SIGUR

Руководство по настройке системы для использования функционала REST API

Редакция от 13.03.2024.

«Промавтоматика», г. Н. Новгород, 2024 г.

Оглавление

1. Введение 3
2. Версии документа 4
3. Используемые определения, обозначения и сокращения 5
4. Системные требования 6
5. Общее описание порядка взаимодействия 7
   5.1. REST API, общие сведения 7
6. Настройка на стороне «Sigur» 9
   6.1. Основные настройки 9
   6.2. Шифрование трафика по TLS 11
7. Контакты 13

1. Введение

Данный документ содержит общее описание интеграционных возможностей системы с использованием REST API и описание процесса первичной настройки ПО Sigur.

Представленная в данном документе информация соответствует функционалу программного обеспечения Sigur версии 1.6.2.10.

Руководство по установке и настройке системы Sigur можно найти в отдельных документах - «Руководство администратора ПО Sigur» и «Руководство пользователя ПО Sigur».

Подробное описание запросов REST API представлено в «Руководстве разработчика по REST API Sigur».

2. Версии документа

Данный документ имеет следующую историю ревизий.

Ревизия	Дата публикации	Что изменилось
0001	11 декабря 2023 г.	Соответствует версии ПО 1.6.0.1. Частично основан на документе для ПО Sigur версии 1.2.0.8. Изменения: обновлен порядок настройки системы, обновлена информация о процессе авторизации, обновлены методы группы Bindings в «Руководстве разработчика по REST API Sigur».
0002	27 декабря 2023 г.	Добавлена информация о предыдущем методе авторизации /api/v1/users/auth в «Руководство разработчика по REST API Sigur».
0003	13 марта 2024 г.	Изменения в «Руководстве разработчика по REST API Sigur»: • Добавлен корректный пример использования фильтра tabId[operation] в запросе к api/v1/employees. • Актуализировано описание полей, передаваемых при использовании предыдущего метода авторизации /api /v1/users/auth. • Добавлено описание эндпойнтов для работы с операторами системы. • Актуализировано содержимое запросов и ответов системы при работе с зонами.

3. Используемые определения, обозначения и сокращения

СКУД	Система контроля и управления доступом. Программно–аппаратный комплекс, предназначенный для осуществления функций контроля и управления доступом.
ПО	Программное обеспечение.
БД	База данных.

4. Системные требования

Рекомендуется руководствоваться конфигурацией сервера, описанной в разделе «Системные требования СКУД Sigur» «Руководства администратора ПО Sigur».

5. Общее описание порядка взаимодействия

5.1. REST API, общие сведения

Сервер Sigur обеспечивает возможность интеграционного взаимодействия посредством RESTful интерфейса. Данный интерфейс обеспечивается веб-сервером Sigur, с которым сторонние системы могут настроить взаимодействие посредством HTTP(S)-запросов.

REST интерфейс позволяет читать данные базы Sigur, изменять их, создавать новые объекты данных и удалять существующие. На текущий момент доступны следующие возможности:

- Получение списка отделов, создание новых, редактирование/удаление существующих.
- Получение списка должностей сотрудников, создание новых, редактирование/удаление существующих.
- Получение списка карт доступа, создание новых, редактирование/удаление существующих.
- Получение списка сотрудников, создание новых, редактирование/удаление существующих.
- Получение списка служебного автотранспорта, создание нового, редактирование/удаление существующего.
- Получение списка пользовательских параметров, создание новых, редактирование/удаление существующих.
- Получение списка точек доступа.
- Получение списка режимов доступа, создание новых, редактирование/удаление существующих.
- Получение списка зон доступа.
- Просмотр расширенной информации по объектам доступа (выданные карты, назначенные режимы доступа), назначение таких связей и удаление существующих.
- Получение списка существующих в системе кодов событий и непосредственно получение исторических событий.

С подробным описанием запросов разработчик интеграционного решения может ознакомиться, перейдя на ресурс *http://<server>:9500/swagger*, где <server> - это сетевой адрес компьютера, на котором установлен сервер Sigur.

