Contenu

Introduction

Afin d'utiliser HTTPS pour la communication protégée entre la finesse et les serveurs du centre d'intelligence de Cisco Unified (CUIC), l'installation de Certificats de Sécurité est nécessaire. Par défaut ces serveurs fournissent les certifcates auto-signés qui sont utilisés ou les clients peuvent obtenir et installer des Certificats d'Autorité de certification (CA). Ces CERT CA peuvent être obtenus d'un fournisseur tiers comme Verisign, Thawte, GeoTrust ou peuvent être produits internaly.

Ce document vise à expliquer en détail les étapes impliquées pour obtenir et installer un certificat de l'autorité de certification (CA), généré d'un fournisseur tiers pour établir une connexion HTTPS entre la finesse et les serveurs du centre d'intelligence de Cisco Unified (CUIC).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco empaquettent le Contact Center Enterprise (PCCE)
- Centre d'intelligence de Cisco Unified (CUIC)
- Cisco Finesse
- Certificats CA

Composants utilisés

Les informations utilisées dans le document sont basées sur la version de la solution PCCE 11.0(1).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle étape.

Procédure

Installant les Certificats pour la transmission HTTPS dans la finesse et des serveurs du centre d'intelligence de Cisco Unified (CUIC) exigent les étapes suivantes

- Générez et téléchargez la demande de signature de certificat (CSR).
- Obtenez le certificat de racine, d'intermédiaire (si c'est approprié) et d'application de l'autorité de certification utilisant le CSR.
- Certificats de téléchargement aux serveurs.

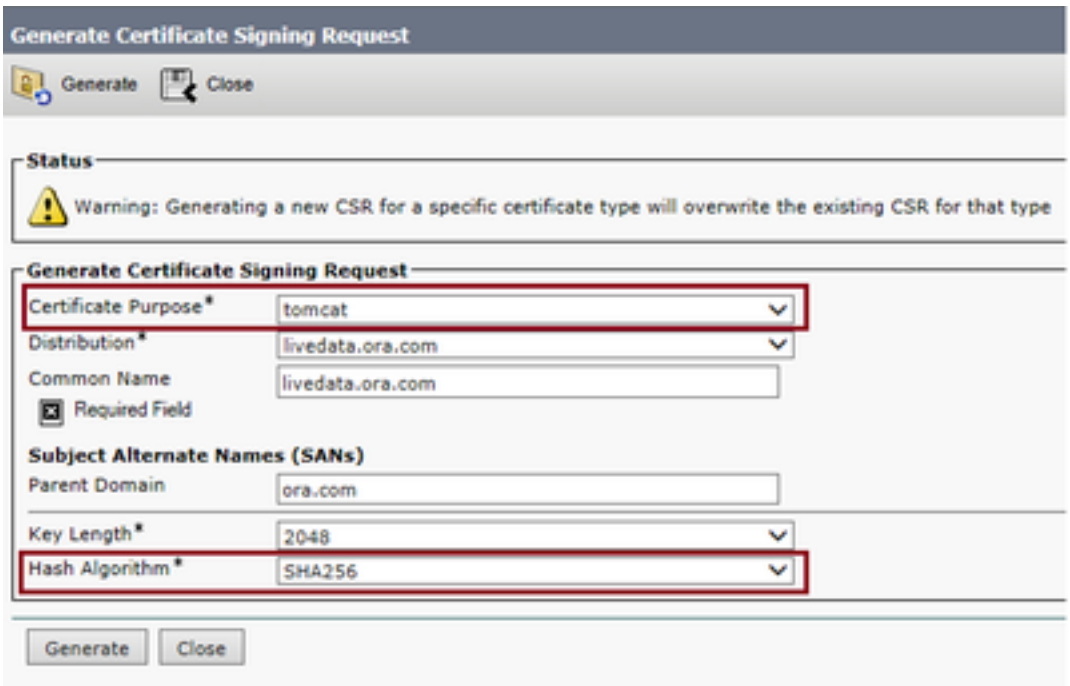
Étape 1 : Générez et téléchargez la demande de signature de certificat (le CSR)

---

1. Les étapes décrites ci-dessous pour générer et télécharger le CSR est mêmes pour la finesse et les serveurs CUIC.

2. Ouvrez la page du système d'exploitation de gestion de Cisco Unified Communications utilisant l'URL indiqué ci-dessous et connectez-vous avec le compte d'admin de SYSTÈME D'EXPLOITATION créé pendant le processus d'installation
https://hostname de serveur/de cmplatform primaires

