

# Konfigurieren von CA-signierten Bereitstellungsserver-Zertifikaten für Prime Collaboration Provisioning

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderung](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument beschreibt das Verfahren zum Hochladen und Überprüfen von Zertifikaten der Zertifizierungsstelle (Certificate Authority, CA) - Signed Provisioning Application Server-Zertifikaten auf Prime Collaboration Provisioning (PCP).

## Voraussetzungen

### Anforderung

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- PCP und interne Microsoft-CA
- Aktueller VM-Snapshot oder PCP-Backup vor dem Hochladen des Zertifikats

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Konfigurieren

Schritt 1: Melden Sie sich bei PCP an, und navigieren Sie zu **Administration > Updates > SSL Certificates Section**.

Schritt 2: Klicken Sie auf **Zertifikatssignierungsanforderung erstellen**, geben Sie das obligatorische Attribut ein, und klicken Sie auf **Generieren** wie im Bild gezeigt.

**Hinweis:** Das Common Name-Attribut muss mit dem vollständig qualifizierten PCP-Domännennamen (FQDN) übereinstimmen.

## Generate Certificate Signing Request

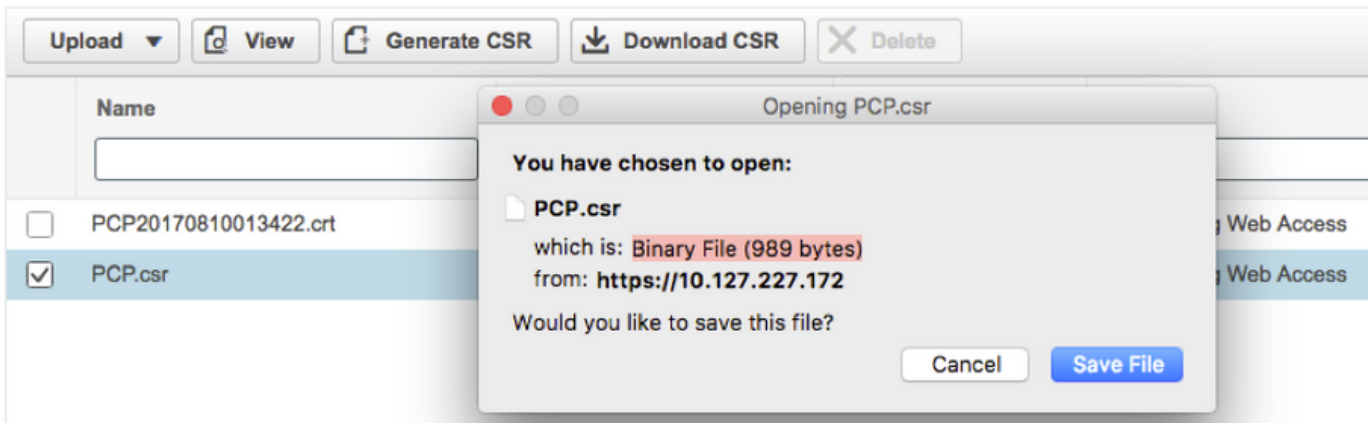


 **Warning: Generating a new certificate signing request will overwrite an existing CSR.**

* 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

Schritt 3: Klicken Sie auf **CSR herunterladen**, um das Zertifikat zu generieren, wie im Bild gezeigt.

▼ SSL Certificates



Schritt 4: Verwenden Sie diese Certificate Signing Request (CSR), um mithilfe eines öffentlichen CA-Anbieters das von der öffentlichen Zertifizierungsstelle signierte Zertifikat zu generieren.

Wenn Sie das Zertifikat mit einer internen oder lokalen Zertifizierungsstelle unterzeichnen möchten, gehen Sie wie folgt vor:

Schritt 1: Melden Sie sich bei der internen CA an, und laden Sie den CSR hoch, wie im Bild gezeigt.

