

Exchange des certificats autosignés dans une solution PCCE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Fond](#)

[Procédure](#)

[Section 1 : Échange de certificats entre serveurs CVP et ADS](#)

[Étape 1. Exporter les certificats de serveur CVP](#)

[Étape 2. Importer le certificat WSM des serveurs CVP sur le serveur ADS](#)

[Étape 3. Exporter le certificat de serveur ADS](#)

[Étape 4. Importer le serveur ADS vers les serveurs CVP et le serveur de rapports](#)

[Section 2 : Échange de certificats entre les applications de la plate-forme VOS et le serveur ADS](#)

[Étape 1. Exporter les certificats du serveur d'applications de la plate-forme VOS.](#)

[Étape 2. Importer l'application de plate-forme VOS sur le serveur ADS](#)

[Section 3 : Échange de certificats entre les serveurs Roggers, PG et ADS](#)

[Étape 1. Exporter le certificat IIS des serveurs Rogger et PG](#)

[Étape 2. Exporter le certificat DFP \(Diagnostic Framework Portico\) des serveurs Rogger et PG](#)

[Étape 3. Importer des certificats dans le serveur ADS](#)

[Section 4 : CVP CallStudio WEBSERVICE Integration](#)

[Informations connexes](#)

Introduction

Ce document décrit comment échanger des certificats auto-signés entre le serveur d'administration principal (ADS/AW) et d'autres serveurs d'applications dans la solution Cisco Packaged Contact Center Enterprise (PCCE).

Contribué par Anuj Bhatia, Robert Rogier et Ramiro Amaya, ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- PCCE version 12.5(1)
- Customer Voice Portal (CVP) version 12.5 (1)

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Fond

Dans la solution PCCE 12.x, tous les périphériques sont contrôlés via le volet unique de verre (SPOG) qui est hébergé sur le serveur principal AW. En raison de la conformité de la gestion de la sécurité (SRC) dans la version PCCE 12.5(1), toutes les communications entre SPOG et les autres serveurs de la solution sont strictement effectuées via le protocole HTTP sécurisé.

Les certificats sont utilisés pour assurer une communication transparente et sécurisée entre SPOG et les autres périphériques. Dans un environnement de certificat auto-signé, l'échange de certificat entre les serveurs devient une nécessité. Cet échange de certificats est également nécessaire pour activer de nouvelles fonctionnalités présentes dans la version 12.5(1), telles que Smart Licensing, Webex Experience Management (WXM) et Customer Virtual Assistant (CVA).

Procédure

Il s'agit des composants à partir desquels les certificats auto-signés sont exportés et des composants dans lesquels les certificats auto-signés doivent être importés.

(i) Serveur principal AW : Ce serveur requiert un certificat de :

- Plate-forme Windows : ICM : Router and Logger(Rogger){A/B}, Peripheral Gateway (PG){A/B}, tous les serveurs ADS et Email and Chat (ECE). Note: Les certificats IIS et de cadre de diagnostic sont nécessaires.CVP : Serveurs CVP, serveur de rapports CVP. Remarque 1 : Le certificat de gestion des services Web (WSM) des serveurs est nécessaire.Remarque 2 : Les certificats doivent être dotés d'un nom de domaine complet (FQDN).
- Plate-forme VOS : Cloud Connect, Cisco Virtual Voice Browser (VVB), Cisco Unified Call Manager (CUCM), Finesse, Cisco Unified Intelligent Center (CUIC), Live Data (LD), Identity Server (IDS) et autres serveurs applicables.

Il en va de même pour les autres serveurs ADS de la solution.

(ii) Router \ Logger Server : Ce serveur requiert un certificat de :

- Plate-forme Windows : certificat IIS de tous les serveurs ADS.

(iii) CUCM PG Server : Ce serveur requiert un certificat de :

- Plate-forme VOS : Éditeur CUCM. Note: Ceci est nécessaire pour télécharger le client JTAPI à partir du serveur CUCM.

