SIGUR

Руководство по настройке интеграции с системой Suprema

Редакция от 11.06.2025.

«Промавтоматика», г. Н. Новгород, 2025 г.

Оглавление

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.

2. Версии документа

Данный документ имеет следующую историю ревизий.

Ревизия	Дата публикации	Что изменилось
0001	11 июня 2025 г.	Первая публикация.

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.

4. Системные требования

- Версия ПО Sigur: 1.6.4.108 и выше.
- Версия сервиса интеграции с устройствами Suprema: 1.2.5 и выше.
- Версия инсталлятора Suprema Device Gateway: 1.7.1.12 и выше.
- Операционная система сервера СКУД: Windows.
- Сервер БД СКУД: MariaDB.
- Остальные системные требования: см. «Руководство администратора ПО Sigur».
- Лицензирование: лицензируется каждое подключённое к СКУД биометрическое устройство Suprema (терминал распознавания лиц, считыватель отпечатков пальцев).

5. Список поддерживаемых моделей

Считыватели отпечатков пальцев:

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

Терминалы распознавания лиц:

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

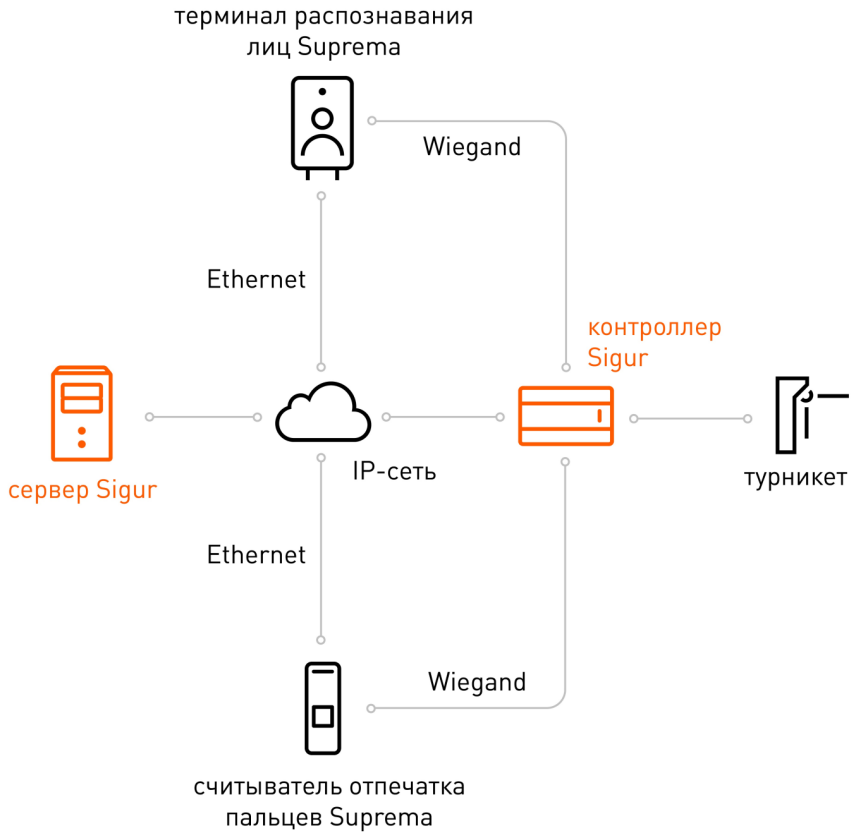
6. Описание интеграции

Настроенная интеграция позволяет:

- подключить терминалы распознавания лиц и считыватели отпечатков пальцев Suprema к СКУД Sigur и привязать 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 код пропуска, привязанного к сотруднику или посетителю для принятия решения о доступе на стороне СКУД Sigur.

7. Подключение и настройка

7.1. Общая схема подключения устройств



Общая схема подключения устройств Suprema к СКУД Sigur.

