Certificati autofirmati di Exchange in una soluzione UCCE 12.6

Sommario

Introduzione

In questo documento viene descritto come scambiare certificati autofirmati in una soluzione UCCE (Unified Contact Center Enterprise).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCCE release 12.6(2)
- Customer Voice Portal (CVP) versione 12.6(2)
- Cisco Virtualized Voice Browser (VB)

Componenti usati

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

- UCCE 12.6(2)
- CVP 12.6(2)
- Cisco VB 12.6(2)
- CVP Operations Console (OAMP)
- CVP Nuovo OAMP (NOAMP)

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 configurazione della soluzione UCCE di nuove funzionalità che coinvolgono applicazioni principali quali Rogger, Peripheral Gateway (PG), Admin Workstation (AW), Finesse, Cisco Unified Intelligent Center (CUIC) e così via viene eseguita tramite la pagina di amministrazione di Contact Center Enterprise (CCE). Per le applicazioni Interactive Voice Response (IVR) come CVP, Cisco VB e gateway, NOAMP controlla la configurazione delle nuove funzionalità. Dalla versione 12.5(1) di CCE, a causa della conformità SRC (Security-Management-Compliance), tutte le comunicazioni con gli amministratori CCE e NOAMP avvengono esclusivamente tramite il protocollo HTTP protetto.

Per garantire una comunicazione sicura e senza problemi tra queste applicazioni in un ambiente con certificati autofirmati, lo scambio di certificati tra i server è un'esigenza imprescindibile. Nella sezione successiva vengono illustrati in dettaglio i passaggi necessari per lo scambio di certificati autofirmati tra:

- Server AW CCE e server applicazioni di base CCE
- Server CVP OAMP e componenti CVP

Nota: questo documento si applica solo alla versione 12.6 di CCE. Per i collegamenti ad altre versioni, vedere la sezione relativa alle informazioni correlate.

Procedura

Server AW CCE e server applicazioni di base CCE

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

Server AW CCE: Il server richiede il certificato da:

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

Nota: sono necessari i certificati IIS e del framework di diagnostica.

- Piattaforma VOS: Cisco Unified Call Manager (CUCM), Finesse, CUIC, Live Data (LD), Identity Server (IDS), Cloud Connect e altri server applicabili che fanno parte del database di inventario.

Lo stesso vale per gli altri server AW della soluzione.

Router \ Server logger: Il server richiede un certificato da:

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

Le fasi necessarie per scambiare efficacemente i certificati autofirmati con CCE sono suddivise in queste sezioni.

Sezione 1: scambio di certificati tra router\registratore, server PG e AW.
Sezione 2: scambio di certificati tra l'applicazione della piattaforma VOS e il server AW.

Sezione 1: Scambio di certificati tra router\registratore, server PG e AW

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

Passaggio 1. Esporta certificati IIS da Router\Logger ,PG e tutti i server AW.
Passaggio 2. Esportare i certificati DFP (Diagnostic Framework Portico) dai server Router\Logger e PG.
Passaggio 3. Importare i certificati IIS e DFP da Router\Logger, PG a server AW.
Passaggio 4. Importa certificato IIS in Router\Logger da server AW.

