

# PCCE 12.6ソリューションでの自己署名証明書の交換

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景](#)

[手順](#)

[セクション1:CVPサーバとADSサーバ間の証明書の交換](#)

[ステップ 1: CVPサーバ証明書のエクスポート](#)

[ステップ 2: CVPサーバのWSM証明書のADSサーバへのインポート](#)

[ステップ 3: ADSサーバ証明書のエクスポート](#)

[ステップ 4: CVPサーバおよびレポーティングサーバへのADSサーバ証明書のインポート](#)

[セクション2:VOSプラットフォームアプリケーションとADSサーバ間の証明書の交換](#)

[ステップ 1: VOSプラットフォームアプリケーションサーバ証明書のエクスポート](#)

[ステップ 2: VOSプラットフォームアプリケーション証明書のADSサーバへのインポート](#)

[ステップ 3: CUCM PGサーバへのCUCMプラットフォームアプリケーション証明書のインポート](#)

[セクション3: Rogger、PG、およびADSサーバ間での証明書の交換](#)

[ステップ 1: RoggerサーバとPGサーバからのIIS証明書のエクスポート](#)

[ステップ 2: RoggerサーバとPGサーバからのDFP証明書のエクスポート](#)

[ステップ 3: ADSサーバへの証明書のインポート](#)

[ステップ 4: RoggerサーバとPGサーバへのADS証明書のインポート](#)

[セクション4:CVP CallStudio Webサービスの統合](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Cisco Packaged Contact Center Enterprise(PCCE)ソリューションで自己署名証明書(SSC)を交換する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- PCCEリリース12.6(2)
- Customer Voice Portal(CVP)リリース12.6(2)
- Virtualized Voice Browser(VVB)12.6(2)
- 管理ワークステーション(AW)/管理日付サーバ(AW/ADS)12.6(2)

- Cisco Unified Intelligenceサーバ(CUIC)
- カスタマーコラボレーションプラットフォーム(CCP)12.6(2)
- エンタープライズチャットおよび電子メール(ECE)12.6(2)

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景

12.x以降のPCCEソリューションでは、すべてのデバイスがプリンシパルAWサーバでホストされるSingle Pane of Glass(SPOG)を介して制御されます。PCCE 12.5(1)バージョンのsecurity-management-compliance(SRC)により、ソリューション内のSPOGと他のサーバ間のすべての通信は、セキュアHTTPプロトコルを使用して厳密に行われます。

証明書は、SPOGとその他のデバイス間でシームレスで安全な通信を実現するために使用されます。自己署名証明書の環境では、サーバ間の証明書交換が必須です。


## 手順

これらは、自己署名証明書のエクスポート元のコンポーネントと、自己署名証明書のインポート先のコンポーネントです。

(i)すべてのAW/ADSサーバ:これらのサーバには次の証明書が必要です。

- Windowsプラットフォーム:
  - ICM:Router and Logger(Rogger){A/B}、ペリフェラルゲートウェイ(PG){A/B}、すべてのAW/ADS、およびECEサーバ。


---

 注:IISと診断フレームワークポート(DFP)が必要です。

---

- CVP:CVPサーバ、CVレポートサーバ。

---

 注:すべてのサーバからのWebサービス管理(WSM)証明書が必要です。証明書は完全修飾ドメイン名(FQDN)で指定する必要があります。

---

- VOSプラットフォーム:Cloud Connect、Cisco Virtualized Voice Browser(VVB)、Cisco Unified Communication Manager(CUCM)、Finesse、Cisco Unified Intelligence

Center(CUIC)、ライブデータ(LD)、アイデンティティサーバ(IDS)、およびその他の該当するサーバ。


(ii) Router \ Logger Servers:これらのサーバには次の証明書が必要です。

- Windowsプラットフォーム：すべてのAW/ADSサーバはIIS証明書です。

(iii)PGサーバ:次の証明書が必要なサーバです。

- Windowsプラットフォーム：すべてのAW/ADSサーバはIIS証明書です。
- VOSプラットフォーム：CUCMパブリッシャ ( CUCM PGサーバのみ )、Cloud ConnectおよびCCP ( MR PGサーバのみ )。

