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

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

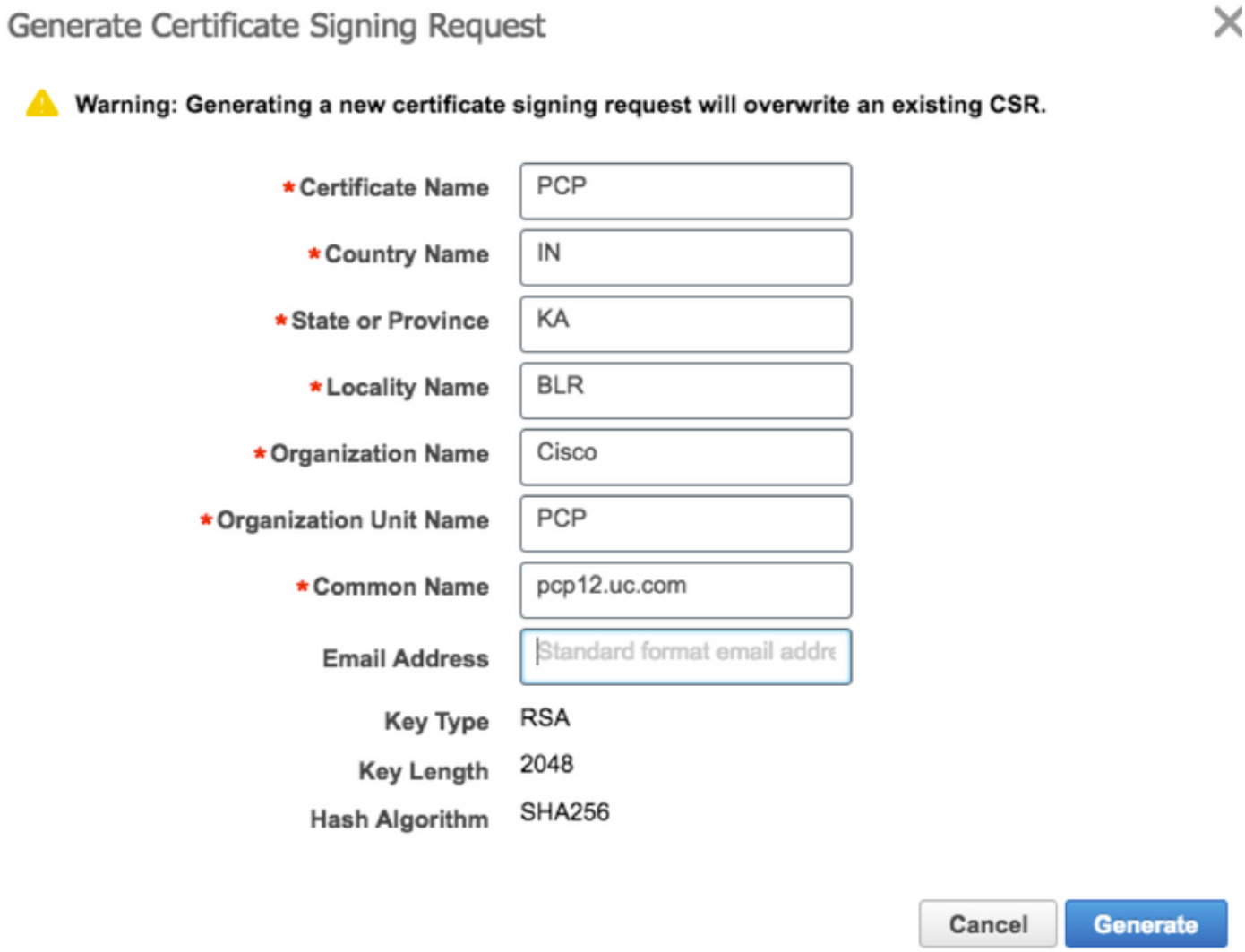
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

