Exchange Certificates with Contact Center Uploader Tool

Contents

Introduction

This document describes the Contact Center Uploader Tool that gets and uploads certificates in the Unified Contact Center Enterprise (UCCE) solution.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- UCCE Release 12.6(1)
- Customer Voice Portal (CVP) Release 12.6(1)
- Enterprise Chat and Email (ECE) Release 12.6(1)

Components Used

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

- UCCE 12.6(1)
- CVP 12.6(1)
- ECE 12.6(1)

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 the UCCE/PCCE solution from 12.x all devices are controlled via Single Pane of Glass (SPOG) which is hosted in the principal Admin Workstation (AW) server. Due to security-management-compliance (SRC) in

PCCE 12.X versions, all the communication between SPOG and other servers in the solution is 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 becomes a must. This certificate exchange is also necessary to enable new features that are present in the 12.5 and 12.6 versions such as Smart Licensing, Webex Experience Management (WXM), and Customer Virtual Assistant (CVA).

Problem

Certificates exchange can be a difficult task for people who are not familiar with the java**keytool**utility, especially when self-service certificates are used.

Wrong actions can cause issues with solution configuration and its health.

Certificates can be expired, and renew of them is another challenge.

Solution

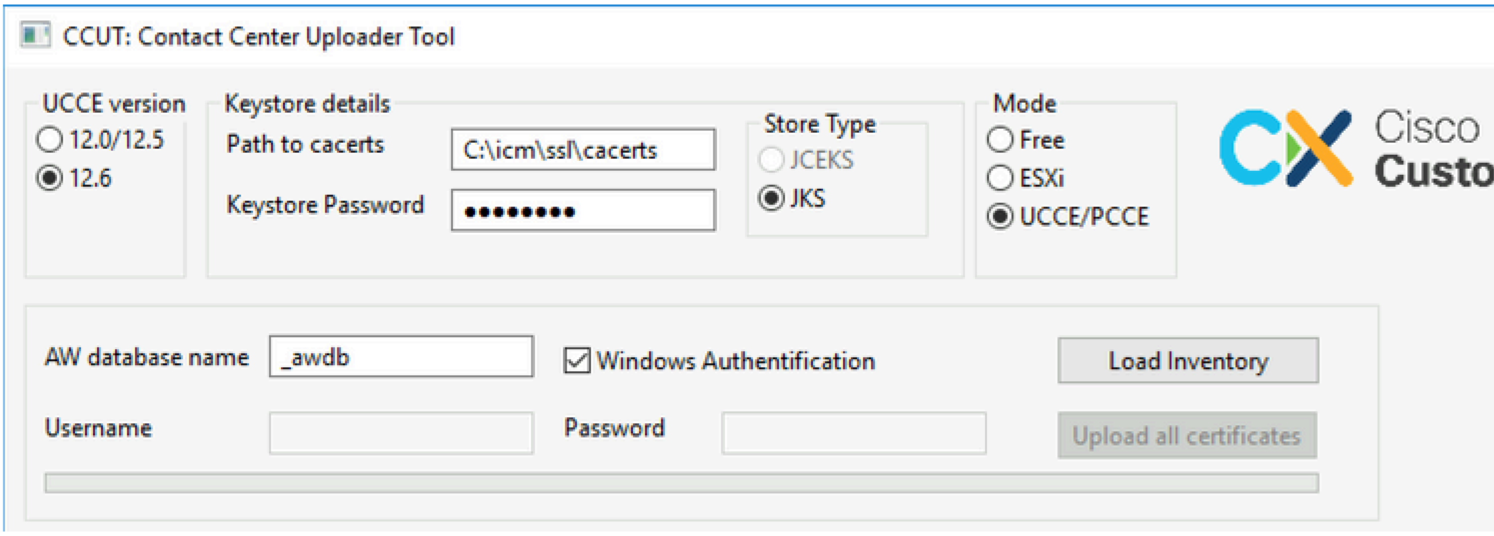
The article contains a link to the Contact Center Uploader Tool (CCUT) written in Java that helps you with the task.

The tool can connect to the UCCE database or to the ESXi host, gets the data about all hosts from there, gets a certificate from each host and uploads it to the java **cacerts** trust store.

Note: The tool is created by Cisco TAC engineers and there is no official support. You can use ccut@cisco.com for feedback, questions, and issues.