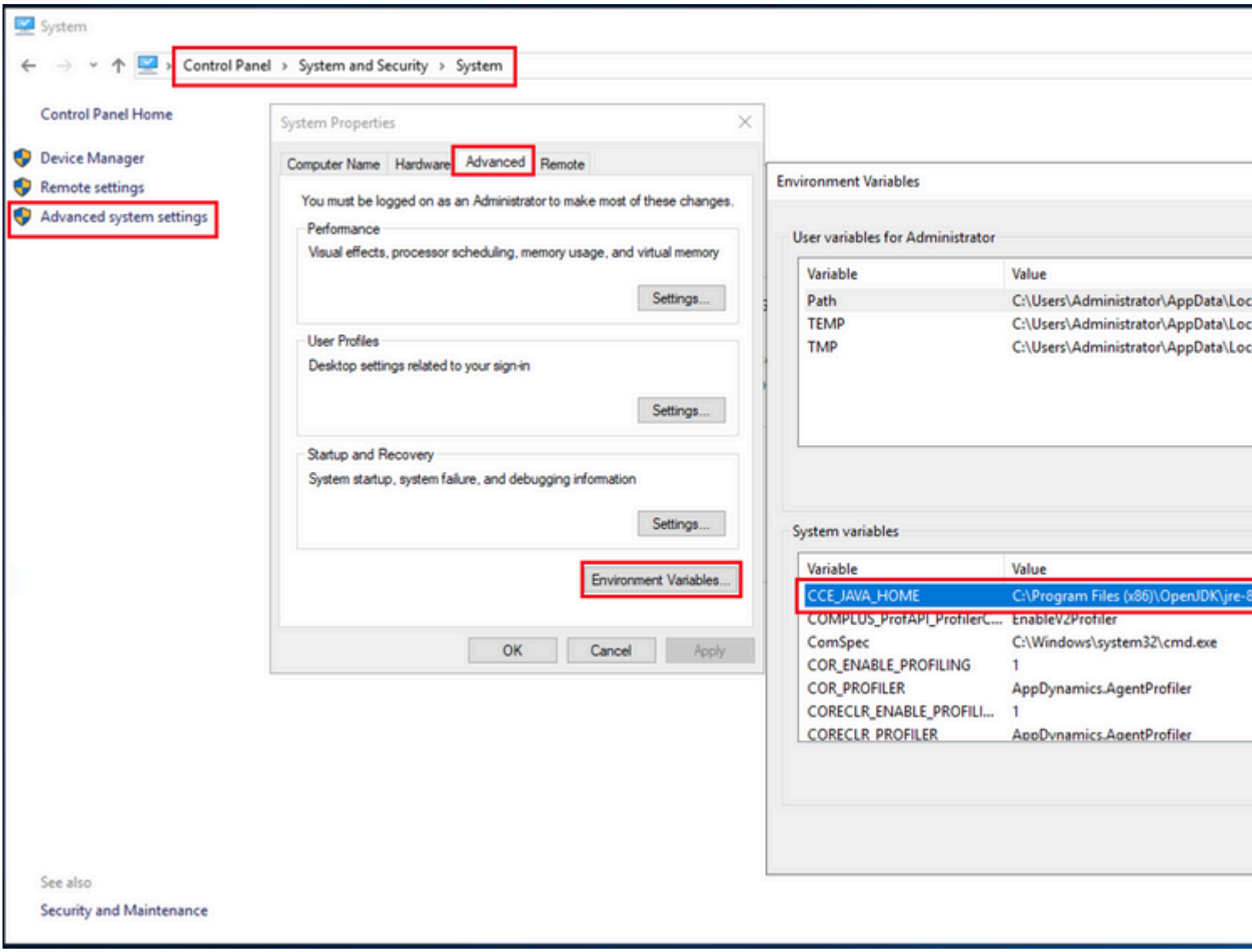
> **Attenzione**: prima di iniziare, è necessario eseguire il backup del keystore ed eseguire i comandi dalla java home come amministratore.

(i) Conoscere il percorso della directory principale di Java per verificare dove è ospitato lo strumento chiave di Java. Ci sono due modi per trovare il percorso di casa java.

Opzione 1: comando CLI: **echo %CCE_JAVA_HOME%**

```
C:\>echo %CCE_JAVA_HOME%
C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot
```

Opzione 2: Manualmente tramite Impostazioni di sistema avanzate, come mostrato nell'immagine

