Configurer la communication sécurisée entre Finesse et CTI Server

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Configuration](#)
[CCE CTI Server Secure](#)
[Configuration sécurisée Finesse](#)
[Générer un certificat PG d'agent (serveur CTI)](#)
[Obtenir le certificat CSR signé par une autorité de certification](#)
[Importer les certificats signés CCE PGs CA](#)
[Générer un certificat Finesse](#)
[Signer le certificat Finesse par une autorité de certification](#)
[Importer les certificats signés de l'application Finesse et de la racine](#)
[Vérification](#)
[Dépannage](#)

Introduction

Ce document décrit comment mettre en oeuvre des certificats signés par l'autorité de certification (CA) entre Cisco Finesse et le serveur CTI (Computer Telephony Integration) dans la solution Cisco Contact Center Enterprise (CCE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version 12.0(1) du CCE
- Finesse Version 12.0(1)
- Serveur CTI

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Packaged CCE (PCCE) 12.0(1)

- Finesse 12.0(1)

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

Dans la version 11.5 de CCE, Cisco a commencé à prendre en charge la version 1.2 de Transport Layer Security (TLS), qui permet le transport sécurisé des messages SIP (Session Initiation Protocol) et RTP (Real-time Transport Protocol) via TLS 1.2. À partir de CCE 12.0 et dans le cadre de la sécurisation des données en mouvement, Cisco a commencé à prendre en charge TLS 1.2 sur la plupart des flux d'appels du centre de contacts : Baisse des données vocales entrantes et sortantes, multicanaux et externes. Ce document est axé sur la voix entrante, en particulier la communication entre Finesse et CTI Server.

Le serveur CTI prend en charge les modes de connexion suivants :

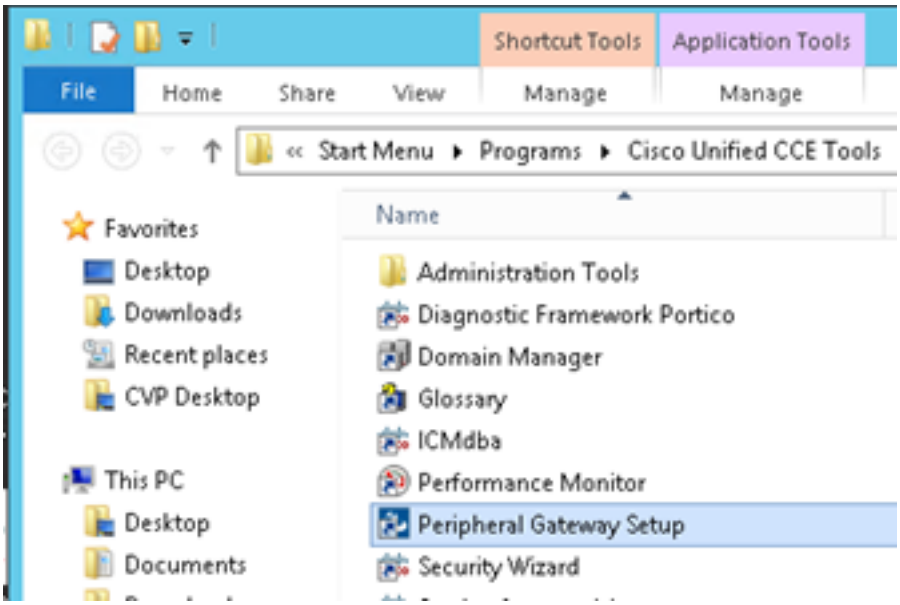
- **Connexion sécurisée uniquement** : Permet une connexion sécurisée entre le serveur CTI et les clients CTI (Finesse, dialer, CTIOS et ctitest).
- **Connexion sécurisée et non sécurisée (mode mixte) :** Permet la connexion sécurisée, ainsi que la connexion non sécurisée entre le serveur CTI et les clients CTI. Il s'agit du mode de connexion par défaut. Ce mode sera configuré lors de la mise à niveau des versions précédentes vers CCE 12.0(1).

  Note: Le mode non sécurisé uniquement n'est pas pris en charge.

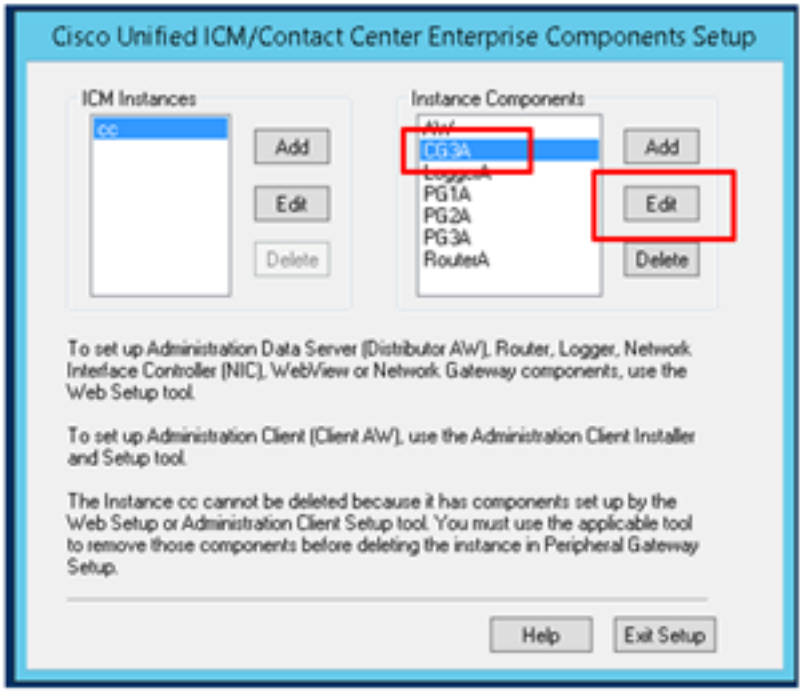
Configuration

CCE CTI Server Secure

Étape 1. Sur la station de travail administrative PCCE (AW), ouvrez le dossier **Outils Unified CCE** et double-cliquez sur **Configuration de la passerelle d'accès aux périphériques**.

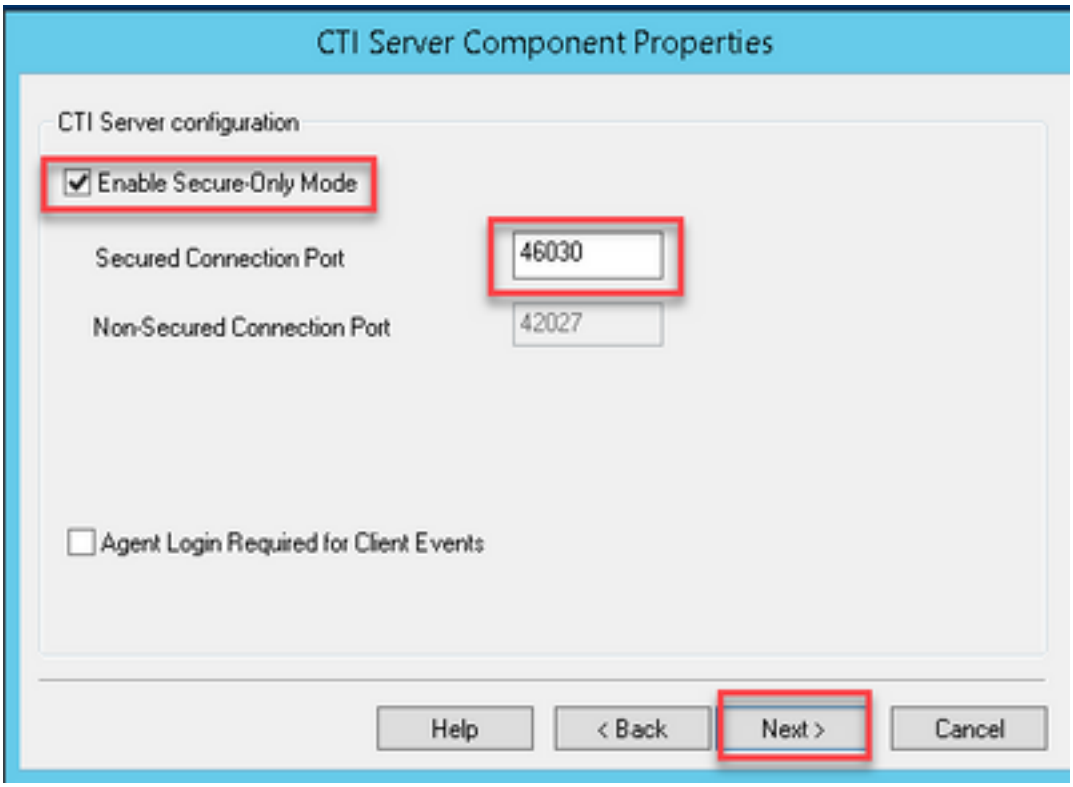


Étape 2. Sélectionnez **CG3A** et cliquez sur **Modifier**.