UCCE/PCCE Mode

The main application window of the tool in **UCCE/PCCE** mode is in the picture:



CCUT: Contact Center Uploader Tool

UCCE version: ○ 12.0/12.5 ● 12.6

Keystore details
Path to cacerts: C:\icm\ssl\cacerts
Keystore Password: •••••••••

Store Type: ○ JCEKS ● JKS

Mode: ○ Free ○ ESXi ● UCCE/PCCE

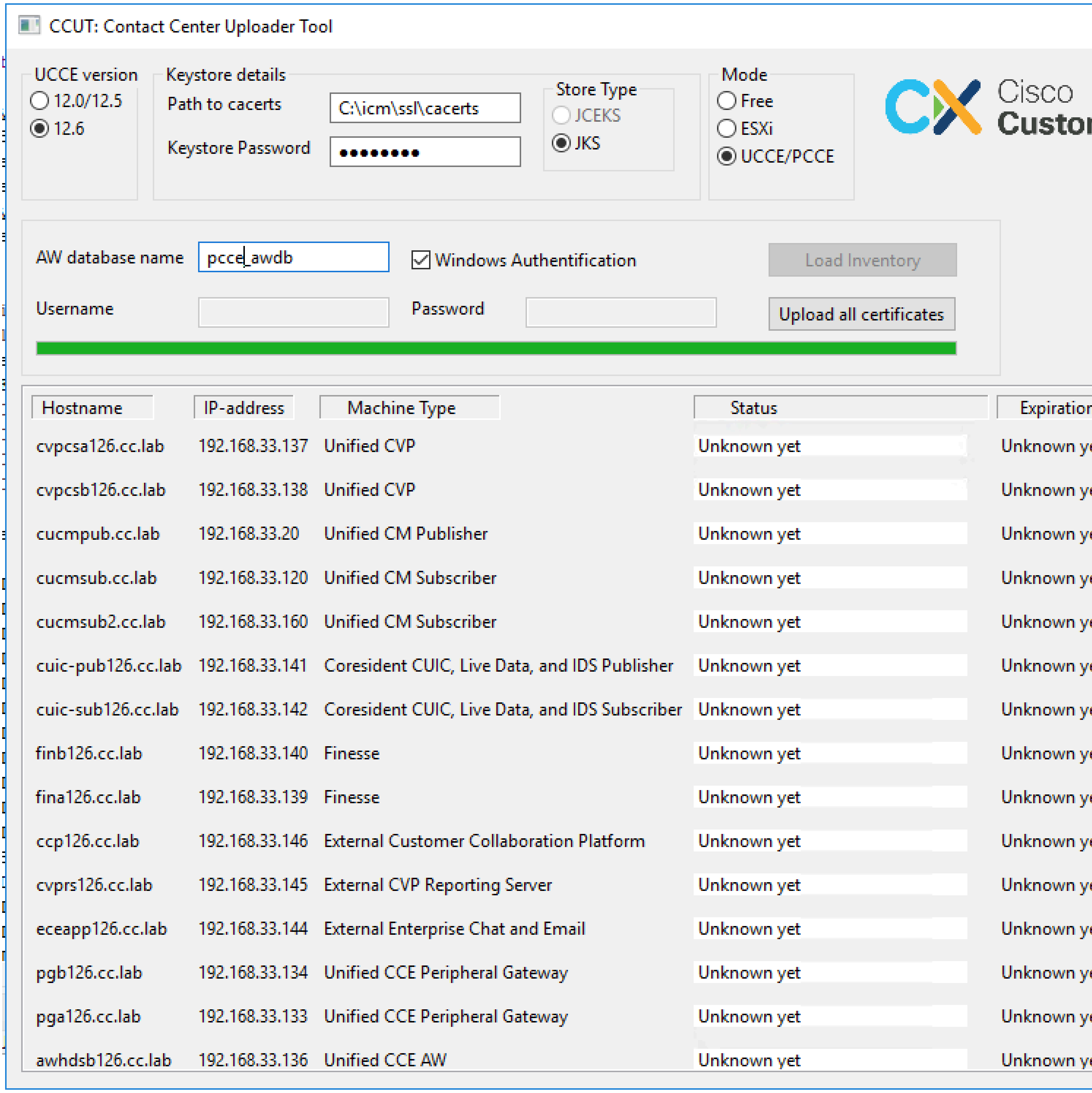
AW database name: _awdb
☑ Windows Authentification
Username:
Password:

- **AW database name:** provide the name of the AW database, Logger, or **pcceinvetory** database. There must be data in the **t_Machine...** tables.
  If the tool runs on the UCCE host where the database component is not installed, the remote

Structured Querry Language (SQL) server name can be added as a prefix to the database name.
For example **AWHDS-A\pcce_awdb**
This is applicable for Peripheral Gateway (PG) or ROUTER machines.

