PCCE-onderdelencertificaat beheren voor SPOG

Inhoud

Inleiding

Dit document beschrijft hoe de zelfgetekende SSL-certificaten van het Admin Workstation (AW) moeten worden uitgewisseld met de Customer Voice Portal (CVP), Finesse, Cisco Enterprise Chat en Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Services (IDS) en Virtualization Voice browser (VVB) voor Packet Contact Center (PCCE) Single Point of Glass (SPOG).

Bijgedragen door Nagarajan Paramasivam en Robert Rogier, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Packaged/Unified Contact Center Enterprises (PCCE/UCCE)
- VOS-platform
- Certificaatbeheer
- certificaatsleutelwinkel

Gebruikte componenten

De informatie in dit document is gebaseerd op deze componenten:

- Admin Workstation (CEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- Cisco ECE

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Aanbevolen wordt dat u de PCCE-handleiding voor beheer en configuratie hebt gelezen en begrepen, in het bijzonder het referentiekaart aan het einde dat de instelling en configuratie van certificaten regelt. PKC-beheergids en -configuratiegids

Nieuwe gebruikersinterface - SPOG

Packaged CCE 12.0 heeft een nieuwe gebruikersinterface die in overeenstemming is met andere toepassingen van het contactcentrum. Met de gebruikersinterface kunt u de oplossing via één applicatie configureren. Meld u aan bij het nieuwe Unified CCE-beheer op https://<IP Address>/Cceadmin. <IP Address> is het adres van Side A of B Unified CCE AW of de optionele externe HDS.

In deze release staat de Unified CCE-beheerinterface u toe om dit te configureren:

- Campaigns
- Rechtstreekse terugbellen
- SIP-servergroepen
- Bestandsoverdrachten: Bestandsoverdracht is alleen mogelijk via Principal AW (Side A AW in 2000-toepassingen en geconfigureerd AW in 4000-eenheden en 12000-eenheden).
- Routing patronen: Het gesloten nummerpatroon in Unified CVP Operations Console wordt nu routingpatroon in Unified CCE-beheer genoemd.
- Locaties: In Unified CCE Administration, is Routing Code nu het prefix van de locatie in plaats van Site-ID.
- Apparaatconfiguratie: Unified CCE-beheer stelt u in staat de volgende apparaten te configureren: CVP Server, CVP Reporting Server, VVB, Finesse, Identity Service (Single Sign-on Setup).
- Teams: Unified CCE-beheer stelt u in staat de volgende bronnen voor agent-teams te definiëren en te associëren: Lay Variables Layout, desktoplayout, telefoonboeken, werkstromen, redenen (niet klaar, aanmelding, afwerking).
- E-mail en chatten

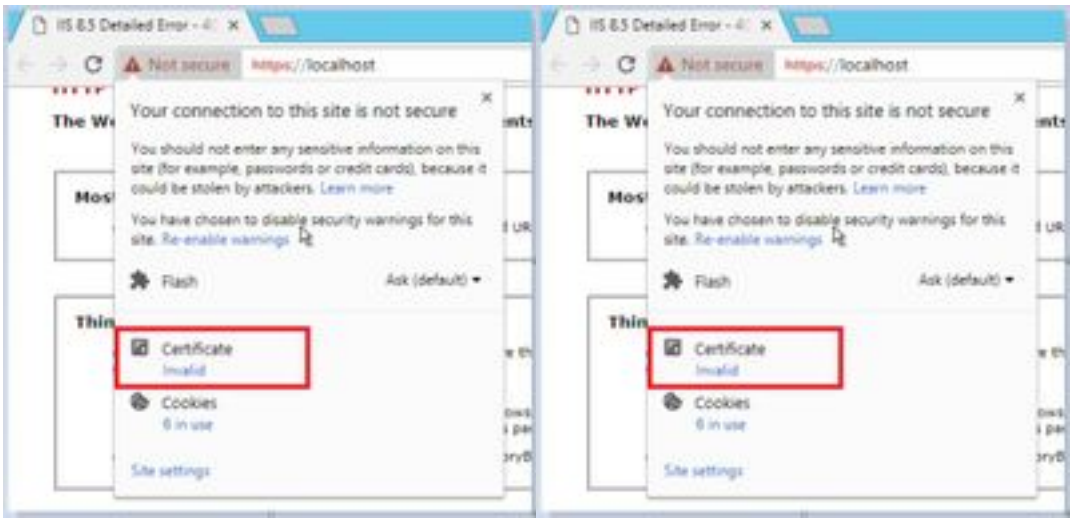
Voordat u het systeem via SPOG wilt beheren, moet u de SSL-certificaten uitwisselen tussen de Customer Voice Portal (CVP), Finse, Cisco Enterprise Chat en Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Services (IDS) en Virtual Voice browser (VVB) en Admin

Workstation (AW) om een vertrouwenscommunicatie tot stand te brengen.

