Dr.WEB®
с 1992 года

Запрет запуска приложений по известным контрольным суммам с помощью Контроля приложений в Dr.Web Enterprise Security Suite 12.0

Dr.Web Enterprise Security Suite 12.0

Запрет запуска приложений по известным контрольным суммам с помощью Контроля приложений

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

MD5	16E627C2696B20810201EDD95175C15E
SHA1	B818F08695CA25B3A8C65374C7B13AFF904D8B73
SHA256	7FAA42F5017E61E354ADB737A0EC82D4DC0AE52B287B8A36105416A99AEF89
Размер файла (байт)	104448

В случае получения такой рассылки (например, из SOC, SIEM, ФинЦЕРТ и т. д.) системный администратор не может знать, имеется ли в антивирусных базах его антивируса информация о данном вредоносном файле, — самого вредоносного файла у него, естественно, нет.

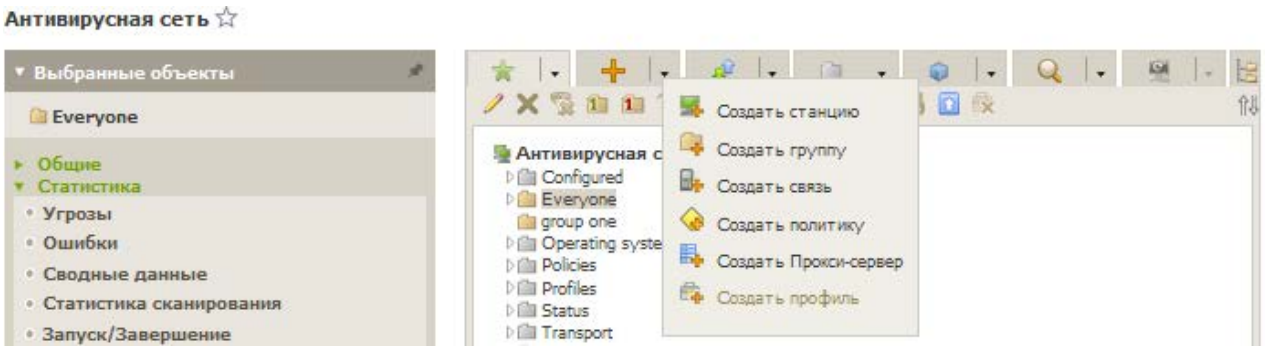
Примечание. Антивирусные базы содержат в себе записи — информацию, позволяющую идентифицировать вредоносный файл и обезвредить его. Это могут быть как сигнатуры — характерные участки кода вредоносных программ, так и специальные процедуры, исполняемые в целях обнаружения вредоносного кода. Антивирусные базы не содержат в себе контрольные суммы файлов, так как их нужно дополнительно высчитывать, что увеличит время проверки.

Для того чтобы блокировать вредоносные файлы, о которых известно только из рассылок, можно использовать функционал модуля **Контроль приложений** Центра управления Dr.Web Enterprise Suite.

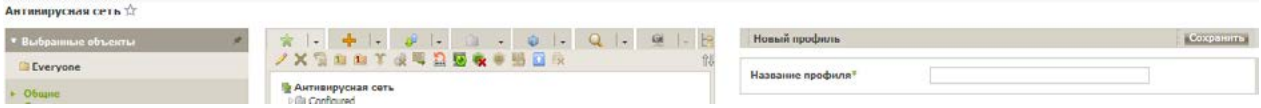
Настройки системы контроля приложений осуществляются с помощью профилей, в соответствии с настройками которых приложения на станциях (или для определенных пользователей) будут запускаться или блокироваться.

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**.

