

將CA簽名的調配應用程式伺服器證書配置到Prime合作調配

目錄

- [簡介](#)
- [必要條件](#)
- [需求](#)
- [採用元件](#)
- [設定](#)
- [驗證](#)
- [疑難排解](#)
- [相關資訊](#)

簡介

本檔案介紹將憑證授權單位(CA) — 簽署式布建應用伺服器憑證上傳和驗證到Prime合作布建(PCP)的程式。

必要條件

需求

思科建議您瞭解以下主題：

- PCP和Microsoft內部CA
- 上傳證書之前的最新虛擬機器(VM)快照或PCP備份

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PCP版本12.3
- Mozilla Firefox 55.0
- Microsoft內部CA

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

步驟1. 登入PCP並導航到Administration > Updates > SSL Certificates部分。

步驟2. 按一下Generate Certificate Signing Request，輸入所需的屬性，然後按一下Generate，如下圖所示。

附註：公用名稱屬性必須與PCP完全限定域名(FQDN)匹配。

Generate Certificate Signing Request



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

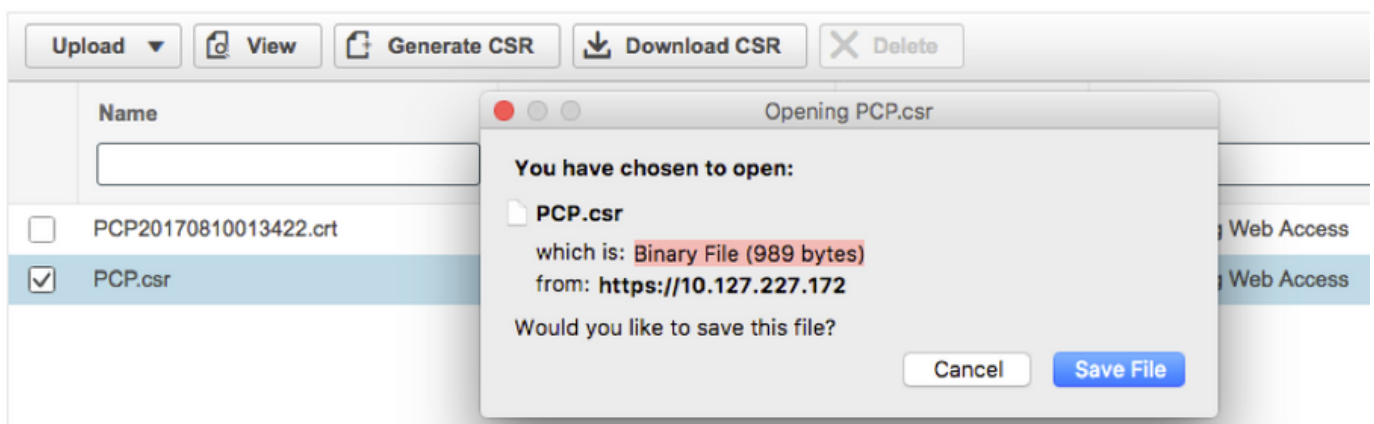
* Certificate Name	<input type="text" value="PCP"/>
* Country Name	<input type="text" value="IN"/>
* State or Province	<input type="text" value="KA"/>
* Locality Name	<input type="text" value="BLR"/>
* Organization Name	<input type="text" value="Cisco"/>
* Organization Unit Name	<input type="text" value="PCP"/>
* 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

步驟3. 按一下Download CSR，產生憑證，如下圖所示。

SSL Certificates



步驟4. 使用此憑證簽署請求(CSR)在公共CA提供者的幫助下產生公共CA簽署的憑證。

如果要使用內部或本地CA簽署憑證，請執行以下步驟：

步驟1. 登入內部CA並上傳CSR，如圖所示。

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):

