# Implémenter des certificats signés CA dans une solution CCE

## Table des matières


Introduction

Conditions préalables

- Exigences
- Composants utilisés

Fond

Procédure

- Serveurs Windows CCE
  - 1. Générer une RSE
  - 2. Obtenir les certificats signés par l'autorité de certification
  - 3. Télécharger les certificats signés par l'autorité de certification
  - 4. Lier le certificat CA-Signed à IIS
  - 5. Lier le certificat CA-Signed au portail de diagnostic
  - 6. Importez le certificat racine et le certificat intermédiaire dans le magasin de clés Java
- Solution CVP
  - 1. Générer des certificats avec FQDN
  - 2. Générer la CSR
  - 3. Obtenir les certificats signés par l'autorité de certification
  - 4. Importer les certificats signés par l'autorité de certification
- Serveurs VOS
  - 1. Générer un certificat CSR
  - 2. Obtenir les certificats signés par l'autorité de certification
  - 3. Télécharger l'application et les certificats racine

Vérifier

Dépannage

InformationsAssociées


## Introduction

Ce document décrit comment implémenter des certificats signés par une autorité de certification (CA) dans la solution Cisco Contact Center Enterprise (CCE).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Unified Contact Center Enterprise (UCCE) version 12.5(1)

- Package Contact Center Enterprise version 12.5(1)
- Customer Voice Portal (CVP) version 12.5 (1)
- Navigateur vocal virtualisé Cisco (VVB)
- Cisco CVP Operations and Administration Console (OAMP)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Unified Communication Manager (CUCM)

### Composants utilisés

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

- PCCE 12.5(1)
- CVP 12.5(1)
- Cisco VVB 12.5
- Finesse 12,5
- CUIC 12,5
- Windows 2016

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.

## Fond

Les certificats sont utilisés pour garantir que la communication est sécurisée avec l'authentification entre les clients et les serveurs. Les utilisateurs peuvent acheter des certificats auprès d'une autorité de certification ou utiliser des certificats auto-signés.

Les certificats auto-signés (comme leur nom l'indique) sont signés par la même entité dont ils certifient l'identité, au lieu d'être signés par une autorité de certification. Les certificats auto-signés ne sont pas considérés comme aussi sécurisés que les certificats d'autorité de certification, mais ils sont utilisés par défaut dans de nombreuses applications.

Dans la version 12.x de la solution Package Contact Center Enterprise (PCCE), tous les composants de la solution sont contrôlés par le panneau de verre unique (SPOG), qui est hébergé sur le serveur principal Admin Workstation (AW).

En raison de la conformité SRC (Security Management Compliance) dans la version PCCE 12.5(1), toutes les communications entre SPOG et les autres composants de la solution sont effectuées via le protocole HTTP sécurisé. Dans UCCE 12.5, la communication entre les composants s'effectue également via le protocole HTTP sécurisé.

Ce document explique en détail les étapes nécessaires à la mise en oeuvre des certificats signés CA dans une solution CCE pour une communication HTTP sécurisée. Pour toute autre considération relative à la sécurité UCCE, reportez-vous aux Directives de sécurité UCCE. Pour toute communication sécurisée CVP supplémentaire différente du protocole HTTP sécurisé,

reportez-vous aux consignes de sécurité du guide de configuration CVP : Directives de sécurité CVP.

# Procédure

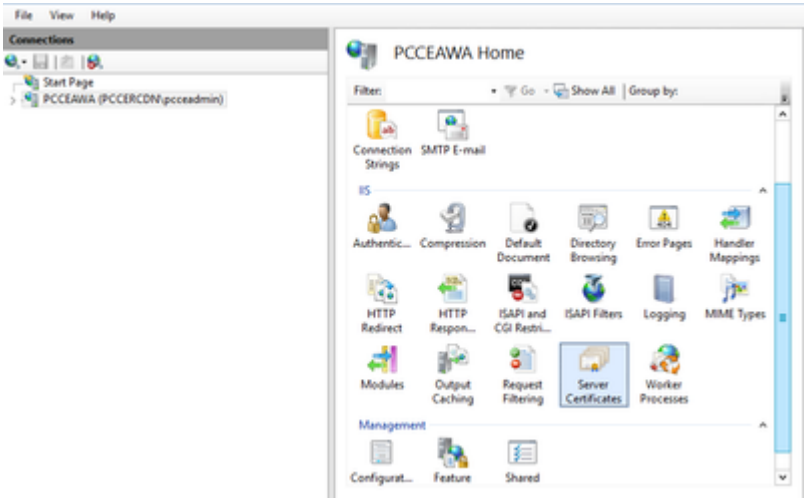
## Serveurs Windows CCE

1. Générer une RSE

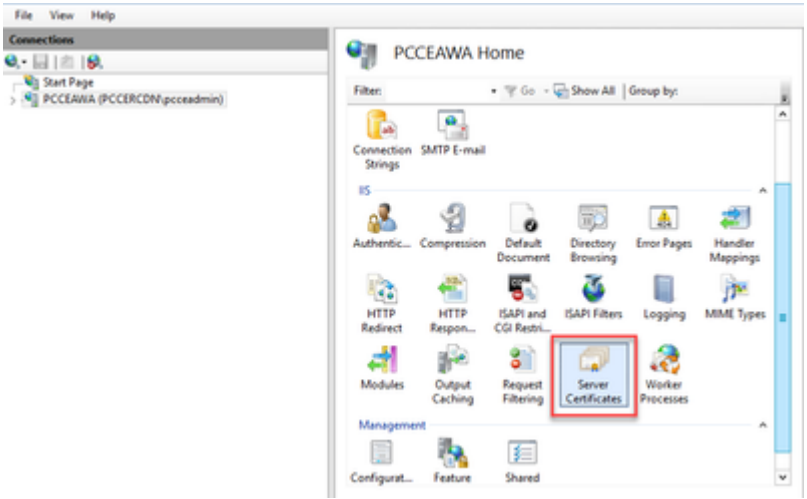
Cette procédure explique comment générer une demande de signature de certificat (CSR) à partir du Gestionnaire des services Internet (IIS).

Étape 1. Connectez-vous à Windows et choisissez Panneau de configuration > Outils d'administration > Gestionnaire des services Internet (IIS).

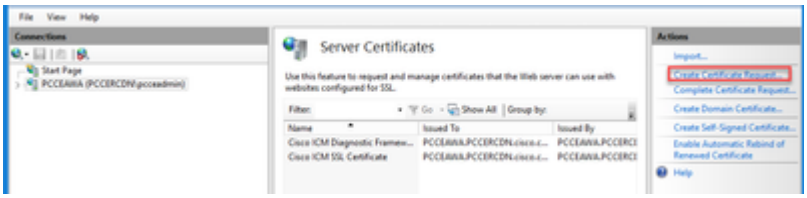
Étape 2. Dans le volet Connexions, cliquez sur le nom du serveur. Le volet Accueil du serveur apparaît.




Étape 3. Dans la zone IIS, double-cliquez sur Server Certificates.

