Échanger des certificats auto-signés dans une solution PCCE 12.6

Table des matières

Introduction

Ce document décrit comment échanger des certificats auto-signés dans la solution Cisco Packaged Contact Center Enterprise (PCCE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- PCCE version 12.6(2)
- Customer Voice Portal (CVP) version 12.6(2)
- Navigateur vocal virtualisé (VVB) 12.6(2)

- Serveur de date d'administration/station de travail Admin (AW/ADS) 12.6(2)
- Serveur Cisco Unified Intelligence (CUIC)
- Plate-forme de collaboration client (CCP) 12.6(2)
- Messagerie instantanée et messagerie électronique (ECE) 12.6(2)

Composants utilisés

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

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

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 de 12.x, tous les périphériques sont contrôlés via le panneau de verre unique (SPOG), qui est hébergé sur le serveur AW principal. En raison de la conformité à la gestion de la sécurité (SRC) de 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 afin d'assurer une communication sécurisée et transparente entre SPOG et les autres périphériques. Dans un environnement de certificats auto-signés, l'échange de certificats entre les serveurs est une nécessité.

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) Tous les serveurs AW/ADS : ces serveurs nécessitent un certificat provenant de :

- Plate-forme Windows :
  - ICM : routeur et enregistreur (Rogger){A/B}, passerelle d'accès aux périphériques (PG){A/B}, tous les serveurs AW/ADS et ECE.

Remarque : IIS et le protocole DFP (Diagnostic Framework Portico) sont nécessaires.

  - CVP : serveurs CVP, serveur CVP Reporting.

Remarque : un certificat WSM (Web Service Management) de tous les serveurs est nécessaire. Les certificats doivent être associés à un nom de domaine complet (FQDN).

- Plate-forme VOS : Cloud Connect, Cisco Virtualized Voice Browser (VVB), Cisco Unified Communication Manager (CUCM), Finesse, Cisco Unified Intelligence Center (CUIC), Live Data (LD), Identity Server (IDS) et autres serveurs applicables.

(ii) Router \ Logger Servers : ces serveurs nécessitent un certificat de :

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

(iii) Serveurs PG : ces serveurs nécessitent un certificat provenant de :

- Plate-forme Windows : certificat IIS de tous les serveurs AW/ADS.
- Plate-forme VOS : éditeur CUCM (serveurs PG CUCM uniquement) ; Cloud Connect et CCP (serveur PG MR uniquement).

Remarque : cette opération est nécessaire pour télécharger le client JTAPI à partir du serveur CUCM.

(iv) Serveurs CVP : ces serveurs nécessitent un certificat de

- Plate-forme Windows : certificat IIS de tous les serveurs ADS
- Plate-forme VOS : serveur Cloud Connect, serveurs VVB.

(v) Serveur de rapports CVP : ce serveur requiert un certificat de :

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

(vi) Serveurs VVB : ce serveur requiert un certificat de :

- Plate-forme Windows : certificat IIS de tous les serveurs ADS, certificat VXML du serveur CVP et certificat Callserver du serveur CVP
- Plate-forme VOS : serveur Cloud Connect.

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 les serveurs 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 les serveurs CVP et ADS

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exporter les certificats WSM des serveurs CVP.

Étape 2. Importer le certificat WSM des serveurs CVP vers les serveurs ADS.

Étape 3. Exporter le certificat du serveur ADS.

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

Étape 1. Exporter les certificats du 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, Virtual Agent Voice (VAV) et la synchronisation CVP avec SPOG peuvent rencontrer des problèmes.

Attention : avant de commencer, vous devez procéder comme suit :
1. Ouvrez une fenêtre de commande en tant qu'administrateur.
2. Pour la version 12.6.2, pour identifier le mot de passe de la banque de clés, accédez au dossier %CVP_HOME%\bin et exécutez le fichier DecryptKeystoreUtil.bat.
3. Pour la version 12.6.1, pour identifier le mot de passe de la banque de clés, exécutez la commande more %CVP_HOME%\conf\security.properties.
4. Vous avez besoin de ce mot de passe lorsque vous exécutez les commandes keytool.
5. À partir du répertoire %CVP_HOME%\conf\security\, exécutez la commande copy .keystore backup.keystore.

