Certificati autofirmati di Exchange in una soluzione UCCE

Sommario

Introduzione

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

Contributo di Anuj Bhatia, Robert Rogier e Ramiro Amaya, Cisco TAC Engineers

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCCE release 12.5(1)
- Customer Voice Portal (CVP) versione 12.5 (1)
- Cisco Virtualized Voice Browser (VB)

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- UCCE 12.5(1)
- CVP 12.5(1)

- Cisco VB 12.5
- 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.

Sfondo

Nella configurazione della soluzione UCCE di nuove funzionalità che coinvolgono le applicazioni principali come Rogger, Peripheral Gateway (PG), Admin Workstation (AW), Finesse, Cisco Unified Intelligent Center (CUIC), ecc. 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 l'amministratore CCE e NOAMP avvengono esclusivamente tramite il protocollo HTTP protetto.

Per garantire una comunicazione sicura tra queste applicazioni in un ambiente di certificazione autofirmato, lo scambio di tali certificati tra i server diventa 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

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

  Nota: Sono necessari 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 di registrazione: Il server richiede il certificato da:

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

In queste sezioni vengono illustrati i passaggi necessari per scambiare efficacemente i certificati autofirmati con CCE.

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.

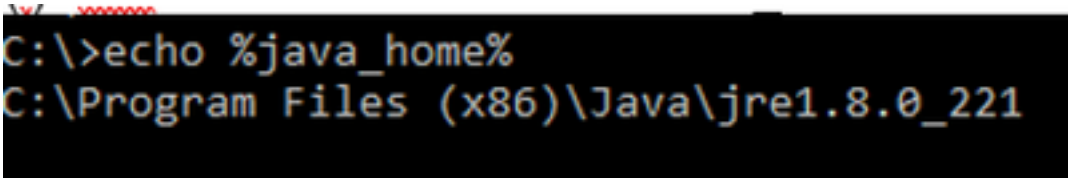
Per completare correttamente questo scambio, è necessario eseguire le seguenti operazioni:

Passaggio 1. Esportare i certificati IIS da Router\Logger ,PG e da 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. Importare il certificato IIS in Router\Logger dai server AW.

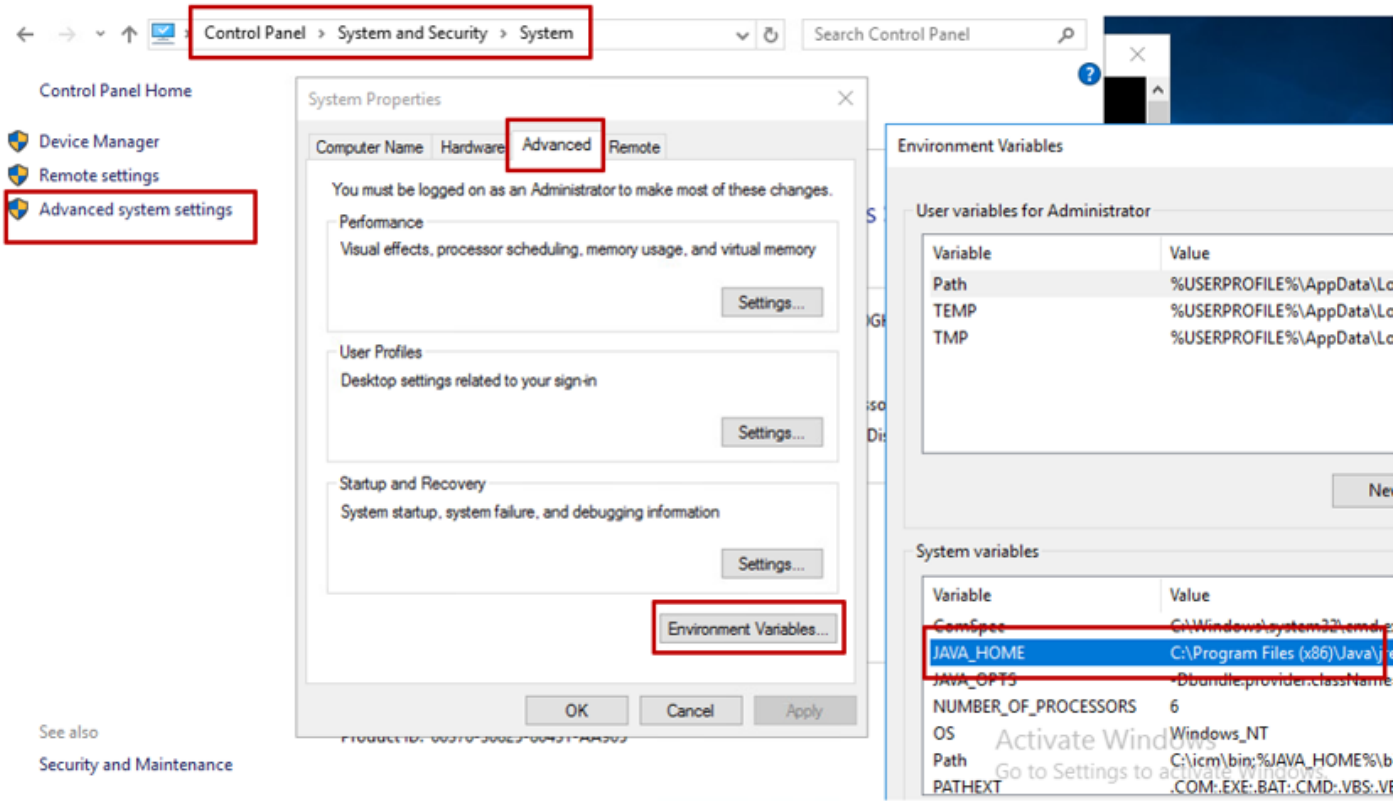
> **Attenzione:** Prima di iniziare, è necessario eseguire il backup del keystore ed eseguire i comandi dalla java home come amministratore.

