SIGUR

Руководство по настройке системы для использования функционала REST API

Редакция от 10.06.2026.

«Промавтоматика», г. Н. Новгород, 2026 г.

Оглавление

1. Введение

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

Представленная в данном документе информация соответствует функциональности ПО Sigur версии 1.8.4.35.

Руководство по установке и настройке системы Sigur можно найти в отдельных документах — «Руководстве администратора ПО Sigur» и «Руководстве 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 и эндпоинтах группы Bindings в «Руководстве разработчика по REST API Sigur».
0002	27 декабря 2023 г.	Добавлена информация о предыдущем эндпоинте авторизации api/v1/application-keys/auth в «Руководство разработчика по REST API Sigur».
0003	13 марта 2024 г.	Изменения в «Руководстве разработчика по REST API Sigur»: • Добавлено описание новых эндпоинтов для работы с операторами системы. • Актуализировано содержимое запросов и ответов системы при работе с зонами. • Добавлен корректный пример использования фильтра tabId[operation] в запросе к api/v1/employees. • Актуализировано описание полей, передаваемых при использовании предыдущего эндпоинта авторизации api/v1/application-keys/auth.

Ревизия	Дата публикации	Что изменилось
0004	4 сентября 2024 г.	Добавлена информация об актуальном способе управления автотранспортом с помощью REST API Sigur. Изменения в «Руководстве разработчика по REST API Sigur»: • Добавлено описание новых эндпоинтов для управления допуском сотрудников и служебных автомобилей на точки доступа. • Эндпоинты для управления личными автомобилями теперь отмечены как устаревшие, пользоваться ими на текущий момент не рекомендуется. • Актуализирована информация об использовании параметров limit и offset для GET-запросов. • Добавлено пояснение о работе с полем "name" в запросе к /api/v1/cards/update.
0005	10 января 2025 г.	Добавлена информация о работе с фильтрами startTime и endTime для эндпоинтов api/v1/events и api/v1/events/parsed в «Руководство разработчика по REST API Sigur».
0006	13 марта 2025 г.	Актуализирована информация о присвоении карт сотрудникам средствами REST API в разделе «Bindings» — «Employees-Cards» — «Assign Cards to Employees» «Руководства разработчика по REST API Sigur».
0007	15 сентября 2025 г.	Актуализированы сведения о требуемой лицензии в системных требованиях и в инструкции по настройке на стороне Sigur. Изменения в «Руководстве разработчика по REST API Sigur»: • Обновлена информация о фильтрации по дополнительным параметрам при выполнении запроса GET api/v1/employees. • Актуализирована структура тела запроса PUT api/v1/cards/{id} и ответа.

Ревизия	Дата публикации	Что изменилось

0008	16 октября 2025 г.	Изменения в «Руководстве разработчика по REST API Sigur»:
		• Добавлены новые эндпоинты для:
		  • управления гостевыми картами (Guest Cards);
		  • выдачи/изъятия карт посетителям, просмотра фото посетителя и списка всех документов, удостоверяющих личность (Guests);
		  • управления гостевыми QR-кодами (Guest QR Codes);
		  • управления режимами доступа посетителей (Bindings: Guests-Access Rules);
		  • выдачи/изъятия гостевых карт сотрудникам (Bindings: Employees-Guest Cards);
		  • управления QR и PIN кодами сотрудников (Employee Virtual Identifiers (PIN, QR Code)).
		• Актуализировано описание эндпоинтов группы Custom Fields.
		• Во введении к документу добавлено описание возможных операторов сравнения.
		• Актуализировано описание тел запросов группы Cards в связи с возможностью менять/указывать значение поля "mfUid".
		• Актуализировано описание эндпоинтов групп Employees и Official Vehicles в связи с добавлением атрибутов "verificationPin" (PIN верификации), "accessStartTime", "accessEndTime" (Начало и окончание срока доступа), "identifiers" (все идентификаторы объекта доступа) а также расширен набор доступных фильтров.
		• Обновлено описание эндпоинта GET api/v1/events/parsed:
		  • Добавлены новые типы событий: «Не удалось взять зону под охрану» (ALARM_LINE_DENY) и «Событие о состоянии охранной зоны» (ALARM_LINE_STATUS).
		См. продолжение на следующей странице.

