Austausch selbstsignierter Zertifikate in einer PCCE 12.6-Lösung

Inhalt

Einleitung

In diesem Dokument wird der Austausch selbstsignierter Zertifikate in der Cisco Packaged Contact Center Enterprise (PCCE)-Lösung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- PCCE-Version 12.6(2)
- Customer Voice Portal (CVP) Version 12.6(2)
- Virtualisierter Sprachbrowser (VB) 12.6(2)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrund

Bei der PCCE-Lösung ab 12.x werden alle Geräte über Single Pane of Glass (SPOG) gesteuert, der im Haupt-AW-Server gehostet wird. Aufgrund von Security-Management-Compliance (SRC) ab Version PCCE 12.5(1) erfolgt die gesamte Kommunikation zwischen SPOG und anderen Servern der Lösung ausschließlich über ein sicheres HTTP-Protokoll.

Zertifikate werden verwendet, um eine nahtlose sichere Kommunikation zwischen dem SPOG und den anderen Geräten zu erreichen. In einer selbstsignierten Zertifikatsumgebung ist der Zertifikataustausch zwischen den Servern ein Muss.

Vorgehensweise

Dies sind die Komponenten, aus denen selbstsignierte Zertifikate exportiert werden, und Komponenten, in die selbstsignierte Zertifikate importiert werden müssen.

(i) AW-Hauptserver: Dieser Server benötigt ein Zertifikat von:

- Windows-Plattform:
  - ICM: Router and Logger (Rogger){A/B}, Peripheral Gateway (PG){A/B}, alle ADS- und E-Mail- und Chat-Server (ECE).

Hinweis: IIS- und Diagnose-Framework-Zertifikate werden benötigt.

  - CVP: CVP-Server, CVP-Reporting-Server.

Hinweis: WSM-Zertifikate (Web Service Management) von den Servern werden benötigt.Zertifikate müssen den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) aufweisen.

- VOS-Plattform: Cloud Connect, Cisco Virtual Voice Browser (VVB), Cisco Unified Call Manager (CUCM), Finesse, Cisco Unified Intelligent Center (CUIC), Live Data (LD), Identity Server (IDS) und andere geeignete Server.

Dasselbe gilt für andere ADS-Server in der Lösung.

(ii) Router \ Protokollierungsserver: Dieser Server benötigt ein Zertifikat von:

- Windows-Plattform: Alle ADS-Server IIS-Zertifikat.

(iii) CUCM PG-Server: Für diesen Server ist ein Zertifikat erforderlich von:

- VOS-Plattform: CUCM-Publisher

Hinweis: Dies ist erforderlich, um den JTAPI-Client vom CUCM-Server herunterzuladen.

(iv) CVP-Server: Dieser Server benötigt ein Zertifikat von

- Windows-Plattform: Alle ADS-Server IIS-Zertifikat
- VOS-Plattform: Cloud Connect-Server, VVB-Server für sichere SIP- und HTTP-Kommunikation.

(v) CVP-Reporting-Server: Dieser Server benötigt ein Zertifikat von:

- Windows-Plattform: Alle ADS-Server IIS-Zertifikat

(vi) VVB-Server: Dieser Server benötigt ein Zertifikat von:

- Windows-Plattform: CVP VXML-Server (Secure HTTP), CVP-Anrufserver (Secure SIP)
- VOS-Plattform: Cloud Connect-Server

Die erforderlichen Schritte zum effektiven Austausch der selbstsignierten Zertifikate in der Lösung sind in drei Abschnitte unterteilt.

Abschnitt 1: Zertifikataustausch zwischen CVP- und ADS-Servern.

Abschnitt 2: Zertifikataustausch zwischen VOS-Plattformanwendungen und dem ADS-Server.

Abschnitt 3: Zertifikataustausch zwischen Roggers, PGs und ADS-Server.

Abschnitt 1: Zertifikataustausch zwischen CVP- und ADS-Servern

Um diesen Austausch erfolgreich abzuschließen, sind folgende Schritte erforderlich:

Schritt 1: CVP-Server-WSM-Zertifikate exportieren

Schritt 2: CVP-Server-WSM-Zertifikat in ADS-Server importieren

Schritt 3: ADS-Serverzertifikat exportieren

Schritt 4: ADS-Server auf CVP-Server und CVP Reporting-Server importieren.

Schritt 1: CVP-Serverzertifikate exportieren

Bevor Sie die Zertifikate von den CVP-Servern exportieren, müssen Sie die Zertifikate mit dem FQDN des Servers regenerieren, da sonst nur wenige Funktionen wie Smart Licensing, CVA und die CVP-Synchronisation mit SPOG Probleme bekommen können.

> **Vorsicht**: Bevor Sie beginnen, müssen Sie dies tun:
> 1. Öffnen Sie für CCE 12.6.2 den Ordner %CVP_HOME%\bin, um das Keystore-Kennwort zu generieren, und führen Sie die Datei DecryptKeystoreUtil.bat aus.
> 2. Führen Sie für 12.6.1 den Befehl %CVP_HOME%\conf\security.properties aus, um das Schlüsselspeicherkennwort zu generieren. Sie benötigen dieses Kennwort, wenn Sie die Befehle keytool ausführen.
> 3. Kopieren Sie den Ordner %CVP_HOME%\conf\security in einen anderen Ordner.
> 4. Öffnen Sie ein Befehlsfenster als Administrator, um die Befehle auszuführen.

> **Hinweis**: Sie können die in diesem Dokument verwendeten Befehle mithilfe des Parameters keytool -storepass optimieren. Für alle CVP-Server fügen Sie das Kennwort ein, das Sie aus der angegebenen Datei security.properties erhalten haben. Für die ADS-Server geben Sie das Passwort ein: **changeIt**

Führen Sie die folgenden Schritte aus, um das Zertifikat auf den CVP-Servern neu zu generieren:

(i) Auflisten der Zertifikate im Server

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

> **Hinweis**: Die CVP-Server verfügen über folgende selbstsignierte Zertifikate: wsm_certificate , vxml_certificate , callserver_certificate. Wenn Sie den Parameter -v des Schlüsselwerkzeugs verwenden, können Sie detailliertere Informationen zu jedem Zertifikat sehen. Darüber hinaus können Sie das ">"-Symbol am Ende des Listenbefehls keytool.exe hinzufügen, um die Ausgabe in eine Textdatei zu senden, z. B.: > test.txt

---

ii) Löschen der alten selbstsignierten Zertifikate

CVP-Server: Befehl zum Löschen der selbstsignierten Zertifikate:

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

CVP-Reporting-Server: Befehl zum Löschen der selbstsignierten Zertifikate:

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

> **Hinweis**: CVP-Reporting-Server verfügen über die selbstsignierten Zertifikate wsm_certificate, callserver_certificate.

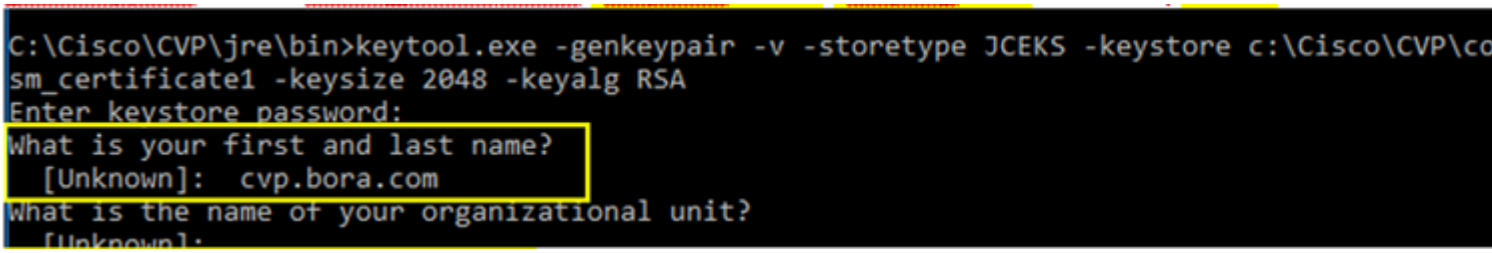
(iii) Generieren der neuen selbstsignierten Zertifikate mit dem FQDN des Servers

CVP-Server

Befehl zum Generieren des selbstsignierten Zertifikats für WSM:

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

Geben Sie den FQDN des Servers an, und **wie lautet Ihr Vor- und Nachname**?



Beantworten Sie die folgenden Fragen:

Wie lautet der Name Ihrer Organisationseinheit?

[Unbekannt]: <OU angeben>

Wie heißt Ihre Organisation?

[Unbekannt]: <Name der Organisation angeben>

Wie lautet der Name Ihrer Stadt oder Gemeinde?

[Unbekannt]: <Name der Stadt/des Ortes angeben>

Wie heißt Ihr Bundesland?

[Unbekannt]: <Name des Bundeslandes angeben>

Wie lautet der aus zwei Buchstaben bestehende Ländercode für diese Einheit?

[Unbekannt]: <Ländercode aus zwei Buchstaben angeben>

Geben Sie für die nächsten beiden Eingaben **yes** (Ja) an.

Führen Sie für vxml_certificate und callserver_certificate die gleichen Schritte aus:

```
%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
```

Neustart des CVP-Anrufservers

CVP-Reporting-Server

Befehl zum Generieren der selbstsignierten Zertifikate für WSM:

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

Geben Sie den FQDN des Servers für die Abfrage an, **wie lautet Ihr Vor- und Nachname?**, und fahren Sie mit den gleichen Schritten wie bei CVP-Servern fort.

Führen Sie für callserver_certificate die gleichen Schritte aus:

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

Starten Sie die Reporting-Server neu.

> **Hinweis**: Die selbstsignierten Zertifikate werden standardmäßig für zwei Jahre generiert. Verwenden Sie -valid XXXX, um das Ablaufdatum festzulegen, an dem Zertifikate neu generiert werden, andernfalls sind Zertifikate 90 Tage gültig. Für die meisten dieser Zertifikate muss eine Validierungszeit von 3-5 Jahren angemessen sein.

Hier sind einige Standardeingaben für die Gültigkeit:

1 Jahr	365
Zwei Jahre	730
Drei Jahre	1095
Vier Jahre	1460
Fünf Jahre	1895
Zehn Jahre	3650

> **Achtung**: Von 12,5 Zertifikate müssen **SHA 256**, Key Size **2048**, und Verschlüsselung Algorithm **RSA**, verwenden Sie diese Parameter, um diese Werte: -keyalg RSA und -keysize 2048. Es ist wichtig, dass die CVP-Keystore-Befehle den -storetype-Parameter JCEKS enthalten. Andernfalls kann das Zertifikat, der Schlüssel oder, schlimmer noch, der Schlüsselspeicher beschädigt werden.

(iv) Export von wsm_Certificate von CVP- und Reporting-Servern

a) Exportieren Sie das WSM-Zertifikat von jedem CVP-Server an einen temporären Speicherort, und benennen Sie das Zertifikat um, und geben Sie ihm den gewünschten Namen. Sie können sie in wsmcsX.crt umbenennen. Ersetzen Sie "X" durch eine eindeutige Zahl oder einen Buchstaben., d. h. wsmcsa.crt, wsmcsb.crt.

Befehl zum Exportieren der selbstsignierten Zertifikate:

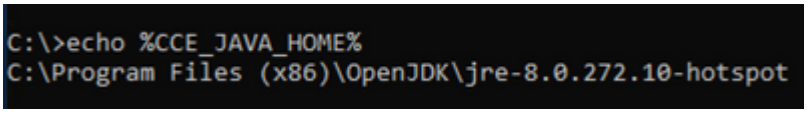
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -export -al
```

b) Kopieren Sie das Zertifikat aus dem Pfad **C:\Cisco\CVP\conf\security\wsm.crt**, benennen Sie es in **wsmcsX.crt um** und verschieben Sie es in einen temporären Ordner auf dem ADS-Server.

Schritt 2: CVP-Server WSM-Zertifikat in ADS-Server importieren

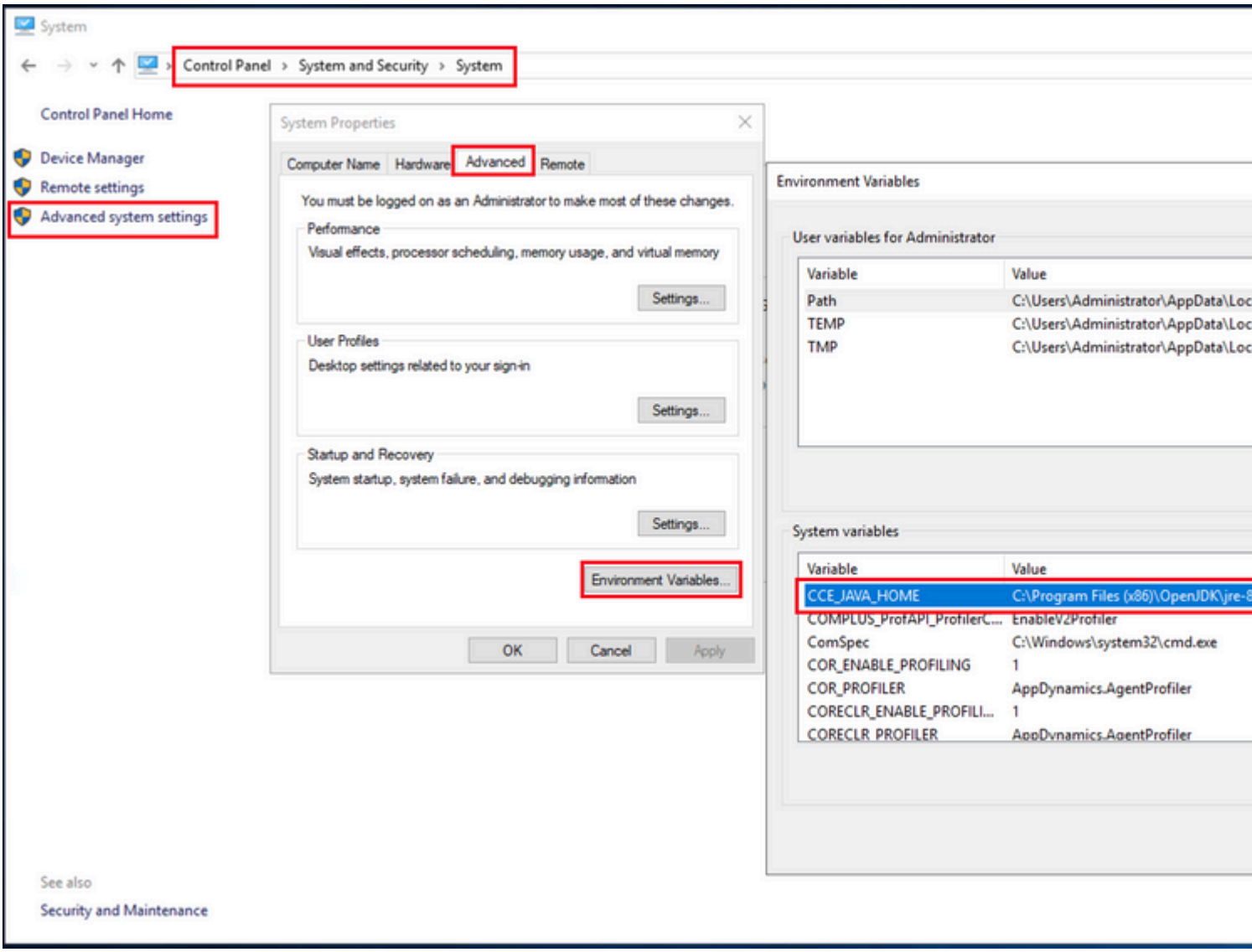
Um das Zertifikat in den ADS-Server zu importieren, müssen Sie das keytool verwenden, das Teil des Java-Toolsets ist. Es gibt mehrere Möglichkeiten, den Java-Home-Pfad zu finden, auf dem dieses Tool gehostet wird.

(i) CLI-Befehl > **echo %CCE_JAVA_HOME%**



Java-Home-Pfad

(ii) Manuell über **erweiterte Systemeinstellungen,** wie im Bild dargestellt.



Umgebungsvariablen

Auf PCCE 12.6 lautet der Standardpfad **C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin**

Befehle zum Importieren der selbstsignierten Zertifikate:

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

> **Hinweis**: Wiederholen Sie die Befehle für jedes CVP in der Bereitstellung, und führen Sie die gleiche Aufgabe für andere ADS-Server aus.

(iii) Starten Sie den Apache Tomcat-Dienst auf den ADS-Servern neu.

Schritt 3: ADS-Serverzertifikat exportieren

Für den CVP Reporting-Server müssen Sie das ADS-Zertifikat exportieren und in den Reporting-Server importieren. So gehen Sie vor:

(i) Navigieren Sie auf dem ADS-Server von einem Browser aus zur Server-URL: **https://{servername}**.

(ii) Speichern Sie das Zertifikat in einem temporären Ordner, z. B.: **c:\temp\certs,**
und geben Sie dem Zertifikat den Namen **ADS{svr}[ab].cer**.

```
keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias {fqdn_of_VOS} -keystore <ICM install
```

Starten Sie den Apache Tomcat-Dienst auf den ADS-Servern neu.

Hinweis: Führen Sie die gleiche Aufgabe auf anderen ADS-Servern aus.

Abschnitt 3: Zertifikataustausch zwischen Roggers-, PG- und ADS-Servern

Um diesen Austausch erfolgreich abzuschließen, sind folgende Schritte erforderlich:

Schritt 1: IIS-Zertifikat von Rogger und PG Server exportieren

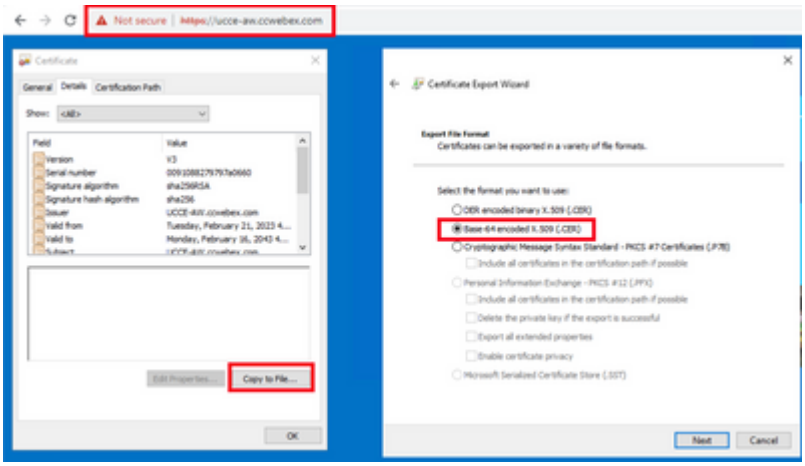
Schritt 2: Exportieren des DFP-Zertifikats (Diagnostic Framework Portico) von Rogger- und PG-Servern

Schritt 3: Zertifikate in ADS-Server importieren

Schritt 1: IIS-Zertifikat von Rogger- und PG-Servern exportieren

(i) Navigieren Sie auf dem ADS-Server von einem Browser zu den Servern (Roggers, PG) url: **https://{servername}**

(ii)Speichern Sie das Zertifikat in einem temporären Ordner, z. B. **c:\temp\certs, und nennen Sie das Zertifikat ICM{svr}[ab].cer.**



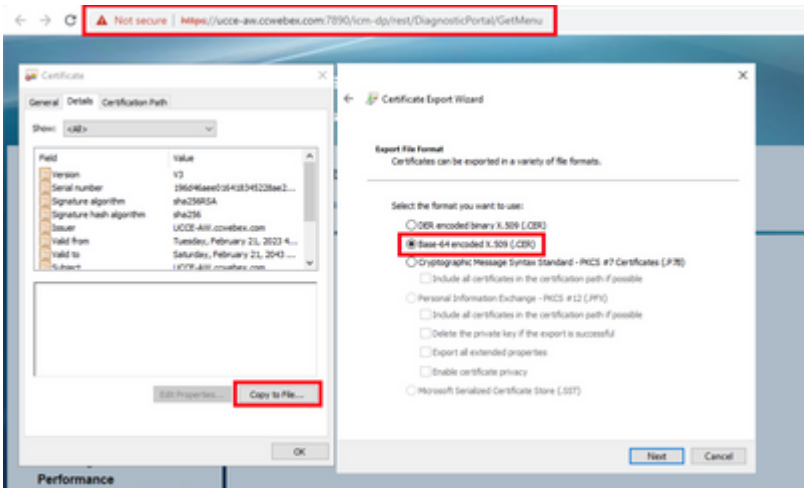
IIS-Zertifikat exportieren

Hinweis: Wählen Sie die Option Base-64-codiertes X.509 (.CER) aus.

Schritt 2: DFP-Zertifikat (Diagnostic Framework Portico) von Rogger- und PG-Servern exportieren

(i) Navigieren Sie auf dem ADS-Server von einem Browser zu den Servern (Roggers, PGs) DFP url : ***https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion***

(ii) Speichern Sie das Zertifikat im Ordner Beispiel c:\temp\certs, und geben Sie dem Zertifikat den Namen dfp{svr}[ab].cer



DFP-Zertifikat exportieren

Hinweis: Wählen Sie die Option Base-64-codiertes X.509 (.CER) aus.

Schritt 3: Zertifikate in ADS-Server importieren

Befehl zum Importieren der selbstsignierten IIS-Zertifikate in den ADS-Server. Der Pfad zum Ausführen des Schlüssel-Tools: **C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin.**

```
keytool.exe -import -file C:\Temp\certs\ICM{svr}[ab].cer -alias {fqdn_of_server}_IIS -keystore <ICM inst

Example: keytool.exe -import -file c:\temp\certs\ICMAWAIIS.cer -alias ICMAWA_IIS -keystore <ICM install
```

Hinweis: Importieren Sie alle in alle ADS-Server exportierten Serverzertifikate.

Befehl zum Importieren der selbstsignierten Diagnosezertifikate in den ADS-Server

```
keytool.exe -import -file C:\Temp\certs\dfp{svr}[ab].cer -alias {fqdn_of_server}_DFP -keystore <ICM inst

Example: keytool.exe -import -file c:\temp\certs\ICMAWADFP.cer -alias ICMAWA_DFP -keystore <ICM install
```

Hinweis: Importieren Sie alle in alle ADS-Server exportierten Serverzertifikate.

Starten Sie den Apache Tomcat-Dienst auf den ADS-Servern neu.

Abschnitt 4: CVP CallStudio WEBService-Integration

Ausführliche Informationen zum Einrichten einer sicheren Kommunikation für Web Services-Element und Rest_Client-Element

siehe [Benutzerhandbuch für Cisco Unified CVP VXML-Server und Cisco Unified Call Studio Release 12.6(2) - Web Service Integration [Cisco Unified Customer Voice Portal] - Cisco]

Zugehörige Informationen

- CVP-Konfigurationsleitfaden: CVP-Konfigurationsleitfaden - Sicherheit
- UCCE-Konfigurationsleitfaden: UCCE-Sicherheitsleitfaden
- PCCE-Administrationshandbuch: PCCE-Administrationshandbuch - Sicherheit
- UCCE-selbstsignierte Zertifikate: Austausch von UCCE-selbstsignierten Zertifikaten
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.