---

 注：これは、CUCMサーバからJTAPIクライアントをダウンロードするために必要です。

---

(iv) CVPサーバ:このサーバには、次の証明書が必要です。

- Windowsプラットフォーム：すべてのADSサーバIIS証明書
- VOSプラットフォーム：Cloud Connectサーバ、VVBサーバ

(v) CVPLレポーティングサーバ:このサーバには、次のURLの証明書が必要です。

- Windowsプラットフォーム：すべてのADSサーバIIS証明書

(vi) VVBサーバ:このサーバには次の証明書が必要です。

- Windowsプラットフォーム：すべてのADSサーバがIIS証明書、CVPサーバからのVXML証明書、およびCVPサーバからのCallserver証明書
- VOSプラットフォーム：Cloud Connectサーバ

ソリューション内の自己署名証明書を効果的に交換するために必要な手順は、3つのセクションに分かれています。

セクション1:CVPサーバとADSサーバ間での証明書の交換。

セクション2:VOSプラットフォームアプリケーションとADSサーバ間の証明書交換。

セクション3:Router、PG、およびADSサーバ間での証明書の交換。

セクション1:CVPサーバとADSサーバ間の証明書の交換

この交換を正常に完了するために必要な手順は次のとおりです。

ステップ 1：CVPサーバのWSM証明書のエクスポート

ステップ 2：CVPサーバのWSM証明書をADSサーバにインポートします。


ステップ 3：ADSサーバ証明書をエクスポートします。

ステップ 4：ADSサーバをCVPサーバおよびCVPLレポーティングサーバにインポートします。

## ステップ 1 : CVPサーバ証明書のエクスポート


CVPサーバから証明書をエクスポートする前に、サーバのFQDNで証明書を再生成する必要があります。そうしないと、Smart Licensing、Virtual Agent Voice(VAV)、およびSPOGとのCVP同期などのいくつかの機能で問題が発生する場合があります。

---

 注意：作業を開始する前に、次の操作を行う必要があります。

1. 管理者としてコマンド・ウィンドウを開きます。
2. 12.6.2の場合、キーストアパスワードを識別するには、%CVP\_HOME%\binフォルダに移動し、DecryptKeystoreUtil.batファイルを実行します。
3. 12.6.1の場合、キーストアパスワードを識別するには、more %CVP\_HOME%\conf\security.propertiesコマンドを実行します。
4. このパスワードは、keytoolコマンドを実行するときに必要です。
5. %CVP\_HOME%\conf\security\ディレクトリから、copy .keystore backup.keystoreコマンドを実行します。

---


 注：このドキュメントで使用するコマンドは、keytoolパラメータ -storepassを使用して合理化できます。すべてのCVPサーバについて、識別したkeytoolパスワードを入力します。ADSサーバのデフォルトパスワードはchangeitです。

CVPサーバで証明書を再生成するには、次の手順を実行します。

### (i)サーバ内の証明書を一覧表示する

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

---

 注：CVPサーバには、wsm\_certificate、vxml\_certificate、callserver\_certificateの自己署名証明書があります。keytoolのパラメータ -vを使用すると、各証明書の詳細情報を確認できます。また、keytool.exe listコマンドの最後に「>」記号を追加して、出力をテキストファイルに送信できます (例：> test.txt)。

### 二旧自己署名証明書の削除

#### CVPサーバ:自己署名証明書を削除するコマンド

```
%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 Reportingサーバ：自己署名証明書を削除するコマンド：

```
%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:CVPレポーティングサーバには、wsm\_certificate、callserver\_certificateという自己署名証明書があります。

---


(iii)サーバのFQDNを使用して新しい自己署名証明書を生成する

CVPサーバ

WSMの自己署名証明書を生成するコマンド：

```
%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：デフォルトでは、証明書は2年間生成されます。-validity XXXXを使用して、証明書を再生成する有効期限を設定します。有効期限を設定しない場合、証明書は90日間有効であり、この時間の前にCAによって署名される必要があります。これらの証明書のほとんどでは、3～5年は妥当な検証期間である必要があります。

---

標準的な有効性入力の一部を次に示します。

1年	365
二年	730
三年	1095
4年間	1460
五年	1895

十年	3650
----	------

**⚠ 注意:**12.5以降の証明書はSHA 256、キーサイズ2048、暗号化アルゴリズムRSAにする必要があります。次のパラメータを使用して値を設定します：-keyalg RSAおよび -keysize 2048。CVPキーストアコマンドに -storetype JCEKSパラメータが含まれていることが重要です。これを行わないと、証明書、キー、または悪い場合にはキーストアが破損する可能性があります。

サーバのFQDNを指定します。質問の最初と最後の名前は何か。

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\conf\security\keystore -alias w
sm_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]:
```