3. Générez la demande de signature de certificat (le CSR)

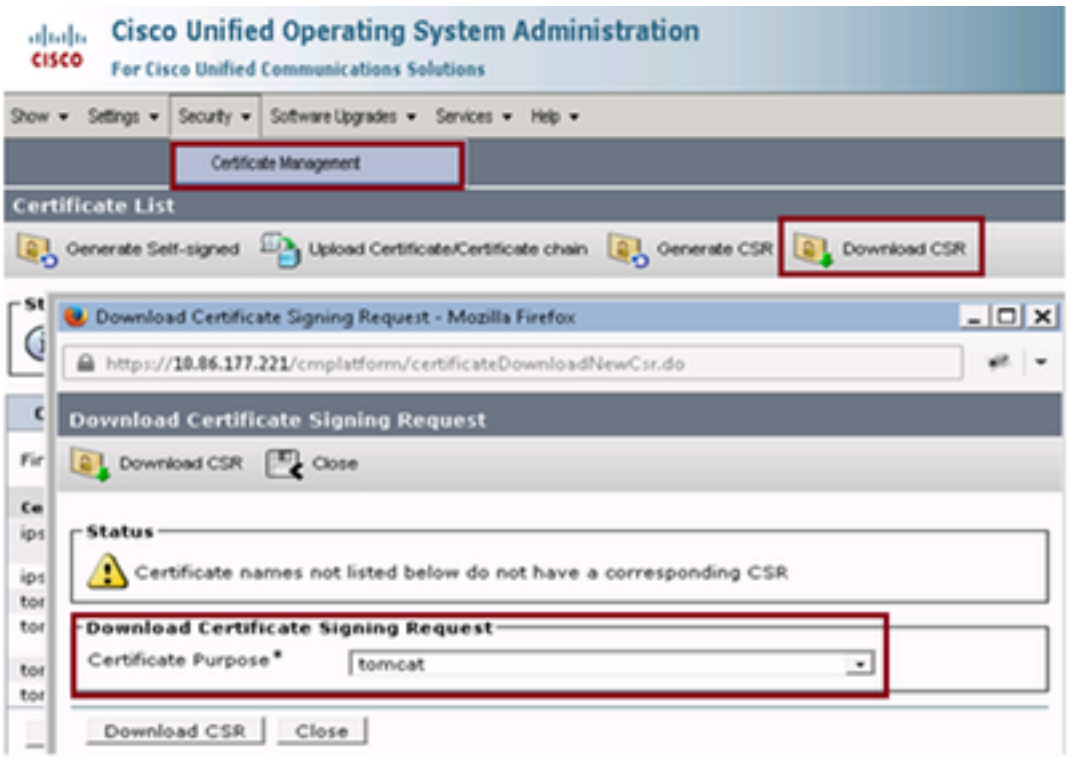


a) La Gestion choisie de Sécurité > de certificat > génèrent le CSR.

b) De la liste déroulante de nom de but de certificat, chat choisi.

c) Algorithme de hachage choisi comme SHA256
d) Le clic génèrent le CSR.

4. Demande de signature de certificat de téléchargement (CSR)



a) CSR Sécurité > de Gestion > de téléchargement de certificat choisis.
b) De la liste déroulante de nom de certificat, chat choisi.
c) Cliquez sur Download le CSR.

Remarque:

Exécutez les étapes mentionnées ci-dessus sur le serveur secondory employant l'URL « https://hostname du serveur/du cmplatform secondory » pour obtenir des CSR pour l'autorité de certification.

Étape 2 : Obtenez le certificat de racine, d'intermédiaire (si c'est approprié) et d'application de l'autorité de certification

---

1. Fournissez les informations primaires et secondory de la demande de signature de certificat de serveurs (CSR) à l'autorité de Certifcate de tiers (CA) comme Verisign, Thawte, GeoTrust etc.

2. De l'autorité de Certifcate (CA) on devrait recevoir la chaîne de certificat suivante pour les serveurs primaires et secondory.

- **Serveurs de finesse :** Certificat de racine, d'intermédiaire et d'application
- **Serveurs CUIC :** Certificat de racine et d'application

Étape 3 : Certificats de téléchargement aux serveurs

Cette section décrit sur la façon dont télécharger la chaîne de certificat correctement sur la finesse et les serveurs du centre d'intelligence de Cisco Unified (CUIC)

Serveurs de finesse :

==========

1. **Certificat primaire de racine du serveur de finesse de téléchargement**

a) À la page du système d'exploitation de gestion de Cisco Unified Communications de serveur primaire, choisie

Gestion de Sécurité > de certificat > certificat de téléchargement.

b) De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
c) Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier de certificat racine.
d) Cliquez sur Upload le fichier.

