

# STAFFCOP ENTERPRISE

Что нового в версии 5.3.1736

# Содержание

Карточка сотрудника.....	3
Консоль инцидентов.....	5
Список доступных действий и соответствующие команды:.....	6
Улучшение словарей .....	7
Исключения мониторинга: Видеозапись .....	8
Обновление агента с включенной защитой.....	9
Глубина цвета пакетных снимков экрана .....	10
Настройка прав доступа.....	11
Деление базы данных сервера.....	12
Поддержка российской СУБД «Jatoba».....	13
Новые возможности передачи данных об инцидентах.....	14
Помощь при ошибках активации .....	14
Нововведения менеджера ВНИ .....	15
Исправления и доработки.....	17

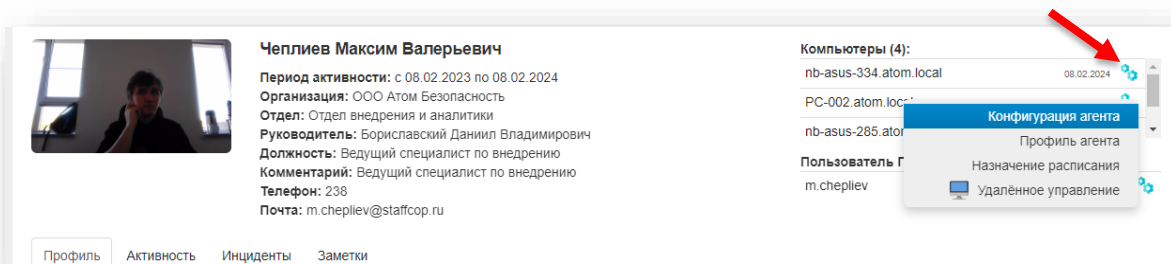


## Карточка сотрудника

Ключевое нововведение карточки – возможность перейти к настройке сбора и обработки данных пользователя. Нажмите две шестеренки справа от названия компьютера или пользователя, чтобы увидеть контекстное меню.

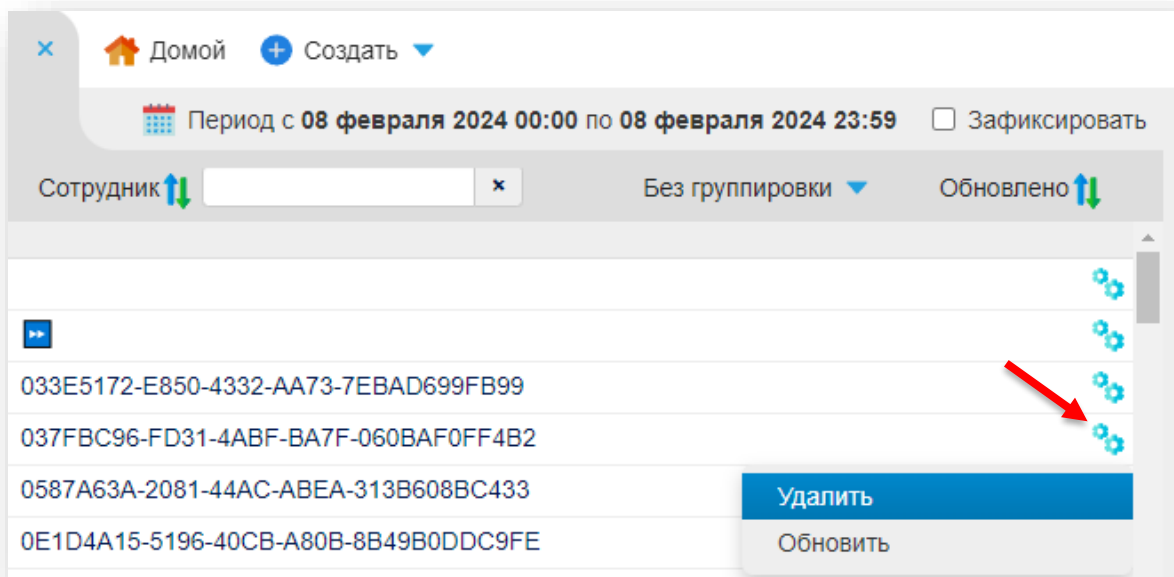
Теперь из меню возможно перейти к настройке конфигурации на любом компьютере, с которого пользователь работает сейчас или делал это ранее.

