SIGUR

Руководство по настройке интеграции с биометрическими считывателями отпечатков пальцев и рисунков вен ладоней BioSmart

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 10
   7.1. Общая схема подключения устройств 10
   7.2. Подключение устройств к контроллеру 10
   7.3. Настройки со стороны BioSmart 11
      7.3.1. Настройка считывателей отпечатков пальцев 11
      7.3.2. Настройка считывателей вен ладоней 14
   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. Работа с базой биометрических шаблонов 21
8. Контакты 24

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 с биометрическими считывателями отпечатков пальцев и рисунка вен ладоней BioSmart.

Инструкции по настройке интеграции с терминалами распознавания лиц BioSmart Quasar и с биометрическими считывателями рисунка вен ладоней BioSmart PalmJet доступны на сайте Sigur в разделе «Документация».

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	20 апреля 2026 г.	Первая публикация.
0002	10 июня 2026 г.	Актуализирована информация в связи с добавлением поддержки ОС RHEL и Windows x64.
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: 1.8.4.35 и выше.
- Версия сервиса интеграции с устройствами BioSmart: 1.1.18 и выше.
- Операционная система сервера СКУД: Windows (x64), Linux Debian, RHEL.
- Сервер БД СКУД: MariaDB.
- Остальные системные требования: см. «Руководство администратора ПО Sigur».
- Лицензирование: функциональность доступна в пакетах лицензий Standard+, Pro и Enterprise. При использовании лицензии модульного типа дополнительные модули не требуются.

SEC.RU | Короткий путь к информации

Скачано с sec.ru

5. Список поддерживаемых моделей

На текущий момент реализована и протестирована поддержка следующего ряда устройств:

- сканеры отпечатков пальцев:
  - считыватели BioSmart 4 и 5 серий;
  - терминал BioSmart WTC2;
  - настольный считыватель BioSmart FS-80.
- сканеры рисунка вен ладоней:
  - терминал BioSmart PV-WTC;
  - настольный считыватель BioSmart DCR-PV.



Работа настольных считывателей BioSmart не поддерживается на клиентских рабочих местах под ОС Linux.

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

6. Описание интеграции

Настроенная интеграция позволяет:

- Подключить биометрические считыватели отпечатков пальцев и вен ладоней BioSmart к СКУД Sigur и назначить их точкам доступа в определённом направлении.
- Добавлять и сохранять в ПО Sigur биометрические шаблоны отпечатков пальцев и вен ладоней и при необходимости синхронизировать их в память устройств BioSmart.
- Организовать доступ по распознаванию биометрического шаблона или в режиме двухфакторной аутентификации: карта + отпечаток пальца, карта + вены ладоней.
- Настроить один из двух режимов работы:
  - **автономный (локальный) режим** — биометрические шаблоны хранятся на сервере Sigur, а также в устройствах BioSmart. При идентификации устройство BioSmart выполняет сопоставление шаблона и, в случае успешного распознавания, передаёт уникальный код идентификатора на контроллер Sigur по интерфейсу Wiegand. Контроллер Sigur выполняет проверку прав доступа и принимает решение о предоставлении доступа. Режим поддерживается всеми считывателями BioSmart.
  - **серверный режим** — биометрические шаблоны хранятся только на сервере Sigur. При идентификации устройство BioSmart передаёт данные на сервер Sigur по сети Ethernet, где выполняется сопоставление шаблона и определяется результат распознавания. Результат передаётся обратно на устройство, после чего уникальный код идентификатора направляется на контроллер Sigur по интерфейсу Wiegand. Контроллер Sigur выполняет проверку прав доступа и принимает решение о предоставлении доступа.

    У моделей устройства BioSmart 5M отсутствует поддержка серверного режима работы:

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

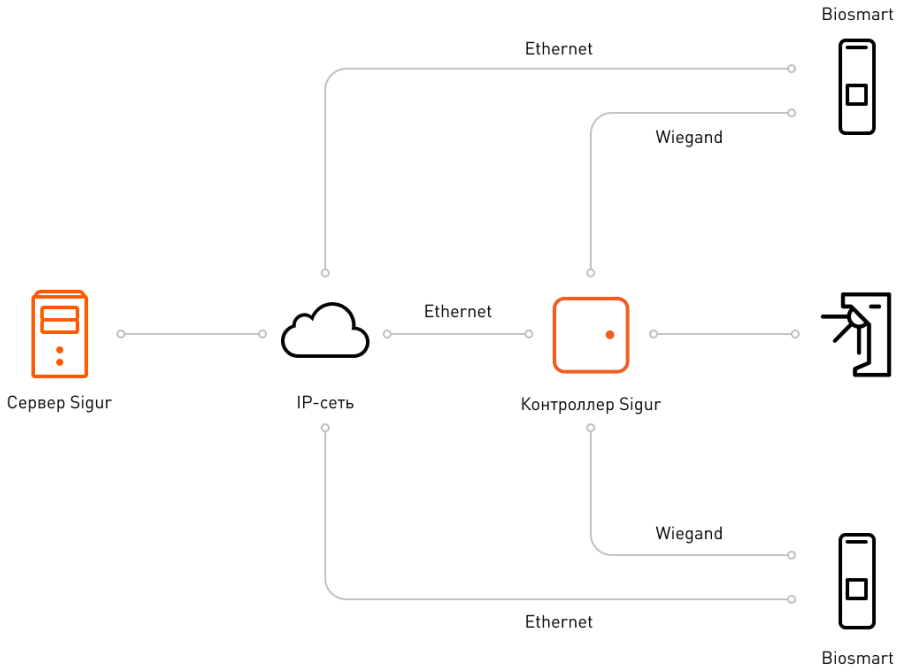
Модель устройства	BioSmart 4	BioSmart 5M	BioSmart WTC-2	BioSmart PV-WTC
Поддержка серверного режима	Да	Нет	Да	Да
Требуемая ОС сервера Sigur	Windows; Linux Debian; RHEL.	—	Windows; Linux Debian; RHEL.	Windows; Linux Debian; RHEL.

