Exchange Self-Signed Certificates in a UCCE Solution

Contents

Introduction

This document describes how to exchange self-signed certificates in the Unified Contact Center Enterprise (UCCE) solution.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software versions:

- UCCE 12.5 (1)
- CVP 12.5 (1)
- Cisco VVB 12.5
- CVP Operations Console (OAMP)
- CVP New OAMP (NOAMP)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

In a UCCE solution, the configuration of new features which involves core applications such as ROGGERs, Peripheral Gateways (PG), Admin Workstations (AW)/Administration Data Servers (ADS), Finesse, Cisco Unified Intelligence Center (CUIC), and so on, is done through the Contact Center Enterprise (CCE) Admin page. For Interactive Voice Response (IVR) applications like CVP, Cisco VVB, and gateways, NOAMP controls the configuration of new features. From CCE 12.5 (1), due to security-management-compliance (SRC), all communications to CCE Admin and NOAMP are strictly done via secure HTTP protocol.

In order to achieve seamless secure communication between these applications in a self-signed certificate environment, the exchange of certificates between the servers becomes a must. The next section explains in detail the steps needed to exchange self-signed certificates between:

- CCE AW Servers and CCE Core Application Servers
- CVP OAMP Server and CVP Component Servers

Procedure

CCE AW Servers and CCE Core Application Servers

These are the components from which self-signed certificates are exported and components into which self-signed certificates must be imported.

CCE AW Servers: This server requires a certificate from:

- Windows platform: Router and Logger (ROGGER) {A/B}, Peripheral Gateway (PG) {A/B}, and all AW/ADS.

Note: IIS and Diagnostic Framework Portico (DFP) certificates are needed.

- VOS Platform: Finesse, CUIC, Live Data (LD), Identity Server (IDS), Cloud Connect, and other applicable servers are part of the inventory database.

The same applies to other AW servers in the solution.

Router\Logger Server: This server requires a certificate from:

- Windows platform: IIS certificate of all AW servers.

The steps needed to exchange the self-signed certificates for CCE effectively are divided into these sections:

Section 1. Certificate Exchange Between Router\Logger, PG, and AW Server.
Section 2. Certificate Exchange Between VOS Platform Application and AW Server.

Section 1. Certificate Exchange Between Router\Logger, PG, and AW Server

The steps needed to complete this exchange successfully are:

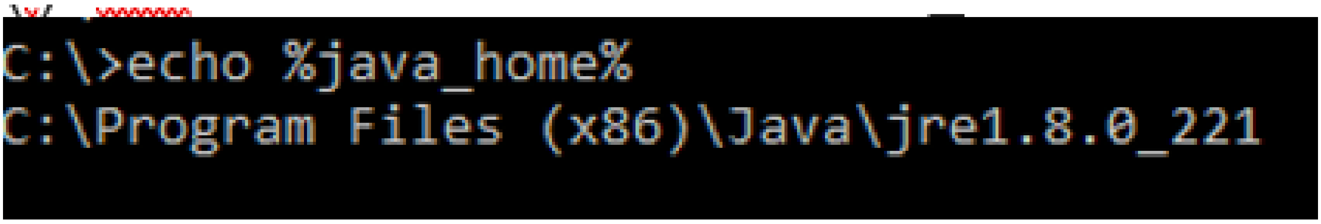
Step 1. Export IIS certificates from Router\Logger, PG, and all AW servers.

Step 2. Export DFP certificates from Router\Logger, PG, and all AW servers.
Step 3. Import IIS and DFP certificates from Router\Logger, PG, and AW to AW servers.
Step 4. Import IIS certificates to Router\Logger and PG from AW servers.

⚠ **Caution**: Before you begin, you must back up the keystore and open the command prompt as Administrator.