(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: **eco %JAVA_HOME%**



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



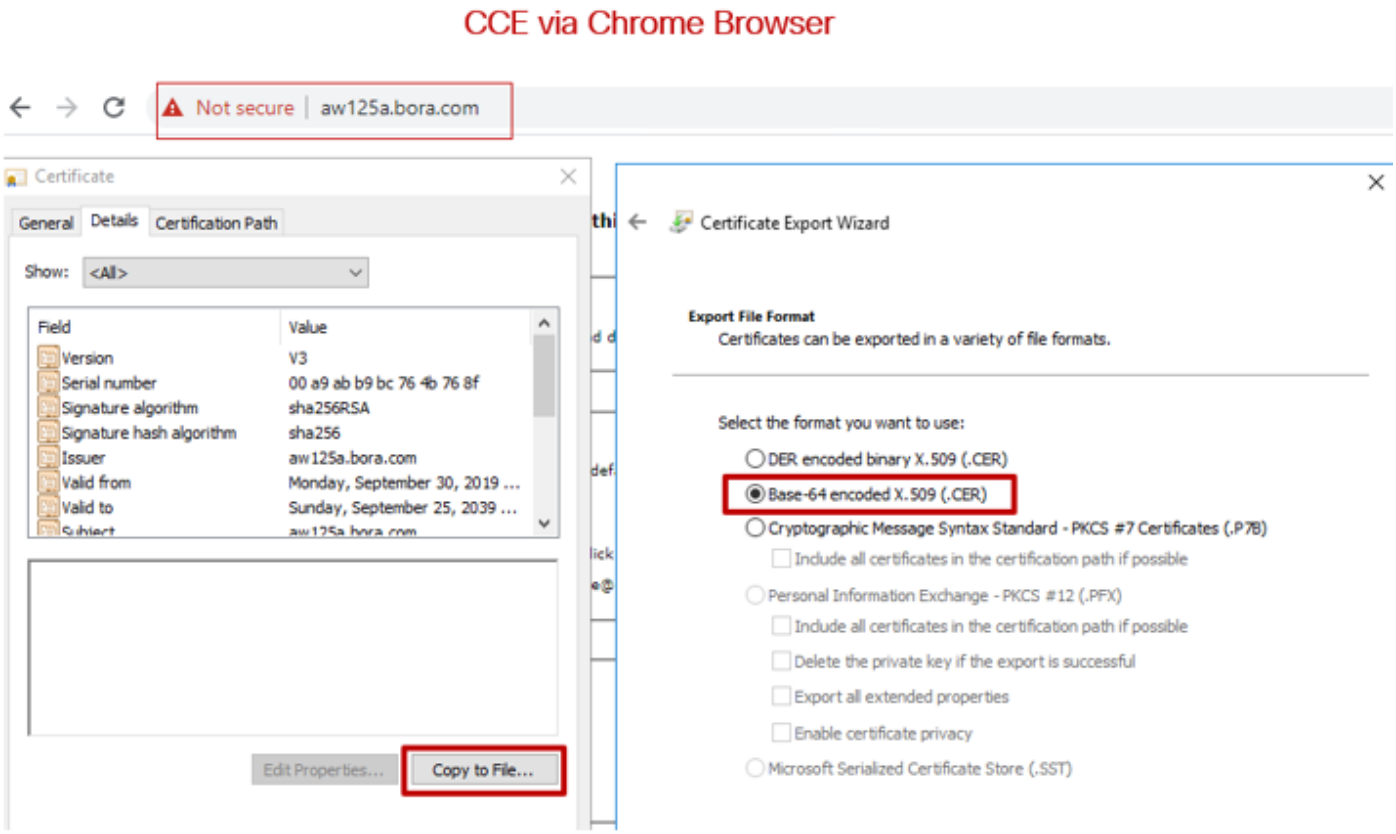
Nota: In UCCE 12.5 il percorso predefinito è C:\Program Files (x86)\Java\jre1.8.0_221\bin. Tuttavia, se è stato utilizzato il programma di installazione 12.5(1a) o se è installato 12.5 ES55 (obbligatorio OpenJDK ES), utilizzare CCE_JAVA_HOME anziché JAVA_HOME poiché il percorso dell'archivio dati è stato modificato con OpenJDK. Ulteriori informazioni sulla migrazione di OpenJDK in CCE e CVP sono disponibili nei seguenti documenti: Installazione e migrazione a OpenJDK in CCE 2.5(1) e installazione e migrazione a OpenJDK in CVP 12.5(1).