SEC.RU | Короткий путь к информации

Скачано с sec.ru

7. Подключение и настройка

7.1. Общая схема подключения устройств



Общая схема подключения биометрических считывателей BioSmart к СКУД Sigur.

7.2. Подключение устройств к контроллеру

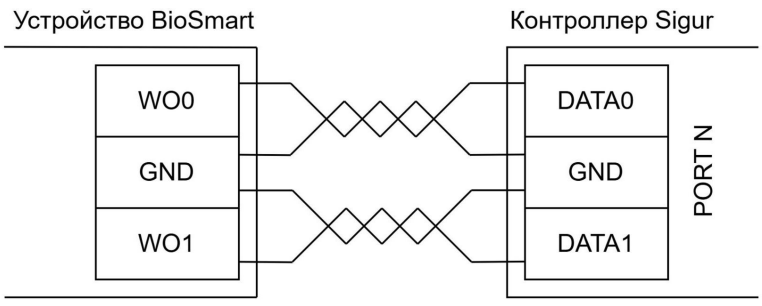


Схема подключения биометрических считывателей BioSmart к контроллеру Sigur по интерфейсу Wiegand.

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

7.3. Настройки со стороны BioSmart

7.3.1. Настройка считывателей отпечатков пальцев

Первоначальную настройку оборудования можно осуществить с помощью ПО BioSmart Studio, скачать которое можно с сайта производителя.

Считыватели BioSmart имеют установленные заводские сетевые настройки. Для их изменения:

1. Временно измените IP-адрес ПК на 172.25.110.XX, где вместо XX установите любое значение от 1 до 254, кроме 71. Маска подсети — 255.255.0.0.
   Адрес 172.25.110.71 присваивается считывателю на предприятии-изготовителе. В случае изменений условий поставки считывателей BioSmart обращайтесь к документации производителя.

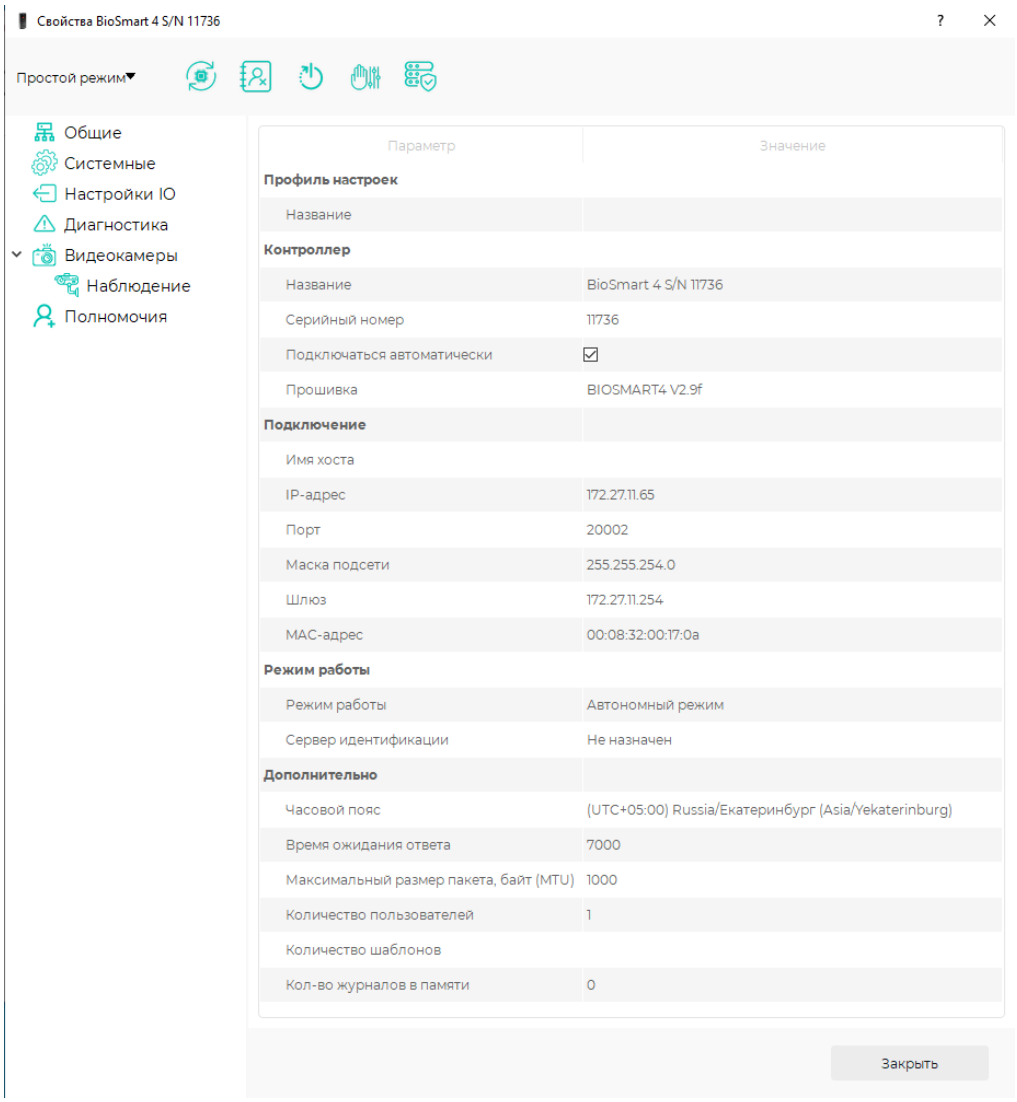
2. Подключите считыватель напрямую к ПК или в ту же подсеть.