Ревизия	Дата публикации	Что изменилось
0008	16 октября 2025 г.	• В событии типа WAITING_FOR_RULE_STAGE добавлена новая причина «Ожидание подтверждения постановки зоны под охрану» (Waiting for confirmation of zone arming), в объект data добавлен новый атрибут alarmZoneId. В предыдущих версиях ПО карты с признаком guestApplicable=true могли использоваться для назначения сотрудникам в качестве «гостевых» карт. Начиная с версий ПО 1.6.7.x, рекомендуется использовать специальные эндпоинты для создания и выдачи гостевых карт сотрудникам и посетителям. Использование этих эндпоинтов позволяет в полной мере задействовать возможности работы с гостевыми пропусками в системе Sigur — в частности, на вкладке «Посетители» в ПО «Клиент» будет сохраняться история выдачи гостевых карт. Признак guestApplicable сохранён в системе для обеспечения обратной совместимости. Создание карт с признаком guestApplicable=true больше не поддерживается, как и изменение его значения с false на true. Если ранее вы использовали карты с guestApplicable=true, рекомендуется использовать фильтрацию по данному признаку, чтобы изменить его значение на false, либо удалить такие карты и добавить их заново как гостевые, с помощью эндпоинтов группы Guest Cards. Изменение признака или удаление карты невозможно, если она назначена какому-либо сотруднику. Допускается дальнейшее использование таких карт, однако рекомендуется выполнять управление гостевыми пропусками через новые эндпоинты. См. продолжение на следующей странице.

Ревизия	Дата публикации	Что изменилось
0008	16 октября 2025 г.	Если в системе есть невыданная карта с признаком guestApplicable=true, и вы создаёте новую гостевую карту методом POST api/v1/guestcards, система выполняет проверку на дубликаты. В случае совпадения значений полей value и format, невыданная карта с признаком guestApplicable=true будет автоматически привязана к создаваемой гостевой карте (ОД типа «Гостевой пропуск»).
0009	5 декабря 2025 г.	Актуализирован перечень функций протокола в разделе «Общее описание порядка взаимодействия».

0010	24 марта 2026 г.	В раздел «Общее описание порядка взаимодействия», а также в «Руководство разработчика по REST API Sigur» добавлено примечание о количестве записей, возвращаемых в ответ на GET-запросы.
		
		Прочие изменения в «Руководстве разработчика по REST API Sigur»:
		• Сортировка по полям assigned и formattedValue для GET /api/v1/guestcards более недоступна.
		• Актуализировано описание тела запроса PUT api/v1/bindings/employees-cards.
		• Обновлено описание GET api/v1/events/parsed:
		  • Добавлены новые типы событий: «Изменение состояния питания контроллера» (DC_STATUS), «Изменение состояния аккумулятора контроллера» (BATTERY_STATUS), «Не удалось сменить режим точки доступа» (AP_MODE_DENY).
		  • Тип события VOLTAGE_STATUS отмечен как устаревший (Deprecated).
		  • В «Событие о состоянии охранной зоны» (ALARM_LINE_STATUS) добавлен новый атрибут armingMethod.
		См. продолжение на следующей странице.

Ревизия	Дата публикации	Что изменилось

0010	24 марта 2026 г.	Обновлено описание GET api/v1/events/parsed:
		• Актуализировано описание события «Не удалось взять зону на охрану» (ALARM_LINE_DENY).
		• Добавлены новые причины для некоторых типов событий:
		  • Событие PASS_DENY — "Access period expired or not started" ("Доступ запрещен. Срок доступа не начался или уже закончился"), "Waiting for confirmation of access point mode change" ("Доступ запрещен. Ожидание подтверждения изменения режима точки доступа").
		  • Событие WAITING_FOR_RULE_STAGE — "Waiting for second access object" ("Ожидание второго объекта для доступа"), "Waiting for confirmation of access point mode change" ("Ожидание подтверждения изменения режима точки доступа").
		  • Событие MNG_STATE_CHANGED — "PIN", "PIN AND PASS" (изменение режима точки доступа с помощью PIN-кода или PIN-кода с подтверждением пропуском).

0011	20 апреля 2026 г.	Актуализирован перечень функций протокола в разделе «Общее описание порядка взаимодействия». Изменения в «Руководстве разработчика по REST API Sigur»: • Добавлены новые атрибуты для управления днями и временными интервалами доступа в режимах (Access Rules). • Теперь в эндпоинтах Employees, Access Rules, Custom Fields, Departments присутствует новый атрибут isGlobal, который отвечает за принадлежность сотрудника/режима/доп.параметра/отдела локальному или центральному серверу. Значение параметра генерируется автоматически. • Добавлены новые эндпоинты для получения, назначения и отзыва ролей операторов системы (Roles).

