PCCE 12.6 솔루션에서 자체 서명 인증서 교환

목차

소개

이 문서에서는 Cisco PCCE(Packaged Contact Center Enterprise) 솔루션에서 자체 서명 인증서를 교환하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- PCCE 릴리스 12.6(2)
- CVP(Customer Voice Portal) 릴리스 12.6(2)
- VVB(Virtualized Voice Browser) 12.6(2)
- 관리 워크스테이션 / 관리 날짜 서버 (AW/ADS) 12.6(2)
- Cisco CUIC(Unified Intelligence Server)

- CCP(Customer Collaboration Platform) 12.6(2)
- ECE(Enterprise Chat and Email) 12.6(2)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

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

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 장치는 주 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 간의 인증서 교환이 필수적입니다.

절차

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

(i) 모든 AW/ADS 서버: 다음 서버의 인증서가 필요합니다.

- Windows 플랫폼:
  - ICM: 라우터 및 로거(Rogger){A/B}, 주변 장치 게이트웨이(PG){A/B}, 모든 AW/ADS 및 ECE 서버.

참고: IIS 및 DFP(Diagnostic Framework Portico)가 필요합니다.

  - CVP: CVP 서버, CVP 보고 서버

참고: 모든 서버의 WSM(Web Service Management) 인증서가 필요합니다. 인증서는 FQDN(Fully Qualified Domain Name)을 사용해야 합니다.

- VOS 플랫폼: Cloud Connect, Cisco VVB(Virtualized Voice Browser), CUCM(Cisco Unified Communication Manager), Finesse, CUIC(Cisco Unified Intelligence Center), LD(Live Data), IDS(Identity Server) 및 기타 해당 서버

(ii) 라우터 \ 로거 서버: 다음 서버의 인증서가 필요합니다.

- Windows 플랫폼: 모든 AW/ADS 서버는 IIS 인증서입니다.

(iii) PG 서버: 다음 서버의 인증서가 필요합니다.

- Windows 플랫폼: 모든 AW/ADS 서버는 IIS 인증서입니다.
- VOS 플랫폼: CUCM 게시자(CUCM PG 서버만 해당), Cloud Connect 및 CCP(MR PG 서버만 해당).

참고: CUCM 서버에서 JTAPI 클라이언트를 다운로드하는 데 필요합니다.

(iv) CVP 서버: 다음 서버에서 인증서를 요구합니다.

- Windows 플랫폼: 모든 ADS 서버 IIS 인증서
- VOS 플랫폼: Cloud Connect 서버, VVB 서버

(v) CVP 보고 서버: 이 서버에는 다음에서 제공하는 인증서가 필요합니다.

- Windows 플랫폼: 모든 ADS 서버 IIS 인증서

(vi) VVB 서버: 이 서버에는 다음에서 발급한 인증서가 필요합니다.

- Windows 플랫폼: 모든 ADS 서버 IIS 인증서, CVP 서버의 VXML 인증서 및 CVP 서버의 Callserver 인증서
- VOS 플랫폼: Cloud Connect 서버.

솔루션에서 자체 서명 인증서를 효과적으로 교환하는 데 필요한 단계는 세 개의 섹션으로 나뉩니다 .

섹션 1: CVP 서버와 ADS 서버 간의 인증서 교환

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

섹션 3: 플레이어, PG 및 ADS 서버 간의 인증서 교환

섹션 1: CVP와 ADS 서버 간의 인증서 교환

이 교환을 성공적으로 완료하는 데 필요한 단계는 다음과 같습니다.

1단계. CVP 서버 WSM 인증서 내보내기

2단계. CVP 서버 WSM 인증서를 ADS 서버로 가져옵니다.

3단계. ADS 서버 인증서 내보내기

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 스마트 라이센싱, VAV(Virtual Agent Voice), SPOG와의 CVP 동기화 등의 몇 가지 기능에서 문제가 발생할 수 있습니다.

주의: 시작하기 전에 다음을 수행해야 합니다.
1. 관리자로 명령 창을 엽니다.
2. 12.6.2의 경우 키 저장소 암호를 식별하려면 %CVP_HOME%\bin 폴더로 이동하여 DecryptKeystoreUtil.bat 파일을 실행합니다.
3. 12.6.1의 경우 키 저장소 암호를 식별하려면 명령을 실행합니다. %CVP_HOME%\conf\security.properties를 더 입력합니다.
4. keytool 명령을 실행할 때 이 비밀번호가 필요합니다.
5. %CVP_HOME%\conf\security\ 디렉터리에서 명령을 실행하고 .keystore backup.keystore를 복사합니다.

참고: keytool 매개 변수 -storepass를 사용하면 이 문서에서 사용되는 명령을 간소화할 수 있습니다. 모든 CVP 서버에 대해, 식별한 keytool 비밀번호를 제공합니다. ADS 서버의 경우 기본 비밀번호는 changeit입니다.