(iv) Serveur CVP : Ce serveur requiert un certificat de

- Plate-forme Windows : certificat IIS de tous les serveurs ADS

- Plate-forme VOS : Serveur Cloud Connect pour l'intégration WXM, serveur VVB pour les communications SIP et HTTP sécurisées.

v) **Serveur de rapports CVP** : Ce serveur requiert un certificat de :

- Plate-forme Windows : certificat IIS de tous les serveurs ADS

vi) **Serveur VVB** : Ce serveur requiert un certificat de :

- Plate-forme Windows : Serveur VXML CVP (HTTP sécurisé), serveur d'appels CVP (SIP sécurisé)

Les étapes nécessaires pour échanger efficacement les certificats auto-signés dans la solution sont divisées en trois sections.

Section 1 : Échange de certificats entre les serveurs CVP et ADS.

Section 2 : Échange de certificats entre les applications de la plate-forme VOS et le serveur ADS.

Section 3 : Échange de certificats entre Rogers, PG et ADS Server.

Section 1 : Échange de certificats entre serveurs CVP et ADS

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exporter les certificats WSM du serveur CVP.

Étape 2. Importer le certificat WSM du serveur CVP sur le serveur ADS.

Étape 3. Exporter le certificat du serveur ADS.

Étape 4. Importez ADS Server vers les serveurs CVP et CVP Reporting Server.

Étape 1. Exporter les certificats de serveur CVP

Avant d'exporter les certificats à partir des serveurs CVP, vous devez régénérer les certificats avec le nom de domaine complet du serveur. Sinon, peu de fonctionnalités telles que Smart Licensing, CVA et la synchronisation CVP avec SPOG peuvent rencontrer des problèmes.

Attention : Avant de commencer, procédez comme suit :

- Obtenez le mot de passe de la banque de clés. Exécutez cette commande :
plus %CVP_HOME%\conf\security.properties
- Copiez le dossier %CVP_HOME%\conf\security dans un autre dossier.
- Ouvrez une fenêtre de commande en tant qu'administrateur pour exécuter les commandes.

Note: Vous pouvez rationaliser les commandes utilisées dans ce document en utilisant le paramètre keytool -storepass. Pour tous les serveurs CVP, collez le mot de passe obtenu à partir du fichier security.properties spécifié. Pour les serveurs ADS, saisissez le mot de passe : **modifier**

Pour régénérer le certificat sur les serveurs CVP, procédez comme suit :

(i) Répertoire les certificats dans le serveur

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

Note: Les serveurs CVP possèdent les certificats auto-signés suivants : wsm_certificate, vxml_certificate, callserver_certificate. Si vous utilisez le paramètre -v de l'outil clé, vous pouvez voir des informations plus détaillées sur chaque certificat. En outre, vous pouvez ajouter le symbole ">" à la fin de la commande keytool.exe list pour envoyer le résultat à un fichier texte, par exemple : > test.txt

ii) Supprimer les anciens certificats autosignés

Serveurs CVP : commande permettant de supprimer les certificats auto-signés :

```
%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
```

Serveurs de rapports CVP : commande permettant de supprimer les certificats auto-signés :

```
%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
```

Note: Les serveurs de rapports CVP ont ces certificats auto-signés wsm_certificate, callserver_certificate.

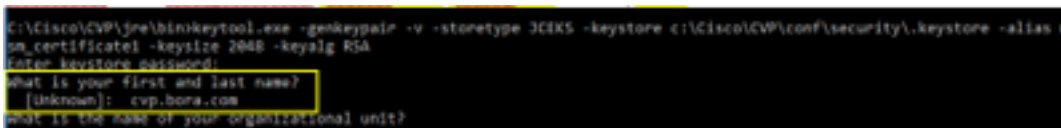
(iii) Générer les nouveaux certificats auto-signés avec le nom de domaine complet du serveur

Serveurs CVP

Commande permettant de générer le certificat auto-signé pour WSM :

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

Spécifiez le nom de domaine complet du serveur, à la question **de savoir quel est votre premier nom et votre nom ?**



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

Répondez aux autres questions suivantes :

Quel est le nom de votre unité organisationnelle ?

