

Certificati di Exchange con lo strumento Contact Center Uploader

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Soluzione](#)

[Modalità UCCE/PCCE](#)

[Modalità ESXi](#)

[Modalità gratuita](#)

[Esecuzione dello strumento](#)

[Dettagli tecnici](#)

Introduzione

Questo documento descrive lo strumento Contact Center Uploader che ottiene e carica certificati nella soluzione Unified Contact Center Enterprise (UCCE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Nella soluzione UCCE/PCCE 12.x tutti i dispositivi sono controllati tramite Single Pane of Glass (SPOG) che è ospitato nel server principale Admin Workstation (AW). A causa della conformità SRC (Security-Management-Compliance) delle versioni PCCE 12.X, tutte le comunicazioni tra SPOG e gli altri server della soluzione avvengono esclusivamente tramite il protocollo HTTP protetto.

I certificati vengono utilizzati per garantire una comunicazione sicura e senza problemi tra SPOG e gli altri dispositivi. In un ambiente con certificati autofirmati, lo scambio di certificati tra i server diventa un must. Questo scambio di certificati è inoltre necessario per abilitare le nuove funzionalità presenti nelle versioni 12.5 e 12.6, ad esempio Smart Licensing, Webex Experience Management (WXM) e Customer Virtual Assistant (CVA).

Problema

Lo scambio di certificati può essere un compito difficile per gli utenti che non hanno familiarità con `Javakeytool`, in particolare quando si utilizzano certificati self-service.

Azioni errate possono causare problemi di configurazione e integrità della soluzione.

I certificati possono essere scaduti e il loro rinnovo è un'altra sfida.

Soluzione

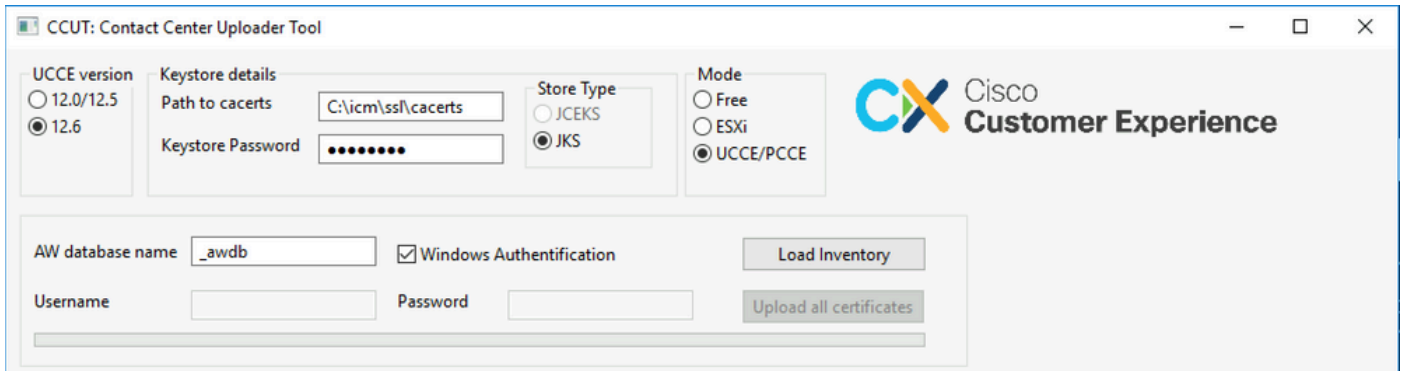
L'articolo contiene un collegamento allo strumento CCUT (Contact Center Uploader Tool) scritto in Java che consente di eseguire l'operazione.

Lo strumento può connettersi al database UCCE o all'host ESXi, ottenere i dati su tutti gli host da lì, ottenere un certificato da ogni host e caricarlo nell'archivio di attendibilità di Java cacerts.

