SIGUR

Руководство по настройке интеграции с биометрическими терминалами IRIS ID

Редакция от 02.10.2026.

«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 IRIS ID 10
   7.4. Настройки со стороны Sigur 10
      7.4.1. Настройка сервера Sigur 10
      7.4.2. Настройка TLS для работы с терминалами 14
      7.4.3. Настройки в ПО «Клиент» и запуск интеграции 16
      7.4.4. Работа с базой биометрических шаблонов 19
      7.4.5. Синхронизация персонала 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 и биометрических терминалов распознавания лиц и радужек глаз IRIS ID.

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	02 октября 2026 г.	Первая публикация.

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: 1.8.5.69 и выше.
- Версия сервиса интеграции с терминалами IRIS ID: 1.0.0 и выше.
- Операционная система сервера СКУД: Windows, Debian Linux, RHEL.
- Сервер БД СКУД: MariaDB, PostgreSQL.
- Остальные системные требования: см. «Руководство администратора ПО Sigur».
- Лицензирование: лицензируется каждый подключённый к СКУД терминал IRIS ID. 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

На текущий момент реализована и протестирована поддержка следующих моделей терминалов IRIS ID:

- iT100;
- iA1000.

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

6. Описание интеграции

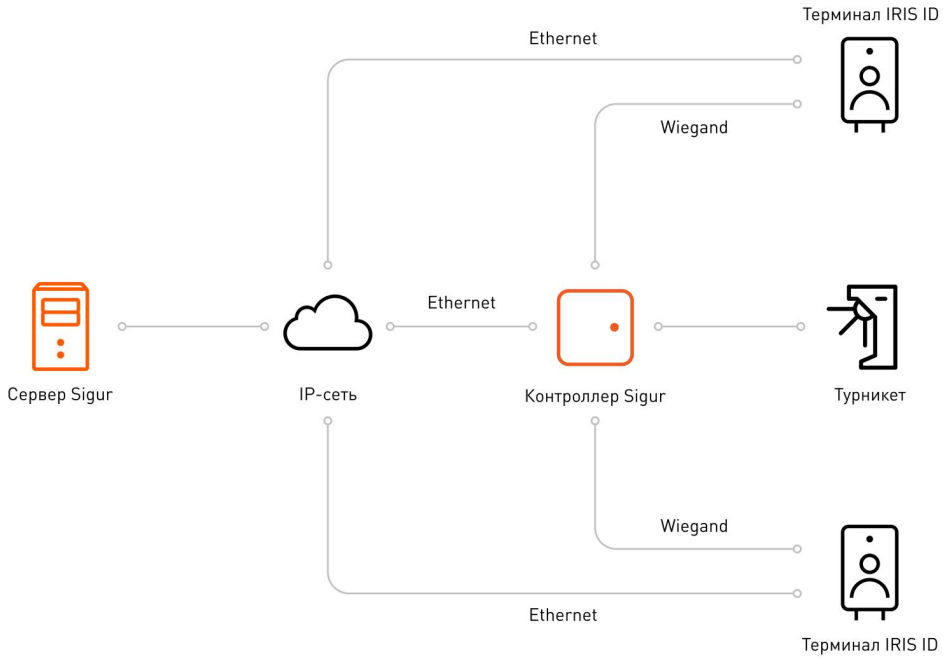
Настроенная интеграция позволяет:

- подключить биометрические терминалы распознавания лиц и радужек глаз IRIS ID к СКУД Sigur и использовать их на точках доступа в определённом направлении;
- добавлять и сохранять в ПО Sigur биометрические шаблоны радужек глаз с помощью терминалов IRIS ID;
- автоматически генерировать номера пропусков, если доступ осуществляется только по распознаванию лиц или радужек глаз, без использования карт;
- синхронизировать сотрудников, посетителей и их данные (номера пропусков, фотографии лиц и биометрические шаблоны радужек глаз) из СКУД Sigur в память терминалов IRIS ID;
- организовать доступ по распознаванию лиц, радужек глаз или в режиме двух/трёхфакторной аутентификации: карта + лицо, карта + радужка глаза и т. д.;
- при успешном распознавании идентификатора получать по Wiegand код пропуска, присвоенного 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 терминалов IRIS ID к СКУД Sigur.

7.2. Подключение устройств к контроллеру

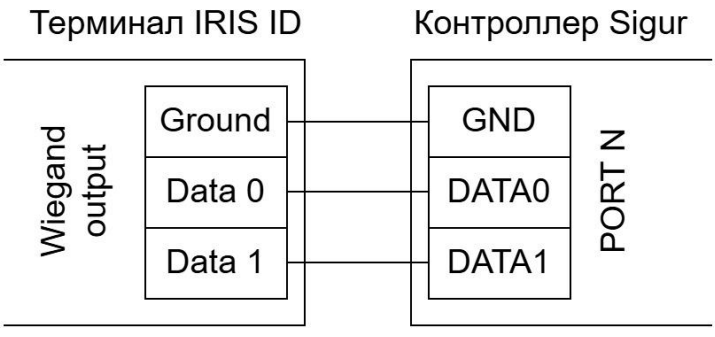


Схема подключения терминалов IRIS ID к контроллеру Sigur.

