Руководство пользователя

Программное обеспечение ЭНТ Контроль доступа

ПОДТВЕРЖДЕНИЕ ДОСТУПА

Сделано в России

Редакция от 27.04.2024 г.

Оглавление

Введение.

Программа «ЭНТ Контроль Доступа — Подтверждение доступа» представляет собой специализированное программное обеспечение, которое позволяет реализовать нестандартное решение для системы контроля и управления доступом (СКУД). После установки эта программа работает как служба в фоновом режиме и запускается вместе с операционной системой Windows по умолчанию. Она функционирует в комплексе с другими программами серии «ЭНТ Контроль Доступа», такими как «Клиент» и «Сервер».

Программа поддерживает сетевые контроллеры серии ЭРА v2 и не совместима с контроллерами других производителей.

Условные обозначения, принятые в руководстве.

- этим знаком будут помечены крайне важные предложения. Не соблюдений правил и условий абзацев, помеченных данным знаком, приведет к неработоспособности системы.

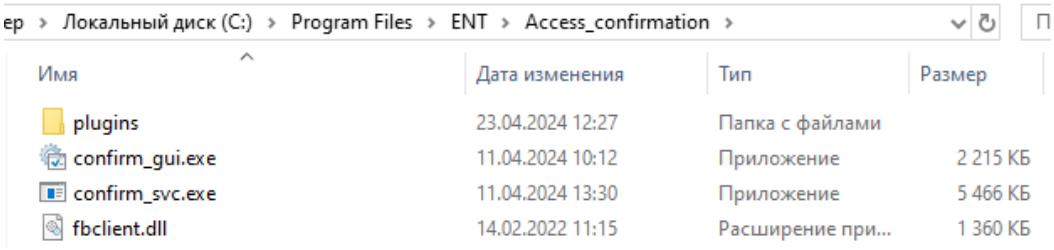
- абзацы, выделенные данным знаком, составляют важную информацию о системе, которая облегчит работу с ней.

- справочная информация, разъясняющая некоторые понятия системы.

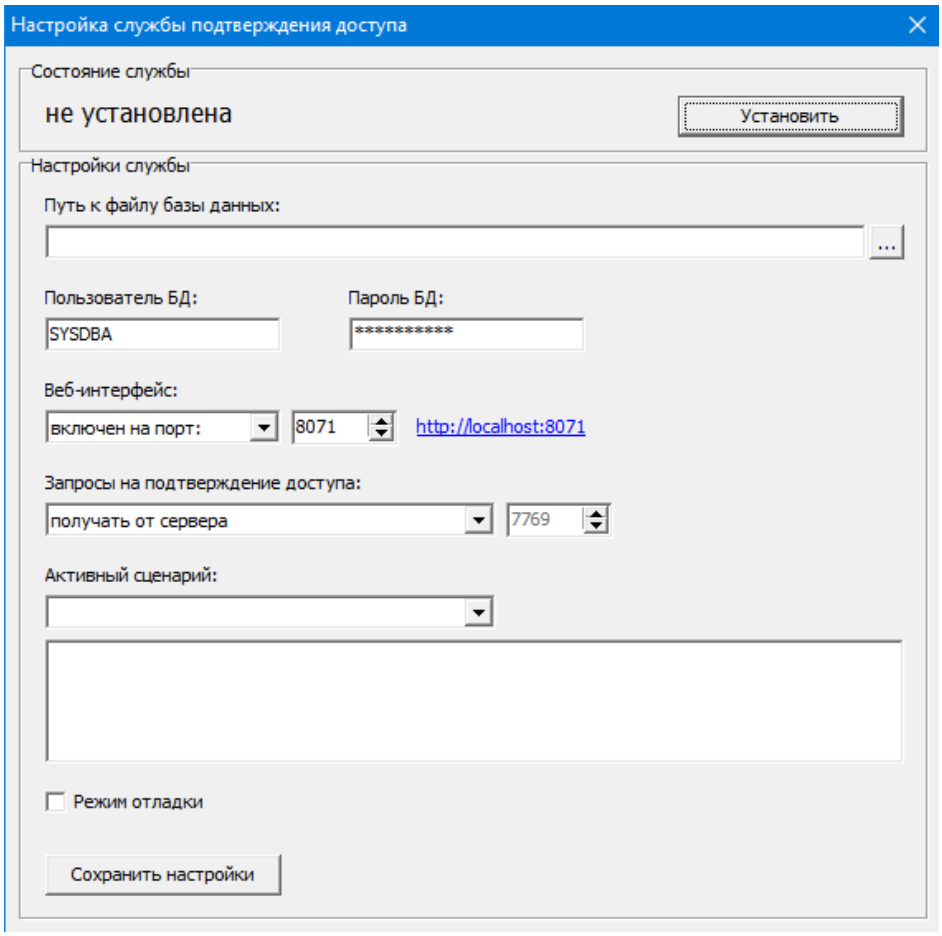
Работа с программой «Подтверждение доступа».

