



INFOWATCH ARMA INDUSTRIAL ENDPOINT



Руководство пользователя по эксплуатации

версия 8 ред. от 25.01.2021

Листов 25

СОДЕРЖАНИЕ

Аннотация.....	3
1 Назначение программы	4
2 Начало работы с ARMA Industrial Endpoint	5
2.1 Настройка сервиса с ОС Windows	5
2.1.1 Создание пользователя с ограниченными правами.....	5
2.2 Настройка связи с ARMA Management Console.....	7
2.3 Установка сервиса	8
2.4 Запуск сервиса	11
2.5 Добавление и настройка Endpoint в ARMA Management Console	12
3 Управление белым списком программ	15
4 Управление контролем целостности	17
5 Управление контролем устройств	19
6 Настройка синхронизации с ARMA Management Console	22
7 Дополнительные настройки.....	23
7.1 Информация о состоянии и лицензии Endpoint.....	23
7.2 Настройка подключения и управления ARMA Industrial Endpoint	23
7.2.1 Режим обучения.....	23
7.3 Настройка сетевого журнала	24
7.4 Настройка журналирования.....	24
8 Просмотр журнала событий в файле Endpoint.log	25

АННОТАЦИЯ

Настоящее руководство пользователя по эксплуатации предназначено для технических специалистов и пользователей, которые выполняют конфигурирование и мониторинг работы InfoWatch ARMA Industrial Endpoint версии 1.0.0.

Руководство пользователя по эксплуатации содержит описание консольного интерфейса, доступных функций с подробным описанием их настройки и использования, а также принципов работы с InfoWatch ARMA Industrial Endpoint.

Перед эксплуатацией InfoWatch ARMA Industrial Endpoint пользователю необходимо изучить настоящее руководство.

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

InfoWatch ARMA Industrial Endpoint представляет собой системный сервис с графическим интерфейсом пользователя. Управление программой возможно локально или посредством InfoWatch ARMA Management Console .

InfoWatch ARMA Industrial Endpoint предназначен для решения следующих задач:

- контроль целостности программного обеспечения;
- ограничение перечня исполняемых программ;
- ограничение подключаемых съемных носителей;
- отправка событий безопасности в централизованную консоль управления.

2 НАЧАЛО РАБОТЫ С ARMA INDUSTRIAL ENDPOINT

2.1 Настройка сервиса с ОС Windows

Для работы программы необходимо предварительно разделить права пользователей в ОС. Для обычных пользователей не рекомендуется предоставлять права администратора.

2.1.1 Создание пользователя с ограниченными правами

От имени администратора необходимо создать пользователя с ограниченными правами. Для этого следует перейти в «Управление компьютером», выбрать «Локальные пользователи и группы», щелкнуть правой кнопкой мыши по пункту «Пользователи» и в контекстном меню выбрать пункт «Новый пользователь...» (Рисунок 1).

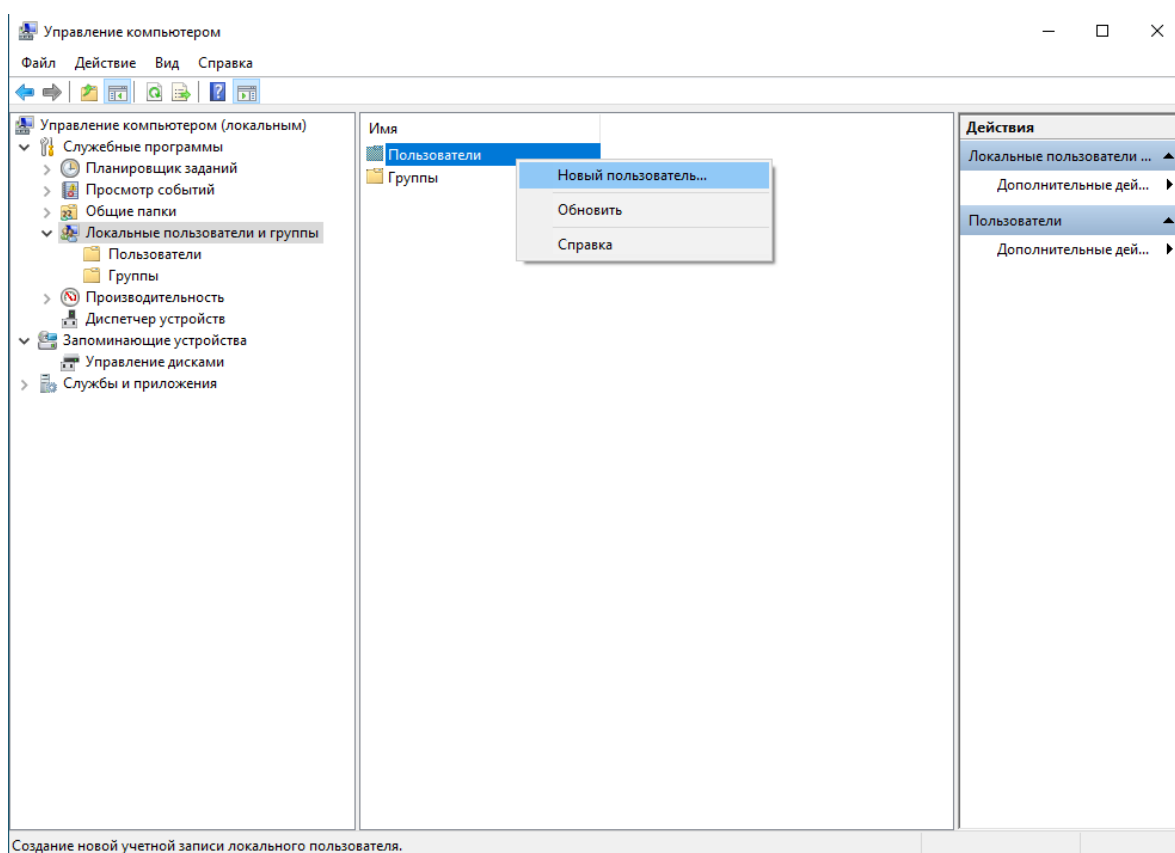


Рисунок 1 – Создание новой учетной записи локального пользователя

В появившемся окне задать имя пользователя (в примере, «userer»), пароль, выбрать пункт «Срок действия пароля не ограничен» и нажать кнопку «Создать», а затем «Закреть» (Рисунок 2).

Новый пользователь

Пользователь: userer

Полное имя:

Описание:

Пароль:

Подтверждение:

☐ Требовать смены пароля при следующем входе в систему

☐ Запретить смену пароля пользователем

☒ Срок действия пароля не ограничен

☐ Отключить учетную запись

Справка Создать Закрыть

Рисунок 2 – Добавление пользователя

Для того чтобы убедиться, что учетная запись «userer» не обладает правами администратора необходимо зайти в учетные записи пользователей («Управление компьютером» - «Локальные пользователи и группы» - «Пользователи») и у пользователя «userer» открыть «Свойства» - «Членство в группах» (Рисунок 3).

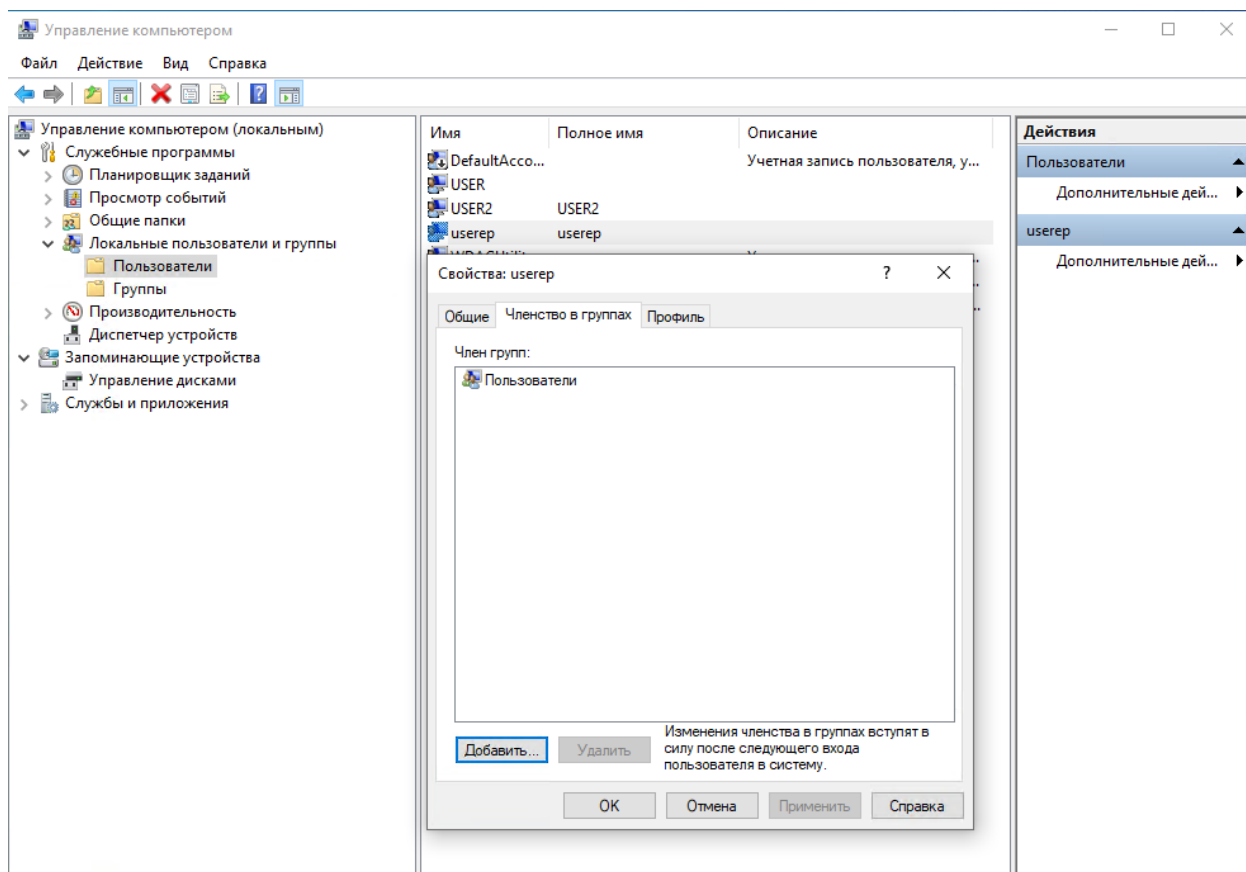
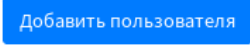


