



# **Руководство по подключению терминалов Biosmart Quasar**

**Редакция от 07.03.2023.**

## Оглавление

1.	Введение .....	3
2.	Используемые определения, обозначения и сокращения .....	4
3.	Системные требования .....	5
4.	Описание интеграции .....	6
5.	Подключение и настройка терминала .....	7
5.1.	Общая схема подключения терминала .....	7
5.2.	Подключение терминала к контроллеру .....	7
5.3.	Настройки со стороны Biosmart Quasar .....	8
5.4.	Настройки со стороны Sigur .....	8
6.	Контакты .....	14

# 1. Введение

Данный документ содержит инструкцию по настройке взаимодействия программного обеспечения системы контроля и управления доступом (СКУД) «Sigur» и интегрированных терминалов Biosmart Quasar.

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

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

## 2. 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.
ТД	Точка доступа.

### 3. Системные требования

- Версия ПО Sigur 1.1.1.37 и выше.
- Версия сервиса интеграции с терминалами Biosmart Quasar - 1.1.2 и выше.
- Операционная система: согласно требованиям в «Руководстве администратора системы Sigur».
- Лицензирование: Каждый подключенный к СКУД терминал лицензируется. Отдельно лицензируются терминалы, на которых требуется осуществлять измерение температуры.

Распознавание лиц происходит на самом терминале, для этого не требуются дополнительные мощности сервера СКУД.

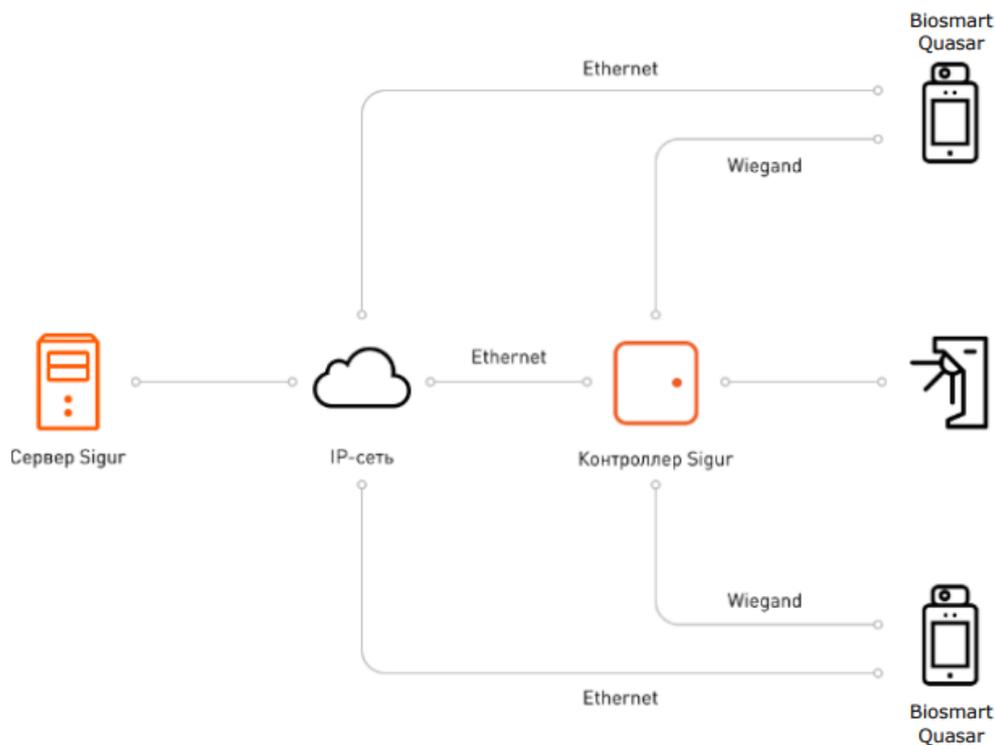
## 4. Описание интеграции

Настроенная интеграция позволяет:

- Подключить терминал Biosmart Quasar к ПО Sigur и назначить его конкретной точке доступа.
- Синхронизировать сотрудников из СКУД Sigur на устройство Biosmart Quasar.
- Организовать доступ сотрудников согласно логике идентификации (проход по лицу) или верификации (в режиме двухфакторной проверки: карта + лицо)
- Получать события о превышении температуры заданных порогов, а также сохранять результат измерения температуры каждого идентифицированного сотрудника.
- Использовать измеренную температуру в качестве дополнительного признака, по которому предоставляется доступ.
- Настраивать реакции на вышеописанные события (при наличии дополнительного модуля ПО «Реакция на события»).

## 5. Подключение и настройка терминала

### 5.1. Общая схема подключения терминала



Общая схема подключения терминала Biosmart Quasar к СКУД Sigur.

### 5.2. Подключение терминала к контроллеру

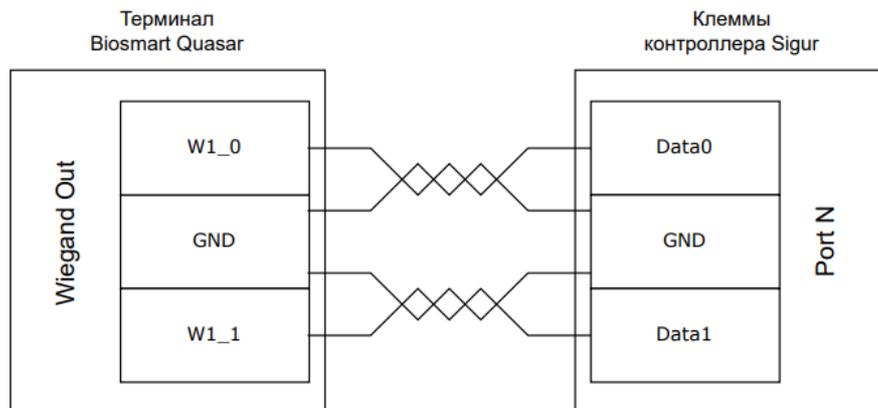


Схема подключения терминала Biosmart Quasar к контроллеру Sigur.

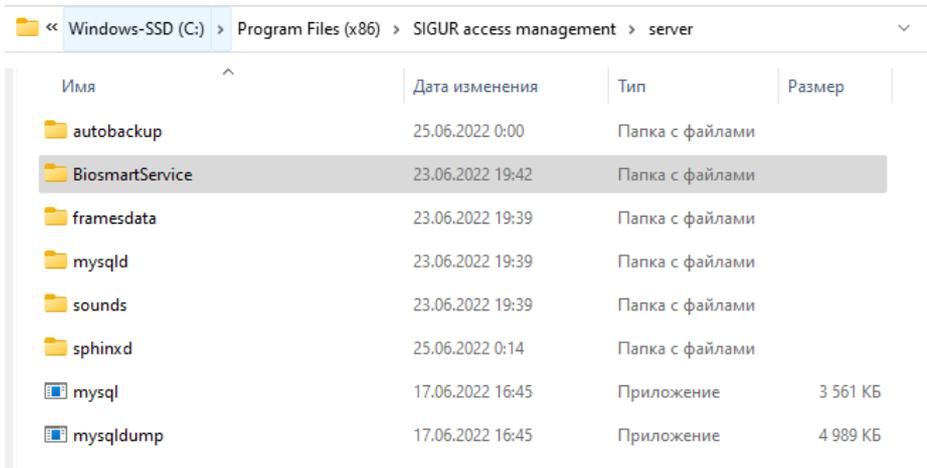
### 5.3. Настройки со стороны Biosmart Quasar

Терминал подключается в локальную сеть объекта. Первичные настройки производятся в меню настроек непосредственно на самом терминале.

