Certificati autofirmati di Exchange in una soluzione PCCE 12.6

Sommario

Introduzione

Questo documento descrive come scambiare certificati autofirmati in una soluzione Cisco Packaged Contact Center Enterprise (PCCE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PCCE release 12.6(2)
- Customer Voice Portal (CVP) versione 12.6(2)
- Virtualized Voice Browser (VB) 12.6(2)
- Admin Workstation/Administration Date Server (AW/ADS) 12.6(2)

- Server Cisco Unified Intelligence (CUIC)
- Customer Collaboration Platform (CCP) 12.6(2)
- Enterprise Chat and Email (ECE) 12.6(2)

Componenti usati

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

- PCCE 12.6(2)
- CVP 12.6(2)

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.

Introduzione

Nella soluzione PCCE a partire dalla versione 12.x, tutti i dispositivi sono controllati tramite Single Pane of Glass (SPOG) che è ospitato nel server AW principale. A causa della conformità alla gestione della sicurezza (SRC) della versione PCCE 12.5(1), 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 è un requisito imprescindibile.

Procedura

Si tratta dei componenti da cui vengono esportati i certificati autofirmati e dei componenti in cui è necessario importare i certificati autofirmati.

(i) Tutti i server AW/ADS: questi server richiedono un certificato da:

- Piattaforma Windows
  - ICM: Router and Logger(Rogger){A/B}, Peripheral Gateway (PG){A/B}, tutti i server AW/ADS e ECE.

Nota: sono necessari IIS e Diagnostic Framework Portico (DFP).

  - CVP: server CVP, server di reporting CVP.

    Nota: è necessario un certificato WSM (Web Service Management) da tutti i server. I certificati devono essere con il nome di dominio completo (FQDN).

- Piattaforma VOS: Cloud Connect, Cisco Virtualized Voice Browser (VB), Cisco Unified

Communication Manager (CUCM), Finesse, Cisco Unified Intelligence Center (CUIC), Live Data (LD), Identity Server (IDS) e altri server applicabili.

(ii) Router \ Server di registrazione: Questi server richiedono un certificato da:

- Piattaforma Windows: certificato IIS per tutti i server AW/ADS.

(iii) Server PG: questi server richiedono un certificato da:

- Piattaforma Windows: certificato IIS per tutti i server AW/ADS.
- Piattaforma VOS: editore CUCM (solo server PG CUCM); Cloud Connect e CCP (solo server PG MR).

Nota: è necessario per scaricare il client JTAPI dal server CUCM.

(iv) Server CVP: questi server richiedono un certificato da

- Piattaforma Windows: certificato IIS per tutti i server ADS
- Piattaforma VOS: server Cloud Connect, server VB.

(v) Server di report CVP: questo server richiede un certificato da:

- Piattaforma Windows: certificato IIS per tutti i server ADS

(vi) Server VB: questo server richiede un certificato da:

- Piattaforma Windows: certificato IIS per tutti i server ADS, certificato VXML dal server CVP e certificato del server chiamante dal server CVP
- Piattaforma VOS: server Cloud Connect.

I passaggi necessari per lo scambio efficace dei certificati autofirmati nella soluzione sono suddivisi in tre sezioni.

Sezione 1: Scambio di certificati tra server CVP e server ADS.

Sezione 2: Scambio di certificati tra applicazioni della piattaforma VOS e server ADS.

Sezione 3: Scambio di certificati tra logger, PG e server ADS.

Sezione 1: Scambio di certificati tra server CVP e ADS

Per completare correttamente questo scambio, è necessario eseguire le seguenti operazioni:

Passaggio 1. Esporta certificati WSM di server CVP.

Passaggio 2. Importare il certificato WSM dei server CVP nei server ADS.

Passaggio 3. Esporta certificato server ADS.

Passaggio 4. Importa il server ADS nei server CVP e nel server di report CVP.

Passaggio 1. Esporta certificati server CVP

Prima di esportare i certificati dai server CVP, è necessario rigenerare i certificati con il nome di dominio completo (FQDN) del server. In caso contrario, è possibile che si verifichino problemi con alcune funzionalità, ad esempio Smart Licensing, Virtual Agent Voice (VAV) e la sincronizzazione CVP con SPOG.

⚠ Attenzione: prima di iniziare, eseguire questa operazione:
1. Aprire una finestra di comando come amministratore.
2. Per la versione 12.6.2, per identificare la password del keystore, passare alla cartella %CVP_HOME%\bin ed eseguire il file DecryptKeystoreUtil.bat.
3. Per la versione 12.6.1, per identificare la password del keystore, eseguire il comando more %CVP_HOME%\conf\security.properties.
4. Questa password è necessaria per eseguire i comandi keytool.
5. Dalla directory %CVP_HOME%\conf\security\, eseguire il comando copy .keystore backup.keystore.

