Dr.WEB®
с 1992 года

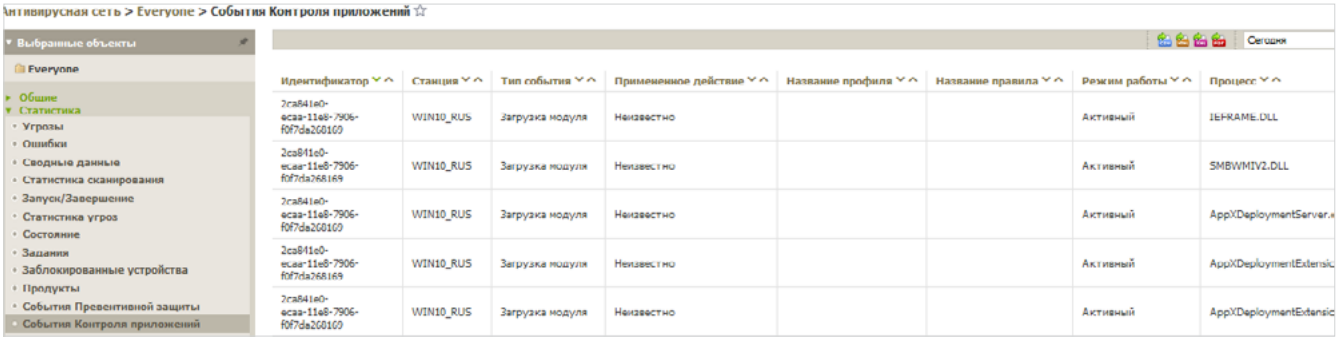
Запрет запуска программ с помощью Контроля приложений в Dr.Web Enterprise Security Suite 13.0

Dr.Web Enterprise Security Suite 13.0

Запрет запуска программ с помощью Контроля приложений

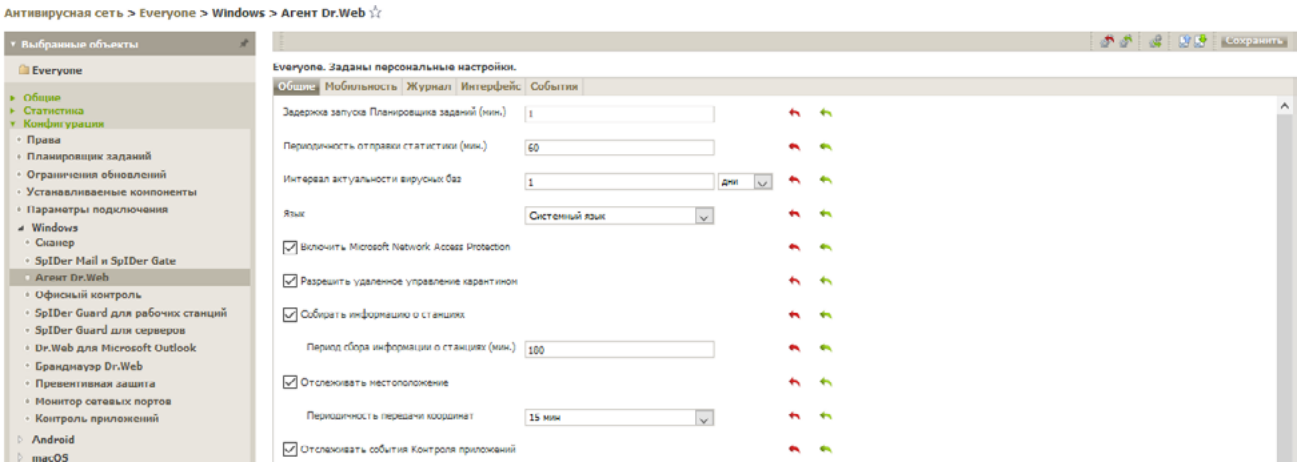
Чтобы создать правило для модуля **Контроль приложений** Центра управления Dr.Web Enterprise Security Suite, нужно иметь информацию о файле, который мы хотим блокировать. Получить такую информацию достаточно просто.

Первым этапом разрешаем сбор и отправку информации со станций для раздела **События Контроля приложений**.