次の質問に教えてください。

組織単位の名前は何か。

[不明]: <OUを指定>

組織の名前は何か。

[不明]: <組織の名前を指定>

市区町村の名前は何か。

[不明]: <市区町村の名前を指定>

都道府県の名前を入力してください。

[不明]: <都道府県の名前を指定>

このユニットの2文字の国番号は何か。

[不明]: <2文字の国番号を指定>

次の2つの入力にはyesを指定します。

vxml\_certificateとcallserver\_certificateに対して同じ手順を実行します。

```
%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
```

CVPコールサーバをリブートします。

CVP Reportingサーバ

WSMの自己署名証明書を生成するコマンド：

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

クエリ用のサーバのFQDN(最初と最後の名前)を指定し、CVPサーバで行った手順と同じ手順を続行します。

callserver\_certificateについても同じ手順を実行します。

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

レポートサーバをリブートします。

(iv) CVPサーバおよびレポートサーバからのwsm\_Certificateのエクスポート

a)各CVPサーバから一時的な場所にWSM証明書をエクスポートし、証明書の名前を任意の名前に変更します。名前はwsmcsX.crtに変更できます。「X」をサーバのホスト名に置き換えます。たとえば、wsmcsa.crt、wsmcsb.crt、wsmrepa.crt、wsmrepb.crtなどです。

自己署名証明書をエクスポートするコマンド：

```
%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)証明書をパス%CVP\_HOME%\conf\security\wsm.crtからコピーし、名前をwsmcsX.crtに変更して、ADSサーバ上の一時フォルダに移動します。

ステップ 2：CVPサーバのWSM証明書のADSサーバへのインポート

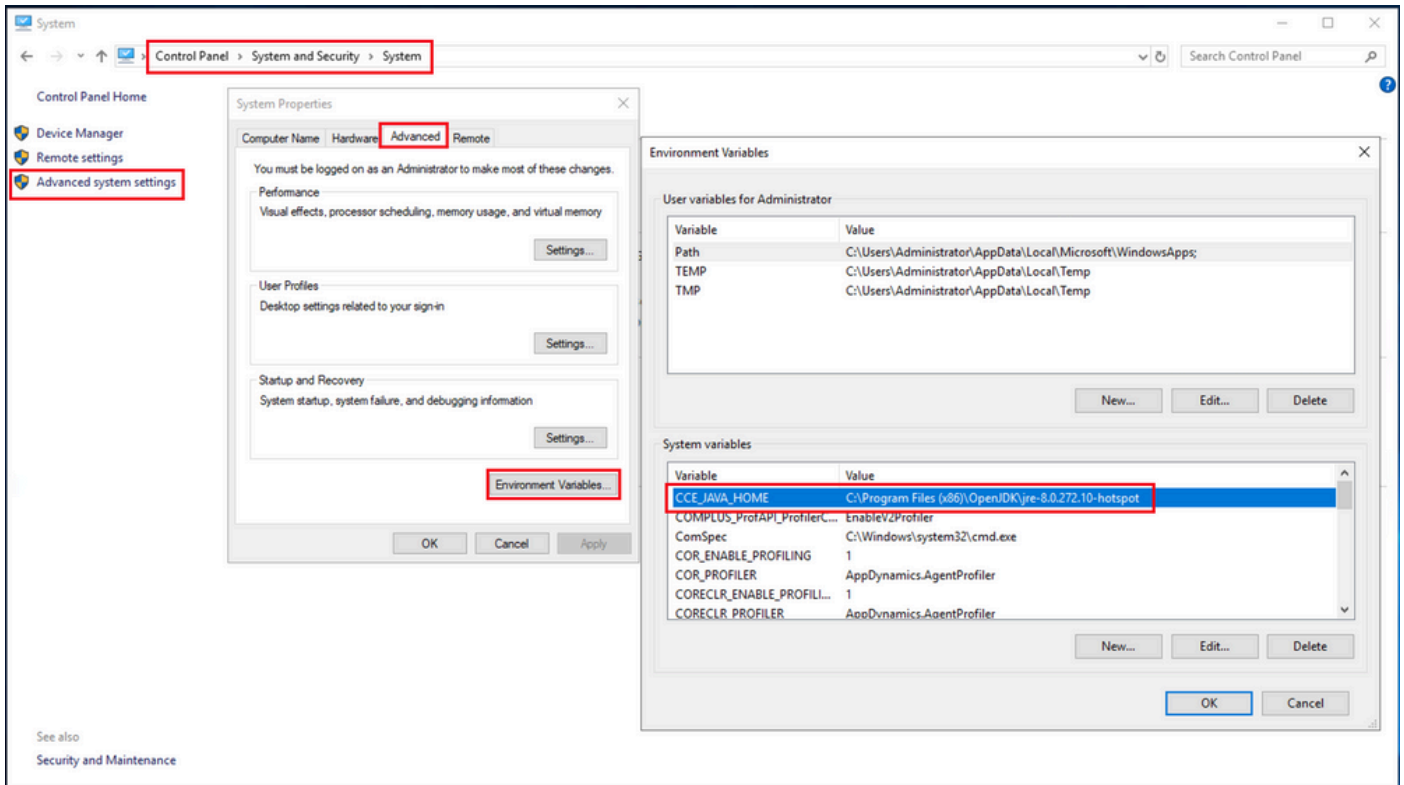
ADSサーバーに証明書をインポートするには、Javaツールセットの一部であるキーツールを使用する必要があります。このツールがホストされているJavaホームパスを見つける方法がいくつかあります。

(i) CLIコマンド>echo %CCE\_JAVA\_HOME%

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

Javaホームパス

(ii)図に示すように、高度なシステム設定を手動で実行します。




環境変数

PCCE 12.6では、OpenJDKのデフォルトパスはC:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\binです。

自己署名証明書をインポートするコマンド：

