

# Configurez les Certificats de serveur d'applications Ca-signés de ravitaillement pour amorcer le ravitaillement de Collaboration

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Condition requise](#)

[Composants utilisés](#)

[Configurez](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

## Introduction

Ce document décrit la procédure pour télécharger et vérifier l'Autorité de certification (CA) - les Certificats de serveur d'applications signés de ravitaillement pour amorcer le ravitaillement de Collaboration (PCP).

## Conditions préalables

### Condition requise

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- PCP et Microsoft CA interne
- Le plus défunt instantané du virtual machine (VM) ou la sauvegarde PCP avant que vous téléchargiez le certificat

### [Composants utilisés](#)

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

- Version 12.3 PCP
- Mozilla Firefox 55.0
- Microsoft CA interne

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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

# Configurez

Étape 1. Connectez-vous dans PCP et naviguez section vers la **gestion > les mises à jour > SSL Certificats**.

Étape 2. Cliquez sur en fonction la **demande de signature de certificat Generate**, écrivez l'attribut obligatoire et le clic **se produisent** suivant les indications de l'image.

**Note:** L'attribut de nom commun doit s'assortir au nom de domaine complet PCP (FQDN).

## Generate Certificate Signing Request



 **Warning: Generating a new certificate signing request will overwrite an existing CSR.**

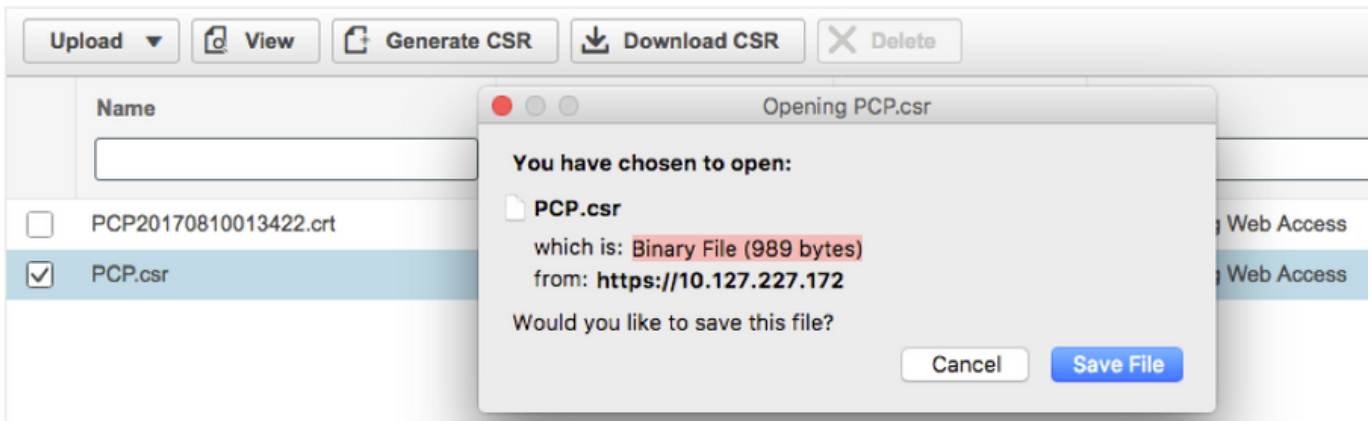
* Certificate Name	<input type="text" value="PCP"/>
* Country Name	<input type="text" value="IN"/>
* State or Province	<input type="text" value="KA"/>
* Locality Name	<input type="text" value="BLR"/>
* Organization Name	<input type="text" value="Cisco"/>
* Organization Unit Name	<input type="text" value="PCP"/>
* Common Name	<input type="text" value="pcp12.uc.com"/>
Email Address	<input type="text" value="Standard format email address"/>
Key Type	RSA
Key Length	2048
Hash Algorithm	SHA256

Cancel

Generate

Étape 3. Cliquez sur Download le **CSR** pour générer le certificat suivant les indications de l'image.

▼ SSL Certificates



Étape 4. Utilisez cette demande de signature de certificat (CSR) de générer le certificat signé du public CA avec l'aide du fournisseur public CA.

Si vous voulez signer le certificat avec interne ou les gens du pays CA, suivez ces étapes :

Étape 1. Connectez-vous dans le CA interne et téléchargez le CSR suivant les indications de l'image.

