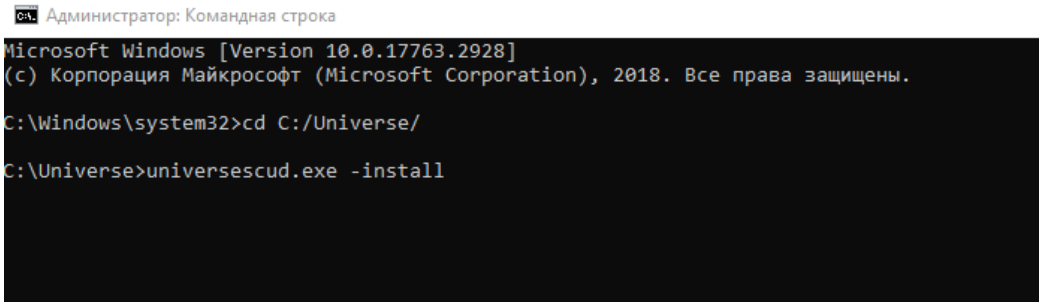
Работа с системой контроля и управления доступом (далее – СКУД) CRM Universe – Фитнес СКУД 1, реализована по средствам API – протокола (далее API) от компании Sigur (Сигур). Актуальная версия API – 1.8.

Базовый процесс установки и подключения одной точки доступа (далее ТД), без биометрии, без синхронизации данных (прямая выгрузка «карт клиентов – пропусков»), без проверки состояния ячеек/шкафов, без автоматического списания услуг. Протокол обмена считывателей - Wiegand 26. Лицензия на программный комплекс Sigur –базовая.

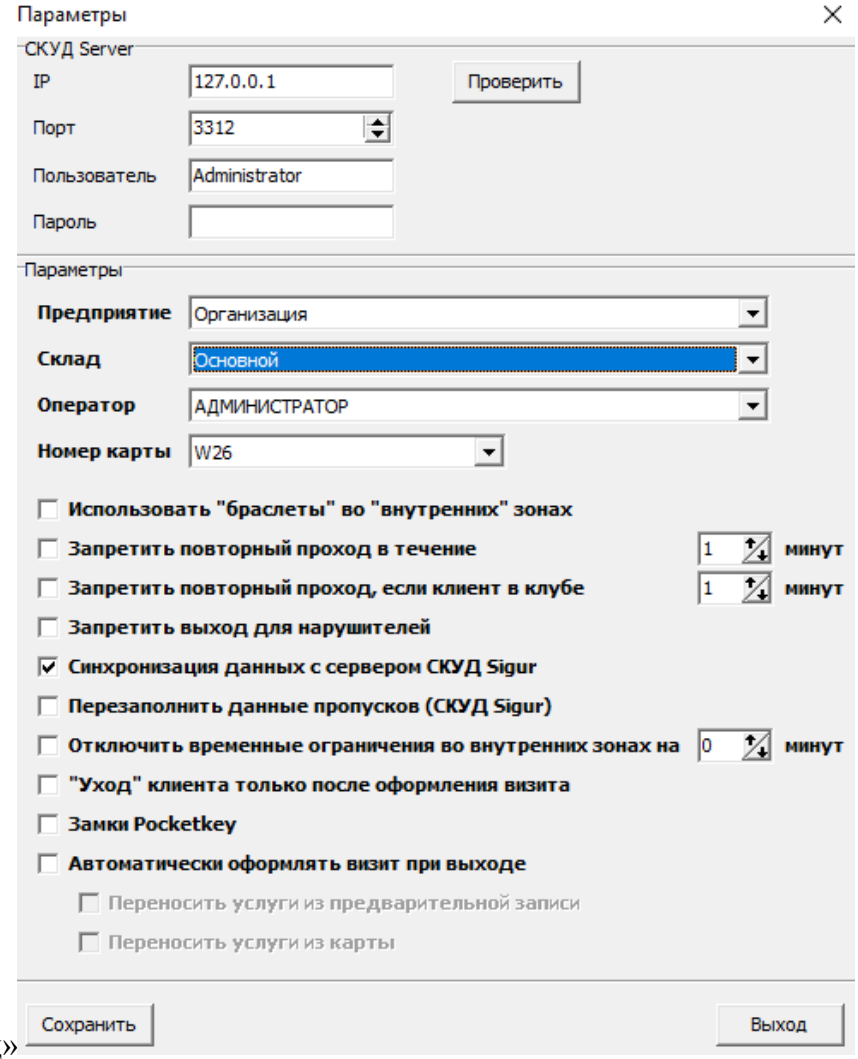
Подготовка дистрибутивов Sigur, Universe-Фитнес, ПО Universe Scud.