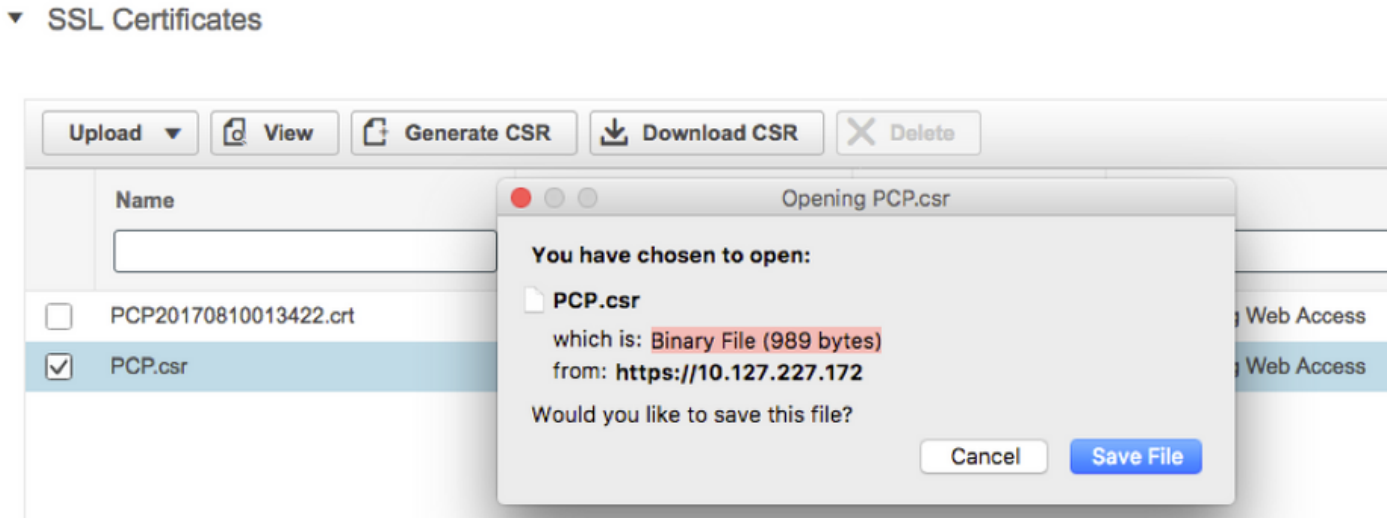
步骤1.登录PCP并导航至Administration > Updates > SSL Certificates部分。