Étape 3. Dans les propriétés du serveur CTI, cliquez sur **Suivant**. Pour la question relative à l'arrêt du service **CG3A**, sélectionnez **Oui**.

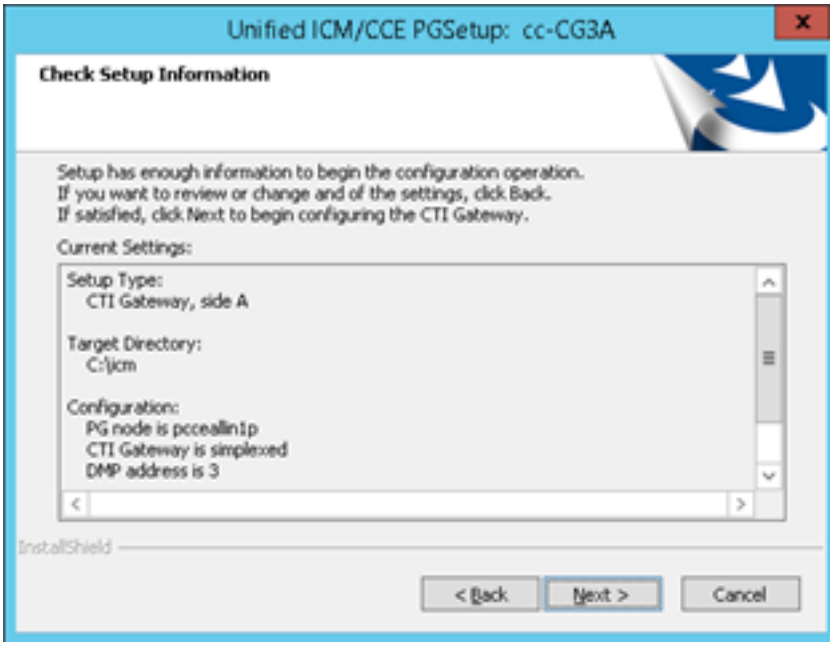
Étape 4. Dans les **propriétés des composants du serveur CTI**, sélectionnez **Activer le mode sécurisé uniquement.** Notez le **port de connexion sécurisé (46030)**, car vous devez configurer le même port dans Finesse dans l'exercice suivant. Cliquez sur **Next** (Suivant).



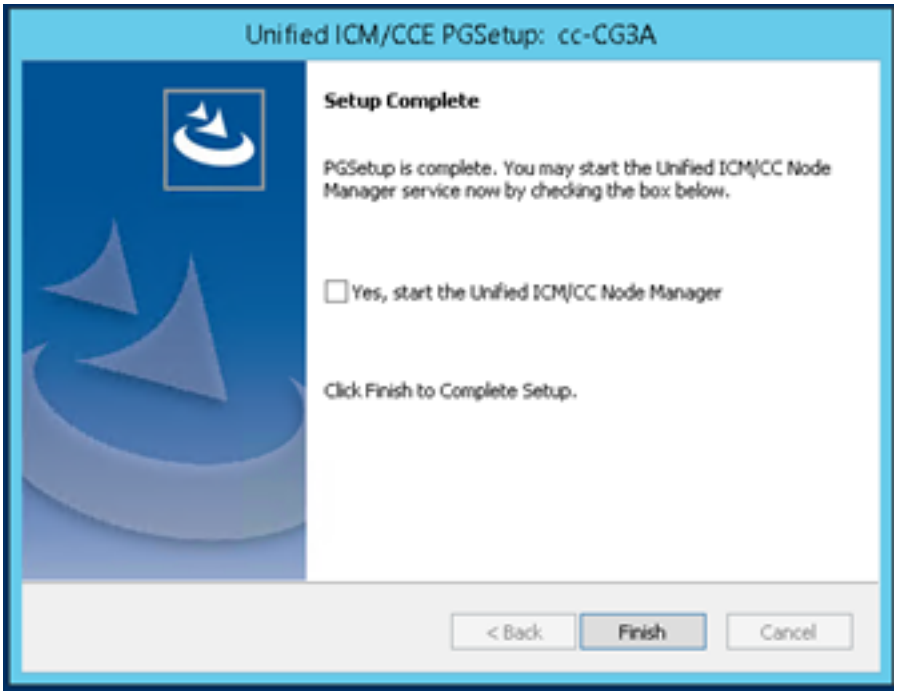
Note: La communication sécurisée par défaut est 42030, mais les travaux pratiques utilisés pour ce document sont 40630. Le numéro de port fait partie d'une formule qui inclut l'ID système ICM. Lorsque l'ID système est 1 (CG1a), le numéro de port par défaut est

généralement 42030. Comme l'ID système du TP est 3 (CG3a), le numéro de port par défaut est 46030.

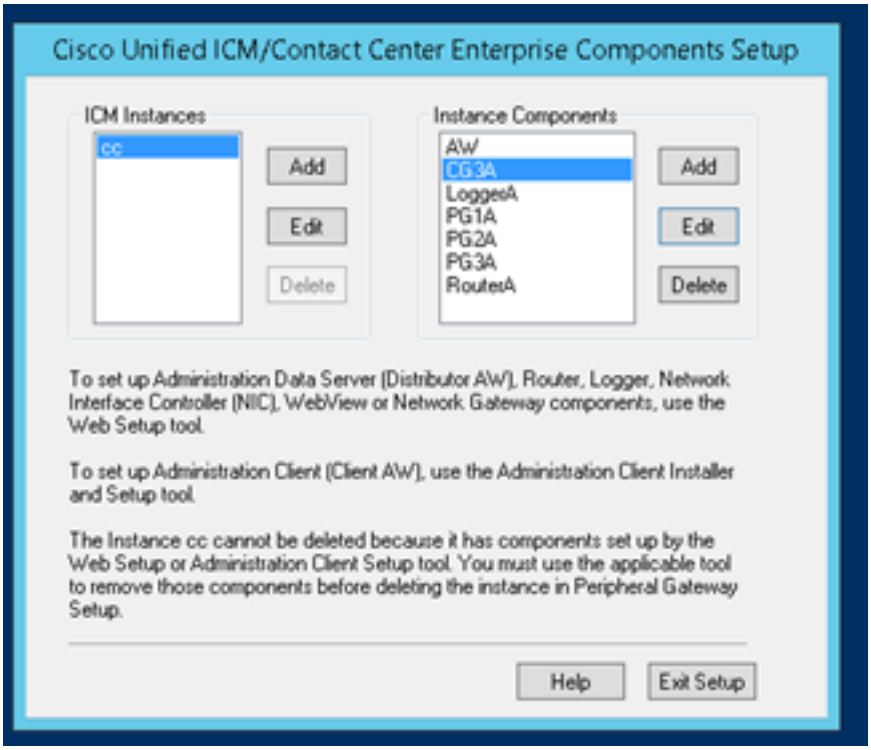
Étape 5. Dans les **propriétés de l'interface réseau CTI**, cliquez sur **Suivant**. Vérifiez les **informations de configuration** et cliquez sur **Suivant**.



Étape 6. Cliquez sur **Terminer** comme indiqué dans l'image.



Étape 7. Cliquez sur **Quitter le programme d'installation** et attendez que la fenêtre de configuration se ferme comme indiqué dans l'image.



Étape 8. Sur le bureau PCCEAllin1, double-cliquez sur **Unified CCE service Control**.