[Inconnu] : <préciser OU>

Quel est le nom de votre organisation ?

[Inconnu] : <indiquez le nom de l'organisation>

Quel est le nom de votre ville ou de votre localité ?

[Inconnu] : <indiquez le nom de la ville/localité>

Quel est le nom de votre État ou de votre province ?

[Inconnu] : <indiquez le nom de l'état/de la province>

Quel est le code pays à deux lettres pour cette unité ?

[Inconnu] : <indiquez le code pays à deux lettres>

Spécifiez **yes** pour les deux entrées suivantes.

Exécutez les mêmes étapes pour `vxml_certificate` et `callserver_certificate` :

```
%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
```

Redémarrez le serveur d'appels CVP.

Serveurs de rapports CVP

Commande permettant de générer les certificats auto-signés pour WSM :

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

Spécifiez le nom de domaine complet du serveur pour la requête **quel est votre premier et votre nom ?** et suivez les mêmes étapes que pour les serveurs CVP.

Exécutez les mêmes étapes pour `callserver_certificate` :

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

Redémarrez les serveurs Reporting.

Note: Par défaut, les certificats auto-signés sont générés pendant deux ans. Utilisez -value XXXX pour définir la date d'expiration lorsque les certificats sont régénérés, sinon les certificats sont valides pendant 90 jours. Pour la plupart de ces certificats, un délai de validation de 3 à 5 ans doit être raisonnable.

Voici quelques entrées de validité standard :

Un an	365
Deux ans	730
Trois ans	1095
Quatre ans	1460
Cinq ans	1895
Dix ans	3650

Attention : Dans 12.5, les certificats doivent être **SHA 256**, Key Size **2048** et encryption Algorithm **RSA**, utilisez ces paramètres pour définir ces valeurs : -keyalg RSA et -keysize 2048. Il est important que les commandes CVP keystore incluent le paramètre -storetype JCEKS. Si cela n'est pas fait, le certificat, la clé ou pire le keystore peut être corrompu.

iv) Exporter wsm_Certificate à partir de serveurs CVP et Reporting

a) Exporter le certificat WSM de chaque serveur CVP vers un emplacement temporaire et renommer le certificat avec le nom souhaité. Vous pouvez le renommer en tant que wsmcsX.crt. Remplacer « X » par un numéro ou une lettre unique. c'est wsmcsa.crt, wsmcsb.crt.

Commande d'exportation des certificats auto-signés :

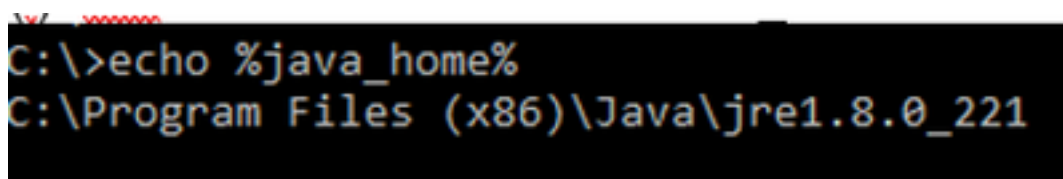
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b) Copiez le certificat à partir du chemin **C:\Cisco\CVP\conf\security\wsm.crt**, renommez-le en **wsmcsX.crt** et déplacez-le vers un dossier temporaire sur le serveur ADS.

