SIGUR

Руководство по настройке интеграции с системой Suprema

Редакция от 03.11.2026

«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 ... 5
4. Системные требования ... 6
5. Список поддерживаемых моделей ... 7
6. Описание интеграции ... 8
7. Подключение и настройка ... 9
   7.1. Общая схема подключения устройств ... 9
   7.2. Подключение устройств к контроллеру ... 9
   7.3. Настройки со стороны Suprema ... 10
      7.3.1. BioStar 2 ... 10
      7.3.2. Suprema Device Gateway ... 13
   7.4. Настройки со стороны Sigur ... 16
      7.4.1. Настройка сервера Sigur ... 16
      7.4.2. Настройки в ПО «Клиент» и запуск интеграции ... 19
      7.4.3. Синхронизация персонала ... 23
8. Контакты ... 26

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

1. Введение

Данный документ содержит инструкцию по настройке взаимодействия программного обеспечения системы контроля и управления доступом (СКУД) Sigur и биометрических устройств Suprema.

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

Предприятие-изготовитель несёт ответственность за точность предоставляемой документации и при существенных модификациях в программном обеспечении обязуется предоставлять обновлённую редакцию данной документации.

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 июня 2025 г.	Первая публикация.
0002	24 марта 2026 г.	Актуализирована информация в связи с добавлением поддержки ОС Linux Debian и RHEL, СУБД PostgreSQL, а также возможности подключения биометрических устройств к контроллеру Sigur по OSDP.
0003	03 ноября 2026 г.	Добавлена рекомендация по установке интеграционного сервиса и сервера Sigur на один компьютер.

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.
ПО	Программное обеспечение.
БД	База данных.
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.

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

4. Системные требования

- Версия ПО Sigur: 1.6.8.101 и выше.
- Версия сервиса интеграции с устройствами Suprema: 1.3.4 и выше.
- Версия инсталлятора Suprema Device Gateway: 1.7.1.55 и выше.
- Операционная система сервера СКУД: Windows, Linux Debian, RHEL.
- Сервер БД СКУД: MariaDB, PostgreSQL.
- Остальные системные требования: см. «Руководство администратора ПО Sigur».
- Лицензирование: лицензируется каждое подключённое к СКУД биометрическое устройство Suprema (терминал распознавания лиц, считыватель отпечатков пальцев). В случае использования пакетного лицензирования также требуется пакет лицензий Standard+, Pro или Enterprise.

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

5. Список поддерживаемых моделей

Считыватели отпечатков пальцев:

- BioEntry P2;
- BioEntry W2;
- BioLite N2.

Терминалы распознавания лиц:

- BioEntry W3;
- BioStation 3;
- FaceStation 2;
- FaceStation F2.

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

6. Описание интеграции

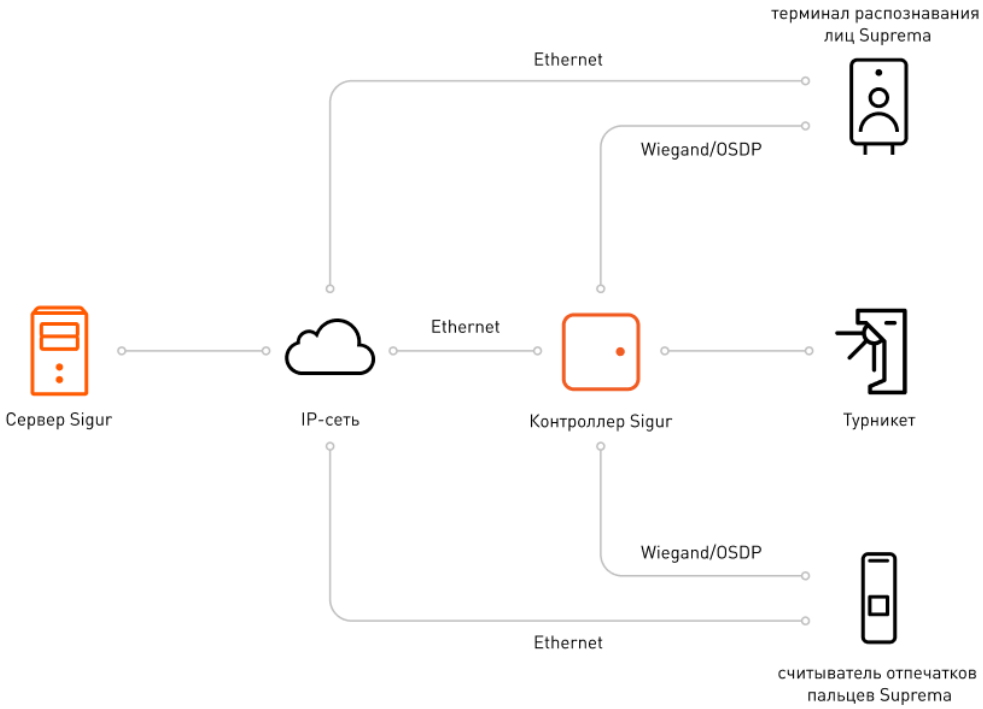
Настроенная интеграция позволяет:

- подключить терминалы распознавания лиц и считыватели отпечатков пальцев Suprema к СКУД Sigur и назначить их к точкам доступа в определённом направлении;
- добавлять и сохранять в ПО Sigur шаблоны отпечатков пальцев с помощью биометрических считывателей Suprema;
- автоматически генерировать номера пропусков, если доступ осуществляется только по распознаванию лиц или отпечатков пальцев – без использования карт;
- синхронизировать сотрудников, посетителей и идентификаторы (номера пропусков, фотографии лиц и шаблоны отпечатков пальцев) из СКУД Sigur в память биометрических устройств Suprema;
- организовать доступ по распознаванию лиц, отпечатков пальцев или в режиме двух/трёхфакторной аутентификации: карта + лицо, карта + отпечаток пальца и т. д.;
- при успешном распознавании идентификатора получать по Wiegand или OSDP код пропуска, привязанного к сотруднику или посетителю, для принятия решения о доступе на стороне СКУД Sigur.

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

7. Подключение и настройка

7.1. Общая схема подключения устройств



Общая схема подключения устройств Suprema к СКУД Sigur.

