SIGUR

Руководство по настройке системы для использования функционала REST API

Редакция от 23.09.2026.

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

SEC.RU | Короткий путь к информации

Скачано с sec.ru

Оглавление

1. Введение ... 3
2. Версии документа ... 4
3. Используемые определения, обозначения и сокращения ... 10
4. Системные требования ... 11
5. Общее описание порядка взаимодействия ... 12
6. Настройка на стороне Sigur ... 14
   6.1. Основные настройки ... 14
   6.2. Шифрование трафика по TLS ... 17
7. Управление автотранспортом в Sigur ... 19
   7.1. Особенности текущей реализации ... 19
   7.2. Практические примеры настройки ... 20
8. Выдача мобильного идентификатора через REST API ... 22
   8.1. Особенности текущей реализации ... 22
   8.2. Выдача в «Пользовательском» режиме ... 23
   8.3. Выдача в «Базовом» режиме ... 23
9. Аудит действий, совершённых через REST API ... 25
   9.1. Отчёт «Журнал действий операторов» ... 25
   9.2. Список действий, фиксируемых в «Журнале действий операторов» ... 25
10. Контакты ... 31

SEC.RU | Короткий путь к информации Скачано с sec.ru

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 1.8.5.69.

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».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

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.
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».

SEC.RU | Короткий путь к информации

Скачано с sec.ru

Ревизия	Дата публикации	Что изменилось
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.

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.

SEC.RU | Короткий путь к информации Скачано с sec.ru

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. 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».

SEC.RU | Короткий путь к информации Скачано с sec.ru

Ревизия	Дата публикации	Что изменилось

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.
		• 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).

SEC.RU | Короткий путь к информации Скачано с sec.ru

Ревизия	Дата публикации	Что изменилось
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). • В описание эндпоинтов Employees, Access Rules, Custom Fields, Departments добавлена информация об атрибуте 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).

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.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Ревизия	Дата публикации	Что изменилось
0013	23 сентября 2026 г.	Добавлены разделы «Выдача мобильного идентификатора через REST API» и «Аудит действий, совершённых через REST API». Актуализирован перечень функций протокола в разделе «Общее описание порядка взаимодействия». Изменения в «Руководстве разработчика по REST API Sigur»: • Актуализирован раздел «Employee virtual identifiers (mobile ID, PIN, QR code)» в части описания выдачи мобильного идентификатора, а также добавлено описание эндпоинта GET api/v1/employees/{id}/identifiers/mobile/link. • В описание эндпоинтов группы Access rules добавлена информация об атрибуте standardWeek, который отвечает за отображение названий дней недели в днях режима в ПО «Клиент» (аналогично опции «Стандартная неделя»). • В описание эндпоинта GET api/v1/events/parsed добавлена информация о кодах запрета доступа: 40 = Waiting for PIN timed out, 41 = Same access object pass, 42 = Escort access object was denied. А также добавлена информация о типах событий: «Связь с устройством BioSmart PalmJet потеряна/восстановлена» (BIOSMART_PALMJET_EVENTS), «Изменение состояния датчика напряжения питания» (READER_POWER_STATE), «Изменение состояния датчика отрыва от стены» (READER_TAMPER_STATE), «Изменение состояния датчика температуры» (READER_TEMPERATURE_STATE), «Перезагрузка контроллера» (CONTROLLER_BOOTUP). • В описание эндпоинтов POST api/v1/employees и POST api/v1/employees/create добавлена информация о параметре bindAccessPoints, который позволяет создать сотрудника без доступа на любые точки доступа. • В описание эндпоинтов группы Employees добавлена информация о поддержке идентификатора чата MAKC — заполнение, редактирование и получение значения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

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.

SEC.RU | Короткий путь к информации Скачано с sec.ru

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».

SEC.RU | Короткий путь к информации Скачано с sec.ru

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). Формирование пригласительной ссылки для мобильного приложения «Sigur Доступ».
- 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.

SEC.RU | Короткий путь к информации Скачано с sec.ru

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.

