

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Procédure](#)

[Étape 1 : Générez et téléchargez la demande de signature de certificat \(le CSR\)](#)

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

[Étape 3 : Certificats de téléchargement aux serveurs.](#)

[Serveurs de finesse :](#)

[Serveurs CUIC :](#)

[Serveurs de données vivants :](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Afin d'utiliser HTTPS pour la communication protégée entre la finesse, le centre d'intelligence de Cisco Unified (CUIC) et les serveurs de données vivants, 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 le certificat 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, le centre d'intelligence de Cisco Unified (CUIC), et pour vivre des serveurs de données.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Enterprise (UCCE)
- Données vivantes de Cisco
- Centre d'intelligence de Cisco Unified (CUIC)
- Cisco Finesse
- CA diplômée

[Composants utilisés](#)

Les informations utilisées dans le document sont basées sur la version de la solution UCCE 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 le certificat pour la transmission HTTPS dans la finesse, CUIIC et serveurs de données vivants exigent les étapes suivantes

- Générez et téléchargez la demande de signature de certificat (CSR).
- Obtenez la racine, l'intermédiaire (si c'est approprié) et le certificat 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, CUIIC et les données vivantes divisent.


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 les provcess d'installation
<https://hostname de serveur/de cmplatform primaires>

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

Generate Certificate Signing Request

 Generate  Close

Status

 Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat
Distribution*	livedata.ora.com
Common Name	livedata.ora.com
<input checked="" type="checkbox"/> Required Field	
Subject Alternate Names (SANs)	
Parent Domain	ora.com
Key Length*	2048
Hash Algorithm*	SHA256

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)

The image shows two screenshots from the Cisco Unified Operating System Administration interface. The top screenshot displays the 'Certificate Management' section with a 'Download CSR' button highlighted. The bottom screenshot shows a 'Download Certificate Signing Request' dialog box with a 'Certificate Purpose' dropdown menu set to 'tomcat', also highlighted.

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 secondary employant l'URL « <https://hostname du serveur/du cmplatform secondary> » 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 secondary de la demande de signature de certificat de serveurs (CSR) à l'autorité de Certificate de tiers (CA) comme Verisign, Thawte, GeoTrust etc.

2. De l'autorité de Certificate (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
- **Services vivants de données** : 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, CUIC et vivre des serveurs de données.

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 parcourt et parcourt au fichier de certificat racine.

d) Cliquez sur Upload le fichier.

2. Certificat intermédiaire de serveur fineese primaire 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. N'incluez pas l'extension (par exemple, racine CA 2048 de TEST).

c) Dans le champ File de téléchargement, le clic parcourt et parcourt 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 parcourt et parcourt au fichier du certificat d'application.

d) Cliquez sur Upload le fichier.

4. Racine du serveur de finesse de Secondary de téléchargement et certificat intermédiaire.

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

Remarque:

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

5. Certificat fineese secondary de serveur d'application de téléchargement.

a)

6. Serveurs de reprise

Accédez au CLI sur les serveurs primaires et secondary de finesse et sélectionnez la commande « redémarrage du système d'utilis » 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 parcourt et parcourt 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 secondary 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. Incluez l'extension .pem (par exemple, TEST-SSL-CA.pem).

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

d) Cliquez sur Upload le fichier

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

a) Sur le serveur cuic secondary 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 secondary elle n'est pas nécessaire pour télécharger le certificat secondary de racine du serveur de CUIC au serveur primaire CUIC.

certificat (primaire) secondary cuic du serveur d'application 4.Upload.

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

6. Serveurs de reprise

Accédez au CLI sur les serveurs primaires et secondary CUIC et sélectionnez la commande « redémarrage du système d'utilis » 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).

Serveurs de données vivants :

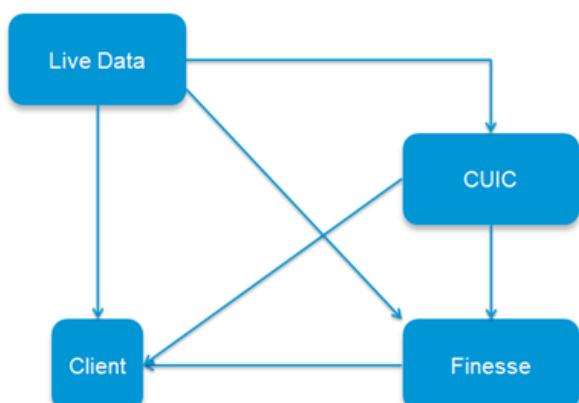
=====

1. Pour télécharger des données vivantes enracinez et le certificate d'application suivent les mêmes étapes que tracées les grandes lignes ci-dessus pour des serveurs CUIC.