CVP 서버에서 인증서를 재생성하려면 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 keytool의 매개 변수 -v를 사용하면 각 인증서에 대한 자세한 정보를 볼 수 있습니다. 또한 keytool.exe list 명령의 끝에 ">" 기호를 추가하여 출력을 텍스트 파일로 보낼 수 있습니다(예: > test.txt).

(ii) 이전 자체 서명 인증서 삭제

CVP 서버: 자체 서명 인증서를 삭제하는 명령:

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

CVP 보고 서버: 자체 서명 인증서를 삭제하는 명령:

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

참고: CVP 보고 서버에는 다음과 같은 자체 서명 인증서(wsm_certificate, callserver_certificate)가 있습니다.

(iii) 서버의 FQDN으로 새 자체 서명 인증서를 생성합니다

CVP 서버

WSM에 대한 자체 서명 인증서를 생성하는 명령:

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

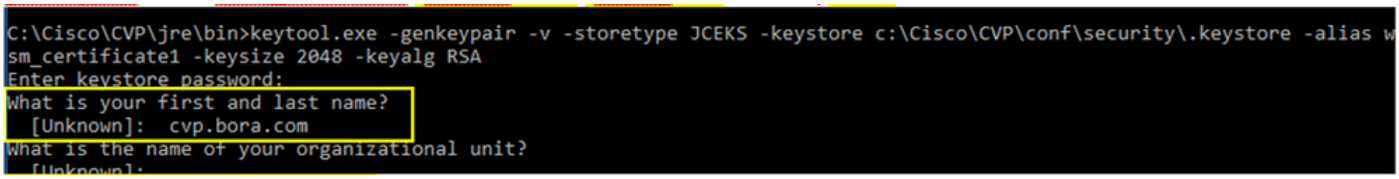
참고: 기본적으로 인증서는 2년간 생성됩니다. -validity XXXX를 사용하여 인증서가 재생성될 때 만료 날짜를 설정합니다. 그렇지 않으면 인증서가 90일 동안 유효하며 이 시간 전에 CA에서 서명해야 합니다. 이러한 인증서의 대부분은 3-5년이 적절한 검증 시간이어야 합니다.

다음은 몇 가지 표준 유효성 입력입니다.

1년	365
2년	730
3년	1095
4년	1460
5년	1895
10년	3650

주의: 12.5 인증서는 SHA 256, Key Size 2048 및 Encryption Algorithm RSA여야 합니다. -keyalg RSA 및 -keysize 2048 매개변수를 사용하여 이 값을 설정합니다. CVP 키 저장소 명령에는 -storetype JCEKS 매개 변수가 포함되어야 합니다. 이 작업을 수행하지 않으면 인증서, 키 또는 더 나쁜 키 저장소가 손상될 수 있습니다.

질문에 서버의 FQDN을 지정합니다. 이름과 성이 무엇입니까?



다음 기타 질문을 완료합니다.

조직 구성 단위의 이름은 무엇입니까?

[알 수 없음]: <OU 지정>

귀사의 이름은 무엇입니까?

[알 수 없음]: <조직 이름 지정>

시 또는 지역의 이름이 무엇입니까?

[알 수 없음]: <시/군/구 이름 지정>

시/도 이름이 어떻게 됩니까?

[알 수 없음]: <시/도 이름 지정>

이 유닛의 국가 번호는 몇 번입니까?

[알 수 없음]: <두 글자로 된 국가 코드 지정>

다음 두 입력에 대해 yes를 지정합니다.

vxml_certificate 및 callserver_certificate에 대해 동일한 단계를 수행합니다.

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

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

CVP 호출 서버를 재부팅합니다.

CVP 보고 서버

WSM에 대한 자체 서명 인증서를 생성하는 명령:

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

쿼리에 대한 서버의 FQDN을 지정하고 CVP 서버를 사용한 것과 동일한 단계를 계속합니다.

callserver_certificate에 대해 동일한 단계를 수행합니다.

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

보고 서버를 재부팅합니다.

(iv) CVP 및 보고 서버에서 wsm_Certificate 내보내기

a) 각 CVP 서버에서 임시 위치로 WSM 인증서를 내보내고 원하는 이름으로 인증서의 이름을 바꿉니다. 이름을 wsmcsX.crt로 바꿀 수 있습니다. "X"를 서버의 호스트 이름으로 바꿉니다. 예: wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt.

