Échanger des certificats auto-signés dans une solution UCCE 12.6

Table des matières

Introduction

Ce document décrit comment échanger des certificats auto-signés dans une solution Unified Contact Center Enterprise (UCCE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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

- UCCE 12.6(2)
- CVP 12.6(2)
- Cisco VB 12.6(2)
- Console des opérations CVP (OAMP)
- CVP New OAMP (NOAMP)

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.

Informations générales

Dans la solution UCCE, la configuration des nouvelles fonctionnalités impliquant des applications principales telles que Rogers, Peripheral Gateways (PG), Admin Workstations (AW)/ Administration Data Server (ADS), Finesse, Cisco Unified Intelligence Center (CUIC), etc., s'effectue via la page d'administration Contact Center Enterprise (CCE). Pour les applications de réponse vocale interactive (IVR) telles que CVP, Cisco VVB et les passerelles, NOAMP contrôle la configuration des nouvelles fonctionnalités. À partir de CCE 12.5(1), en raison de la conformité à la gestion de la sécurité (SRC), toutes les communications vers CCE Admin et NOAMP sont strictement effectuées via le protocole HTTP sécurisé.

Pour assurer une communication sécurisée et transparente entre ces applications dans un environnement de certificats auto-signés, l'échange de certificats entre les serveurs est indispensable. La section suivante explique en détail les étapes nécessaires pour échanger un certificat auto-signé entre :

- Serveurs CCE AW et serveurs d'applications de base CCE
- Serveur CVP OAMP et serveurs de composants CVP

Remarque : ce document s'applique UNIQUEMENT à la version 12.6 du CCE. Consultez la section Informations connexes pour obtenir des liens vers d'autres versions.

Procédure

Serveurs CCE AW et serveurs d'applications de base CCE

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.

Serveurs CCE AW : ce serveur requiert un certificat de :

- Plate-forme Windows : Router and Logger(Rogger){A/B}, Peripheral Gateway (PG){A/B} et tous les AW/ADS.

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

- Plate-forme VOS : Finesse, CUIC, Live Data (LD), Identity Server (IDS) , Cloud Connect et d'autres serveurs applicables faisant partie de la base de données d'inventaire. Il en va de même pour les autres serveurs AW de la solution.

Router \ Logger Server : ce serveur requiert un certificat de :

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

Les étapes nécessaires à l'échange efficace des certificats auto-signés pour CCE sont divisées en ces sections.

Section 1 : échange de certificats entre le routeur/enregistreur, le PG et le serveur AW
Section 2 : Échange de certificats entre l'application de la plate-forme VOS et le serveur AW

Section 1 : échange de certificats entre le routeur/enregistreur, le PG et le serveur AW

Les étapes nécessaires pour réussir cet échange sont les suivantes :

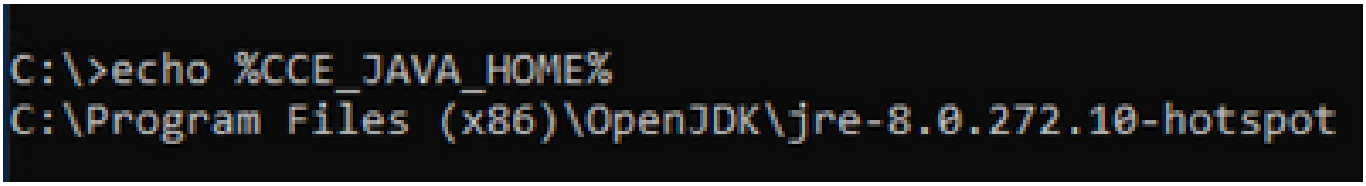
Étape 1. Exportez les certificats IIS depuis Router\Logger, PG et tous les serveurs AW.
Étape 2. Exportez les certificats DFP depuis Router\Logger, PG et tous les serveurs AW.
Étape 3. Importez des certificats IIS et DFP depuis Router\Logger, PG et AW vers des serveurs AW.

Étape 4. Importez le certificat IIS dans Router\Logger et PG à partir des serveurs AW.

