

Intercambie certificados con la herramienta Contact Center Uploader

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

[Modo UCCE/PCCE](#)

[Modo ESXi](#)

[Modo libre](#)

[Ejecutar la herramienta](#)

[Detalles técnicos](#)

Introducción

Este documento describe la herramienta Contact Center Uploader Tool que obtiene y carga certificados en la solución Unified Contact Center Enterprise (UCCE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCCE versión 12.6(1)
- Customer Voice Portal (CVP) versión 12.6(1)
- Chat empresarial y correo electrónico (ECE), versión 12.6(1)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- UCCE 12.6(1)
- CVP 12.6(1)
- CEPE 12.6(1)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En la solución UCCE/PCCE de 12.x, todos los dispositivos se controlan mediante un único panel de acceso

(SPOG) alojado en el servidor principal de la estación de trabajo de administración (AW). Debido a la conformidad con la gestión de seguridad (SRC) en las versiones de PCCE 12.X, toda la comunicación entre SPOG y otros servidores de la solución se realiza estrictamente a través del protocolo HTTP seguro.

Los certificados se utilizan para lograr una comunicación segura y sin problemas entre SPOG y los otros dispositivos. En un entorno de certificados autofirmado, el intercambio de certificados entre los servidores se convierte en una obligación. Este intercambio de certificados también es necesario para habilitar las nuevas funciones presentes en las versiones 12.5 y 12.6, como Smart Licensing, Webex Experience Management (WXM) y Customer Virtual Assistant (CVA).

Problema

El intercambio de certificados puede ser una tarea difícil para las personas que no están familiarizadas con el `javakeytool`, especialmente cuando se utilizan certificados de autoservicio.

Las acciones incorrectas pueden causar problemas con la configuración de la solución y su estado.

Los certificados pueden haber caducado y su renovación es otro reto.

Solución

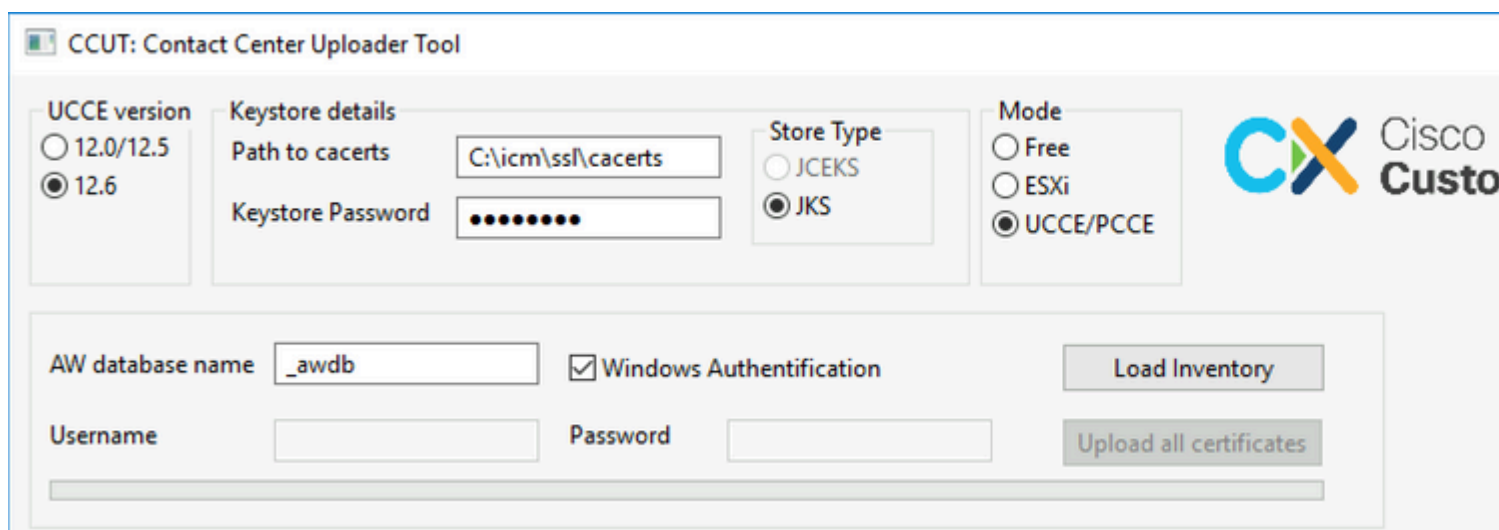
El artículo contiene un vínculo a la herramienta Contact Center Uploader Tool (CCUT) escrita en Java que le ayuda con la tarea.

La herramienta puede conectarse a la base de datos de UCCE o al host de ESXi, obtener los datos de todos los hosts desde allí, obtener un certificado de cada host y cargarlo en el almacén de confianza de `cacerts` de java.

Nota: La herramienta la crean los ingenieros del TAC de Cisco y no hay asistencia oficial. Puede utilizar ccut@cisco.com para comentarios, preguntas y problemas.

