

Exchange Self-Signed Certificates in a PCCE 12.6 Solution

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background](#)

[Procedure](#)

[Section 1: Certificate Exchange Between CVP and ADS Servers](#)

[Step 1. Export CVP Server Certificates](#)

[Step 2. Import CVP Servers WSM Certificate to ADS Server](#)

[Step 3. Export ADS Server Certificate](#)

[Step 4. Import ADS Server Certificate to CVP Servers and Reporting Server](#)

[Section 2: Certificate Exchange Between VOS Platform Applications and ADS Server](#)

[Step 1. Export VOS Platform Application Server Certificates.](#)

[Step 2. Import VOS Platform Application Certificate to ADS Server](#)

[Step 3. Import CUCM Platform Application Certificate to CUCM PG Server](#)

[Section 3: Certificate Exchange Between Rogger , PG and ADS Servers](#)

[Step 1. Export IIS Certificate from Rogger and PG Servers](#)

[Step 2. Export DFP Certificate from Rogger and PG Servers](#)

[Step 3. Import Certificates into ADS Server](#)

[Step 4. Import ADS Certificate into Rogger and PG Servers](#)

[Section 4: CVP CallStudio Web Service Integration](#)

[Related Information](#)

Introduction

This document describes how to exchange self-signed certificates in Cisco Packaged Contact Center Enterprise (PCCE) solution.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- PCCE Release 12.6(2)
- Customer Voice Portal (CVP) Release 12.6(2)
- Virtualized Voice Browser (VVB) 12.6(2)
- Admin Workstation / Administration Data Server (AW/ADS) 12.6(2)
- Cisco Unified Intelligence server (CUIC)
- Customer Collaboration Platform (CCP) 12.6(2)
- Enterprise Chat and Email (ECE) 12.6(2)

Components Used

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

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

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

In PCCE solution from 12.x all devices are controlled via Single Pane of Glass (SPOG) which is hosted in the principal AW server. Due to security-management-compliance (SRC) from PCCE 12.5(1) version all the communication between SPOG and other servers in the solution are strictly done via secure HTTP protocol.

Certificates are used in order to achieve seamless secure communication between SPOG and the other devices. In a self-signed certificate environment, certificate exchange between the servers is a must.

Procedure

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

(i) All AW/ADS Servers: These servers requires certificate from:

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

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

- CVP: CVP servers, CVP Reporting server.

Note: Web Service Management (WSM) certificate from all the servers are needed. Certificates must be with Fully Qualified Domain Name (FQDN).

- VOS Platform: Cloud Connect, Cisco Virtualized Voice Browser (VVB), Cisco Unified Communication Manager (CUCM), Finesse, Cisco Unified Intelligence Center (CUIC), Live Data (LD), Identity Server (IDS), and other applicable servers.

(ii) Router \ Logger Servers: These servers require certificate from:

- Windows platform: All AW/ADS servers IIS certificate.

(iii) PG Servers: These servers require certificate from:

- Windows platform: All AW/ADS servers IIS certificate.
- VOS Platform: CUCM publisher (CUCM PG servers only); Cloud Connect and CCP (MR PG Server only).

Note: This is needed to download the JTAPI client from CUCM server.

(iv) CVP Servers: These servers require certificate from

- Windows platform: All ADS servers IIS certificate
- VOS Platform: Cloud Connect server, VVB Servers.

(v) CVP Reporting server: This server requires certificate from:

- Windows platform: All ADS servers IIS certificate

(vi) VVB Servers: This server requires certificate from:

- Windows platform: All ADS servers IIS certificate, VXML certificate from CVP server, and Callserver certificate from CVP server
- VOS Platform: Cloud Connect server.

The steps needed to effectively exchange the self-signed certificates in the solution are divided in three sections.

Section 1: Certificate Exchange Between CVP Servers and ADS Servers.

Section 2: Certificate Exchange Between VOS Platform Applications and ADS Server.

Section 3: Certificate Exchange Between Roggers, PGs and ADS Server.

Section 1: Certificate Exchange Between CVP and ADS Servers

The steps needed to complete this exchange successfully are:

Step 1. Export CVP Servers WSM Certificates.

Step 2. Import CVP Servers WSM Certificate to ADS Servers.

Step 3. Export ADS Server Certificate.

Step 4. Import ADS Server to CVP Servers and CVP Reporting Server.

Step 1. Export CVP Server Certificates

Before you export the certificates from the CVP servers, you need to regenerate the certificates with the FQDN of the server, otherwise, few features like Smart Licensing, Virtual Agent Voice (VAV), and the CVP synchronization with SPOG can experience problems.