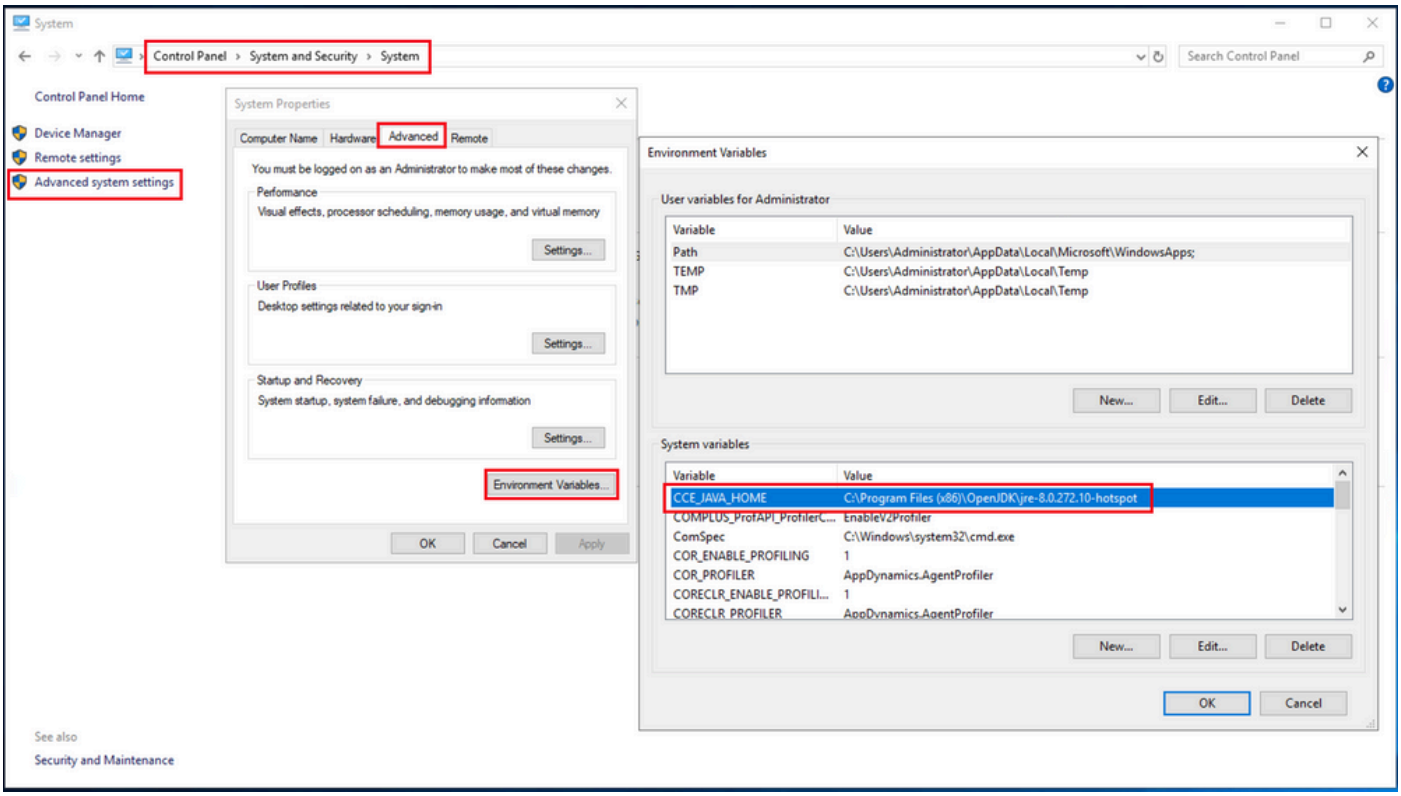
> Attention : avant de commencer, vous devez sauvegarder la banque de clés et ouvrir une invite de commandes en tant qu'administrateur.

(i) Connaître le chemin d'accès au répertoire d'origine Java pour savoir où l'outil de saisie Java est hébergé. Il existe plusieurs façons de trouver le chemin d'accès java.

