Generate a CSR With Alternate Name Guide in Prime Collaboration Provisioning (PCP)

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Procedure and Steps
Further Notes

Introduction

This document describes how to generate a Certificate Signing Request (CSR) in the prime provisioning to allow for alternate names.

Prerequisites

Requirements

- A Certificate Authority (CA) will need to sign the certificate you generate from PCP, you can use a Windows server or have a CA sign it online.

If you are unsure how to have your Certificate signed by a CA online resource, please reference the link below

https://www.digicert.com/

- Root Access to the Command Line interface (CLI) of the Prime Provisioning will be needed. Root access is generated upon Install.

> **Note**: For PCP Version(s) 12.X and above please refer to the bottom of this document under Further Notes

Components Used

Prime Collaboration Provisioning

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, ensure that you understand the potential impact of any command.

Background Information

This will allow you to access the Prime Collaboration Provisioning (PCP) for business purposes with multiple Domain Name Server (DNS) entries using the same certificate and not encounter the certificate error when you access the webpage.

Procedure and Steps

At the time of this document wasw written, from the Graphical User interface (GUI) you can only generate the CSR with no alternate name, These are the instructions to accomplish this task.

Step 1. Log in to PCP as the root user

Step 2. Navigate to **/opt/cupm/httpd/** by the input **cd /opt/cupm/httpd/**

Step 3. Type: **vi san.cnf**

> **Note**: This will create a new file called san.cnf which will be empty at the moment

Step 4. Press **I** for insert (this will allow to edit the file) and copy/paste the below in the grey field

Please note as well the entry at the bottom DNS.1 = pcptest23.cisco.ab.edu is the primary DNS entry that will be used for the CSR and DNS.2 will be the secondary; This way you can access PCP and use either of the DNS entries.

After a copy/paste in this example, please remove the pcptest examples with the ones you need for your application.

```
[ req ] default_bits = 2048 distinguished_name = req_distinguished_name req_extensions = req_ext [
req_distinguished_name ] countryName = Country Name (2 letter code) stateOrProvinceName = State or Province Name
(full name) localityName = Locality Name (eg, city) organizationName = Organization Name (eg, company) commonName =
Common Name (e.g. server FQDN or YOUR name) [ req_ext ] subjectAltName = @alt_names [alt_names] DNS.1 =
pcptest23.cisco.ab.edu DNS.2 = pcptest.gov.cisco.ca
```

Step 5. Type: **esc** then type **:wq!** (this will save the file and the changes just made).

Step 6. Restart services for the config file to take affect properly. Type: **/opt/cupm/bin/cpcmcontrol.sh stop**

type **/opt/cupm/bin/cpcmcontrol.sh status** to ensure all services have stopped

Step 7. Type this command to allow the services to come back up: **/opt/cupm/bin/cpcmcontrol.sh start**

Step 8. You should still be in the **/opt/cupm/httpd/** directory, you can type **pwd** to find your current directory to make sure.

Step 9. Run this command to generate the Private key and CSR.

openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout PCPSAN.key -config san.cnf

```
[root@ryPCP11-5 httpd]# openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout private.key -config san.cnf
Generating a 2048 bit RSA private key .........+++ .........+++ writing new private key to 'private.key' ----- You
are about to be asked to enter information that will be incorporated into your certificate request. What you are
about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some
blank For some fields there will be a default value, If you enter '.', the field will be left blank. ----- Country
Name (2 letter code) []:US State or Province Name (full name) []:TX Locality Name (eg, city) []:RCDN Organization
Name (eg, company) []:CISCO Common Name (e.g. server FQDN or YOUR name) []:doctest.cisco.com [root@ryPCP11-5 httpd]#
```

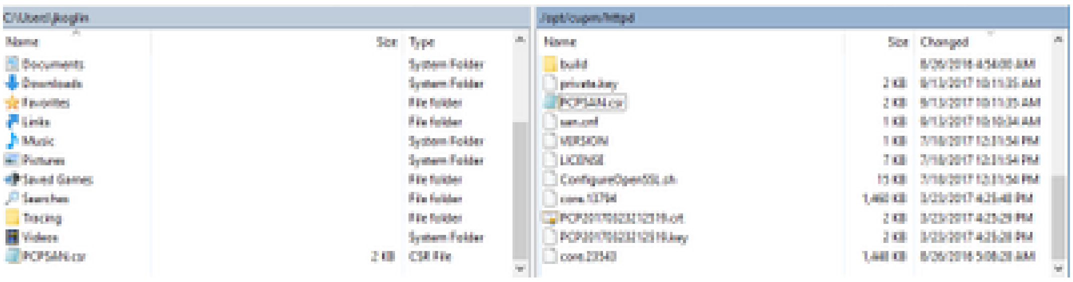
The CSR gets generated and to verify if the CSR contains the correct Alternate names type this command

openssl req -noout -text -in PCPSAN.csr | grep DNS

```
[root@ryPCP11-5 httpd]# openssl req -noout -text -in PCPSAN.csr | grep DNS DNS:pcptest23.cisco.ab.edu,
DNS:pcptest.gov.cisco.ca [root@ryPCP11-5 httpd]#
```

> **Note**: If the DNS entries are the same as shown below step 4, you should see the same as you entered in step 4. After you verify it, proceed to next step

Step 10. Use a program called winscp or filezilla connect to PCP as the root user and navigate to the **/opt/cupm/httpd/** directory and move the .csr from the PCP server to your desktop.



