

# Configuración de certificados de servidor de aplicaciones de aprovisionamiento firmado por CA para aprovisionamiento de colaboración Prime

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requisito](#)

[Componentes Utilizados](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento describe el procedimiento para cargar y verificar certificados de servidor de Certificate Authority (CA) - Signed Provisioning Application a Prime Collaboration Provisioning (PCP).

## Prerequisites

### Requisito

Cisco recomienda que tenga conocimiento sobre estos temas:

- PCP y Microsoft Internal CA
- Copia de seguridad de PCP o instantánea de la última máquina virtual (VM) antes de cargar el certificado

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- PCP versión 12.3
- Mozilla Firefox 55.0
- CA interna de Microsoft

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Configurar

Paso 1. Inicie sesión en PCP y navegue hasta **Administración > Actualizaciones > Sección Certificados SSL**.

Paso 2. Haga clic en **Generar solicitud de firma de certificado**, introduzca el atributo obligatorio y haga clic en **Generar** como se muestra en la imagen.

**Nota:** El atributo Common Name debe coincidir con el nombre de dominio completo (FQDN) de PCP.

## Generate Certificate Signing Request

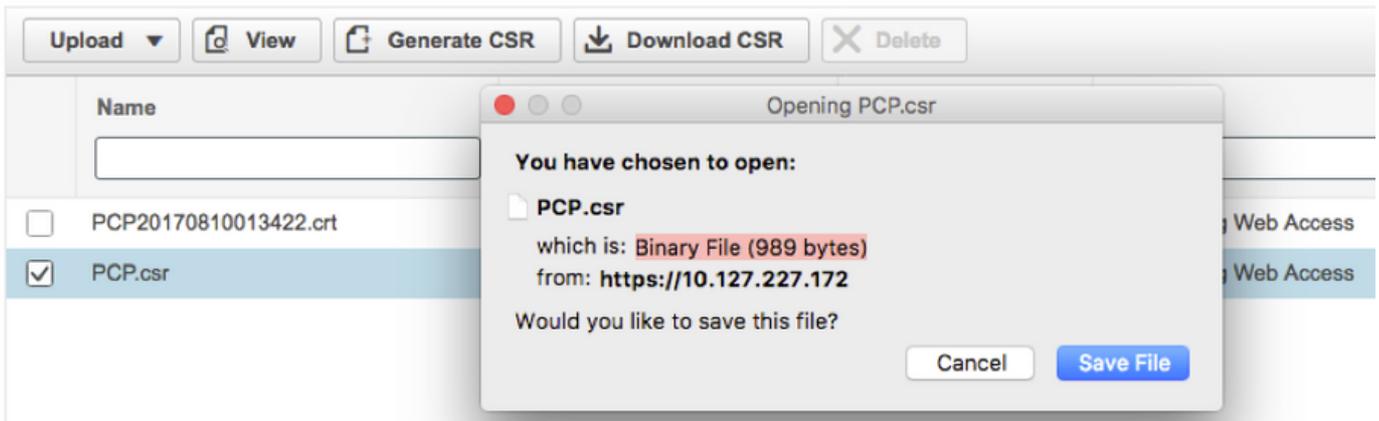


 **Warning: Generating a new certificate signing request will overwrite an existing CSR.**

* 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

Paso 3. Haga clic en **Descargar CSR** para generar el certificado como se muestra en la imagen.

▼ SSL Certificates



Paso 4. Utilice esta solicitud de firma de certificado (CSR) para generar el certificado firmado por la CA pública con la ayuda del proveedor público de la CA.

Si desea firmar el certificado con CA interna o local, siga estos pasos:

Paso 1. Inicie sesión en CA interna y cargue el CSR como se muestra en la imagen.

## 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):

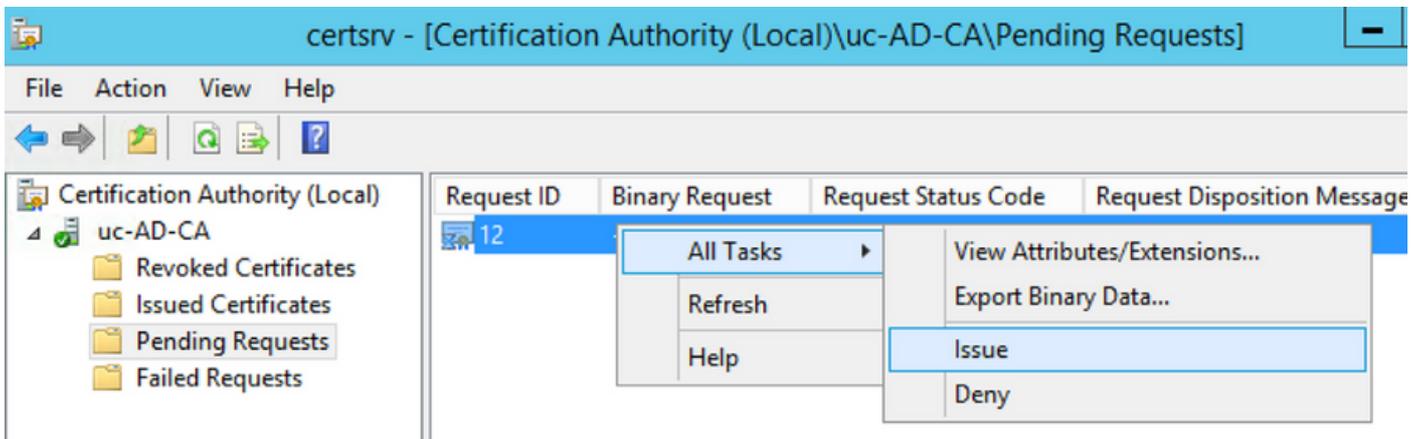
```
rgjs0D7CqaEV3Q0QUObohfilsh7EGp2r20oH3qPc  
rqYIeXDxJtwR7ULyyhUd3JJSI3blYK/Wipb4Vg/l  
zfgMY3ZQ2R9JP5+C0vGr5YRGpu28ZUePaqRSWub6  
IAHfSmWZ3srSp/Hlw5R+dEkmQ4UcXHpOJxKGoh4n  
IwJBKmfC  
-----END CERTIFICATE REQUEST-----
```

