

Selbstsignierte Zertifikate in einer UCCE 12.6-Lösung austauschen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Vorgehensweise](#)

[CCE AW-Server und CCE Core-Anwendungsserver](#)

[Abschnitt 1: Zertifikataustausch zwischen Router/Logger, PG und AW-Server](#)

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

[CVP OAMP-Server und CVP-Komponentenserver](#)

[Abschnitt 1: Zertifikataustausch zwischen CVP OAMP-Server und CVP-Server und Reporting-Server](#)

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

[Abschnitt 3: Zertifikataustausch zwischen CVP-Server- und VOS-Plattformanwendungen](#)

[CVP CallStudio-Webdienstintegration](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird der Austausch selbstsignierter Zertifikate in der Unified Contact Center Enterprise (UCCE)-Lösung beschrieben.

Voraussetzungen

Anforderungen

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

- UCCE-Version 12.6(2)
- Customer Voice Portal (CVP) Version 12.6(2)
- Cisco Virtualized Voice Browser (VB)

Verwendete Komponenten

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

- UCCE 12.6(2)
- CVP 12.6(2)
- Cisco VVB 12,6 (2)
- CVP Operations Console (OAMP)
- CVP New OAMP (NOAMP)

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.

Hintergrundinformationen

Bei der UCCE-Lösung erfolgt die Konfiguration neuer Funktionen, die Kernanwendungen wie Roggers, Peripheral Gateways (PG), Admin Workstations (AW), Finesse, Cisco Unified Intelligent Center (CUIC) usw. umfassen, über die Administratorseite von Contact Center Enterprise (CCE). Bei Interactive Voice Response (IVR)-Anwendungen wie CVP, Cisco VVB und Gateways steuert NOAMP die Konfiguration neuer Funktionen. Ab CCE 12.5(1) erfolgt die gesamte Kommunikation zu CCE Admin und NOAMP aufgrund von Security-Management-Compliance (SRC) ausschließlich über ein sicheres HTTP-Protokoll.

Um eine nahtlose sichere Kommunikation zwischen diesen Anwendungen in einer selbstsignierten Zertifikatumgebung zu erreichen, ist der Austausch von Zertifikaten zwischen den Servern ein Muss. Im nächsten Abschnitt werden die erforderlichen Schritte für den Austausch selbstsignierter Zertifikate zwischen den folgenden Komponenten detailliert beschrieben:

- CCE AW-Server und CCE Core-Anwendungsserver
- CVP OAMP-Server und CVP-Komponentenserver

Hinweis: Dieses Dokument bezieht sich NUR auf CCE-Version 12.6. Links zu anderen Versionen finden Sie im Abschnitt mit verwandten Informationen.

Vorgehensweise

CCE AW-Server und CCE Core-Anwendungsserver

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

CCE AW-Server: Dieser Server benötigt ein Zertifikat von:

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

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

- VOS-Plattform: Cisco Unified Call Manager (CUCM), Finesse, CUIC, Live Data (LD), Identity Server (IDS), Cloud Connect und andere geeignete Server, die Teil der Bestandsdatenbank sind.

Dasselbe gilt für andere AW-Server in der Lösung.

Router \ Protokollierungsserver: Dieser Server benötigt ein Zertifikat von:

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

Die erforderlichen Schritte für einen effektiven Austausch der selbstsignierten Zertifikate gegen CCE sind in diese Abschnitte unterteilt.

Abschnitt 1: Zertifikataustausch zwischen Router\Logger, PG und AW-Server.

Abschnitt 2: Zertifikataustausch zwischen VOS-Plattformanwendung und AW-Server.

Abschnitt 1: Zertifikataustausch zwischen Router\Logger, PG und AW-Server

Um diesen Austausch erfolgreich abzuschließen, sind folgende Schritte erforderlich:

Schritt 1: Exportieren Sie IIS-Zertifikate von Router\Logger ,PG und allen AW-Servern.

Schritt 2: Exportieren Sie DFP-Zertifikate (Diagnostic Framework Portal) von Router\Logger- und PG-Servern.