```
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：導入環境内の各CVPに対してコマンドを繰り返し、他のADSサーバで同じタスクを実行します

(iii) ADSサーバでApache Tomcatサービスを再起動します。

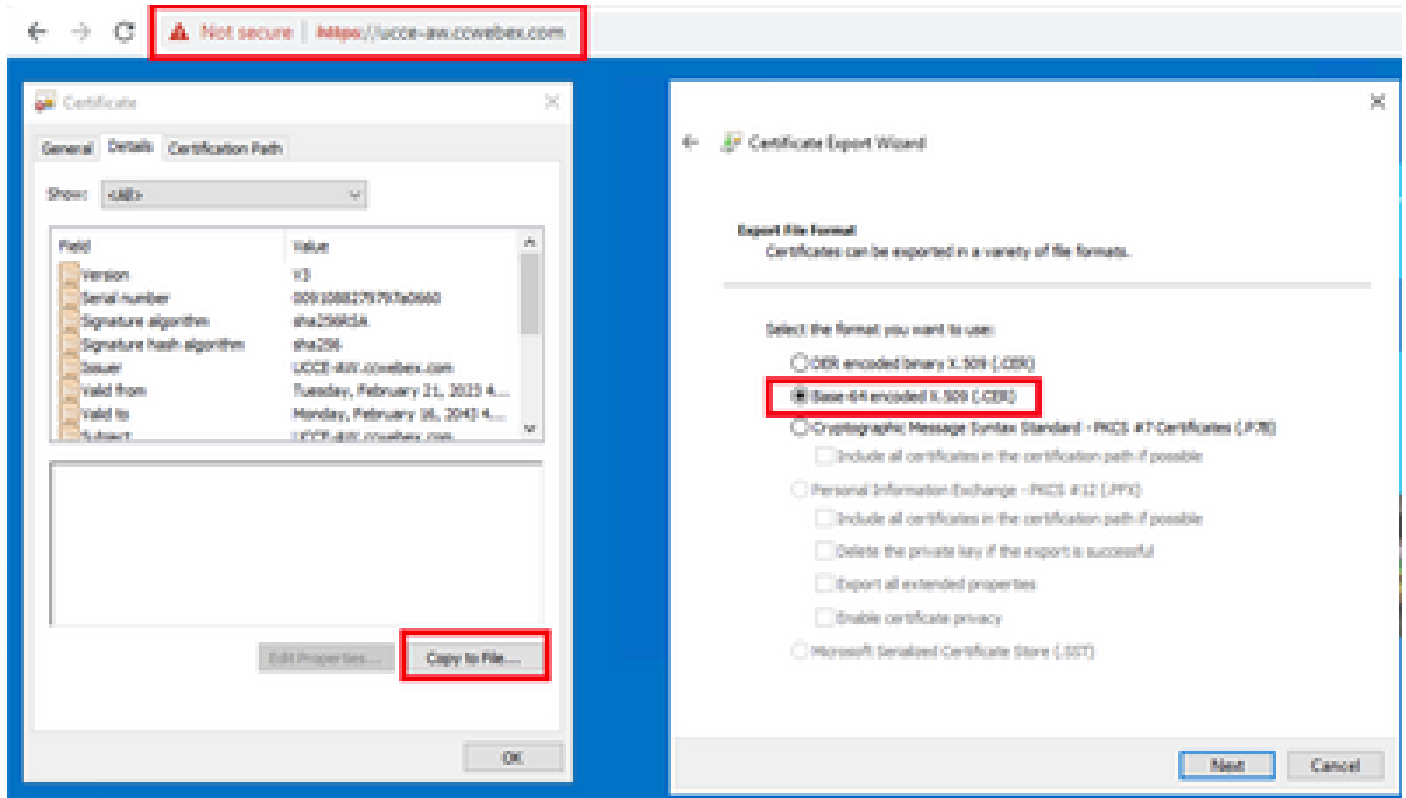
ステップ 3：ADSサーバー証明書のエクスポート



次に、ADS証明書をエクスポートする手順を示します。

(i) ADSサーバで、ブラウザからサーバURL `https://<servername>`に移動します。

(ii) 証明書を一時フォルダ(例 : `c:\temp\certs`)に保存し、証明書に`ADS<svr>[ab].cer`という名前を付けます。



ADS証明書のエクスポート

 注 : オプションBase-64 encoded X.509 (.CER)を選択します。

ステップ 4 : CVPサーバおよびレポーティングサーバへのADSサーバ証明書のインポート

(i) 証明書をディレクトリ`%CVP_HOME%\conf\security`にあるCVPサーバおよびCVPレポートサーバにコピーします。

(ii) CVPサーバおよびCVPレポーティングサーバに証明書をインポートします。

```
%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
```

他のADSサーバーの証明書についても同じ手順を実行します。

(iii) CVPサーバとレポートサーバを再起動する

## セクション2:VOSプラットフォームアプリケーションとADSサーバ間の証明書の交換

この交換を正常に完了するために必要な手順は次のとおりです。

ステップ 1 : VOSプラットフォームアプリケーションサーバ証明書のエクスポート

ステップ 2 : VOSプラットフォームアプリケーション証明書をADSサーバにインポートします。

ステップ 3 : CUCM PGサーバへのCUCMプラットフォームアプリケーション証明書のインポート

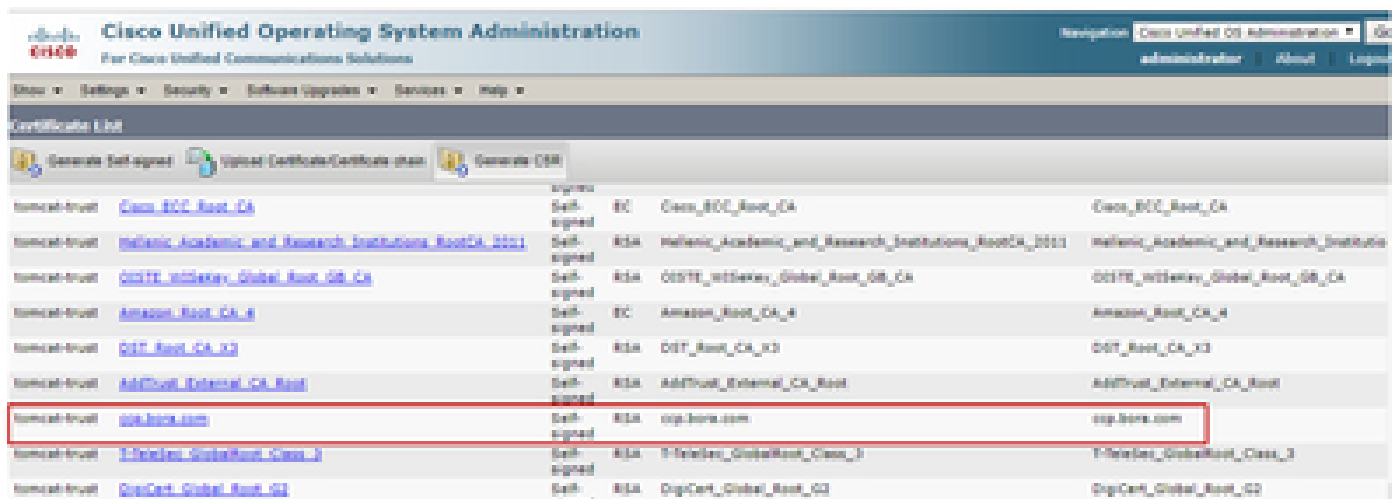
このプロセスは、次のようなすべてのVOSアプリケーションに適用できます。

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- Cloud Connect

ステップ 1 : VOSプラットフォームアプリケーションサーバ証明書のエクスポート

(i) Cisco Unified Communications Operating System Administrationページ  
(<https://FQDN:8443/cmplatform>)に移動します。