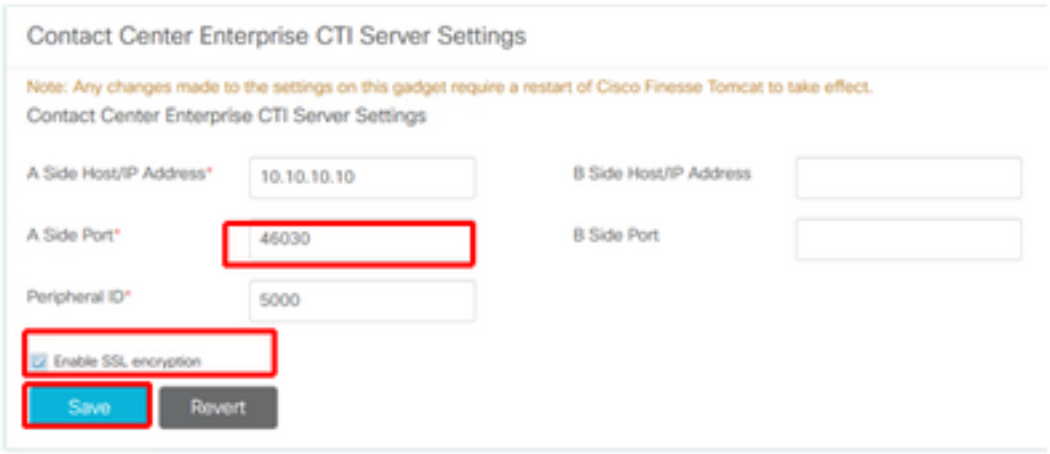
Étape 9. Sélectionnez Cisco ICM cc CG3A et cliquez sur **Démarrer**.

Configuration sécurisée Finesse

Étape 1. Ouvrez un navigateur Web et accédez à **Finesse Administration**.

Étape 2. Faites défiler jusqu'à la section **Paramètres du serveur CTI du centre de contacts de l'entreprise** comme indiqué dans l'image.

Étape 3. Modifiez le port latéral A du port de communication sécurisé configuré sur CG3A dans l'exercice précédent : **46030.** Cochez **Activer le chiffrement SSL** et cliquez sur **Enregistrer**.



Remarque : pour tester la connexion, vous devez d'abord redémarrer Finesse Tomcat Service ou redémarrer le serveur Finesse.

Étape 4. Déconnectez-vous de la page Administration Finesse.

Étape 5. Ouvrez une session SSH avec Finesse.

Étape 6. Dans la session SSH FINESSEA, exécutez la commande suivante :

utils system restart

Entrez **yes** lorsque vous êtes invité à redémarrer le système.

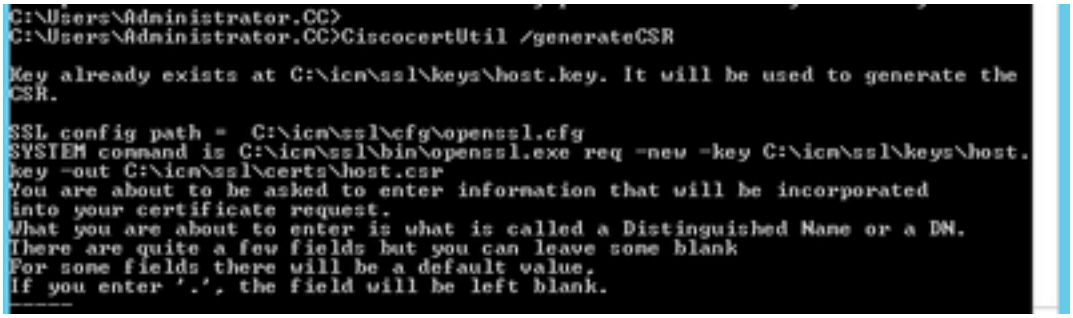
```
Using username "administrator".
Command Line Interface is starting up, please wait ...

   Welcome to the Platform Command Line Interface

VMware Installation:
        2 vCPU: Intel(R) Xeon(R) CPU E5-2680 0 @ 2.70GHz
        Disk 1: 146GB, Partitions aligned
        8192 Mbytes RAM

admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? yes


 Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
```

Générer un certificat PG d'agent (serveur CTI)

CiscoCertUtils est un nouvel outil disponible sur CCE Version 12. Cet outil vous permet de gérer tous les certificats CCE pour la voix entrante. Dans ce document, vous utilisez ces CiscoCertUtils

afin de générer les demandes de signature de certificat des passerelles de périphérique (PG).

Étape 1. Exécutez cette commande pour générer un certificat CSR : **CiscocertUtil /generateCSR**



Fournir les informations demandées, par exemple :

Nom du pays : États-Unis

Nom de l'État ou de la province : MA

Nom de la localité : BXB

Nom de l'organisation : Cisco

Unité organisationnelle : CX

Nom commun : PCCEAllin1.cc.lab

E-mail : jdoe@cc.lab

Mot de passe de vérification : Train1ng !

Nom de société facultatif : Cisco

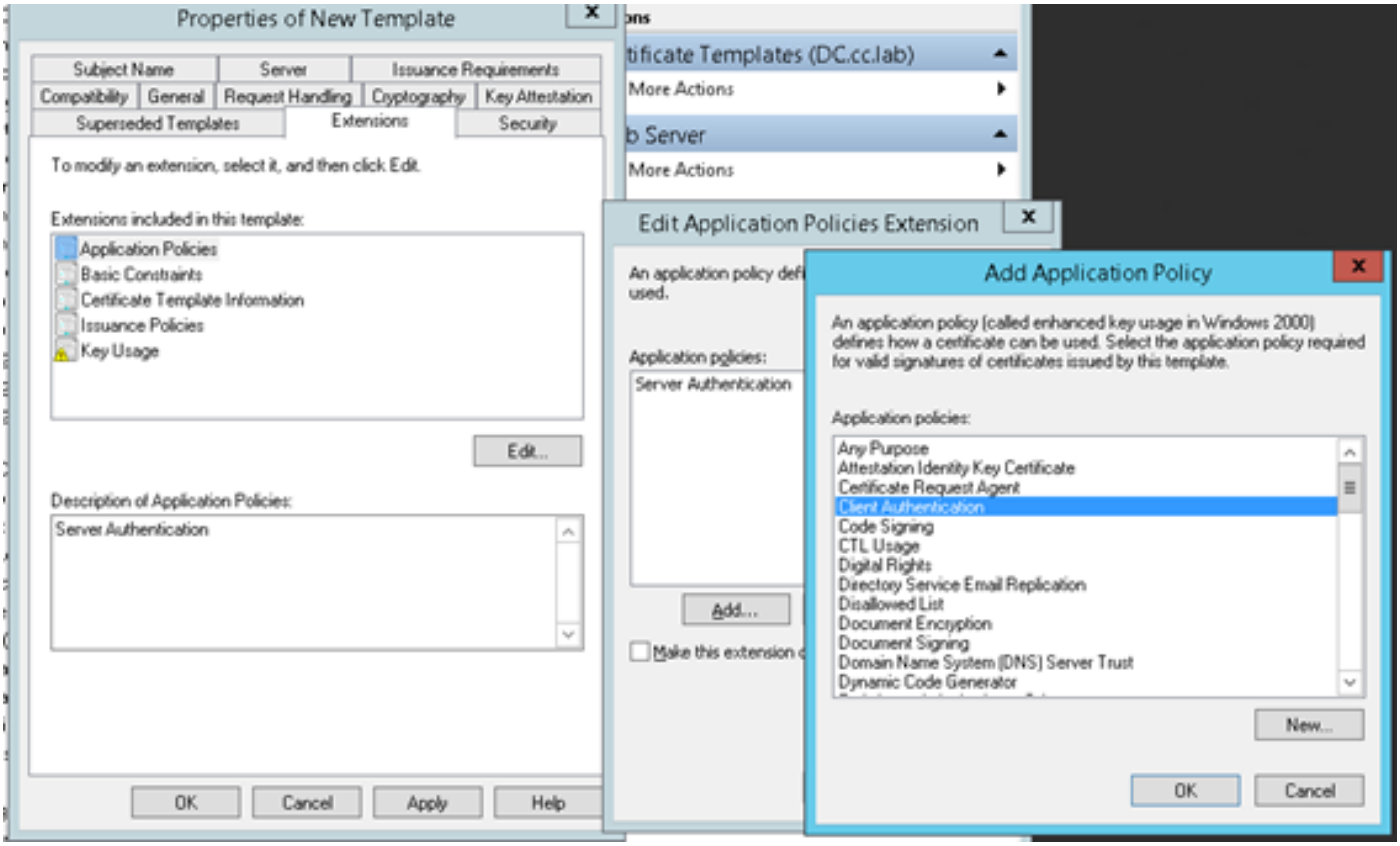
Le certificat et la clé de l'hôte sont stockés dans **C:\icm\ssl\certs** et **C:\icm\ssl\keys**.

Étape 2. Accédez au dossier **C:\icm\ssl\certs** et vérifiez que le fichier **host.csr** a été généré.

