Контроллер
UEM SKD control

Руководство по установке, настройке и эксплуатации ПО

Версия документа 1.0.16

Содержание

1 Описание

Пользовательская программа для работы с контроллером СКУД UEM состоит из двух основных частей - серверного и клиентского ПО.

Серверное ПО осуществляет хранение и обработку данных, взаимодействие с контроллерами и прочие функции. Клиентское ПО осуществляет доступ к серверному ПО для его конфигурирования и взаимодействия с данными.

Серверное и клиентское ПО не обязательно должны быть размещены на одном устройстве; клиентское ПО поддерживает удалённый доступ к серверному ПО (в том числе по защищённому протоколу HTTPS).

Серверное ПО поставляется в виде файла с форматом .msi с названием «UEM Server.msi»

Клиентское ПО поставляется в виде файла с форматом .msi с названием «UEM Interface.msi»

2 Технические требования

Минимальная конфигурация **серверного ПО**:

- 64-разрядная ОС Windows 10 или выше;
- 8 ГБ Оперативной памяти;
- Процессор скоростью 2 ГГц и не менее 4 потоков;
- 1 ГБ Свободного места на жёстком диске (плюс место для базы данных).

Минимальна конфигурация **клиентского ПО**:

- 64-разрядная ОС Windows 10 или выше;
- 8 ГБ Оперативной памяти;
- Процессор скоростью 2 ГГц и не менее 4 потоков;
- 3 ГБ Свободного места на жёстком диске

3 Установка и настройка

3.1 Установка сервера

Установка серверного ПО производится через .msi файл с названием «UEM Server.msi». После его запуска пользователю будет предложено выбрать путь для установки ПО, путь по умолчанию: *Program Files/MicroEM/UEMServer.* Сервер устанавливается как Windows-сервис, поэтому его последующий запуск производится в автоматическом режиме.

Текущая версия серверного ПО UEM Server поставляется как готовый к использованию пакет со стандартными настройками.

3.2 Настройка сервера через web-интерфейс UEM Dashboard.

3.2.1 Настройка через UEM Dashboard

Для удобства пользователя серверное ПО поставляется с веб-интерфейсом UEM Dashboard, доступном по адресу */WebAdmin*. По умолчанию, доступ к панели управления можно получить по адресу *http://localhost:5142/WebAdmin*.

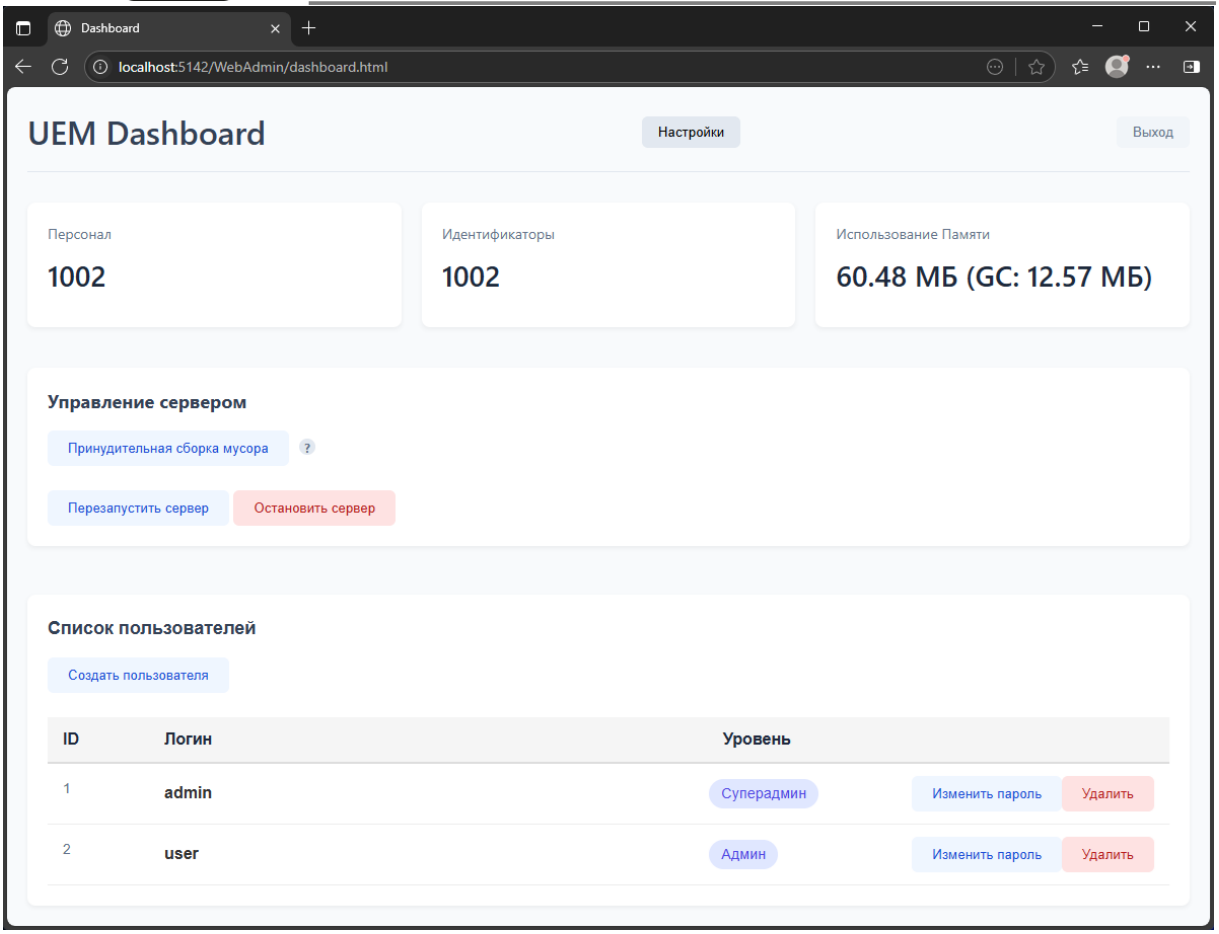
Если нет возможности воспользоваться панелью управления, предусмотрена настройка через файл настройки appsetting с форматом .json, который описан в соответствующем разделе документации.

Ознакомительная версия серверного ПО UEM Server не предполагает глубокой настройки и поставляется как готовый к использованию пакет. Дополнительные настройки будут добавлены в полную версия серверного ПО.

> **ВНИМАНИЕ!**
> Настройки применяются только после перезапуска сервера.

3.2.2 Введение в UEM Dashboard

UEM Dashboard - это веб-интерфейс для настройки сервера и управления им.

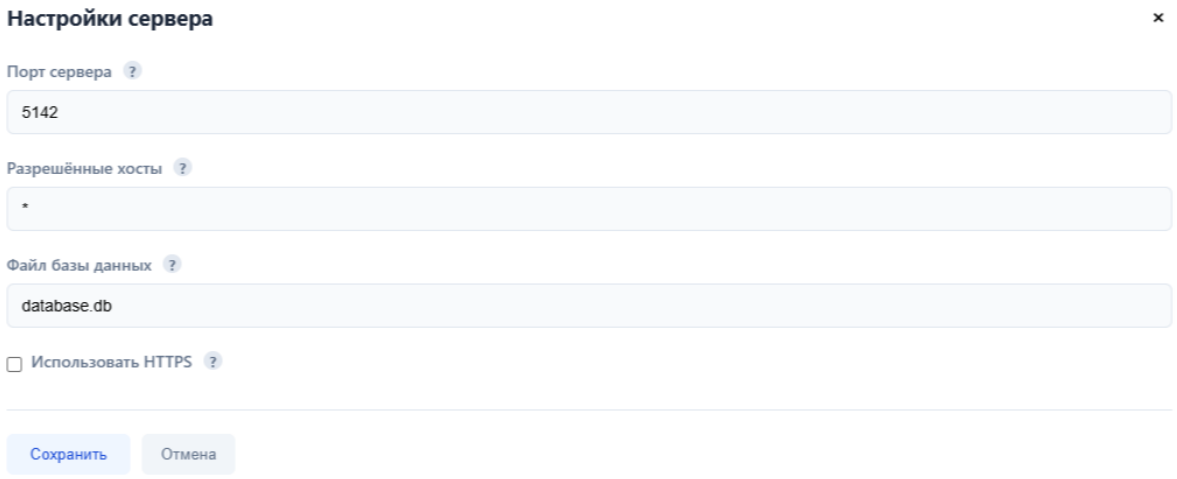


UEM Dashboard

С помощью UEM Dashboard можно выполнить первоначальную настройку сервера; перезагрузить сервер; остановить сервер; отслеживать статистику сервера (количество идентификаторов, количество персонала, потребление памяти); а также выполнять базовое администрирование.

3.2.3 Настройка сервера

Для открытия меню настройки сервера, нажмите кнопку «Настройки» в веб-интерфейсе UEM Dashboard.