Option 1 : commande CLI : echo %CCE_JAVA_HOME%



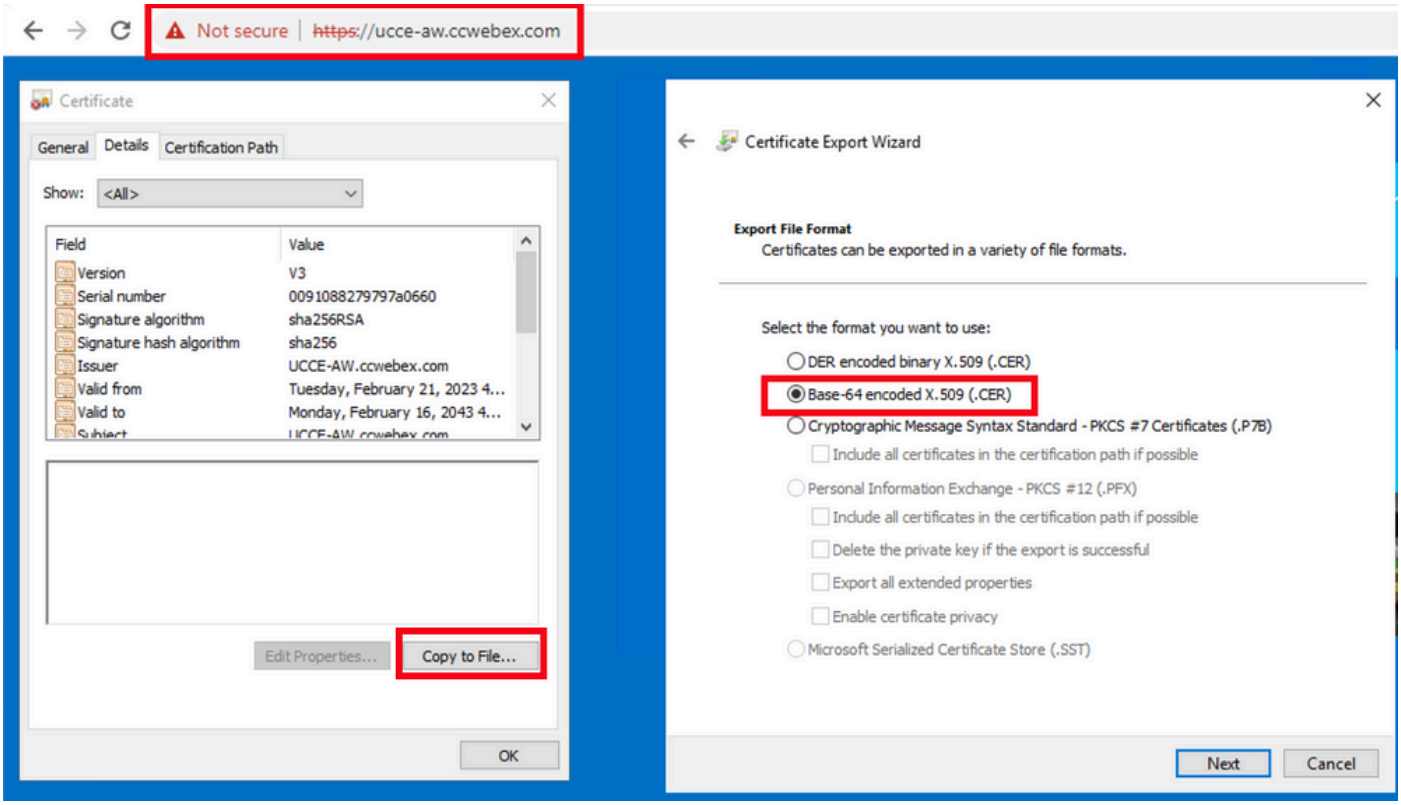
Option 2 : manuellement via le paramètre système avancé, comme illustré dans l'image



(ii) Sauvegardez le fichier cacerts à partir du dossier <ICM install directory>ssl\ . Vous pouvez le copier à un autre emplacement.

Étape 1. Exportez les certificats IIS depuis Router\Logger, PG et tous les serveurs AW.

