Dr.WEB®
с 1992 года

Dr.Web Enterprise Security Suite 13.0
Запрет запуска приложений по известным контрольным суммам с помощью компонента Контроль приложений

© ООО «Доктор Веб», 2021

Dr.Web Enterprise Security Suite 13.0
Запрет запуска приложений по известным контрольным суммам с помощью компонента Контроль приложений

Цель документа

Правила компонента **Контроль приложений** Центра управления Dr.Web Enterprise Security Suite позволяют блокировать запуск приложений, загрузку драйверов и модулей, запуск MSI-пакетов и использование скриптовых интерпретаторов по большому количеству критериев. В том числе по контрольной сумме, содержащейся в рассылке (из SOC, SIEM, Фин-CERT и т. д.) или вычисленной самостоятельно. Пример создания правила блокировки по контрольной сумме и будет рассмотрен ниже.

Содержание

1. Введение 3
2. Режимы работы компонента Контроль приложений 3
3. Порядок настройки правил Контроль приложений 5
   3.1. Создание профиля Контроль приложений 5
   3.2. Включение и первичная настройка профиля Контроль приложений с использованием Запрещающего режима 6
   3.3. Назначение станций, групп станций или пользователей профилю Контроль приложений 7
4. Создание правила Запрещающего режима компонента Контроль приложений на основе контрольной суммы 8

1. Введение

Пример одной из рассылок, содержащих информацию о вредоносных файлах, в частности их контрольные суммы:

MD5	16E627C2696B20810201EDD95175C15E
SHA1	B818F08695CA25B3A8C65374C7B13AFF904D8B73
SHA256	7FAA42F5017E61E354ADB737A0EC82D4DC0AE52B2F87B8A36105416A99AEF89
Размер файла (байт)	104448

В случае получения такой рассылки системный администратор не может знать, имеется ли в вирусных базах его антивируса информация о данном вредоносном файле, — самого вредоносного файла у него, естественно, нет.

Примечание. Вирусные базы содержат записи — информацию, позволяющую идентифицировать вредоносный файл и обезвредить его. Это могут быть как сигнатуры (характерные участки кода вредоносных программ), так и специальные процедуры, исполняемые в целях обнаружения вредоносного кода. Вирусные базы не содержат контрольные суммы файлов (как и самих вредоносных файлов), так как их нужно дополнительно высчитывать, что увеличит время проверки. Более подробно с технологиями, используемыми для обнаружения угроз различных типов, можно ознакомиться в разделе документации «Методы обнаружения угроз».

2. Режимы работы компонента Контроль приложений

Внимание!

Если используется Запрещающий режим, то по умолчанию запуск любых приложений разрешен. Блокировка запуска производится добавлением правил Запрещающего режима.

