

Exchange Certificates with Contact Center Uploader Tool

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Problème](#)

[Solution](#)

[Mode UCCE/PCCE](#)

[Mode ESXi](#)

[Mode libre](#)

[Exécuter l'outil](#)

[Détails techniques](#)

Introduction

Ce document décrit l'outil de téléchargement du centre de contact qui obtient et télécharge des certificats dans la solution Unified Contact Center Enterprise (UCCE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- UCCE version 12.6(1)
- Customer Voice Portal (CVP) version 12.6(1)
- Messagerie instantanée et messagerie d'entreprise (ECE) version 12.6(1)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- UCCE 12.6(1)
- CVP 12.6(1)
- CEE 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. Si votre réseau

est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Dans la solution UCCE/PCCE de 12.x, tous les périphériques sont contrôlés via un panneau de verre unique (SPOG) hébergé sur le serveur principal de la station de travail Admin (AW). En raison de la conformité à la gestion de la sécurité (SRC) dans les versions PCCE 12.X, toutes les communications entre SPOG et les autres serveurs de la solution s'effectuent strictement via le protocole HTTP sécurisé.

Les certificats sont utilisés afin d'assurer une communication sécurisée et transparente entre SPOG et les autres périphériques. Dans un environnement de certificats auto-signés, l'échange de certificats entre les serveurs devient une nécessité. Cet échange de certificat est également nécessaire pour activer les nouvelles fonctionnalités présentes dans les versions 12.5 et 12.6, telles que les licences Smart, Webex Experience Management (WXM) et Customer Virtual Assistant (CVA).

Problème

L'échange de certificats peut être une tâche difficile pour les personnes qui ne connaissent pas le `javakeytool`, en particulier lorsque des certificats en libre-service sont utilisés.


Des actions incorrectes peuvent entraîner des problèmes de configuration et d'intégrité de la solution.

Les certificats peuvent être expirés et leur renouvellement constitue un autre défi.

Solution

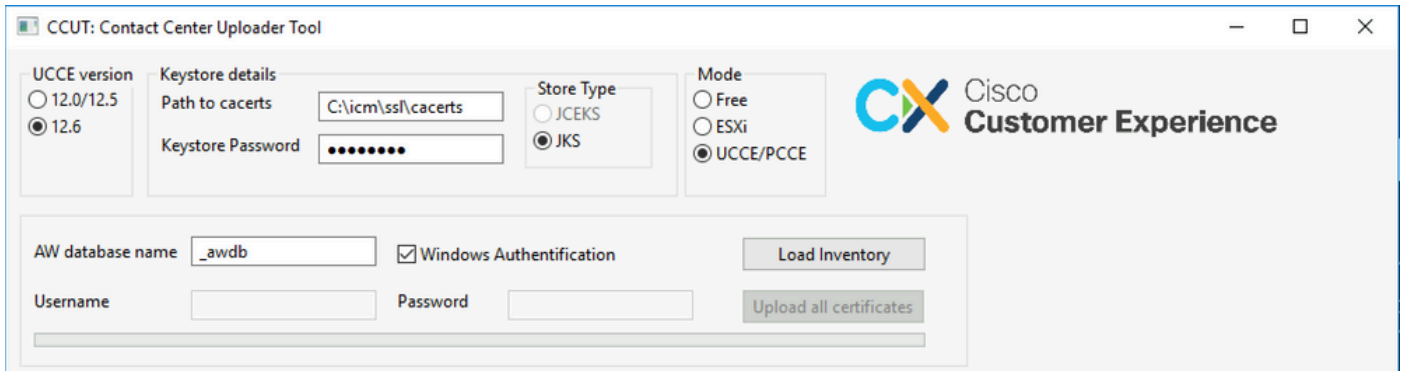
L'article contient un lien vers l'outil Contact Center Uploader Tool (CCUT) écrit en Java qui vous aide dans cette tâche.

L'outil peut se connecter à la base de données UCCE ou à l'hôte ESXi, obtenir les données sur tous les hôtes à partir de là, obtient un certificat de chaque hôte et le télécharge vers le magasin de confiance cacerts java.