Ревизия	Дата публикации	Что изменилось

0012	10 июня 2026 г.	Изменения в «Руководстве разработчика по REST API Sigur»:
		• В описание эндпоинтов POST /api/v1/guests/guestcards/assign и POST /api/v1/guests/QR/assign добавлено примечание о том, что при выдаче посетителю через REST API гостевой карты или гостевого QR-кода пропуску автоматически выдаётся доступ на **все** точки доступа. Управлять правами доступа гостевых пропусков необходимо через режимы.
		Изменение вступает в силу, начиная с версии ПО 1.8.4.35 и касается только вновь выданных гостевых карт/QR-кодов.
		• Для эндпоинта POST api/v1/employees/{id}/identifiers добавлена:
		  • информация о возможности выдать мобильный идентификатор средствами REST API в «Базовом» режиме;
		  • информация о новом атрибуте replace, позволяющем перезаписать существующий нефизический идентификатор сотрудника новым значением.

3. Используемые определения, обозначения и сокращения

СКУД	Система контроля и управления доступом. Программно-аппаратный комплекс, предназначенный для осуществления функций контроля и управления доступом.
Точка доступа (ТД)	Место, где осуществляется контроль доступа. Например: дверь, турникет, ворота, шлагбаум, оборудованные считывателем, электромеханическим замком и другими необходимыми средствами.
Объект доступа (ОД)	Сотрудник, посетитель, автомобиль или другое транспортное средство, действия которого регламентируются правилами разграничения доступа.
ПО	Программное обеспечение.
БД	База данных.

4. Системные требования

- Для использования REST API Sigur необходимо наличие лицензии:
  - в случае использования пакетной лицензии — пакет Pro или Enterprise;
  - в случае использования модульной лицензии — дополнительный модуль «Лицензии Web: REST API» (по количеству интегрируемых систем).
- Рекомендуется руководствоваться конфигурацией сервера, описанной в разделе «Системные требования СКУД Sigur» «Руководства администратора ПО Sigur».

5. Общее описание порядка взаимодействия

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 и информации об их количестве, создание новых, редактирование и удаление существующих.
- Получение списка должностей сотрудников, создание новых, редактирование и удаление существующих.
- Получение списка карт доступа, создание новых, редактирование и удаление существующих.
- Получение списка сотрудников и информации об их количестве, создание новых, редактирование и удаление существующих. Блокировка и разблокировка доступа.
- Выдача, редактирование сроков действия и удаление нефизических идентификаторов сотрудников (мобильный идентификатор, PIN, QR-код). Выдача мобильного идентификатора средствами REST API на текущий момент возможна только в «Базовом» режиме.
- Получение списка служебного автотранспорта, создание нового, редактирование и удаление существующего.
- Получение списка операторов системы, назначение прав оператора существующим сотрудникам, редактирование и удаление назначенных ранее прав.
- Получение списка дополнительных параметров, создание новых, редактирование и удаление существующих.
- Получение списка точек доступа и информации об их количестве, получение каталогов точек доступа.
- Получение списка режимов доступа и информации об их количестве, создание новых, редактирование и удаление существующих. Задание циклических и специальных дней режима.
- Получение списка зон доступа.
- Просмотр расширенной информации по объектам доступа (выданные карты, предоставленный доступ к точкам доступа, назначенные режимы), режимам (привязка режимов к точкам доступа), назначение таких связей и удаление существующих.
- Управление гостевыми картами и QR-кодами:
    - Создание, редактирование, удаление гостевых карт (объектов доступа типа «Гостевой пропуск»). Получение списка гостевых карт.
    - Выдача, редактирование фактов выдачи и изъятие гостевых карт и QR-кодов посетителей. Получение гостевых карт и QR-кодов, выданных посетителям.

- Выдача, редактирование фактов выдачи и изъятие гостевых карт сотрудников. Получение гостевых карт, выданных сотрудникам.
- Назначение и изъятие режимов доступа для фактов выдачи гостевых карт и QR-кодов. Получение назначенных режимов.
- Получение всех типов документов, удостоверяющих личность.
- Получение фотографии посетителя.

- Получение списка кодов событий, существующих в системе, и получение самих событий в кратком или расширенном представлении.
- Получение, назначение и отзыв ролей операторов системы.

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.