C:\Users\jkoglin

Name	Size	Type
Documents		System Folder
Downloads		System Folder
Favorites		File folder
Links		File folder
Music		System Folder
Pictures		System Folder
Saved Games		File folder
Searches		File folder
Tracing		File folder
Videos		System Folder
PCPSAN.csr	2 KB	CSR File

/opt/cupm/httpd

Name	Size	Changed
build		8/26/2016 4:54:00 AM
private.key	2 KB	9/13/2017 10:11:35 AM
PCPSAN.csr	2 KB	9/13/2017 10:11:35 AM
san.cnf	1 KB	9/13/2017 10:10:34 AM
VERSION	1 KB	7/18/2017 12:21:54 PM
LICENSE	7 KB	7/18/2017 12:21:54 PM
ConfigureOpenSSL.sh	15 KB	7/18/2017 12:21:54 PM
core.13794	1,460 KB	3/23/2017 4:25:48 PM
PCP20170323212519.crt	2 KB	3/23/2017 4:25:29 PM
PCP20170323212519.key	2 KB	3/23/2017 4:25:28 PM
core.23540	1,440 KB	8/26/2016 5:08:28 AM

Step 11. Sign the CSR with your CA and either use a windows server or online via a third party vendor such as DigiCert.

Step 12. Install the PCP Certificate in the Gui, Navigate: **Administration>Updates>SSL Certificates.**

Step 13. Install the certificate through your browser, references per browser is as below.

Google Chrome:

https://www.tbs-certificates.co.uk/FAQ/en/installer_certificat_client_google_chrome.html

Internet Explorer:

http://howtonetworking.com/Internet/iis8.htm

https://support.securly.com/hc/en-us/articles/206082128-Securly-SSL-certificate-manual-install-in-Internet-Explorer

Mozilla Firefox:

https://wiki.wmtransfer.com/projects/webmoney/wiki/Installing_root_certificate_in_Mozilla_Firefox

Step 14. After you install the certificate on the server and your browser, clear the cache and close out of the browser.

Step 15. Re-open the url and you should not encounter the security error.

Further Notes

> Note: PCP version 12.x and above you need TAC to provide you with the CLI Access as this is restricted.

Process to request CLI Access

Step 1. Log in to PCP GUI

Step 2. Navigate to **Administration>Logging and Showtech>Click on troubleshooting account>create the userid** and select an appropriate time you will need root access to accomplish this.

Step 3. Provide to TAC the challenge string and they will provide you the password (this password will be very lengthy, do not worry it will work).

```
Example:
AQAAAAEAAAC8srFZB2prb2dsaW4NSm9zZXBoIEtvZ2xpbgAAAbgBAAIBAQIABAAA FFFFEBE0
AawDAJEEAEBDTj1DaXNjb1N5c3RlbXM7T1U9UHJpbWVDb2xsYWJvcmF0aW9uUHJv FFFFEB81
dmlzaW9uaW5nO089Q2lzY29TeXN0ZW1zBQAIAAAAAFmxsrwGAEBDTj1DaXNjb1N5 FFFFEB8A
c3RlbXM7T1U9UHJpbWVDb2xsYWJvcmF0aW9uUHJvdmlzaW9uaW5nO089Q2lzY29T FFFFEAD0
eXN0ZW1zBwABAAgAAQEJAAEACgABAQsBAJUhvhhxkM6YNYVFRPT3jcqAsrl/1ppr FFFFEB2B
yr1AYzJa9FtO1A4l8VBlp8IVqbqHrrCAIYUmVXWnzXTuxtWcY2wPSsIzW2GSdFZM FFFFE9F3
LplEKeEX+q7ZADshWeSMYJQkY7I9oJTfD5P4QE2eHZ2opiiCScgf3Fii6ORuvhiM FFFFEAD9
kbbO6JUguABWZU2HV0OhXHfjMZNqpUvhCWCCIHNKfddwB6crb0yV4xoXnNe5/2+X FFFFEACE
7Nzf2xWFaIwJOs4kGp5S29u8wNMAIb1t9jn7+iPg8Rezizeu+HeUgs2T8a/LTmou FFFFEA8F
Vu9Ux3PBOM4xIkFpKa7provli1PmIeRJodmObfS1Y9jgqb3AYGgJxMAMAAFB6w== FFFFEAA7
DONE.
```

Step 4. Logout of your current user and login with the userid you created and the password provided by TAC.

Step 5. Navigate to **Troubleshooting Account>>Launch>>Click on Console Account** and create your cli user id and password.

Step 6. Now login to PCP as the user you created and perform the initial steps decribed in this document.

> Note: PCP version 12.x and above you need to input in the command **sudo** prior to all instructions for it to work. For step 9, the command therefore will be **sudo openssl req -out PCPSAN.csr -newkey rsa:2048 -nodes -keyout PCPSAN.key -config san.cnf.** To verify the dns you then would use the command **sudoopenssl req -noout -text -in PCPSAN.csr | grep DNS**