UCCE 12.6ソリューションでのExchange自己署名証明書

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[手順](#)
[CCE AWサーバおよびCCEコアアプリケーションサーバ](#)
[セクション1:Router\Logger、PG、およびAWサーバ間の証明書交換](#)
[セクション2: VOSプラットフォームアプリケーションとAWサーバ間の証明書交換](#)
[CVP OAMPサーバおよびCVPコンポーネントサーバ](#)
[セクション1:CVP OAMPサーバとCVPサーバおよびレポーティングサーバ間での証明書の交換](#)
[セクション2:CVP OAMPサーバとVOSプラットフォームアプリケーション間の証明書交換](#)
[セクション3:CVPサーバとVOSプラットフォームアプリケーション間の証明書交換](#)
[CVP CallStudio Webサービスの統合](#)
[関連情報](#)

概要

このドキュメントでは、Unified Contact Center Enterprise(UCCE)ソリューションで自己署名証明書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。

- UCCEリリース12.6(2)
- Customer Voice Portal(CVP)リリース12.6(2)
- Cisco Virtualized Voice Browser(VVB)

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。

- UCCE 12.6(2)
- CVP 12.6(2)

- Cisco VVB 12.6(2)
- CVP Operations Console（OAMP）
- CVPの新しいOAMP(NOAMP)

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。

背景説明

Rogger、Peripheral Gateway(PG)、管理ワークステーション(AW)/管理データサーバ(ADS)、Finesse、Cisco Unified Intelligence Center(CUIC)などのコアアプリケーションを含む新機能のUCCEソリューションの設定は、Contact Center Enterprise(CCE)の管理ページを通じて行われます。CVP、Cisco VVB、ゲートウェイなどの音声自動応答装置(IVR)アプリケーションでは、NOAMPが新機能の設定を制御します。CCE 12.5(1)以降では、security-management-compliance(SRC)により、CCE AdminおよびNOAMPへのすべての通信は、セキュアHTTPプロトコルを使用して厳密に行われます。

自己署名証明書の環境でこれらのアプリケーション間のシームレスでセキュアな通信を実現するには、サーバ間での証明書の交換が必須です。次のセクションでは、次の間で自己署名証明書を交換するために必要な手順について詳しく説明します。

- CCE AWサーバおよびCCEコアアプリケーションサーバ
- CVP OAMPサーバおよびCVPコンポーネントサーバ

注：このドキュメントは、CCEバージョン12.6にのみ適用されます。他のバージョンへのリンクについては、「関連情報」のセクションを参照してください。

手順

CCE AWサーバおよびCCEコアアプリケーションサーバ

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。

CCE AW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：Router and Logger(Rogger){A/B}、Peripheral Gateway(PG){A/B}、およびすべてのAW/ADS。

注:IISとDiagnostic Framework Portico(DFP)が必要です。

- VOSプラットフォーム：インベントリデータベースの一部であるFinesse、CUIC、ライブデータ(LD)、アイデンティティサーバ(IDS)、Cloud Connect、およびその他の該当するサーバ

。ソリューション内の他のAWサーバにも同じことが適用されます。

Router \ Logger Server：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AWサーバのIIS証明書

CCE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、次のセクションに分かれています。

セクション1:Router\Logger、PG、およびAWサーバ間の証明書交換
セクション2: VOSプラットフォームアプリケーションとAWサーバ間の証明書交換

セクション1:Router\Logger、PG、およびAWサーバ間の証明書交換

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。

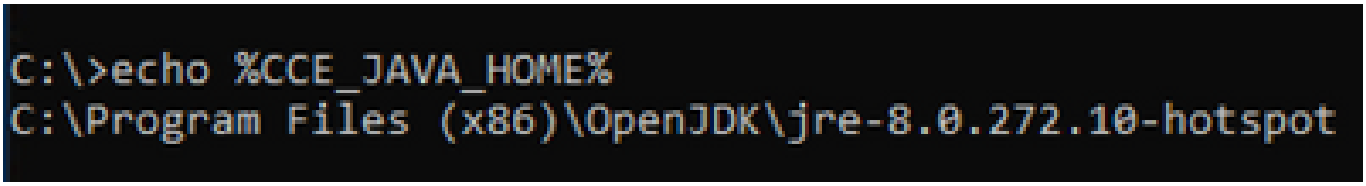
ステップ 1：Router\Logger、PG、およびすべてのAWサーバからIIS証明書をエクスポートします。
ステップ 2：Router\Logger、PG、およびすべてのAWサーバからDFP証明書をエクスポートします。
ステップ 3：IISおよびDFP証明書をRouter\Logger、PG、およびAWからAWサーバにインポートします。