Также можно отредактировать **Профиль агента**, настроить **Назначение расписания** для учетных записей сотрудника или перейти к просмотру рабочего стола.



В общий отчет на вкладку **Профиль** добавили быстрый переход к анализу событий сотрудника в **Линзе**.

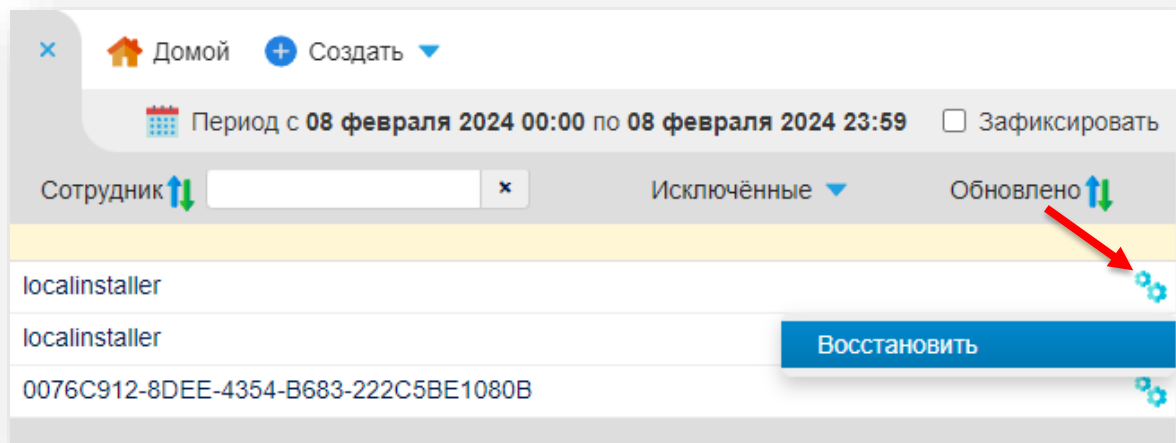
Изменили способ управления пользователями, для которых не нужна карточка.



Иногда нужно удалить из списка сотрудников карточки, которые появились из-за перехвата технических учетных записей. Также иногда нужно удалить карточку сотрудника, для которого запрещено выводить агрегированную информацию по пользователю в карточке, или скрыть карточку уволенного сотрудника.

Ранее в интерфейсе не было возможности просмотреть удаленные карточки, поэтому **Администратор** системы должен был обращаться к базе данных, чтобы посмотреть список пользователей, по которым карточки не ведутся или чтобы восстановить удаленные карточки.

Теперь все удаленные карточки мы заносим в отдельный список. Это позволяет Администратору быстро увидеть список удаленных карточек и при необходимости восстановить карточку.



## Консоль инцидентов

В новой версии мы улучшили процесс работы с задачами.

Добавили ряд предустановленных отчетов. С их помощью **Администраторы** смогут быстро получать агрегированную информацию об инцидентах и процессе расследования.

ID ↓	Наименование
9	Высокий приоритет
8	Отчет по критичности инцидентов
7	Детальный отчет по участникам инцидентов
6	Отчет по участникам инцидентов
5	Детальный отчет по обработке инцидентов
4	Отчет по обработке инцидентов
3	Отчёт по инцидентам детально
2	Отчёт по решённым инцидентам
1	Отчет по инцидентам

Расширили возможности настройки прав доступа. Добавили возможность более тонкой настройки прав доступа к инцидентам и управлению задачами расследования. Например, можно предоставить сотруднику доступ к обработке задачи инцидента и ограничить ему доступ к изменению шаблонов и статусов, которые применимы ко всем инцидентам.

Права можно настроить в группах **Администраторов**.