Obtenir le certificat CSR Signé par une autorité de certification

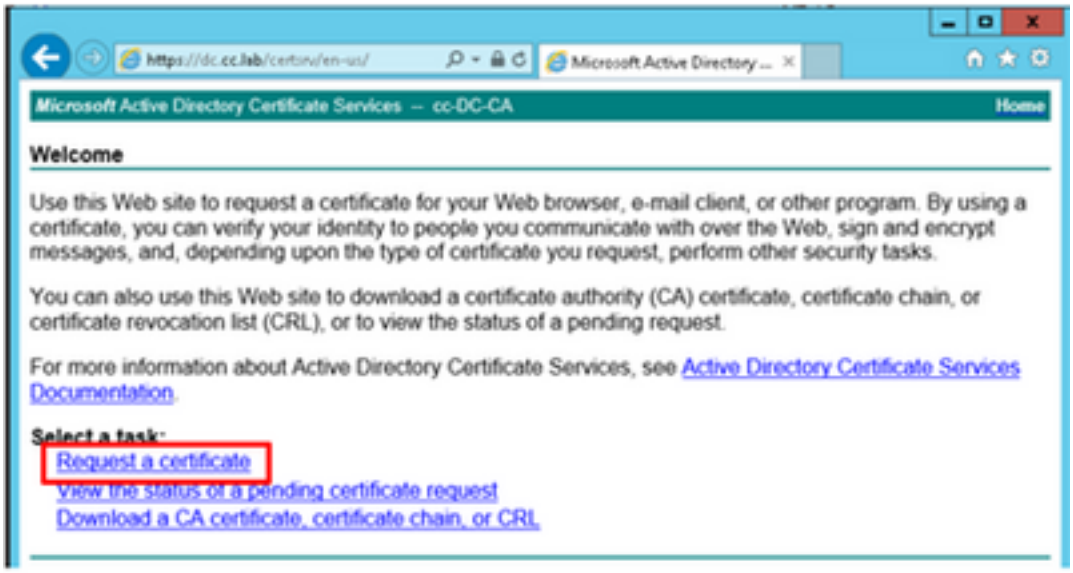
Une fois les certificats CSR générés, ils doivent être signés par une autorité de certification tierce. Dans cet exercice, l'autorité de certification Microsoft installée dans le contrôleur de domaine est utilisée comme autorité de certification tierce.

Assurez-vous que le modèle de certificat utilisé par l'autorité de certification inclut l'authentification du client et du serveur, comme indiqué dans l'image lorsque l'autorité de certification Microsoft est utilisée.

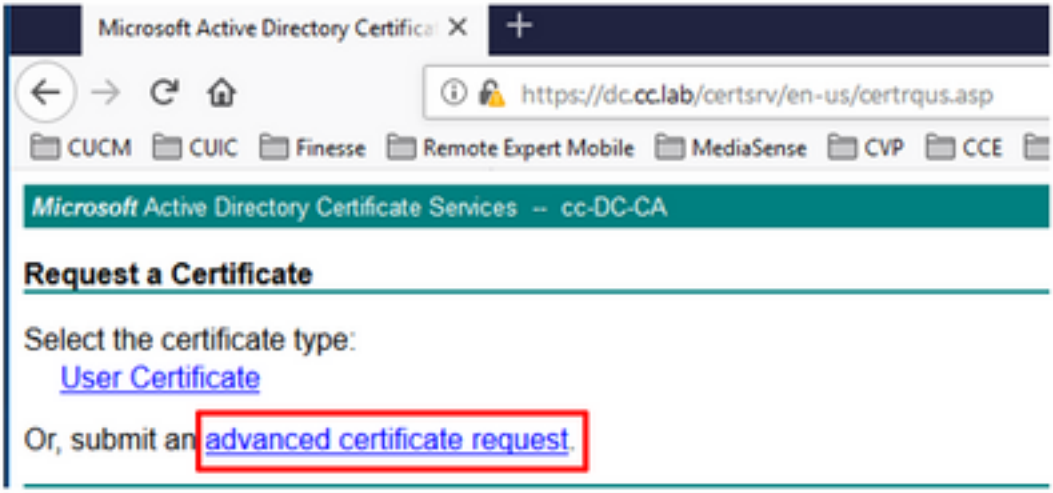


Étape 1. Ouvrez un navigateur Web et accédez à l'autorité de certification.

Étape 2. Dans les **services de certificats Microsoft Active Directory**, sélectionnez **Demander un certificat**.

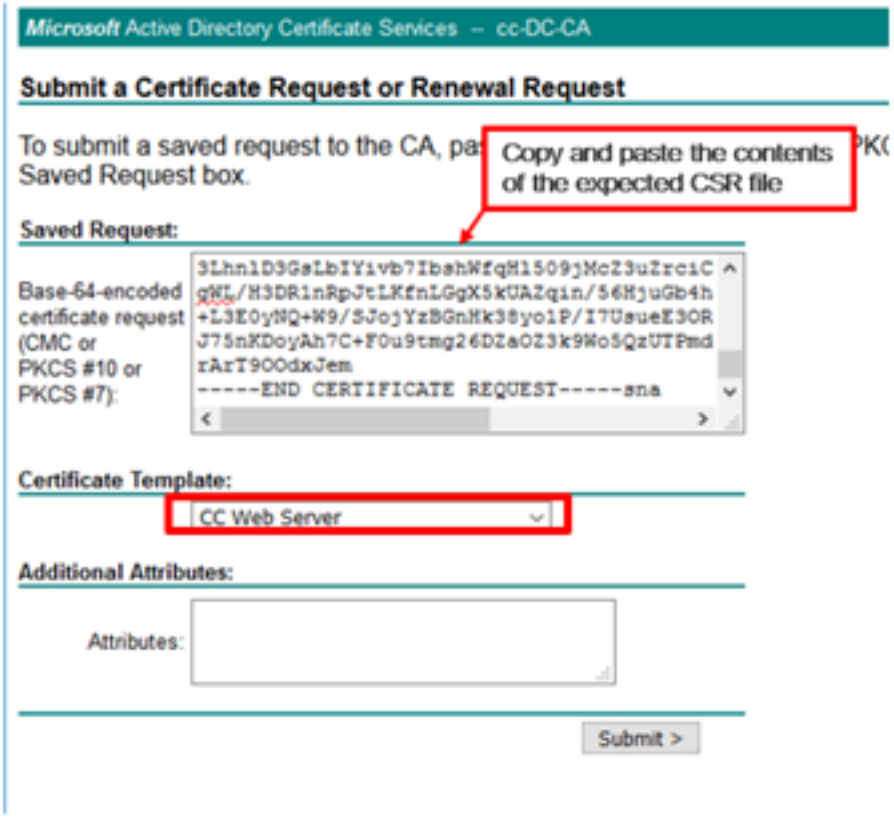


Étape 3. Sélectionnez l'option de **demande de certificat avancée**.



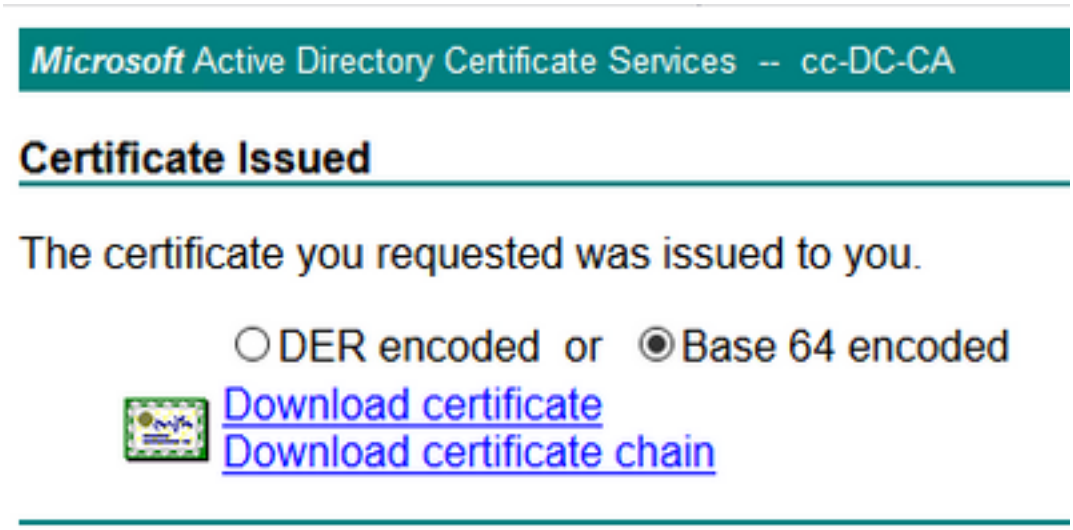
Étape 4. Sur la **demande de certificat avancée,** copiez et collez le contenu du certificat CSR de l'agent PG dans la zone **Requête enregistrée**.