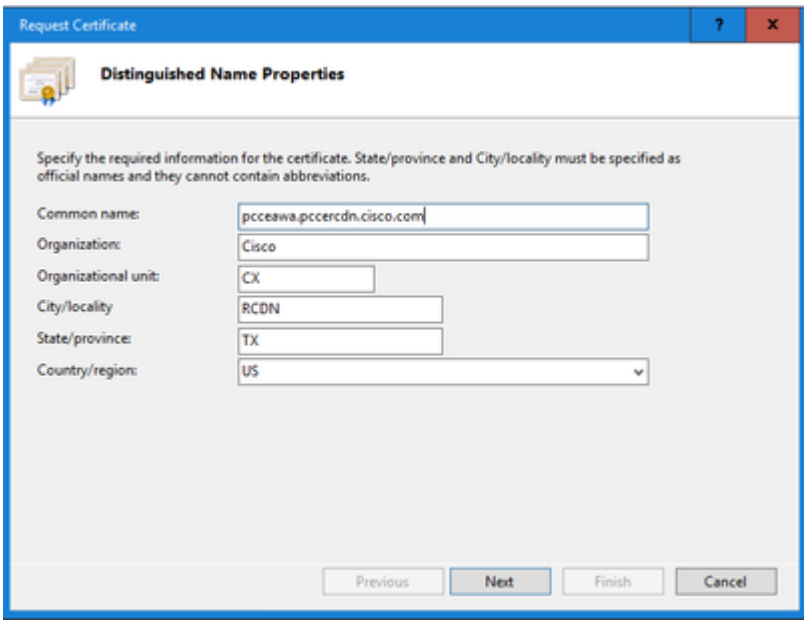



Étape 4. Dans le volet Actions, cliquez sur Créer une demande de certificat.



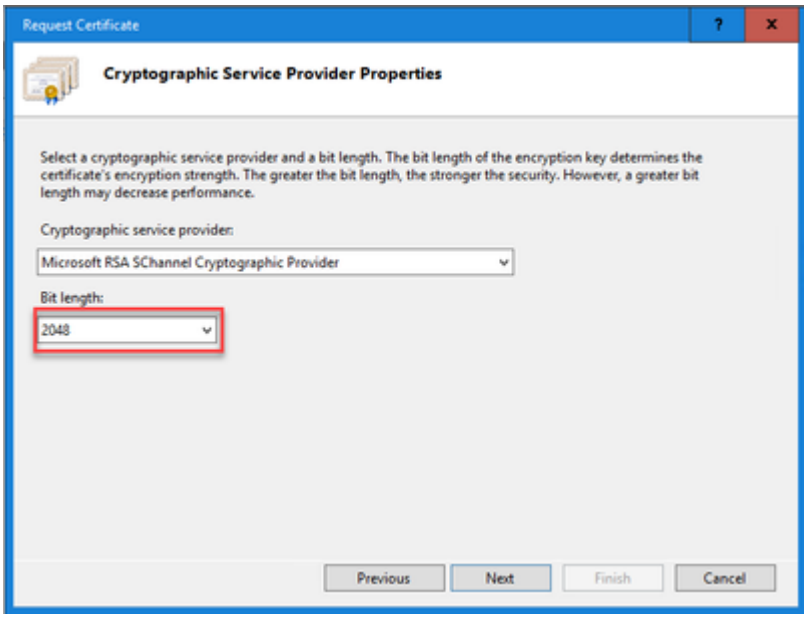

Étape 5. Dans la boîte de dialogue Demander un certificat, procédez comme suit :

a. Spécifiez les informations requises dans les champs affichés et cliquez sur Next.

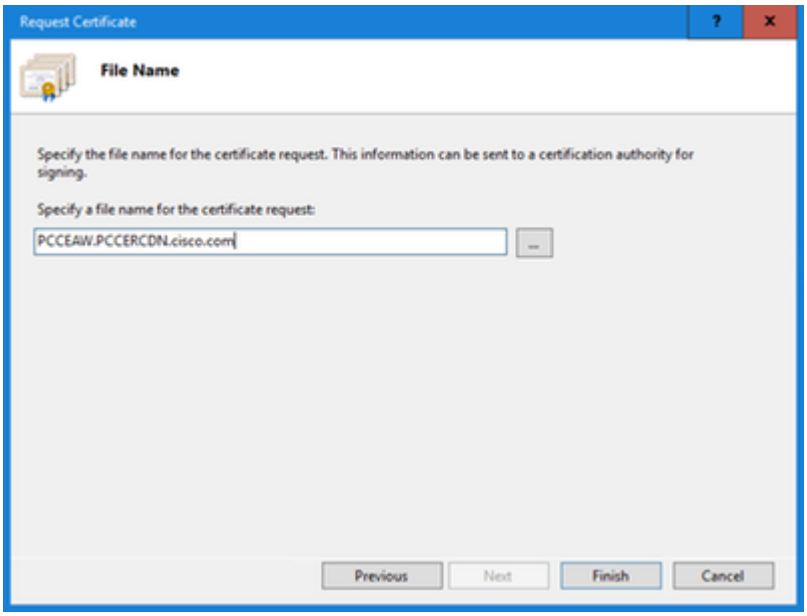



b. Dans la liste déroulante Fournisseur de services de chiffrement, conservez le paramètre par défaut.

c. Dans la liste déroulante Bit length, sélectionnez 2048.




Étape 6. Spécifiez un nom de fichier pour la demande de certificat et cliquez sur Finish.




2. Obtenir les certificats signés par l'autorité de certification

Étape 1 : signature du certificat sur une autorité de certification

---

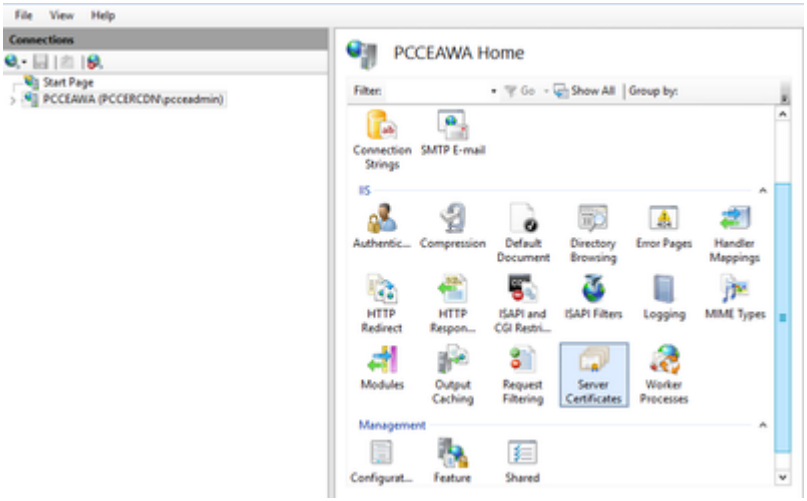
Remarque : Assurez-vous que le modèle de certificat utilisé par l'autorité de certification inclut l'authentification client et serveur.

---

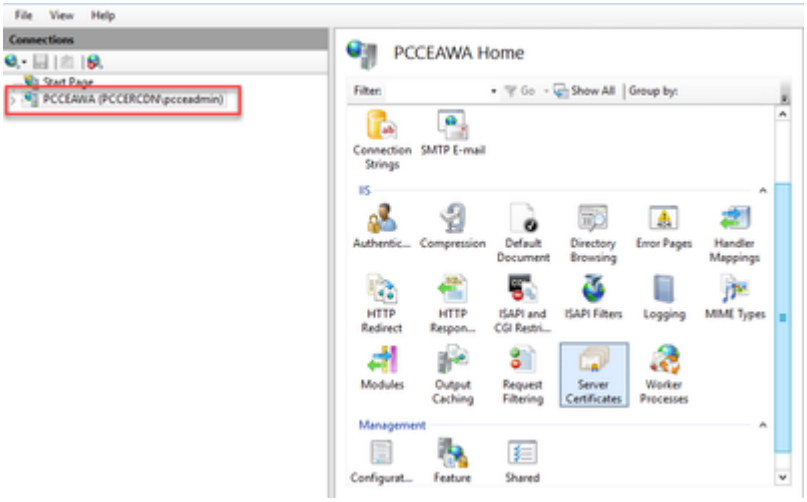
Étape 2. Obtenez les certificats CA signés auprès de votre autorité de certification (racine, application et intermédiaire, le cas échéant).

