UCCE 12.6 솔루션에서 자체 서명 인증서 교환

목차

소개

이 문서에서는 UCCE(Unified Contact Center Enterprise) 솔루션에서 자체 서명 인증서를 교환하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- UCCE 릴리스 12.6(2)
- CVP(Customer Voice Portal) 릴리스 12.6(2)
- Cisco VVB(Virtualized Voice Browser)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- UCCE 12.6(2)
- CVP 12.6(2)
- Cisco VVB 12.6(2)
- CVP 운영 콘솔(OAMP)

- CVP 신규 OAMP(NOAMP)

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 정보

Rogger, PG(Peripheral Gateway), AW(Admin Workstation)/ADS(Administration Data Server), Finesse, CUIC(Cisco Unified Intelligence Center) 등의 핵심 애플리케이션이 포함된 새로운 기능의 UCCE 솔루션 컨피그레이션은 CCE(Contact Center Enterprise) 관리 페이지를 통해 수행됩니다. CVP, Cisco VVB 및 게이트웨이와 같은 IVR(Interactive Voice Response) 애플리케이션의 경우 NOAMP가 새로운 기능의 컨피그레이션을 제어합니다. CCE 12.5(1)에서는 SRC(Security-Management-Compliance) 때문에 보안 HTTP 프로토콜을 통해 CCE 관리자 및 NOAMP에 대한 모든 통신이 엄격하게 수행됩니다.

자체 서명 인증서 환경에서 이러한 애플리케이션 간의 원활한 보안 통신을 위해서는 서버 간의 인증서 교환이 필수적입니다. 다음 섹션에서는 다음 항목 간에 자체 서명 인증서를 교환하는 데 필요한 단계에 대해 자세히 설명합니다.

- CCE AW 서버 및 CCE 코어 애플리케이션 서버
- CVP OAMP 서버 및 CVP 구성 요소 서버

참고: 이 문서는 CCE 버전 12.6에만 적용됩니다. 다른 버전에 대한 링크는 관련 정보 섹션을 참조하십시오.

절차

CCE AW 서버 및 CCE 코어 애플리케이션 서버

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

CCE AW 서버: 이 서버에는 다음 서버의 인증서가 필요합니다.

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

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

- VOS 플랫폼: Finesse, CUIC, LD(Live Data), IDS(Identity Server), Cloud Connect 및 인벤토리 데이터베이스에 속하는 기타 적용 가능한 서버 솔루션의 다른 AW 서버에도 동일하게 적용됩니다.

라우터 \ 로거 서버: 이 서버에는 다음에서 온 인증서가 필요합니다.

- Windows 플랫폼: 모든 AW 서버 IIS 인증서

CCE용 자체 서명 인증서를 효과적으로 교환하는 데 필요한 단계는 다음 섹션으로 나뉩니다.

섹션 1: 라우터/로거, PG 및 AW 서버 간 인증서 교환
섹션 2: VOS 플랫폼 애플리케이션과 AW 서버 간의 인증서 교환

섹션 1: 라우터/로거, PG 및 AW 서버 간 인증서 교환

이 교환을 성공적으로 완료하는 데 필요한 단계는 다음과 같습니다.

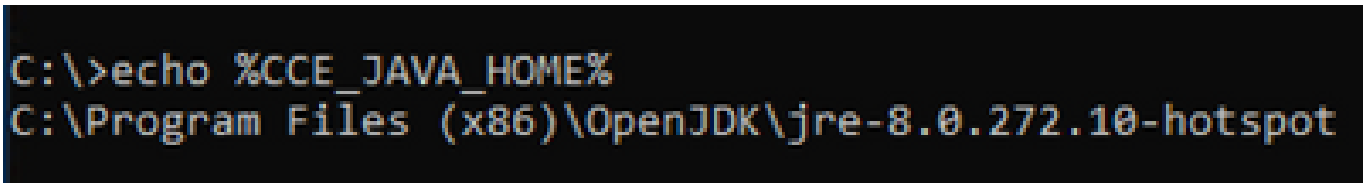
1단계. 라우터\로거, PG 및 모든 AW 서버에서 IIS 인증서를 내보냅니다.
2단계. 라우터\로거, PG 및 모든 AW 서버에서 DFP 인증서를 내보냅니다.
3단계. Router\Logger, PG 및 AW에서 AW 서버로 IIS 및 DFP 인증서를 가져옵니다.