✎ Nota: è possibile semplificare i comandi utilizzati in questo documento utilizzando il parametro keytool -storepass. Per tutti i server CVP, fornire la password dello strumento chiave identificata. Per i server ADS la password predefinita è: changeit

---

Per rigenerare il certificato sui server CVP, eseguire i seguenti passaggi:

(i) Elencare i certificati nel server

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list
```

✎ Nota: i server CVP dispongono dei certificati autofirmati wsm_certificate, vxml_certificate, callserver_certificate. Se si utilizza il parametro -v dello strumento chiave, è possibile visualizzare informazioni più dettagliate su ogni certificato. È inoltre possibile aggiungere il simbolo ">" alla fine del comando keytool.exe list per inviare l'output a un file di testo, ad esempio: > test.txt

---

(ii) Eliminare i vecchi certificati autofirmati

Server CVP: comandi per eliminare i certificati autofirmati:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias vxml_certificate
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias callserver_certificate
```

Server di report CVP: comandi per eliminare i certificati autofirmati:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias callserver_certificate
```

Nota: i server di report CVP dispongono dei certificati autofirmati wsm_certificate, callserver_certificate.

(iii) Generare i nuovi certificati autofirmati con il nome FQDN del server

Server CVP

Comando per generare il certificato autofirmato per WSM:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Nota: per impostazione predefinita, i certificati vengono generati per due anni. Utilizzare -valid XXXX per impostare la data di scadenza per la rigenerazione dei certificati. In caso contrario, i certificati saranno validi per 90 giorni e dovranno essere firmati da una CA prima di questo periodo. Per la maggior parte di questi certificati, 3-5 anni devono essere un periodo di convalida ragionevole.

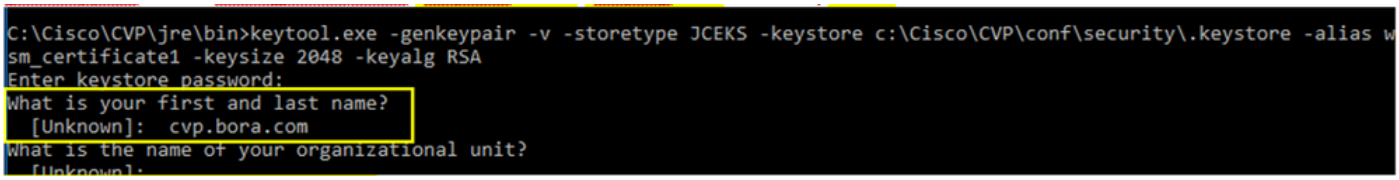
Di seguito sono riportati alcuni input di validità standard:

Un anno	365
Due anni	730
Tre anni	1095
Quattro anni	1460

Cinque anni	1895
Dieci anni	3650

⚠ Attenzione: da 12.5 i certificati devono essere SHA 256, Key Size 2048 e encryption Algorithm RSA, utilizzare questi parametri per impostare i seguenti valori: -keyalg RSA e -keysize 2048. È importante che i comandi del keystore CVP includano il parametro -storetype JCEKS. In caso contrario, il certificato, la chiave o, peggio, il keystore potrebbe danneggiarsi.