3. В ПО BioSmart Studio перейдите на вкладку «Устройства» и добавьте новое устройство вручную или воспользуйтесь автопоиском.

4. Откройте свойства нового устройства.

5. В открывшемся окне на вкладке «Общее» задайте желаемые параметры считывателя: IP-адрес, маску подсети, шлюз. Номер порта можно оставить в значении по умолчанию (20002), в случае изменения этого значения не забудьте указать новое значение при настройке в ПО Sigur «Клиент».

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



Пример IP-настроек считывателя BioSmart в ПО BioSmart Studio.

6. Настройте нужный режим работы (автономный или серверный) устройства BioSmart.

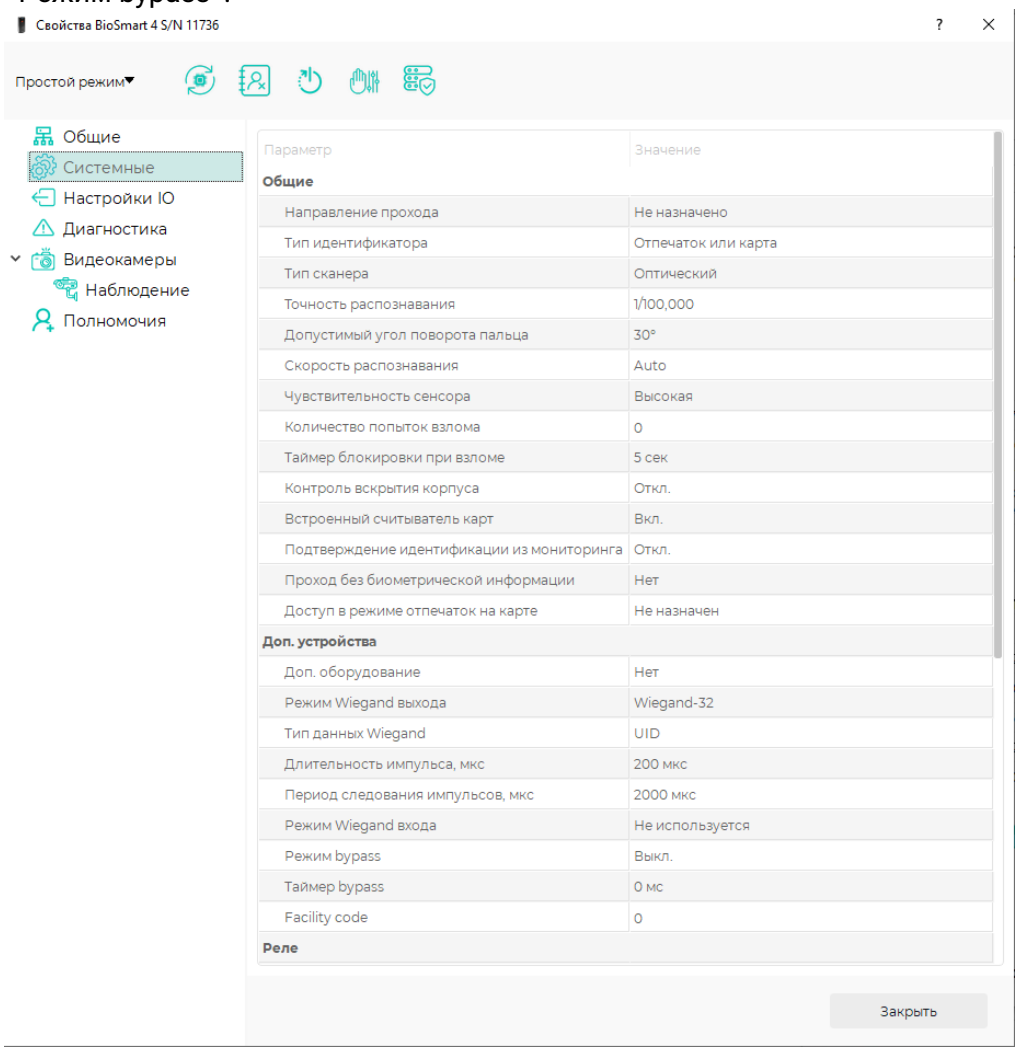
7. В случае выбора серверного режима работы необходимо указать «Сервер идентификации» — сетевой адрес сервера Sigur.