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

7.3. Настройки со стороны IRIS ID

Терминал IRIS ID подключается к локальной сети объекта. Первичные настройки производятся в интерфейсе терминала. Необходимо выполнить следующее:

1. Перейдите в меню «IrisAccess» – «ID & Password» – «Настройки».

2. На вкладке «Сеть» задайте статический IP-адрес устройства, длину префикса и адрес шлюза.

3. На вкладке «Режим»:

3.1. Выберите «Режим сопоставления»:

- «Идентификация» – терминал распознаёт биометрические признаки при появлении пользователя в области действия.
- «Верификация» – терминал ожидает поднесения карты, после чего выполняется подтверждение с помощью биометрии.

3.2. Установите «Режим распознавания» – «Устройство», после чего выберите требуемую комбинацию распознавания биометрических признаков и доступа по карте.

4. На вкладке «Считыватель карт» включите одноимённый параметр для работы встроенного считывателя.

5. Активируйте терминал согласно документации производителя. После активации сохраните значение ApiKey с вкладки «Активация» для последующего использования в ПО «Клиент».

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 ниже указанной в разделе «Системные требования», то обновите ПО.

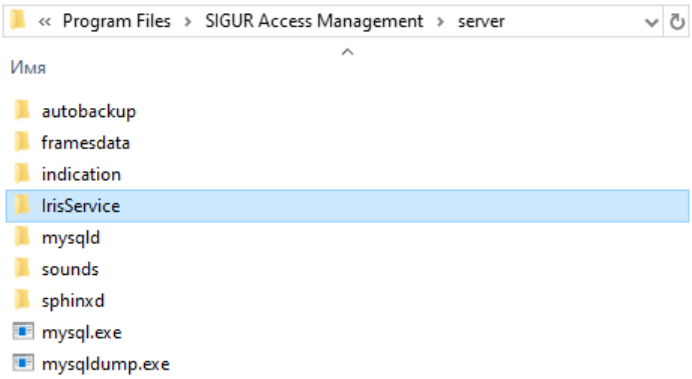
2. Скачайте сервис интеграции с терминалами IRIS ID (версия для Windows 64-bit, Debian Linux, RHEL).

3. Выполните шаги настройки соответственно операционной системе сервера Sigur.

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

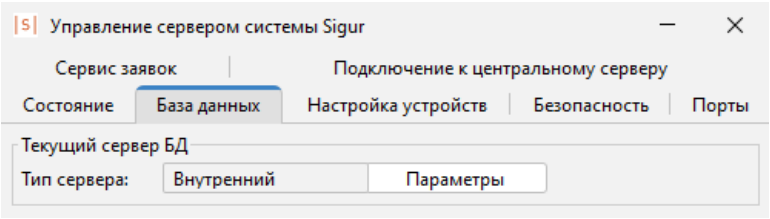
Для сервера Sigur, установленного на Windows:

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



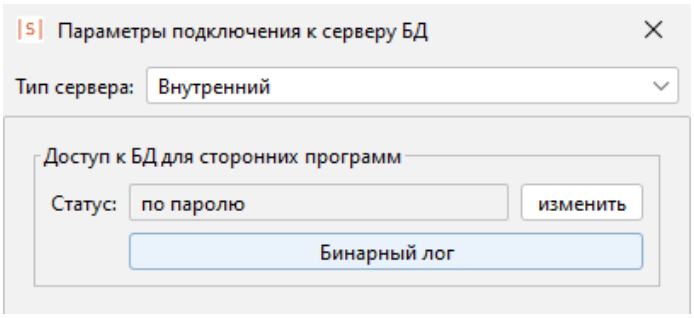
Каталог \SIGUR Access Management\server.

2. В программе «Управление сервером» перейдите на вкладку «База данных». В блоке «Текущий сервер БД» нажмите кнопку «Параметры».



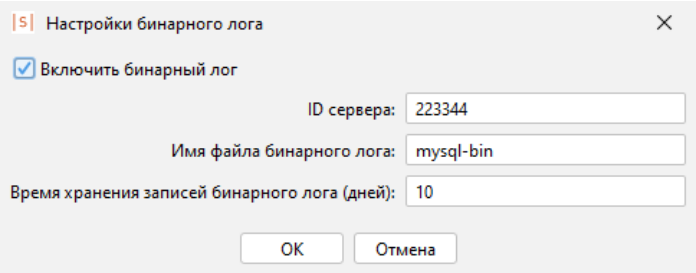
Вкладка «База данных» программы «Управление сервером».