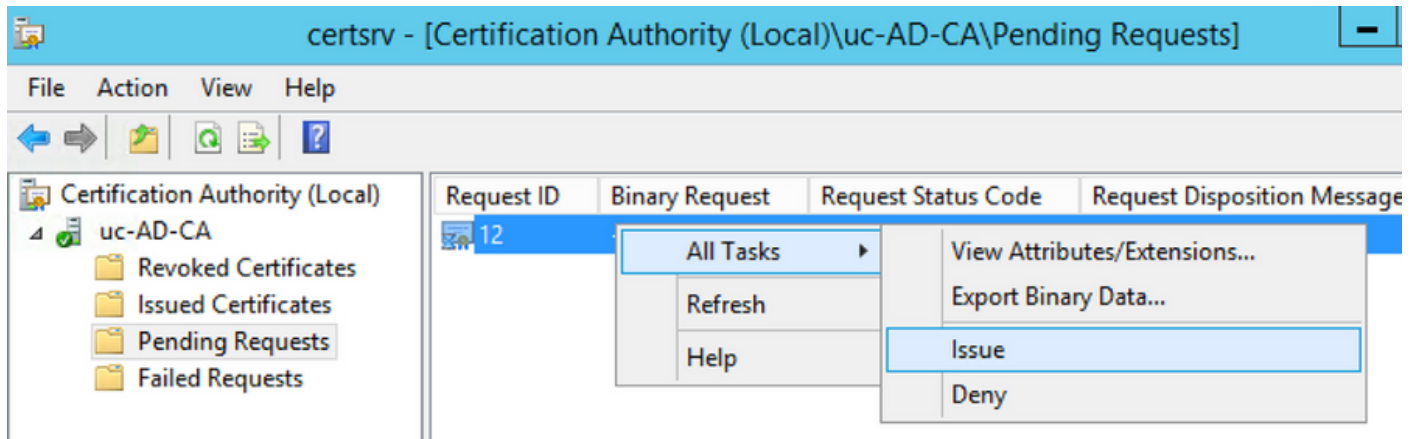
```
rgjs0D7CqaEV3Q0QUObohfilsh7EGp2r20oH3qPc  
rqYIeXDxJtwR7ULyyhUd3JJSI3blYK/Wipb4Vg/l  
zfgMY3ZQ2R9JP5+C0vGr5YRGpu28ZUePaqRSWub6  
IAHfSmWZ3srSp/Hlw5R+dEkmQ4UcXHpOJxKGoh4n  
IwJBKmfC  
-----END CERTIFICATE REQUEST-----
```

Additional Attributes:

Attributes:

Submit >

步驟2.連線到內部CA伺服器，按一下右鍵Pending Requests > All Tasks > Select Issue以取得簽名的憑證，如下圖所示。



步驟3.然後，選擇單選按鈕Base 64 encoded format，然後按一下Download certificate，如下圖所示。

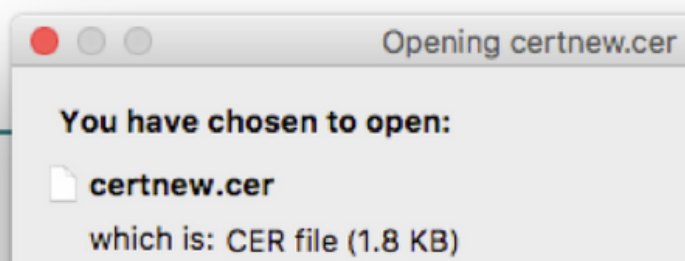
Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



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



步驟4.在PCP Web GUI中，導覽至Administration > Updates > SSL Certificates部分，按一下Upload，選擇產生的憑證，然後按一下Upload，如下圖所示。

附註：您只需要上傳PCP Web伺服器證書，由於PCP是單節點伺服器，因此不需要上傳根證書。

Upload New Provisioning Certificate



i Restart all processes to activate new SSL certificate.

certnew.cer .cer or .crt file type required

Cancel

Upload

步驟5.上傳CA簽名的憑證後，導覽至Administration > Process Management，然後按一下Restart Apache(Web Server)Serviceing，如下圖所示。