3. Télécharger les certificats signés par l'autorité de certification

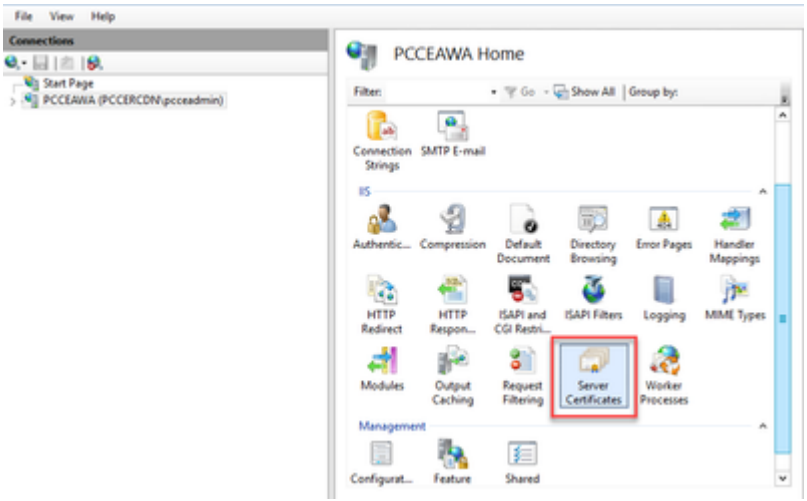
Étape 1. Connectez-vous à Windows et choisissez Panneau de configuration > Outils d'administration > Gestionnaire des services Internet (IIS).



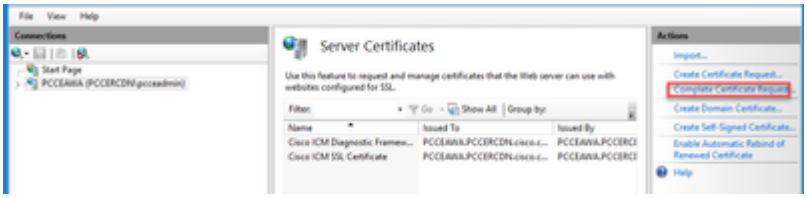

Étape 2. Dans le volet Connexions, cliquez sur le nom du serveur.




Étape 3. Dans la zone IIS, double-cliquez sur Server Certificates.




Étape 4. Dans le volet Actions, cliquez sur Terminer la demande de certificat.




Étape 5. Dans la boîte de dialogue Terminer la demande de certificat, renseignez les champs suivants :

a. Dans le champ Nom de fichier qui contient la réponse de l'autorité de certification, cliquez sur le bouton de sélection ( ... ).

b. Accédez à l'emplacement où le certificat d'application signé est stocké, puis cliquez sur Ouvrir.

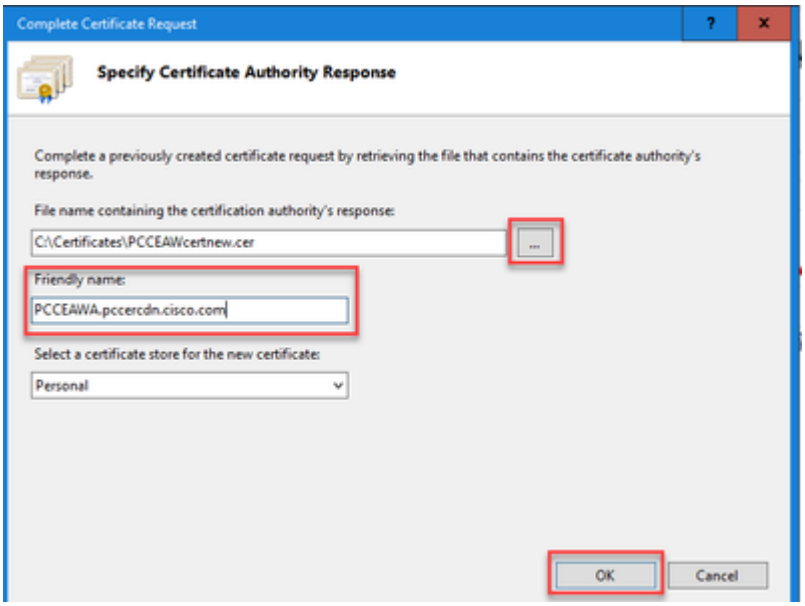
---

Remarque : S'il s'agit d'une implémentation d'autorité de certification de niveau 2 et que le certificat racine ne se trouve pas déjà dans le magasin de certificats du serveur, le certificat racine doit être téléchargé dans le magasin Windows avant d'importer le certificat signé. Reportez-vous à ce document si vous devez télécharger l'autorité de certification racine vers

---

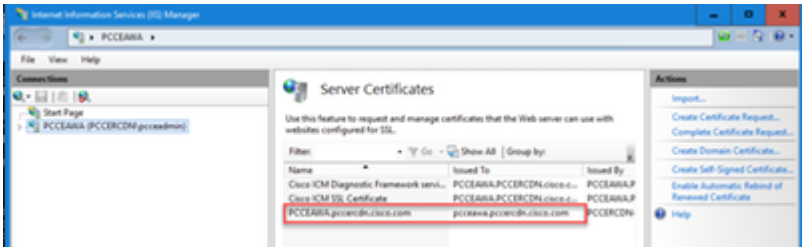
le Windows Store https://learn.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate.

c. Dans le champ Nom convivial, saisissez le nom de domaine complet (FQDN) du serveur ou tout nom significatif pour vous. Assurez-vous que la liste déroulante Sélectionner un magasin de certificats pour le nouveau certificat reste Personnel.




Étape 6. Cliquez sur OK pour télécharger le certificat.

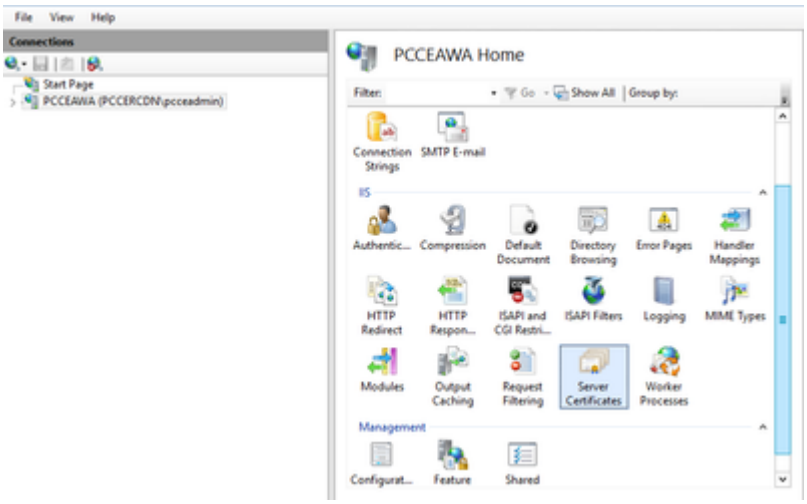
Si le téléchargement du certificat a réussi, le certificat apparaît dans le volet Certificats du serveur.