7.2. Подключение устройств к контроллеру

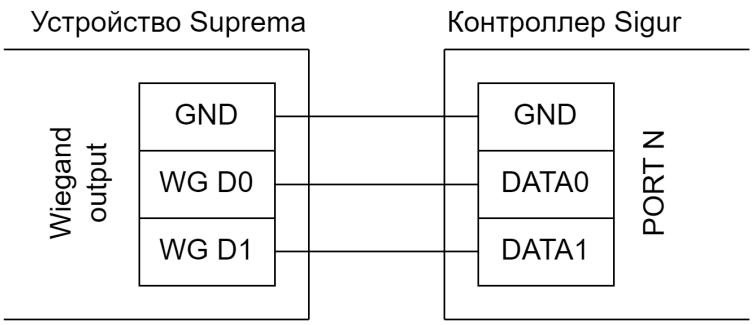


Схема подключения устройств Suprema к контроллеру Sigur по интерфейсу Wiegand.

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

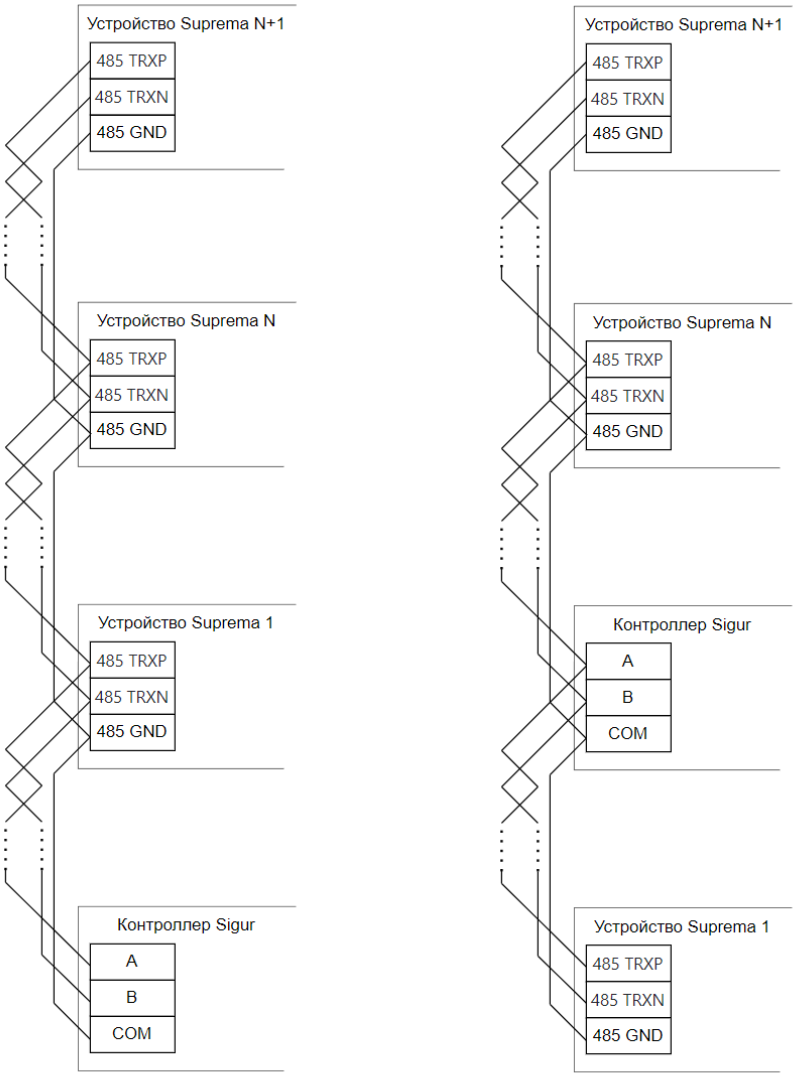


Схема подключения устройств Suprema к контроллеру Sigur по интерфейсу OSDP.

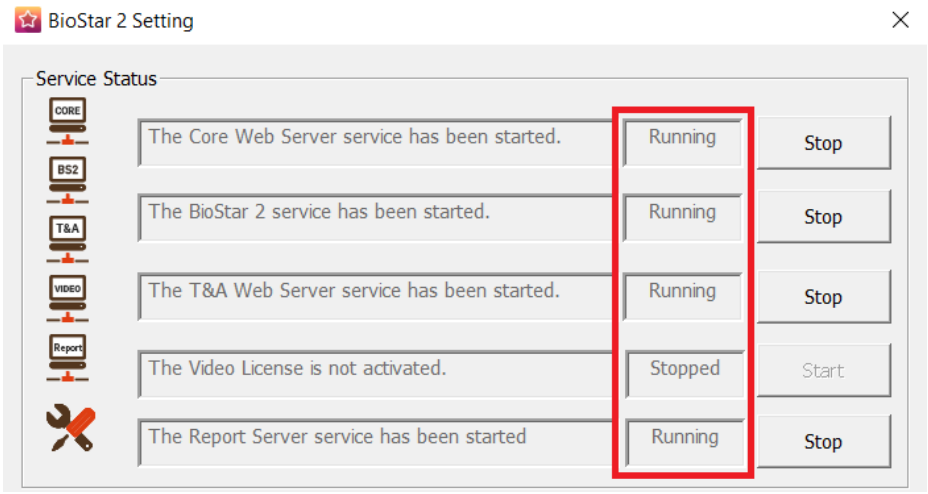
7.3. Настройки со стороны Suprema

7.3.1. BioStar 2

Для конфигурирования устройств Suprema используется ПО BioStar 2. Дистрибутив (доступен только для Windows) можно скачать после регистрации в Suprema Download Center по данной ссылке.

После установки программы необходимо запустить утилиту BioStar 2 Setting через меню «Пуск» – «BioStar 2» – «BioStar 2 Setting». Убедитесь, что сервисы BioStar 2 находятся в статусе Running (за исключением модуля Video License). При необходимости нажмите кнопку Start для их запуска.

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



Сервисы BioStar 2.

В случае если интеграция уже настроена, перед началом работы с BioStar 2 остановите службу Suprema Device Gateway service.

