PCCE 솔루션에서 자체 서명 인증서 교환

목차

소개

이 문서에서는 Cisco PCCE(Packaged Contact Center Enterprise) 솔루션의 주요 관리 서버(ADS/AW)와 다른 애플리케이션 서버 간에 자체 서명 인증서를 교환하는 방법에 대해 설명합니다.

기고자: Anuj Bhatia, Robert Rogier 및 Ramiro Amaya, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- PCCE 릴리스 12.5(1)
- CVP(Customer Voice Portal) 릴리스 12.5(1)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- PCCE 12.5(1)
- CVP 12.5(1)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경

12.x의 PCCE 솔루션에서 모든 디바이스는 기본 AW 서버에서 호스팅되는 SPOG(Single Pane of Glass)를 통해 제어됩니다. PCCE 12.5(1) 버전의 SRC(security-management-compliance)로 인해 솔루션의 SPOG와 다른 서버 간의 모든 통신은 보안 HTTP 프로토콜을 통해 엄격하게 수행됩니다.

인증서는 SPOG와 다른 디바이스 간의 원활한 보안 통신을 위해 사용됩니다. 자체 서명 인증서 환경에서는 서버 간 인증서 교환이 필수 조건이 됩니다. 이 인증서 교환은 Smart Licensing, Webex Experience Management(WXM) 및 CVA(Customer Virtual Assistant)와 같은 12.5(1) 버전에 있는 새로운 기능을 활성화하는 데 필요합니다.

절차

자체 서명 인증서를 내보내는 구성 요소와 자체 서명 인증서를 가져와야 하는 구성 요소입니다.

자. 주 AW 서버: 이 서버에는 다음 위치의 인증서가 필요합니다.

- Windows 플랫폼: ICM: 라우터 및 로거(Rogger){A/B}, PG(주변 장치 게이트웨이){A/B}, 모든 ADS 및 ECE(Email and Chat) 서버. 참고: IIS 및 진단 프레임워크 인증서가 필요합니다.CVP: CVP 서버, CVP 보고 서버 참고 1: 서버의 WSM(Web Service Management) 인증서가 필요합니다.참고 2: 인증서는 FQDN(Fully Qualified Domain Name)이어야 합니다.
- VOS 플랫폼: Cloud Connect, Cisco VB(Virtual Voice Browser), Cisco CUCM(Unified Call Manager), Finesse, Cisco CUIC(Unified Intelligent Center), LD(Live Data), IDS(Identity Server) 및 기타 해당 서버.

솔루션의 다른 ADS 서버에도 마찬가지입니다.

(ii) 라우터 \ 로거 서버: 이 서버에는 다음 위치의 인증서가 필요합니다.

- Windows 플랫폼: 모든 ADS 서버 IIS 인증서

(iii) CUCM PG 서버: 이 서버에는 다음 위치의 인증서가 필요합니다.

- VOS 플랫폼: CUCM 게시자입니다. 참고: CUCM 서버에서 JTAPI 클라이언트를 다운로드하는 데 필요합니다.

(iv) CVP 서버: 이 서버에는

- Windows 플랫폼: 모든 ADS 서버 IIS 인증서
- VOS 플랫폼: WXM 통합을 위한 Cloud Connect 서버, 보안 SIP 및 HTTP 통신을 위한 VB 서버
.

(v) CVP 보고 서버: 이 서버에는 다음 위치의 인증서가 필요합니다.

- Windows 플랫폼: 모든 ADS 서버 IIS 인증서

(vi) VB 서버: 이 서버에는 다음 위치의 인증서가 필요합니다.

- Windows 플랫폼: CVP VXML 서버(보안 HTTP), CVP 호출 서버(보안 SIP)

솔루션에서 자체 서명 인증서를 효과적으로 교환하는 데 필요한 단계는 세 섹션으로 구분되어 있습니다.

섹션 1: CVP 서버와 ADS 서버 간 인증서 교환.

섹션 2: VOS 플랫폼 애플리케이션과 ADS 서버 간 인증서 교환.

섹션 3: 로거, PG 및 ADS 서버 간 인증서 교환

섹션 1: CVP와 ADS 서버 간 인증서 교환

이 교환을 성공적으로 완료하는 데 필요한 단계는 다음과 같습니다.

1단계. CVP 서버 WSM 인증서를 내보냅니다.

2단계. CVP 서버 WSM 인증서를 ADS 서버로 가져옵니다.