(ii) Eseguire il backup del file **cacerts** dalla cartella **C:\Program Files (x86)\Java\jre1.8.0_221\lib\security.** È possibile copiarlo in un'altra posizione.

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

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

(i) Su un server AW da un browser, passare ai server (Roggers , PG , altri server AW) url: **https://{nomeserver}.**

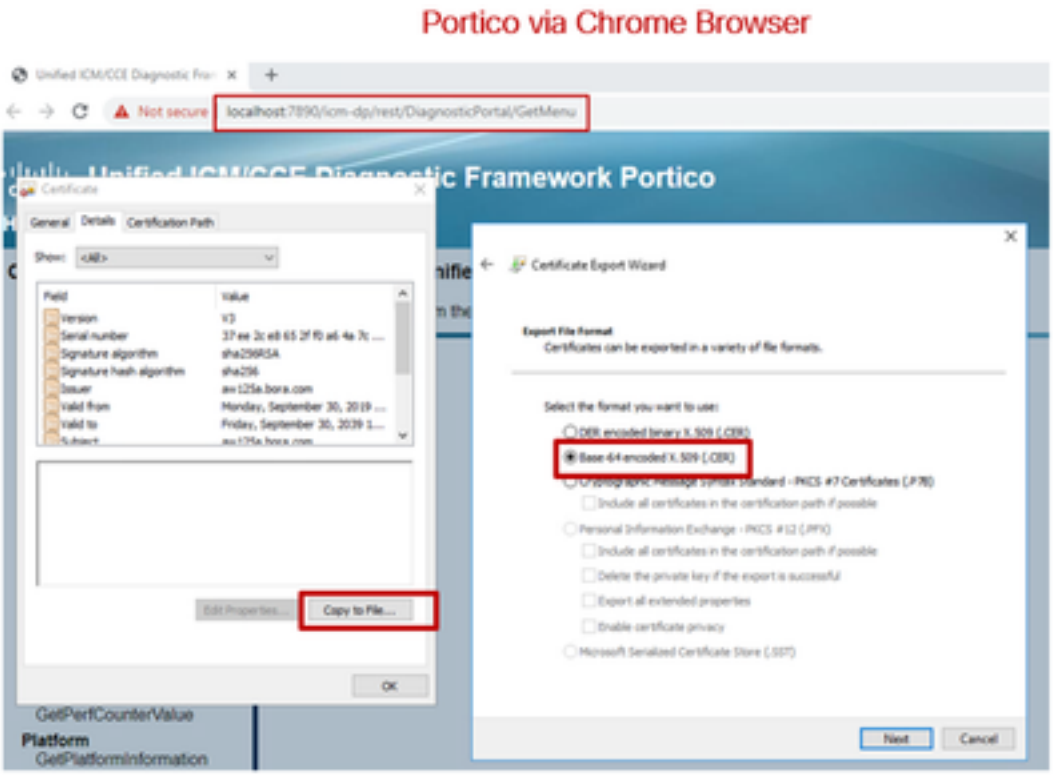


(ii)Salvare il certificato in una cartella temporanea, ad esempio c:\temp\certs e denominare il certificato ICM{svr}[ab].cer.