Schritt 3: Importieren Sie IIS- und DFP-Zertifikate von Router\Logger, PG auf AW-Server.

Schritt 4: IIS-Zertifikat von AW-Servern in Router\Logger importieren

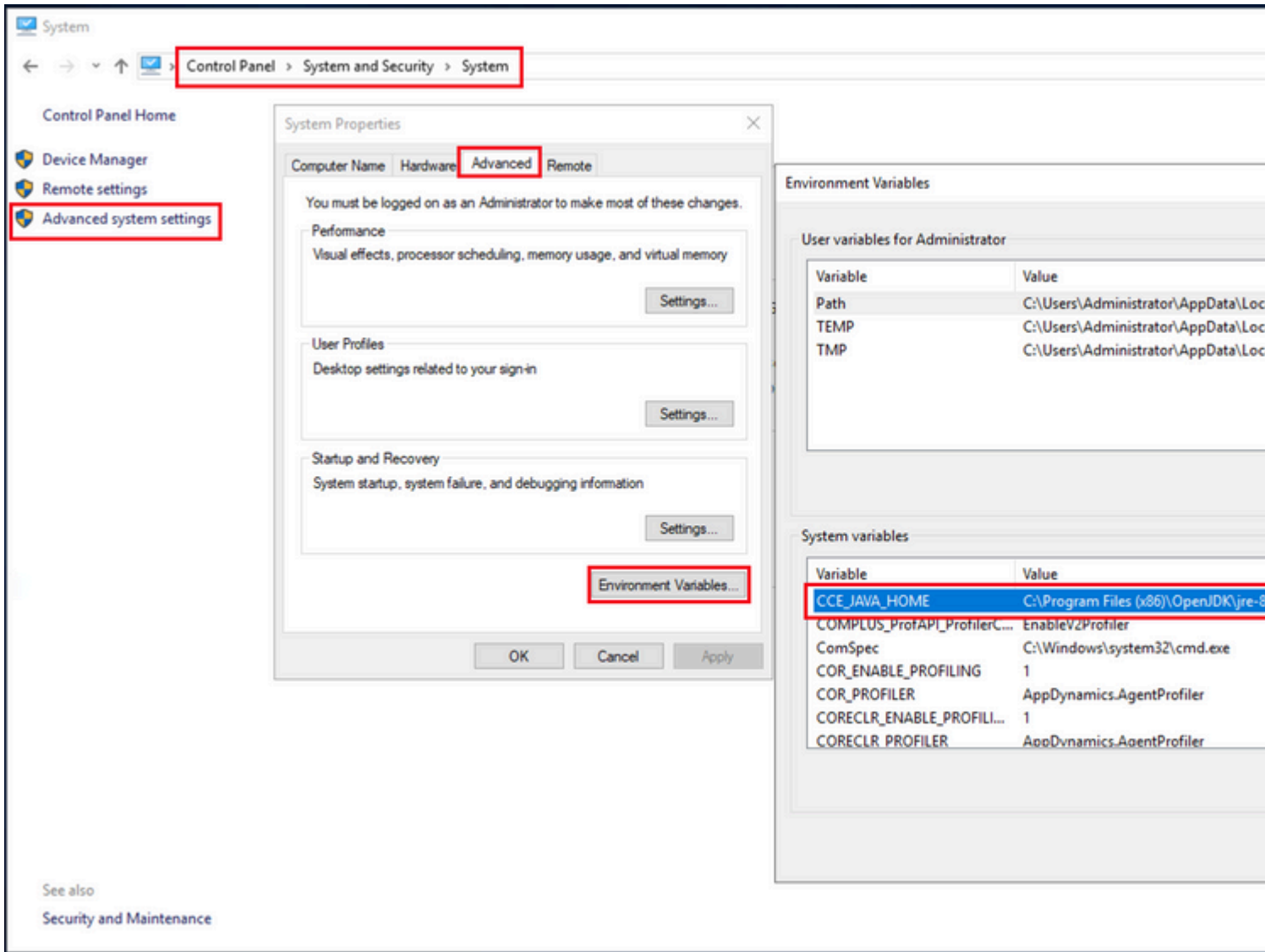
Vorsicht: Bevor Sie beginnen, müssen Sie den Schlüsselspeicher sichern und die Befehle vom Java-Home als Administrator ausführen.