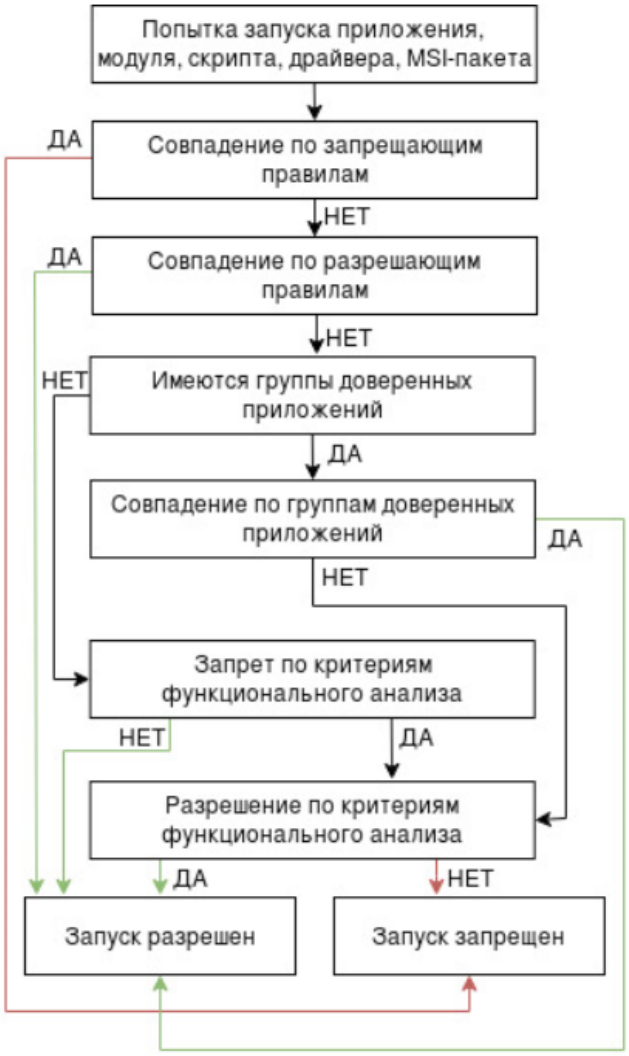
Если используется Разрешающий режим, то по умолчанию запуск любых приложений запрещен – его нужно разрешить. Разрешение запуска производится добавлением правил Разрешающего режима и использованием базы данных доверенных приложений (назначением групп доверенных приложений в разделе разрешающего режима).

Если используется одновременно как Разрешающий, так и Запрещающий режим и не используются базы данных доверенных приложений, то Контролем приложений по умолчанию будет разрешен запуск любых приложений. Блокировка запуска производится добавлением правил Запрещающего режима и Разрешающего режима, при этом разрешающие правила будут действовать как дополнение к правилам Запрещающего режима.

Если разрешено использование как Разрешающего, так и Запрещающего режима и используются базы данных, содержащие хеши доверенных приложений, то Контролем приложений будет запрещен запуск любых приложений, кроме приложений из баз данных. Допол-

нительно разрешения могут быть добавлены правилами Разрешающего режима. Правила Запрещающего режима будут блокировать запуск, даже если соответствующие разрешения есть в базе данных или разрешающих правилах. Контролем приложений будет разрешено запустить или использовать только то, что явно разрешено и еще не заблокировано запрещающими правилами.

Критерии функционального анализа Контроля приложений анализируются, только если ни запрещающие, ни разрешающие правила не нашли совпадений с анализируемым файлом.



Правила распространяются на станции, группы станций, локальных пользователей станции, пользователей Active Directory, назначенных на профиль с данным правилом. Если необходимо, чтобы некое правило было назначено на определенную станцию, данную станцию нужно назначить для профиля, содержащего это правило.

Чтобы заблокировать вредоносные файлы, о которых известно только из рассылок, можно использовать возможности Запрещающего режима компонента **Контроль приложений** Центра управления Dr.Web Enterprise Security Suite.

Режим блокировки по имени файла, контрольным суммам, сертификату и другим признакам файла также может быть полезен, когда необходимо заблокировать конкретное приложение. Наиболее гибкой и надежной является блокировка по имени файла и сертификату.

Настройки системы контроля приложений осуществляются с помощью профилей, в соответствии с которыми приложения на станциях будут запускаться или блокироваться.

Профили создаются администратором и назначаются конкретным станциям, группам станций или отдельным пользователям (локальным или пользователям Active Directory). Профили определяют режим работы Контроля приложений.

3. Порядок настройки правил Контроля приложений

Активируйте сбор и отправку событий Контроля приложений с защищаемых рабочих станций.

1. Разрешите сбор и отправку информации со станций для раздела **События Контроля приложений**, установив флаг **Отслеживать события Контроля приложений** на вкладке **Общие** компонента **Агент Dr.Web** для станций или группы станций с установленным **Контролем приложений**, с которых вы хотите получать информацию о запуске приложений.
2. Разрешите сбор информации антивирусным сервером для раздела **События Контроля приложений**, установив флаги **Статистика Контроля приложений по активности процессов** и **Статистика Контроля приложений по блокировке процессов** в разделе **Администрирование → Конфигурация Сервера Dr.Web** на вкладке **Статистика**.
3. Перезапустите антивирусный сервер.