#### Additional Attributes:

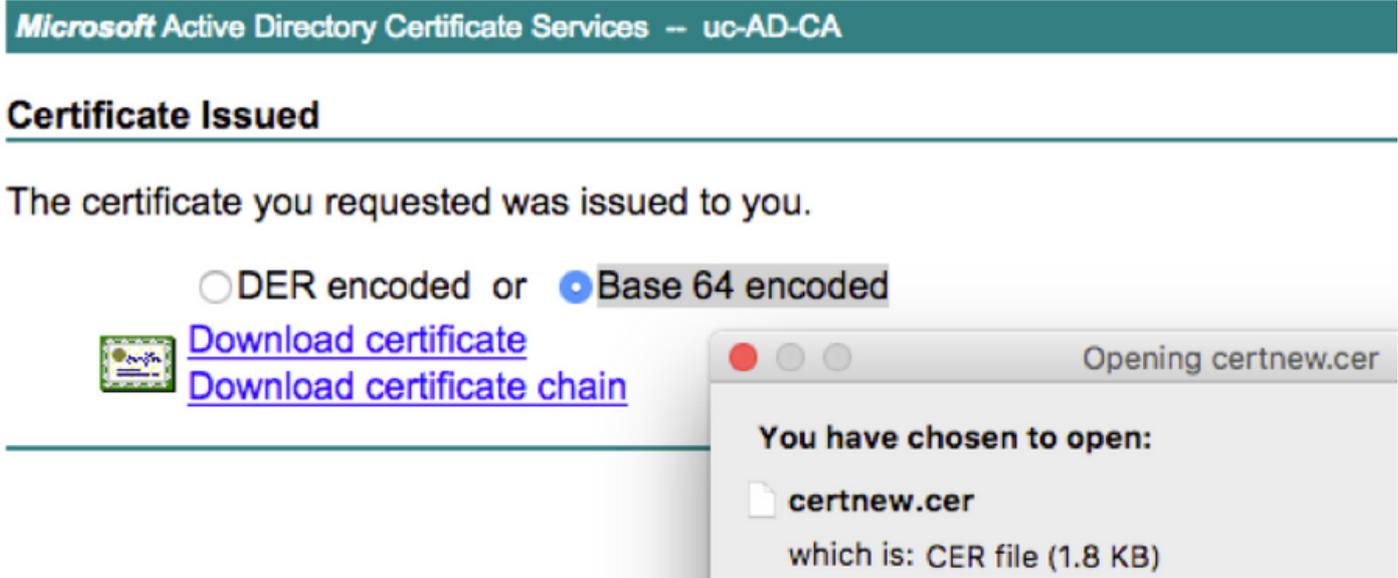
Attributes:

Submit >

Paso 2. Conéctese al servidor interno de la CA, haga clic con el botón derecho en **Solicitudes pendientes** > **Todas las tareas** > Seleccione **Problema** para obtener un certificado firmado como se muestra en la imagen.



Paso 3. A continuación, seleccione el botón de opción **Formato codificado Base 64** y haga clic en **Descargar certificado** como se muestra en la imagen.



Paso 4. En PCP Web GUI, navegue hasta **Administration > Updates > SSL Certificates Section**, haga clic en **Upload**, elija el certificado que se generó y haga clic en **Upload** como se muestra en la imagen.

**Nota:** Solo debe cargar el certificado de servidor Web PCP, no es necesario cargar los certificados raíz, ya que PCP es un servidor de nodo único.

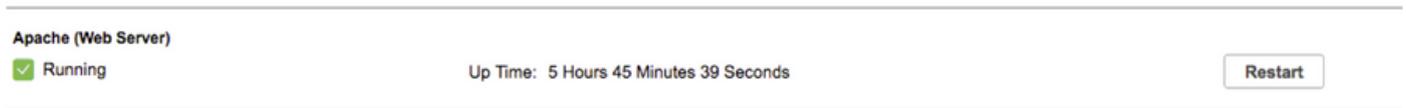
### Upload New Provisioning Certificate

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

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

**Cancel** **Upload**

Paso 5. Después de cargar el certificado firmado por CA, navegue hasta **Administración > Administración de procesos** y haga clic en **Reiniciar** Servicios Apache (Servidor Web) que se muestran en la imagen.