 Remarque : l'outil est créé par les ingénieurs du TAC Cisco et il n'y a pas d'assistance officielle. Vous pouvez utiliser ccut@cisco.com pour obtenir des commentaires, poser des questions et résoudre des problèmes.

Mode UCCE/PCCE

La fenêtre d'application principale de l'outil en mode UCCE/PCCE est dans l'image :



- **AW database name:** indiquez le nom de la base de données AW, de l'enregistreur ou de la base de données pcceinventory. Les tables t_Machine... doivent contenir des données. Si l'outil s'exécute sur l'hôte UCCE où le composant de base de données n'est pas installé, le nom du serveur SQL (Structured Query Language) distant peut être ajouté en tant que préfixe au nom de la base de données. Par exemple AWHDS-A\pcce_awdb Ceci s'applique aux machines de passerelle d'accès aux périphériques (PG) ou de routeur.
- **Username et Password** pour l'utilisateur SQL disposant du droit d'accès pour lire les données de la base de données. Vérifiez la **Windows Authentication** pour utiliser l'authentification Windows intégrée au lieu de SQL.
- **UCCE version:** correctif du fichier cacerts dépend de la version installée d'UCCE.
- **Path to cacerts:** Emplacement du fichier cacerts. Dans UCCE 12.6.X, le système utilise C:\icm\ssl\cacerts, UCCE 12.5 utilise le magasin de confiance Java par défaut (%CCE_JAVA_HOME%\lib\security\cacert).
- **Keystore Password:** le mot de passe par défaut pour le cacerts store est changeit.
- **Store Type:** UCCE utilise le type JKS du magasin, tandis que CVP utilise JCEKS.
- **Load Inventory button :** L'outil se connecte à la base de données mentionnée et affiche les données d'inventaire.
- **Upload all certificates button :** le bouton est disponible une fois que l'outil a récupéré les données de la base de données.

Exemple des données chargées dans l'image :

CCUT: Contact Center Uploader Tool

UCCE version: 12.0/12.5 12.6

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

Keystore Password: [REDACTED]