3단계. ADS 서버 인증서를 내보냅니다.

4단계. ADS 서버를 CVP 서버 및 CVP 보고 서버로 가져옵니다.

1단계. CVP 서버 인증서 내보내기

CVP 서버에서 인증서를 내보내기 전에 서버의 FQDN을 사용하여 인증서를 다시 생성해야 합니다. 그렇지 않으면 Smart Licensing, CVA 및 SPOG와의 CVP 동기화와 같은 일부 기능에서 문제가 발생할 수 있습니다.

> **주의:** 시작하기 전에 다음을 수행해야 합니다.

- 키 저장소 암호를 가져옵니다. 다음 명령을 실행합니다.
  추가 %CVP_HOME%\conf\security.properties
- %CVP_HOME%\conf\security 폴더를 다른 폴더에 복사합니다.
- 명령 창을 관리자로 열어 명령을 실행합니다.

> **참고:** keytool 매개 변수 -storepass를 사용하여 이 문서에 사용된 명령을 간소화할 수 있습니다. 모든 CVP 서버의 경우 지정된 security.properties 파일에서 가져온 비밀번호를 붙여넣습니다. ADS 서버의 경우 비밀번호를 입력합니다. **변경**

CVP 서버에서 인증서를 다시 생성하려면 다음 단계를 수행합니다.

(i) 서버에 인증서 나열

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

> **참고:** CVP 서버에는 다음과 같은 자체 서명 인증서가 있습니다. wsm_certificate , vxml_certificate , callserver_certificate 키 도구의 -v 매개 변수를 사용하는 경우 각 인증서에 대한 자세한 정보를 볼 수 있습니다. 또한 keytool.exe list 명령의 끝에 ">" 기호를 추가하여 출

력을 텍스트 파일로 보낼 수 있습니다. 예를 들면 다음과 같습니다. > test.txt

(ii) 이전 자체 서명 인증서 삭제

CVP servers: 자체 서명 인증서를 삭제하는 명령:

```
%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
```

CVP 보고 서버: 자체 서명 인증서를 삭제하는 명령:

```
%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
```

> **참고:** CVP 보고 서버에는 이러한 자체 서명 인증서 wsm_certificate, callserver_certificate가 있습니다.

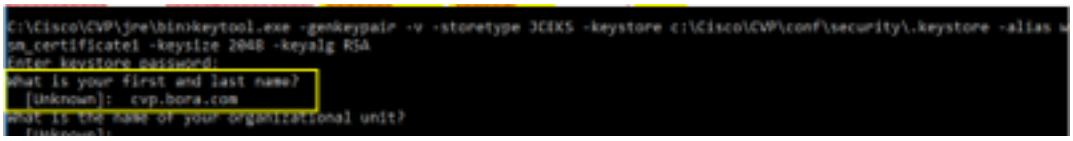
(iii) 서버의 FQDN을 사용하여 새 자체 서명 인증서 생성

CVP 서버

WSM용 자체 서명 인증서를 생성하는 명령:

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

서버의 FQDN을 지정합니다. 질문에 **이름과 성은 무엇입니까**?



다음과 같은 기타 질문을 완료합니다.

조직 구성 단위 이름이 무엇입니까?

[알 수 없음]: <OU 지정>

귀사의 이름은 무엇입니까?

[알 수 없음]: <조직 이름 지정>

구/군/시 이름이 무엇입니까?

[알 수 없음]: <구/군/시 이름 지정>

시/도 이름이 무엇입니까?

[알 수 없음]: <시/도의 이름 지정>

이 유닛의 2자 국가 코드는 무엇입니까?

[알 수 없음]: <두 글자로 된 국가 코드 지정>

다음 두 입력에 **yes**를 지정합니다.

vxml_certificate 및 callserver_certificate에 대해 동일한 단계를 수행합니다.

```
%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
```

CVP 통화 서버를 재부팅합니다.

CVP 보고 서버

WSM용 자체 서명 인증서를 생성하는 명령:

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

쿼리에 대한 서버의 FQDN을 **지정하시겠습니까?** CVP 서버와 동일한 단계를 수행합니다.

callserver_certificate에 대해 동일한 단계를 수행합니다.

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

보고 서버를 재부팅합니다.

