

将CA签名的调配应用服务器证书配置为Prime协作调配

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍将证书颁发机构(CA) — 签名调配应用服务器证书上传和验证到Prime协作调配(PCP)的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- PCP和Microsoft内部CA
- 上传证书之前，最新虚拟机(VM)快照或PCP备份

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

步骤1.登录PCP并导航至Administration > Updates > **SSL Certificates**部分。

步骤2.单击“生成证书签名请求”，输入必填属性，然后单击“生成”，如图所示。

注意：公用名属性必须与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.

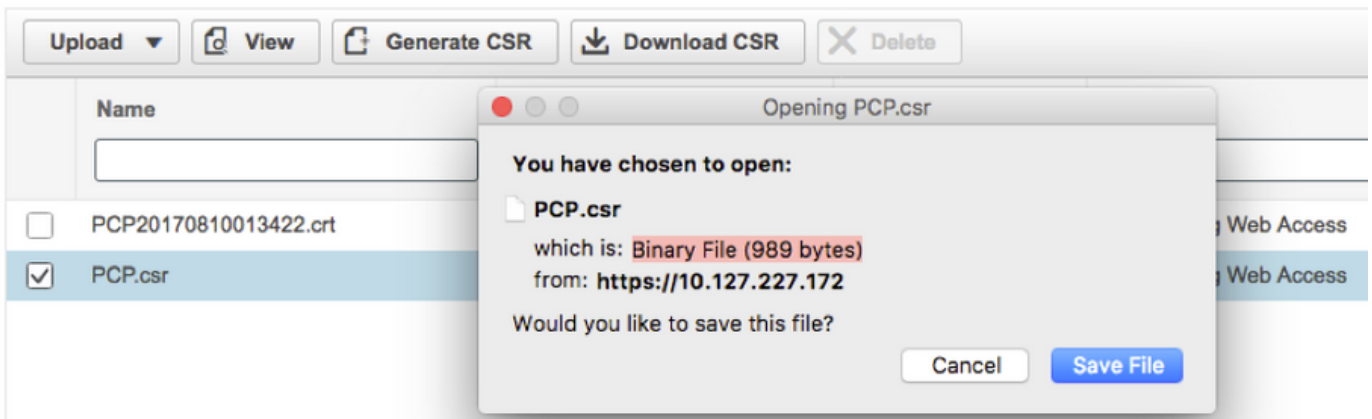
* Certificate Name	<input type="text" value="PCP"/>
* Country Name	<input type="text" value="IN"/>
* State or Province	<input type="text" value="KA"/>
* Locality Name	<input type="text" value="BLR"/>
* Organization Name	<input type="text" value="Cisco"/>
* Organization Unit Name	<input type="text" value="PCP"/>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

步骤3.单击Download CSR 以生成如图所示的证书。

SSL Certificates



步骤4.使用此证书签名请求(CSR)在公共CA提供商的帮助下生成公共CA签名证书。

如果要使用内部或本地CA签署证书，请执行以下步骤：

步骤1.登录内部CA并上传CSR，如图所示。

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):

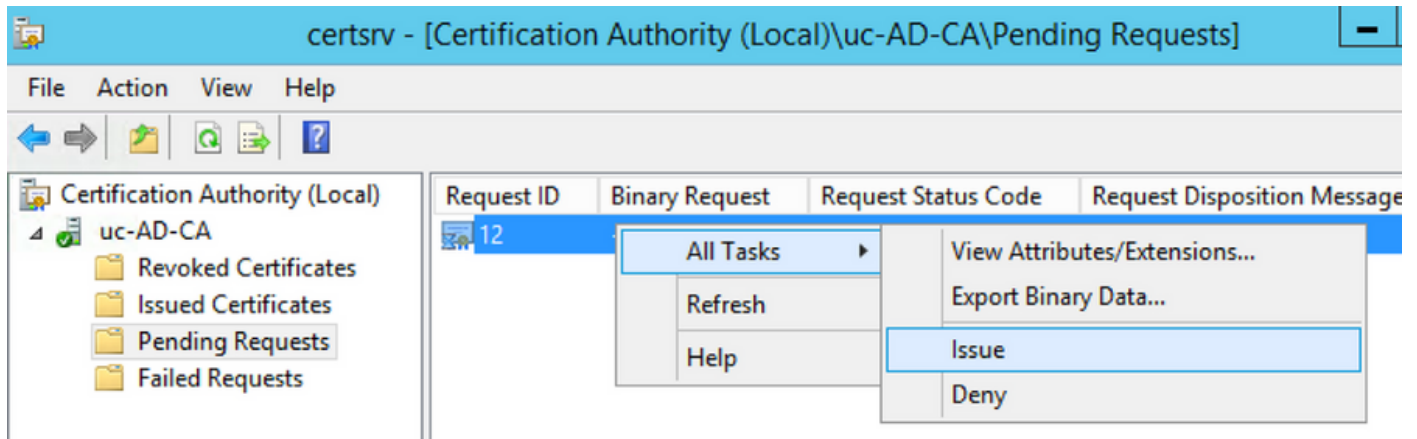
```
rgjs0D7CqaEV3Q0QUObohfilsh7EGp2r20oH3qPc  
rqYIeXDxJtwR7ULyyhUd3JJSI3blYK/Wipb4Vg/l  
zfgMY3ZQ2R9JP5+C0vGr5YRGpu28ZUePaqRSWub6  
IAHfSmWZ3srSp/Hlw5R+dEkmQ4UcXHpOJxKGoh4n  
IwJBKmfC  
-----END CERTIFICATE REQUEST-----
```