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。



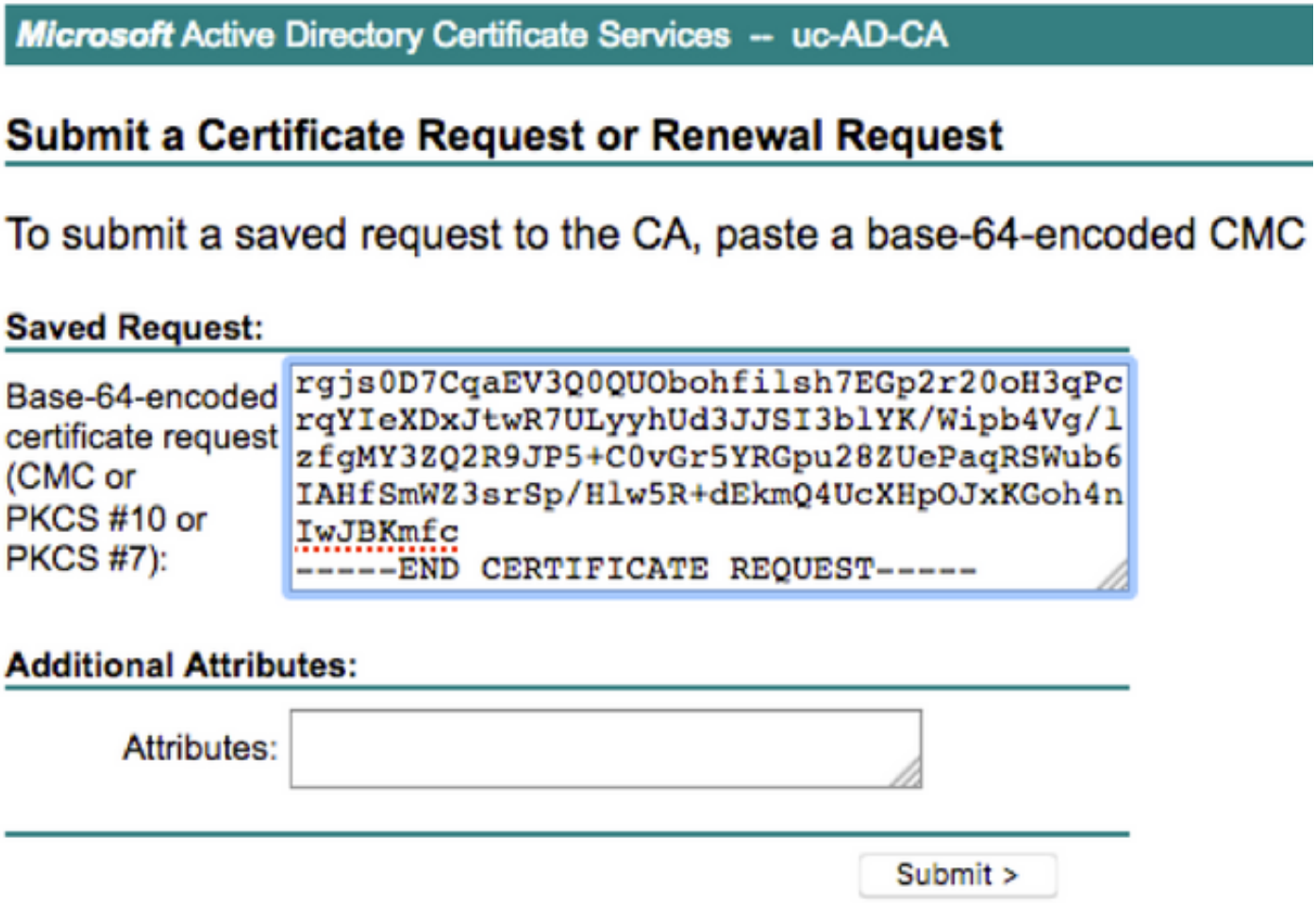
步骤3.单击**Download CSR** 以生成如图所示的证书。



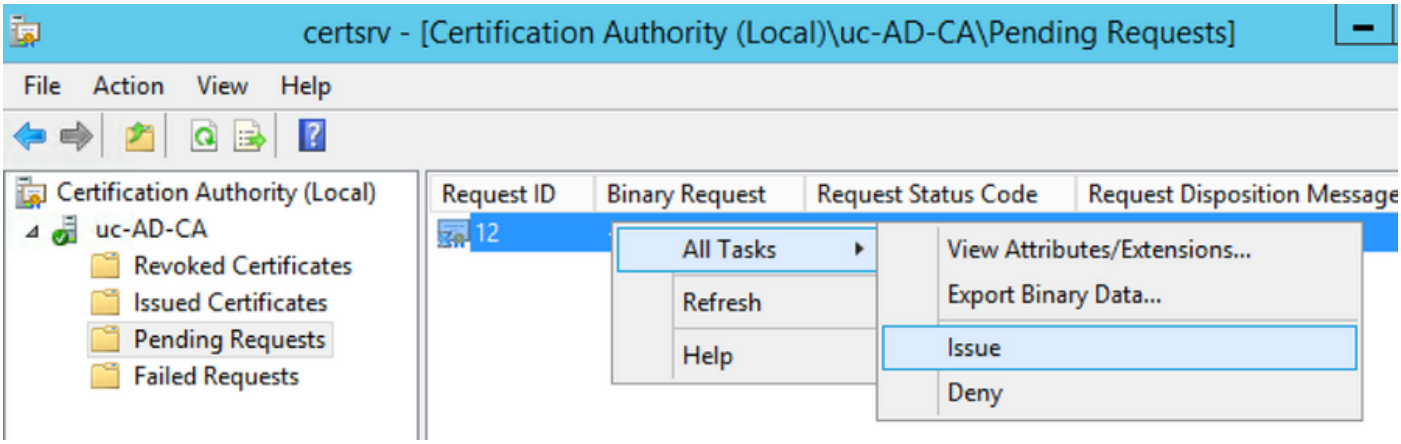
步骤4.使用此证书签名请求(CSR)在公共CA提供商的帮助下生成公共CA签名证书。