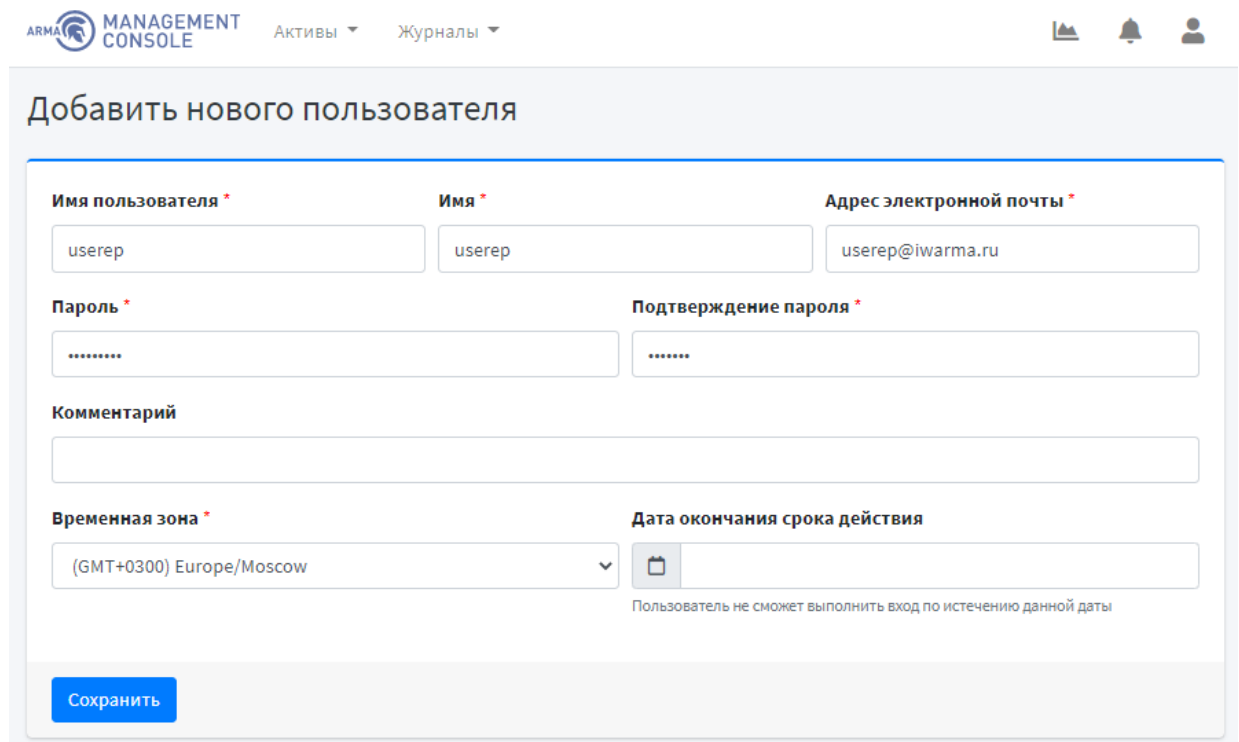
Рисунок 3 – Свойства учетной записи

2.2 Настройка связи с ARMA Management Console

Для связи с ARMA Management Console необходимо создать технического пользователя, от лица которого будет производиться связь с ARMA Industrial Endpoint.

Для добавления учетной записи пользователя в ARMA Management Console необходимо нажать на  в верхнем меню и выбрать «Просмотреть список пользователей». Затем нажать кнопку .

Добавить пользователя согласно рисунку ниже (Рисунок 4).

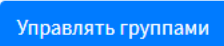


The screenshot shows the 'Добавить нового пользователя' (Add new user) form in the ARMA Management Console. The form includes the following fields and controls:

- Имя пользователя *** (Username): Input field with 'userrep'.
- Имя *** (Name): Input field with 'userrep'.
- Адрес электронной почты *** (Email): Input field with 'userrep@iwarma.ru'.
- Пароль *** (Password): Input field with masked characters '*****'.
- Подтверждение пароля *** (Confirm password): Input field with masked characters '*****'.
- Комментарий** (Comment): Text area.
- Временная зона *** (Time zone): Dropdown menu showing '(GMT+0300) Europe/Moscow'.
- Дата окончания срока действия** (Expiration date): Calendar icon and input field.
- Пользователь не сможет выполнить вход по истечению данной даты (User will not be able to log in after this date).
- Сохранить** (Save): Blue button at the bottom left.

Рисунок 4 – Добавление пользователя в ARMA Management Console

Для того чтобы пользователю назначить привилегию «Может скачивать конфигурацию Endpoint» необходимо создать группу с такой привилегией и добавить туда пользователя.

Для создания группы в ARMA Management Console необходимо нажать на  в верхнем меню, выбрать «Просмотреть список пользователей» и нажать на кнопку . Создать группу «Endpoint» с привилегией «Может скачивать конфигурацию Endpoint», нажав на кнопку  и добавить в неё пользователя «userrep» (Рисунок 5).

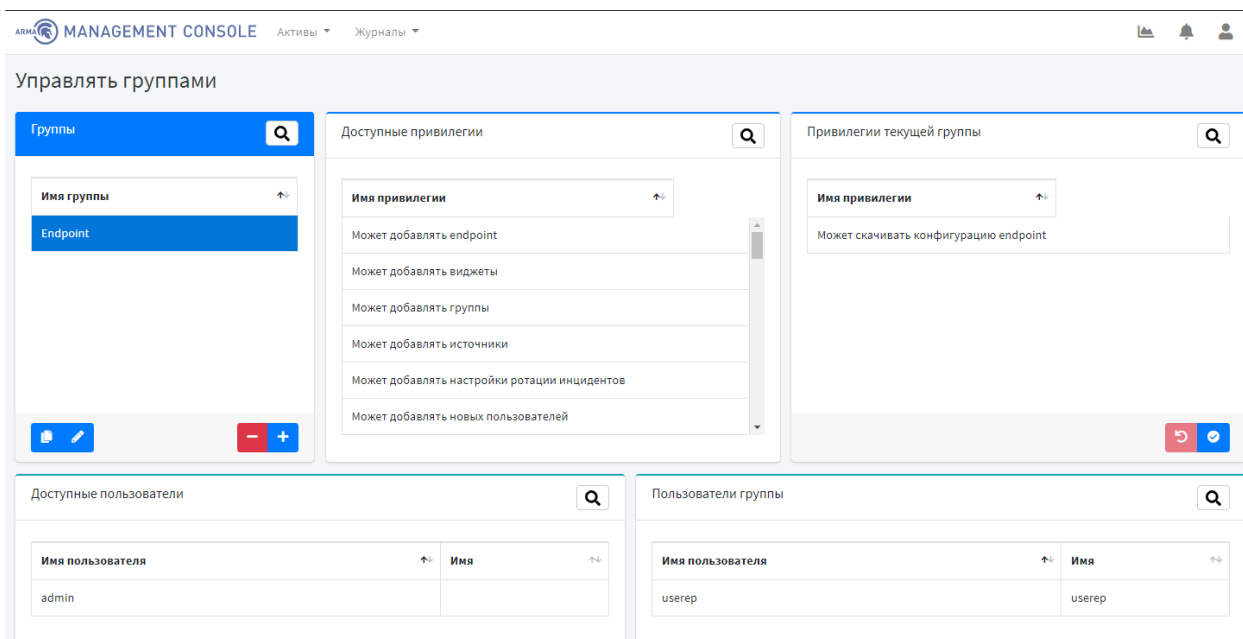


Рисунок 5 – Добавление группы в ARMA Management Console

2.3 Установка сервиса

Для установки сервиса ARMA Industrial Endpoint, используя учетную запись администратора, необходимо запустить установщик «ARMA Industrial Endpoint installer.msi» и установить, следуя подсказкам мастера установки (Рисунок 6, Рисунок 7, Рисунок 8, Рисунок 9).