ステップ4.AWサーバからRouter\LoggerおよびPGにIIS証明書をインポートします。

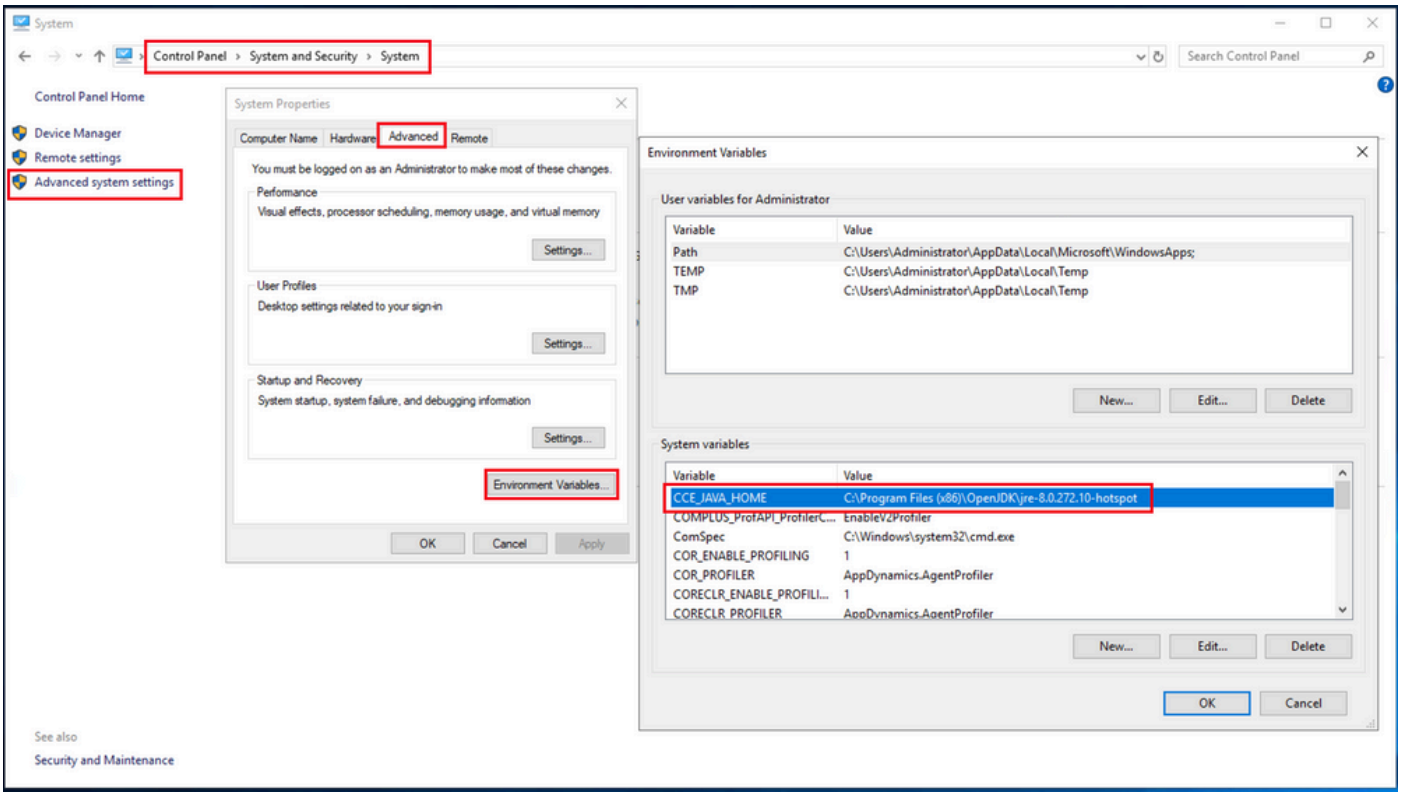
注意：作業を開始する前に、キーストアをバックアップし、管理者としてコマンドプロンプトを開く必要があります。