4단계. AW 서버에서 라우터\로거 및 PG로 IIS 인증서를 가져옵니다.

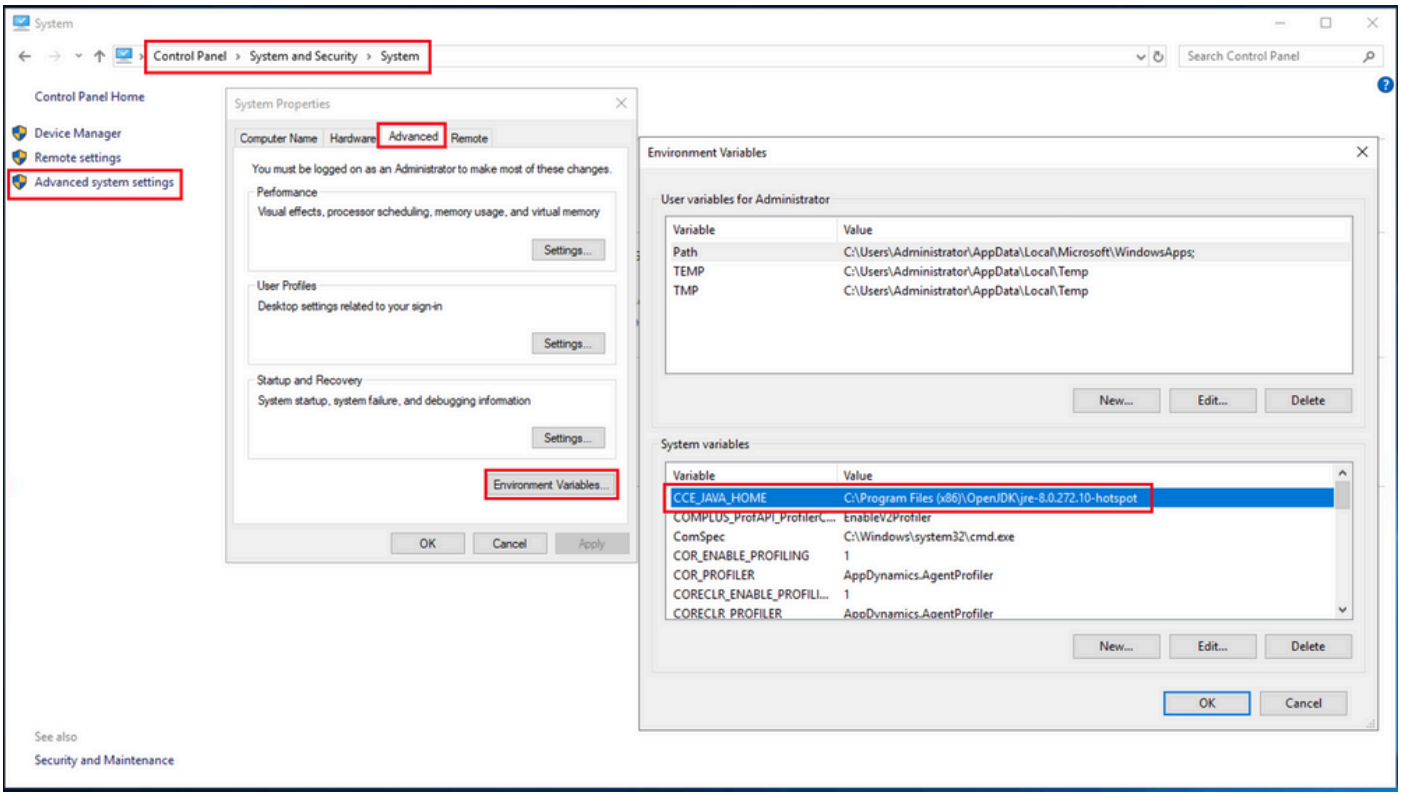
주의: 시작하기 전에 키 저장소를 백업하고 관리자로 명령 프롬프트를 열어야 합니다.

(i) java keytool이 호스팅되는 위치를 확인하려면 java 홈 경로를 알아야 합니다. Java 홈 경로를 찾을 수 있는 방법에는 두 가지가 있습니다.

