Получение и импорт SSL сертификата Let's Encrypt

Let’s Encrypt — центр сертификации, предоставляющий бесплатные криптографические сертификаты в автоматическом режиме. Получить и импортировать сертификат на Ваш WCS-сервер можно следующим образом:

Получение сертификата при помощи certbot

Установка Certbot

Centos

1. Установите репозиторий epel-release

в Centos 7

```
yum install epel-release
```

в Centos 8

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

2. Установите certbot

в Centos 7

```
yum install certbot python2-certbot
```

в Centos 8

```
sudo dnf install certbot python3-certbot
```

Ubuntu

Установите certbot командой

```
sudo apt-get install certbot
```

Другие операционные системы

Установите certbot в соответствии с официальной инструкцией

Получение сертификата

1. Откройте порты HTTP 80 и HTTPS 443 на сервере для входящих соединений, чтобы certbot мог проверить сервер корректно

2. Запустите certbot

Если на этом же сервере работает веб-сервер, запустите

```
sudo certbot certonly --apache
```

или

```
sudo certbot certonly --nginx
```

Если на сервере установлен только WCS, запустите

```
sudo certbot certonly --standalone
```

В интерактивном режиме certbot запросит необходимые сведения и загрузит файлы сертификатов на сервер.

Если сертификат был получен успешно, переходите к следующему шагу. Если при получении сертификата возникли какие-либо ошибки, обратитесь к документации на certbot

3. Убедитесь, что на вашем сервере в каталоге /etc/letsencrypt/live/yourdomain/ находятся следующие файлы:

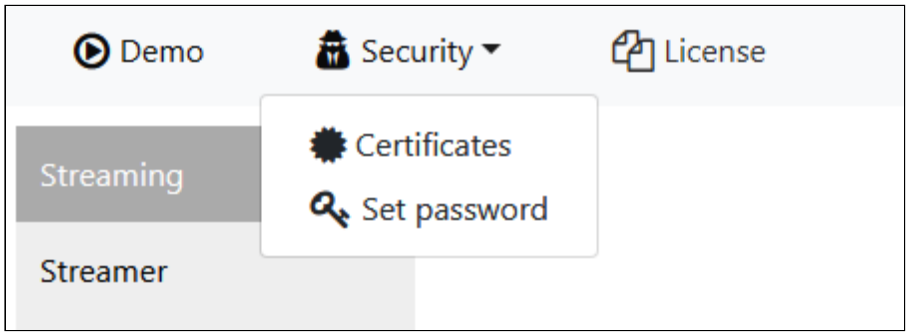
```
cert.pem
chain.pem
```

```
fullchain.pem
privkey.pem
```

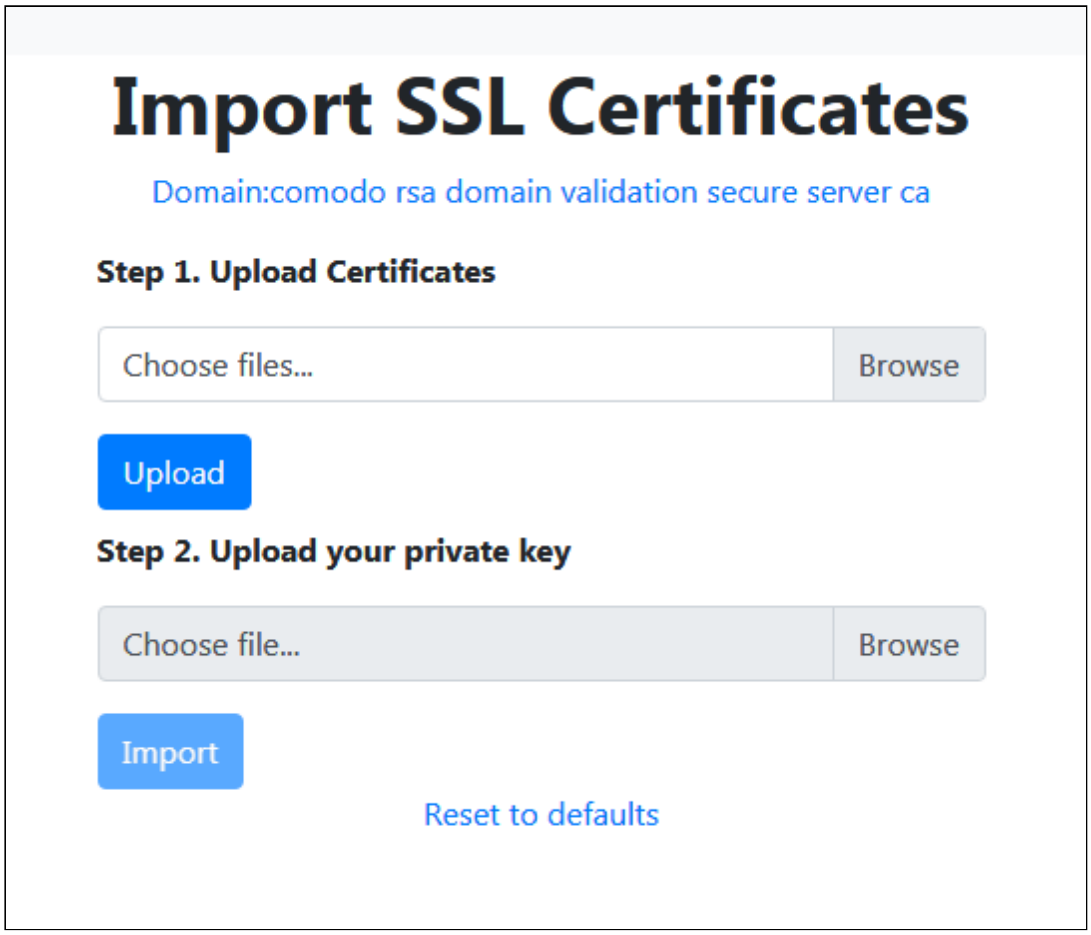
Скопируйте файлы на ПК.

Импорт сертификатов в хранилище WCS

1. Войдите в веб-интерфейс WCS. Выберите в верхнем меню пункт "Security", а в подменю - пункт "Certificates":



2. На странице импорта загрузите файл сертификата fullchain.pem и файл ключа privkey.pem:



Перезагрузите WCS сервер, чтобы применить новые настройки. После перезагрузки сервера откройте URL https://yourdomain:8443. Если сертификат был импортирован правильно, вы увидите, что браузер принимает сертификат WCS сервера.

Если при импорте сертификата возникли какие-либо ошибки, переходите к импорту при помощи keytool.

3. Удалите self-signed сертификат из хранилища

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

4. Создайте новое хранилище на базе сертификата и приватного ключа

```
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
```

На этом шаге нужно ввести пароль для вашего приватного ключа yourdomain.key, а также установить пароль для самого хранилища. Устанавливаем 'password'.

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

5. Импортируйте вновь созданное хранилище в существующее хранилище wss.jks

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

На этом шаге придется ввести пароли от импортируемого хранилища и от хранилища wss.jsk.

```
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
```

Перезагрузите WCS сервер, чтобы применить новые настройки. После перезагрузки сервера откройте URL https://yourdomain:8443. Если сертификат был импортирован правильно, вы увидите, что браузер принимает сертификат WCS сервера.

Attachments:

- SSL-letsencrypt-fullchain.jpg (image/jpeg)
- SSL-letsencrypt-chain.jpg (image/jpeg)

- SSL-menu.jpg (image/jpeg)
- wsc52-SSL-menu.PNG (image/png)
- wcs52-SSL-import.PNG (image/png)