Configurar certificados do servidor de aplicativos de provisionamento com assinatura CA para o provisionamento Prime Collaboration

Contents

Introduction

Este documento descreve o procedimento para carregar e verificar a autoridade de certificação (CA) - certificados do servidor de aplicativo de provisionamento assinado para o Prime Collaboration Provisioning (PCP).

Prerequisites

Requisito

A Cisco recomenda que você tenha conhecimento destes tópicos:

- PCP e AC interna da Microsoft
- Instantâneo de Máquina Virtual (VM) mais recente ou Backup de PCP antes de carregar o certificado

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- PCP versão 12.3
- Mozilla Firefox 55.0
- AC interna da Microsoft

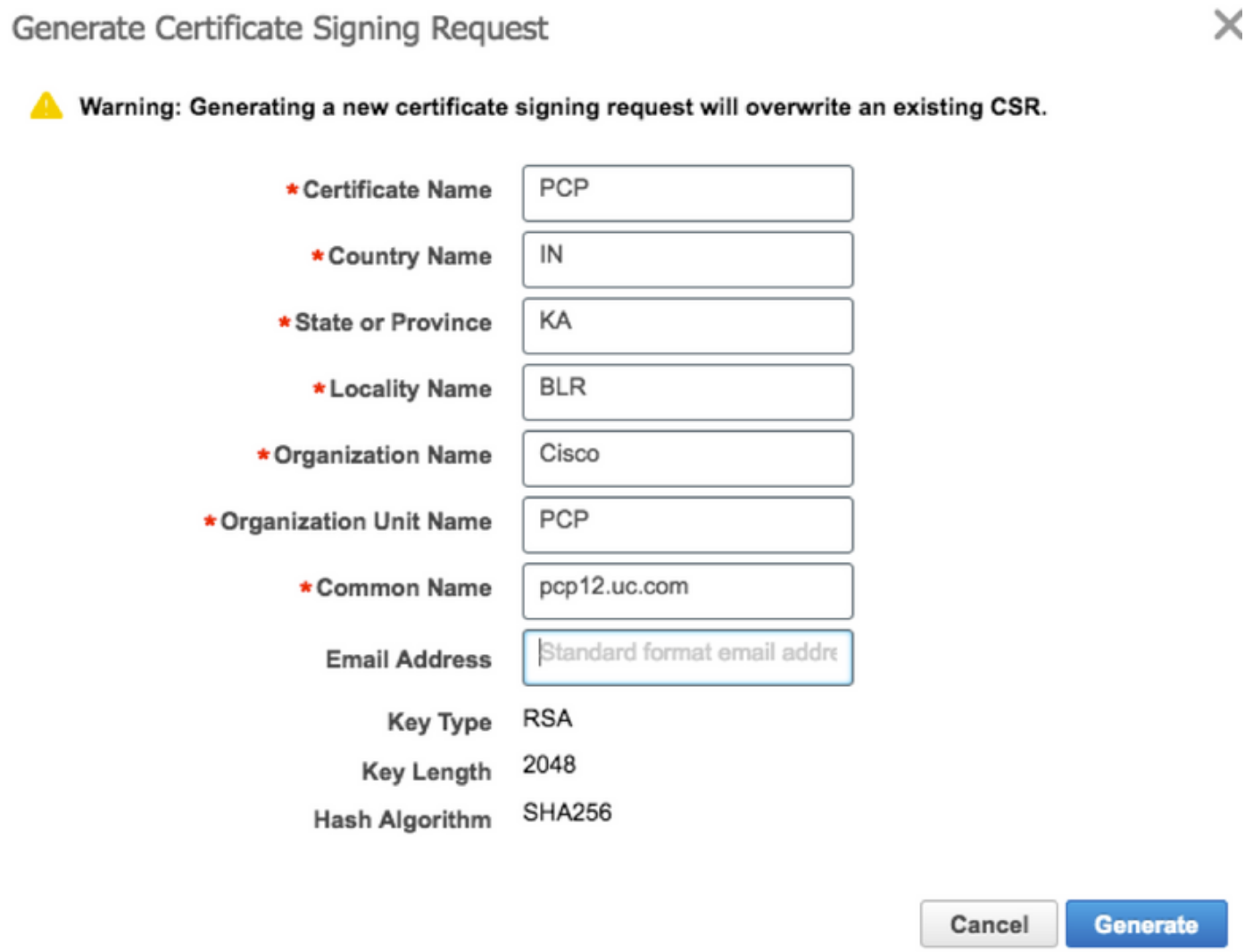
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

