Solution du module CCE : Procédure pour obtenir et télécharger de tiers Certificats CA

Contenu

Introduction

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

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

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco empaquettent le Contact Center Enterprise (PCCE)
- CUIC
- Cisco Finesse
- Certificats CA

Composants utilisés

Les informations utilisées dans le document sont basées sur la version de la solution 11.0 PCCE

(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

Afin d'installer des Certificats pour la transmission HTTPS dans la finesse et des serveurs CUIC, suivez ces étapes :

- Générez et téléchargez la demande de signature de certificat (le CSR)
- Obtenez le certificat de racine, d'intermédiaire (si c'est approprié) et d'application du CA avec l'utilisation du CSR
- Certificats de téléchargement aux serveurs

Générez et téléchargez le CSR

1. Les étapes décrites ici sont afin de générer et télécharger le CSR. Ces étapes sont identiques pour la finesse et les serveurs CUIC.

2. Ouvrez la page **du système d'exploitation de gestion de Cisco Unified Communications** avec l'URL et connectez-vous avec le compte du système d'exploitation d'admin (de SYSTÈME D'EXPLOITATION) créé au moment du processus d'installation. **https://hostname de serveur/de cmplatform primaires**

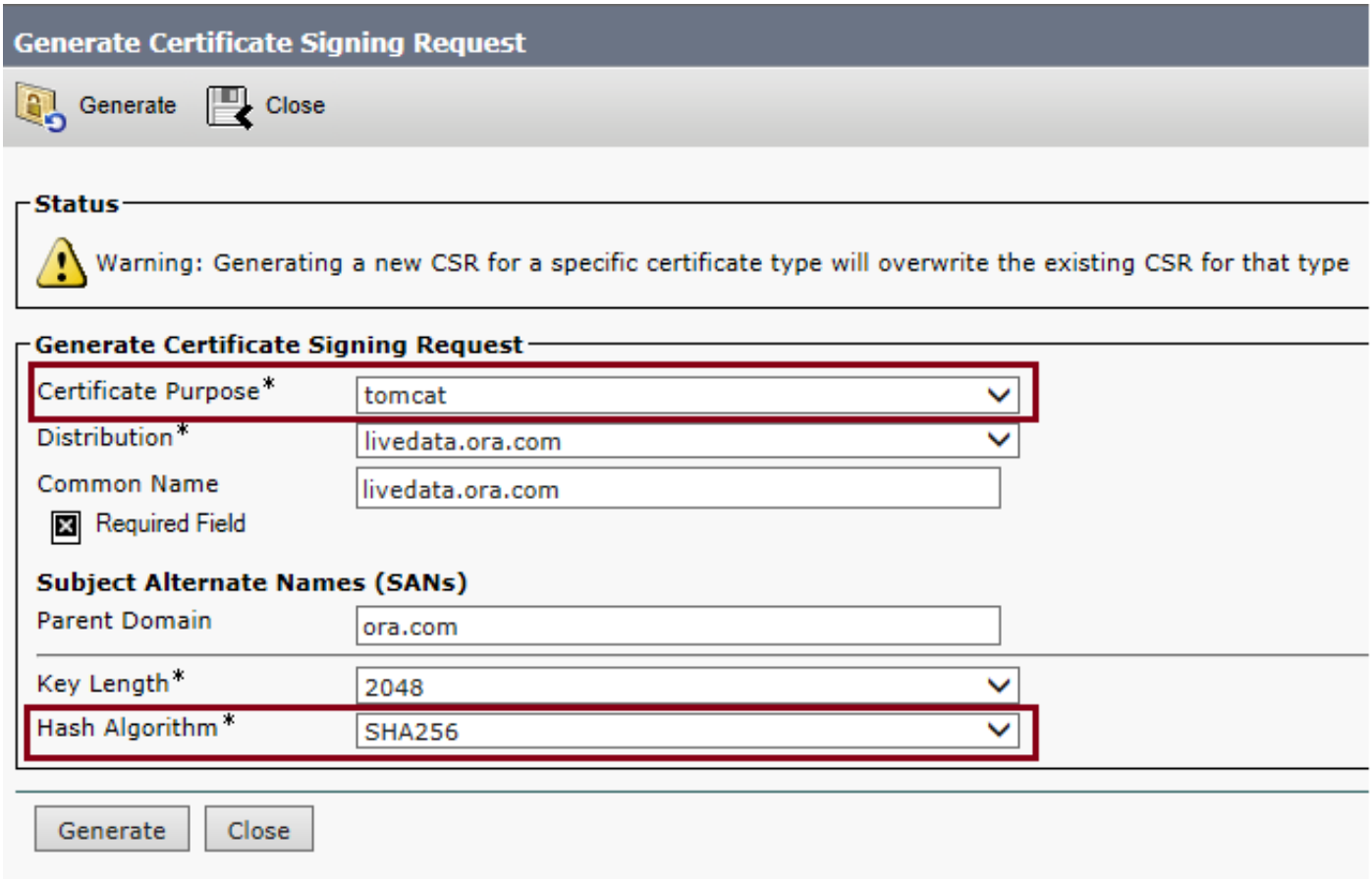
3. Générez la demande de signature de certificat.

