

Certificaten voor CA-ondertekende Provisioning-toepassingservers configureren op basis van Prime Collaboration Provisioning

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de procedure voor het uploaden en controleren van certificaatautoriteit (CA) - Signed Provisioning Application Server-certificaten aan Prime Collaboration Provisioning (PCP).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- PCP en Microsoft interne CA
- Nieuwste virtuele machine (VM) - Snapshot of PCP-back-up voordat u het certificaat uploadt

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Stap 1. Meld u aan bij PCP en navigeer naar **Administratie > updates > SSL-certificaten**.

Stap 2. Klik op **Generate certificaataanvraag**, voer de verplichte eigenschap in en klik op **Generate** zoals in de afbeelding.

Opmerking: De eigenschap Common Name moet overeenkomen met de PC Full Qualified Domain Name (FQDN).

Generate Certificate Signing Request

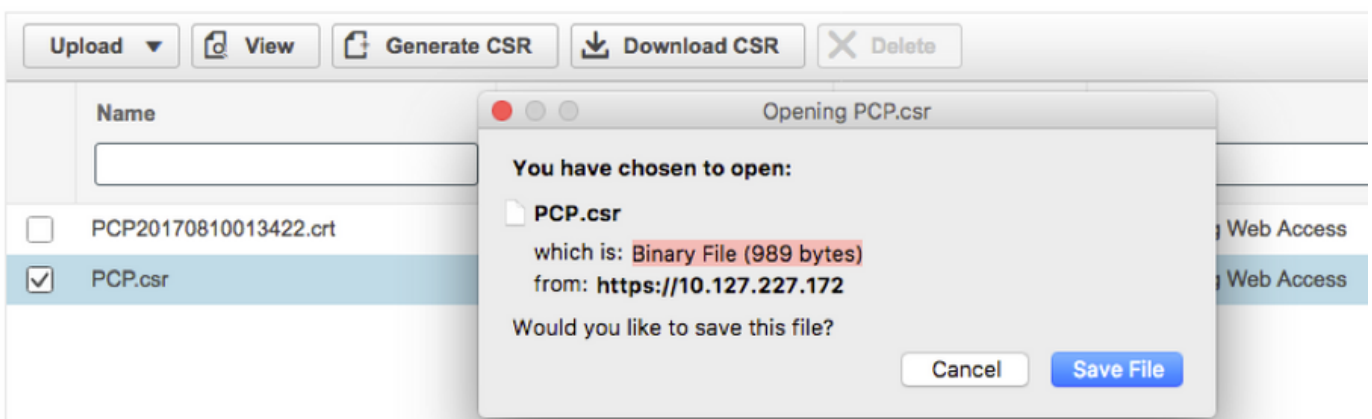


Warning: Generating a new certificate signing request will overwrite an existing CSR.

* 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

Stap 3. Klik op **CSR downloaden** om het certificaat te genereren zoals in de afbeelding.

SSL Certificates



Stap 4. Gebruik dit certificaatverzoek (CSR) om het openbare CA-ondertekende certificaat te genereren met de hulp van een openbare CA-provider.

Als u het certificaat wilt ondertekenen met interne of lokale CA, volgt u deze stappen:

Stap 1. Meld u aan bij Intern CA en uploadt u de CSR zoals in de afbeelding.

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):