Étape 2. Importer le certificat WSM des serveurs CVP sur le serveur ADS

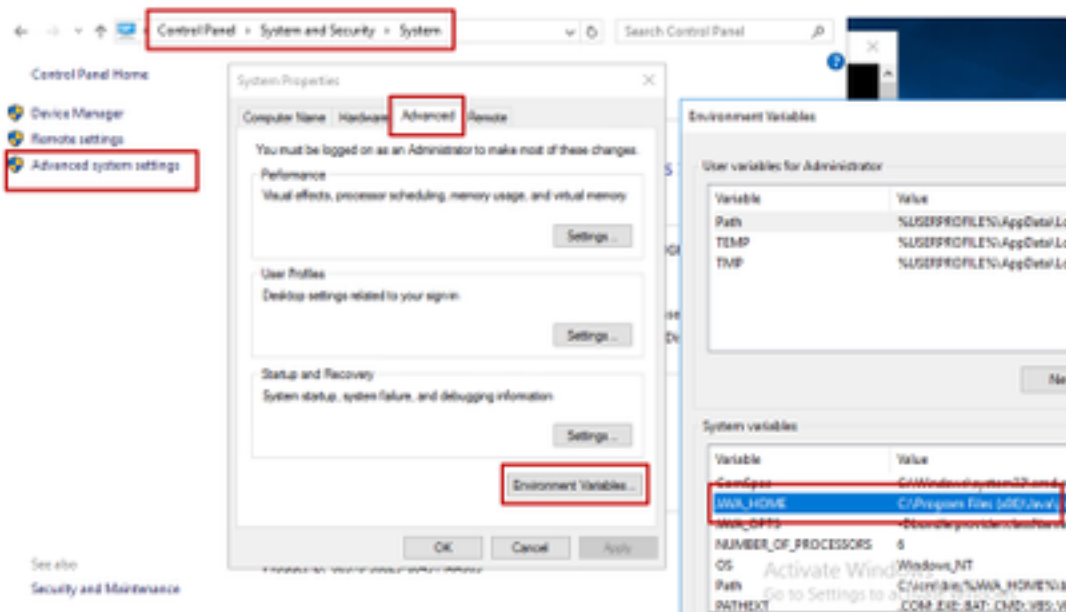
Pour importer le certificat dans le serveur ADS, vous devez utiliser le keytool qui fait partie de l'ensemble d'outils java. Il existe plusieurs façons de trouver le chemin d'accès de la maison java où cet outil est hébergé.

(i) Commande CLI > **écho %JAVA_HOME%**



```
C:\>echo %java_home%  
C:\Program Files (x86)\Java\jre1.8.0_221
```

(ii) Manuellement par **réglage avancé du système**, comme le montre l'image.



Sur PCCE 12.5, le chemin par défaut est **C:\Program Files (x86)\Java\jre1.8.0_221\bin**

Commande d'importation des certificats auto-signés :

```
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
```

Note: Répétez les commandes de chaque CVP dans le déploiement et effectuez la même tâche sur les autres serveurs ADS

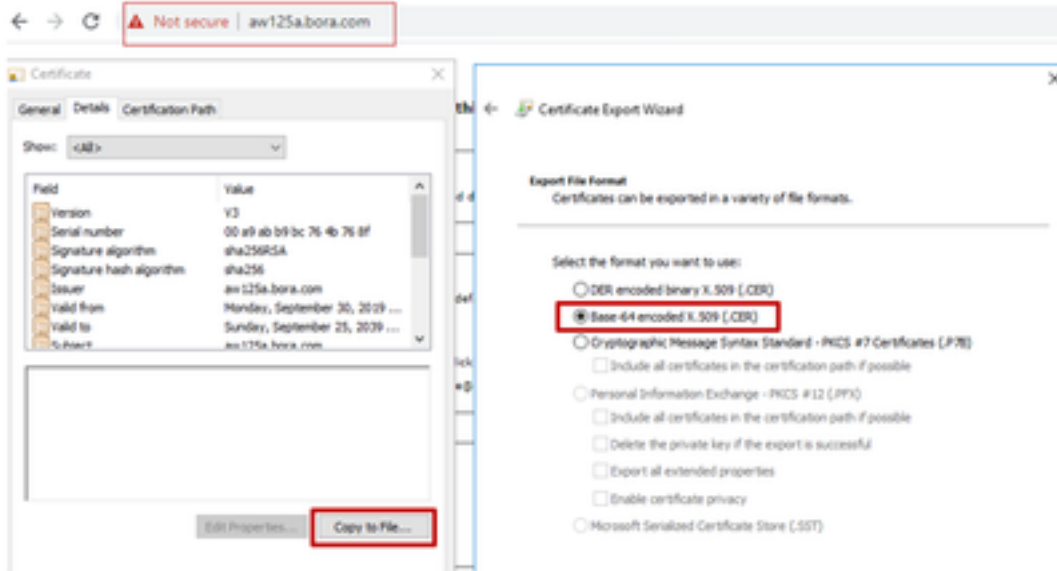
d) Redémarrez le service Apache Tomcat sur les serveurs ADS.