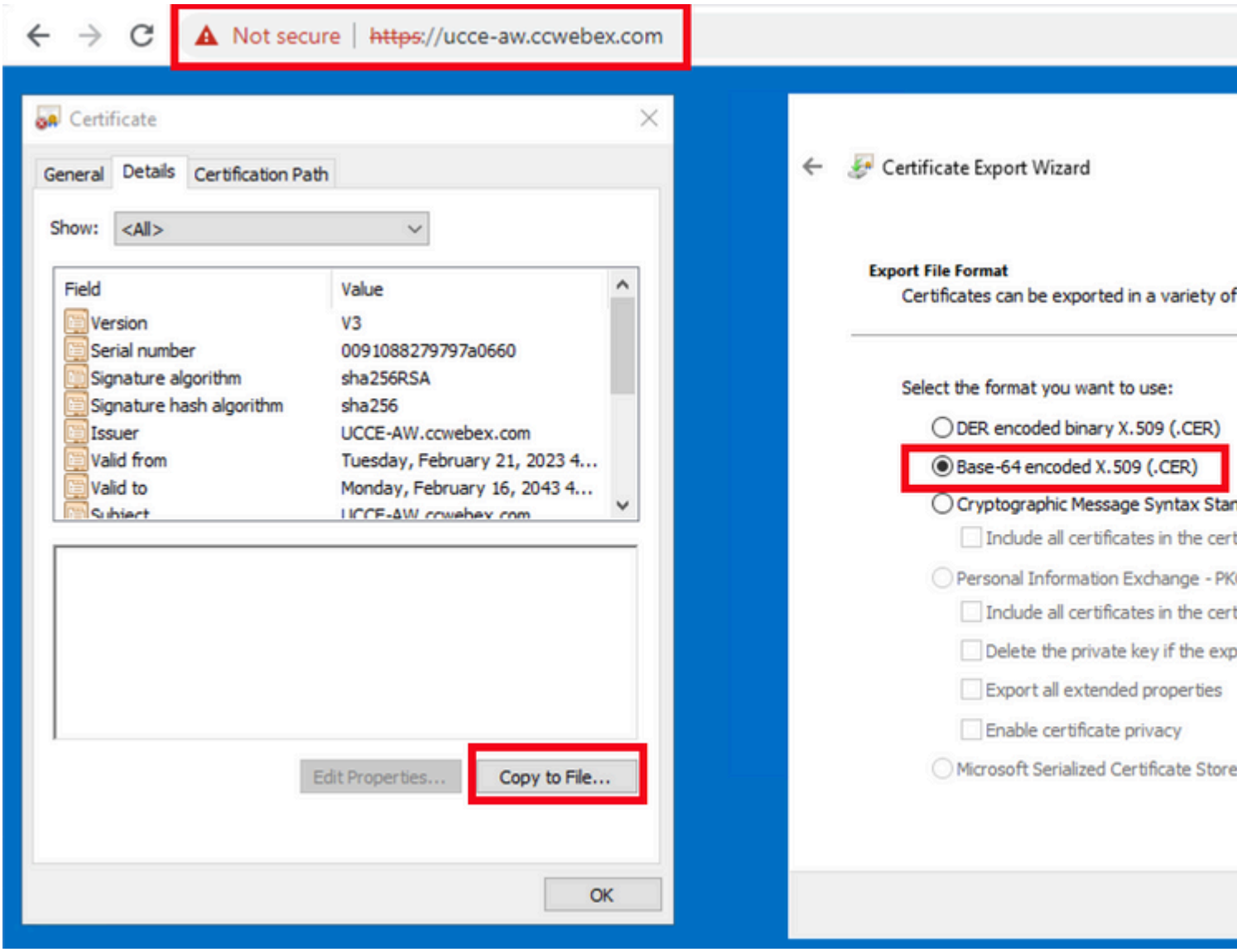


(ii) Eseguire il backup del file cacerts dalla cartella <ICM install directory>ssl\ **.** È possibile copiarlo in un'altra posizione.

(iii) Aprire una finestra di comando come amministratore per eseguire i comandi.

Passaggio 1. Esporta certificati IIS da Router\Logger, PG e tutti i server AW.

