

Prime Collaboration ProvisioningへのCA署名付きProvisioning Application Server証明書の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Certificate Authority(CA)-Signed Provisioning Applicationサーバ証明書をPrime Collaboration Provisioning(PCP)にアップロードして確認する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- PCPおよびMicrosoft内部CA
- 証明書をアップロードする前の最新の仮想マシン(VM)スナップショットまたはPCPバックアップ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- PCPバージョン12.3
- Mozilla Firefox 55.0
- Microsoft内部CA

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

ステップ1:PCPにログインし、[Administration] > [Updates] > [SSL Certificates]セクションに移動

します。

ステップ2：図に示すように、[Generate Certificate Signing Request]をクリックし、必須属性を入力して[Generate]をクリックします。

注：共通名属性は、PCP完全修飾ドメイン名(FQDN)と一致する必要があります。

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

ステップ3：図に示すように、[Download CSR]をクリックして証明書を生成します。

▼ SSL Certificates

The screenshot shows a web interface with a toolbar containing buttons for 'Upload', 'View', 'Generate CSR', 'Download CSR', and 'Delete'. Below the toolbar is a table with two columns: 'Name' and a checkbox. The table contains two entries: 'PCP20170810013422.crt' (unchecked) and 'PCP.csr' (checked). A dialog box titled 'Opening PCP.csr' is overlaid on the table, displaying the message: 'You have chosen to open: PCP.csr which is: Binary File (989 bytes) from: https://10.127.227.172 Would you like to save this file?'. The dialog box has 'Cancel' and 'Save File' buttons.

ステップ4：この証明書署名要求(CSR)を使用して、パブリックCAプロバイダーの助けを借りてパブリックCA署名付き証明書を生成します。

内部CAまたはローカルCAで証明書に署名する場合は、次の手順を実行します。

ステップ1：内部CAにログインし、図に示すようにCSRをアップロードします。

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):

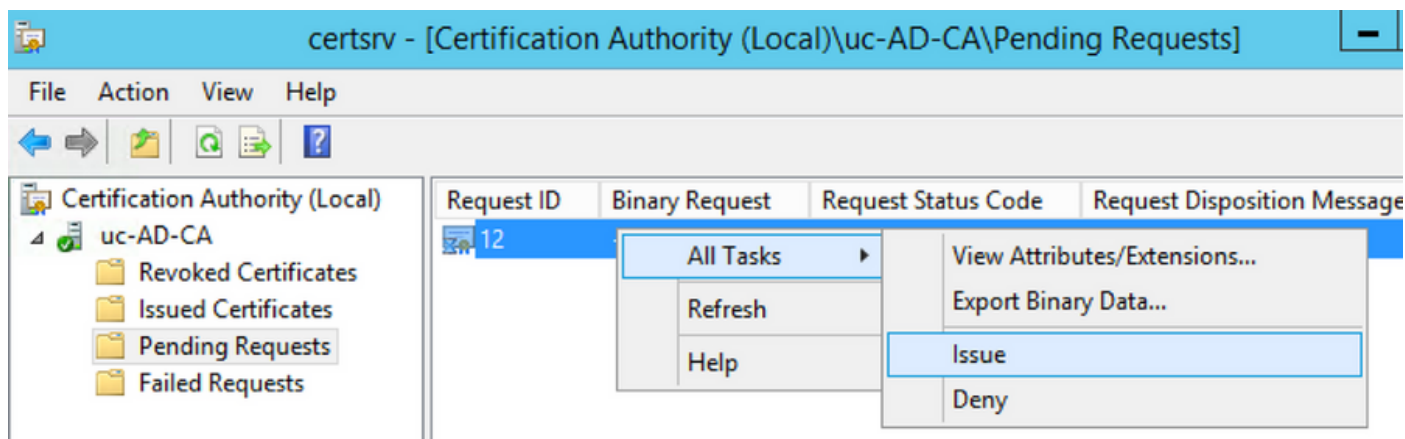
```
rgjs0D7CqaEV3Q0QUObohfilsh7EGp2r20oH3qPc
rqYIeXDxJtwR7ULyyhUd3JJSI3blYK/Wipb4Vg/l
zfgMY3ZQ2R9JP5+C0vGr5YRGpu28ZUePaqRSWub6
IAHfSmWZ3srSp/Hlw5R+dEkmQ4UcXHpOJxKGoh4n
IwJBKmfC
-----END CERTIFICATE REQUEST-----
```

Additional Attributes:

Attributes:

Submit >

ステップ2：内部CAサーバに接続し、図に示すように、[Pending Requests] > [All Tasks] > [Select Issue]を右クリックして署名付き証明書を取得します。



ステップ3：次に、オプションボタン[Base 64 encoded format]を選択し、図に示すように[Download certificate]をクリックします。