1. Установите актуальную версию программного комплекса Sigur (далее ПО Sigur). Процесс установки и базовой настройки «сервера» (ПК/Сервер на котором и будет происходить обработка «событий», проходящих с устройства – контроллер СКУД) и рабочего места «оператора СКУД» (при необходимости контроля сервера на дополнительном рабочем месте) подробно описан в руководстве для системного администратора от компании Sigur – Sigur Admin Guide. Ознакомиться с руководством вы можете по следующей ссылке.
   Страница 9 и далее.
2. Установите подключения к вашей модели контроллера. Universe-Soft реализует контроллеры СКУД Sigur моделей E500, E500U, E510. Процедура описана в том же руководстве Sigur Admin Guide доступном по ссылке выше.
   Страница 30 и далее.
3. Установите CRM Universe – Фитнес, в рамках руководства по установке. Обратите внимание, для функций СКУД внутри Universe – Фитнес, вам необходима лицензия на ключе защиты HASP или HW – лицензия в дистрибутиве.
4. Установите API обработчик Universe Scud (служба).
   1) Скопируйте файлы universescud.exe и UConfigServiceScud.exe в папку с дистрибутивом и базой данных Universe-Фитнес.
   2) Запустите Командную строку от имени Администратора (далее cmd) и перейдите в папку с дистрибутивом (например, C:/Universe). Используйте ключ установки –install и пропишите название обработчика universescd.exe. Пример работы в cmd на скриншоте ниже.



   3) Нажмите “Enter”, после чего, в случае успешной установки появиться окно со содержанием: System Service Successfully Installed

5. Произведите настройку обработчика через утилиту UConfigServiceScud.exe, запустив ее от имени администратора, в рамках требований клиента. Нажмите «Сохранить», далее «Выход»



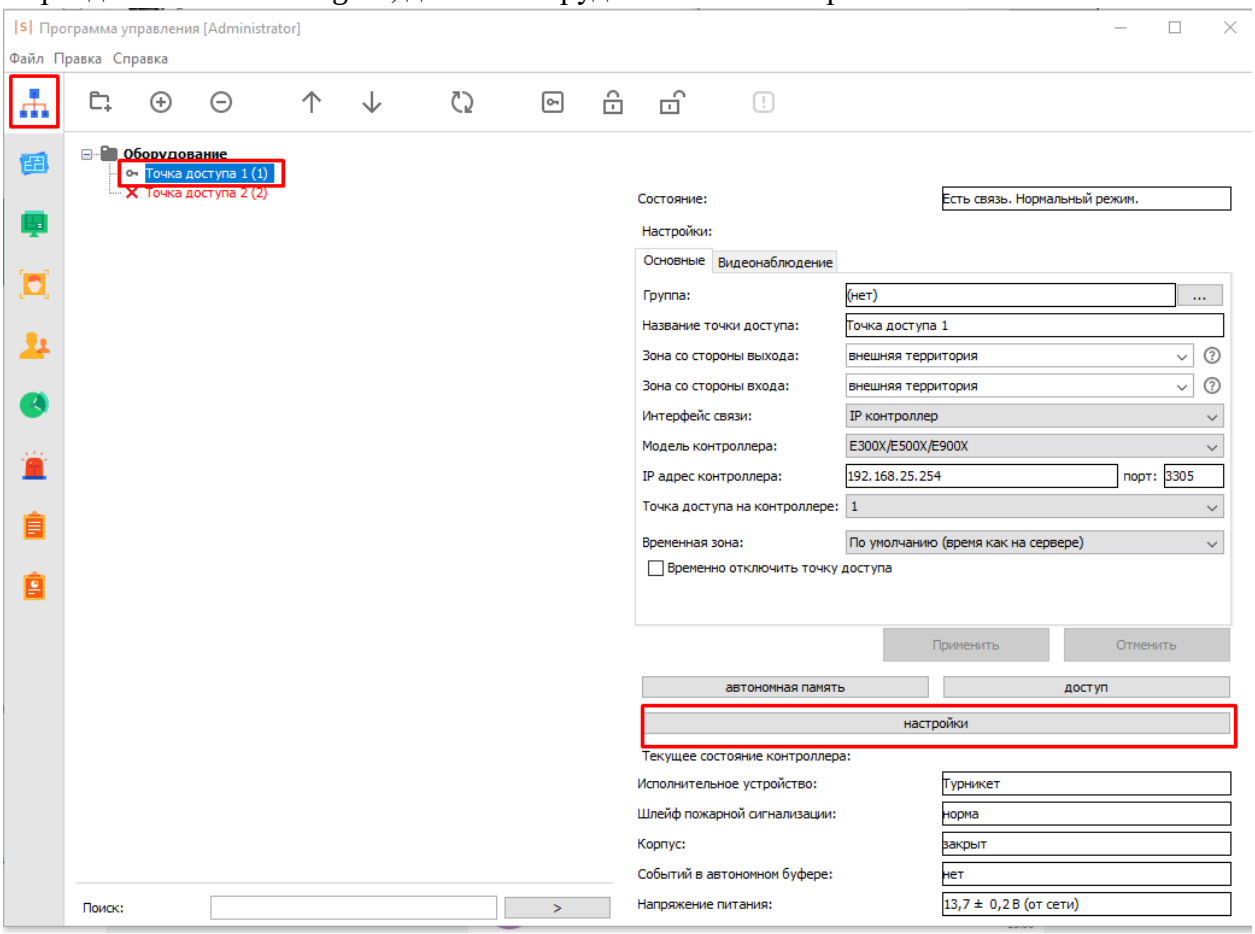
Описание для всех пунктов в конфигураторе обработчика UConfigServiceScud:

- **IP** – здесь указывается IP- адрес «сервера» Sigur на котором установлен программный комплекс Sigur. В рамках данного руководства рассматривается только установка «сервера», соответственно подключение к API Sigur будет происходить локально (localhost/127.0.0.1).
- **Порт** – данное поле не подлежит редактированию, т.к изменение порта необходимо производить внутренними средствами ПО Sigur. Только после изменения на стороне ПО Sigur мы можем изменить порт. По умолчанию номер порта, всегда 3312
- **Пользователь** – при необходимости или по желанию клиента обходимо вписать пользователя из «Клиент Sigur», без ограничения доступа. По умолчанию - Administrator
- **Пароль** - при необходимости или по желанию клиента обходимо вписать пароль от пользователя из «Клиент Sigura», без ограничения доступа. По умолчанию пароль отсутствует.
- **Проверить** - после настройки полей подключения нажмите на «проверить» для того что бы конфигуратор проверил подключение к программному комплексу

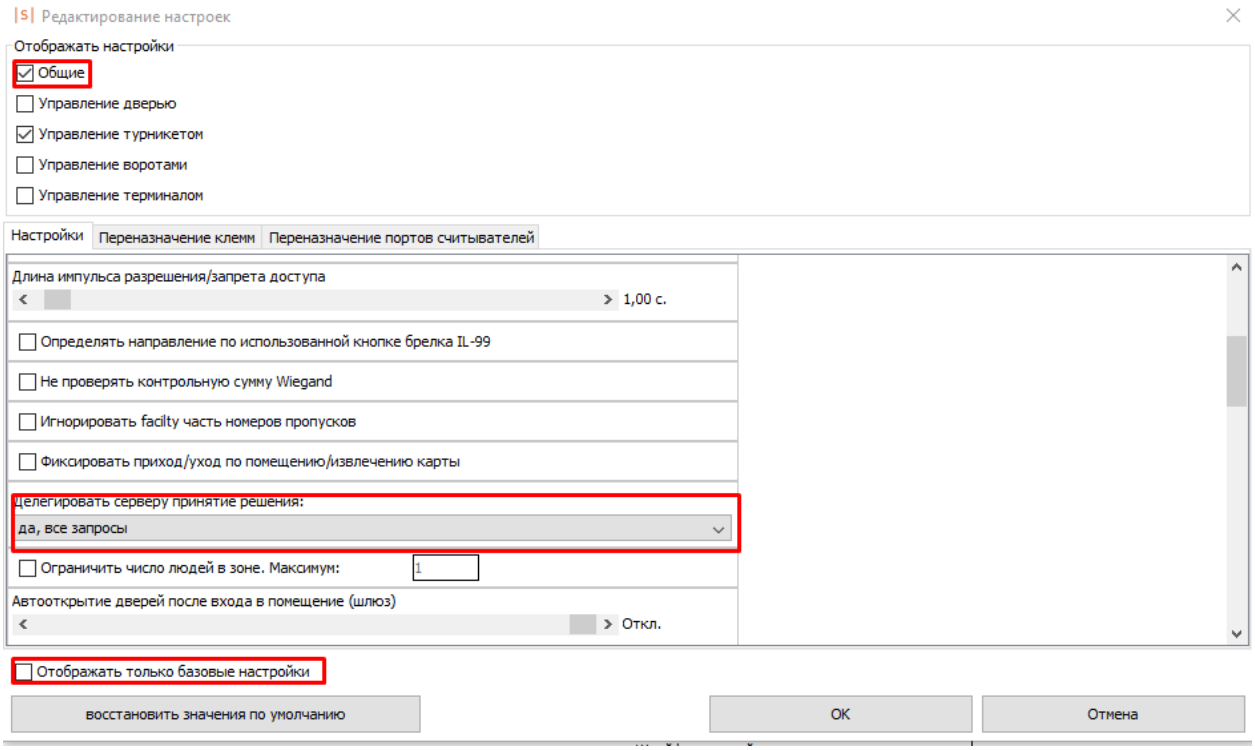
Sigur. В случае успешного подключения вы увидите сообщение: «соединение установлено».

- **Использовать “браслеты” во “внутренних” зонах** – используется для работы с «браслетами», заранее занесенными в «Справочники» -«Карты»-«Номера ключей (браслетов)» и их ручного назначения через форму «Операции» - «Обслуживаются». Вход в клуб и доступ осуществляется после присвоения браслета администратором фитнес-клуба.
- **Запретить повторный проход в течении** – запрет повторного прохода, в рамках указанного времени через ТД. Логика работы – клиент прошел в 12:00, при указании 120 минут, следующий проход через ТД он сможет совершить только через 120 минут, т.е в 14:00. Ограничение работает для всех типов точек доступа. По умолчанию ограничения нет.