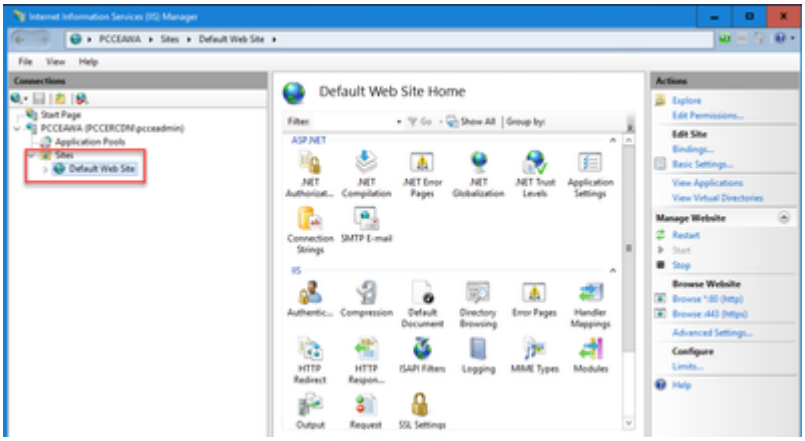

4. Lier le certificat CA-Signed à IIS

Cette procédure explique comment lier un certificat CA signé dans le Gestionnaire des services Internet.

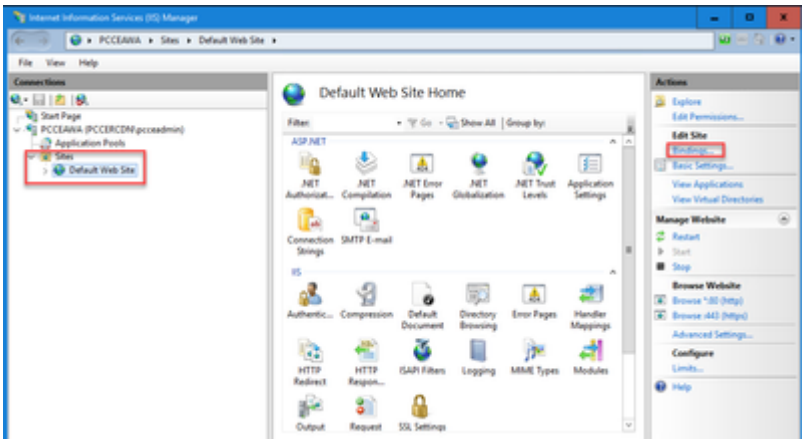
Étape 1. Connectez-vous à Windows et choisissez Panneau de configuration > Outils d'administration > Gestionnaire des services Internet (IIS).



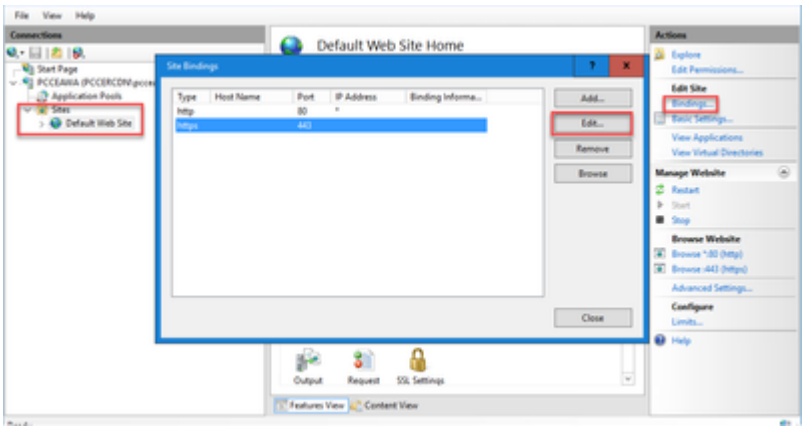

Étape 2. Dans le volet Connexions, choisissez <nom_serveur> > Sites > Site Web par défaut.



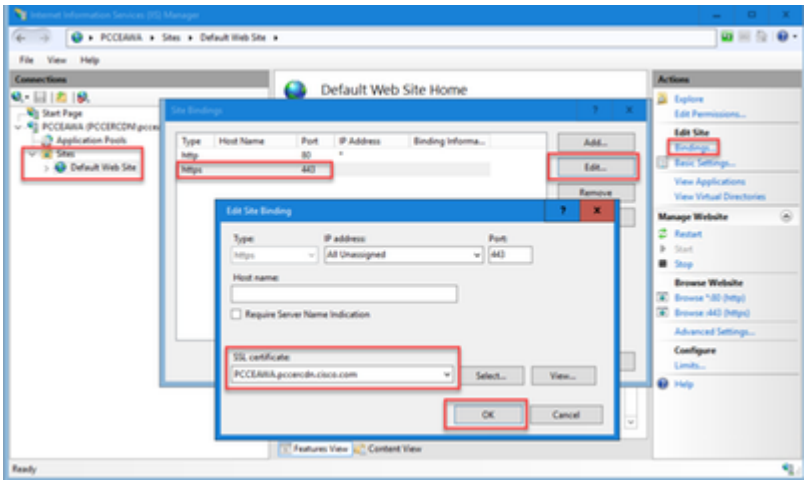

Étape 3. Dans le volet Actions, cliquez sur Liaisons....




Étape 4. Cliquez sur le type https avec le port 443, puis cliquez sur Edit....

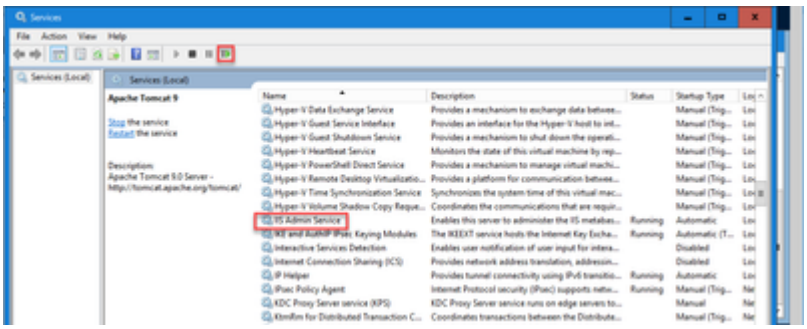



Étape 5. Dans la liste déroulante SSL certificate, sélectionnez le certificat portant le même nom convivial que celui indiqué à l'étape précédente.




Étape 6. Cliquez sur OK.

Étape 7. Accédez à Démarrer > Exécuter > services.msc et redémarrez le service d'administration IIS.



Si IIS est redémarré avec succès, les avertissements d'erreur de certificat n'apparaissent pas lors du lancement de l'application.

5. Lier le certificat CA-Signed au portail de diagnostic

Cette procédure explique comment lier un certificat signé par une autorité de certification dans le portail de diagnostic.

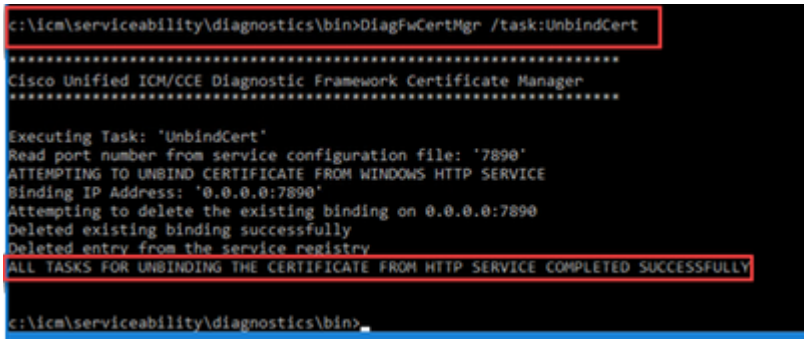
Étape 1. Ouvrez l'invite de commandes (Exécuter en tant qu'administrateur).

