Gérer le certificat des composants PCCE pour SPOG

Contenu

Introduction

Ce document décrit comment échanger les certificats SSL auto-signés de la station de travail Admin vers le portail vocal du client (CVP), Finesse, Cisco Enterprise Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) et le navigateur vocal virtualisé (VVB) pour le volet de verre unique du centre de contact du package Enterprise (PCCE).

Contribué par Nagarajan Paramasivam et Robert Rogier, ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Entreprises de centre de contacts unifiés/groupés (PCCE/UCCE)
- Plate-forme VOS
- Gestion des certificats

- Clavier de certificat

Components Used

Les informations de ce document sont basées sur les composants suivants :

- Station de travail Admin (CCEADMIN/SPOG)
- CVP
- Finesse
- CUIC, IDS
- VVB
- CEE de Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Il est recommandé de lire et de comprendre le Guide d'administration et de configuration de PCCE, en particulier l'annexe Référence à la fin qui couvre la configuration et la configuration des certificats. Guide d'administration et de configuration de PCCE

Nouvelle interface utilisateur - SPOG

Packaged CCE 12.0 dispose d'une nouvelle interface utilisateur conforme aux autres applications du centre de contacts. L'interface utilisateur vous permet de configurer la solution via une application unique. Connectez-vous à la nouvelle administration Unified CCE à l'adresse https://<IP Address>/cceadmin. <Adresse IP> est l'adresse de l'AW Unified CCE côté A ou B ou du HDS externe facultatif.

Dans cette version, l'interface Unified CCE Administration vous permet de configurer ceci :

- Campagnes
- Avec l'aimable autorisation de Callback
- Groupes de serveurs SIP
- Transferts de fichiers : Le transfert de fichiers n'est possible que par le biais de l'AW principal (Side A AW dans le déploiement d'agents en 2000 et configuré AW dans 4000 déploiements d'agents et 12000).
- Modèles de routage : Le modèle de numéro composé dans Unified CVP Operations Console s'appelle maintenant Routing Pattern dans Unified CCE Administration.
- Emplacements : Dans Unified CCE Administration, le code de routage est désormais le préfixe d'emplacement au lieu de l'ID de site.
- Configuration de périphériques: Unified CCE Administration vous permet de configurer les périphériques suivants : Serveur CVP, serveur de rapports CVP, VVB, Finesse, service d'identité (configuration de connexion unique).
- Ressources de l'équipe : Unified CCE Administration vous permet de définir et d'associer les ressources suivantes pour les équipes d'agents : Disposition des variables d'appel, disposition du bureau, annuaires téléphoniques, Workflows, raisons (Non prêt, Déconnexion, Post-appel).
- E-mail et discussion

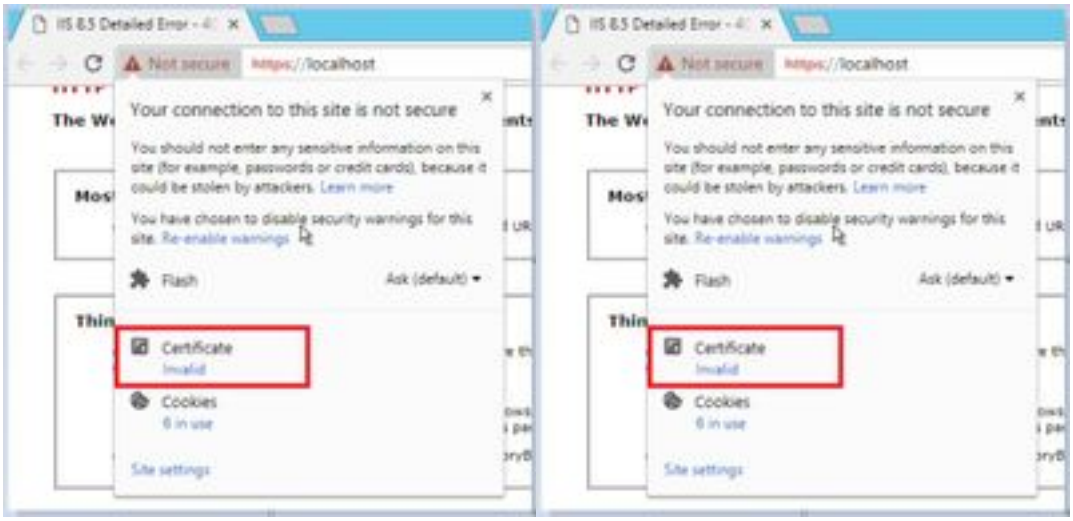
Avant de tenter de gérer le système via SPOG, il est nécessaire d'échanger les certificats SSL

entre Customer Voice Portal (CVP), Finesse, Cisco Enterprice Chat and Email (ECE), Cisco Unified Intelligence Center (CUIC), Cisco Identity Service (idS) et Virtual Voice Browser (VVB) et Admin Workstation (AW) afin d'établir une communication de confiance.

