

Tauschen Sie selbstsignierte Zertifikate in einer UCCE-Lösung aus.

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrund](#)

[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-Servern.](#)

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

[Abschnitt 3: Zertifikataustausch zwischen CVP-Server und CVVB-Servern.](#)

[CVP CallStudio-WEBService-Integration](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt den Austausch selbstsignierter Zertifikate in der Unified Contact Center Enterprise (UCCE)-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:

- UCCE-Version 12.5(1)
- Customer Voice Portal (CVP) Version 12.5 (1)
- Cisco Virtualized Voice Browser (VVB)

Verwendete Komponenten

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

- UCCE 12.5(1)

- CVP 12.5(1)
- Cisco VVB 12,5
- 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 verstehen.

Hintergrund

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

Um eine nahtlose sichere Kommunikation zwischen diesen Anwendungen in einer selbstsignierten Zertifikatsumgebung zu erreichen, wird der Austausch dieser Zertifikate zwischen den Servern zum Muss. Im nächsten Abschnitt werden die Schritte für den Austausch eines selbstsignierten Zertifikats zwischen den folgenden Elementen ausführlich erläutert:

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

Vorgehensweise

CCE AW-Server und CCE Core-Anwendungsserver

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

CCE AW-Server: Für diesen Server ist ein Zertifikat von erforderlich:

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

Anmerkung: IIS- und Diagnostic-Framework-Zertifikate werden benötigt.

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

Gleiches gilt für andere AW-Server in der Lösung.

Router \ Logger-Server: Für diesen Server ist ein Zertifikat von erforderlich:

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

Die Schritte für den effektiven Austausch der selbstsignierten Zertifikate für 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, müssen folgende Schritte ausgeführt werden:

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

Schritt 2: Exportieren von DFP-Zertifikaten (Diagnostic Framework Portico) von Router\Logger- und PG-Servern.

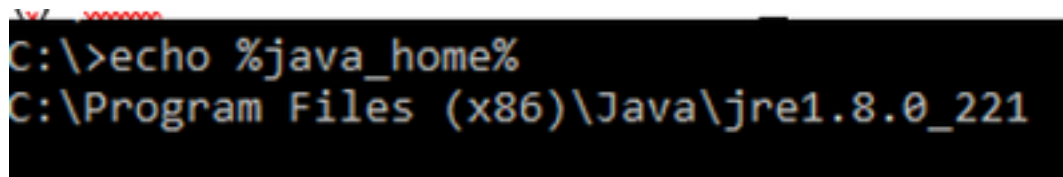
Schritt 3: Importieren Sie IIS- und DFP-Zertifikate von Router\Logger, PG auf AW-Server.

Schritt 4: Importieren Sie das IIS-Zertifikat von den AW-Servern in Router\Logger.

Vorsicht: Bevor Sie beginnen, müssen Sie den Keystore sichern und die Befehle von der Java-Startseite aus als Administrator ausführen.

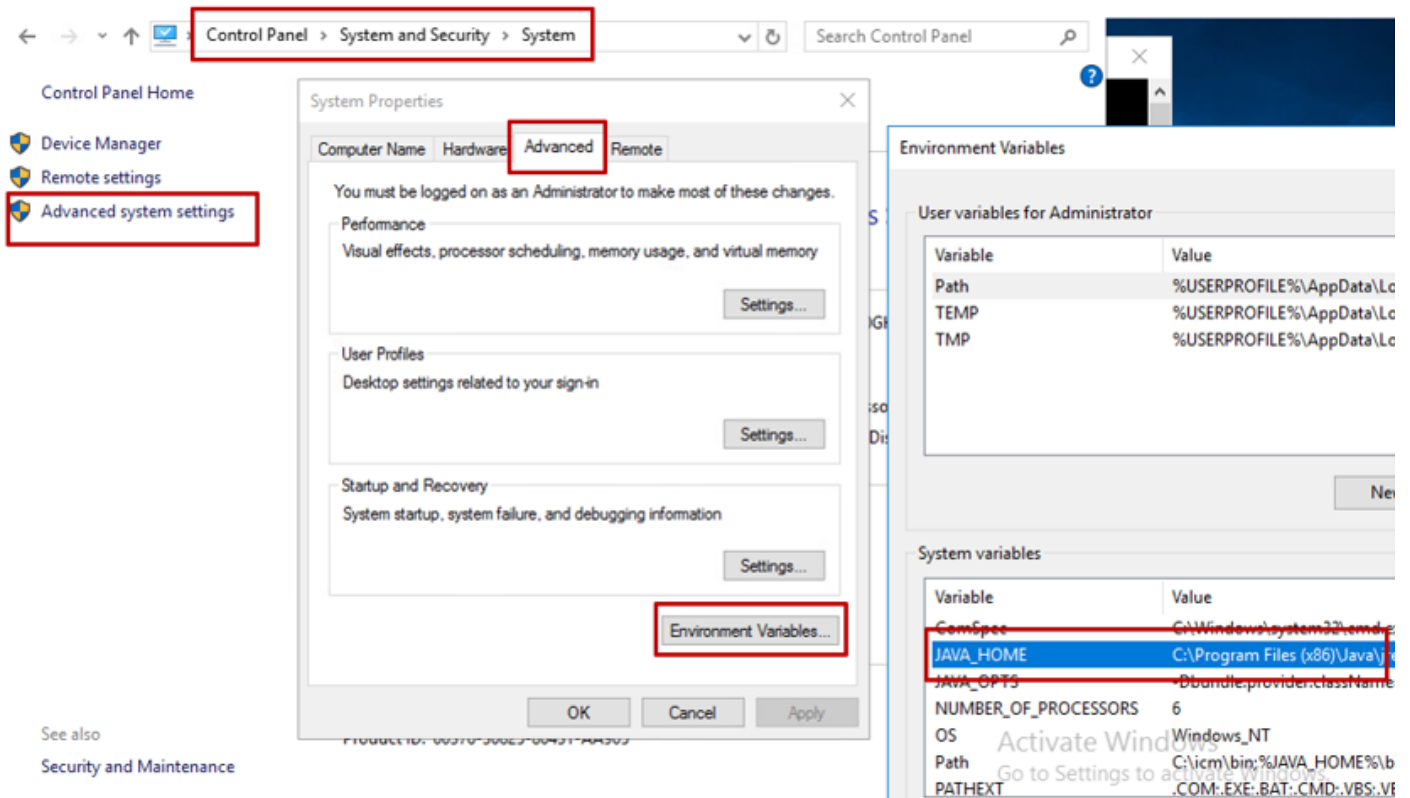
(i) Kennen Sie den Java-Home-Pfad, um sicherzustellen, wo das Java-Schlüsselprogramm gehostet wird. Es gibt mehrere Möglichkeiten, den Java-Heim-Pfad zu finden.

Option 1: CLI-Befehl: `echo %JAVA_HOME%`



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

Option 2: Manuell über die Systemeinstellung "Erweitert", wie im Bild gezeigt



Anmerkung: Auf UCCE 12.5 lautet der Standardpfad C:\Program Dateien (x86)\Java\jre1.8.0_221\bin. Wenn Sie jedoch den 12.5(1a) Installer verwendet haben oder 12.5 ES55 installiert haben (obligatorisches OpenJDK ES), dann verwenden Sie CCE_JAVA_HOME anstelle von JAVA_HOME, da sich der Datenspeicherpfad mit OpenJDK geändert hat. Weitere Informationen zur OpenJDK-Migration in CCE und CVP finden Sie in diesen Dokumenten: [Installation und Migration zu OpenJDK in CCE 2.5\(1\)](#) und [Installation und Migration zu OpenJDK in CVP 12.5\(1\)](#).

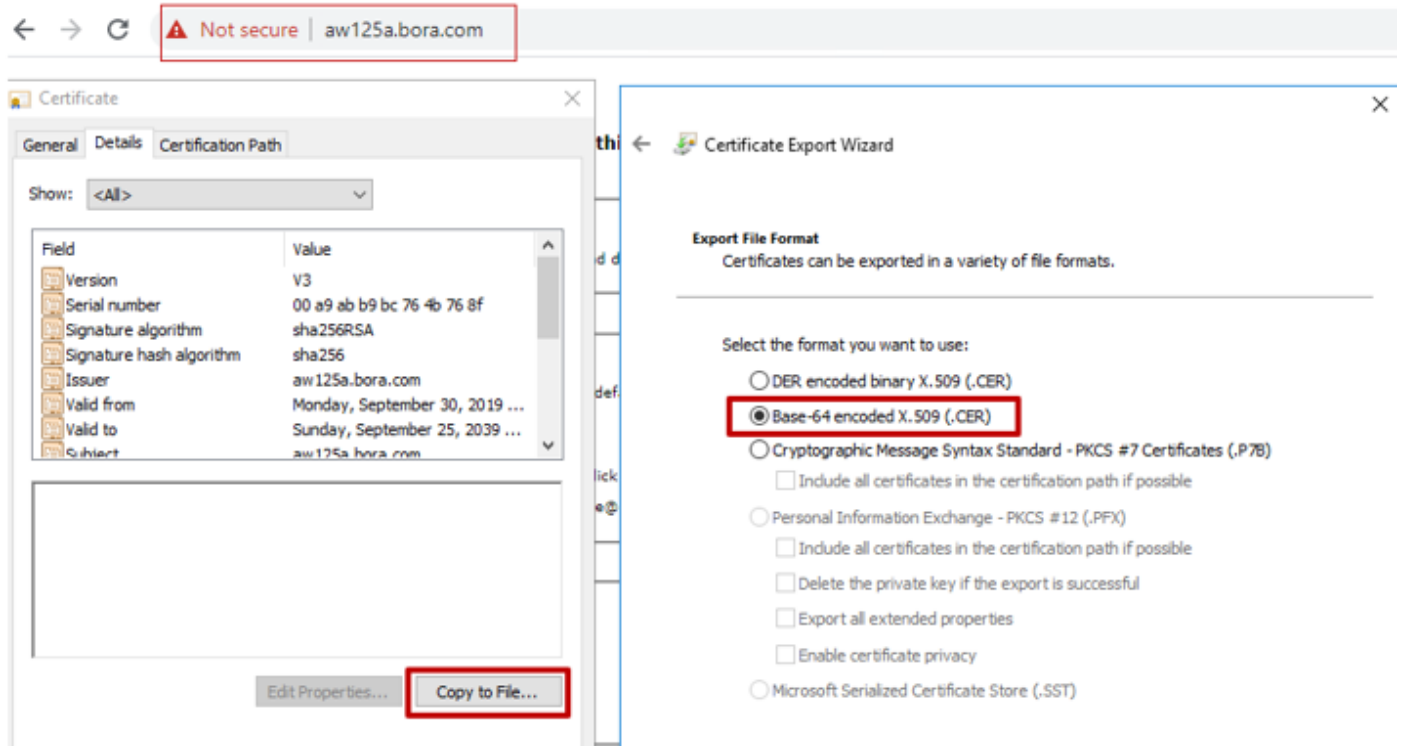
(ii) Sichern Sie die Aktwaredatei aus dem Ordner **C:\Program Dateien (x86)\Java\jre1.8.0_221\lib\security**. Sie können es an einen anderen Speicherort kopieren.

(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 dem AW-Server von einem Browser zu den Servern (Roggers , PG , andere AW-Server) url: **https://{servername}**.

