



Руководство по работе с мобильным терминалом Sigur

Редакция от 02.06.2023.

Оглавление

1.	Введение	3
2.	Используемые определения, обозначения и сокращения	4
3.	Требования	5
4.	Начало работы с терминалом	6
5.	Настройка на стороне ПО «Sigur»	8
5.1.	Санкционирование проходов сотрудников с NFC-терминала	10
6.	Настройка на мобильном устройстве	13
7.	Контакты	19

1. Введение

Данный документ содержит инструкцию по установке и эксплуатации NFC-терминала «Sigur» в составе системы контроля и управления доступом (СКУД) «Sigur».

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

Последнюю версию данного документа всегда можно найти на [странице](#).

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.
БД	База данных.

3. Требования

- ОС Android 4.0 и выше.
- Наличие встроенного NFC-чипа или поддержка OTG для подключения внешнего USB-считывателя.



Обратите внимание, для работы с внешними USB-считывателем необходимо, чтобы сам считыватель имел режим эмуляции набора на клавиатуре считанного кода в десятичном формате (т.е. например, для пропуска «072,61947» это должно быть «0004780539» или «4780539»), с переводом строки в конце кода.

- Версия сервера СКУД «Sigur» 1.1.1.48 и выше.
- Свободное место – 8,8 МБ.

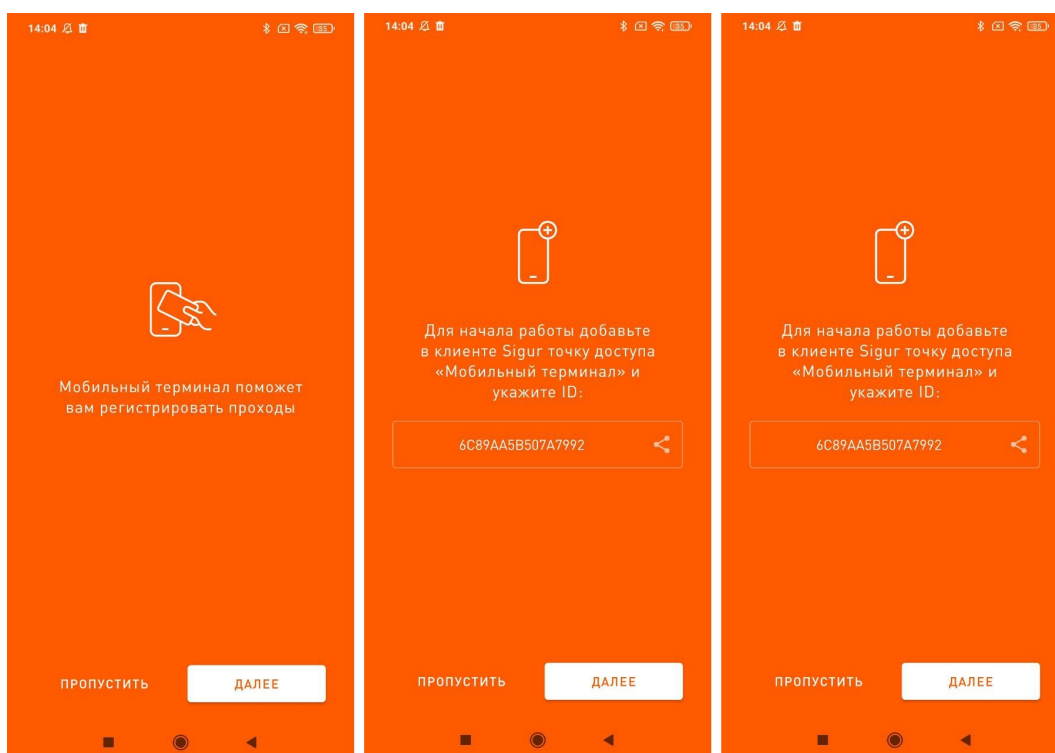
Известные проблемные модели смартфонов и устройств:

Не поддерживается работа приложения «NFC-терминал» на устройствах Samsung Galaxy совместно с использованием карт Mifare Classic. Данная проблема специфична для этого устройства, на нём не работает так же большинство других приложений, использующих NFC-модуль устройств.