자체 서명 인증서를 내보내는 명령:

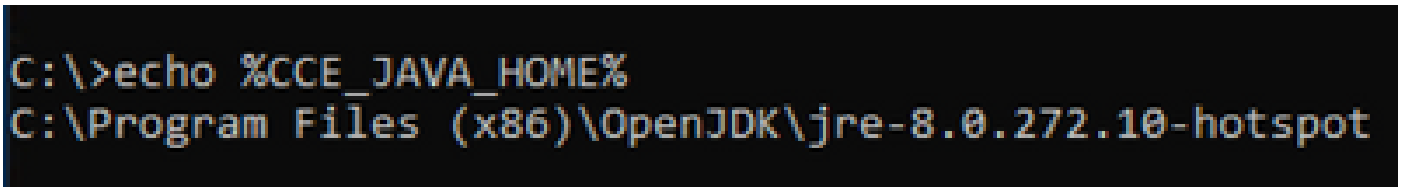
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -export -a
```

b) %CVP_HOME%\conf\security\wsm.crt 경로에서 인증서를 복사하고, 이름을 wsmcsX.crt로 바꾸고 ADS 서버의 임시 폴더로 옮깁니다.

2단계. ADS 서버로 CVP 서버 WSM 인증서 가져오기

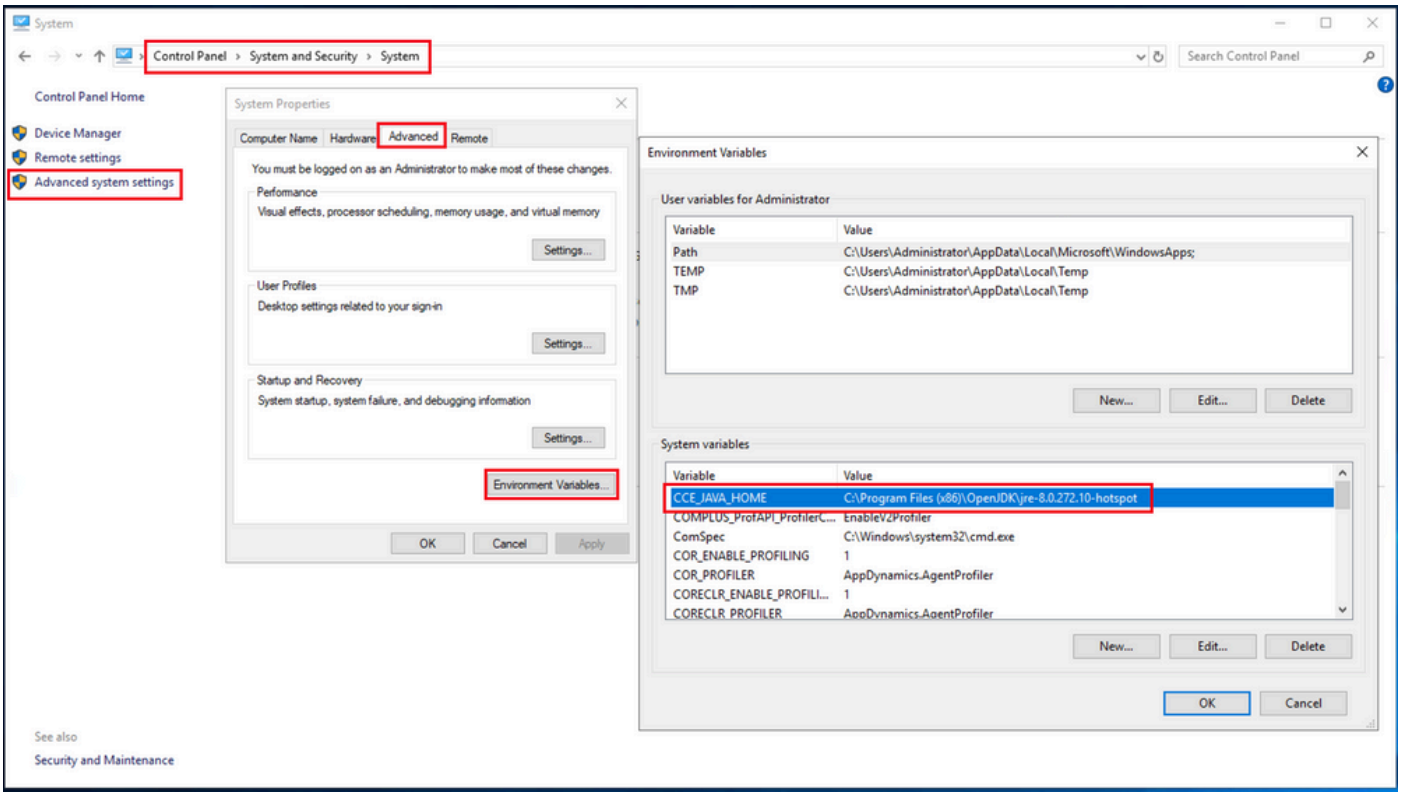
ADS 서버에서 인증서를 가져오려면 java 도구 세트의 일부인 keytool을 사용해야 합니다. 이 툴이 호스팅되는 Java 홈 경로를 찾을 수 있는 방법에는 몇 가지가 있습니다.

(i) CLI 명령 > 에코 %CCE_JAVA_HOME%



Java 홈 경로

(ii) 이미지에 표시된 대로 고급 시스템 설정을 통해 수동으로 수행합니다.



환경 변수

PCCE 12.6에서 OpenJDK의 기본 경로는 C:\Program Files (x86)\OpenJDK\jre-8.0.272.10-hotspot\bin입니다.

자체 서명 인증서를 가져오는 명령:

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

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

