Zertifikat für PCCE-Komponenten für SPOG verwalten

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die selbstsignierten SSL-Zertifikate der Admin Workstation (AW) an das Customer Voice Portal (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (IDS) und Virtualized Voice Browser (VB) for Package Contact Center Enterprise (PCCE) Single Pane of Glass (SPOG) austauschen.

Unterstützt von Nagarajan Paramasivam und Robert Rogier, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Packaged/Unified Contact Center Enterprises (PCCE/UCCE)
- VOS-Plattform
- Zertifikatsverwaltung

- Zertifikatsschlüssel

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Komponenten:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Es wird empfohlen, den PCCE-Administrations- und Konfigurationsleitfaden, insbesondere den Referenzanhang am Ende, in dem die Zertifikateinrichtung und -konfiguration behandelt werden, zu lesen und zu verstehen. PCCE-Administrations- und Konfigurationsleitfaden

Neue Benutzeroberfläche - SPOG

Packaged CCE 12.0 verfügt über eine neue Benutzeroberfläche, die mit anderen Contact Center-Anwendungen übereinstimmt. Über die Benutzeroberfläche können Sie die Projektmappe über eine Anwendung konfigurieren. Melden Sie sich bei der neuen Unified CCE Administration unter https://<IP-Adresse>/cceadmin an. <IP-Adresse> ist die Adresse der Seite A oder B Unified CCE AW oder des optionalen externen HDS.

In dieser Version können Sie mit der Unified CCE Administration-Schnittstelle Folgendes konfigurieren:

- Kampagnen
- Rückruf mit freundlicher Genehmigung
- SIP-Servergruppen
- Dateiübertragungen: Die Dateiübertragung ist nur über das Principal AW möglich (Seite A AW bei der Bereitstellung von Agenten im Jahr 2000 und konfigurierte AW in Bereitstellungen mit 4.000 Agenten und 1.200 Agenten).
- Routingmuster: Das Nummernmuster in der Unified CVP Operations Console heißt jetzt Routing Pattern in der Unified CCE Administration.
- Standorte: In der Unified CCE-Administration ist Routingcode jetzt das Standortpräfix anstelle der Standort-ID.
- Gerätekonfiguration: Die Unified CCE Administration ermöglicht die Konfiguration der folgenden Geräte: CVP-Server, CVP Reporting Server, VVB, Finesse, Identity Service (Single Sign-on Setup).
- Teamressourcen: Mithilfe der Unified CCE Administration können Sie die folgenden Ressourcen für Agenten-Teams definieren und zuordnen: Layout der Anrufvariablen,

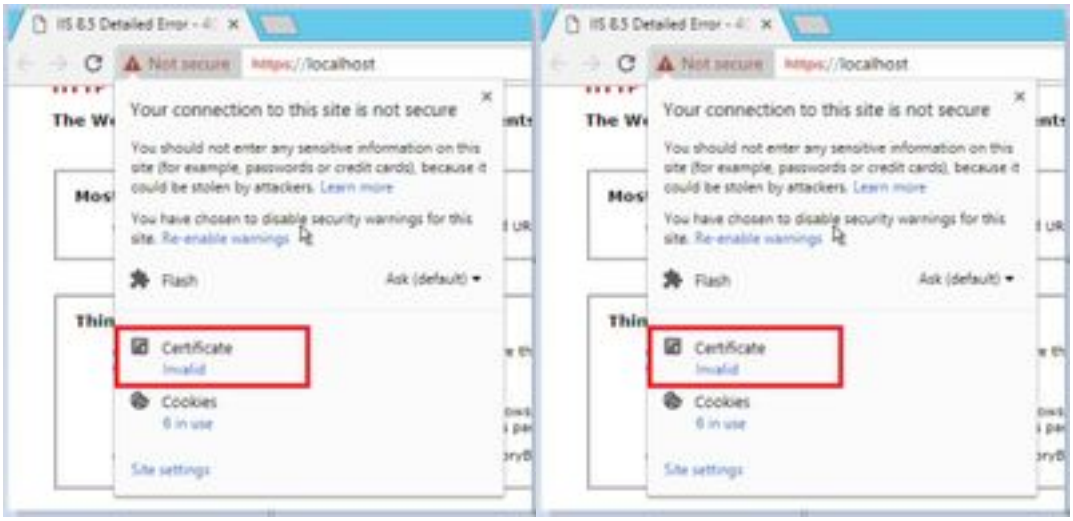
Desktop-Layout, Telefonbücher, Workflows, Gründe (nicht bereit, Abmelden, Zusammenfassung)
- E-Mail und Chat

Bevor das System über SPOG verwaltet werden kann, müssen die SSL-Zertifikate zwischen Customer Voice Portal (CVP), Finesse, Cisco Enterprice Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (IDS) und Virtual Voice Browser (VVB) sowie Admin Workstation (AW) ausgetauscht werden, um eine Vertrauenskommunikation aufzubauen.