4. Начало работы с терминалом

Для установки программного обеспечения мобильного терминала системы «Sigur» зайдите в Google Play Market под своей учётной записью, выберите «Установить» и предоставьте запрашиваемые приложением разрешения. Дальнейших действий от пользователя не требуется, по завершении процесса установки в рабочей области появится иконка приложения.

При первом запуске приложения пользователю будет предложено ознакомиться с небольшой инструкцией.

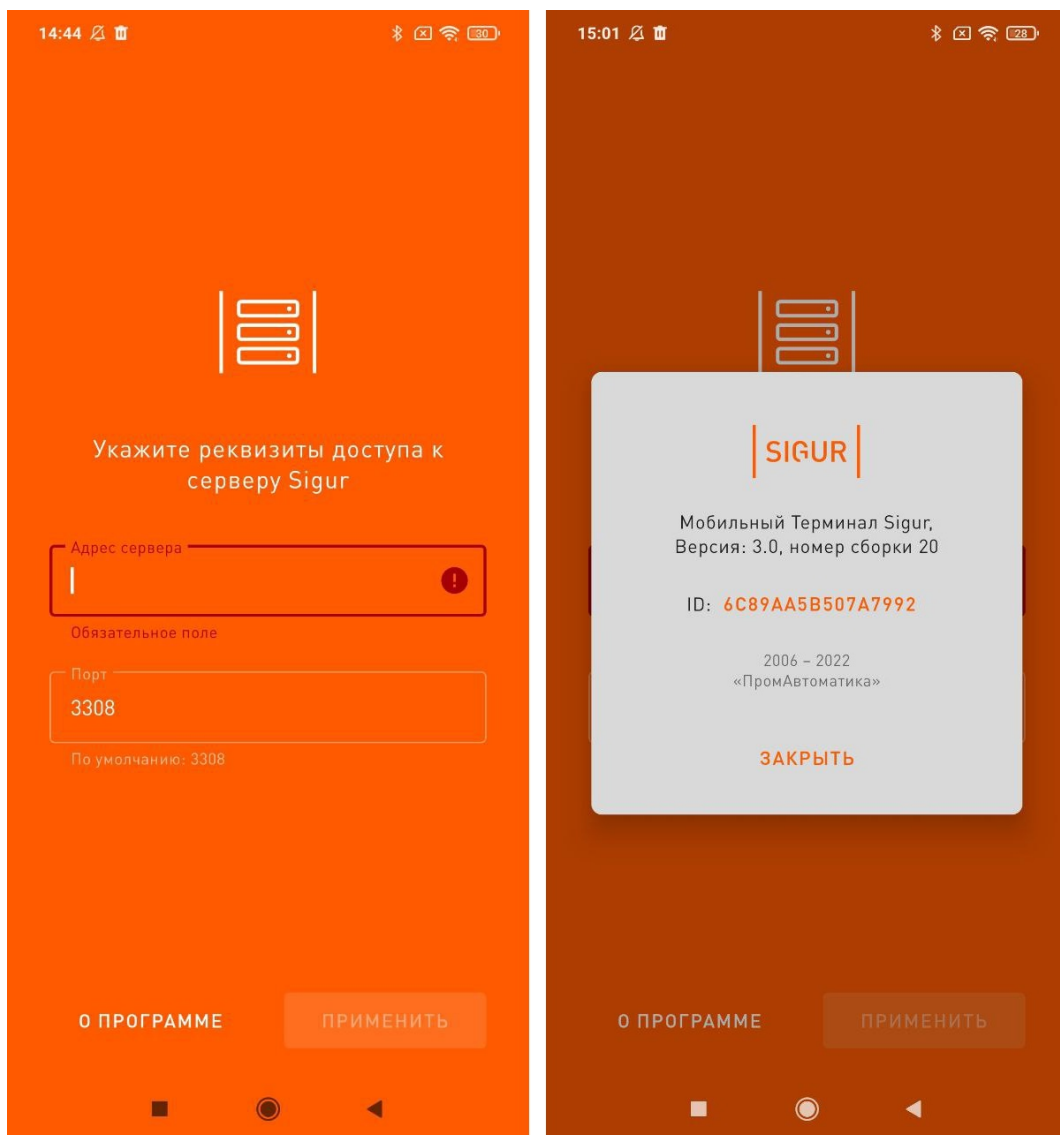


Первый запуск приложения.