(i) Kennen Sie den Java-Home-Pfad, um sicherzustellen, wo das Java-Keytool gehostet wird. Es gibt mehrere Möglichkeiten, den Java-Home-Pfad zu finden.

Option 1: CLI-Befehl: **echo %CCE_JAVA_HOME%**

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

Option 2: Manuell über die erweiterte Systemeinstellung, wie im Bild dargestellt

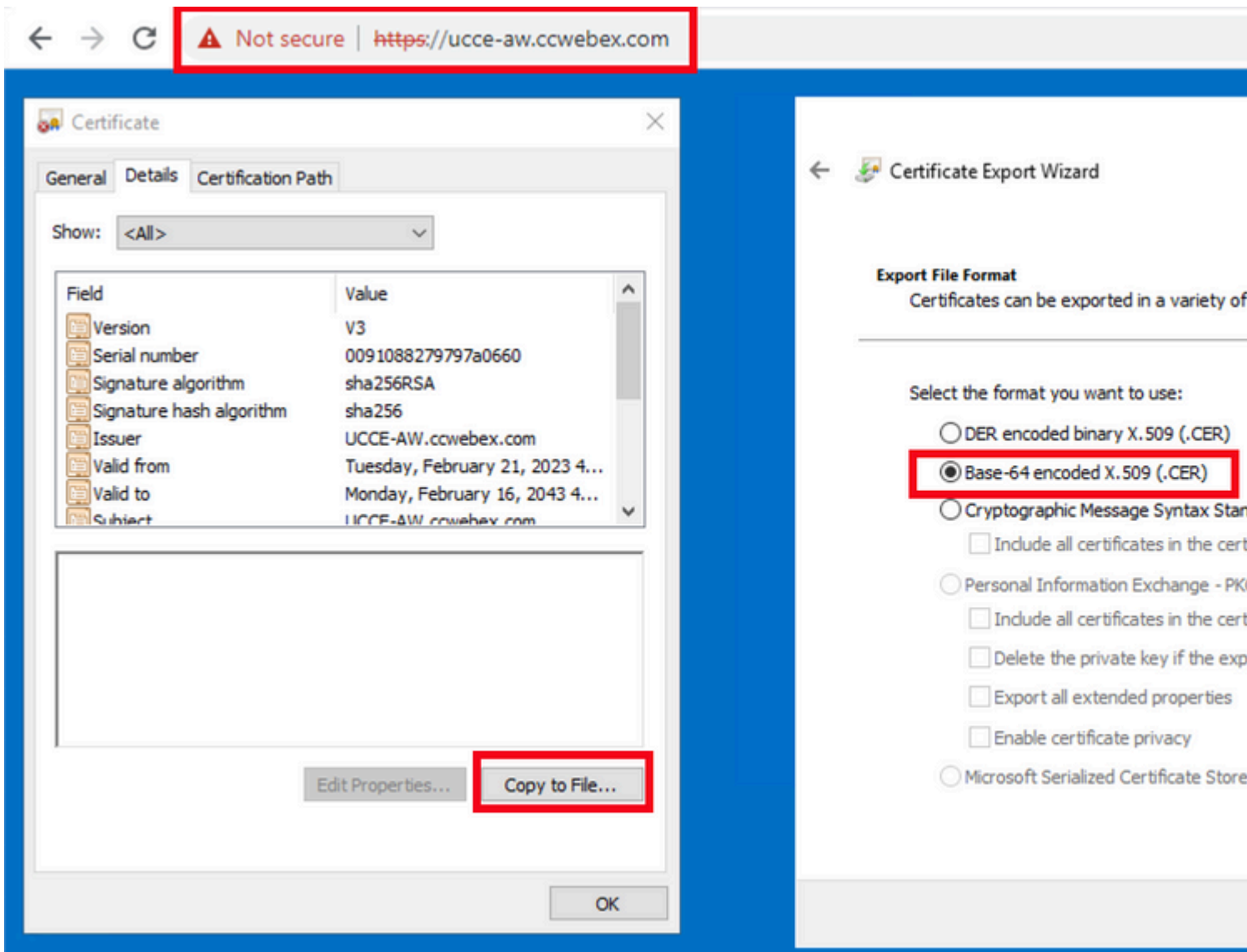


(ii) Sichern Sie die Datei cacerts aus dem Ordner <ICM install directory>ssl\ . Sie können es an einen anderen Speicherort kopieren.