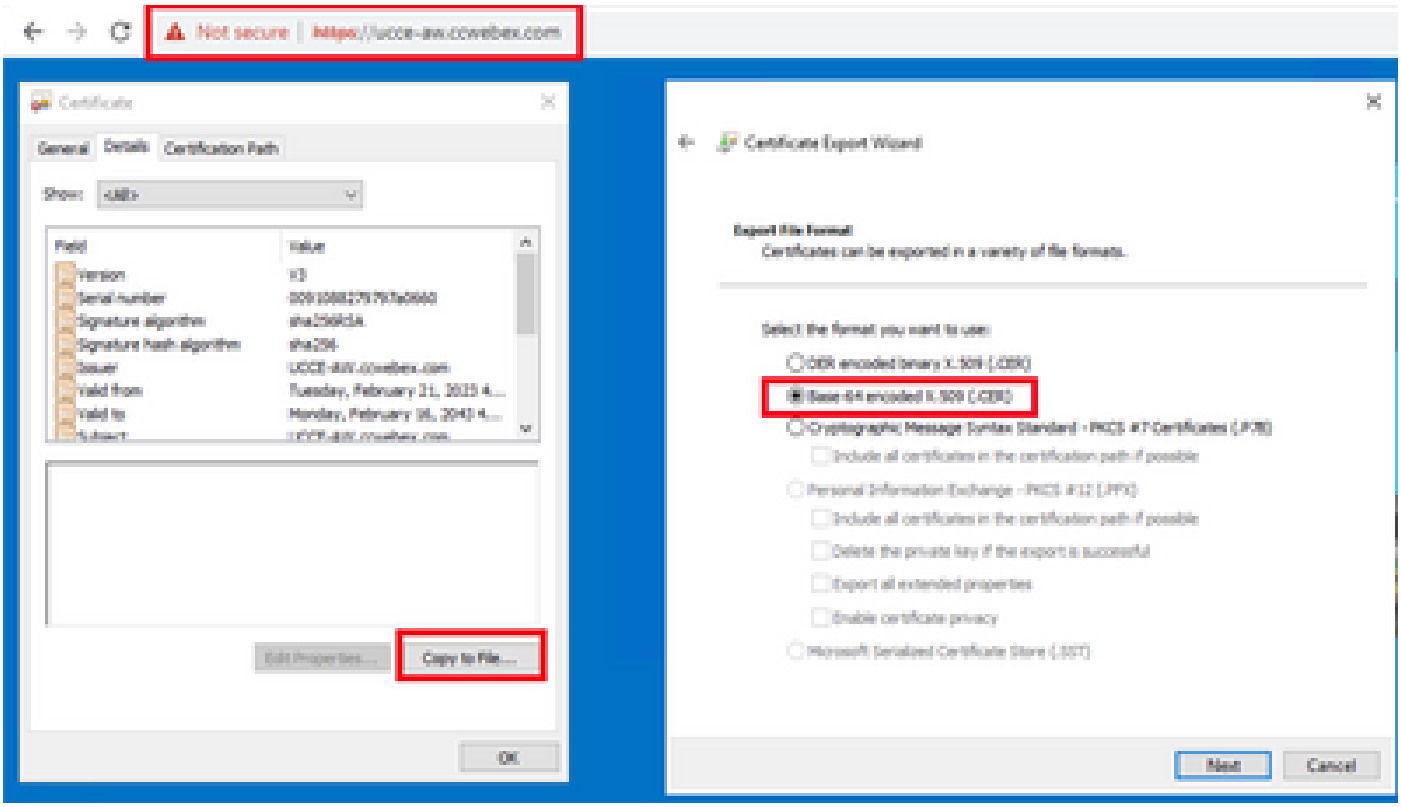
(iii) ADS 서버에서 Apache Tomcat 서비스를 재시작합니다.

3단계. ADS 서버 인증서 내보내기

ADS 인증서를 내보내는 단계는 다음과 같습니다.

(i) 브라우저에서 ADS 서버의 서버 url로 이동합니다. https://<servername>.

(ii) 인증서를 임시 폴더(예: c:\temp\certs)에 저장하고 인증서의 이름을 ADS<svr>[ab].cer로 지정합니다.



ADS 인증서 내보내기

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

4단계. ADS 서버 인증서를 CVP 서버 및 보고 서버로 가져오기

(i) 인증서를 %CVP_HOME%\conf\security 디렉토리의 CVP Servers 및 CVP Reporting Server에 복사합니다.

(ii) 인증서를 CVP 서버 및 CVP 보고 서버로 가져옵니다.

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

다른 ADS 서버 인증서에 대해서도 동일한 단계를 수행합니다.

(iii) CVP 서버 및 보고 서버를 다시 시작합니다.

섹션 2: VOS 플랫폼 애플리케이션과 ADS 서버 간의 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.

