SPOG용 PCCE 구성 요소 인증서 관리

목차

소개

이 문서에서는 AW(Admin Workstation) 자체 서명 SSL 인증서를 CVP(Customer Voice Portal), Finesse, Cisco ECE(Enterprise Chat and Email), Cisco CUIC(Unified Intelligence Center), Cisco IDs(Identity Service) 및 VB(Virtualized Voice Browser) for Package PCCE(Single Spog) Spog Pane(Spurge of Spog)로 교환하는 방법에 대해 설명합니다.).

기고자: Nagarajan Paramasivam 및 Robert Rojer, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 패키지/통합 컨택 센터 엔터프라이즈(PCCE/UCCE)
- VOS 플랫폼
- 인증서 관리
- 인증서 키 저장소

사용되는 구성 요소

이 문서의 정보는 다음 구성 요소를 기반으로 합니다.

- 관리 워크스테이션(CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VB
- Cisco ECE

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

PCCE , . PCCE

새 사용자 인터페이스 - SPOG

Packaged CCE 12.0에는 다른 컨택 센터 애플리케이션에 맞는 새로운 사용자 인터페이스가 있습니다.사용자 인터페이스를 사용하면 하나의 애플리케이션을 통해 솔루션을 구성할 수 있습니다.새 Unified CCE 관리(https://<IP 주소>/cceadmin)에 로그인합니다.<IP Address>는 A측 또는 B Unified CCE AW의 주소이거나 선택 사항인 외부 HDS입니다.

이 릴리스에서는 Unified CCE 관리 인터페이스를 사용하여 다음을 구성할 수 있습니다.

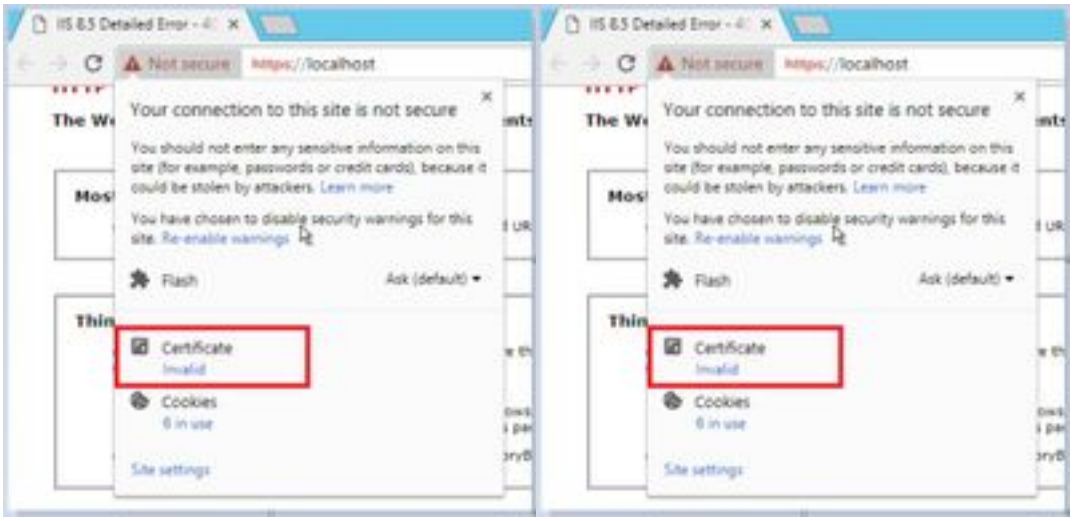
- 캠페인
- 콜백 서비스
- SIP 서버 그룹
- 파일 전송:파일 전송은 보안 주체 AW(2000년 에이전트 구축의 A측 AW 및 4000개의 에이전트 및 12000개의 에이전트 구축에서 구성된 AW를 통해서만 가능합니다.)
- 라우팅 패턴:이제 Unified CVP Operations Console에서 전화 건 번호 패턴을 Unified CCE 관리에서 라우팅 패턴이라고 합니다.
- 위치:Unified CCE 관리에서 라우팅 코드가 사이트 ID 대신 위치 접두사가 되었습니다.
- 장치 구성:Unified CCE 관리를 사용하면 다음 디바이스를 구성할 수 있습니다.CVP 서버, CVP 보고 서버, VB, Finesse, ID 서비스(Single Sign-on 설정).
- 팀 리소스:Unified CCE 관리를 사용하면 상담원 팀에 대해 다음 리소스를 정의하고 연결할 수 있습니다.통화 변수 레이아웃, 데스크톱 레이아웃, 전화 번호부, 워크플로, 이유(준비 안 됨, 로그아웃, 요약)
- 이메일 및 채팅