Caution: Before you begin, you must do this:

1. Open a command window as administrator.
2. For 12.6.2, to identify the keystore password, go to the %CVP_HOME%\bin folder and run the DecryptKeystoreUtil.bat file.
3. For 12.6.1, to identify the keystore password, run the command, **more %CVP_HOME%\conf\security.properties.**
4. You need this password when running the keytool commands.
5. From the %CVP_HOME%\conf\security\ directory, run the command, **copy .keystore backup.keystore.**

Note: You can streamline the commands used in this document by the use of the keytool parameter -

storepass. For all CVP servers, provide the keytool password you identified. For the ADS servers the default password is: **changeit**

To regenerate the certificate on the CVP servers execute these steps:

(i) List the certificates in the server

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

Note: The CVP Servers have these self-signed certificates: wsm_certificate, vxml_certificate, callserver_certificate. If you use the parameter -v of the keytool, you are able to see more detailed information of each certificate. In addition, you can add the ">" symbol at the end of the keytool.exe list command to send the output to a text file, for example: > test.txt

(ii) Delete the old self-signed certificates

CVP servers: Commands to delete the self-signed certificates:

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

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

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

CVP Reporting servers: Commands to delete the self-signed certificates:

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

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

Note: CVP Reporting servers have these self-signed certificates: wsm_certificate, callserver_certificate.

(iii) Generate the new self-signed certificates with the FQDN of the server

CVP servers

Command to generate the self-signed certificate for WSM:

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

Note: By default, the certificates are generated for two years. Use -validity XXXX to set the expiry date when certificates are regenerated, otherwise certificates are valid for 90 days and need to be signed by a CA before this time. For most of these certificates, 3-5 years must be a reasonable validation time.

Here are some standard validity inputs:

One Year	365
Two Years	730
Three Years	1095
Four Year	1460
Five Years	1895
Ten Years	3650

Caution: From 12.5 certificates must be **SHA 256**, Key Size **2048**, and encryption Algorithm **RSA**, use these parameters to set these values: -keyalg RSA and -keysize 2048. It is important that the CVP keystore commands include the -storetype JCEKS parameter. If this is not done, the certificate, the key, or worse the keystore can become corrupted.

Specify the FQDN of the server, on the question **what is your fist and last name?**

```
C:\Cisco\CVP\jre\bin>keytool.exe -genkeypair -v -storetype JCEKS -keystore c:\Cisco\CVP\co
sm_certificate1 -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]:
```

Complete these other questions:

What is the name of your organizational unit?

[Unknown]: <specify OU>

What is the name of your organization?

[Unknown]: <specify the name of the org>

What is the name of your City or Locality?

[Unknown]: <specify the name of the city/locality>

What is the name of your State or Province?

[Unknown]: <specify the name of the state/province>

What is the two-letter country code for this unit?

[Unknown]: <specify two-letter Country code>

Specify **yes** for the next two inputs.

Perform the same steps for vxml_certificate and callserver_certificate:

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

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

Reboot the CVP call server.

CVP Reporting servers

Command to generate the self-signed certificates for WSM:

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

Specify the FQDN of the server for the query **what is your first and last name ?** and continue with the same steps as done with CVP servers.

Perform the same steps for callserver_certificate:

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

Reboot the Reporting servers.

(iv) Export wsm_Certificate from CVP and Reporting servers

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

Command to export the self-signed certificates:

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

b) Copy the certificate from the path **%CVP_HOME%\conf\security\wsm.crt**, rename it to **wsmcsX.crt**

and move it to a temporary folder on the ADS server.