> **참고:** 기본적으로 자체 서명 인증서는 2년 동안 생성됩니다. -validity XXXX를 사용하여 인증서가 재생성될 때 만료 날짜를 설정하고, 그렇지 않으면 인증서가 90일 동안 유효합니다. 대부분의 경우 3-5년은 적절한 검증 시간이 되어야 합니다.

다음은 몇 가지 표준 유효성 입력입니다.

1년	365
2년	730
3년	1095
4년	1460

5년	1895
10년	3650

주의: 12.5 인증서에서는 **SHA 256**, Key Size **2048** 및 Encryption Algorithm **RSA**가 되어야 합니다. 다음 매개변수를 사용하여 다음 값을 설정합니다. -keyalg RSA 및 -keysize 2048. CVP 키 저장소 명령에는 -storetype JCEKS 매개 변수가 포함되어야 합니다. 이렇게 하지 않으면 인증서, 키 또는 더 나쁜 키 저장소가 손상될 수 있습니다.

(iv) CVP 및 보고 서버에서 wsm_Certificate 내보내기

a) 각 CVP 서버에서 임시 위치로 WSM 인증서를 내보내고 원하는 이름으로 인증서 이름을 바꿉니다. wsmcsX.crt로 이름을 바꿀 수 있습니다. "X"를 고유한 숫자 또는 문자로 바꿉니다. wsmcsa.crt, wsmcsb.crt입니다.

자체 서명 인증서를 내보내는 명령:

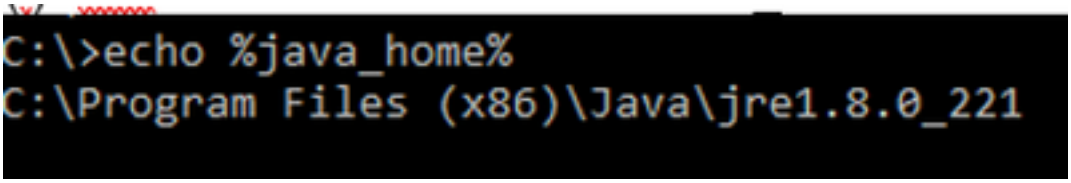
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b) C:\Cisco\CVP\conf\security\wsm.crt 경로에서 인증서를 복사하고 **이름을 wsmcsX**.*crt*로 변경하고 ADS 서버의 임시 폴더로 옮깁니다.

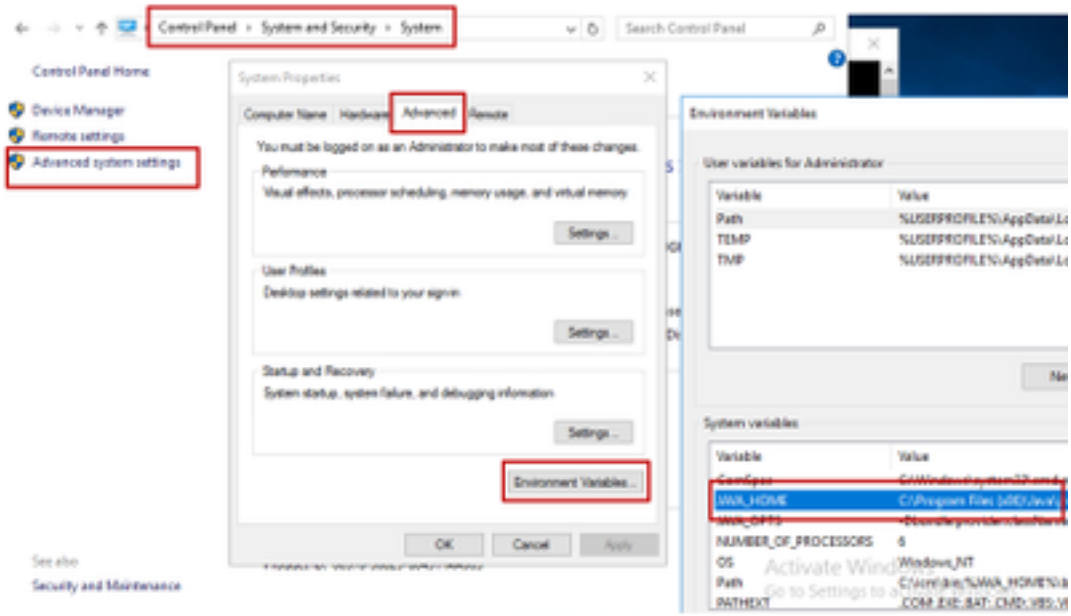
2단계. CVP 서버 WSM 인증서를 ADS 서버로 가져오기

ADS 서버에서 인증서를 가져오려면 Java 툴세트의 일부인 키 도구를 사용해야 합니다. 이 툴이 호스팅되는 Java 홈 경로를 찾을 수 있는 방법에는 두 가지가 있습니다.