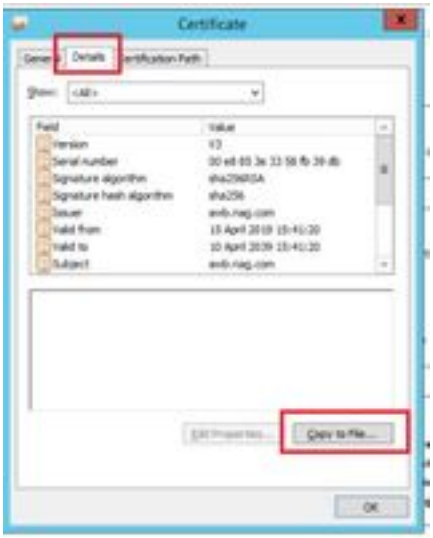
SSL-Zertifikatsexport

Verwaltungs-Workstation (AW)

Schritt 1: Rufen Sie die https://localhost URL im AW-Server auf, und laden Sie die SSL-Serverzertifikate herunter.



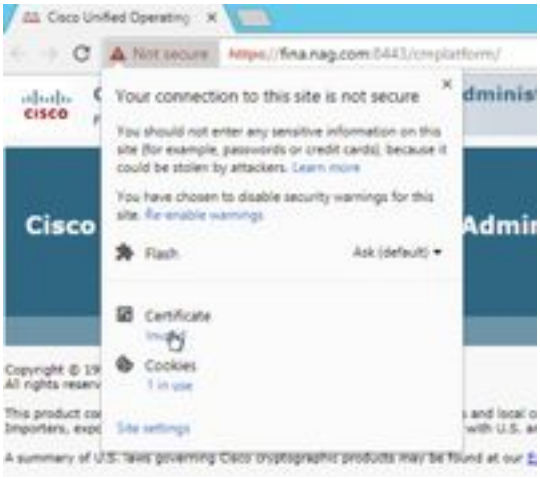
Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.



Schritt 3: Wählen Sie Base-64-codiertes X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

Finesse

Schritt 1: Rufen Sie das https://Finesseserver:8443/cmplatform auf, und laden Sie das Tomcat-Zertifikat herunter.

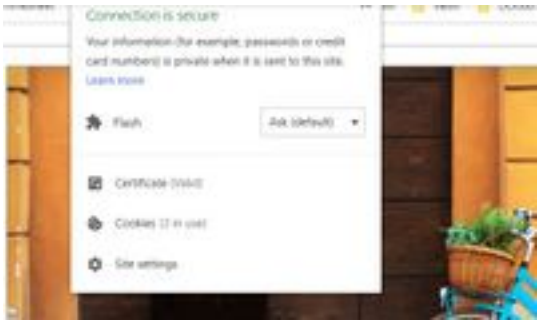


Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

Cisco ECE

Schritt 1: Rufen Sie das https://ECEWebServer auf, und laden Sie das SSL-Serverzertifikat herunter.



Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

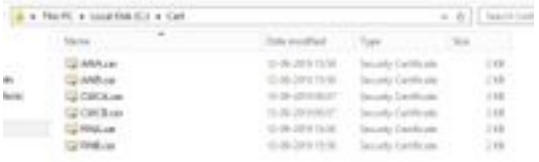
Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

CUIC

Schritt 1: Rufen Sie das https://CUICServer:8443/cmplatform auf, und laden Sie das Tomcat-Zertifikat herunter.

Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

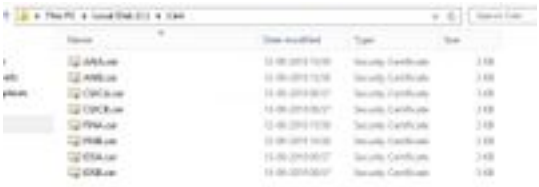


Cisco IDs

Schritt 1: Rufen Sie das https://IDSServer:8553/idsadmin/ auf, und laden Sie das Tomcat-Zertifikat herunter.

Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.

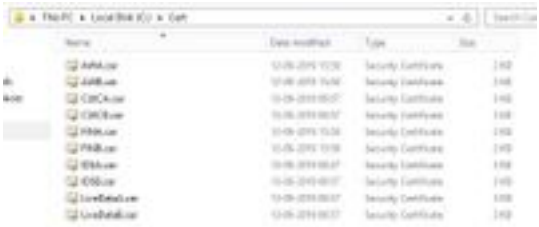


LiveData

Schritt 1: Rufen Sie das https://LiveDataServer:8444/cuic/gadget/LiveData/ auf, und laden Sie das Tomcat-Zertifikat herunter.