Установка.

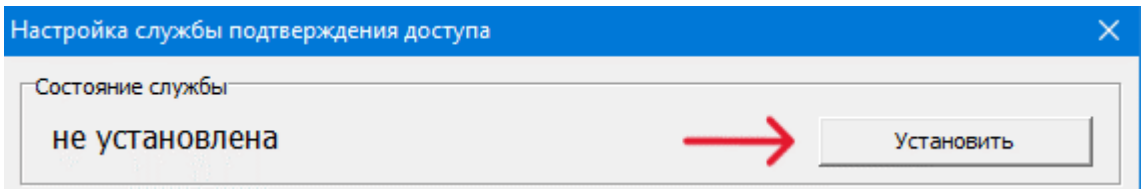
Распакуйте папку Access_confimation из архива в папку ENT.



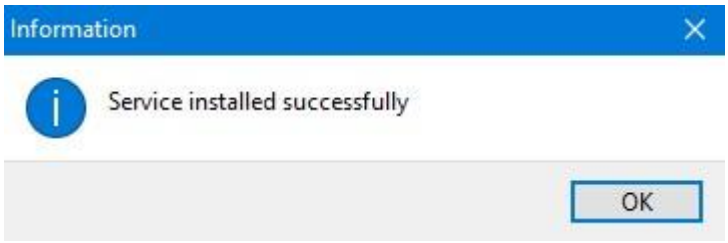
Для удобства использования программы, мы создали графический интерфейс. Чтобы его открыть, щелкните правой кнопкой мыши на файле confirm_gui.exe и выберите пункт «Запуск от имени администратора».



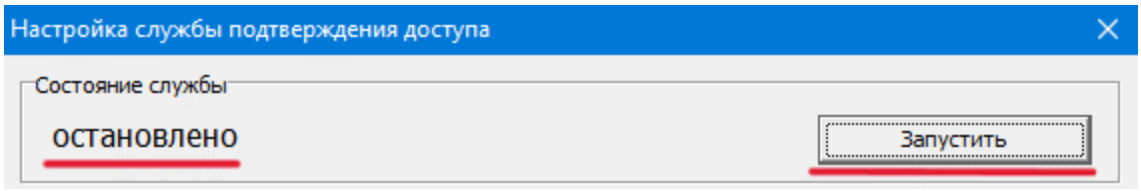
Для установки службы нажмите кнопку «Установить».



После успешной установки появится информационное окно с подтверждением:

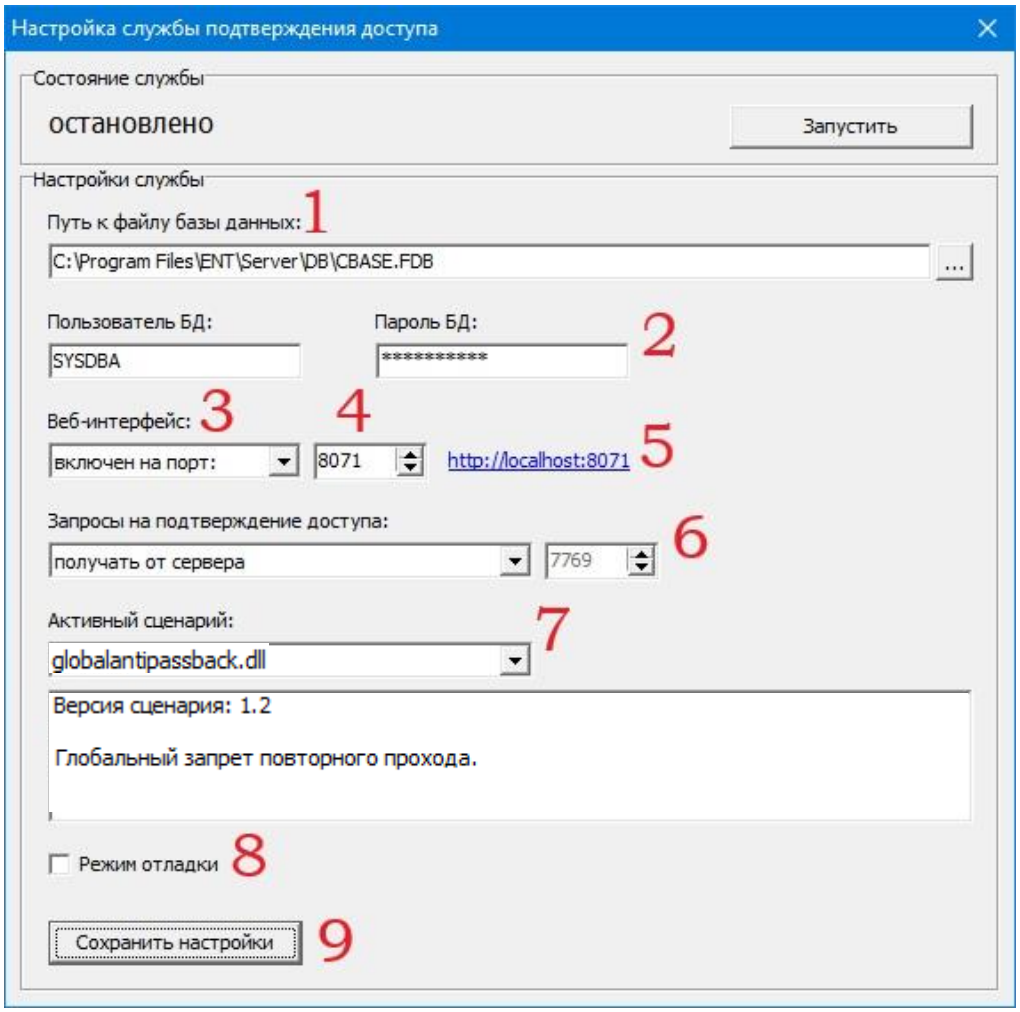


Нажмите «OK». Служба установлена. Состояние службы при этом измениться на «остановлено», а кнопка «Установить» на «Запустить».



Настройка.

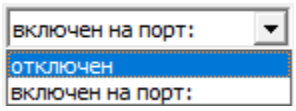
Перед запуском необходимо отредактировать параметры службы.



1. Путь к файлу базы данных. Укажите путь до файла CBASE.FDB, расположенный в папке …\ENT\Server\DB.

2. Пользователь БД и **пароль БД.** По умолчанию в СУБД Firebird: SYSDBA и masterkey соответственно.

3. **Веб-интерфейс**. Включите или отключите веб-интерфейс службы, выбрав соответствующий параметр. *Подробнее см. раздел «Веб-интерфейс».*



4. При выборе значения «включен на порт», укажите порт для взаимодействия с веб-интерфейсом службы. По умолчанию используется порт 8071.

5. Ссылка для открытия страницы веб-интерфейса.

6. Запросы на подтверждение доступа. Выберите, откуда программа будет получать запросы.

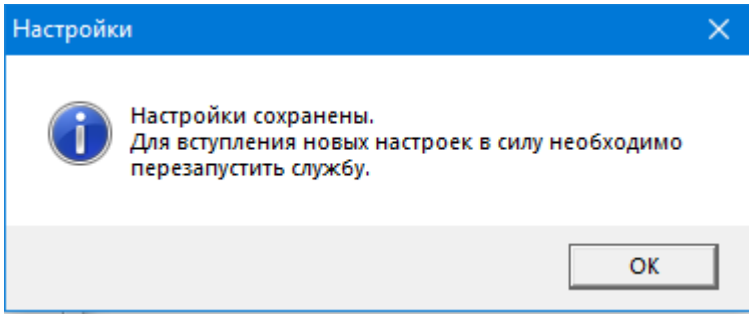
При выборе значения «получать от контроллеров на указанный порт», укажите порт для подключения, например, по порту 7769, который используется по умолчанию.