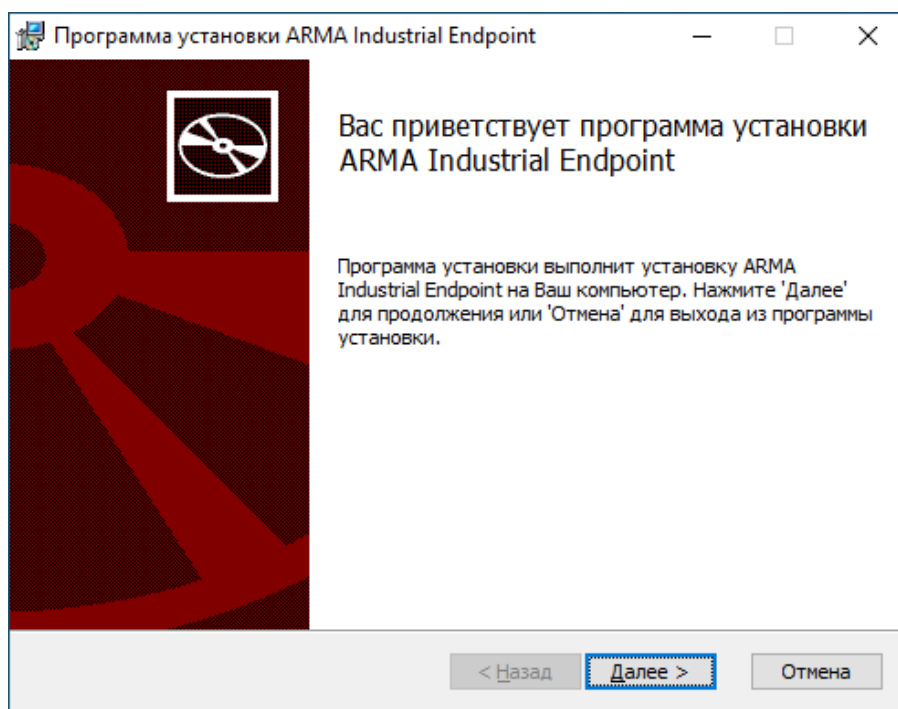


Рисунок 6 – Установка ARMA Industrial Endpoint (1)

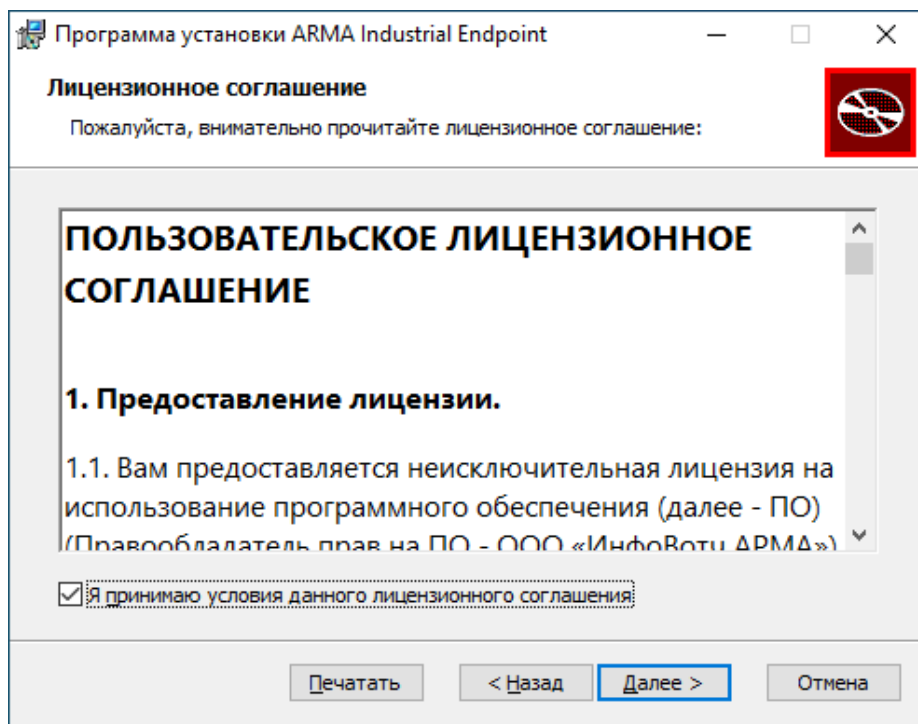


Рисунок 7 – Установка ARMA Industrial Endpoint (2)

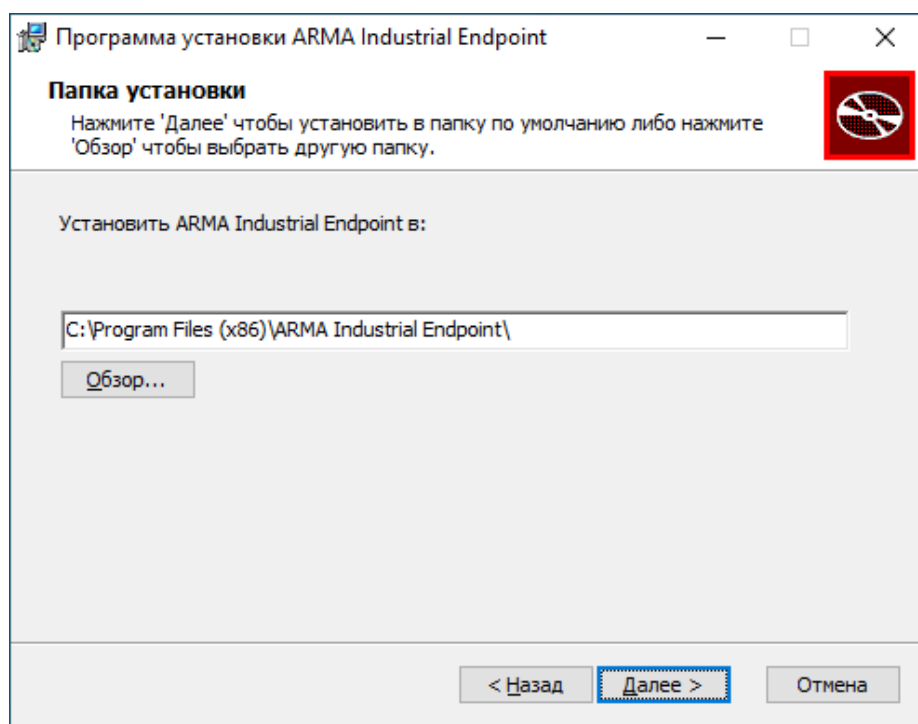


Рисунок 8 – Установка ARMA Industrial Endpoint (3)

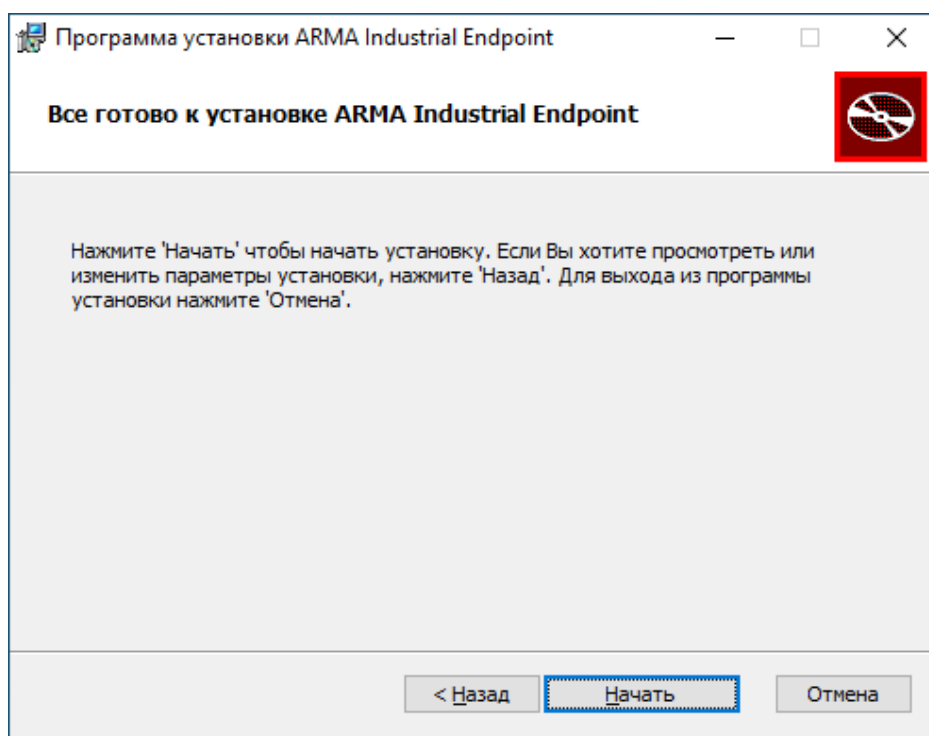


Рисунок 9 – Установка ARMA Industrial Endpoint (4)

После нажатия на кнопку «Начать» во всплывающем окне нужно подтвердить действие и установка запустится. После завершения установки и нажатия на кнопку «Готово» во всплывающем окне будет предложено перезагрузить компьютер (Рисунок 10).

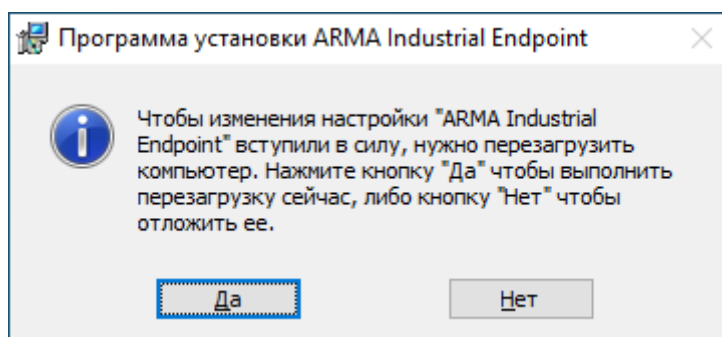


Рисунок 10 – Всплывающее окно перезагрузки

После установки ARMA Industrial Endpoint и перезагрузки компьютера будет автоматически запущен сервис «ARMA Industrial Endpoint», который можно просмотреть в службах Windows (Рисунок 11) и создано правило межсетевого экрана, которое можно просмотреть в Брандмауэр Защитника Windows (Дополнительные параметры – Правила для входящих подключений) (Рисунок 12).