Modo UCCE/PCCE

La ventana principal de la aplicación de la herramienta en el modo **UCCE/PCCE** se encuentra en la imagen:



The screenshot shows the main configuration window of the CCUT application. The title bar reads "CCUT: Contact Center Uploader Tool". The interface is divided into several sections:

- UCCE version:** Radio buttons for "12.0/12.5" and "12.6". "12.6" is selected.
- Keystore details:** A text field for "Path to cacerts" containing "C:\icm\ssl\cacerts" and a password field for "Keystore Password" with masked characters.
- Store Type:** Radio buttons for "JCEKS" and "JKS". "JKS" is selected.
- Mode:** Radio buttons for "Free", "ESXi", and "UCCE/PCCE". "UCCE/PCCE" is selected.
- AW database name:** A text field containing "_awdb".
- Authentication:** A checked checkbox for "Windows Authentication".
- Buttons:** "Load Inventory" and "Upload all certificates".
- Username and Password:** Text fields for "Username" and "Password".

The Cisco logo and "Custo" are visible in the top right corner.

- **AW database name:** proporcione el nombre de la base de datos AW, Logger o **pcceinventario**. Debe

haber datos en las tablas **t_Machine...**

Si la herramienta se ejecuta en el host de UCCE en el que no está instalado el componente de base de datos, el nombre del servidor SQL (Lenguaje de consulta estructurado) remoto se puede agregar como prefijo al nombre de la base de datos.

Por ejemplo, **AWHDS-A\pcce_awdb**

Esto se aplica a las máquinas con puertos de enlace periféricas (PG) o ROUTER.

- **Username y Password** para que el usuario SQL con derecho de acceso lea los datos de la base de datos. Compruebe el **Windows Authentication** para utilizar la autenticación de windows integrada en lugar de SQL.
- **UCCE version:** La revisión del **archivo cacerts** depende de la versión de UCCE instalada.
- **Path to cacerts:** Ubicación del archivo **cacerts**. En UCCE 12.6.X, el sistema utiliza **C:\icm\ssl\cacerts**, UCCE 12.5 utiliza el almacén de confianza predeterminado de Java (**%CCE_JAVA_HOME%\lib\security\cacert**).
- **Keystore Password:** la contraseña predeterminada para el almacén **cacerts** es **changeit**.
- **Store Type:** UCCE utiliza el tipo **JKS** del almacén, mientras que CVP utiliza **JCEKS**.
- **Load Inventory botón:** La herramienta se conecta a la base de datos mencionada y muestra los datos de inventario.
- **Upload all certificates button:** El botón está disponible después de que la herramienta obtenga los datos de la base de datos.

Ejemplo de los datos cargados en la imagen:

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: pccel_awddb Windows Authentication

Username: Password:

Hostname	IP-address	Machine Type	Status	Expiration
cvpcs126.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
fin126.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

Los datos de inventario constan de 6 columnas:

- Hostname
- ip-address
- Tipo de máquina
- Estado de los datos del certificado o detalles del error
- Fecha de vencimiento del certificado
- Detalles

Los resultados del botón **Upload all Certificates**:

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: pccel_awddb Windows Authentication Load Inventory

Username: Password: Upload all certificates

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 required for this machine type	Unknown y
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
ecweb126.cc.lab	192.168.33.143	ECE Web Server	Done: Certificate is already trusted	Fri, 29 Sep 2

Cada fila marcada como verde es un éxito.

La fila roja o amarilla requiere atención.

Modo ESXi

El modo ESXi se puede utilizar para la instalación nueva de PCCE/UCCE cuando el inventario no está configurado y las tablas **t_Machine...** no contienen datos.

La herramienta se conecta al host ESXi y obtiene los datos de todas las máquinas virtuales desde allí.

Solicita el nombre de la máquina virtual (VM), las anotaciones de VM y el nombre de host del sistema

operativo invitado.

Las anotaciones de VM se utilizan para identificar el tipo de máquina.

Las herramientas de VMware deben ejecutarse en las VM; de lo contrario, el nombre de host no se rellena.

La herramienta del modo ESXi se muestra en la imagen:

CCUT: Contact Center Uploader Tool

UCCE version: 12.0/12.5 12.6

Keystore details: Path to cacerts: C:\vicm\ssl\cacerts, Keystore Password: [masked]

Store Type: JCEKS JKS

Mode: Free ESXi UCCE/PCCE

ESXi server address: esxi.cc.lab, Username: root, Password: [masked]

Buttons: Load VMs, Upload all certificates

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 2023
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	

Nota: VCenter no es compatible con las conexiones.

Modo libre

Otro modo de la herramienta es el modo **Libre**.

No es necesario disponer de una base de datos de UCCE y la herramienta se puede utilizar para cargar certificados en CVP o ECE.

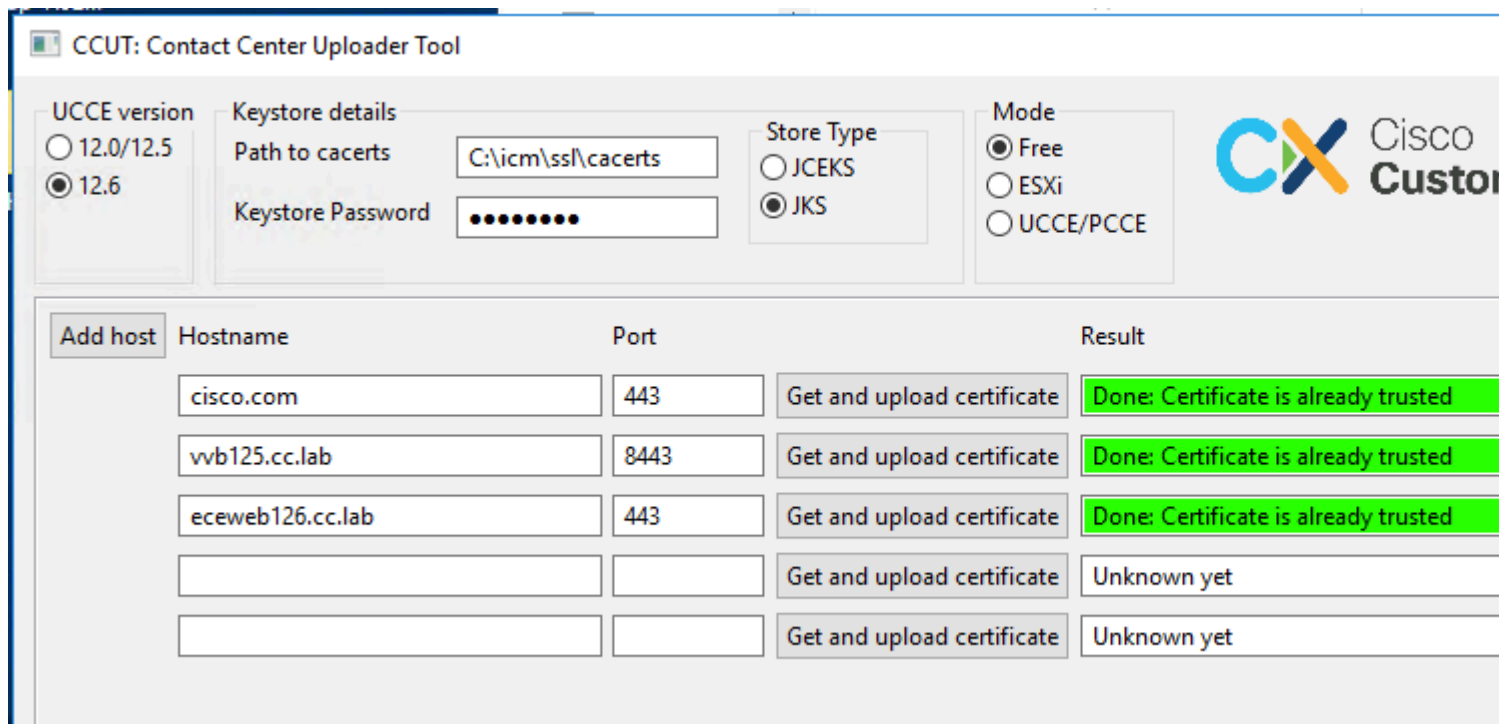
Ejemplo de casos prácticos:

- Obtenga y cargue un certificado de servicio web de terceros en CVP.
- Obtener y cargar certificados de servidores de correo en el servidor de servicios ECE.

- Obtener y cargar certificados del Sistema de detección de intrusiones (IDS) en el servidor de aplicaciones ECE.

Nota: la herramienta no puede cargar certificados en el archivo **.keystore de CVP** debido a algunas restricciones.

Un ejemplo de la herramienta en el modo **Libre** está en la imagen:



Ejecutar la herramienta

Descargue la [herramienta Contact Center Uploader](#).

Extraiga el archivo descargado.

El archivo **Launcher** contiene rutas de acceso al jar y Java.

Actualice la ruta a Java y al archivo jar si es necesario.

Abra el símbolo del sistema (cmd) con permisos de administrador.

Vaya a la carpeta extraída por el comando **cd** y ejecute **LauncherX86.bat** para iniciar la herramienta.

Precaución: realice siempre una copia de seguridad del archivo del almacén de confianza.

Detalles técnicos

- La herramienta se conecta al host y comprueba si el certificado es de confianza o no. Si no es de confianza, se carga el certificado.
- El certificado se carga con el alias **util-[hostname]-[port]**, por ejemplo **util-vvb125.cc.lab-8443**.
- Un host puede enviar varios certificados. En este caso, la herramienta carga todos estos certificados como prefijos raíz y/o intermedios.

- La herramienta se compila con java 1.8.
- La herramienta se conecta a la base de datos por **localhost:1433** de forma predeterminada.
- La resolución de pantalla mínima es 1024x768. No se admite el modo escalado.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).