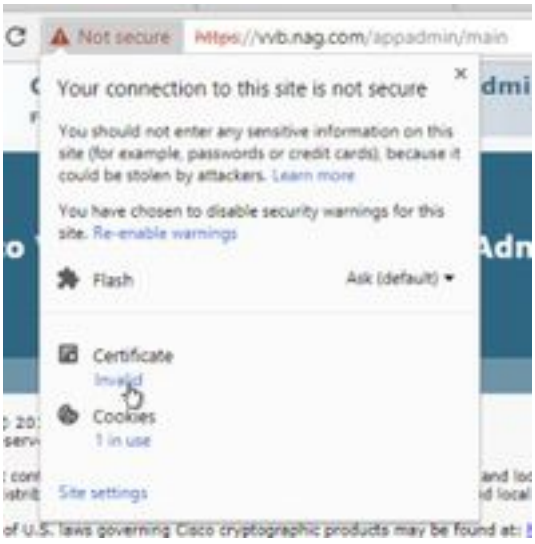
Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.



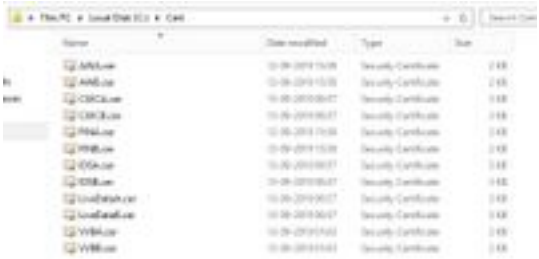
VVB

Schritt 1: Rufen Sie das https://VVBServer/appadmin/main auf, und laden Sie das Tomcat-Zertifikat herunter.



Schritt 2: Navigieren Sie im Zertifikatsfenster zur Registerkarte Details, und klicken Sie auf die Schaltfläche In Datei kopieren.

Schritt 3: Wählen Sie Base-64-codierte X.509 (CER) aus, und speichern Sie das Zertifikat im lokalen Speicher.



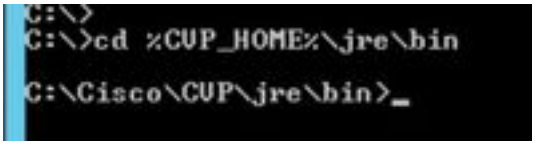
Importieren von SSL-Zertifikaten in Keystore

CVP-Anrufserver und Reporting-Server

Schritt 1: Melden Sie sich beim CVP-Server an, und kopieren Sie die AW CCE-Administratorzertifikate auf die **C:\cisco\cvp\conf\security**.

Schritt 2: Navigieren Sie zu **%CVP_HOME%\conf**, und öffnen Sie die security.properties, um das Keystore-Kennwort zu kopieren.

Schritt 3: Öffnen Sie die Eingabeaufforderung als Administrator, und führen Sie den Befehl **cd %CVP_HOME%\jre\bin aus**.



Schritt 4: Verwenden Sie diesen Befehl, um die AW-Zertifikate in den CVP-Server zu importieren.

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

Schritt 5: Fügen Sie an der Kennworteingabeaufforderung das aus den security.properties kopierte Kennwort ein.

Schritt 6: Geben Sie **yes ein**, um dem Zertifikat zu vertrauen, und stellen Sie sicher, dass das Ergebnis-**Zertifikat zum Keystore hinzugefügt wurde.**

Schritt 7: Bei einem erfolgreichen Import wird eine Warnung angezeigt. Das liegt an dem proprietären Format Keystore, das Sie ignorieren können.

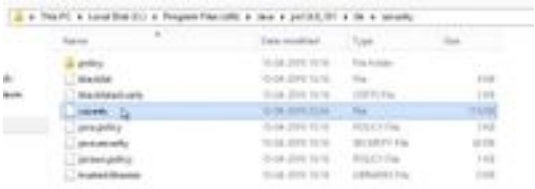
Warnung:

Der JCEKS-Keystore verwendet ein proprietäres Format. Es wird empfohlen, zu PKCS12 zu migrieren, einem Standardformat, das "keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore -deststoretype pkcs12" verwendet.

Administrator-Workstation

Schritt 1: Melden Sie sich beim AW-Server an, und öffnen Sie die Eingabeaufforderung als Administrator.

Schritt 2: Navigieren Sie zu C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist.



Schritt 3: Geben Sie den Befehl **cd %JAVA_HOME%** ein und geben Sie ein.

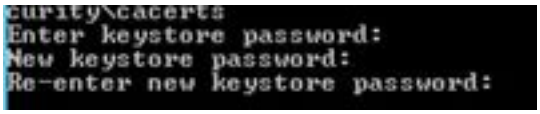
Schritt 4: Verwenden Sie diesen Befehl, um die Finesse-Zertifikate in den AW-Server zu

importieren.