8. Перейдите на вкладку «Системные» и установите значение параметра «Режим Wiegand выхода» — «Wiegand-26 (W/P)», а значение параметра «Тип данных Wiegand» — «UID».

9. Если требуется идентификация «карта или отпечаток» — включите «Режим bypass». Коды карт, незарегистрированных в системе, будут сразу передаваться на контроллер Sigur по интерфейсу Wiegand. При наличии в настройках параметра «Таймер bypass» его значение должно быть равно 0 мс.

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

10. Если требуется идентификация «карта + отпечаток» — выключите «Режим bypass».



Системные настройки считывателей BioSmart 4 и 5 серий в ПО BioSmart Studio.

11. Сохраните внесённые изменения.

12. Выполните настройку для всех считывателей системы, повторив для них пункты 2-11.

13. Закройте ПО BioSmart Studio и верните сетевые настройки ПК к исходным.

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

14. Отключите службы BioSmart DB Server, BioSmart Remote Scanner Server и BioSmart Server. Путь к управлению службами в Windows: «Пуск» — «Панель управления» — «Администрирование» — «Службы». В зависимости от версии ОС путь может немного отличаться. Тип запуска замените на «Вручную» или «Отключён».

Службы BioSmart должны быть выключены. Совместная работа служб BioSmart и ПО Sigur приводит к некорректной работе считывателей.

На этом настройка считывателей отпечатков пальцев завершена. Далее можно переходить к настройке системы Sigur.

7.3.2. Настройка считывателей вен ладоней

Необходимо выполнить следующее:

1. Измените IP-адрес устройства на нужный. Это можно сделать, выполнив пункты 1–7 из инструкции по настройке считывателей отпечатков пальцев (через ПО BioSmart Studio), либо через меню настроек на самом приборе. Если считывателей несколько, повторите данную настройку для каждого из них.

2. Перейдите в меню настроек прибора. В «Меню» — «Настройки» — «Система» установите значение пункта «Количество ладоней на пользователя» равным 10.

3. Если настройки IP-адресов выполнялись через ПО BioSmart Studio, закройте его и верните сетевые настройки ПК к исходным.

4. Отключите службы BioSmart DB Server, BioSmart Remote Scanner Server и BioSmart Server. Путь к управлению службами в Windows: «Пуск» — «Панель управления» — «Администрирование» — «Службы». В зависимости от версии ОС путь может немного отличаться. Тип запуска замените на «Вручную» или «Отключён».

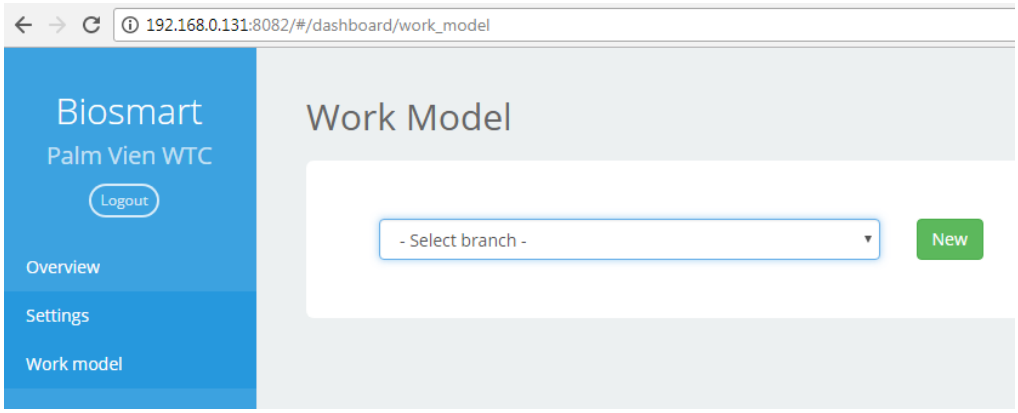
Службы BioSmart должны быть выключены. Совместная работа служб BioSmart и ПО Sigur приводит к некорректной работе считывателей.