Store Type: JCEKS JKS

Mode: Free ESXi UCCE/PCCE

AW database name: pcce_awdb Windows Authentication

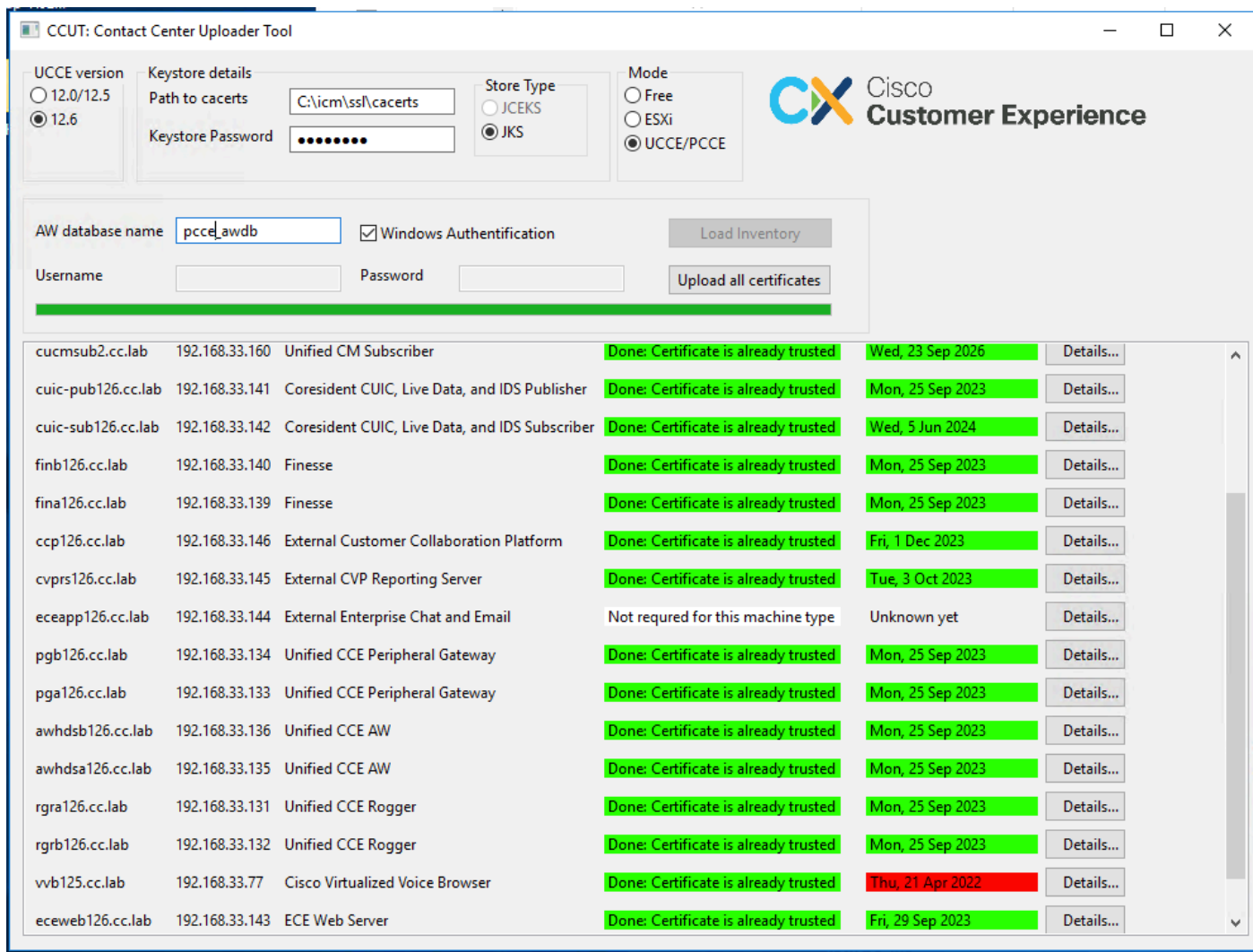
Username: [REDACTED] Password: [REDACTED]

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

Les données d'inventaire se composent de 6 colonnes :

- Nom de l'hôte
- Adresse IP
- Type de machine
- État des données du certificat ou des détails de l'erreur
- Date d'expiration du certificat
- Détails

Les résultats du bouton Upload all Certificates :



Chaque ligne marquée comme verte est un succès.

La ligne rouge ou jaune nécessite votre attention.

Mode ESXi

Le mode ESXi peut être utilisé pour une nouvelle installation PCCE/UCCE lorsque l'inventaire n'est pas encore configuré et que les tables t_Machine... ne contiennent aucune donnée.

L'outil se connecte à l'hôte ESXi et obtient les données sur toutes les machines virtuelles à partir de là.


Il demande le nom de la machine virtuelle (VM), les annotations de la machine virtuelle et le nom d'hôte au système d'exploitation invité.

Les annotations de machine virtuelle permettent d'identifier le type de machine.

Les outils VmWare doivent être exécutés sur les machines virtuelles. Sinon, le nom d'hôte n'est pas renseigné.

L'outil en mode ESXi se trouve dans l'image :

VM name	VM Type	Hostname	Ports	Status	Expiration date	Details...
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 2023	Details...
cvp	CVP	CVPCSA126	8111	Done: Certificate is already trusted	Mon, 25 Sep 2023	Details...
Finesse	Finesse	FINB126	8443	Done: Certificate is already trusted	Mon, 25 Sep 2023	Details...
CUIC	CUIC	CUIC-PUB126	8443	Done: Certificate is already trusted	Mon, 25 Sep 2023	Details...
VMware vCenter Server	Unknown	Not available		N/A		

 Remarque : VCenter n'est pas pris en charge pour les connexions.

Mode libre

Un autre mode de l'outil est le mode Libre.