 Nota: questo strumento è stato creato dai tecnici TAC di Cisco e non è disponibile alcun supporto ufficiale. È possibile utilizzare ccut@cisco.com per commenti, domande e problemi.

Modalità UCCE/PCCE

La finestra principale dell'applicazione dello strumento in modalità UCCE/PCCE è nella figura:



- **AW database name:** fornire il nome del database AW, del logger o del database pcceinventory. È necessario che siano presenti dati nelle tabelle t_Machine...
Se lo strumento viene eseguito sull'host UCCE in cui non è installato il componente di database, è possibile aggiungere il nome del server SQL (Structured Query Language) remoto come prefisso al nome del database.
Ad esempio, AWHDS-A\pcce_awdb
Questa procedura è valida per i gateway periferici (PG) o per i computer ROUTER.
- **Username e Password** per l'utente SQL con diritto di accesso per la lettura dei dati del database. Controllare la **Windows Authentication** per utilizzare l'autenticazione integrata di windows anziché SQL.
- **UCCE version:** patch al file cacerts dipende dalla versione UCCE installata.
- **Path to cacerts:** Percorso del file cacerts. In UCCE 12.6.X il sistema utilizza C:\icm\ssl\cacerts, UCCE 12.5 utilizza il truststore Java predefinito (%CCE_JAVA_HOME%\lib\security\cacert).
- **Keystore Password:** la password predefinita per l'archivio cacerts è changeit.
- **Store Type:** UCCE utilizza il tipo JKS dell'archivio, mentre CVP utilizza JCEKS.
- **Load Inventory** pulsante: lo strumento si connette al database indicato e visualizza i dati di inventario.
- **Upload all certificates** button: il pulsante è disponibile dopo che lo strumento ha ottenuto i dati dal database.

Esempio dei dati caricati nell'immagine:

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: Windows Authentication

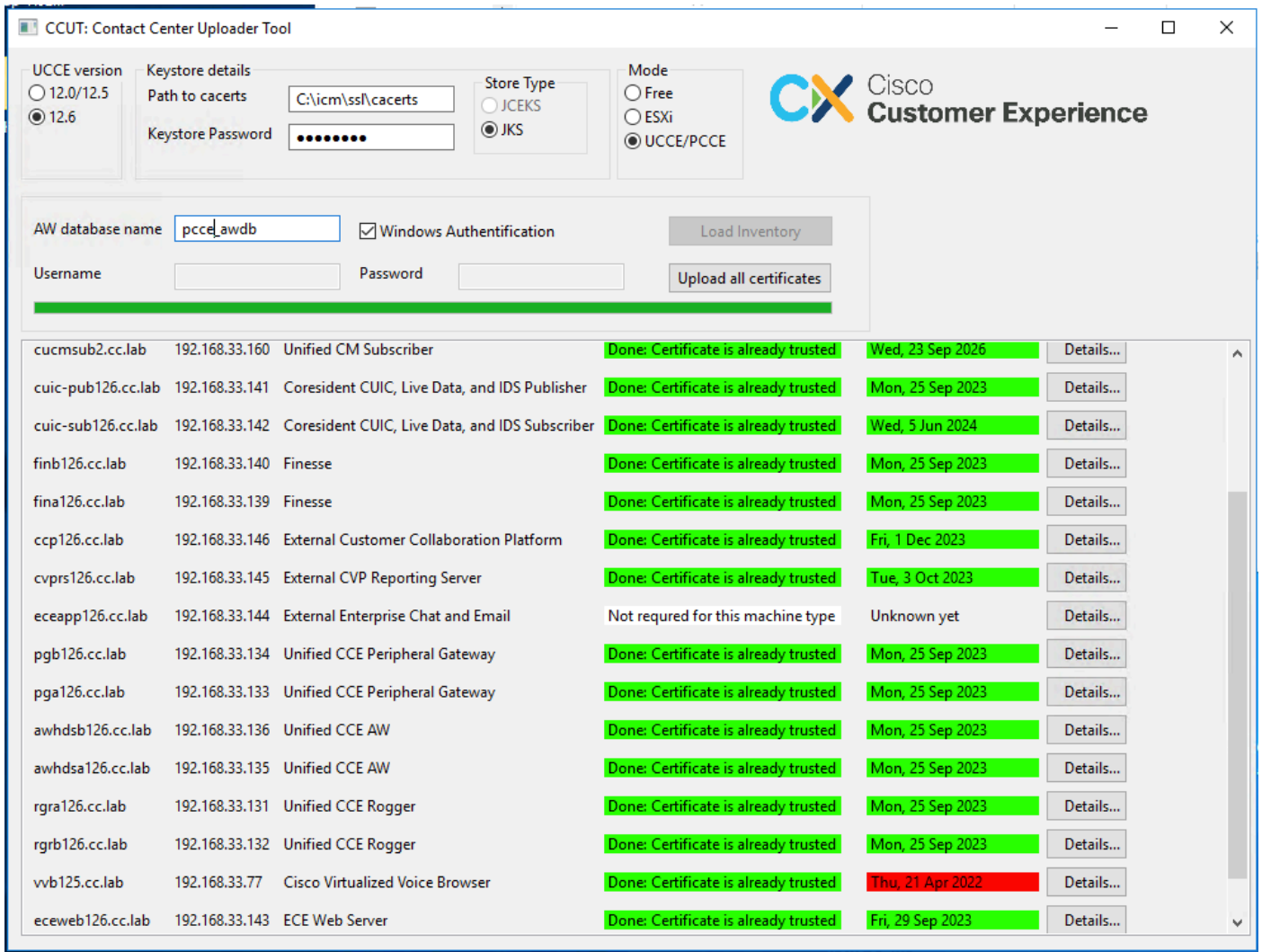
Username: Password:

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..."/>
cuc-pub126.cc.lab	192.168.33.141	Coresident CUIC, Live Data, and IDS Publisher	Unknown yet	Unknown yet	<input type="button" value="Details..."/>
cuc-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..."/>

I dati di inventario sono composti da 6 colonne:

- Nome host
- Indirizzo-IP
- Tipo di computer
- Stato dei dati del certificato o dettagli dell'errore
- Data di scadenza del certificato
- Dettagli

I risultati restituiti dal pulsante Carica tutti i certificati sono:



Ogni riga contrassegnata come verde è un successo.

La riga rossa o gialla richiede attenzione.

Modalità ESXi

La modalità ESXi può essere utilizzata per l'installazione di aggiornamenti PCCE/UCCE quando Inventory non è ancora configurato e le tabelle t_Machine... non contengono dati.

Lo strumento si connette all'host ESXi e da lì ottiene i dati relativi a tutte le macchine virtuali.

Richiede il nome della macchina virtuale (VM), le annotazioni della macchina virtuale e il nome host dal sistema operativo guest.

Le annotazioni della macchina virtuale vengono utilizzate per identificare il tipo di macchina.

Gli strumenti VmWare devono essere eseguiti sulle VM, altrimenti il nome host non viene popolato.

Lo strumento in modalità ESXi è nell'immagine:

CCUT: Contact Center Uploader Tool

UCCE version: 12.0/12.5 12.6

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

Store Type: JCEKS JKS

Mode: Free ESXi UCCE/PCCE

ESXI server address: esxi.cc.lab

Username: root Password: [masked]

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		

Nota: VCenter non è supportato per le connessioni.

Modalità gratuita

Un'altra modalità dello strumento è la modalità Libero.