SEC.RU | Короткий путь к информации Скачано с sec.ru

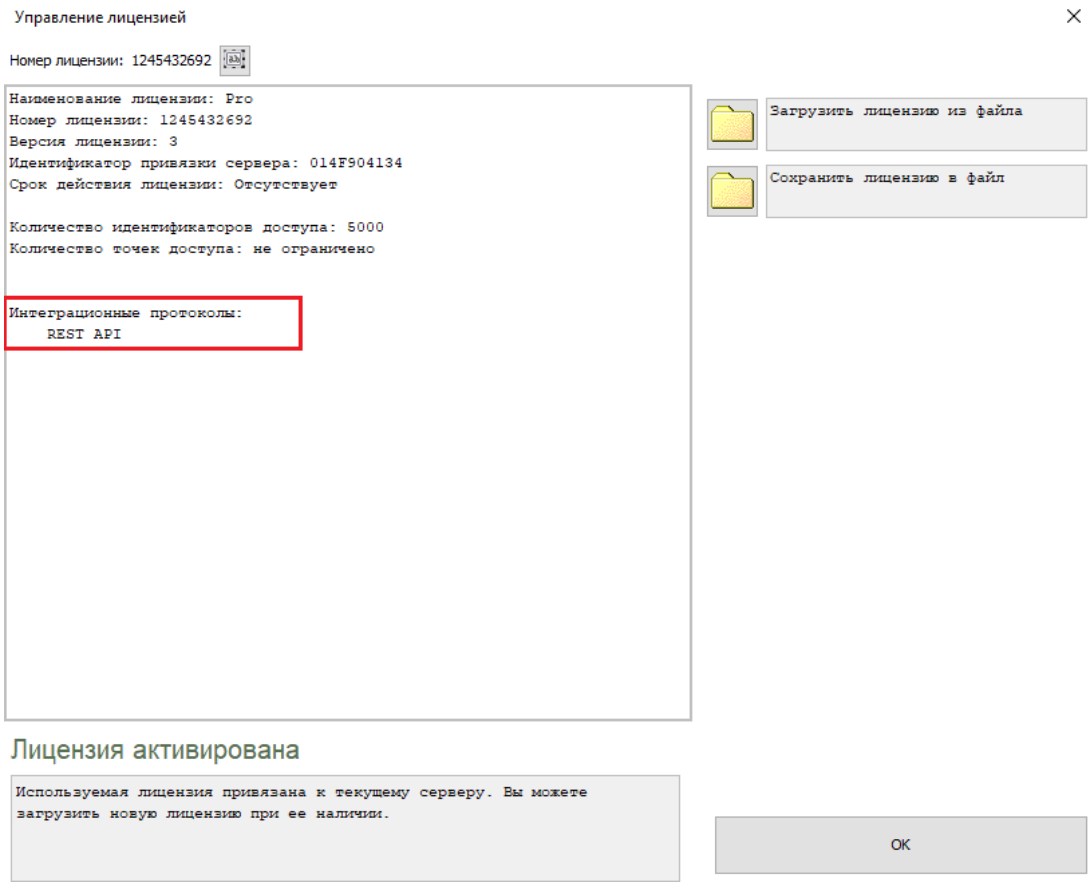
6. Настройка на стороне Sigur

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».

