Receiving and importing Let's Encrypt SSL certificate

Let’s Encrypt is a certification center that automatically issues free cryptographic certificates. You can receive and import such a certificate to your WCS server as described below:

1. Run the tool to get a certificate that is shipped with WCS

```
cd /usr/local/FlashphonerWebCallServer/tools
./certbot-auto certonly
```

This will install all necessary dependencies, and the certbot tool starts. In response to the query enter:

- the domain name of your server, for example, yourdomain;
- a method to install and verify certificates: if a web server is running on your server select webroot then specify the root folder path of the server. Otherwise, select standalone.

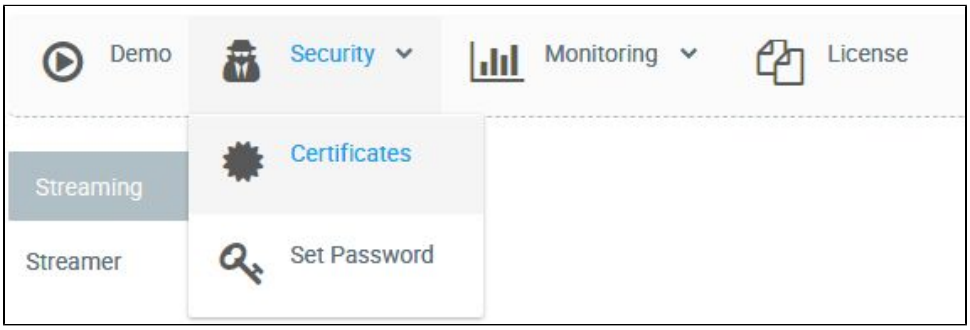
If you received the certificate successfully, proceed to the next step. If any errors occurred, refer to the certbot-auto documentation.

2. Make sure the /etc/letsencrypt/live/yourdomain/ folder on your server has the following files:

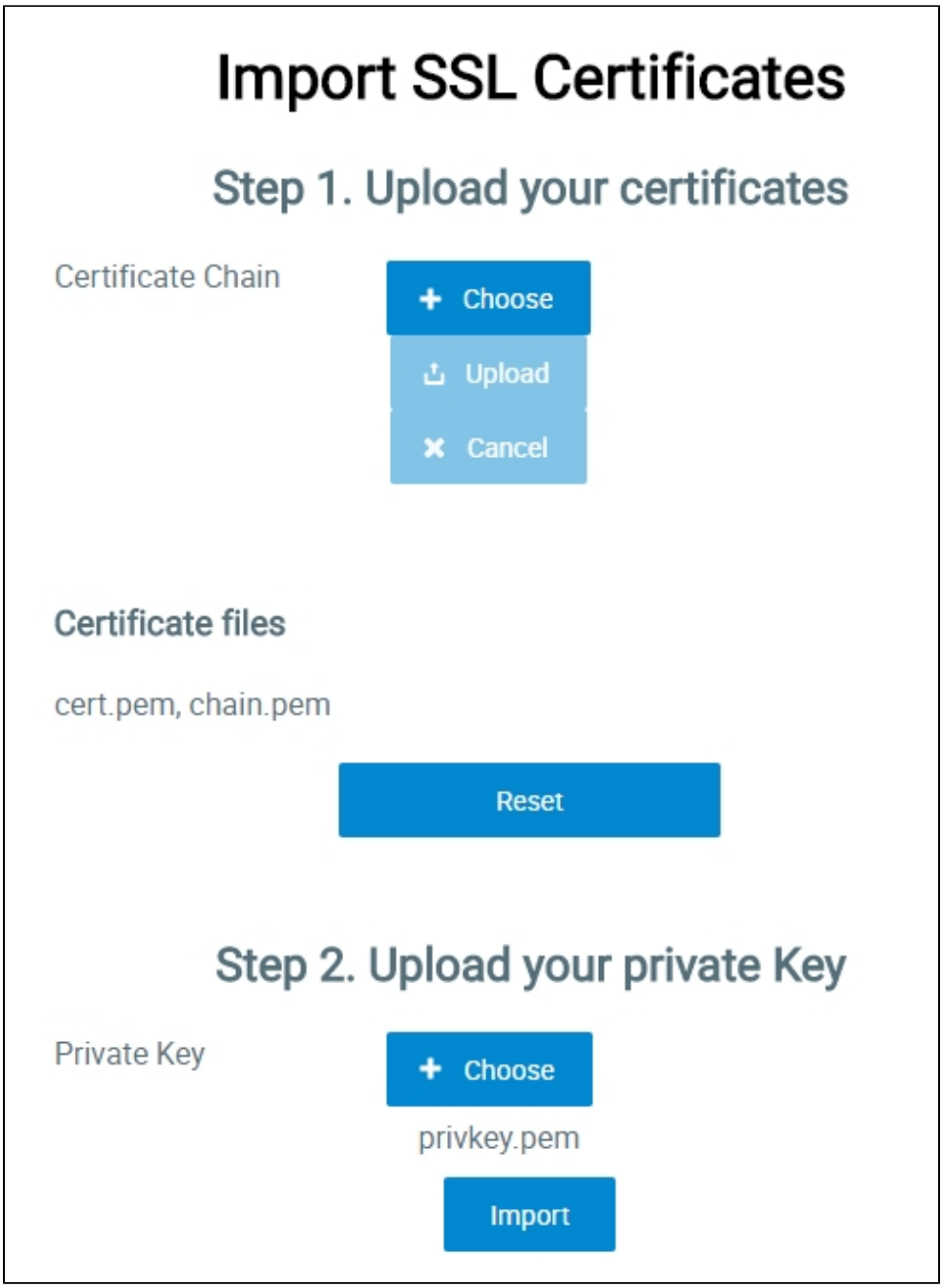
```
cert.pem
chain.pem
fullchain.pem
privkey.pem
```