a. Naviguez vers la **Gestion de Sécurité > de certificat > génèrent le CSR**.

b. De la liste déroulante de Purpose* de certificat, **chat** choisi.

c. Algorithme de hachage choisi comme **SHA256**.

d. Le clic **se produisent** suivant les indications de l'image.

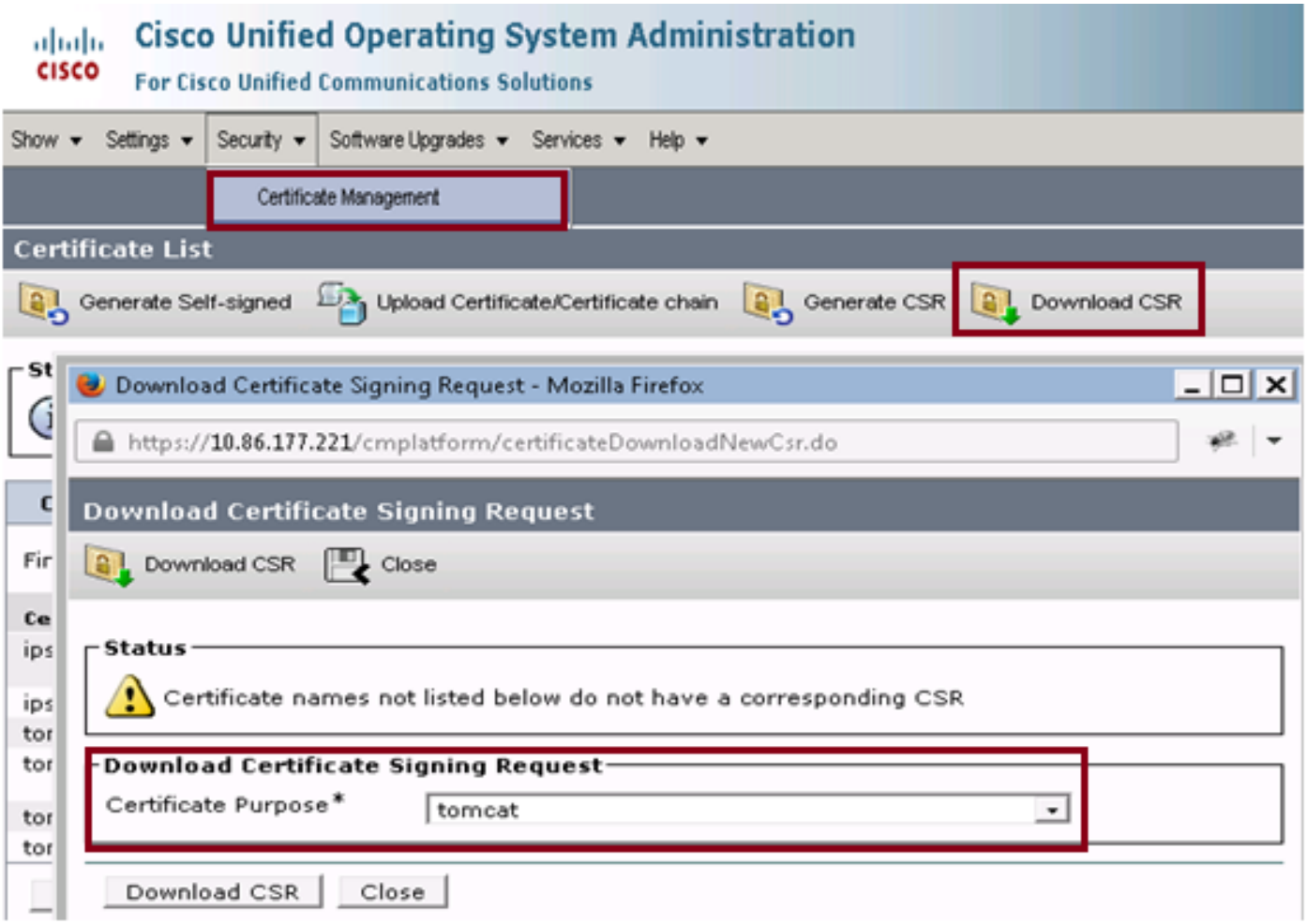


4. CSR de téléchargement.

a. Naviguez vers le **CSR de Sécurité > de Gestion > de téléchargement de certificat**.

b. De la liste déroulante de Purpose* de certificat, **chat** choisi.

c. Cliquez sur Download le **CSR** suivant les indications de l'image.



Note: Exécutez ces étapes sur le serveur secondaire avec l'URL **https://hostname du serveur/du cmplatform secondaires** afin d'obtenir des CSR pour le CA.

Obtenez le certificat de racine, d'intermédiaire (si c'est approprié) et d'application du CA

1. Fournissez les informations CSR du serveur primaire et secondaire au tiers CA comme Verisign, Thawte, GeoTrust etc.

2. Du CA, vous devez recevoir ces la chaîne de certificat pour les serveurs primaires et secondaires :

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

Certificats de téléchargement aux serveurs

Cette section décrit sur la façon dont télécharger la chaîne de certificat correctement sur la finesse et les serveurs 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 du** serveur primaire, naviguez vers la **Gestion de Sécurité > de certificat > le certificat de téléchargement**.

b. De la liste déroulante de but de certificat, Tomcat-**confiance** choisie.

c. Dans le champ File de téléchargement, le clic **parcourent** et parcourent le **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 but de certificat, Tomcat-**confiance** choisie.