Additional Attributes:

Attributes:

Submit >

步骤2. 连接到内部CA服务器，右键单击Pending Requests > All Tasks > Select Issue 以获取签名证书，如图所示。



步骤3. 然后，选择单选按钮Base 64编码格式，然后单击Download certificate，如图所示。

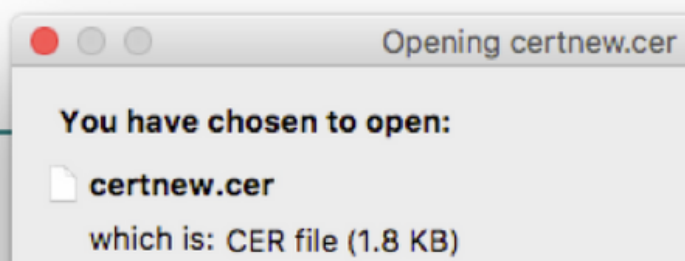
Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



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



步骤4.在PCP Web GUI中，导航至Administration > Updates > SSL Certificates Section，单击Upload，选择生成的证书，然后单击Upload，如图所示。

注意：您只需上传PCP Web服务器证书，无需上传根证书，因为PCP是单节点服务器。

Upload New Provisioning Certificate



Restart all processes to activate new SSL certificate.

certnew.cer .cer or .crt file type required

Cancel

Upload

步骤5.上传CA签名证书后，导航到Administration > Process Management，然后单击Restart Apache(Web Server)Service，如图所示。

Apache (Web Server)

Running

Up Time: 5 Hours 45 Minutes 39 Seconds

验证

使用本部分可确认配置能否正常运行。

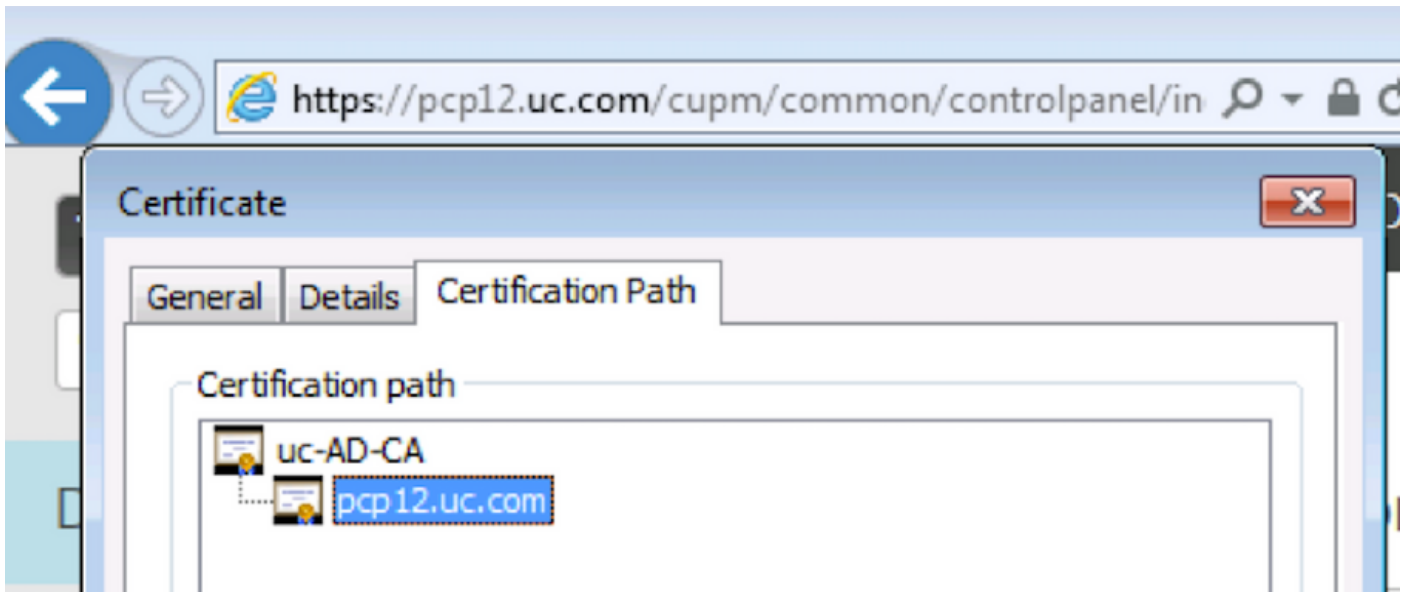
以下是验证CA签名证书是否已上传到PCP的步骤。

步骤1.上传CA签名证书将取代PCP自签名证书，类型显示为CA Signed with the Expiration Date，如图所示。

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						

步骤2.使用FQDN登录PCP，然后在浏览器上单击安全锁符号。单击“More (详细)”，并验证认证路径，如图所示。



故障排除

本部分提供了可用于对配置进行故障排除的信息。

从PCP 12.X，无法以根用户身份访问CLI/Secure Shell(SSH)。如有任何问题，请联系思科技术支持中心(TAC)，上传证书或PCP网络界面后无法访问。

相关信息

- [思科Prime协作调配](#)
- [从Prime协作调配的GUI收集ShowTech日志](#)
- [技术支持和文档 - Cisco Systems](#)