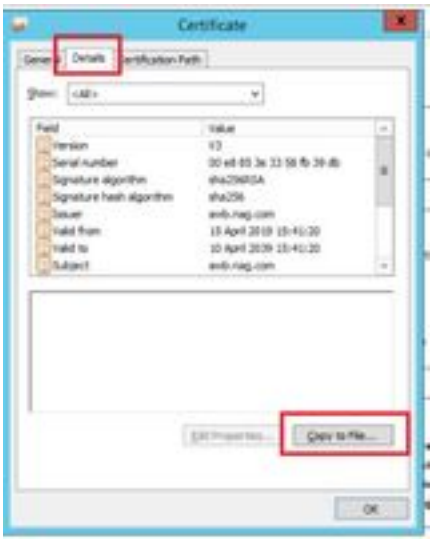
SSL-certificaat exporteren

Werkstation voor beheer (AW)

Stap 1. Toegang tot de https://localhost URL in de AW server en download de server SSL certificaten.



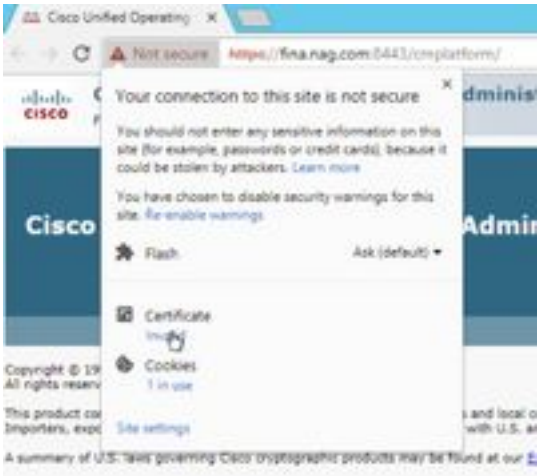
Stap 2. Klik in het Documentvenster op het tabblad Details en klik op de knop Kopie naar bestand.



Stap 3. Selecteer Base-64 gecodeerd X.509 (CER) en bewaar het certificaat in de lokale opslag.

Finesse

Stap 1. Toegang tot de https://Finesseserver:8443/cmplatform en download het papieren certificaat.

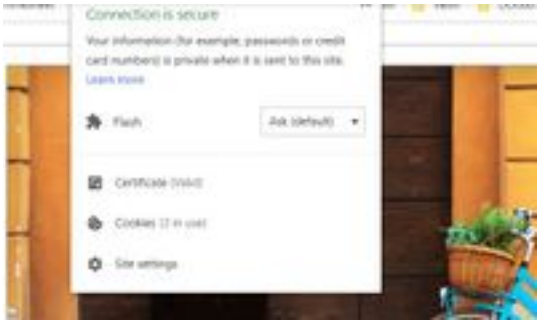


Stap 2. Klik in het Documentvenster op het tabblad Details en klik op de knop Kopie naar bestand.

Stap 3. Selecteer Base-64 gecodeerd X.509 (CER) en bewaar het certificaat in de lokale opslag.

Cisco ECE

Stap 1. Toegang tot de https://ECEWebServer en download het SSL-certificaat van de server.



Stap 2. Klik in het Documentvenster op het tabblad Details en klik op de knop Kopie naar bestand.

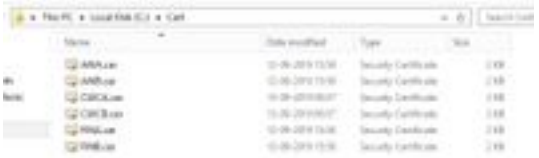
Stap 3. Selecteer Base-64 gecodeerd X.509 (CER) en bewaar het certificaat in de lokale opslag.

CUIC

Stap 1. Toegang tot de https://CUICServer:8443/cmplatform en download het papieren certificaat.

Stap 2. Klik in het Documentvenster op het tabblad Details en klik op de knop Kopie naar bestand.

Stap 3. Selecteer Base-64 gecodeerd X.509 (CER) en bewaar het certificaat in de lokale opslag.

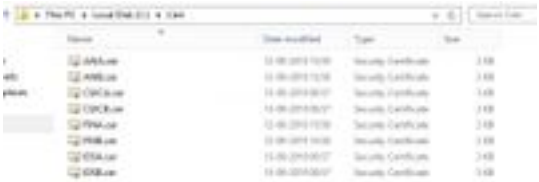


Cisco idS

Stap 1. Toegang tot de https://IDSServer:8553/idsadmin/ en download het papieren certificaat.

Stap 2. Klik in het Documentvenster op het tabblad Details en klik op de knop Kopie naar bestand.