1. В разделе **Антивирусная сеть** выберите в дереве станции или группы станций с установленным **Контролем приложений**, с которых вы хотите получать информацию о запуске приложений.
2. В управляющем меню выберите пункт **Windows → Агент Dr.Web**.
3. На вкладке **Общие** установите флаг **Отслеживать события Контроля приложений**, чтобы отслеживать активность процессов на станциях, зафиксированную Контролем приложений, и отправлять события на Сервер.

   Внимание! Если флаг снят, активность процессов игнорируется.

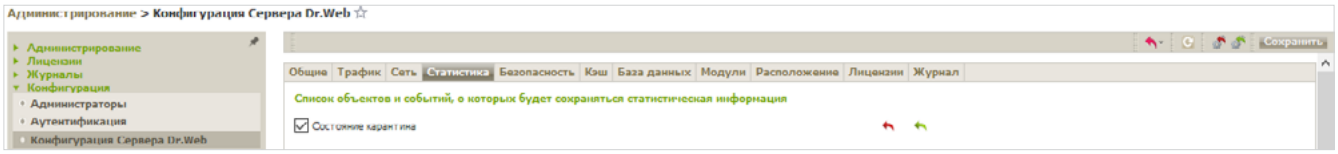


   При отсутствии подключения к Серверу события накапливаются и отправляются при подключении.

4. Нажмите **Сохранить**.

Разрешите сбор информации антивирусным сервером для раздела **События Контроля приложений**.

1. В разделе **Администрирование** → **Конфигурация Сервера Dr.Web** перейдите на вкладку **Статистика**.



2. Установите одну из следующих опций:

   - **Статистика Контроля приложений по активности процессов**, чтобы получать и записывать информацию по любой активности всех процессов: как разрешенных для запуска, так и запрещенных Контролем приложений.

     При выборе этой опции в справочник будут заноситься все приложения на станциях вне зависимости от того, созданы ли профили для контроля запуска приложений или нет.

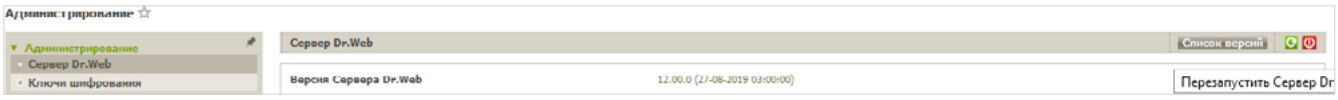
     Внимание! Установка данного флага может значительно повысить ресурсоемкость сбора статистики по всей антивирусной сети.

   - **Статистика Контроля приложений по блокировке процессов**, чтобы получать и записывать информацию по активности всех процессов, запрещенных для запуска Контролем приложений.

     При выборе этой опции в справочник будут заноситься приложения только после создания профилей, по настройкам которых запуск приложений будет блокироваться, и назначения этих профилей на станции антивирусной сети.

3. Нажмите кнопку **Сохранить**.

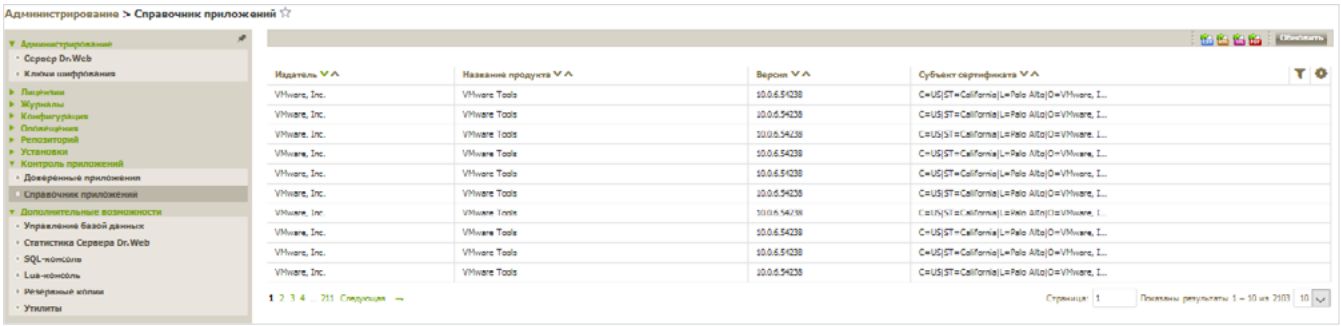
4. Перезапустите антивирусный сервер.