Имя:

Права:

инци

- Доступ не только к своим инцидентам
- Может добавлять группа инцидентов
- Может добавлять инцидент
- Может добавлять фильтр инцидентов
- Может изменять группа инцидентов
- Может изменять событие инцидента
- Может изменять фильтр инцидентов
- Может удалять группа инцидентов
- Может удалять событие инцидента
- Может удалять фильтр инцидентов
- Настройки инцидентов
- Чтение инцидентов
- Экспорт инцидентов

Выбранные права:

- Может добавлять событие инцидента
- Может изменять инцидент
- Может удалять инцидент

Выбрать все →      ← Удалить все

Вернули возможность печати отчетов в **Консоли инцидентов**.

Добавили возможности удалять настройки консоли инцидентов и сами инциденты из архива. **Администратор** может сделать это посредством терминала сервера Staffcop Enterprise.

## Список доступных действий и соответствующие команды:

- очистить весь архив консоли инцидентов

```
staffcop incident_clean all
```

- удалить инциденты в архиве консоли инцидентов

```
staffcop incident_clean incident
```

- удалить статусы в архиве консоли инцидентов

```
staffcop incident_clean status
```

- удалить группы в архиве консоли инцидентов

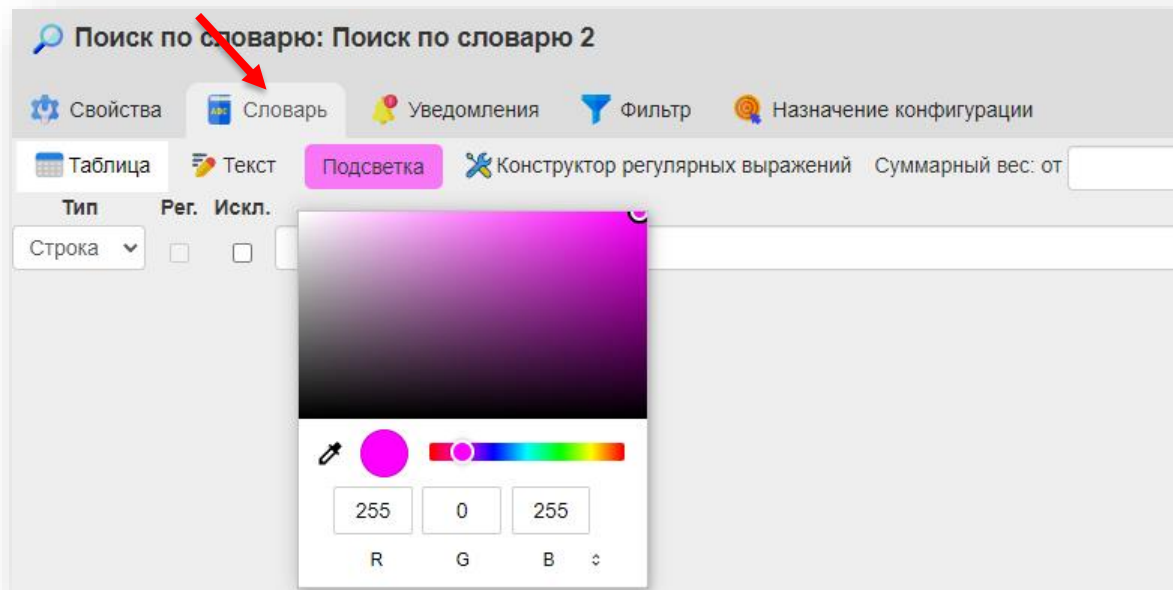
```
staffcop incident_clean group
```

- удалить шаблоны реагирования в архиве консоли инцидентов

```
staffcop incident_clean responsepattern
```

## Улучшение словарей

Для обнаружения утечек используется довольно большое количество словарей, что приводит к проблеме при анализе: разные словари подсвечивают реакции одним и тем же цветом. Мы предоставили **Администраторам** расширенную палитру выбора цвета словаря для решения этой проблемы. Теперь можно настроить уникальную подсветку для каждого словаря.