Во время ознакомления с инструкцией рекомендуется зафиксировать уникальный ID NFC-терминала, он потребуется вам при дальнейшей настройке терминала через ПО «Sigur». Можно отправить идентификатор на email/мессенджер, нажав на соответствующий значок:



ID терминала, а также версию используемого мобильного приложения можно также узнать, нажав кнопку «О программе» на странице ввода настроек сервера Sigur. В этом окне можно нажать на значение ID терминала и поделиться им предпочтительным способом.



Просмотр информации о терминале.

5. Настройка на стороне ПО «Sigur»

1. На вкладке «Персонал» выберите уже существующего сотрудника или создайте новую запись для оператора, от имени которого будет работать NFC-терминал Sigur.

Перейдите на вкладку «Оператор» и, пролистав до самого конца, найдите пункт «Доступ к NFC терминалу».

Доступны следующие права:

- регистрировать проходы в направлении вход;
- регистрировать проходы в направлении выход;
- регистрировать проходы автоматически;
- санкционировать проход сотрудников из NFC терминала при запрещённом доступе.

Режимы Оправдания Расчетные счета Уведомления Active Directory Оператор

Использовать

- Редактировать посетителей
- Удалять персональные данные посетителей
- Доступ к вкладке "События"
- Доступ к вкладке "Охрана"
- Редактировать конфигурацию охранных зон
- Выполнять команды над охранными зонами
- Доступ к вкладке "Архив"
- Доступ к вкладке "Отчеты"
- Доступ по протоколу OIF (интеграция)
- Доступ к NFC терминалу
 - Регистрировать проходы в направлении вход
 - Регистрировать проходы в направлении выход
 - Регистрировать проходы автоматически
 - Санкционировать проход сотрудников из NFC терминала при запрещенном доступе
- Доступ к вкладке "KeyGuard"
- Доступ к вкладке "Ячейки"
 - Открывать ячейки
 - Редактировать настройки ячеек

Применить Отменить

Пример настройки прав для оператора NFC-терминала.

Первая пара предоставляет возможность оператору выбирать направление отметки вручную в случае каждого факта предъявления пропуска, установка опции "регистрировать проходы автоматически" в дополнение к первым двум позволяет предварительно выбрать направление, в котором будут автоматически регистрироваться последующие отметки.

При необходимости можно позволить оператору санкционировать проходы сотрудников при запрещённом доступе. Более подробно этот функционал описан в отдельной [главе](#).

2. Перейдите на вкладку «Оборудование». Создайте новую точку доступа и в области основных настроек в качестве «Интерфейса связи» выберите «NFC терминал».
 - Тип NFC терминала:
 - онлайн — терминал находится на постоянной связи с сервером, при потере связи автономная работа невозможна;
 - офлайн — терминал не требует постоянного наличия связи с сервером, информация по картам доступа и совершаемым отметкам прописывается в память устройства, при восстановлении связи с сервером происходит синхронизация;
 - онлайн касса — терминал работает в специальном режиме, позволяющем продавать позиции меню (при установленном модуле «Платёжная система») находится на постоянной связи с сервером.
 - ID терминала - уникальный ID устройства, узнать его можно из приложения на мобильном устройстве.

Настройки:

Основные | Видеонаблюдение | NFC терминал

Группа:	(нет)	...
Название точки доступа:	Терминал	
Зона со стороны выхода:	Рабочая территория	?
Зона со стороны входа:	внешняя территория	?
Интерфейс связи:	NFC терминал	
Тип NFC терминала:	онлайн терминал	
ID NFC терминала:	6C89AA5B507A7992	

Использовать для учета рабочего времени
 Временно отключить точку доступа

Применить Отменить

Пример настройки терминала в ПО «Sigur».