Étape 5. Sélectionnez le modèle **Web Server** avec authentification client et serveur. Au cours des travaux pratiques, le modèle serveur Web CC a été créé avec l'authentification du client et du serveur.



Étape 6. Cliquez sur **Soumettre**.

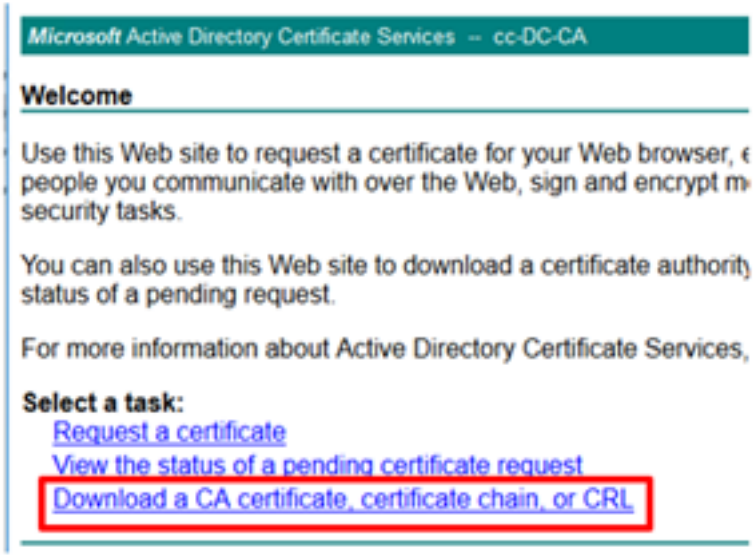
Étape 7. Sélectionnez **Base 64 encodé** et cliquez sur **Télécharger le certificat** comme indiqué dans l'image.



Étape 8. Enregistrez le fichier et cliquez sur **OK**. Le fichier est enregistré dans le dossier **Téléchargements**.

Étape 9. Renommez le fichier en **host.cer** (facultatif).

Étape 10. Vous devez également générer un certificat racine. Retournez à la page de certificat de l'autorité de certification, puis sélectionnez **Télécharger un certificat de l'autorité de certification, une chaîne de certificats ou une liste de révocation de certificats**. Vous n'avez qu'à effectuer cette étape une fois, puisque le certificat racine sera le même pour tous les serveurs (Agent PG et Finesse).



Étape 11. Cliquez sur **Base 64** et sélectionnez **Télécharger le certificat CA**.

Étape 12. Cliquez sur Enregistrer le fichier et sélectionnez **OK**. Le fichier sera enregistré à l'emplacement par défaut, **Téléchargements**.

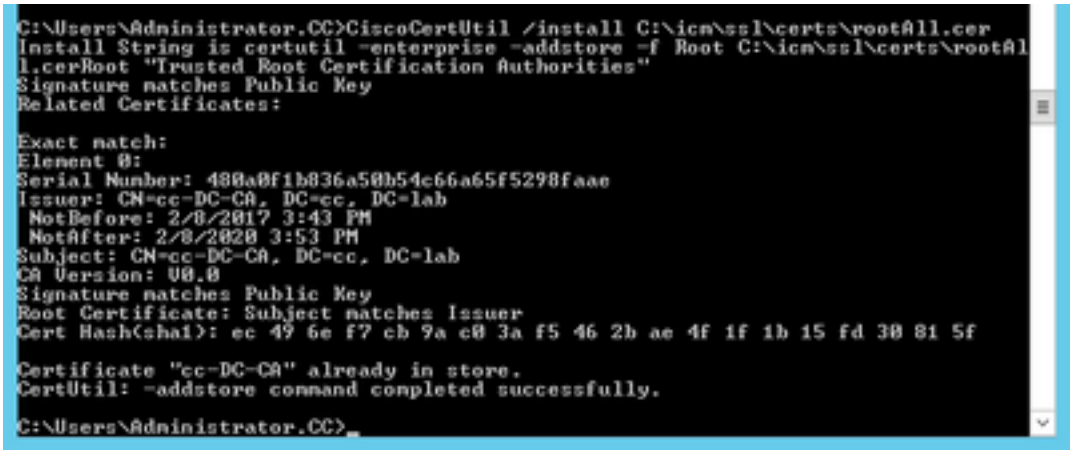
Importer les certificats signés CCE PGs CA

Étape 1. Sur l'agent PG, accédez à **C:\icm\ssl\certs** et collez les fichiers racine et l'agent PG signés ici.

Étape 2. Renommez le certificat host.pem sur **c:\icm\ssl\certs** en tant que **selfhost.pem**.

Étape 3. Renommez host.cer en host.pem sur le dossier **c:\icm\ssl\certs** .

Étape 4. Installez le certificat racine. À l'invite de commandes, exécutez cette commande : **CiscoCertUtil /install C:\icm\ssl\certs\rootAll.cer**



Étape 5. Installez le certificat signé de l'application exécutant la même commande : **CiscoCertUtil /install C:\icm\ssl\certs\host.pem**

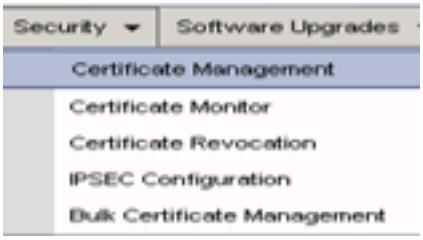
```
C:\Users\Administrator.CC>CiscoCertUtil /install C:\icm\ssl\certs\host.pem
Install String is certutil -enterprise -addstore -f Root C:\icm\ssl\certs\host.p
emRoot "Trusted Root Certification Authorities"
Certificate "PCCALLin1.cc.lab" added to store.
CertUtil: -addstore command completed successfully.

C:\Users\Administrator.CC>_
```

Étape 6. Cycle de la PG. Ouvrez Unified CCE Service Control, puis passez en revue la PG Cisco ICM Agent.

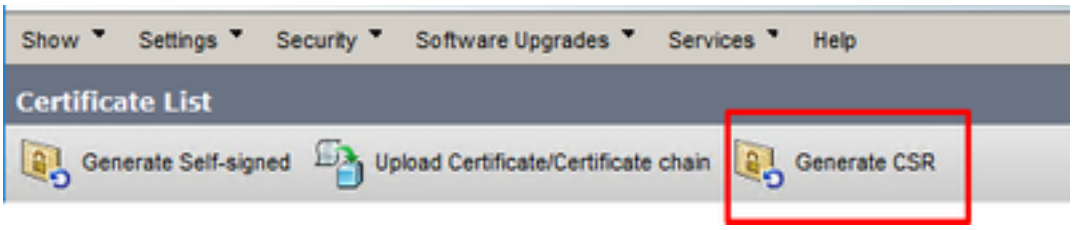
Générer un certificat Finesse

Étape 1. Ouvrez le navigateur Web et accédez à **Finesse OS Admin**.

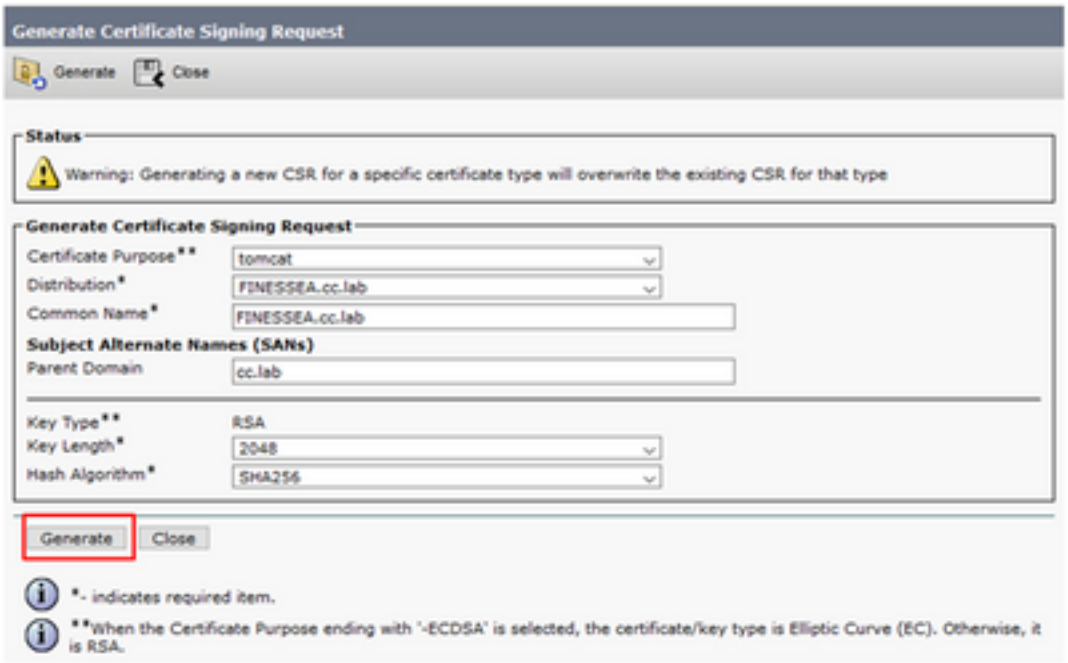
Étape 2. Connectez-vous avec les informations d'identification de l'administrateur du système d'exploitation et accédez à **Security > Certificate Management** comme indiqué dans l'image.