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

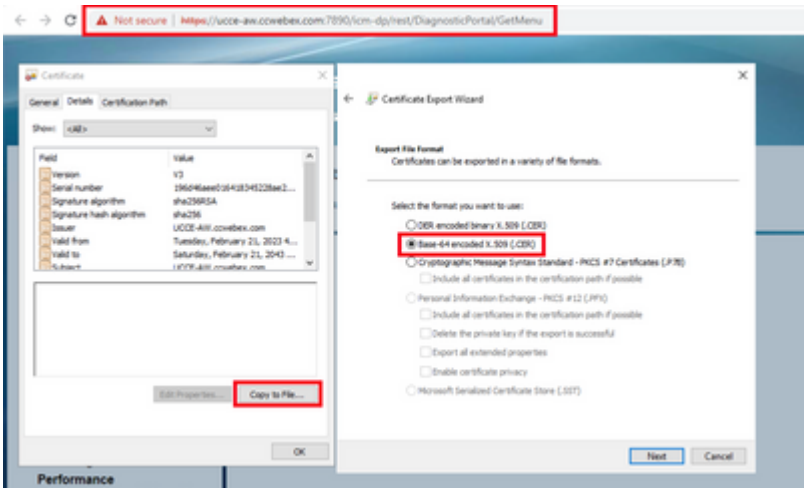


(ii) Salvare il certificato in una cartella temporanea. Ad esempio, c:\temp\certs e denominare il certificato ICM{svr}[ab].cer.

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

Passaggio 2. Esporta certificati DFP (Diagnostic Framework Portico) da router\Logger e server PG.

(i) Su un server AW, aprire un browser e passare ai server (Router, Logger o Rogger, 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

---

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

Passaggio 3. Importare il certificato IIS e DFP da Rogger, PG a AW Server.

Comando per importare i certificati autofirmati di IIS nel server AW. Percorso per eseguire lo strumento Chiave: C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_IIS
Example:%CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore
```

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

Comando per importare i certificati autofirmati DFP nei server AW:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp{svr}[ab].cer -alias {fqdn_of_server}_DFP
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\dfpAWA.cer -alias AWA_DFP -keystore
```

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

Riavviare il servizio Apache Tomcat sui server AW.

Passaggio 4. Importa certificato IIS in Router\Logger da AW Server.

Comando per importare i certificati autofirmati di IIS nei server Rogger:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\IIS{svr}[ab].cer -alias {fqdn_of_server}_IIS
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file c:\temp\certs\IISAWA.cer -alias AWA_IIS -keystore
```

Nota: importare tutti i certificati del server IIS AW esportati sui lati del router A e B.

Riavviare il servizio Apache Tomcat sui server Rogger.

Sezione 2: Scambio di certificati tra le applicazioni della piattaforma VOS e il server AW

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

Passaggio 1. Esporta certificati server applicazioni piattaforma VOS.
Passaggio 2. Importazione dei certificati delle applicazioni della piattaforma VOS in un server AW.

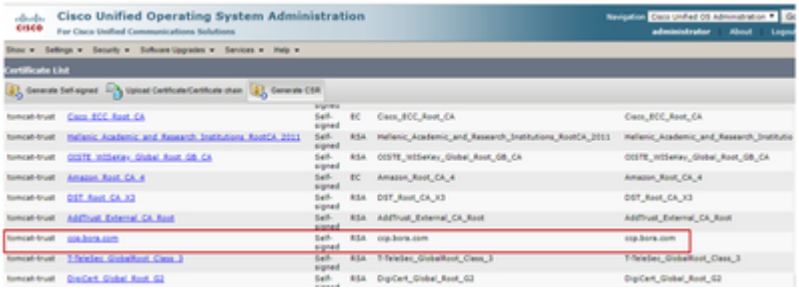
Questo processo è applicabile ad applicazioni VOS quali:

- Finesse
- CUIC \ LD \ IDS
- Cloud Connect

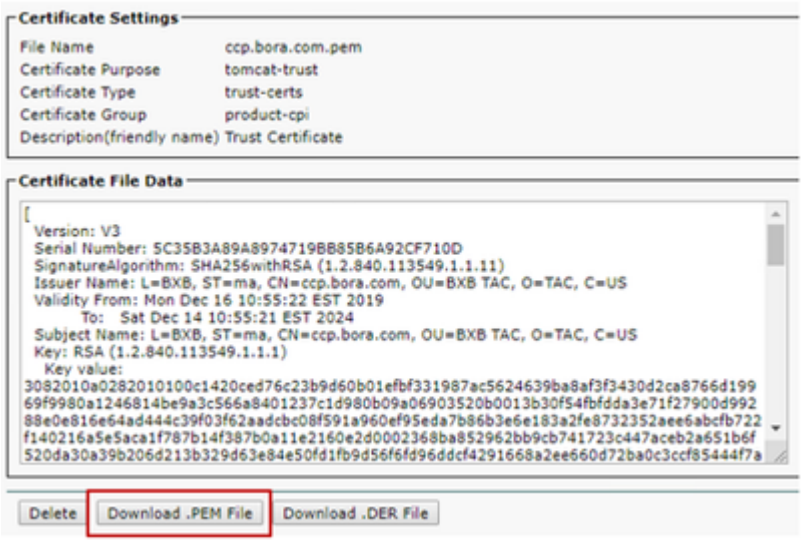
Passaggio 1. Esporta certificati server applicazioni piattaforma VOS.

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

(ii) Selezionare **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 AW.



Nota: eseguire la stessa procedura per il sottoscrittore.

Passaggio 2. Importazione dell'applicazione della piattaforma VOS nel server AW.

Percorso per eseguire lo strumento Chiave: C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin

Comando per importare i certificati autofirmati:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.pem -alias {fqdn_of_VOS} -ke
Example: %CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\CUICPub.pem -alias CUICPub -keysto
```