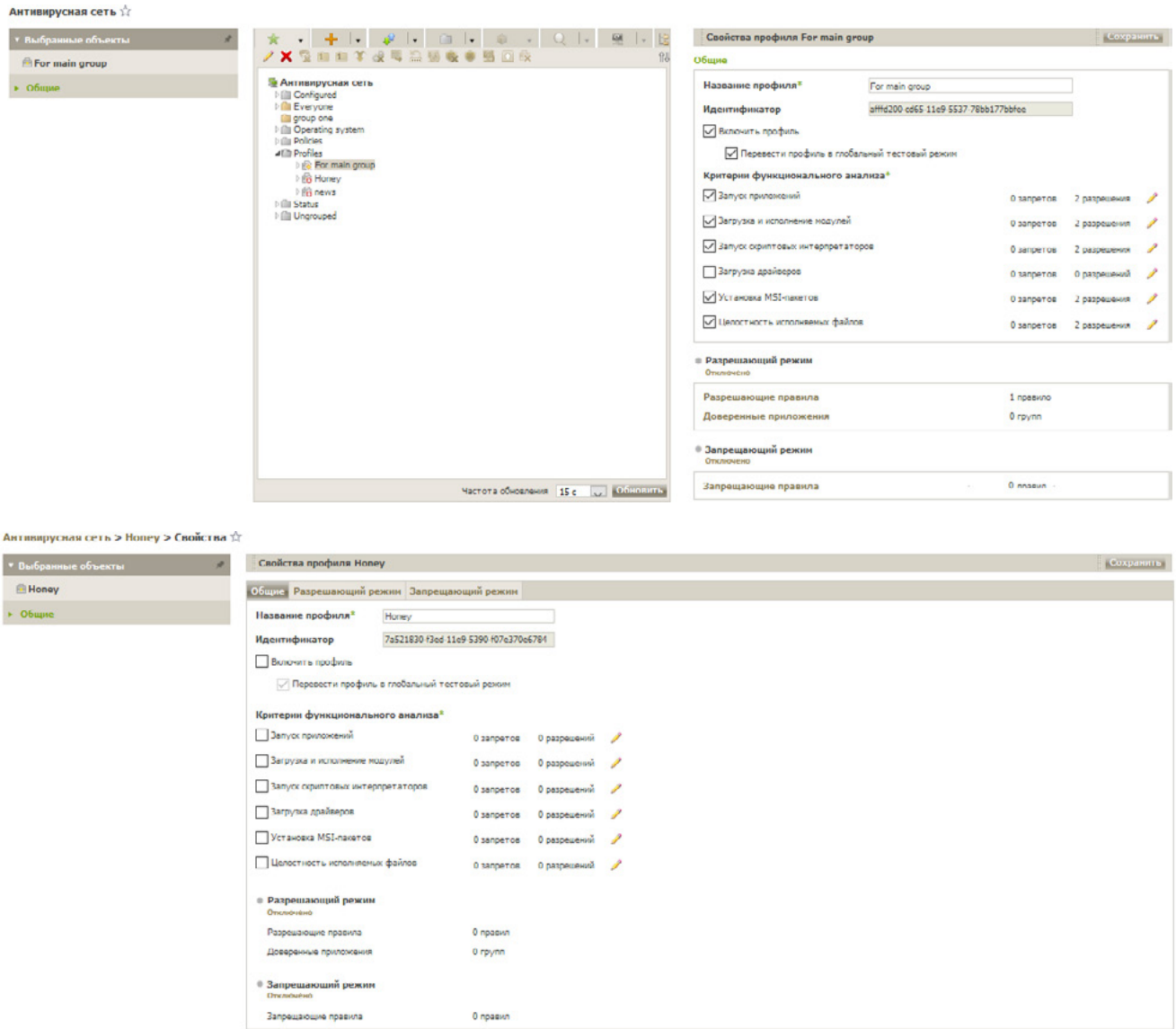


4. Нажмите кнопку **Сохранить**.

5. Новый профиль будет создан и помещен в группу **Profiles** дерева Антивирусной сети. После создания профиля его нужно настроить (установить нужные ограничения, правила работы), а также назначить станциям и пользователям антивирусной сети.

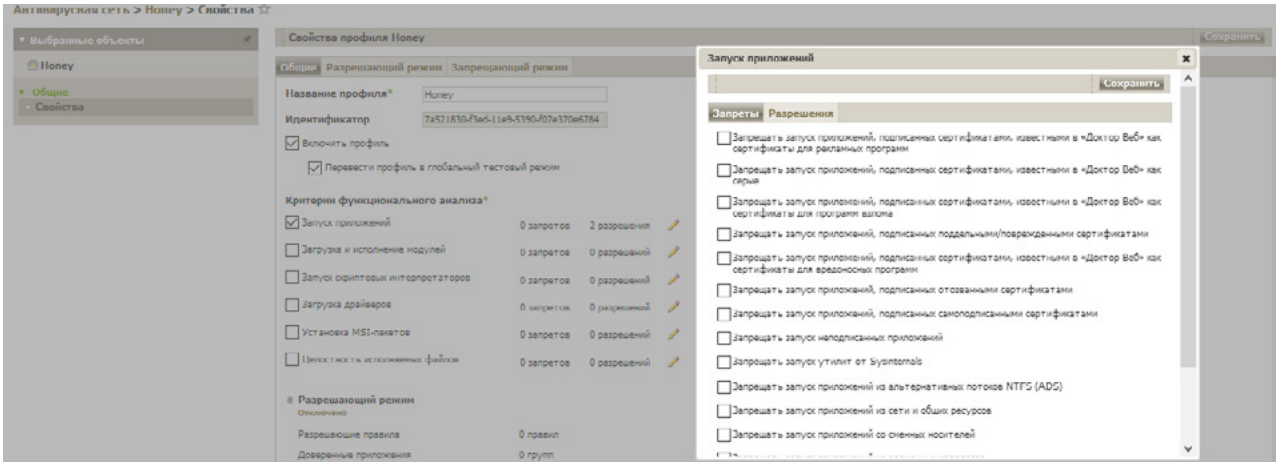
Внимание! Настройку работы профилей рекомендуется производить в тестовом режиме. Тестовый режим имитирует работу Контроля приложений с полным ведением журнала статистики активности на защищаемых станциях, однако фактическая блокировка приложений не производится.