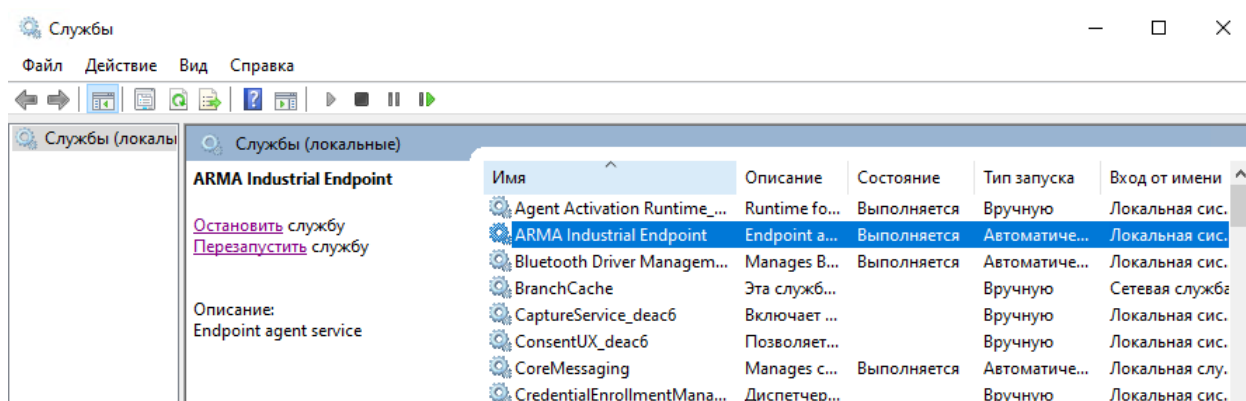


Рисунок 11 – Сервис «ARMA Industrial Endpoint»

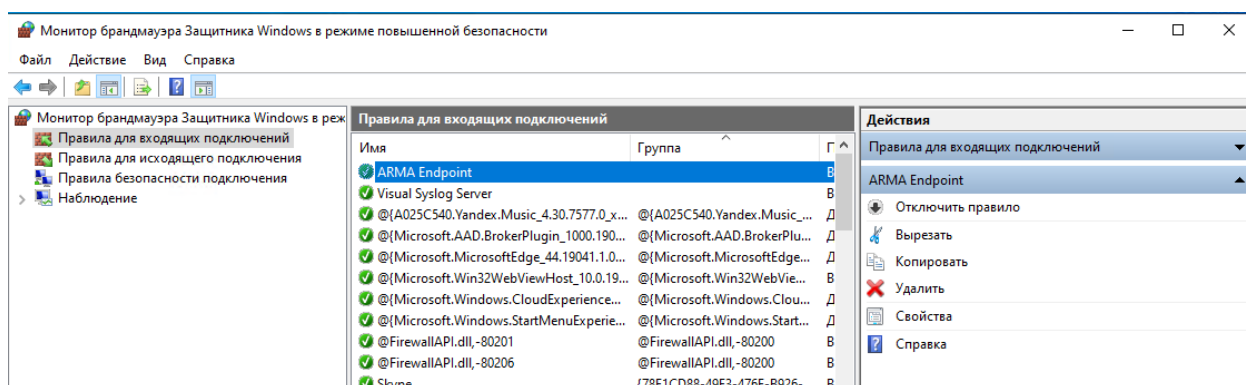
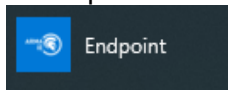


Рисунок 12 – Правило межсетевого экрана

2.4 Запуск сервиса

Для запуска сервиса ARMA Industrial Endpoint необходимо открыть графический интерфейс, нажав на иконку  в меню «Пуск». Откроется главное окно графического интерфейса (Рисунок 13).

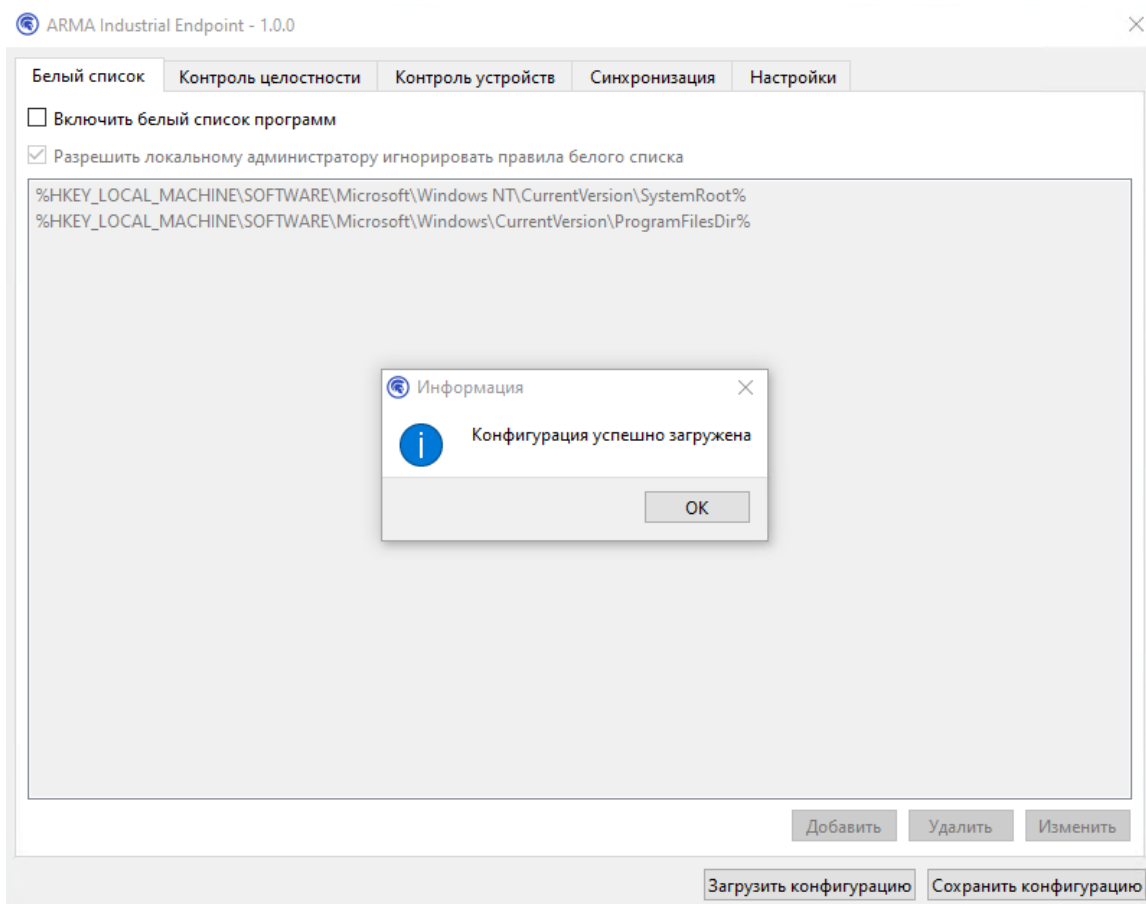
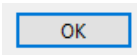


Рисунок 13 – Главное окно веб-интерфейса ARMA Industrial Endpoint

После загрузки конфигурации, нажав на кнопку  можно пользоваться сервисом.

2.5 Добавление и настройка Endpoint в ARMA Management Console

Для настройки Endpoint в ARMA Management Console необходимо перейти на страницу «Активы» - «Endpoint» (Рисунок 14).

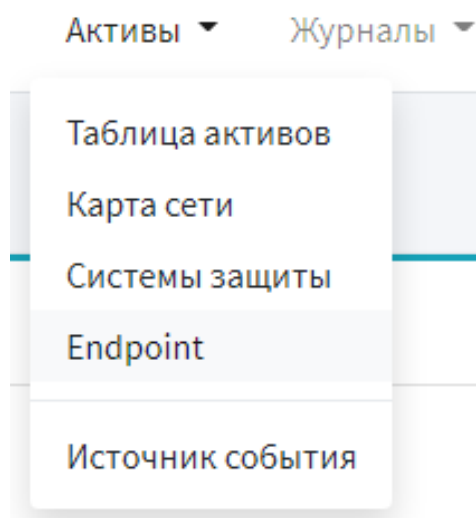
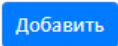


Рисунок 14 – Переход в настройки Endpoint

Нажать на кнопку  и настроить конфигурацию Endpoint согласно рисункам 14-16.