(ii) Security > Certificate Managementの順に移動し、tomcat-trustフォルダ内にアプリケーションプライマリサーバ証明書があることを確認します。



tomcat-trust	Self-signed	EC	Self-signed	Self-signed
<a href="#">Cisco_ECC_Root_CA</a>	Self-signed	EC	Cisco_ECC_Root_CA	Cisco_ECC_Root_CA
<a href="#">Hellenic_Academic_and_Research_Institutions_RootCA_2011</a>	Self-signed	RSA	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Hellenic_Academic_and_Research_Institutions
<a href="#">OCITE_wiSecurity_Global_Root_CA</a>	Self-signed	RSA	OCITE_wiSecurity_Global_Root_CA	OCITE_wiSecurity_Global_Root_CA
<a href="#">Amazon_Root_CA_4</a>	Self-signed	EC	Amazon_Root_CA_4	Amazon_Root_CA_4
<a href="#">DIT_Root_CA_X3</a>	Self-signed	RSA	DIT_Root_CA_X3	DIT_Root_CA_X3
<a href="#">AddTrust_Internal_CA_Root</a>	Self-signed	RSA	AddTrust_Internal_CA_Root	AddTrust_Internal_CA_Root
<a href="#">osp.bora.com</a>	Self-signed	RSA	osp.bora.com	osp.bora.com
<a href="#">T-TeleSec_GlobalRoot_Class_3</a>	Self-signed	RSA	T-TeleSec_GlobalRoot_Class_3	T-TeleSec_GlobalRoot_Class_3
<a href="#">DigiCert_Global_Root_G2</a>	Self-signed	RSA	DigiCert_Global_Root_G2	DigiCert_Global_Root_G2


(iii)証明書を選択し、「download .PEM file」をクリックしてADSサーバの一時フォルダに保存します。

**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
```

 注：サブスクリバに対して同じ手順を実行します。


ステップ 2：VOSプラットフォームアプリケーション証明書のADSサーバへのインポート

キーツールを実行するパス： %CCE\_JAVA\_HOME%\bin

自己署名証明書をインポートするコマンド：

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias {fqdn_of_VOS>} -keystore {ICM install directory}\ssl\cacerts
```