(i) Sur un serveur AW à partir d'un navigateur, accédez à l'URL des serveurs (Rogers, PG, autres serveurs AW) : https://{servername}.

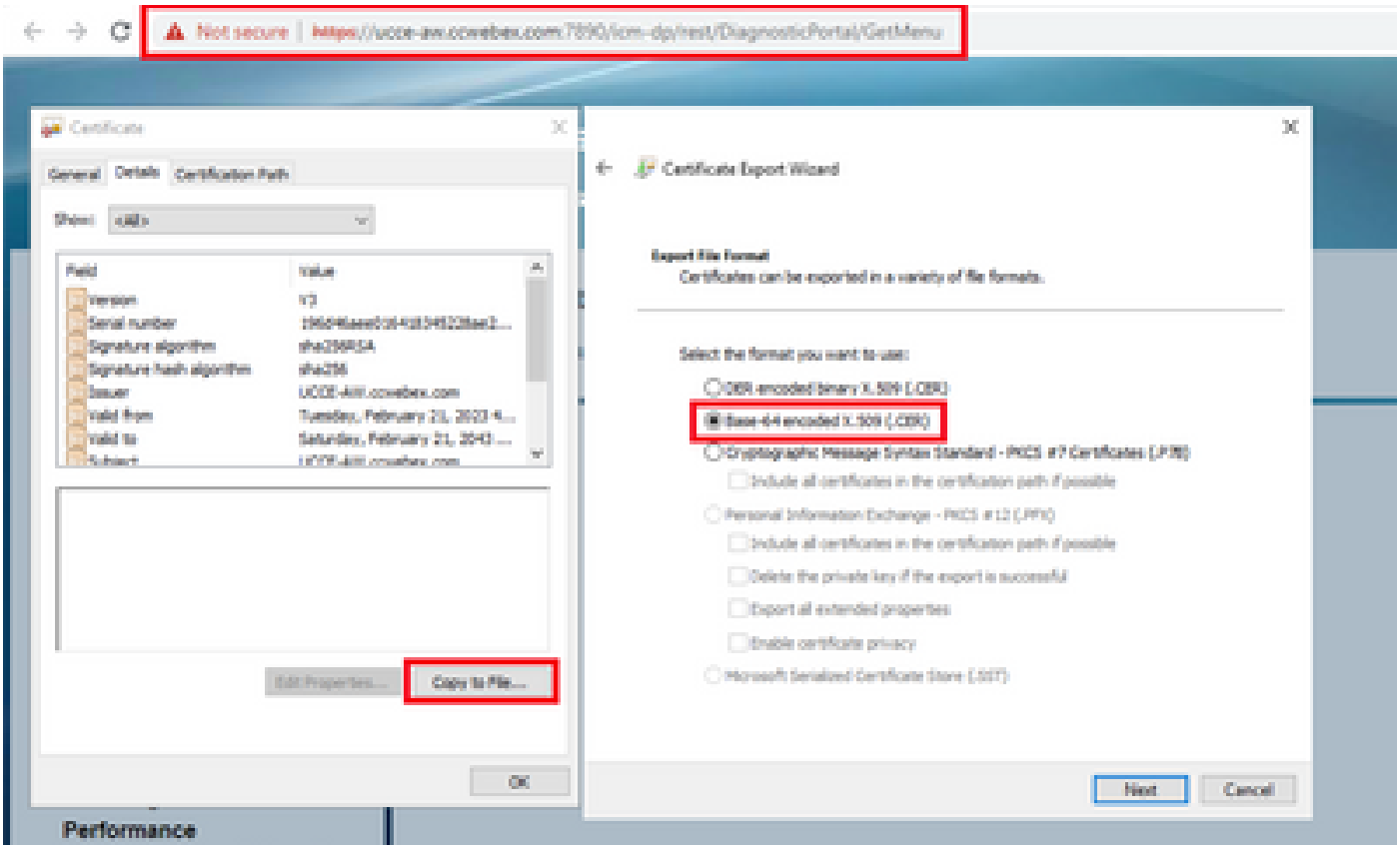


(ii) Enregistrez le certificat dans un dossier temporaire. Par exemple, c:\temp\certs et nommez le certificat ICM{svr}[ab].cer.

