



## Подключение REST-сервиса

Задаются параметры подключения, запроса и ответа REST-сервиса. Выходные данные подключения используются узлом REST-запрос.

### Параметры подключения

- **URL сервиса** — задается адрес отправки запросов к REST-сервису.
- **Метод** — выбирается один из HTTP-методов, используемых при отправке запросов к сервису: GET, DELETE, POST, PUT, PATCH.
  - При выборе методов GET, DELETE доступны настройки:
    - *Допустимый Content-type ответа* — узел REST-запрос, использующий данное подключение, проверяет тип ответа на соответствие заявленному в данном параметре. При несоответствии типов выходной набор этого узла будет содержать сообщение об ошибке. Данная проверка не осуществляется, если параметр имеет значение `*/*`.
    - *Параметры запроса* — задается перечень параметров запроса, их имена и типы данных. В последующем, в узле вызова REST-сервиса значения параметров подставляются в URL запроса.
  - При выборе методов POST, PUT, PATCH доступны настройки:
    - *Тип Content-type запроса* — задается значение заголовка `Content-type` HTTP-запроса к REST-сервису. Доступен как выбор из списка predefined значений, так и ввод произвольного значения.
    - *Допустимый Content-type ответа* — то же, что и для GET, DELETE методов (см. выше).
- **Таймаут подключения (мс)** — максимальное время установки TCP-соединения с сервером в миллисекундах, по истечении которого соединение будет прервано со статусом ошибки. Если параметр равен нулю, то таймаут не ограничен.
- **Таймаут обмена данными (мс)** — максимальное время, которое будет затрачено на отправку HTTP-запроса и получение ответа, по истечении которого обмен будет прерван со статусом ошибки. Если параметр равен нулю, то таймаут не ограничен.
- **Игнорировать ошибки SSL сертификата** — если данный флаг установлен, то ошибки при проверке сертификата сервера, к которому производится подключение, игнорируются.

### Аутентификация для выполнения запроса

- **Тип аутентификации** — представляет выпадающий список с вариантами аутентификации:
  - **Не требуется** — при выборе этого пункта Loginom не проводит аутентификацию при подключении к сервису.

- **Имя пользователя и пароль** — выбирается, если требуется аутентификация по имени/паролю. Поддерживаются следующие типы аутентификации по имени пользователя и паролю:
  - Basic;
  - Digest;
  - NTLM;
  - Passport;
  - Negotiate.
- **Токен OAuth** — выбирается при подключении к веб-сервису посредством протокола OAuth версии 2.0.
- **Клиентский сертификат из хранилища** — выбирается для аутентификации по SSL посредством сертификата. Данный тип аутентификации используется для операционной системы Windows.
- **Файлы сертификата клиента** — выбирается, если требуется аутентификация по сертификату клиента. При этом типе аутентификации необходимо выбрать нужный сертификат и приватный ключ из файлового хранилища, а также ввести пароль приватного ключа.
- **Имя пользователя, Пароль** — поле становится активным, если выбран тип *Имя пользователя и пароль*. Задают параметры аутентификации пользователя при его регистрации в системе веб-сервиса.
- **Токен OAuth** — поле становится активным, если выбран тип *Токен OAuth*. Вводится строка токена.
- **Хранилище сертификатов** — выпадающий список, который становится доступен при выборе *Клиентский сертификат из хранилища*. Из списка выбирается одно из хранилищ сертификатов, имеющихся в системе. Затем в таблице под списком выбирается используемый для аутентификации сертификат.
- **Сертификат пользователя** — поле становится доступно при выборе *Файлы сертификата клиента*, в нем указывается расположение (в файловом хранилище) сертификата, используемого для подключения к REST-сервису.
- **Приватный ключ** — поле становится доступно при выборе *Файлы сертификата клиента*, в нем указывается расположение (в файловом хранилище) приватного ключа, используемого для подключения к REST-сервису.
- **Пароль приватного ключа** — поле становится активным, если выбран тип *Файлы сертификата клиента*. Это пароль, позволяющий расшифровать ключ.