3단계. CUCM 플랫폼 애플리케이션 인증서를 CUCM PG 서버로 가져옵니다.

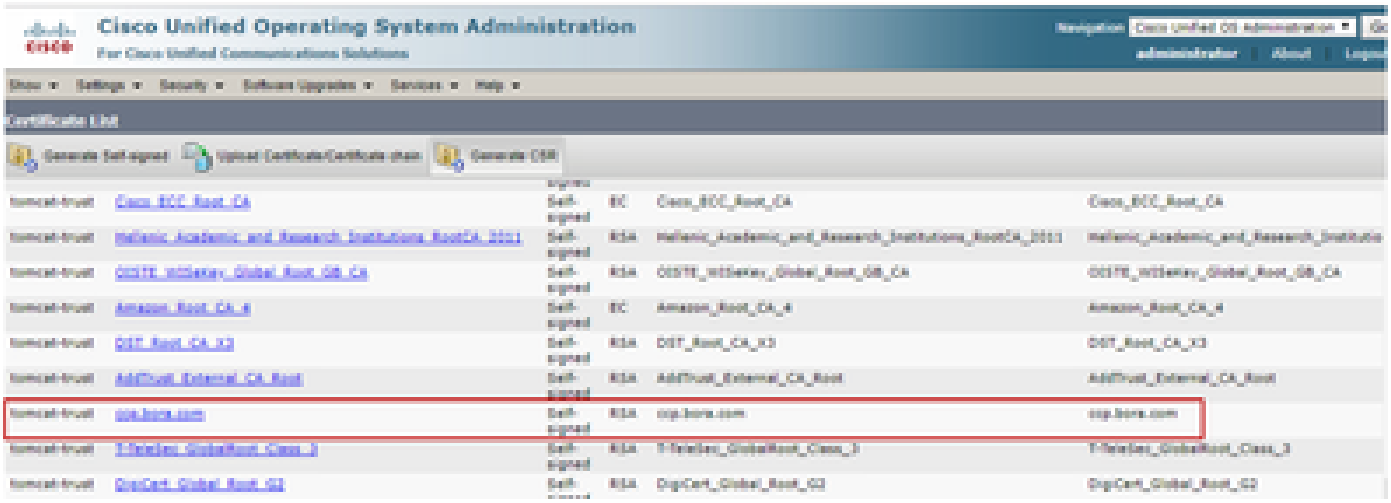
이 프로세스는 다음과 같은 모든 VOS 애플리케이션에 적용 가능합니다.

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

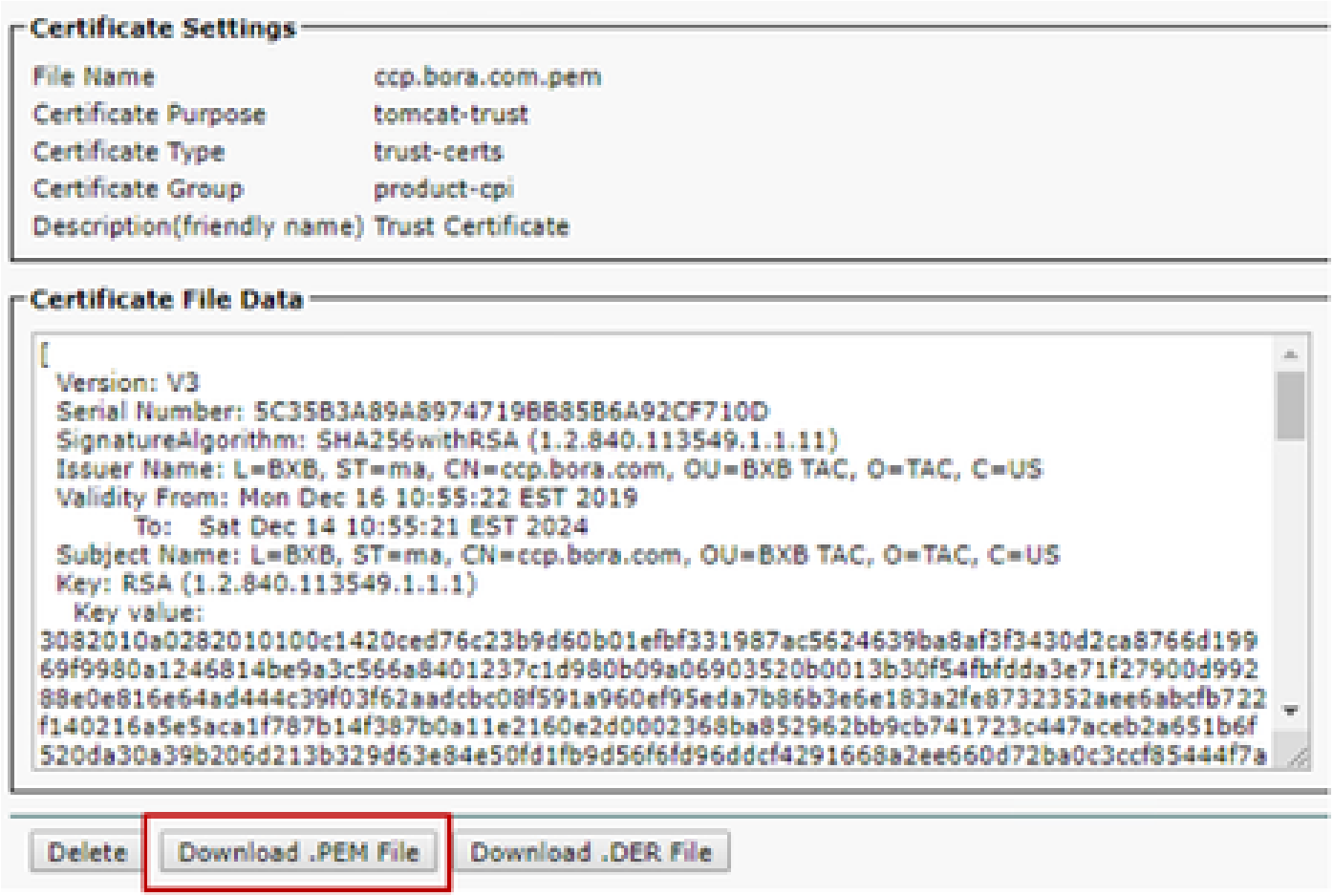
1단계. VOS 플랫폼 애플리케이션 서버 인증서를 내보냅니다.

(i) Cisco Unified Communications Operating System Administration(Cisco Unified Communications 운영 체제 관리) 페이지(https://FQDN:8443/cmplatform)로 이동합니다.

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



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



참고: 가입자에 대해 동일한 단계를 수행합니다.

2단계. ADS 서버에 VOS 플랫폼 애플리케이션 인증서 가져오기

키 도구 실행 경로: %CCE_JAVA_HOME%\bin

자체 서명 인증서를 가져오는 명령:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\vosapplicationX.cer -alias {fqdn_of_VOS>} -
```