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

Passaggio 2. Esportare i certificati DFP (Diagnostic Framework Portico) dai server Router\Logger e 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 Codificato Base 64 X.509 (.CER).

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

Comando per importare i certificati autofirmati di IIS nel server AW. Percorso per l'esecuzione dello strumento Chiave: **C:\Program Files (x86)\Java\jre1.8.0_221\bin**:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -
storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}[ab].cer
Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -
import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer
```

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

Comando per importare i certificati autofirmati DFP nei server AW:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -
storepass changeit -alias {fqdn_of_server}_DFP -file c:\temp\certs\ dfp{svr}[ab].cer
Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -
import -storepass changeit -alias myrgra.domain.com_DFP -file c:\temp\certs\dfprgra.cer
```

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

Riavviare il servizio Apache Tomcat sui server AW.

Passaggio 4. Importare il certificato IIS in Router\Logger dai server AW.

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

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -
storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}[ab].cer
Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -
import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer
```

Nota: Importare tutti i certificati del server IIS AW esportati nei 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. Esportare i certificati del server applicazioni della piattaforma VOS.
Passaggio 2. Importare i certificati dell'applicazione della piattaforma VOS nel server AW.

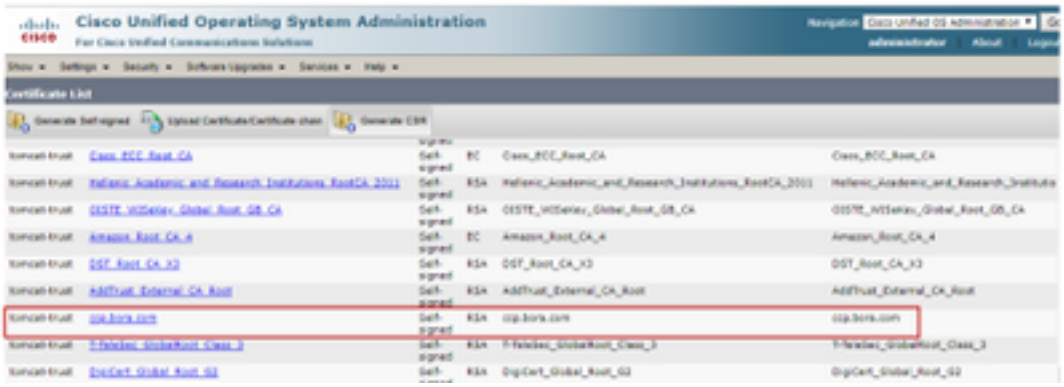
Questo processo è applicabile a tutte le applicazioni VOS, quali:

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

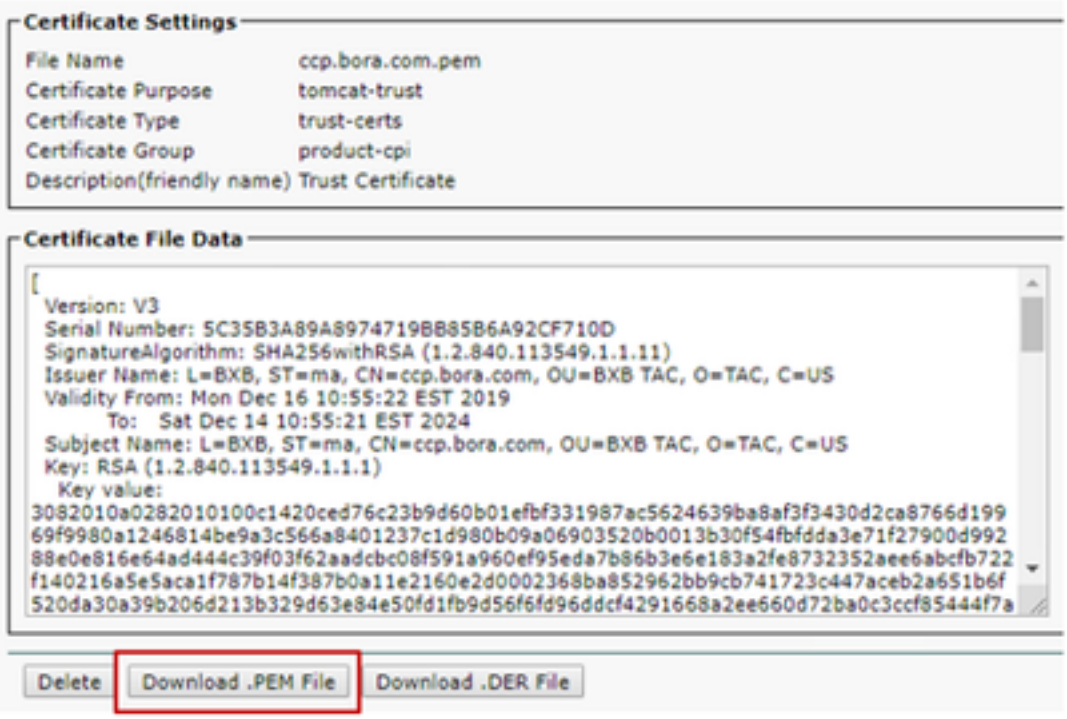
Passaggio 1. Esportare i certificati del server applicazioni della piattaforma VOS.

(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 gli stessi passaggi per il sottoscrittore.

Passaggio 2. Importare l'applicazione della piattaforma VOS nel server AW.

Percorso per eseguire lo strumento Chiave: **C:\Program Files (x86)\Java\jre1.8.0_221\bin**

Comando per importare i certificati autofirmati:

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts" -import -
storepass changeit -alias {fqdn_of_vos} -file c:\temp\certs\vosapplicationX.pem
```