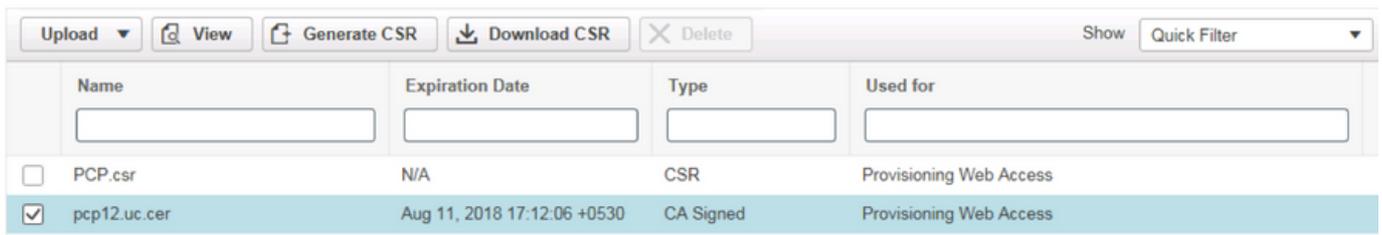
## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Estos son los pasos para verificar que el certificado firmado por CA se carga en el PCP.

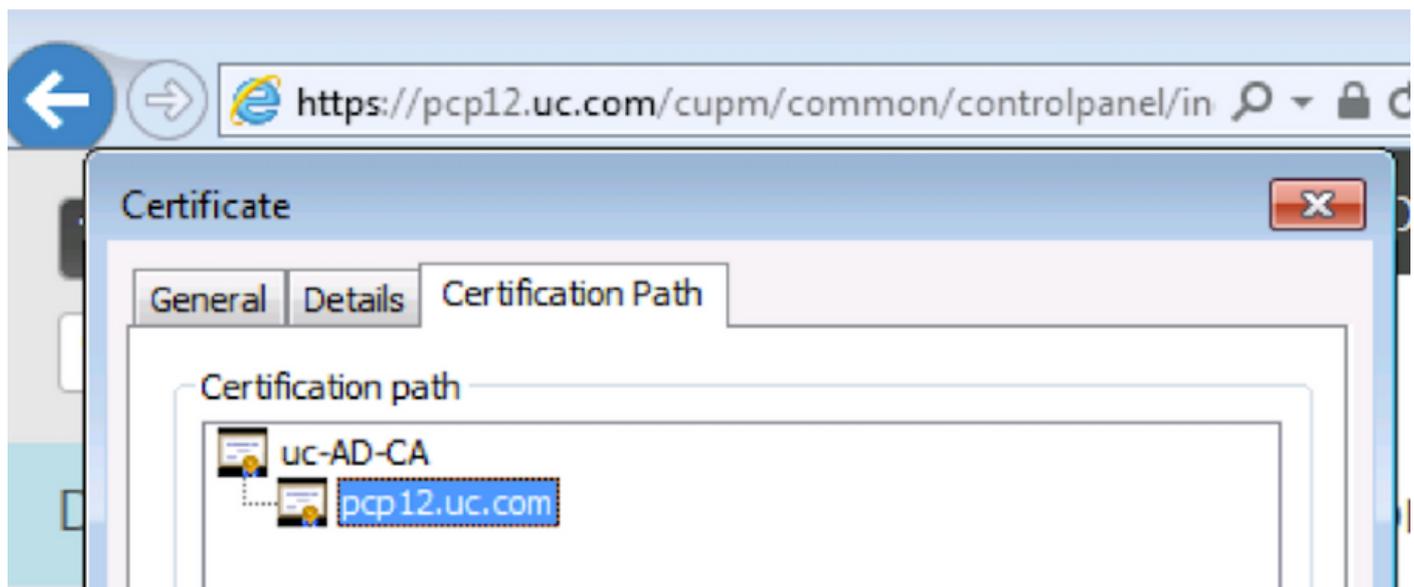
Paso 1. La carga del certificado firmado por la CA reemplaza el certificado autofirmado por el PCP y el tipo se muestra como firmado por la CA con la fecha de vencimiento, como se muestra en la imagen.

### ▼ 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

Paso 2. Inicie sesión en PCP con el uso del FQDN y haga clic en el **símbolo de bloqueo seguro** en el navegador. Haga clic en **Más información** y verifique la **Trayectoria de Certificación** como se muestra en la imagen.



## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su

configuración.

Desde PCP 12.X, no hay acceso a CLI/Secure Shell (SSH) como raíz. Para cualquier problema, para cargar el certificado o no se puede acceder a la interfaz web de PCP después de la carga del certificado, póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC).

## Información Relacionada

- [Aprovisionamiento de Cisco Prime Collaboration](#)
- [Recopilación de registros ShowTech desde la GUI del aprovisionamiento de Prime Collaboration](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)