Specificare il nome di dominio completo (FQDN) del server, alla domanda qual è il nome e il cognome?



Rispondere alle seguenti domande:

Qual è il nome dell'unità organizzativa?

[Sconosciuto]: <specificare OU>

Qual è il nome dell'organizzazione?

[Sconosciuto]: <specificare il nome dell'organizzazione>

Indicare il nome della città o della località.

[Sconosciuto]: <specificare il nome della città/località>

Qual è il nome della provincia?

[Sconosciuto]: <specificare il nome della provincia>

Qual è il codice paese di due lettere per questo apparecchio?

[Sconosciuto]: <specifica il codice paese a due lettere>

Specificare yes per i due input successivi.

Eseguire la stessa procedura per vxml_certificate e callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias vxml_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Riavviare il server di chiamata CVP.

Server di reporting CVP

Comando per generare i certificati autofirmati per WSM:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Specificare il nome di dominio completo (FQDN) del server per la query che cos'è il nome e il cognome e continuare con gli stessi passaggi eseguiti con i server CVP.

Eseguire la stessa procedura per callserver_certificate:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

Riavviare i server di report.

(iv) Esportare wsm_Certificate da CVP e server di report

a) Esportare il certificato WSM da ciascun server CVP in una posizione temporanea e rinominare il certificato con il nome desiderato. È possibile rinominarlo come wsmcsX.crt. Sostituire "X" con il nome host del server. Ad esempio, wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt.

Comando per esportare i certificati autofirmati:

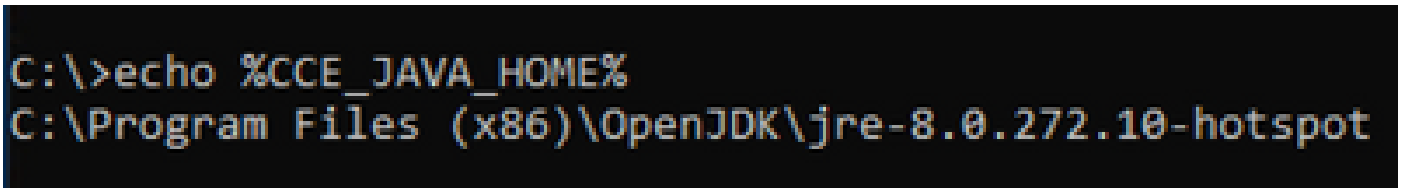
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b) Copiare il certificato dal percorso %CVP_HOME%\conf\security\wsm.crt, rinominarlo in wsmcsX.crt e spostarlo in una cartella temporanea sul server ADS.

Passaggio 2. Importa certificato WSM server CVP in server ADS

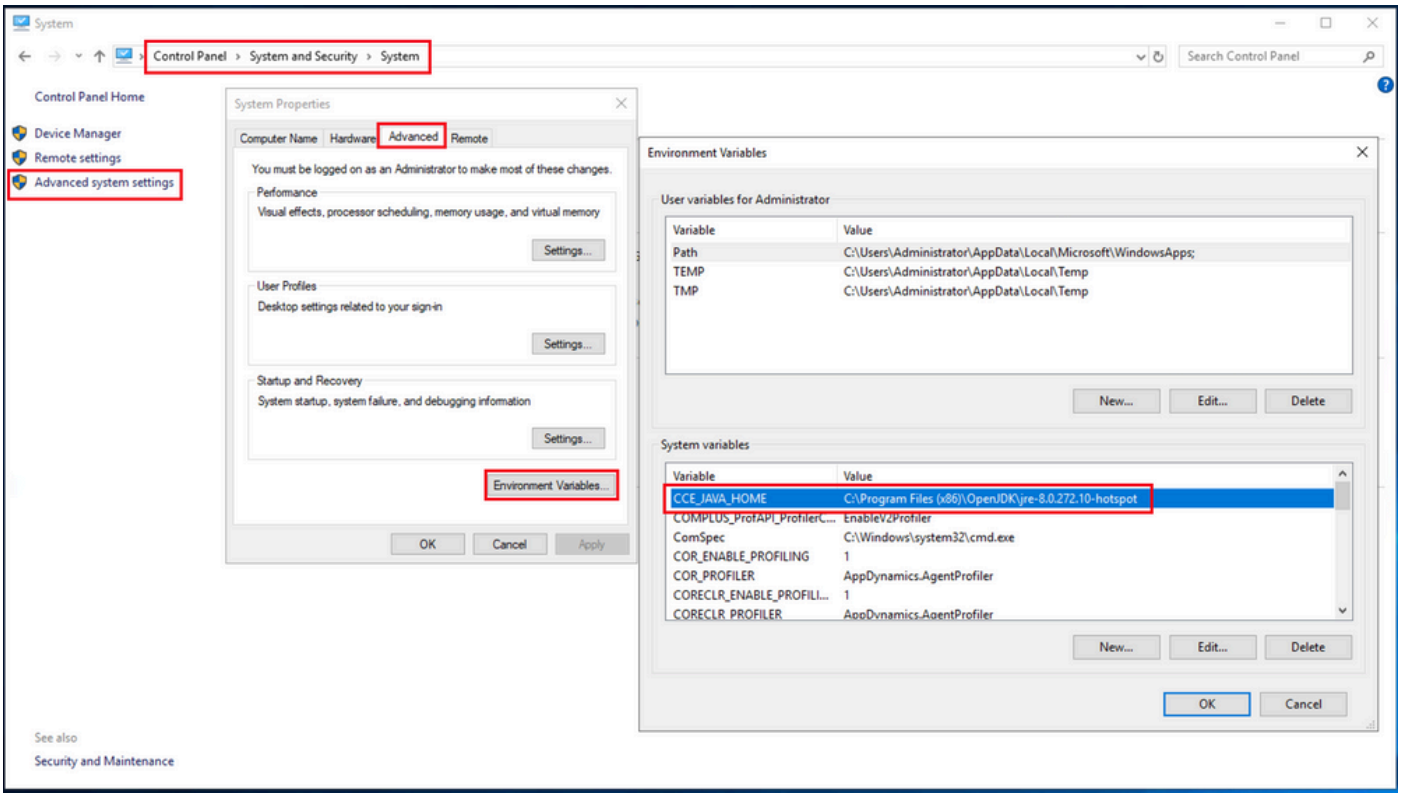
Per importare il certificato nel server ADS è necessario utilizzare lo strumento chiave che fa parte del set di strumenti java. Ci sono due modi per trovare il percorso della java home in cui è ospitato questo strumento.

(i) Comando CLI > echo %CCE_JAVA_HOME%



percorso home java

(ii) Manualmente tramite Impostazioni di sistema avanzate, come mostrato nell'immagine.



Variabili di ambiente

In PCCE 12.6 il percorso predefinito di OpenJDK è C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

Comandi per importare i certificati autofirmati:

```
cd %CCE_JAVA_HOME%\bin
keytool.exe -import -file C:\Temp\certs\wsmcsX.crt -alias {fqdn_of_CVP} -keystore {ICM install directory}\ssl\cacerts
```

Nota: ripetere i comandi per ogni CVP nella distribuzione ed eseguire la stessa operazione su altri server ADS

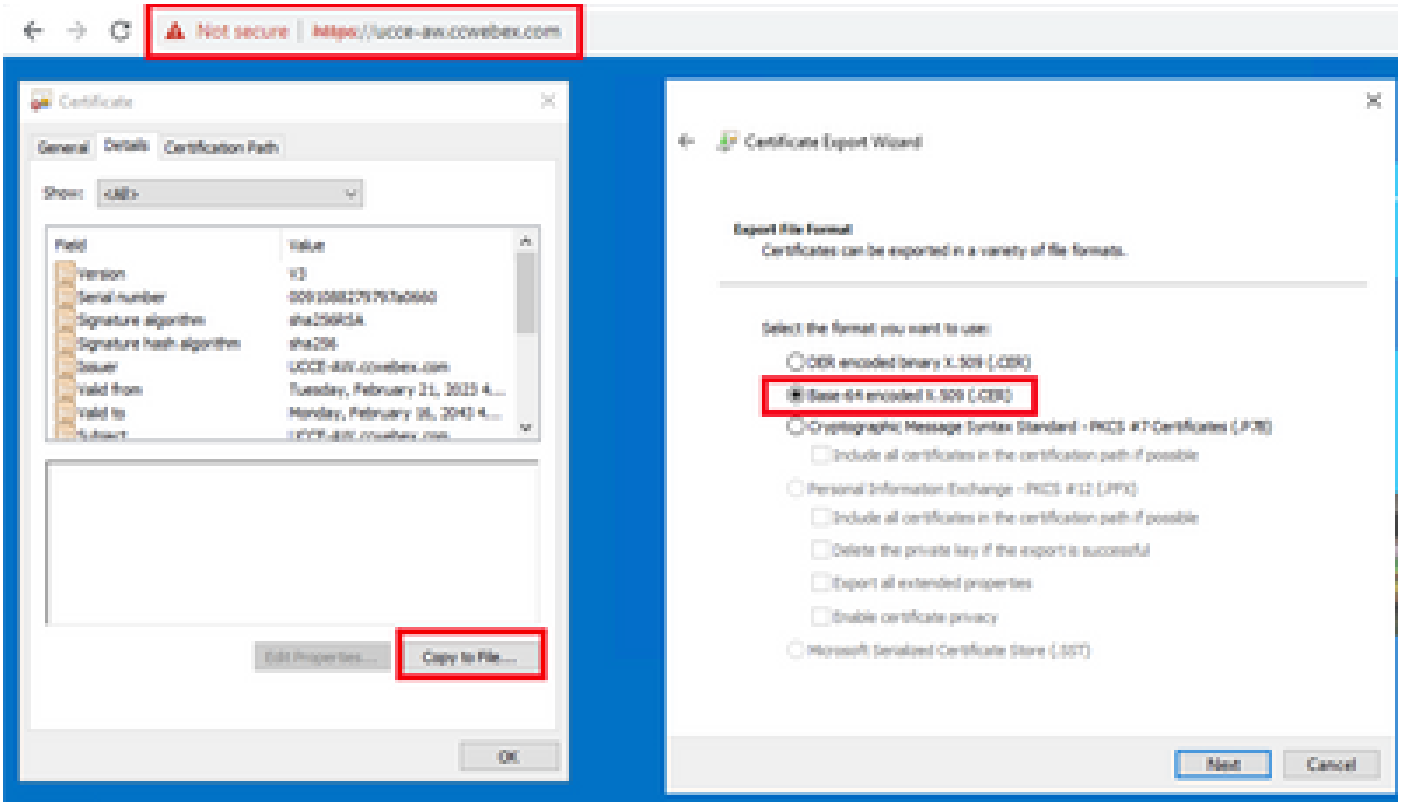
iii) Riavviare il servizio Apache Tomcat sui server ADS.

Passaggio 3. Esporta certificato server ADS

Di seguito sono riportati i passaggi per esportare il certificato ADS:

(i) Su un server ADS da un browser, passare all'URL del server: https://<servername>.

(ii) Salvare il certificato in una cartella temporanea, ad esempio: c:\temp\certs e denominare il certificato ADS<svr>[ab].cer.



Esporta certificati ADS

Nota: selezionare l'opzione X.509 con codifica Base 64 (.CER).

Passaggio 4. Importazione del certificato del server ADS nei server CVP e nel server di report

(i) Copiare il certificato nei server CVP e nel server di report CVP nella directory %CVP_HOME%\conf\security.

(ii) Importare il certificato nei server CVP e nel server di report CVP.

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -trustcacerts -alias {fqdn_of_ads} -file %CVP_HOME%\conf\security\ADS{svr}[ab].cer
```

Eseguire la stessa procedura per gli altri certificati dei server ADS.