Выполните следующую последовательность действий.

1. Создайте профиль.

До создания профилей и назначения их на станции антивирусной сети запуск всех приложений разрешается.

2. Задайте настройки профиля.
3. Назначьте станции, пользователей и группы, на которых будут распространяться настройки созданного профиля.

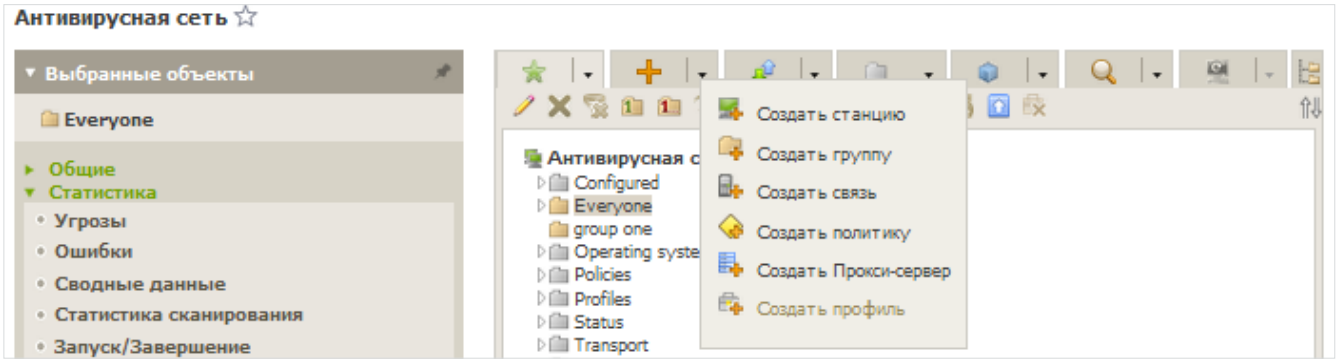
Внимание! Настройку работы профилей рекомендуется производить в тестовом режиме. Он имитирует работу Контроля приложений с полным ведением журнала статистики активности на защищаемых станциях, однако фактическая блокировка приложений не производится.

Не рекомендуется устанавливать слишком долгий тестовый период. После короткой проверки созданного правила или группы правил следует перевести как правила, так и профиль в целом в активный режим, поскольку в противном случае возникает риск пропуска вредоносного файла, правило на которого заведено в системе ранее.

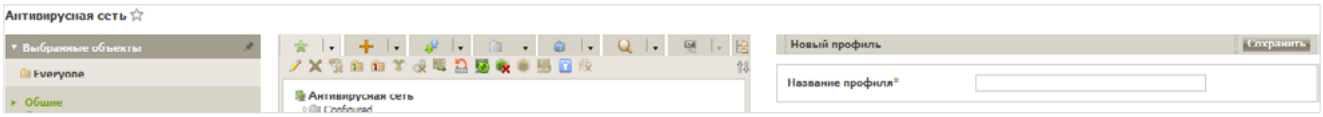
3.1. Создание профиля Контроль приложений

Чтобы создать профиль

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне на панели инструментов выберите пункт **Добавить объект сети → Создать профиль**.



3. На открывшейся панели задайте **Название профиля**.