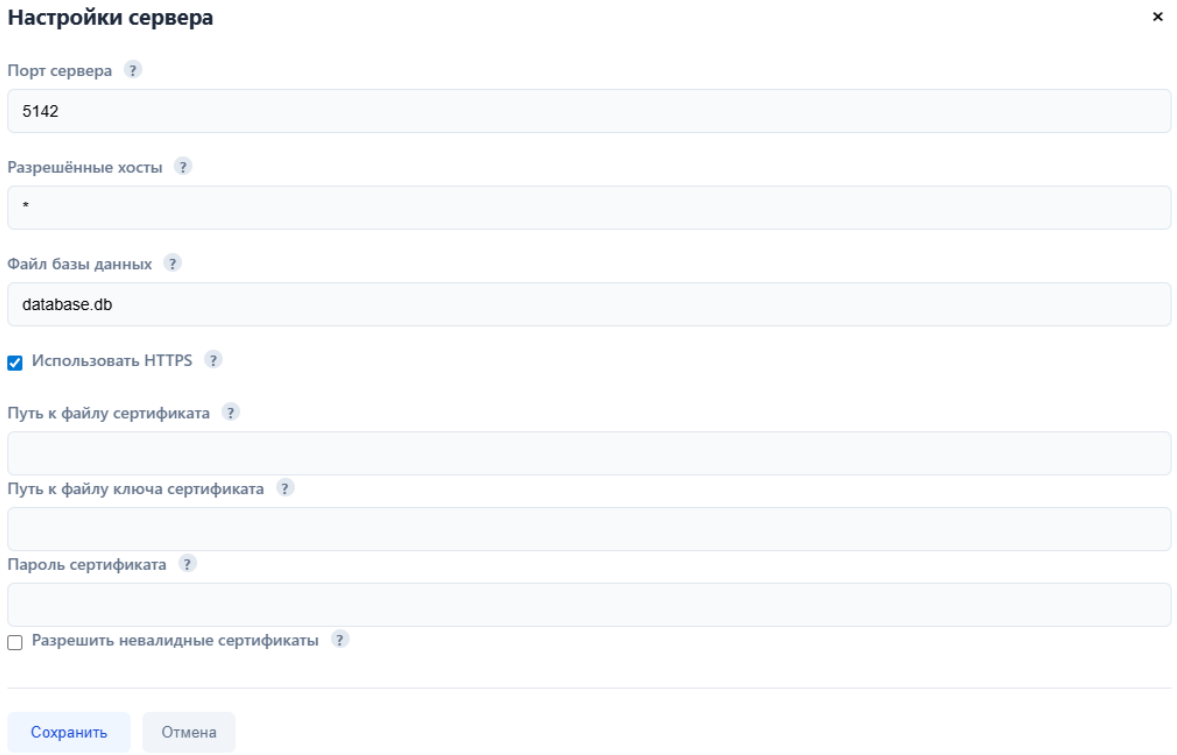
Настройки сервера

Установите необходимые настройки, после чего нажмите кнопку «Сохранить». UEM Dashboard попросит подтвердить намерение сохранить настройки, после чего (в случае корректно установленных настроек) применит их и автоматически перезапустит сервер. При этом окно браузера будет перенаправлено на новый адрес сервера.

3.2.4 Настройка HTTPS

Серверное ПО поддерживает работу по защищённому протоколу HTTPS. Для его настройки потребуется валидный SSL сертификат.

Для включения режима HTTPS, отметьте соответствующий пункт в настройках сервера. После этого появится дополнительное меню.



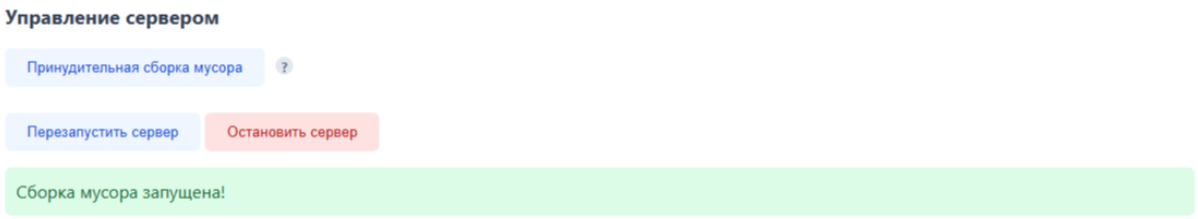
Заполните соответствующие поля:

- В случае сертификата в формате .pem, заполните путь к файлу сертификата и путь к файлу ключа сертификата;
- В случае сертификата в формате .pfx, заполните путь к файлу сертификата и пароль сертификата (если имеется);
- Отметьте пункт «Разрешить невалидные сертификаты», если сертификат самоподписанный (например, локально).

После этого сохраните изменения и сервер автоматически перезагрузится, а веб-страница будет перенаправлена на новый, защищённый адрес.

3.2.5 Управление сервером

Управление сервером происходит на панели «Управление сервером» веб-интерфейса UEM Dashboard.



Управление сервером

Нажмите соответствующую кнопка для запуска действия.

> **ПРИМЕЧАНИЕ!**
> Сборка мусора - специальная функция, позволяющая высвободить немного оперативной памяти, если сервер начал использовать слишком много.

3.2.6 Управление пользователями

UEM Dashboard позволяет управлять учётными записями пользователей системы. Управление производится в меню "Список пользователей".

3.2.7 Добавление пользователя

Нажмите кнопку "Создать пользователя" на панели "Список пользователей". Во всплывающем диалоге заполните все поля.

Создание нового пользователя

Нажмите кнопку "Создать".

WebAdmin предоставляет возможность управления учетными записями, которые используются для доступа к серверу через:

- WebAdmin (веб-интерфейс администратора),
- клиентское приложение,
- API (Swagger). (Находится в разработке. Доступ предоставляется по запросу.)

Доступ к WebAdmin разрешён только для пользователей с уровнями доступа **0 (Супер-админ)** и **1 (Админ)**.

3.2.8 Уровни доступа

Уровень	Название	Возможности
0	Супер-администратор	Полный доступ ко всем функциям WebAdmin. Единственная учетная запись уровня 0 в системе. Может управлять всеми учетными записями, включая администраторов. Доступ к авторизации и функционалу клиентского приложения.
1	Администратор	Имеет доступ к WebAdmin. Может управлять учетными записями с уровнем доступа ниже (Пользователь, уровень 2). Доступ к авторизации и функционалу клиентского приложения.
2	Пользователь	Не имеет доступа к WebAdmin. Может работать только через клиентское приложение. Доступ к авторизации и функционалу клиентского приложения.

В будущем список уровней может быть расширен.

Учетная запись Супер-администратора

- В системе может существовать **только одна** учетная запись уровня 0.
- При **чистой установке сервера** автоматически создается учетная запись супер-админа со стандартными данными:
  - **Логин:** admin
  - **Пароль:** admin
- Только для этой учетной записи разрешено изменение логина.
- Удаление или изменение уровня доступа для этой учетной записи **недоступны**.
- Учетную запись супер-админа **нельзя удалить** или изменить её уровень доступа.

3.2.9 Удаление пользователя

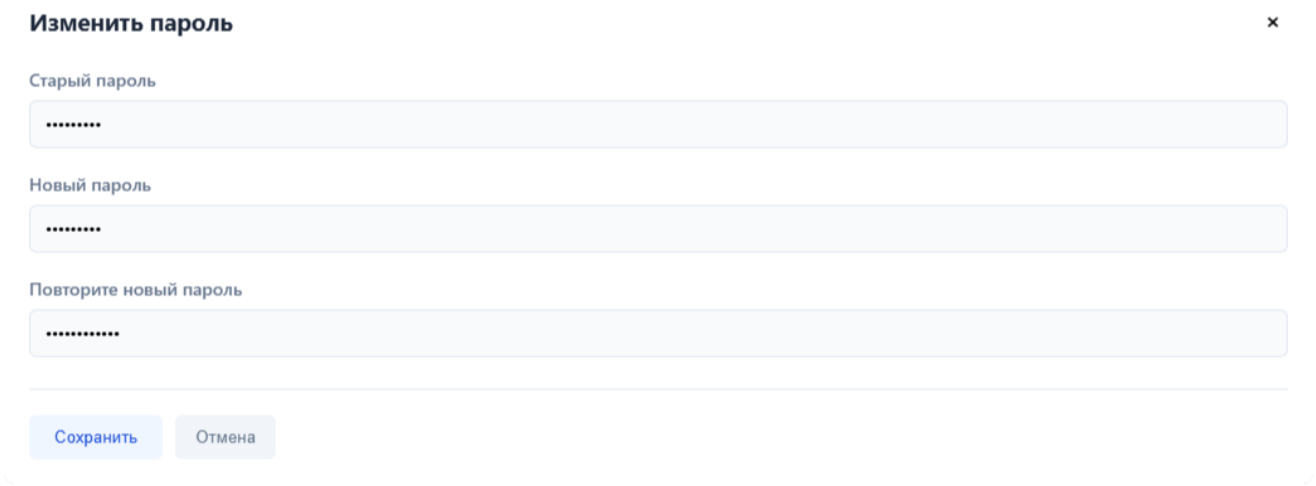
Для удаления пользователя, нажмите кнопку "Удалить" напротив соответствующего пользователя.

> **ПРИМЕЧАНИЕ!**
> Не любого пользователя можно удалить. Удалить можно только пользователя с меньшим уровнем доступа чем на текущем аккаунте.

3.2.10 Редактирование пользователя

Смена пароля

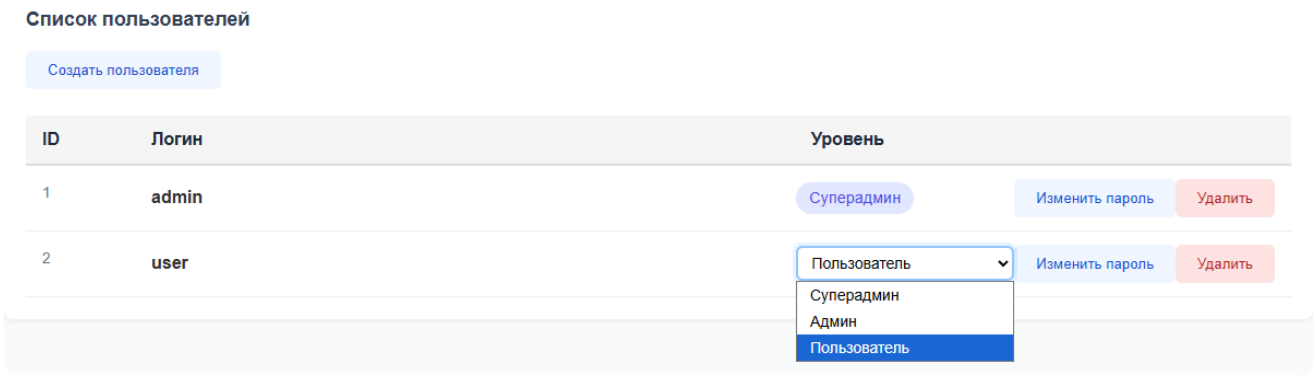
Для смены пароля пользователя, нажмите кнопку "Поменять пароль" напротив соответствующего пользователя. Во всплывающем диалоге заполните все необходимые поля, после чего нажмите "Сохранить".