На вкладке «NFC терминал» можно указать дополнительные параметры для работы терминала:

- «Интервал информирования о скором истечении пропуска (часов):» - поле для указания временного интервала, в рамках которого до наступления окончания срока действия пропуска объекта на мобильном

терминале будет выводиться соответствующее предупреждение оператору системы.

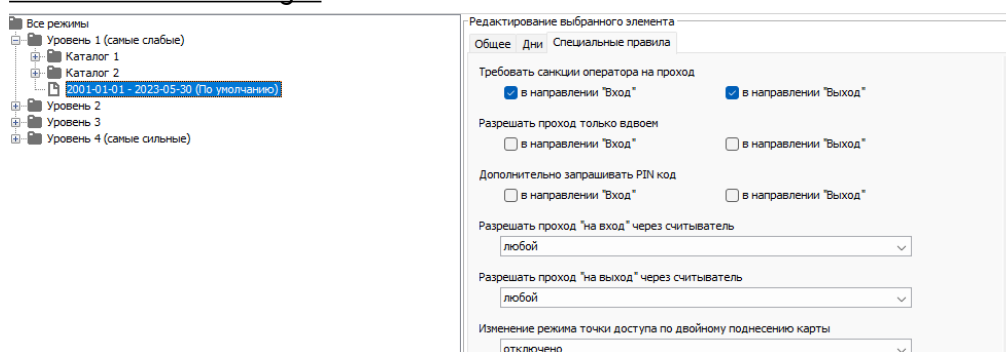
- «Время ожидания санкции оператора» - актуально для санкционирования проходов сотрудников при запрещённом доступе. Более подробно этот функционал описан в отдельной [главе](#).

Добавление пропусков производится на вкладке «Персонал», о заведении можно прочитать подробнее в «[Руководстве пользователя](#)».

5.1. Санкционирование проходов сотрудников с NFC-терминала

Опционально оператор может санкционировать проходы сотрудников из мобильного приложения в том случае, если сотруднику по каким-то причинам запрещён доступ. Для работы этого функционала необходимо:

1. В правах оператора-пользователя NFC-терминала должна быть активирована функция «санкционировать проход сотрудников из NFC терминала при запрещённом доступе»;
2. Сотруднику должен быть назначен режим доступа, в специальных правилах которого включена опция «Требовать санкции оператора на проход» для интересующего направления. При этом в момент идентификации сотрудника на терминале доступ должен быть запрещён по какой-либо причине (например, режим не позволяет проход в определённый интервал времени). Подробнее с настройкой режимов доступа можно ознакомиться в соответствующем разделе «[Руководства пользователя ПО Sigur](#)».



Пример настроек режима, требующего санкции оператора при проходе.

В настройках точки доступа на вкладке «Оборудование» в разделе «NFC-терминал» можно отрегулировать время ожидания санкции оператора:

Настройки:

Основные | Дополнительно | NFC терминал


Интервал информирования о скором истечении пропуска (часов):

Время ожидания санкции оператора:

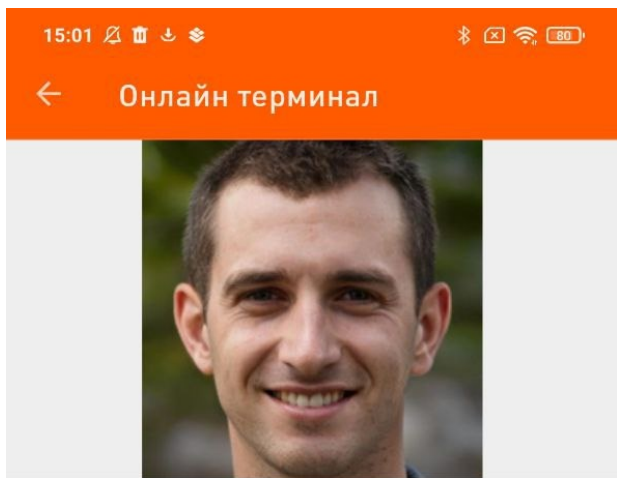
10,73 сек.

Применить | Отменить

Настройка времени ожидания санкции оператора в разделе «NFC-терминал».

 На текущий момент санкционировать проход сотрудника через терминал можно только при запрещённом доступе. При этом если сотрудник идентифицировался на точке доступа мобильный терминал, то санкцию на проход может предоставить только оператор этого мобильного терминала, предоставить санкцию на проход иными способами (через программу «Клиент», нажатием на физическую кнопку, через USB-считыватель) в такой ситуации нельзя.

В результате по факту идентификации сотрудника для прохода в определённом направлении оператору будет предложено санкционировать проход:



Илья Петров

НОМЕР	0000-0133
ДОЛЖНОСТЬ	РАБОЧИЙ
ПРИМЕЧАНИЕ	ДНЕВНАЯ СМЕНА

Требуется санкция оператора



Пример отображения запроса санкции оператора в мобильном терминале.

При этом в системе регистрируются события ожидания санкции при запрещённом доступе, а также события запрета доступа в том случае, если санкция на проход не была предоставлена. Просмотреть события можно через программу «Клиент» на вкладках «Наблюдение» или «Архив».

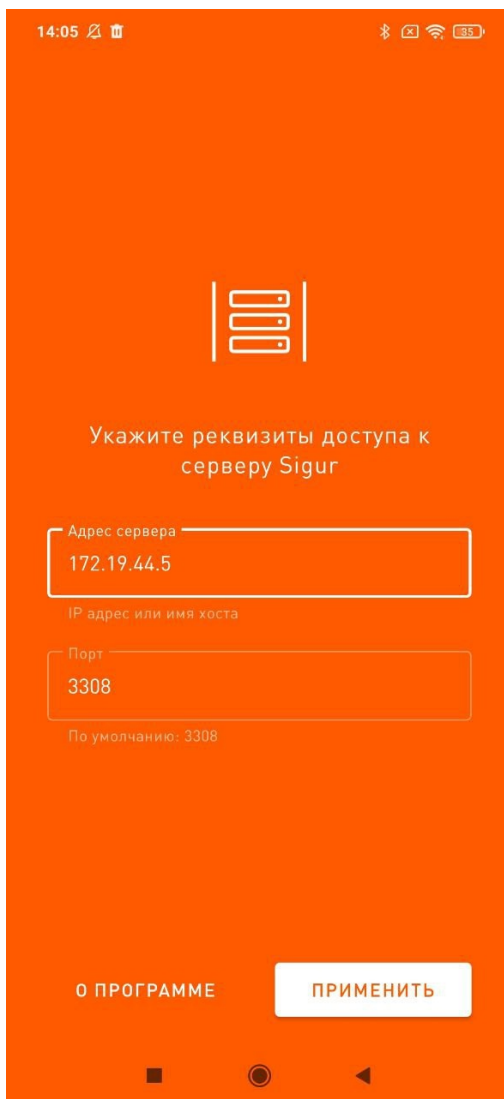
Список событий:

Время	Точка	Событие
2023-05-30 15:01:54	Точка доступа 3	Ожидание санкции оператора (доступ запрещен). Объект: Илья П. . Напр.: вход.
2023-05-30 15:01:35	Точка доступа 3	Зарегистрирован проход. Объект: Илья П. . Напр.: вход.
2023-05-30 15:02:15	Точка доступа 3	Ожидание санкции оператора (доступ запрещен). Объект: Илья П. . Напр.: вход.
2023-05-30 15:01:51	Точка доступа 3	Доступ запрещен. Оператор отказал в доступе. Объект: Илья П. . Напр.: вход.

Пример отображения событий на вкладке «Наблюдение» для санкционированного прохода и отказа в предоставлении санкции на проход.