Étape 3. Exporter le certificat de serveur ADS

Pour le serveur de rapports CVP, vous devez exporter le certificat ADS et l'importer dans le serveur de rapports. Voici les étapes :

- (i) Sur le serveur ADS à partir d'un navigateur, accédez à l'URL du serveur : **https://{servername}**
- (ii) Enregistrez le certificat dans un dossier temporaire, par exemple : **c:\temp\certs** et nommez le certificat **ADS{svr}[ab].cer**

CCE via Chrome Browser



Note: Sélectionnez l'option Base-64 encoded X.509 (.CER).

Étape 4. Importer le serveur ADS vers les serveurs CVP et le serveur de rapports

(i) Copiez le certificat sur les serveurs CVP et le serveur de rapports CVP dans le répertoire **C:\Cisco\CVP\conf\security**.

(ii) Importez le certificat sur les serveurs CVP et CVP Reporting.

```
%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
```

Effectuez les mêmes étapes pour les autres serveurs ADS.

(iii) Redémarrer le serveur CVP Server and Reporting

Section 2 : Échange de certificats entre les applications de la plate-forme VOS et le serveur ADS

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exporter les certificats du serveur d'applications de la plate-forme VOS.

Étape 2. Importer des certificats d'application de plate-forme VOS vers le serveur ADS.

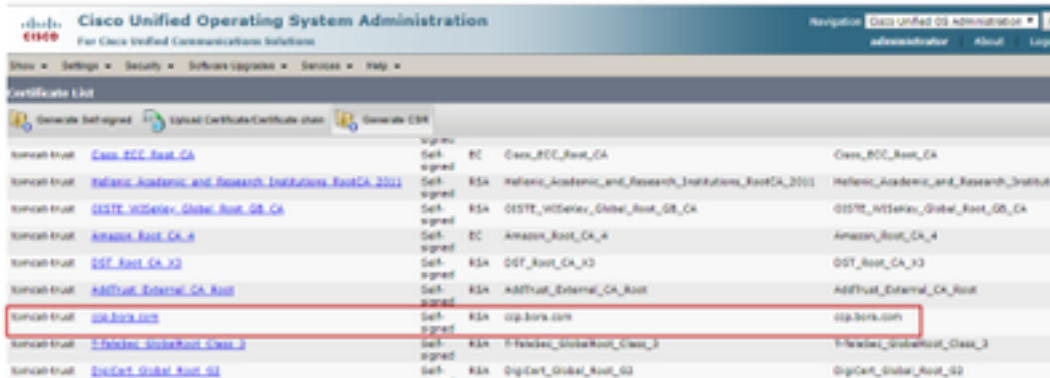
Ce processus s'applique à toutes les applications VOS telles que :

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

Étape 1. Exporter les certificats du serveur d'applications de la plate-forme VOS.