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

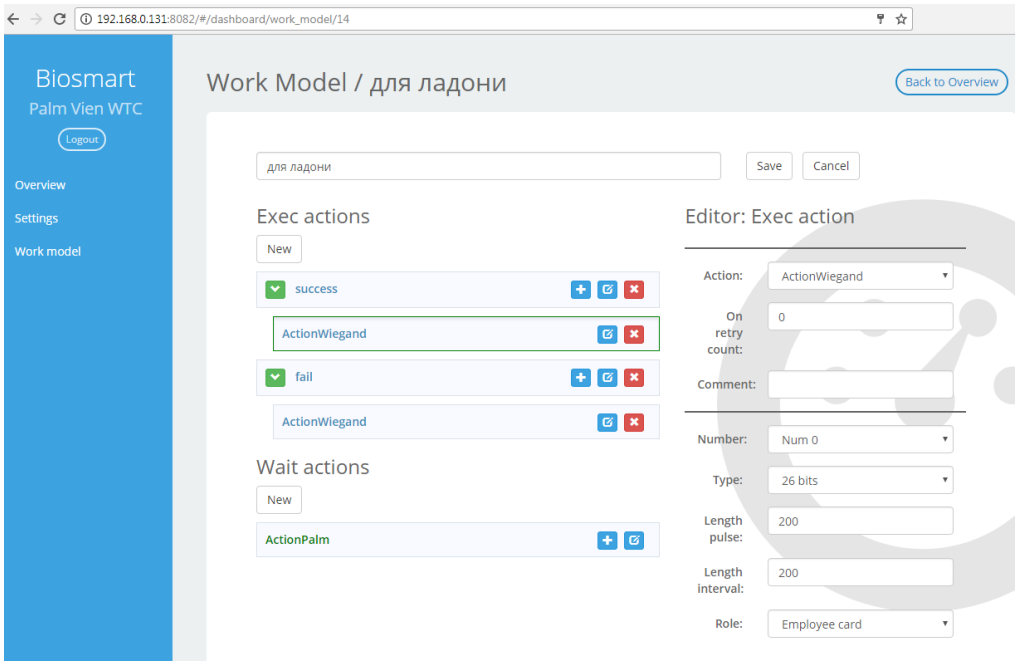
5. Откройте браузер и в адресной строке наберите *«ip-адрес устройства:8082»* (без кавычек, пример – 192.168.0.131:8082) и нажмите «Enter».

6. Откроется приветственное окно устройства, логин/пароль по умолчанию — root / bioroot.

7. В меню слева выберите пункт Work Model. Откроется окно выбора, создания и редактирования возможных режимов работы считывателя вен ладоней. Настройте нужный режим работы (на определённые действия — выдавать Wiegand-код).



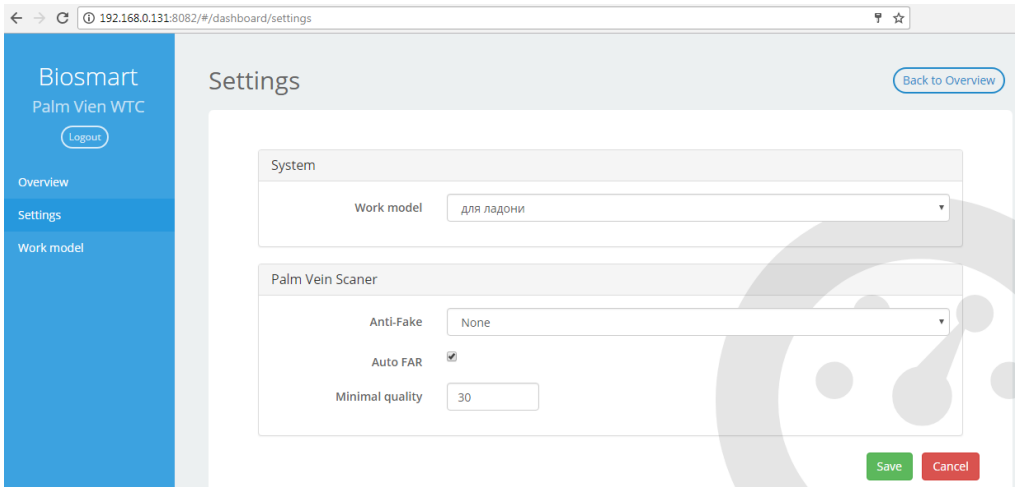
Пример окна настройки модели работы считывателя вен ладоней BioSmart.



Пример готовой модели работы считывателя вен ладоней BioSmart.

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

8. Завершив настройку рабочей модели, перейдите в пункт меню Settings. В разделе System из выпадающего списка напротив Work Model выберите настроенную в предыдущем пункте модель. Нажмите кнопку «Save».



Окно выбора рабочей модели и сохранения настроек.