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

Étape 2. Exportez les certificats DFP depuis Router\Logger, PG et tous les serveurs AW.

(i) Sur le serveur AW, ouvrez un navigateur et accédez aux serveurs (Router, Logger ou Rogers, PGs) URL DFP : 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

---

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

Étape 3. Importez des certificats IIS et DFP depuis Router\Logger, PG et AW vers des serveurs AW.

Commande pour importer les certificats auto-signés IIS dans le serveur AW. Chemin d'exécution de l'outil Clé : %CCE_JAVA_HOME%\bin :

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_II
Example:%CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore
```

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

Commande pour importer les certificats autosignés DFP dans les serveurs AW :

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp{svr}[ab].cer -alias {fqdn_of_server}_DF
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\dfpAWA.cer -alias AWA_DFP -keystor
```

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

Redémarrez le service Apache Tomcat sur les serveurs AW.

Étape 4. Importez le certificat IIS dans Router\Logger et PG à partir des serveurs AW.

Commande pour importer les certificats auto-signés IIS AW dans les serveurs Router\Logger et PG :

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_II
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystor
```

Remarque : importez tous les certificats de serveur IIS AW exportés vers les serveurs Rogger et PG sur les côtés A et B.

Redémarrez le service Apache Tomcat sur les serveurs Router\Logger et PG.

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

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. Importez les certificats d'application de la plate-forme VOS sur le serveur AW.

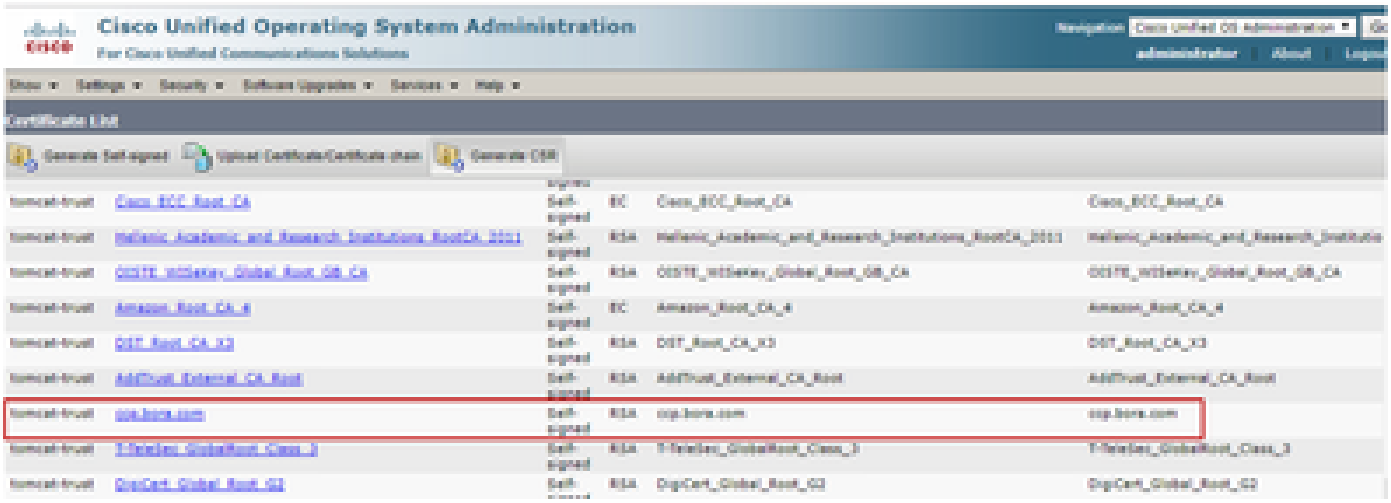
Ce processus s'applique aux applications VOS telles que :

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

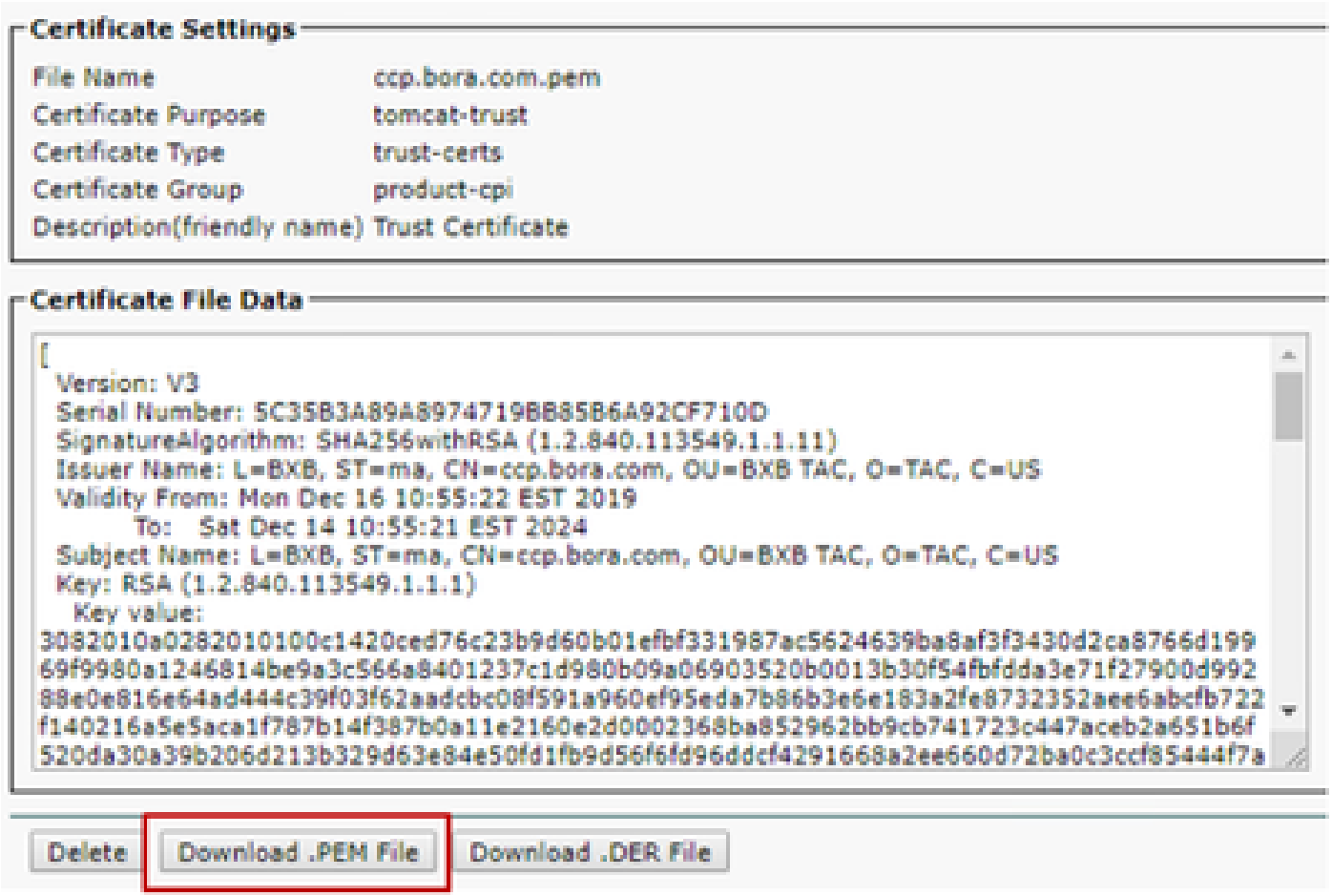
Étape 1. Exporter les certificats du serveur d'applications de la plate-forme VOS.

(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 d'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 AW.



Remarque : effectuez les mêmes étapes pour l'abonné.

Étape 2. Importez l'application de plate-forme VOS sur le serveur AW.

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

Commande pour importer les certificats auto-signés :

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.pem -alias {fqdn_of_VOS} -k
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\CUICPub.pem -alias CUICPub -keysto
```

Redémarrez le service Apache Tomcat sur les serveurs AW.