Далее необходимо войти в веб-интерфейс BioStar 2. Для этого введите в адресную строку браузера адрес https://127.0.0.1:443, где:

- 127.0.0.1 – IP-адрес компьютера, на котором установлено BioStar 2;
- 443 – порт по умолчанию (может быть изменён в настройках BioStar 2).

Для авторизации используется имя пользователя admin и пароль администратора, заданный во время установки BioStar 2.

В веб-интерфейсе перейдите на вкладку Device, выполните поиск и добавьте устройство Suprema. Нажмите на устройство, чтобы перейти к настройке.

Необходимо выполнить следующее:

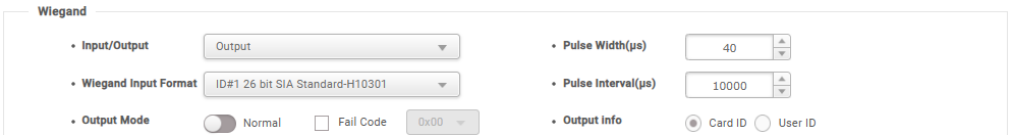
1. В блоке «Authentication» – «Card Type» задать порядок чтения карт.



Настройки чтения карт.

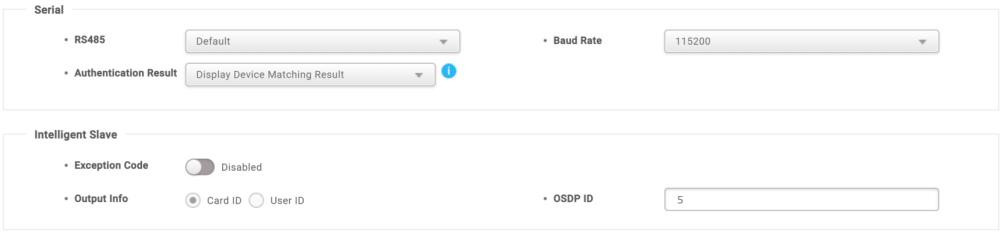
SEC.RU | Короткий путь к информации Скачано с sec.ru

2. При подключении к контроллеру Sigur по интерфейсу Wiegand: в блоке «Advanced» – «Wiegand» сконфигурировать Wiegand-выход устройства.



Настройки Wiegand-выхода.

3. При подключении к контроллеру Sigur по интерфейсу OSDP: в блоке «Network» – «Serial» для параметра RS485 установить значение Default. Также необходимо установить значения скорости передачи данных (Baud Rate) и адрес устройства (OSDP ID).



Настройки OSDP-интерфейса.

Обратите внимание, что параметры скорости передачи данных и адрес устройства необходимо также указать в настройках контроллера. Для этого обратитесь к разделу «Настройки со стороны Sigur».

4. Сохранить настройки, нажав кнопку Apply внизу страницы.

Для установления соединения сервера Sigur с устройством Suprema необходимо знать его IP-адрес и порт. Настройка сетевых параметров может выполняться непосредственно через интерфейс биометрического устройства или через веб-интерфейс BioStar 2 в разделе «Device» – «Network» (например, для моделей без дисплея).

Способ проверки личности (по карте, по карте и лицу, по отпечатку пальца и т. д.) можно изменить через интерфейс терминала или в веб-интерфейсе BioStar 2 в разделе «Device» – «Authentication».

По окончании настройки устройств необходимо остановить сервисы BioStar 2 для корректной работы интеграции. Если ранее вы останавливали службу Suprema Device Gateway service, запустите её.

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

7.3.2. Suprema Device Gateway

Для соединения и работы с биометрическими устройствами Suprema требуется компонент Suprema Device Gateway. Он может быть установлен и запущен как на сервере СКУД Sigur, так и на другом компьютере под управлением ОС Windows, Linux Debian или RHEL.

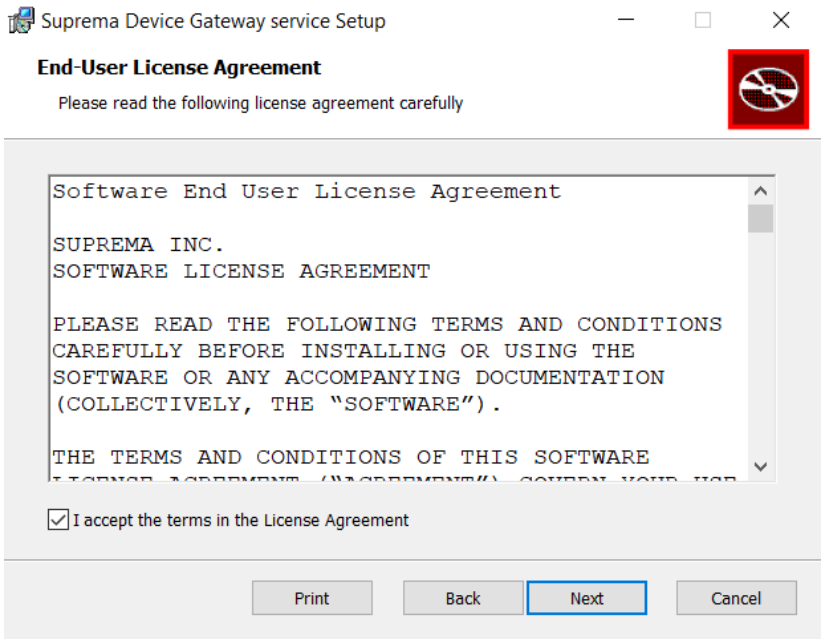
Установка Suprema Device Gateway (Windows, Linux Debian).