ADSサーバでApache Tomcatサービスを再起動します。

 注：他のADSサーバでも同じタスクを実行します

ステップ 3：CUCM PGサーバへのCUCMプラットフォームアプリケーション証明書のインポート

キーツールを実行するパス： %CCE\_JAVA\_HOME%\bin

自己署名証明書をインポートするコマンド：

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\cucmapplicationX.cer -alias {fqdn_of_cucm>} -keystore {ICM install directory}\ssl\cacerts
```

PGサーバでApache Tomcatサービスを再起動します。



注：他のCUCM PGサーバでも同じタスクを実行します

---

### セクション3: Rogger、PG、およびADSサーバ間での証明書の交換

この交換を正常に完了するために必要な手順は次のとおりです。

ステップ 1：RoggerサーバとPGサーバからのIIS証明書のエクスポート

ステップ 2：RoggerサーバとPGサーバからのDFP証明書のエクスポート

ステップ 3：ADSサーバへの証明書のインポート

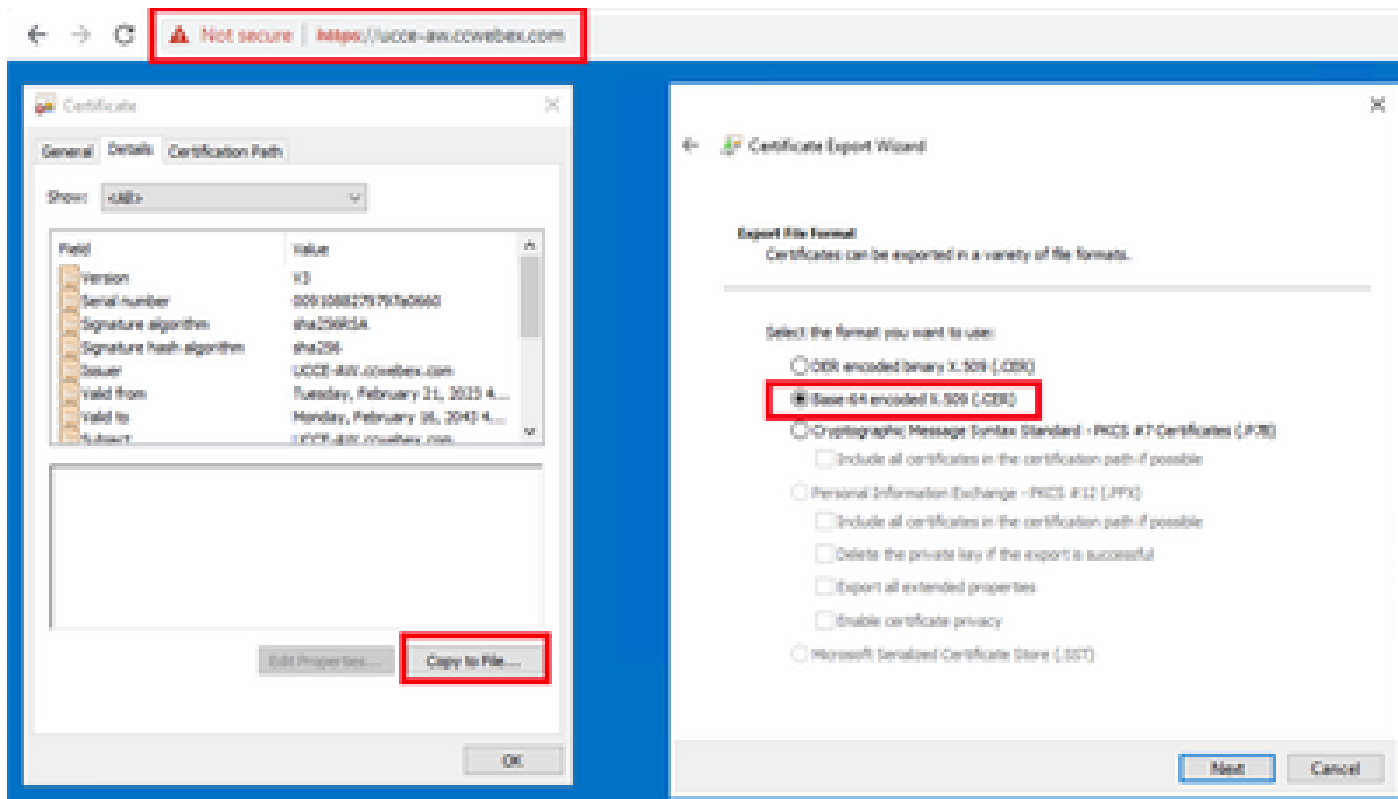
ステップ 4：RoggerサーバとPGサーバへのADS証明書のインポート

ステップ 1：RoggerサーバとPGサーバからのIIS証明書のエクスポート