(i) javaキーツールがホストされている場所を確認するためのJavaホームパスを知っています。
Javaホームパスを見つける方法はいくつかあります。

オプション1:CLIコマンド：echo %CCE_JAVA_HOME%



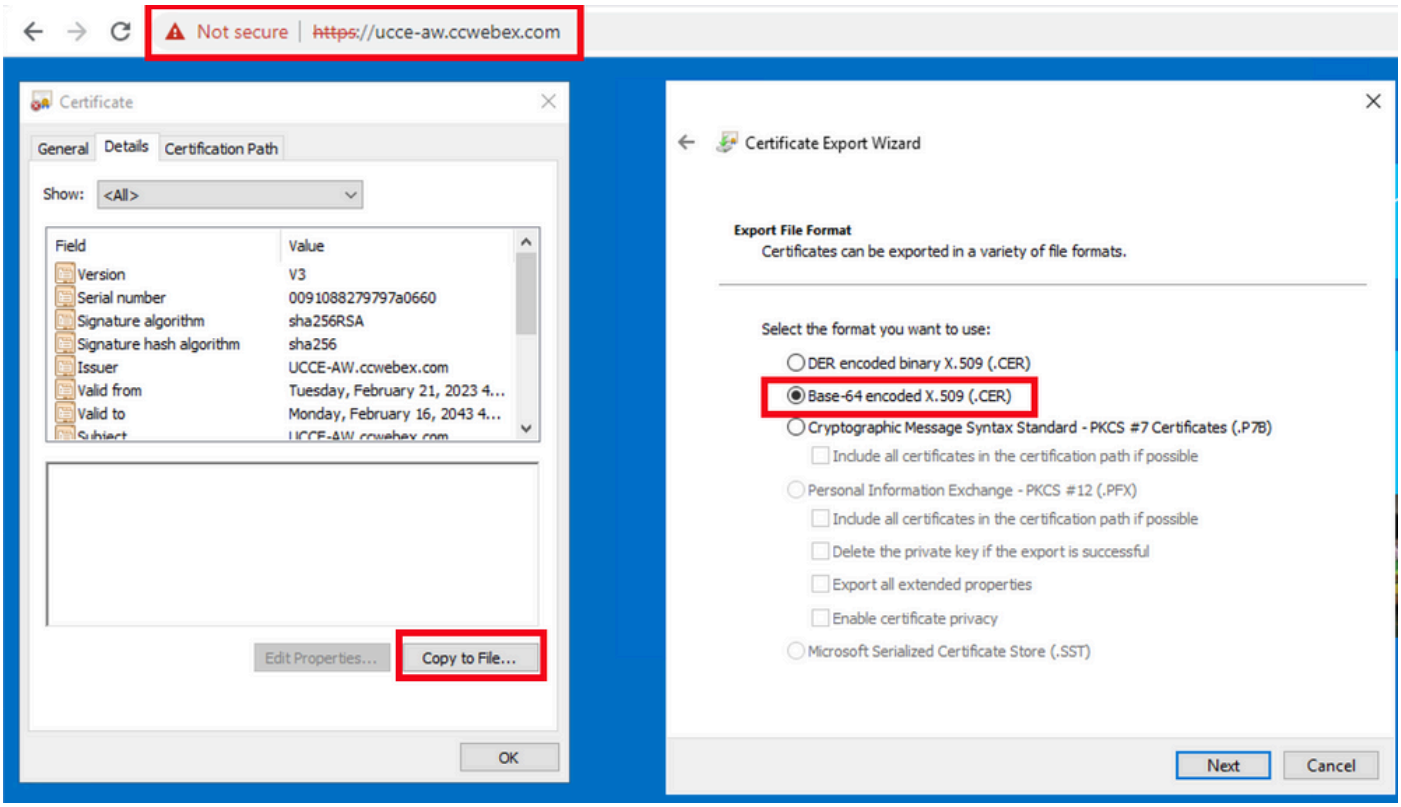
オプション2：図に示すように、高度なシステム設定を使用して手動で



(ii) cacertsファイルを<ICM install directory>ssl\フォルダからバックアップします。 別の場所にコピーできます。

ステップ 1：Router\Logger、PG、およびすべてのAWサーバからIIS証明書をエクスポートします。

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

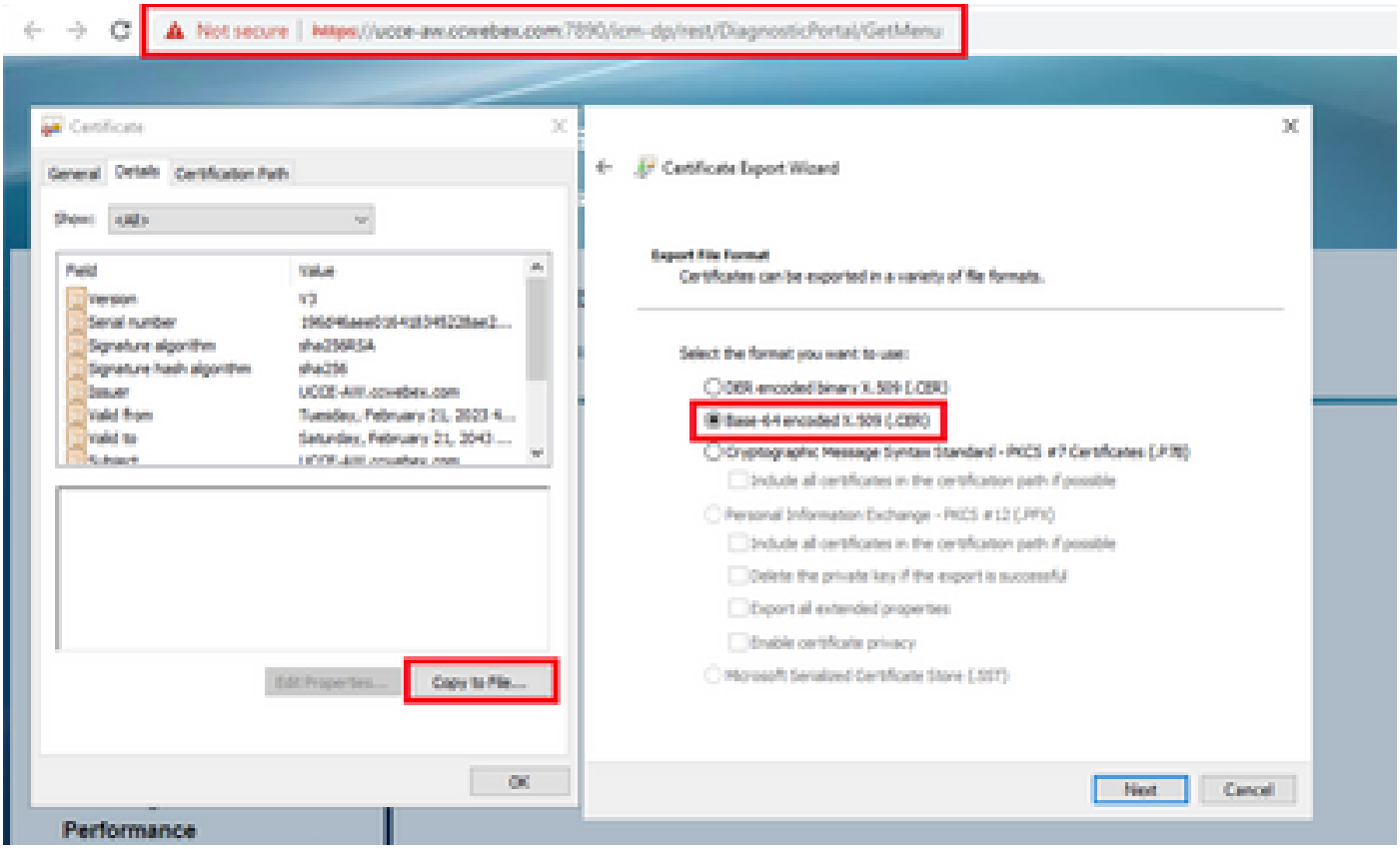


(ii)証明書を一時フォルダに保存します。たとえば、c:\temp\certsと入力し、証明書にICM{svr}[ab].cerという名前を付けます。

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

ステップ 2：Router\Logger、PG、およびすべてのAWサーバからDFP証明書をエクスポートします。

(i) AWサーバでブラウザを開き、サーバ（Router、Loggerまたは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

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

ステップ 3：IISおよびDFP証明書をRouter\Logger、PG、およびAWからAWサーバにインポートします。

IIS自己署名証明書をAW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\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
```

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AWサーバにインポートします。

AWサーバにDFP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\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
```