- **Запретить повторный проход, если клиент в клубе -** запрет повторного прохода, в рамках указанного времени через «внешнюю» ТД (клиент при успешном проходе попадает в «Операции» - «Обслуживаются» автоматически). Логика работы - клиент пришел в «клуб» в 12:00, при указании 120 минут, следующий «вход в клуб» этого же клиента будет возможен только в 14.00. По умолчанию ограничения нет.
- **Запретить выход нарушителей** – запрет «выхода из клуба», через внешнюю ТД, при выявлении нарушений (мед. Справка т д)
- **Синхронизация данных с сервером СКУД Sigur** – необходима при использовании биометрии и обмена данными с базой пропусков Sigur.
- **Перезаполнять данные пропусков (СКУД Sigur) -** необходима при использовании биометрии и при необходимости пакетной и полной «чистке» (перезаполнению) пропусков.
- **Отключить временные ограничения во внутренних зонах на –** корректировка смещения ограничений по времени на проходы через «внутренние» ТД. Логика работы: при использовании временных ограничений на «Видах карт», например, с 12:00 до 14:00 посетитель может войти в данную ТД в 13:58 и ему обязаны оказать услугу. При попытке пройти проход будет запрещен, т.к это нарушение временных ограничений на карте. При указании 0 и установки галочки в «чекбоксе», данное временное ограничение будет игнорироваться, но только во «внутренних» ТД. Во «внешних» ТД ограничения продолжат работать в полном объеме.
- **«Уход» клиента только после оформления визита –** «выход из клуба» только после оформления визита.
- **Замки PocketKey –** необходимо для корректной работы проверки состояния закрытого шкафа, с замками про-ва PocketKey
- **Автоматически оформлять визит при выходе (Переносить услуги из предварительной записи/карты) –** необходимо для автоматического списания услуг с проданной карты посетителю(клиенту)

6. Перейдите в «Клиент Sigur», далее «Оборудование» - «Настройки»

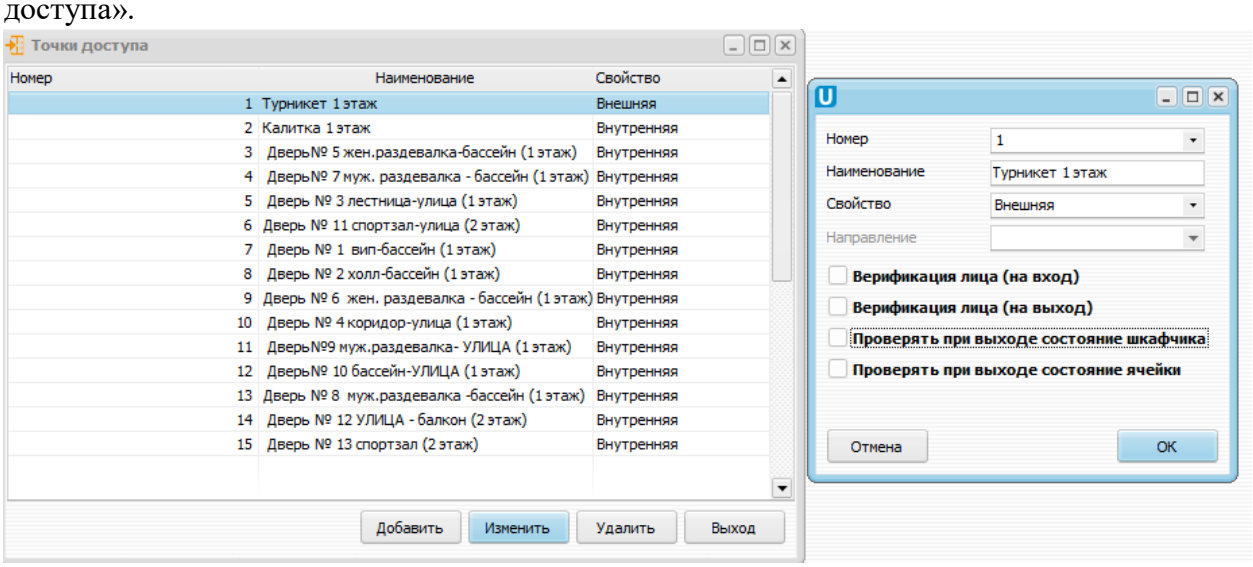


7. Установить чекбокс «Общее», очистите чекбокс «отображать только базовые настройки» и установите «делегировать серверу принятие решения: да, все запросы». Нажмите «Ок».



8. Запустите службу Universe Scud удобным способом (cmd/services.msc)
9. Запустите Universe – Фитнес. Перейдите в «Операции» - «СКУД» - «Точки доступа»

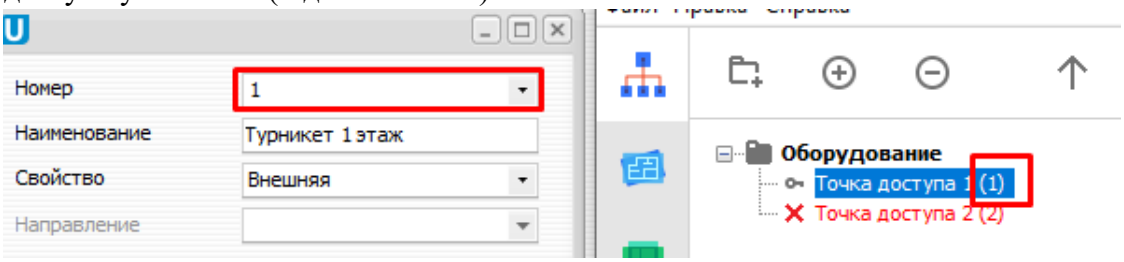
10. На данном этапе, **нужно разграничить и понимать,** что такое «Свойство точки доступа».



Свойство ТД может быть, как внутренним, так и внешним. Внешняя ТД – это точка доступа на вход и выход «из клуба». Только при таком свойстве ТД «клиент» будет попадать в «Обслуживаются». Внутренняя ТД – это точка доступа, когда клиент пересек внешнюю ТД и уже находиться «в клубе». В рамках данного руководства мы рассматриваем только самую простую модель из одной Внешней ТД.

Описание для всех пунктов в настройках точки доступа:

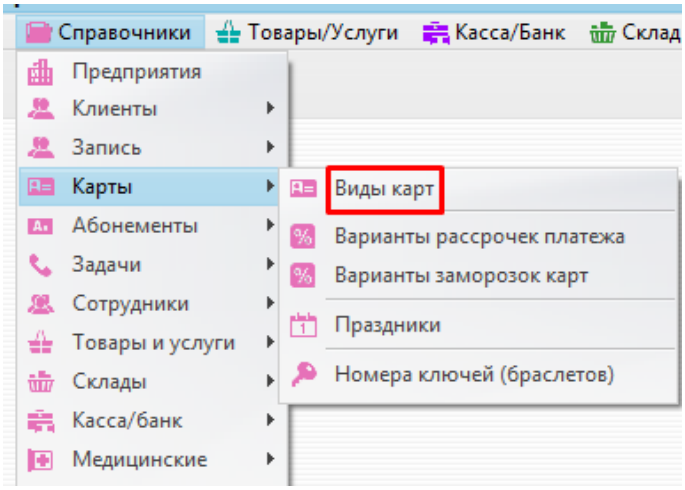
- **Номер** – номер точки доступа должен строго соответствовать номеру точки доступа указанной (и добавленной) в Клиенте



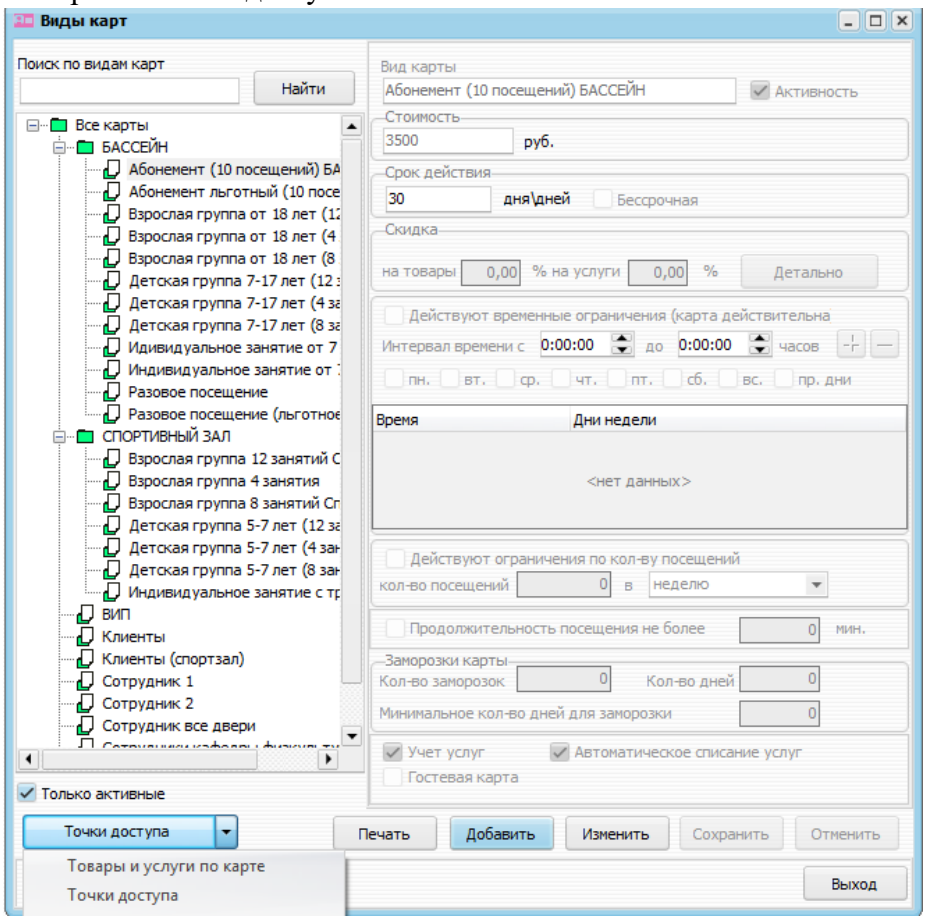
- **Наименование** – для ввода желаемого названия ТД в рамках Universe-Фитнес
- **Свойство** – выбор свойства редактируемой ТД.
- **Направление** – недоступно для изменения.
- **Верификация лица (на вход)** – включение биометрии на вход (двухфакторная проверка лицо + метка. С **версии 2.4.2.13 тестовая** и выше, данная настройка работает на любое свойство ТД. Внимание! На момент написания данного руководства в «релизной» версии 2.4.2.13 данного функционал работает только на свойство Внешняя!
- **Верификация лица (на выход)** - включение биометрии на выход (двухфакторная проверка лицо + метка)
- **Проверять при выходе состояние шкафчика** – проверка статуса замков Kerong/WT
- **Проверять при выходе состояние ячейки** – проверка статуса «ячеек» для замков Kerong/WT.

После окончания настройки нажмите «Ок». Нажмите «Выход».

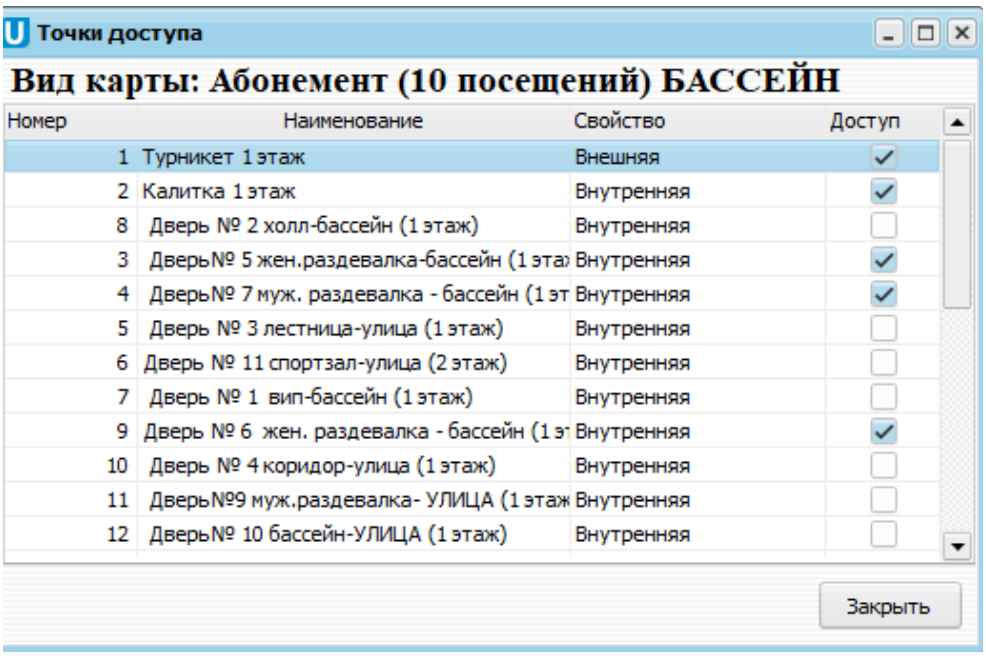
11. Перейдите в «Справочники» - «Карты» - «Виды карт»



12. Выберите нужную карту или добавьте новую. После «выбора» карты, в левом углу выберете «Точки доступа»



Далее, в открывшемся окне, разрешите доступ в чекбоксе «доступ»



Таким образом, вы сможете разграничить доступ конкретного вида карт, на конкретные ТД.

13. Нажмите «закрыть».
14. Перейдите в директорию, куда был установлен обработчик Universe Scud. После запуска службы, сделанного ранее, в директории дылжен был появиться файл event.txt. Отройте его удобным для вас способом (например «блокнот»). Если все было настроено корректно, вы увидите следующее:

```
15.06.2022 17:21:38 LOGIN 1.8 "Administrator" ""
15.06.2022 17:21:38 OK
15.06.2022 17:21:39 SUBSCRIBE
15.06.2022 17:21:39 OK
15.06.2022 17:21:40 DELEGATION_START
15.06.2022 17:21:40 OK
```

15. Выполните тестовый проход через вашу ТД (турникет, эл.замок, калитка и т.д)