Websocket SSL

WCS использует по умолчанию порт 8080 для приема Websocket - соединений и порт 8443 для приема Secure Websocket соединений.

Для подключения к WCS-серверу по протоколу Secure Websockets с использованием Web SDK в функцию Flashphoner.createSession() должен быть передан параметр urlServer с wss.

Пример:

```
Flashphoner.createSession({urlServer:'wss://192.168.1.5:8443'});
```

Настройки

За Secure Websockets отвечают следующиенастройки в файле flashphoner.properties:

Настройка	Значение по умолчанию
wss.port	8443
wss.keystore.file	wss.jks
wss.keystore.password	password
wss.cert.password	password

Сгенерированные сертификаты (self-signed)

WCS по умолчанию использует простые сгенерированные сертификаты, поэтому для того чтобы соединение прошло успешно, предварительно нужно обратиться из браузера по адресу:

https://192.168.1.5:8444/

Здесь, на месте 192.168.1.5 должен быть адрес вашего WCS сервера.

Браузер выдаст предупреждение о том, что сертификат безопасности, используемый WCS-сервером не известен браузеру или операционной системе. Это нормально, т.к. используется сгенерированный сертификат для тестовых целей. В зависимости от браузера продолжите переход по этому адресу или добавьте для этого адреса исключение безопасности. После этого клиентский сертификат WCS будет добавлен в кэш вашего браузера и дальнейшие соединения будут проходить успешно.

Действительные сертификаты

Self-signed сертификаты могут быть использованы только для тестирования и разработки, т.к. в противном случае вашим веб-пользователям придется проходить процедуру подтверждения неизвестного сертификата перед коннектом.

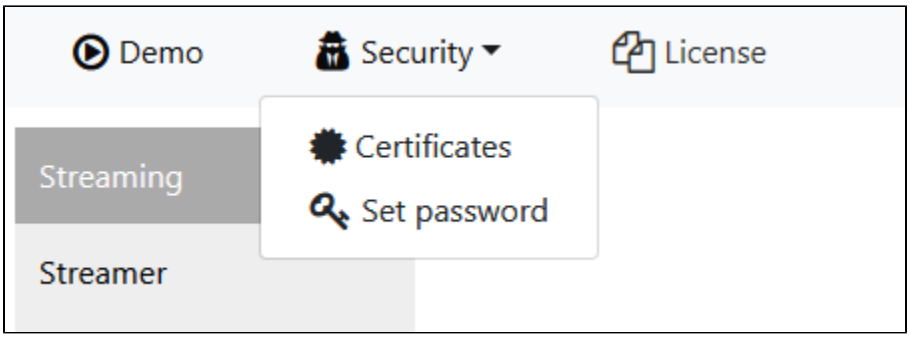
Для работы в production потребуются SSL сертификаты, выданные авторизованным центром сертификации. Эти сертификаты как правило платные и их можно заказать для домена или поддоменов. Сертификаты должны быть импортированы в хранилище сертификатов wss.jks. См. разделНастройки.

Импорт сертификата при помощи веб-интерфейса

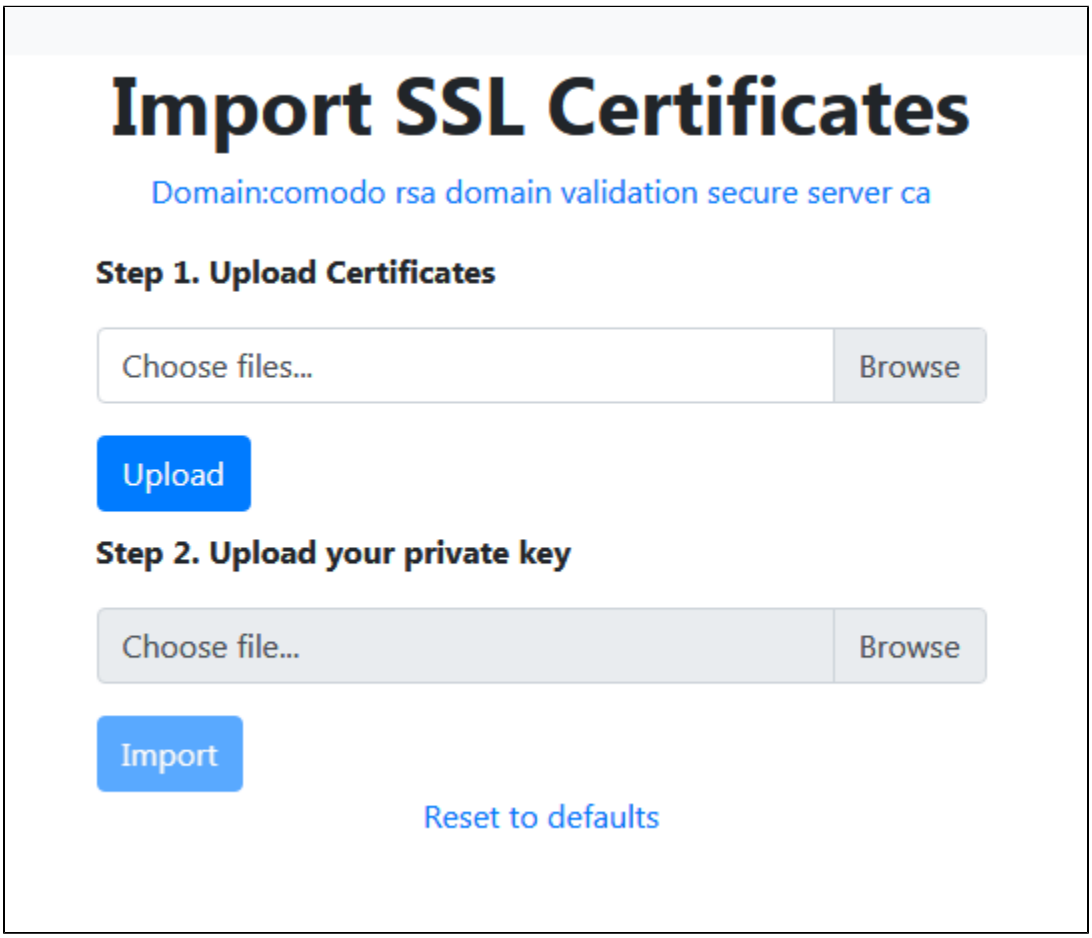
SSL сертификат может быть импортирован через веб-интерфейс WCS следующим образом:

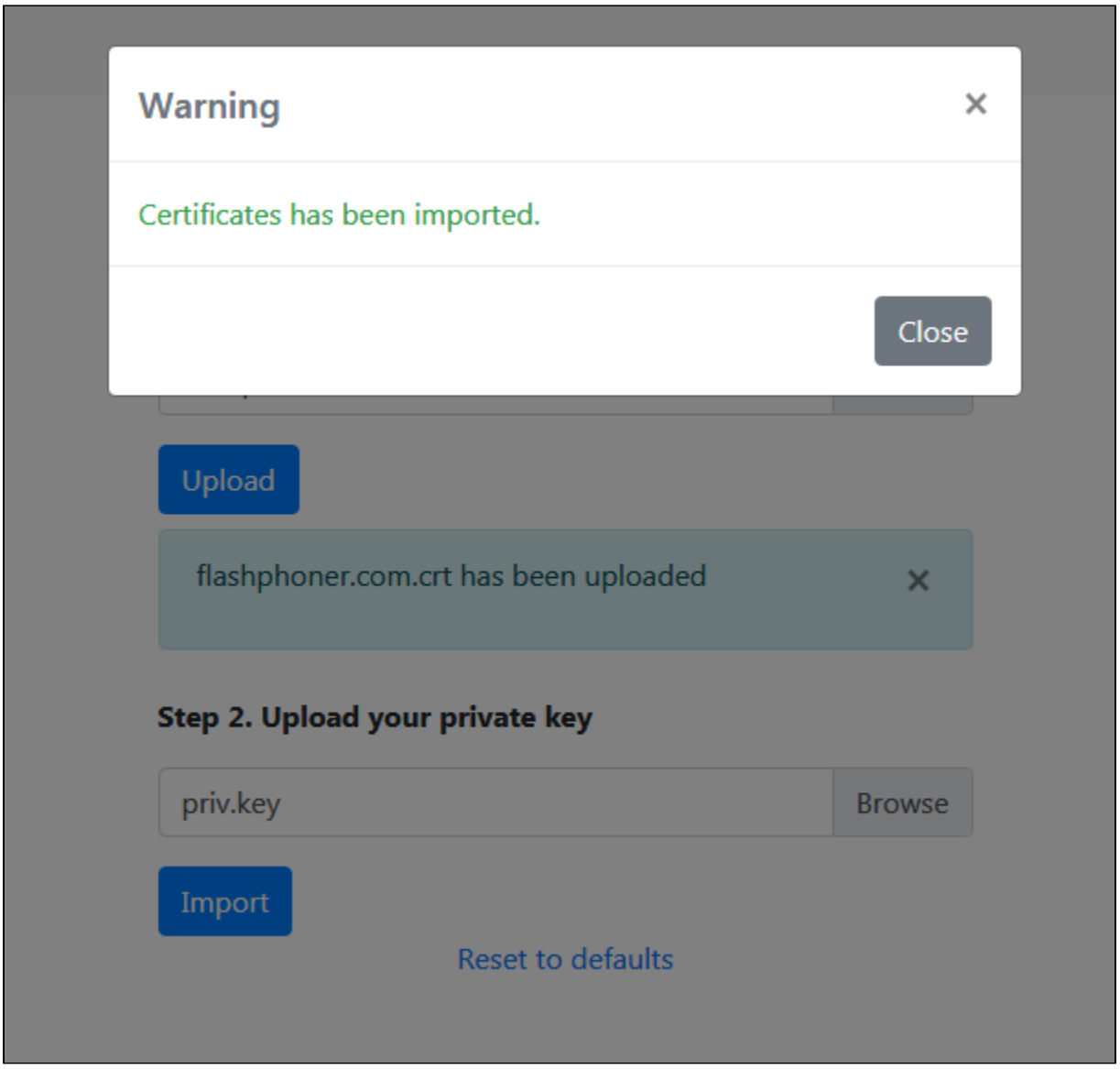
1. Получите SSL сертификат у вашего SSL-провайдера.