如果要使用内部或本地CA签署证书，请执行以下步骤：

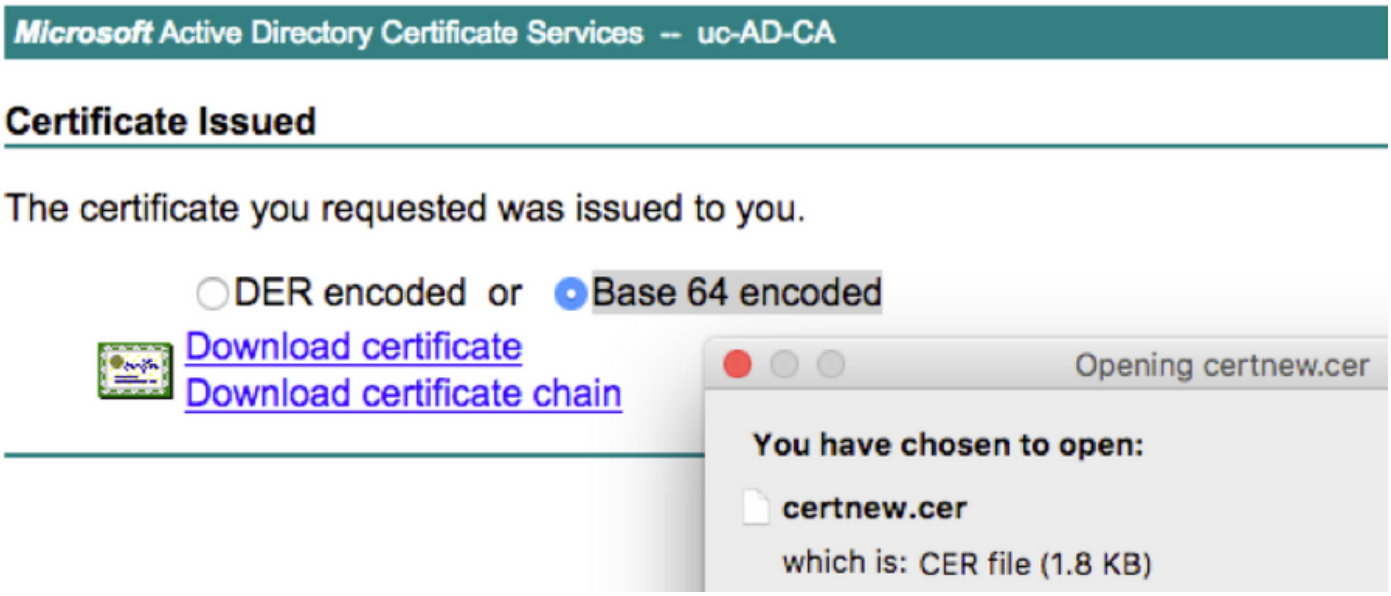
步骤1.登录内部CA并上传CSR，如图所示。



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。



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。

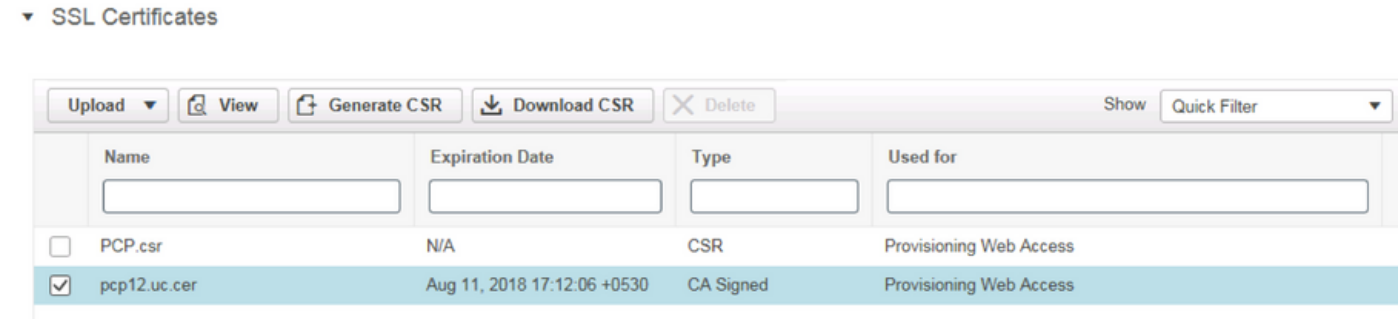