6. Настройка на мобильном устройстве

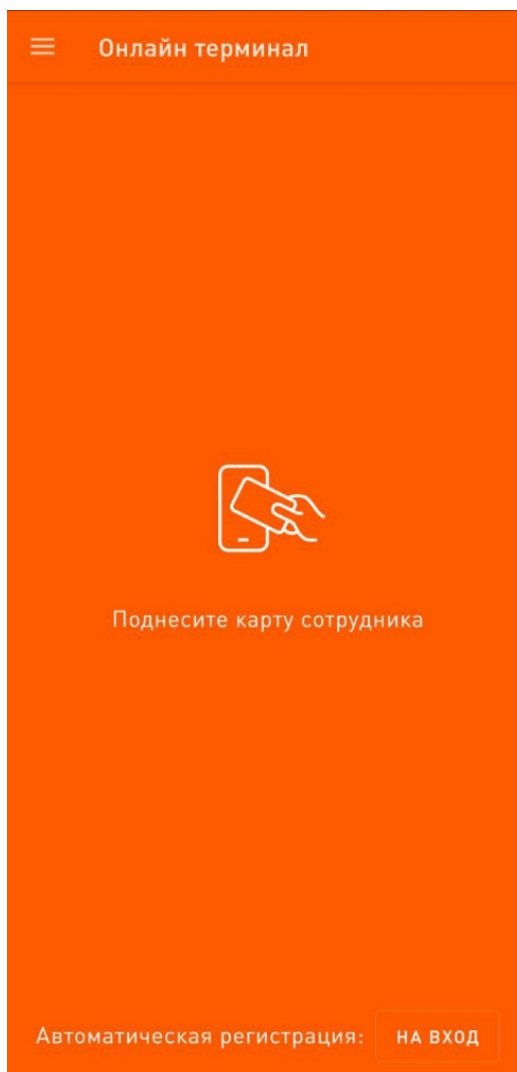
Если подключение к серверу ранее установлено не было, то пользователю будет предложено ввести реквизиты для подключения к серверу Sigur: IP-адрес и TCP-порт. После ввода параметров необходимо нажать кнопку «Применить».



Окно для настройки параметров подключения к серверу Sigur.

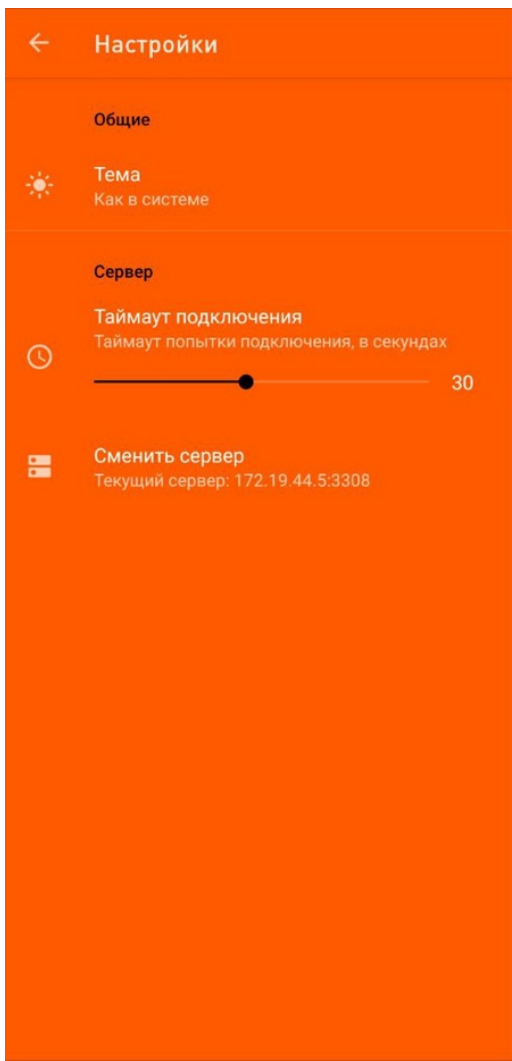
Если подключение к серверу ранее было установлено, а оператор уже авторизован в системе, то изменить параметры подключения к серверу можно нажав в основном окне приложения на следующую пиктограмму:





Основное окно приложения.