7. **Активный сценарий**. Выберите необходимый сценарий. При выборе сценария отображается его описание и принцип работы.

8. Режим отладки. Установите флажок для отображения дополнительной информации в файле с логами *confirm_svc.log*, который будет создан при запуске службы и появится в папке с файлами службы.

9. После ввода параметров необходимо их сохранить. Для этого нажмите кнопку «Сохранить настройки».

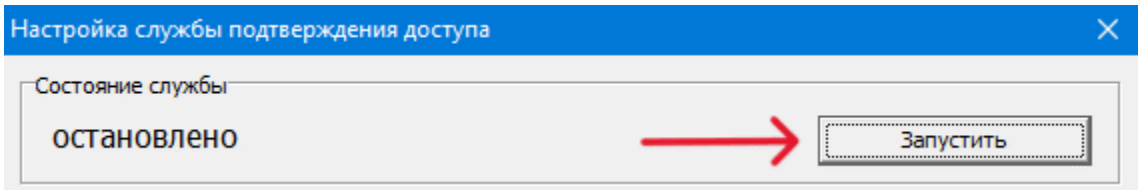
Появится информационное окно. Нажмите «ОК».



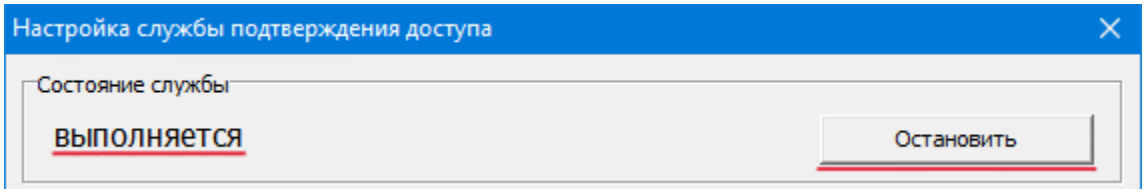
В папке с файлами службы появится конфигурационный файл *settings.ini*.

Запуск/остановка.

Для запуска службы можно использовать её графический интерфейс. Для этого щелкните правой кнопкой мыши на файле confirm_gui.exe и выберите пункт «Запуск от имени администратора». Откроется окно «Настройка службы подтверждения доступа». Нажмите кнопку «Запустить».



После запуска состояние службы измениться на «выполняется», а кнопка «Запустить» на «Остановить».



Для остановки службы нажмите «Остановить».

Окно для настройки службы можно закрыть. Служба будет работать в фоновом режиме и по умолчанию запускаться вместе с ОС Windows.

При изменении параметров службы и вступлении их в силу, необходимо перезапустить работу службы.

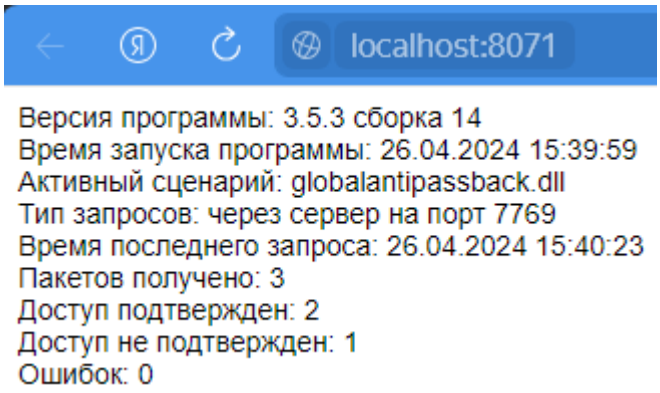
Программа не работает одновременно с аппаратной функцией запрета повторного прохода (Antipassback). Доступна на контроллерах ЭРА-2000/10000 v2, ЭРА-60000 v2, Эра-2000 GSM, Эра-10000M.

Сценарий.

Файлы сценариев хранятся в папке *plugins* с файлами службы. По умолчанию, доступно три сценария подтверждения доступа. При выборе соответствующего сценария отображается его описание и принцип работы.