(iii) Riavviare i server CVP e il server di report

Sezione 2: scambio di certificati tra applicazioni della piattaforma VOS e server ADS

Per completare correttamente questo scambio, è necessario eseguire le seguenti operazioni:

Passaggio 1. Esporta certificati server applicazioni piattaforma VOS.

Passaggio 2. Importare i certificati dell'applicazione piattaforma VOS nel server ADS.

Passaggio 3. Importare i certificati dell'applicazione piattaforma CUCM nei server PG CUCM.

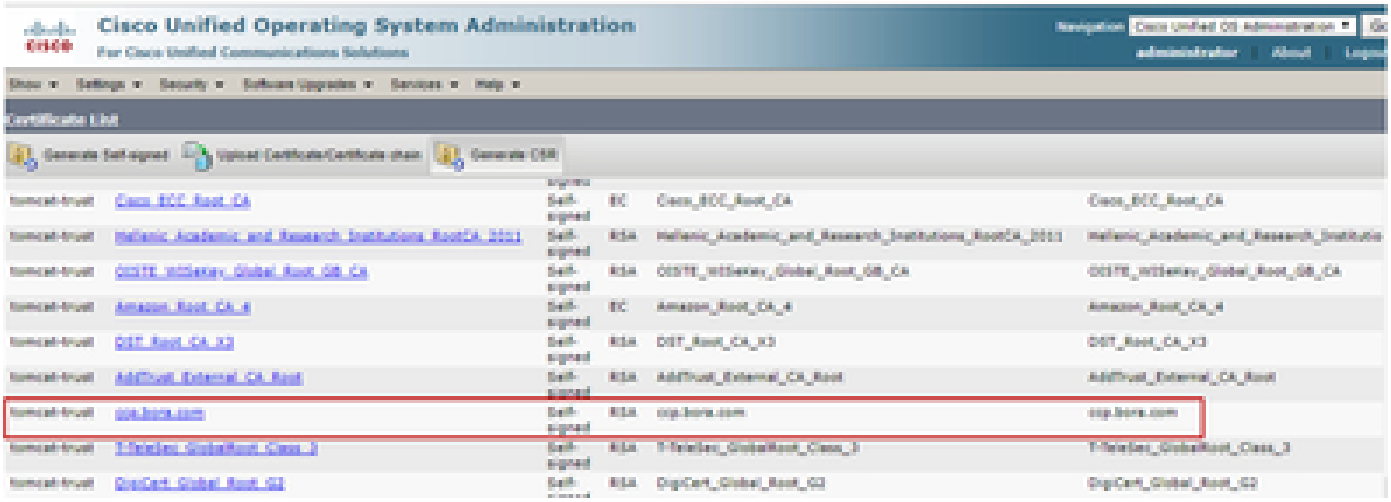
Questo processo è applicabile a tutte le applicazioni VOS, quali:

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- Cloud Connect

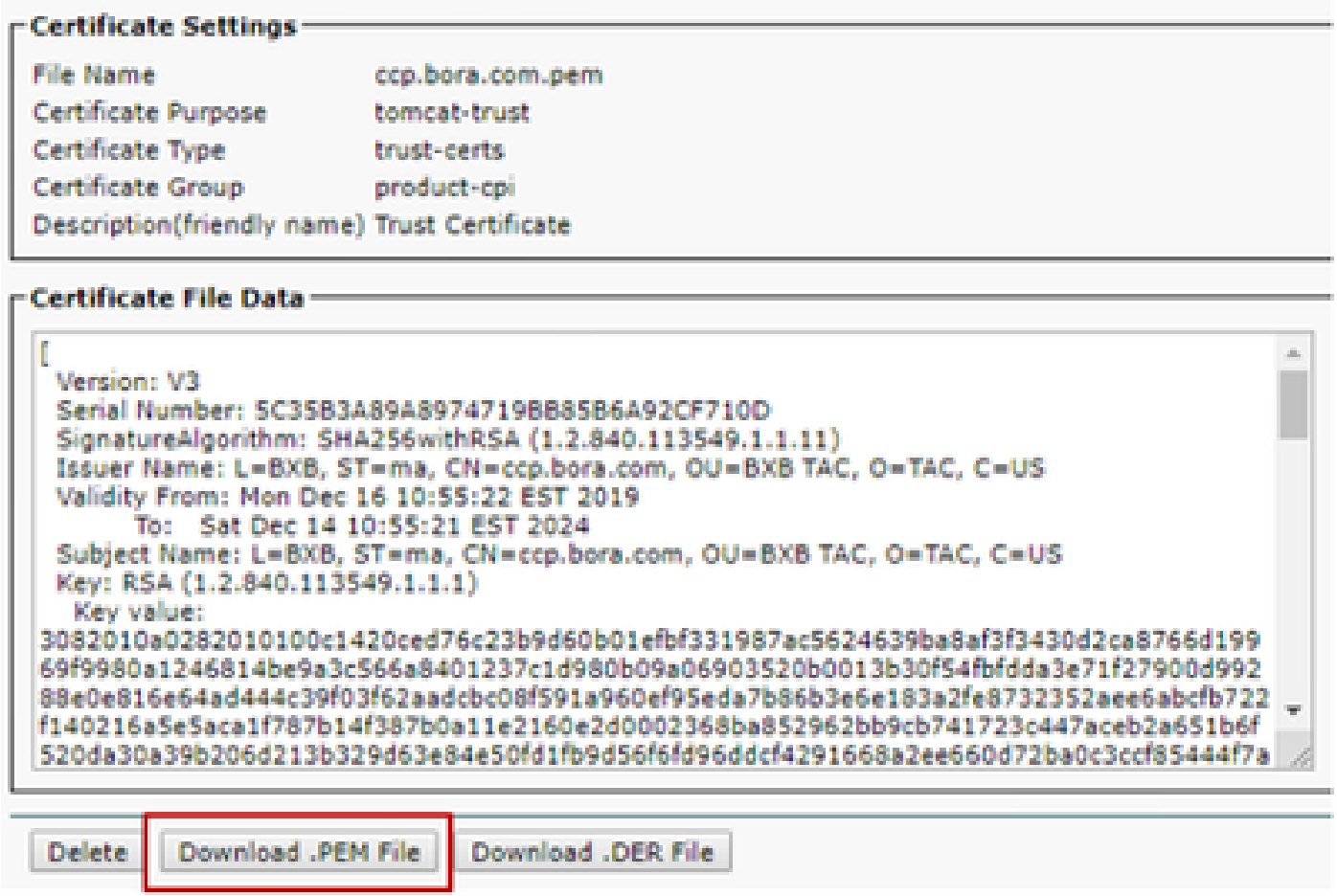
Passaggio 1. Esporta certificati server applicazioni piattaforma VOS.

(i) Passare alla pagina di amministrazione del sistema operativo Cisco Unified Communications: https://FQDN:8443/cmplatform.

(ii) Passare a Protezione > Gestione certificati e individuare i certificati del server principale dell'applicazione nella cartella tomcat-trust.



(iii) Selezionare il certificato e fare clic su Scarica file .PEM per salvarlo in una cartella temporanea sul server ADS.



Nota: eseguire la stessa procedura per il sottoscrittore.

Passaggio 2. Importa certificato applicazione piattaforma VOS nel server ADS

Percorso per eseguire lo strumento Chiave: %CCE_JAVA_HOME%\bin

Comandi per importare i certificati autofirmati:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias
{fqdn_of_VOS>} -keystore {ICM install directory}\ssl\cacerts
```

Riavviare il servizio Apache Tomcat sui server ADS.

Nota: eseguire la stessa operazione su altri server ADS

Passaggio 3. Importa certificato applicazione piattaforma CUCM su server PG CUCM

Percorso per eseguire lo strumento Chiave: %CCE_JAVA_HOME%\bin

Comandi per importare i certificati autofirmati:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\cucmapplicationX.cer -alias
{fqdn_of_cucm>} -keystore {ICM install directory}\ssl\cacerts
```

Riavviare il servizio Apache Tomcat sui server PG.

Nota: eseguire la stessa operazione su altri server PG CUCM

Sezione 3: scambio di certificati tra server Rogger , PG e ADS

Per completare correttamente questo scambio, è necessario eseguire le seguenti operazioni:

Passaggio 1. Esporta certificato IIS da server Rogger e PG

Passaggio 2. Esporta certificato DFP da server Rogger e PG

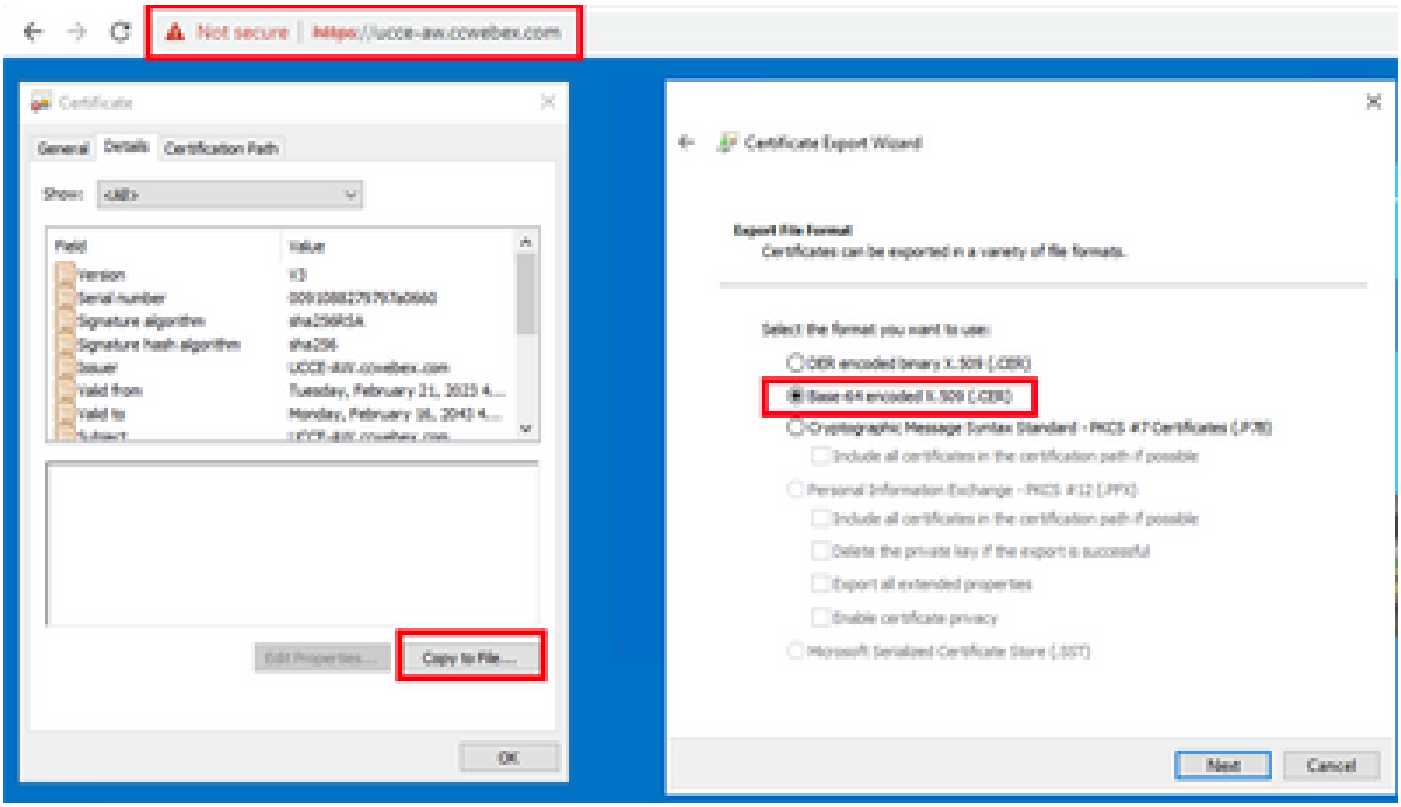
Passaggio 3. Importa certificati in server ADS

Passaggio 4. Importa certificato ADS in server Rogger e PG

Passaggio 1. Esporta certificato IIS da server Rogger e PG

(i) Su un server ADS da un browser, passare ai server (Roggers , PG) URL: https://{servername}

(ii)Salvare il certificato in una cartella temporanea, ad esempio c:\temp\certs e denominare il certificato ICM<svr>[ab].cer