**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:**

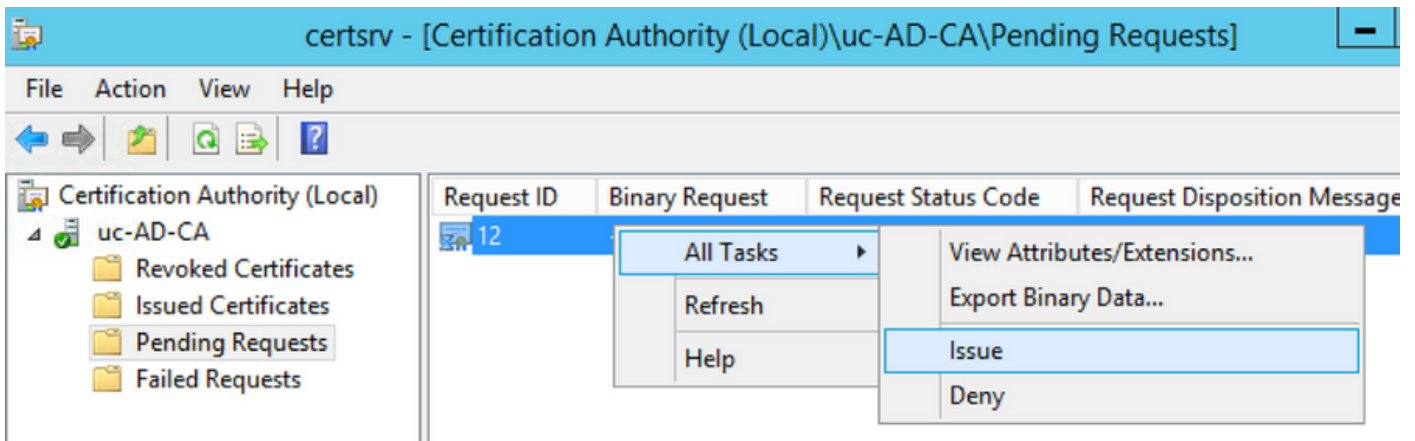
```
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7): rgjs0D7CqaEV3Q0QUObohfilsh7EGp2r20oH3qPc  
rqYIeXDxJtwR7ULyyhUd3JJSI3blYK/Wipb4Vg/l  
zfgMY3ZQ2R9JP5+C0vGr5YRGpu28ZUePaqRSWub6  
IAHfSmWZ3srSp/Hlw5R+dEkmQ4UcXHpOJxKGoh4n  
IwJBKmfC  
-----END CERTIFICATE REQUEST-----
```

**Additional Attributes:**

Attributes:

Submit >

Schritt 2: Stellen Sie eine Verbindung zum internen CA-Server her, und klicken Sie mit der rechten Maustaste auf **Ausstehende Anforderungen > Alle Aufgaben > Problem** auswählen, um ein signiertes Zertifikat zu erhalten, wie im Bild gezeigt.



Schritt 3: Wählen Sie anschließend das Optionsfeld **Base 64-verschlüsseltes** Format aus, und klicken Sie auf **Zertifikat herunterladen**, wie im Bild gezeigt.

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

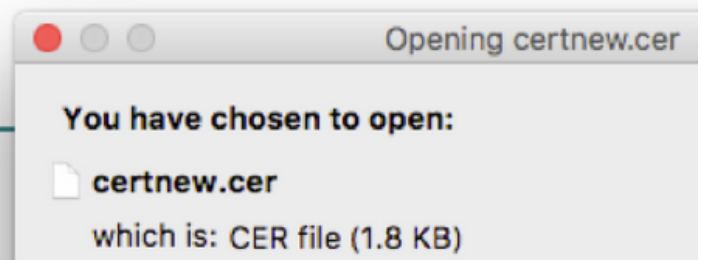
#### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



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



Schritt 4: Navigieren Sie in der PCP-Webbenutzeroberfläche zu **Administration > Updates > SSL Certificates Section**, klicken Sie auf **Upload**, wählen Sie das generierte Zertifikat aus und klicken Sie auf **Upload (Hochladen)** wie im Bild gezeigt.

**Hinweis:** Sie müssen nur das PCP-Webserver-Zertifikat hochladen. Root-Zertifikate müssen nicht hochgeladen werden, da PCP ein Single Node-Server ist.

#### Upload New Provisioning Certificate

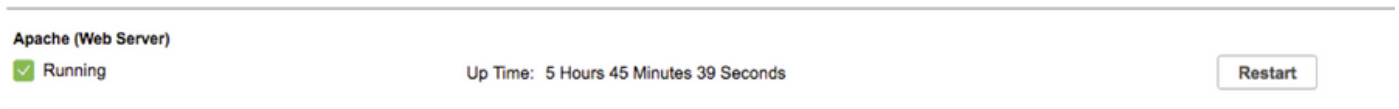


**i** Restart all processes to activate new SSL certificate.

**Choose File** .cer or .crt file type required

**Cancel** **Upload**

Schritt 5: Navigieren Sie nach dem Hochladen des Zertifizierungsstellenzertifikats zu **Administration > Process Management**, und klicken Sie auf **Restart Apache (Webserver) Service** (Neustarten des Apache-Dienstes), wie im Bild gezeigt.