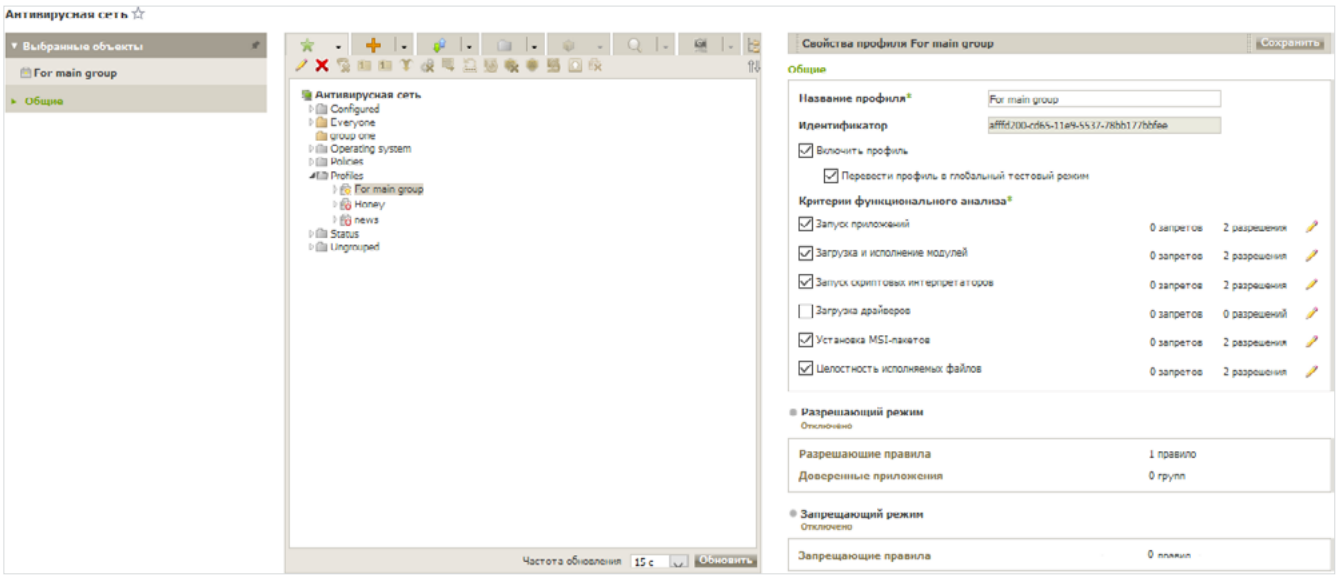
4. Нажмите кнопку **Сохранить**.

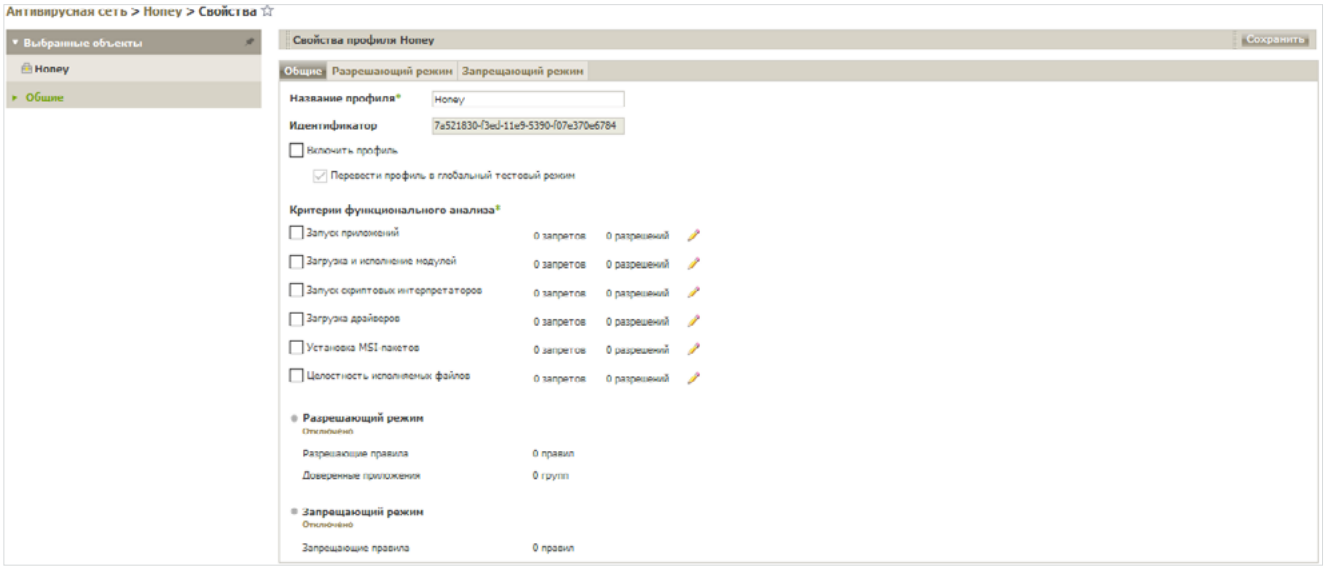
5. Новый профиль будет создан и помещен в группу **Profiles** дерева Антивирусной сети.