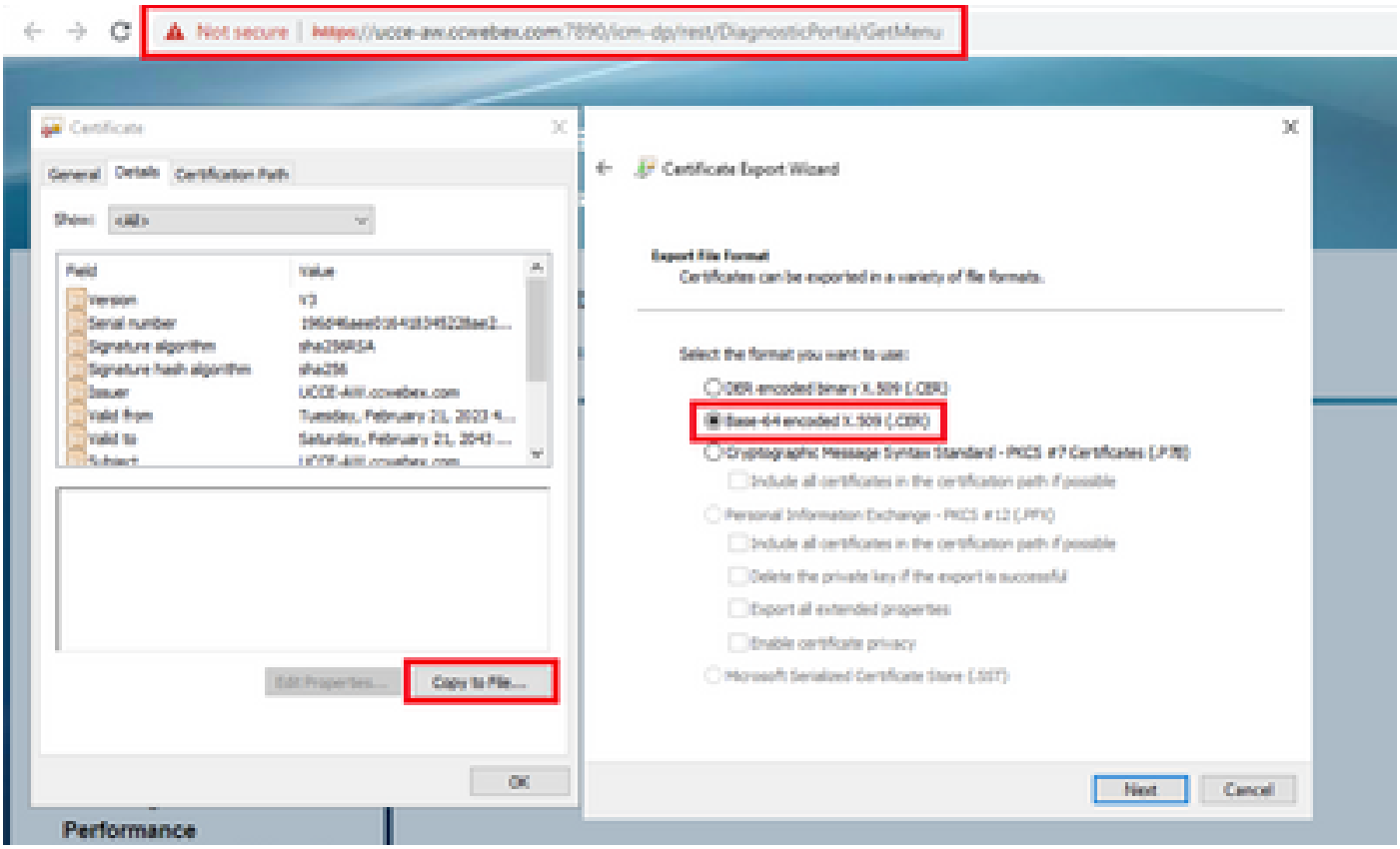
Esporta certificato IIS

Nota: selezionare l'opzione X.509 con codifica Base 64 (.CER).

Passaggio 2. Esporta certificato DFP da server Rogger e PG

(i) Su un server ADS da un browser, passare ai server (Roggers, PG) URL DFP: https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion

(ii) Salvare il certificato nella cartella example c:\temp\certs e denominare il certificato dfp{svr}[ab].cer



Esporta certificato DFP

Nota: selezionare l'opzione X.509 con codifica Base 64 (.CER).

Passaggio 3. Importa certificati nel server ADS

Comando per importare i certificati autofirmati di IIS nel server ADS. Percorso per l'esecuzione dello strumento Chiave: %CCE_JAVA_HOME%\bin

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\temp\certs\ICM<svr>[ab].cer -alias
{fqdn_of_server}_IIS -keystore {ICM install directory}\ssl\cacerts
```

Nota: importare tutti i certificati server esportati in tutti i server ADS.

Comando per importare i certificati autofirmati di diagnostica nel server ADS

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp<svr>[ab].cer -alias
{fqdn_of_server}_DFP -keystore {ICM install directory}\ssl\cacerts
```

Nota: importare tutti i certificati server esportati in tutti i server ADS.

Riavviare il servizio Apache Tomcat sui server ADS.

Passaggio 4. Importa certificato ADS in server Rogger e PG

Comando per importare i certificati autofirmati di IIS nei server Rogger e PG. Percorso per l'esecuzione dello strumento Chiave: %CCE_JAVA_HOME%\bin.

```
%CCE_JAVA_HOME%\bin\keytool -keystore ..\lib\security\cacerts  -import -storepass changeit -
alias {fqdn_of_server}_IIS -file c:\temp\certs\ICM{svr}[ab].cer
```

Nota: importare tutti i certificati IIS del server ADS esportati in tutti i server Rogger e PG.

Riavviare il servizio Apache Tomcat sui server Rogger e PG.

Sezione 4: Integrazione del servizio Web CVP CallStudio

Per informazioni dettagliate su come stabilire una comunicazione protetta per gli elementi Web Services Element e Rest_Client

Per ulteriori informazioni, fare riferimento al Manuale dell'utente per Cisco Unified CVP VXML Server e Cisco Unified Call Studio versione 12.6(2) - Integrazione dei servizi Web [Cisco Unified Customer Voice Portal] - Cisco

Informazioni correlate

- Guida alla configurazione di CVP - Sicurezza
- UCCE Security Guide
- Guida per l'amministratore PCCE
- Certificati autofirmati PCCE di Exchange - PCCE 12.5
- Certificati autofirmati Exchange UCCE - UCCE 12.5
- Certificati autofirmati Exchange UCCE - UCCE 12.6
- Implementazione di certificati firmati CA - CCE 12.6
- Certificati di Exchange con lo strumento Contact Center Uploader
- Documentazione e supporto tecnico – Cisco Systems

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).