# Replacing the Self-Signed SSL Certificate in PowerChute Business Edition versions 10.0.2 and above - Linux

**NOTE:** The following steps require Administrator access.

Inform PowerChute of keystore password change

1. Stop the PowerChute daemon via the services console or using the command `service pbeagent stop` or `systemctl stop PBEAgent.service`
2. Navigate to the installation directory and open the pcbeconfig.ini file under the agent directory. By default, this is located at /opt/APC/PowerChuteBusinessEdition/Agent/pcbeconfig.ini
3. In the `[Credentials]` section, add the line `KS_Access_Data =` **`<new password>.`** **<new password>** can be replaced with a password of your choice. It must be at least 6 characters in length. Save the INI file.
   **NOTE:** The `KS_Access_Data` value must match the keystore password provided in step 4 of "Create a new Keystore for the trusted SSL cert".

```
[Credentials]
KS_Access_Data = <new password>
```

4. Start the PowerChute daemon via the services console or using the command `service pbeagent start` or `systemctl start PBEAgent.service`. This ensures PowerChute stores the password in memory before you remove the keystore itself.

## Create a new Keystore for the trusted SSL cert

1. Stop the PowerChute service.
2. Delete the existing keystore file. By default, this is located at /opt/APC/PowerChuteBusinessEdition/Agent/keystore
3. Open a command prompt and change the directory to agent, e.g.

```
cd /opt/APC/PowerChuteBusinessEdition/Agent/
```

4. Create a new keystore and private key. Use the same password that was specified in step 3 of "Inform PowerChute of keystore password change".
   **NOTE:** The "first and last name" specified must match the hostname or FQDN (Fully Qualified Domain Name) of the server where PowerChute is installed. For example: localhost. The confirmation response (yes or no) is locale specific, so it expects the answer in the same language as the question.

```
[root@localhost Agent]# ../jre/bin/keytool -genkey -alias securekey -keyalg RSA -
keystore keystore -keysize 2048
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  localhost
What is the name of your organizational unit?
  [Unknown]:  PowerChute Business Edition
What is the name of your organization?
  [Unknown]:  SE
What is the name of your City or Locality?
  [Unknown]:  Galway
What is the name of your State or Province?
  [Unknown]:  Galway
What is the two-letter country code for this unit?
  [Unknown]:  IE
Is CN=localhost, OU=PowerChute Business Edition, O=SE, L=Galway, ST=Galway, C=IE
correct?
  [no]:  yes
```

```
Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with
a validity of 90 days
     for: CN=localhost, OU=PowerChute Business Edition, O=SE, L=Galway, ST=Galway,
C=IE
```

5. You can verify that the file 'keystore' now exists in the agent folder. The following command lists the contents of the keystore:

```
[root@localhost Agent]# ../jre/bin/keytool -list -v -keystore keystore -storepass <new
password>
```

   The keytool generates a self-signed cert from the private key. This can be updated with a signed CA cert later if required.

6. PowerChute can be restarted at this point while you create a CSR and get it signed.

## Create a Certificate Signing Request (CSR)

Use keytool to create a CSR from the private key and self-signed cert in the keystore. You will be prompted to enter the keystore password:

```
[root@localhost Agent]# ../jre/bin/keytool -certreq -alias securekey -keystore keystore -
file pcbe.csr
```

## Create a new SSL cert signed by a Trusted CA

Use the .CSR file to create a new certificate signed by the Trusted CA. This process will usually be done by a CA and depends on the Trusted CA software being used. The CA may need to contact you, or you may need to install certain software, to verify your authenticity.

## Import the Root CA and Web Server SSL certs to the PowerChute Keystore

The output of the CA signing should be the CA root cert, and a signed cert for PowerChute based on the CSR. This section assumes certs have been generated by OpenSSL. If the certs returned from a third-party CA are not in a format compatible with the Java keystore, you may have to convert them. For example, you may need to bundle both CA and your signed certificate into a p.12 file.