3.2. Включение и первичная настройка профиля Контроль приложений с использованием Запрещающего режима

После создания профиля его нужно настроить (установить нужные ограничения, правила работы), а затем назначить станциям и/или пользователям антивирусной сети (локальным и Active Directory).

1. В дереве **Антивирусная сеть** в главном меню Центра управления нажмите на название профиля в иерархическом списке антивирусной сети (в правой части окна Центра управления автоматически откроется панель со свойствами профиля), нажмите на иконку профиля в дереве Антивирусной сети или выберите профиль и затем пункт **Свойства** управляющего меню (откроется окно со свойствами профиля).





2. Установите флаг **Включить профиль**, чтобы начать использовать этот профиль. По умолчанию установлен флаг **Перевести профиль в глобальный тестовый режим** – это означает, что все настройки профиля будут применены к станциям/пользователям, но никакие действия по блокировке не будут применяться: будет осуществляться только запись журнала активности как при включенных настройках.
3. Чтобы применить настройки, заданные в окне настроек профиля **Общие**, нажмите **Сохранить**.

Вы не сможете сохранить профиль (ни один из критериев не включен – профиль не сохранится):

- если не включен ни один критерий в разделе Критерии функционального анализа, то сам профиль будет отключен;
- если при задании настроек профиля ни для одного из критериев в разделе Критерии функционального анализа не заданы расширенные настройки и отключены Запрещающий и Разрешающий режимы, то данная конфигурация настроек не будет сохранена;
- если не заданы ни разрешающие правила, ни доверенные приложения, разрешающий режим будет отключен;
- если не заданы запрещающие правила, запрещающий режим будет отключен.

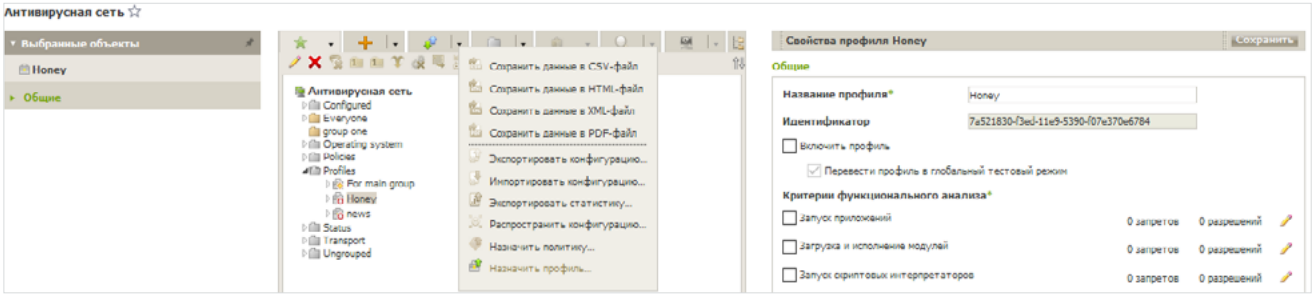
4. Чтобы включить Запрещающий режим, перейдите в раздел **Запрещающий режим**.
    1. Чтобы использовать запрещающий режим, установите флаг **Использовать запрещающий режим** на вкладке **Запрещающий режим**.
    2. Нажмите **Сохранить**.