Stap 3. Selecteer Base-64 gecodeerd X.509 (CER) en bewaar het certificaat in de lokale opslag.

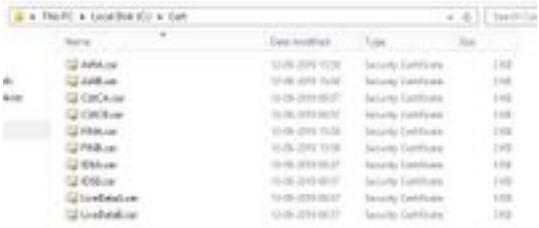


LiveData

Stap 1. Toegang tot de https://LiveDataServer:8444/cuic/gadget/LiveData/ en download het papieren certificaat.

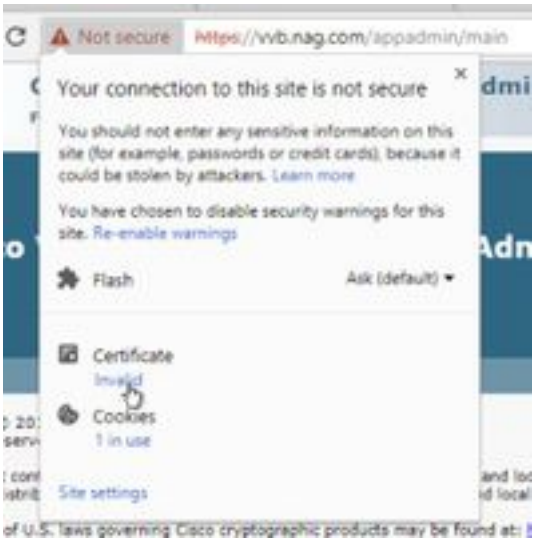
Stap 2. Klik in het Documentvenster op het tabblad Details en klik op de knop Kopie naar bestand.

Stap 3. Selecteer Base-64 gecodeerd X.509 (CER) en bewaar het certificaat in de lokale opslag.



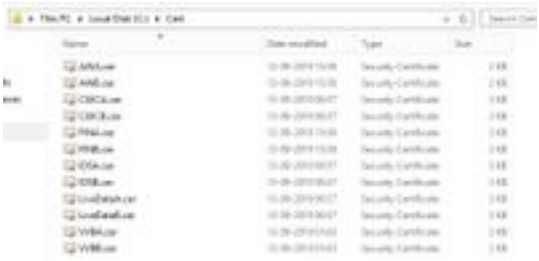
VVB

Stap 1. Toegang tot de https://VVBServer/appadmin/main en download het papieren certificaat.



Stap 2. Klik in het Documentvenster op het tabblad Details en klik op de knop Kopie naar bestand.

Stap 3. Selecteer Base-64 gecodeerd X.509 (CER) en bewaar het certificaat in de lokale opslag.



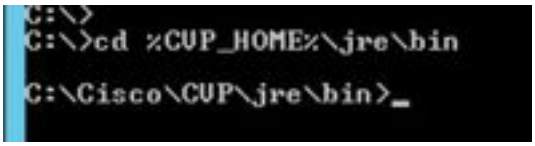
SSL-certificaat importeren naar Keystore

CVP-gespreksserver en -rapportage

Stap 1. Meld u aan bij de CVP-server en kopieer de AW CCE Admin-certificaten naar de **C:\cisco\cvp\conf\security**.

Stap 2. Navigeer naar de **%CVP_HOME%\conf** en open de security.eigenschappen om het Keystore-wachtwoord te kopiëren.

Stap 3. Open de opdrachtmelding als beheerder en voer de opdrachtregel **cd %CVP_HOME%\jre\bin uit**.



Stap 4. Gebruik deze opdracht om de AW-certificaten te importeren naar de CVP-server.

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

Stap 5. Plaats het wachtwoord in de Password-prompt en plak het wachtwoord dat is gekopieerd aan de security.eigenschappen.

Stap 6. Type **ja** om het certificaat te vertrouwen en ervoor te zorgen dat u het resultaat **certificaat aan de toetsencombinatie** hebt **toegevoegd.**

Stap 7. Er wordt een waarschuwing samen met de geslaagde invoer gevraagd. Dit is te danken

aan het eigen formaat Keystore, dat u kunt negeren.

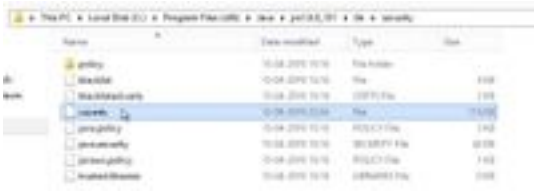
Waarschuwing:

De JCEKS keystore gebruikt een eigen formaat. Het wordt aanbevolen om naar PKCS12 te migreren, wat een industriestandaard is met behulp van "keytool-importkeystore-srckeystore C:\Cisco\CVP\conf\security\.keystore-destkeystore C:\Cisco\CVP\conf\security\.keystore-deststoretype pkcs12".