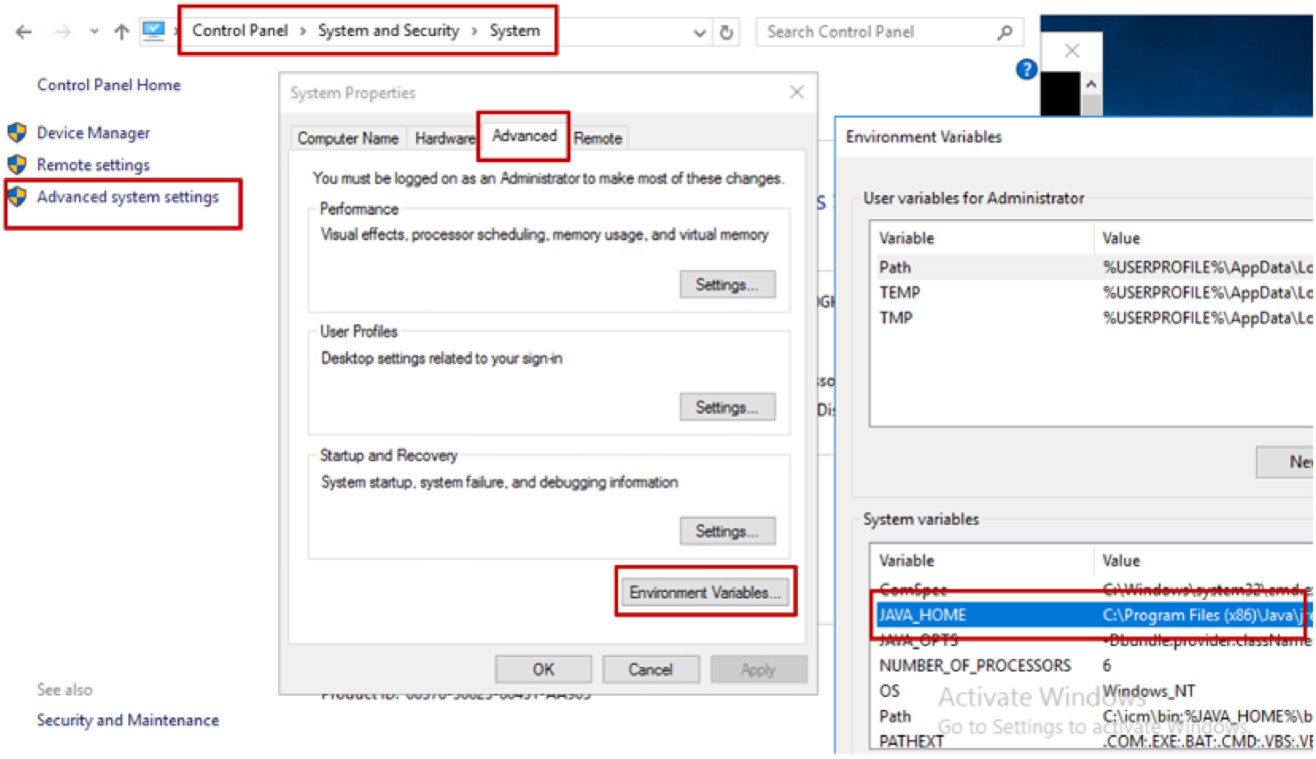
1. Know the Java home path in order to ensure where the Java keytool is hosted. There are a couple of ways you can find the Java home path.

   Option 1. CLI command: echo %JAVA_HOME%



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

   Option 2. Manually via the Advanced system setting, as shown in the image.



Control Panel › System and Security › System

You must be logged on as an Administrator to make most of these changes.

Performance
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles
Desktop settings related to your sign-in

Startup and Recovery
System startup, system failure, and debugging information

Environment Variables

User variables for Administrator

Variable	Value
Path	%USERPROFILE%\AppData\Lo
TEMP	%USERPROFILE%\AppData\Lo
TMP	%USERPROFILE%\AppData\Lo

System variables

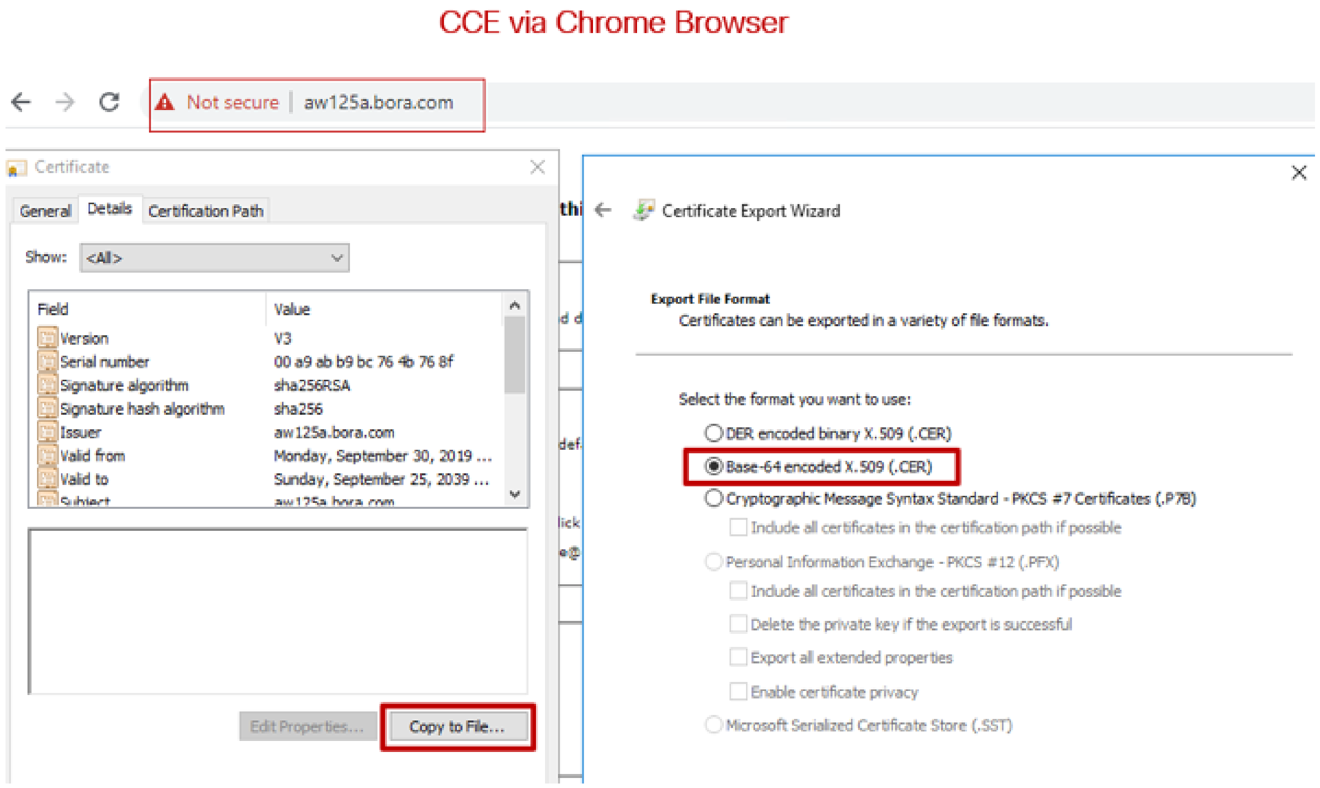
Variable	Value
ComSpec	C:\Windows\system32\cmd.e
JAVA_HOME	C:\Program Files (x86)\Java\j
JAVA_OPTS	-Dbundle.provider.className
NUMBER_OF_PROCESSORS	6
OS	Windows_NT
Path	C:\icm\bin;%JAVA_HOME%\b
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VE