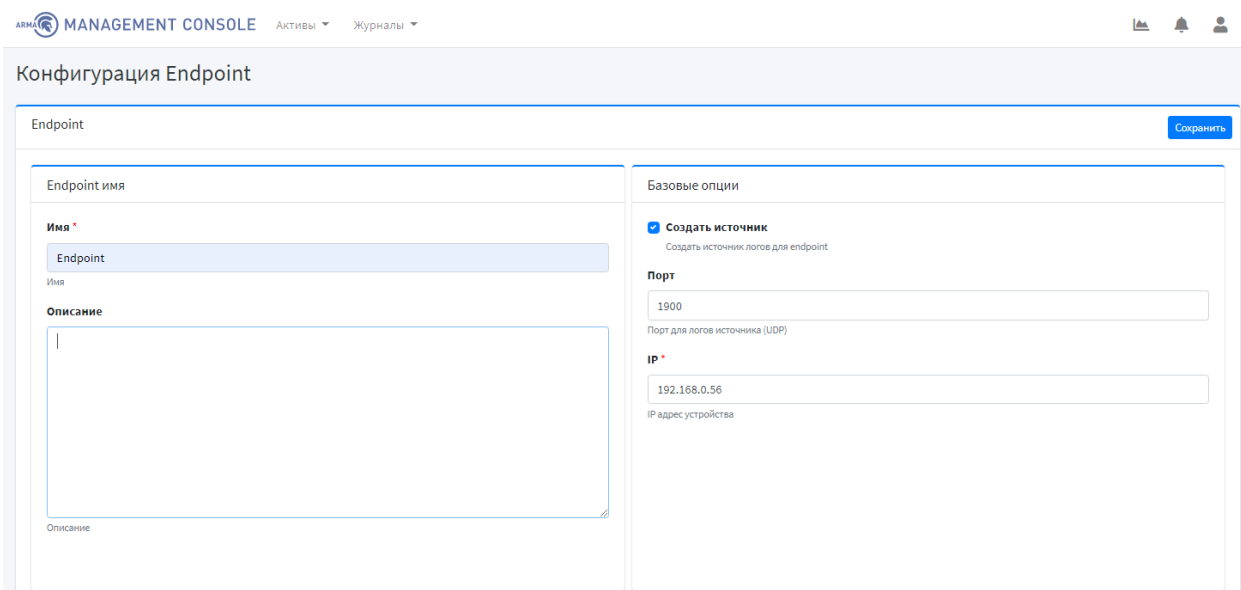


Рисунок 15 – Добавление Endpoint (1)

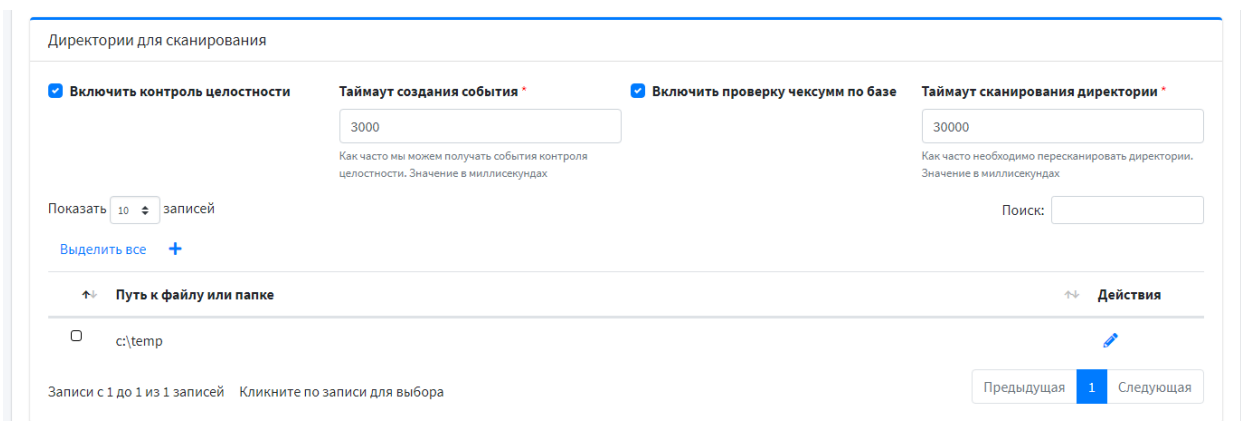


Рисунок 16 – Добавление Endpoint (2)

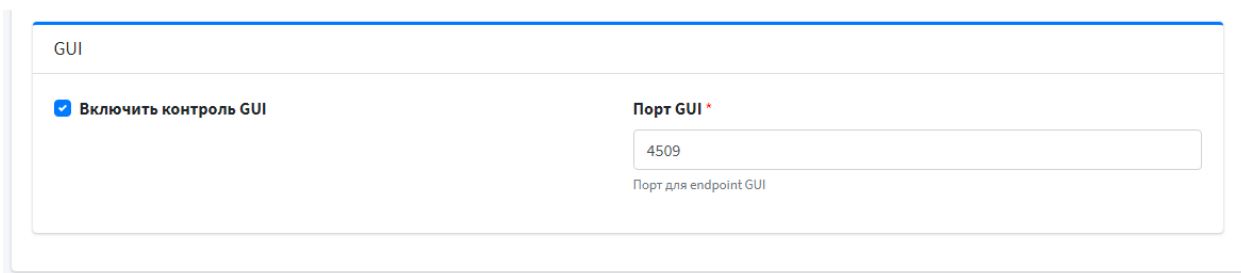


Рисунок 17 – Добавление Endpoint (3)

При добавлении сервиса Endpoint ему автоматически присваивается порядковый номер («ID»), который можно увидеть в общем списке Endpoint (Рисунок 18), а так же при нажатии на кнопку  напротив нужного Endpoint в адресной строке (Рисунок 19).

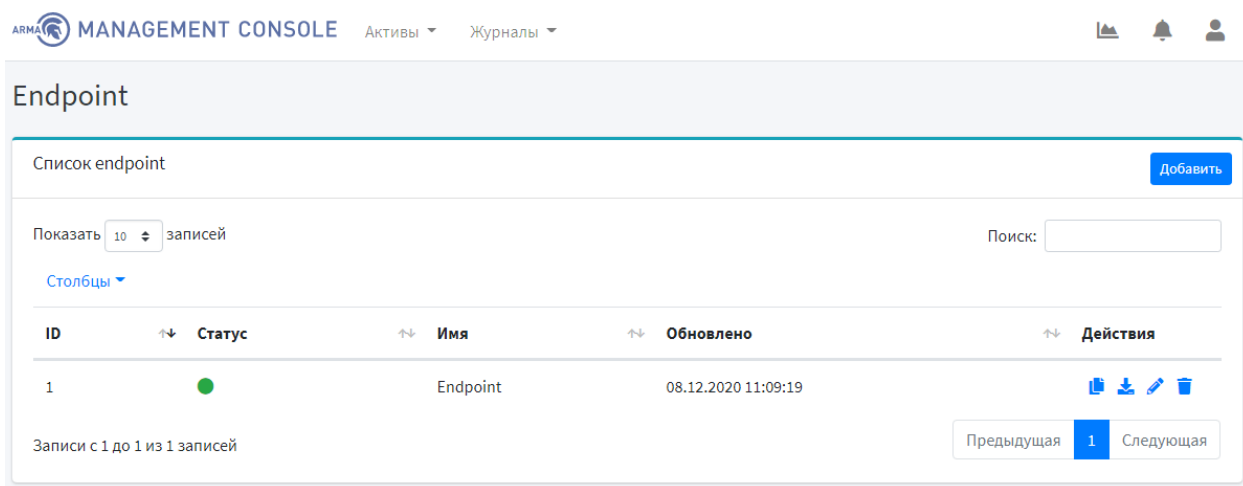


Рисунок 18 – Список Endpoint

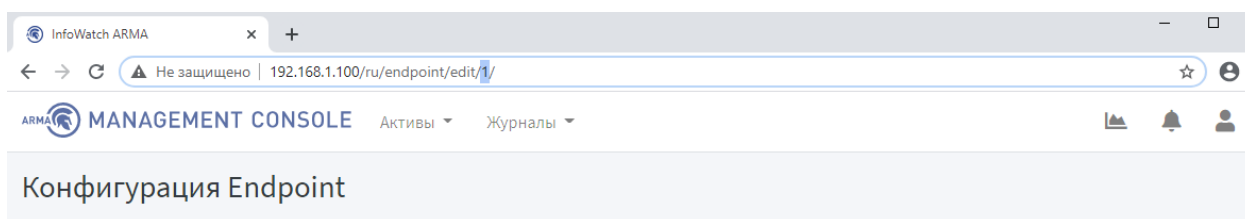


Рисунок 19 – Адрес сервиса Endpoint

3 УПРАВЛЕНИЕ БЕЛЫМ СПИСКОМ ПРОГРАММ

Управление белым списком программ осуществляется либо через единый центр управления ARMA Management Console, либо в графическом интерфейсе ARMA Industrial Endpoint.

Для ограничения перечня исполняемых программ в ARMA Management Console в настройках Endpoint (страница «Активы» - «Endpoint») в блоке «Белый список приложений» необходимо добавить путь к файлу или папке, доступ к которым будет разрешен, и нажать на кнопку **Сохранить** (Рисунок 20).

Белый список приложений

☒ Включить белый список

☒ Включить gpupdate
Включить принудительное обновление политики.
Выполнение может занять больше времени

☒ Локальный администратор игнорирует белый список

Показать 10 записей

Поиск:

Выделить все +

Путь к файлу или папке	Действия
☐ %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	
☐ %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	
☐ c:\syslog	

Записи с 1 до 3 из 3 записей Кликните по записи для выбора

Предыдущая 1 Следующая

Рисунок 20 – Белый список приложений

Для ограничения перечня исполняемых программ в графическом интерфейсе ARMA Industrial Endpoint во вкладке «Белый список программ» необходимо добавить путь к файлу или папке, доступ к которым будет разрешен, нажав на кнопку **Добавить**, и нажать на кнопку **Сохранить конфигурацию** (Рисунок 21).

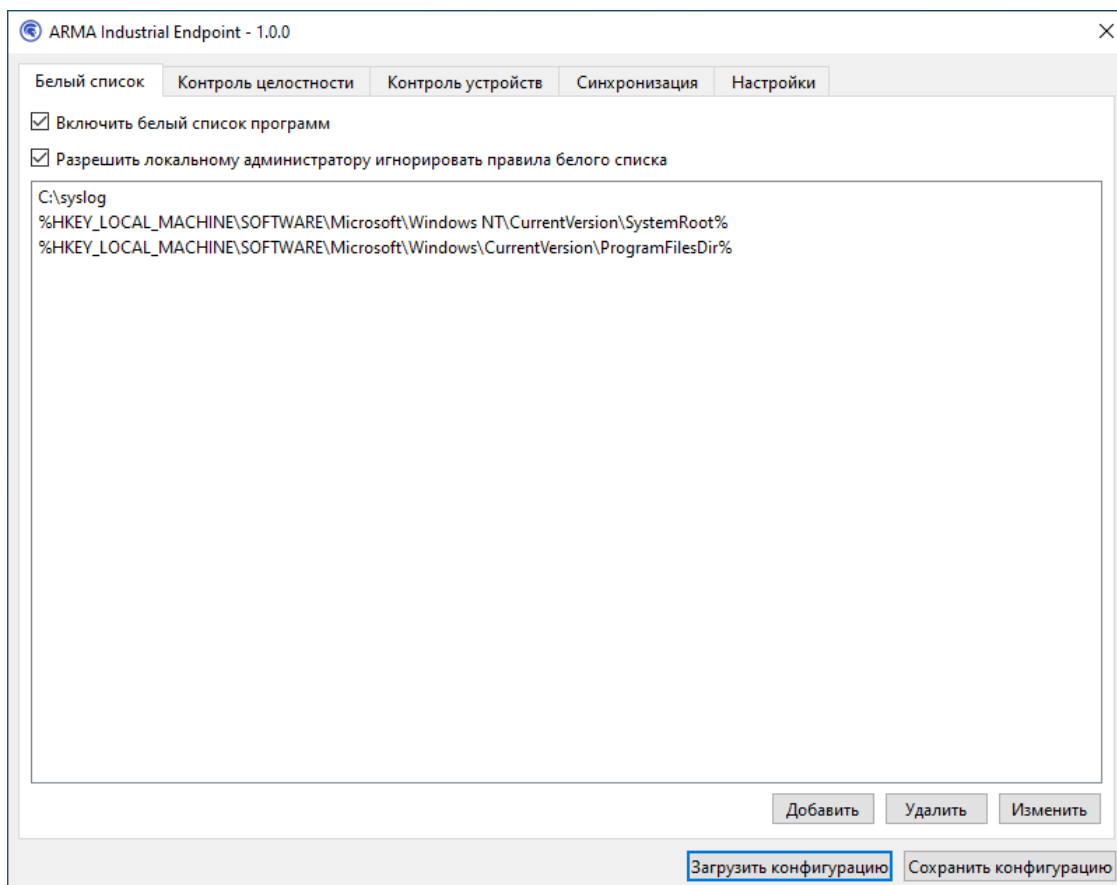


Рисунок 21 – Белый список программ

Для того чтобы проверить, что белый список приложений работает необходимо попробовать установить любую программу не входящую в этот список. При попытке установки программы не из белого списка появится следующее сообщение (Рисунок 22).

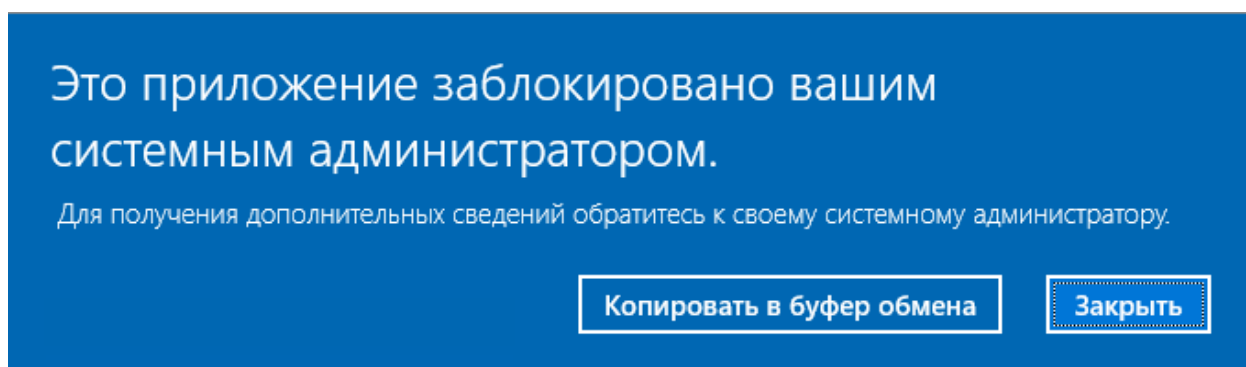


Рисунок 22 – Сообщение об ошибке

4 УПРАВЛЕНИЕ КОНТРОЛЕМ ЦЕЛОСТНОСТИ

Управление контролем целостности программного обеспечения осуществляется либо через единый центр управления ARMA Management Console, либо в графическом интерфейсе ARMA Industrial Endpoint.

Для добавления директории для сканирования в ARMA Management Console в настройках Endpoint (страница «Активы» - «Endpoint») в блоке «Директории для сканирования» необходимо задать путь к файлу или папке, которые необходимо сканировать (Рисунок 16).

Для добавления директории для сканирования в графическом интерфейсе ARMA Industrial Endpoint во вкладке «Контроль целостности» необходимо выбрать контролируемые директории, нажав на кнопку **Добавить** и сохранить изменения, нажав на кнопку **Сохранить конфигурацию** (Рисунок 23).

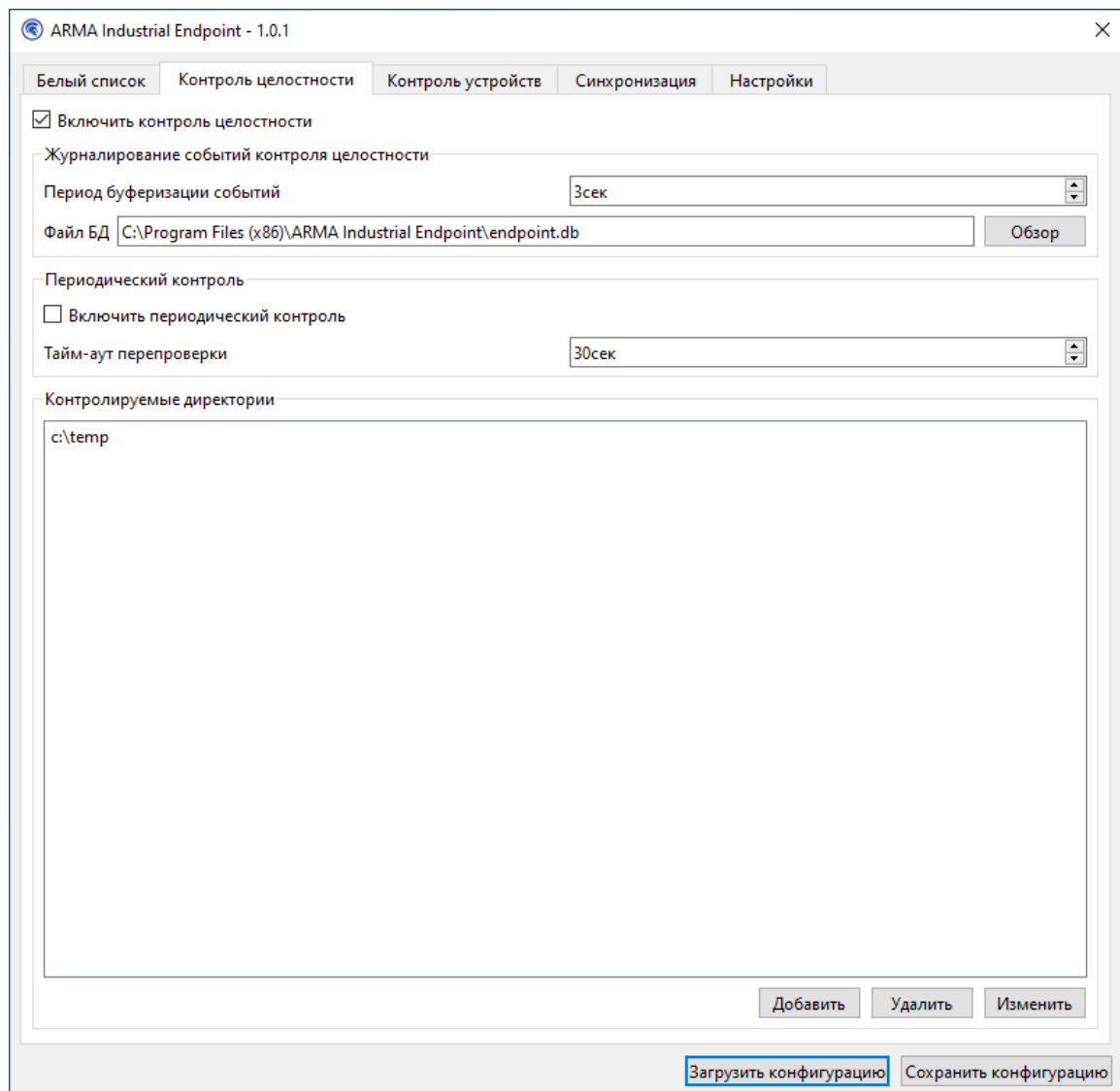


Рисунок 23 – Контроль целостности

При настроенном контроле целостности сообщения об изменениях будут отражены в журнале событий в ARMA Management Console («Журналы» - «Журнал событий») (Рисунок 24) и в файле логов «endpoint.log» (Рисунок 25), расположенном в папке сервиса «ARMA Industrial Endpoint» (по умолчанию C:\Program Files (x86)\ARMA Industrial Endpoint).

