Tauschen Sie Zertifikate mit dem Contact Center Uploader-Tool aus

Inhalt

Einleitung

In diesem Dokument wird das Contact Center Uploader Tool beschrieben, mit dem Zertifikate in der Unified Contact Center Enterprise (UCCE)-Lösung abgerufen und hochgeladen werden.

Voraussetzungen

Anforderungen

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

- UCCE-Version 12.6(1)
- Customer Voice Portal (CVP) Version 12.6(1)
- Enterprise Chat und E-Mail (ECE) Version 12.6(1)

Verwendete Komponenten

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

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

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/PCCE-Lösung ab 12.x werden alle Geräte über eine zentrale, transparente Schnittstelle

(Single Pane of Glass, SPOG) gesteuert, die auf dem Haupt-AW-Server (Admin Workstation) gehostet wird. Aufgrund der Sicherheitsmanagement-Compliance (SRC) in PCCE 12.X-Versionen erfolgt die gesamte Kommunikation zwischen SPOG und anderen Servern der Lösung ausschließlich über ein sicheres HTTP-Protokoll.

Zertifikate werden verwendet, um eine nahtlose sichere Kommunikation zwischen dem SPOG und den anderen Geräten zu erreichen. In einer selbstsignierten Zertifikatsumgebung ist der Zertifikataustausch zwischen den Servern ein Muss. Dieser Zertifikataustausch ist auch erforderlich, um neue Funktionen der Versionen 12.5 und 12.6 zu aktivieren, z. B. Smart Licensing, WebEx Experience Management (WXM) und Customer Virtual Assistant (CVA).

Problem

Der Austausch von Zertifikaten kann für Personen, die mit dem Java nicht vertraut sind, eine schwierige Aufgabe sein**keytool**verwendet, insbesondere wenn Self-Service-Zertifikate verwendet werden.

Falsche Aktionen können Probleme mit der Lösungskonfiguration und deren Zustand verursachen.

Zertifikate können abgelaufen sein, und ihre Verlängerung ist eine weitere Herausforderung.

Lösung

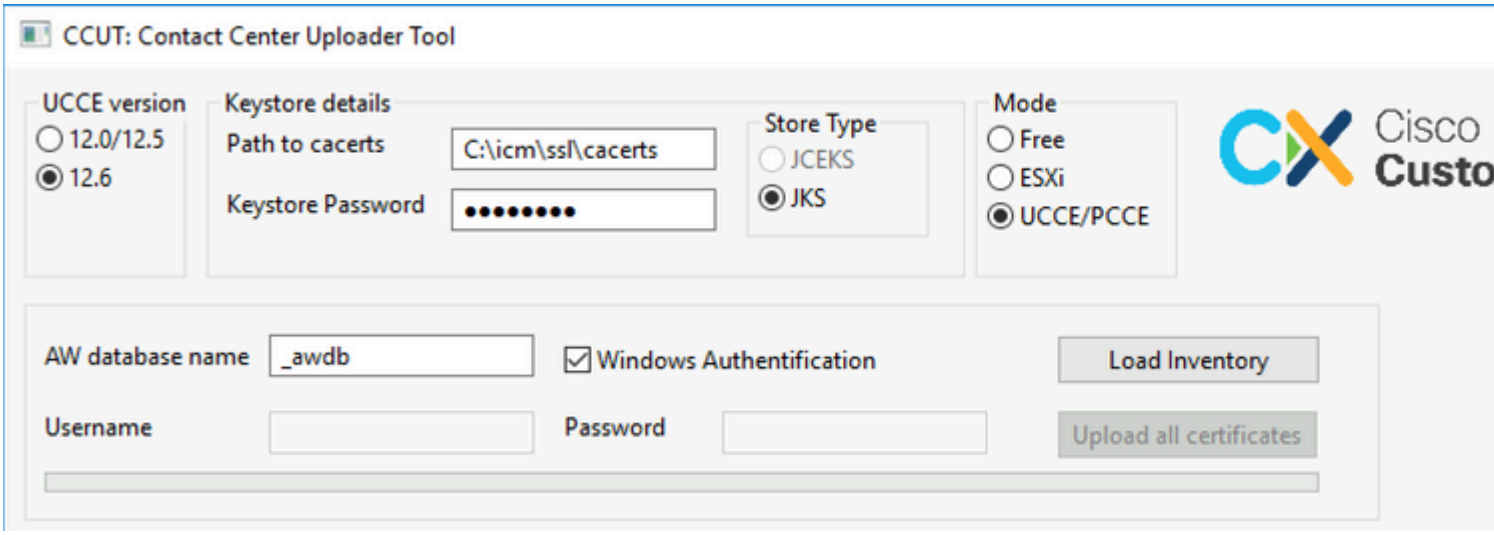
Der Artikel enthält einen Link zum Contact Center Uploader Tool (CCUT) in Java, der Ihnen bei der Durchführung dieser Aufgabe behilflich ist.