9. Настройте нужный режим работы (локальный или серверный) непосредственно на устройстве BioSmart.

На этом настройка считывателей вен ладоней завершена. Далее можно переходить к настройке системы Sigur.

7.4. Настройки со стороны Sigur

7.4.1. Настройка сервера Sigur

Необходимо выполнить следующее:

1. Проверьте, что установлена актуальная версия ПО Sigur. Если версия ПО Sigur ниже указанной в главе «Системные требования», то произведите обновление ПО.

2. Скачайте сервис интеграции с биометрическими считывателями BioSmart:

   - сервис интеграции для Windows x64;
   - сервис интеграции для Linux Debian;
   - сервис интеграции для RHEL .

3. Скачайте конфигурационный файл базы данных Sigur (enable_bss.sql).

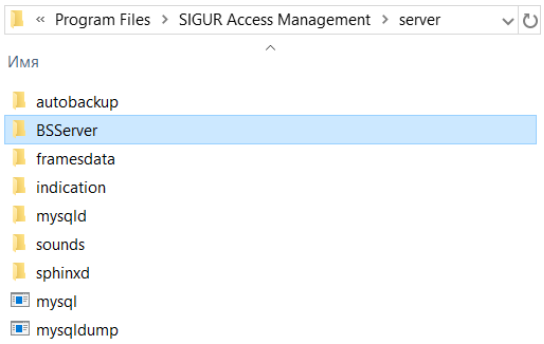
4. Выполните шаги настройки соответственно операционной системе сервера Sigur.

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

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

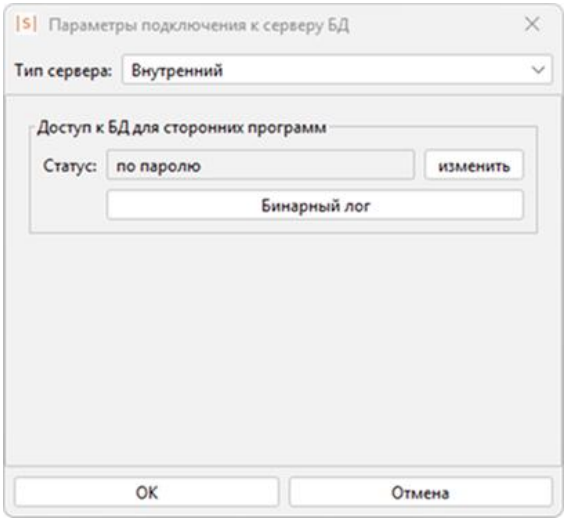
Для сервера Sigur, установленного на Windows:

1. Распакуйте скачанный архив в каталог server, содержащийся в папке установки ПО Sigur (например, C:\Program Files\SIGUR Access Management\server). В каталоге server должна появиться папка BSServer.



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

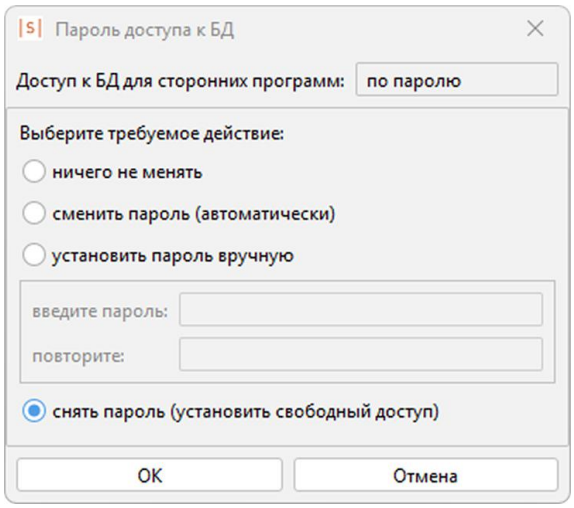
2. В программе «Управление сервером» перейдите на вкладку «База данных» и нажмите кнопку «Параметры». В открывшемся окне измените пароль доступа к БД сторонних программ, нажав кнопку «Изменить».



Окно «Параметры подключения к серверу БД».

3. Установите новый пароль или свободный доступ сторонних программ к базе данных. Нажмите «OK».

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



Окно «Пароль доступа к БД».

4. Загрузите конфигурационный файл в базу данных с помощью командной строки. Файл mysql.exe находится в каталоге установки ПО Sigur в папке server. Ниже приведён пример команды:

```
"C:\Program Files\SIGUR Access Management\server\mysql.exe" --port=3305 --user=root --password < "C:\path\to\enable_bss.sql"
```

Здесь:

- "C:\path\to\enable_bss.sql" — путь файлу enable_bss.sql.

5. Когда командная строка запросит пароль, введите его. Если пароль не задан, нажмите Enter.

6. После завершения импорта конфигурационного файла рекомендуется восстановить автоматически сгенерированный пароль базы данных в ПО «Управление сервером».

7. Запустите серверный модуль с помощью кнопки «Старт» на вкладке «Состояние» ПО «Управление сервером».