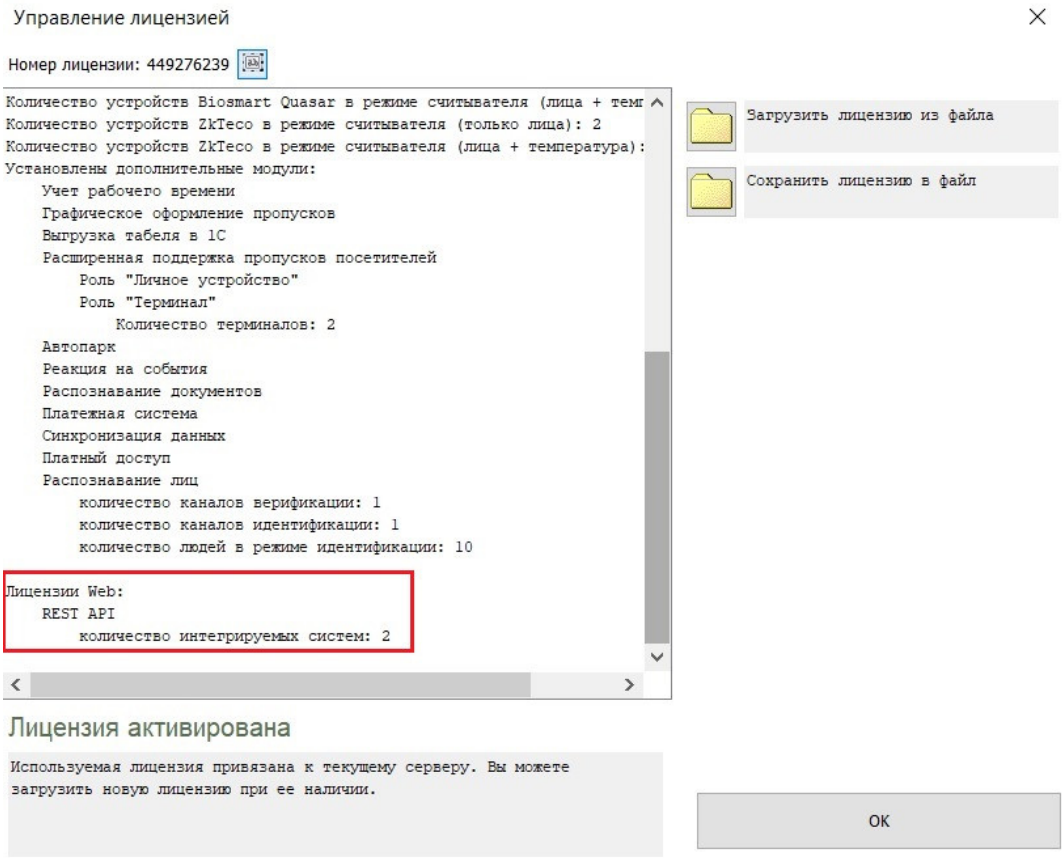
Подробное описание запросов также доступно в «Руководстве разработчика по REST API Sigur».

В ответ на GET-запросы по умолчанию возвращается 50 записей. Для конфигурирования количества возвращаемых записей предназначен параметр запроса limit. Получение большого количества записей рекомендуется осуществлять итерационно, сочетая параметры limit и offset. Параметр offset определяет количество записей с начала, которые должны быть пропущены в ответе.

6. Настройка на стороне «Sigur»

6.1. Основные настройки

Для организации успешного общения с сервером Sigur по REST API необходимо предварительно загрузить на сервер дополнительный лицензионный модуль «Лицензии Web: REST API» (процесс загрузки лицензии описан в разделе «Лицензирование функционала ПО» «Руководства пользователя ПО Sigur»). Функционал лицензируется по количеству интегрируемых систем.