Das Tool kann eine Verbindung zur UCCE-Datenbank oder zum ESXi-Host herstellen, ruft die Daten aller Hosts von dort ab, erhält ein Zertifikat von jedem Host und lädt es in den Java **Acerts** Trust Store hoch.

> **Hinweis**: Das Tool wird von Cisco TAC-Technikern erstellt. Es gibt keinen offiziellen Support. Sie können ccut@cisco.com für Feedback, Fragen und Probleme verwenden.

UCCE-/PCCE-Modus

Das Hauptanwendungsfenster des Tools im **UCCE/PCCE**-Modus ist in der Abbildung dargestellt:

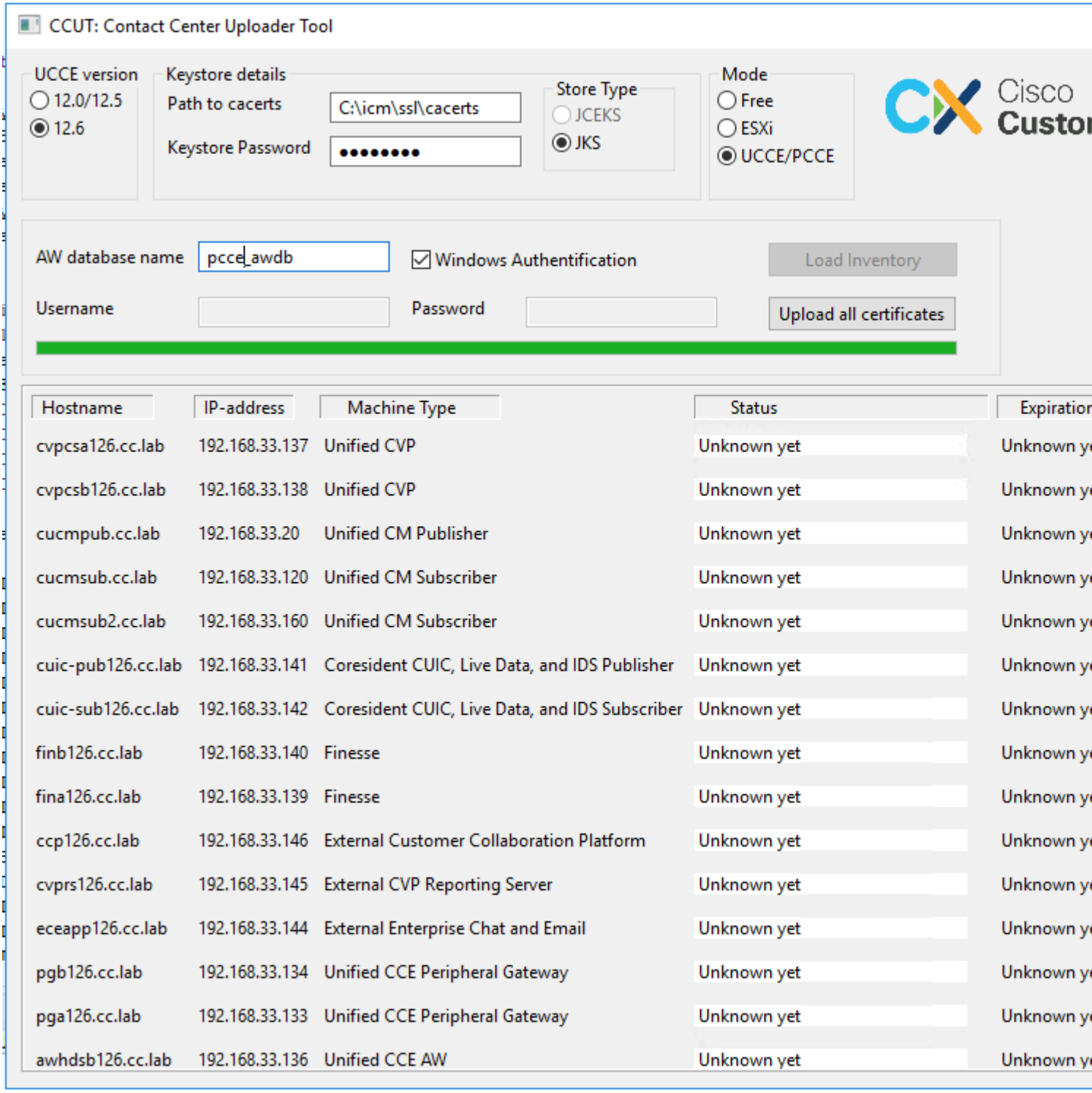


- **AW database name:** Geben Sie den Namen der AW-Datenbank, der Protokollierung oder der

pcceinventory-Datenbank an. In den Tabellen **t_Machine...** müssen Daten vorhanden sein.