3. В открывшемся окне нажмите кнопку «Бинарный лог», после чего включите бинарный лог, оставив предложенные по умолчанию значения параметров. Сохраните настройки, нажав «ОК».



Окно «Параметры подключения к серверу БД».

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



Окно «Настройки бинарного лога».

4. Перезапустите сервер базы данных и серверный модуль на вкладке «Состояние» ПО «Управление сервером», используя кнопки «Стоп» и «Старт».

Для сервера Sigur, установленного на Debian Linux или RHEL:

1. Установите скачанный пакет сервиса интеграции. Пример команд:

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

2. Выполните настройки сервера базы данных Sigur соответственно используемой СУБД.

MariaDB:

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

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

2. Перезапустите сервер базы данных командой:

```
sudo systemctl restart mariadb
```

3. Для пользователя базы данных Sigur 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'@'%';
```


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

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

PostgreSQL:

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

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

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

```
local replication postgres     trust
```

3. Предоставьте пользователю базы данных Sigur права репликации:

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

4. Настройте replica identity для таблиц базы данных Sigur, которые необходимы для работы интеграции:

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

5. Перезапустите сервер базы данных командой:

```
sudo systemctl restart postgresql
```

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

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

7.4.2. Настройка TLS для работы с терминалами

Для взаимодействия с терминалами IRIS ID используется защищённый протокол HTTPS, использование HTTP недоступно. Поддерживаются два варианта работы с терминалами:

- Использование TLS в недоверенном режиме. Основной способ взаимодействия. Используется по умолчанию и не требует дополнительной настройки.

- Использование TLS в доверенном режиме. Дополнительный способ взаимодействия с терминалами IRIS ID. Используется, если требуется самостоятельно настроить проверку сертификатов.

Для работы в доверенном режиме сервис интеграции использует индивидуальный сертификат для каждого терминала. Сертификаты должны храниться в специальной папке certs, а название каждого файла должно быть строго в формате iris-<IP-адрес терминала>.crt.

Для настройки доверенного режима:

1. Подготовьте файлы сертификатов терминалов. Получить сертификаты можно:

- Через веб-браузер. Введите в адресной строке IP-адрес и порт терминала (например, https://172.19.40.51:4747) и нажмите Enter. Браузер выведет предупреждение о небезопасном подключении. Откройте сведения о сертификате (например, нажав значок слева от адресной строки) и экспортируйте сертификат в файл, указав в названии IP-адрес терминала (например, iris-172.19.40.51.crt).

- С помощью команды в Windows PowerShell (требуется Windows PowerShell версии 5.1). Для этого скопируйте команду, указанную ниже, в открытую консоль и нажмите Enter:

```
& {
$ip=Read-Host "Введите IP-адрес терминала (например 192.168.1.100)";
[System.Net.ServicePointManager]::ServerCertificateValidationCallback={$true};
$r=[Net.HttpWebRequest]::Create("https://$ip`:4747");
$r.Host=$ip;
try{$r.GetResponse()|Out-Null}catch{};
$c=$r.ServicePoint.Certificate;
if($c){"-----BEGIN CERTIFICATE-----`n"+
[Convert]::ToBase64String($c.Export('Cert'),'InsertLineBreaks')+
"`n-----END CERTIFICATE-----"|Out-File "iris-$ip.crt" -Encoding ascii -Force;
Write-Host "Сохранено: iris-$ip.crt"}else{Write-Host "Сертификат не получен"}
}
```


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

Далее введите в консоли IP-адрес терминала, для которого необходимо получить сертификат, и нажмите Enter. Сертификат будет сохранён в папку, откуда была выполнена команда. Название файла будет содержать IP-адрес терминала (например, iris-172.19.40.51.crt).

2. Создайте папку certs в директории сервиса интеграции (например, C:\Program Files\SIGUR Access Management\server\IrisService\config\certs в ОС Windows или /etc/sphinx/irisservice/certs/ в ОС Linux). Поместите в папку полученные файлы сертификатов.

3. Перейдите в папку C:\Program Files\SIGUR Access Management\server\IrisService\config в ОС Windows или /etc/sphinx/irisservice/ в ОС Linux. Откройте конфигурационный файл application.yaml в текстовом редакторе, запущенном от имени администратора.

4. Скопируйте строки, указанные ниже, и вставьте их в файл application.yaml.