- **Username** and **Password** for the SQL user with access right to read the database data. Check the **Windows Authentification** to use integrated windows authentication instead of SQL.
- **UCCE version:** patch to the **cacerts** file depends on the installed UCCE version.
- **Path to cacerts:** Location of the **cacerts** file. In the UCCE 12.6.X the system uses **C:\icm\ssl\cacerts**, UCCE 12.5 uses the default Java truststore **(%CCE_JAVA_HOME%\lib\security\cacert)**.
- **Keystore Password:** default password for the **cacerts** store is **changeit.**
- **Store Type:** UCCE uses **JKS** type of the store, while CVP uses **JCEKS.**
- **Load Inventory** button**:** The tool connects to the mentioned database and shows the inventory data.
- **Upload all certificates** button**:** The button is available after the tool gets the data from the database.

Example of the loaded data in the picture:



CCUT: Contact Center Uploader Tool

UCCE version: ○ 12.0/12.5 ● 12.6

Keystore details

Path to cacerts: C:\icm\ssl\cacerts

Keystore Password: ••••••••

Store Type: ○ JCEKS ● JKS

Mode: ○ Free ○ ESXi ● UCCE/PCCE

AW database name: pcce_awdb

☑ Windows Authentification

Username:

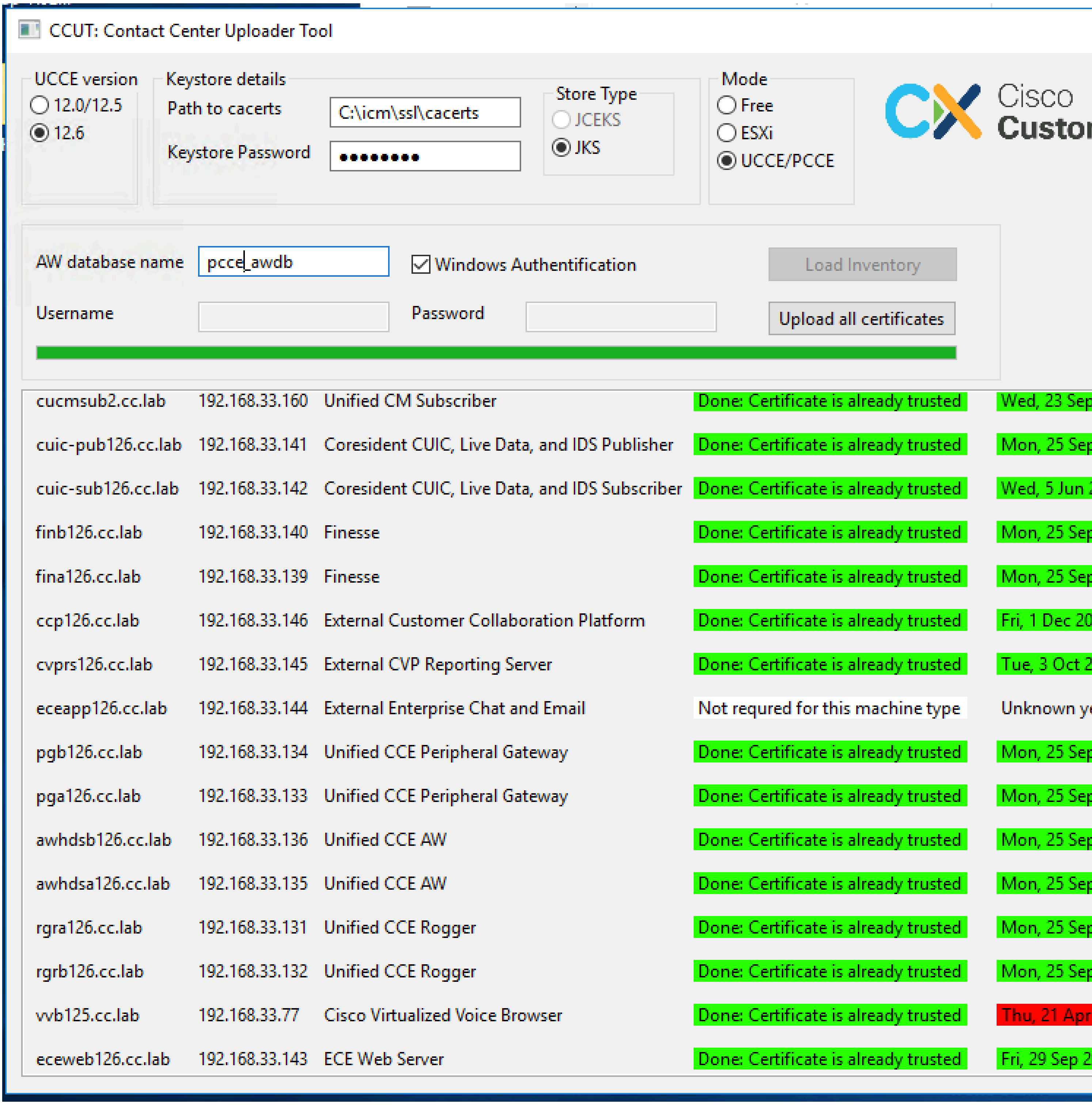
Password:

Hostname	IP-address	Machine Type	Status	Expiratio
cvpcsa126.cc.lab	192.168.33.137	Unified CVP	Unknown yet	Unknown y
cvpcsb126.cc.lab	192.168.33.138	Unified CVP	Unknown yet	Unknown y
cucmpub.cc.lab	192.168.33.20	Unified CM Publisher	Unknown yet	Unknown y
cucmsub.cc.lab	192.168.33.120	Unified CM Subscriber	Unknown yet	Unknown y
cucmsub2.cc.lab	192.168.33.160	Unified CM Subscriber	Unknown yet	Unknown y
cuic-pub126.cc.lab	192.168.33.141	Coresident CUIC, Live Data, and IDS Publisher	Unknown yet	Unknown y
cuic-sub126.cc.lab	192.168.33.142	Coresident CUIC, Live Data, and IDS Subscriber	Unknown yet	Unknown y
finb126.cc.lab	192.168.33.140	Finesse	Unknown yet	Unknown y
fina126.cc.lab	192.168.33.139	Finesse	Unknown yet	Unknown y
ccp126.cc.lab	192.168.33.146	External Customer Collaboration Platform	Unknown yet	Unknown y
cvprs126.cc.lab	192.168.33.145	External CVP Reporting Server	Unknown yet	Unknown y
eceapp126.cc.lab	192.168.33.144	External Enterprise Chat and Email	Unknown yet	Unknown y
pgb126.cc.lab	192.168.33.134	Unified CCE Peripheral Gateway	Unknown yet	Unknown y
pga126.cc.lab	192.168.33.133	Unified CCE Peripheral Gateway	Unknown yet	Unknown y
awhdsb126.cc.lab	192.168.33.136	Unified CCE AW	Unknown yet	Unknown y

The inventory data consists of 6 columns:

- Hostname
- IP-Address
- Machine type
- Status of the certificate data or error details
- Certificate expiration date
- Details

The results of the **Upload all Certificates** button:



CCUT: Contact Center Uploader Tool

UCCE version
○ 12.0/12.5
● 12.6

Keystore details
Path to cacerts: C:\icm\ssl\cacerts
Keystore Password: ●●●●●●●●●

Store Type
○ JCEKS
● JKS

Mode
○ Free
○ ESXi
● UCCE/PCCE

AW database name: pcce_awdb
☑ Windows Authentification
Username:
Password:

cucmsub2.cc.lab	192.168.33.160	Unified CM Subscriber	Done: Certificate is already trusted	Wed, 23 Sep
cuic-pub126.cc.lab	192.168.33.141	Coresident CUIC, Live Data, and IDS Publisher	Done: Certificate is already trusted	Mon, 25 Sep
cuic-sub126.cc.lab	192.168.33.142	Coresident CUIC, Live Data, and IDS Subscriber	Done: Certificate is already trusted	Wed, 5 Jun
finb126.cc.lab	192.168.33.140	Finesse	Done: Certificate is already trusted	Mon, 25 Sep
fina126.cc.lab	192.168.33.139	Finesse	Done: Certificate is already trusted	Mon, 25 Sep
ccp126.cc.lab	192.168.33.146	External Customer Collaboration Platform	Done: Certificate is already trusted	Fri, 1 Dec 20
cvprs126.cc.lab	192.168.33.145	External CVP Reporting Server	Done: Certificate is already trusted	Tue, 3 Oct 2
eceapp126.cc.lab	192.168.33.144	External Enterprise Chat and Email	Not requred for this machine type	Unknown ye
pgb126.cc.lab	192.168.33.134	Unified CCE Peripheral Gateway	Done: Certificate is already trusted	Mon, 25 Sep
pga126.cc.lab	192.168.33.133	Unified CCE Peripheral Gateway	Done: Certificate is already trusted	Mon, 25 Sep
awhdsb126.cc.lab	192.168.33.136	Unified CCE AW	Done: Certificate is already trusted	Mon, 25 Sep
awhdsa126.cc.lab	192.168.33.135	Unified CCE AW	Done: Certificate is already trusted	Mon, 25 Sep
rgra126.cc.lab	192.168.33.131	Unified CCE Rogger	Done: Certificate is already trusted	Mon, 25 Sep
rgrb126.cc.lab	192.168.33.132	Unified CCE Rogger	Done: Certificate is already trusted	Mon, 25 Sep
vvb125.cc.lab	192.168.33.77	Cisco Virtualized Voice Browser	Done: Certificate is already trusted	Thu, 21 Apr
eceweb126.cc.lab	192.168.33.143	ECE Web Server	Done: Certificate is already trusted	Fri, 29 Sep 2

Every row marked as green is a success.

The red or yellow row is required attention.

ESXi Mode

ESXi mode can be used for PCCE/UCCE fresh installation when the Inventory is not yet configured and **t_Machine...** tables do not contain any data.

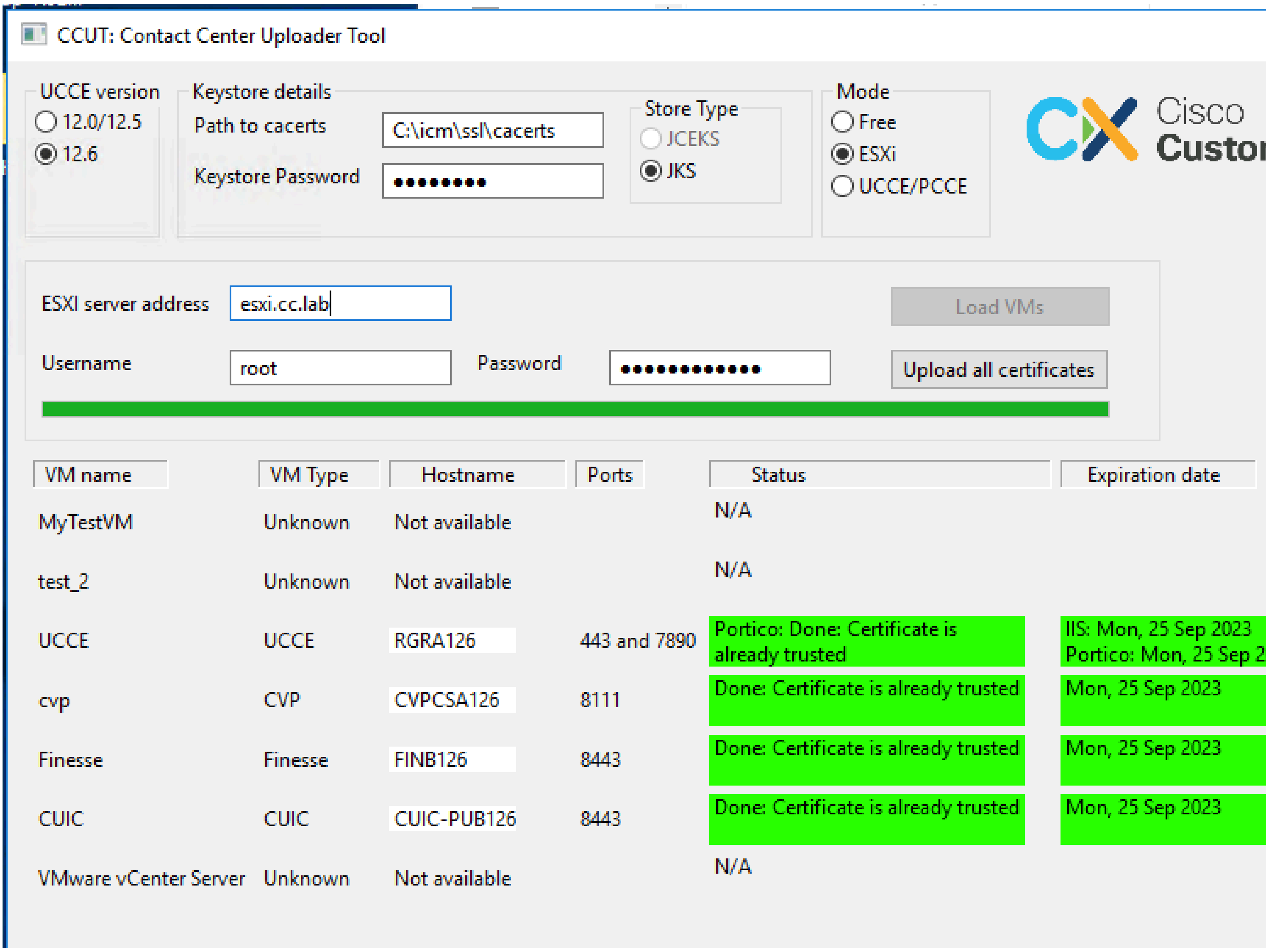
The tool connects to the ESXi host and gets the data about all virtual machines from there.