Étape 2. Accédez au dossier d'accueil de Diagnostic Portico. Exécutez cette commande :

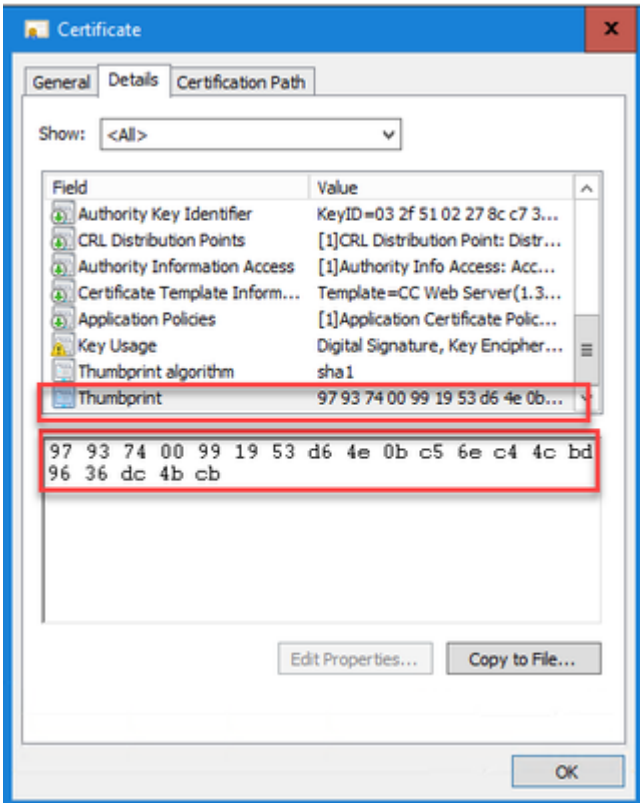
```
cd c:\icm\serviceability\diagnostics\bin
```

Étape 3 : suppression de la liaison de certificat actuelle au portlet de diagnostic Exécutez cette commande :

```
DiagFwCertMgr /task:UnbindCert
```

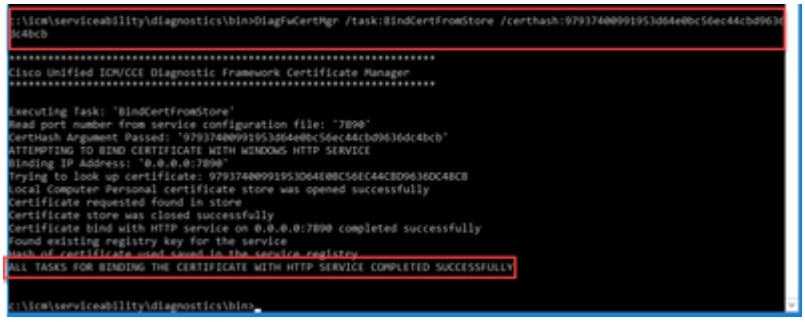



Étape 4. Ouvrez le certificat signé et copiez le contenu de hachage (sans espaces) du champ Empreinte numérique.



Étape 5. Exécutez cette commande et collez le contenu de hachage.

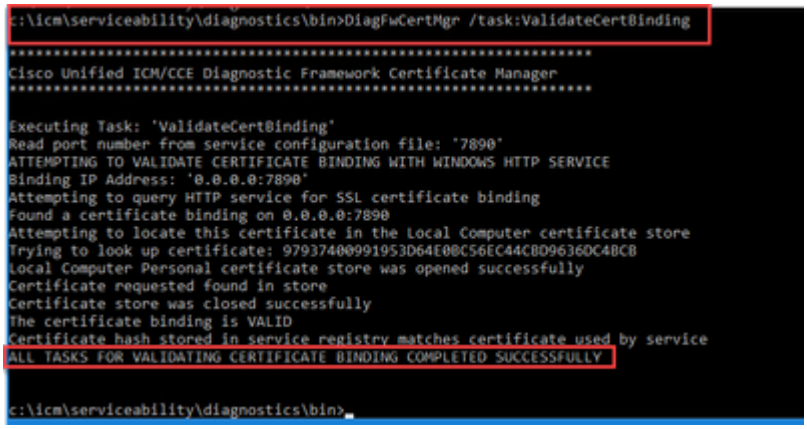
```
DiagFwCertMgr /task:BindCertFromStore /certhash:<hash_value>
```




Si la liaison de certificat a réussi, le message La liaison de certificat est VALIDE s'affiche.

Étape 6 : validation de la liaison du certificat Exécutez cette commande :

```
DiagFwCertMgr /task:ValidateCertBinding
```




---

Remarque : DiagFwCertMgr utilise le port 7890 par défaut.

---

Si la liaison de certificat a réussi, le message La liaison de certificat est VALIDE s'affiche.

Étape 7. Redémarrez le service Diagnostic Framework. Exécutez ces commandes :

```
net stop DiagFwSvc
net start DiagFwSvc
```

Si Diagnostic Framework redémarre avec succès, les avertissements d'erreur de certificat n'apparaissent pas lors du lancement de l'application.

6. Importez le certificat racine et le certificat intermédiaire dans le magasin de clés Java

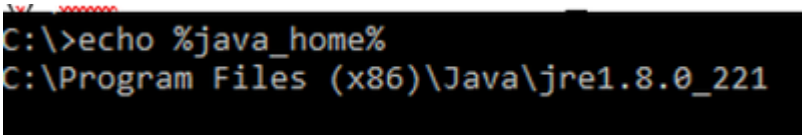
---

⚠ Mise en garde : Avant de commencer, vous devez sauvegarder le keystore et exécuter les commandes à partir du répertoire d'origine java en tant qu'administrateur.