(i) CLI 명령 > **에코 %JAVA_HOME%**



(ii) 이미지에 표시된 대로 **고급 시스템 설정**을 통해 수동으로 설정합니다.



PCCE 12.5의 기본 경로는 C:\Program **Files (x86)\Java\jre1.8.0_221\bin입니다.**

자체 서명 인증서를 가져오는 명령:

```
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
```

참고: 구축의 각 CVP에 대해 명령을 반복하고 다른 ADS 서버에서 동일한 작업을 수행합니다.

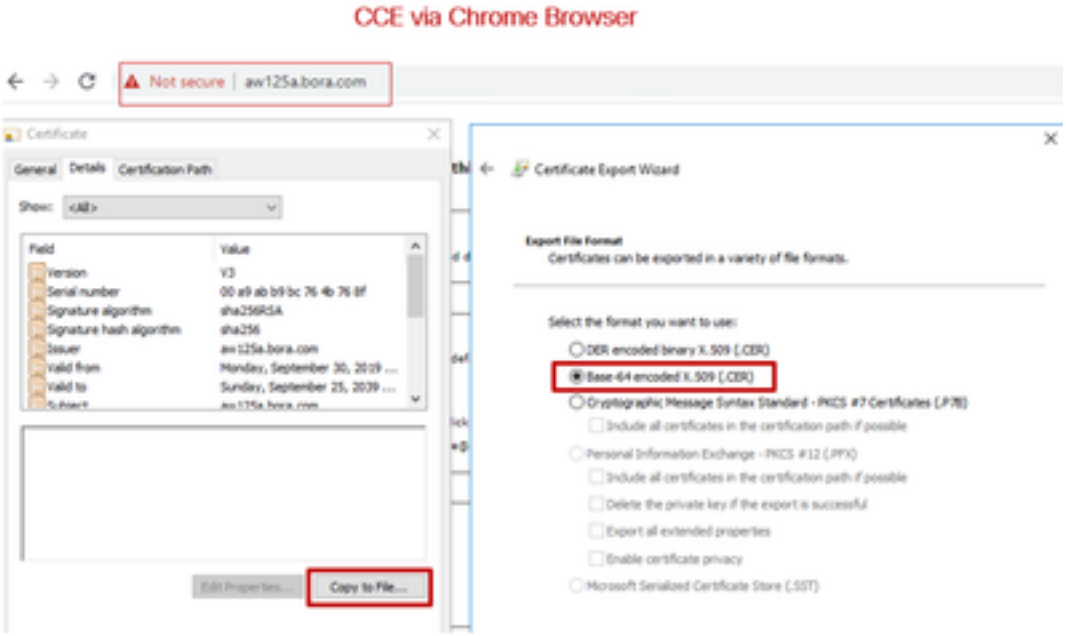
d) ADS 서버에서 Apache Tomcat 서비스를 재시작합니다.

3단계. ADS 서버 인증서 내보내기

CVP 보고 서버의 경우 ADS 인증서를 내보내고 Reporting 서버로 가져와야 합니다. 다음은 단계입니다.

(i) 브라우저에서 ADS 서버에서 서버 URL https://으로 이동합니다. **{servername}**

(ii) 임시 폴더에 인증서를 저장합니다. 예를 들면 다음과 같습니다. **c:\temp\certs** 인증서 이름을 **ADS{svr}[ab].cer로 지정합니다.**



참고: Base-64 인코딩 X.509(.CER) 옵션을 선택합니다.

4단계. ADS 서버를 CVP 서버 및 보고 서버로 가져오기

(i) C:\Cisco\CVP\conf\security디렉토리에 있는 CVP 서버 및 CVP 보고 서버에 인증서를 **복사합니다.**

(ii) CVP 서버 및 CVP 보고 서버로 인증서를 가져옵니다.

```
%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
```

다른 ADS 서버에 대해 동일한 단계를 수행합니다.

(iii) CVP 서버 및 보고 서버 재시작

섹션 2: VOS 플랫폼 애플리케이션과 ADS 서버 간 인증서 교환

이 교환을 성공적으로 완료하는 데 필요한 단계는 다음과 같습니다.