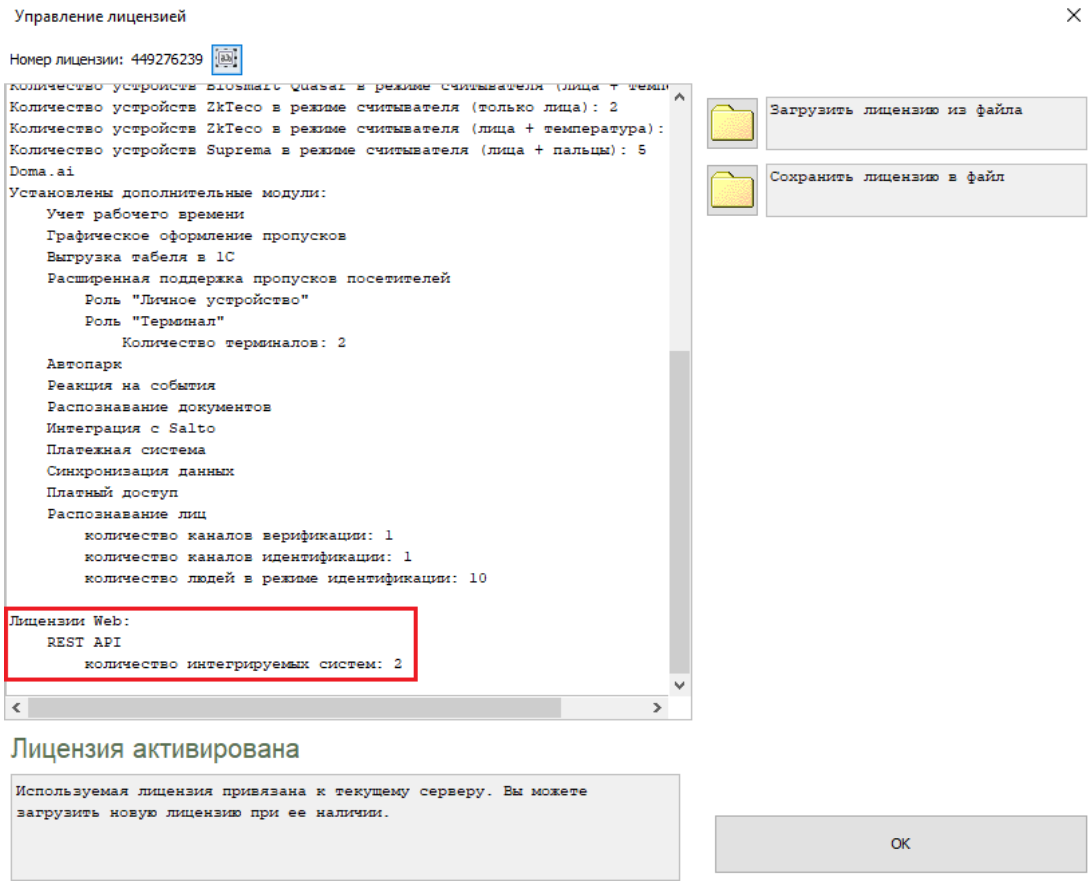


Меню «Файл» — «Управление модулями» ПО «Клиент».

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».

SEC.RU | Короткий путь к информации Скачано с sec.ru

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



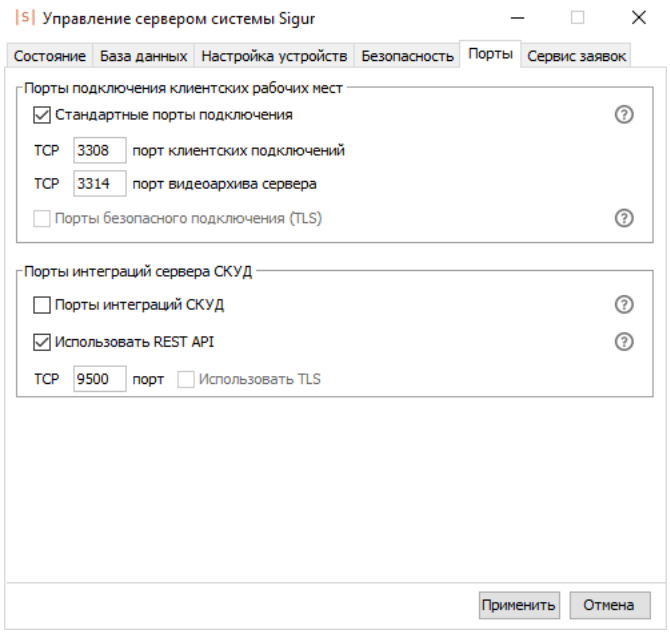
Меню «Файл» — «Управление модулями» ПО «Клиент».

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.

SEC.RU | Короткий путь к информации Скачано с sec.ru



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».