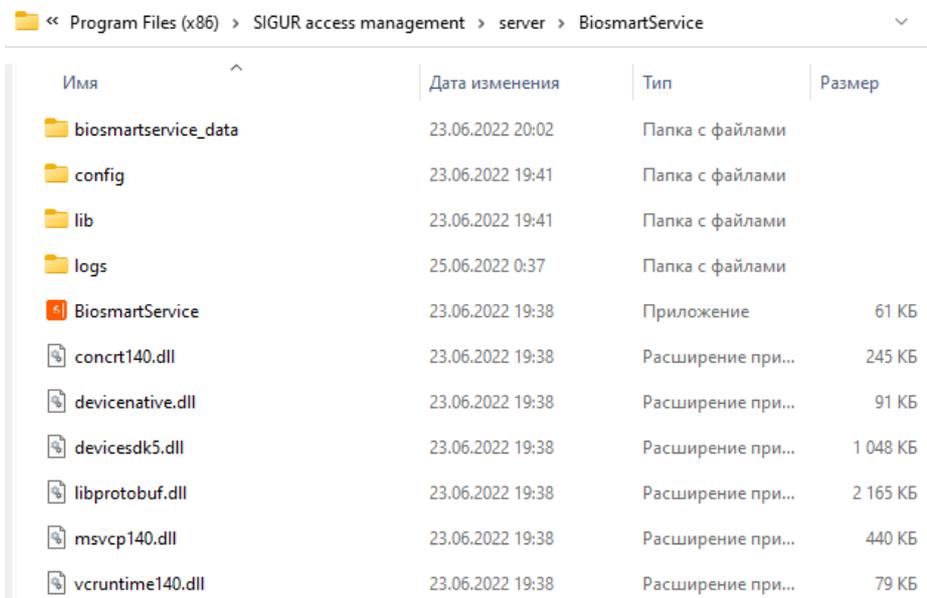
- Для настройки сетевых параметров необходимо перейти в «Меню» - «Настройки» - «Сеть». Далее задать статический IP-адрес, маску сети и адрес шлюза.
- Настройка взаимодействия по Wiegand с контроллером осуществляется через «Меню» - «Настройки» - «Система». В разделе «Wiegand 0» (задает параметры клемм W0\_0 и W0\_1) или «Wiegand 1» (задает параметры клемм W1\_0 и W1\_1) указать направление «Wiegand Out», выбрать необходимый формат Wiegand.
- Включить измерение температуры можно через «Меню» - «Система» и установить ползунок «Измерение температуры» на Вкл.
- Опционально можно настроить ограничение доступа по температуре на самом терминале в «Меню» - «Настройка внешних устройств» - «Допустимое значение температуры». В этом же меню можно указать, пропускать или нет сотрудника при превышении допустимого значения.
- Настройка типа идентификации происходит через «Меню» - «Система». Выбрать тип идентификации: «Идентификация по лицу» или «Карта + лицо».

### 5.4. Настройки со стороны Sigur

- Проверить, что установлена актуальная версия ПО «Sigur». Если версия ПО Sigur ниже, указанной в разделе «Системные требования», произвести обновление ПО.
- Скачать сервис интеграции с терминалами Biosmart Quasar ([версия для Windows](#), [версия для Linux Debian](#)).
- В случае сервера Sigur, установленного на Windows:
  - Распаковать скачанный архив с сервисом в каталог установки программы: \SIGUR access management\server\. В результате должна появиться папка BiosmartService, содержащая в себе все необходимые компоненты для работы сервиса интеграции:

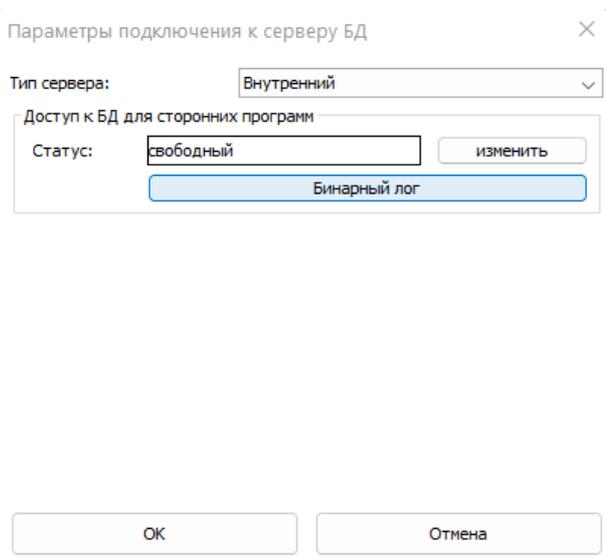


Содержимое каталога \SIGUR access management\server\.

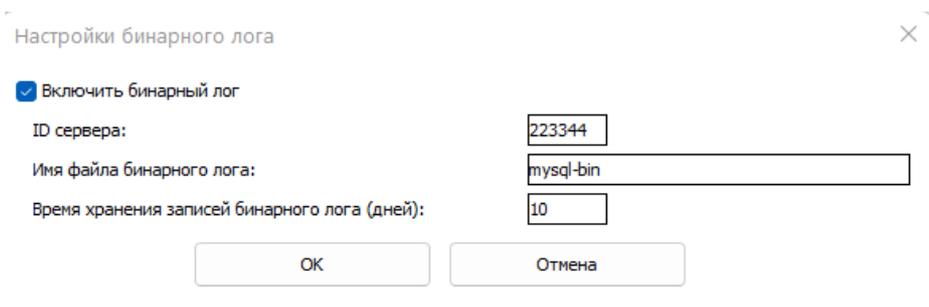


Результат распаковки архива с сервисом Biosmart.

- В программе «Управление сервером» перейти на вкладку «База данных», в блоке «Текущий сервер БД» нажать кнопку «Параметры», а в следующем окне - кнопку «Бинарный лог», после чего включить бинарный лог, оставив предложенные по умолчанию значения параметров:



Окно «Параметры подключения к серверу БД» программы «Управление сервером».



Окно «Настройки бинарного лога» программы «Управление сервером».

- Перезапустить сервер БД через программу «Управление сервером» с помощью кнопок «Стоп»/«Старт» на вкладке «Состояние».
- В случае сервера Sigur, установленного на Linux Debian:
  - Распаковать deb-пакет сервиса после установки пакета `srpxserver`.
  - Включить бинарный лог сервера БД. Для этого в конфигурационный файл сервера БД (например, `/etc/mysql/mariadb.conf.d/50-server.cnf`) в блоке параметров `[mysqld]` выставить значения для следующих параметров:

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

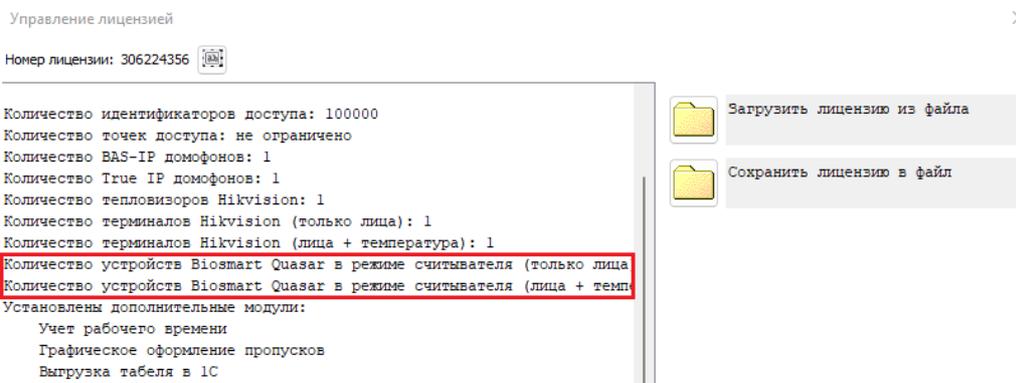
После этого перезагрузить сервер БД командой:

`sudo systemctl restart mariadb.`

- Для Linux-пользователя базы данных нужны дополнительные права на выполнение команд при работе с БД: RELOAD , SHOW DATABASES , REPLICATION SLAVE , REPLICATION CLIENT  
Добавить их можно командой:

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

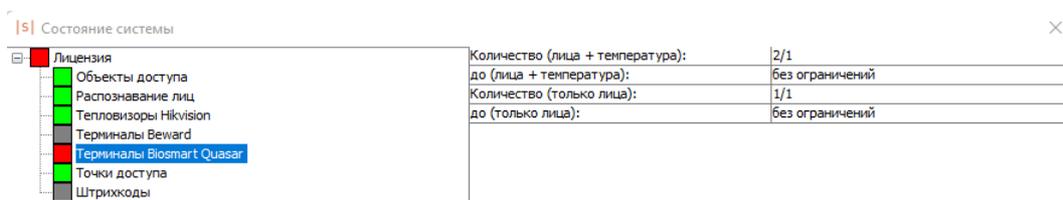
- Проверить в ПО «Клиент», что присутствует лицензия на подключение терминалов Biosmart (через диалог «Файл» - «Управление модулями»).



Отображение информации о лицензии на подключение терминалов Biosmart Quasar.

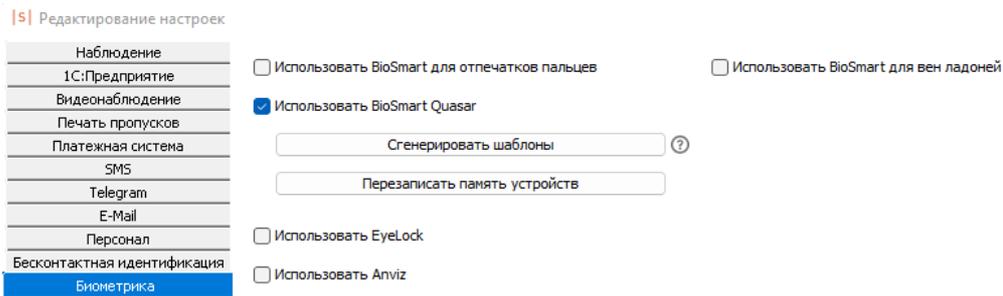


Если лицензия на подключение терминалов отсутствует, либо она приобретена на меньшее количество терминалов, чем добавлено в систему, будет выведено сообщение о превышении лицензионных ограничений.



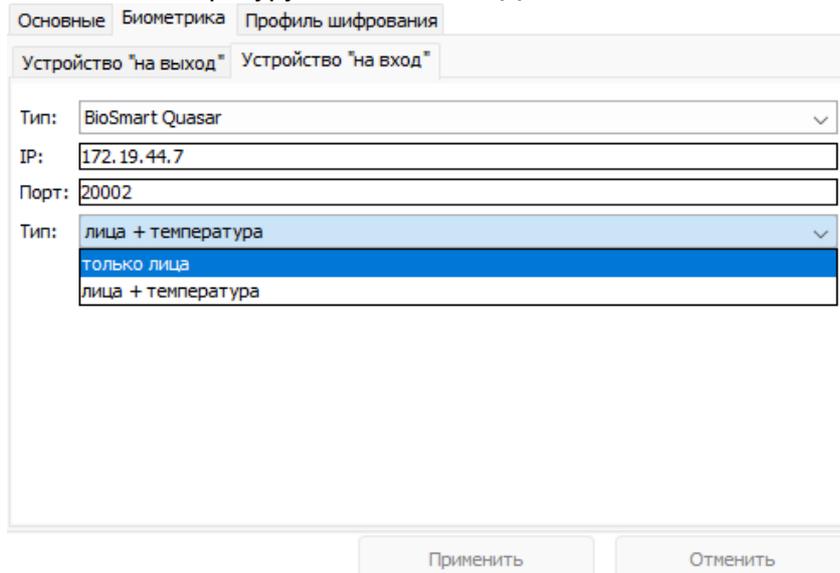
Превышение лицензионных ограничений.