ADS 서버에서 Apache Tomcat 서비스를 재시작합니다.

참고: 다른 ADS 서버에서 동일한 작업을 수행합니다.

3단계. CUCM 플랫폼 애플리케이션 인증서를 CUCM PG 서버로 가져오기

키 도구 실행 경로: %CCE_JAVA_HOME%\bin

자체 서명 인증서를 가져오는 명령:

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\cucmapplicationX.cer -alias {fqdn_of_cucm>}
```

PG 서버에서 Apache Tomcat 서비스를 재시작합니다.

참고: 다른 CUCM PG 서버에서도 동일한 작업을 수행합니다

섹션 3: 플레이어, PG 및 ADS 서버 간의 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 인증서 내보내기

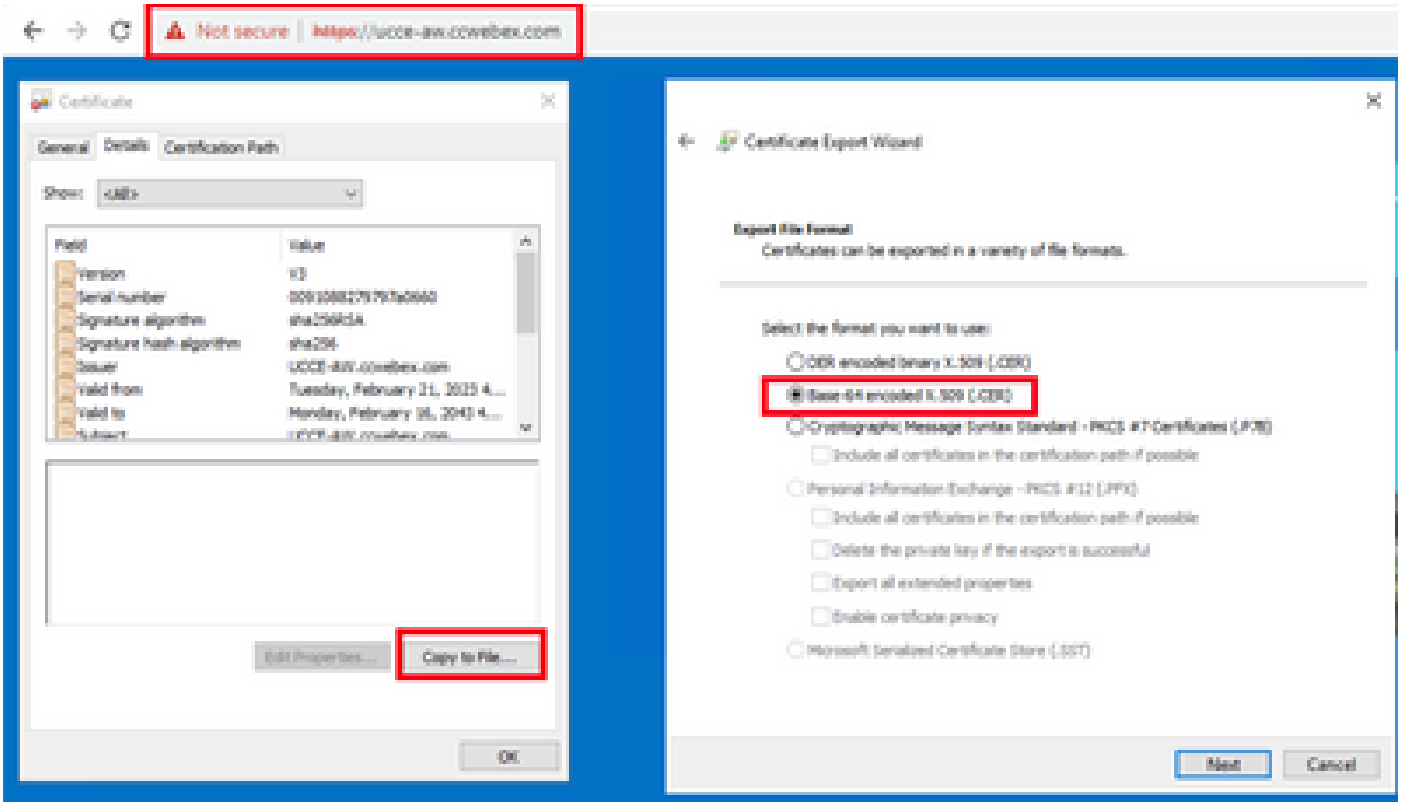
3단계. ADS 서버로 인증서 가져오기

4단계. Rogger 및 PG 서버로 ADS 인증서 가져오기

1단계. Rogger 및 PG 서버에서 IIS 인증서 내보내기

(i) 브라우저의 ADS 서버에서 서버(Rogers , PG) url: https://{servername}(으)로 이동합니다.