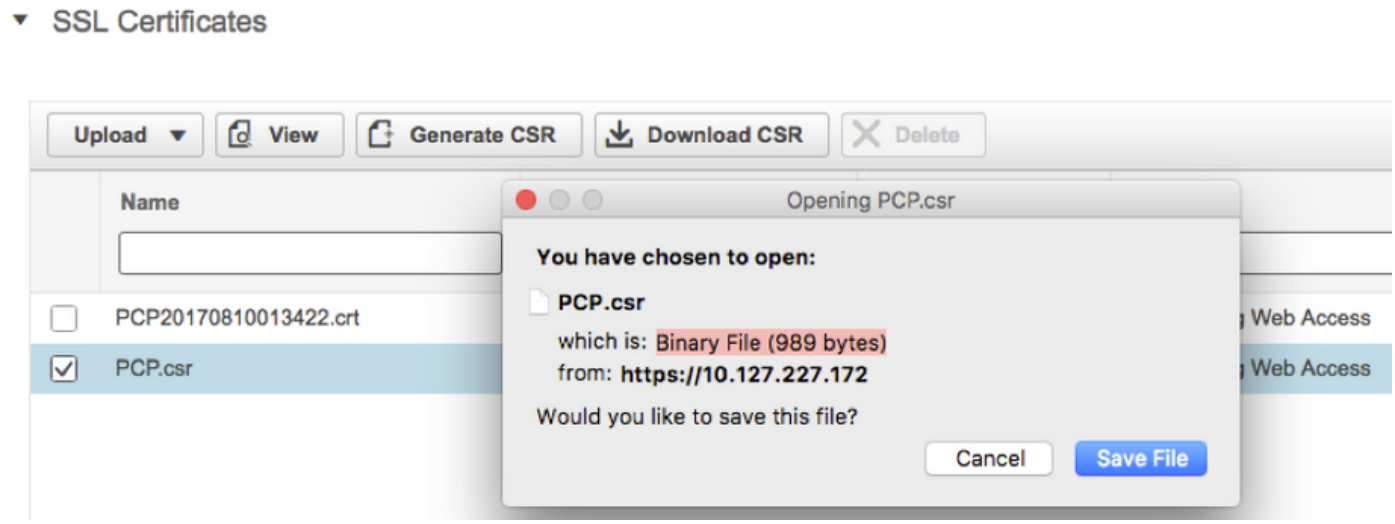
Etapa 1. Efetue login no PCP e navegue para **Administração > Atualizações >** Seção Certificados **SSL**.

Etapa 2. Clique em **Gerar solicitação de assinatura de certificado**, insira o atributo obrigatório e clique em **Gerar** conforme mostrado na imagem.

> **Note**: O atributo Nome Comum deve corresponder ao Nome de Domínio Totalmente Qualificado (FQDN) do PCP.