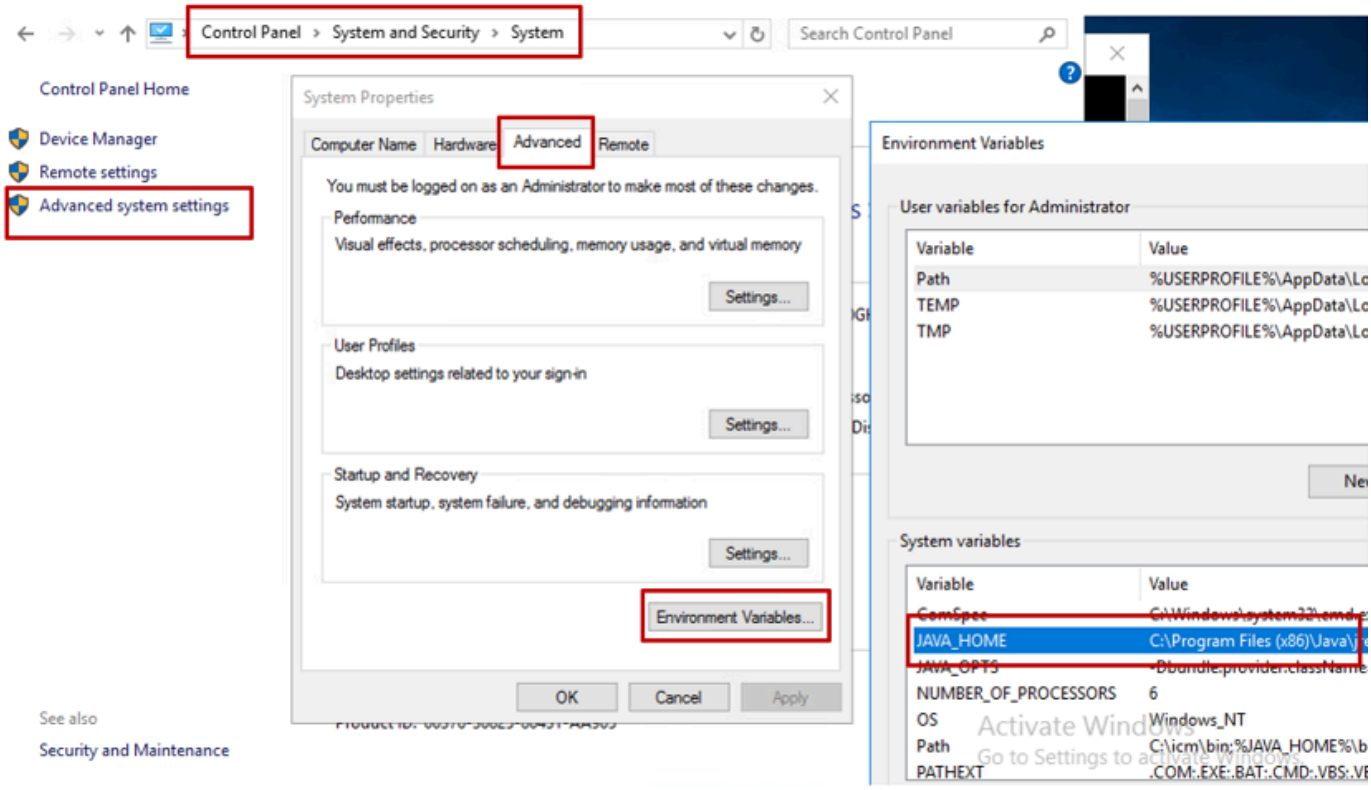
---

Étape 1. Connaître le chemin d'accès au répertoire d'origine Java afin de vous assurer que l'outil clavier Java est hébergé. Il existe plusieurs façons de trouver le chemin d'accès java.

Option 1 : Commande CLI : echo %JAVA_HOME%




Option 2 : Manuellement via les paramètres système avancés, comme indiqué dans l'image




---

✎ Remarque : Sur UCCE 12.5, le chemin d'accès par défaut est C:\Program Files (x86)\Java\jre1.8.0_221\bin. Cependant, si vous avez utilisé le programme d'installation 12.5(1a) ou si vous avez installé 12.5 ES55 (OpenJDK ES obligatoire), utilisez CCE_JAVA_HOME au lieu de JAVA_HOME puisque le chemin du data store a changé avec OpenJDK.

---

Étape 2. Sauvegardez le fichier cacerts à partir du dossier C:\Program Files (x86)\Java\jre1.8.0_221\lib\security. Vous pouvez le copier à un autre emplacement.

Étape 3. Ouvrez une fenêtre de commande en tant qu'Administrateur pour exécuter la commande :

```
keytool.exe -keystore ./cacerts -import -file <path where the Root, or Intermediate certificate are sto
```

Remarque : Les certificats spécifiques requis dépendent de l'autorité de certification que vous utilisez pour signer vos certificats. Dans une autorité de certification à deux niveaux, qui est typique des autorités de certification publiques et plus sécurisée que les autorités de certification internes, vous devez importer à la fois les certificats racine et intermédiaires. Dans une autorité de certification autonome sans intermédiaire, généralement vue dans un laboratoire ou dans une autorité de certification interne plus simple, vous n'avez qu'à importer le certificat racine.

## Solution CVP

1. Générer des certificats avec FQDN

Cette procédure explique comment générer des certificats avec le nom de domaine complet pour les services Web Service Manager (WSM), Voice XML (VXML), Call Server et Operations Management (OAMP).

Remarque : Lorsque vous installez CVP, le nom du certificat inclut uniquement le nom du serveur et non le nom de domaine complet. Vous devez donc régénérer les certificats.

Mise en garde : Avant de commencer, vous devez procéder comme suit :
1. Obtenez le mot de passe du keystore. Exécutez la commande : plus %CVP_HOME%\conf\security.properties. Vous avez besoin de ce mot de passe lorsque vous exécutez les commandes keytool.
2. Copiez le dossier %CVP_HOME%\conf\security dans un autre dossier.
3. Ouvrez une fenêtre de commande en tant qu'Administrateur pour exécuter les commandes.

Serveurs CVP

Étape 1. Pour supprimer les certificats des serveurs CVP, exécutez les commandes suivantes :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

Étape 2. Pour générer le certificat WSM, exécutez cette commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

Remarque : Par défaut, les certificats sont générés pour une durée de deux ans. Utilisez -valid XXXX pour définir la date d'expiration lorsque les certificats sont régénérés, sinon les certificats sont valides pendant 90 jours et doivent être signés par une autorité de certification avant cette date. Pour la plupart de ces certificats, un délai de validation de 3 à 5 ans doit être raisonnable.

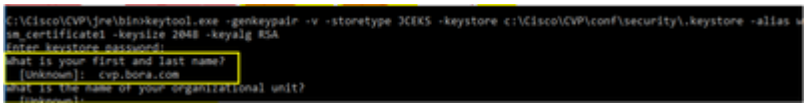
Voici quelques entrées de validité standard :

| | |
|---|---|
| Un an | 365 |
| Deux ans | 730 |
| Trois ans | 1095 |
| Quatre ans | 1460 |
| Cinq ans | 1895 |
| Dix ans | 3650 |

Mise en garde : Dans la version 12.5, les certificats doivent être SHA 256, Key Size 2048 et encryption Algorithm RSA, utilisez ces paramètres pour définir ces valeurs : -keyalg RSA et -keysize 2048. Il est important que les commandes CVP keystore incluent le paramètre -storetype JCEKS. Si ce n'est pas le cas, le certificat, la clé ou, pire, le magasin de clés peut être endommagé.

Spécifiez le nom de domaine complet du serveur, à la question quel est votre prénom et votre

nom ?




Répondez aux autres questions suivantes :

Quel est le nom de votre unité organisationnelle ?

[Inconnu] : <spécifier l'unité d'organisation>

Quel est le nom de votre entreprise ?

[Inconnu] : <indiquez le nom de l'organisation>

Quel est le nom de votre ville ou localité ?

[Inconnu] : <indiquer le nom de la ville/localité>

Quel est le nom de votre État ou de votre province ?

[Inconnu] : <indiquez le nom de l'état/de la province>

Quel est le code de pays à deux lettres de cette unité ?

[Inconnu] : <indiquer le code pays à deux lettres>

Spécifiez yes pour les deux entrées suivantes.

Étape 3. Effectuez les mêmes étapes pour vxml_certificate et callserver_certificate :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Serveur de rapports CVP

Étape 1. Pour supprimer les certificats WSM et Reporting Server, exécutez les commandes suivantes :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

Étape 2. Pour générer le certificat WSM, exécutez cette commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

Spécifiez le nom de domaine complet du serveur pour la requête. Quels sont vos nom et prénom ? et poursuivez avec les mêmes étapes que pour les serveurs CVP.

Étape 3. Effectuez les mêmes étapes pour callserver_certificate :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

CVP OAMP (déploiement UCCE)

Dans la version 12.x de la solution PCCE, tous les composants de la solution sont contrôlés par le SPOG et OAMP n'est pas installé. Ces étapes sont uniquement requises pour une solution de déploiement UCCE.