Admin Workstation

Stap 1. Meld u aan bij de AW-server en open de opdrachtmelding als beheerder.

Stap 2. navigeren naar C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist.



Stap 3. Typ de opdracht **cd %JAVA_HOME%** en voer het volgende in.

Stap 4. Gebruik deze opdracht om de Fins-certificaten in de AW-server te importeren.

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

Stap 5. De eerste keer dat u dit gereedschap gebruikt, gebruikt u de **wachtwoordwijziging** om het wachtwoord van een certificaatwinkel te wijzigen.

Stap 6. Voer een nieuw wachtwoord in voor Keystore en voer het wachtwoord nogmaals in om het te bevestigen.

Stap 7. Type **ja** om het certificaat te vertrouwen en ervoor te zorgen dat u het resultaat **certificaat aan de winkel** hebt **toegevoegd.**

Opmerking: Stap 1 tot en met 7 moet worden herhaald met alle andere Finse knooppunten en alle

CUIC-knooppunten

Stap 8. Als het wachtwoord voor het opslaan verkeerd is ingevoerd of de stappen zonder resetten heeft uitgevoerd, wordt verwacht dat het deze uitzondering krijgt.

Vertrouw dit certificaat? [neen]: ja

Het certificaat is toegevoegd aan de keystore

Belangrijkste fout: java.io.FileNotFoundException: .\lib\security\cacerts (Het systeem kan het opgegeven pad niet vinden)

Voer een wachtwoord in:
Belangrijkste fout: java.io.IOUitzondering: Keystore is geknoeid met, of het wachtwoord was onjuist

Stap 9. Gebruik deze opdracht om het wachtwoord voor het opslaan te wijzigen en start de procedure opnieuw uit Stap 4 met het nieuwe wachtwoord.

toetsenbord voor werktuigopslag -toetsenbord.\lib\security\cacerts

Stap 10. Gebruik deze opdracht om het certificaat vanaf het toetsenbord te bekijken.

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

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

Finesse, CUIC, Cisco idS en VVB

Stap 1. Meld u aan bij de beheerpagina van het Finse server-OS en uploadt u de AW SSL-certificaten in het zoekfunctie.

Stap 2. Navigeer naar **OS-beheer > Beveiliging > certificaatbeheer.**

Stap 3. Klik op de knop Certificaat uploaden en selecteer de optie Vertrouwen vanaf de vervolgkeuzelijst.

Stap 4. Blader naar de certificaatopslag in het lokale opslagsysteem en klik op de knop Upload.

Stap 5. Herhaal de stappen om al het AW-servercertificaat te uploaden naar de Finse cluster.

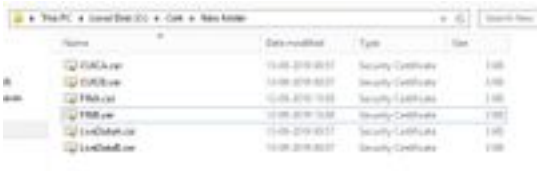
> **Opmerking:** Het is niet vereist om het certificaat van het kartelvertrouwen aan het secundaire knooppunt te uploaden, dit wordt automatisch herhaald.

Stap 6. Start de tomatenservice opnieuw om de wijzigingen in het certificaat te kunnen doorvoeren.

Stap 7. In CUIC, IDS en VVB volgt u de stappen van 2 tot 4 en uploadt u het AW-certificaat.

Certificaatuitwisseling tussen boetes en CUIC/LiveData

Stap 1. Bewaar de Fins-, CUIC- en LiveData-certificaten in een afzonderlijke map.



Stap 2. Meld u aan bij de beheerpagina Fins, CUIC en LiveData OS.

Stap 3. Navigeer naar **OS-beheer > Beveiliging > certificaatbeheer.**

Stap 4. Klik op de knop Certificaat uploaden\certificaatketen en selecteer de optie vertrouwen in de droger.

Stap 5. Bladeren in de opslagruimte voor certificaten in de lokale opslag en selecteer vervolgens een servercertificaat zoals hieronder, en klik vervolgens op Upload.

In Finse server - CUIC en LiveData als Tomcat vertrouwen

In CUIC Server - Finesse en LiveData als u wilt vertrouwen

In LiveData Server - CUIC en financiën als vertrouwen in de computer

> **Opmerking:** Het is niet vereist om het certificaat van het kartelvertrouwen aan het secundaire knooppunt te uploaden, dit wordt automatisch herhaald.

Stap 6. Start de tomatenservice op elk knooppunt opnieuw om de certificaatwijzigingen in werking te laten treden.