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

В ответ на GET-запросы по умолчанию возвращается 50 записей, максимальное количество — 3000, при этом ограничение для запроса GET api/v1/employees отсутствует. Получение большого количества записей рекомендуется осуществлять итерационно, сочетая параметры limit и offset:

- параметр limit определяет общее количество записей, возвращаемых в ответе;
- параметр offset определяет количество записей с начала, которые должны быть пропущены в ответе.

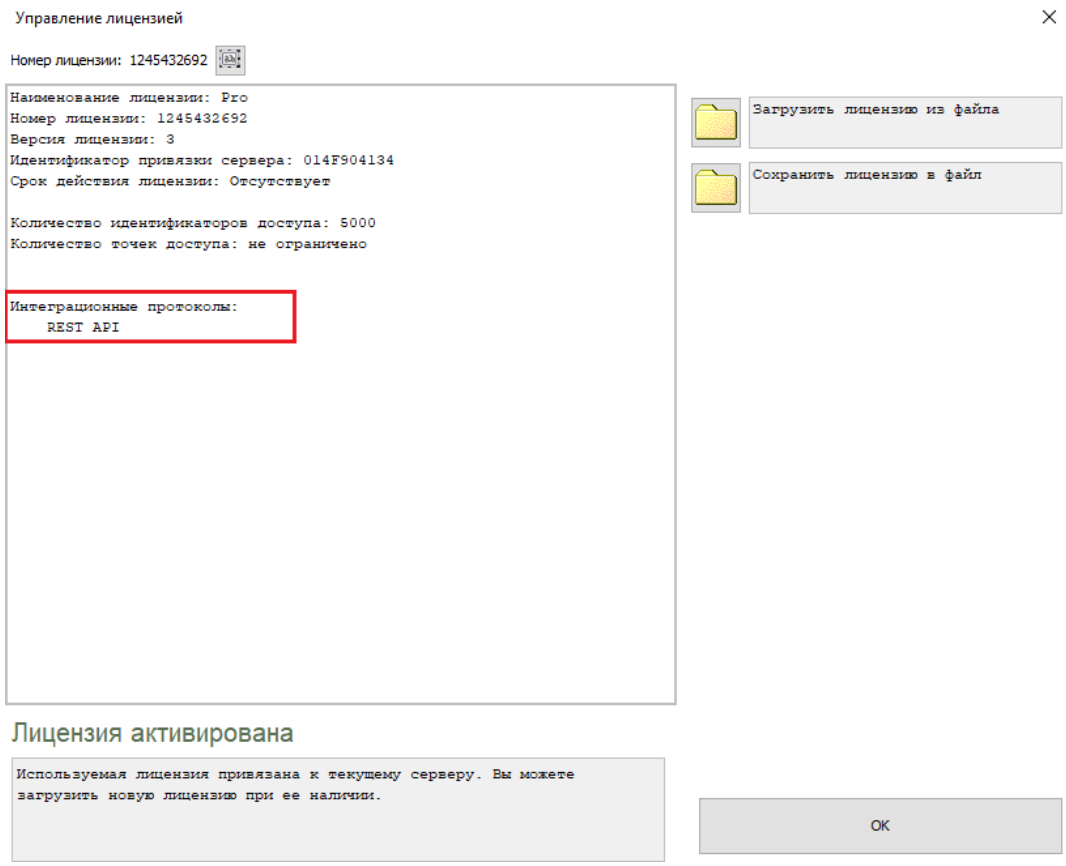
6. Настройка на стороне Sigur

6.1. Основные настройки

Выполните следующее:

1. При использовании пакетной лицензии необходимо активировать возможность работы с данным протоколом через Партнёрский портал Sigur. Подробнее об активации API — см. «Руководство по использованию партнёрского портала».