b. Dans le certificat racine classé, écrivez le nom du certificat racine qui est téléchargé dans l'étape précédente. C'est un fichier **.pem** qui est généré quand la racine/certificat public a été installée.

Afin de visualiser ce fichier, naviguez vers la **Gestion de certificat > la découverte**. Dans la liste de certificat, le nom du fichier **.pem** est répertorié contre la Tomcat-confiance.

c. Dans le champ File de téléchargement, le clic **parcourent** et parcourent le **fichier du certificat intermédiaire**.

d. Cliquez sur Upload le **fichier**.

> **Note**: Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondaires, elle n'est pas nécessaire pour télécharger la racine du serveur primaire de finesse ou le certificat intermédiaire au serveur secondaire de finesse.

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

a. De la liste déroulante de but de certificat, **chat** choisi.

b. Dans le domaine de certificat racine, écrivez le nom du certificat intermédiaire qui est 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 le **fichier du certificat d'application**.

d. Cliquez sur Upload le **fichier**.

4. Racine du serveur secondaire de finesse de téléchargement et certificat intermédiaire :

a. Suivez les mêmes étapes que mentionnées dans les étapes 1 et 2 sur le serveur secondaire pour ses Certificats.

> **Note**: Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondaires, elle n'est pas nécessaire pour télécharger la racine du serveur secondaire de finesse ou le certificat intermédiaire au serveur primaire de finesse.

5. Certificat secondaire de serveur d'application de finesse de téléchargement :

a. Suivez les mêmes étapes que mentionnées dans l'étape 3. sur le serveur secondaire pour ses propres Certificats.