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AWサーバにインポートします。

AWサーバでApache Tomcatサービスを再起動します。

ステップ 4：AWサーバからRouter\LoggerおよびPGにIIS証明書をインポートします。

AW IIS自己署名証明書をRouter\LoggerおよびPG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\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
```

注:A側とB側のRoggerサーバとPGサーバにエクスポートされたすべてのAW IISサーバ証明書をインポートします。

Router\Logger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2: VOSプラットフォームアプリケーションとAWサーバ間の証明書交換

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：AWサーバへのVOS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

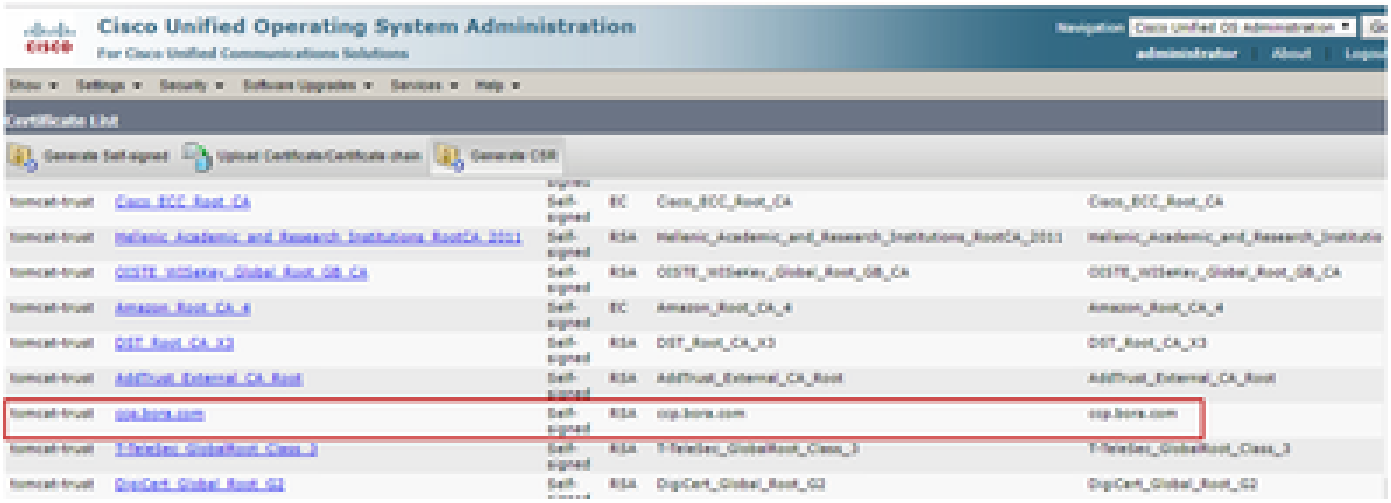
このプロセスは、次のようなVOSアプリケーションに適用できます。

- Finesse
- CUIC \ LD \ IDS
- クラウド接続

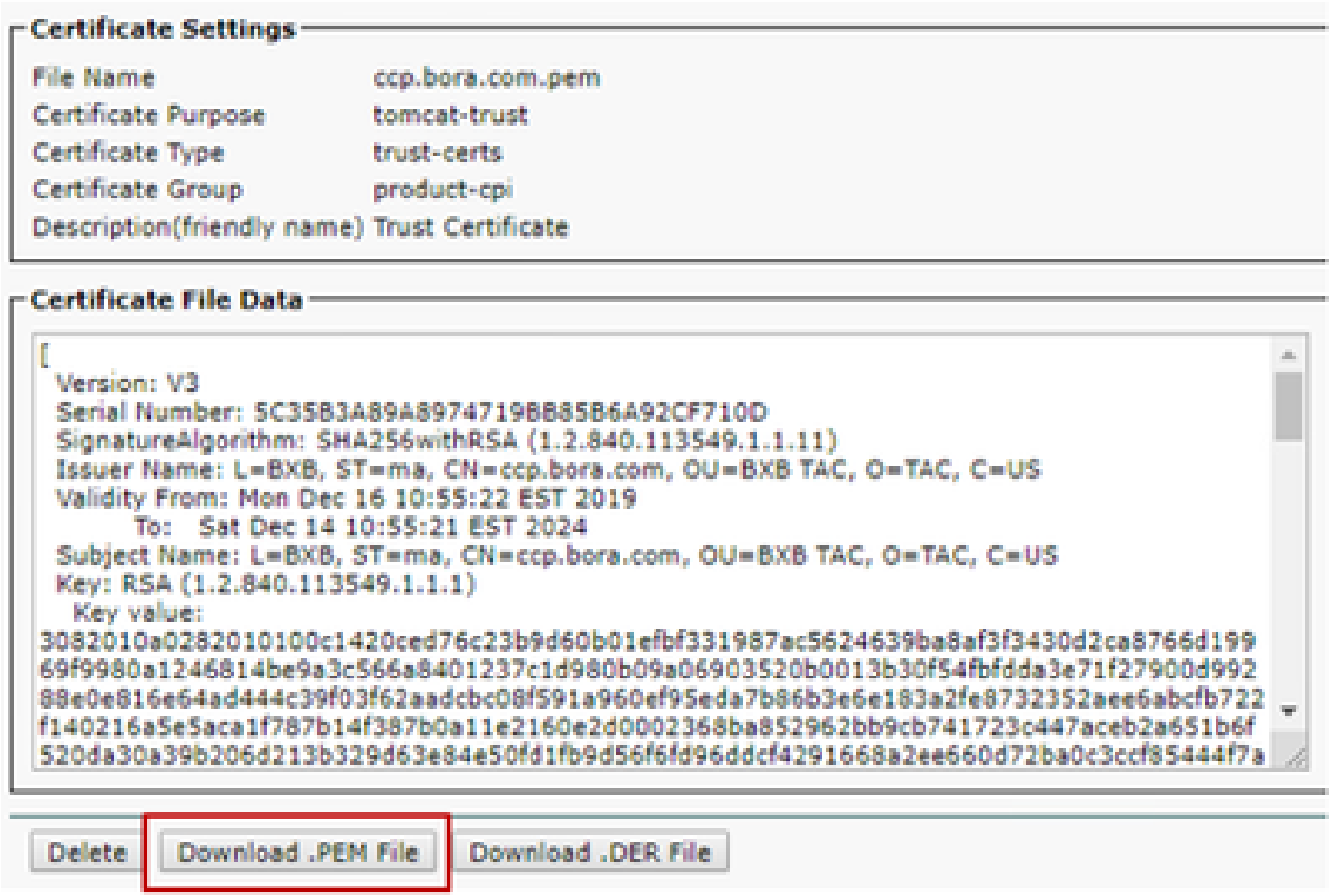
ステップ 1：VOSプラットフォームアプリケーションサーバ証明書のエクスポート

(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フォルダ内のアプリケーションプライマリサーバ証明書を見つけます。



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



注：サブスクライバに対して同じ手順を実行します。

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

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

AWサーバでApache Tomcatサービスを再起動します。

注：他のAWサーバでも同じタスクを実行します。

CVP OAMPサーバおよびCVPコンポーネントサーバ

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) CVP OAMPサーバ：このサーバは、