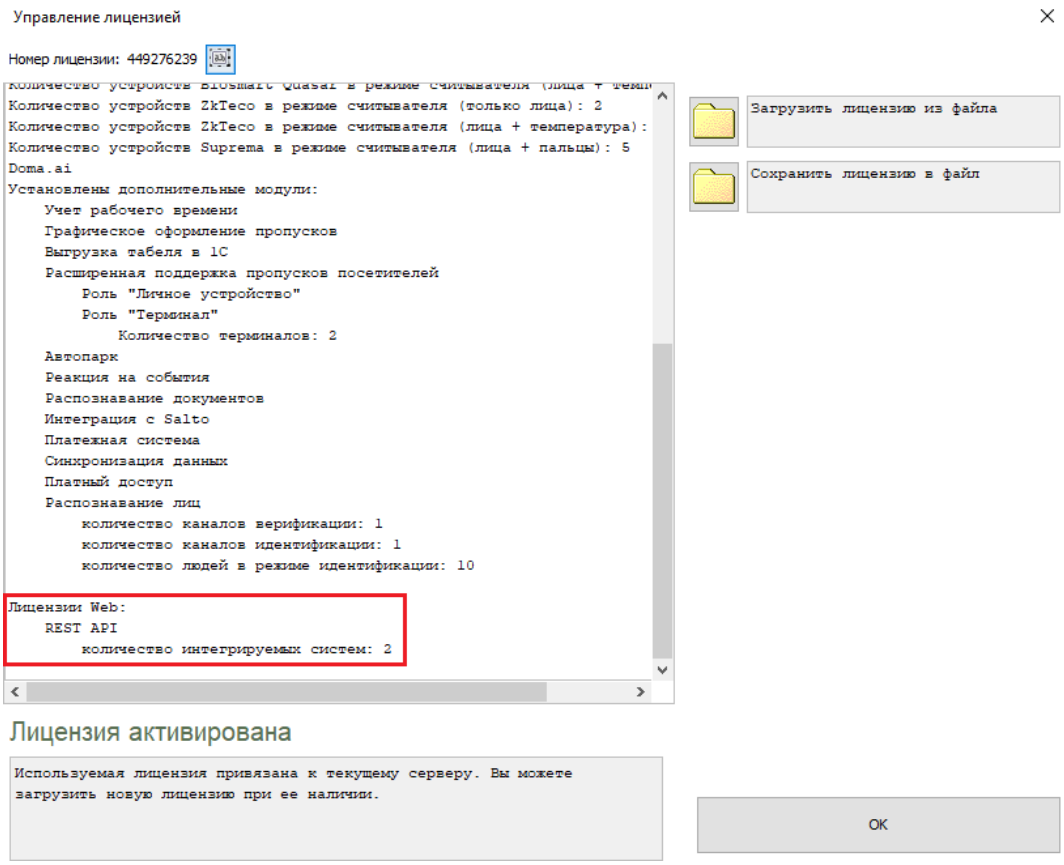
Состав текущей лицензии можно проверить в меню «Файл» — «Управление модулями» ПО «Клиент».



Меню «Файл» — «Управление модулями» ПО «Клиент».

2. При использовании модульной лицензии требуется загрузить на сервер дополнительный лицензионный модуль «Лицензии Web: REST API». Процесс загрузки лицензии описан в разделе «Лицензирование функционала ПО» «Руководства пользователя ПО Sigur».

После загрузки файла необходимо перезапустить ПО «Клиент». Также после изменения состава лицензии автоматически будет перезагружен серверный модуль Sigur.

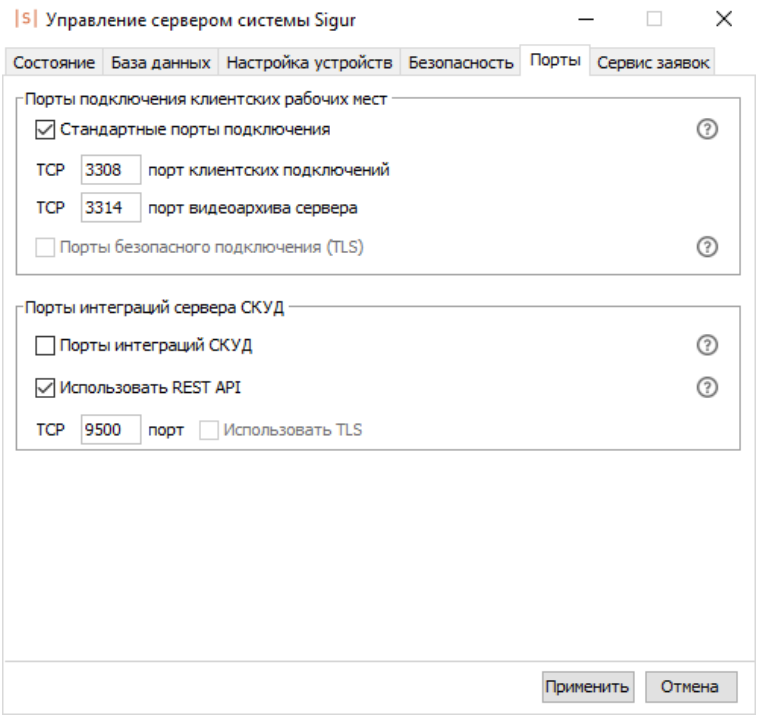


Меню «Файл» — «Управление модулями» ПО «Клиент».