1. Copy the CA cert and PowerChute host cert signed by the CA to the PowerChute Agent directory.
2. Stop the PowerChute service if necessary.
3. Open a command prompt and change the directory to agent. By default, /opt/APC/PowerChuteBusinessEdition/Agent/
4. Import the root CA cert to the Java keystore. You will be prompted to enter your password.
5. Enter the new keystore password, then confirm you trust the cert.

```
[root@localhost Agent]# ../jre/bin/keytool -import -trustcacerts -alias root -file
ca.crt -keystore keystore
Enter keystore password:

<certificate information displayed here>

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

6. Import the PowerChute Web Server SSL cert signed by the CA to the Java keystore:

```
[root@localhost Agent]# ../jre/bin/keytool -import -trustcacerts -alias securekey -
file pcbe.crt -keystore keystore
Enter keystore password:
Certificate reply was installed in keystore
```

# Import the CA cert into the Trusted Root Certification Authorities

Import the root CA cert so that the web browser will be able to confirm that the PowerChute cert was indeed signed by the specified CA.

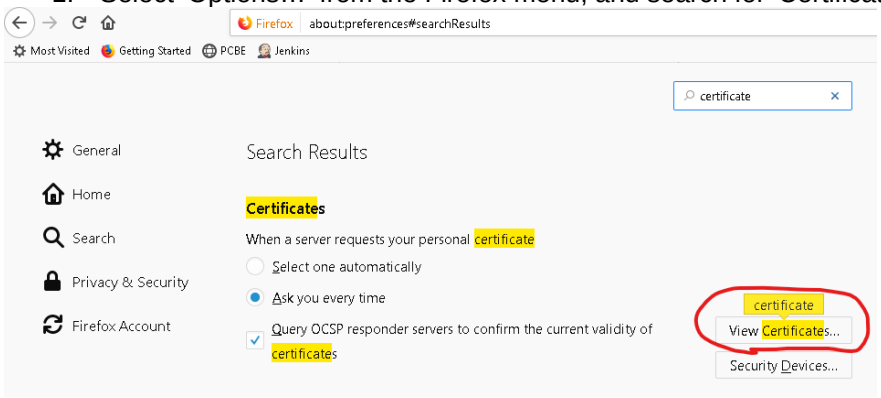
**Internet Explorer and Chrome**

1. Double-click on the root CA cert and click 'Install Certificate' to start the Certificate Import Wizard.