Для сервера Sigur, установленного на Linux Debian или RHEL:

1. Установите скачанный пакет интеграционного сервиса. Пример команды:

Linux Debian	*sudo dpkg -i biosmartserver_*.deb*
RHEL	*sudo rpm -i biosmartserver_*.rpm*

2. Загрузите конфигурационный файл в базу данных. В случае MariaDB можно воспользоваться командой:

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

```
mysql -u <user> -P 3306 -p <userpass> < enable_bss.sql
```

Здесь:

- <user> — имя пользователя БД.
- <userpass> — пароль указанного пользователя БД.
- enable_bss.sql — наименование импортируемого файла.

3. Перезапустите серверный модуль через ПО «Управление сервером» или утилиту AdminCLI.

7.4.2. Настройки в ПО «Клиент» и запуск интеграции

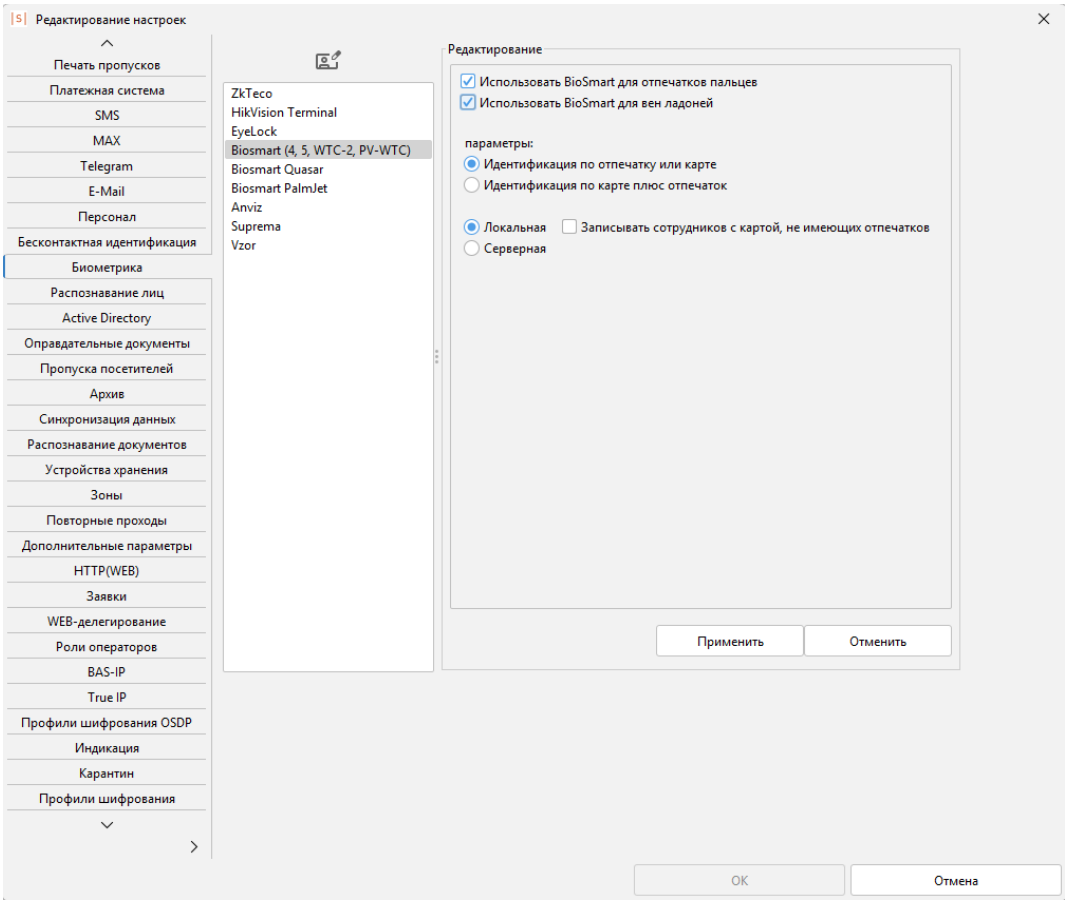
Необходимо выполнить следующее:

1. Убедитесь, что службы BioSmart остановлены/отключены.

2. Включите интеграцию с BioSmart. Для этого:

2.1. В ПО «Клиент» перейдите в меню «Файл» — «Настройки» — «Биометрика» — «BioSmart (4, 5, WTC-2, PV-WTC)» и активируйте опцию «Использовать Biosmart для отпечатков пальцев» или «Использовать Biosmart для вен ладоней» в зависимости от того, какие считыватели будут использоваться в системе. Остальные параметры конфигурировать не нужно, режим конфигурируется на устройстве, а не в ПО «Клиент». Кнопка «Перезаписать память устройств» в ПО «Клиент» также неактуальна.

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



Меню «Файл» — «Настройки» — «Биометрика» — « BioSmart(4, 5, WTC-2, PV-WTC)» в ПО «Клиент».

2.2. Сохраните настройки, нажав кнопки «Применить» и «ОК».