Смена пароля

Смена уровня доступа

Для смены уровня доступа пользователя, кликните на текущий уровень доступа в таблице напротив соответствующего пользователя. Поле превратится в выкидной список.



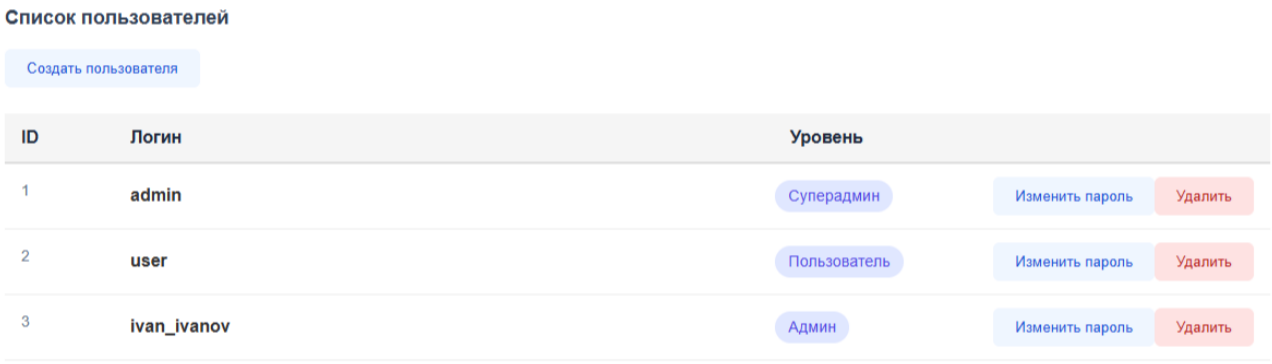
Смена уровня доступа

В выкидном списке выберите нужный уровень доступа. В случае успеха, изменения сохранятся автоматически.

> **ПРИМЕЧАНИЕ!**
> Менять уровни доступа может только супер-пользователь. Также, в системе может быть только один супер-пользователь.

3.2.11 Панель управления учетными записями

В разделе "Список пользователей" отображается таблица всех зарегистрированных в системе пользователей:



Список пользователей

Все учетные записи, независимо от уровня, могут быть использованы для авторизации через клиентское приложение.

3.3 Ручная настройка сервера

3.3.1 Остановка и запуск сервера

Остановка и запуск сервера осуществляется через встроенный в Windows интерфейс «Службы».

Чтобы остановить сервер:

- Запустите встроенное в Windows приложение «Службы»;
- Найдите в списке служб службу с названием «UEM Server»;
- Щёлкните правой кнопкой мыши;
- Щёлкните левой кнопкой мыши по пункту меню «Остановить».

Чтобы запустить остановленный сервер:

- Запустите встроенное в Windows приложение «Службы»;
- Найдите в списке служб службу с названием «UEM Server»;
- Щёлкните правой кнопкой мыши;
- Щёлкните левой кнопкой мыши по пункту меню «Запустить».

3.3.2 Установка порта сервера

Чтобы изменить порт, на котором работает сервер, необходимо:

- Открыть папку с установленным сервером (по умолчанию *Program Files/MicroEM/UEMServer*);
- Открыть для редактирования файл appsettings с форматом .json;
- Отредактировать пункт «Urls» в объекте Kestrel/Endpoints/Https.
    - Значение по умолчанию: *http://localhost:5142*. Это значит, что сервер принимает соединения на порту 5142;
    - Чтобы изменить порт, необходимо изменить цифры в конце адреса. Например, чтобы задать порт 1234, необходимо указать *http://localhost:1234*.

3.3.3 Настройка SSL соединения

Серверное ПО поддерживает работу по защищённому протоколу HTTPS. Для его настройки потребуется валидный SSL сертификат.

Чтобы сервер начал работать по защищённому протоколу HTTPS, необходимо соответствующим образом отредактировать файл appsettings.json, находящийся в корневом каталоге установленного серверного ПО (по умолчанию *Program Files/MicroEM/UEMServer*). Необходимо добавить объект "Certificate" следующим образом:

```
"Certificate": {
  "Path": "C:/путь/к/сертификату",
  "KeyPath": "C:/путь/к/ключу",
  "AllowInvalid": true
}
```

Где:

- Path - путь к сертификату в формате .pem
- KeyPath - путь к ключу в формате .pem
- AllowInvalid - переключатель, позволяющий использовать самоподписанные сертификаты. Если сертификат подписан в CA, то этот переключатель можно установить в false

Также, необходимо установить параметр «Urls» в объекте Kestrel/Endpoints/Https на https, например, *https://localhost:5142*

> **ВАЖНО!**
> Обратите внимание, что в начале url «http» поменялось на «https».

После изменения настроек необходимо перезапустить сервис (описано в разделе «Остановка и запуск сервера»).

> **ВАЖНО!**
> После установки SSL сертификата, сервер будет отвергать соединения по HTTP.

3.3.4 Использование сертификата в формате .pfx

При использовании сертификата в формате .pfx, необходимо указать настройку «Certificate» следующим образом:

```
"Certificate": {
  "Path": "C:/путь/к/сертификату",
  "Password": "пароль"
}
```

Если при создании сертификата пароль не устанавливался, его можно пропустить

Также, необходимо установить параметр «Urls» в объекте Kestrel/Endpoints/Https на https, например, *https://localhost:5142*

> **ВАЖНО!**
> Обратите внимание, что в начале url http поменялось на https.

После изменения настроек необходимо перезапустить сервис (описано в разделе «Остановка и запуск сервера»).

> **ВАЖНО!**
> После установки SSL сертификата, сервер будет отвергать соединения по HTTP.

3.3.5 Настройка разрешенных хостов

По умолчанию, сервер принимает любые соединения с любых хостов. Для изменения принимаемых хостов, необходимо отредактировать файл appsettings.json, находящийся в корневой папке установленного серверного ПО (по умолчанию *Program Files/MicroEM/UEMServer*), следующим образом:

"AllowedHosts": "имя_хоста"

Таким образом, сервер будет принимать подключения только в том случае, если обращаться к нему по *http://имя_хоста*.

Данная настройка предоставляет возможность указать имена хостов через запятую, например

"AllowedHosts": "localhost,127.0.0.1,123.123.123.123"

После изменения разрешённых хостов необходимо перезапустить сервер.

3.3.6 Настройка базы данных

База данных серверного ПО хранится локально. По умолчанию, файл базы данных называется **database.db** и находится в корневом каталоге установленного серверного ПО (по умолчанию *Program Files/MicroEM/UEMServer*).

Для изменения пути к файлу базы данных, необходимо изменить поле "DatabasePath" объекта "DatabaseSettings", например:

```
"DatabaseSettings": {
  "DatabasePath": "path/to/database.db"
},
```

Если файл базы данных не существует, то сервером будет предпринята попытка создать его, включая все каталоги и подкаталоги.

При изменении пути к файлу базы данных, старый файл сохраняется, но не переносится на новое место. Если предполагается перенос базы данных, необходимо перенести файл базы данных вручную.

После изменения пути к файлам базы данных, необходимо перезапустить сервер.

3.3.7 Удаление серверного ПО

Удаление серверного ПО производится через встроенную в ОС Windows утилиту «Установка и удаление программ»

Чтобы удалить сервер:

- Запустите приложение «Установка и удаление программ»;
- Найдите в списке UEM Server и щёлкните левой кнопкой по нему;
- Щёлкните «удалить»;
- Подтвердите удаление.

Удаление серверного ПО **не приводит** к удалению базы данных и прочих пользовательских данных, связанных с результатами использования серверного ПО. После переустановки база данных и прочие пользовательские данные будут снова доступны для использования с серверным и клиентским ПО.

3.3.8 Удаление пользовательских данных

Пользовательские данные находятся в той же папке, что и серверное ПО. Для их удаления необходимо после удаления серверного ПО вручную удалить папку установки сервера (по умолчанию *Program Files/MicroEM/UEMServer*).

3.4 Установка клиентского интерфейса

Установка клиентского ПО производится через msi файл с названием UEM Interface.msi. После его запуска пользователю будет предложено выбрать путь для установки ПО, путь по умолчанию: *Program Files/MicroEM/UEMInterface*.

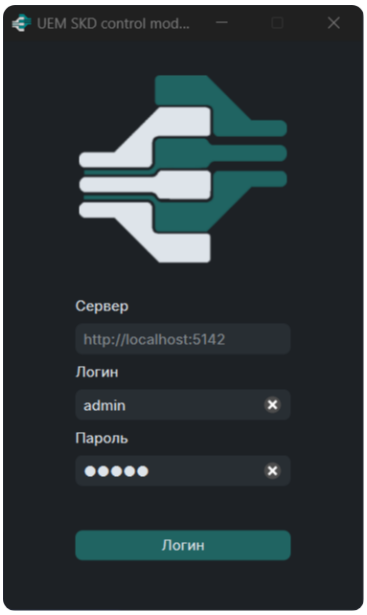
4 Подключение и конфигурация контроллера

4.1 Запуск клиентского ПО

После установки сервера и клиента, а также создания первой учетной записи для входа, пользователь может запустить клиентское приложение и авторизоваться, используя данные созданной учетной записи. Если учетная запись не была настроена заранее, используйте логин и пароль по умолчанию.