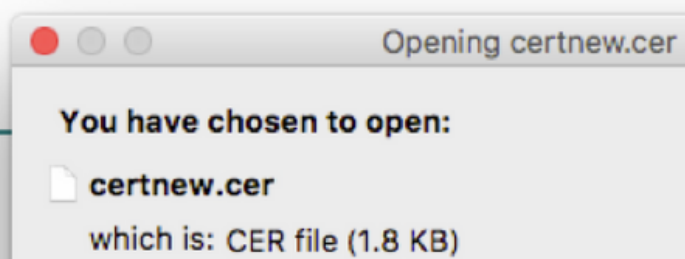
Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



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



ステップ4:PCP Web GUIで、[Administration] > [Updates] > [SSL Certificates Section]に移動し、[Upload]をクリックし、生成された証明書を選択して、図に示すように[Upload]をクリックします。

注：PCP Webサーバ証明書のみをアップロードする必要があります。PCPはシングルノードサーバであるため、ルート証明書をアップロードする必要はありません。

Upload New Provisioning Certificate



Restart all processes to activate new SSL certificate.

certnew.cer .cer or .crt file type required

Cancel

Upload

ステップ5:CA署名付き証明書をアップロードした後、[Administration] > [Process Management]に移動し、図に示す[Restart Apache (Web Server) Services]をクリックします。

Apache (Web Server)

Running

Up Time: 5 Hours 45 Minutes 39 Seconds

確認

ここでは、設定が正常に機能しているかどうかを確認します。

CA署名付き証明書がPCPにアップロードされていることを確認する手順を次に示します。

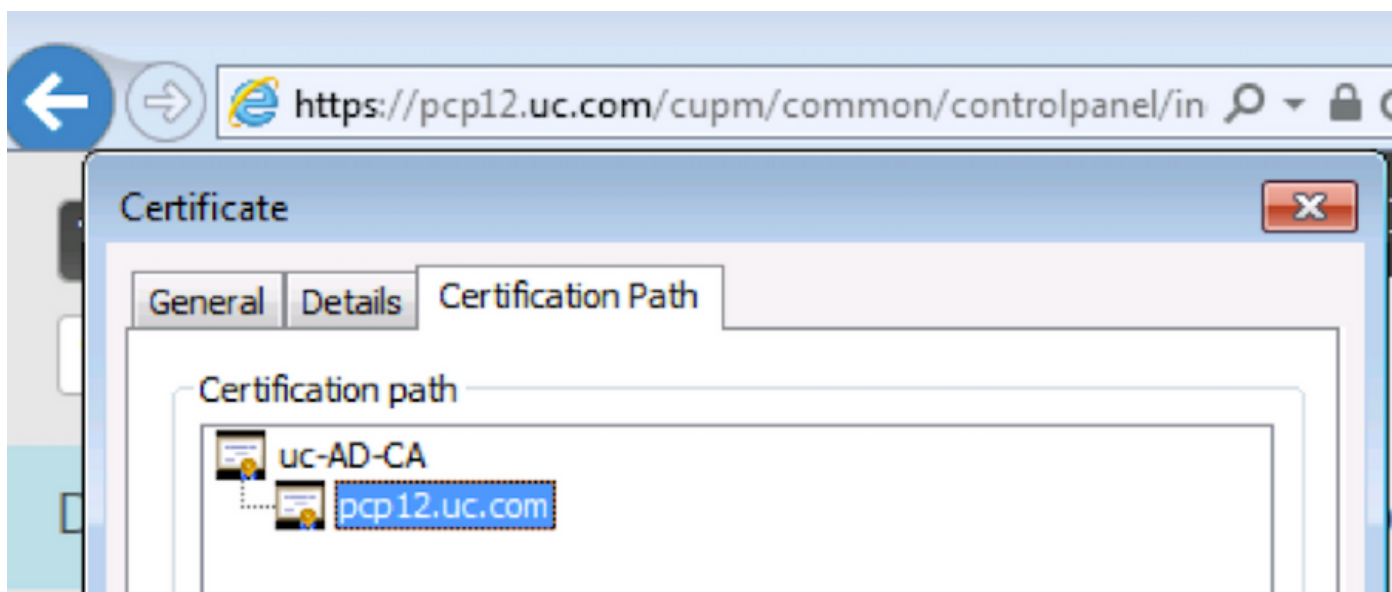
ステップ1:CA署名付き証明書のアップロードによってPCP自己署名証明書が置き換えられ、図に

示すように、[Type]は[CA Signed with the Expiration Date]と表示されます。

▼ 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

ステップ2:FQDNを使用してPCPにログインし、ブラウザでセキュリックスymbolをクリックします。[詳細]をクリックし、図に示すように[Certification Path]を確認します。



トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

PCP 12.Xから、rootとしてCLI/Secure Shell(SSH)にアクセスできません。証明書のアップロード後に証明書をアップロードするか、PCP Webインターフェイスにアクセスできない問題については、Cisco Technical Assistance Center(TAC)にお問い合わせください。

関連情報

- [Cisco Prime Collaboration Provisioning](#)
- [Prime Collaboration Provisioning の GUI から ShowTech のログの収集](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)