(ii) 인증서를 임시 폴더(예: c:\temp\certs)에 저장하고 인증서 이름을 ICM<svr>[ab].cer로 지정합니다.



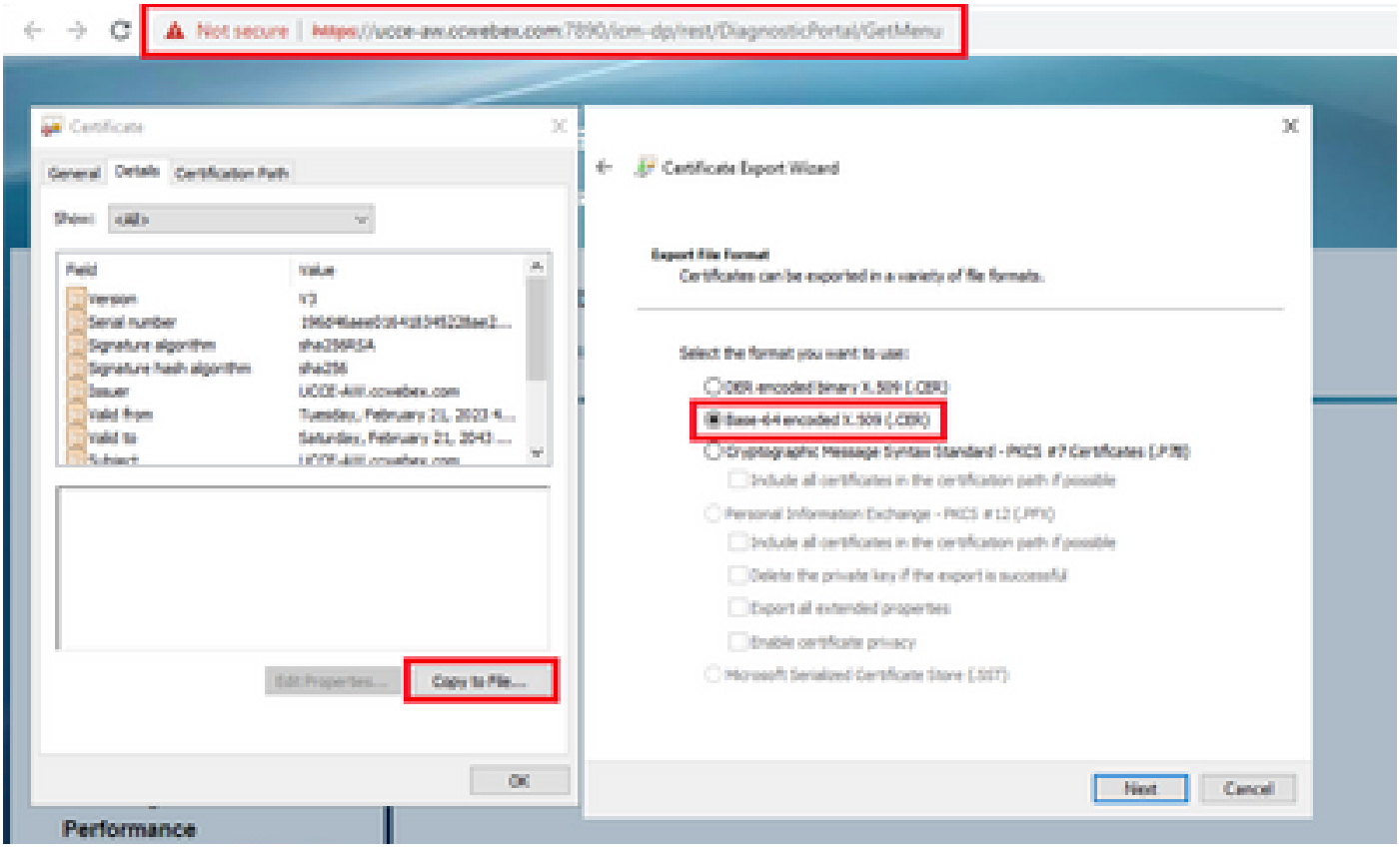
IIS 인증서 내보내기

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

2단계. Rogger 및 PG 서버에서 DFP 인증서 내보내기

(i) 브라우저에서 ADS 서버에서 서버(Rogers, PG) DFP url로 이동합니다.
https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion

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



DFP 인증서 내보내기

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

3단계. ADS 서버로 인증서 가져오기

IIS 자체 서명 인증서를 ADS 서버로 가져오는 명령입니다. 키 도구 실행 경로:
%CCE_JAVA_HOME%\bin

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\temp\certs\ICM<svr>[ab].cer -alias {fqdn_of_server}_II
```