3.3. Назначение станций, групп станций или пользователей профилю Контроль приложений

Завершающим этапом настройки системы контроля запуска приложений является назначение созданного и настроенного профиля станциям и/или пользователям.

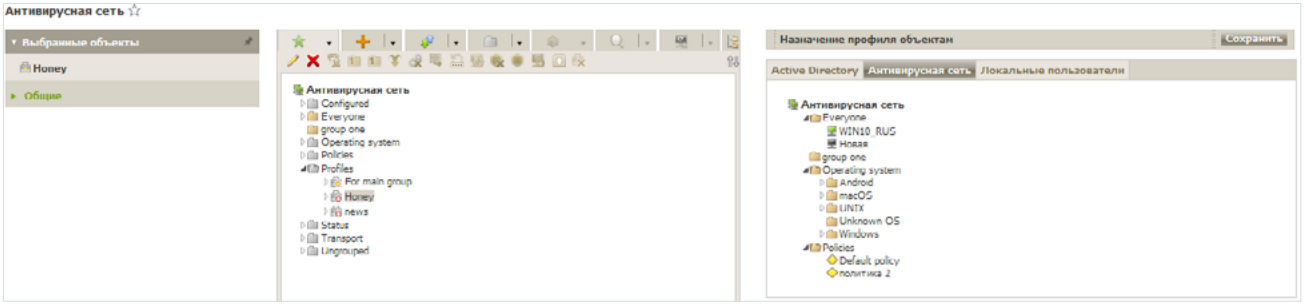
1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне в иерархическом списке выберите профиль, который вы хотите назначить.

3. На панели инструментов нажмите **Экспортировать данные** → **Назначить профиль**.



4. В открывшемся окне выберите объект, который будет назначен на профиль. Если мы рассматриваем случай глобального запрета на исполнение вредоносного кода, то наиболее логично назначить данное ограничение на все станции антивирусной сети или всех ее пользователей.

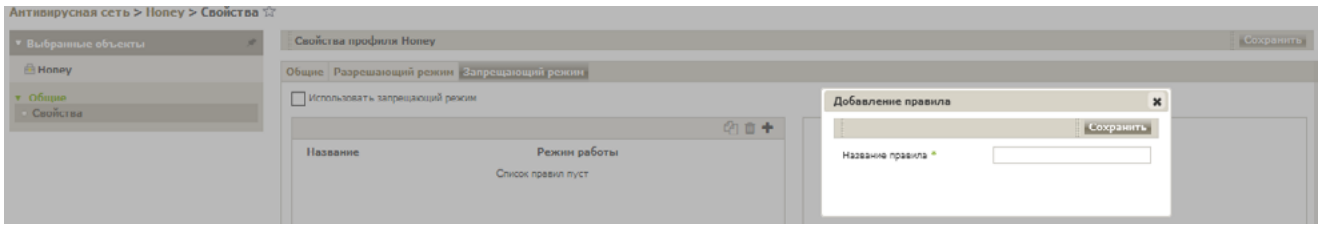
   На вкладке **Антивирусная сеть** вы можете выбрать группы станций (настройки будут распространяться на учетные записи всех пользователей всех станций, входящих в данные группы) или отдельные станции в группах (настройки будут распространяться на учетные записи всех пользователей выбранных станций).



5. Нажмите кнопку **Сохранить**. Все выбранные объекты будут добавлены в список, на который распространяется настраиваемый профиль, и будут отображены в дереве как вложенные объекты настраиваемого профиля.