옵션 1: CLI 명령: echo %CCE_JAVA_HOME%



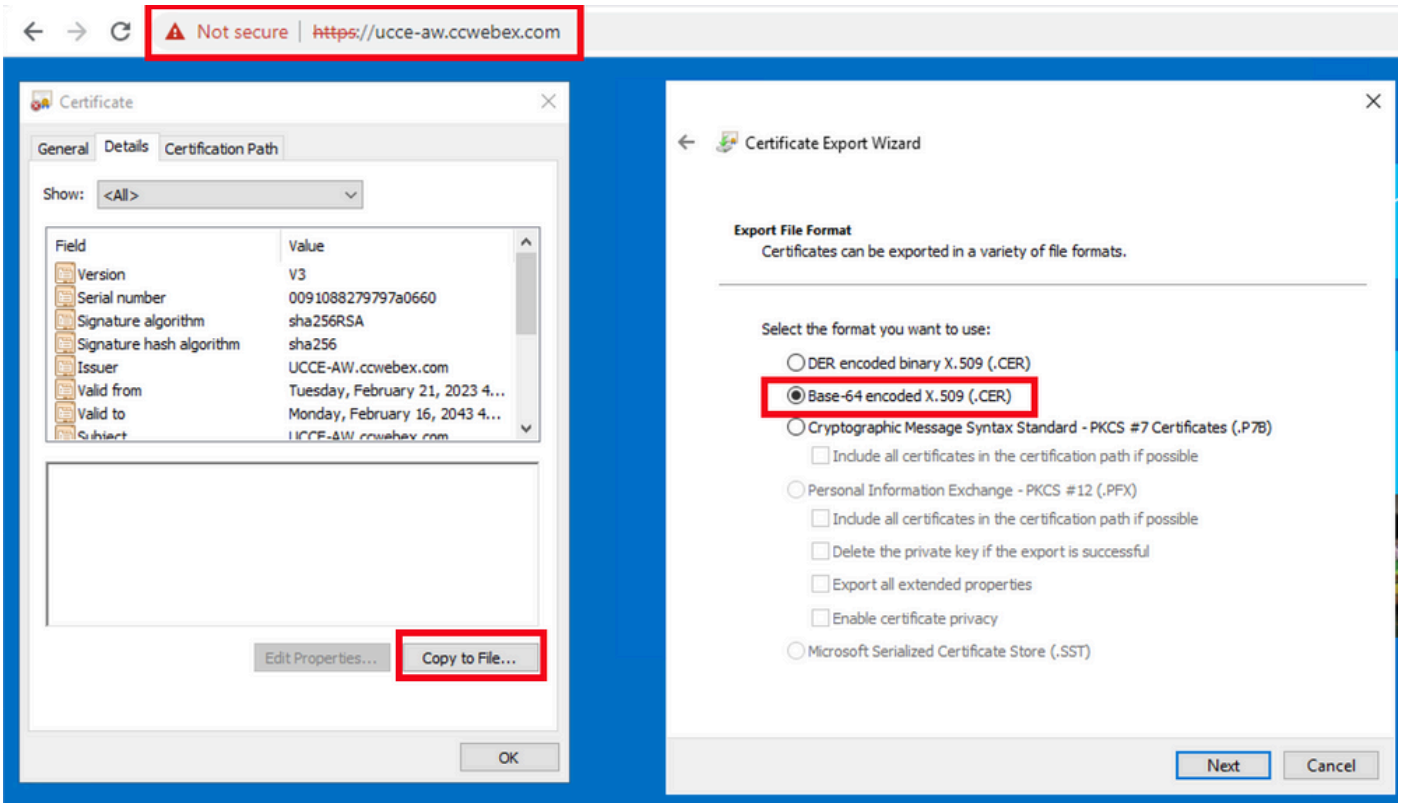
옵션 2: 그림과 같이 Manually via Advanced system setting(고급 시스템 설정을 통해 수동으로)



(ii) <ICM install directory>ssl\ 폴더에서 cacerts 파일을 백업합니다. 다른 곳으로 복사하시면 됩니다

1단계. 라우터\로거, PG 및 모든 AW 서버에서 IIS 인증서를 내보냅니다.

(i) 브라우저에서 AW 서버에서 서버(Rogers, PG, 기타 AW 서버) url로 이동합니다. https://{servername}.



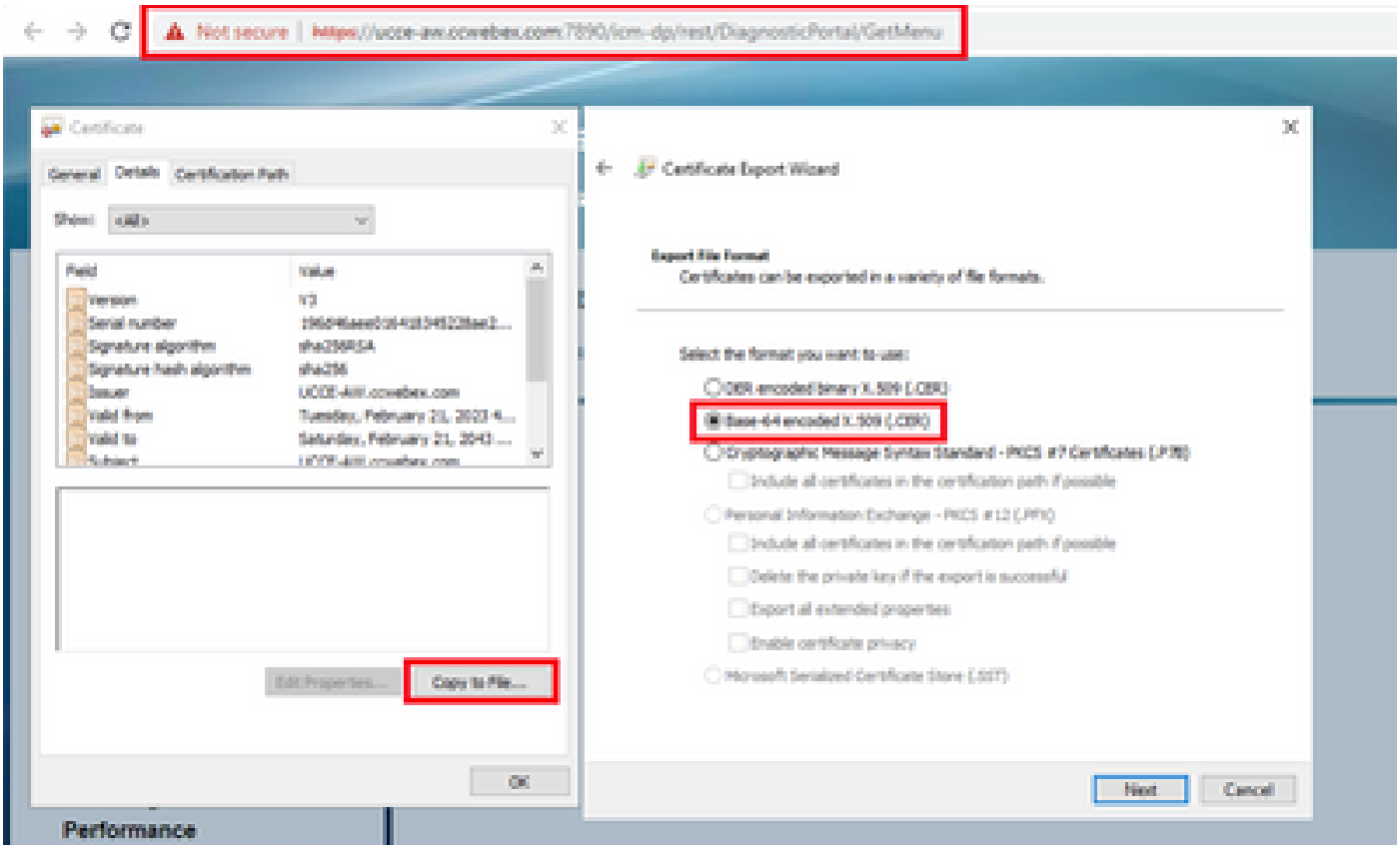
(ii) 임시 폴더에 인증서를 저장합니다. 예를 들어 c:\temp\certs를 선택하고 인증서 이름을

ICM{svr}[ab].cer로 지정합니다.

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

2단계. 라우터\로거, PG 및 모든 AW 서버에서 DFP 인증서를 내보냅니다.

(i) AW 서버에서 브라우저를 열고 서버(라우터, 로거 또는 로거, 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.

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

3단계. Router\Logger, PG 및 AW에서 AW 서버로 IIS 및 DFP 인증서를 가져옵니다.

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

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

참고: 모든 AW 서버로 내보낸 모든 서버 인증서를 가져옵니다.

DFP 자체 서명 인증서를 AW 서버로 가져오는 명령:

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

참고: 모든 AW 서버로 내보낸 모든 서버 인증서를 가져옵니다.

AW 서버에서 Apache Tomcat 서비스를 재시작합니다.

4단계. AW 서버에서 라우터\로거 및 PG로 IIS 인증서를 가져옵니다.

AW IIS 자체 서명 인증서를 Router\Logger 및 PG 서버로 가져오는 명령:

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

참고: A측과 B측의 Rogger 및 PG 서버로 내보낸 모든 AW IIS 서버 인증서를 가져옵니다.

Router\Logger 및 PG 서버에서 Apache Tomcat 서비스를 재시작합니다.

섹션 2: VOS 플랫폼 애플리케이션과 AW 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 AW 서버로 가져옵니다.

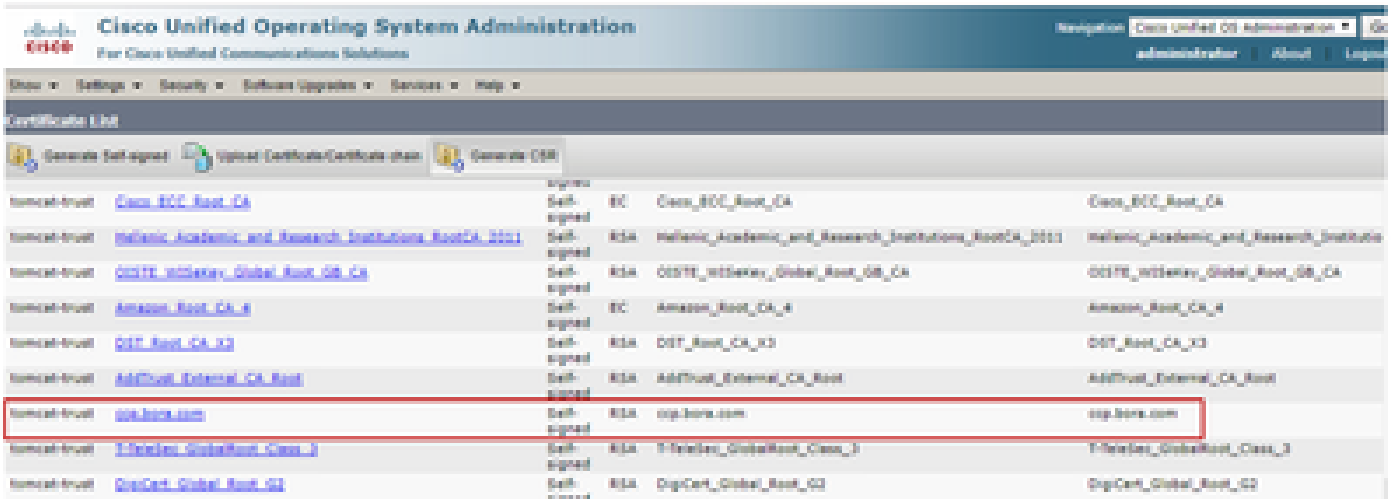
이 프로세스는 다음과 같은 VOS 애플리케이션에 적용 가능합니다.

- Finesse
- CUIC \ LD \ IDS
- 클라우드 연결

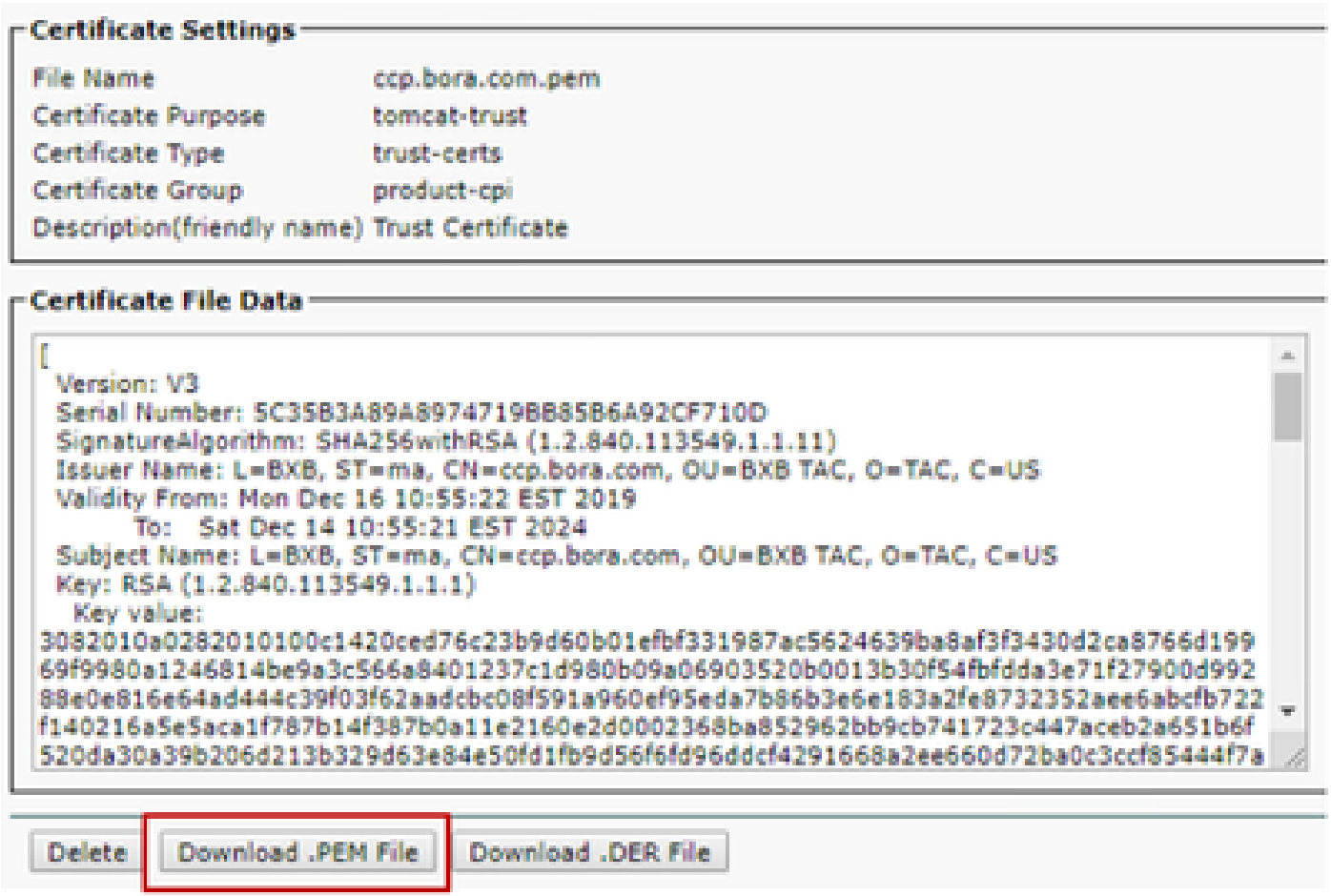
1단계. VOS 플랫폼 애플리케이션 서버 인증서를 내보냅니다.

(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 .PEM 파일 다운로드를 클릭하여 AW 서버의 임시 폴더에 저장합니다.



참고: 가입자에 대해 동일한 단계를 수행합니다.

2단계. VOS 플랫폼 응용 프로그램을 AW 서버로 가져옵니다.

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

AW 서버에서 Apache Tomcat 서비스를 재시작합니다.

참고: 다른 AW 서버에서도 동일한 작업을 수행합니다.

CVP OAMP 서버 및 CVP 구성 요소 서버

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

(i) CVP OAMP 서버: 이 서버에는

- Windows 플랫폼: CVP 서버 및 보고 서버의 WSM(Web Services Manager) 인증서
- VOS 플랫폼: Cisco VVB 및 Cloud Connect 서버.

(ii) CVP 서버: 이 서버에는 다음에서 인증서가 필요합니다.

- Windows 플랫폼: OAMP 서버의 WSM 인증서
- VOS 플랫폼: Cloud Connect 서버 및 Cisco VVB 서버.

(iii) CVP 보고 서버: 이 서버에는

- Windows 플랫폼: OAMP 서버의 WSM 인증서

(iv) Cisco VVB 서버: 이 서버에는

- Windows 플랫폼: CVP 서버의 VXML 인증서 및 CVP 서버의 Callserver 인증서
- VOS Platform: Cloud Connect 서버

CVP 환경에서 셀프 서명 인증서를 효과적으로 교환하는 데 필요한 단계는 다음 세 섹션을 통해 설명합니다.

섹션 1: CVP OAMP 서버와 CVP 서버 및 보고 서버 간의 인증서 교환
섹션 2: CVP OAMP 서버와 VOS 플랫폼 애플리케이션 간의 인증서 교환
섹션 3: CVP 서버와 VOS 플랫폼 애플리케이션 간의 인증서 교환

섹션 1: CVP OAMP 서버와 CVP 서버 및 보고 서버 간의 인증서 교환

이 교환을 성공적으로 완료하는 데 필요한 단계는 다음과 같습니다.

1단계. CVP 서버, 보고 및 OAMP 서버에서 WSM 인증서를 내보냅니다.
2단계. CVP 서버 및 보고 서버에서 OAMP 서버로 WSM 인증서를 가져옵니다.
3단계. CVP OAMP 서버 WSM 인증서를 CVP 서버 및 보고 서버로 가져옵니다.

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.

1단계. CVP 서버, 보고 및 OAMP 서버에서 WSM 인증서를 내보냅니다.

(i) 각 CVP 서버에서 임시 위치로 WSM 인증서를 내보내고 원하는 이름으로 인증서의 이름을 바꿉니다. wsmX.crt로 이름을 바꿀 수 있습니다. X를 서버의 호스트 이름으로 바꿉니다. 예: wsmcsa.crt, wsmcsb.crt, wsmrepa.crt, wsmrepb.crt, wsmoamp.crt.

자체 서명 인증서를 내보내는 명령:

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

(ii) 각 서버의 %CVP_HOME%\conf\security\wsm.crt 경로에서 인증서를 복사하고 서버 유형에 따라 이름을 wsmX.crt로 바꿉니다.

2단계. CVP 서버 및 보고 서버에서 OAMP 서버로 WSM 인증서를 가져옵니다.

(i) 각 CVP 서버 및 보고 서버 WSM 인증서(wsmX.crt)를 OAMP 서버의 %CVP_HOME%\conf\security 디렉토리에 복사합니다.

(ii) 다음 명령을 사용하여 이러한 인증서를 가져옵니다.

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

(iii) 서버를 재부팅합니다.

3단계. CVP OAMP 서버 WSM 인증서를 CVP 서버 및 보고 서버로 가져옵니다.

(i) 모든 CVP 서버 및 보고 서버의 %CVP_HOME%\conf\security 디렉터리에 OAMP 서버 WSM 인증서(wsmoampX.crt)를 복사합니다.

(ii) 다음 명령을 사용하여 인증서를 가져옵니다.

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

(iii) 서버를 재부팅합니다.

섹션 2: CVP OAMP 서버와 VOS 플랫폼 애플리케이션 간의 인증서 교환

이 교환을 성공적으로 완료하는 데 필요한 단계는 다음과 같습니다.

1단계. VOS 플랫폼에서 애플리케이션 인증서를 내보냅니다.

2단계. VOS 애플리케이션 인증서를 OAMP 서버로 가져옵니다.

이 프로세스는 다음과 같은 VOS 애플리케이션에 적용 가능합니다.

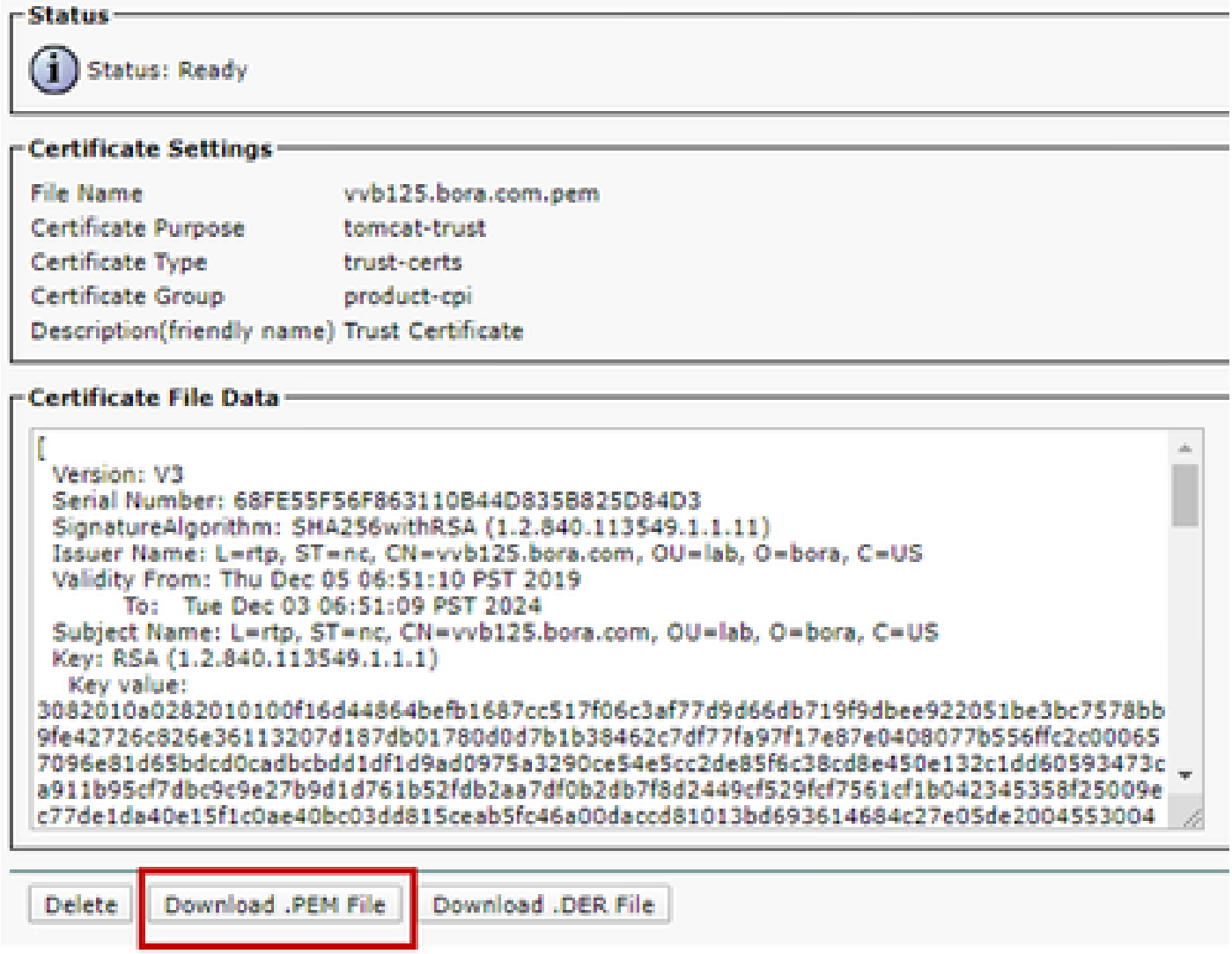
- CUCM
- VVB
- 클라우드 연결

1단계. VOS 플랫폼에서 애플리케이션 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 download .PEM file(.PEM 파일 다운로드)을 클릭하여 OAMP 서버의 임시 폴더에 저장합니다.



2단계. VOS 애플리케이션 인증서를 OAMP 서버로 가져옵니다.

(i) VOS 인증서를 OAMP 서버의 %CVP_HOME%\conf\security 디렉토리에 복사합니다.

(ii) 다음 명령을 사용하여 인증서를 가져옵니다.

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

(ii) 서버를 재부팅합니다.

섹션 3: CVP 서버와 VOS 플랫폼 애플리케이션 간의 인증서 교환

이는 CVP와 기타 컨택 센터 구성 요소 간의 SIP 통신을 보호하기 위한 선택적 단계입니다. 자세한 내용은 CVP 컨피그레이션 가이드: CVP 컨피그레이션 가이드 - 보안을 참조하십시오.

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 PCCE 자체 서명 인증서 - PCCE 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.