Remarque : effectuez la même tâche sur d'autres serveurs AW.

Serveur CVP OAMP et serveurs de composants CVP

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 CVP OAMP : ce serveur requiert un certificat de

- Plate-forme Windows : certificat WSM (Web Services Manager) du serveur CVP et des serveurs de rapports.
- Plate-forme VOS : serveur Cisco VVB et Cloud Connect.

(ii) Serveurs CVP : ce serveur requiert un certificat de

- Plate-forme Windows : certificat WSM du serveur OAMP.
- Plate-forme VOS : serveur Cloud Connect et serveur Cisco VVB.

(iii) Serveurs CVP Reporting : ce serveur requiert un certificat de

- Plate-forme Windows : certificat WSM du serveur OAMP

(iv) Serveurs Cisco VVB : ce serveur requiert un certificat de

- Plate-forme Windows : certificat VXML du serveur CVP et certificat Callserver du serveur CVP
- Plate-forme VOS : serveur Cloud Connect

Les étapes nécessaires à l'échange efficace des certificats auto-signés dans l'environnement CVP sont expliquées dans ces trois sections.

Section 1 : Échange de certificats entre le serveur CVP OAMP et le serveur CVP et les serveurs de rapports
Section 2 : Échange de certificats entre le serveur CVP OAMP et les applications de la plate-forme VOS
Section 3 : Échange de certificats entre le serveur CVP et les applications de la plate-forme VOS

Section 1 : Échange de certificats entre le serveur CVP OAMP et le serveur CVP et les serveurs de rapports

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exportez le certificat WSM à partir du serveur CVP, du serveur Reporting et du serveur OAMP.
Étape 2. Importez les certificats WSM du serveur CVP et du serveur de rapports dans le serveur OAMP.
Étape 3. Importez le certificat WSM du serveur CVP OAMP dans les serveurs CVP et les serveurs de rapports.

> 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.

Étape 1. Exportez le certificat WSM depuis CVP Server, Reporting et OAMP Server.

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

Commande pour exporter les certificats auto-signés :

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

(ii) Copiez le certificat à partir du chemin d'accès %CVP_HOME%\conf\security\wsm.crt à partir de chaque serveur et renommez-le wsmX.crt en fonction du type de serveur.

Étape 2. Importez les certificats WSM du serveur CVP et du serveur de rapports dans le serveur OAMP.

(i) Copiez chaque certificat WSM du serveur CVP et du serveur Reporting (wsmX.crt) dans le répertoire %CVP_HOME%\conf\security du serveur OAMP.

(ii) Importez ces certificats avec la commande suivante :

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

(iii) Redémarrez le serveur.

Étape 3. Importez le certificat WSM du serveur CVP OAMP dans les serveurs CVP et les serveurs de rapports.

(i) Copiez le certificat WSM du serveur OAMP (wsmoampX.crt) dans le répertoire %CVP_HOME%\conf\security sur tous les serveurs CVP et les serveurs de rapports.

(ii) Importez les certificats avec la commande suivante :

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

(iii) Redémarrez les serveurs.

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

Les étapes nécessaires pour réussir cet échange sont les suivantes :

Étape 1. Exportez le certificat d'application depuis la plate-forme VOS.

Étape 2. Importez le certificat d'application VOS dans le serveur OAMP.

Ce processus s'applique aux applications VOS telles que :