CCE via Chrome Browser



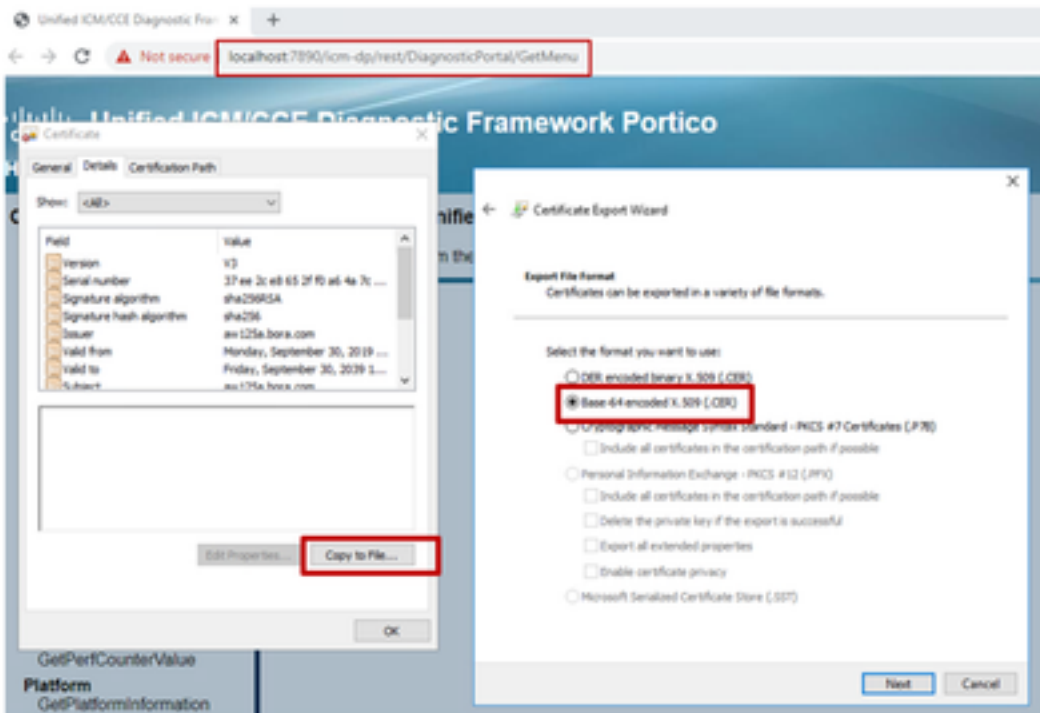
(ii) Speichern Sie das Zertifikat in einem temporären Ordner, z. B. c:\temp\certs, und nennen Sie das Zertifikat als ICM{svr}[ab].cer.

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

Schritt 2: Exportieren von DFP-Zertifikaten (Diagnostic Framework Portico) von Router\Logger- und PG-Servern.

(i) Öffnen Sie auf dem 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**.

Portico via Chrome Browser



(ii) Speichern Sie das Zertifikat im Ordner "Beispiel c:\temp\certs" und nennen Sie das Zertifikat als dfp{svr}[ab].cer.

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

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

Befehl zum Importieren der selbstsignierten IIS-Zertifikate in den AW-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
```

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

Befehl zum Importieren der selbstsignierten DFP-Zertifikate in AW-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 AW-Server exportierten Serverzertifikate.

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

Schritt 4: Importieren Sie das IIS-Zertifikat von den AW-Servern in Router\Logger.

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