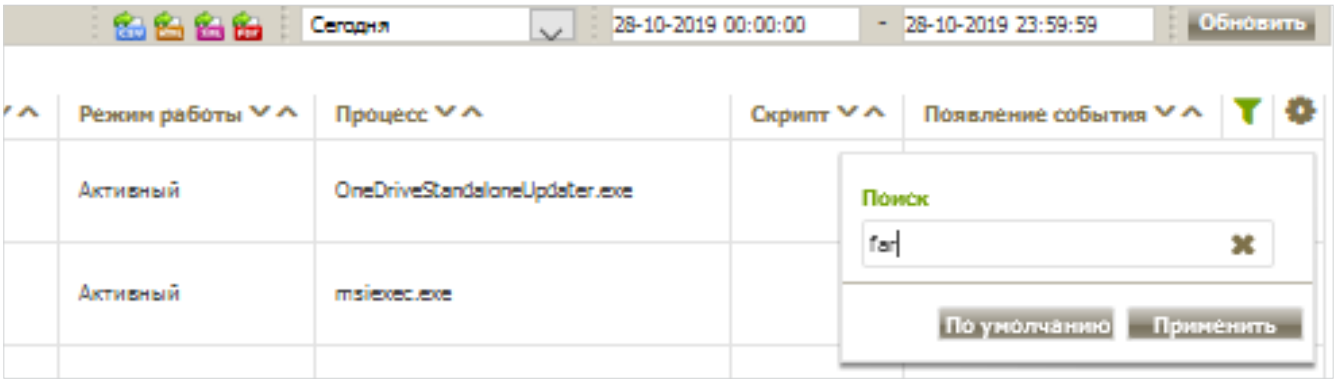
После перезагрузки Сервер начнет фиксировать всю статистику по запуску приложений, присылаемую со всех станций с установленным Контролем приложений. Информация о каждом приложении отправляется Агентом на сервер единожды при первой активности этого приложения.

Информация о запусках приложений, установленных на защищаемых станциях под ОС Windows, подключенных к антивирусному Серверу Dr.Web, фиксируется в **Справочнике приложений**.

Для просмотра справочника приложений перейдите в раздел **Администрирование** → **Контроль приложений** → **Справочник приложений**.