ARMA MANAGEMENT CONSOLE Активы Журналы

Журнал событий

Список событий Помощь 2020.12.08

Показать 10 записей Поиск:

Столбцы

Дата	ID	Сообщение	Критичность	Категория	IP источника	IP получателя
08.12.2020 13:13:46	de0b3d32-2882-4953-925d-5684d9ae4dfc	RENAME:c:\temp\1\Новый текстовый документ (2).txt -> c:\temp\1_Новый текстовый документ_.txt, DESKTOP-DSTKMJO	4	Integrity control	192.168.0.65	
08.12.2020 13:13:28	77d49994-d18e-43b3-a5e6-c22d9c450915	WRITE:c:\temp\1, DESKTOP-DSTKMJO	4	Integrity control	192.168.0.65	
08.12.2020 13:13:28	ff937147-2cdc-44cb-ad3a-d410b3bf2c4d	CREATE:c:\temp\1\Новый текстовый документ (2).txt, DESKTOP-DSTKMJO	4	Integrity control	192.168.0.65	
08.12.2020 13:13:22	17f44bc5-0362-4baf-bf9c-5e98da1aa392	WRITE:c:\temp\1\test.txt, DESKTOP-DSTKMJO	4	Integrity control	192.168.0.65	

Записи с 1 до 4 из 4 записей Предыдущая 1 Следующая

Рисунок 24 – Журнал событий ARMA Management Console

```
time="2020-12-08T13:13:22+03:00" level=info msg="Got event: FILE \"test.txt\" WRITE [c:\\temp\\1\\test.txt]" duration=3s part=icontrol
time="2020-12-08T13:13:28+03:00" level=info msg="Got event: DIRECTORY \"1\" WRITE [c:\\temp\\1]" duration=3s part=icontrol
time="2020-12-08T13:13:28+03:00" level=info msg="Got event: FILE \"Новый текстовый документ (2).txt\" CREATE [c:\\temp\\1\\Новый текстовый документ (2).txt]" duration=
time="2020-12-08T13:13:46+03:00" level=info msg="Got event: DIRECTORY \"1\" WRITE [c:\\temp\\1]" duration=3s part=icontrol
time="2020-12-08T13:13:46+03:00" level=info msg="Got event: FILE \"Новый текстовый документ (2).txt\" RENAME [c:\\temp\\1\\_Новый текстовый документ_.txt]" duration=3s
```

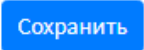
Рисунок 25 – Журнал логов «endpoint.log»

5 УПРАВЛЕНИЕ КОНТРОЛЕМ УСТРОЙСТВ

Управление контролем устройств осуществляется либо через единый центр управления ARMA Management Console, либо в графическом интерфейсе ARMA Industrial Endpoint.

Программа позволяет ограничивать следующие типы съемных носителей: дискеты, CD/DVD диски, USB, кассеты и мобильные устройства (Windows Portable Devices (WDP)).

Для ограничения подключаемых съемных носителей в ARMA Management Console в настройках Endpoint (страница «Активы» - «Endpoint») в блоке «Права доступа» необходимо установить флажок напротив того типа съемных носителей,

доступ к которым должен быть ограничен и нажать на кнопку  (Рисунок 26).

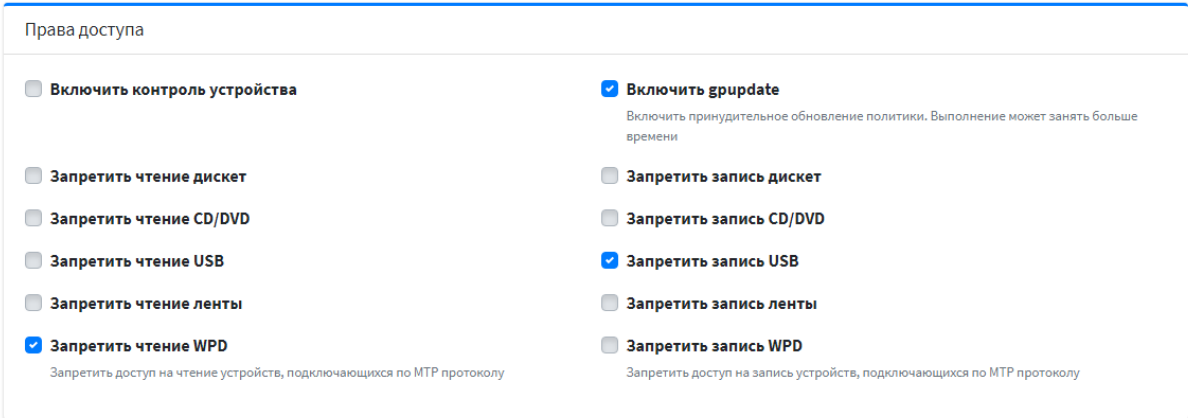
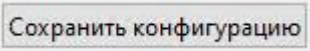


Рисунок 26 – Настройка прав доступа

Для ограничения подключаемых съемных носителей в графическом интерфейсе ARMA Industrial Endpoint во вкладке «Контроль устройств» необходимо сначала включить управление устройствами, установив флажок в соответствующем поле, а затем установить флажок напротив того съемного носителя, доступ к которому должен быть ограничен и нажать на кнопку  (Рисунок 27).

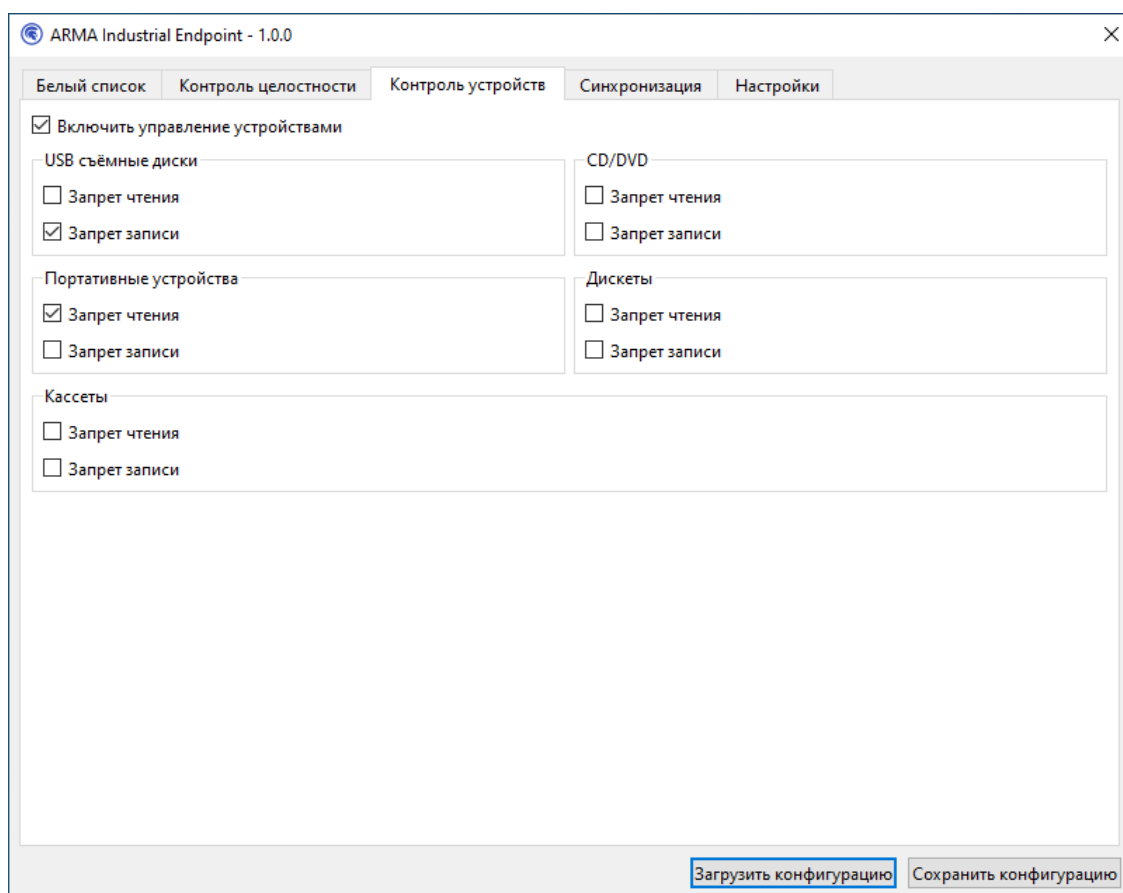


Рисунок 27 – Контроль устройств

Примечание – в ОС Windows 7 после применения политик необходимо перезагрузить компьютер.

Для того чтобы проверить, что ограничение записи, допустим на USB, работает, необходимо либо создать новый текстовый файл, либо скопировать любой файл на USB. При попытке это сделать появится всплывающее окно (Рисунок 28).

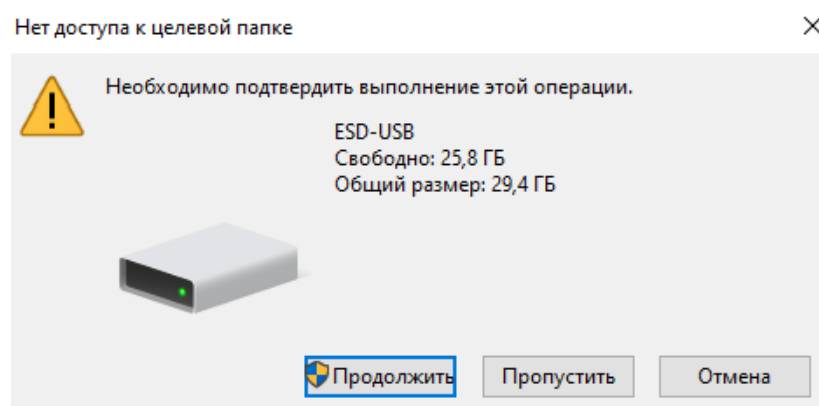


Рисунок 28 – Всплывающее окно «Нет доступа к целевой папке»

При проверке ограничения чтения на USB появится следующее всплывающее окно (Рисунок 29).