2. **Certificat intermédiaire de serveur primaire de finesse de téléchargement.**

a) De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
b) Dans le certificat racine classé, écrivez le nom du certificat racine que vous avez téléchargé dans l'étape précédente.

C'est un fichier .pem qui est généré quand la racine/certificat public a été installée. Pour visualiser ce fichier naviguez vers la Gestion de certificat > le ClickFind. Dans la liste .pem de certificat le nom du fichier sera répertorié contre la Tomcat-confiance.
c) Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier du certificat intermédiaire.
d) Cliquez sur Upload le fichier.

Remarque:
Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondory elle n'est pas nécessaire pour télécharger la racine du serveur primaire de finesse ou intermédiaire délivrez un certificat au serveur secondaire de finesse.

3. Certificat primaire de serveur d'application de finesse de téléchargement.

a) De la liste déroulante de nom de certificat, chat choisi.

b) Dans le domaine de certificat racine, écrivez le nom du certificat intermédiaire que vous avez téléchargé dans l'étape précédente. Incluez l'extension .pem (par exemple, TEST-SSL-CA.pem).

c) Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier du certificat d'application.
d) Cliquez sur Upload le fichier.

4. **Racine du serveur secondory de finesse de téléchargement et certificat intermédiaire.**

a) Suivez les mêmes étapes que mentionnées ci-dessus en (1) et (2) sur le serveur secondory pour ses Certificats

Remarque:
Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondory elle n'est pas nécessaire pour télécharger la racine du serveur secondory de finesse ou intermédiaire délivrez un certificat au serveur primaire de finesse.

5. Certificat secondory de serveur d'application de finesse de téléchargement.

a)

6. **Serveurs de reprise**

Accédez au CLI sur les serveurs primaires et secondory de finesse et sélectionnez la commande « redémarrage du système d'utils » de redémarrer les serveurs.

Serveurs CUIC :

==========

1. **Certificat primaire cuic de racine du serveur de téléchargement (public)**

a) À la page du système d'exploitation de gestion de Cisco Unified Communications de serveur primaire, choisie

Gestion de Sécurité > de certificat > certificat de téléchargement.

b) De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
c) Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier de certificat racine.
d) Cliquez sur Upload le fichier.

Remarque:
Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondory elle n'est pas nécessaire pour télécharger le certificat primaire de racine du serveur CUIC aux serveurs secondaires CUIC.

2. **Certificat (primaire) primaire cuic de serveur d'application de téléchargement**
a) De la liste déroulante de nom de certificat, chat choisi.
b) Dans le domaine de certificat racine, écrivez le nom du certificat racine que vous avez téléchargé dans l'étape précédente.

C'est un fichier .pem qui est généré quand la racine/certificat public a été installée. Pour visualiser ce fichier naviguez vers la Gestion de certificat > le ClickFind. Dans la liste .pem de certificat le nom du fichier sera répertorié contre la Tomcat-confiance. Incluez cette extension .pem (par exemple, TEST-SSL-CA.pem).

c) Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier du certificat (primaire) d'application.
d) Cliquez sur Upload le fichier

3. **Certificat secondory cuic de racine du serveur de téléchargement (public)**

a) Sur le serveur cuic secondory suivez les mêmes étapes que mentionnées dans l'étape (1) pour son certificat racine.

Remarque:
Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondory elle n'est pas nécessaire pour télécharger le certificat secondory de racine du serveur de CUIc au serveur primaire CUIC.

certificat (primaire) secondory cuic du serveur d'application 4.Upload.
a) Suivez le même processus comme stipulé dans l'étape (2) sur le serveur secondory pour son propre certificat.

6. **Serveurs de reprise**

Accédez au CLI sur les serveurs primaires et secondory CUIC et sélectionnez la commande « redémarrage du système d'utils » de redémarrer les serveurs.

Remarque:

Pour éviter l'exception de certificat vous avertissant doit accéder aux serveurs utilisant le nom du nom de domaine complet (FQDN).