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

Schritt 5: Wenn Sie dieses Schlüsselprogramm zum ersten Mal verwenden, können Sie das Kennwort **ändern**, um das Kennwort eines Zertifikatsspeichers zu ändern.

Schritt 6: Geben Sie ein neues Kennwort für den Keystore ein, und bestätigen Sie das Kennwort erneut.



Schritt 7: Geben Sie **yes ein**, um das Zertifikat zu vertrauen, und stellen Sie sicher, dass das Ergebnis-**Zertifikat zum Keystore hinzugefügt wurde.**

Schritt 8: Wenn das Schlüsselwort falsch eingegeben wurde oder die Schritte ohne Zurücksetzen ausgeführt wurden, wird diese Ausnahme erwartet.

Vertrauen Sie diesem Zertifikat? [Nein]: Ja

Zertifikat wurde dem Keystore hinzugefügt

Tastaturfehler: java.io.FileNotFoundException: .\lib\security\cacerts (Das System kann den angegebenen Pfad nicht finden.)

Eingabe des Keystore-Kennworts:
Tastaturfehler: java.io.IOException: Keystore wurde manipuliert, oder das Kennwort war falsch.

Schritt 9: Um das Keystore-Kennwort zu ändern, verwenden Sie diesen Befehl, und starten Sie das Verfahren erneut mit dem neuen Kennwort von Schritt 4 aus.

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

Schritt 10: Verwenden Sie nach dem erfolgreichen Import diesen Befehl, um das Zertifikat vom Keystore anzuzeigen.

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

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

Finesse, CUIC, Cisco IDS und VVB

Schritt 1: Melden Sie sich auf der Verwaltungsseite für das Betriebssystem des Finesse-Servers an, und laden Sie die AW SSL-Zertifikate in die Vertrauenswürdigkeit von Tomcat hoch.

Schritt 2: Navigieren Sie zu **Betriebssystemverwaltung > Sicherheit > Zertifikatsverwaltung.**

Schritt 3: Klicken Sie auf Upload Certificate\Certificate Chain, und wählen Sie in der Dropdown-Liste die Option tomcat-trust aus.

Schritt 4: Durchsuchen Sie den Zertifikatsspeicher im lokalen Speicher, und klicken Sie auf die Schaltfläche Upload (Hochladen).

Schritt 5: Wiederholen Sie die Schritte, um das gesamte AW-Serverzertifikat in das Finesse-Cluster hochzuladen.

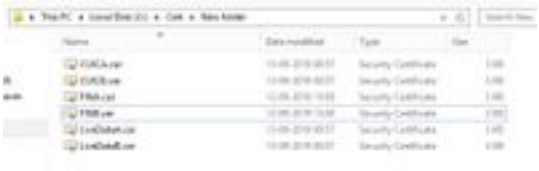
> **Hinweis**: Es ist nicht erforderlich, das Zertifikat "tomcat-trust" in den sekundären Knoten hochzuladen. Dies wird automatisch repliziert.

Schritt 6: Starten Sie den Tomcat-Dienst neu, damit die Zertifikatänderungen wirksam werden.

Schritt 7: In CUIC, IDS und VVB folgen Sie den Schritten von 2 bis 4 und laden das AW-Zertifikat hoch.

Zertifikataustausch zwischen Finesse und CUIC/LiveData

Schritt 1: Bewahren Sie die Zertifikate Finesse, CUIC und LiveData in einem separaten Ordner auf.



Schritt 2: Melden Sie sich bei der Seite Finesse, CUIC und LiveData OS Administration an.

Schritt 3: Navigieren Sie zu **Betriebssystemverwaltung > Sicherheit > Zertifikatsverwaltung.**

Schritt 4: Klicken Sie auf Upload Certificate\Certificate Chain, und wählen Sie in der Dropdown-Liste die Option tomcat-trust aus.

Schritt 5: Durchsuchen Sie den Zertifikatsspeicher im lokalen Speicher, und wählen Sie "Entweder-Server-Zertifikat" wie unten aus, und klicken Sie dann auf die Schaltfläche Hochladen.

In Finesse Server - CUIC und LiveData als Tomcat Trust

In CUIC Server - Finesse und LiveData als tomcat trust

In LiveData Server - CUIC und Finesse als Tomcat Trust

> **Hinweis**: Es ist nicht erforderlich, das Zertifikat "tomcat-trust" in den sekundären Knoten hochzuladen. Dies wird automatisch repliziert.

Schritt 6: Starten Sie den Tomcat-Dienst für jeden Knoten neu, damit die Zertifikatänderungen wirksam werden.