

# REST HTTPS

- [Настройки](#)
- [Входящий HTTPS](#)
  - [Профили](#)
  - [Сертификаты](#)
- [Исходящий HTTPS](#)

## Настройки

По умолчанию для взаимодействия с веб-сервером используется REST / HTTP без шифрования. В этом случае легко можно посмотреть HTTP-трафик, который ходит между WCS и web-сервером.

WCS Manager слушает HTTP на порту 9091, а HTTPS на порту 8888.

Настройки административного модуля WCS в файле [wcs-manager.properties](#), относящиеся к HTTPS:

Настройка	По умолчанию
manager.enable_https	true
manager.https_port	8888
manager.keystore	wss.jks
manager.keystore_password	password
spring.profiles.active	dev
rest_template.allow_self_signed	true

## Входящий HTTPS

### Профили

Входящие HTTPS-запросы используются только для обратных вызовов 'sendData'. См. в документации Web Call Server - Call Flow.

Эти запросы идут с Web-сервера на WCS и WCS - выступает в данном случае в качестве HTTPS-сервера.

Для переключения режимов HTTP и HTTPS используются профили:

- dev
- production

Эти профили могут быть указаны в настройках WCS Manager, в файле [wcs-manager.properties](#).

Пример:

```
spring.profiles.active = dev
```

Даже если профиль production включен, HTTPS можно отключить с помощью настройки manager.enable\_https=false. В этом случае порт HTTPS не будет слушаться WCS-сервером.

### Сертификаты

В качестве SSL сертификатов для REST / HTTPS Web Call Server использует по умолчанию то же хранилище, которое используется для Websockets - wss.jks, указанное параметром manager.keystore.

Управление этим хранилищем подробно описано в разделе [Websocket SSL](#).

## Исходящий HTTPS

При обращении к web-серверу, WCS сервер смотрит на URL обращения и инициирует HTTPS запрос если этот URL начинается с https. Например <https://localhost/ConnectionStatusEvent>. Для обращения к веб-серверу использующему сгенерированный сертификат (self-signed) используется настройка rest\_template.allow\_self\_signed=true.

Если эту настройку выставить в false, то обращения проходить не будут и вам нужно будет сконфигурировать ваш веб-сервер для работы с действительными SSL-сертификатами, выданными центром сертификации. Для этого обратитесь к документации вашего веб-сервера.