## Исключения мониторинга: Видеозапись

Правила с новым типом событий **DesktopVideo** позволят снизить нагрузку на сервер и агента исключив из процесса записи ненужные изображения. Также это позволит исключить из записи информацию, которую запрещено передавать в другие системы, например ввод пароля.

В конфигурации агента в разделе **Исключения мониторинга** включите модуль «Исключения мониторинга» и настройте правила. Агент не включит в запись изображения, соответствующие правилам.

Поле	Оператор	Значение	Добавить выражение
Тип события	равно	DesktopVideo	И Или x
Имя пользователя	равно	m.chepliev	И Или x
Заголовок окна	совпадает	password	И Или x

event\_type == "DesktopVideo" and user\_name == "m.chepliev" and window\_title matches "(password)"

Правило можно настроить так, что видеозапись не будет происходить в определенные моменты активности пользователя, например, когда пользователь работает в заданном приложении. В такие моменты изображение на видеозаписи будет заменено черным экраном.



## Обновление агента с включенной защитой

Агенты для Windows начиная с версии 5.8.2564 защищены от внешнего вмешательства паролем. Включение защиты мешало обновлению агента.

После установки версии агента 5.8.2574 можно будет обновлять агенты из панели управления без отключения защиты. На более ранних версиях такой возможности нет и перед обновлением защиту агента необходимо отключить.

Если на компьютере пользователя установлен агент версии 5.8.2574 запустите на сервере в панели управления компьютерами обновление агентов до последней версии.

Компьютер	Версия ОС	Статус	Лицензия	IP	Версия агента	Последняя проверка
<input checked="" type="checkbox"/> ● <b>DESKTOP-FFOLON0</b>	10.0.19041	Нет данных от агента более 10 минут	Назначена	95.170.152.32	2574	13:19:09 26 (3 часа наз
<input type="checkbox"/> ● <b>DESKTOP-OV4O6V5</b>	10.0.19041	Нет данных от агента более 10 минут	Назначена	194.35.118.40	2570 (требуется)	23:02:47 24 (1 день, 18

## Глубина цвета пакетных снимков экрана

Изменили способ выбора **глубины цвета** снимков в пакете. Заменили ручной ввод на выбор из выпадающего списка. **Администратор** теперь может выбрать **глубину цвета** снимков в пакете только из фиксированного списка значений.

Это позволит избежать ошибок, например, когда пользователи вводили значения параметра, которые могли исказить результат.

Пакет снимков экрана

Пакеты снимков экрана Создавать пакеты снимков экрана.

Интервал снимков, миллисекунд:  Интервал между снимками в миллисекундах.

Продолжительность пакета, секунд:  Продолжительность непрерывной записи снимков в секундах.

Бит на пиксель:  Выбор глубины цветности снимков в пакете.

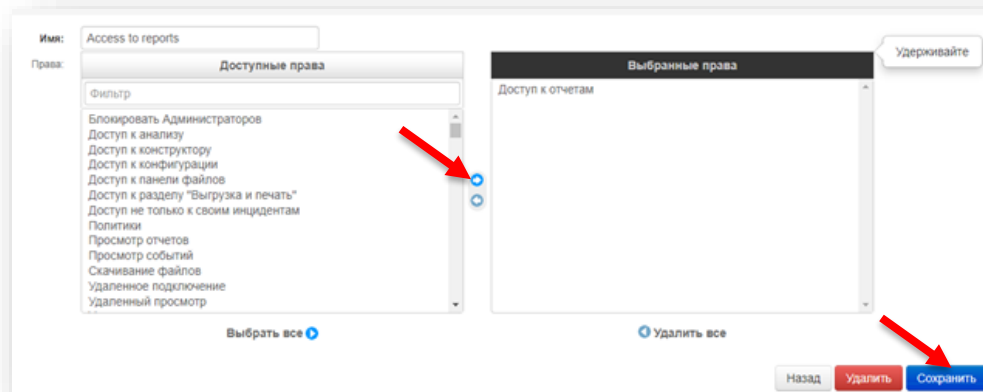
Алгоритм сжатия:

Уровень сжатия:

Автонастройка уровня сжатия Автоматическое снижение уровня сжатия, при недостатке вычислительных мощностей.

