Certificati autofirmati di Exchange in una soluzione PCCE

Sommario

Introduzione

In questo documento viene descritto come scambiare certificati autofirmati tra il server di amministrazione principale (ADS/AW) e altri server applicazioni nella soluzione Cisco Packaged Contact Center Enterprise (PCCE).

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

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PCCE release 12.5(1)
- Customer Voice Portal (CVP) versione 12.5 (1)

Componenti usati

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

- PCCE 12.5(1)
- CVP 12.5(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.

Sfondo

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) nella 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 diventa un must. Questo scambio di certificati è inoltre necessario per abilitare le nuove funzionalità presenti nella versione 12.5(1), ad esempio Smart Licensing, Webex Experience Management (WXM) e Customer Virtual Assistant (CVA).

Procedura

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

i) server AW principale: Il server richiede il certificato da:

- Piattaforma Windows: ICM: Router and Logger(Rogger){A/B}, Peripheral Gateway (PG){A/B}, tutti i server ADS e Email and Chat (ECE). Nota: Sono necessari certificati IIS e del framework di diagnostica.CVP Server CVP, server di reporting CVP. Nota 1: È necessario un certificato di Gestione servizi Web (WSM) dai server.Nota 2: I certificati devono essere con il nome di dominio completo (FQDN).
- Piattaforma VOS: Cloud Connect, Cisco Virtual Voice Browser (VB), Cisco Unified Call Manager (CUCM), Finesse, Cisco Unified Intelligent Center (CUIC), Live Data (LD), Identity Server (IDS) e altri server applicabili.

Lo stesso vale per altri server ADS nella soluzione.

(ii) Router \ Server di registrazione: Il server richiede il certificato da:

- Piattaforma Windows: Certificato IIS di tutti i server ADS.

iii) Server PG CUCM: Il server richiede il certificato da:

- Piattaforma VOS: editore CUCM. Nota: Questa operazione è necessaria per scaricare il client JTAPI dal server CUCM.

iv) Server CVP: Il server richiede il certificato di

- Piattaforma Windows: Certificato IIS per tutti i server ADS

- Piattaforma VOS: Server Cloud Connect per integrazione WXM, server VB per comunicazione SIP protetta e HTTP.

v) server di reporting CVP: Il server richiede il certificato da:

- Piattaforma Windows: Certificato IIS per tutti i server ADS

vi) Server VVB: Il server richiede il certificato da:

- Piattaforma Windows: Server VXML CVP (HTTP protetto), server di chiamata CVP (SIP protetto)

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. Esportare i certificati WSM del server CVP.

Passaggio 2. Importare il certificato WSM del server CVP nel server ADS.

Passaggio 3. Esportare il certificato del server ADS.

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

Passaggio 1. Esportare 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, alcune funzionalità, quali Smart Licensing, CVA e la sincronizzazione CVP con SPOG, potrebbero presentare problemi.

Attenzione: Prima di iniziare, eseguire le operazioni seguenti:

- Ottenere la password del keystore. Eseguire questo comando: altre %CVP_HOME%\conf\security.properties
- Copiare la cartella %CVP_HOME%\conf\security in un'altra cartella.
- Aprire una finestra di comando come amministratore per eseguire i comandi.

Nota: È possibile semplificare i comandi utilizzati in questo documento utilizzando il parametro -storepass. Per tutti i server CVP, viene incollata la password ottenuta dal file security.properties specificato. Per i server ADS digitare la password: **modificare**

Per rigenerare il certificato nei server CVP, eseguire la procedura seguente:

(i) Elenca 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 seguenti 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: comando 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: comando 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 di questi certificati autofirmati wsm_certificate, callserver_certificate.