SEC.RU | Короткий путь к информации Скачано с sec.ru

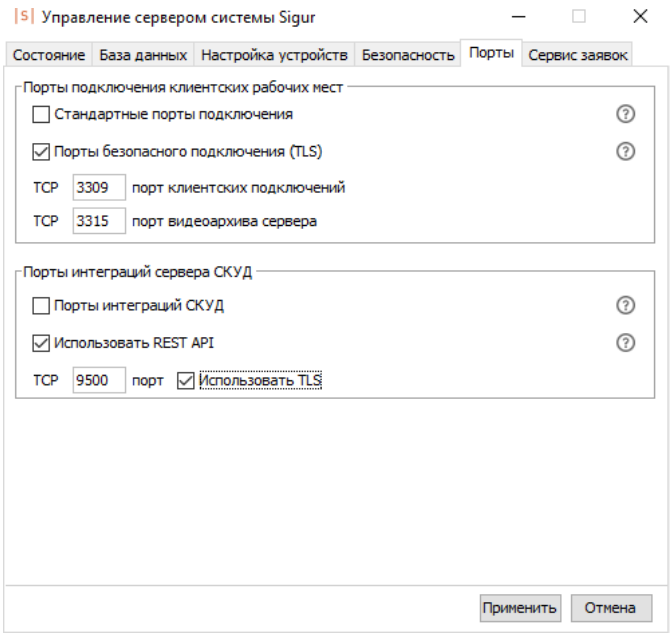
6.2. Шифрование трафика по TLS

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.

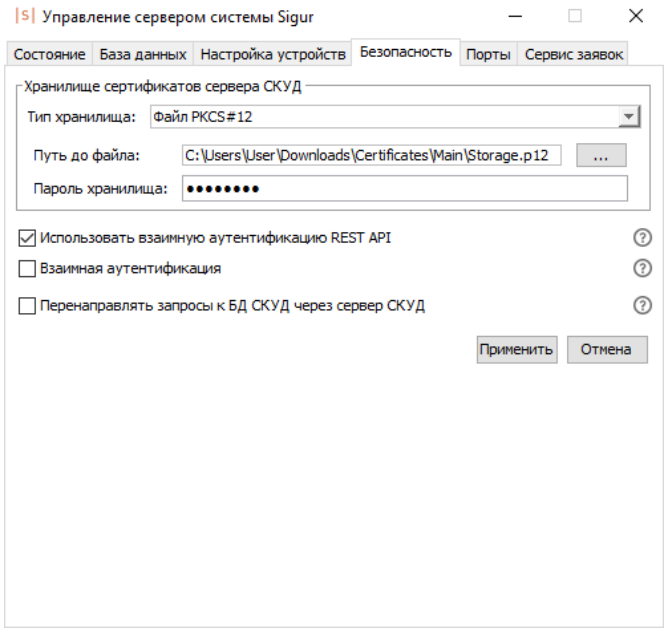
Опционально можно активировать взаимную аутентификацию при подключении на порт веб-сервера Sigur. В этом случае внешняя система, пытающаяся установить защищённое соединение, также должна предоставить свой сертификат безопасности.

Для этого необходимо:

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

SEC.RU | Короткий путь к информации Скачано с sec.ru

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.

SEC.RU | Короткий путь к информации Скачано с sec.ru

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.

SEC.RU | Короткий путь к информации Скачано с sec.ru

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).

SEC.RU | Короткий путь к информации Скачано с sec.ru

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».

SEC.RU | Короткий путь к информации Скачано с sec.ru

8. Выдача мобильного идентификатора через REST API

8.1. Особенности текущей реализации

Мобильный идентификатор может быть выдан сотруднику двумя способами: вручную оператором в ПО «Клиент» или средствами внешней системы через REST API Sigur. Оба способа доступны одновременно, использование одного из них не исключает другой. Порядок выдачи мобильного идентификатора из ПО «Клиент» описан в руководстве на используемый считыватель Sigur.

При выдаче через REST API инициатором выступает внешняя система. Система Sigur формирует мобильный идентификатор и, при необходимости, пригласительную ссылку для мобильного приложения «Sigur Доступ». Передача ссылки сотруднику выполняется средствами внешней системы.