## Настройка прав доступа

Добавили возможность сохранить новую группу из уже созданной с небольшими изменениями. Теперь можно быстро настроить права доступа для множества сотрудников с похожими задачами.



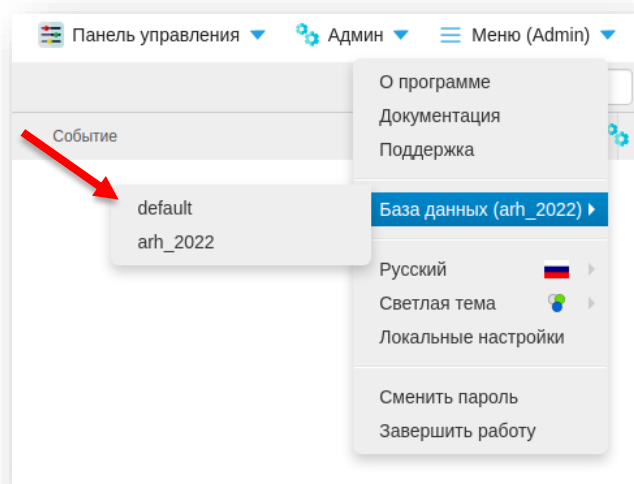
Для предустановленных групп добавили возможность восстановить исходные значения.

Загрузить значения по умолчанию    Сохранить как новый    Сохранить и продолжить

## Деление базы данных сервера

Теперь возможен переход между **архивными** «холодными» и **актуальными** «горячими» баз данных без дополнительной аутентификации.

Переход происходит в основном интерфейсе системы в меню выбора базы данных.



## Поддержка российской СУБД «Jatoba»

Используйте отечественную СУБД «Jatoba» как альтернативу свободно распространяемой PostgreSQL.

Для перенастройки на использование новой СУБД требуется воспользоваться инструкцией по использованию базы данных на другом хосте -

[https://docs.staffcop.ru/maintenance/linux\\_faq\\_db\\_another\\_host.html](https://docs.staffcop.ru/maintenance/linux_faq_db_another_host.html)

После этого на сервере СУБД «Jatoba» выполните команду

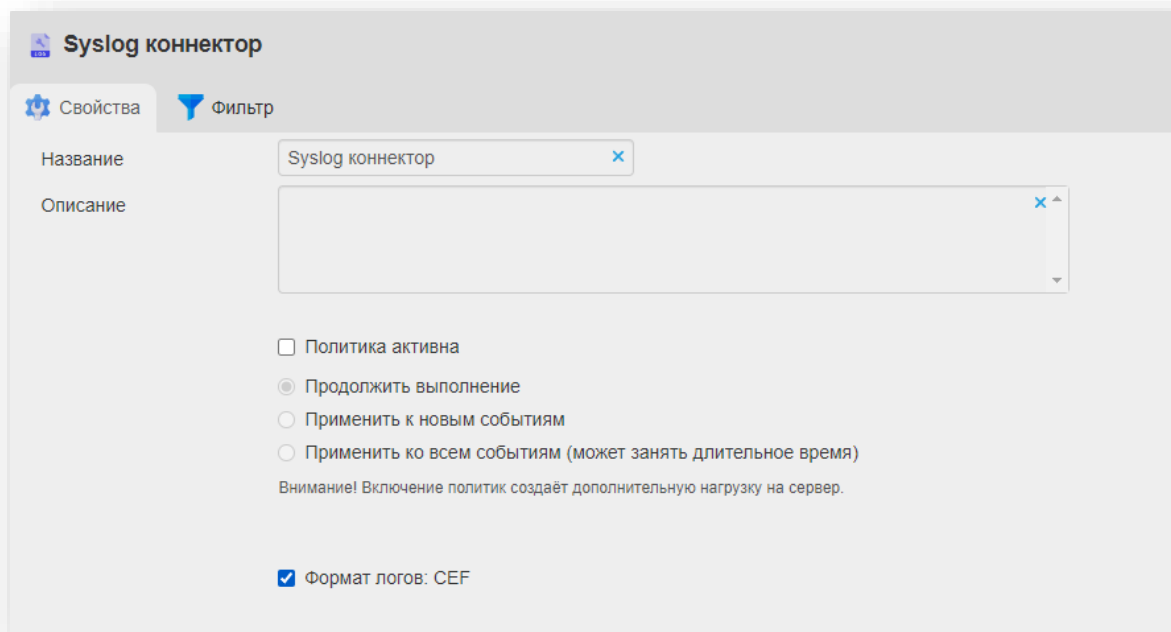
```
sudo -u postgres psql -d staffcop
```