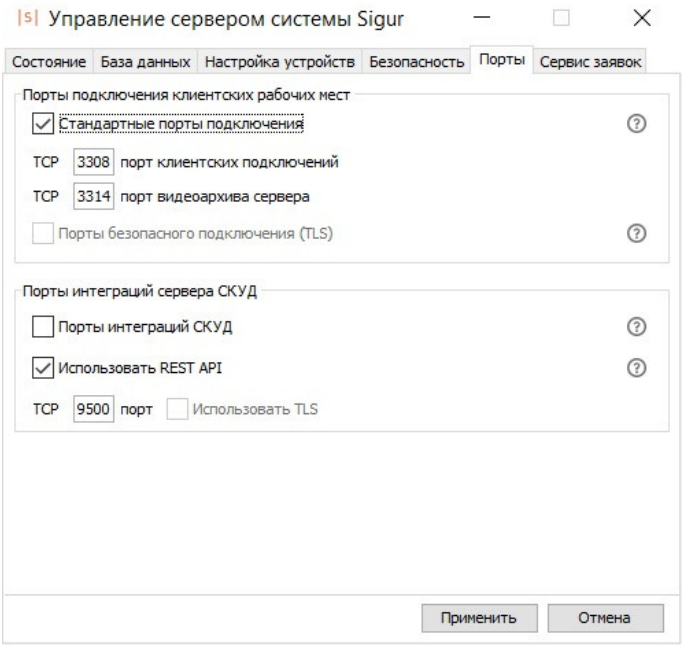


Окно «Управление лицензией».

В случае использования программной лицензии, после загрузки файла необходимо перезапустить ПО «Клиент». Также после изменения состава лицензии автоматически будет перезагружен серверный модуль Sigur.

Для активации порта веб-сервера необходимо перейти на вкладку «Порты» ПО «Управление сервером» и включить чек-бокс «Использовать REST API» в блоке «Порты интеграций сервера СКУД». По умолчанию для подключения в защищенном и незащищенном режиме к веб-серверу СКУД используется порт TCP 9500. Вы можете использовать порт по умолчанию или изменить это значение. Для сохранения настроек нажмите кнопку «Применить» и

перезагрузите серверный модуль.



Вкладка «Порты» ПО «Управление сервером».

Далее требуется создать реквизиты для авторизации на веб-сервере Sigur. Для этого необходимо:

1. Предоставить какому-либо сотруднику на вкладке «Персонал» права оператора (процесс создания оператора описан в разделе «Операторы системы» «Руководства пользователя ПО Sigur»).

2. Активировать чек-бокс «Доступ по REST API (Интеграции)» в списке прав оператора.

3. Задать логин и пароль оператора, от имени которого внешний сервис будет производить авторизацию. Логин оператора может содержать цифры и буквы латинской или русской раскладки.

4. Сохранить изменения, нажав кнопку «Применить».

Система, авторизовавшаяся на веб-сервере с данными реквизитами, имеет доступ к использованию всех запросов, перечисленных в «Руководстве разработчика по REST API Sigur».

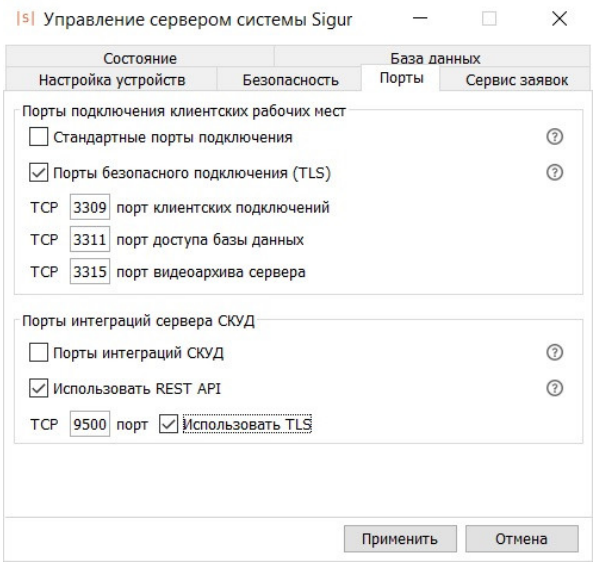
6.2. Шифрование трафика по TLS

Вы можете активировать шифрование трафика по протоколу TLS между веб-сервером Sigur и сторонними интеграционными сервисами.