```
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
```

Anmerkung: Importieren Sie alle AW IIS-Serverzertifikate, die in Rogger-A- und -B-Seiten exportiert werden.

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, müssen folgende Schritte ausgeführt werden:

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

Schritt 2: Importieren von VOS-Plattform-Anwendungszertifikaten in einen AW-Server.

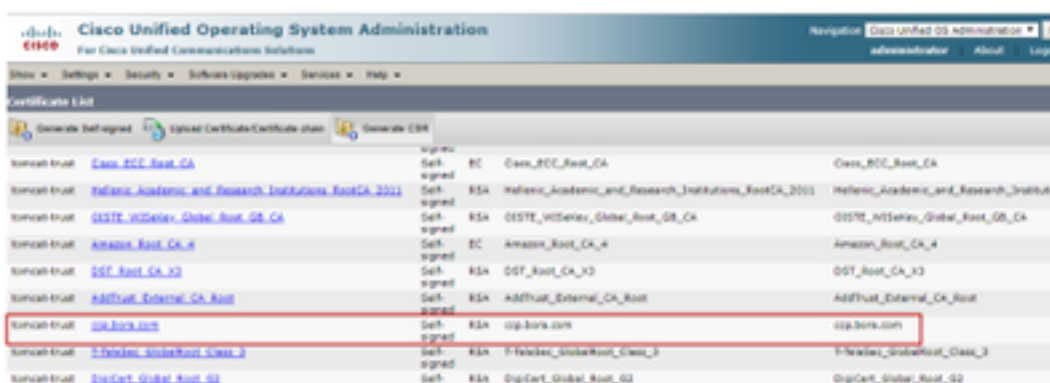
Dieser Prozess gilt für alle VOS-Anwendungen, z. B.:

- CUCM
- 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.



tomcat-trust	Self-Signed	Self-Signed	Self-Signed	Self-Signed
Class_BCC_Root_CA	Self-Signed	EC	Class_BCC_Root_CA	Class_BCC_Root_CA
Hellenic_Academic_and_Research_Institutions_RootCA_2011	Self-Signed	RSA	Hellenic_Academic_and_Research_Institutions_RootCA_2011	Hellenic_Academic_and_Research_Institutions
OSTE_WISEKey_Global_Root_GB_CA	Self-Signed	EC	OSTE_WISEKey_Global_Root_GB_CA	OSTE_WISEKey_Global_Root_GB_CA
Amazon_Root_CA_4	Self-Signed	EC	Amazon_Root_CA_4	Amazon_Root_CA_4
DST_Root_CA_33	Self-Signed	EC	DST_Root_CA_33	DST_Root_CA_33
ADTrust_External_CA_Root	Self-Signed	EC	ADTrust_External_CA_Root	ADTrust_External_CA_Root
sip.sip.com	Self-Signed	EC	sip.sip.com	sip.sip.com
T-TeleSec_GlobalRoot_Class_3	Self-Signed	EC	T-TeleSec_GlobalRoot_Class_3	T-TeleSec_GlobalRoot_Class_3
DigCert_Global_Root_G2	Self-Signed	EC	DigCert_Global_Root_G2	DigCert_Global_Root_G2

(iii) Wählen Sie das Zertifikat aus, und klicken Sie auf .PEM-Datei herunterladen, 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: 5C35B3A89A8974719BB8586A92CF710D	
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:	
3082010a0282010100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199	
69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992	
88e0e816e64ad44c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722	
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f	
520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a	

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

Schritt 2: Importieren der VOS-Plattformanwendung in den AW-Server

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.pem
```

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

Anmerkung: 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 die Komponenten, in die selbstsignierte Zertifikate importiert werden müssen.

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

- Windows-Plattform: Web Services Manager (WSM)-Zertifikat von CVP-Server und Reporting-Servern.
- VOS-Plattform: Integration von Cisco VB für Customer Virtual Agent (CVA), Cloud Connect-Server für die Integration von WebEx Experience Management (WXM).

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

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

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

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

(iv) Cisco VVB-Server: Dieser Server benötigt ein Zertifikat von

- Windows-Plattform: CVP-Server VXML (sicheres HTTP), CVP-Server-Callserver (sicheres SIP)

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

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

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

Abschnitt 3: Zertifikataustausch zwischen CVP-Server und VVB-Servern.

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

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

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

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

Schritt 3: Importieren des CVP OAMP-Server-WSM-Zertifikats in CVP-Server und Reporting-Server.

Vorsicht: Bevor Sie beginnen, müssen Sie Folgendes tun:

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

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 mit einem gewünschten Namen um. Sie können es als wsmX.crt umbenennen. Ersetzen Sie X durch eine eindeutige Nummer oder einen Buchstaben. 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 -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

(ii) Kopieren Sie das Zertifikat aus dem Pfad **C:\Cisco\CVP\conf\security\wsm.crt** von jedem Server und benennen Sie es je nach Servertyp als 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 C:\Cisco\CVP\conf\security auf dem OAMP-Server.