и создайте расширение

```
CREATE EXTENSION ltree
```

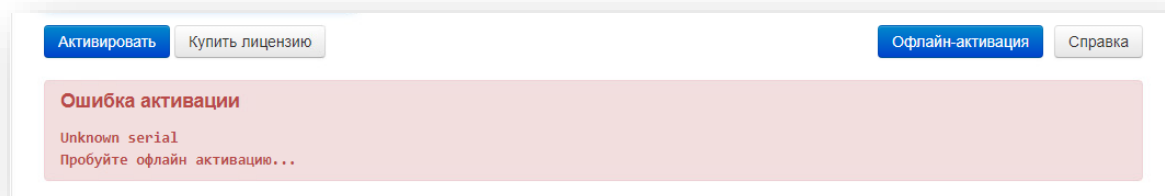
## Новые возможности передачи данных об инцидентах

С последним обновлением сервер начал передавать в формате CEF адрес сервера и исключил из передачи лишнюю информацию о HWID APМа, на котором было обнаружено событие.



## Помощь при ошибках активации

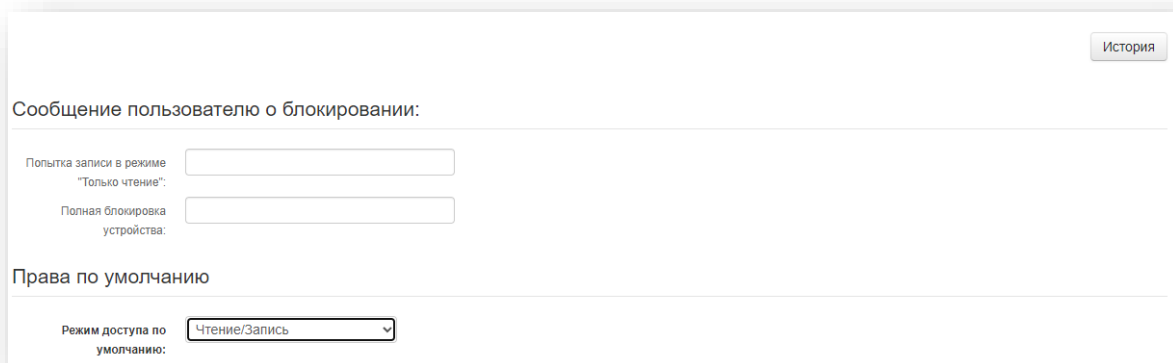
Добавили больше информации и ссылку на документацию, когда пользователь не может активировать сервер онлайн.



## Нововведения менеджера ВНИ

Изменены права доступа к незарегистрированным носителям, которые задаются по умолчанию, после включения компонента Менеджер ВНИ.

Это изменение позволит продолжать работать с носителями в том же режиме, в котором работали до включения менеджера. После активации Менеджера ВНИ настройте правила доступа, которые будут действовать для всех незарегистрированных носителей.