При запуске программы в окне авторизации введите данные:
- адрес сервера (по умолчанию: localhost:5142, если сервер запущен на одной машине с клиентским ПО и не изменялся в настройках сервера);

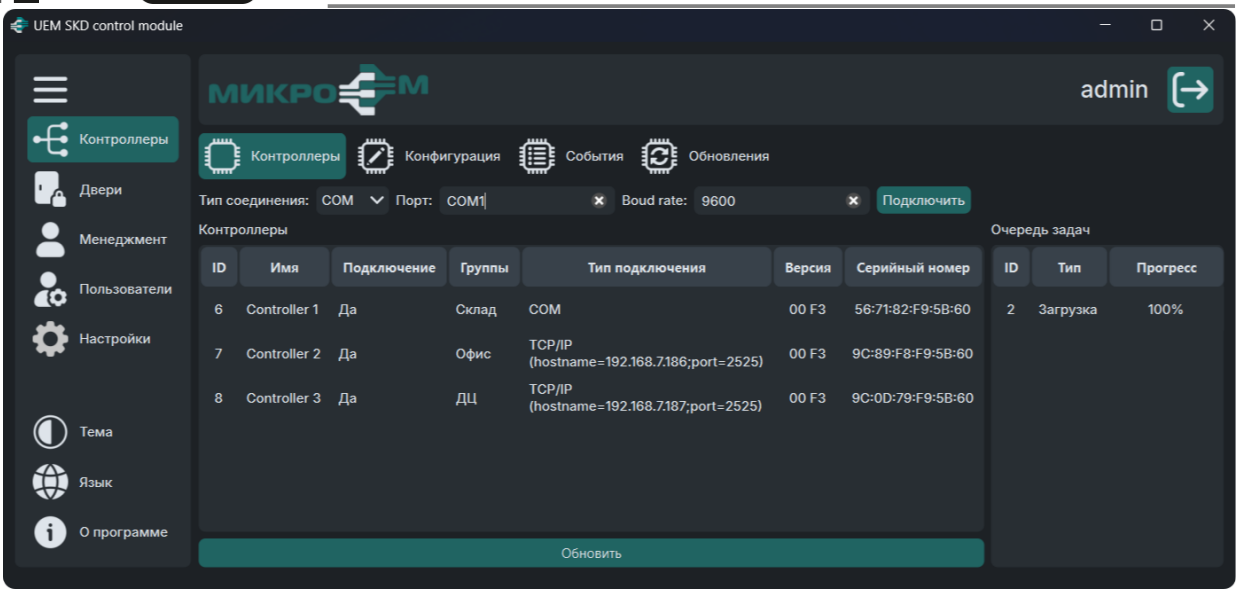
- логин и пароль (по умолчанию: admin/admin).



Окно авторизации

4.2 Подключение контроллера

Подключение и управление контроллерами осуществляется в основном окне программы в категории «Контроллеры».



Список контроллеров

Через данную вкладку доступен функционал:

- Просмотр подключенных и имеющихся на сервере контроллеров;
- Просмотр информации о контроллерах;
- Подключение, отключение и удаление контроллера из базы данных сервера;
- Загрузка и синхронизация идентификаторов из базы данных сервера с базой данных контроллера;
- Присвоение или изменение имени контроллера;
- Присвоение группы контроллеру, к которой привязаны идентификаторы для выгрузки в контроллер;
- Ручная синхронизация времени контроллера с временем операционной системы.

4.2.1 Добавление контроллера

Для добавления контроллера необходимо выбрать соответствующие параметры в верхней части окна программы. В зависимости от типа подключения, необходимые параметры будут отличаться. Контроллеры поддерживают следующие типы подключения:

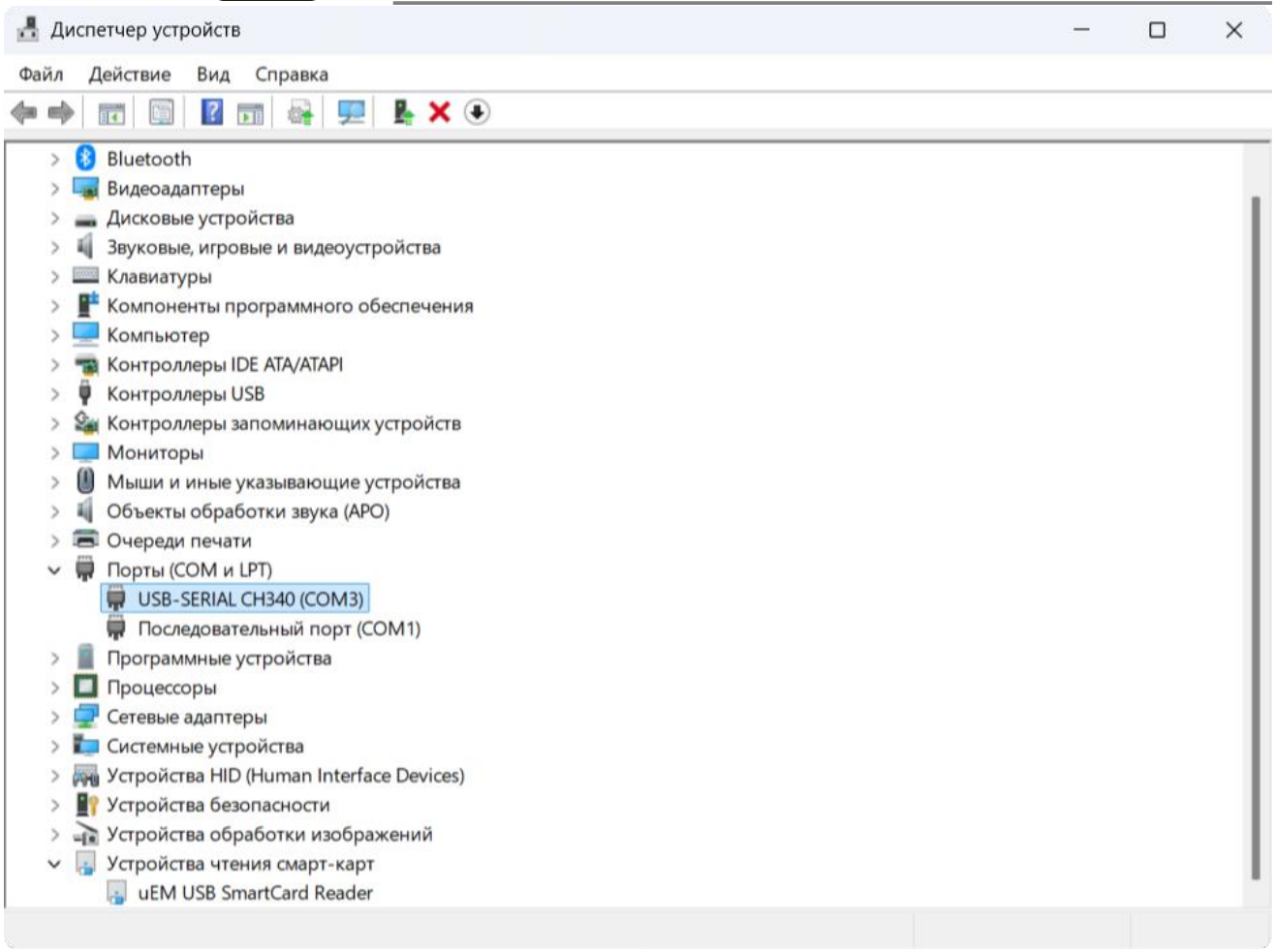
- COM-порт;
- TCP/IP;
- USB.

Подключение по COM-порту

1. Выберите «тип соединения» COM;
2. Введите имя порта (например, COM1);
3. Установите скорость «Baud Rate» соединения (например, 9600);
4. Нажмите кнопку «Подключить».

Определение номера COM-порта

Определить номер COM-порта можно в диспетчере устройств.



Диспетчер устройств

Подключение по TCP/IP

1. Выберите «тип соединения» TCP/IP;
2. Введите адрес контроллера;
3. Введите порт контроллера;
4. Нажмите кнопку «Подключить».

Подключение по USB

1. Выберите «тип соединения» USB;
2. Введите номер контроллера (поле «порт»);
3. Нажмите кнопку «Подключить».

Определение номера USB-порта

Если подключено только одно USB-устройство, его порт всегда будет номер 0. Если подключено несколько устройств, нумерация портов присваивается в порядке подключения – сначала подключенное устройство получает номер 0, следующее – 1, и так далее.

Защищенный алгоритм шифрования соединения с хостом AES-128

Для обеспечения безопасности обмена данными между контроллером и хост-системой возможно использование шифрование по алгоритму AES-128 (Advanced Encryption Standard, 128-битный ключ).

Перед установлением соединения хост и контроллер выполняют процедуру аутентификации, после чего весь обмен данными осуществляется в зашифрованном виде. Ключ шифрования задаётся при конфигурировании устройства и может быть изменён только авторизованным пользователем.

Сейчас контроллер поддерживает шифрование AES-128, где можно задать ключи и активировать шифрование через использование API (для разработчиков). В ближайшем будущем такая возможность будет добавлена в интерфейс клиентского приложения.

Проверка состояния контроллера

Подключенные контроллеры отобразятся списком во вкладке «Контроллеры» Список контроллеров содержит колонку со статусом подключения («Да» или «Нет»).