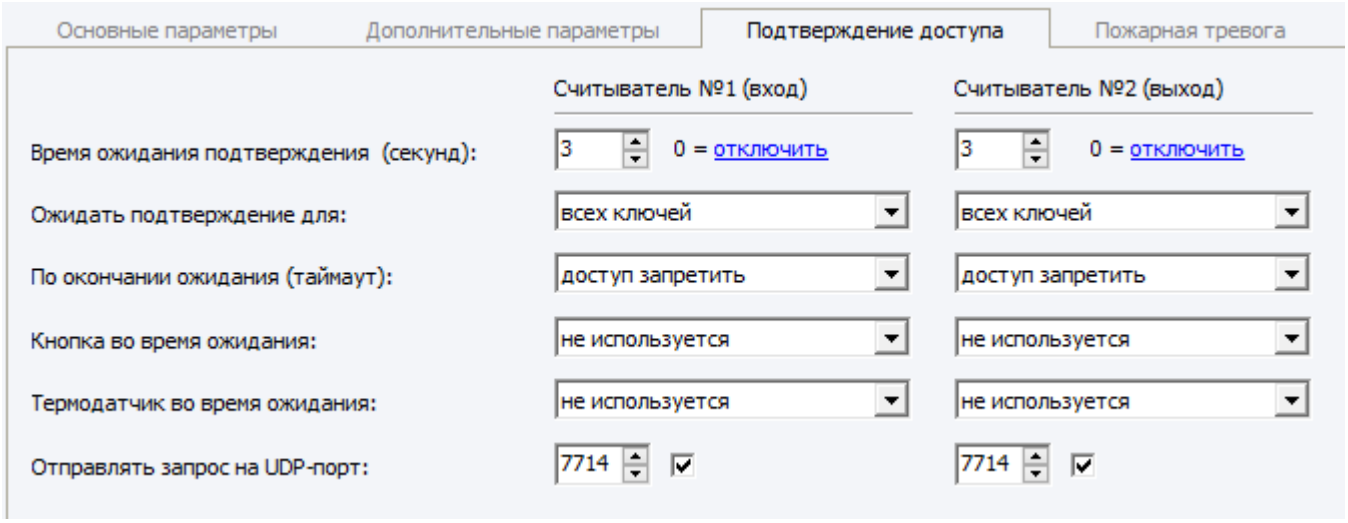
Веб-интерфейс.

В веб-интерфейсе отображается системная информация.



- **Версия программы.**
- **Время запуска программы Подтверждение доступа.**
- **Активный сценарий.**
- **Тип запросов.**
- **Время последнего запроса.**
- **Пакетов получено.** Количество запросов на подтверждение доступа, полученные программой.
- **Доступ подтвержден**. Количество успешных подтверждений прохода.
- **Доступ не подтвержден**. Количество отказов в доступе по определенным причинам, указанным в алгоритме сценария.
- **Ошибок**. Количество ошибок в результате работы алгоритма.

Настройки в программе «ЭНТ Контроль доступа – Клиент».

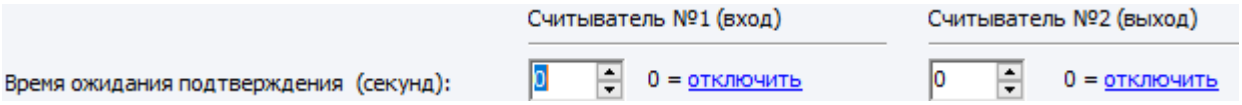


В программе «Клиент» в конфигурации контроллера необходимо активировать подтверждение доступа. Для этого выберите пункт «Конфигурация»> «Устройства». В таблице добавленных контроллеров выберите контроллер, настройки которого хотите изменить. Откройте

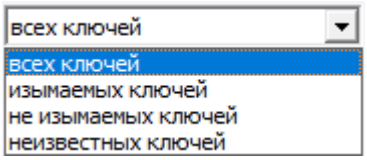
закладку «Изменить/удалить выбранный контроллер»> «Подтверждение доступа» и в параметрах ниже укажите необходимые значения.