(iii) Öffnen Sie ein Befehlsfenster als Administrator, um die Befehle auszuführen.

Schritt 1: Exportieren Sie IIS-Zertifikate von Router\Logger, PG und allen AW-Servern.

(i) Navigieren Sie auf einem AW-Server von einem Browser zu den Servern (Roggers, PG, andere AW-Server) url: <https://{servername}>.

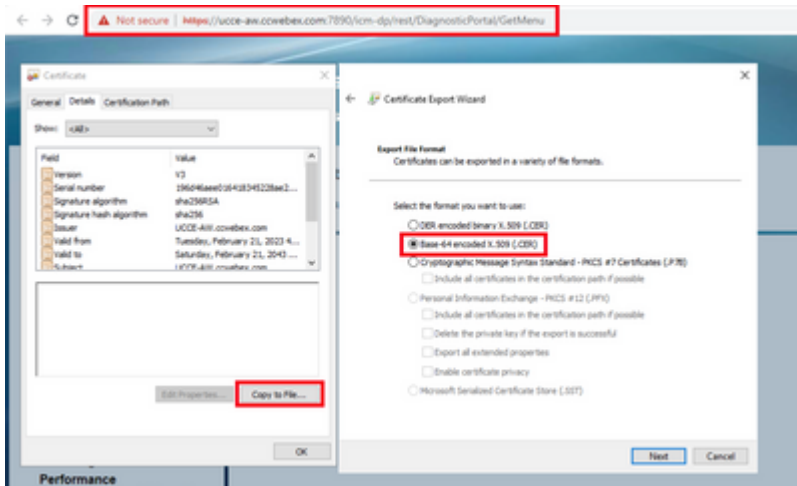


(ii) Speichern Sie das Zertifikat in einem temporären Ordner. Beispiel: c:\temp\certs und geben Sie dem Zertifikat den Namen ICM{svr}[ab].cer.

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

Schritt 2: Exportieren Sie DFP-Zertifikate (Diagnostic Framework Portal) von Router\Logger und PG-Servern.

(i) Öffnen Sie auf einem AW-Server einen Browser, und navigieren Sie zu den Servern (Router, Logger oder 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

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

Schritt 3: IIS- und DFP-Zertifikat von Rogger, PG auf AW-Server importieren.

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

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

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

Befehl zum Importieren der selbstsignierten DFP-Zertifikate in AW-Server:

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

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

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

Schritt 4: IIS-Zertifikat von AW-Servern in Router\Logger importieren

Befehl zum Importieren der selbstsignierten IIS-Zertifikate in Rogger-Server:

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

Hinweis: Importieren Sie alle AW IIS-Serverzertifikate, die in die Roger A- und B-Seiten exportiert wurden.

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

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

Um diesen Austausch erfolgreich abzuschließen, sind folgende Schritte erforderlich:

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

Schritt 2: Importieren von Zertifikaten der VOS-Plattformanwendung in einen AW-Server.

Dieser Prozess gilt für VOS-Anwendungen wie:

- Finesse
- CUIC \ LD \ IDS
- Cloud Connect

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

(i) Navigieren Sie zur Seite "Cisco Unified Communications Operating System Administration" (Cisco Unified Communications-Betriebssystemverwaltung): <https://FQDN:8443/cmplatform>.