   Note: On UCCE 12.5, the default path is C:\Program Files (x86)\Java\jre1.8.0_221\bin. However, if you have used the 12.5 (1a) installer or have 12.5 ES55 installed (mandatory OpenJDK ES), then use %CCE_JAVA_HOME% instead of %JAVA_HOME% since the datastore path has changed with OpenJDK. More information about OpenJDK migration in CCE and CVP can be found in these documents: [Install and Migrate to OpenJDK in CCE 12.5(1)]() and [Install and Migrate to OpenJDK in CVP 12.5(1)]().

2. Backup the cacerts file from the folder {JAVA_HOME}\lib\security. You can copy it to another location.

Step 1. Export IIS certificates from Router\Logger, PG, and all AW servers.

1. On the AW server from a browser, navigate to the servers (ROGGERs, PG, other AW servers) URL: https://{servername}.



CCE via Chrome Browser

Not secure | aw125a.bora.com

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	00 a9 ab b9 bc 76 4b 76 8f
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	aw125a.bora.com
Valid from	Monday, September 30, 2019 ...
Valid to	Sunday, September 25, 2039 ...
Subject	aw125a.bora.com

Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

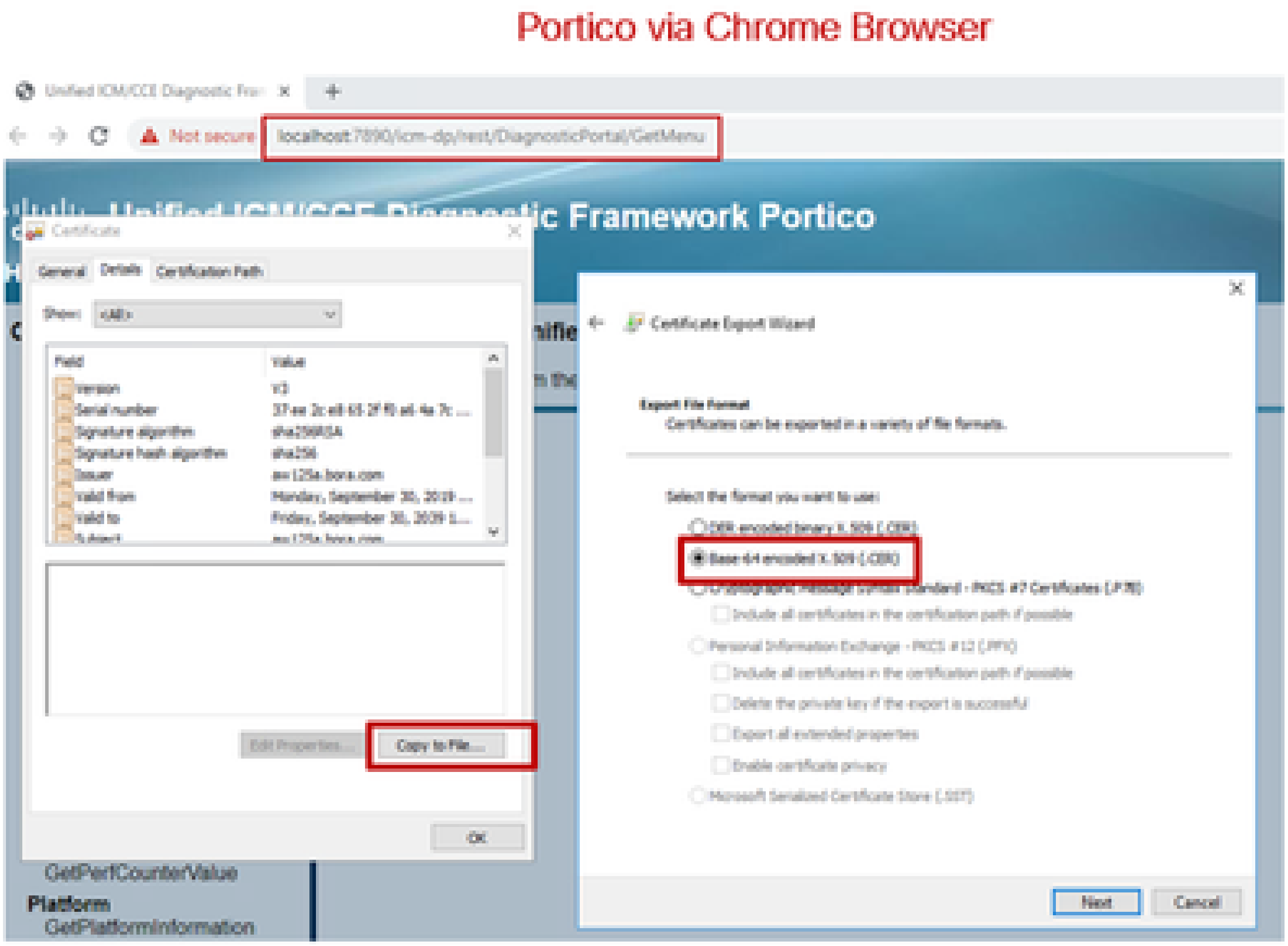
○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
□ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

2. Save the certificate to a temporary folder, for example, c:\temp\certs and name the cert as ICM{svr}[ab].cer.

Note: Choose the option Base-64 encoded X.509 (.CER).

Step 2. Export DFP certificates from Router\Logger, PG, and all AW servers.

1. On the AW server, open a browser, and navigate to the servers (Router, Logger or ROGGERs, PGs, AWs) DFP URL: https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion.



Portico via Chrome Browser

Unified ICM/CCE Diagnostic Fra

Not secure | localhost:7890/icm-dp/rest/DiagnosticPortal/GetMenu

Unified ICM/CCE Diagnostic Framework Portico

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	37 ee 2c e8 65 2f f0 a6 4a 7c ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	aw125a.bora.com
Valid from	Monday, September 30, 2019 ...
Valid to	Friday, September 30, 2039 1...
Subject	aw125a.bora.com

Edit Properties... | Copy to File...

OK

GetPerfCounterValue

Platform

GetPlatformInformation

Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

Next | Cancel

2. Save the certificate to the folder example c:\temp\certs and name the cert as dfp{svr}[ab].cer.

Note: Choose the option Base-64 encoded X.509 (.CER).

Step 3. Import IIS and DFP certificates from Router\Logger, PG, and AW to AW servers.

Note: The example commands use the default keystore password of changeit. You must change this if you have modified the password on your system.

Command to import the IIS self-signed certificates into the AW server. The path to run the keytool is: %JAVA_HOME%\bin.

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com
```

Note: Import all the server certificates exported into all AW servers.

Command to import the DFP self-signed certificates into AW servers:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_DFP -file
```

```
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com_
```

Note: Import all the server certificates exported into all AW servers.

Restart the Apache Tomcat service on the AW servers.

Step 4. Import IIS certificates to Router\Logger and PG from AW servers.

Command to import the AW IIS self-signed certificates into Router\Logger and PG servers:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myawa.domain.com_
```

Note: Import all the AW IIS server certificates exported into Router\Logger and PG servers on the A and B sides.

Restart the Apache Tomcat service on the Router\Logger and PG servers.

Section 2. Certificate Exchange Between VOS Platform Applications and AW Server

The steps needed to complete this exchange successfully are:

Step 1. Export VOS Platform Application Server Certificates.
Step 2. Import VOS Platform Application Certificates to AW Server.

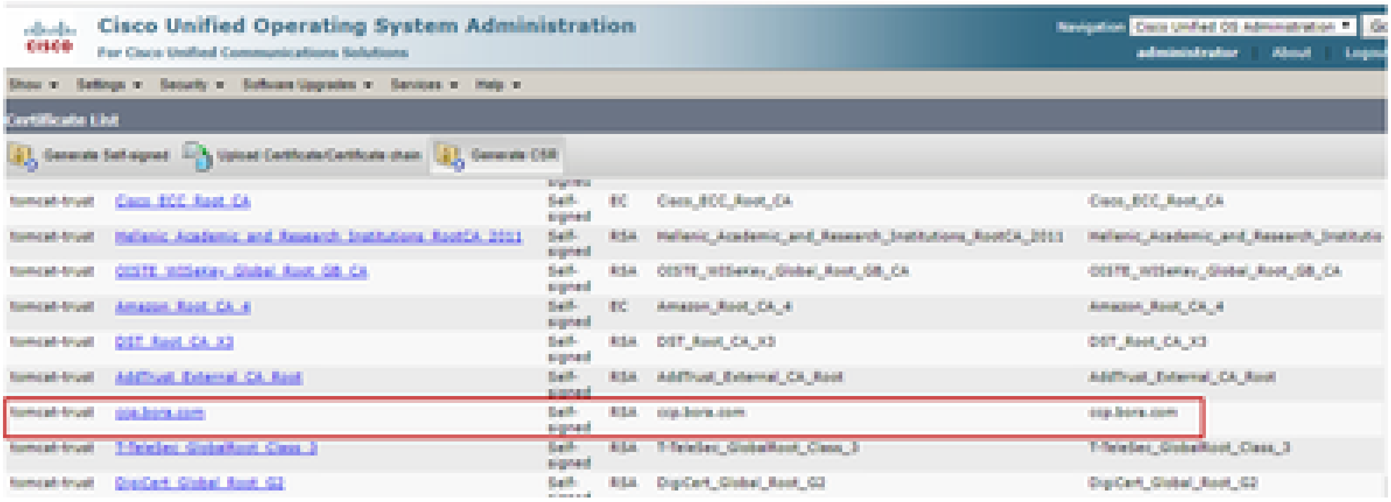
This process is applicable for all VOS applications such as:

- Finesse
- CUIC\LD\IDS
- Cloud Connect

Step 1. Export VOS Platform Application Server Certificates.

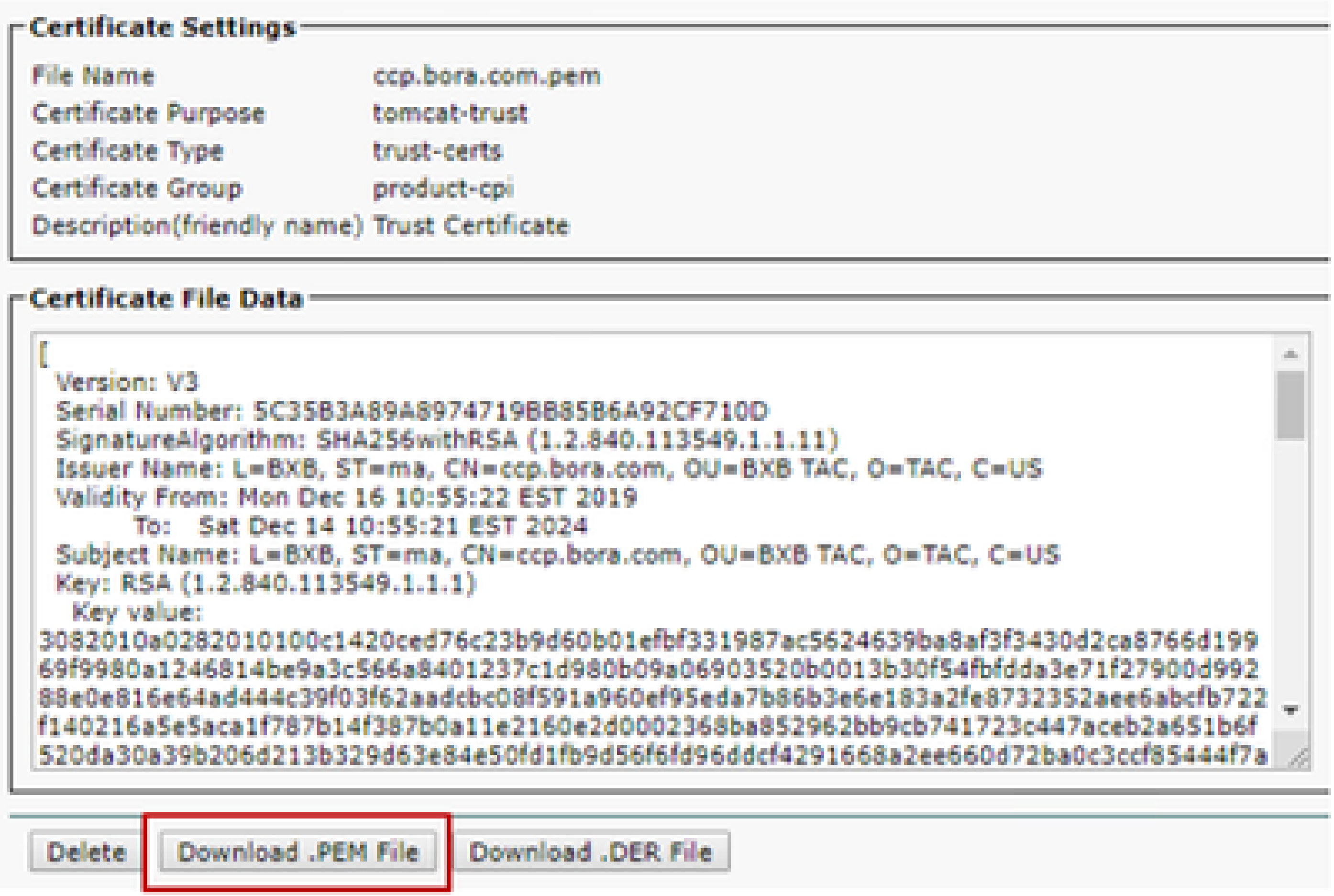
i. Navigate to the Cisco Unified Communications Operating System Administration page: **https://{FQDN}:8443/cmplatform.**

ii. Navigate to Security > Certificate Management and find the primary server certificates of the application in the tomcat-trust folder.


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration
administrator
About
Logout
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR

tomcat-trust	Cisco_ECC_Root_CA	Self-signed	EC	Cisco_ECC_Root_CA	Cisco_ECC_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_Institutio
tomcat-trust	OISTE_WISeKey_Global_Root_GB_CA	Self-signed	RSA	OISTE_WISeKey_Global_Root_GB_CA	OISTE_WISeKey_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-TeleSec_GlobalRoot_Class_3	Self-signed	RSA	T-TeleSec_GlobalRoot_Class_3	T-TeleSec_GlobalRoot_Class_3
tomcat-trust	DigiCert_Global_Root_G2	Self-signed	RSA	DigiCert_Global_Root_G2	DigiCert_Global_Root_G2

iii. Choose the certificate and click Download .PEM File in order to save it in a temporary folder on the AW server.



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: 5C35B3A89A89747198B85B6A92CF710D
 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
88e0e816e64ad444c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
```