Step 2. Import CVP Servers WSM Certificate to ADS Server

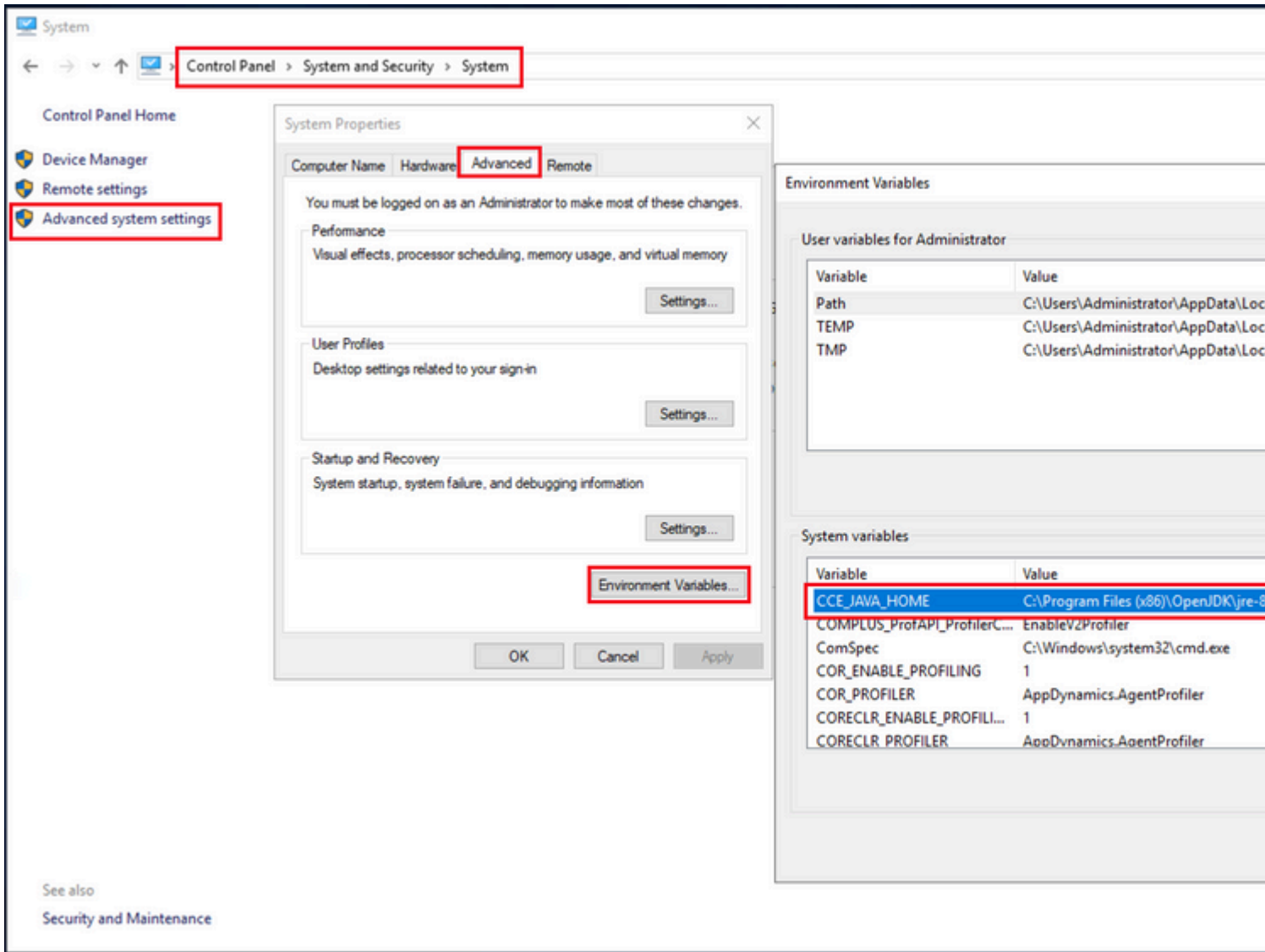
To import the certificate in ADS server you need to use the keytool which is a part of java toolset. There are couple of ways you can find the java home path where this tool is hosted.

(i) CLI command > **echo %CCE_JAVA_HOME%**

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

java home path

(ii) Manually via **Advanced system setting**, as shown in the image.



Environment Variables

On PCCE 12.6 default path of OpenJDK is **C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin**

Commands to import the self-signed certificates:

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

Note: Repeat the commands for each CVP in the deployment and perform the same task on other ADS servers

(iii) Restart the Apache Tomcat service on the ADS servers.

Step 3. Export ADS Server Certificate

Here are the steps to export the ADS certificate:

(i) On ADS server from a browser, navigate to the server url : **https://<servername>**.

(ii) Save the certificate to a temporary folder, for example: **c:\temp\certs** and name the certificate as **ADS<svr>[ab].cer**.

Related Information

- [CVP Configuration Guide - Security](#)
- [UCCE Security Guide](#)
- [PCCE Admin Guide](#)
- [Exchange PCCE Self-Signed Certificates - PCCE 12.5](#)
- [Exchange UCCE Self-Signed Certificates - UCCE 12.5](#)
- [Exchange UCCE Self-Signed Certificates - UCCE 12.6](#)
- [Implement CA-Signed Certificates - CCE 12.6](#)
- [Exchange Certificates with Contact Center Uploader Tool](#)
- [Technical Support & Documentation - Cisco Systems](#)