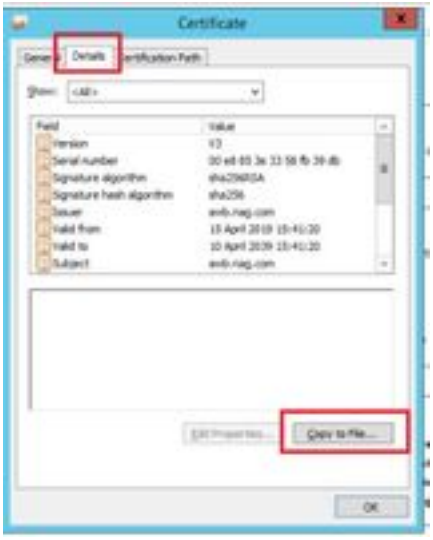
Exportation de certificat SSL

Station de travail d'administration (AW)

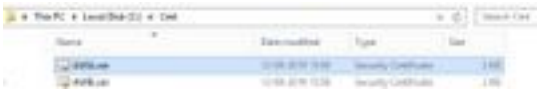
Étape 1. Accédez à l'URL https://localhost dans le serveur AW et téléchargez les certificats SSL du serveur.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

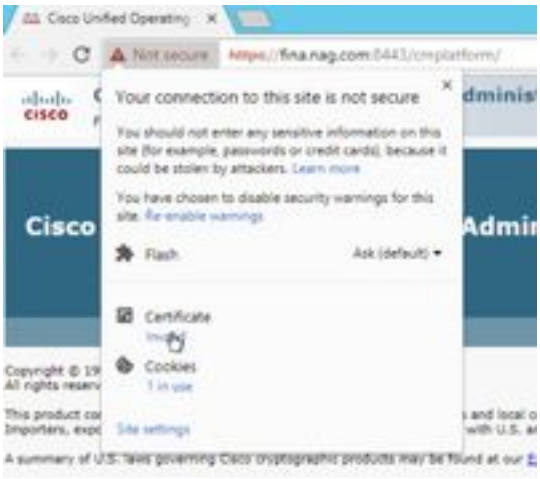


Étape 3.Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.



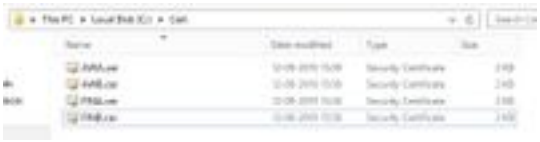
Finesse

Étape 1. Accédez au site https://Finesseserver:8443/cmplatform et téléchargez le certificat tomcat.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.



CEE de Cisco

Étape 1. Accédez au site https://ECEWebServer et téléchargez le certificat SSL du serveur.

Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

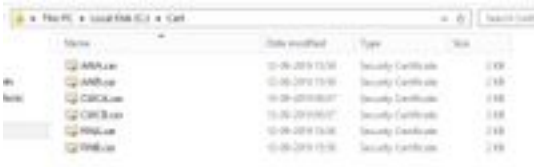
Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.

CUIC

Étape 1. Accédez au site https://CUICServer:8443/cmplatform et téléchargez le certificat tomcat.

Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.

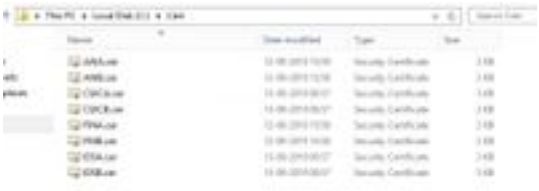


Cisco idS

Étape 1. Accédez au site https://IDSServer:8553/idsadmin/ et téléchargez le certificat tomcat.

Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.

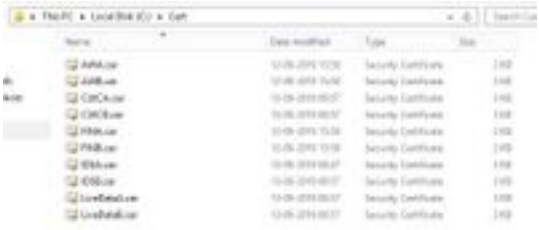


Données en direct

Étape 1. Accédez au site https://LiveDataServer:8444/cuic/gadget/LiveData/ et téléchargez le certificat tomcat.