3. Для активации порта веб-сервера необходимо перейти на вкладку «Порты» ПО «Управление сервером» и включить чекбокс «Использовать REST API» в блоке «Порты интеграций сервера СКУД».

По умолчанию для подключения к веб-серверу СКУД в защищённом и незащищённом режиме используется порт TCP 9500. Вы можете использовать порт по умолчанию или изменить это значение.

Нажмите кнопку «Применить» и перезагрузите серверный модуль для сохранения настроек.



Вкладка «Порты» ПО «Управление сервером».

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

- Предоставить какому-либо сотруднику на вкладке «Персонал» права оператора (процесс создания оператора описан в разделе «Операторы системы» «Руководства пользователя ПО Sigur»).
- Активировать чекбокс «Доступ по REST API (Интеграции)» в списке прав оператора.
- Задать логин и пароль оператора, от имени которого внешний сервис будет производить авторизацию. Логин оператора может содержать цифры и буквы латинской или русской раскладки.
- 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».

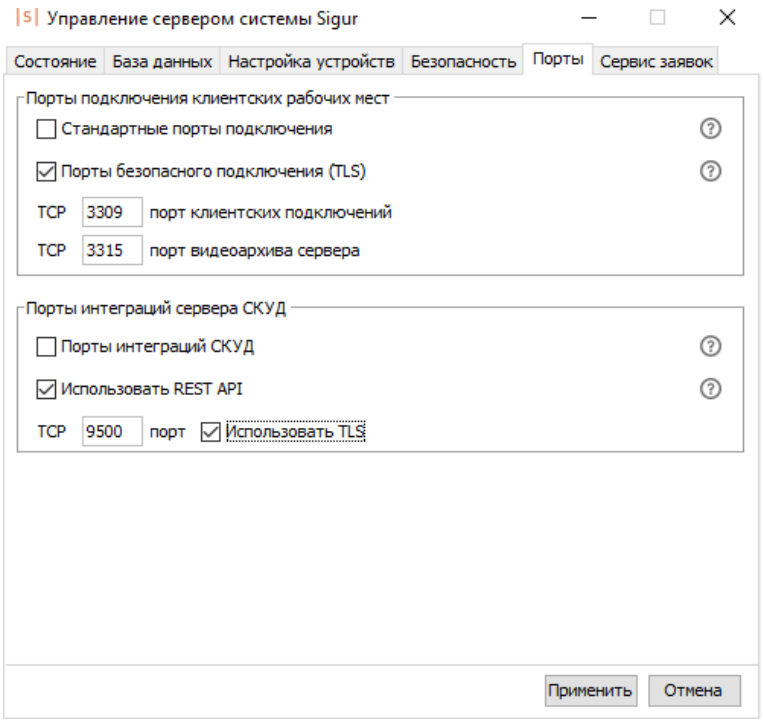
6.2. Шифрование трафика по TLS

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.

1. 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»).

2. На вкладке «Порты» ПО «Управление сервером» необходимо включить чекбокс «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.



Вкладка «Порты» ПО «Управление сервером».

3. На стороне внешней системы, подключающейся на порт веб-сервера Sigur 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.

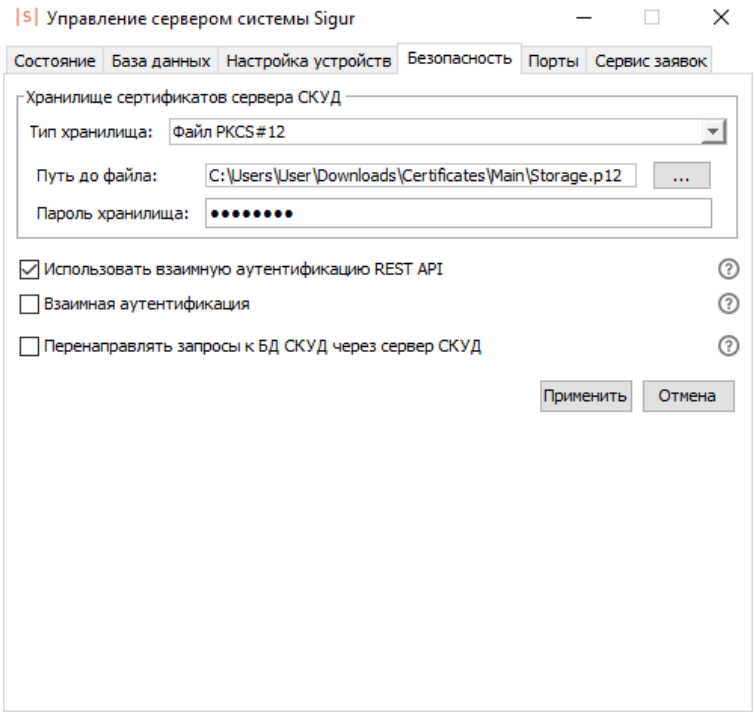
Настройка взаимной аутентификации и списка отозванных сертификатов.