3. Настройте точку доступа. Для этого:

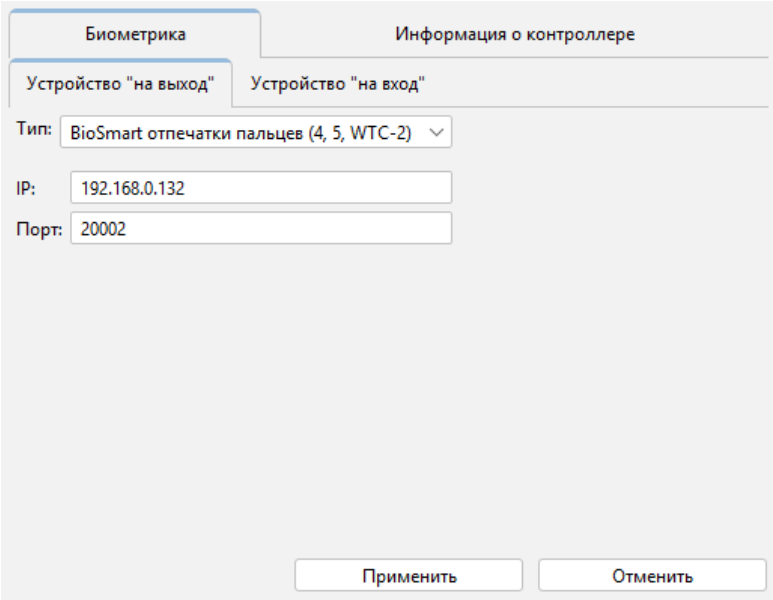
3.1. На вкладке «Оборудование» в ПО «Клиент» выделите точку доступа, с которой необходимо связать считыватель BioSmart. Раскройте подвкладку «Биометрика» и выберите направление на вход или на выход.

3.2. В выпадающем списке «Тип» выберите необходимый тип устройства, а затем укажите:

- IP-адрес устройства;
- порт (по умолчанию — 20002). При изменении номера порта следует убедиться, что в настройках считывателя установлено соответствующее значение.

3.3. Сохраните настройки, нажав «Применить».

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



Настройка точки доступа, на которой используются считыватели BioSmart.

7.4.3. Работа с базой биометрических шаблонов

Добавление и удаление биометрических шаблонов производится в карточке объекта доступа на вкладке «Персонал» ПО «Клиент», в разделе «Основное». Для одного объекта доступа можно добавить до 10 шаблонов отпечатков пальцев и до 2 шаблонов рисунка вен ладоней.

1. Выделите объект в списке персонала и выберите нужное устройство BioSmart в блоке «Биометрия».

2. Добавьте шаблон с помощью одной из кнопок:

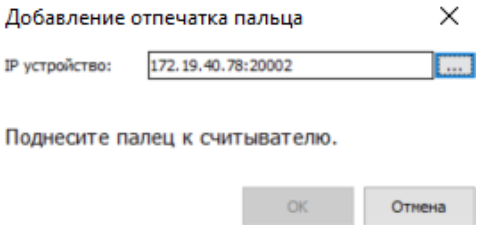
	**«Добавить биометрический шаблон с USB-устройства»** При нажатии на данную кнопку начнётся процесс сканирования биометрического шаблона с помощью настольного USB-считывателя. В процессе сканирования имеется возможность визуально проконтролировать качество отпечатка.

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



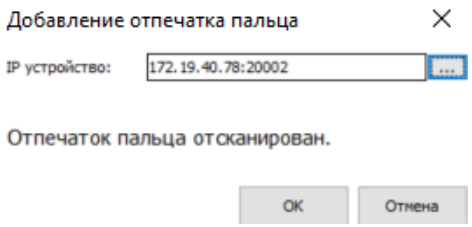
Пример сканирования отпечатка пальца с помощью BioSmart FS-80.

	**«Добавить биометрический шаблон с IP-устройства»** При нажатии на данную кнопку начнётся процесс сканирования биометрического шаблона с сетевого считывателя, подключённого к одной из точек доступа. При этом необходимо, чтобы в настройках ПО BioSmart Studio для устройства был активирован режим bypass. Данный режим позволяет передавать на контроллер СКУД по интерфейсу Wiegand код идентификатора, не зарегистрированного в памяти устройства. Для выбора устройства нажмите кнопку «...». В дереве оборудования выберите точку доступа, к которой подключено устройство, укажите направление и само устройство. В случае успеха откроется информационное окно, оповещающее о том, что считыватель готов к работе и ожидает поднесения пальца/ладони к сканеру. В результате успешного сканирования будет выдано соответствующее оповещение. Шаблон будет сохранён в базу данных Sigur после нажатия кнопки «OK». Кнопки закрытия и отмены сбрасывают отпечаток.



Окно ожидания сканирования.

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



Окно оповещения об успешном результате сканирования пальца.

3. Для сохранения внесённых изменений нажмите кнопку «Применить».

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