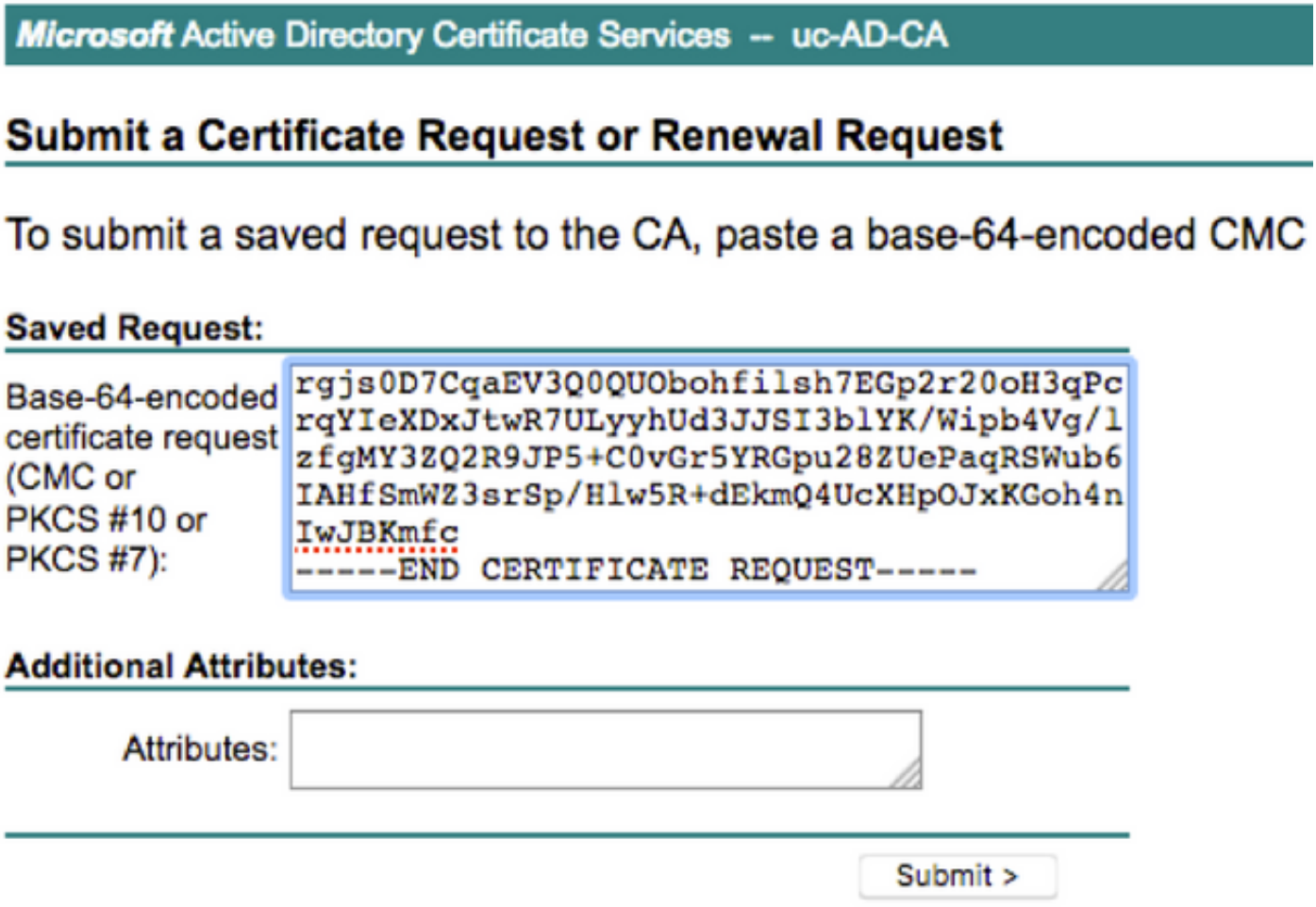
Etapa 3. Clique em **Download CSR** para gerar o certificado conforme mostrado na imagem.



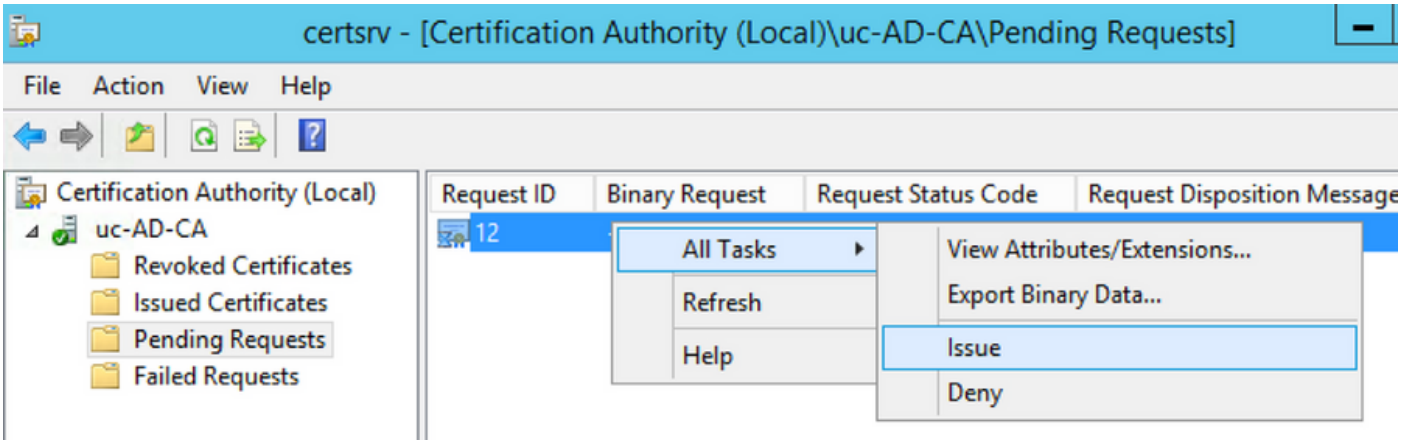
Etapa 4. Use esta Solicitação de Assinatura de Certificado (CSR) para gerar o certificado assinado de CA pública com a ajuda do Provedor de CA público.