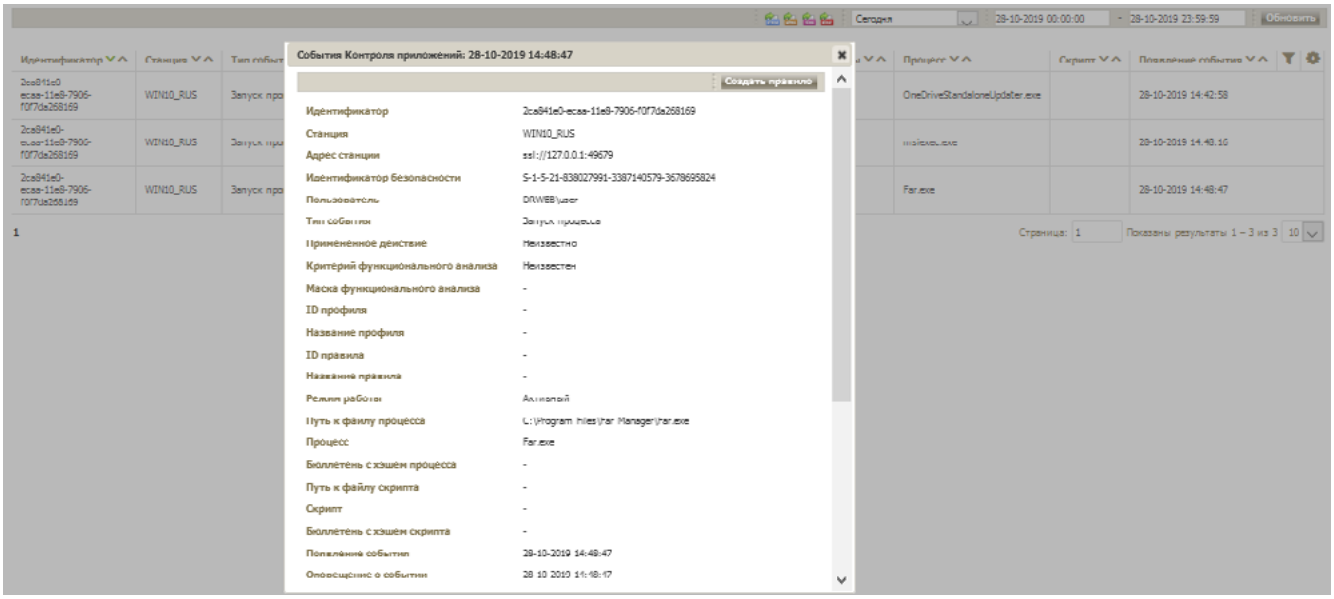


Теперь используем поиск на странице статистики.

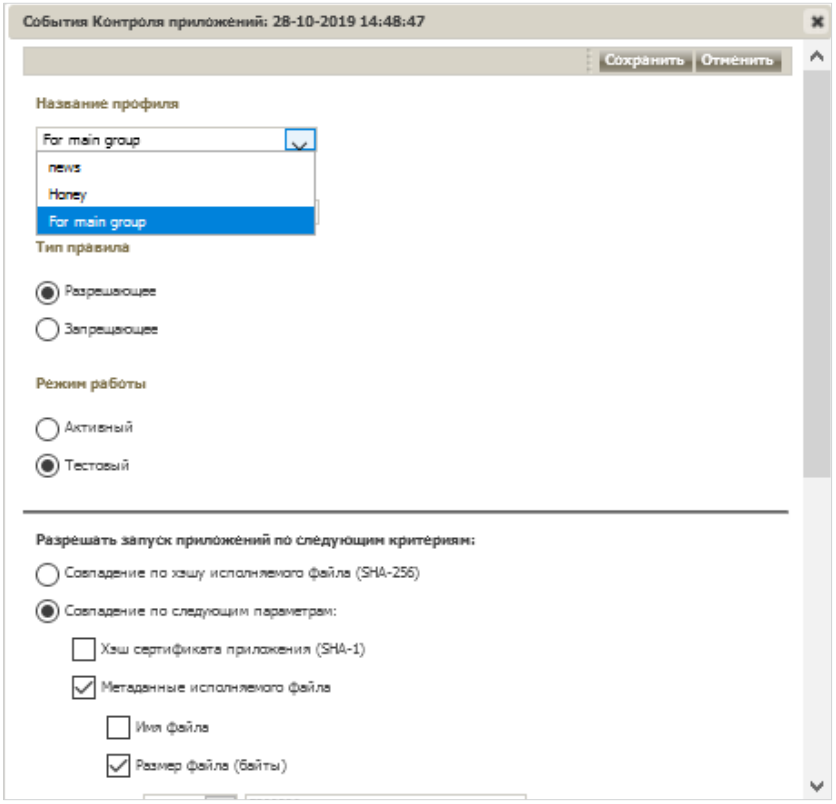


Нажмите **Применить**.

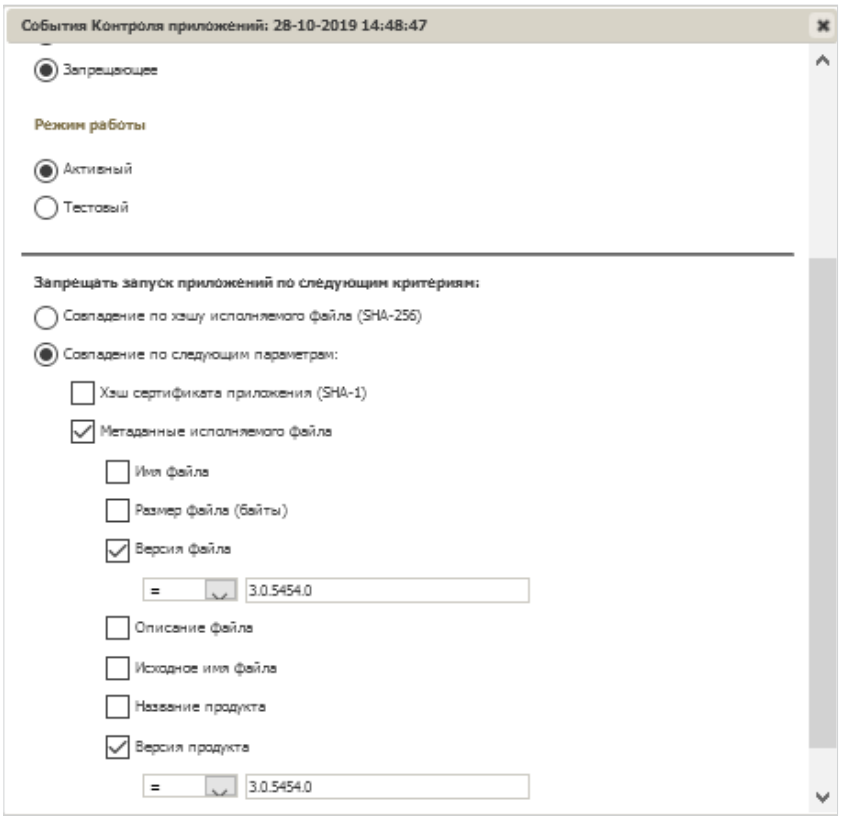
Кликните по строке с информацией о запущенной программе.