SPOG를 통해 시스템을 관리하려면 먼저 CVP(Customer Voice Portal), Finesse, Cisco Enterprise Chat and Email(ECE), Cisco CUIC(Unified Intelligence Center), Cisco IDs(Identity Service) 및 VVB(Virtual Voice Browser) 및 AW(Admin Workstation) 간에 SSL 인증서를 교환해야 신뢰를 얻을 수 있습니다.

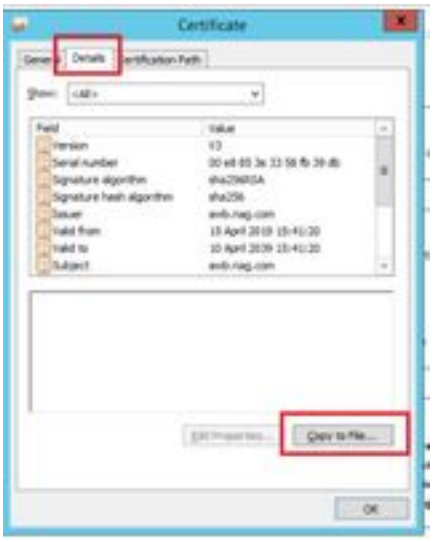
SSL 인증서 내보내기

관리 워크스테이션(AW)

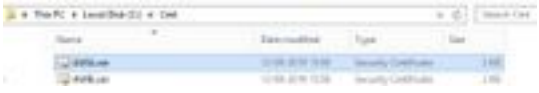
1단계. AW 서버에서 https://localhost URL에 액세스하여 서버 SSL 인증서를 다운로드합니다.



2단계. 인증서 창에서 Details(세부사항) 탭으로 이동하여 Copy To File(파일로 복사) 버튼을 클릭합니다.

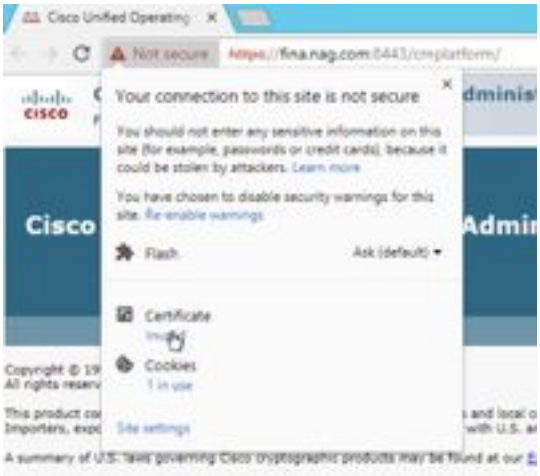


3단계. Base-64 인코딩 X.509(CER)를 선택하고 인증서를 로컬 스토리지에 저장합니다.



Finesse

1단계. https://Finesseserver:8443/cmplatform에 액세스하여 tomcat 인증서를 다운로드합니다.