Wenn das Tool auf dem UCCE-Host ausgeführt wird, auf dem die Datenbankkomponente nicht installiert ist, kann der SQL-Servername (Structured Query Language) als Präfix zum Datenbanknamen hinzugefügt werden.
Beispiel: **AWHDS-A\pcce_awdb**
Dies gilt für Peripheral Gateway (PG)- oder ROUTER-Systeme.

- **Username** und **Password** für den SQL-Benutzer mit Zugriffsberechtigung zum Lesen der Datenbankdaten. Überprüfen Sie **Windows Authentification** , um die integrierte Windows-Authentifizierung anstelle von SQL zu verwenden.
- **UCCE version:** hängt von der installierten UCCE-Version ab.
- **Path to cacerts:** Speicherort der **Cacerts**-Datei. In UCCE 12.6.X verwendet das System **C:\icm\ssl\cacerts**, UCCE 12.5 verwendet den Standard-Java-TrustStore **(%CCE_JAVA_HOME%\lib\security\cacert)**.
- **Keystore Password:** Das Standardkennwort für den **Zertifikatspeicher** wird **geändert.**
- **Store Type:** UCCE verwendet den **JKS**-Typ des Speichers, während CVP **JCEKS** verwendet**.**
- **Load Inventory** button**:** Das Tool stellt eine Verbindung zur genannten Datenbank her und zeigt die Inventardaten an.
- **Upload all certificates** button**:** Die Schaltfläche ist verfügbar, nachdem das Tool die Daten aus der Datenbank abgerufen hat.

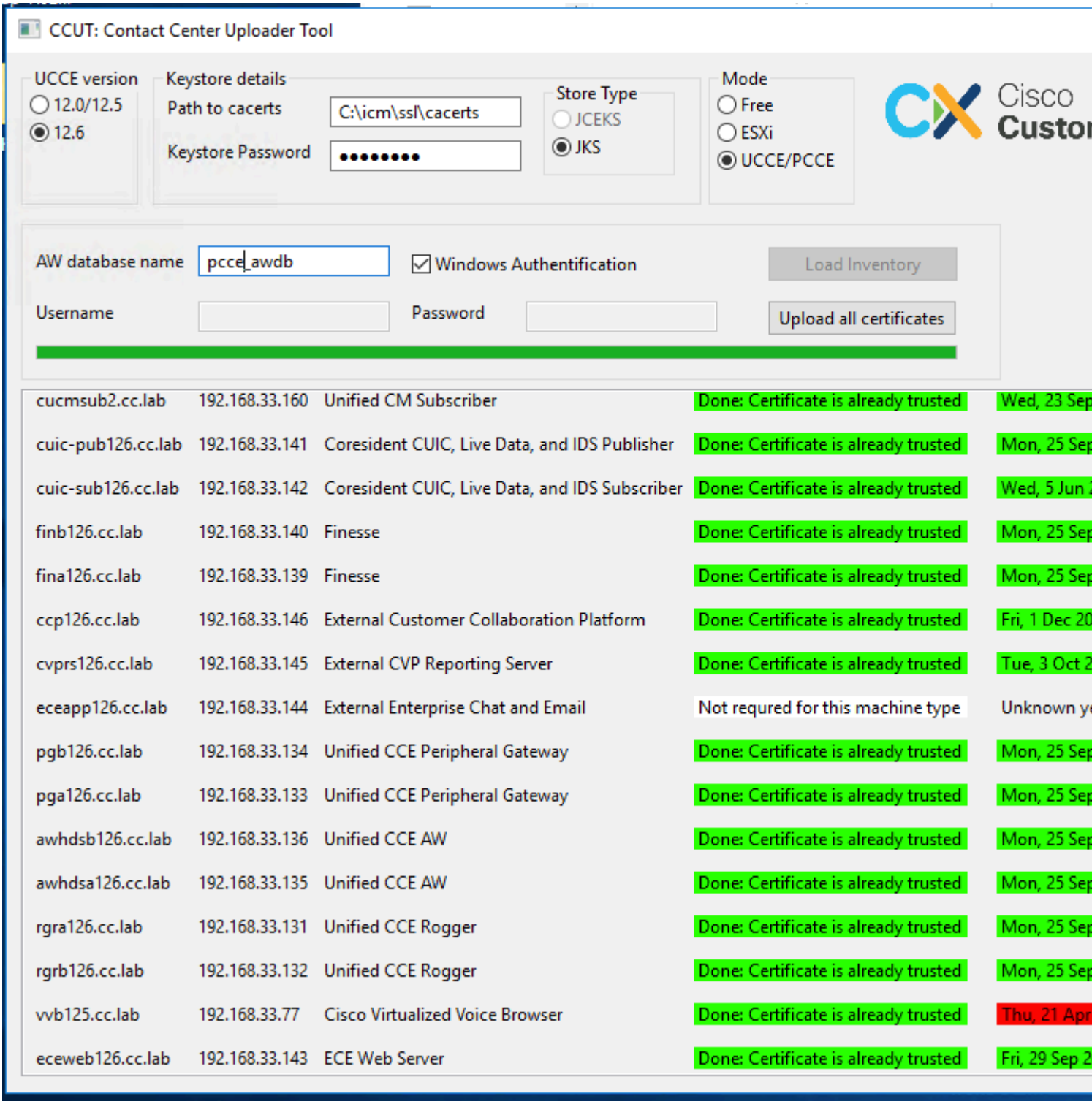
Beispiel der geladenen Daten im Bild:



Die Bestandsdaten umfassen 6 Spalten:

- Hostname
- IP-Adresse
- Maschinentyp
- Status der Zertifikatsdaten oder Fehlerdetails
- Ablaufdatum des Zertifikats
- Details

Die Ergebnisse der Schaltfläche **"Alle Zertifikate hochladen"**:



Jede als grün markierte Zeile ist ein Erfolg.

Die rote oder gelbe Zeile muss beachtet werden.

ESXi-Modus

Der ESXi-Modus kann für die Neuinstallation von PCCE/UCCE verwendet werden, wenn der Bestand noch nicht konfiguriert ist und die Tabellen **t_Machine...** keine Daten enthalten.

Das Tool stellt eine Verbindung zum ESXi-Host her und ruft von dort die Daten aller virtuellen Systeme ab.

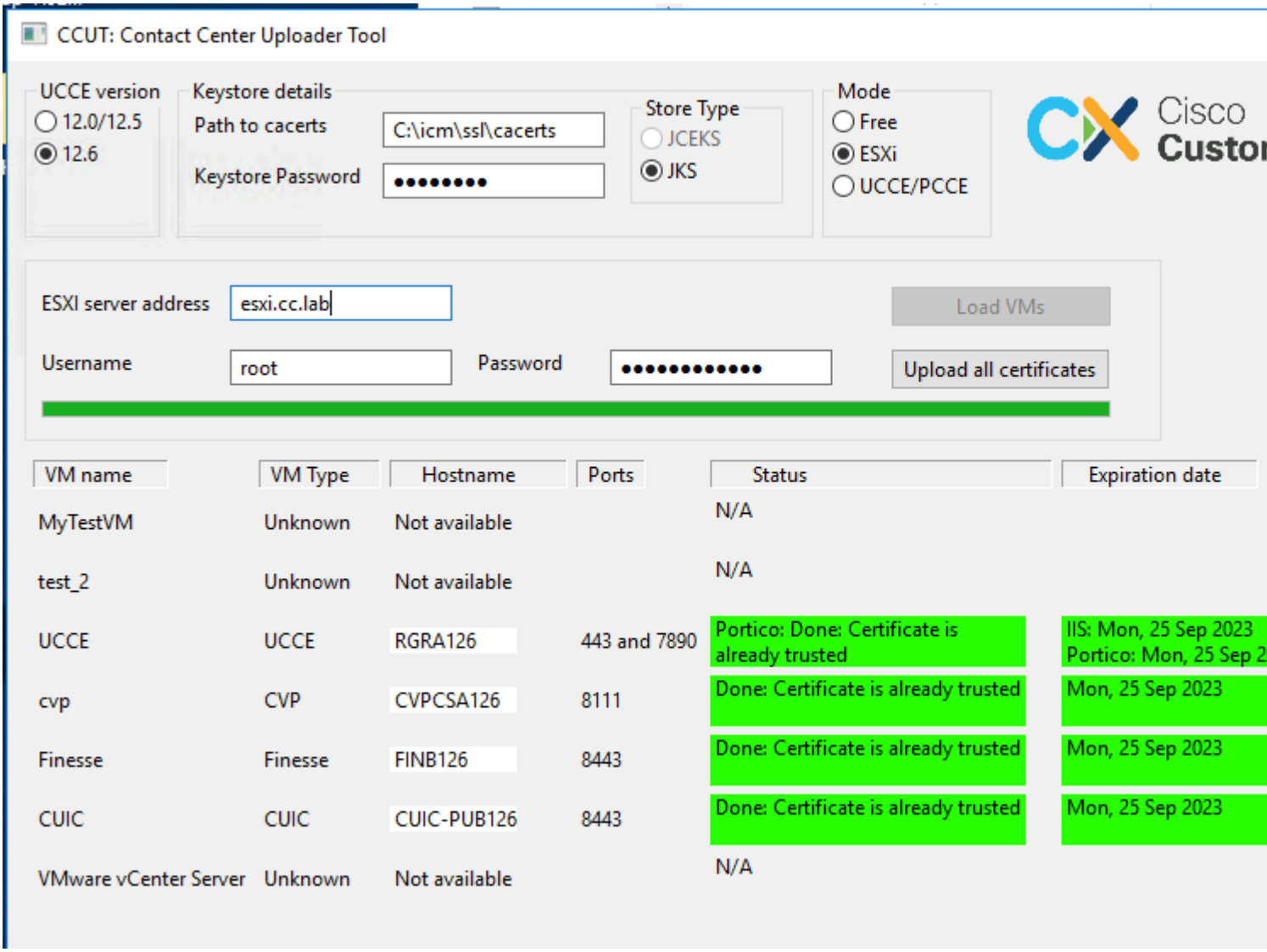
Es fordert den Namen des virtuellen Systems (VM), VM-Anmerkungen und den Hostnamen vom

Gastbetriebssystem an.

VM-Anmerkungen werden verwendet, um den Maschinentyp zu identifizieren.

VmWare-Tools müssen auf VMs ausgeführt werden, andernfalls wird der Hostname nicht eingetragen.

Das Tool im ESXi-Modus ist in der Abbildung dargestellt:



Hinweis: VCenter wird für Verbindungen nicht unterstützt.

Freier Modus

Ein weiterer Modus des Tools ist der **Frei**-Modus.

Es ist nicht erforderlich, dass eine UCCE-Datenbank verfügbar ist, und das Tool kann zum Hochladen von Zertifikaten für CVP oder ECE verwendet werden.

Anwendungsbeispiele:

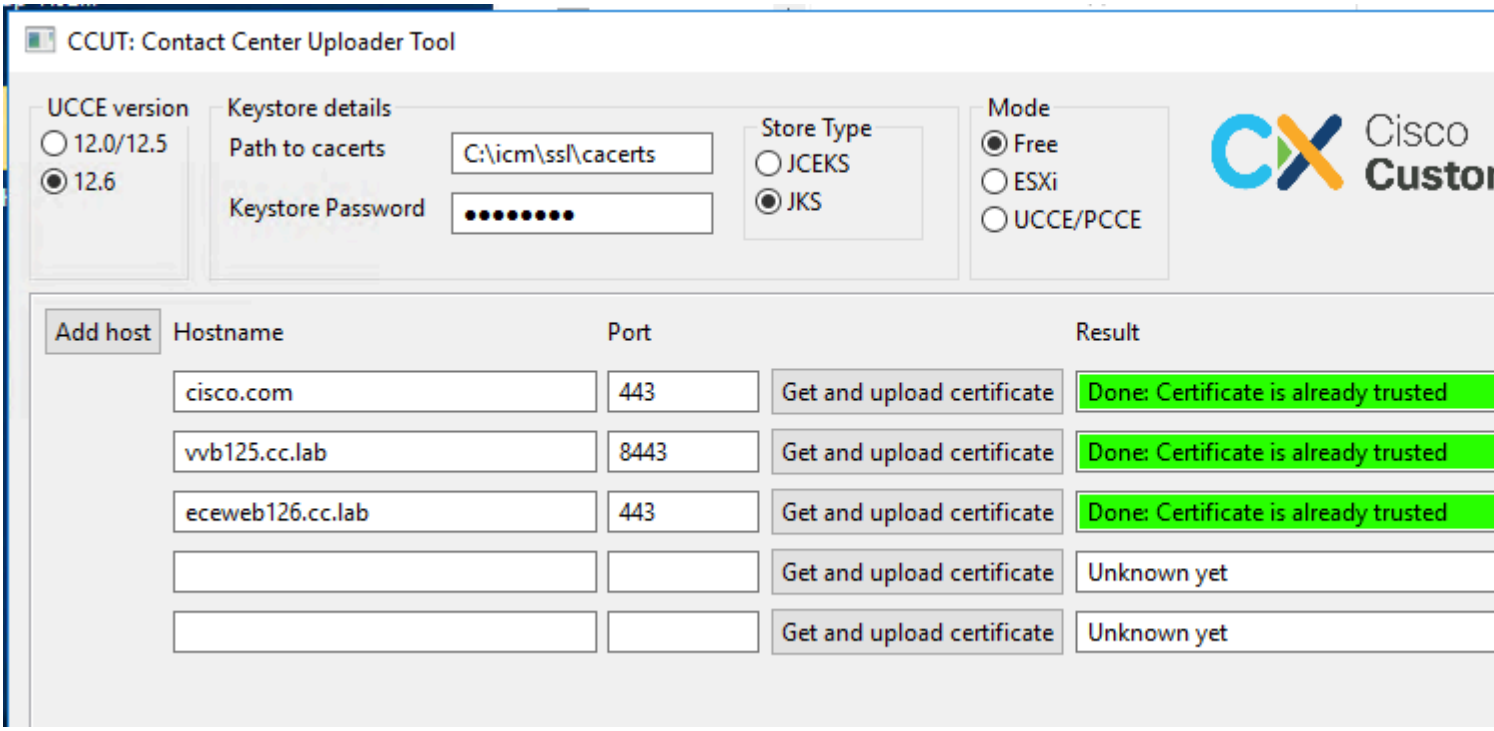
- Holen Sie sich ein Webdienstzertifikat eines Drittanbieters, und laden Sie es auf CVP hoch.

- Abrufen und Hochladen der Zertifikate der Mail-Server auf den ECE-Services-Server.

- Laden Sie Intrusion Detection System (IDS)-Zertifikate auf den ECE-Anwendungsserver hoch.

Hinweis: Das Tool kann aufgrund einiger Einschränkungen keine Zertifikate in die CVP**.keystore**-Datei hochladen.

Ein Beispiel für das Werkzeug im **freien** Modus ist im Bild:



Ausführen des Tools

Laden Sie das Contact Center Uploader Tool herunter.

Extrahieren Sie die heruntergeladene Archivdatei.

Die **Launcher**-Datei enthält Pfade zum Glas und Java.

Aktualisieren Sie den Pfad zu Java und die jar-Datei, wenn erforderlich.

Öffnen Sie die Eingabeaufforderung (cmd) mit Administratorberechtigungen.

Wechseln Sie zum extrahierten Ordner mit dem **Befehl cd**, und führen Sie die Datei **LauncherX86.bat** aus, um das Tool zu starten.

Vorsicht: Sichern Sie immer die Truststore-Datei.

Technische Details

- Das Tool stellt eine Verbindung zum Host her und überprüft, ob das Zertifikat vertrauenswürdig ist. Wenn es nicht vertrauenswürdig ist, wird das Zertifikat hochgeladen.
- Das Zertifikat wird mit dem Alias **util-[hostname]-[port]** hochgeladen, z. B**. util-vvb125.cc.lab-8443**.
- Ein Host kann mehr als ein Zertifikat senden. In diesem Fall lädt das Tool alle diese Zertifikate als

Stamm- und/oder Zwischenpräfixe hoch.

- Das Tool ist mit java 1.8 kompiliert.
- Das Tool stellt standardmäßig über **localhost:1433** eine Verbindung zur Datenbank her.
- Die minimale Bildschirmauflösung beträgt 1024x768. Der Skalierungsmodus wird nicht unterstützt.

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.