1단계. VOS 플랫폼 애플리케이션 서버 인증서를 내보냅니다.

2단계. VOS 플랫폼 애플리케이션 인증서를 ADS 서버로 가져옵니다.

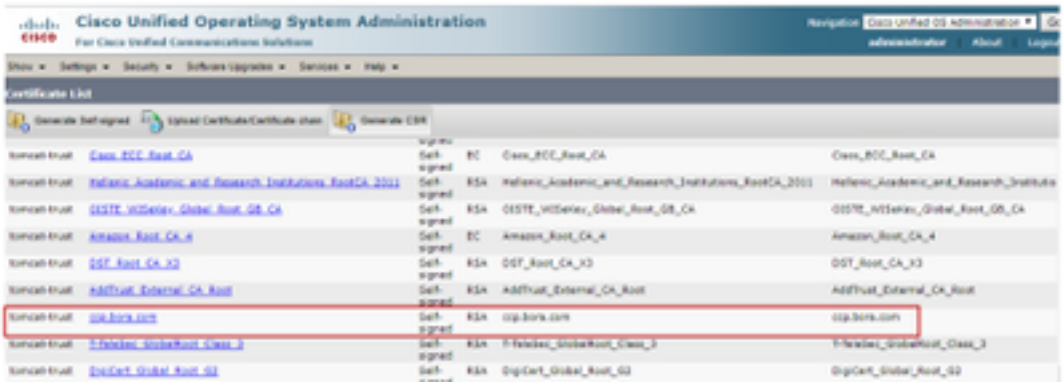
이 프로세스는 다음과 같은 모든 VOS 애플리케이션에 적용됩니다.

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- 클라우드 연결

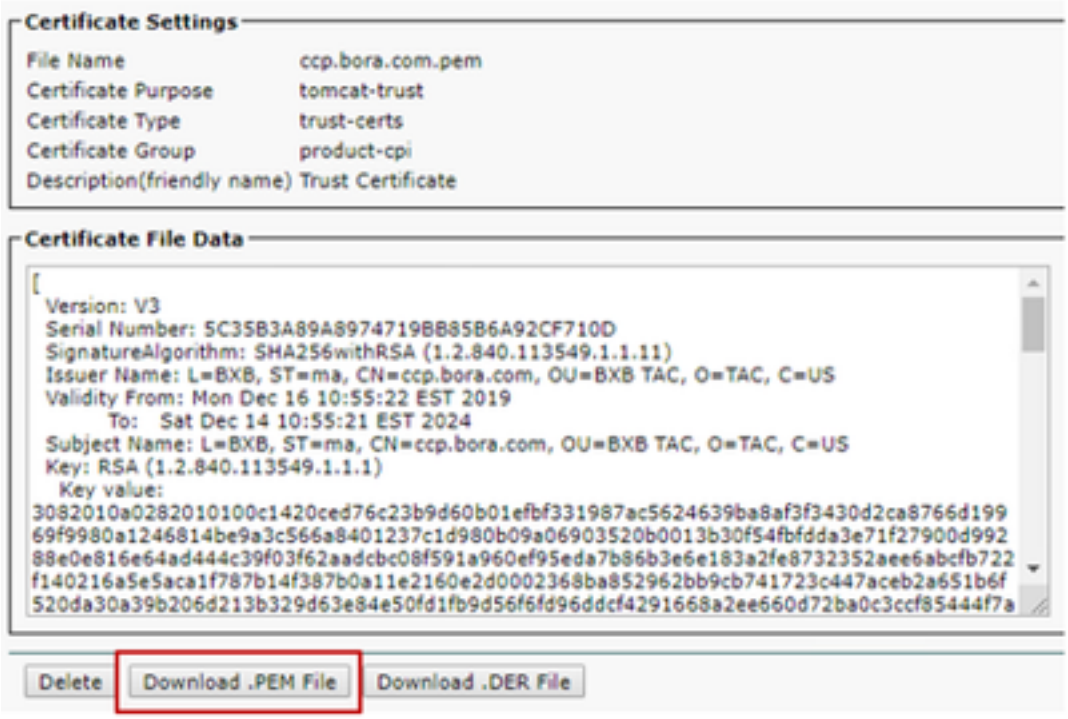
1단계. VOS 플랫폼 애플리케이션 서버 인증서를 내보냅니다.