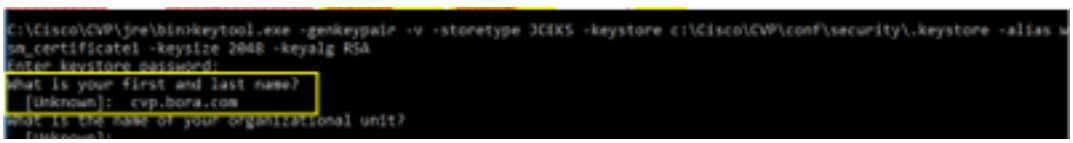
(iii) Generare i nuovi certificati autofirmati con il nome FQDN del server

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
```

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]: <specifica unità organizzativa>

Qual è il nome dell'organizzazione?

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

Indicare il nome della città o 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]: <specificare il codice del 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 seguire la stessa procedura utilizzata per 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.

Nota: Per impostazione predefinita, i certificati autofirmati 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. 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: In 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.

(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 un numero o una lettera univoci. ovvero wsmcsa.crt, wsmcsb.crt.

Comando per esportare i certificati autofirmati:

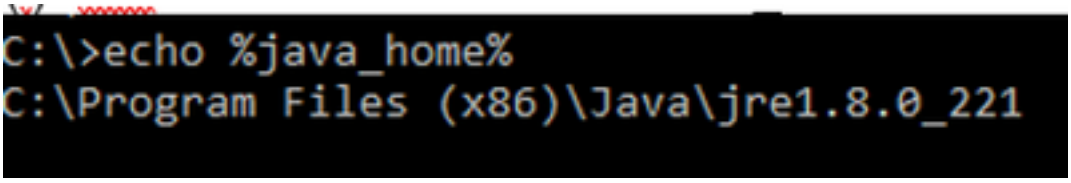
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b) Copiare il certificato dal percorso **C:\Cisco\CVP\conf\security\wsm.crt**, rinominarlo in **wsmcsX.crt** e spostarlo in una cartella temporanea sul server ADS.

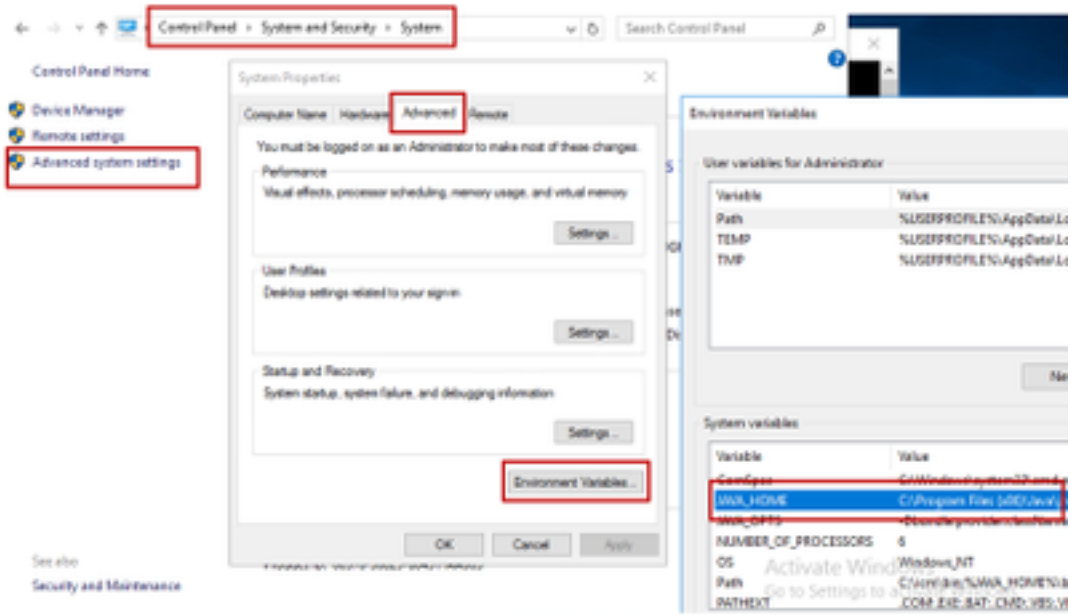
Passaggio 2. Importare il certificato WSM dei server CVP nel server ADS

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

(i) Comando CLI > **echo %JAVA_HOME%**



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



In PCCE 12.5 il percorso predefinito è **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_cvp} -file c:\temp\certs\wsmcsX.crt
```