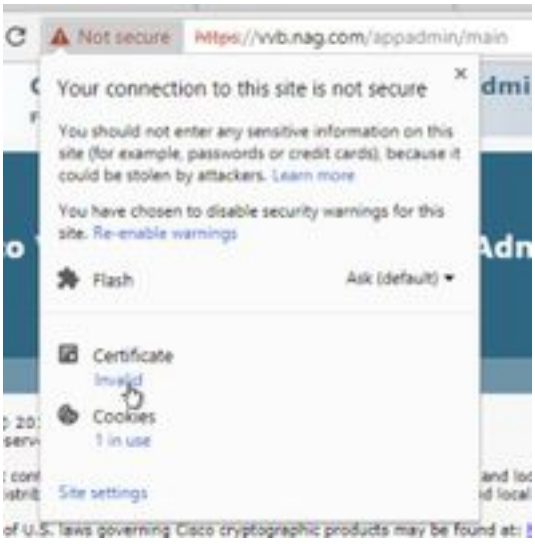
Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.



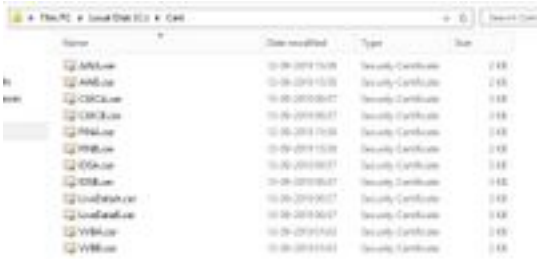
VVB

Étape 1. Accédez au site https://VVBServer/appadmin/main et téléchargez le certificat tomcat.



Étape 2. Dans la fenêtre de certificat, accédez à l'onglet Détails et cliquez sur le bouton Copier dans le fichier.

Étape 3. Sélectionnez Base-64 encoded X.509 (CER) et stockez le certificat dans le stockage local.



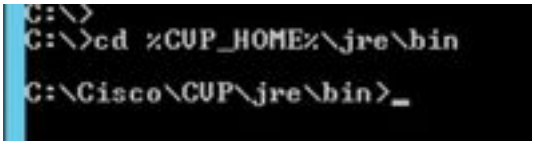
Importation de certificat SSL dans le magasin de clés

Serveur d'appels CVP et serveur de rapports

Étape 1. Connectez-vous au serveur CVP et copiez les certificats AW CCE Admin sur le **site C:\cisco\cvp\conf\security**.

Étape 2. Accédez à **%CVP_HOME%\conf** et ouvrez security.properties pour copier le mot de passe du magasin de clés.

Étape 3. Ouvrez l'invite de commandes en tant qu'administrateur et exécutez la commande **cd %CVP_HOME%\jre\bin**.



Étape 4. Utilisez cette commande pour importer les certificats AW sur le serveur CVP.

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

Étape 5. À l'invite du mot de passe, collez le mot de passe copié à partir du fichier security.properties.

Étape 6. Tapez **yes** pour faire confiance au certificat et vous assurer que le **certificat** de résultat **a été ajouté au keystore.**

Étape 7. Un avertissement s'affiche avec l'importation réussie. Ceci est dû au format propriétaire Keystore, vous pouvez l'ignorer.

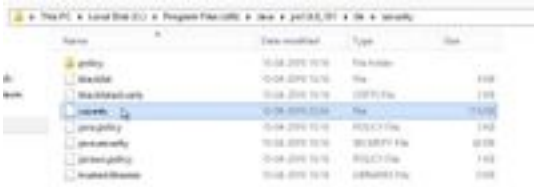
Avertissement :

Le keystore JCEKS utilise un format propriétaire. Il est recommandé de migrer vers PKCS12, qui est un format standard de l'industrie en utilisant « keytool -importkeystore -srckeystore C:\Cisco\CVP\conf\security\.keystore -destkeystore C:\Cisco\CVP\conf\security\.keystore -deststoretype pkcs12 ».

Station de travail Admin

Étape 1. Connectez-vous au serveur AW et ouvrez l'invite de commande en tant qu'administrateur.

Étape 2. Accédez à C:\Program Files(x86)\Java\jre1.8.0_181\lib\security and ensure the cacerts file exist.