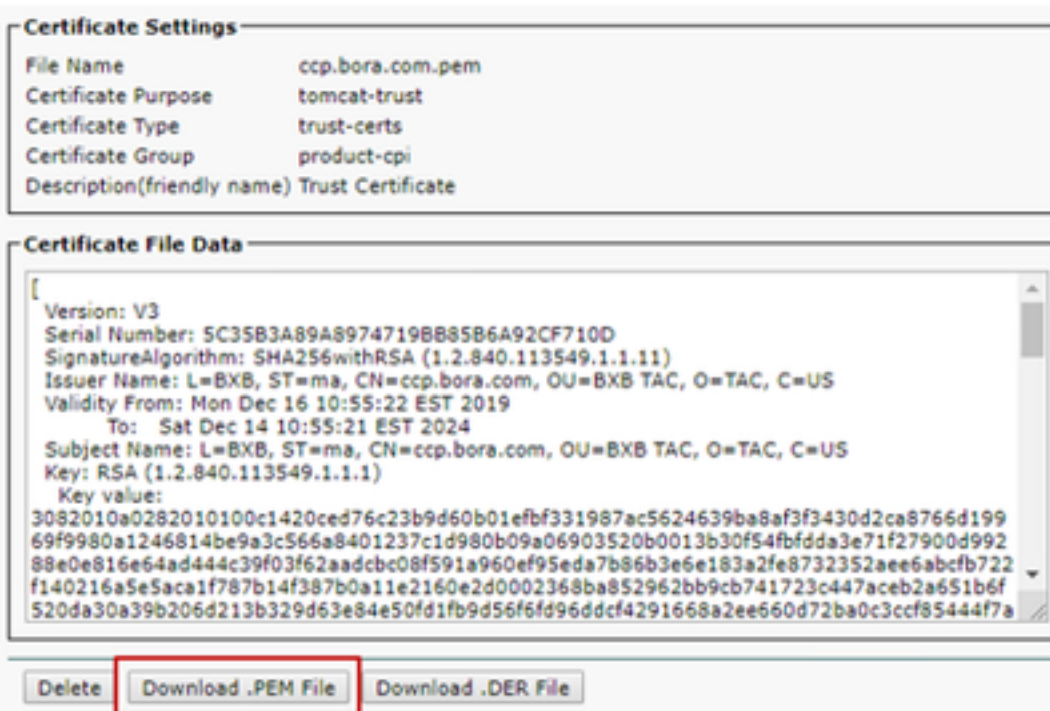
(i) Accédez à la page Cisco Unified Communications Operating System Administration :
<https://FQDN:8443/cmplatform>

(ii) Accédez à **Security > Certificate Management** et recherchez les certificats du serveur principal de l'application dans le dossier **tomcat-trust**.



Source	Destination	Signature	Key	Key	Key
tomcat-trust	Cisco_ECC_Root_CA	Self-signed	EC	Cisco_ECC_Root_CA	Cisco_ECC_Root_CA
tomcat-trust	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Self-signed	RS4	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Hellenic_Academic_and_Research_Institutions
tomcat-trust	OISTE_WISetec_Global_Root_GB_CA	Self-signed	RS4	OISTE_WISetec_Global_Root_GB_CA	OISTE_WISetec_Global_Root_GB_CA
tomcat-trust	Amazon_Root_CA_4	Self-signed	EC	Amazon_Root_CA_4	Amazon_Root_CA_4
tomcat-trust	DST_Root_CA_X3	Self-signed	RS4	DST_Root_CA_X3	DST_Root_CA_X3
tomcat-trust	AddTrust_Eternal_CA_Root	Self-signed	RS4	AddTrust_Eternal_CA_Root	AddTrust_Eternal_CA_Root
tomcat-trust	ccp.bora.com	Self-signed	RS4	ccp.bora.com	ccp.bora.com
tomcat-trust	T-TeleSec_GlobalRoot_Class_3	Self-signed	RS4	T-TeleSec_GlobalRoot_Class_3	T-TeleSec_GlobalRoot_Class_3
tomcat-trust	DigCert_Global_Root_G2	Self-signed	RS4	DigCert_Global_Root_G2	DigCert_Global_Root_G2

(iii) Sélectionnez le certificat et cliquez sur télécharger le fichier .PEM pour l'enregistrer dans un dossier temporaire sur le serveur ADS.