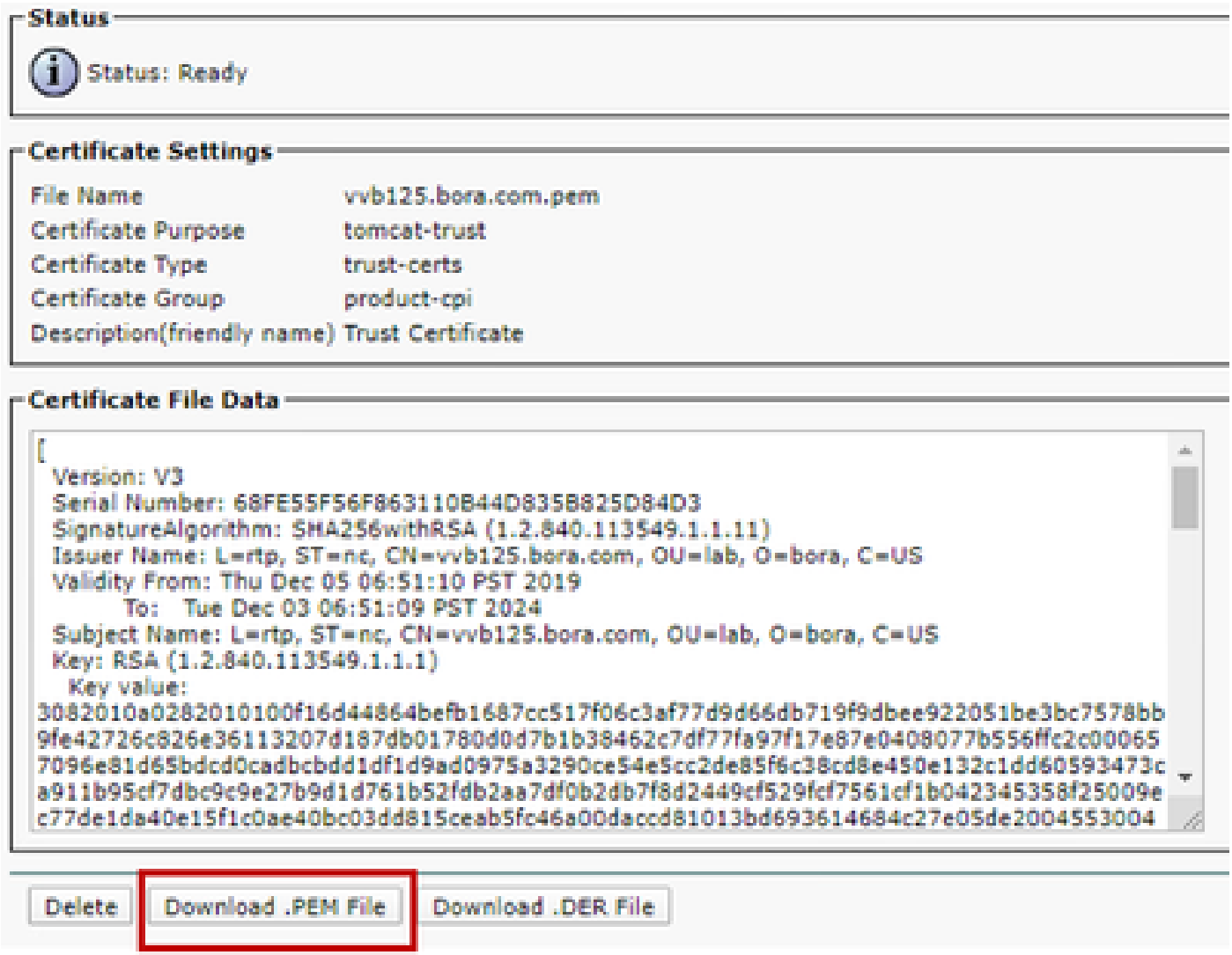
- CUCM
- VVB
- Connexion au cloud

Étape 1. Exportez le certificat d'application depuis 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 OAMP.



Étape 2. Importez le certificat d'application VOS dans le serveur OAMP.

(i) Copiez le certificat VOS dans le répertoire %CVP_HOME%\conf\security du serveur OAMP.

(ii) Importez les certificats avec la commande suivante :

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

(ii) Redémarrer le serveur.

Section 3 : Échange de certificats entre le serveur CVP et les applications de la plate-forme VOS

Il s'agit d'une étape facultative pour sécuriser la communication SIP entre CVP et d'autres composants du centre de contact. Pour plus d'informations, reportez-vous au Guide de configuration CVP : Guide de configuration CVP - Sécurité.

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 autosignés PCCE Exchange - PCCE 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.