- Windowsプラットフォーム：CVPサーバおよびレポートサーバからのWebサービスマネージャ(WSM)証明書。
- VOSプラットフォーム：Cisco VVBおよびCloud Connectサーバ。

(ii) 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：OAMPサーバからのWSM証明書。
- VOSプラットフォーム：Cloud Connectサーバ、およびCisco VVBサーバ

(iii) CVP Reportingサーバ：このサーバは、

- Windowsプラットフォーム：OAMPサーバからのWSM証明書

(iv) Cisco VVBサーバ：このサーバは、

- Windowsプラットフォーム：CVPサーバからのVXML証明書と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

CVP環境で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、次の3つのセクションで説明します。

セクション1:CVP OAMPサーバとCVPサーバおよびレポーティングサーバ間での証明書の交換
セクション2:CVP OAMPサーバとVOSプラットフォームアプリケーション間の証明書交換
セクション3:CVPサーバとVOSプラットフォームアプリケーション間の証明書交換

セクション1:CVP OAMPサーバとCVPサーバおよびレポーティング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：CVPサーバ、Reporting and OAMPサーバからWSM証明書をエクスポートします。
ステップ 2：CVPサーバおよびレポートサーバからOAMPサーバにWSM証明書をインポートします。
ステップ 3：CVP OAMPサーバのWSM証明書をCVPサーバとレポートサーバにインポートします。

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。

ステップ 1：CVPサーバ、Reporting and OAMPサーバからWSM証明書をエクスポートします。

(i) WSM証明書を各CVPサーバから一時的な場所にエクスポートし、証明書の名前を任意の名前に変更します。名前はwsmX.crtに変更できます。Xはサーバのホスト名で置き換えます。たとえば、wsmcsa.crt、wsmcsb.crt、wsmrepa.crt、wsmrepb.crt、wsmoamp.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 -a
```