Note: Perform the same steps for the subscriber.

Step 2. Import VOS Platform Application to AW Server.

Path to run the Key tool: {JAVA_HOME}\bin

Command to import the self-signed certificates:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_vos} -file c:\tem
```

Restart the Apache Tomcat service on the AW servers.

Note: Perform the same task on other AW servers.

CVP OAMP Server and CVP Component Servers

These are the components from which self-signed certificates are exported and components into which self-signed certificates must be imported.

i. CVP OAMP server: This server requires a certificate from:

- Windows platform: Web Services Manager (WSM) certificate from CVP server and Reporting servers.
- VOS Platform: Cisco VVB for Customer Virtual Agent (CVA) integration, Cloud Connect server for Webex Experience Management (WXM) Integration.

ii. CVP Servers: This server requires a certificate from:

- Windows platform: WSM certificate from OAMP server.
- VOS Platform: Cloud Connect server for WXM Integration and Cisco VVB server.

iii. CVP Reporting servers: This server requires a certificate from:

- Windows platform: WSM certificate from OAMP server.

iv. Cisco VVB servers: This server requires a certificate from:

- Windows platform: VXML certificate from CVP server and Callserver certificate from CVP server.

The steps required to effectively exchange the self-signed certificates in the CVP environment are explained in these three sections.

Section 1. Certificate Exchange Between CVP OAMP Server and CVP Server and Reporting Servers.
Section 2. Certificate Exchange Between CVP OAMP Server and VOS Platform Applications.
Section 3. Certificate Exchange Between CVP Server and VVB Servers.

Section 1. Certificate Exchange Between CVP OAMP Server and CVP Server and Reporting Servers

The steps required to complete this exchange successfully are:

Step 1. Export the WSM certificate from the CVP server, Reporting server, and OAMP server.
Step 2. Import WSM certificates from the CVP server and Reporting server into the OAMP server.
Step 3. Import the CVP OAMP server WSM certificate into the CVP server and Reporting server.

Caution: Before you begin, you must accomplish this:
1. Open a command window as administrator.
2. In order to identify the keystore password, run the command, more %CVP_HOME%\conf\security.properties.
3. You need this password when running the keytool commands.
4. From the %CVP_HOME%\conf\security\ directory, run the command, copy **.keystore backup.keystore**.

Step 1. Export the WSM certificate from the CVP server, Reporting server, and OAMP server.

i. Export the WSM certificate from each server to a temporary location, and rename the certificate with a desired name. You can rename it as wsmX.crt. Replace X with the hostname of the server. For example, wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.crt.

Command to export the self-signed certificates:

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

ii. Copy the certificate from the path C:\Cisco\CVP\conf\security\wsm.crt from each server and rename it as wsmX.crt based on the server type.

Step 2. Import the WSM certificates from the CVP servers and Reporting servers into the OAMP server.

i. Copy the WSM certificate from each CVP server and Reporting server (wsmX.crt) to the %CVP_HOME%\conf\security directory on the OAMP server.

ii. Import these certificates with the command:

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

iii. Reboot the server.

Step 3. Import the WSM certificate from the CVP OAMP server into CVP servers and Reporting servers.

i. Copy the OAMP server WSM certificate (wsmoampX.crt) to the %CVP_HOME%\conf\security directory on all the CVP servers and Reporting servers.

ii. Import the certificates with the command:

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

iii. Reboot the servers.

Section 2. Certificate Exchange Between CVP OAMP Server and VOS Platform Applications

The steps required to complete this exchange successfully are:

Step 1. Export the application certificate from the VOS platform.

Step 2. Import the VOS application certificate into the OAMP server.

This process is applicable for VOS applications such as:

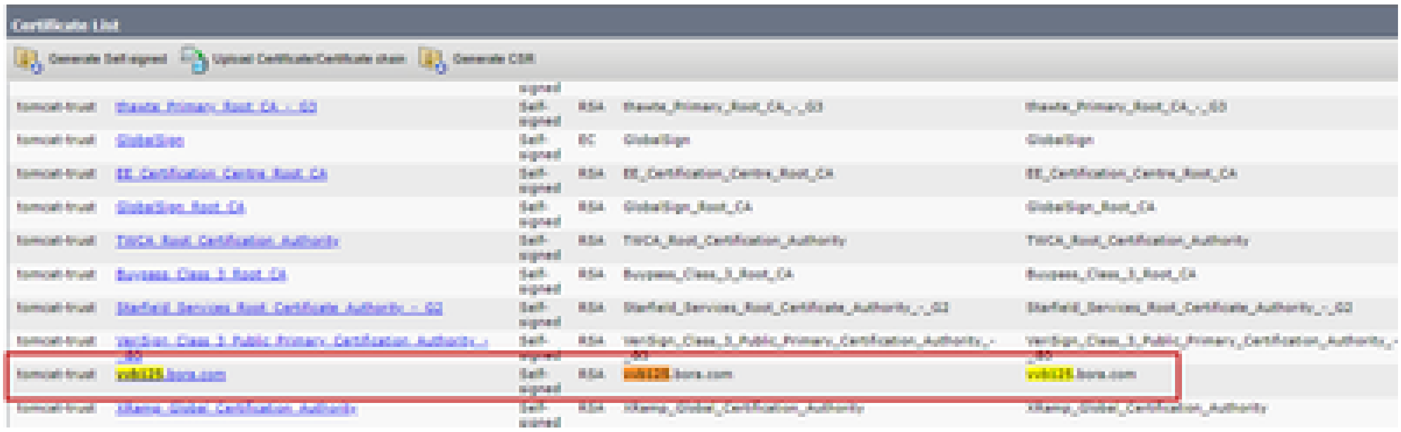
- CUCM

- VVB
- Cloud Connect

Step 1. Export the application certificate from the VOS platform.

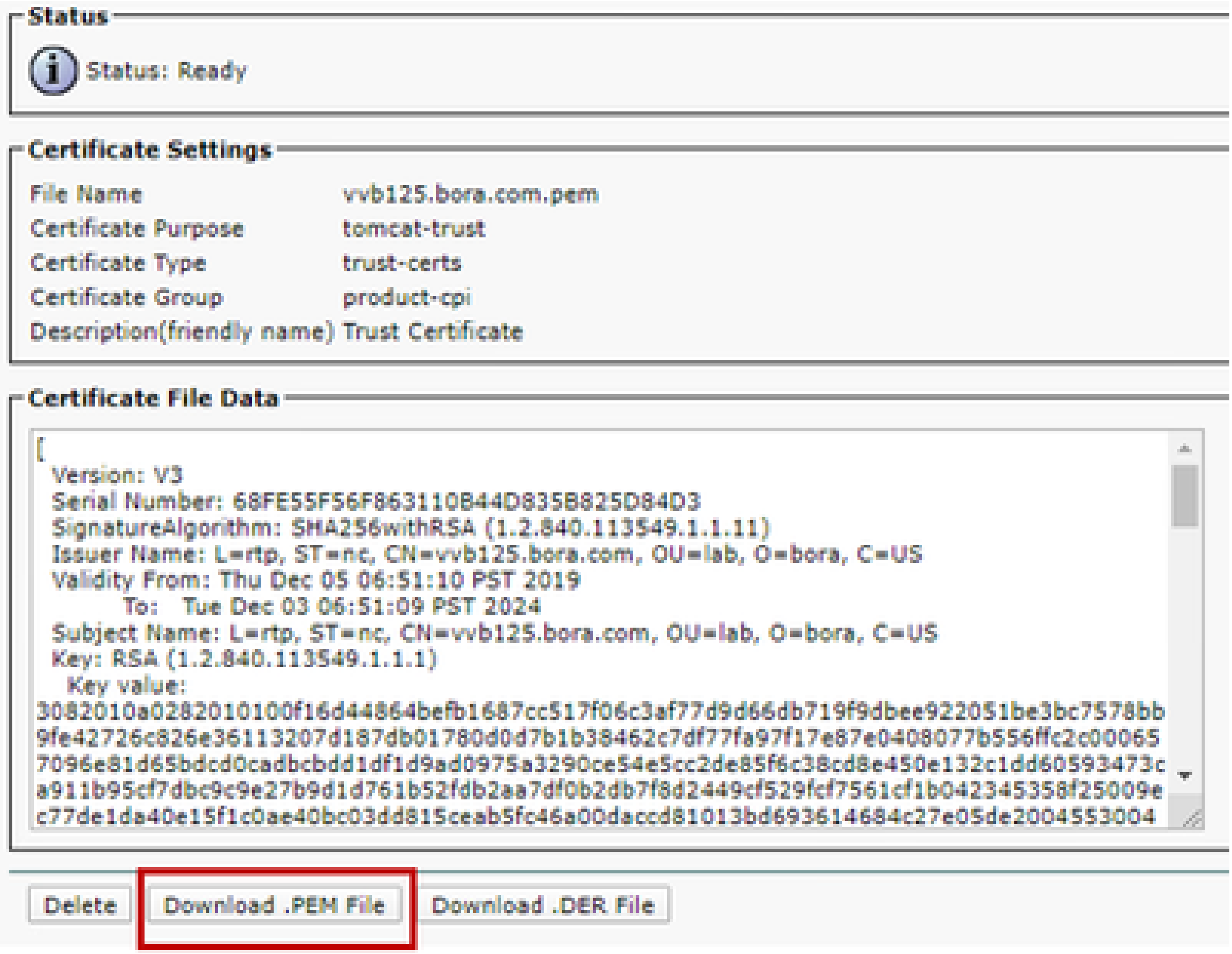
i. Navigate to the Cisco Unified Communications Operating System Administration page: https://{FQDN}:8443/cmplatform.

ii. Navigate to Security > Certificate Management and find the primary server certificates of the application in the tomcat-trust folder.



		signed			
tomcat-trust	thawte_Primary_Root_CA_-_G3	Self-signed	RSA	thawte_Primary_Root_CA_-_G3	thawte_Primary_Root_CA_-_G3
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	TWCA_Root_Certification_Authority	Self-signed	RSA	TWCA_Root_Certification_Authority	TWCA_Root_Certification_Authority
tomcat-trust	Buypass_Class_3_Root_CA	Self-signed	RSA	Buypass_Class_3_Root_CA	Buypass_Class_3_Root_CA
tomcat-trust	Starfield_Services_Root_Certificate_Authority_-_G2	Self-signed	RSA	Starfield_Services_Root_Certificate_Authority_-_G2	Starfield_Services_Root_Certificate_Authority_-_G2
tomcat-trust	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	Self-signed	RSA	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5
tomcat-trust	vvb125.bora.com	Self-signed	RSA	vvb125.bora.com	vvb125.bora.com
tomcat-trust	XRamp_Global_Certification_Authority	Self-signed	RSA	XRamp_Global_Certification_Authority	XRamp_Global_Certification_Authority

iii. Choose the certificate and click Download .PEM File in order to save it in a temporary folder on the OAMP server.



Status: Ready

File Name	vvb125.bora.com.pem
Certificate Purpose	tomcat-trust
Certificate Type	trust-certs
Certificate Group	product-cpi
Description(friendly name)	Trust Certificate