Время ожидания подтверждения. Укажите время в секундах для необходимого считывателя (направления прохода), ожидающего управляющей команды. По истечении заданного времени, если команда не будет получена, контроллер самостоятельно примет решение в соответствии с пунктом "**По окончании ожидания**".

Для отключения подтверждения доступа укажите значение времени ожидания подтверждения – 0 или нажмите «отключить».



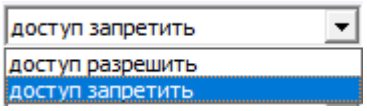
Ожидать подтверждения для. Выберите для каких ключей использовать функцию подтверждения доступа. Остальные ключи будут работать по стандартному сценарию.



- *«всех ключей» - для типа ключа «обычный» и «гостевой».*
- *«изымаемых ключей» - только для типа «гостевой ключ».*
- *«не изымаемых ключей» - только для типа «обычный ключ».*
- *«неизвестных ключей» - только для «неизвестных ключей».*

Тип ключа выбирается при добавлении в программу «Клиент» (см. Руководство пользователя ПО «ЭНТ Контроль доступа – Клиент»> раздел «Ключи»).

По окончании ожидания (таймаут). Если программа по каким-либо причинам не приняла решения о подтверждении доступа за указанное время в параметре «**Время ожидания подтверждения**» контроллер самостоятельно примет решение в соответствии с выбранным значением.



- *«Доступ запретить» - контроллер запретит доступ.*
- *«Доступ разрешить» - контроллер разрешит доступ.*

Кнопка во время ожидания подтверждения. Выберите «*не используется*».

Термодатчик во время ожидания. Выберите «*не используется*».

Отправлять запрос на UDP-порт. Данный параметр необходимо активировать и указать UDP-порт, куда будут отправляться запросы для подтверждения доступа.

Для работы через «Сервер» указать UDP-порт 7714.

Чтобы работать напрямую от контроллера, необходимо указать тот же порт, который указан в параметре ПО «ЭНТ Контроль доступа – Подтверждение доступа»> «**Запросы на подтверждение доступа**» если выбрано значении «*получать от контроллеров на указанный порт*». Например, порт 7769, который используется по умолчанию.

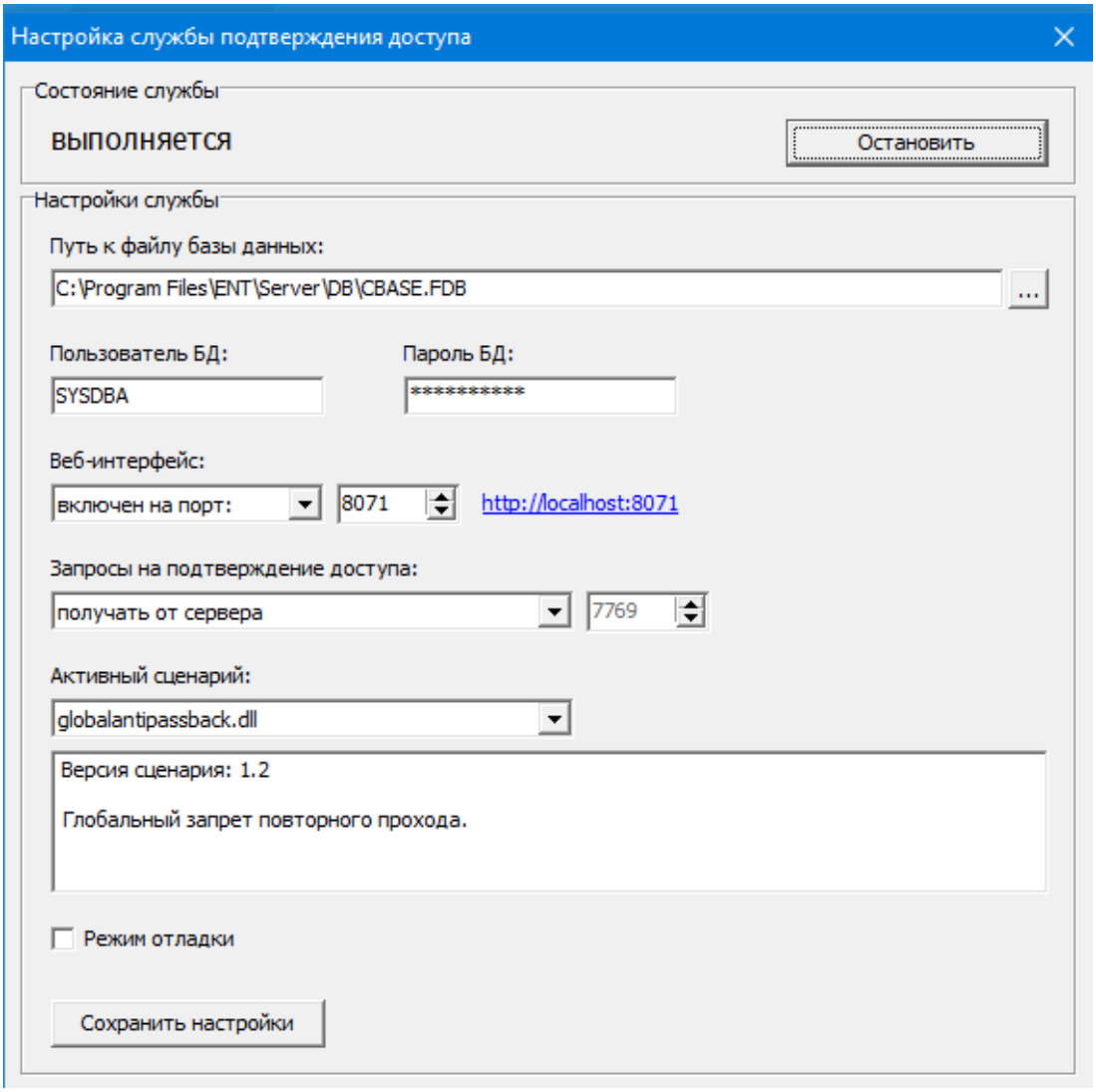
После ввода параметров для их применения, нажмите на кнопку «Изменить».