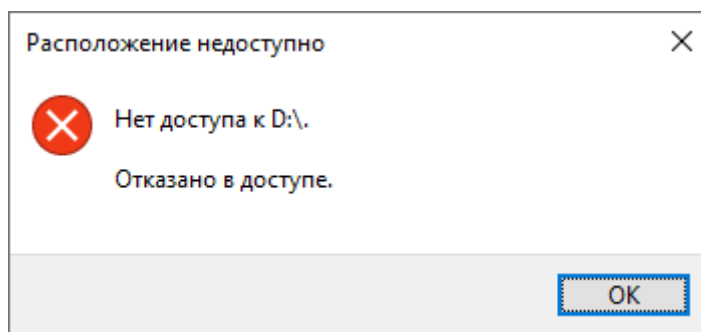


Рисунок 29 – Всплывающее окно «Расположение недоступно»

6 НАСТРОЙКА СИНХРОНИЗАЦИИ С ARMA MANAGEMENT CONSOLE

Для настройки синхронизации ARMA Industrial Endpoint с ARMA Management Console необходимо в веб-интерфейсе перейти во вкладку «Синхронизация», задать настройки согласно рисунку (Рисунок 30) и нажать на кнопку **Сохранить конфигурацию**.

ARMA Industrial Endpoint - 1.0.0

Белый список Контроль целостности Контроль устройств Синхронизация Настройки

☒ Включить синхронизацию с ARMA Management Console
☒ Не пытаться восстановить соединение в случае ошибки

Аутентификация

Логин
Пароль
ID

Синхронизация

Хост ARMA MC
Тайм-аут KeepAlive
Тайм-аут синхронизации конфигурации

Загрузить конфигурацию Сохранить конфигурацию

Рисунок 30 – Вкладка настройки синхронизации

7 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ

7.1 Информация о состоянии и лицензии Endpoint

В блоке «Состояние» представлена информация о текущем состоянии Endpoint и действующей лицензии (Рисунок 31).

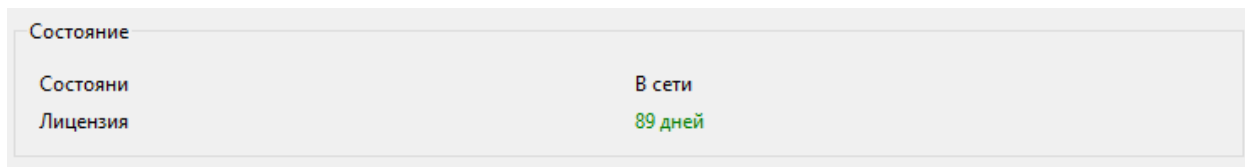


Рисунок 31 – Состояние

Если лицензия истекла, то в веб-интерфейсе блокируются кнопки управления, форма данных подключения, кнопки загрузки и сохранения конфигурации, а также блокируется контроль устройств и белый список.

7.2 Настройка подключения и управления ARMA Industrial Endpoint

В блоке «Графический интерфейс» предоставляется возможность настраивать подключение графического интерфейса к ARMA Industrial Endpoint (для удаленного доступа к ARMA Industrial Endpoint) и непосредственно управлять ARMA Industrial Endpoint.

В блоке «Управление» предоставляется возможность разрешать или запрещать управление ARMA Industrial Endpoint из графического интерфейса.

Кнопка **Перезагрузка сервиса** позволяет перезапустить сервис ARMA Industrial Endpoint. Кнопка **Обновление БД** позволяет обновить базу данных (БД) (Рисунок 32).

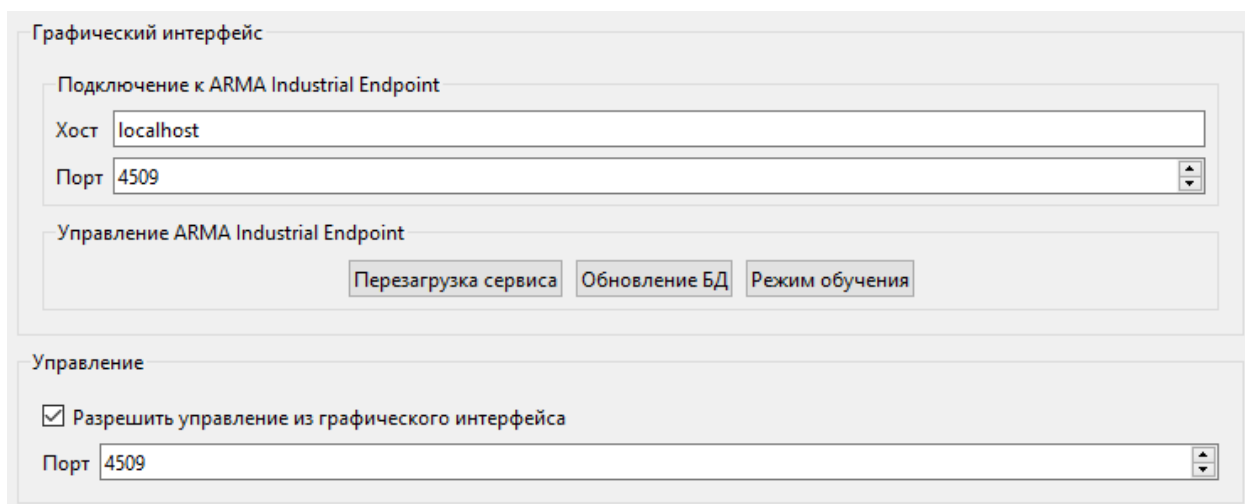


Рисунок 32 – Графический интерфейс и управление

7.2.1 Режим обучения

Режим обучения запускает сканирование запущенных программ и записывает их в белый список. Для проверки режима обучения необходимо нажать на кнопку **Режим обучения**, затем перейти на вкладку «Белый список» и

нажать на кнопку **Загрузить конфигурацию**, убедиться в том, что контролируемые им папки появились в списке и нажать на кнопку **Сохранить конфигурацию**.

7.3 Настройка сетевого журнала

В блоке «Сетевой журнал» предоставляется возможность настроить получение событий от ARMA Industrial Endpoint.

Для того чтобы настроить экспорт событий от ARMA Industrial Endpoint необходимо задать настройки согласно рисунку (Рисунок 33), а затем нажать на кнопку **Сохранить конфигурацию**. При успешном сохранении настроек появится всплывающее окно информации (Рисунок 34).



Рисунок 33 – Вкладка «Настройки» - «Сетевой журнал»

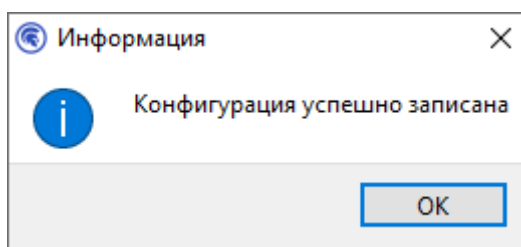


Рисунок 34 – Сообщение об успешной записи конфигурации

7.4 Настройка журналирования

В блоке «Журналирование» предоставляется возможность включить журналирование событий, очистку журнала при запуске и настраивать уровень детализации событий (Рисунок 35).

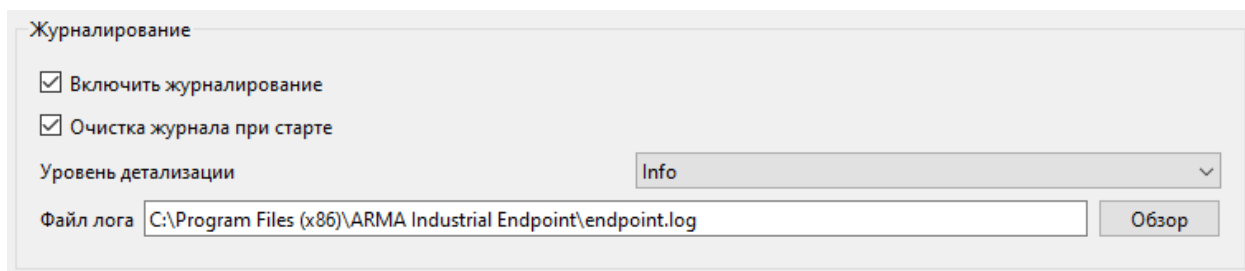


Рисунок 35 – Журналирование

8 ПРОСМОТР ЖУРНАЛА СОБЫТИЙ В ФАЙЛЕ ENDPOINT.LOG

Все события, регистрируемые программой, сохраняются в файле «endpoint.log» и отправляются на ARMA Management Console.

В таблице 1 представлены некоторые события из файла «endpoint.log». Для экономии места в таблице дата и время для записей в журнале не указаны.

Таблица 1 – События, регистрируемые программой

№ п.п.	Запись в журнале	Описание события
1	Runing in service mode	Сервис запущен
2	Control server started on port 4509	Сервер управления запущен на порту 4509
3	Initializing check from db	Инициализация проверки из БД
4	Got event: FILE \"test.txt\" WRITE [c:\\temp\\1\\test.txt]	Изменение файла test.txt
5	Got event: FILE \"Новый текстовый документ (2).txt\" RENAME [c:\\temp\\1\\Приказ.txt]	Добавлен новый текстовый документ с названием Приказ.txt
6	Got event: FILE \"test_1.txt\" REMOVE [c:\\temp\\1\\test_1.txt]	Удаление файла test_1.txt
7	Syslog init finish. Connected to 192.168.0.68:1800	Завершение инициализации системного журнала. Подключено к 192.168.0.68:1800
8	Config updated	Конфигурация обновлена
9	Restarting endpoint	Перезапуск endpoint
10	Starting console sync	Запуск синхронизации консоли
11	Intergrity control started	Контроль целостности запущен
12	Check done	Проверка выполнена