Para assinar o certificado com CA interna ou local, siga estas etapas:

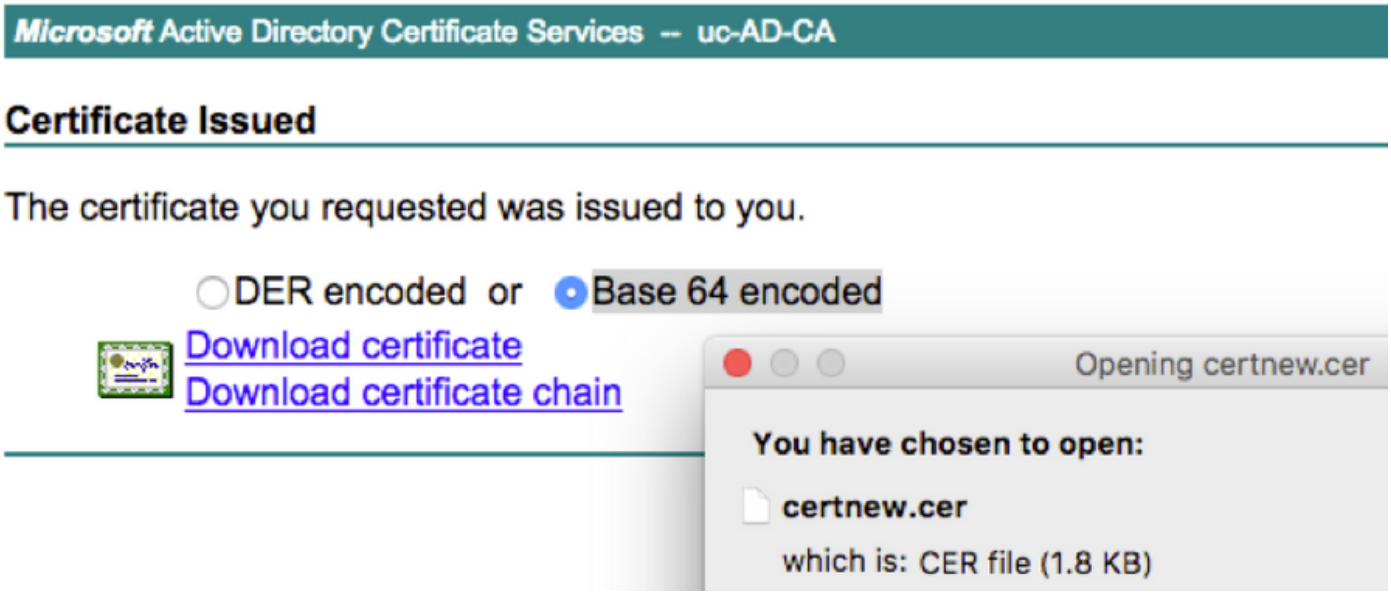
Etapa 1. Faça login na CA interna e carregue o CSR como mostrado na imagem.



Etapa 2. Conecte-se ao servidor CA interno, clique com o botão direito em **Solicitações pendentes > Todas as tarefas >** Selecionar **problema** para obter um certificado assinado conforme mostrado na imagem.



Etapa 3. Em seguida, selecione o botão de opção **Base 64 encoded** format e clique em **Download certificate** conforme mostrado na imagem.



Etapa 4. Na GUI da Web do PCP, navegue para **Administração > Atualizações > Seção Certificados SSL**, clique em **Carregar**, escolha o certificado que foi gerado e clique em **Carregar** como mostrado na imagem.

> **Note**: Você precisa carregar somente o certificado do servidor Web PCP. Os certificados raiz não precisam ser carregados, pois o PCP é um servidor de nó único.

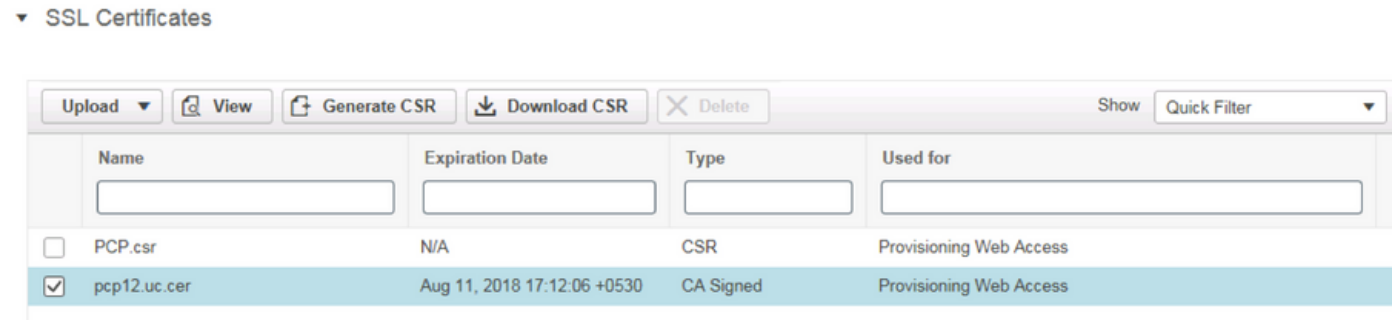
Etapa 5. Depois de carregar o certificado CA-Signed, navegue para **Administration > Process Management** e clique em **Restart** Apache (Web Server) Service, conforme mostrado na imagem.