7.2. Подключение устройств к контроллеру

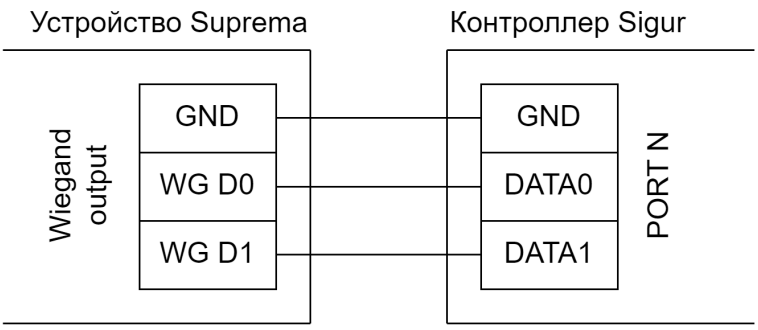


Схема подключения устройств Suprema к контроллеру Sigur.

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.

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).

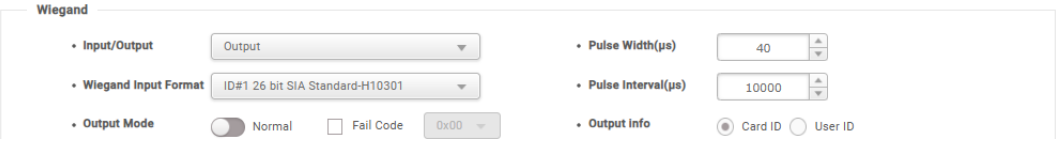
Для авторизации используется имя пользователя admin и пароль администратора, заданный во время установки BioStar 2.

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

- в блоке Authentication – Card Type задать порядок чтения карт;

Настройки чтения карт.

- в блоке Advanced – Wiegand сконфигурировать Wiegand-выход устройства;



Настройки Wiegand-выхода.

- 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.

7.3.2. Suprema Device Gateway

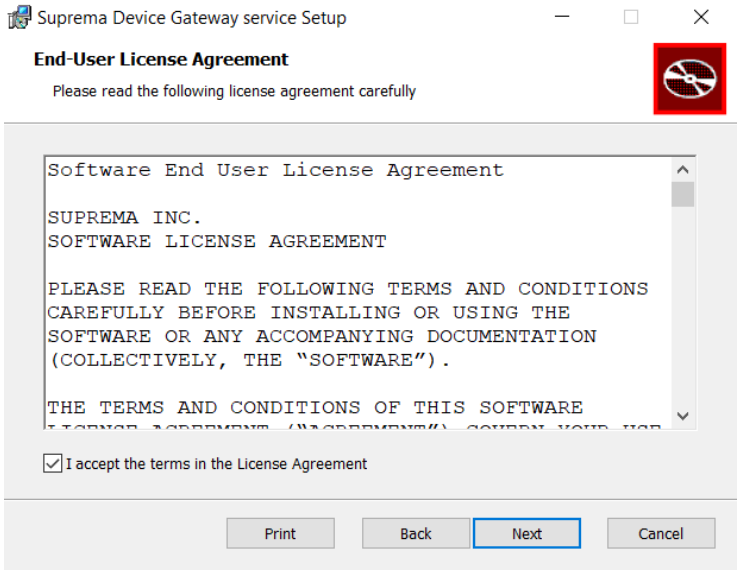
Установка Suprema Device Gateway.

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.

Необходимо выполнить следующее:

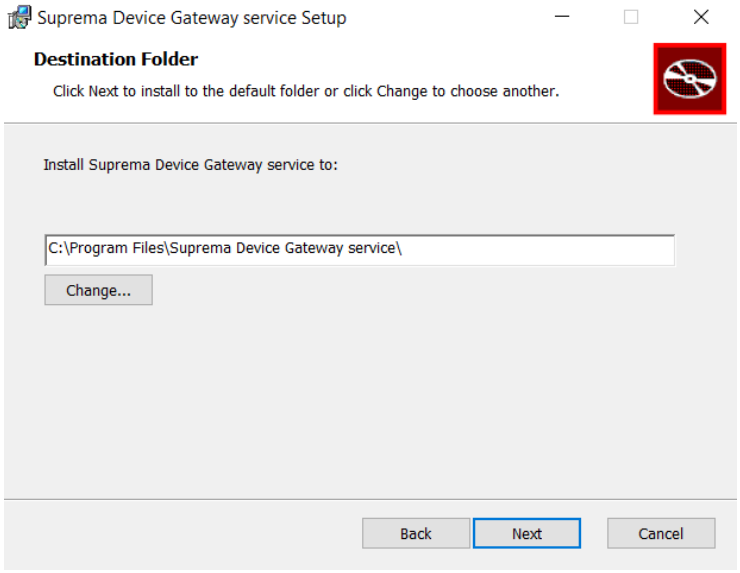
1. Скачать установочный файл по этой ссылке.
2. Запустить файл и выполнить шаги мастера установки:

   - На этапе End-User License Agreement необходимо ознакомиться и принять условия лицензионного соглашения Suprema.



Лицензионное соглашение.

   - На этапе Destination Folder можно указать директорию установки, отличную от стандартной (C:\Program Files\Suprema Device Gateway service\).



Выбор папки для установки программы.

- После подтверждения установки система запросит административные права. Подтвердите запрос, чтобы продолжить.

3. В случае первой установки появится окно генерации пользовательских сертификатов. Система последовательно предложит создать корневой, а затем серверный сертификат. Установка будет прервана, если этот шаг пропустить.

   - В командной строке необходимо ввести значения для каждого атрибута сертификата. Можно использовать одну и ту же информацию для обоих сертификатов.
   - На шаге с вопросом «More IPv4 address?» необходимо указать все внешние IP-адреса/доменные имена, по которым будет происходить подключение к Suprema Device Gateway. Если установка выполняется 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
   ```

4. Завершить установку, нажав кнопку Finish.

После установки будет зарегистрирована и автоматически запущена служба Suprema Device Gateway service.

Созданные сертификаты сохраняются в каталоге cert (по умолчанию C:\Program Files\Suprema Device Gateway service\cert). Для 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. Актуальный установочный файл можно скачать по этой ссылке. Запустите его и следуйте инструкциям инсталлятора, чтобы пройти все шаги процесса обновления. По завершении обновления служба Suprema Device Gateway service будет запущена автоматически.

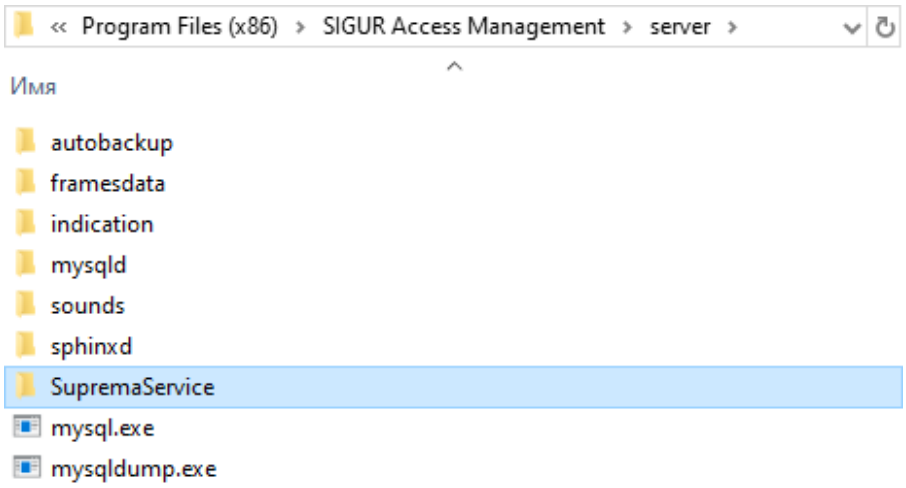
7.4. Настройки со стороны Sigur

Необходимо выполнить следующее:

- Проверить, что установлена актуальная версия ПО Sigur. Если версия ПО Sigur ниже указанной в разделе «Системные требования», то произвести обновление ПО.
- Скачать сервис интеграции с системой Suprema (версия для Windows).

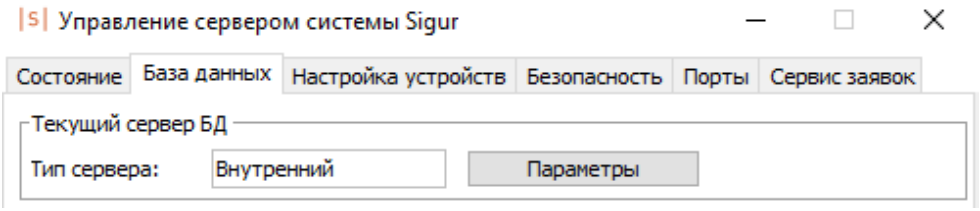
Для сервера Sigur, установленного на Windows:

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.



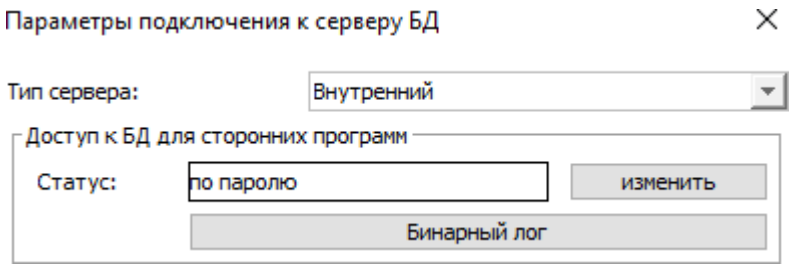
Каталог \SIGUR access management\server.

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

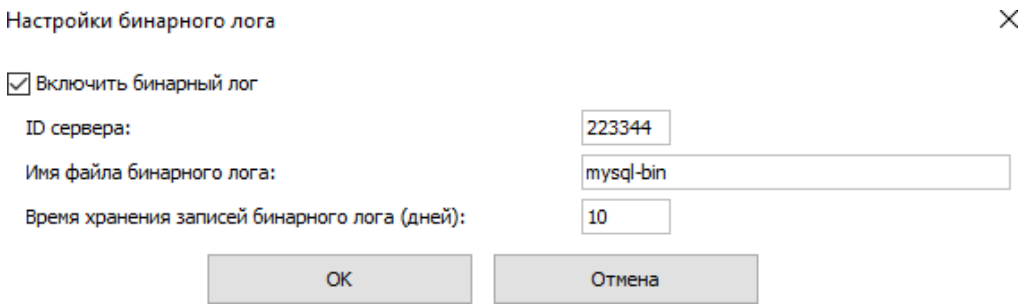


Вкладка «База данных» программы «Управление сервером».

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».

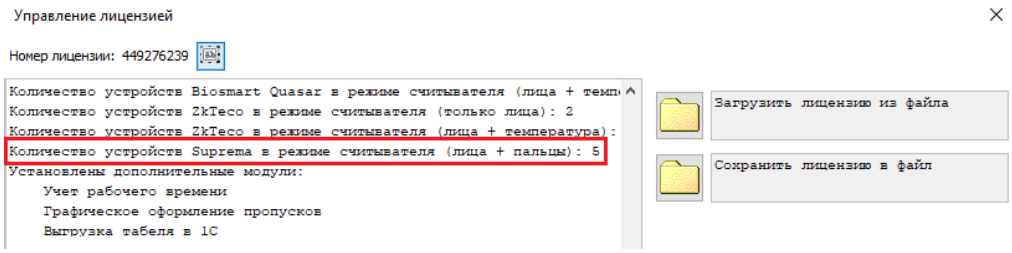
4. Перезапустить серверный модуль и сервер базы данных с помощью кнопок «Стоп»/«Старт» на вкладке «Состояние» ПО «Управление сервером».

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

Настройки в ПО «Клиент».

Далее необходимо:

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



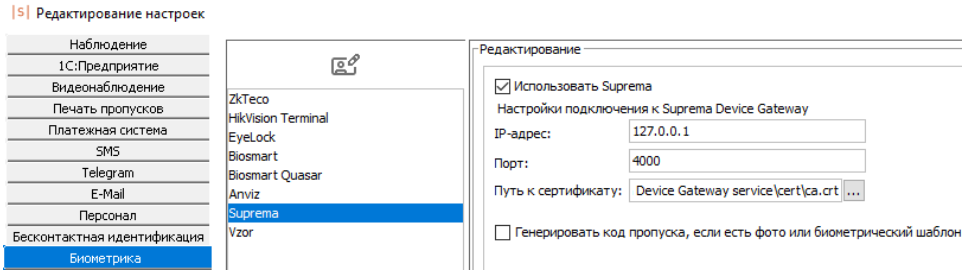
Лицензия на подключение устройств Suprema.