```
sigur:
  southbound:
    devices:
      certificate:
        path: ./config/certs/
        validation:
          strategy: trust_client
```

При копировании отступы могут не сохраниться. Проверьте, что строки расположены как в примере: каждый следующий уровень сдвинут на два пробела относительно предыдущего. Для отступов используйте пробелы, а не клавишу Tab.

Укажите значения параметров:

- path – путь до папки с сертификатами. Для Windows: ./config/certs/, для Linux: /etc/sphinx/irisservice/certs/;
- strategy – стратегия проверки сертификатов устройств. Доступные значения:

  - trust_all – не проверять сертификаты, доверять всем;
  - trust_client – доверять клиентскому сертификату, который предоставил терминал.

Сохраните изменения в файле.

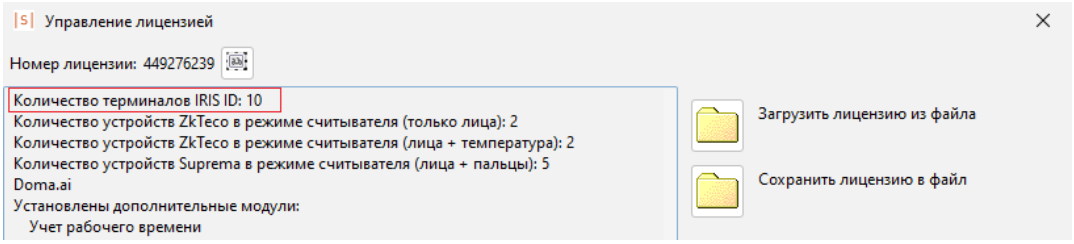
5. Для завершения настройки перезапустите серверный модуль Sigur через ПО «Управление сервером» или утилиту AdminCLI.

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

7.4.3. Настройки в ПО «Клиент» и запуск интеграции

Необходимо выполнить следующее:

1. Через меню «Файл» – «Управление модулями» в ПО «Клиент» проверьте, что присутствует лицензия на необходимое количество терминалов IRIS ID.



Лицензия на подключение терминалов IRIS ID.

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. Включите интеграцию с IRIS ID. Для этого:

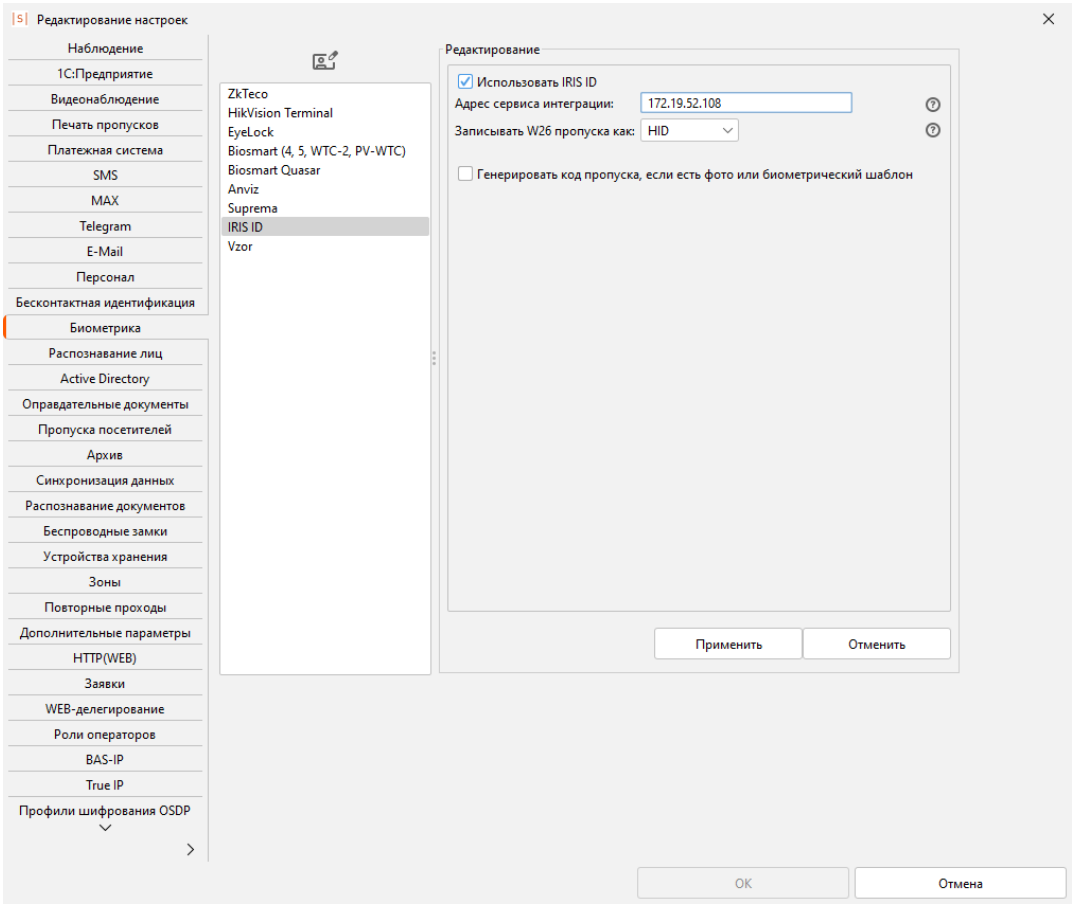
2.1. В ПО «Клиент» перейдите в меню «Файл» – «Настройки» – «Биометрика» – «IRIS ID» и включите опцию «Использовать IRIS ID».

2.2. Выполните настройки интеграции:

- В поле «Адрес сервиса интеграции» укажите IP-адрес или доменное имя компьютера, на котором запущен сервис интеграции. Не допускается использовать значение 127.0.0.1 или localhost.
- В случае использования карт в формате Wiegand-26 в поле «Записывать W26 пропуска как» выберите тип карт, используемых на объекте, – HID или Em-Marine. Чтение карт этих типов на терминалах IRIS ID различается.

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

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



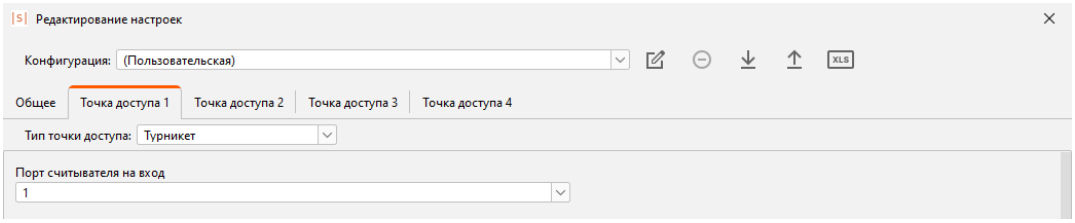