(ii) Navigieren Sie zu **Security > Certificate Management**, und suchen Sie im Ordner tomcat-trust nach den Zertifikaten des primären Anwendungsservers.

tomcat-trust	Class_BCC_Root_CA	Self-signed	EC	Class_BCC_Root_CA	Class_BCC_Root_CA
tomcat-trust	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Self-signed	RSA	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Hellenic_Academic_and_Research_Institutions
tomcat-trust	OSITE_WISetax_Global_Root_GB_CA	Self-signed	RSA	OSITE_WISetax_Global_Root_GB_CA	OSITE_WISetax_Global_Root_GB_CA
tomcat-trust	Amazon_Root_CA_4	Self-signed	EC	Amazon_Root_CA_4	Amazon_Root_CA_4
tomcat-trust	DST_Root_CA_X3	Self-signed	RSA	DST_Root_CA_X3	DST_Root_CA_X3
tomcat-trust	AddTrust_External_CA_Root	Self-signed	RSA	AddTrust_External_CA_Root	AddTrust_External_CA_Root
tomcat-trust	ccp.bora.com	Self-signed	RSA	ccp.bora.com	ccp.bora.com
tomcat-trust	T-Trustee_GlobalRoot_Class_3	Self-signed	RSA	T-Trustee_GlobalRoot_Class_3	T-Trustee_GlobalRoot_Class_3
tomcat-trust	DigCert_Global_Root_G2	Self-signed	RSA	DigCert_Global_Root_G2	DigCert_Global_Root_G2

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

Certificate Settings

File Name	ccp.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly name)	Trust Certificate

Certificate File Data

```
[
  Version: V3
  Serial Number: 5C35B3A89A8974719BB85B6A92CF710D
  SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
  Issuer Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
  Validity From: Mon Dec 16 10:55:22 EST 2019
  To: Sat Dec 14 10:55:21 EST 2024
  Subject Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
  3082010a0282010100c1420ced76c23b9d6b01efbf331987ac5624639ba8af3f3430d2ca8766d199
  69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54bfd3e71f27900d992
  88e0e816e64ad44c39f03f62aadcb08f591a960ef95eda7b86b3e6e183a2fe8732352ae6abcfb722
  f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
  520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
]
```

Buttons: Delete, **Download .PEM File**, Download .DER File

Hinweis: Führen Sie die gleichen Schritte für den Abonnenten durch.

Schritt 2: VOS-Plattformanwendung in AW-Server importieren

Pfad zum Ausführen des Schlüssel-Tools: C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

Befehl zum Importieren der selbstsignierten Zertifikate:

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

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

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

CVP OAMP-Server und CVP-Komponentenserver

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

(i) CVP OAMP-Server: Dieser Server benötigt ein Zertifikat von

- Windows-Plattform: WSM-Zertifikat (Web Services Manager) des CVP-Servers und der Reporting-Server.
- VOS-Plattform: Cisco VB und Cloud Connect-Server.

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

- Windows-Plattform: WSM-Zertifikat vom OAMP-Server.
- VOS-Plattform: Cloud Connect-Server und Cisco VB-Server für die sichere SIP- und HTTP-Kommunikation.

(iii) CVP-Reporting-Server: Für diesen Server ist ein Zertifikat von

- Windows-Plattform: WSM-Zertifikat vom OAMP-Server.

(iv) Cisco VVB-Server: Für diesen Server ist ein Zertifikat von

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

In diesen drei Abschnitten werden die Schritte erläutert, die für einen effektiven Austausch der selbstsignierten Zertifikate in der CVP-Umgebung erforderlich sind.

Abschnitt 1: Zertifikataustausch zwischen CVP OAMP-Server und CVP-Server und Reporting-Server

Abschnitt 2: Zertifikataustausch zwischen CVP OAMP-Server- und VOS-Plattformanwendungen

Abschnitt 3: Zertifikataustausch zwischen CVP-Server- und VOS-Plattformanwendungen

Abschnitt 1: Zertifikataustausch zwischen CVP OAMP-Server und CVP-Server und Reporting-

Server

Um diesen Austausch erfolgreich abzuschließen, sind folgende Schritte erforderlich:

Schritt 1: WSM-Zertifikat vom CVP-Server, Reporting- und OAMP-Server exportieren.

