotar_Global_Root_CA_X3		DigiNotar_Global_Root_CA_X3
tomcat-trust	AddTrust_Internal_CA_Root	Self-signed	RSA		AddTrust_Internal_CA_Root		AddTrust_Internal_CA_Root
tomcat-trust	ccp.bora.com	Self-signed	RSA		ccp.bora.com		ccp.bora.com
tomcat-trust	Trustee_GlobalRoot_Class_3	Self-signed	RSA		Trustee_GlobalRoot_Class_3		Trustee_GlobalRoot_Class_3
tomcat-trust	DigiCert_Global_Root_G2	Self-signed	RSA		DigiCert_Global_Root_G2		DigiCert_Global_Root_G2

iii. 選擇證書並按一下Download .PEM File，以便將其儲存在AW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: 5C35B3A89A89747198885B6A92CF710D
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
88e0e816e64ad44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
```

Delete Download .PEM File Download .DER File

註：對訂戶執行相同步驟。


步驟 2. 將VOS平台應用程式匯入AW伺服器。

運行Key工具的路徑：{JAVA_HOME}\bin

用於匯入自簽名證書的命令：

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

在AW伺服器上重新啟動Apache Tomcat服務。

 注意：在其他AW伺服器上執行相同的任務。

CVP OAMP伺服器 and CVP 元件伺服器

這些是匯出自簽名證書的元件和必須將自簽名證書匯入其中的元件。

i. CVP OAMP伺服器：此伺服器需要來自以下位置的證書：

- Windows平台：來自CVP伺服器和報告伺服器的Web服務管理器(WSM)證書。
- VOS平台：適用於客戶虛擬代理(CVA)整合的Cisco VVB，適用於Webex體驗管理(WXM)整合的雲連線伺服器。

ii. CVP伺服器：此伺服器需要來自以下位置的證書：

- Windows平台：來自OAMP伺服器的WSM證書。
- VOS平台：適用於WXM整合的雲連線伺服器和Cisco VVB伺服器。

iii. CVP報告伺服器：此伺服器需要來自以下位置的證書：

- Windows平台：來自OAMP伺服器的WSM證書。

iv. Cisco VVB伺服器：此伺服器需要來自以下位置的證書：

- Windows平台：來自CVP伺服器的VXML證書和來自CVP伺服器的Callserver證書。

以下三節介紹了在CVP環境中有效交換自簽名證書所需的步驟。

第1部分。CVP OAMP伺服器與CVP伺服器及報告伺服器之間的證書交換。

第2部分。CVP OAMP伺服器和VOS平台應用之間的證書交換。

第3部分。CVP伺服器和VVB伺服器之間的證書交換。


第1部分。CVP OAMP伺服器與CVP伺服器及報告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CVP伺服器、報告伺服器和OAMP伺服器匯出WSM證書。

步驟 2. 將WSM證書從CVP伺服器和報告伺服器匯入OAMP伺服器。

步驟 3. 將CVP OAMP伺服器WSM證書匯入CVP伺服器和報告伺服器。

 注意：開始之前，必須完成以下操作：

1. 以管理員身份開啟命令視窗。
 2. 要識別金鑰庫密碼，請運行命令 `more %CVP_HOME%\conf\security.properties`。
 3. 運行keytool命令時需要此密碼。
-

 4. 從目錄% CVP_HOME%\conf\security\ , 運行命令 `copy .keystore backup.keystore`。

步驟 1. 從CVP伺服器、報告伺服器和OAMP伺服器匯出WSM證書。

i. 將WSM證書從每台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wsmX.crt。將X替換為伺服器的主機名。例如wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.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
```

