



# Возможности модуля Контроль приложений в Dr.Web Enterprise Security Suite 12.0



# Dr.Web Enterprise Security Suite 12.0

## Возможности модуля Контроль приложений

**Внимание!** Перед началом процедуры обновления рекомендуется изучить соответствующие разделы документации по продукту Dr.Web Enterprise Security Suite 12.

### Содержание

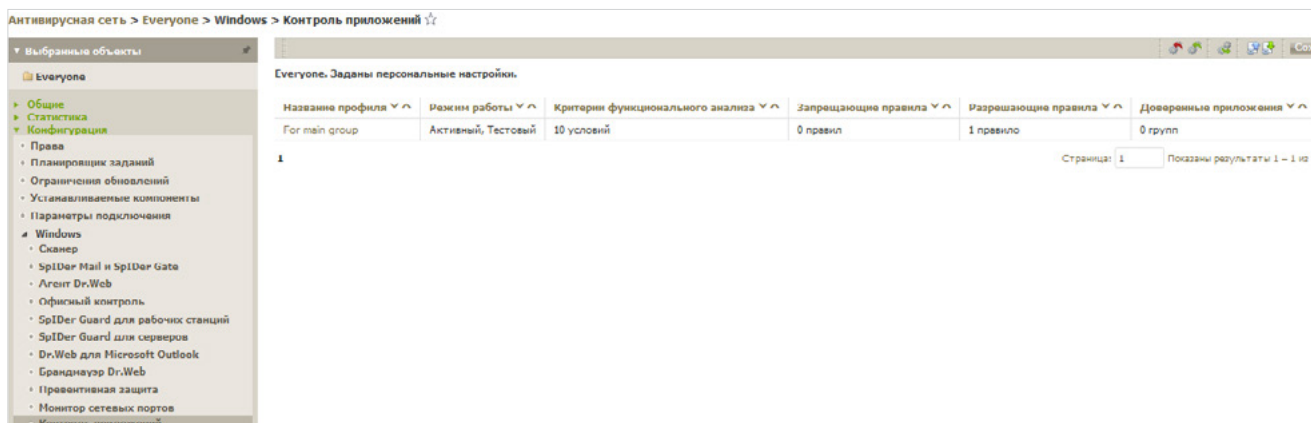
1.	Назначение и порядок настройки модуля.....	3
1.1.	Настройка состава статистики активности на защищаемых станциях.....	3
1.2.	Создание Профиля Контроля приложений.....	5
1.3.	Определение списка доверенных приложений.....	7
1.4.	Установка режима работы Профиля Контроля приложений.....	9
1.5.	Настройка Профиля Контроля приложений.....	15
1.5.1.	Создание правила на основе данных журнала активности.....	15
1.5.2.	Создание правила на основе данных справочника приложений.....	16
1.6.	Назначение Профиля защищаемым объектам.....	18
2.	Просмотр статистики активности на защищаемых станциях.....	20

## 1. Назначение и порядок настройки модуля

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

Данный модуль осуществляет мониторинг активности всех запущенных процессов на защищаемых станциях антивирусной сети. **Контроль приложений** позволяет системному администратору (или специалисту безопасности) регулировать, какие приложения разрешать, а какие — запрещать запускать на защищаемых станциях — станциях, на которых установлен Агент Dr.Web для Windows.

Наличие модуля **Контроль приложений** зависит от типа защищаемой операционной системы.



**Внимание!** Настройка модуля **Контроль приложений** производится только со стороны Центра управления — возможности настройки модуля со стороны станций, на которых установлен Агент Dr.Web, отсутствуют.

Чтобы настроить **Контроль приложений**, необходимо выполнить следующую последовательность действий.

1. Создайте профиль.

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

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

3. Задайте настройки профиля.

**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.

### 1.1. Настройка состава статистики активности на защищаемых станциях

Разрешите сбор и отправку информации со станций для раздела **События Контроля приложений**.