## Microsoft Active Directory Certificate Services – uc-AD-CA

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC

#### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

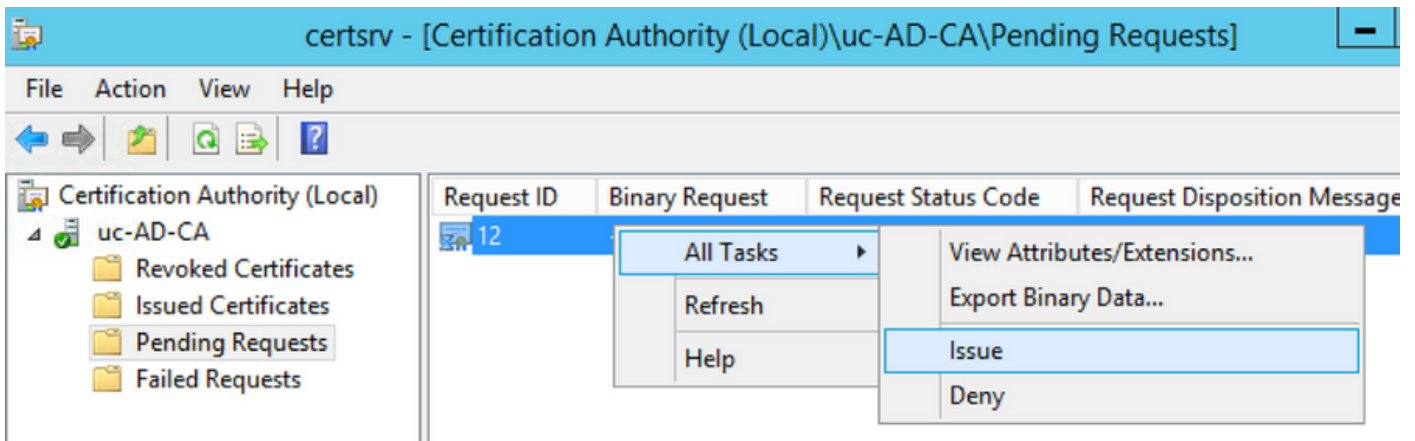
```
rgjs0D7CqaEV3Q0QUobohfilsh7EGp2r20oH3qPc  
rqYIeXDxJtwR7ULyyhUd3JJSI3blYK/Wipb4Vg/l  
zfgMY3ZQ2R9JP5+C0vGr5YRGpu28ZUePaqRSWub6  
IAHfSmWZ3srSp/Hlw5R+dEkmQ4UcXHpOJxKGoh4n  
IwJBKmfC  
-----END CERTIFICATE REQUEST-----
```

#### Additional Attributes:

Attributes:

Submit >

Étape 2. Connectez au serveur interne CA, clic droit sur des **demandes en suspens > toutes les tâches > question** choisie pour obtenir un certificat signé suivant les indications de l'image.



Étape 3. Puis, le format **encodé de la base 64** choisis de case d'option et cliquent sur Download le **certificat** suivant les indications de l'image.

### Microsoft Active Directory Certificate Services -- uc-AD-CA

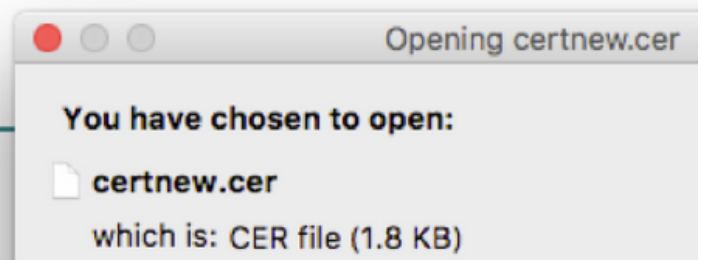
#### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download certificate](#)  
[Download certificate chain](#)



Étape 4. Dans le GUI de Web PCP, naviguez **section** vers la **gestion > les mises à jour > SSL Certificats**, cliquent sur Upload, choissent le certificat qui a été généré et cliquent sur Upload **suivant les indications de l'image**.

**Note:** Vous devez télécharger le certificat de serveur Web PCP seulement, des certificats racine n'êtes pas prié d'être téléchargé puisque PCP est un serveur de noeud simple.

#### Upload New Provisioning Certificate

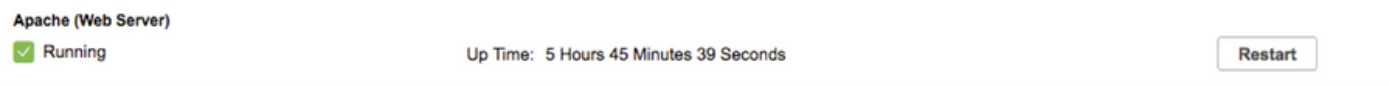
**i** Restart all processes to activate new SSL certificate.

certnew.cer  .cer or .crt file type required

Cancel

Upload

Étape 5. Après que vous téléchargez le certificat Ca-signé, naviguez vers la **gestion > la gestion de processus** et cliquez sur la **reprise** Apache (serveur Web) Serviceas affiché dans l'image.