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), или нажмите на иконку профиля в дереве антивирусной сети, или выберите профиль и затем выберите пункт **Свойства** управляющего меню (откроется окно со свойствами профиля).



2. Установите флаг **Включить профиль**, чтобы начать использовать этот профиль. Если установлен флаг **Перевести профиль в глобальный тестовый режим**, все настройки профиля не будут применяться к станциям, однако будет осуществляться запись журнала активности как при включенных настройках.
3. В разделе **Критерии функционального анализа** установите флаги для событий, которые вы хотите отслеживать.

Для задания расширенных настроек по каждому выбранному типу событий критерию нажмите (**Редактировать**) напротив соответствующего типа событий. Откроется окно со списком настроек.



Установите флаги для тех настроек, которые должны выполняться.

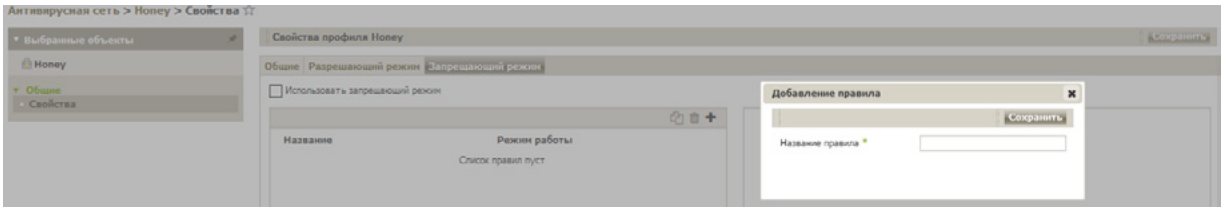
Если вы включите использование какого-либо из типов событий, но не зададите его расширенные настройки, то контроль запуска будет производиться для всех объектов по этому критерию в соответствии с настройками разрешающего или запрещающего режимов. Если вы зададите расширенные настройки, но не включите использование самого типа события, то ни расширенные настройки, ни сам критерий выполняться не будут.

Для сохранения расширенных настроек нажмите **Сохранить** в окне со списком расширенных настроек.

4. Чтобы применить настройки, заданные в разделе **Общие**, нажмите **Сохранить** в настройках профиля.
5. **Запрещающий режим** подразумевает, что на всех контролируемых станциях запрещается запуск только тех приложений, которые соответствуют запрещающим правилам. Все остальные приложения разрешаются.

   Чтобы включить или отключить режим, а также настроить правила, перейдите в раздел **Запрещающий режим** для перехода в соответствующий раздел.

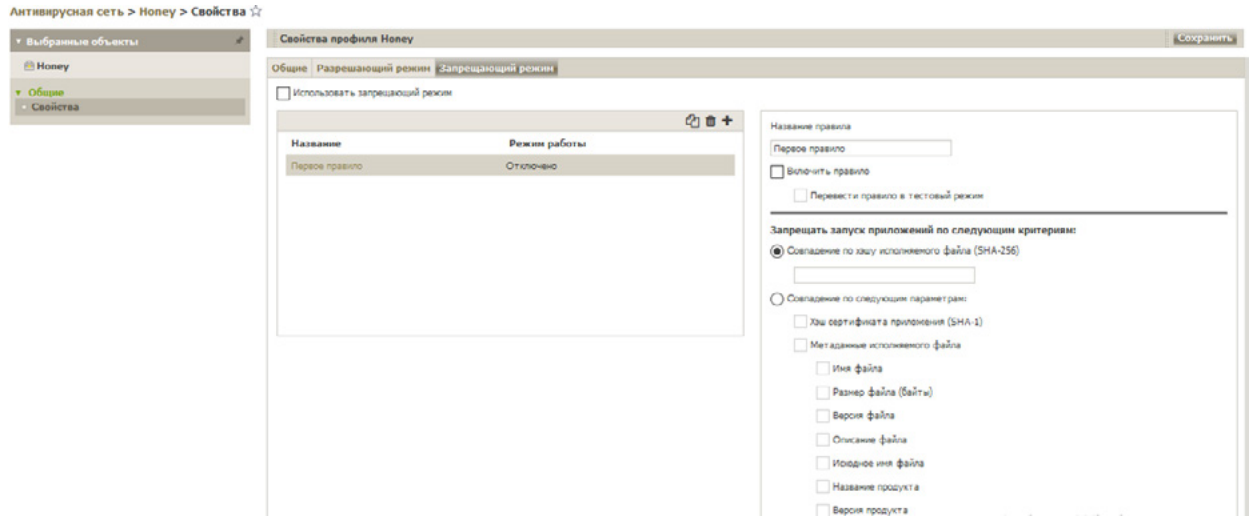
   1. Чтобы использовать запрещающий режим, установите флаг **Использовать запрещающий режим** на вкладке **Запрещающий режим**.
   2. Создайте запрещающие правила.
      a. Нажмите кнопку (**Создать правило**).
      b. В окне **Добавление правила** задайте **Название правила**.