В нижеследующих разделах описан порядок выдачи мобильного идентификатора через REST API. Порядок зависит от режима работы с мобильными идентификаторами, выбранного в ПО «Клиент», меню «Файл» – «Настройки» – «Бесконтактная идентификация» – «Мобильная идентификация»:

- «Пользовательский» режим. Считыватель реагирует только на те смартфоны, на которых мобильный идентификатор был добавлен по пригласительной ссылке. Прочие смартфоны считывателем игнорируются.
- «Базовый» режим. Считыватель реагирует на любой смартфон с установленным и запущенным приложением «Sigur Доступ».
- «Не использовать». Выдача мобильных идентификаторов недоступна.

Перед выдачей мобильных идентификаторов убедитесь, что считыватель запрограммирован на работу с мобильной идентификацией в том же режиме, в котором выдаётся идентификатор. Если на считывателе отключена мобильная идентификация или задан другой режим, выданный идентификатор не будет считан. Порядок программирования считывателя описан в руководстве на используемый считыватель.



Система Sigur не контролирует дальнейшее распространение пригласительной ссылки.

Сотрудник, получивший ссылку, может передать её сторонним лицам, которые смогут добавить мобильный идентификатор в приложение «Sigur Доступ» на своём смартфоне и совершать проходы. Все такие проходы будут зарегистрированы в системе на сотрудника, которому был выдан мобильный идентификатор. Контроль за распространением ссылки остаётся на стороне внешней системы.

Выполнение пользователем каких-либо нештатных действий со смартфоном (например, hard reset или переустановка приложения) может повлечь за собой необходимость повторной выдачи мобильного идентификатора. Также известны случаи, когда мобильный идентификатор изменялся при обновлении ОС Android.

SEC.RU | Короткий путь к информации Скачано с sec.ru

8.2. Выдача в «Пользовательском» режиме

Необходимо выполнить следующее:

1. Выдать сотруднику мобильный идентификатор запросом POST api/v1/employees/{id}/identifiers, указав значение параметра type (тип идентификатора) равным "MOBILE_ID". Номер пропуска можно задать вручную в параметре value либо сформировать автоматически с помощью параметра autogenerate. Запрос выполняется при соблюдении следующих условий:

   - объект доступа имеет тип «Сотрудник»;
   - в ПО «Клиент» выбран «Пользовательский» режим работы с мобильными идентификаторами и задан ненулевой ключ;
   - сотруднику назначено менее 5 пропусков (или 5, один из которых является мобильным идентификатором).

   В результате выполнения запроса сотруднику будет добавлен пропуск с типом «Мобильный ID». Если сотруднику ранее был выдан мобильный идентификатор, поведение запроса определяется параметром replace: при значении true ранее выданный идентификатор заменяется новым, при значении false в ответ возвращается ошибка.

2. Получить пригласительную ссылку запросом GET api/v1/employees/{id}/identifiers/mobile/link. Ссылка формируется только в том случае, если сотруднику был выдан мобильный идентификатор.
3. Передать полученную ссылку сотруднику средствами внешней системы.
4. Открыть ссылку на смартфоне с установленным приложением «Sigur Доступ» версии 1.4.0 или выше. Мобильный идентификатор сохраняется в приложении, после чего сотрудник сможет совершать проходы.

В приложении «Sigur Доступ» может храниться только один мобильный идентификатор для одного сервера Sigur. При добавлении нового идентификатора для того же сервера ранее добавленный перезаписывается. Ограничение на количество идентификаторов, выданных разными серверами Sigur, отсутствует.

