

Tauschen Sie selbstsignierte Zertifikate in einer PCCE-Lösung aus.

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrund](#)

[Vorgehensweise](#)

[Abschnitt 1: Zertifikataustausch zwischen CVP und ADS-Servern](#)

[Schritt 1: CVP-Serverzertifikate exportieren](#)

[Schritt 2: Importieren des CVP-Server-WSM-Zertifikats in den ADS-Server](#)

[Schritt 3: ADS-Serverzertifikat exportieren](#)

[Schritt 4: ADS-Server in CVP-Server und Reporting Server importieren](#)

[Abschnitt 2: Zertifikataustausch zwischen VOS-Plattformanwendungen und ADS-Server](#)

[Schritt 1: Exportieren von Zertifikaten für den Anwendungsserver der VOS-Plattform](#)

[Schritt 2: VOS-Plattformanwendung in ADS-Server importieren](#)

[Abschnitt 3: Zertifikataustausch zwischen Roggers , PG und ADS-Servern](#)

[Schritt 1: Exportieren des IIS-Zertifikats von nicht autorisierten und PG-Servern](#)

[Schritt 2: DFP-Zertifikat \(Export Diagnostic Framework Portico\) von Rogger- und PG-Servern](#)

[Schritt 3: Zertifikate in ADS-Server importieren](#)

[Abschnitt 4: CVP CallStudio-WEBService-Integration](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt den Austausch selbstsignierter Zertifikate zwischen dem Hauptverwaltungsserver (ADS/AW) und anderen Anwendungsservern in der Cisco Packaged Contact Center Enterprise (PCCE)-Lösung.

Unterstützt von Anuj Bhatia, Robert Rogier und Ramiro Amaya, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

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

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

Verwendete Komponenten

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

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

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 verstehen.

Hintergrund

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

Zertifikate werden verwendet, um eine nahtlose sichere Kommunikation zwischen SPOG und den anderen Geräten zu gewährleisten. In einer selbstsignierten Zertifikatsumgebung wird der Zertifikataustausch zwischen den Servern zum Muss. Dieser Zertifikataustausch ist auch erforderlich, um neue Funktionen zu aktivieren, die in der Version 12.5(1) vorhanden sind, wie z. B. Smart Licensing, WebEx Experience Management (WXM) und Customer Virtual Assistant (CVA).

Vorgehensweise

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

(i) Hauptserver für AW: Für diesen Server ist ein Zertifikat von erforderlich:

- Windows-Plattform: ICM: Router and Logger(Rogger){A/B}, Peripheral Gateway (PG){A/B}, alle ADS- sowie E-Mail- und Chat-Server (ECE). Anmerkung: IIS- und Diagnostic-Framework-Zertifikate werden benötigt.CVP: CVP-Server, CVP Reporting Server. Anmerkung 1: Das WSM-Zertifikat (Web Service Management) der Server wird benötigt.Anmerkung 2: Zertifikate müssen mit Fully Qualified Domain Name (FQDN) versehen sein.
- 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 relevante Server.

Gleiches gilt für andere ADS-Server in der Lösung.

(ii) Router \ Logger Server: Für diesen Server ist ein Zertifikat von erforderlich:

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

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

- VOS-Plattform: CUCM-Publisher. Anmerkung: 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-Zertifikate
- VOS-Plattform: Cloud Connect-Server für die WXM-Integration, VVB-Server für sichere SIP- und HTTP-Kommunikation.

v) **CVP-Reporting-Server:** Für diesen Server ist ein Zertifikat von erforderlich:

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

vi) **VVB-Server:** Für diesen Server ist ein Zertifikat von erforderlich:

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

Die Schritte für den effektiven Austausch der selbstsignierten Zertifikate in der Lösung sind in drei Abschnitte unterteilt.

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

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

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

Abschnitt 1: Zertifikataustausch zwischen CVP und ADS-Servern

Um diesen Austausch erfolgreich abzuschließen, müssen folgende Schritte ausgeführt werden:

Schritt 1: Exportieren von CVP-Server-WSM-Zertifikaten.