Étape 1. Pour supprimer les certificats WSM et OAMP Server, exécutez les commandes suivantes :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -a
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

Étape 2. Pour générer le certificat WSM, exécutez cette commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

Spécifiez le nom de domaine complet du serveur pour la requête. Quels sont vos nom et prénom ? et poursuivez avec les mêmes étapes que pour les serveurs CVP.

Étape 3. Effectuez les mêmes étapes pour oamp_certificate :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypai
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

2. Générer la CSR

---

Remarque : Le navigateur conforme à la norme RFC5280 nécessite que le nom alternatif du sujet (SAN) soit inclus avec chaque certificat. Pour ce faire, utilisez le paramètre -ext avec SAN lors de la génération du CSR.

---

Autre nom du sujet

Le paramètre -ext permet à un utilisateur d'utiliser des postes spécifiques. L'exemple ci-contre ajoute un autre nom de sujet (SAN) avec le nom de domaine complet (FQDN) du serveur ainsi que localhost. Des champs SAN supplémentaires peuvent être ajoutés sous forme de valeurs séparées par des virgules.

Les types de SAN valides sont :

```
ip:192.168.0.1
dns:myserver.mydomain.com
email:name@mydomain.com
```

Exemple :  -ext san=dns:mycvp.mydomain.com,dns:localhost

Serveurs CVP

Étape 1 : génération de la demande de certificat pour l’alias Exécutez cette commande et enregistrez-la dans un fichier (par exemple, wsm_certificate) :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

Étape 2 : exécution des mêmes étapes pour vxml_certificate et callserver_certificate

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

Serveur de rapports CVP

Étape 1 : génération de la demande de certificat pour l'alias Exécutez cette commande et enregistrez-la dans un fichier (par exemple, oampreport_certificate) :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

Étape 2. Effectuez les mêmes étapes pour le certificat callserver_certificate :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

CVP OAMP (déploiement UCCE)

Étape 1 : génération de la demande de certificat pour l'alias Exécutez cette commande et enregistrez-la dans un fichier (par exemple, oamp_certificate) :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
Ensure to replace "mycvp.mydomain.com" with your OAMP FQDN.
Enter the keystore password when prompted.
```

Étape 2. Effectuez les mêmes étapes pour wsm_certificate :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -
```

Entrez le mot de passe keystore lorsque vous y êtes invité.

3. Obtenir les certificats signés par l'autorité de certification

Étape 1 : signature des certificats sur un serveur AC (WSM, Callserver et VXML) pour le serveur CVP ; WSM et OAMP pour le serveur CVP OAMP, et WSM et Callserver pour le serveur Reporting).

Étape 2. Téléchargez les certificats d'application et le certificat racine à partir de l'autorité de certification.

Étape 3. Copiez le certificat racine et les certificats signés par l'autorité de certification dans le dossier %CVP_HOME%\conf\security\ de chaque serveur.

4. Importer les certificats signés par l'autorité de certification

Appliquez ces étapes à tous les serveurs de la solution CVP.  Seuls les certificats des composants sur ce serveur doivent avoir le certificat signé par l'autorité de certification importé.

Étape 1 : importation du certificat racine Exécutez cette commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Entrez le mot de passe keystore lorsque vous y êtes invité. À l'invite Trust this certificate, tapez Yes.

S'il existe un certificat intermédiaire, exécutez cette commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermediate_ca -file
```

Entrez le mot de passe keystore lorsque vous y êtes invité. À l'invite Trust this certificate, tapez Yes.

Étape 2. Importez le WSM CA signé pour ce certificat de serveur ( CVP, Reporting et OAMP). Exécutez cette commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Entrez le mot de passe keystore lorsque vous y êtes invité. À l'invite Trust this certificate, tapez Yes.

Étape 3. Dans les serveurs CVP et Reporting, importez le certificat CA signé Callserver. Exécutez cette commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Entrez le mot de passe keystore lorsque vous y êtes invité. À l'invite Trust this certificate, tapez Yes.

Étape 4. Dans les serveurs CVP, importez le certificat CA signé du serveur VXML. Exécutez cette commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Étape 5. Dans le serveur OAMP CVP (pour UCCE uniquement), importez le certificat CA signé du serveur OAMP. Exécutez cette commande :

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v
```

Étape 6. Redémarrez les serveurs.

---

Remarque : Dans le déploiement UCCE, veillez à ajouter les serveurs ( Reporting, CVP Server, etc.) dans CVP OAMP avec le nom de domaine complet que vous avez fourni lors de la génération du CSR.

---

## Serveurs VOS

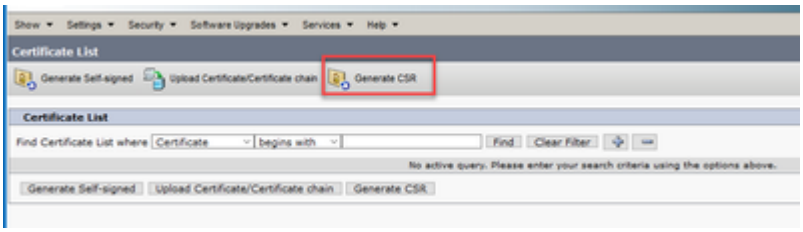
1. Générer un certificat CSR

Cette procédure explique comment générer un certificat CSR Tomcat à partir d'une plate-forme Cisco VOS (Voice Operating System). Ce processus s'applique à toutes les applications basées sur VOS telles que :

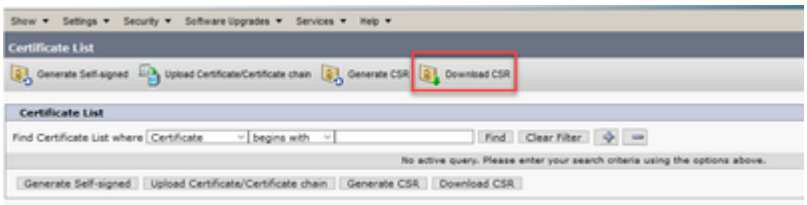
- CUCM
- Finesse
- CUIC \ Données actives (LD) \Serveur d'identités (IDS)
- Connexion au cloud
- Cisco VVB

Étape 1. Accédez à la page Cisco Unified Communications Operating System Administration : https://FQDN:<8443 or 443>/cmplatform.

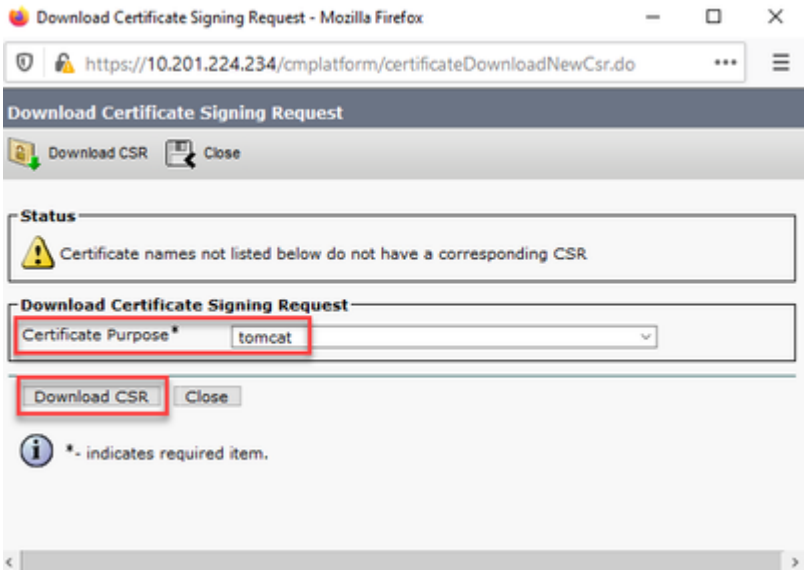
Étape 2. Accédez à Security > Certificate Management et sélectionnez Generate CSR.