8.3. Выдача в «Базовом» режиме

Необходимо выполнить следующее:

1. Получить ID из мобильного приложения «Sigur Доступ». Для этого необходимо нажать на три точки в правом верхнем углу экрана, далее нажать «О программе» и в открывшемся окне скопировать значение из строки «ID».
2. Сократить скопированный ID до нужной битности Wiegand, на работу с которым запрограммирован считыватель. Используются последние байты ID: для Wiegand-26 – 3 байта, Wiegand-34 – 4 байта, Wiegand-58 – 7 байт. Например, для ID 6196540B-05C7-401D-8CFF-37E295-E635C4 и формата Wiegand-58 используются последние 7 байт: FF37E295E635C4.
3. Выдать сотруднику мобильный идентификатор запросом POST api/v1/employees/{id}/identifiers. Указать значение параметра type (тип идентификатора) равным "MOBILE_ID" и передать часть ID из приложения «Sigur Доступ» в параметре value. Параметр autogenerate в данном режиме не используется. Запрос выполняется при соблюдении следующих условий:

   - объект доступа имеет тип «Сотрудник»;

SEC.RU | Короткий путь к информации Скачано с sec.ru

- в ПО «Клиент» выбран «Базовый» режим работы с мобильными идентификаторами;
- сотруднику назначено менее 5 пропусков (или 5, один из которых является мобильным идентификатором).

В результате выполнения запроса сотруднику будет добавлен пропуск с типом «Мобильный ID». После этого сотрудник может совершать проходы с помощью приложения «Sigur Доступ», дополнительных действий не требуется.

Если сотруднику уже выдан мобильный идентификатор, поведение запроса определяется параметром replace: при значении true ранее выданный идентификатор заменяется новым, при значении false в ответ возвращается ошибка.

SEC.RU | Короткий путь к информации Скачано с sec.ru

9. Аудит действий, совершённых через REST API

9.1. Отчёт «Журнал действий операторов»

Действия, выполненные внешней системой через REST API, фиксируются в отчёте «Журнал действий операторов». Подробную информацию о назначении отчёта, порядке его формирования, составе параметров и полном перечне фиксируемых действий см. в разделе «Отчёт «Журнал действий операторов» «Руководства пользователя ПО Sigur».

Чтобы получить информацию о действиях, выполненных через REST API:

1. На вкладке «Отчёты» ПО «Клиент» сформируйте отчёт «Журнал действий операторов» за нужный период. Убедитесь, что в блоке «Включать в отчёт» активирован параметр «Источник и способ выполнения действия» (включён по умолчанию).
2. Отфильтруйте полученный файл по колонке «Источник действия», значение «REST API».

Колонка «Способ выполнения действия» содержит информацию о методе и эндпоинте API, колонка «Описание» – текстовое описание самого действия.

Протоколируются только запросы, изменяющие данные в системе. Выполнение GET-запросов не фиксируется.

При изменении секретных атрибутов (пароли, PIN-коды) их значения в отчёте не отображаются: в соответствующих колонках выводится системное значение «недоступно», при этом факт изменения атрибута фиксируется.

Ниже перечислены запросы REST API, выполнение которых фиксируется в «Журнале действий операторов», и соответствующие им записи.

9.2. Список действий, фиксируемых в «Журнале действий операторов»

Отделы (Departments).

Запрос	Условие	Описание действия в отчёте
POST /api/v1/departments, POST /api/v1/departments/create	При указании любых параметров	Создан отдел "Название отдела" в надотделе "Название надотдела".
PUT /api/v1/departments/{id}, POST /api/v1/departments/update	Изменение параметра parentId	Отдел "Название отдела" перемещён в "Название надотдела".
PUT /api/v1/departments/{id}, POST /api/v1/departments/update	Изменение параметров name, tabId, description, customField	Изменена информация об отделе "Название отдела".
DELETE /api/v1/departments/{id}, POST /api/v1/departments/delete	_	Отдел "Название отдела" удалён.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Должности (Positions).

Запрос	Условие	Описание действия в отчёте
POST /api/v1/positions, POST /api/v1/positions/create	При указании любых параметров	Создана должность "Название должности".
PUT /api/v1/positions/{id}, POST /api/v1/positions/update	Изменение параметра name	Изменено название должности с "Предыдущее название должности" на "Название должности".
DELETE /api/v1/positions/{id}, POST /api/v1/positions/delete	_	Должность "Название должности" удалена.

Объекты доступа (Employees, Official vehicles, Guests).

Тип объекта доступа в записи отчёта определяется группой эндпоинтов, к которой выполнен запрос: сотрудник, служебный автотранспорт или гостевой пропуск.