Copy these files to your computer.

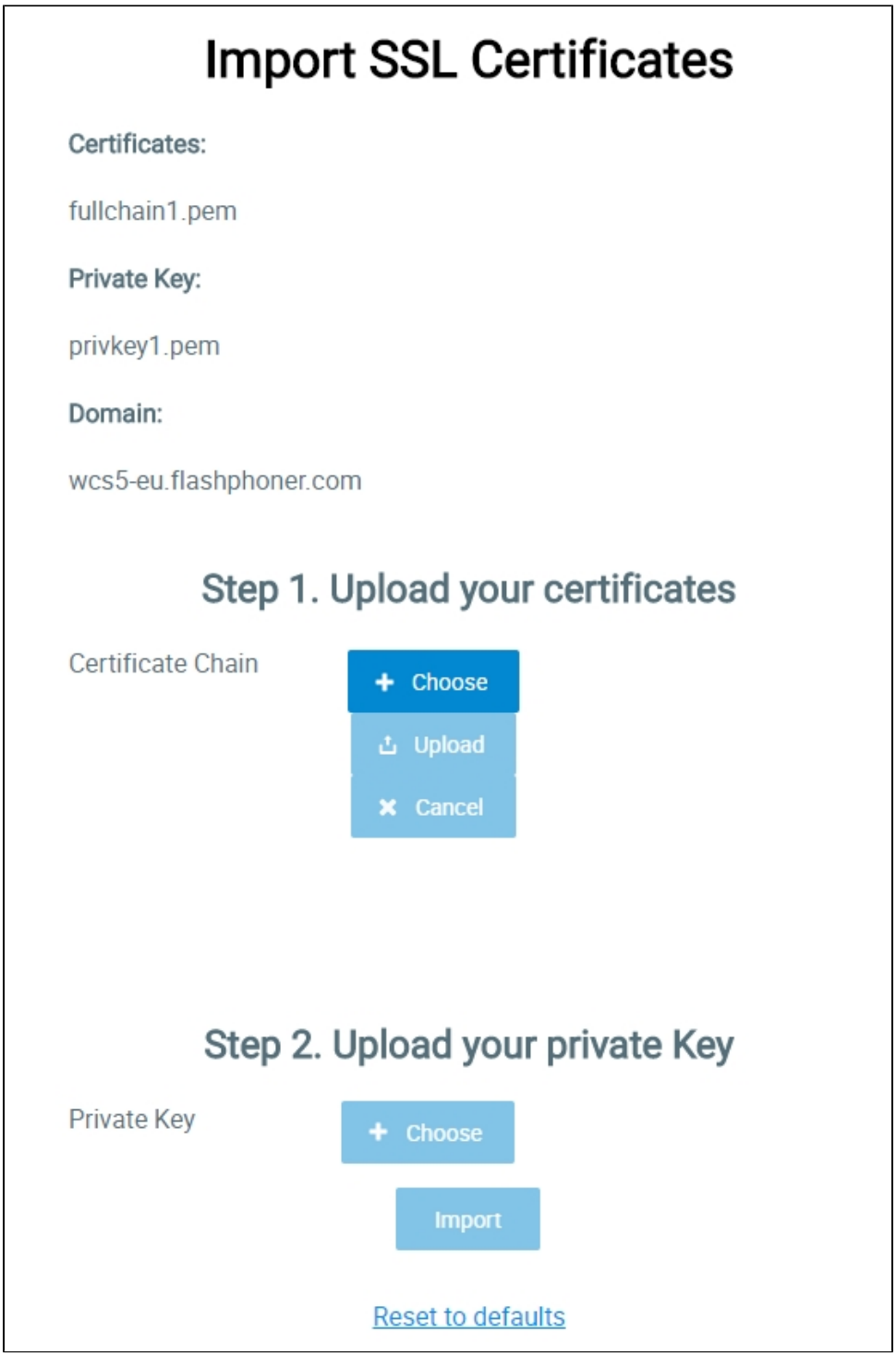
3. Open the web interface of WCS. Select "Security" in the upper menu, then "Certificates":



4. On the import page, upload the certificate files: cert.pem, chain.pem and the key file privkey.pem:



Or upload the certificate file fullchain.pem and the key file privkey.pem:



Restart the WCS server to apply new settings. After restarting the server, open http://yourdomain:8443. If the certificate was imported correctly, you should see that the browser accept the certificate of the WCS server.

If importing of the certificate failed with some errors, proceed to the keytool importing.

5. Remove the self-signed certificate from the keystore

```
keytool -delete -alias selfsigned -keystore /usr/local/FlashphonerWebCallServer/conf/wss.jks
```

6. Create a new keystore based on the certificate and the private key

```
openssl pkcs12 -export -in /etc/letsencrypt/live/yourdomain/fullchain.pem -inkey /etc/letsencrypt/live
/yourdomain/privkey.pem -out /etc/letsencrypt/live/yourdomain/pkcs.p12 -name yourdomain
```

At this stage you need to enter the password from your private key test.flashphoner.com.key as well as set a password for the keystore itself. Here we set 'password'.

```
Enter pass phrase for yourdomain.key: ******
Enter Export Password: password
```

7. Import the newly created keystore to the existing wss.jks

```
keytool -importkeystore -srckeystore /etc/letsencrypt/live/yourdomain/pkcs.p12 -srcstoretype PKCS12 -
destkeystore /usr/local/FlashphonerWebCallServer/conf/wss.jks
```

At this stage you have to enter passwords from the imported keystore and the wss.jsk keystore.

```
Enter destination keystore password: password
Enter source keystore password: password
Entry for alias yourdomain successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

Restart the WCS server to apply the new settings. After restarting the server, open http://test.flashphoner.com:8443 again. If certificates are imported correctly, you should see that the browser accepts the WCS server certificate.