(ii) Importieren Sie diese Zertifikate mit folgendem Befehl:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmcsX.crt
```

(iii) Starten Sie den Server neu.

Schritt 3: Importieren des CVP OAMP-Server-WSM-Zertifikats in CVP-Server und Reporting-Server.

(i) Kopieren Sie das OAMP-Server-WSM-Zertifikat (wsmoampX.crt) in das Verzeichnis C:\Cisco\CVP\conf\security auf allen CVP-Servern und Reporting-Servern.

ii) Importieren Sie die Zertifikate mit dem Befehl:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmoampX.crt
```

(iii) Starten Sie die Server neu.

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

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

Schritt 1: Exportieren des Anwendungszertifikats von der VOS-Plattform

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

Schritt 1: Exportieren des Anwendungszertifikats von 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.

- Schritt 1: Exportieren Sie das CVVB-Anwendungszertifikat von der VOS-Plattform.
 Schritt 2: Importieren Sie das vos-Anwendungszertifikat in die CVP-Server.
 Schritt 3: Exportieren des Anrufservers und des VXML-Zertifikats von den CVP-Servern.
 Schritt 4: Importieren von Anrufserver- und VXML-Zertifikaten in CVVB-Server.

Schritt 1: Exportieren Sie das Anwendungszertifikat von der vos-Plattform.

(i) Befolgen Sie für CVVB-Server die gleichen Heftklammern wie in Abschnitt 2 Schritt 1 angegeben.

Schritt 2: Importieren des VOS-Anwendungszertifikats in den CVP-Server

(i) Befolgen Sie auf allen CVP-Servern die gleichen Schritte wie in Schritt 2 von Abschnitt 2 beschrieben.

Schritt 3: Anrufserver und VXML-Zertifikat von CVP-Servern exportieren

(i) Exportieren von Anrufservern und VXML-Zertifikaten von jedem CVP-Server an einen temporären Speicherort und Umbenennen des Zertifikats mit einem gewünschten Namen. Sie können es als callserverX.crt \ vxmlX.crt Replace X durch eine eindeutige Zahl oder einen Buchstaben umbenennen.

Befehl zum Exportieren der selbstsignierten Zertifikate:

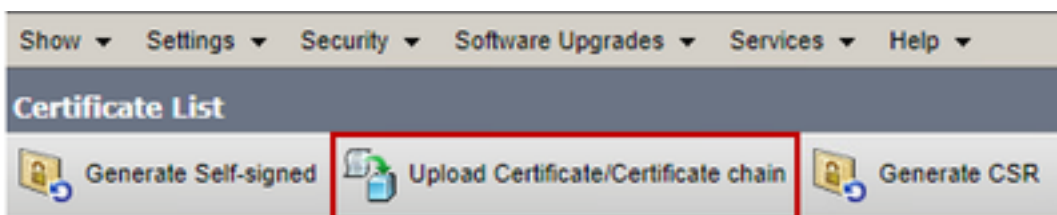
```
Callserver certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore
%CVP_HOME%\conf\security\keystore -export -alias callserver_certificate -file
%CVP_HOME%\conf\security\callserverX.crt
Vxml certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore
%CVP_HOME%\conf\security\keystore -export -alias vxml_certificate -file
%CVP_HOME%\conf\security\vxmlX.crt
```

(ii) Kopieren Sie das Zertifikat aus dem Pfad C:\Cisco\CVP\conf\security\wsm.crt von jedem Server und benennen Sie es basierend auf dem Zertifikatstyp als callserverX.crt \ vxmlX.crt um.

Schritt 4: Importieren von Anrufserver- und VXML-Zertifikaten in CVVB-Server.

(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 wählen Sie die Option Zertifikat/Zertifikatskette hochladen aus.



(iii) Wählen Sie auf dem Upload-Zertifikat/der Zertifikatskette "tomcat trust" im Zertifikatszweckfeld

aus, und laden Sie die exportierten Zertifikate gemäß Schritt 3 hoch.

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* tomcat-trust

Description(friendly name)

Upload File Choose File No file chosen

Upload Close

(iv) Starten Sie den Server neu.

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.](#)
- Selbstsignierte PCCE-Zertifikate: [Tauschen Sie selbstsignierte PCCE-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](#)

[Technischer Support und Dokumentation für Cisco Systeme](#)