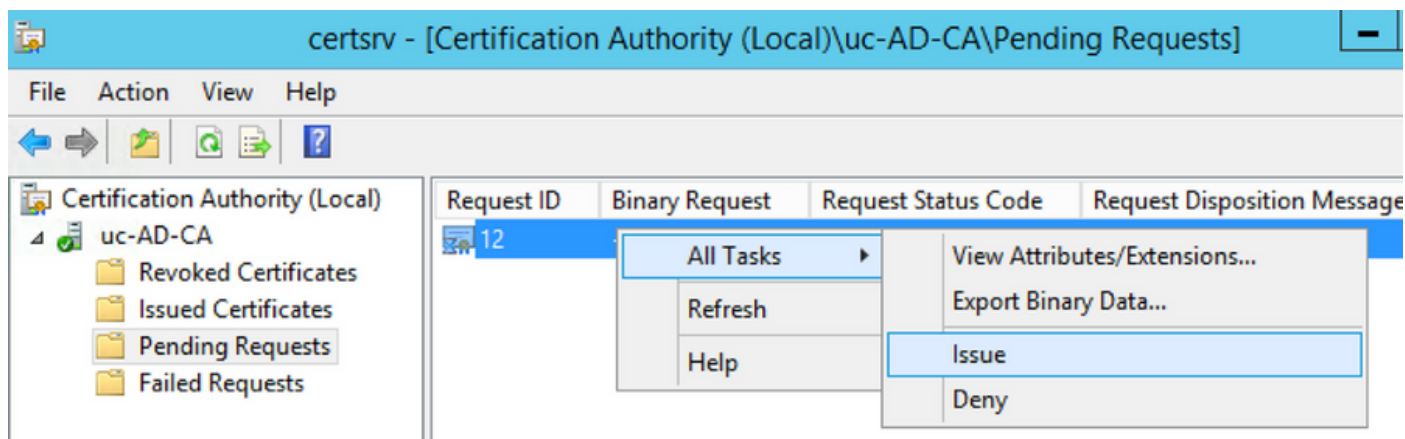
```
rgjs0D7CqaEV3Q0QUObohfilsh7EGp2r20oH3qPc  
rqYIeXDxJtwR7ULyyhUd3JJSI3blYK/Wipb4Vg/l  
zfgMY3ZQ2R9JP5+C0vGr5YRGpu28ZUePaqRSWub6  
IAHfSmWZ3srSp/Hlw5R+dEkmQ4UcXHpOJxKGoh4n  
IwJBKmfC  
-----END CERTIFICATE REQUEST-----
```

Additional Attributes:

Attributes:

Submit >

Stap 2. Sluit aan op de interne CA-server en klik met de rechtermuisknop op **Verzoeken > Alle taken > Selecteer Problemen** om een ondertekend certificaat te verkrijgen zoals in de afbeelding.



Stap 3. Selecteer vervolgens de radioknop **Base 64 gecodeerde** indeling en klik op **Download certificaat** zoals in de afbeelding.

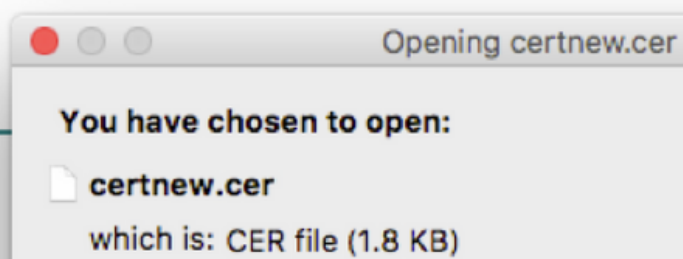
Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



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



Stap 4. In PCP Web GUI, navigeer naar **Administratie > updates > SSL Certificaten Sectie**, klik op **Upload**, kies het certificaat dat werd gegenereerd en klik op **Upload** zoals in de afbeelding.

Opmerking: U hoeft alleen PCP-webservercertificaat te uploaden, er hoeven geen Root-certificaten te worden geüpload omdat PCP een Single Node Server is.

Upload New Provisioning Certificate



Restart all processes to activate new SSL certificate.

.cer or .crt file type required

Stap 5. Nadat u het CA-ondertekende certificaat hebt geüpload, navigeer dan naar **Administratie > Procesbeheer** en klik op Start Apache (Web Server) Services zoals in de afbeelding weergegeven.