Указанный для запросов UDP-порт необходимо добавить в правило для входящих подключений брандмауэра Защитника Windows, программы-антивирусы (если установлены), настраиваемые коммутаторы (switch) или маршрутизаторы (если присутствуют в сети). Подробности по настройке стороннего программного обеспечения и/или оборудования смотрите в соответствующих руководствах производителя или обратитесь к системному администратору.

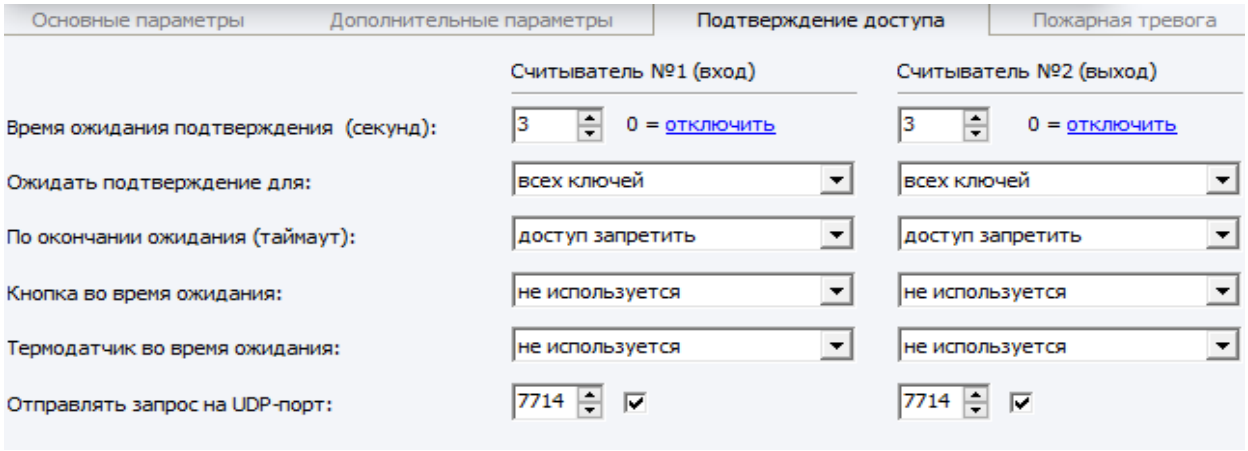
Примеры настроек в ПО «ЭНТ Контроль доступа».