Меню «Файл» – «Настройки» – «Биометрика» – «IRIS ID».

3. Настройте точку доступа. Для этого:

3.1. На вкладке «Оборудование» в ПО «Клиент» выделите точку доступа, на которой установлен терминал IRIS ID.

3.2. Настройте подключение терминала к контроллеру по Wiegand:

- На вкладке «Оборудование» нажмите кнопку «Настройки».
- В открывшемся окне для параметра «Порт считывателя на вход» (или «Порт считывателя на выход», в зависимости от направления, в котором установлено устройство) выберите из выпадающего списка номер физического Wiegand-порта контроллера, к которому подключён терминал.
- Сохраните настройки, нажав «OK».

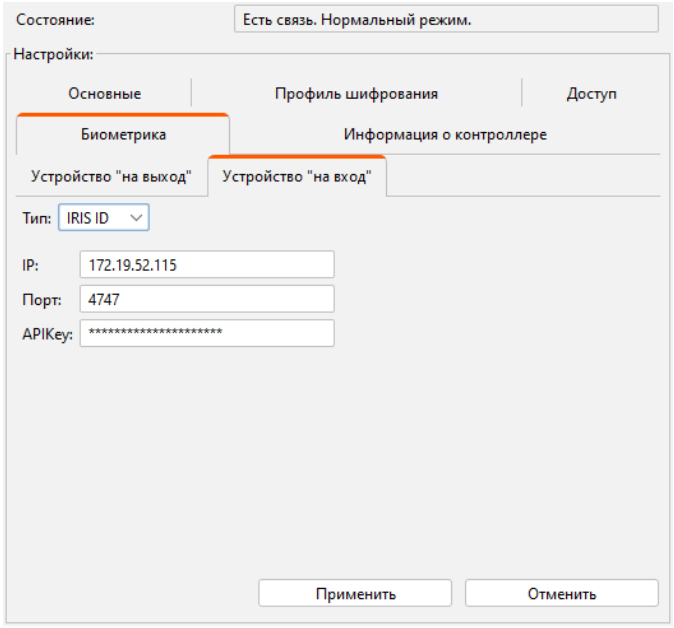


Пример настройки порта контроллера.

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

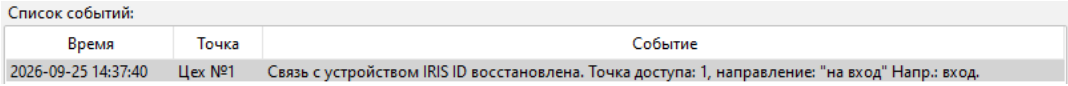
3.3. Настройте подключение к терминалу по сети:

- На вкладке «Оборудование» раскройте подвкладку «Биометрика».
- Выберите направление для терминала IRIS ID (на вход или на выход, соответственно настройкам порта контроллера). Один терминал можно подключить только к одному направлению одной точки доступа.
- В выпадающем списке «Тип» выберите «IRIS ID», а затем укажите:
  - IP-адрес терминала;
  - порт (по умолчанию – 4747);
  - значение APIKey (получить ключ можно в настройках терминала).
- Сохраните настройки, нажав «Применить».



Пример настроек точки доступа на подвкладке «Биометрика».

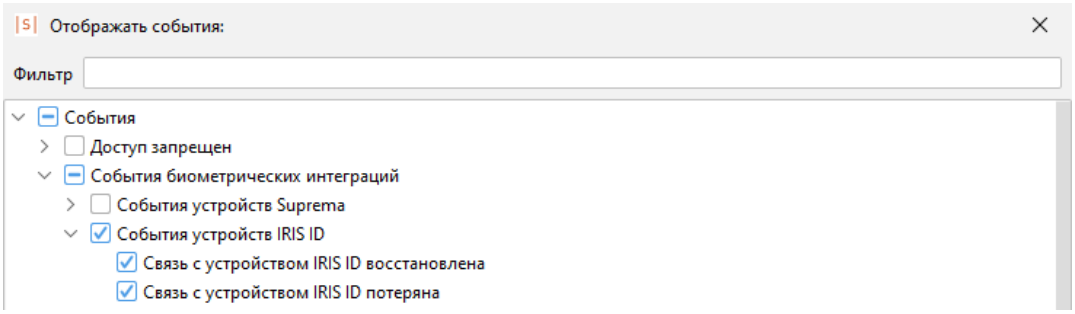
Если все настройки выполнены корректно, на вкладке «Наблюдение» ПО «Клиент» появится событие «Связь с устройством IRIS ID восстановлена».



Успешное установление связи с терминалом IRIS ID.

На вкладках «Архив», «Наблюдение», а также при построении отчётов можно настроить отображение событий восстановления и потери связи с терминалами IRIS ID с помощью соответствующих фильтров.

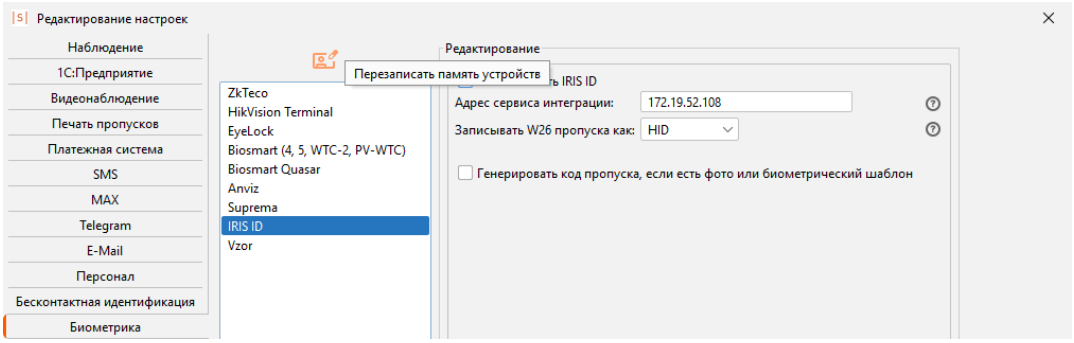
SEC.RU | Короткий путь к информации Скачано с sec.ru



Фильтры событий устройств IRIS ID.

Перезапись памяти устройств.