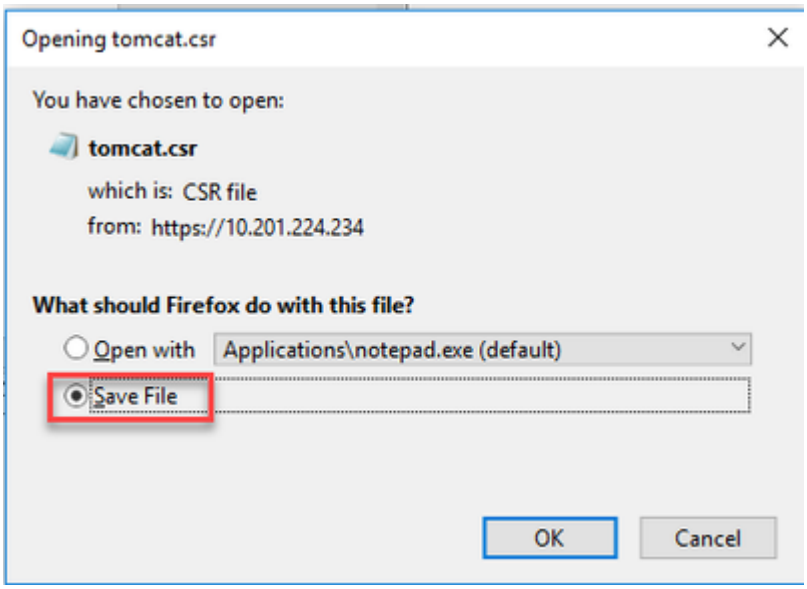

Étape 3. Une fois le certificat CSR généré, fermez la fenêtre et sélectionnez Download CSR.




Étape 4. Assurez-vous que l'objectif du certificat est d'agir et cliquez sur Download CSR.




Étape 5. Cliquez sur Save File. Le fichier est enregistré dans le dossier Téléchargement.



2. Obtenir les certificats signés par l'autorité de certification

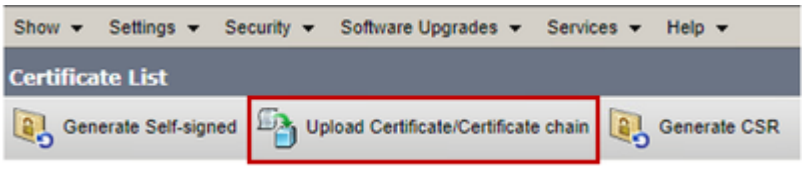
Étape 1 : signature du certificat tomcat exporté sur une autorité de certification

Étape 2. Téléchargez l'application et le certificat racine de l'autorité de certification.

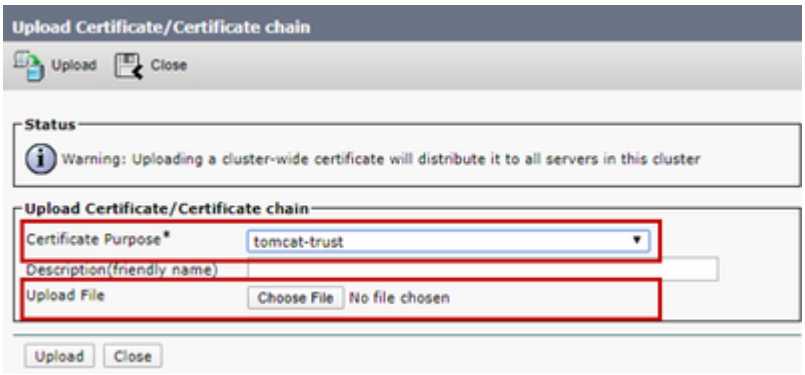
3. Télécharger l'application et les certificats racine

Étape 1. Accédez à la page Cisco Unified Communications Operating System Administration : https://FQDN:<8443 or 443>/cmplatform.

Étape 2. Accédez à Security > Certificate Management et sélectionnez Upload Certificate/Certificate chain.

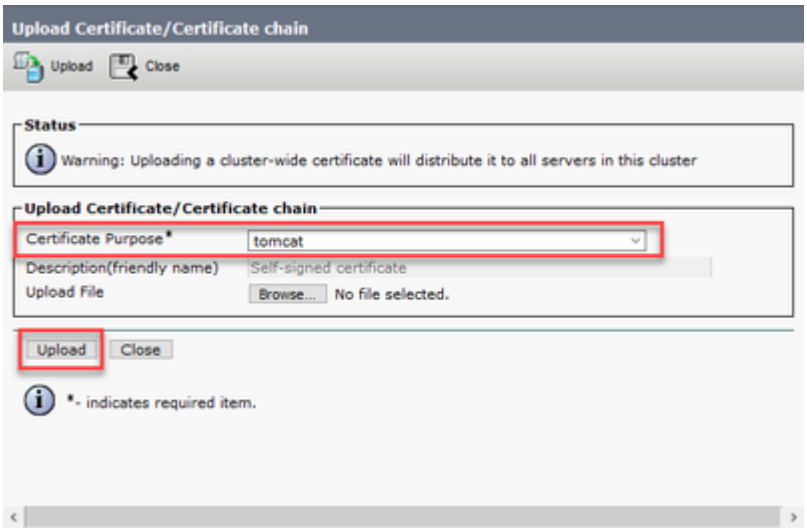



Étape 3. Dans la fenêtre Télécharger le certificat/la chaîne de certificats, sélectionnez tomcat-trust dans le champ Fonction du certificat et téléchargez le certificat racine.




Étape 4. Téléchargez un certificat intermédiaire (le cas échéant) comme tomcat-trust.

Étape 5. Dans la fenêtre Upload certificate/Certificate chain, sélectionnez maintenant to cat dans le champ Certificate Purpose et téléchargez le certificat signé par l'autorité de certification de l'application.




Étape 6. Redémarrez le serveur.

## Vérifier

Après avoir redémarré le serveur, exécutez ces étapes pour vérifier l'implémentation signée par l'autorité de certification :

Étape 1. Ouvrez un navigateur Web et videz le cache.

Étape 2. Fermez et ouvrez à nouveau le navigateur.

Maintenant, vous devez voir le commutateur de certificat pour commencer le certificat signé par l'autorité de certification et l'indication dans la fenêtre du navigateur que le certificat est auto-signé et donc pas approuvé, doit disparaître.

## Dépannage

Ce guide ne contient aucune étape de dépannage de la mise en oeuvre des certificats CA signés.

## Informations connexes

- Guide de configuration CVP : Guide de configuration CVP - Sécurité
- Guide de configuration UCCE : Guide de configuration UCCE - Sécurité
- Guide d'administration PCCE : Guide d'administration PCE - Sécurité
- Certificats auto-signés UCCE : certificats auto-signés UCCE Exchange
- Certificats autosignés PCCE : certificats autosignés PCCE d'Exchange
- Installation et migration vers OpenJDK dans CCE 12.5(1) : Migration CCE OpenJDK
- Installation et migration vers OpenJDK dans CVP 12.5(1) :&nbspbCVP OpenJDK Migration

Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.