2. En tant que serveurs de données vivants interagissez avec CUIC et serveurs un de finesse doit télécharger des certificats racine de ces serveurs aussi bien dans l'ordre suivant pour mettre à jour des dépendances de certificat.

- **Téléchargez la** racine de finesse \ intermédiaire et les certificats racine CUIC sur le serveur de données vivant
- Téléchargez le certificat racine de serveurs de Vivant-données sur le serveur primaire de finesse
- Téléchargez le certificat racine de serveurs CUIC sur le serveur primaire de finesse
- Certificats racine de Vivant-données de téléchargement sur le serveur primaire CUIC
- Racine de finesse de téléchargement \ certificat intermédiaire sur le serveur primaire CUIC

Certificate Dependencies



a) Téléchargez la racine de finesse \ intermédiaire et les certificats racine CUIC sur le serveur de données vivant

1. Certificat racine primaire de finesse de téléchargement

i) Sur le serveur de données vivant primaire en page du système d'exploitation de gestion de Cisco Unified Communications, choisie

Gestion de Sécurité > de certificat > certificat de téléchargement

ii) De la liste déroulante de nom de certificat, Tomcat-confiance choisie.

III) Dans le champ File de téléchargement, le clic parcourt et parcourt au fichier de certificat racine primaire de finesse.

iv) Cliquez sur Upload le fichier.

2. 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. N'incluez pas l'extension (par exemple, racine CA 2048 de TEST).

iii) Dans le champ File de téléchargement, le clic parcourt et parcourt au fichier du certificat intermédiaire.

iv) Cliquez sur Upload le fichier.

3. Certificat racine primaire du téléchargement CUIC

i) Sur le serveur de données vivant primaire en page du système d'exploitation de gestion de Cisco Unified Communications, choisie

Gestion de Sécurité > de certificat > certificat de téléchargement

ii) De la liste déroulante de nom de certificat, Tomcat-confiance choisie.

iii) Dans le champ File de téléchargement, le clic parcourt et parcourt au fichier de certificat racine primaire CUIC.

iv) Cliquez sur Upload le fichier.

4. Exécutez les mêmes étapes (1 et 2) pour la racine de finesse \ intermédiaire et les certificats racine secondary CUIC sur le serveur de données vivant primaire.

Remarque:

Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondary elle n'est pas nécessaire pour télécharger la racine de finesse/intermediate et les certificats racine CUIC au serveur de données vivant secondary.

5. Accédez au CLI sur les serveurs de données vivants primaires et secondary et sélectionnez la commande « redémarrage du système d'utilis » de redémarrer les serveurs.

b)

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 processus d'installation

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

certificat racine vivant primaire des données 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 parcourt et parcourt au fichier de certificat racine.
- d) Cliquez sur Upload le fichier.

certificat racine vivant de données 3.Upload Secondary.

- 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 parcourt et parcourt 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 secondary elle n'est pas nécessaire pour télécharger le certificat racine vivant de données au serveur secondaire de finesse.

c)

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 processus d'installation

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

certificat racine primaire 2.Upload CUIIC.

- 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 parcourt et parcourt au fichier de certificat racine.
- d) Cliquez sur Upload le fichier.

certificat racine 3.Upload Secondary CUIIC.

- 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 parcourt et parcourt 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 racine vivant de données 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'utilis » de redémarrer les serveurs.

d) Certificats racine de Vivant-données de téléchargement sur le serveur primaire CUIIC

1. À la page du système d'exploitation ouverte de gestion de Cisco Unified Communications de serveur primaire CUIIC utilisant l'URL indiqué ci-dessous et connectez-vous avec le compte d'admin de SYSTÈME D'EXPLOITATION créé pendant les processus d'installation
<https://hostname de serveur primaire/de cmplatform CUIIC>

certificat racine vivant primaire des données 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 parcourt et parcourt au fichier de certificat racine.
- d) Cliquez sur Upload le fichier.

certificat racine vivant de données 3.Upload Secondary.

- 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 parcourt et parcourt 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 racine vivant de données aux serveurs secondaires CUIIC.

e) Racine de finesse de téléchargement \ certificat intermédiaire sur le serveur primaire CUIIC

la page du système d'exploitation ouverte de gestion de Cisco Unified Communications CUIIC 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 processus d'installation
<https://hostname de serveur primaire/de cmplatform CUIIC>

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 parcourt et parcourt 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 parcourt et parcourt au fichier du certificat intermédiaire.
- iv) Cliquez sur Upload le fichier.

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

Remarque:

Pendant que la mémoire de Tomcat-confiance est répliquée entre les serveurs primaires et secondary 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 secondary CUIC et sélectionnez la commande « redémarrage du système d'utilis » de redémarrer les serveurs.