2. Select 'Local Machine'.
3. Select 'Place all certificates in the following store' and click the 'Browse' button.
4. Select the Trusted Root Certification Authorities folder and click 'OK'.
5. Click 'Next'.
6. Click 'Finish'.

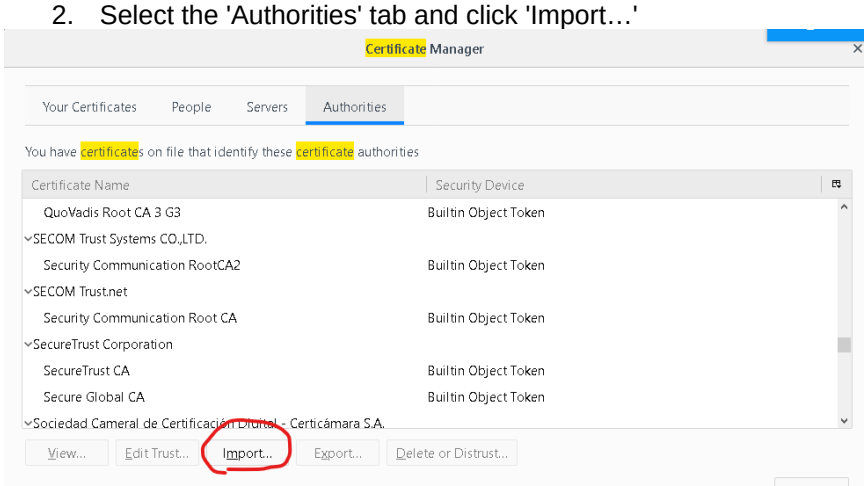
**Firefox**

Firefox has its own trusted cert store.

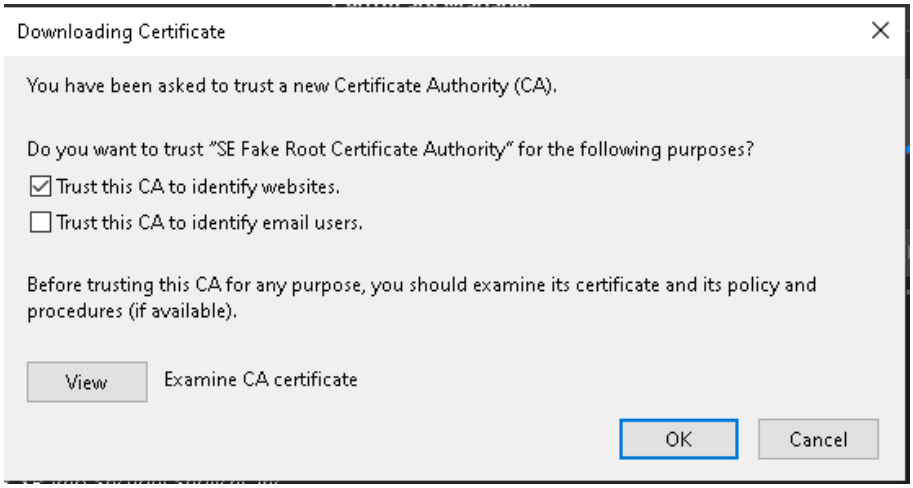
1. Select ‘Options…’ from the Firefox menu, and search for 'Certificates':



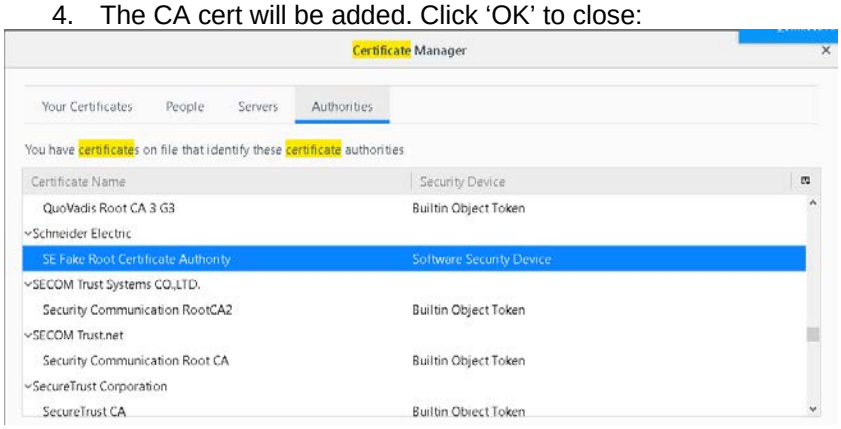

2. Select the 'Authorities' tab and click 'Import…'




3. Select the CA cert and add to 'Trust this CA to identify websites'.




4. The CA cert will be added. Click 'OK' to close:




**NOTE:** Some versions of Firefox have issues deleting older certificates from the same CA. If you need to replace a CA cert, you need to ensure it is overwritten correctly, or reinstall Firefox before deleting an existing cert. See https://support.mozilla.org/bm/questions/1272865 for more details.

## Start PowerChute

Start the PowerChute daemon via the services console or using the command `service pbeagent start` or `systemctl start PBEAgent.service`

PowerChute should be using the new signed certificate and there should not be an SSL cert security warning displayed by the browser when the PowerChute Web Interface is launched.