2. Войдите в веб-интерфейс WCS с доступным по умолчанию пользователем admin (пароль admin). Выберите в верхнем меню пункт "Security", а в подменю - пункт "Certificates":

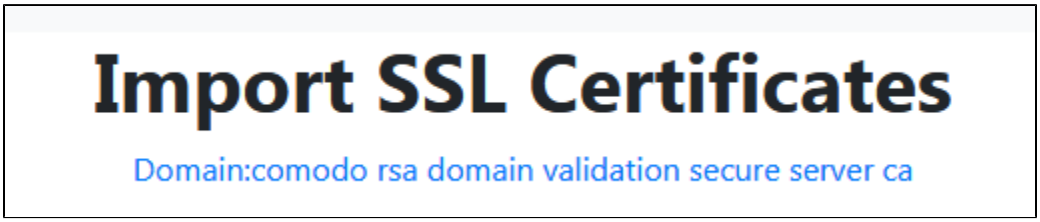


3. На странице импорта загрузите файлы сертификата, полученные от Вашего SSL-провайдера, и файл ключа:





4. SSL-сертификаты, импортированные при помощи веб-интерфейса, записываются в хранилище сертификатов wss.jks и в базу данных WCS-сервера и отображаются в разделе "Security - Certificates":



Перезагрузите WCS сервер, чтобы применить новые настройки. После перезагрузки сервера откройте URLhttps://yourdomain:8444. Если сертификат был импортирован правильно, вы увидите, что браузер принимает сертификат WCS сервера.

Если импортировать SSL-сертификат через веб-интерфейс не удается, он может быть импортированпри помощи инструмента keytool.

Импорт сертификата при помощи инструмента keytool

SSL-сертификата может быть импортирован из командной строки Linux с помощью инструмента keytool, который поставляется с JDK. Если у вас не установлена JDK, обратитесь к разделуУстановка JDK.

Исполняемый файл keytool находится в каталоге JDK_HOME/bin, например /usr/java/default/bin. Для удобства можно создать ссылку:

```
ln -sf /usr/java/default/bin/keytool /usr/bin/keytool
```

Кроме этого вам может потребоваться openssl для конвертации файлов сертификатов. Если openssl не установлен, установите его командой:

```
yum install -y openssl  apt-get install openssl
```

Получите SSL - сертификат у вашего SSL-провайдера.

Мы рассмотрим импорт сертификата от провайдера StartSSL.

От провайдера мы получили сертификат для домена test.flashphoner.com и следующий набор файлов:

test.flashphoner.com.crt - файл сертификата
test.flashphoner.com.key - файл приватного ключа
ca.pem - корневой сертификат
sub.class2.server.ca.pem - промежуточный сертификат

Далее выполняем следующие 5 шагов:

1. Удаляем self-signed сертификат из хранилища

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

2. Создаем новое хранилище на базе сертификата и приватного ключа

```
openssl pkcs12 -export -out test.flashphoner.com.p12 -inkey test.flashphoner.com.key -in test.flashphoner.com.
crt -certfile ca.pem -certfile sub.class2.server.ca.pem -name test.flashphoner.com
```

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

```
Enter pass phrase for test.flashphoner.com.key: ******
Enter Export Password: password
```

Обратите внимание, что файлы сертификатов могут иметь другие расширения, а также что вместо отдельных корневого и промежуточного сертификатов центр сертификации может предоставить один "bundle" сертификат (в этом случае в openssl команде для создания нового хранилища потребуется только одна опция -certfile).

3. Импортируем вновь созданное хранилище в существующее хранилище wss.jks

```
keytool -importkeystore -srckeystore test.flashphoner.com.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 test.flashphoner.com successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

Готово. Сертификаты успешно импортированы в хранилище.Перезагрузите WCS сервер, чтобы применить новые настройки.

4. После перезагрузки сервера откройте URLhttps://test.flashphoner.com:8444снова. Если сертификаты были импортированы правильно, вы увидите, что браузер принимает сертификат WCS сервера.

5. Далее нужно использовать URL wss://test.flashphoner.com:8443 при коннекте к серверу в методе 'connect'. Обратите внимание, что мы используем в данном случае доменное имя вместо IP-адреса. Сертификат, выданный на это доменное имя, был импортирован в хранилище и используется WCS-сервером. Домен test.flashphoner.com, использующийся в примере, вам нужно заменить вашим доменом, на который был выдан SSL-сертификат.

Импорт двух и более сертификатов для нескольких доменов

Иногда к одному и тому же серверу необходимо обеспечить доступ пользователей с разных доменов, подписанных различными сертификатами. В таких случаях сертификаты должны быть импортированы при помощи keytool. При этом:

1. Доступ к функциям сервера через SSL (Secure Websocket, HTTPS) будет работать для всех доменов.

2. Доступ к веб-интерфейсу через SSL будет работать только для одного домена, сертификат которого был импортирован первым.