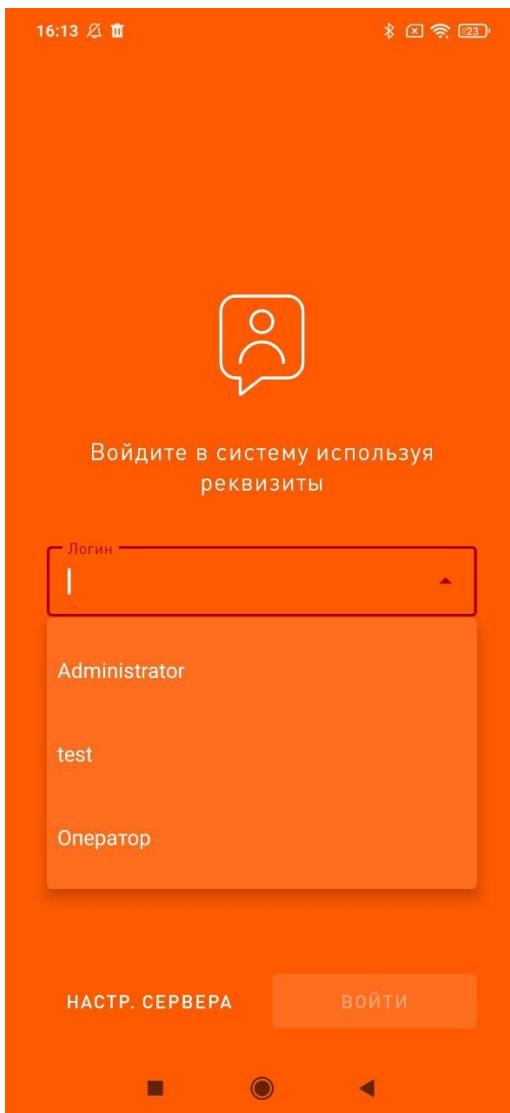
После чего перейти в «Настройки», выбрать «Сменить сервер» и подтвердить действия:



Окно настроек приложения.

При необходимости в окне настроек можно изменить таймаут на ожидание подключения к серверу, в течение которого терминал будет осуществлять попытку подключения на указанные IP-адресу и порт.

При успешном подключении к серверу в окне ввода реквизитов оператора будет предложено выбрать одного из операторов, которым разрешён доступ к NFC-терминалу:

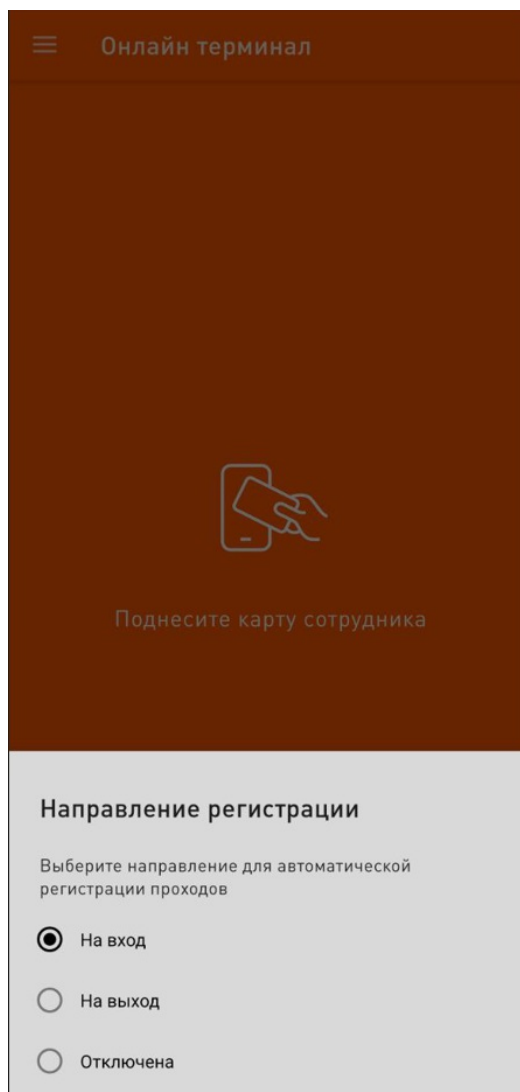


Окно ввода реквизитов оператора при успешном подключении к серверу.

После добавления устройства в ПО Sigur, создания оператора и логина от его имени в ПО на устройстве терминал готов к работе.