ii. 從每台伺服器的路徑複製C:\Cisco\CVP\conf\security\wsm.crt證書，並根據伺服器類wsmX.crt型將其重新命名。

步驟 2. 將WSM證書從CVP伺服器和報告伺服器匯入OAMP伺服器。

i. 將WSM證書從每個CVP伺服器和報告伺服器(wsmX.crt)複製到% CVP_HOME%\conf\security OAMP伺服器上的目錄。

ii. 使用以下命令匯入這些證書：

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

iii. 重新啟動伺服器。

步驟 3. 將WSM證書從CVP OAMP伺服器匯入CVP伺服器和報告伺服器。

i. 將OAMP伺服器WSM證書(wsmoampX.crt)複製到% CVP_HOME%\conf\security所有CVP伺服器和報告伺服器上的目錄。

ii. 使用以下命令匯入證書：

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

iii. 重新啟動伺服器。

第2部分。CVP OAMP伺服器和VOS平台應用程式之間的證書交換

成功完成此交換所需的步驟為：

步驟 1. 從VOS平台匯出應用證書。

步驟 2.將VOS應用程式證書匯入OAMP伺服器。


此過程適用於VOS應用程式，例如：

- CUCM
- VVB
- 雲端連線

步驟 1.從VOS平台匯出應用證書。

i.導航到Cisco Unified Communications作業系統管理頁面: <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的主伺服器證書。



Name	Status	Key Size	Issuer	Expiration Date
tomcat-trust: theste_primary_root_ca_-_03	signed	self-signed	RSA: theste_primary_root_ca_-_03	theste_primary_root_ca_-_03
tomcat-trust: GlobalSign	self-signed	EC	GlobalSign	GlobalSign
tomcat-trust: EE_Certification_Centre_Root_CA	self-signed	RSA	EE_Certification_Centre_Root_CA	EE_Certification_Centre_Root_CA
tomcat-trust: GlobalSign_Root_CA	self-signed	RSA	GlobalSign_Root_CA	GlobalSign_Root_CA
tomcat-trust: TruCA_Root_Certification_Authority	self-signed	RSA	TruCA_Root_Certification_Authority	TruCA_Root_Certification_Authority
tomcat-trust: Business_Class_3_Root_CA	self-signed	RSA	Business_Class_3_Root_CA	Business_Class_3_Root_CA
tomcat-trust: Starfield_Services_Root_Certificate_Authority_-_03	self-signed	RSA	Starfield_Services_Root_Certificate_Authority_-_03	Starfield_Services_Root_Certificate_Authority_-_03
tomcat-trust: VeriSign_Class_3_Public_Primary_Certification_Authority_-_03	self-signed	RSA	VeriSign_Class_3_Public_Primary_Certification_Authority_-_03	VeriSign_Class_3_Public_Primary_Certification_Authority_-_03
tomcat-trust: vob123.ibm.com	self-signed	RSA	vob123.ibm.com	vob123.ibm.com
tomcat-trust: Xtreme_Global_Certification_Authority	self-signed	RSA	Xtreme_Global_Certification_Authority	Xtreme_Global_Certification_Authority

iii.選擇證書並按一下Download .PEM File，以便將其儲存在OAMP伺服器上的臨時資料夾中。

Status

 Status: Ready

Certificate Settings

File Name	vvb125.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: 68FE55F56F863110B44D835B825D84D3
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Validity From: Thu Dec 05 06:51:10 PST 2019
To: Tue Dec 03 06:51:09 PST 2024
Subject Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb
9fe42726c826e36113207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065
7096e81d65bdcd0cadbcdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c
a911b95cf7dbc9c9e27b9d1d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e
c77de1da40e15f1c0ae40bc03dd815ceab5fc46a00dacc81013bd693614684c27e05de2004553004
```

步驟 2. 將VOS應用程式證書匯入OAMP伺服器。

i. 將VOS憑證複製到OAMP%`CVP_HOME%\conf\security`伺服器上的目錄。

ii. 使用以下命令匯入證書：

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

iii. 重新啟動伺服器。

第3部分。CVP伺服器和VVB伺服器之間的證書交換

這是一個可選步驟，用於保護CVP和其他聯絡中心元件之間的SIP通訊。更多資訊，請參閱CVP配置指南：[CVP配置指南 — 安全](#)。

CVP Call Studio 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 and 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 — 安全](#)
- [UCCE 安全指南](#)
- [PCCE 管理員指南 — 安全](#)
- [Exchange PCCE 自簽名證書 — PCCE 12.5](#)
- [Exchange UCCE 自簽名證書 — UCCE 12.5](#)
- [Exchange PCCE 自簽名證書 — PCCE 12.6](#)
- [實施 CA 簽名的證書 — CCE 12.6](#)
- [CCE OpenJDK 遷移](#)
- [CVP OpenJDK 遷移](#)
- [證書交換實用程式](#)
- [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）。