Необходимо выполнить следующее:

1. Скачать и запустить/установить установочный файл (Windows, Linux Debian). Пример команды для Linux Debian:

```
sudo dpkg -i suprema-device-gateway*.deb
```

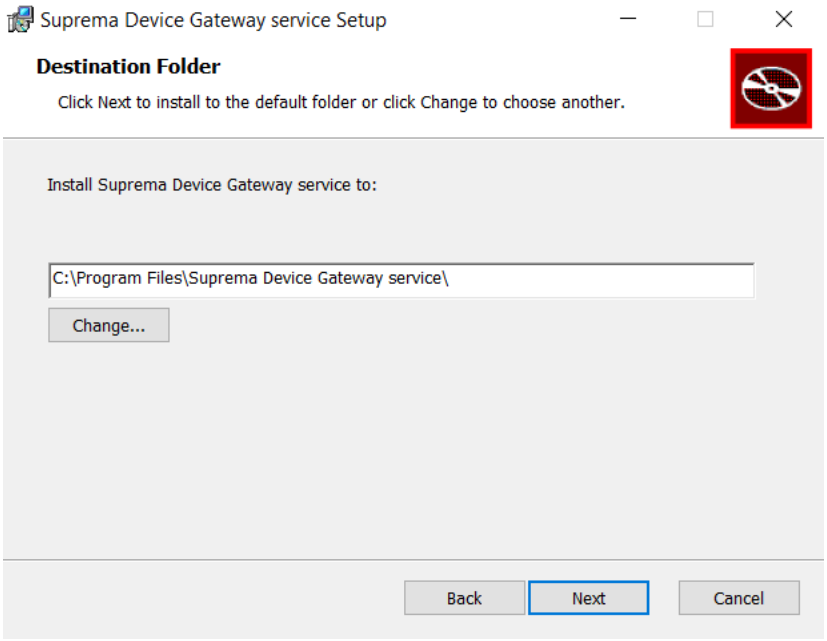
2. Выполнить шаги установки в интерактивном режиме. На одном из этапов будет необходимо ознакомиться и принять условия лицензионного соглашения Suprema.



Просмотр лицензионного соглашения на Windows.

3. В случае Windows на этапе «Destination Folder» дополнительно можно указать директорию установки, отличную от стандартной («C:\Program Files\Suprema Device Gateway service\»). После подтверждения установки система запросит административные права. Подтвердите запрос, чтобы продолжить.

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



Выбор папки для установки программы на Windows.

4. При первой установке система предложит сгенерировать пользовательские сертификаты. Сначала будет необходимо создать корневой, а затем серверный сертификат. Если пропустить этот шаг, установка будет прервана.

   - В командной строке необходимо ввести значения для каждого атрибута сертификата. Допускается использовать одинаковые данные для обоих сертификатов.
   - На шаге с вопросом «More IPv4 address?» необходимо указать все внешние IP-адреса/доменные имена, по которым будет выполняться подключение к Suprema Device Gateway. Если установка осуществляется на сервере СКУД, укажите адрес 127.0.0.1. Пример:

   ```
   >>> More IPv4 address? [y/N]: y
   >>> IPv4 Address (eg, 8.8.8.8) []: 127.0.0.1
   ```

5. Установка завершена. В системе будет зарегистрирована и автоматически запущена служба Suprema Device Gateway service (Windows) или suprema-device-gateway.service (Linux).

Установка Suprema Device Gateway (RHEL).

Необходимо выполнить следующее:

1. Скачать и установить пакет (RHEL). Пример команды:

   ```
   sudo rpm -i suprema-device-gateway*.rpm
   ```


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

2. Запустить скрипт инициализации от имени пользователя suprema-dg:

```
/opt/suprema-device-gateway/init.sh
```

3. Скрипт выведет лицензионное соглашение Suprema. Необходимо ознакомиться и согласиться с его условиями.

4. Далее будет запущен мастер генерации сертификатов. Сначала будет необходимо создать корневой, а затем серверный сертификат. Наличие сертификатов является обязательным для дальнейшей работы интеграции.

   - В командной строке необходимо ввести значения для каждого атрибута сертификата. Допускается использовать одинаковые данные для обоих сертификатов.
   - На шаге с вопросом «More IPv4 address?» необходимо указать все внешние IP-адреса/доменные имена, по которым будет выполняться подключение к Suprema Device Gateway. Если установка осуществляется на сервере СКУД, укажите адрес 127.0.0.1. Пример:

   ```
   >>> More IPv4 address? [y/N]: y
   >>> IPv4 Address (eg, 8.8.8.8) []: 127.0.0.1
   ```

5. Запустить службу suprema-device-gateway.service. Пример команд:

```
sudo systemctl enable suprema-device-gateway
sudo systemctl start suprema-device-gateway
```

6. Установка завершена.

На Windows созданные сертификаты сохраняются в каталоге cert (по умолчанию C:\Program Files\Suprema Device Gateway service\cert). На Linux сертификаты можно найти в директории /opt/suprema-device-gateway/cert. Для дальнейшей настройки интеграции потребуется CA-сертификат. При необходимости вы можете скопировать его на компьютер, где запущен сервер СКУД.

Обновление Suprema Device Gateway.

Обновление выполняется поверх установленной версии. Необходимо скачать актуальный установочный файл, запустить его и следовать всем шагам процесса обновления.

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

7.4. Настройки со стороны Sigur

7.4.1. Настройка сервера Sigur

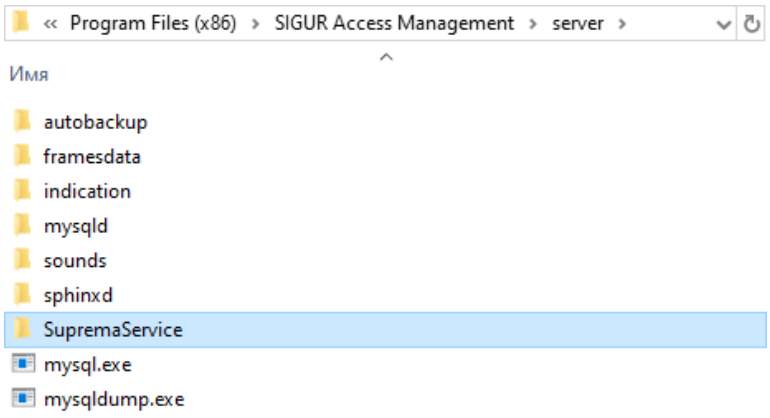
Необходимо:

1. Проверить, что установлена актуальная версия ПО Sigur. Если версия ПО Sigur ниже указанной в разделе «Системные требования», то произвести обновление ПО.
2. Скачать сервис интеграции с системой Suprema (Windows, Linux Debian, RHEL).
3. Выполнить шаги настройки соответственно операционной системе сервера Sigur.