Schritt 2: Importieren Sie WSM-Zertifikate vom CVP-Server und vom Reporting-Server in den OAMP-Server.

Schritt 3: CVP OAMP-Server-WSM-Zertifikat in CVP-Server und Reporting-Server importieren.

Vorsicht: Bevor Sie beginnen, müssen Sie dies tun:

1. Öffnen Sie ein Befehlsfenster als Administrator.
 2. Für 12.6.2 rufen Sie zur Identifizierung des Keystore-Kennworts den Ordner %CVP_HOME%\bin auf, und führen Sie die Datei DecryptKeystoreUtil.bat aus.
 3. Für 12.6.1 führen Sie den Befehl, um das Schlüsselspeicherkennwort zu identifizieren, mehr %CVP_HOME%\conf\security.properties aus.
 4. Sie benötigen dieses Kennwort, wenn Sie die Befehle keytool ausführen.
 5. Führen Sie im Verzeichnis %CVP_HOME%\conf\security\ den Befehl copy .keystore backup.keystore aus.
-

Schritt 1: WSM-Zertifikat vom CVP-Server, Reporting- und OAMP-Server exportieren.

(i) Exportieren Sie das WSM-Zertifikat von jedem CVP-Server an einen temporären Speicherort, und benennen Sie das Zertifikat um den gewünschten Namen. Sie können sie in wsmX.crt umbenennen. Ersetzen Sie X durch den Hostnamen des Servers. Beispiel: wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.crt.

Befehl zum Exportieren der selbstsignierten Zertifikate:

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

(ii) Kopieren Sie das Zertifikat aus dem Pfad %CVP_HOME%\conf\security\wsm.crt von jedem Server, und benennen Sie es je nach Servertyp in wsmX.crt um.

Schritt 2: Importieren von WSM-Zertifikaten vom CVP-Server und Reporting-Server in den OAMP-Server.

(i) Kopieren Sie alle CVP-Server- und Reporting-Server-WSM-Zertifikate (wsmX.crt) in das Verzeichnis %CVP_HOME%\conf\security auf dem OAMP-Server.

ii) diese Zertifikate mit dem folgenden Befehl importieren:

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

(iii) Neustart des Servers.

Schritt 3: CVP OAMP-Server-WSM-Zertifikat in CVP-Server und Reporting-Server importieren.

(i) Kopieren Sie das WSM-Zertifikat des OAMP-Servers (wsmoampX.crt) in das Verzeichnis

%CVP_HOME%\conf\security auf allen CVP-Servern und Reporting-Servern.

ii) Importieren Sie die Zertifikate mit dem folgenden Befehl:

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

(iii) Starten Sie die Server neu.

Abschnitt 2: Zertifikataustausch zwischen CVP OAMP-Server- und VOS-Plattformanwendungen

Um diesen Austausch erfolgreich abzuschließen, sind folgende Schritte erforderlich:

Schritt 1: Exportieren des Anwendungszertifikats von der VOS-Plattform

Schritt 2: Import des VOS-Anwendungszertifikats in den OAMP-Server

Dieser Prozess gilt für VOS-Anwendungen wie:

- CUCM
- VVB
- Cloud Connect

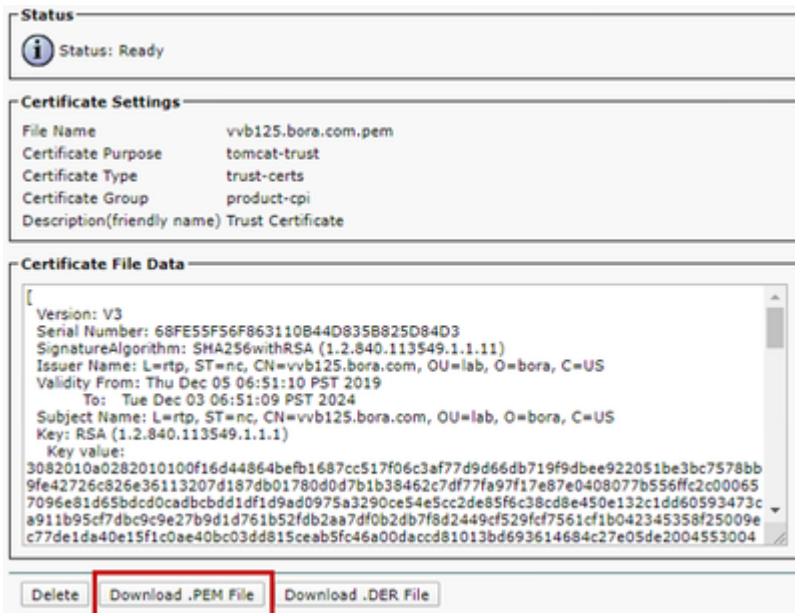
Schritt 1: Exportieren des Anwendungszertifikats von der VOS-Plattform