Riavviare il servizio Apache Tomcat sui server AW.

Nota: Eseguire la stessa operazione su altri server AW.

Server CVP OAMP e server CVP Component

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: Il server richiede il certificato di

- Piattaforma Windows: Certificato di Web Services Manager (WSM) dal server CVP e dai server di report.
- Piattaforma VOS: Cisco VB per l'integrazione di Customer Virtual Agent (CVA), Cloud Connect Server per l'integrazione di Webex Experience Management (WXM).

(ii) Server CVP: Il server richiede il certificato di

- Piattaforma Windows: Certificato WSM dal server OAMP.
- Piattaforma VOS: Cloud Connect server per l'integrazione WXM, Cisco VB server per la comunicazione SIP e HTTP protetta.

iii) server di reporting CVP: Il server richiede il certificato di

- 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)

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 e 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 server CVP e server VB.

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

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

Passaggio 1. Esportare il certificato WSM dal server CVP, dal server di reporting e dal server OAMP.
Passaggio 2. Importare 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 report.

> **Attenzione:** Prima di iniziare, eseguire le operazioni seguenti:
> 1. Ottenere la password del keystore. Eseguire il comando: altre %CVP_HOME%\conf\security.properties
> 2. Copiare la cartella %CVP_HOME%\conf\security in un'altra cartella.
> 3. Aprire una finestra di comando come amministratore per eseguire i comandi.

Passaggio 1. Esportare il certificato WSM dal server CVP, dal server di reporting e dal server 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 un numero o una lettera univoci. 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 -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

(ii) Copiare il certificato dal percorso **C:\Cisco\CVP\conf\security\wsm.crt** da ciascun server e rinominarlo come wsmX.crt in base al tipo di server.

Passaggio 2. Importare 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 C:\Cisco\CVP\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 -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmcsX.crt
```

(iii) Riavviare il server.

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

(i) Copiare il certificato WSM del server OAMP (wsmoampX.crt) nella directory C:\Cisco\CVP\conf\security su tutti i server CVP e di reporting.

ii) Importare i certificati con il comando:

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -alias {fqdn_of_cvp}_wsm -file c:\cisco\cvp\conf\security\wsmoampX.crt
```

(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. Esportare il certificato dell'applicazione dalla piattaforma VOS.