- Включить интеграцию в ПО «Клиент» в меню «Файл» - «Настройки» - «Биометрика» установкой чек-бокса «Использовать Biosmart Quasar».



Окно «Файл - Настройки - Биометрика» в программе Клиент.

- На вкладке «Оборудование» в ПО «Клиент» выбрать точку доступа, с которой необходимо связать терминал. Нажать кнопку «Настройки» и в открывшемся окне указать следующие параметры: «Порт считывателя на вход» (или «Порт считывателя на выход» в зависимости от направления), Номер порта - «N», где N – номер физического wiegand-порта контроллера, к которому подключен терминал.
- В настройках ТД на вкладке «Оборудование» в разделе «Биометрика» выбрать направление, на которое будет назначен терминал (на вход или выход). Указать тип «Biosmart Quasar», IP – адрес (заданный в настройках терминала), порт (по умолчанию используется порт 20002). Здесь также задается тип работы с устройством:
  - «Только лица» - температура, измеренная устройством, в СКУД не используется и не отображается в событиях, полученных от терминала.
  - «Лица + температура» - позволяет использовать измеренную терминалом температуру в логиках СКУД.



Назначение терминала точке доступа СКУД.

- При необходимости установить пороговые значения проверки температуры. Для этого в настройках терминала необходимо перейти в

«Меню - Настройки - Настройка внешних устройств» и изменить значение параметра «Допустимое значение температуры, С». Опционально можно настроить логику работы терминала по факту превышения максимально допустимой температуры. Для этого в настройках предусмотрен специальный параметр «При повышенной температуре:», можно установить значение «блокировать», либо «пропускать».

- Генерация биометрических шаблонов лица сотрудников доступна только на клиентских местах на Windows. Генерировать шаблон можно одним из двух возможных способов:
  - В меню «Файл - Настройки - Биометрика» с помощью кнопки «Сгенерировать шаблоны». Этот вариант подходит для массовой генерации шаблонов (например, при первоначальной настройке терминала). Так будут созданы биометрические шаблоны лица всех сотрудников, имеющих фотографию в СКУД.
  - На вкладке «Персонал» в карточке сотрудника для параметра «Биометрия». необходимо выбрать тип «Biosmart Quasar» и нажать соответствующую кнопку напротив. Шаблон генерируется из фотографии сотрудника. Если у сотрудника нет Wiegand-кода, то он будет назначен автоматически.

По факту успешной идентификации сотрудника в ПО «Клиент» на вкладке «Наблюдение» появятся соответствующие события, содержащие информацию об объекте и его опционально - температуре. Если температура человека превышает допустимый порог, то доступ будет запрещен.

Список событий:

Время	Точка	Событие
2022-06-25 05:34:09	Тестовая	[BioSmart] Превышена допустимая температура сотрудника. Температура: 37,4 °C. Объект: Тест. Напр.: вход
2022-06-25 05:34:31	Тестовая	[BioSmart] Успешная идентификация сотрудника (лицо). Температура: 36,2 °C. Объект: Тест. Напр.: вход
2022-06-25 05:34:33	Тестовая	[BioSmart] Успешная идентификация сотрудника (лицо). Температура: 35,0 °C. Объект: Тест. Напр.: вход

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

## 6. 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](http://www.sigur.com)

По общим вопросам: [info@sigur.com](mailto:info@sigur.com)

Техническая поддержка: [support@sigur.com](mailto:support@sigur.com)

Телефон: +7 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260 12 93