История

Сообщение пользователю о блокировании:

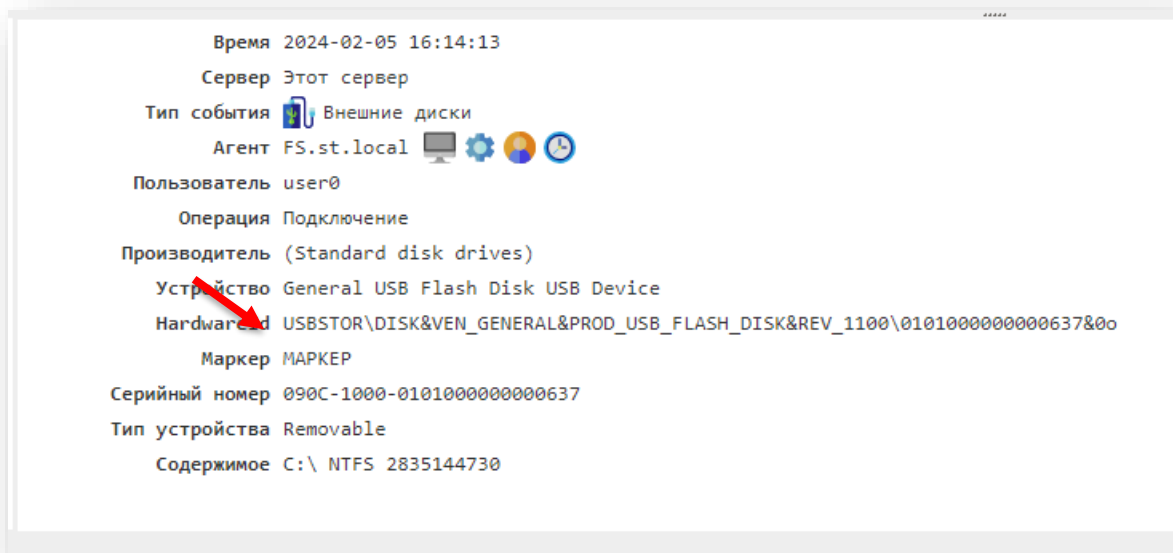
Попытка записи в режиме "Только чтение":

Полная блокировка устройства:

Права по умолчанию


Режим доступа по умолчанию:




В событии, связанном с носителем информации, теперь отображается наименование маркера ВНИ, что позволяет точнее идентифицировать инцидент.



Время 2024-02-05 16:14:13

Сервер Этот сервер

Тип события  Внешние диски


Агент FS.st.local    

Пользователь user0

Операция Подключение

Производитель (Standard disk drives)

Устройство General USB Flash Disk USB Device

HardwareId  USBSTOR\DISK&VEN\_GENERAL&PROD\_USB\_FLASH\_DISK&REV\_1100\0101000000000637&00

Маркер МАРКЕР

Серийный номер 090C-1000-0101000000000637

Тип устройства Removable

Содержимое C:\ NTFS 2835144730

Для установки маркера зайдите в интерфейс Менеджера ВНИ, выберите носитель, который требуется промаркировать, введите значение в поле Маркер ВНИ и нажмите кнопку Сохранить.

Серийный номер: 3538-0901-01AF0000000019A

Ответственный:

Маркер ВНИ:

Описание:

Режим доступа по умолчанию:

### Права

Режим доступа	Пользователь	Удалить?
6 <input type="text" value="Только чтение"/>	Олеся@WORKGROUP	<input type="checkbox"/>

Добавить еще Разрешение

### Устройства

Устройство	Label
Generic USB Flash Disk USB Device 1555 USBSTOR\DISK&VEN_GENERIC&PROD_USB_FLASH_DISK&REV_0.00\01AF0000000019A&0	Работники
Generic USB Flash Disk USB Device 1554 USB\VID_3538&PID_0901\01AF0000000019A	Работники

После этого все события связанные с маркированным носителем будут содержать указанный маркер, по которому можно будет их идентифицировать.



# Исправления

- Исправили проблемы перехвата **WhatsApp** и **Битрикс24**, проявившиеся после обновления мессенджеров.
- Решили ряд проблем, приводящих к конфликту **агента** и **Outlook**.
- Снизили нагрузку на ПК при использовании функции создания **пакетов снимков экрана**.
- Исправили проблемы, связанные с просмотром **пакетных снимков экрана**: искаженные изображения и черные кадры.
- Исправили поведение системы при выборе времени в конструкторе.
- Исправили процесс идентификации некоторых носителей информации.
- Исправили ошибки работы интерфейса и опечатки в текстах веб-консоли.