Schritt 2: Importieren des CVP-Server-WSM-Zertifikats in den ADS-Server

Schritt 3: ADS-Serverzertifikat exportieren.

Schritt 4: Importieren Sie den ADS-Server in CVP-Server und den CVP Reporting Server.

Schritt 1: CVP-Serverzertifikate exportieren

Bevor Sie die Zertifikate von den CVP-Servern exportieren, müssen Sie die Zertifikate mit dem FQDN des Servers neu generieren. Andernfalls können nur wenige Funktionen wie Smart Licensing, CVA und die CVP-Synchronisierung mit SPOG Probleme verursachen.

Vorsicht: Bevor Sie beginnen, müssen Sie Folgendes tun:

- Rufen Sie das Keystore-Kennwort ab. Führen Sie diesen Befehl aus:
mehr %CVP_HOME%\conf\security.properties
- Kopieren Sie den Ordner %CVP_HOME%\conf\security in einen anderen Ordner.
- Öffnen Sie ein Befehlsfenster als Administrator, um die Befehle auszuführen.

Anmerkung: Sie können die in diesem Dokument verwendeten Befehle mithilfe des keytool-Parameters -storepass rationalisieren. 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 Kennwort ein: **Änderung**

So generieren Sie das Zertifikat auf den CVP-Servern:

(i) Listet die Zertifikate im Server auf

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

Anmerkung: Die CVP-Server verfügen über folgende selbstsignierte Zertifikate: wsm_certificate , vxml_certificate , callserver_certificate. Wenn Sie den Parameter -v des keytools verwenden, können Sie detailliertere Informationen zu jedem Zertifikat anzeigen. Darüber hinaus können Sie das Symbol ">" am Ende des Listenbefehls keytool.exe hinzufügen, um die Ausgabe an 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 -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
```

CVP Reporting Server: Befehl zum Löschen der selbstsignierten Zertifikate:

```
%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
```

Anmerkung: CVP-Reporting-Server verfügen über diese 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 -genkeypair -v -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Geben Sie den FQDN des Servers an. **Wie lautet Ihr Vor- und Nachname?**

```
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
Enter keystore password:
What is your first and last name?
[unknown]: cvp.bora.com
What is the name of your organizational unit?
[unknown]:
```

Beantworten Sie die folgenden Fragen:

Wie lautet der Name Ihrer Organisationseinheit?

[Unbekannt]: <OU angeben>

Wie lautet der Name Ihrer Organisation?

[Unbekannt]: <Name des Orgs angeben>

Wie lautet der Name Ihrer Stadt bzw. Ihres Ortes?

[Unbekannt]: <Stadt/Ort angeben>

Wie heißt Ihr Bundesland?

[Unbekannt]: <Bundesland/Region angeben>

Wie lautet der Ländercode aus zwei Buchstaben für diese Einheit?

[Unbekannt]: <Ländercode aus zwei Buchstaben angeben>

Geben Sie **yes** für die nächsten zwei Eingaben an.

Führen Sie die gleichen Schritte für `vxml_certificate` und `callserver_certificate` aus:

```
%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
```

Starten Sie den CVP-Anrufserver neu.

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 -genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Geben Sie den FQDN des Servers für die Abfrage an, **was ist Ihr erster und Nachname?** und befolgen Sie die gleichen Schritte wie bei CVP-Servern.

Führen Sie die gleichen Schritte für `callserver_certificate` aus:

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

Starten Sie die Reporting-Server neu.

Anmerkung: Standardmäßig werden die selbstsignierten Zertifikate für zwei Jahre generiert. Verwenden Sie -Validität XXXX, um das Ablaufdatum festzulegen, wenn Zertifikate neu generiert werden. Andernfalls sind Zertifikate 90 Tage gültig. Für die meisten dieser Zertifikate müssen 3-5 Jahre eine angemessene Validierungszeit sein.

Hier einige Angaben zur Standardgültigkeit:

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

Vorsicht: Bei 12.5-Zertifikaten muss es sich um **SHA 256**, Key Size **2048** und Verschlüsselungsalgorithmus **RSA** handeln. Verwenden Sie diese Parameter, um folgende Werte festzulegen: -keyalg RSA und -keysize 2048. Es ist wichtig, dass die CVP-Keystore-Befehle den -storetype-JCEKS-Parameter enthalten. Andernfalls kann das Zertifikat, der Schlüssel oder, schlimmer noch, der Keystore beschädigt werden.

(iv) Exportieren Sie 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 mit einem gewünschten Namen um. Sie können es als wsmcsX.crt umbenennen. Ersetzen Sie "X" durch eine eindeutige Nummer oder einen Buchstaben. das wsmcsa.crt, wsmcsb.crt ist.

Befehl zum Exportieren der selbstsignierten Zertifikate:

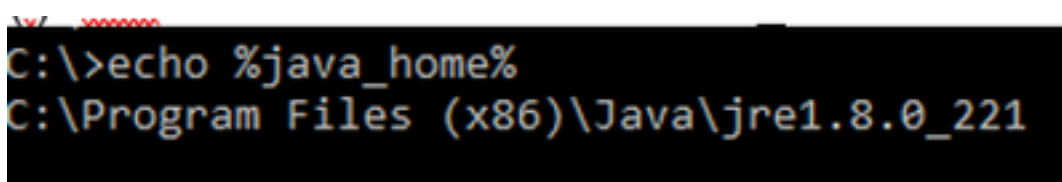
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\keystore -export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b) 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: Importieren des CVP-Server-WSM-Zertifikats in den ADS-Server

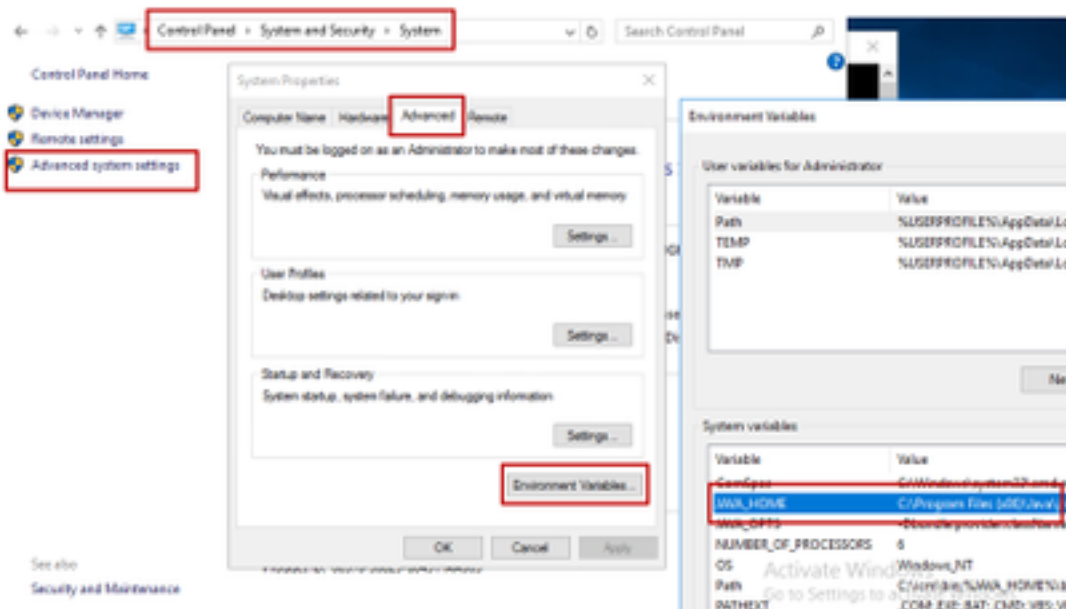
Um das Zertifikat im ADS-Server zu importieren, müssen Sie das keytool verwenden, das Teil des Java-Toolsets ist. Es gibt mehrere Möglichkeiten, den Java-Home-Pfad zu finden, auf dem dieses Tool gehostet wird.

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



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

(ii) Manuell über die **erweiterte Systemeinstellung**, wie im Bild gezeigt.



Auf PCCE 12.5 lautet der Standardpfad **C:\Program Dateien (x86)\Java\jre1.8.0_221\bin**.

Befehl zum Importieren der selbstsignierten Zertifikate:

```
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
```

Anmerkung: Wiederholen Sie die Befehle für jedes CVP in der Bereitstellung, und führen Sie die gleiche Aufgabe auf anderen ADS-Servern aus.

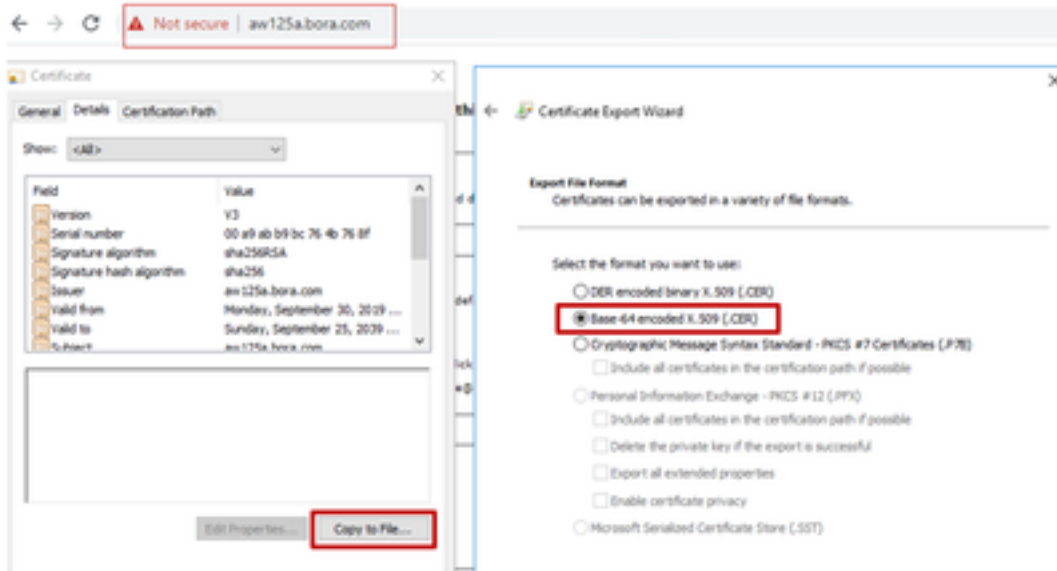
d) Starten Sie den Apache Tomcat-Dienst auf den ADS-Servern neu.

Schritt 3: ADS-Serverzertifikat exportieren

Für den CVP-Reporting-Server müssen Sie das ADS-Zertifikat exportieren und in den Reporting-Server importieren. Die folgenden Schritte sind erforderlich:

- (i) Navigieren Sie auf dem ADS-Server von einem Browser zur Server-URL: **https://{servername}**
- (ii) Speichern Sie das Zertifikat in einem temporären Ordner, z. B.: **c:\temp\certs** und nennen Sie das Zertifikat als **ADS{svr}{ab}.cer**.

CCE via Chrome Browser



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

Schritt 4: ADS-Server in CVP-Server und Reporting Server importieren

(i) Kopieren Sie das Zertifikat in CVP-Server und den CVP-Reporting-Server im Verzeichnis **C:\Cisco\CVP\conf\security**.

(ii) Importieren Sie das Zertifikat auf CVP-Server und den CVP Reporting Server.