По умолчанию шифрование отключено, взаимодействие с веб-сервером осуществляется по протоколу HTTP.

Перед активацией шифрования необходимо настроить хранилище сертификатов формата PKCS#12 на сервере СКУД (подробнее – в разделе «Установка зашифрованного соединения между клиентом и сервером» «Руководства администратора ПО Sigur»).

На вкладке «Порты» ПО «Управление сервером» необходимо включить чек-бокс «Использовать TLS» в разделе «Порты интеграций сервера СКУД», нажать кнопку «Применить» и перезапустить серверный модуль. После этого внешнее подключение на порт веб-сервера Sigur будет возможно только по протоколу HTTPS.



Чек-бокс «Использовать TLS» на вкладке «Порты» ПО «Управление сервером».

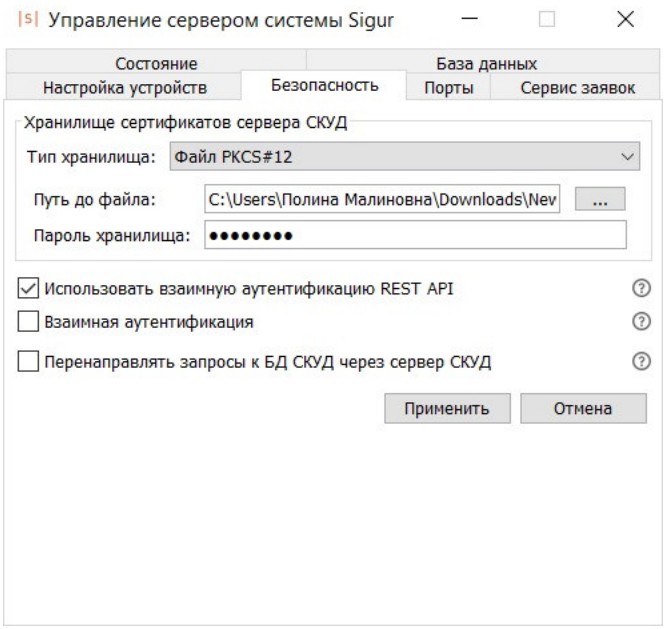
На стороне внешней системы, подключающейся на порт веб-сервера с использованием TLS, должно быть сконфигурировано хранилище доверенных сертификатов для валидации сертификата сервера Sigur. В противном случае внешняя система не сможет подключиться к веб-серверу Sigur.

Настройка взаимной аутентификации и списка отозванных сертификатов

Опционально Вы можете активировать взаимную аутентификацию при подключении на порт веб-сервера. В этом случае внешняя система, пытающаяся установить защищенное соединение, также должна

предоставить свой сертификат безопасности.

Для этого необходимо произвести предварительную настройку веб-сервера согласно описанию выше и затем активировать чек-бокс «Использовать взаимную аутентификацию REST API» на вкладке «Безопасность» ПО «Управление сервером». После сохранения настроек необходимо перезапустить серверный модуль. Сертификат внешней системы должен быть подписан доверенным корневым центром сертификации или промежуточным центром в цепочке доверия сервера Sigur.



Чек-бокс «Использовать взаимную аутентификацию REST API» на вкладке «Безопасность» ПО «Управление сервером».

Если ранее в системе уже был задан список отозванных сертификатов, он также будет использоваться для проверки статуса сертификатов внешних систем, подключающихся на порт веб-сервера Sigur. Подробнее о настройке списка отозванных сертификатов – в разделе «Проверка статуса отзыва сертификата» «Руководства администратора ПО Sigur».

Хранилище сертификатов сервера и список отозванных сертификатов являются общими для всей системы Sigur.

7. Контакты

ООО «Промышленная автоматика – контроль доступа»
Адрес: 603001, Нижний Новгород, ул. Керченская, д. 13, 4 этаж.

Система контроля и управления доступом «Sigur»
Сайт: www.sigur.com
По общим вопросам: info@sigur.com
Техническая поддержка: support@sigur.com
Телефон: +7 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260 12 93