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

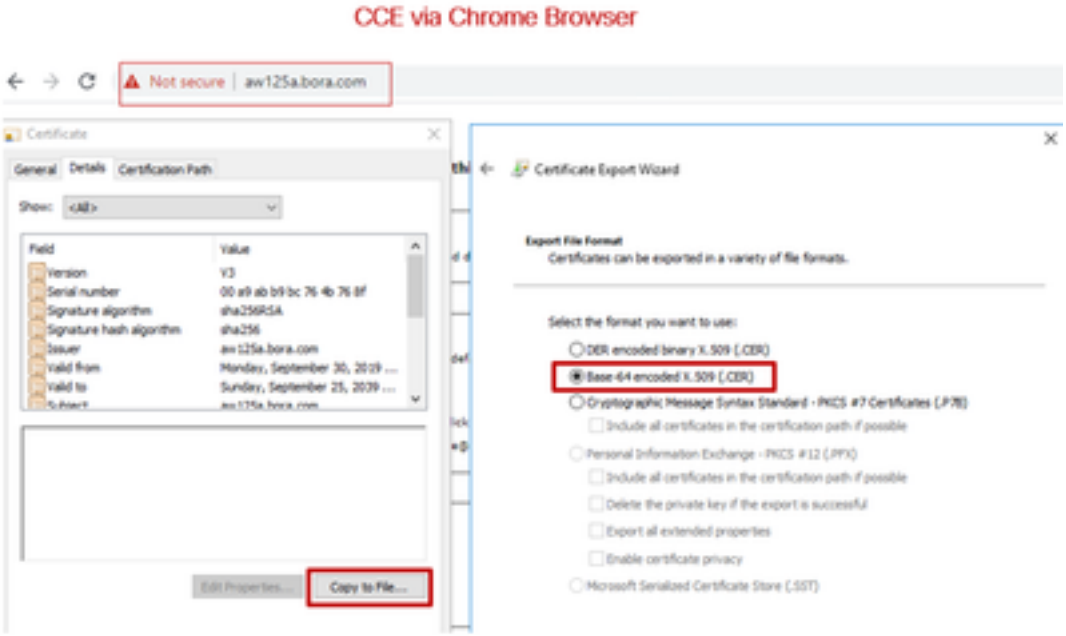
d) Riavviare il servizio Apache Tomcat sui server ADS.

Passaggio 3. Esportare il certificato del server ADS

Per il server di report CVP è necessario esportare il certificato ADS e importarlo nel server di report. Di seguito sono riportati i passaggi:

(i) Nel 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**



Nota: Selezionare l'opzione Codificato Base 64 X.509 (.CER).