В случаях, когда интеграция долгое время была неактивна или на сервере восстанавливалась резервная копия базы данных, можно выполнить перезапись памяти терминалов для повторной синхронизации информации на устройства. Для этого в ПО «Клиент» перейдите в меню «Файл» – «Настройки» – «Биометрика» – «IRIS ID» и нажмите кнопку «Перезаписать память устройств».



Отображение кнопки «Перезаписать память устройств».

7.4.4. Работа с базой биометрических шаблонов

Для добавления шаблонов радужек глаз необходимо выполнить следующее:

1. Перейдите на вкладку «Персонал» ПО «Клиент». Выделите объект доступа (далее – ОД) в списке персонала.

2. В блоке «Биометрия» в разделе «Основное» выберите пункт «IRIS ID» из выпадающего списка.



Блок «Биометрия».

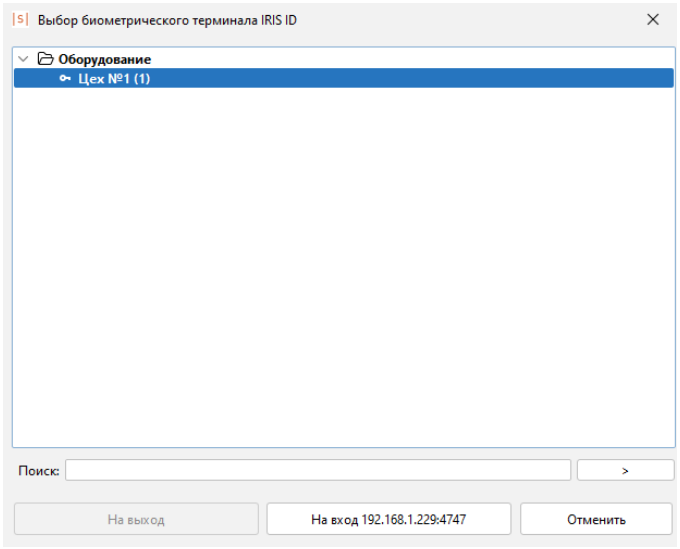
3. Нажмите кнопку «Добавить биометрический шаблон с IP-устройства».



Кнопка «Добавить биометрический шаблон с IP-устройства».

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

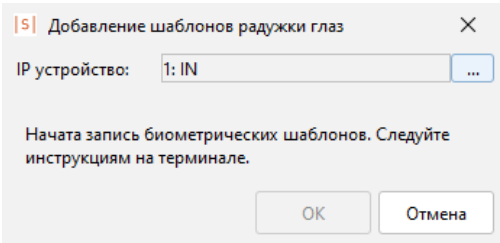
4. В открывшемся окне нажмите кнопку «...». В дереве оборудования выделите точку доступа, к которой подключён терминал IRIS ID, и нажмите кнопку «На вход» или «На выход» в нижней части окна.



Выбор точки доступа.

При повторном добавлении шаблонов окно откроется с ранее выбранным терминалом и запись начнётся сразу. Чтобы выбрать другой терминал, нажмите кнопку «...».

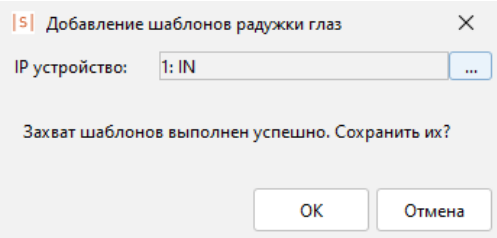
5. После выбора терминал перейдёт в режим ожидания и будет готов к сканированию радужек глаз. Сотруднику или посетителю, для которого записываются шаблоны, необходимо подойти к терминалу и следовать инструкциям на его экране.



Запись биометрических шаблонов.

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

6. В результате успешного сканирования будет выдано соответствующее оповещение. При сканировании для одного ОД записывается до двух шаблонов радужки (правый и левый глаз). Шаблоны будут присвоены ОД после нажатия кнопки «ОК». При нажатии кнопки «Отмена» или закрытии окна шаблоны не сохраняются.



Подтверждение сохранения шаблонов.

7. Для сохранения внесённых изменений нажмите кнопку «Применить» в карточке ОД.