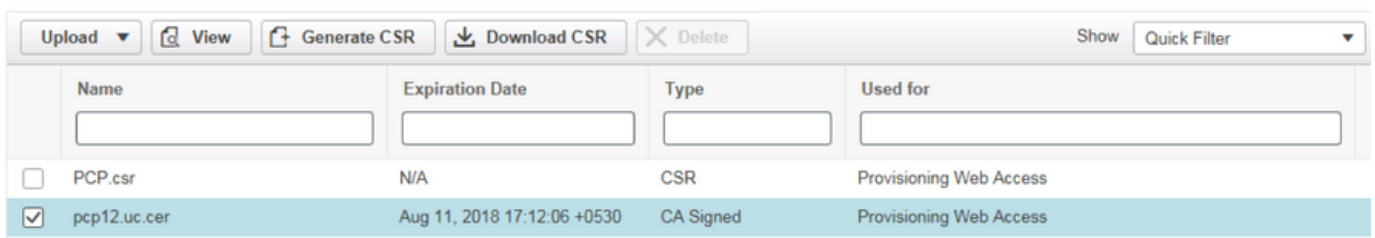
## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Im Folgenden finden Sie die Schritte, um zu überprüfen, ob das signierte Zertifikat der CA auf den PCP hochgeladen wird.

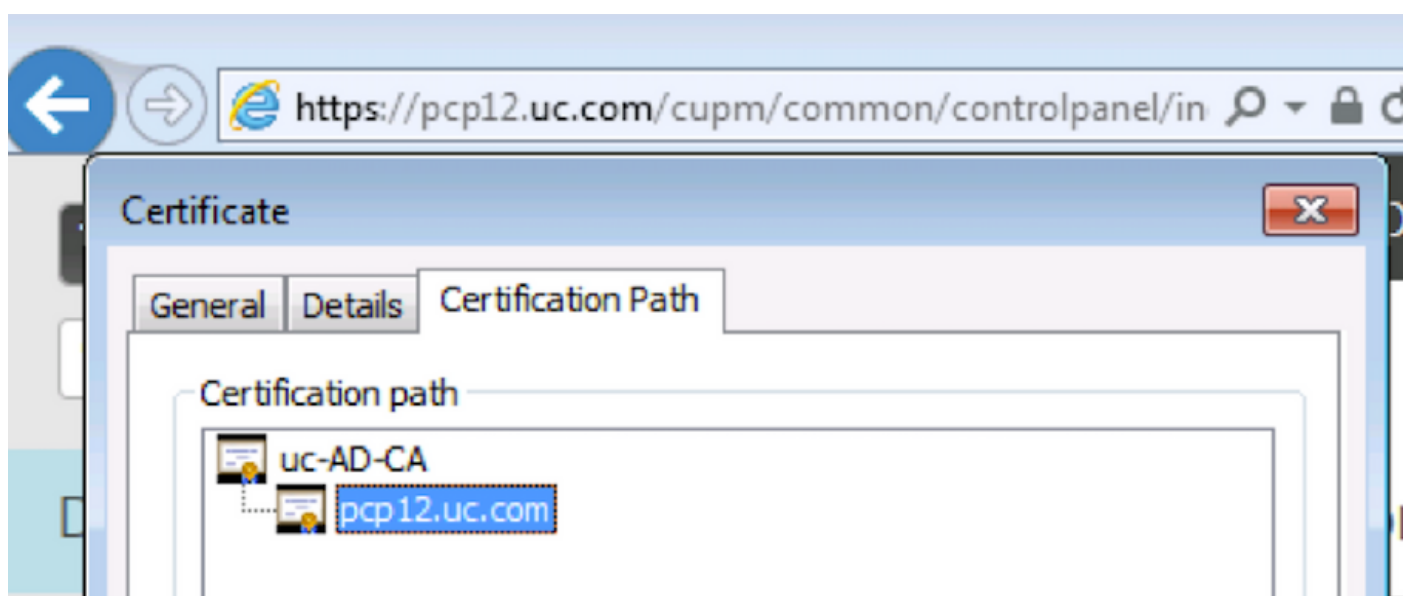
Schritt 1: Das Hochladen des signierten Zertifikats der Zertifizierungsstelle ersetzt das selbstsignierte PCP-Zertifikat, und der Typ wird als mit dem Ablaufdatum signierte Zertifizierungsstelle angezeigt, wie im Bild gezeigt.

### ▼ 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

Schritt 2: Melden Sie sich mithilfe des FQDN bei PCP an, und klicken Sie im Browser auf das **Symbol für sichere Sperre**. Klicken Sie auf **Weitere Informationen** und überprüfen Sie den **Zertifizierungspfad** wie im Bild gezeigt.



## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

PCP 12.X bietet keinen Zugriff auf CLI/Secure Shell (SSH) als Root. Bei Problemen, wenn Sie das Zertifikat hochladen möchten oder die PCP-Webschnittstelle nach dem Hochladen des Zertifikats nicht verfügbar ist, wenden Sie sich an das Cisco Technical Assistance Center (TAC).

## Zugehörige Informationen

- [Cisco Prime Collaboration-Bereitstellung](#)
- [Erfassen Sie ShowTech-Protokolle über die Benutzeroberfläche von Prime Collaboration Provisioning.](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)