Remarque : vous pouvez rationaliser les commandes utilisées dans ce document en utilisant le paramètre keytool -storepass. Pour tous les serveurs CVP, indiquez le mot de passe d'outil clé que vous avez identifié. Pour les serveurs ADS, le mot de passe par défaut est : changeit

---

Pour régénérer le certificat sur les serveurs CVP, exécutez les étapes suivantes :

(i) Répertoriez les certificats dans le serveur

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

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

---

ii) Supprimer les anciens certificats auto-signés

Serveurs CVP : commandes pour supprimer les certificats auto-signés :

```
%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 Reporting servers : commandes pour supprimer les certificats auto-signés :

```
%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
```

Remarque : les serveurs de rapports CVP possèdent les certificats auto-signés suivants : wsm_certificate, callserver_certificate.

(iii) Générez 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 -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Remarque : par défaut, les certificats sont générés pour deux ans. Utilisez -valid XXXX pour définir la date d'expiration lorsque les certificats sont régénérés, sinon les certificats sont valides pendant 90 jours et doivent être signés par une autorité de certification avant cette date. Pour la plupart de ces certificats, un délai de validation de 3 à 5 ans doit être raisonnable.

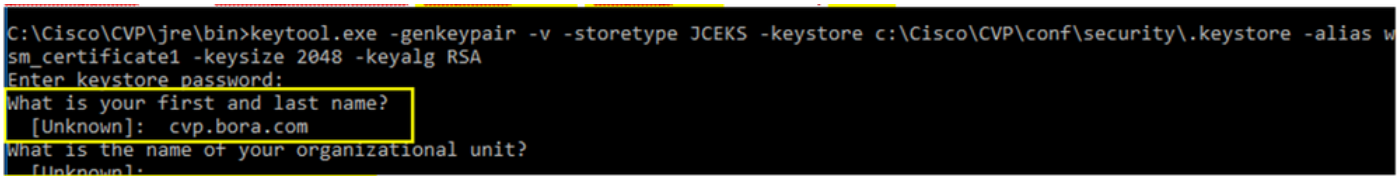
Voici quelques entrées de validité standard :

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

Dix ans	3650

Attention : à partir de 12.5, les certificats doivent être SHA 256, Key Size 2048, et l'algorithme de chiffrement 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 ce n'est pas le cas, le certificat, la clé ou, pire, le magasin de clés peut être endommagé.

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



Répondez aux autres questions suivantes :

Quel est le nom de votre unité organisationnelle ?

[Inconnu] : <précisez l'unité d'organisation>

Quel est le nom de votre entreprise ?

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

Quel est le nom de votre ville ou localité ?

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

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

[Inconnu] : <indiquer le nom de l'État/de la province>

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

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

Spécifiez yes pour les deux entrées suivantes.

Suivez les mêmes étapes pour vxml_certificate et callserver_certificate :

```
%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
```

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 -genkeypai
```

Spécifiez le nom de domaine complet du serveur pour la requête, quels sont vos nom et prénom ? et poursuivez avec les mêmes étapes que pour les serveurs CVP.

Suivez les mêmes étapes pour callserver_certificate :

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

Redémarrez les serveurs de rapports.

(iv) Exporter wsm_Certificate à partir des serveurs CVP et Reporting

a) Exportez le certificat WSM de chaque serveur CVP vers un emplacement temporaire et renommez le certificat avec le nom souhaité. Vous pouvez le renommer wsmcsX.crt. Remplacez « X » par le nom d'hôte du serveur. Par exemple, wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt .

Commande pour exporter les certificats auto-signés :

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

b) Copiez le certificat à partir du chemin d'accès %CVP_HOME%\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 vers le serveur ADS

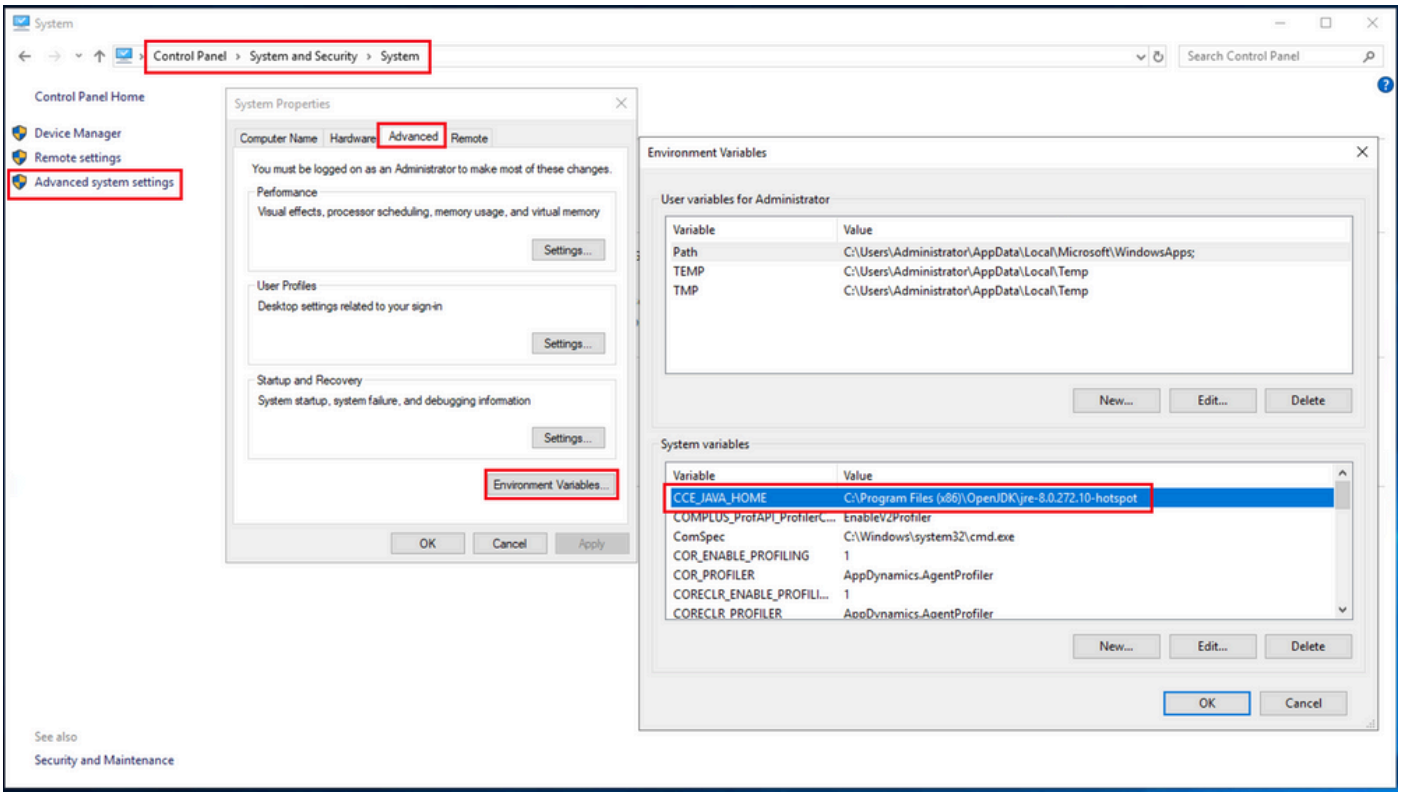
Pour importer le certificat dans le serveur ADS, vous devez utiliser l'outil de touches qui fait partie de l'ensemble d'outils Java. Il existe plusieurs façons de trouver le chemin d'accès à la page d'accueil Java où cet outil est hébergé.

(i) Commande CLI > echo %CCE_JAVA_HOME%

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

java home path

(ii) Manuellement via le réglage avancé du système, comme indiqué dans l'image.



Variables d'environnement

Sur PCCE 12.6, le chemin d'accès par défaut d'OpenJDK est C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

Commandes pour importer les certificats auto-signés :

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

> Remarque : répétez les commandes pour chaque CVP du déploiement et effectuez la même tâche sur les autres serveurs ADS

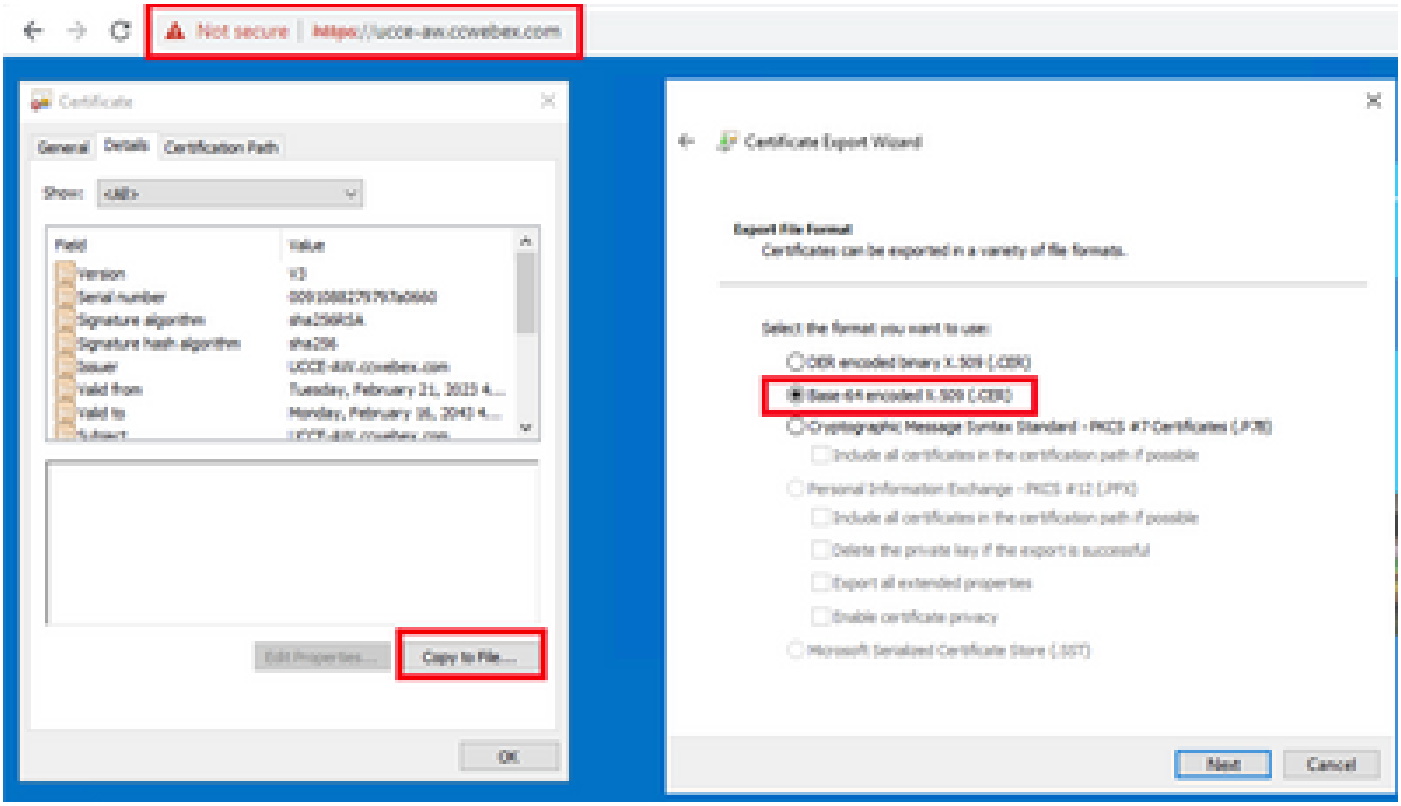
(iii) Redémarrez le service Apache Tomcat sur les serveurs ADS.

Étape 3. Exporter le certificat du serveur ADS

Voici les étapes à suivre pour exporter le certificat ADS :

(i) Sur le serveur ADS à partir d'un navigateur, accédez à l'URL du serveur : https://<nomserveur>.

(ii) Enregistrez le certificat dans un dossier temporaire, par exemple : c:\temp\certs et nommez le certificat ADS<svr>[ab].cer.



Exporter les certificats ADS

Remarque : sélectionnez l'option X.509 codé en base 64 (.CER).

Étape 4. Importer le certificat du serveur ADS vers les serveurs CVP et Reporting Server

(i) Copiez le certificat sur les serveurs CVP et le serveur de rapports CVP dans le répertoire %CVP_HOME%\conf\security.

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

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

Procédez de la même manière pour les certificats des autres serveurs ADS.

(iii) Redémarrer les serveurs CVP et 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 sur le serveur ADS.

Étape 3. Importer les certificats d'application de la plate-forme CUCM sur les serveurs PG CUCM.

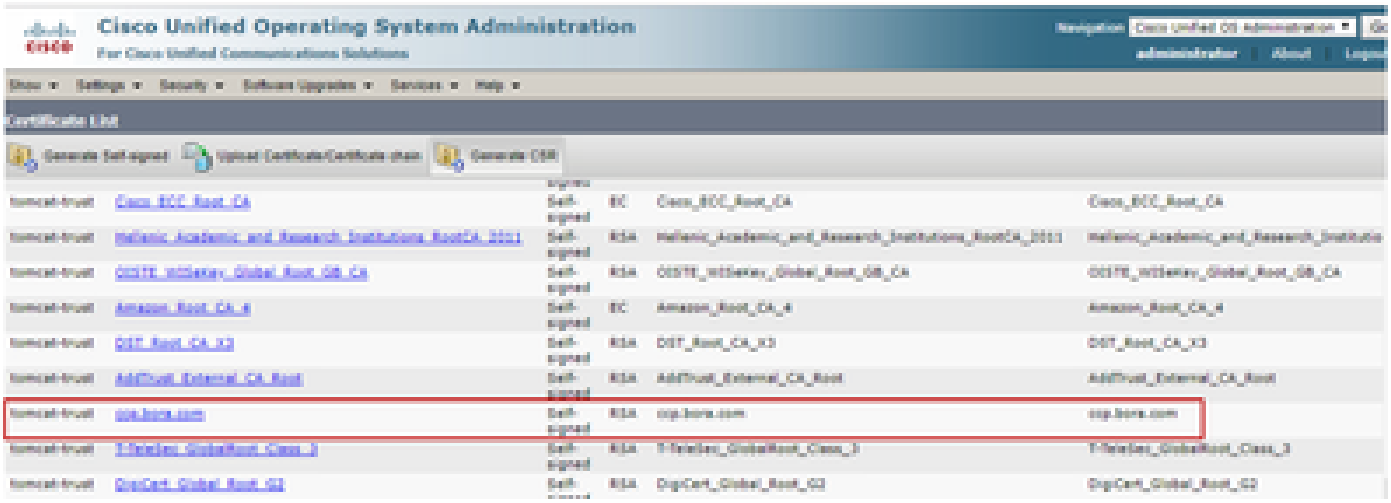
Ce processus s'applique à toutes les applications VOS telles que :

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- Connexion au cloud

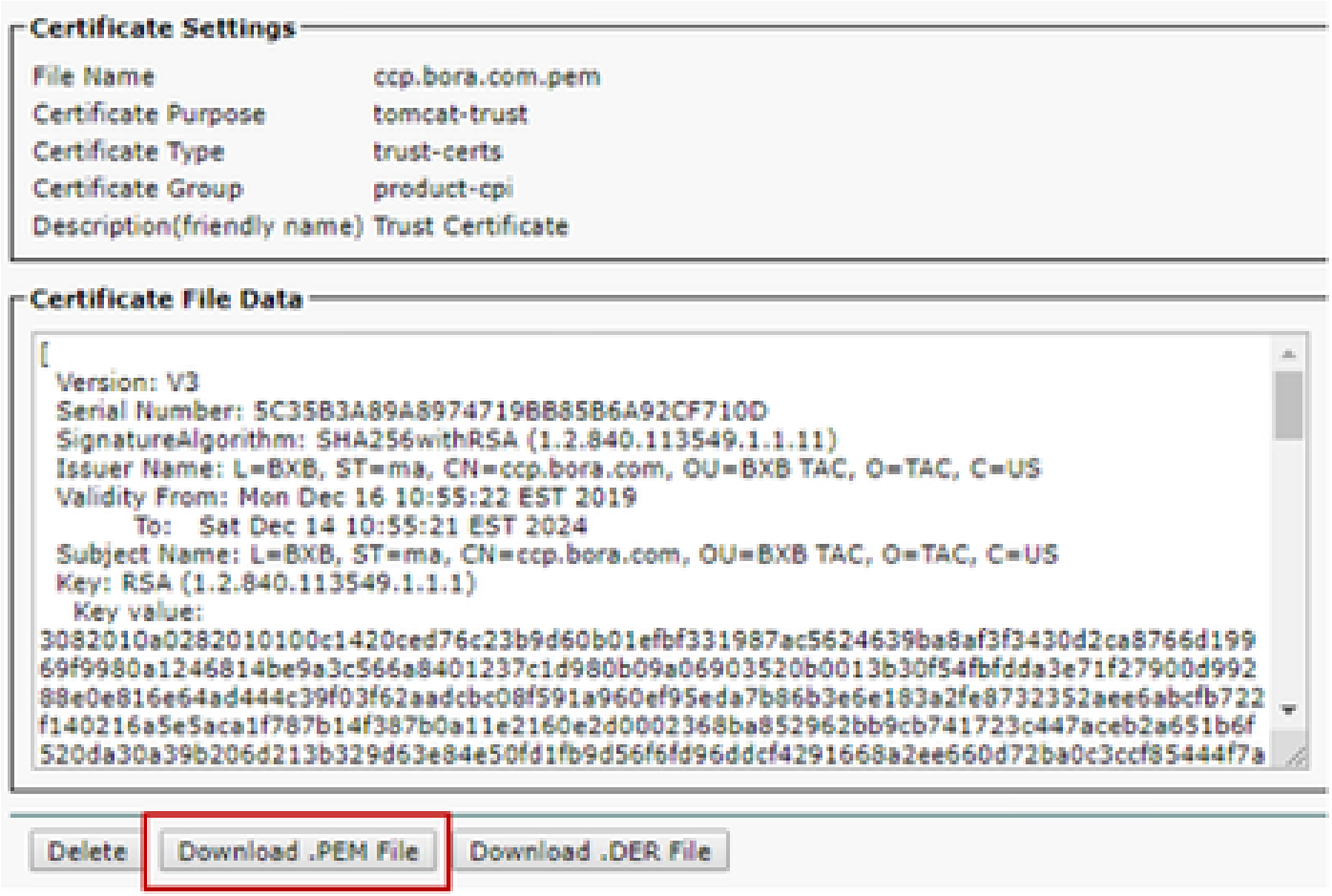
Étape 1. Exporter les certificats du serveur d'applications de la plate-forme VOS.

(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.



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



Remarque : effectuez les mêmes étapes pour l'abonné.

Étape 2. Importer le certificat d'application de la plate-forme VOS sur le serveur ADS

Chemin d'exécution de l'outil Clé : %CCE_JAVA_HOME%\bin

Commandes pour importer les certificats auto-signés :

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

Redémarrez le service Apache Tomcat sur les serveurs ADS.

Remarque : effectuez la même tâche sur d'autres serveurs ADS

Étape 3. Importer le certificat d'application de la plate-forme CUCM sur le serveur CUCM PG

Chemin d'exécution de l'outil Clé : %CCE_JAVA_HOME%\bin

Commandes pour importer les certificats auto-signés :

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

Redémarrez le service Apache Tomcat sur les serveurs PG.

Remarque : effectuez la même tâche sur d'autres serveurs CUCM PG

Section 3 : Échange de certificats entre les serveurs Rogers, 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 des serveurs Rogger et PG

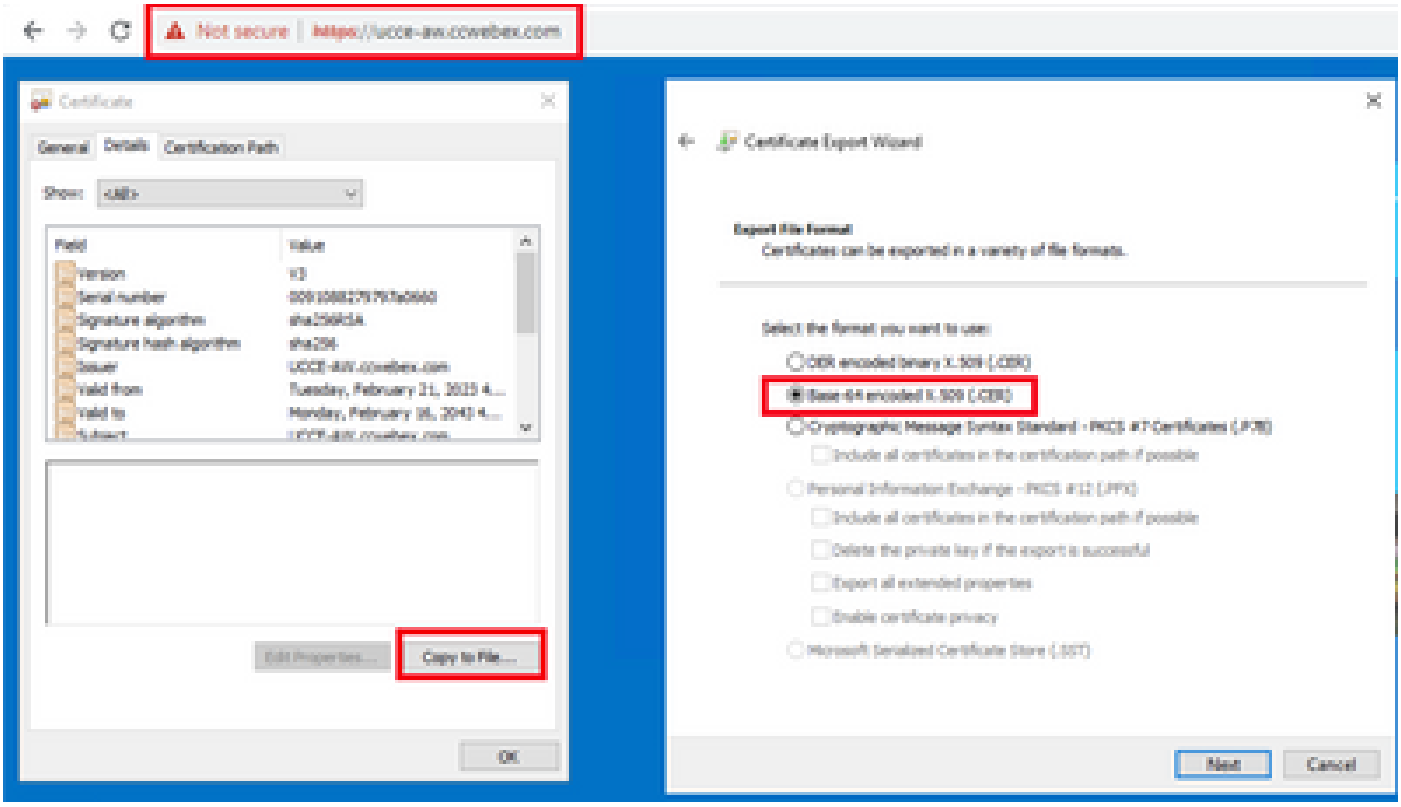
Étape 3. Importer des certificats dans les serveurs ADS

Étape 4. Importer le certificat ADS dans les serveurs Rogger et PG

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 (Rogers, PG) : https://{nomserveur}