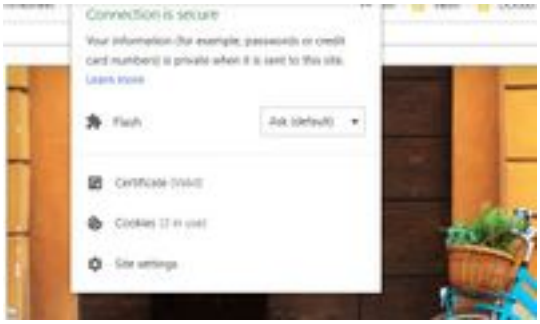


2단계. 인증서 창에서 Details(세부사항) 탭으로 이동하여 Copy To File(파일로 복사) 버튼을 클릭합니다.

3단계. Base-64 인코딩 X.509(CER)를 선택하고 인증서를 로컬 스토리지에 저장합니다.

Cisco ECE

1단계. https://ECEWebServer에 액세스하여 서버 SSL 인증서를 다운로드합니다.



2단계. 인증서 창에서 Details(세부사항) 탭으로 이동하여 Copy To File(파일로 복사) 버튼을 클릭합니다.

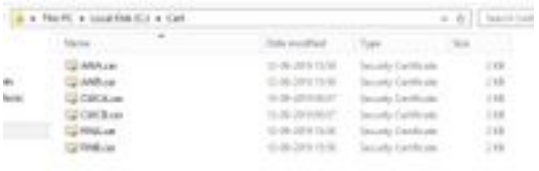
3단계. Base-64 인코딩 X.509(CER)를 선택하고 인증서를 로컬 스토리지에 저장합니다.

CUIC

1단계. https://CUICServer:8443/cmplatform에 액세스하여 tomcat 인증서를 다운로드합니다.

2단계. 인증서 창에서 Details(세부사항) 탭으로 이동하여 Copy To File(파일로 복사) 버튼을 클릭합니다.

3단계. Base-64 인코딩 X.509(CER)를 선택하고 인증서를 로컬 스토리지에 저장합니다.

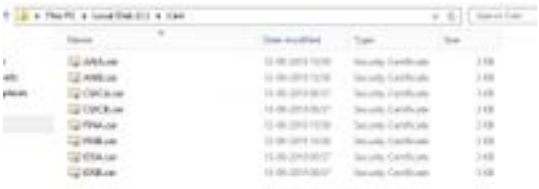


Cisco idS

1단계. https://IDSServer:8553/idsadmin/에 액세스하여 tomcat 인증서를 다운로드합니다.

2단계. 인증서 창에서 Details(세부사항) 탭으로 이동하여 Copy To File(파일로 복사) 버튼을 클릭합니다.

3단계. Base-64 인코딩 X.509(CER)를 선택하고 인증서를 로컬 스토리지에 저장합니다.

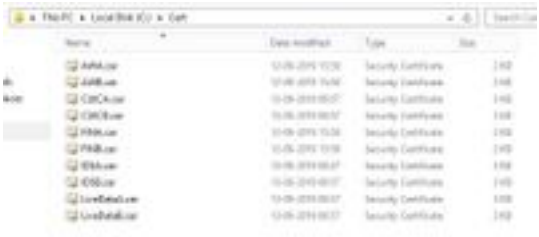


라이브 데이터

1단계. https://LiveDataServer:8444/cuic/gadget/LiveData/에 액세스하여 tomcat 인증서를 다운로드합니다.

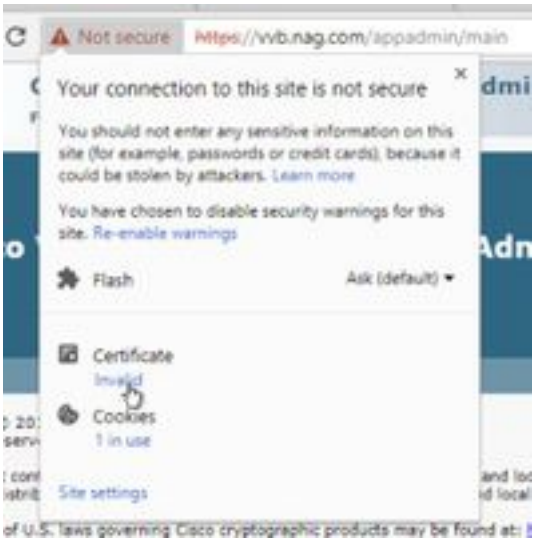
2단계. 인증서 창에서 Details(세부사항) 탭으로 이동하여 Copy To File(파일로 복사) 버튼을 클릭합니다.