```
%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
```

Führen Sie die gleichen Schritte für andere ADS-Server aus.

(iii) Neustarten der CVP-Server und des Reporting-Servers

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

Um diesen Austausch erfolgreich abzuschließen, müssen folgende Schritte ausgeführt werden:

Schritt 1: Exportieren von Zertifikaten für den Anwendungsserver der VOS-Plattform

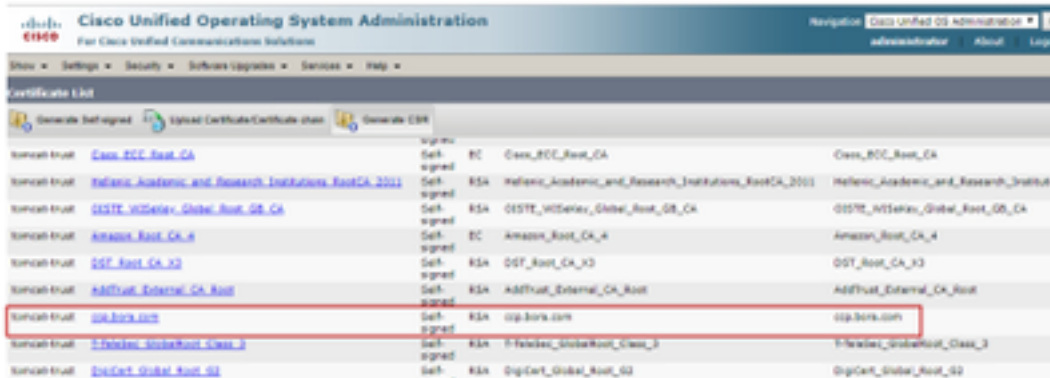
Schritt 2: Importieren von Anwendungszertifikaten für die VOS-Plattform in den ADS-Server

Dieser Prozess gilt für alle VOS-Anwendungen, z. B.:

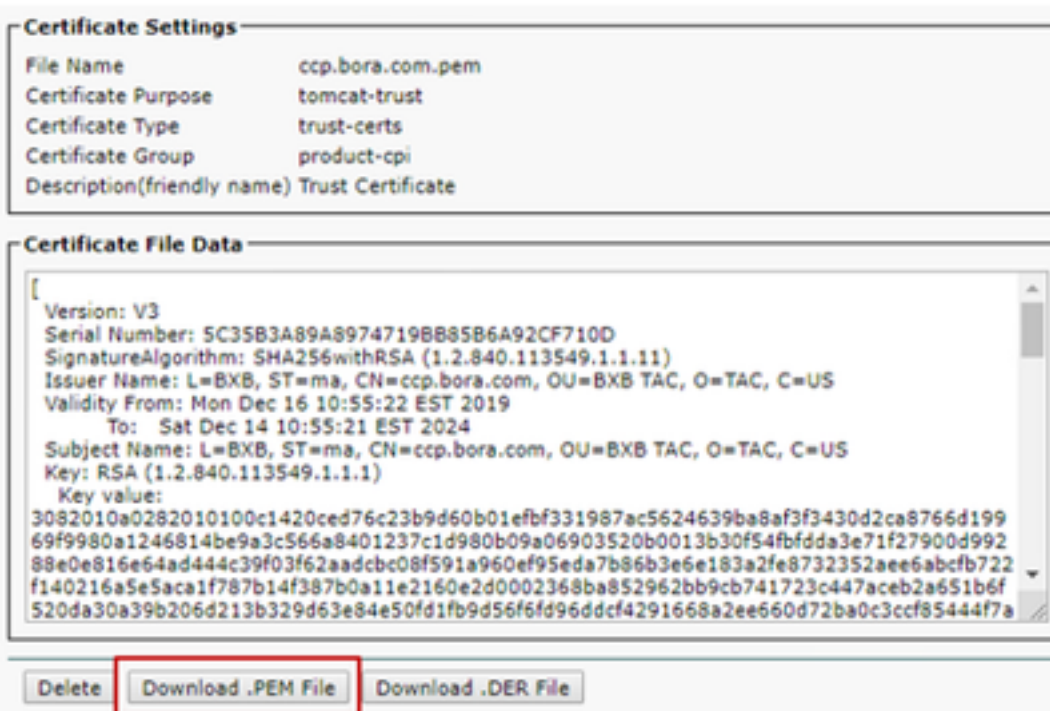
- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- Cloud Connect

Schritt 1: Exportieren von Zertifikaten für den Anwendungsserver der VOS-Plattform

- (i) Navigieren Sie zur Seite "Cisco Unified Communications Operating System Administration" (Verwaltung des Cisco Unified Communications-Betriebssystems): <https://FQDN:8443/cmplatform>
- (ii) Navigieren Sie zu **Sicherheit > Zertifikatsverwaltung**, und suchen Sie die primären Serverzertifikate der Anwendung im Ordner **tomcat-trust**.



- (iii) Wählen Sie das Zertifikat aus, und klicken Sie auf **.PEM-Datei herunterladen**, um es in einem temporären Ordner auf dem ADS-Server zu speichern.



Anmerkung: Führen Sie die gleichen Schritte für den Abonnenten aus.

Schritt 2: VOS-Plattformanwendung in ADS-Server importieren

Pfad zum Ausführen des Key-Tools: **C:\Program Dateien (x86)\Java\jre1.8.0_221\bin**

Befehl zum Importieren der selbstsignierten Zertifikate:

```
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
```

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

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

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

Um diesen Austausch erfolgreich abzuschließen, müssen folgende Schritte ausgeführt werden:

Schritt 1: Exportieren des IIS-Zertifikats von nicht autorisierten und PG-Servern

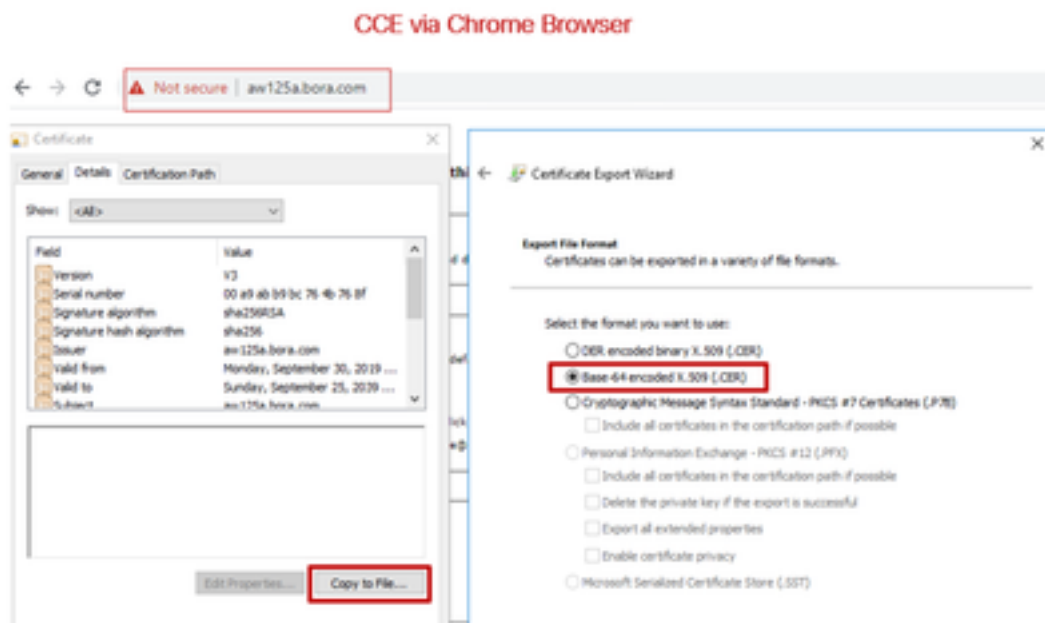
Phase 2: DFP-Zertifikat (Export Diagnostic Framework Portico) von Rogger- und PG-Servern

Schritt 3: Importieren von Zertifikaten in ADS-Server

Schritt 1: Exportieren des IIS-Zertifikats von nicht autorisierten und PG-Servern

(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 als `ICM{svr}[ab].cer`



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

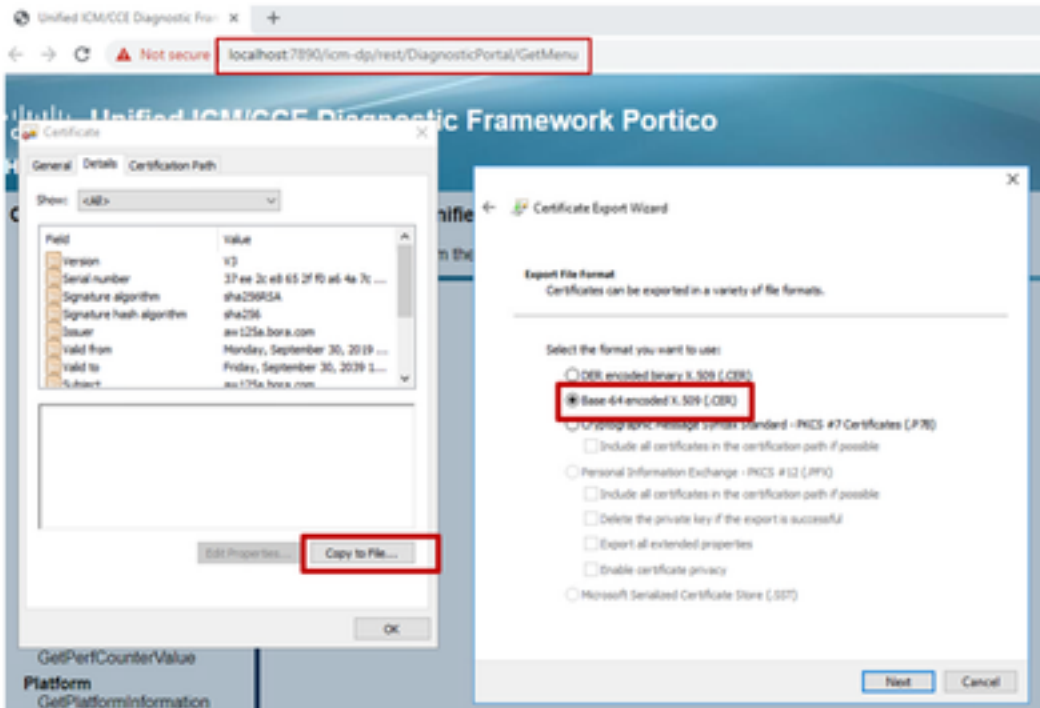
Schritt 2: DFP-Zertifikat (Export Diagnostic Framework Portico) von Rogger- und PG-Servern

(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 nennen Sie das Zertifikat

als dfp{svr}[ab].cer.

Portico via Chrome Browser



Anmerkung: 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 Key-Tools: **C:\Program Dateien (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
```

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

Befehl zum Importieren der selbstsignierten Diagnosezertifikate in den ADS-Server

```
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
```

Anmerkung: 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 Herstellen einer sicheren Kommunikation für Webdienstelement und REST_Client-Element

Weitere Informationen finden Sie im [Benutzerhandbuch für Cisco Unified CVP VXML Server und Cisco Unified Call Studio Release 12.5\(1\) - Web Service Integration \[Cisco Unified Customer Voice Portal\] - Cisco](#)

Zugehörige Informationen

- CVP-Konfigurationsleitfaden: [CVP-Konfigurationsleitfaden - Sicherheit](#)
- UCCE-Konfigurationsleitfaden: [UCCE-Konfigurationsleitfaden - Sicherheit](#)
- PCCE-Administrationsleitfaden: [PCE-Administratorhandbuch - Sicherheit](#)
- Selbstsignierte UCCE-Zertifikate: [Tauschen Sie selbstsignierte UCCE-Zertifikate aus.](#)
- Installation und Migration zu OpenJDK in CCE 12.5(1): [CCE OpenJDK-Migration](#)
- Installation und Migration zu OpenJDK in CVP 12.5(1): [CVP OpenJDK Migration](#)