Запрос	Условие	Описание действия в отчёте
POST /api/v1/employees, POST /api/v1/employees/create, POST /api/v1/vehicles/official, POST /api/v1/vehicles/official/create, POST /api/v1/guests/guestcards, POST /api/v1/guests/guestcards/create	При указании любых параметров	Создан объект доступа "Имя объекта доступа" в отделе "Название отдела".
POST /api/v1/employees, PUT /api/v1/employees/{id}, POST /api/v1/employees/update, POST /api/v1/vehicles/official, PUT /api/v1/vehicles/official/{id}, POST /api/v1/vehicles/official/update	Изменение параметра photo, если фотография ранее отсутствовала	Добавлена фотография объекта доступа "Имя/Гос.номер/Название объекта доступа".
PUT /api/v1/employees/{id}, POST /api/v1/employees/update, PUT /api/v1/vehicles/official/{id}, POST /api/v1/vehicles/official/update	Изменение параметра photo	Изменена фотография объекта доступа "Имя/Гос.номер/Название объекта доступа".
PUT /api/v1/employees/{id}, POST /api/v1/employees/update, PUT /api/v1/vehicles/official/{id}, POST /api/v1/vehicles/official/update	Изменение параметров departmentId, departmentName	Объект доступа "Имя/Гос.номер/Название объекта доступа" перемещён в отдел "Название нового отдела".
PUT /api/v1/employees/{id}, POST /api/v1/employees/update	Изменение параметров name, tabId, description, positionId, customField	Изменена информация об объекте доступа "Имя/Гос.номер/Название объекта доступа".

SEC.RU | Короткий путь к информации Скачано с sec.ru

Запрос	Условие	Описание действия в отчёте
PUT /api/v1/vehicles/official/{id}, POST /api/v1/vehicles/official/update	Изменение параметра lpNumber	Изменена информация об объекте доступа "Имя/Гос.номер/Название объекта доступа".
PUT /api/v1/guests/guestcards/{id}, POST /api/v1/guests/guestcards/update	Изменение параметров name, description, customField	Изменена информация об объекте доступа "Имя/Гос.номер/Название объекта доступа".
PUT /api/v1/employees/{id}, POST /api/v1/employees/update	Изменение параметра contactDetails	Изменены контактные данные объекта доступа "Имя/Гос.номер/Название объекта доступа".
PUT /api/v1/employees/{id}, POST /api/v1/employees/update, PUT /api/v1/vehicles/official/{id}, POST /api/v1/vehicles/official/update	Изменение параметра verificationPin	Изменён PIN (верификации) у объекта доступа "Имя/Гос.номер/Название объекта доступа".
PUT /api/v1/employees/{id}, POST /api/v1/employees/update, PUT /api/v1/vehicles/official/{id}, POST /api/v1/vehicles/official/update	Изменение параметров accessStartTime, accessEndTime	Изменён срок доступа объекта доступа "Имя/Гос.номер/Название объекта доступа".
PUT /api/v1/employees/{id}/block, POST /api/v1/employees/block	–	Объект доступа "Имя/Гос.номер/Название объекта доступа" заблокирован.
PUT /api/v1/employees/{id}/unblock, POST /api/v1/employees/unblock	–	Объект доступа "Имя/Гос.номер/Название объекта доступа" разблокирован.
DELETE /api/v1/employees/{id}, POST /api/v1/employees/delete, DELETE /api/v1/vehicles/official/{id}, POST /api/v1/vehicles/official/delete, DELETE /api/v1/guests/guestcards/{id}, POST /api/v1/guests/guestcards/delete	–	Объект доступа "Имя/Гос.номер/Название объекта доступа" удалён.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Пропуска (Cards, Bindings: Employees and cards, Vehicles and cards).