Apache (Web Server)

Running

Up Time: 5 Hours 45 Minutes 39 Seconds

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

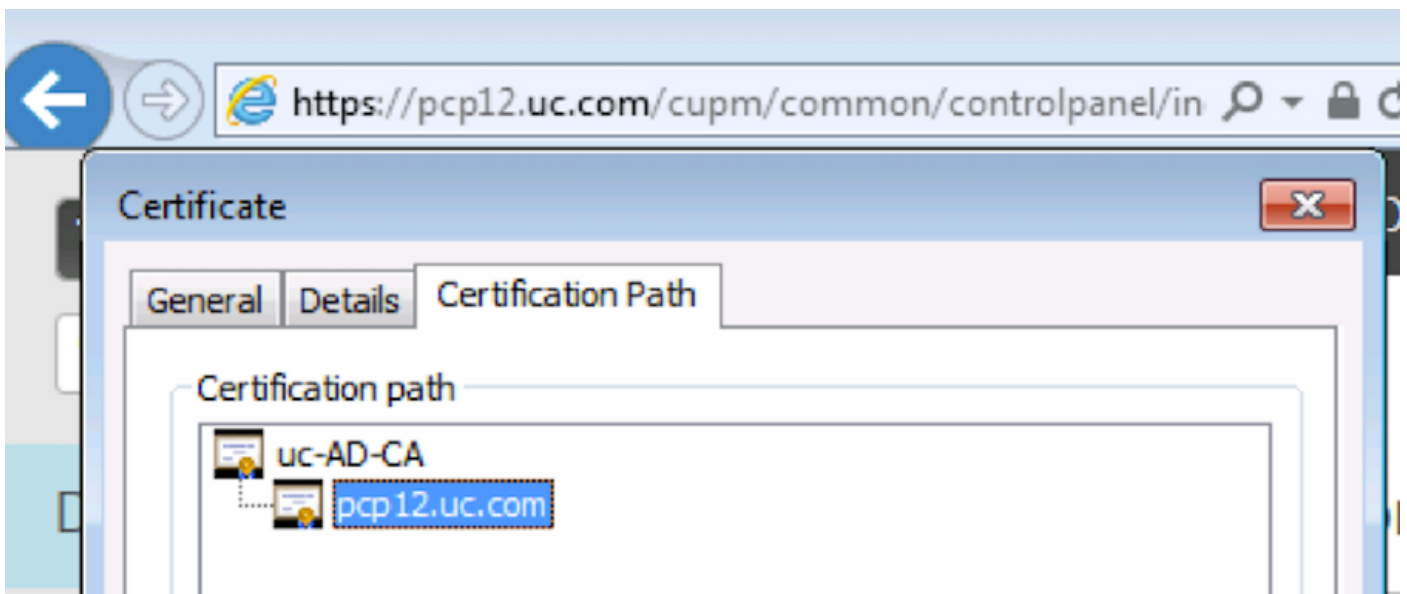
Hier volgen de stappen om te controleren of het door CA ondertekende certificaat wordt geüpload naar de PC.

Stap 1. Het uploaden van het door CA ondertekende certificaat vervangt het door PCP zelf ondertekende certificaat en het type wordt weergegeven als CA Signed met de Verlooptdatum zoals getoond in de afbeelding.

▼ 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

Stap 2. Meld u aan bij PCP met het gebruik van de FQDN en klik op het **beveiligde vergrendelings**symbool in de browser. Klik op **Meer informatie** en controleer het **certificeringspad** zoals in de afbeelding wordt weergegeven.



Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Vanaf PCP 12.X is er geen toegang tot CLI/Secure Shell (SSH) als wortel. Om het certificaat te uploaden of de PCP-webinterface niet toegankelijk is na het uploaden van het certificaat, neemt u contact op met Cisco Technical Assistance Center (TAC).

Gerelateerde informatie

- [Cisco Prime-provisioning voor samenwerking](#)
- [TechLogs van de GUI van de Provisioning voor Prime-collaboration](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)