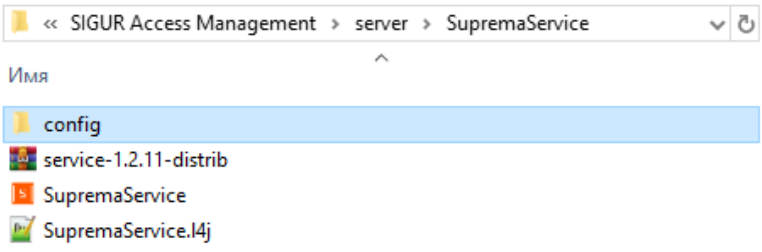
Перед установкой интеграционного сервиса убедитесь, что он устанавливается на тот же компьютер, на котором находится сервер Sigur. Это необходимо для корректной работы интеграции.

Для сервера Sigur, установленного на Windows:

1. Распаковать скачанный архив в каталог server, содержащийся в папке установки ПО Sigur (например, C:\Program Files (x86)\SIGUR access management\server). В каталоге server должна появиться папка SupremaService.



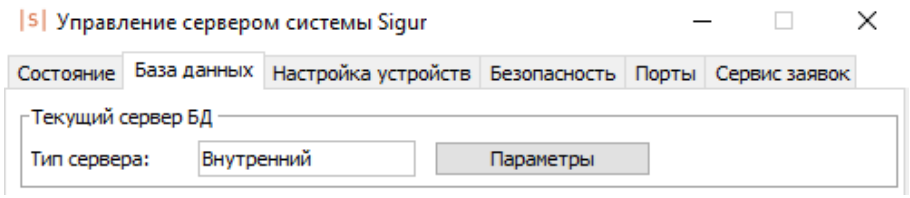
Результат распаковки архива в каталог \SIGUR access management\server.



Пример содержимого каталога SupremaService.

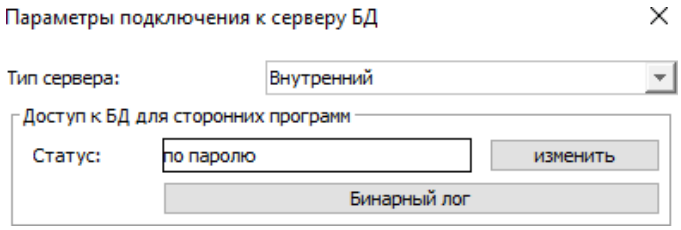
SEC.RU | Короткий путь к информации Скачано с sec.ru

2. В программе «Управление сервером» перейти на вкладку «База данных» и в блоке «Текущий сервер БД» нажать кнопку «Параметры».

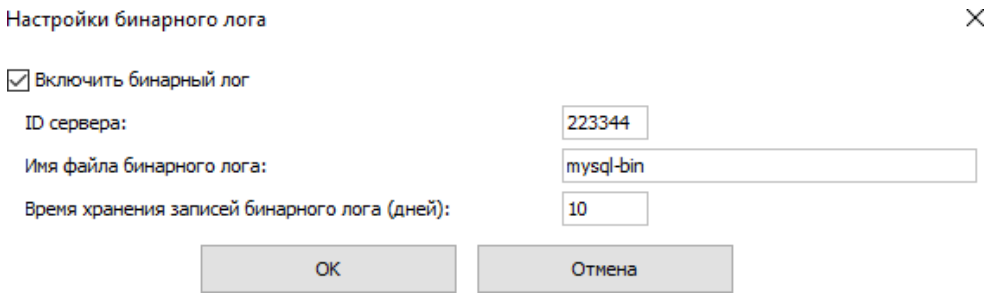


Вкладка «База данных» программы «Управление сервером».

3. В открывшемся окне нажать кнопку «Бинарный лог», после чего включить бинарный лог, оставив предложенные по умолчанию значения параметров. Сохранить настройки, нажав «ОК».



Окно «Параметры подключения к серверу БД».



Окно «Настройки бинарного лога».

4. Перезапустить серверный модуль и сервер базы данных с помощью кнопок «Стоп»/«Старт» на вкладке «Состояние» ПО «Управление сервером».

Для успешного запуска интеграции убедитесь, что сервисы BioStar 2 остановлены.

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

Для сервера Sigur, установленного на Linux Debian или RHEL:

1. Установить скачанный пакет интеграционного сервиса. Пример команд:

Linux Debian	*sudo dpkg -i suprema-service*.deb*
RHEL	*sudo rpm -i suprema-service*.rpm*

2. Перезапустить серверный модуль через ПО «Управление сервером» или утилиту AdminCLI.
3. Выполнить настройки сервера базы данных СКУД соответственно используемой СУБД.

MariaDB:

1. В конфигурационном файле сервера базы данных (например, /etc/mysql/mariadb.conf.d/50-server.cnf) в блоке параметров [mysqld] указать следующие значения для параметров:

```
server-id = 1
log_bin = mysql-bin
binlog_format = ROW
binlog_row_image = FULL
expire_logs_days = 10
```

2. Перезапустить сервер базы данных командой:

```
sudo systemctl restart mariadb
```

3. Для пользователя базы данных СКУД нужны дополнительные права на выполнение команд при работе с базой данных: RELOAD, SHOW DATABASES, REPLICATION SLAVE, REPLICATION CLIENT. Добавить их можно командой:

```
GRANT RELOAD, SHOW DATABASES, REPLICATION SLAVE, REPLICATION CLIENT ON *.* TO 'user'@'%';
```

PostgreSQL:

1. Включить WAL на стороне PostgreSQL. Необходимо указать следующие опции в конфигурационном файле postgresql.conf:

```
wal_level = logical
max_replication_slots = 1
```


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

2. Убедиться, что для хоста, где располагается интеграция, разрешены соединения для репликации. Это конфигурируется в файле pg_hba.conf. Для localhost-соединений (когда интеграция запущена на одном хосте с базой данных СКУД) разрешение включено по умолчанию строкой вида:

```
local replication postgres     trust
```

3. Предоставить пользователю базы данных СКУД права репликации:

```
CREATE ROLE repl REPLICATION LOGIN;
GRANT repl TO user;
```