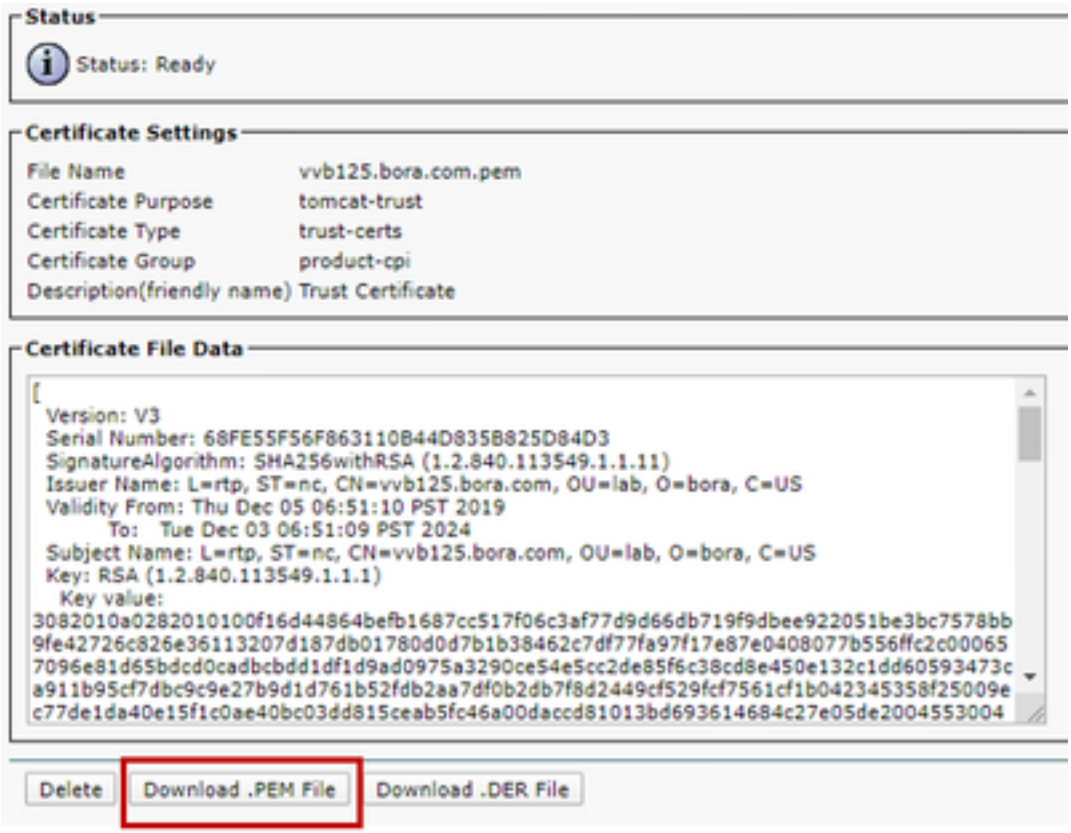
Passaggio 2. Importare il certificato dell'applicazione VOS nel server OAMP.

Passaggio 1. Esportare il certificato dell'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. Importare il certificato dell'applicazione VOS nel server OAMP.