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

(i) Copiare il certificato sui server CVP e sul server CVP Reporting nella directory **C:\Cisco\CVP\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\ICM{svr}[ab].cer
```

Eseguire la stessa procedura per altri 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. Esportare i certificati del server applicazioni della piattaforma VOS.

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

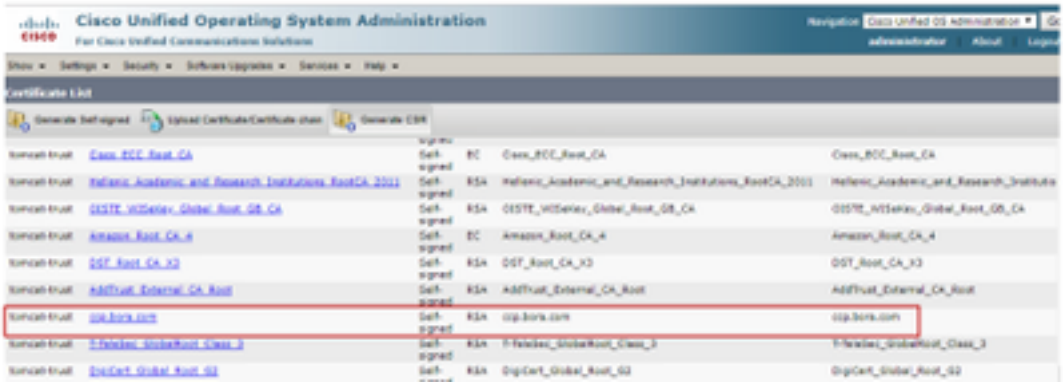
Questo processo è applicabile a tutte le applicazioni VOS, quali:

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

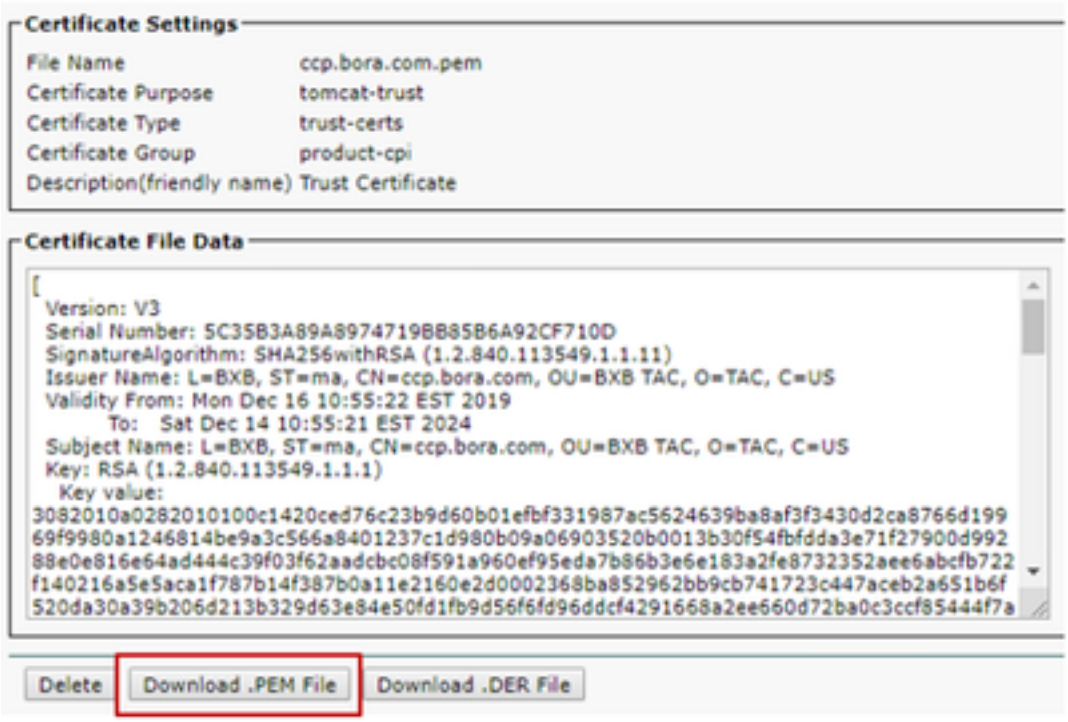
Passaggio 1. Esportare i certificati del server applicazioni della piattaforma VOS.

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

(ii) 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 gli stessi passaggi per il sottoscrittore.

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

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.cer
```

Riavviare il servizio Apache Tomcat sui server ADS.

> **Nota:** Esegui la stessa attività su altri server ADS

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

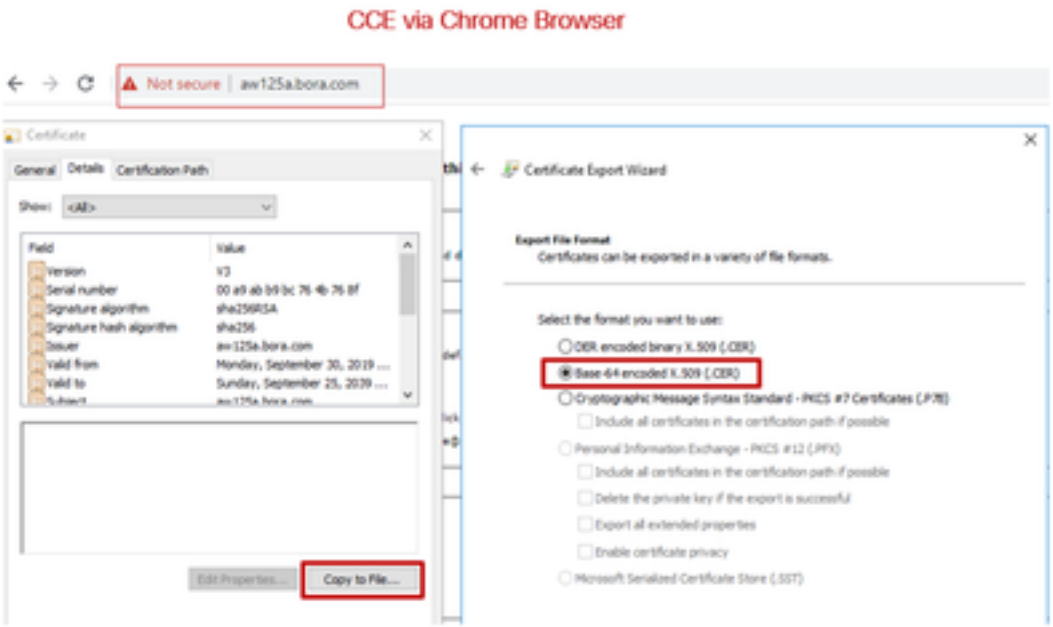
Passaggio 2: Esporta certificato DFP (Diagnostic Framework Portico) da server Rogger e PG