3단계. Base-64 인코딩 X.509(CER)를 선택하고 인증서를 로컬 스토리지에 저장합니다.



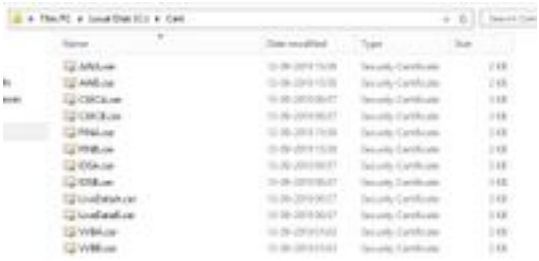
VB

1단계. https://VVBServer/appadmin/main에 액세스하여 tomcat 인증서를 다운로드합니다.



2단계. 인증서 창에서 Details(세부사항) 탭으로 이동하여 Copy To File(파일로 복사) 버튼을 클릭합니다.

3단계. Base-64 인코딩 X.509(CER)를 선택하고 인증서를 로컬 스토리지에 저장합니다.



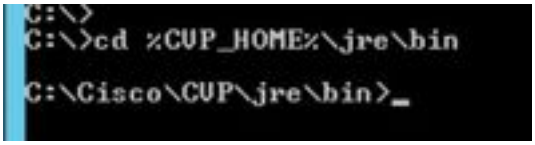
키 저장소로 SSL 인증서 가져오기

CVP 통화 서버 및 보고 서버

1단계. CVP 서버에 로그인하고 AW CCE 관리 인증서를 C:\cisco\cvp\conf\security디렉터리에 **복사합니다**.

2단계. %CVP_**HOME%\conf**로 이동하고 security.properties를 열어 키 저장소 암호를 복사합니다.

3단계. 관리자 권한으로 명령 프롬프트를 열고 명령 **cd %CVP_HOME%\jre\bin을 실행합니다**.



4단계. AW 인증서를 CVP 서버로 가져오려면 이 명령을 사용합니다.

keytool -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias awa.nag.com -file C:\Cisco\CVP\conf\security\AWA.cer

5단계. 비밀번호 프롬프트에 security.properties에서 복사한 비밀번호를 붙여넣습니다.

6단계. **yes를** 입력하여 인증서를 신뢰하고 **키 저장소에 인증서가 추가되었는지 확인합니다.**

7단계. 성공적으로 가져오기에 대한 경고 메시지가 표시됩니다.이는 독점적 형식 Keystore이므로 무시할 수 있습니다.

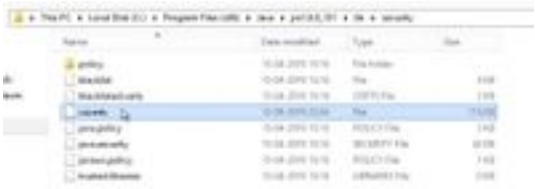
경고:

JECKS 키 저장소는 전용 형식을 사용합니다."keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore -deststoretype pkcs12"를 사용하여 업계 표준 형식인 PKCS12로 마이그레이션하는 것이 좋습니다.

관리 워크스테이션

1단계. AW 서버에 로그인하고 관리자로 명령 프롬프트를 엽니다.

2단계. C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist으로 이동합니다.



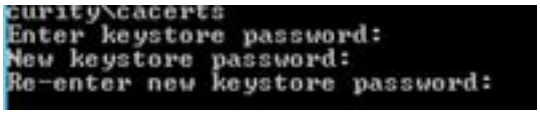
3단계. 명령 **cd %JAVA_HOME%을** 입력하고 입력합니다.