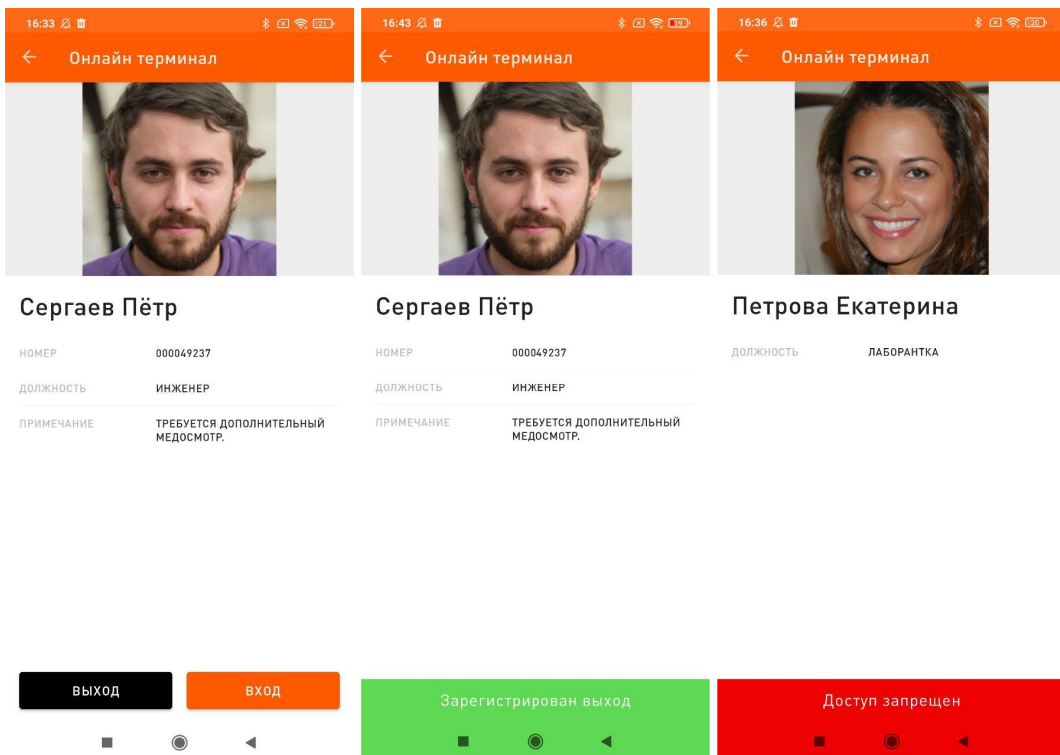
В основном окне отображается тип NFC-терминала: онлайн или офлайн, а также режим регистрации проходов.

Если оператору разрешено регистрировать проходы и на вход, и на выход, а также доступна возможность автоматической регистрации, то при нажатии на текущий режим регистрации проходов пользователь может изменить его:

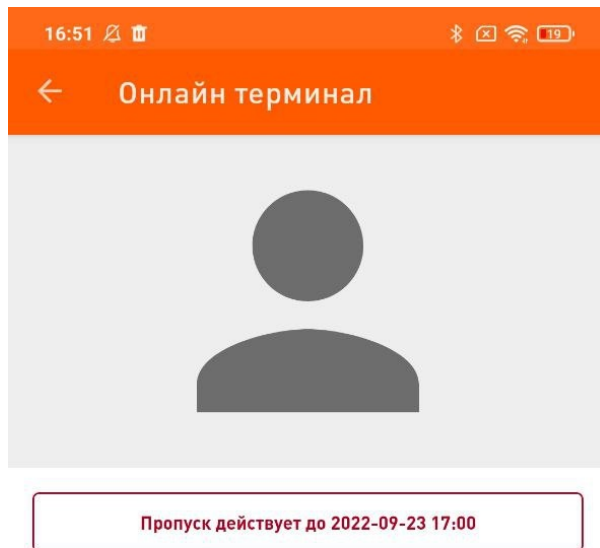


Выбор режима регистрации проходов.

При поднесении карты объекта доступа оператору терминала будет либо предложено вручную зафиксировать проход в нужном направлении, либо регистрация произойдёт автоматически, либо будет выведено сообщение о запрете доступа.



Примеры успешной идентификации с возможностью выбора направления прохода, успешной регистрации прохода и запрета доступа.



Ладанов Павел

Вид оповещения о приближении окончания срока действия пропуска.

7. 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