Passaggio 3: Importa certificati in server ADS

Passaggio 1. Esportare il certificato IIS dai 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**

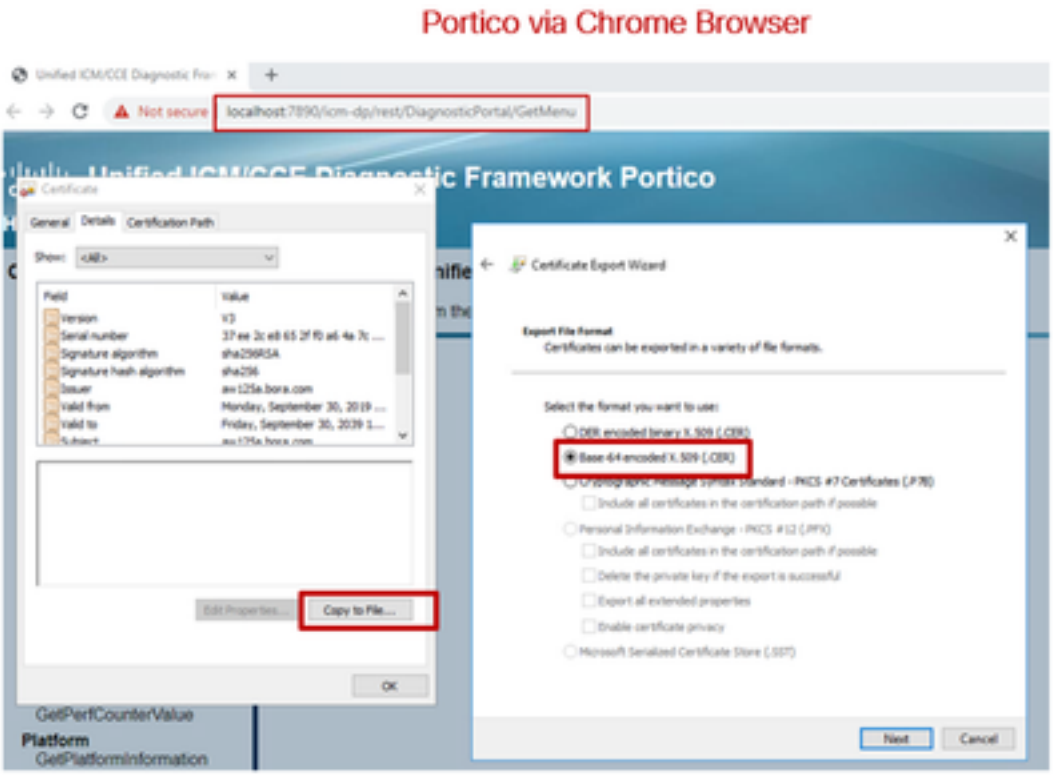


> **Nota:** Selezionare l'opzione Codificato Base 64 X.509 (.CER).

Passaggio 2. Esportare il certificato DFP (Diagnostic Framework Portico) dai 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



Nota: Selezionare l'opzione Codificato Base 64 X.509 (.CER).

Passaggio 3. Importare certificati nel server ADS

Comando per importare i certificati autofirmati di IIS nel server ADS. 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: Importa tutti i certificati server esportati in tutti i server ADS.

Comando per importare i certificati autofirmati di diagnostica nel server ADS

```
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: Importa tutti i certificati server esportati in tutti i server ADS.

Riavviare il servizio Apache Tomcat sui server ADS.

Sezione 4: 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
- 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