(ii)パス%CVP_HOME%\conf\security\wsm.crtの証明書を各サーバからコピーし、サーバタイプに基づいてwsmX.crtという名前に変更します。

ステップ 2：CVPサーバおよびレポートサーバからOAMPサーバにWSM証明書をインポートします。

(i)各CVPサーバとレポーティングサーバのWSM証明書(wsmX.crt)をOAMPサーバの%CVP_HOME%\conf\securityディレクトリにコピーします。

(ii)次のコマンドを使用して、これらの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 -a
```

(iii)サーバをリブートします。

ステップ 3：CVP OAMPサーバのWSM証明書をCVPサーバとレポートサーバにインポートします。

(i) OAMPサーバのWSM証明書(wsmoampX.crt)をすべてのCVPサーバとレポートサーバの%CVP_HOME%\conf\securityディレクトリにコピーします。

(ii)次のコマンドを使用して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 -a
```

(iii)サーバをリブートします。

セクション2:CVP OAMPサーバとVOSプラットフォームアプリケーション間の証明書交換

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プラットフォームからアプリケーション証明書を エクスポートします。

ステップ 2：OAMPサーバにVOSアプリケーション証明書をインポートします。

このプロセスは、次のようなVOSアプリケーションに適用できます。

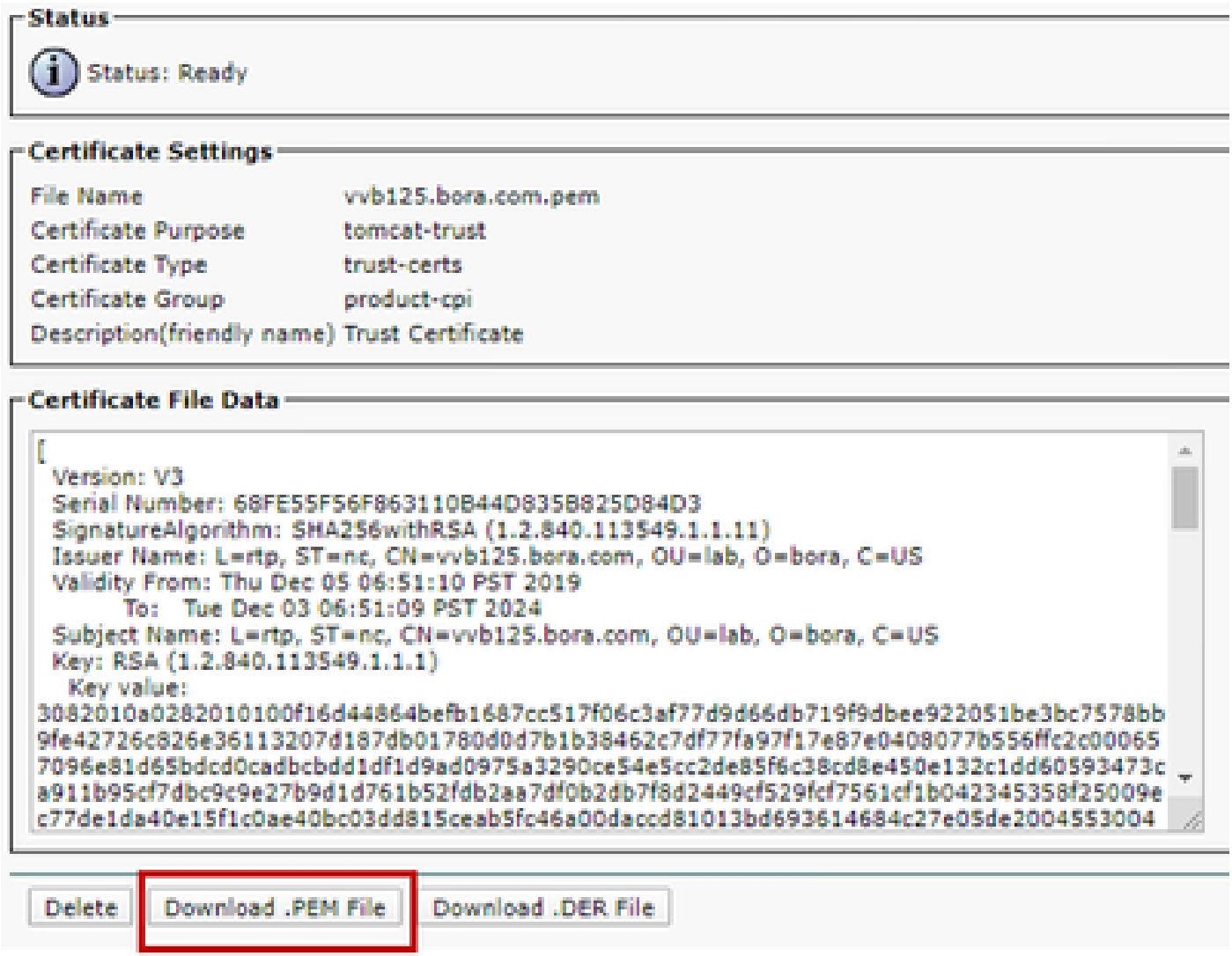
- CUCM
- VVB
- クラウド接続

ステップ 1：VOSプラットフォームからアプリケーション証明書を エクスポートします。

(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フォルダ内のアプリケーションプライマリサーバ証明書を見つけます。

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



ステップ 2：OAMPサーバにVOSアプリケーション証明書をインポートします。

(i) OAMPサーバの%CVP_HOME%\conf\securityディレクトリにVOS証明書をコピーします。

(ii)次のコマンドを使用して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 -a
```

(ii)サーバをリブートします。

セクション3:CVPサーバとVOSプラットフォームアプリケーション間の証明書交換

これは、CVPと他のコンタクトセンターコンポーネント間のSIP通信を保護するためのオプションの手順です。詳細については、『CVP Configuration Guide: CVP Configuration Guide - Security』を参照してください。

CVP CallStudio Webサービスの統合

Web Services Element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、

『Cisco Unified CVP VXML ServerおよびCisco Unified Call Studioリリース12.6(2)ユーザガイド – Webサービスの統合[Cisco Unified Customer Voice Portal] – シスコ』を参照してください。

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 PCCE自己署名証明書 – PCCE 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。