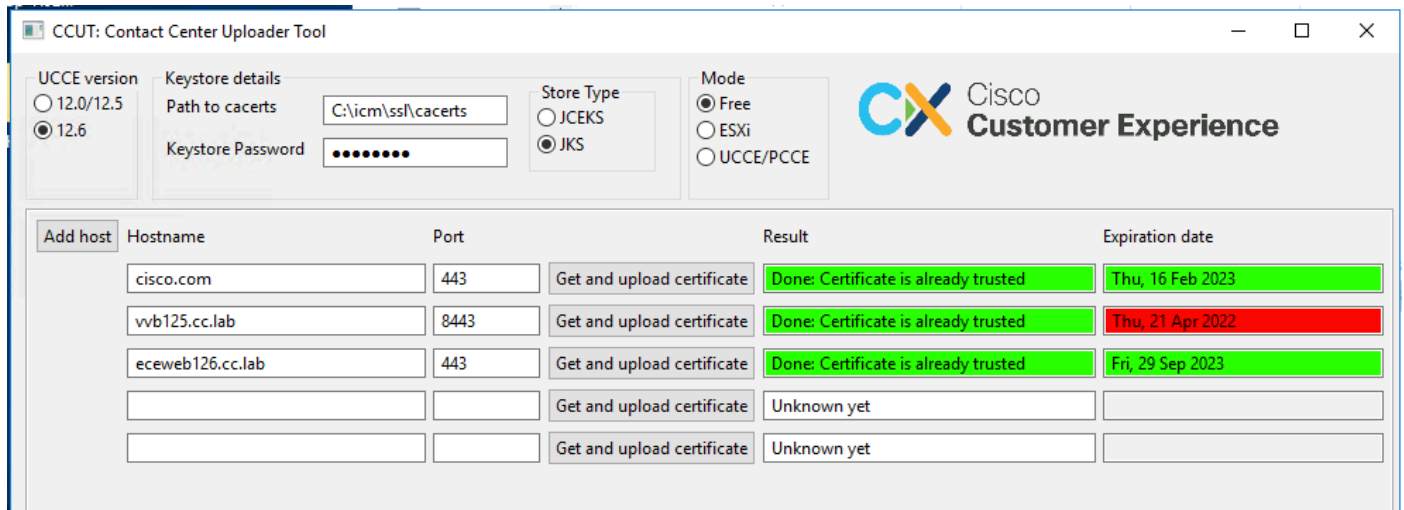
Il n'est pas nécessaire de disposer d'une base de données UCCE et l'outil peut être utilisé pour télécharger des certificats vers CVP ou ECE.

Exemples d'utilisation :

- Obtenez et téléchargez un certificat de service Web tiers vers CVP.
- Obtenir et télécharger les certificats des serveurs de messagerie sur le serveur des services ECE.
- Obtenir et télécharger des certificats IDS (Intrusion Detection System) sur le serveur d'applications ECE.

 Remarque : l'outil ne peut pas télécharger de certificats vers le fichier CVP .keystore en raison de certaines restrictions.

Un exemple de l'outil en mode Libre est dans l'image :



Exécuter l'outil

Téléchargez l'[outil de téléchargement Contact Center](#).

Extrayez le fichier d'archive téléchargé.

Le fichier Launcher contient les chemins d'accès au jar et à Java.

Si nécessaire, mettez à jour le chemin vers Java et le fichier jar.

Ouvrez l'invite de commandes (cmd) avec des autorisations d'administrateur.

Accédez au dossier extrait par la commande cd et exécutez LauncherX86.bat pour démarrer l'outil.

 Attention : effectuez toujours une sauvegarde du fichier du magasin de confiance.

Détails techniques

- L'outil se connecte à l'hôte et vérifie si le certificat est approuvé ou non. S'il n'est pas approuvé, le certificat est téléchargé.
- Le certificat est téléchargé avec l'alias util-[hostname]-[port], par exemple util-vvb125.cc.lab-8443.
- Un hôte peut envoyer plusieurs certificats. Dans ce cas, l'outil télécharge tous ces certificats en tant que préfixes racine et/ou intermédiaires.
- L'outil est compilé avec java 1.8.
- L'outil se connecte à la base de données par localhost:1433 par défaut.
- La résolution d'écran minimale est 1024x768. Le mode évolutif n'est pas pris en charge.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.