步骤5.上传CA签名证书后，导航到**Administration > Process Management**，然后单击**Restart** Apache(Web Server)Service，如图所示。

验证

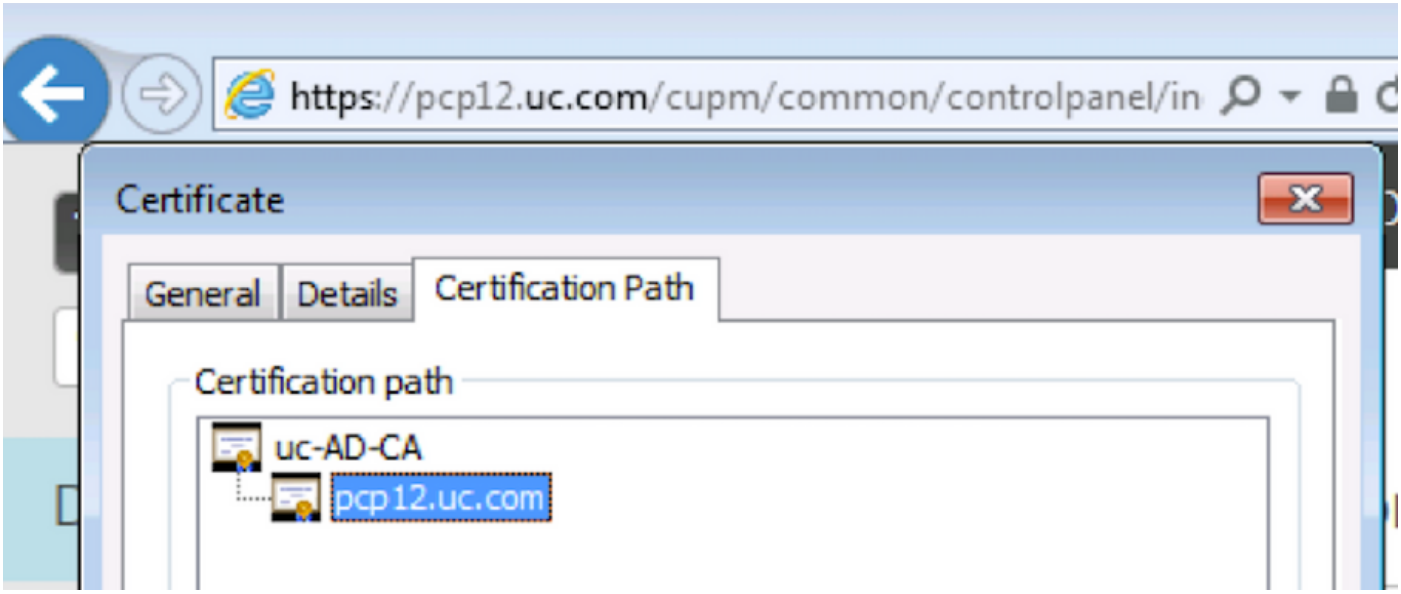
使用本部分可确认配置能否正常运行。

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。



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]