6. Serveurs de reprise :

a. Accédez au CLI sur les serveurs primaires et secondaires de finesse et exécutez le **redémarrage du système d'utils de** commande afin de redémarrer les serveurs.

Serveurs CUIC

1. Certificat primaire de racine du serveur du téléchargement CUIC (public) :

a. À la page **du système d'exploitation de gestion de Cisco Unified Communications du** serveur primaire, naviguez vers la **Gestion de Sécurité > de certificat > le certificat de téléchargement**.

b. De la liste déroulante de but de certificat, Tomcat-**confiance** choisie.

c. Dans le champ File de téléchargement, le clic **parcourent** et parcourent le **fichier de certificat racine**.

d. Cliquez sur Upload le **fichier**.

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

2. Certificat (primaire) primaire de serveur d'application du téléchargement CUIC :

a. De la liste déroulante de but de certificat, **chat** choisi.

b. Dans le domaine de certificat racine, écrivez le nom du certificat racine qui est téléchargé dans l'étape précédente.

C'est un fichier **.pem** qui est généré quand la racine/certificat public a été installée. Afin de visualiser ce fichier, naviguez vers la **Gestion de certificat > la découverte**.

Dans la liste **.pem de** certificat le nom du fichier est 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 le **fichier du certificat (primaire) d'application**.

d. Cliquez sur Upload le **fichier**.

3. Certificat secondaire de racine du serveur du téléchargement CUIC (public) :

a. Sur le serveur secondaire CUIC, suivez les mêmes étapes que mentionnées dans l'étape 1. pour son certificat racine.

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

4. Certificat (primaire) secondaire de serveur d'application du téléchargement CUIC :

a. Suivez le même processus comme stipulé dans l'étape 2. sur le serveur secondaire pour son propre certificat.

5. Serveurs de reprise :

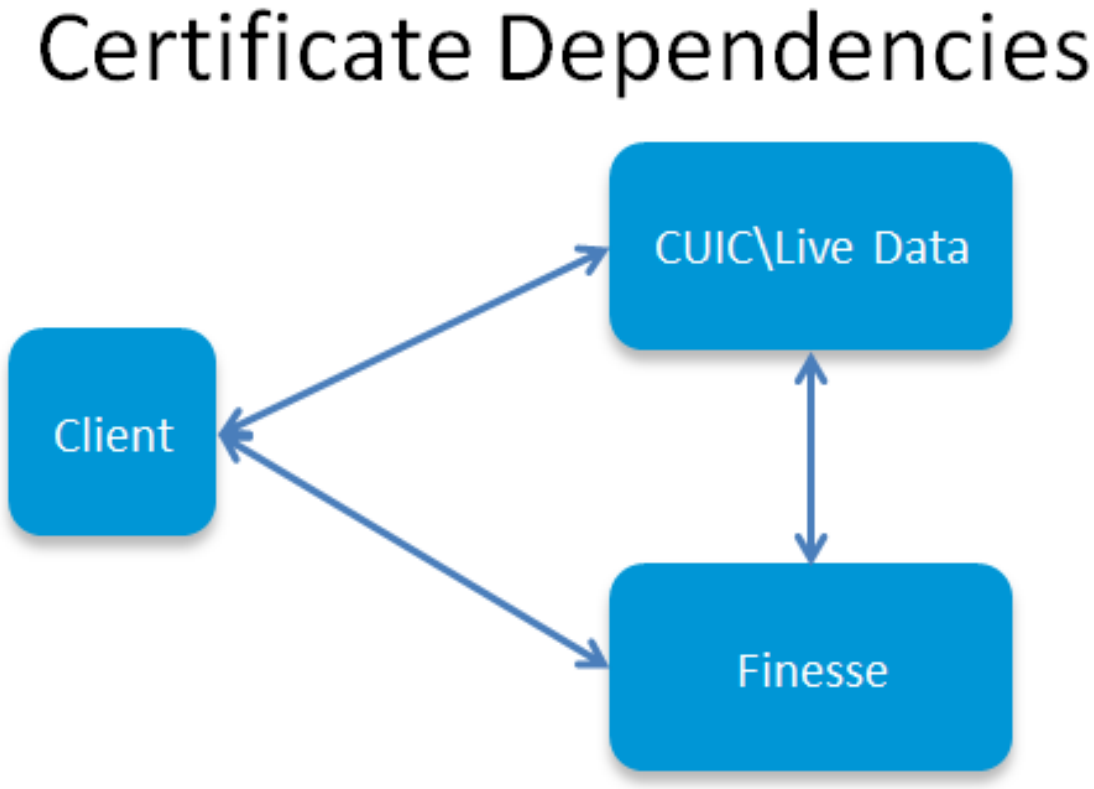
a. Accédez au CLI sur les serveurs primaires et secondaires CUIC et exécutez le **redémarrage du système d'utils de** commande afin de redémarrer les serveurs.