Антивирусная сеть > Everyone > События Контроля приложений

Идентификатор	Станция	Тип события	Примененное действие	Название профиля	Название правила	Режим работы	Процесс
2ca841e0-aca8-11e8-7906-f07da268169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	IFFRAMP.DLL
2ca841e0-eca8-11e8-7906-f07da268169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	SMBWMI2.DLL
2ca841e0-eca8-11e8-7906-f07da268169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	AppXDeploymentService
2ca841e0-aca8-11e8-7906-f07da268169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	AppXDeploymentExtension
2ca841e0-eca8-11e8-7906-f07da268169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	AppXDeploymentExtension

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.

Антивирусная сеть > Everyone > Windows > Агент Dr.Web

Everyone. Заданы персональные настройки.

Общие | Мобильность | Журнал | Интерфейс | События

Задержка запуска Планировщика заданий (мин.)  [red] [green]

Периодичность отправки статистики (мин.)  [red] [green]

Интервал актуальности вирусных баз  дни [red] [green]

Язык  [red] [green]

Включить Microsoft Network Access Protection [red] [green]

Разрешить удаленное управление карантинем [red] [green]

Собирать информацию о станциях [red] [green]

Период сбора информации о станциях (мин.)  [red] [green]

Отслеживать местоположение [red] [green]

Периодичность передачи координат  мин [red] [green]

Отслеживать события Контроля приложений [red] [green]

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**.

Администрирование > Конфигурация Сервера Dr.Web

Общие | Трафик | Сеть | Статистика | Безопасность | Юз | База данных | Модули | Расположение | Лицензии | Журнал

Список объектов и событий, в которых будет сохраняться статистическая информация

Службные карантинные [red] [green]

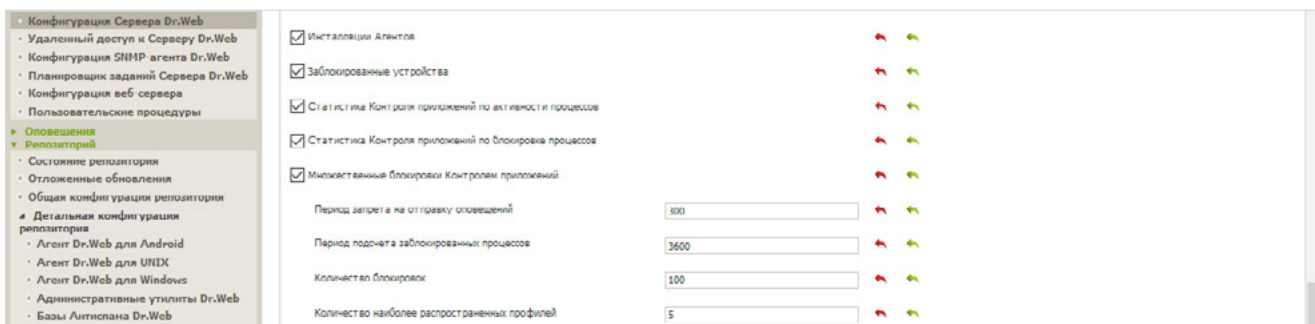
2. Установите одну из следующих опций:
  - **Статистика Контроля приложений по активности процессов**, чтобы получать и записывать информацию по любой активности всех процессов: как разрешенных для запуска, так и запрещенных Контролем приложений.

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.

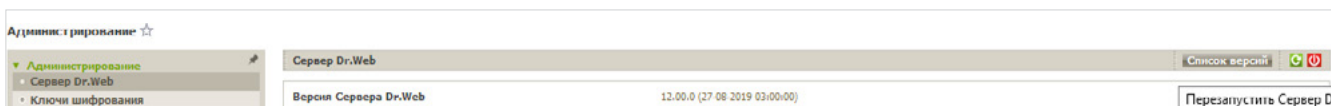
- **Статистика Контроля приложений по блокировке процессов**, чтобы получать и записывать информацию по активности всех процессов, запрещенных для запуска Контролем приложений.