(i) ブラウザからADSサーバで、サーバ(Rogger、PG)のURL: <https://{servername}> に移動します。

(ii) 証明書を一時フォルダ(c:\temp\certsなど)に保存し、証明書の名前をICM<svr>[ab].cerとします

。



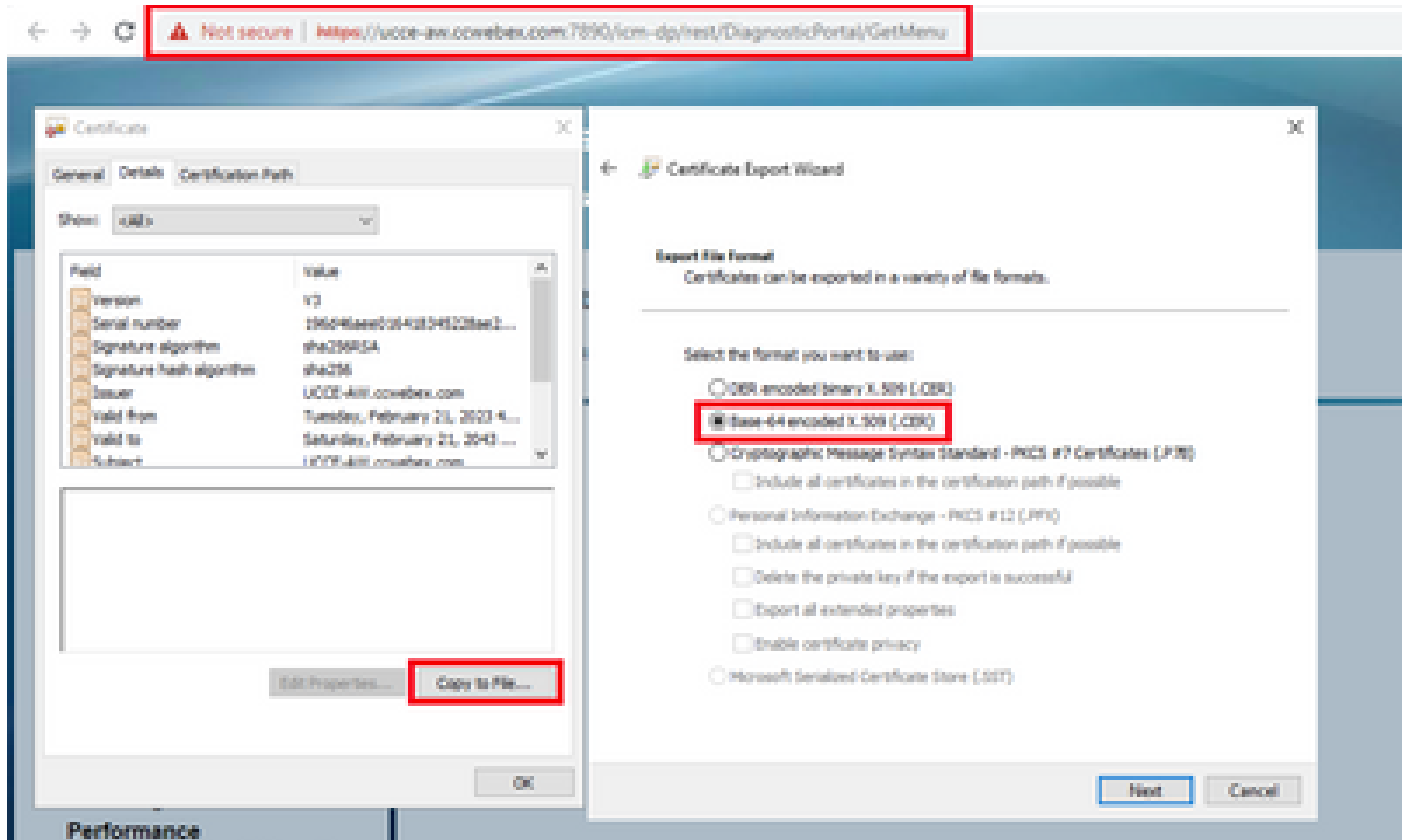
IIS証明書のエクスポート

 注：オプションBase-64 encoded X.509 (.CER)を選択します。

ステップ 2：RogerサーバとPGサーバからのDFP証明書のエクスポート

(i) ブラウザからADSサーバで、サーバ(Rogger、PG)のDFP url:https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersionに移動します。

(ii) 証明書をフォルダexample c:\temp\certsに保存し、証明書にdfp{svr}[ab].cerという名前を付けます



DFP証明書のエクスポート

 注：オプションBase-64 encoded X.509 (.CER)を選択します。

### ステップ 3：ADSサーバへの証明書のインポート

IIS自己署名証明書をADSサーバにインポートするコマンド。キーツールを実行するパス：  
%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：エクスポートされたすべてのサーバ証明書をすべてのADSサーバにインポートします。

### 診断のための自己署名証明書をADSサーバにインポートするコマンド