Riavviare il servizio Apache Tomcat sui server AW.

Nota: eseguire la stessa operazione su altri server AW.

Server CVP OAMP e server dei componenti CVP

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

(i) Server CVP OAMP: questo server richiede un certificato da

- Piattaforma Windows: certificato di Web Services Manager (WSM) dal server CVP e dai server di report.
- Piattaforma VOS: Cisco VB e server Cloud Connect.

(ii) Server CVP: questo server richiede un certificato da

- Piattaforma Windows: certificato WSM dal server OAMP.
- Piattaforma VOS: server Cloud Connect e server Cisco VB per comunicazioni SIP e HTTP sicure.

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

- Piattaforma Windows: certificato WSM dal server OAMP.

(iv) Server VB Cisco: questo server richiede un certificato da

- Piattaforma Windows: CVP Server VXML (HTTP protetto), CVP Server callserver (SIP protetto)
- Piattaforma VOS: server Cloud Connect

In queste tre sezioni vengono illustrati i passaggi necessari per scambiare in modo efficace i certificati autofirmati nell'ambiente CVP.

Sezione 1: Scambio di certificati tra il server CVP OAMP, il server CVP e i server di reporting
Sezione 2: scambio di certificati tra il server CVP OAMP e le applicazioni della piattaforma VOS
Sezione 3: scambio di certificati tra il server CVP e le applicazioni della piattaforma VOS

Sezione 1: Scambio di certificati tra il server CVP OAMP, il server CVP e i server di reporting

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

Passaggio 1. Esporta il certificato WSM dal server CVP, dal server di reporting e dal server OAMP.
Passaggio 2. Importa i certificati WSM dal server CVP e dal server di report nel server OAMP.
Passaggio 3. Importare il certificato WSM del server CVP OAMP nel server CVP e nei server di reporting.

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.

Passaggio 1. Esporta certificato WSM da server CVP, server di reporting e OAMP.

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

Comando per esportare i certificati autofirmati:

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

(ii) Copiare il certificato dal percorso %CVP_HOME%\conf\security\wsm.crt da ciascun server e rinominarlo come wsmX.crt in base al tipo di server.

Passaggio 2. Importa i certificati WSM dal server CVP e dal server di report nel server OAMP.