Apache (Web Server)

Running

Up Time: 5 Hours 45 Minutes 39 Seconds

驗證

使用本節內容，確認您的組態是否正常運作。

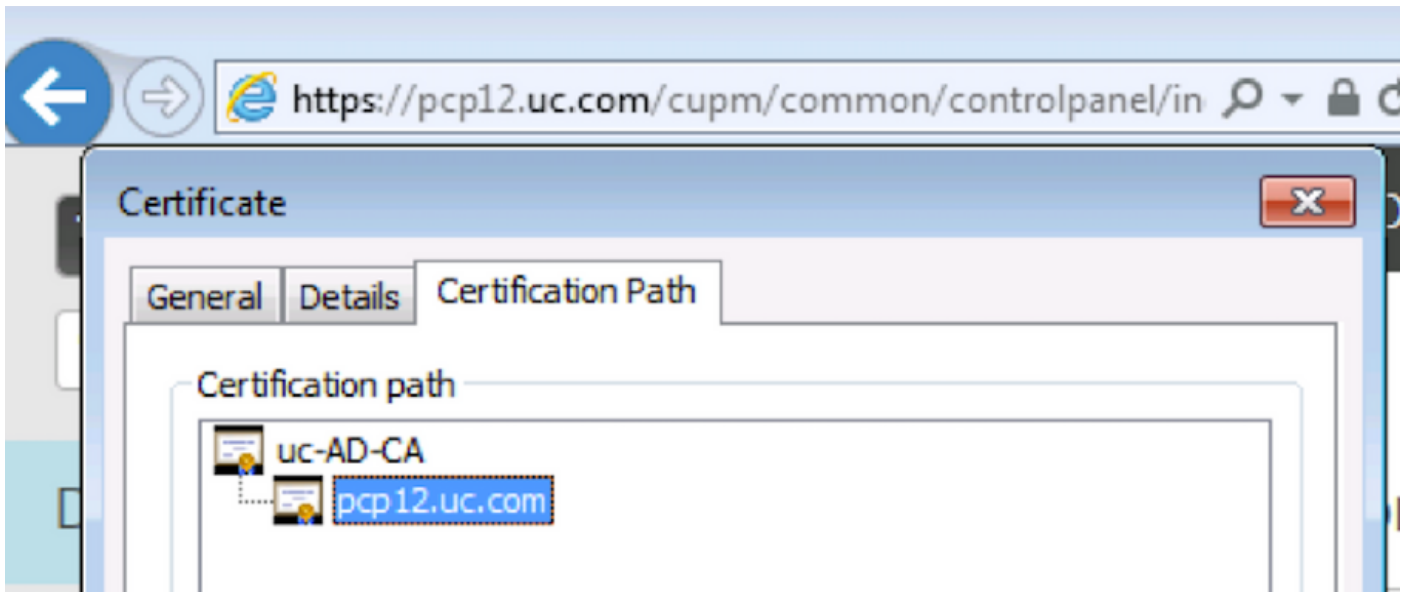
以下是驗證CA簽名證書是否已上傳到PCP的步驟。

步驟1. 上傳CA簽名的證書將替換PCP自簽名的證書，並且型別顯示為CA簽名，過期日期如下圖所示。

▼ SSL Certificates

Upload ▾ View Generate CSR Download CSR Delete Show Quick Filter ▾			
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

步驟2.使用FQDN登入到PCP，然後在瀏覽器上按一下安全鎖定符號。按一下「More information」，然後驗證「Certification Path」，如下圖所示。



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

從PCP 12.X無法作為根訪問CLI/安全外殼(SSH)。如果發生任何問題，若要上傳證書或在上傳證書後無法訪問PCP Web介面，請聯絡思科技術支援中心(TAC)。

相關資訊

- [Cisco Prime Collaboration Provisioning](#)
- [從Prime合作調配的GUI收集ShowTech日誌](#)
- [技術支援與文件 - Cisco Systems](#)