Étape 3. Cliquez sur **Generate CSR** comme indiqué dans l'image.

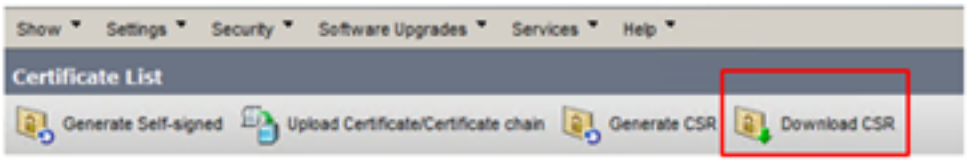


Étape 4. Dans la **demande de signature de certificat**, utilisez les valeurs par défaut, puis cliquez sur **Générer.**

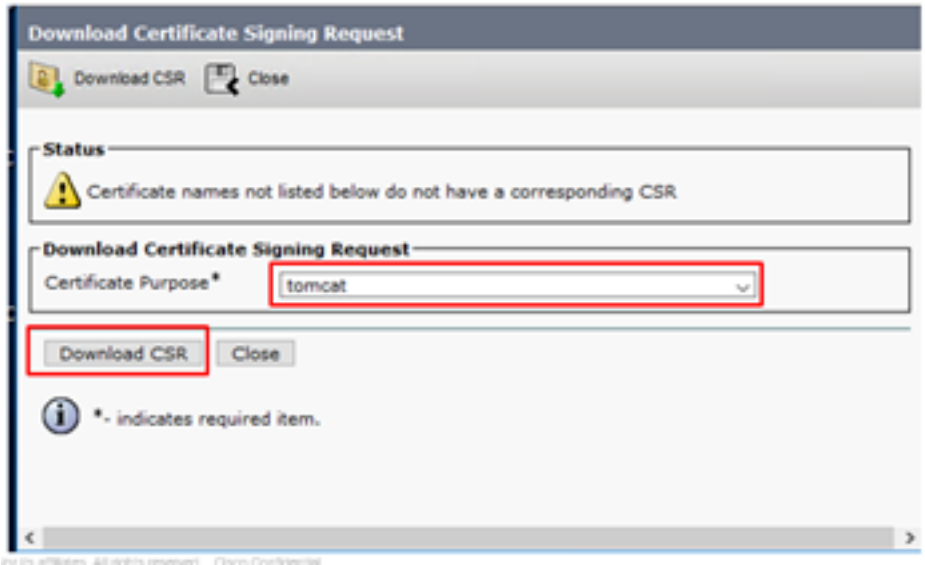


Étape 5. Fermez la fenêtre **Générer une demande de signature de certificat** et sélectionnez

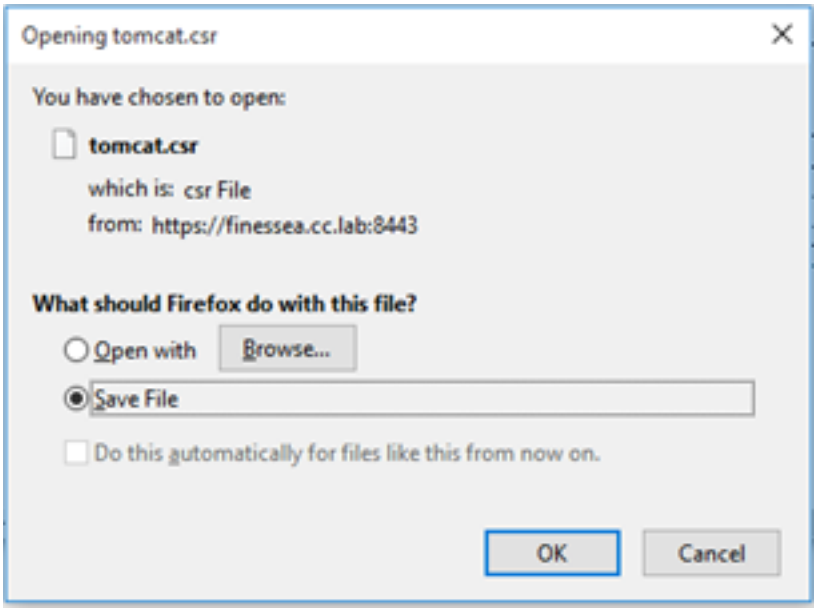
Télécharger CSR.



Étape 6. Dans l'objet du certificat, sélectionnez **tomcat** et cliquez sur **Télécharger CSR**.



Étape 7. Sélectionnez **Enregistrer le fichier** et cliquez sur **OK** comme indiqué dans l'image.



Étape 8. Fermez la fenêtre **Télécharger la demande de signature de certificat**. Le certificat est enregistré à l'emplacement par défaut **(Cet ordinateur > Téléchargements)**.

Étape 9. Ouvrez l'Explorateur Windows et accédez à ce dossier. Cliquez avec le bouton droit sur ce certificat et renommez-le : **finessetomcat.csr**

Signer le certificat Finesse par une autorité de certification

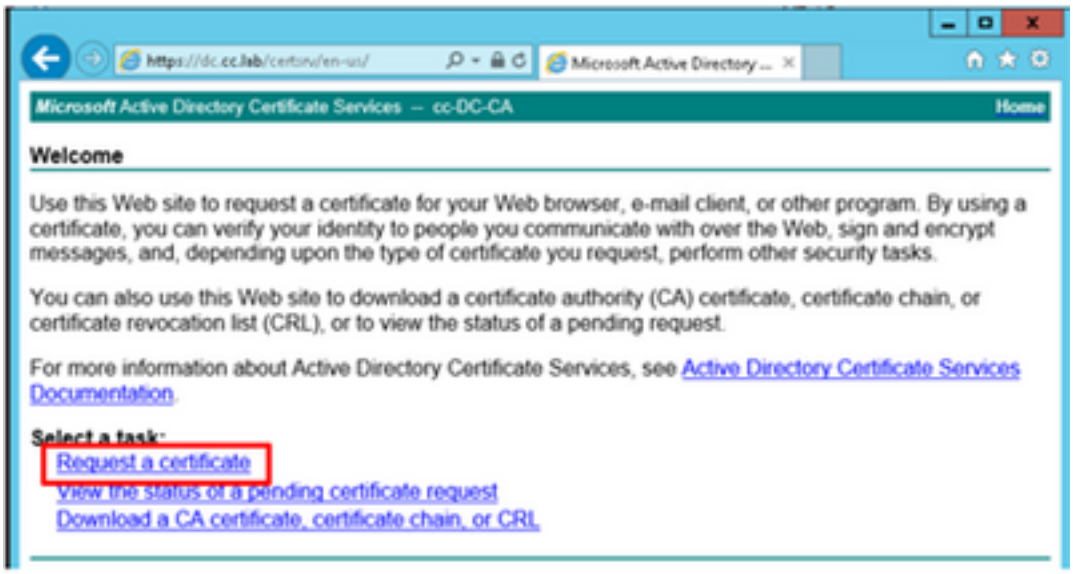
Dans cette section, la même autorité de certification Microsoft utilisée à l'étape précédente est

utilisée comme autorité de certification tierce.