4. Настроить replica identity для таблиц базы данных СКУД, которые необходимы для работы интеграции:

```
alter table accessrules replica identity full;
alter table personal replica identity full;
alter table personal_keys replica identity full;
alter table bio_templates replica identity full;
alter table devbindings replica identity full;
alter table rulebindings replica identity full;
alter table guestbindings replica identity full;
alter table guestphoto replica identity full;
alter table photo replica identity full;
alter table devices replica identity full;
```

5. Перезапустить сервер базы данных командой:

```
sudo systemctl restart postgresql
```

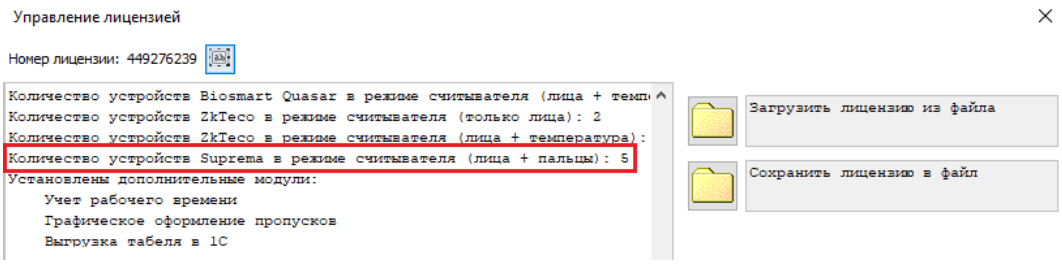
6. Перезапустить серверный модуль СКУД через ПО «Управление сервером» или утилиту AdminCLI.

7.4.2. Настройки в ПО «Клиент» и запуск интеграции

Необходимо:

1. Проверить, что присутствует лицензия на необходимое количество устройств Suprema через меню «Файл» – «Управление модулями» в ПО «Клиент».

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



Лицензия на подключение устройств Suprema.

Если лицензия на подключение терминалов отсутствует, истекла либо приобретена на меньшее количество терминалов, чем добавлено в систему, впоследствии будет выведено сообщение о превышении лицензионных ограничений.

2. Включить интеграцию с Suprema. Для этого:

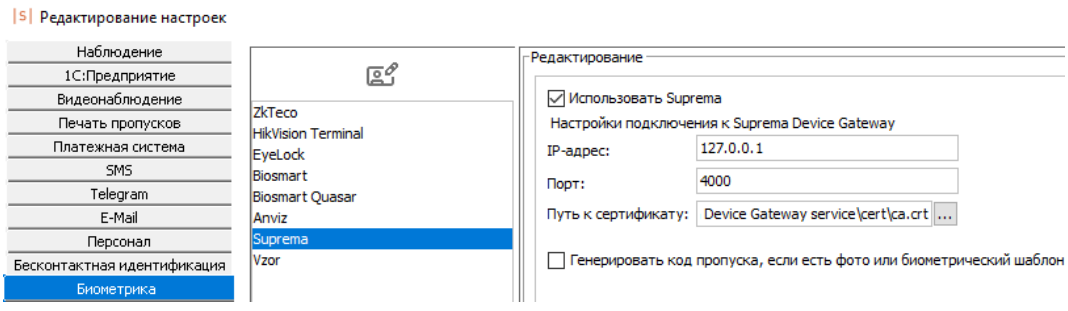
2.1. Перейти в меню ПО «Клиент» – «Файл» – «Настройки» – «Биометрика» – «Suprema» и включить опцию «Использовать Suprema».

2.2. Указать:

- IP-адрес компьютера, на котором запущен Suprema Device Gateway;
- порт (по умолчанию – 4000);
- путь к корневому сертификату Suprema Device Gateway (по умолчанию C:\Program Files\Suprema Device Gateway service\cert\ca.crt (Windows), либо /opt/suprema-device-gateway/cert/ca.crt (Linux)).

  Функция генерации кодов пропусков рассмотрена ниже в разделе «Синхронизация персонала».

2.3. Сохранить настройки, нажав кнопки «Применить» и «ОК».



Меню «Файл» – «Настройки» – «Биометрика» – «Suprema».

3. Настроить точку доступа. Для этого:

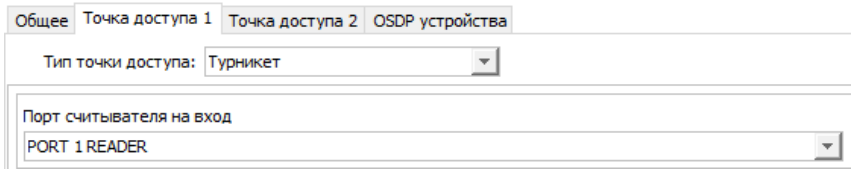
3.1. На вкладке «Оборудование» в ПО «Клиент» выделить точку доступа, с которой необходимо связать биометрическое устройство Suprema.

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

3.2. Настроить подключение устройства к контроллеру по Wiegand или OSDP.

Wiegand:

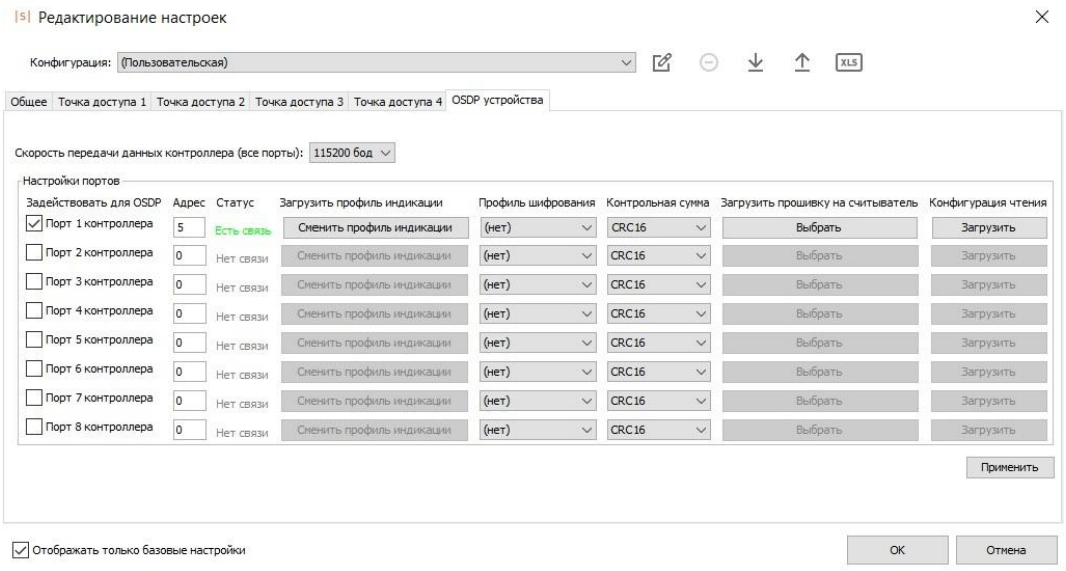
- На вкладке «Оборудование» нажать кнопку «Настройки».
- В открывшемся окне для параметра «Порт считывателя на вход» (или «Порт считывателя на выход», в зависимости от места размещения биометрического устройства) выбрать из выпадающего списка номер физического Wiegand-порта контроллера, к которому подключено устройство Suprema.
- Сохранить настройки, нажав «ОК».



Пример настройки порта контроллера.

OSDP:

- На вкладке «Оборудование» нажать кнопку «Настройки».
- В открывшемся окне перейти на вкладку «OSDP-устройства», где настраивается скорость обмена контроллера с подключёнными считывателями, а также параметры подключения биометрических устройств к логическим портам контроллера.
- Выбрать ту же скорость обмена, которая была установлена при конфигурировании устройства в веб-интерфейсе BioStar2 (подробнее в разделе «BioStar 2»).



Пример конфигурирования OSDP-устройств.

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

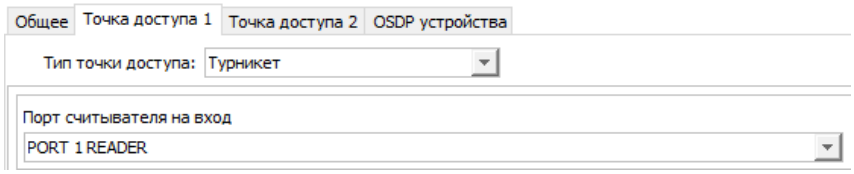
- В колонке «Задействовать для OSDP» выбрать логические порты контроллера, которые будут работать с устройствами по интерфейсу OSDP.

> При «включении» конкретного порта на вкладке «OSDP устройства» физический Wiegand-порт контроллера с таким же номером автоматически «деактивируется».

- После выбора порта указать адрес устройства на шлейфе (диапазон: от 1 до 127). Этот параметр задаётся в настройках устройства в веб-интерфейсе BioStar 2.

- Нажать кнопку «Применить». После этого можно проверить корректность настроек и подключения, отслеживая состояние в графе «Статус». Если всё выполнено правильно, появится сообщение «Есть связь».

- После конфигурирования OSDP-устройства необходимо в том же окне перейти на вкладку «Точка доступа N» и определить функцию для соответствующего логического порта считывателя. На скриншоте ниже приведён пример настройки для устройства, подключённого к первому логическому порту контроллера и выполняющего функцию считывателя в направлении «вход».



Пример настройки порта контроллера.

- Сохранить настройки, нажав «ОК».

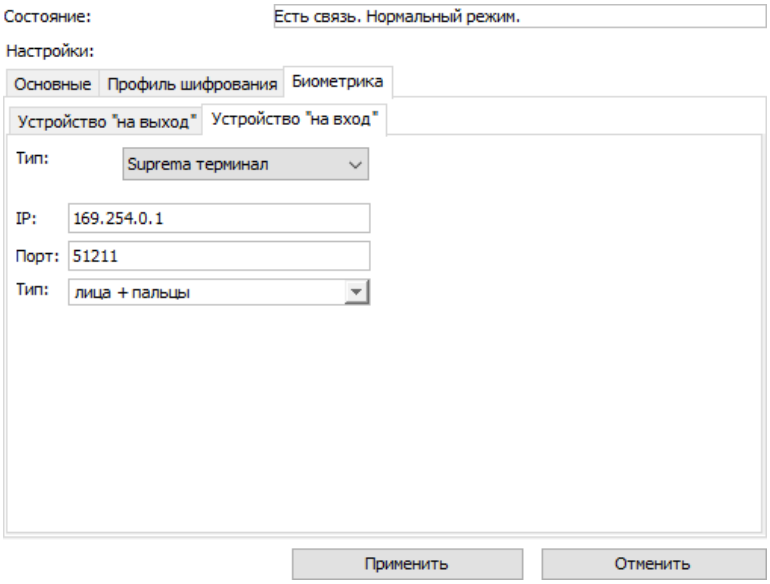
3.3. Привязать к точке доступа биометрическое устройство. Для этого:

- На вкладке «Оборудование» раскрыть подвкладку «Биометрика».
- Выбрать направление для биометрического устройства Suprema (на вход или на выход, соответственно настройкам порта контроллера).
- В выпадающем списке «Тип» выбрать «Suprema терминал», а затем указать:

  - IP-адрес устройства;
  - порт (по умолчанию – 51211, может быть изменён в интерфейсе устройства или через ПО BioStar 2 Settings);
  - тип работы устройства – «лица+пальцы» (по умолчанию).

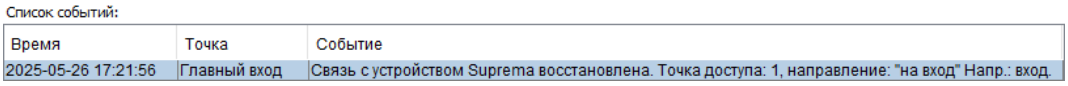
SEC.RU | Короткий путь к информации Скачано с sec.ru

- Сохранить настройки, нажав «Применить».