Verificar

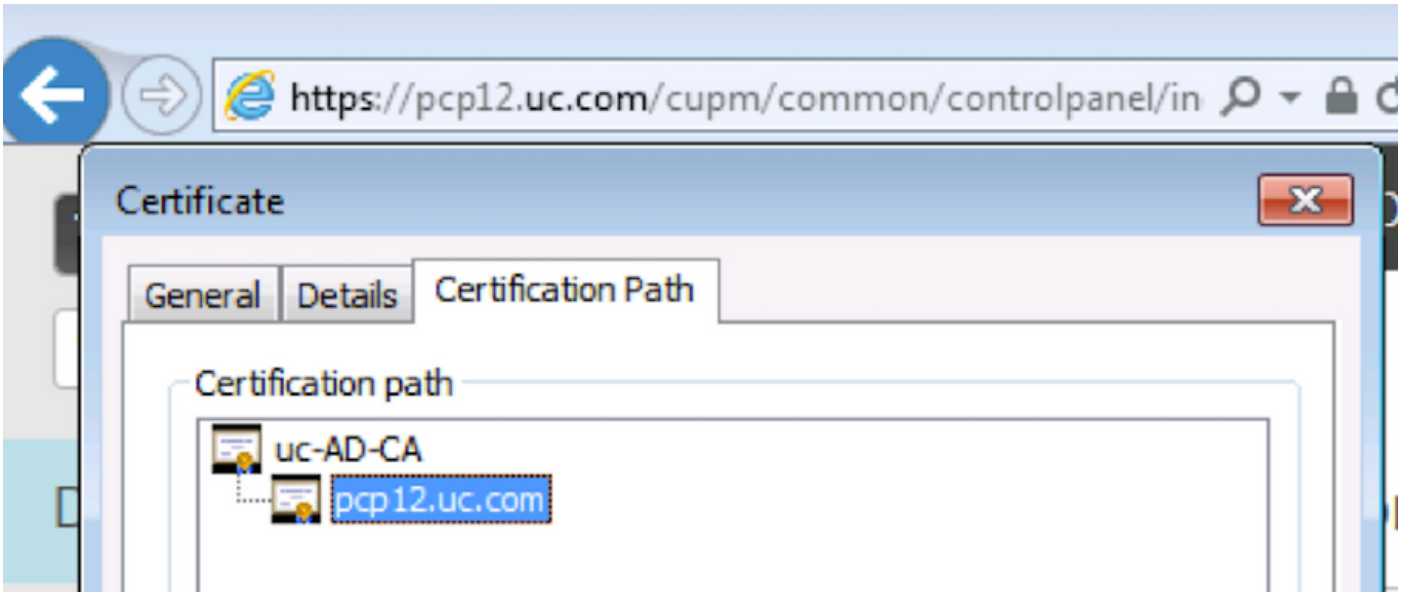
Use esta seção para confirmar se a sua configuração funciona corretamente.

Aqui estão as etapas para verificar se o certificado CA assinado foi carregado para o PCP.

Etapa 1. O carregamento do certificado assinado pela CA substitui o certificado autoassinado PCP e o Tipo é mostrado como CA Assinado com a Data de expiração, como mostrado na imagem.



Etapa 2. Faça login no PCP com o uso do FQDN e clique no **símbolo de bloqueio seguro** no navegador. Clique em **Mais informações** e verifique o **Caminho de certificação** conforme mostrado na imagem.



Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Do PCP 12.X, não há acesso ao CLI/Secure Shell (SSH) como raiz. Em caso de problemas, para fazer o upload do certificado ou se a Interface da Web do PCP não estiver acessível após o upload do certificado, entre em contato com o Cisco Technical Assistance Center (TAC).

Informações Relacionadas

- Provisionamento do Cisco Prime Collaboration
- Coletar registros da ShowTech na GUI do Prime Collaboration Provisioning
- Suporte Técnico e Documentação - Cisco Systems