(i) Cisco Unified Communications 운영 체제 관리 페이지로 이동합니다.
https://FQDN:8443/cmplatform

(ii) Security(**보안**) > **Certificate Management(인증서 관리)**로 이동하고 tomcat-**trust** 폴더에서 애플리케이션 기본 서버 인증서**를** 찾습니다.



(iii) 인증서를 선택하고 다운로드 .PEM 파일을 클릭하여 ADS 서버의 임시 폴더에 저장합니다.



참고: 가입자에 대해 동일한 단계를 수행합니다.

2단계. VOS 플랫폼 애플리케이션을 ADS 서버로 가져오기

키 도구를 실행할 경로: **C:\Program 파일(x86)\Java\jre1.8.0_221\bin**

자체 서명 인증서를 가져오는 명령:

```
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
```

ADS 서버에서 Apache Tomcat 서비스를 다시 시작합니다.

참고: 다른 ADS 서버에서 동일한 작업 수행

섹션 3: 로거, PG 및 ADS 서버 간 인증서 교환

이 교환을 성공적으로 완료하는 데 필요한 단계는 다음과 같습니다.

1단계: Rogger 및 PG 서버에서 IIS 인증서 내보내기

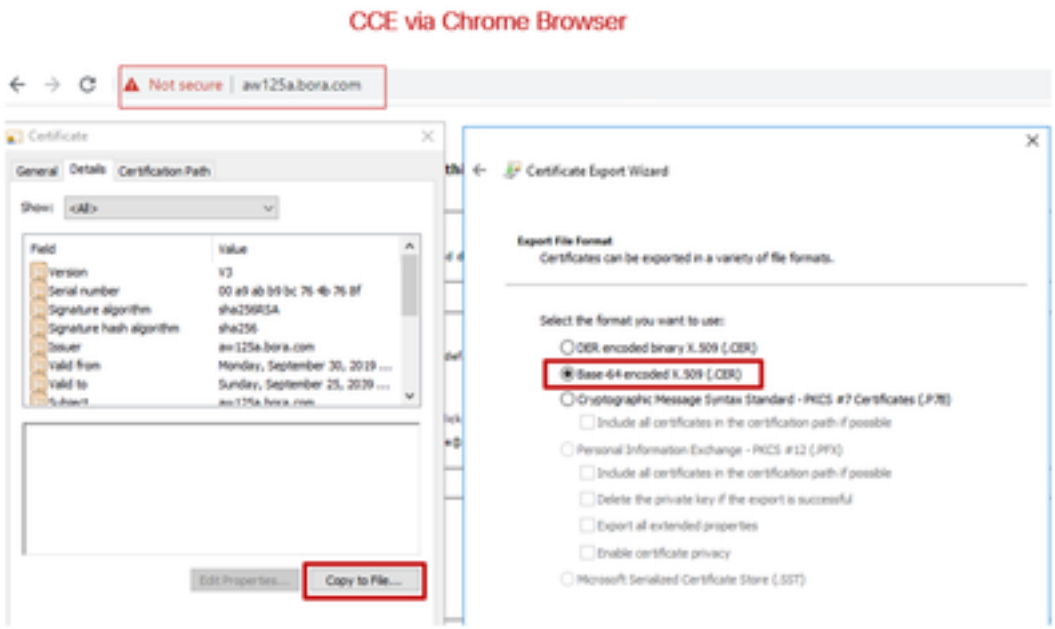
2단계: Rogger 및 PG 서버에서 DFP(Diagnostic Framework Portico) 인증서 내보내기