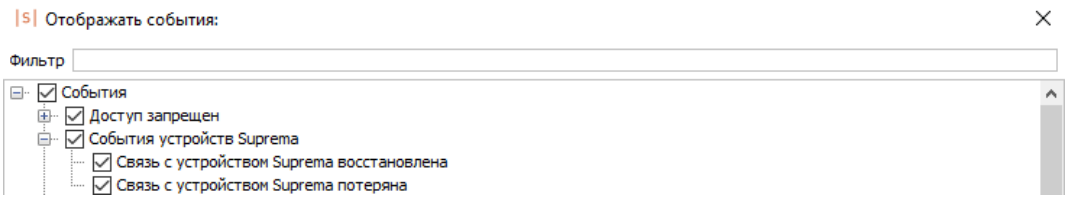
Пример настроек точки доступа на подвкладке «Биометрика».

Если все настройки выполнены корректно, в архиве событий и на вкладке «Наблюдение» ПО «Клиент» появится событие «Связь с устройством Suprema восстановлена».



Успешное установление связи с устройством Suprema.

При построении отчётов и архивной выгрузки можно настроить отображение событий восстановления и потери связи с устройствами Suprema с помощью соответствующих фильтров.



Фильтры событий устройств Suprema.

7.4.3. Синхронизация персонала

Для синхронизации данных в память устройств требуется предоставить персоналу доступ на точки доступа, к которым привязано оборудование Suprema. Синхронизируются объекты доступа (далее – ОД) типа «Сотрудник» и выданные гостевые пропуска.

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

Дополнительно необходимо:

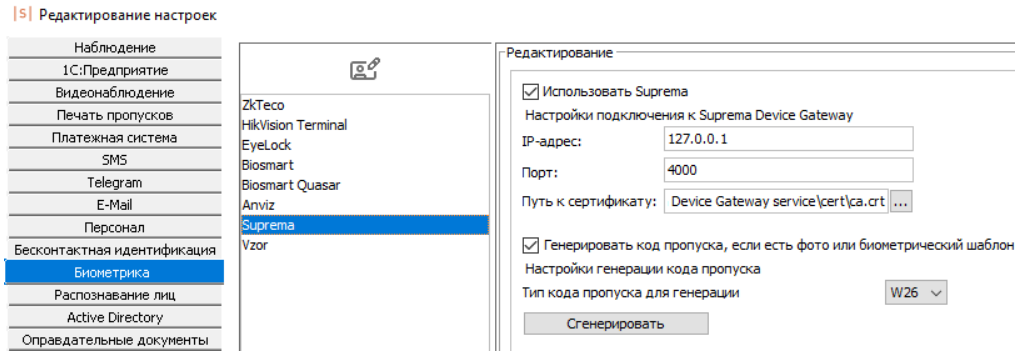
- Для доступа по распознаванию отпечатков пальцев – присвоить ОД биометрический шаблон отпечатка пальца и код пропуска в формате Wiegand-26. Добавить биометрический шаблон можно с помощью захвата с IP-устройства, выбрав пункт «Suprema терминал» из выпадающего списка «Биометрия» в учётной карточке ОД на вкладке «Персонал». Процесс описан в разделе «Работа с базой биометрических шаблонов в СКУД Sigur» в «Руководстве пользователя ПО Sigur».

- Для доступа по распознаванию лиц – присвоить ОД фотографию и код пропуска в формате Wiegand-26. При синхронизации гостевых пропусков учитывается наличие фото гостя на вкладке «Посетители».

При синхронизации ОД и пропусков учитываются их сроки действия: если срок доступа ОД или срок действия пропуска истёк или ещё не наступил, ОД или пропуск не будут синхронизированы.

Если у ОД нет физического пропуска, то вы можете вручную присвоить любой произвольный номер в указанном формате либо воспользоваться функцией генерации кодов пропусков. Для этого необходимо:

1. Перейти в меню ПО «Клиент» – «Файл» – «Настройки» – «Биометрика» – «Suprema».
2. Включить соответствующую опцию. На текущий момент доступна генерация пропусков только в формате Wiegand-26.
3. Сохранить изменения кнопками «Применить» и «ОК».



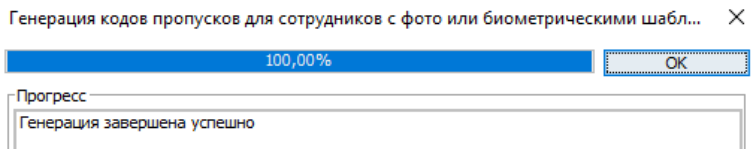
Меню «Файл» – «Настройки» – «Биометрика» – «Suprema».

Если опция включена, то пропуска будут автоматически генерироваться при каждом последующем добавлении фотографии или биометрического шаблона отпечатка пальца Suprema. Исключение – случаи, когда у ОД уже есть пропуск в формате Wiegand-26 или ему присвоено 5 номеров карт. Для гостевых пропусков генерация выполняется при добавлении шаблона отпечатка пальца на вкладке «Персонал» или фото на вкладке «Посетители».

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

Если в базе уже есть ранее добавленные ОД без пропусков, то генерацию для них нужно запустить вручную:

1. В том же меню нажать кнопку «Сгенерировать».
2. В открывшемся окне выбрать ОД в левой части, перенести их в правую с помощью кнопки >> и нажать «ОК».
3. Система выведет сообщение о результате операции. Пропуска будут сгенерированы только для тех ОД, у которых есть фотография или биометрический шаблон отпечатка пальца Suprema (за исключением случаев, когда у ОД уже есть пропуск в формате Wiegand-26 или присвоено 5 номеров карт).



Результат генерации кодов пропусков.

При успешном распознавании идентификатора биометрическое устройство отправляет на контроллер Sigur код пропуска ОД в формате Wiegand-26. Принятие решения о доступе осуществляется на стороне СКУД согласно настроенным правилам.

Список событий:

Время	Точка	Событие
2025-05-26 17:21:56	Главный вход	Связь с устройством Suprema восстановлена. Точка доступа: 1, направление: "на вход" Напр.: вход.
2025-05-26 17:23:14	Главный вход	Доступ разрешен. Объект: Иванов П. А. . Напр.: вход.
2025-05-26 17:23:15	Главный вход	Зарегистрирован проход. Объект: Иванов П. А. . Напр.: вход.

Отображение событий на вкладке «Наблюдение» по факту успешной идентификации.

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

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

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