Запрос	Условие	Описание действия в отчёте
POST /api/v1/bindings/employees-cards, POST /api/v1/employees/{id}/identifiers, POST /api/v1/bindings/vehicles-cards	При указании любых параметров	Выдан пропуск с типом "Тип пропуска" объекту доступа "Имя/Гос.номер/Название объекта доступа".
PUT /api/v1/cards/{id}, POST /api/v1/cards/update	Изменение параметров name, value, formattedValue, format, customField	Изменён комментарий к пропуску "Номер пропуска" с типом "Тип пропуска" объекта доступа "Имя/Гос.номер/Название объекта доступа".
PUT /api/v1/bindings/employees-cards, PATCH /api/v1/bindings/employees-cards, PATCH /api/v1/employees/{id}/identifiers, PUT /api/v1/bindings/vehicles-cards	Изменение параметров startDate, expirationDate	Изменён период действия пропуска "Номер пропуска" с типом "Тип пропуска" у объекта доступа "Имя/Гос.номер/Название объекта доступа".
POST /api/v1/bindings/employees-cards/delete, POST /api/v1/employees/{id}/identifiers/delete, POST /api/v1/bindings/vehicles-cards/delete	–	Изъят пропуск "Номер пропуска" с типом "Тип пропуска" у объекта доступа "Имя/Гос.номер/Название объекта доступа".

Назначение точки доступа (Bindings: Employees and access points, Vehicles and access points).

Запрос	Условие	Описание действия в отчёте
POST /api/v1/bindings/employees-accesspoints	Изменение параметров employeeIds, accessPointIds	Точка доступа "Название ТД (ID)" назначена объекту доступа "Имя/Гос.номер/Название объекта доступа".
POST /api/v1/bindings/vehicles-accesspoints	Изменение параметров vehicleIds, accessPointIds	Точка доступа "Название ТД (ID)" назначена объекту доступа "Имя/Гос.номер/Название объекта доступа".
POST /api/v1/bindings/employees-accesspoints/delete, POST /api/v1/bindings/vehicles-accesspoints/delete	–	Точка доступа "Название ТД (ID)" снята с объекта доступа "Имя/Гос.номер/Название объекта доступа".

SEC.RU | Короткий путь к информации Скачано с sec.ru

Назначение режима доступа (Bindings: Employees and access rules, Vehicles and access rules).

Запрос	Условие	Описание действия в отчёте
POST /api/v1/bindings/employees-accessrules, POST /api/v1/bindings/vehicles-accessrules	Если параметр level для accessRule равен 1	Изменён основной режим объекта доступа "Имя/Гос.номер/Название объекта доступа" на "Название режима Уровня 1".
POST /api/v1/bindings/employees-accessrules, POST /api/v1/bindings/vehicles-accessrules	Если параметр level для accessRule равен 2, 3, 4	Режим "Название режима" назначен объекту доступа "Имя/Гос.номер/Название объекта доступа".
POST /api/v1/bindings/employees-accessrules/delete, POST /api/v1/bindings/vehicles-accessrules/delete	–	Режим "Название режима" снят с объекта доступа "Имя/Гос.номер/Название объекта доступа".

Операторы системы (Users).

Запрос	Условие	Описание действия в отчёте
POST /api/v1/users	При указании любых параметров	Назначен статус оператора объекту доступа "Имя объекта доступа".
PUT /api/v1/users/{id}	Изменение параметра username	Изменены параметры оператора "Имя оператора".
PUT /api/v1/users/{id}	Изменение параметра password	Изменён пароль оператора "Имя оператора".
PUT /api/v1/users/{id}	Изменение параметров depRestriction, depAccessList	Изменён доступ к отделу "Название отдела" для оператора "Имя оператора".
POST /api/v1/roles/{roleId}/assign-to/{userId}	Изменение параметра roleId	Изменена роль оператора "Имя оператора" на "Новая роль".
DELETE /api/v1/roles/remove-from/{userId}	–	Изменена роль оператора "Имя оператора" на "Без доступа".

SEC.RU | Короткий путь к информации Скачано с sec.ru

Запрос	Условие	Описание действия в отчёте
DELETE /api/v1/users/{id}	–	Статус оператора снят с объекта доступа "Имя объекта доступа".

SEC.RU | Короткий путь к информации Скачано с sec.ru

10. 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

SEC.RU | Короткий путь к информации
Скачано с sec.ru