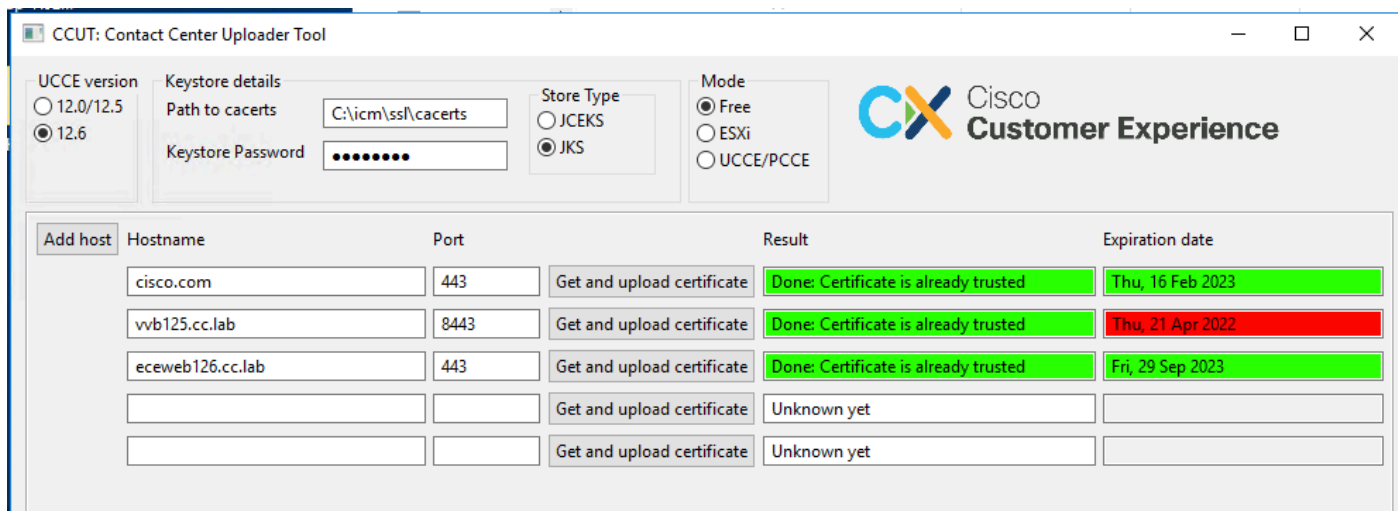
Non è necessario disporre di un database UCCE e lo strumento può essere utilizzato per caricare qualsiasi certificato in CVP o ECE.

Esempi di casi di utilizzo:

- Ottenere e caricare certificati di servizi Web di terze parti su CVP.
- Ottenere e caricare i certificati dei server di posta nel server di servizi ECE.
- Ottenere e caricare i certificati Intrusion Detection System (IDS) sul server applicazioni ECE.

Nota: lo strumento non può caricare certificati nel file CVP.keystore a causa di alcune restrizioni.

Un esempio dello strumento nella modalità Libero è l'immagine:



Esecuzione dello strumento

Scarica [lo strumento di caricamento di Contact Center](#).


Estrarre il file di archivio scaricato.

Il file Launcher contiene i percorsi di jar e Java.

Se necessario, aggiornare il percorso di Java e del file jar.

Aprire il prompt dei comandi (cmd) con autorizzazioni di amministratore.

Andare alla cartella estratta con il comando cd ed eseguire il file LauncherX86.bat per avviare lo strumento.

 **Attenzione:** eseguire sempre un backup del file dell'archivio attendibile.

Dettagli tecnici

- Lo strumento si connette all'host e verifica se il certificato è attendibile o meno. Se non è attendibile, il certificato viene caricato.
- Il certificato viene caricato con l'alias util-[nome host]-[porta], ad esempio util-vvb125.cc.lab-8443.
- Un host può inviare più certificati. In questo caso, lo strumento carica tutti questi certificati come prefissi radice e/o intermedi.
- Lo strumento viene compilato con Java 1.8.
- Per impostazione predefinita, lo strumento si connette al database mediante localhost:1433.
- La risoluzione minima dello schermo è 1024x768. Modalità ridimensionata non supportata.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).