(i) Copiare ogni certificato WSM del server CVP e del server di report (wsmX.crt) nella directory %CVP_HOME%\conf\security del server OAMP.

ii) Importare i certificati con il comando:

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

(iii) Riavviare il server.

Passaggio 3. Importare il certificato WSM del server OAMP CVP nel server CVP e nei server di reporting.

(i) Copiare il certificato WSM del server OAMP (wsmoampX.crt) nella directory %CVP_HOME%\conf\security in tutti i server CVP e i server di reporting.

ii) Importare i certificati con il comando:

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

(iii) Riavviare i server.

Sezione 2: scambio di certificati tra il server CVP OAMP e le applicazioni della piattaforma VOS

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

Passaggio 1. Esporta certificato applicazione dalla piattaforma VOS.

Passaggio 2. Importa certificato applicazione VOS nel server OAMP.

Questo processo è applicabile ad applicazioni VOS quali:

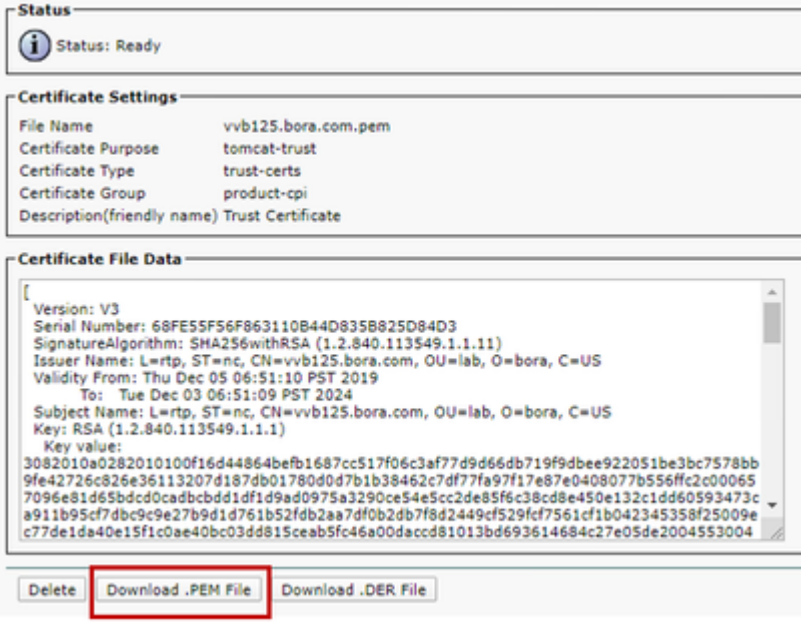
- CUCM
- VVB
- Cloud Connect

Passaggio 1. Esporta certificato applicazione dalla piattaforma VOS.

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

(ii) Selezionare **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 OAMP.



Passaggio 2. Importa certificato applicazione VOS nel server OAMP.

(i) Copiare il certificato VOS nella directory %CVP_HOME%\conf\security sul server OAMP.

ii) Importare i certificati con il comando:

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

(ii) Riavviare il server.

Sezione 3: scambio di certificati tra il server CVP e le applicazioni della piattaforma VOS

Questa operazione è facoltativa e consente di proteggere la comunicazione SIP tra CVP e altri componenti del Contact Center. Per ulteriori informazioni, consultare la guida alla configurazione del CVP: guida alla configurazione del CVP - sicurezza.

Integrazione 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: Guida alla configurazione di CVP - Sicurezza
- Guida alla configurazione UCCE: Guida alla sicurezza UCCE
- Guida all'amministrazione di PCCE: Guida all'amministrazione di PCCE
- Certificati autofirmati PCCE 12.6: Certificati autofirmati PCCE di Exchange
- Certificati autofirmati PCCE 12.5: Certificato autofirmato PCCE 12.5

- Certificato autofirmato UCCE 12.5: Certificati autofirmati UCCE 12.5
- Certificati firmati CCE CA 12.5: Certificati firmati CCE CA 12.5
- **Documentazione e supporto tecnico â€“ 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).