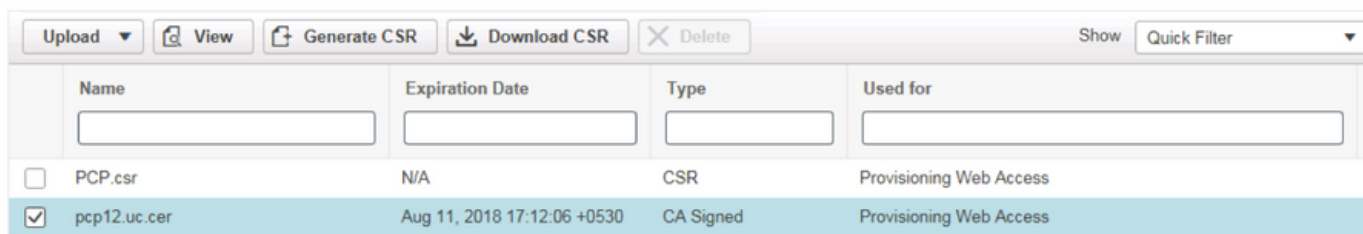
## Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Voici les étapes à vérifier que le certificat signé CA sont téléchargés au PCP.

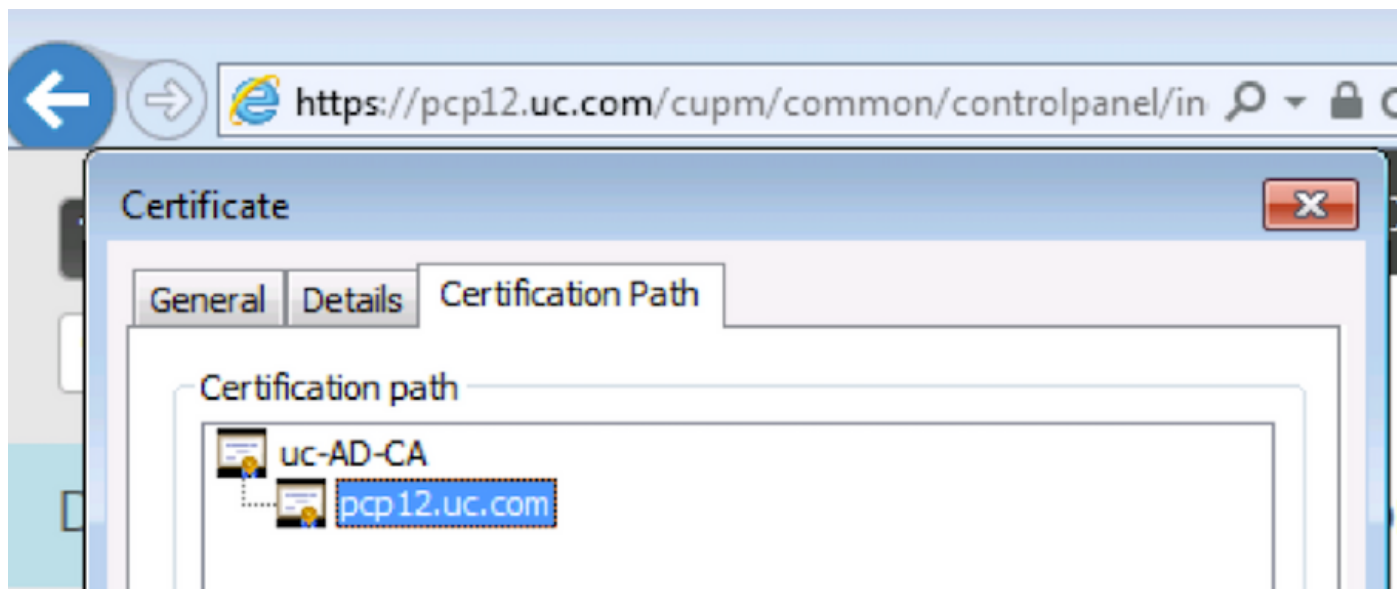
Étape 1. Le téléchargement du certificat signé CA remplace le certificat auto-signé par PCP, et le type est affiché comme CA signé avec la date d'expiration suivant les indications de l'image.

### ▼ SSL Certificates



Name	Expiration Date	Type	Used for
<input type="checkbox"/> PCP.csr	N/A	CSR	Provisioning Web Access
<input checked="" type="checkbox"/> pcp12.uc.cer	Aug 11, 2018 17:12:06 +0530	CA Signed	Provisioning Web Access

Étape 2. Connectez-vous dans PCP avec l'utilisation du FQDN et cliquez sur en fonction le **symbole sécurisé de verrouillage** sur le navigateur. Cliquez sur en fonction **plus d'informations** et vérifiez le **chemin de certification** suivant les indications de l'image.



## Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

De PCP 12.X, il n'y a aucun accès au shell CLI/Secure (SSH) comme racine. Pour aucune

question, télécharger le certificat ou l'interface web PCP n'est pas accessible après que téléchargement de certificat, le centre d'assistance technique Cisco de contact (TAC).

## **Informations connexes**

- [Ravitaillement de Collaboration de perfection de Cisco](#)
- [Collectez les logs de ShowTech du GUI du ravitaillement principal de Collaboration](#)
- [Support et documentation techniques - Cisco Systems](#)