Для работы через «Сервер».

Настройки в ПО «Подтверждение доступа»:

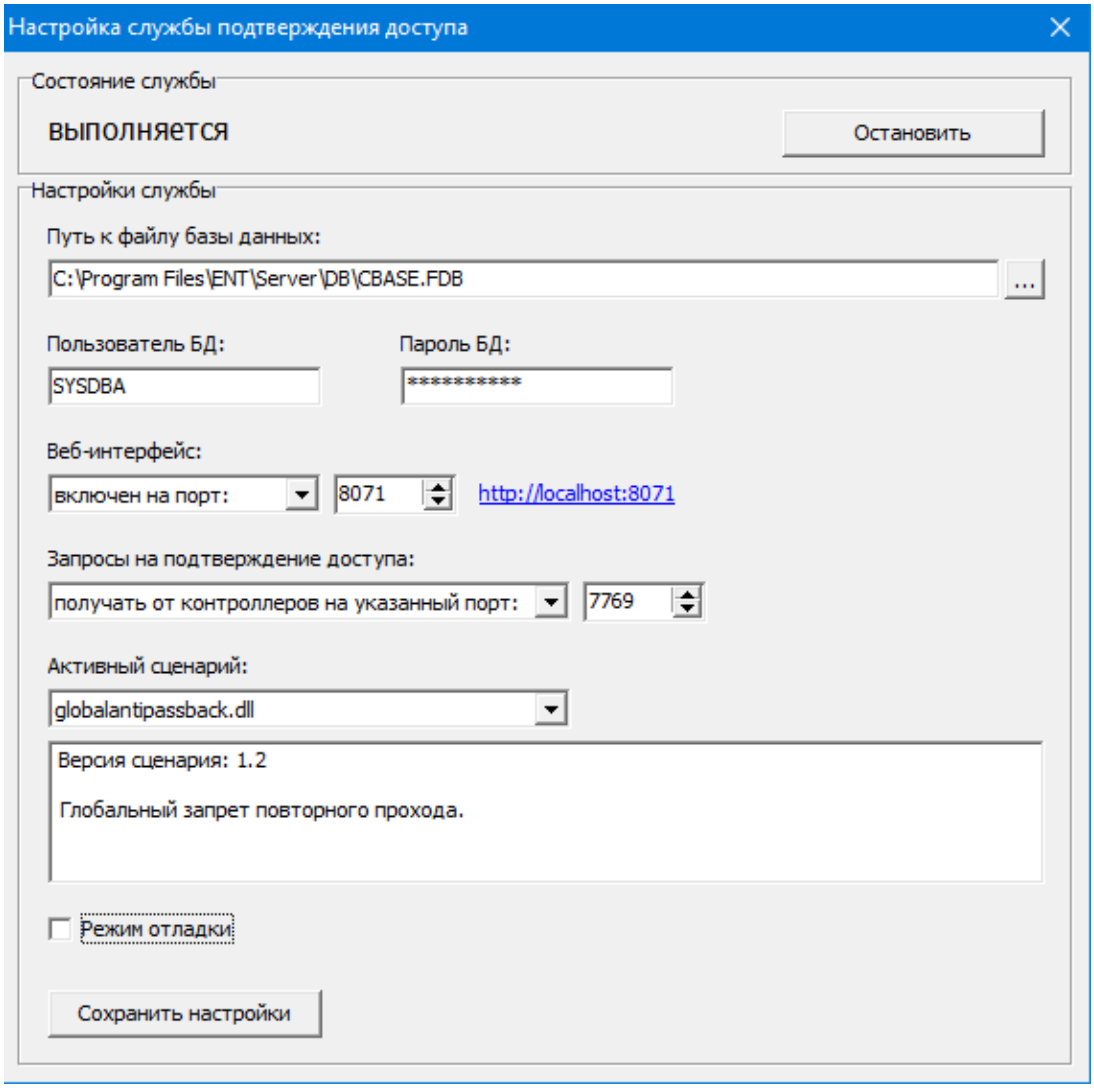


Настройки в ПО «Клиент»:



Для работы напрямую от контроллеров.

Настройки в ПО «Подтверждение доступа»:



Настройки в ПО «Клиент»: