

UCCE 솔루션에서 자체 서명 인증서 교환

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[절차](#)

[CCE AW 서버 및 CCE 코어 애플리케이션 서버](#)

[섹션 1. 라우터/로거, PG 및 AW 서버 간의 인증서 교환](#)

[섹션 2. VOS 플랫폼 애플리케이션과 AW 서버 간의 인증서 교환](#)

[CVP OAMP 서버 및 CVP 구성 요소 서버](#)

[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 VVB 서버 간의 인증서 교환](#)

[CVP Call Studio 웹 서비스 통합](#)

[관련 정보](#)

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 12.5(1)
- CVP(Customer Voice Portal) 릴리스 12.5(1)
- Cisco VVB(Virtualized Voice Browser)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- UCCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12.5
- 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

UCCE 솔루션에서 ROgger, PG(Peripheral Gateway), AW(Admin Workstation)/ADS(Administration Data Servers), Finesse, CUI(Cisco Unified Intelligence Center) 등의 핵심 애플리케이션과 관련된 새로운 기능의 컨피그레이션은 Contact Center Enterprise(CCE) 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)로 인해 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

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 위치의 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) 인증서가 필요합니다.

- VOS 플랫폼: Finesse, CUI, LD(Live Data), IDS(Identity Server), Cloud Connect 및 기타 적용 가능한 서버가 인벤토리 데이터베이스에 포함됩니다.

솔루션의 다른 AW 서버에도 동일하게 적용됩니다.

Router\Logger 서버: 이 서버에는 다음 위치의 인증서가 필요합니다.

- Windows 플랫폼: 모든 AW 서버의 IIS 인증서

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

섹션 1. 라우터/로거, PG 및 AW 서버 간의 인증서 교환

섹션 2. VOS 플랫폼 애플리케이션과 AW 서버 간의 인증서 교환

섹션 1. 라우터/로거, PG 및 AW 서버 간의 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 IIS 인증서를 Router\Logger 및 PG로 가져옵니다.

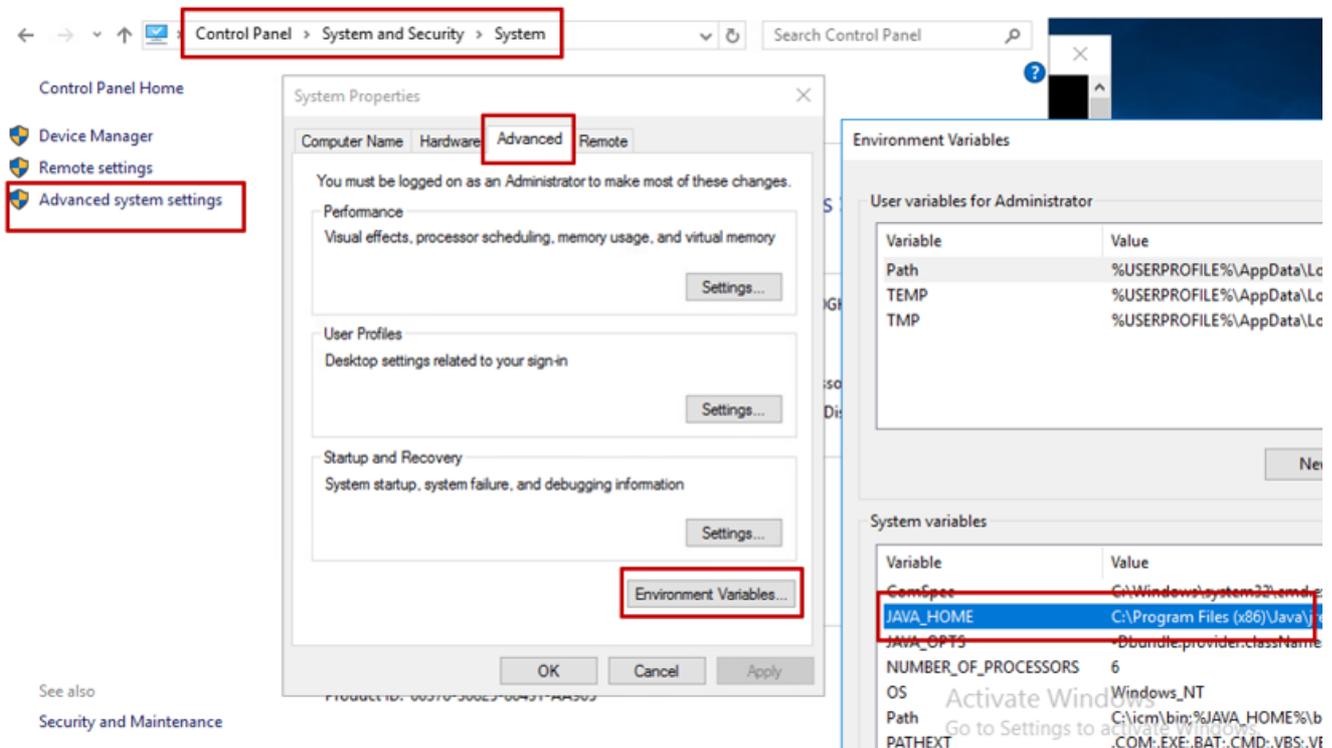
⚠ 주의: 시작하기 전에 키 저장소를 백업하고 관리자 권한으로 명령 프롬프트를 열어야 합니다.

1. Java keytool이 호스팅되는 위치를 확인하기 위해 Java 홈 경로를 파악합니다. Java 홈 경로를 찾을 수 있는 방법에는 두 가지가 있습니다.

옵션 1. CLI 명령: `echo %JAVA_HOME%`

```
C:\>echo %java_home%
C:\Program Files (x86)\Java\jre1.8.0_221
```

옵션 2. 그림과 같이 Advanced(고급) 시스템 설정을 통해 수동으로 수행합니다.



참고: UCCE 12.5에서 기본 경로는 `C:\Program Files (x86)\Java\jre1.8.0_221\bin`입니다. 그러나 12.5 (1a) 설치 프로그램을 사용했거나 12.5 ES55를 설치한 경우(필수 OpenJDK ES),

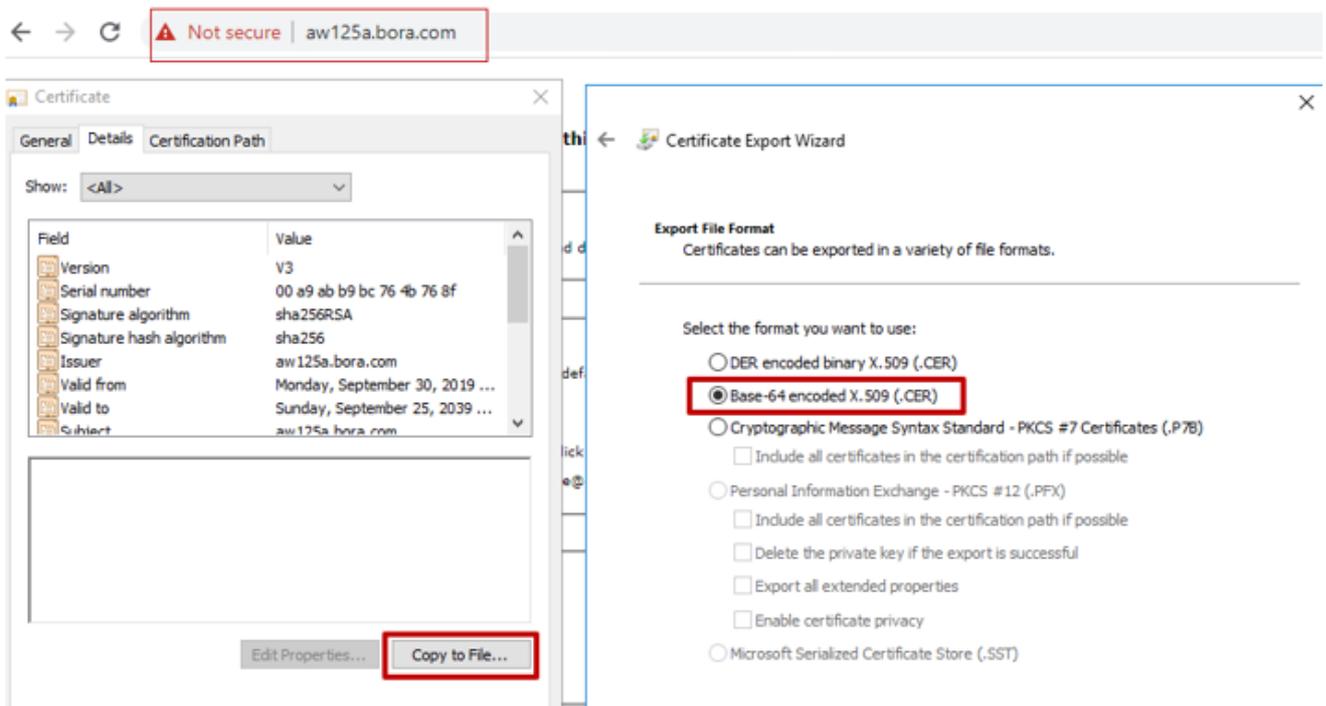
 OpenJDK를 사용하여 데이터 저장소 경로가 변경되었으므로 %CCE_JAVA_HOME% 대신 %JAVA_HOME% 사용합니다. CCE 및 CVP에서의 OpenJDK 마이그레이션에 대한 자세한 내용은 다음 문서에서 확인할 수 있습니다. [Install and Migrate to OpenJDK in CCE 12.5\(1\)](#) 및 [Install and Migrate to OpenJDK in CVP 12.5\(1\)](#).

2. 폴더에서 cacerts 파일을 백업합니다 {JAVA_HOME}\lib\security. 다른 곳으로 복사하시면 됩니다

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

1. 브라우저의 AW 서버에서 서버(ROGGER, PG, 기타 AW 서버) URL:https://{servername} 로 이동합니다.

CCE via Chrome Browser



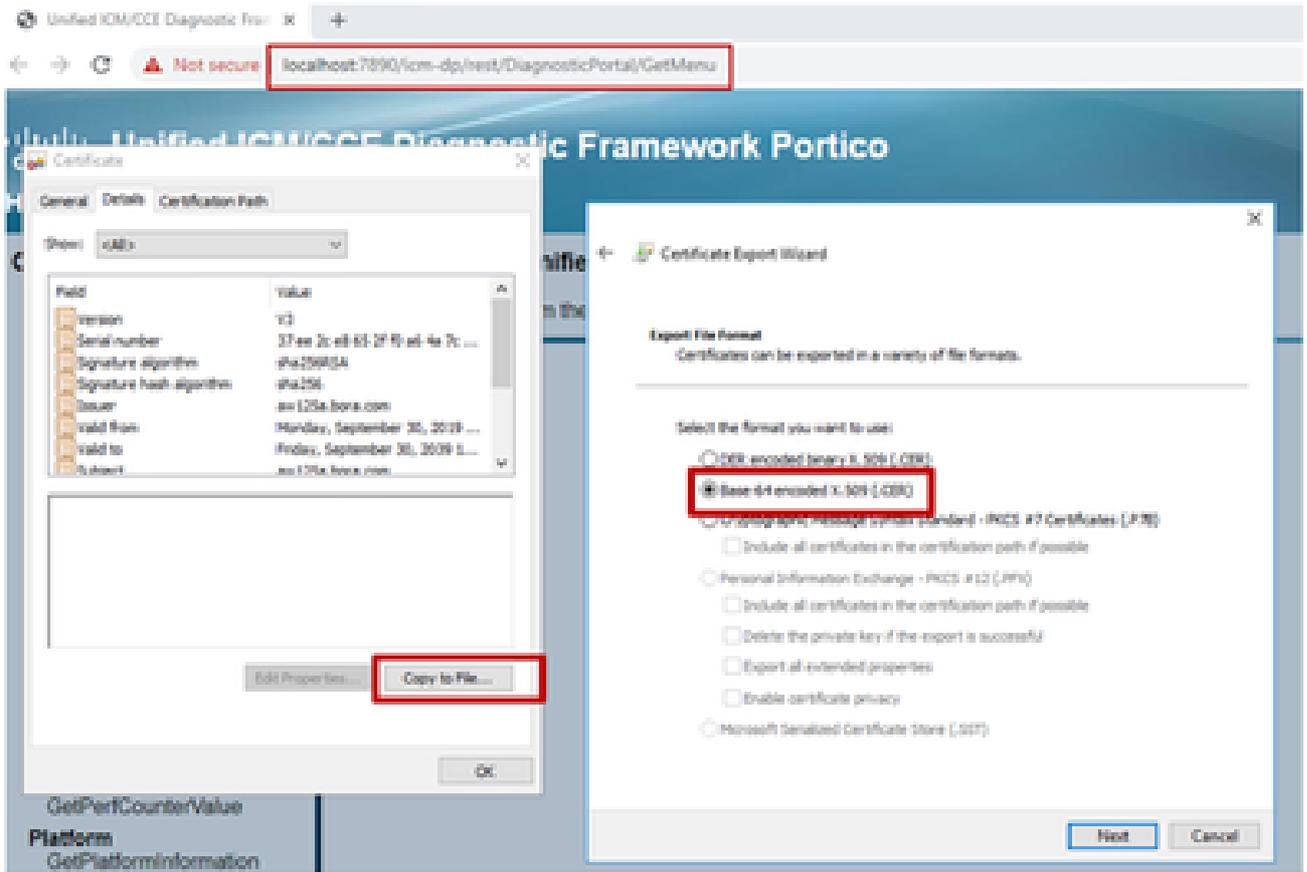
2. 임시 폴더에 인증서를 저장하고 c:\temp\certs 인증서의 이름을 로 ICM{svr}[ab].cer 지정합니다.

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

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

1. AW 서버에서 브라우저를 열고 서버(Router, Logger 또는 ROGGER, PG, AW) DFP URL:(DFP URL:)로 이동합니다 https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersion.

Portico via Chrome Browser



2. 인증서를 폴더 예제에 저장하고 인증서의 `c:\temp\certs` 이름을 로 지정합니다 `dfp{svr}[ab].cer`.

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

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

 참고: 예제 명령에서는 의 기본 키 저장소 비밀번호를 사용합니다 `changeit`. 시스템에서 비밀번호를 수정한 경우 이를 변경해야 합니다.

IIS 자체 서명 인증서를 AW 서버로 가져오는 명령입니다. `keytool`을 실행하는 경로는 다음과 같습니다 `%JAVA_HOME%\bin`.

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com
```

 참고: 모든 AW 서버로 내보낸 모든 서버 인증서를 가져옵니다.

DFP 자체 서명 인증서를 AW 서버로 가져오는 명령:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_DFP -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myrgra.domain.com
```

 참고: 모든 AW 서버로 내보낸 모든 서버 인증서를 가져옵니다.

AW 서버에서 Apache Tomcat 서비스를 재시작합니다.

4단계. AW 서버에서 IIS 인증서를 Router\Logger 및 PG로 가져옵니다.

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

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_server}_IIS -file
Example: keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias myawa.domain.com
```

 참고: A측과 B측의 라우터로거 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 모든 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. tomcat-trust(tomcat-trust) 폴더에서 애플리케이션의 주 서버 인증서로 이동하여 Security > Certificate Management 찾습니다.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration | administrator | About | Logout

Home » Settings » Security » Software Updates » Services » Help »

Certificates List

Generate Self-Signed | Upload Certificate/Certificate Chain | Generate CSR

| tomcat-trust | Issuer | Self-Signed | Key | Subject | Issued To |
|--------------|---|-------------|-----|---|---|
| tomcat-trust | Cisco_BCC_Root_CA | Self-Signed | EC | Cisco_BCC_Root_CA | Cisco_BCC_Root_CA |
| tomcat-trust | Hellenic_Academic_and_Research_Institutions_RootCA_2011 | Self-Signed | RSA | Hellenic_Academic_and_Research_Institutions_RootCA_2011 | Hellenic_Academic_and_Research_Institutions |
| tomcat-trust | GDITL_WebServer_Global_Root_CA_CA | Self-Signed | RSA | GDITL_WebServer_Global_Root_CA_CA | GDITL_WebServer_Global_Root_CA_CA |
| tomcat-trust | Amazon_Root_CA_4 | Self-Signed | EC | Amazon_Root_CA_4 | Amazon_Root_CA_4 |
| tomcat-trust | DIT_Root_CA_X3 | Self-Signed | RSA | DIT_Root_CA_X3 | DIT_Root_CA_X3 |
| tomcat-trust | AddTrust_Internal_CA_Root | Self-Signed | RSA | AddTrust_Internal_CA_Root | AddTrust_Internal_CA_Root |
| tomcat-trust | ccp.bora.com | Self-Signed | RSA | ccp.bora.com | ccp.bora.com |
| tomcat-trust | T-Trustee_GlobalRoot_Class_3 | Self-Signed | RSA | T-Trustee_GlobalRoot_Class_3 | T-Trustee_GlobalRoot_Class_3 |
| tomcat-trust | DigCert_Global_Root_G2 | Self-Signed | RSA | DigCert_Global_Root_G2 | DigCert_Global_Root_G2 |

iii. 인증서를 선택하고 AW 서버의 임시 폴더에 저장하려면 클릭합니다Download .PEM File.

Certificate Settings

File Name: ccp.bora.com.pem
 Certificate Purpose: tomcat-trust
 Certificate Type: trust-certs
 Certificate Group: product-cpi
 Description(friendly name): Trust Certificate

Certificate File Data

```
[
  Version: V3
  Serial Number: 5C35B3A89A89747198B85B6A92CF710D
  SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
  Issuer Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
  Validity From: Mon Dec 16 10:55:22 EST 2019
  To: Sat Dec 14 10:55:21 EST 2024
  Subject Name: L=BXB, ST=ma, CN=ccp.bora.com, OU=BXB TAC, O=TAC, C=US
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
  3082010a0282010100c1420ced76c23b9d60b01efbf331987ac5624639ba8af3f3430d2ca8766d199
  69f9980a1246814be9a3c566a8401237c1d980b09a06903520b0013b30f54fbfdda3e71f27900d992
  88e0e816e64ad444c39f03f62aadcbc08f591a960ef95eda7b86b3e6e183a2fe8732352aee6abcfb722
  f140216a5e5aca1f787b14f387b0a11e2160e2d0002368ba852962bb9cb741723c447aceb2a651b6f
  520da30a39b206d213b329d63e84e50fd1fb9d56f6fd96ddcf4291668a2ee660d72ba0c3ccf85444f7a
]
```

Delete | **Download .PEM File** | Download .DER File

참고: 가입자에 대해 동일한 단계를 수행합니다.

2단계. VOS 플랫폼 응용 프로그램을 AW 서버로 가져옵니다.

키 도구 실행 경로: {JAVA_HOME}\bin

자체 서명 인증서를 가져오는 명령:

```
keytool -keystore ..\lib\security\cacerts -import -storepass changeit -alias {fqdn_of_vos} -file c:\tem
```

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 다음에서 제공하는 인증서가 필요합니다.

- Windows 플랫폼: CVP 서버 및 보고 서버의 WSM(Web Services Manager) 인증서
- VOS 플랫폼: CVA(Customer Virtual Agent) 통합을 위한 Cisco VVB, WXM(Webex Experience Management) 통합을 위한 Cloud Connect 서버.

ii. CVP 서버: 이 서버에는 다음에서 제공하는 인증서가 필요합니다.

- Windows 플랫폼: OAMP 서버의 WSM 인증서
- VOS 플랫폼: WXM 통합 및 Cisco VVB 서버용 Cloud Connect 서버

iii. CVP 보고 서버: 이 서버에는 다음에서 제공하는 인증서가 필요합니다.

- Windows 플랫폼: OAMP 서버의 WSM 인증서

iv. Cisco VVB 서버: 이 서버에는 다음에서 발급한 인증서가 필요합니다.

- Windows 플랫폼: CVP 서버의 VXML 인증서 및 CVP 서버의 Callserver 인증서

CVP 환경에서 셀프 서명 인증서를 효과적으로 교환하는 데 필요한 단계는 다음 세 섹션에 설명되어 있습니다.

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 VVB 서버 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, Reporting 서버 및 OAMP 서버에서 WSM 인증서를 내보냅니다.

2단계. CVP 서버 및 Reporting 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. 키 저장소 비밀번호를 식별하려면 명령을 실행합니다 `more %CVP_HOME%\conf\security.properties.`



3. keytool 명령을 실행할 때 이 비밀번호가 필요합니다.

4. 디렉토리에서 %CVP_HOME%\conf\security\ 명령, 을 copy .keystore backup.keystore 실행합니다.

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

i. 각 서버의 WSM 인증서를 임시 위치로 내보낸 다음 원하는 이름으로 인증서의 이름을 바꿉니다. 이름을 (으)로 바꿀 수 wsmX.crt 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 경로에서 C:\Cisco\CVP\conf\security\wsmX.crt 인증서를 복사하고 서버 유형에 따라 wsmX.crt 이름을 변경합니다.

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

i. 각 CVP 서버 및 보고 서버(wsmX.crt)의 WSM 인증서를 OAMP 서버의 %CVP_HOME%\conf\security 디렉토리로 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 서버에서 CVP 서버 및 보고 서버로 WSM 인증서를 가져옵니다.

i. OAMP 서버 WSM 인증서(wsmoampX.crt)를 모든 CVP 서버 및 보고 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
```

iii. 서버를 재부팅합니다.

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

Status

 Status: Ready

Certificate Settings

| | |
|----------------------------|---------------------|
| File Name | vvb125.bora.com.pem |
| Certificate Purpose | tomcat-trust |
| Certificate Type | trust-certs |
| Certificate Group | product-cpi |
| Description(friendly name) | Trust Certificate |

Certificate File Data

```
[
Version: V3
Serial Number: 68FE55F56F863110B44D835B8825D84D3
Signature Algorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Validity From: Thu Dec 05 06:51:10 PST 2019
To: Tue Dec 03 06:51:09 PST 2024
Subject Name: L=rtp, ST=nc, CN=vvb125.bora.com, OU=lab, O=bora, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100f16d44864befb1687cc517f06c3af77d9d66db719f9dbee922051be3bc7578bb
9fe42726c826e36113207d187db01780d0d7b1b38462c7df77fa97f17e87e0408077b556ffc2c00065
7096e81d65bdcd0cadbcdd1df1d9ad0975a3290ce54e5cc2de85f6c38cd8e450e132c1dd60593473c
a911b95cf7dbc9c9e27b9d1d761b52fdb2aa7df0b2db7f8d2449cf529fcf7561cf1b042345358f25009e
c77de1da40e15f1c0ae40bc03dd815ceab5fc46a00dacc81013bd693614684c27e05de2004553004
```

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
```

iii. 서버를 재부팅합니다.

섹션 3. CVP 서버와 VVB 서버 간의 인증서 교환

이는 CVP와 다른 컨택 센터 구성 요소 간의 SIP 통신을 보호하기 위한 선택적 단계입니다. 추가 정보, 을 참조하십시오. CVP 컨피그레이션 가이드: [CVP 컨피그레이션 가이드 - 보안](#).

CVP Call Studio 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 12.5\(1\) - 웹 서비스 통합 \[Cisco Unified Customer Voice Portal\] - Cisco 사용 설명서를 참조하십시오.](#)

관련 정보

- [CVP 컨피그레이션 가이드 - 보안](#)
- [UCCE 보안 가이드](#)
- [PCCE 관리 가이드 - 보안](#)
- [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](#)
- [CCE OpenJDK 마이그레이션](#)
- [CVP OpenJDK 마이그레이션](#)
- [인증서 교환 유틸리티](#)
- [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.