(i) Copiare il certificato VVB C nella directory C:\Cisco\CVP\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 -alias {fqdn_of_vos} -file c:\cisco\cvp\conf\security\vvb.pem
```

(ii) Riavviare il server.

Sezione 3: Scambio di certificati tra server CVP e server CVB.

Questo passaggio è facoltativo per proteggere la comunicazione SIP e HTTP tra i server CVB e CVP. Per completare correttamente questo scambio, è necessario eseguire le seguenti operazioni:

Passaggio 1. Esportare il certificato dell'applicazione CVB dalla piattaforma VOS.
Passaggio 2. Importare il certificato dell'applicazione vos nei server CVP.
Passaggio 3: Esporta il server di chiamata e il certificato vxml dai server CVP.
Passaggio 4: Importare il server di chiamata e il certificato vxml nei server CVB.

Passaggio 1. Esportare il certificato dell'applicazione dalla piattaforma vos.

(i) Seguire le stesse procedure indicate nella fase 1 della sezione 2 per i server CVB.

Passaggio 2. Importare il certificato dell'applicazione VOS nel server CVP.

(i) Seguire la stessa procedura descritta nella fase 2 della sezione 2 su tutti i server CVP.

Passaggio 3: Esporta il server di chiamata e il certificato vxml dai server CVP

(i) Esportare il server di chiamata e il certificato vxml da ciascun server CVP in una posizione temporanea e rinominare il certificato con il nome desiderato. È possibile rinominarlo callserverX.crt \ vxmlX.crt Sostituire **X** con un numero o una lettera univoci.

Comando per esportare i certificati autofirmati:

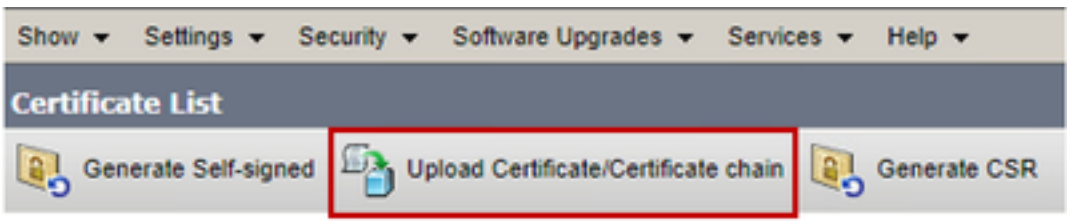
```
Callserver certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore
%CVP_HOME%\conf\security\.keystore -export -alias callserver_certificate -file
%CVP_HOME%\conf\security\callserverX.crt
Vxml certificate : %CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore
%CVP_HOME%\conf\security\.keystore -export -alias vxml_certificate -file
%CVP_HOME%\conf\security\vxmlX.crt
```

(ii) Copiare il certificato dal percorso C:\Cisco\CVP\conf\security\wsm.crt da ogni server e rinominarlo come callserverX.crt \ vxmlX.crt in base al tipo di certificato.

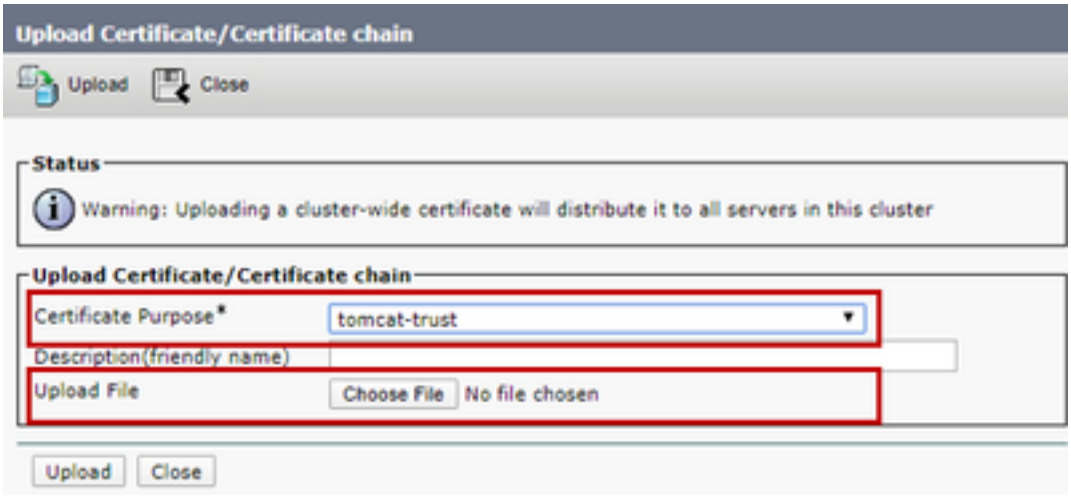
Passaggio 4: Importare il server di chiamata e il certificato vxml nei server CVB.

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

(ii) Selezionare Protezione > Gestione certificati e selezionare l'opzione di caricamento della catena di certificati/certificati.



(iii) Nella catena di caricamento del certificato/certificato selezionare tomcat-trust nel campo scopo del certificato e caricare i certificati esportati come eseguito nel passaggio 3.



(iv) Riavviare il server.

CISCO CallStudio WEBService Integration

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

fare riferimento alla Guida per l'utente di Cisco Unified CVP VXML Server e Cisco Unified Call Studio versione 12.5(1) - 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 configurazione UCCE - Sicurezza
- Guida all'amministrazione di PCCE: PCE Admin Guide - Sicurezza
- Certificati autofirmati UCCE: certificati autofirmati UCCE di Exchange
- Certificati autofirmati PCCE: certificati autofirmati PCCE di Exchange
- Installazione e migrazione a OpenJDK in CCE 12.5(1): Migrazione CCE OpenJDK
- Installazione e migrazione a OpenJDK in CVP 12.5(1): CVP OpenJDK Migration

Documentazione e supporto tecnico – Cisco Systems