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: 5C35B3A89A8974719BB8586A92CF710D
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:
3082010a0282010100c1420ced76c23b9d60b01efbf331967ac5624639ba8af3f3430d2ca8766d199
69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54bfd3e71f27900d992
88e0e816e64ad444c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
520da30a39b206d213b329d63e84e50fd1fb9d56f6d96ddcf4291668a2ee660d72ba0c3ccf85444f7a
]
```

Delete Download .PEM File Download .DER File

Note: Effectuez les mêmes étapes pour l'abonné.

Étape 2. Importer l'application de plate-forme VOS sur le serveur ADS

Chemin d'accès à l'outil Clé : C:\Program Fichiers (x86)\Java\jre1.8.0_221\bin

Commande d'importation des certificats auto-signés :

```
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
```

Redémarrez le service Apache Tomcat sur les serveurs ADS.

Note: Effectuer la même tâche sur les autres serveurs ADS

Section 3 : Échange de certificats entre les serveurs Roggers, PG et ADS

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1 : Exporter le certificat IIS des serveurs Rogger et PG

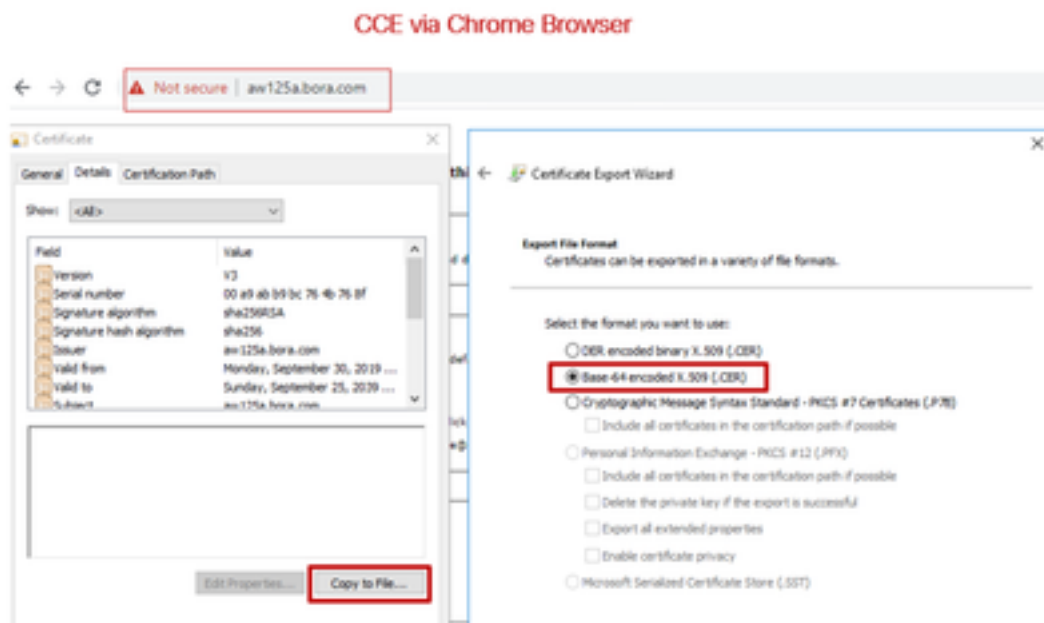
Étape 2 : Exporter le certificat DFP (Diagnostic Framework Portico) des serveurs Rogger et PG

Étape 3 : Importer des certificats dans des serveurs ADS

Étape 1. Exporter le certificat IIS des serveurs Rogger et PG

(i) Sur le serveur ADS à partir d'un navigateur, accédez à l'URL des serveurs (Roggers, PG) : <https://{servername}>

(ii) Enregistrez le certificat dans un dossier temporaire, par exemple `c:\temp\certs` et nommez le certificat en `ICM{svr}[ab].cer`



Note: Sélectionnez l'option Base-64 encoded X.509 (.CER).

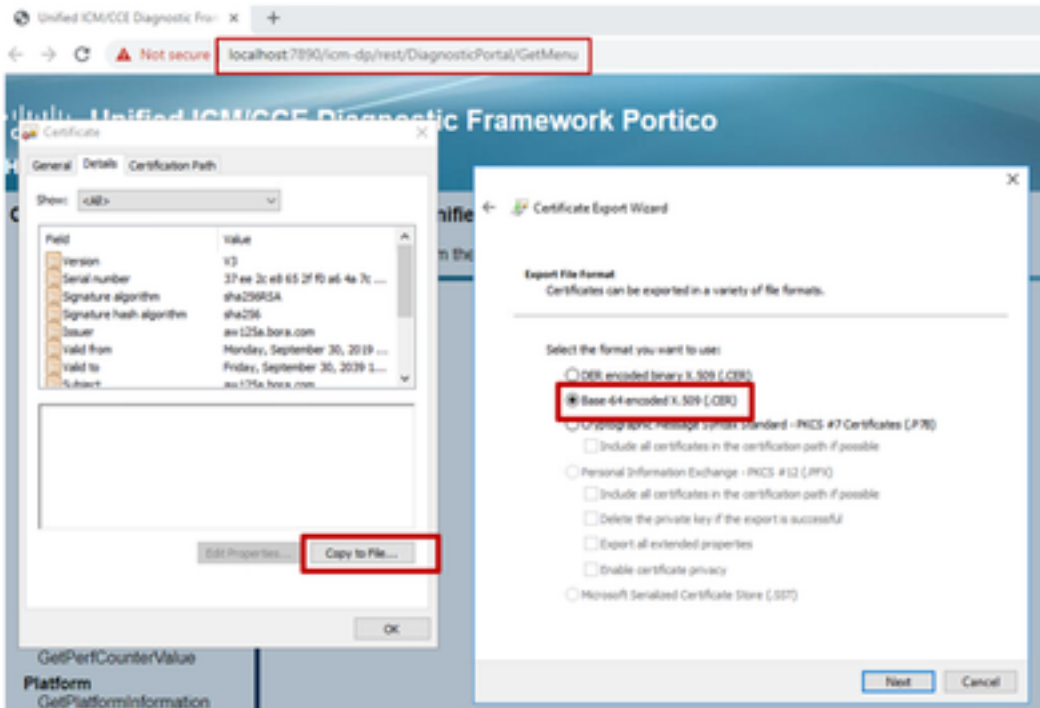
Étape 2. Exporter le certificat DFP (Diagnostic Framework Portico) des serveurs Rogger et PG

(i) Sur le serveur ADS à partir d'un navigateur, accédez à l'URL DFP des serveurs (Roggers, PG) : <https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion>

(ii) Enregistrez le certificat dans l'exemple de dossier `c:\temp\certs` et nommez le certificat en

dfp{svr}{ab}.cer

Portico via Chrome Browser



Note: Sélectionnez l'option Base-64 encoded X.509 (.CER).

Étape 3. Importer des certificats dans le serveur ADS

Commande pour importer les certificats auto-signés IIS dans le serveur ADS. Chemin d'accès à l'outil Clé : C:\Program Fichiers (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
```