```
%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：エクスポートされたすべてのサーバ証明書をすべてのADSサーバにインポートします。


ADSサーバでApache Tomcatサービスを再起動します。

ステップ 4 : RoggerサーバとPGサーバへのADS証明書のインポート

IIS自己署名証明書をRoggerおよびPGサーバにインポートするコマンド。キーツールを実行するパス : %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 : すべてのRoggerおよびPGサーバにエクスポートされたすべてのADSサーバIIS証明書をインポートします。

---

RoggerサーバとPGサーバでApache Tomcatサービスを再起動します。

## セクション4:CVP CallStudio Webサービスの統合

Webサービス要素とRest\_Client要素のセキュアな通信を確立する方法の詳細については、

詳細については、『[Cisco Unified CVP VXML ServerおよびCisco Unified Call Studioリリース 12.6\(2\) - Webサービスの統合\[Cisco Unified Customer Voice Portal\] – シスコのユーザガイド](#)』

## 関連情報

- [CVP設定ガイド – セキュリティ](#)
- [UCCEセキュリティガイド](#)
- [PCCE管理ガイド](#)
- [Exchange PCCE自己署名証明書 – PCCE 12.5](#)
- [Exchange UCCE自己署名証明書 – UCCE 12.5](#)
- [Exchange UCCE自己署名証明書 – UCCE 12.6](#)
- [CA署名付き証明書の実装 – CCE 12.6](#)
- [Contact Center Uploaderツールを使用した証明書の交換](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。