(i) Navigieren Sie zur Seite "Cisco Unified Communications Operating System Administration" (Cisco Unified Communications-Betriebssystemverwaltung): <https://FQDN:8443/cmplatform>.

(ii) Navigieren Sie zu **Security > Certificate Management**, und suchen Sie im Ordner tomcat-trust nach den Zertifikaten des primären Anwendungsservers.

tomcat-trust	thrust_primary_root_CA_..._03	self-signed	RSA	thrust_primary_root_CA_..._03	thrust_primary_root_CA_..._03
tomcat-trust	GlobalSign	self-signed	EC	GlobalSign	GlobalSign
tomcat-trust	EE_Certification_Centre_Root_CA	self-signed	RSA	EE_Certification_Centre_Root_CA	EE_Certification_Centre_Root_CA
tomcat-trust	GlobalSign_Root_CA	self-signed	RSA	GlobalSign_Root_CA	GlobalSign_Root_CA
tomcat-trust	Trustix_Root_Certification_Authority	self-signed	RSA	Trustix_Root_Certification_Authority	Trustix_Root_Certification_Authority
tomcat-trust	Business_Class_3_Root_CA	self-signed	RSA	Business_Class_3_Root_CA	Business_Class_3_Root_CA
tomcat-trust	Starfield_Services_Root_Certificate_Authority_..._02	self-signed	RSA	Starfield_Services_Root_Certificate_Authority_..._02	Starfield_Services_Root_Certificate_Authority_..._02
tomcat-trust	VeriSign_Class_3_Public_Primary_Certification_Authority_...	self-signed	RSA	VeriSign_Class_3_Public_Primary_Certification_Authority_...	VeriSign_Class_3_Public_Primary_Certification_Authority_...
tomcat-trust	jboss.com	self-signed	RSA	jboss.com	jboss.com
tomcat-trust	ikang_global_certification_Authority	self-signed	RSA	ikang_global_certification_Authority	ikang_global_certification_Authority

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



Schritt 2: Import des VOS-Anwendungszertifikats in den OAMP-Server

(i) Kopieren Sie das VOS-Zertifikat in das Verzeichnis %CVP_HOME%\conf\security auf dem OAMP-Server.

ii) Importieren Sie die Zertifikate mit dem folgenden Befehl:

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

(ii) Starten Sie den Server neu.

Abschnitt 3: Zertifikataustausch zwischen CVP-Server- und VOS-Plattformanwendungen

Dies ist ein optionaler Schritt zum Sichern der SIP-Kommunikation zwischen CVP und anderen Contact Center-Komponenten. Weitere Informationen finden Sie im CVP-Konfigurationsleitfaden: [CVP-Konfigurationsleitfaden - Sicherheit](#).

CVP CallStudio-Webdienstintegration

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](#)
- Selbstsignierte PCCE-Zertifikate 12.6: [Austausch selbstsignierter PCCE-Zertifikate](#)
- Selbstsignierte PCCE-Zertifikate 12.5: [Selbstsigniertes PCCE-Zertifikat 12.5](#)

- UCCE-selbstsigniertes Zertifikat 12.5: [UCCE-selbstsignierte Zertifikate 12.5](#)
- CCE CA Signed Certificates 12.5: [CCE CA Signed Certificates 12.5](#)
- **[Technischer Support und Dokumentation für Cisco Systeme](#)**

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.