Remarque : Importez tous les certificats de serveur exportés vers tous les serveurs ADS.

Commande pour importer les certificats autosignés de diagnostic dans le serveur ADS

```
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
```

Note: Importez tous les certificats de serveur exportés vers tous les serveurs ADS.

Redémarrez le service Apache Tomcat sur les serveurs ADS.

Section 4 : CVP CallStudio WEBSERVICE Integration

Pour plus d'informations sur la façon d'établir une communication sécurisée pour l'élément Web Services et l'élément Rest_Client

reportez-vous au [Guide de l'utilisateur pour Cisco Unified CVP VXML Server et Cisco Unified Call Studio version 12.5\(1\) - Web Service Integration \[Cisco Unified Customer Voice Portal\] - Cisco](#)

Informations connexes

- Guide de configuration du CVP : [Guide de configuration CVP - Sécurité](#)
- Guide de configuration UCCE : [Guide de configuration UCCE - Sécurité](#)
- Guide d'administration de PCCE : [Guide d'administration PCE - Sécurité](#)
- Certificats UCCE auto-signés : [certificats autosignés Exchange UCCE](#)
- Installer et migrer vers OpenJDK dans CCE 12.5(1) : [Migration CCE OpenJDK](#)
- Installer et migrer vers OpenJDK dans CVP 12.5(1) : [Migration CVP OpenJDK](#)