Опционально можно активировать взаимную аутентификацию при подключении на порт веб-сервера Sigur. В этом случае внешняя система, пытающаяся установить защищённое соединение, также должна предоставить свой сертификат безопасности.

Для этого необходимо:

1. Произвести предварительную настройку веб-сервера Sigur согласно описанию выше.

2. Активировать чекбокс «Использовать взаимную аутентификацию REST API» на вкладке «Безопасность» ПО «Управление сервером» и перезапустить серверный модуль.



Вкладка «Безопасность» ПО «Управление сервером».

3. Сертификат внешней системы должен быть подписан доверенным корневым центром сертификации или промежуточным центром в цепочке доверия сервера Sigur.

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. Управление автотранспортом в Sigur

Система Sigur позволяет управлять как личным, так и служебным автотранспортом с помощью ПО «Клиент» и REST API.

7.1. Особенности текущей реализации

В настоящее время существуют два рекомендуемых способа администрирования данных, которые описаны ниже. Выбор способа зависит от конкретной задачи.

1. Автомобиль выступает в качестве дополнительного параметра сотрудника.

Такой способ актуален для тех задач, когда для предоставления доступа персонал может использовать не только идентификаторы типа карт/смартфонов/браслетов и пр., но также и идентификаторы автотранспорта (радиометка/брелок/гос. номер). При этом предполагается, что идентификатор автомобиля постоянно закреплён за конкретным человеком, то есть автомобиль является личным.

Для этого в учётную карточку сотрудника добавляется идентификатор автомобиля. В зависимости от типа идентификации это будет либо дополнительный номер пропуска (актуально для радиобрелоков, радиометок), либо специальный дополнительный параметр, в котором указывается гос. номер. При проезде автотранспорта система будет регистрировать событие прохода сотрудника.

При взаимодействии через REST API можно управлять идентификаторами автомобилей с помощью эндпоинтов групп Cards (радиобрелоки, радиометки) и Custom fields (гос. номера). Добавить идентификаторы автомобилей в учётные карточки сотрудников и назначить персоналу права доступа можно с использованием эндпоинтов групп Bindings и Employees.

Система также позволяет создавать отдельные объекты доступа типа «Личный автомобиль» (Employee vehicle). Однако в настоящее время не рекомендуется управлять личными автомобилями таким методом. Вместо этого рекомендуется использовать указанные выше способы, такие как добавление кода пропуска или доп. параметра в карточку сотрудника.

2. Автомобиль является отдельной сущностью в рамках системы, в конкретный момент времени он может быть связан с тем или иным сотрудником.

Чаще всего такая схема применима для организации работы со служебным автотранспортом и путевыми листами. Для использования в Sigur подобной функциональности необходим программный модуль «Автопарк».

Принцип работы состоит в том, что отдельные сущности типа «Служебный автомобиль» временно ассоциируются с ранее созданными сотрудниками с помощью функции администрирования путевых листов, предусмотренной в модуле «Автопарк». В системе создаётся «Служебный автомобиль» и ему присваивается либо Wiegand-идентификатор, либо гос. номер (в зависимости от способа идентификации автотранспорта). При попытке идентификации система учитывает права доступа автомобиля, а не сотрудника, который связан с ним на этот момент. Проезд транспорта фиксируется как два события: проход сотрудника и проход, совершенный объектом «Служебный автомобиль».

Через REST API можно создавать, редактировать и удалять служебные автомобили с помощью эндпоинтов группы Official Vehicles, а управлять их правами доступа — с помощью эндпоинтов группы Bindings.