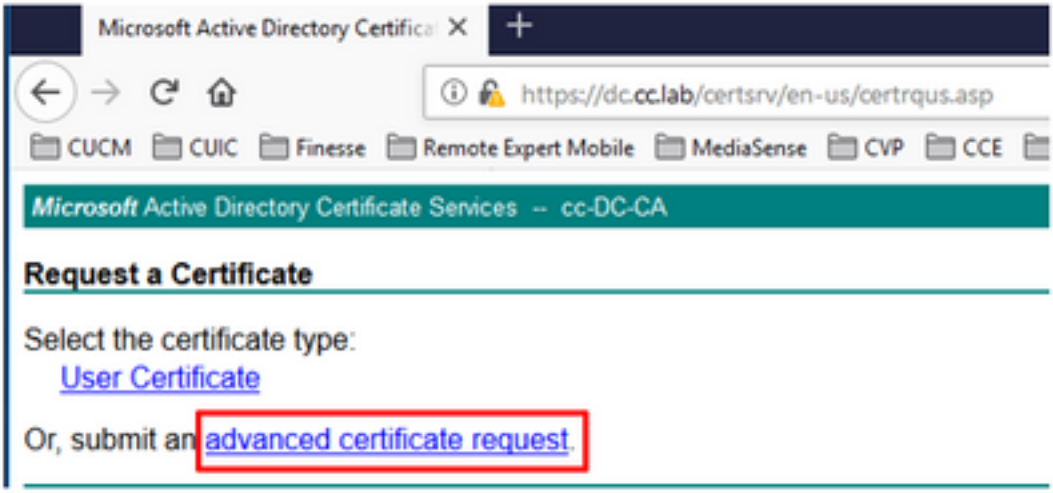
> **Remarque** : assurez-vous que le modèle de certificat utilisé par l'autorité de certification inclut l'authentification du client et du serveur.

Étape 1. Ouvrez un navigateur Web et accédez à l'autorité de certification.

Étape 2. Dans les **services de certificats Microsoft Active Directory**, sélectionnez **Demander un certificat**.

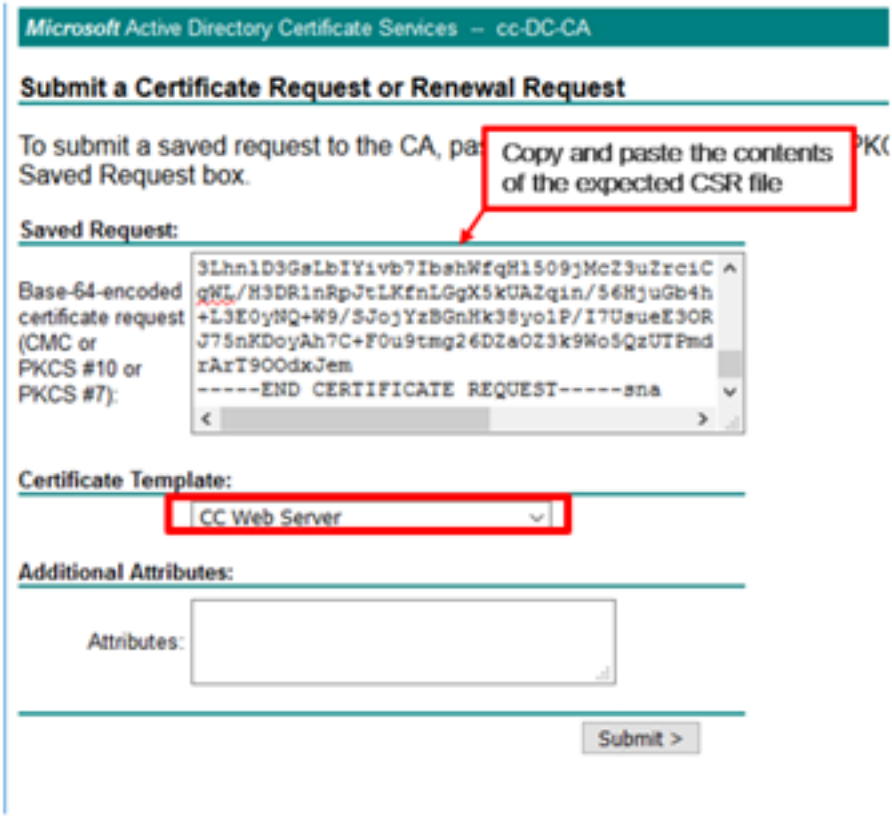


Étape 3. Sélectionnez l'option de **demande de certificat avancée** comme indiqué dans l'image.



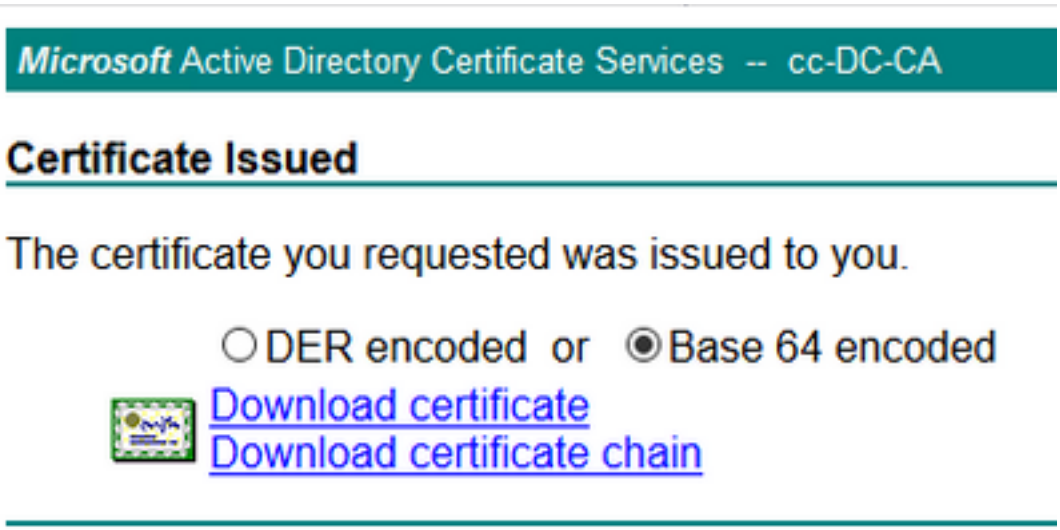
Étape 4. Sur la **demande de certificat avancée,** copiez et collez le contenu du certificat CSR Finesse dans la zone **Demande enregistrée**.

Étape 5. Sélectionnez le modèle de serveur Web avec authentification client et serveur. Au cours de ces travaux pratiques, le modèle serveur Web CC a été créé avec l'authentification du client et du serveur.



Étape 6. Cliquez sur **Soumettre**.

Étape 7. Sélectionnez **Base 64 encodé** et cliquez sur **Télécharger le certificat** comme indiqué dans l'image.



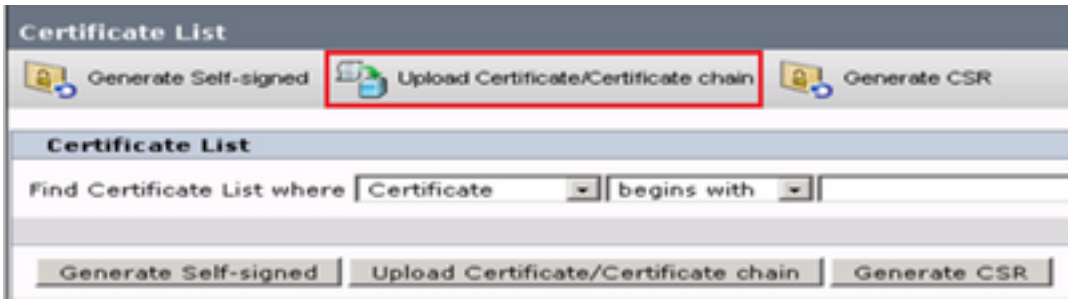
Étape 8. Enregistrez le fichier et cliquez sur **OK**. Le fichier est enregistré dans le dossier **Téléchargements**.

Étape 9. Renommez le fichier en **finesse.cer**.

Importer les certificats signés de l'application Finesse et de la racine

Étape 1. Sur un navigateur Web, ouvrez la page **Finesse OS Admin** et accédez à **Security > Certificate Management**.