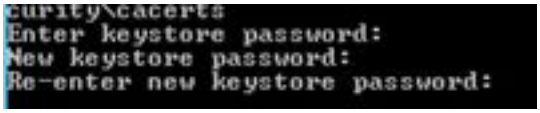
Étape 3. Tapez la commande **cd %JAVA_HOME%** et saisissez.

Étape 4. Utilisez cette commande afin d'importer les certificats Finesse sur le serveur AW.

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

Étape 5. La première fois que vous utilisez ce keytool, utilisez le mot de passe **changeit** afin de changer le mot de passe d'un magasin de certificats.

Étape 6. Saisissez un nouveau mot de passe pour le Keystore et saisissez-le à nouveau pour confirmer le mot de passe.



Étape 7. Tapez **yes** afin de faire confiance au certificat et de vous assurer que vous obtenez le **certificat** de résultat **a été ajouté à la banque de clés.**

Note: Les étapes 1 à 7 doivent être répétées avec tous les autres noeuds Finesse et tous les noeuds CUIC également

Étape 8. Si le mot de passe de la banque de clés a été saisi à tort ou a effectué les étapes sans réinitialiser, il est attendu qu'il obtienne cette exception.

Faire confiance à ce certificat ? [non] : oui

Le certificat a été ajouté à la banque de clés

erreur keytool : java.io.FileNotFoundException : .\lib\security\cacerts (Le système ne trouve pas le chemin spécifié)

Entrez le mot de passe de la banque de clés :
erreur keytool : java.io.IOException : Le magasin de clés a été modifié ou le mot de passe est incorrect

Étape 9. Afin de modifier le mot de passe keystore, utilisez cette commande et redémarrez la procédure à partir de l'étape 4 avec le nouveau mot de passe.

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

Étape 10. Après l'importation réussie, utilisez cette commande pour afficher le certificat à partir du magasin de clés.

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

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

Finesse, CUIC, Cisco idS et VVB

Étape 1. Connectez-vous à la page d'administration du système d'exploitation du serveur Finesse et téléchargez les certificats SSL AW dans l'approbation tomcat.

Étape 2. Accédez à **Administration du système d'exploitation > Sécurité > Gestion des certificats.**

Étape 3. Cliquez sur Upload Certificate\Certificate Chain et sélectionnez tomcat-trust dans la liste déroulante.

Étape 4. Parcourez le magasin de certificats dans le stockage local et cliquez sur le bouton Télécharger.

Étape 5. Répétez les étapes pour télécharger tous les certificats de serveur AW dans le cluster Finesse.

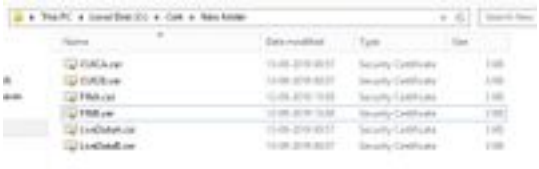
> **Note**: Il n'est pas nécessaire de télécharger le certificat tomcat-trust sur le noeud secondaire, il est automatiquement répliqué.

Étape 6. Redémarrez le service tomcat afin que les modifications de certificat prennent effet.

Étape 7. Dans CUIC, IDS et VVB, suivez les étapes de 2 à 4 et téléchargez le certificat AW.

Échange de certificats entre Finesse et CUIC/LiveData

Étape 1. Conservez les certificats Finesse, CUIC et LiveData dans un dossier distinct.



Étape 2. Connectez-vous à la page Finesse, CUIC et LiveData OS Administration.

Étape 3. Accédez à **Administration du système d'exploitation > Sécurité > Gestion des certificats.**

Étape 4. Cliquez sur Upload Certificate\Certificate Chain et sélectionnez tomcat-trust dans la liste déroulante.

Étape 5. Parcourez le magasin de certificats dans le stockage local et sélectionnez L'un des certificats de serveurs comme ci-dessous, puis cliquez sur le bouton Télécharger.

Dans le serveur Finesse - CUIC et LiveData comme confiance Tomcat

Dans CUIC Server - Finesse et LiveData comme confiance tomcat

In LiveData Server - CUIC et Finesse comme approbation Tomcat

> **Note**: Il n'est pas nécessaire de télécharger le certificat tomcat-trust sur le noeud secondaire, il est automatiquement répliqué.

Étape 6. Redémarrez le service tomcat sur chaque noeud afin que les modifications de certificat prennent effet.