참고: 모든 ADS 서버로 내보낸 모든 서버 인증서를 가져옵니다.

진단 자체 서명 인증서를 ADS 서버로 가져오는 명령

```
%CCE_JAVA_HOME%\bin\keytool.exe -import -file C:\Temp\certs\dfp<svr>[ab].cer -alias {fqdn_of_server}_DF
```

> 참고: 모든 ADS 서버로 내보낸 모든 서버 인증서를 가져옵니다.

ADS 서버에서 Apache Tomcat 서비스를 재시작합니다.

4단계. Rogger 및 PG 서버로 ADS 인증서 가져오기

Rogger 및 PG 서버로 IIS 자체 서명 인증서를 가져오는 명령입니다. 키 도구 실행 경로: %CCE_JAVA_HOME%\bin.

```
%CCE_JAVA_HOME%\bin\keytool -keystore ..\lib\security\cacerts  -import -storepass changeit -alias {fqdn
```

> 참고: 모든 Rogger 및 PG 서버로 내보낸 모든 ADS 서버 IIS 인증서를 가져옵니다.

Rogger 및 PG 서버에서 Apache Tomcat 서비스를 재시작합니다.

섹션 4: CVP CallStudio 웹 서비스 통합

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

Cisco Unified CVP VXML Server 및 Cisco Unified Call Studio 릴리스 12.6(2) - 웹 서비스 통합 [Cisco Unified Customer Voice Portal] - Cisco 사용 설명서를 참조하십시오.

관련 정보

- CVP 컨피그레이션 가이드 - 보안
- UCCE 보안 가이드
- PCCE 관리 가이드
- Exchange PCCE 자체 서명 인증서 - PCCE 12.5
- Exchange UCCE 자체 서명 인증서 - UCCE 12.5
- Exchange UCCE 자체 서명 인증서 - UCCE 12.6
- CA 서명 인증서 구현 - CCE 12.6
- Contact Center Uploader 툴을 사용하여 인증서 교환
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.