4단계. Finesse 인증서를 AW 서버로 가져오려면 이 명령을 사용합니다.

keytool -import -file C:\Users\Administrator.NAG\Downloads\Cert\FINA.cer -alias fina.nag.com-keystore .\lib\security\cacerts

5단계. 이 키 도구를 처음 사용할 때는 인증서 저장소의 암호를 변경하기 위해 암호 **변경**을 사용합니다.

6단계. 키 저장소의 새 암호를 입력하고 다시 입력하여 암호를 확인합니다.



7단계. **yes를** 입력하여 인증서를 신뢰하고 결과 인증서가 키 저장소에 **추가되었는지 확인합니다.**

참고:1~7단계는 다른 모든 Finesse 노드 및 모든 CUIC 노드와 함께 반복되어야 합니다.

8단계. 키 저장소 암호가 잘못 입력되었거나 재설정 없이 단계를 수행한 경우 이 예외가 발생합니다.

이 인증서를 신뢰합니까?[아니요]: 예

인증서가 키 저장소에 추가되었습니다.

키 도구 오류:java.io.FileNotFound예외:.\lib\security\cacerts (지정된 경로를 찾을 수 없습니다.)

키 저장소 암호 입력:
키 도구 오류:java.io.IO예외:키 저장소가 변경되었거나 암호가 잘못되었습니다.

9단계. 키 저장소 비밀번호를 변경하려면 이 명령을 사용하고 새 비밀번호로 4단계에서 절차를 다시 시작합니다.

keytool -storpasswd -keystore .\lib\security\cacerts

10단계. 성공적으로 가져온 후 이 명령을 사용하여 키 저장소에서 인증서를 봅니다.

keytool -list -keystore .\lib\security\cacerts -alias fina.nag.com

keytool -list -keystore .\lib\security\cacerts -alias cuic.nag.com

Finesse, CUIC, Cisco idS 및 VB

1단계. Finesse 서버 OS 관리 페이지에 로그인하여 tomcat 트러스트에 AW SSL 인증서를 업로드합니다.

2단계. **OS Administration > Security > Certificate Management로 이동합니다.**

3단계. Upload Certificate\Certificate Chain(인증서 체인 업로드)을 클릭하고 드롭다운에서 tomcat-trust를 선택합니다.

4단계. 로컬 저장소에서 인증서 저장소를 찾아 Upload(업로드) 버튼을 클릭합니다.

5단계. 모든 AW 서버 인증서를 Finesse 클러스터에 업로드하는 단계를 반복합니다.

:tomcat-trust .

6단계. 인증서 변경 사항을 적용하려면 tomcat 서비스를 다시 시작합니다.

7단계. CUIC, IDS 및 VB에서 2~4단계를 따라 AW 인증서를 업로드합니다.

Finesse와 CUIC/LiveData 간 인증서 교환

1단계. Finesse, CUIC 및 LiveData 인증서를 별도의 폴더에 보관합니다.

2. Finesse, CUIC 및 LiveData OS 관리 페이지에 로그인합니다.

3단계. **OS 관리 > 보안 > 인증서 관리로 이동합니다.**

4단계. Upload Certificate\Certificate Chain(인증서 체인 업로드)을 클릭하고 드롭다운에서 tomcat-trust를 선택합니다.

5단계. 로컬 저장소에서 인증서 저장소를 찾은 다음 Either servers certificate as below(서버 인증서 중 하나)를 선택한 다음 Upload(업로드) 버튼을 클릭합니다.

Finesse 서버 - CUIC 및 LiveData를 Tomcat 트러스트

CUIC 서버 - Finesse 및 LiveData를 tomcat 신뢰로 사용

LiveData 서버 - CUIC 및 Finesse에서 Tomcat 신뢰

참고:tomcat-trust 인증서를 보조 노드에 업로드할 필요는 없으며 자동으로 복제됩니다.

6단계. 인증서 변경 사항을 적용하려면 각 노드에서 tomcat 서비스를 다시 시작합니다.