      c. Нажмите **Сохранить**.
   3. В списке правил выберите созданное правило и задайте его настройки на открывшейся панели свойств — в данном примере укажите контрольную сумму вредоносного файла.
      a. Установите флаг **Включить правило**, чтобы начать использовать правило.

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

c. В разделе **Запрещать запуск приложений по следующим критериям** укажите контрольную сумму вредоносного файла.



d. Нажмите **Сохранить**.

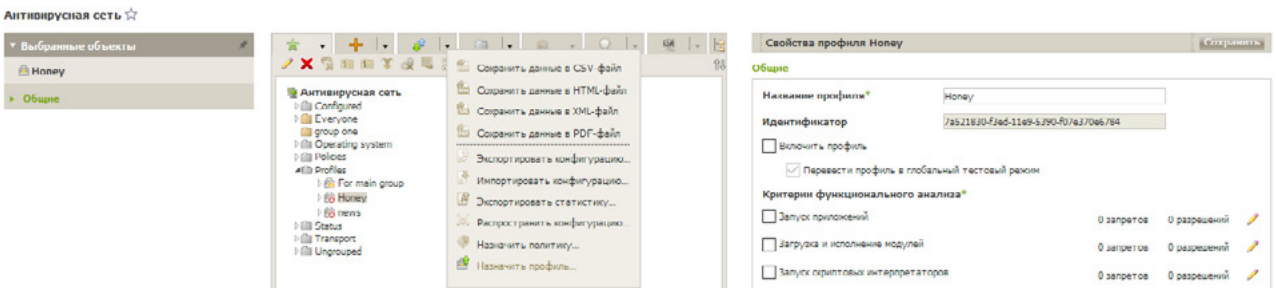
4. Нажмите **Сохранить**.

Если вы ранее 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**.

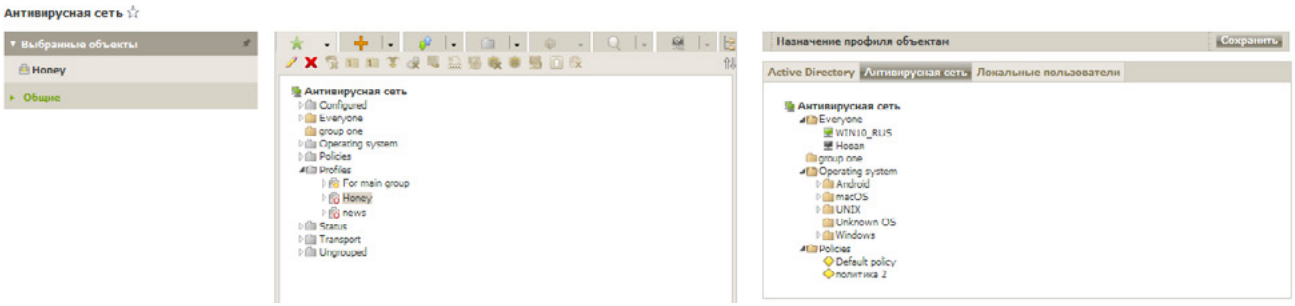
Завершающим этапом настройки системы контроля запуска приложений является назначение созданного и настроенного профиля станциям или пользователям антивирусной сети.

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. Выберите объект распространения настроек в открывшемся окне. Если мы рассматриваем случай глобального запрета на исполнение вредоносного кода, то наиболее логично назначить данное ограничение на все станции антивирусной сети.

   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.

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.com.

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.

125040, 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