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:

   - Перейти в меню ПО «Клиент» – «Файл» – «Настройки» – «Биометрика» – «Suprema».
   - Включить опцию «Использовать Suprema».

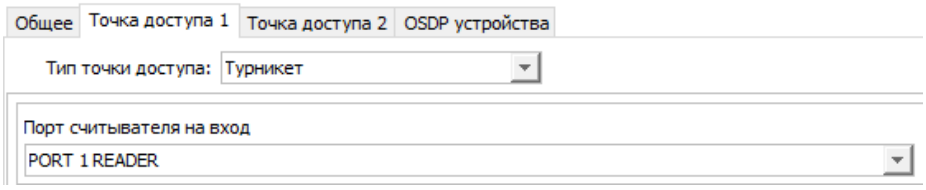
- Указать:
  - IP-адрес компьютера, на котором запущен Suprema Device Gateway;
  - порт (по умолчанию – 4000);
  - путь к корневому сертификату Suprema Device Gateway (по умолчанию C:\Program Files\Suprema Device Gateway service\cert\ca.crt).
- Сохранить настройки, нажав кнопки «Применить» и «ОК».



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

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

3. Настроить точку доступа. Для этого:
   - На вкладке «Оборудование» в ПО «Клиент» выделить в списке точку доступа, с которой необходимо связать биометрическое устройство Suprema.
   - Нажать кнопку «Настройки». В открывшемся окне для параметра «Порт считывателя на вход» (или «Порт считывателя на выход», в зависимости от места размещения биометрического терминала) из выпадающего списка выбрать номер физического Wiegand-порта контроллера, к которому подключено устройство Suprema. Сохранить настройки, нажав «ОК».

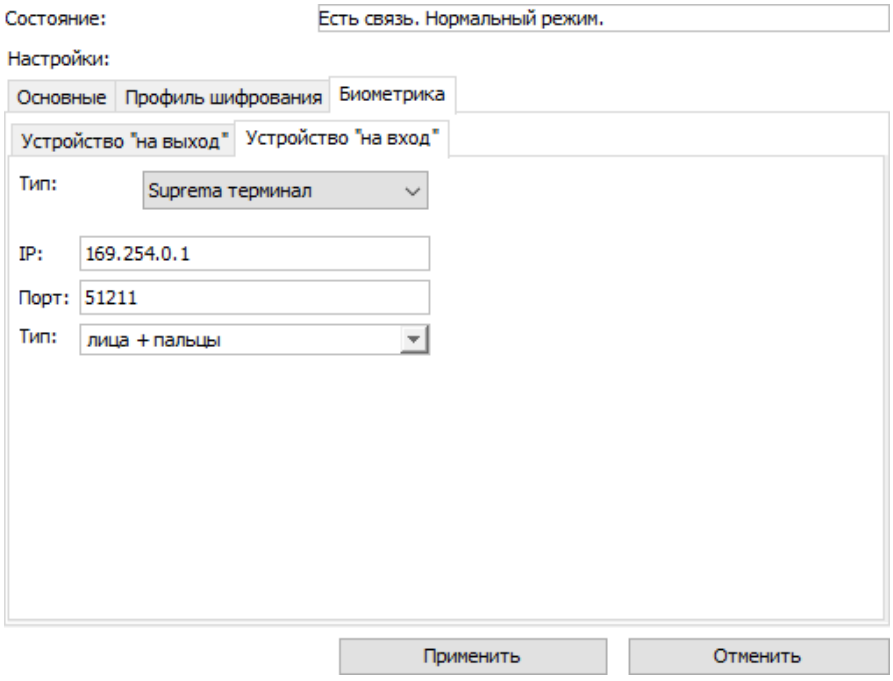


Пример настройки порта контроллера.

- Раскрыть вкладку «Биометрика» и выбрать направление подключения биометрического устройства (на вход или на выход). В выпадающем списке «Тип» необходимо выбрать «Suprema терминал», а затем указать:

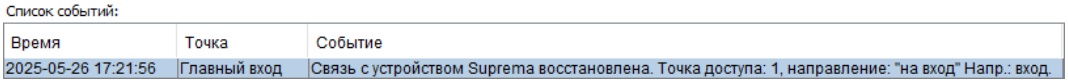
- IP-адрес устройства;
- порт (по умолчанию – 51211, может быть изменён в интерфейсе устройства или через ПО BioStar 2);
- тип работы с устройством – «лица+пальцы» (по умолчанию).

Сохраните настройки, нажав «Применить».



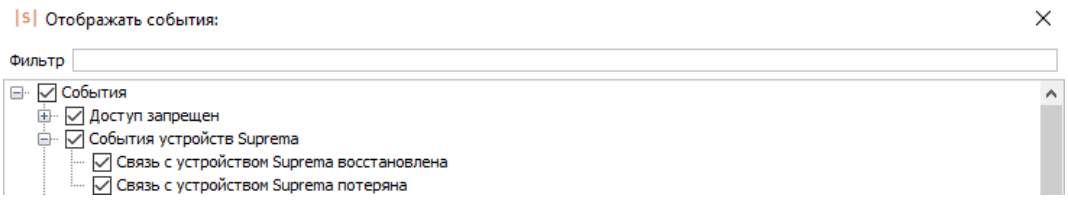
Пример настроек точки доступа на вкладке «Биометрика».

Если 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.

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.

Дополнительно необходимо:

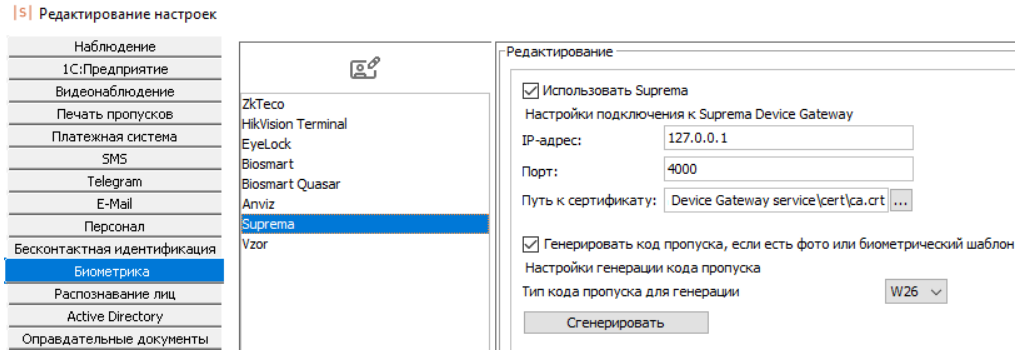
- Для доступа по распознаванию отпечатков пальцев – присвоить ОД биометрический шаблон отпечатка пальца и код пропуска в формате Wiegand-26. Добавить биометрический шаблон можно с помощью захвата с IP-устройства, выбрав пункт «Suprema терминал» из выпадающего списка «Биометрия» в учётной карточке ОД 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».



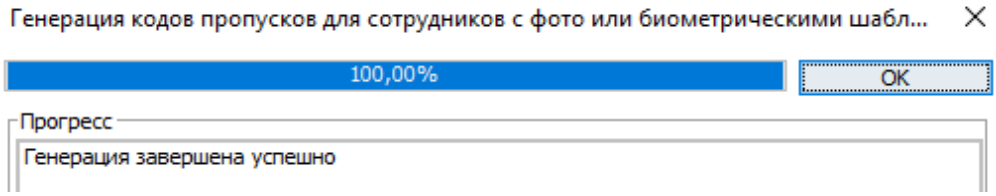
Меню «Файл» – «Настройки» – «Биометрика» – «Suprema».

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».

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

1. В том же меню нажмите кнопку «Сгенерировать».
2. В открывшемся окне выберите ОД в левой части, перенесите их в правую с помощью кнопки >> и нажмите «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.

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