4. Создание правила Запрещающего режима компонента Контроль приложений с использованием контрольной суммы

1. Чтобы настроить правила Запрещающего режима, перейдите в данный раздел.
2. Создайте запрещающее правило.
   a. Нажмите кнопку ➕ (**Создать правило**).
   b. В окне **Добавление** правила задайте **Название правила**.

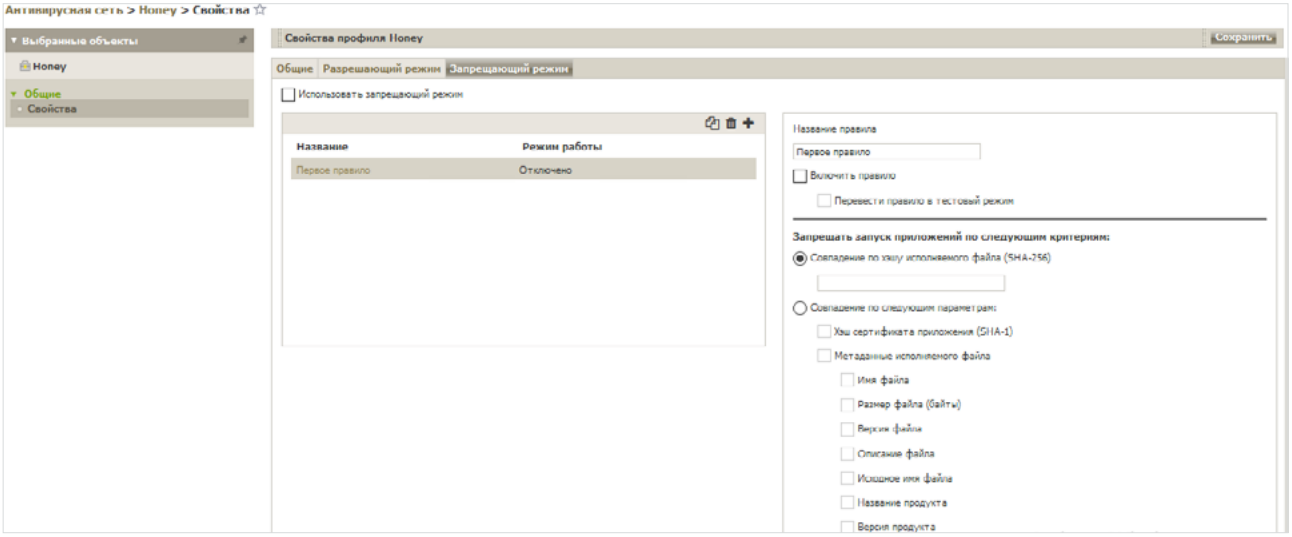


   c. Нажмите **Сохранить**.

Если ранее вы создавали правило, то вы можете создать дубликат запрещающего правила и отредактировать его свойства.

1. Выберите правило, которое вы хотите продублировать для этого профиля.
2. Нажмите кнопку (**Дублировать правило**).
3. В таблице правил появится новое правило, настройки которого будут полностью скопированы из правила, выбранного на шаге 1. В имени правила добавится цифра **1**.

3. В списке правил выберите созданное правило и задайте его настройки на открывшейся панели свойств — в данном примере укажите контрольную сумму вредоносного файла в соответствии с требуемым форматом.
   a. В разделе **Запрещать запуск приложений по следующим критериям** укажите контрольную сумму вредоносного файла.



   b. Нажмите **Сохранить**.

4. В списке правил выберите созданное правило и установите флаг **Включить правило** на открывшейся панели свойств, чтобы начать его использовать.

   Если вы хотите проверить работу правила без его фактического исполнения, установите флаг **Перевести правило в тестовый режим**. В противном случае правило будет работать в активном режиме с блокировкой приложений по заданным настройкам правила.

   Нажмите **Сохранить**.

5. Для сохранения свойств правила нажмите **Сохранить**.

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: 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.

© ООО «Доктор Веб», 2003–2021

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