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



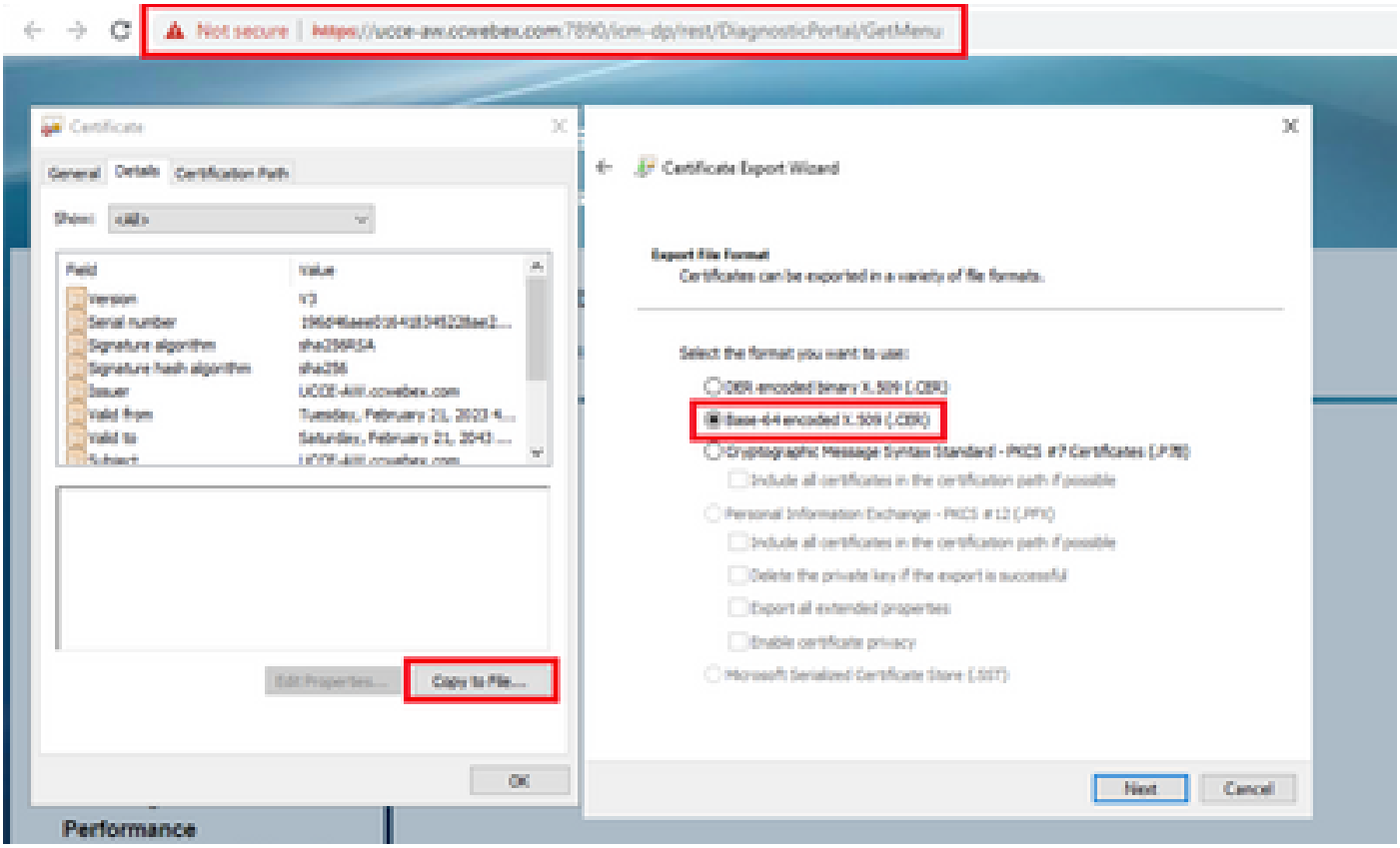
Exporter le certificat IIS

Remarque : sélectionnez l'option X.509 codé en base 64 (.CER).

Étape 2. Exporter le certificat DFP des serveurs Rogger et PG

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

(ii) Enregistrez le certificat dans le dossier exemple c:\temp\certs et nommez le certificat dfp{svr}[ab].cer



Exporter le certificat DFP

Remarque : sélectionnez l'option X.509 codé en base 64 (.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 : %CCE_JAVA_HOME%\bin

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

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

Commande pour importer les certificats auto-signés de diagnostic dans le serveur ADS

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

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

Redémarrez le service Apache Tomcat sur les serveurs ADS.

Étape 4. Importer le certificat ADS dans les serveurs Rogger et PG

Commande permettant d'importer les certificats auto-signés IIS dans les serveurs Rogger et PG. Chemin d'accès à l'outil Clé : %CCE_JAVA_HOME%\bin.

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

Remarque : importez tous les certificats IIS du serveur ADS exportés dans tous les serveurs Rogger et PG.

Redémarrez le service Apache Tomcat sur les serveurs Rogger et PG.

Section 4 : Intégration du service Web CVP CallStudio

Pour obtenir des informations détaillées sur l'établissement d'une communication sécurisée pour les éléments Web Services et Rest_Client

reportez-vous au Guide de l'utilisateur de Cisco Unified CVP VXML Server et de Cisco Unified Call Studio version 12.6(2) - Web Service Integration [Cisco Unified Customer Voice Portal] - Cisco

Informations connexes

- Guide de configuration CVP - Sécurité
- Guide de sécurité UCCE
- Guide d'administration PCCE
- Certificats autosignés PCCE Exchange - PCCE 12.5
- Certificats auto-signés UCCE Exchange - UCCE 12.5
- Certificats auto-signés UCCE Exchange - UCCE 12.6
- Implémenter des certificats signés par une autorité de certification - CCE 12.6
- Exchange Certificates with Contact Center Uploader Tool

- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.