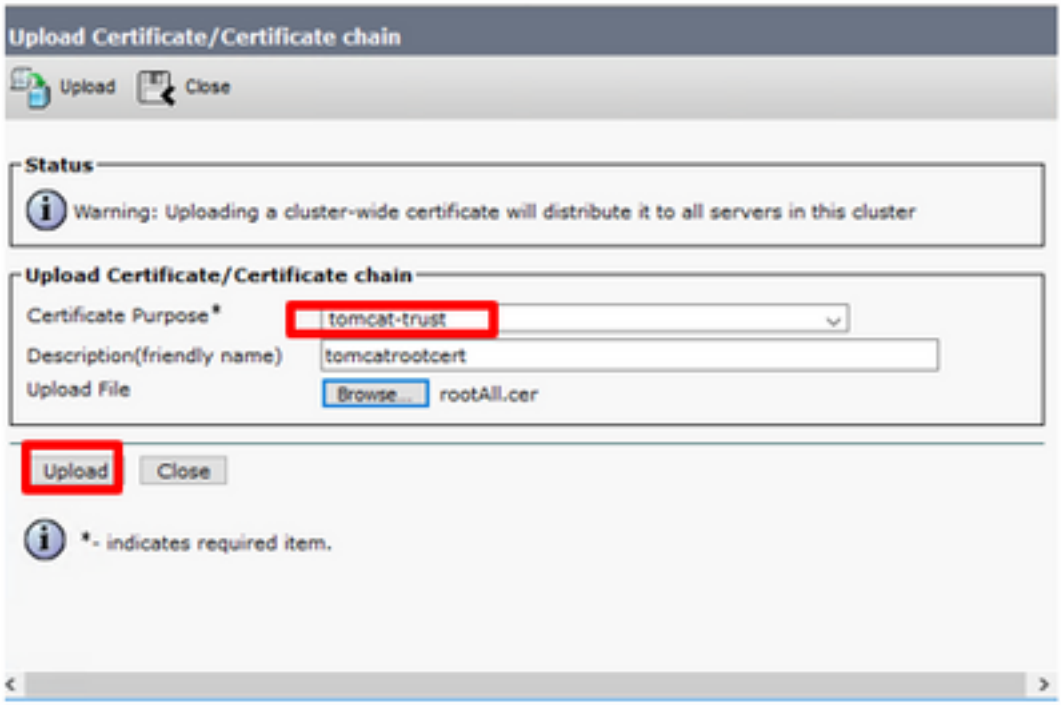
Étape 2. Cliquez sur le bouton **Upload Certificate/Certificate chain** comme indiqué dans l'image.



Étape 3. Dans la fenêtre contextuelle, sélectionnez **tomcat-trust** pour **l'objet du certificat**.

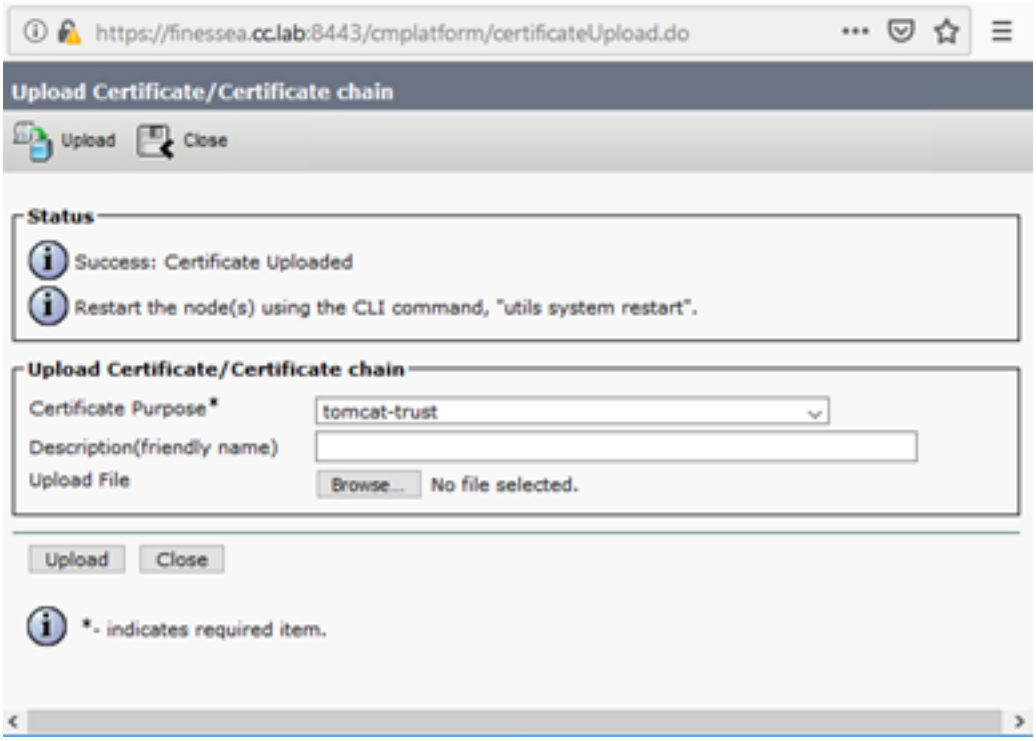
Étape 4. Cliquez sur le bouton **Parcourir...** et sélectionnez le fichier de certificat racine à importer. Cliquez ensuite sur le bouton **Ouvrir**.

Étape 5. Dans la description, écrivez quelque chose comme **tomcatrootcert** et cliquez sur **Upload** button comme indiqué dans l'image.

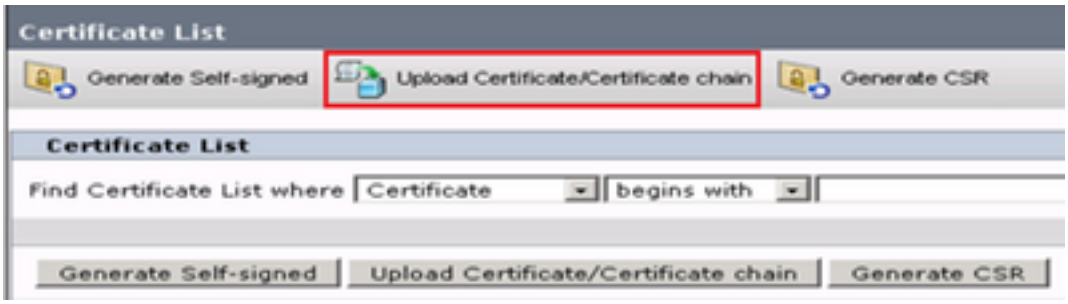


Étape 6. Attendez de voir la **réussite :** Message **téléchargé du certificat** pour fermer la fenêtre.

Vous serez invité à redémarrer le système, mais commencez par télécharger le certificat signé de l'application Finesse, puis vous pourrez redémarrer le système.



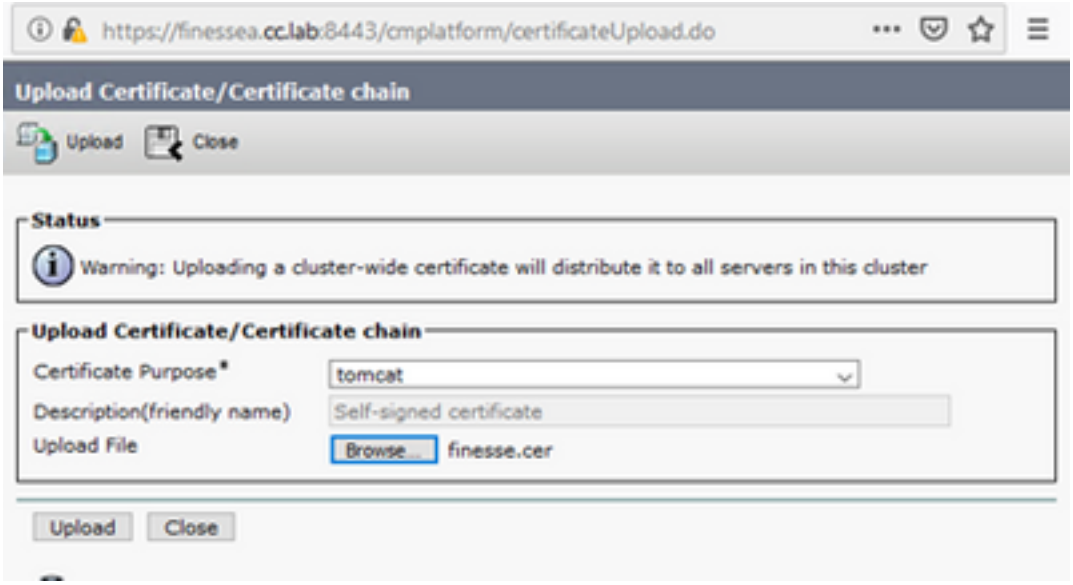
Étape 7. Cliquez sur le bouton **Télécharger le certificat/la chaîne de certificats** pour importer le certificat d'application Finesse.



Étape 8. Dans la fenêtre contextuelle, sélectionnez **tomcat** pour **l'objet du certificat**.

Étape 9. Cliquez sur le bouton **Parcourir...** et sélectionnez le fichier signé de l'Autorité de certification Finesse, **finesse.cer**. Cliquez ensuite sur le bouton **Ouvrir**.

Étape 10. Cliquez sur le bouton **Télécharger**.



Étape 11. Attendez de voir la **réussite :** Message **téléchargé du certificat**.

Encore une fois, vous êtes invité à redémarrer le système. Fermez la fenêtre et continuez à redémarrer le système.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.