Для администрирования через REST API доступен следующий набор атрибутов объектов «Служебный автомобиль» (Official vehicle):

- ID.
- Гос. номер (помещается в штатное поле «Гос. номер» в карточке автомобиля на вкладке «Персонал»).
- Отдел, к которому относится объект.
- Произвольные дополнительные параметры. При создании дополнительных параметров для автотранспорта в ПО «Клиент» нужно установить опцию «Применимо к автомобилям», а при создании через REST API — убедиться, что значение параметра "entity" содержит "VEHICLES".

Управление другими информационными атрибутами автомобилей (модель, примечание и пр.) производится в интерфейсе ПО «Клиент».

В настоящее время невозможно связывать служебные автомобили с персоналом через REST API для открытия и закрытия путевых листов. Если в системе есть открытый путевой лист, то управление этим сотрудником и служебным автомобилем через REST API также будет ограничено (например, удаление таких сущностей невозможно). Для управления путевыми листами и другими функциями модуля «Автопарк» следует использовать интерфейс ПО «Клиент».

7.2. Практические примеры настройки

Рассмотрим следующие ситуации:

1. Необходимо разрешить доступ на предприятие сотруднику по распознаванию RFID-метки или гос. номера его личного автомобиля.

Для решения этой задачи можно выполнить следующие действия:

- При необходимости распознавания RFID-метки:
  - Создать новый идентификатор с помощью запроса POST api/v1/cards.
  - Добавить Wiegand-код метки в учётную карточку сотрудника с помощью запроса POST api/v1/bindings/employees-cards.
- При необходимости распознавания гос. номера:
  - Создать дополнительный параметр «Гос. номер» для сотрудников (в англоязычной локализации — LP number). Если планируется добавлять некоторым сотрудникам несколько гос. номеров, то нужно создать параметр «Гос. номера» (LP numbers). В него можно внести как один, так и несколько номеров, перечисленных через запятую.

    Параметр можно создать с помощью запроса POST api/v1/custom/fields. При этом название параметра нужно помещать в атрибут "description", а значение параметра "entity" должно содержать "EMPLOYEES".
  - Создать или отредактировать данные сотрудника, указав в доп. параметре гос. номер автомобиля. Для выполнения этой операции через REST API используются эндпоинты группы Employees. В Sigur необходимо добавлять гос. номера в том же формате, в котором их отправляет внешняя видеосистема (например, Trassir отправляет гос. номера в SIgur на латинице).

    Важно, чтобы в системе отсутствовали самостоятельные объекты доступа типа «Личный/Служебный автомобиль» с такими же гос. номерами. В таком случае система расценит факт распознавания как попытку доступа самостоятельного объекта-автомобиля, а не сотрудника с таким же гос. номером в доп. параметре.
- Далее нужно создать режим доступа с помощью запроса POST api/v1/accessrules. По умолчанию новый режим разрешает доступ по распознаванию гос. номеров на вход и на выход. При необходимости правила режима можно отредактировать через интерфейс ПО «Клиент».

- Привязать режим к сотруднику и нужной точке доступа с помощью запросов POST api/v1/bindings/employees-accessrules и POST api/v1/bindings/accessrules-accesspoints.

- Предоставить сотруднику доступ на точку доступа с помощью запроса POST api/v1/bindings/employees-accesspoints.

2. Необходимо добавить в систему служебную машину, которой поочерёдно пользуются несколько сотрудников.

В этом случае можно выполнить следующие настройки:

- Создать объект типа Official vehicle (соответствует типу «Служебный автомобиль» в ПО «Клиент») с помощью запроса POST api/v1/vehicles/official.

- При необходимости распознавания RFID-метки — создать новый идентификатор с помощью запроса POST api/v1/cards и присвоить его служебному автомобилю с помощью запроса POST api/v1/bindings/vehicles-cards.

- Создать режим доступа с помощью запроса POST api/v1/accessrules. По умолчанию новый режим разрешает доступ по распознаванию гос. номеров на вход и на выход. При необходимости правила режима можно отредактировать через интерфейс ПО «Клиент».

- Присвоить созданный режим служебному автомобилю и точкам доступа запросами POST api/v1/bindings/vehicles-accessrules и POST api/v1/bindings/accessrules-accesspoints.

- Предоставить служебному автомобилю доступ на нужные точки доступа с помощью запроса POST api/v1/bindings/vehicles-accesspoints.

Открытие/закрытие путевых листов и иные действия, связанные с модулем «Автопарк», выполняются в ПО «Клиент».

8. 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