```
[
  Version: V3
  Serial Number: 68FE55F56F863110B44D835B825D84D3
  SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
  Issuer Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
  Validity From: Thu Dec 05 06:51:10 PST 2019
           To:   Tue Dec 03 06:51:09 PST 2024
  Subject Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
3082010a0282010100f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb
9fe42726c826e36113207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065
7096e81d65bdcd0cadbcbdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c
a911b95cf7dbc9c9e27b9d1d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e
c77de1da40e15f1c0ae40bc03dd815ceab5fc46a00daccd81013bd693614684c27e05de2004553004
```

Step 2. Import the VOS application certificate into the OAMP server.

i. Copy the VOS certificate to the %CVP_HOME%\conf\security directory on the OAMP server.

ii. Import the certificates with the command:

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

iii. Reboot the server.

Section 3. Certificate Exchange Between CVP Server and VVB Servers

This is an optional step in order to secure the SIP communication between CVP and other Contact Center components. For more information, refer to the CVP Configuration Guide: CVP Configuration Guide - Security.

CVP Call Studio Web Service Integration

For detailed information about how to establish a secure communication for Web Services Element and

Rest_Client element, refer to User Guide for Cisco Unified CVP VXML Server and Cisco Unified Call Studio Release 12.5(1) - Web Service Integration [Cisco Unified Customer Voice Portal] - Cisco.

Related Information

- CVP Configuration Guide - Security
- UCCE Security Guide
- PCCE Admin guide - Security
- Exchange PCCE Self-Signed Certificates - PCCE 12.5
- Exchange UCCE Self-Signed Certificates - UCCE 12.5
- Exchange PCCE Self-Signed Certificates - PCCE 12.6
- Implement CA-Signed Certificates - CCE 12.6
- CCE OpenJDK Migration
- CVP OpenJDK Migration
- Certificate Exchange Utility
- Technical Support & Documentation - Cisco Systems