В случае необходимости удаления шаблонов нажмите кнопку «Удалить биометрические шаблоны» (крестик) в блоке «Биометрия» и сохраните изменения.

7.4.5. Синхронизация персонала

Для синхронизации данных в память устройств требуется предоставить персоналу доступ на точки доступа, к которым подключены устройства IRIS ID. Синхронизируются ОД типа «Сотрудник» и «Гостевой пропуск».

Дополнительно необходимо:

- Для доступа по распознаванию радужки глаза – присвоить ОД биометрический шаблон радужки и пропуск типа «Карта» в формате Wiegand-26, Wiegand-34 или Wiegand-58. Подробнее о добавлении шаблонов см. в разделе «Работа с базой биометрических шаблонов».
- Для доступа по распознаванию лиц – присвоить ОД фотографию и пропуск типа «Карта» в формате Wiegand-26, Wiegand-34 или Wiegand-58.

При синхронизации учитываются сроки действия ОД и пропусков: если срок доступа ОД истёк или ещё не наступил либо у ОД нет ни одного действующего пропуска типа «Карта», ОД не будет синхронизирован.

При выдаче гостевого пропуска посетителю через модуль «Расширенная поддержка пропусков посетителей» на терминал передаются ФИО и фотография, указанные на вкладке «Посетители». Биометрические шаблоны радужек глаз присваиваются гостевому пропуску на вкладке «Персонал».

Если гостевой пропуск выдан сотруднику, на терминале номер этого пропуска добавляется к пропускам сотрудника. При этом сохраняются все ранее присвоенные сотруднику биометрические шаблоны. При изъятии гостевого пропуска его номер удаляется из списка пропусков сотрудника на терминале.

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

Особенности работы с картами.

При занесении карт в систему Sigur необходимо указывать полный UID:

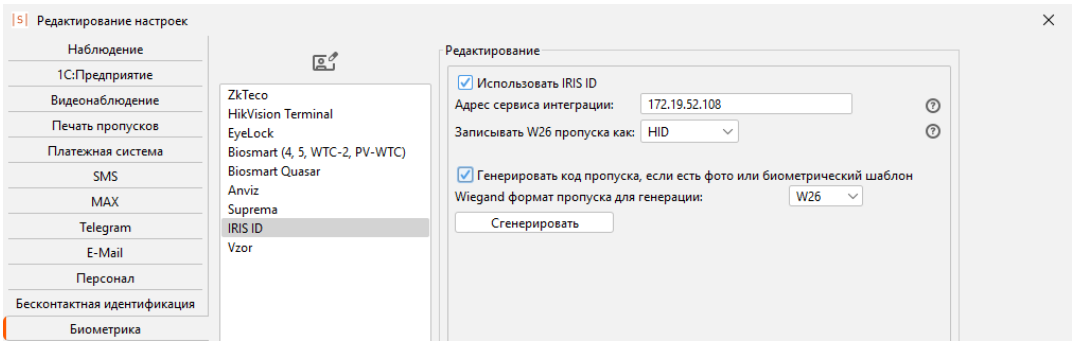
- если UID карты составляет 7 байт, карту необходимо заносить в ПО «Клиент» как Wiegand-58;
- если UID карты составляет 4 байта, карту необходимо заносить в ПО «Клиент» как Wiegand-34.

Поддержка типов карт зависит от встроенного считывателя карт терминала. В рамках интеграции не поддерживается работа с внешними считывателями, подключёнными к терминалу, и с картами Mifare DESFire.