Правой кнопкой мыши по контроллеру вызывается контекстное меню, где доступны следующие действия проверки состояния:

- Получение списка событий контроллера;
- Просмотр очереди задач контроллера и действия с контроллером;

4.2.2 Отключение и удаление контроллера

Отключение контроллера

Для отключения контроллера необходимо нажать правой кнопкой мыши на подключенный контроллер во вкладке «Контроллеры» и выбрать «Отключить». В таком случае контроллер останется в списке, но будет считаться отключенным. Все связанные с ним данные в БД и на сервере останутся до последующего включения.

Удаление контроллера

Для полного удаления данных о контроллере необходимо выбрать «Удалить». В таком случае действие поведет за собой удаление всех связанных данных с этим контроллером на сервере и из БД.

4.2.3 Время и дата работы устройства

Нажмите правой кнопкой мыши по подключенному контроллеру и выберите «**Синхронизировать время контроллера с временем системы**».

При включении питания устройство начинает отсчёт системного времени, основываясь на Unix-времени (количестве секунд, прошедших с 1 января 1970 года, 00:00:00 UTC).

Если в устройстве **не установлена резервная батарея (RTC-батарея)**, то при каждом выключении питания текущее время и дата **сбрасываются** до исходного значения — **01.01.1970 00:00:00 (UTC)**.

Для сохранения точного времени при отключении основного питания рекомендуется установить батарею для часов реального времени (RTC), если она отсутствует в комплектации и не установлена с завода. В этом случае время будет сохраняться и корректно обновляться после повторного включения устройства. В зависимости от типа

установленной батареи, она может держать заряд до нескольких лет. Если батарея разрядится, то при следующем отключении контроллера от питания время и дата сбросятся.

4.3 Конфигурация контроллера

4.3.1 Автоматическая конфигурация OSDP-считывателей

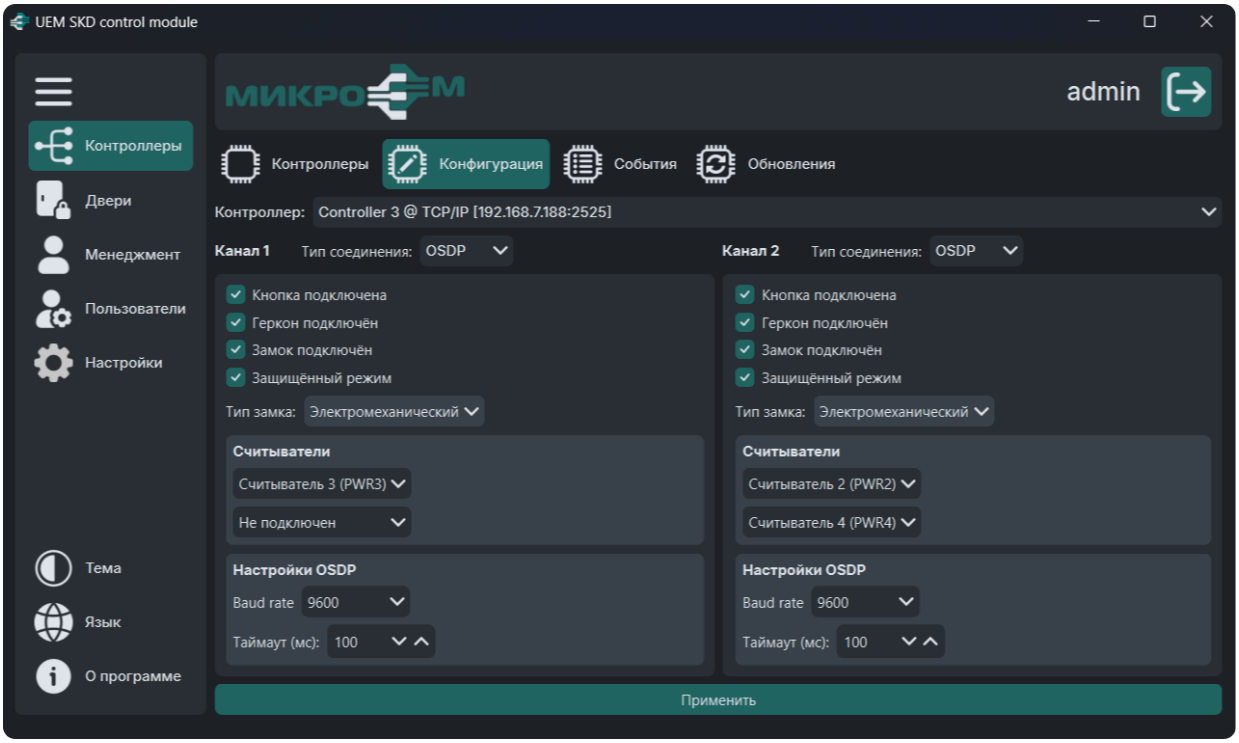
При подаче питания на контроллер, устройство автоматически предпримет попытку обнаружить подключенные OSDP-считыватели и установить с ними связь, используя ранее заданные настройки во вкладке «Конфигурация» (или настройки по умолчанию, если не заданы ранее). Считыватели автоматически получат адреса и перейдут на установленную скорость Baud rate (по умолчанию: 9600). Имейте ввиду, что если считыватели ранее были настроены с помощью стороннего софта на определенные адреса и скорость, то они будут перезаписаны. Для изменения Baud rate и Timeout, установите необходимые значения во вкладке «Конфигурация».

Корректная автоматическая настройка доступна только в случае, если считыватели подключены в соответствии с руководством «Controller-Installation-Guide», где питание каждого считывателя подключено в отдельную клемму PWRx.

Рекомендуется подключать питание считывателей в соответствии с инструкцией, даже если автоматическая конфигурация не требуется.

4.3.2 Ручная конфигурация контроллера

Во вкладке «Конфигурация» необходимо осуществить настройку контроллера и выбрать необходимые опции.



Конфигурация

Вкладка «Конфигурация» представляет собой настройку каналов контроллера.

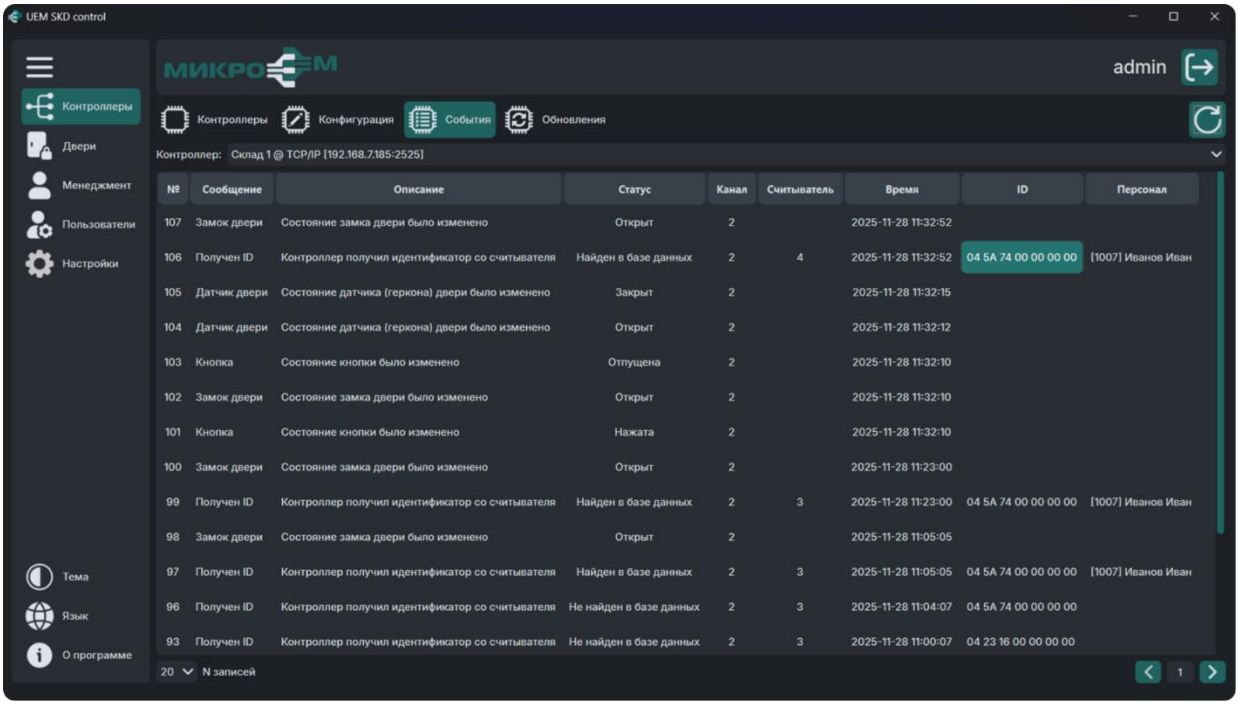
Настройка контроллеров:

- Настройка контроллера по 2 каналам;
- Выбор типа соединения (OSDP, Wiegand, 1-Wire);
- Опция «Кнопка подключена»;
- Опция «Геркон подключен»;
- Опция «Замок подключен»;
- Выбор типа замка.
- Настройка защищенного подключения OSDP;
    - Настройка значения «Baud Rate»;
    - Настройка значения «Timeout».
- Выбор подключенных считывателей и их привязка к каналам.
- Опция «Защищённый режим» OSDP-соединения.

4.4 События контроллера

Во вкладке «События» отображаются события контроллера, которые содержат информацию:

- Сообщение события
- Описание события
- Время
- Канал
- Считыватель
- Статус
- Raw ID
- Персонал, которому принадлежит событие



События

В столбце «Канал» отображается номер канала на котором сработало событие.
В столбце «Считыватель» отображается номер считывателя на котором сработало событие.
В столбце «Время» отображается точное время, когда было выполнено событие.
В столбце «ID» отображается уникальный идентификатор, который был получен со считывателя. Скопировать идентификатор можно с помощью сочетаний клавиш Ctrl+C предварительно выделив нужную ячейку с содержимым.
В столбце «Персонал» отображается ID и имя персонала, который вызвал событие.

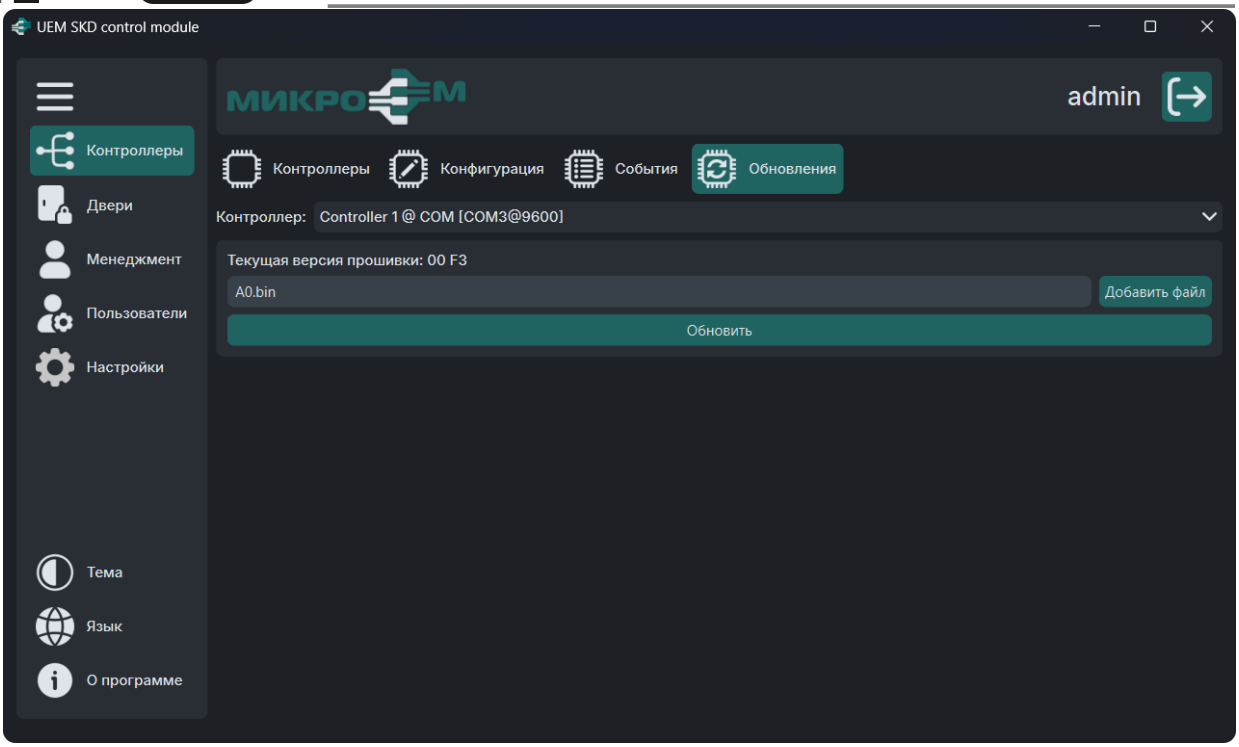
Список возможных событий:

№	Сообщение	Описание	Статус
1	Получен ID	Контроллер получил идентификатор со считывателя	Найден в базе данных/ Не найден в базе данных
2	Кнопка	Состояние кнопки было изменено	Нажата/Отпущена
3	Замок двери	Состояние замка двери было изменено	Открыт/Закрыт
4	Датчик двери	Состояние датчика (геркона) двери было изменено	Открыт/Закрыт
5	Вскрытие корпуса	Изменение статуса датчика вскрытия корпуса	Вскрыт/Закрыт
6	Охранная сигнализация	Изменение статуса состояния сенсора охранной сигнализации	Включен режим тревоги/ Выключен режим тревоги
7	Пожарная сигнализация	Изменение статуса состояния сенсора пожарной сигнализации	Включен режим тревоги/ Выключен режим тревоги
8	Питание считывателя	Возникло короткое замыкание в цепи питания считывателей	Считыватель выключен
9	Экстренное открытие дверей	Изменение состояния режима экстренного открытия дверей	Включен/Выключен
10	Питание	Обнаружен источник питания	Питания от батареи/ Внешний источник питания

4.5 Обновление контроллера

Во вкладке «Обновление» доступна возможность обновления прошивки для каждого контроллера.

Для обновления контроллера выберите контроллер, программное обеспечение которого необходимо обновить, затем нажмите «Добавить файл» и выберите файл с расширением .bin заранее скачанный с сайта производителя и нажмите кнопку «Обновить». Обновление контроллера займет какое-то время. Статус процесса можно наблюдать в «Контроллеры» > «Контроллеры» > «Очередь задач». Чтобы отобразить очередь задач для контроллера, необходимо вызвать контекстное меню нажав правой кнопкой мыши по нужному контроллеру и выбрать пункт «Получить очередь задач контроллера».

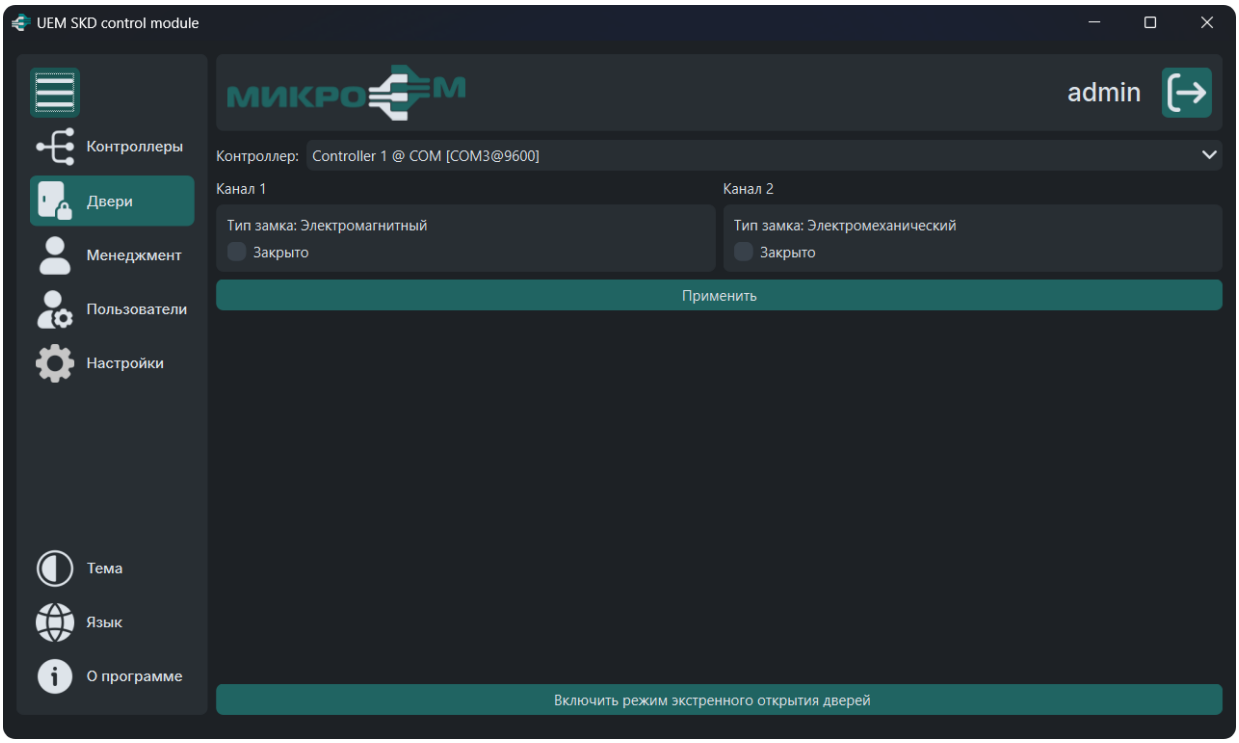


Обновление прошивки контроллера

5 Работа с контроллером

5.1 Управление замками

ПО позволяет напрямую управлять замками двери. Управление производится из категории «Двери».



Управление замками

5.1.1 Открытие и закрытие замков

Для того, чтобы открыть или закрыть замок:

- Откройте категорию «Двери»
- Выберите из выпадающего списка соответствующий контроллер
- Установите необходимое состояние замков при помощи чек-боксов первого и второго каналов
- Нажмите кнопку «применить»

5.1.2 Специфика открытия замков разного типа

В зависимости от типа установленного замка, который следует указать при конфигурации, логика открытия замка будет отличаться: если указан ***электромагнитный*** замок, то в закрытом состоянии на замок подано питание, а при открытии (установить галочку на «Закрыто» и нажать «Применить») питания с замка будет снято до тех пор, пока не будут проделаны обратные действия (снять галочку с «Закрыто» и нажать «Применить»; если выбран ***электромеханический*** замок, то в закрытом состоянии у замка будет снято питание, а при открытии (установить галочку на «Закрыто» и нажать «Применить») будет подано питание на 0.9 секунд, что спровоцирует открытие защелки. Далее состояние замка в данной вкладке сменится на «Закрыто».

Если на двери установлены герконы (датчики двери) и выбраны при конфигурации, то на данной вкладке будут отображаться также статусы состояния дверей помимо статуса замков.

5.1.3 Режим экстренного открытия дверей

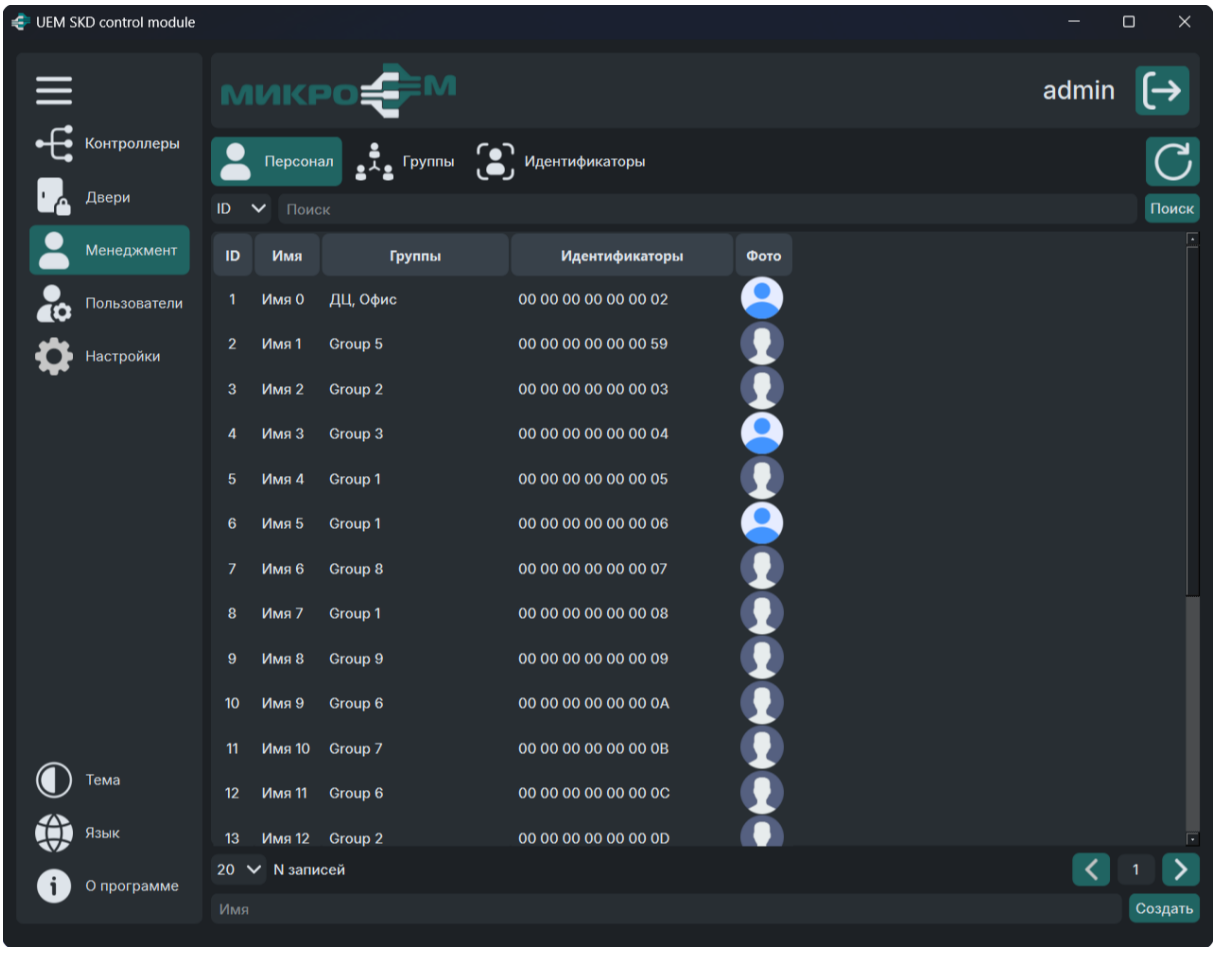
Для экстренного открытия замка:

- Откройте категорию «Двери»
- Выберите из выпадающего списка соответствующий контроллер
- Нажмите кнопку «Экстренно открыть двери на этом считывателе»

При нажатии на кнопку «Экстренно открыть двери» выбранный контроллер перейдет в режим экстренного открытия замков, снимет питание со всех электромагнитных замков и будет периодически подавать питание на 0.9 секунд на все электромеханические замки. Чтобы отменить режим экстренного открытия замков, необходимо еще раз нажать кнопку «Экстренное открытие дверей»

5.2 База данных персонала и идентификаторов

Управление персоналом осуществляется во вкладке «Персонал» в категории «Менеджмент».



Управление персоналом

Персонал - это сотрудники организации, для которых в системе создаются учетные записи доступа. Каждому пользователю может быть присвоено имя, группа, уникальный идентификатор и фотография.

Персонал обладает индивидуальными правами доступа к объектам и зонам, определенным через группы.

Для того, чтобы загружать базу данных идентификаторов в контроллер, необходимо проделать следующие действия:

- Добавить 7-байтовый идентификатор карты во вкладке «Менеджмент» - > «Идентификаторы». После этого они попадают в категорию свободных идентификаторов (которые никому еще не присвоены). Затем при создании персонала, можно будет присвоить один из свободных идентификаторов из списка выбранному человеку.
- Создать запись человека и добавить данные о нем (ФИО) во вкладке «Менеджмент» - > «Персонал».
- Присвоить человеку из персонала идентификатор из списка свободных.
- Создать группу для персонала. С помощью групп можно управлять идентификаторами персонала и далее присваивать группу определенным контроллерам для доступа ко входу. Идентификаторы персонала.
- Присвоить одну или несколько групп выбранному контроллеру и загрузить базу в контроллер. Все идентификаторы персонала, которые находятся в группах, которые выбраны для контроллера будут загружены в базу данных контролера и смогут с помощью своих пропусков с этими идентификаторами открывать замки выбранного контроллера и осуществлять вход.

5.3 Управление персоналом

5.3.1 Создание персонала

Для создания персонала необходимо ввести имя персонала в соответствующее поле вкладки «Персонал» и нажать кнопку «Создать». Дополнительных действий не требуется.

5.3.2 Удаление персонала

Для удаления персонала необходимо ввести ID персонала в соответствующее поле и нажать кнопку «Удалить».

5.3.3 Назначение группы персоналу

Для назначения персоналу группы или групп, необходимо сначала найти соответствующую запись в таблице персонала. Далее, необходимо дважды щёлкнуть левой кнопкой мыши по полю «Группы» и выбрать необходимые группы.

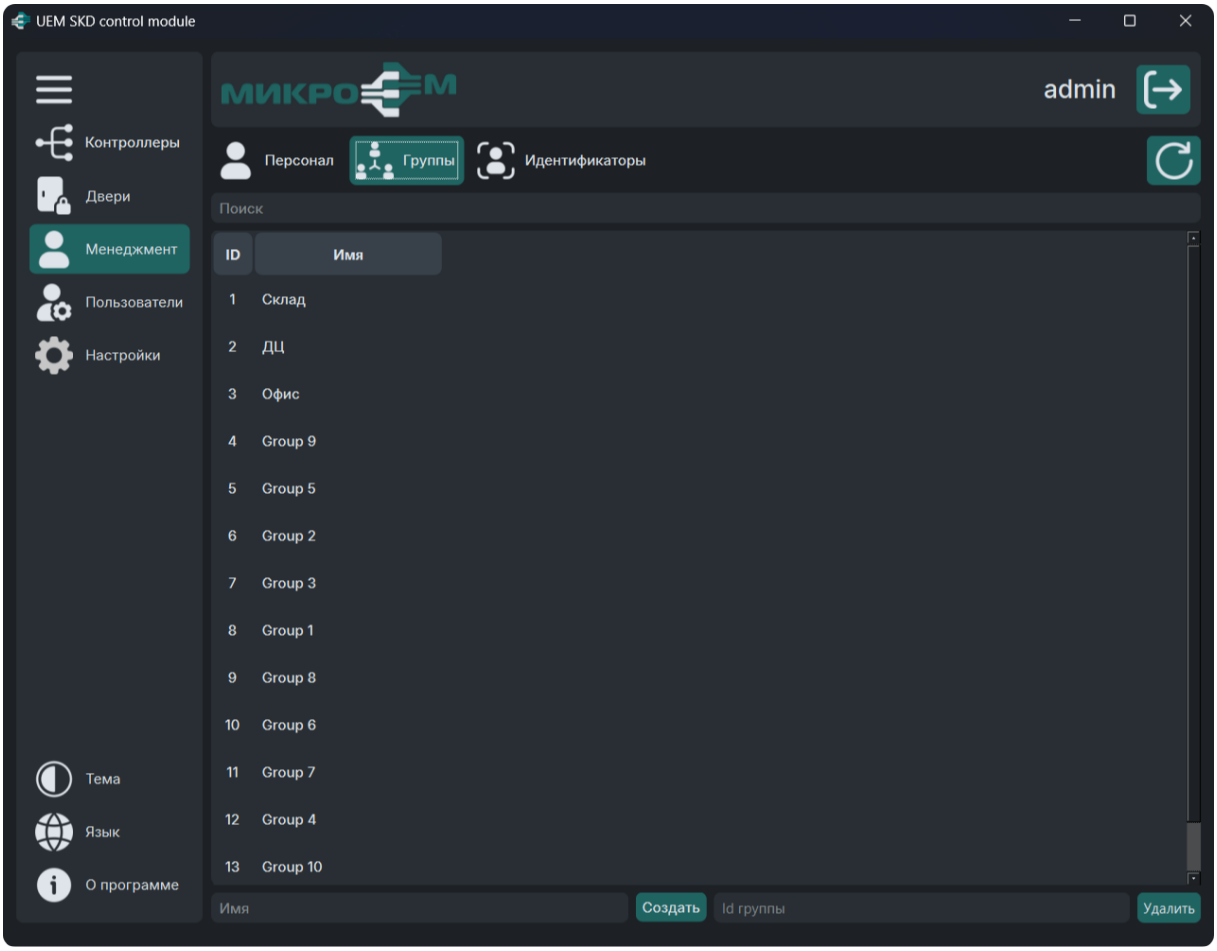
5.3.4 Назначение идентификаторов персоналу

Для назначения персоналу идентификатора или идентификаторов, необходимо сначала найти соответствующую запись в таблице персонала. Далее, необходимо дважды щёлкнуть левой кнопкой мыши по полю «Идентификаторы» и отметить необходимые.

5.4 Управление группами

Управление персоналом осуществляется во вкладке «Группы» в категории «Менеджмент».

Группы – это наборы правил, определяющих, какие сотрудники (персонал) могут получать доступ к определенным зонам, дверям или устройствам. Группы используются для централизованного управления правами доступа.



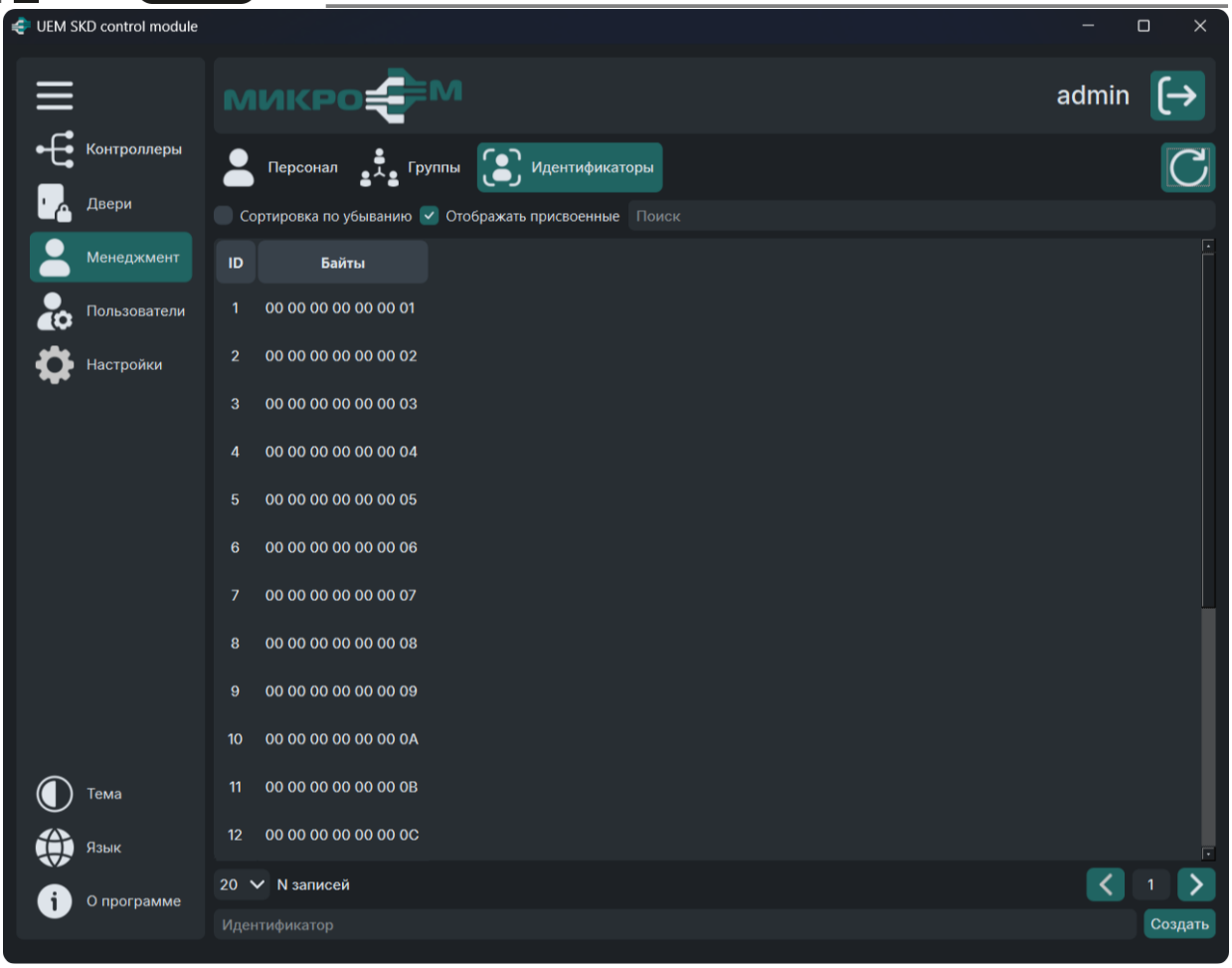
Управление группами

5.4.1 Создание группы

Для создания группы персонала, необходимо ввести имя новой группы в соответствующее поле на вкладке «Группы», после чего нажать кнопку «Создать».

5.5 Управление идентификаторами

Управление идентификаторами осуществляется во вкладке «Идентификаторы» в категории «Менеджмент».



Управление идентификаторами

5.5.1 Создание идентификатора

Для создания идентификатора необходимо ввести 7 байтов идентификатора в шестнадцатеричном формате.

Пример: «AB CD EF AB CD EF 10»

5.5.2 Удаление идентификатора

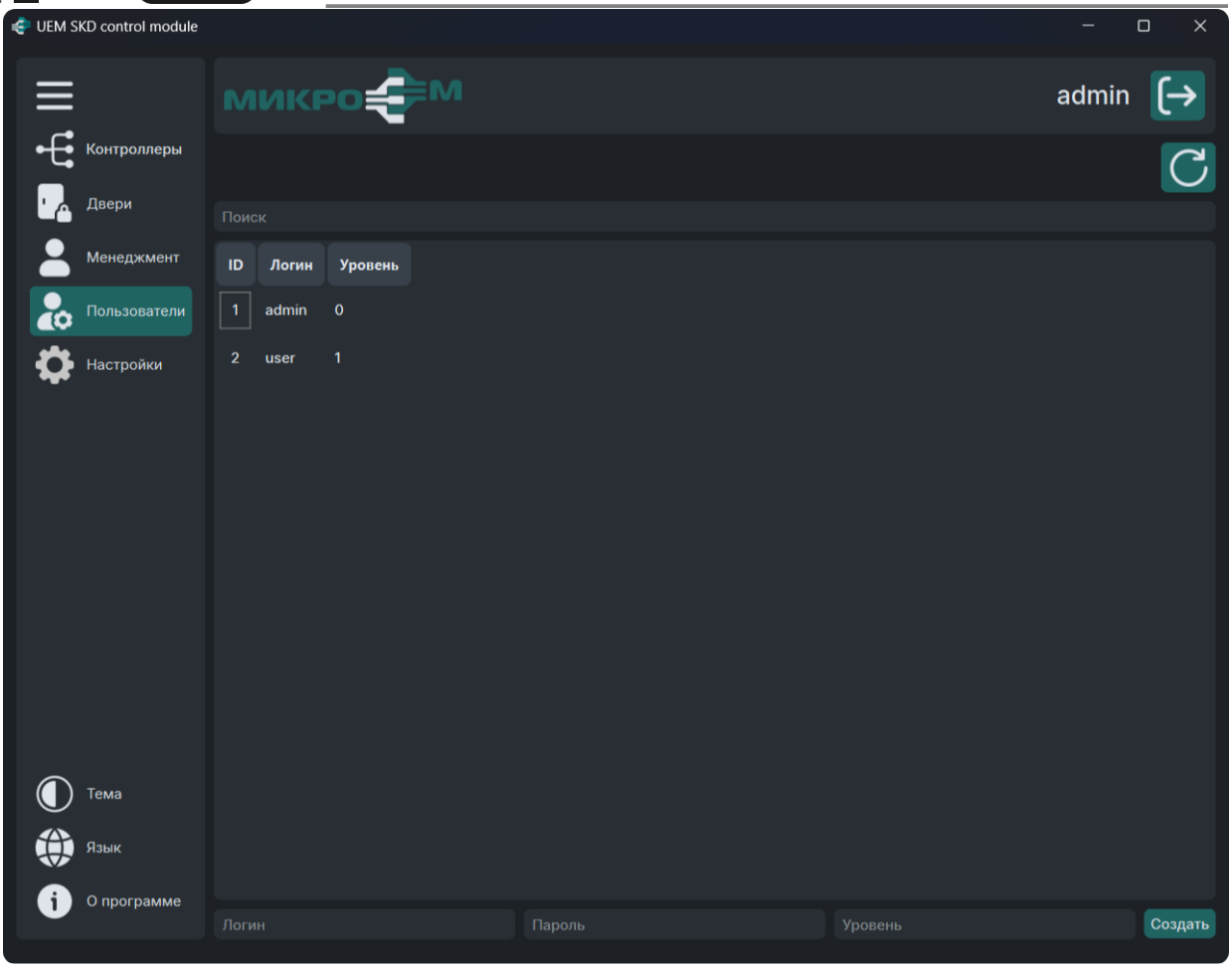
Для удаления идентификатора необходимо нажать правую кнопку мыши на идентификатор, затем «Удалить».

5.6 Управление учетными записями пользователя системы

Управление учетными записями осуществляется в категории «Пользователи».

Пользователи – это лица, имеющие доступ к клиентскому приложению для администрирования системы. Они управляют контроллерами, устройствами, персоналом, уровнями доступа и другими параметрами системы.

Данное окно доступно для просмотра и управления только пользователям системы с правами супер-админ (уровень 0) и админ (уровень 1).



Управление учетными записями пользователей

Пользователи разделены по уровню доступа. Чем меньше уровень доступа, тем больше прав доступа у пользователя.

Уровень доступа «0» - это уровень с максимальными доступами. Такая учетная запись может создавать и управлять другими учетными записями.

Уровень доступа «1» - это базовый уровень доступа. Учетная запись не имеет прав создавать и управлять другими учетными записями.

Уровень доступа «2» - это уровень доступа пользователя без прав администратора. Учетная запись не имеет прав управлять другими учетными записями и настройками сервера в WebAdmin.