3단계: ADS 서버로 인증서 가져오기

1단계. Rogger 및 PG 서버에서 IIS 인증서 내보내기

(i) 브라우저에서 ADS 서버에서 서버(로거, PG) url로 이동합니다. **https://{servername}**

(ii) 임시 폴더에 인증서를 저장합니다(예: **c:\temp\certs). 인증서 이름을 ICM{svr}[ab].cer로 지정합니다.**

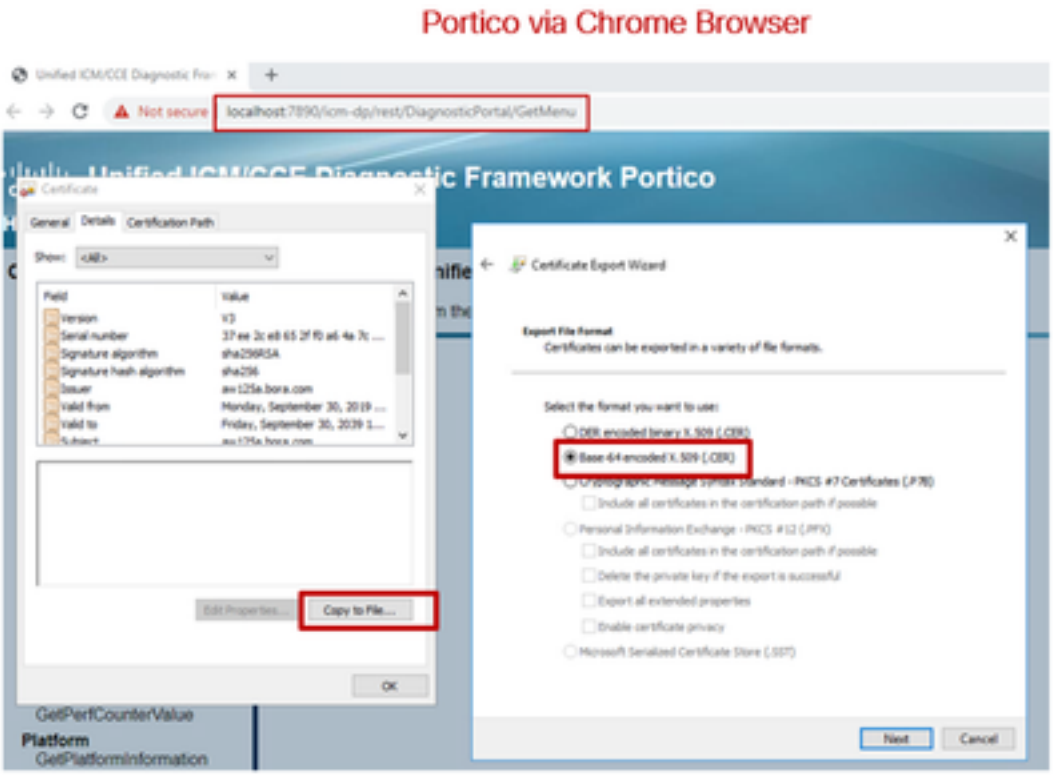


참고: Base-64 인코딩 X.509(.CER) 옵션을 선택합니다.

2단계. Rogger 및 PG 서버에서 DFP(Diagnostic Framework Portico) 인증서 내보내기

(i) 브라우저에서 ADS 서버에서 서버(로거, PG) DFP URL: ***https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion***

(ii) 인증서를 c:\temp\certs 폴더에 저장하고 인증서 이름을 dfp{svr}[ab].cer로 지정합니다.



참고: Base-64 인코딩 X.509(.CER) 옵션을 선택합니다.

3단계. ADS 서버로 인증서 가져오기

IIS 자체 서명 인증서를 ADS 서버로 가져오는 명령입니다. 키 도구를 실행할 경로: **C:\Program 파일 (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
```

참고: 모든 ADS 서버로 내보낸 모든 서버 인증서를 가져옵니다.

진단 자체 서명 인증서를 ADS 서버로 가져오는 명령

```
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
```

참고: 모든 ADS 서버로 내보낸 모든 서버 인증서를 가져옵니다.

ADS 서버에서 Apache Tomcat 서비스를 다시 시작합니다.

섹션 4: CVP CallStudio 웹서비스 통합

웹 서비스 요소 및 Rest_Client 요소에 대한 보안 통신을 설정하는 방법에 대한 자세한 내용을 보려면

Cisco Unified CVP VXML Server 및 Cisco Unified Call Studio 릴리스 12.5(1) - 웹 서비스 통합 [Cisco Unified Customer Voice Portal] - Cisco 사용 설명서를 참조하십시오.

관련 정보

- CVP 구성 가이드: CVP 컨피그레이션 가이드 - 보안
- UCCE 컨피그레이션 가이드: UCCE 컨피그레이션 가이드 - 보안
- PCCE 관리 가이드: PCE 관리 가이드 - 보안
- UCCE 자체 서명 인증서: Exchange UCCE 자체 서명 인증서
- CCE 12.5(1)에서 OpenJDK로 설치 및 마이그레이션: CCE OpenJDK 마이그레이션
- CVP 12.5(1)의 OpenJDK 설치 및 마이그레이션: CVP OpenJDK 마이그레이션