Генерация кодов пропусков.

Если у ОД нет физического пропуска, вручную присвойте ОД пропуск типа «Карта» с произвольным номером в указанном формате или воспользуйтесь функцией генерации кодов пропусков. Для настройки генерации:

1. В ПО «Клиент» перейдите в меню «Файл» – «Настройки» – «Биометрика» – «IRIS ID».
2. Включите опцию «Генерировать код пропуска, если есть фото или биометрический шаблон» и выберите формат Wiegand.
3. Сохраните изменения кнопками «Применить» и «ОК».



Настройки генерации кодов пропусков.

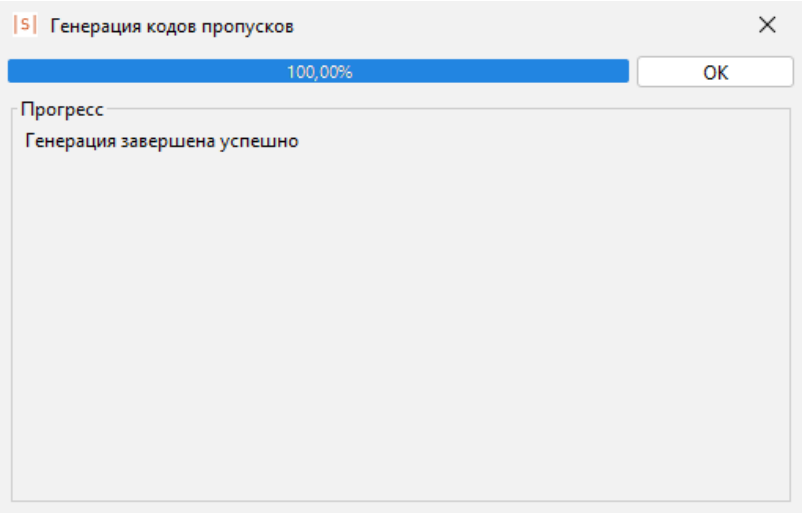
Если опция включена, то пропуска будут автоматически генерироваться при каждом последующем добавлении фотографии или биометрического шаблона радужки глаза. Исключение – случаи, когда у ОД уже есть карта в выбранном формате или ему присвоено 5 пропусков. Для гостевых пропусков генерация выполняется при добавлении шаблона радужки глаза на вкладке «Персонал» или фото на вкладке «Посетители».

Если в системе уже есть ранее добавленные ОД без пропусков в выбранном формате, 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».

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

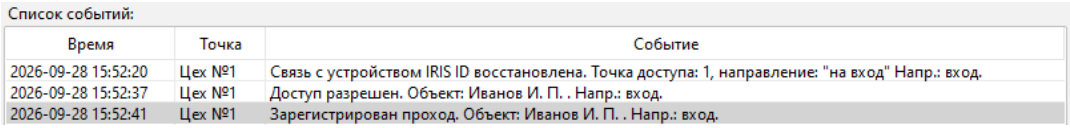
3. Система выведет сообщение о результате операции. Пропуска будут сгенерированы только для тех ОД, у которых есть фотография или биометрический шаблон радужки глаза (за исключением случаев, когда у ОД уже есть карта в выбранном формате или присвоено 5 пропусков).



Результат генерации кодов пропусков.

Идентификация и предоставление доступа.

При успешном распознавании идентификатора терминал IRIS ID отправляет на контроллер Sigur код пропуска ОД. Принятие решения о доступе осуществляется на стороне СКУД согласно настроенным правилам.


Список событий:

Время	Точка	Событие
2026-09-28 15:52:20	Цех №1	Связь с устройством IRIS ID восстановлена. Точка доступа: 1, направление: "на вход" Напр.: вход.
2026-09-28 15:52:37	Цех №1	Доступ разрешен. Объект: Иванов И. П. . Напр.: вход.
2026-09-28 15:52:41	Цех №1	Зарегистрирован проход. Объект: Иванов И. П. . 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