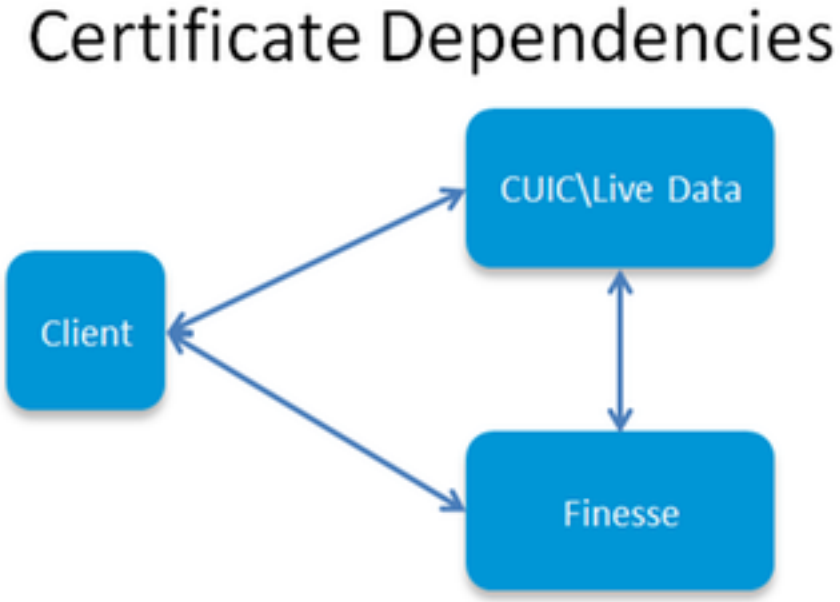
Dépendances de certificat :

==========

As

Les agents et les superviseurs de finesse utilisent des instruments CUIC pour signaler les buts

- Téléchargez le certificat racine de serveurs CUIC sur le service primaire de finesse
- Racine de finesse de téléchargement \ certificat intermédiaire sur le serveur primaire CUIC



a) **Téléchargez le certificat racine de serveurs CUIC sur le serveur primaire de finesse**

----

la page du système d'exploitation ouverte de gestion de Cisco Unified Communications de serveur

primaire de la finesse 1.On utilisant l'URL indiqué ci-dessous et se connectent avec le compte d'admin de SYSTÈME D'EXPLOITATION créé pendant les provcess d'installation

https://hostname de serveur/de cmplatform primaires de finesse

certificat racine primaire 2.Upload CUIC.
a) Gestion choisie de Sécurité > de certificat > certificat de téléchargement.
b) De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
c) Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier de certificat racine.
d) Cliquez sur Upload le fichier.

certificat racine 3.Upload Secondory CUIC.

a) Gestion choisie de Sécurité > de certificat > certificat de téléchargement.
b) De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
c) Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier de certificat racine.
d) Cliquez sur Upload le fichier.

Remarque:
Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondory elle n'est pas nécessaire pour télécharger les certificats racine CUIC au serveur secondaire de finesse.

4. Accédez au CLI sur les serveurs primaires et secondory de finesse et sélectionnez la commande « redémarrage du système d'utils » de redémarrer les serveurs.

b) Racine de finesse de téléchargement \ certificat intermédiaire sur le serveur primaire CUIC

---

la page du système d'exploitation ouverte de gestion de Cisco Unified Communications CUIC de serveur primaire 1.On utilisant l'URL indiqué ci-dessous et se connectent avec le compte d'admin de SYSTÈME D'EXPLOITATION créé pendant les provcess d'installation
https://hostname de serveur primaire/de cmplatform CUIC

certificat racine primaire de la finesse 2.Upload.
a) Gestion choisie de Sécurité > de certificat > certificat de téléchargement.
b) De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
c) Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier de certificat racine.
d) Cliquez sur Upload le fichier.

3. Certificat intermédiaire de finesse primaire de téléchargement

i) De la liste déroulante de nom de certificat, Tomcat-confiance choisie.
ii) Dans le certificat racine classé, écrivez le nom du certificat racine que vous avez téléchargé dans l'étape précédente.
iii) Dans le champ File de téléchargement, le clic parcourent et parcourent au fichier du certificat

intermédiaire.
iv) Cliquez sur Upload le fichier.

4. Exécutez les mêmes étapes (2 et 3) pour la racine secondory de finesse \ Certificats intermédiaires sur le serveur de données vivant primaire.

Remarque:

Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondory elle n'est pas nécessaire pour télécharger le certificat de /intermediate de racine de finesse aux serveurs secondaires CUIC.

5. Accédez au CLI sur les serveurs primaires et secondory CUIC et sélectionnez la commande « redémarrage du système d'utils » de redémarrer les serveurs.