It requests Virtual Machine (VM) name, VM annotations, and hostname from the guest operating system.

VM annotations are used to identify the machine type.

VmWare tools must run on VMs, otherwise, the hostname is not populated.

The tool in the ESXi mode is in the picture:



CCUT: Contact Center Uploader Tool

UCCE version
○ 12.0/12.5
● 12.6

Keystore details
Path to cacerts: C:\icm\ssl\cacerts
Keystore Password: ••••••••

Store Type
○ JCEKS
● JKS

Mode
○ Free
● ESXi
○ UCCE/PCCE

ESXI server address: esxi.cc.lab

Username: root

Password: •••••••••••••

VM name	VM Type	Hostname	Ports	Status	Expiration date
MyTestVM	Unknown	Not available		N/A	
test_2	Unknown	Not available		N/A	
UCCE	UCCE	RGRA126	443 and 7890	Portico: Done: Certificate is already trusted	IIS: Mon, 25 Sep 2023 Portico: Mon, 25 Sep 2
cvp	CVP	CVPCSA126	8111	Done: Certificate is already trusted	Mon, 25 Sep 2023
Finesse	Finesse	FINB126	8443	Done: Certificate is already trusted	Mon, 25 Sep 2023
CUIC	CUIC	CUIC-PUB126	8443	Done: Certificate is already trusted	Mon, 25 Sep 2023
VMware vCenter Server	Unknown	Not available		N/A	

Note: VCenter is not supported for connections.

Free Mode

Another mode of the tool is the **Free** mode.

There is no requirement to have UCCE Database available and the tool can be used to upload any certificates to CVP or ECE.

Example use cases:

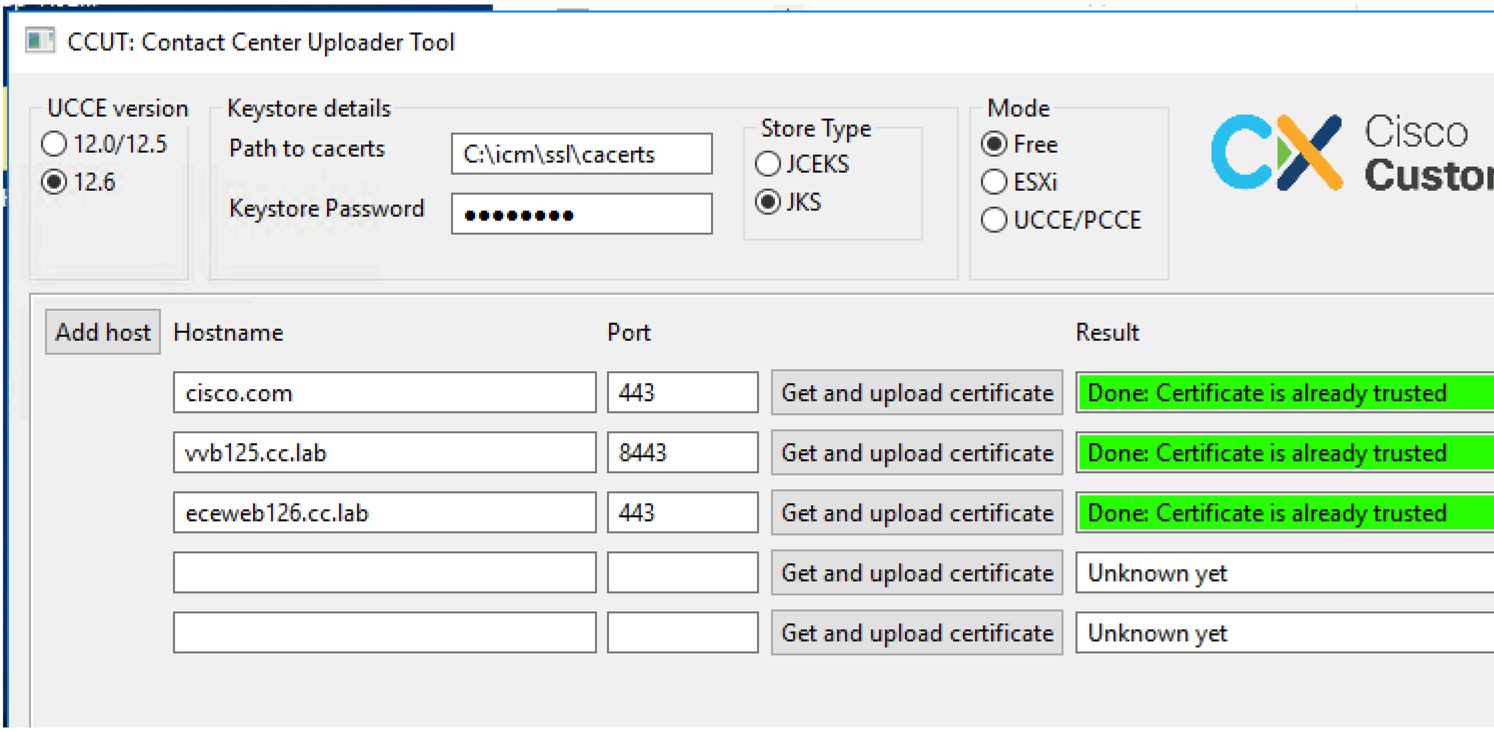
- Get and upload 3-rd party web-service certificate to CVP.

- Get and upload mail servers' certificates to ECE services server.

- Get and upload Intrusion Detection System (IDS) certificates to ECE application server.

Note: The tool cannot upload certificates to the CVP **.keystore** file due to some restrictions.

An example of the tool in the **Free** mode is in the picture:



CCUT: Contact Center Uploader Tool

UCCE version: ○ 12.0/12.5 ● 12.6

Keystore details

Path to cacerts: C:\icm\ssl\cacerts

Keystore Password: •••••••••

Store Type: ○ JCEKS ● JKS

Mode: ● Free ○ ESXi ○ UCCE/PCCE

Add host	Hostname	Port		Result
	cisco.com	443	Get and upload certificate	Done: Certificate is already trusted
	vvb125.cc.lab	8443	Get and upload certificate	Done: Certificate is already trusted
	eceweb126.cc.lab	443	Get and upload certificate	Done: Certificate is already trusted
			Get and upload certificate	Unknown yet
			Get and upload certificate	Unknown yet

Run the Tool

Download Contact Center Uploader Tool.

Extract the downloaded archive file.

The **Launcher** file contains paths to the jar and Java.

Update the path to Java and to the jar file if required.

Open the command prompt(cmd) with Administrator permissions.

Go to the extracted folder by **cd** command and run the **LauncherX86.bat** to start the tool.

Caution: Always take a backup of the trust store file.

Technical Details

- The tool connects to the host and checks if the certificate is trusted or not. If it is not trusted, then the certificate is uploaded.
- The certificate is uploaded with the alias **util-[hostname]-[port]**, for example **util-vvb125.cc.lab-8443**.
- A host can send more than one certificate. In this case, the tool uploads all these certificates as root and/or intermediate prefixes.
- The tool is compiled with java 1.8.
- The tool connects to the database by **localhost:1433** by default.
- The minimum screen resolution is 1024x768. Scaled mode is not supported.