Note: Afin d'éviter l'avertissement d'exception de certificat, vous devez accéder aux serveurs avec l'utilisation du nom de domaine complet (FQDN).

Dépendances de certificat

Car les agents et les superviseurs de finesse utilisent des instruments CUIC pour signaler des buts, vous devez télécharger des certificats racine de ces serveurs aussi bien, dans la commande mentionnée ici pour mettre à jour des dépendances de certificat pour la transmission HTTPS entre ces serveurs et suivant les indications de l'image.

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



Certificat racine de serveurs du téléchargement CUIC sur le serveur primaire de finesse

1. Sur le serveur primaire de finesse, la page **du système d'exploitation** ouverte de **gestion de Cisco Unified Communications** avec l'URL et se connectent avec le compte d'admin de SYSTÈME D'EXPLOITATION créé au moment du processus d'installation :

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

2. Certificat racine primaire du téléchargement CUIC.

a. Naviguez vers la **Gestion de Sécurité > de certificat > le certificat de téléchargement**.

b. De la liste déroulante de but de certificat, Tomcat-**confiance** choisie.

c. Dans le champ File de téléchargement, le clic **parcourent** et parcourent le **fichier de certificat racine**.

d. Cliquez sur Upload le **fichier**.

3. Certificat racine secondaire du téléchargement CUIC.

a. Naviguez vers la **Gestion de Sécurité > de certificat > le certificat de téléchargement**.

b. De la liste déroulante de but de certificat, Tomcat-**confiance** choisie.

c. Dans le champ File de téléchargement, le clic **parcourent** et parcourent le **fichier de certificat racine**.

d. Cliquez sur Upload le **fichier**.

> **Note**: Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondaires, 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 secondaires de finesse et exécutez le **redémarrage du système d'utils de** commande afin de redémarrer les serveurs.

Racine de finesse de téléchargement/certificat intermédiaire sur le serveur primaire CUIC

1. Sur le serveur primaire CUIC, la page **du système d'exploitation** ouverte de **gestion de Cisco Unified Communications** avec l'URL et se connectent avec le compte d'admin de SYSTÈME D'EXPLOITATION créé au moment du processus d'installation :

https://hostname de serveur primaire/de cmplatform CUIC

2. Certificat racine primaire de finesse de téléchargement :

a. Naviguez vers la **Gestion de Sécurité > de certificat > le certificat de téléchargement**.

b. De la liste déroulante de but de certificat, Tomcat-**confiance** choisie.

c. Dans le champ File de téléchargement, le clic **parcourent** et parcourent le **fichier de certificat racine**.

d. Cliquez sur Upload le **fichier**.

certificat intermédiaire de la finesse 3.Upload primaire :

a. De la liste déroulante de but de certificat, Tomcat-**confiance** choisie.

b. Dans le certificat racine classé, écrivez le nom du certificat racine qui est téléchargé dans l'étape précédente.

c. Dans le champ File de téléchargement, le clic **parcourent** et parcourent le **fichier du certificat intermédiaire**.

d. Cliquez sur Upload le **fichier**.

4. Exécutez la même étape 2 et l'étape 3. pour la racine secondaire de finesse \ Certificats intermédiaires sur le serveur de données vivant primaire.

> **Note**: Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondaires, 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 secondaires CUIC et exécutez le **redémarrage du système d'utils de** commande afin de redémarrer les serveurs.