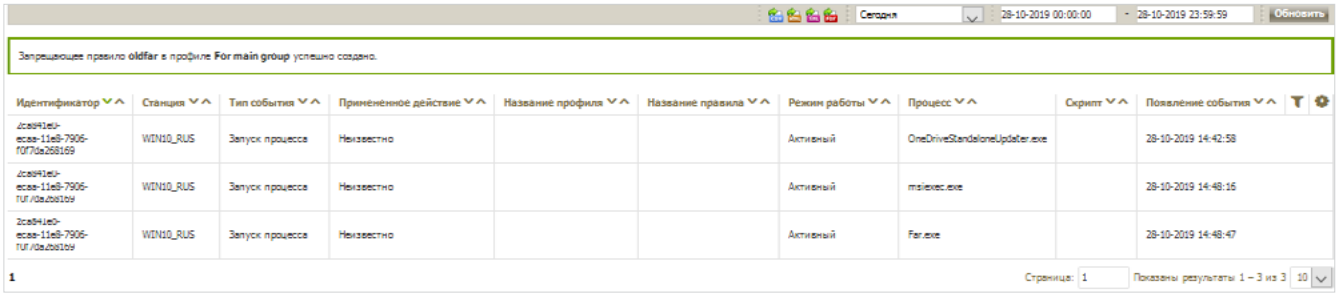
Кликните **Создать правило**.



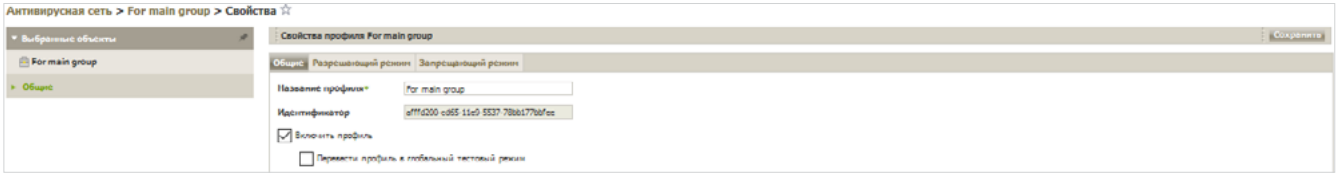
В выпадающем списке профилей выберите тот, где будете создавать запрещающее правило.



Отметьте переключатели типа правила (**Запрещающее**) и режима работы (для простоты выберем **Активный**). Выберите опции, согласно которым правило будет срабатывать. В данном случае это версия программы. Завершите создание правила.



Не забудьте, что для работы запрещающих правил в профиле должен быть отключен тестовый режим для профиля в целом и включена работа запрещающих правил.



Если эти свойства не установлены, установите их и нажмите **Сохранить**.

Проблема решена.

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании. Вот только некоторые клиенты Dr.Web: https://customers.drweb.ru.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.**

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

- «Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недекларированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.
- Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).
  Его использование позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:
  – информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
  – отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	Сертификаты Минобороны России	Сертификаты ФСБ России	Все сертификаты и товарные знаки

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789–45–87 (многоканальный) | Факс: +7 495 789–45–97
https://антивирус.рф | https://www.drweb.ru | https://curenet.drweb.ru | https://free.drweb.ru