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**.

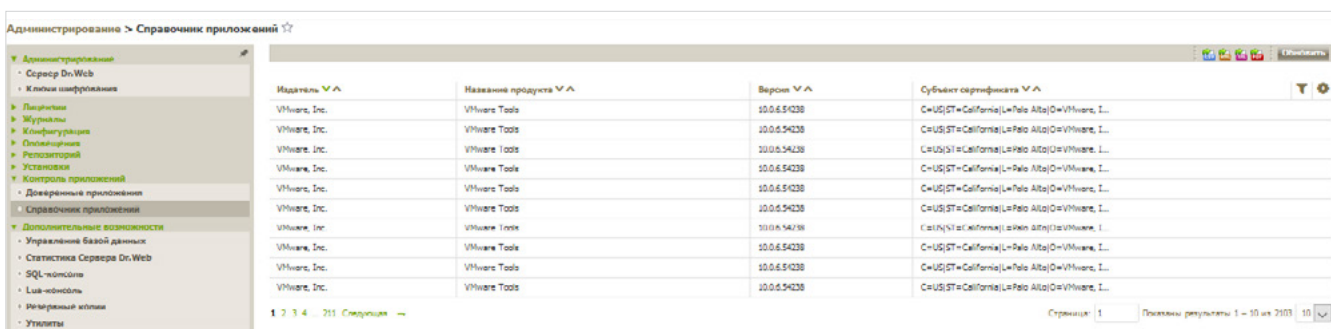
4. Перезапустите антивирусный сервер.



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 единой порцией 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**.



Справочник может быть использован для создания запрещающих и разрешающих правил Контроля приложений. Использование справочника упрощает процесс создания правил, поскольку вся информация о приложении заполняется автоматически на основе данных о выбранном известном приложении.

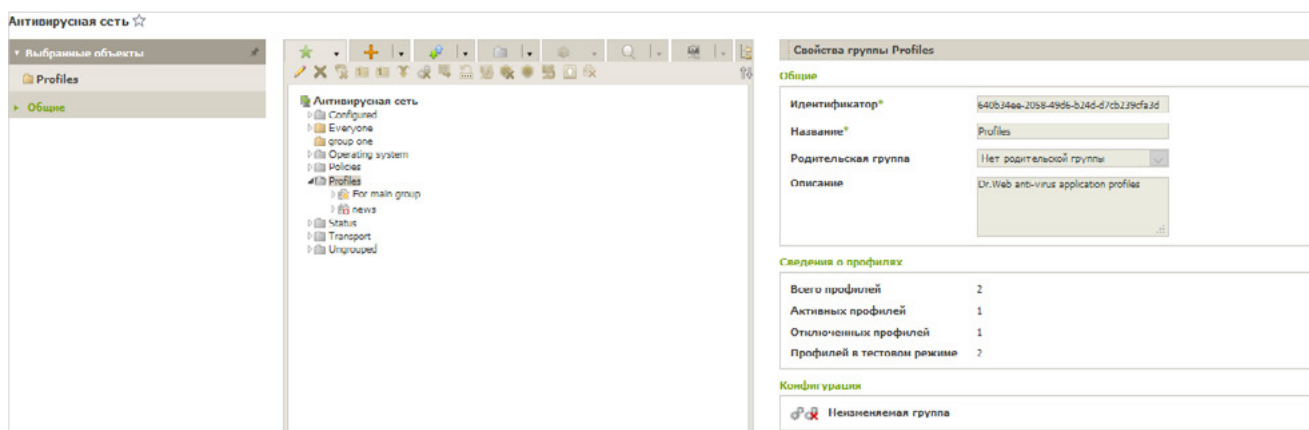
## 1.2. Создание Профиля Контроля приложений

Профили используются для задания настроек компонента **Контроль приложений**, в соответствии с которыми приложения на станциях будут запускаться или блокироваться.



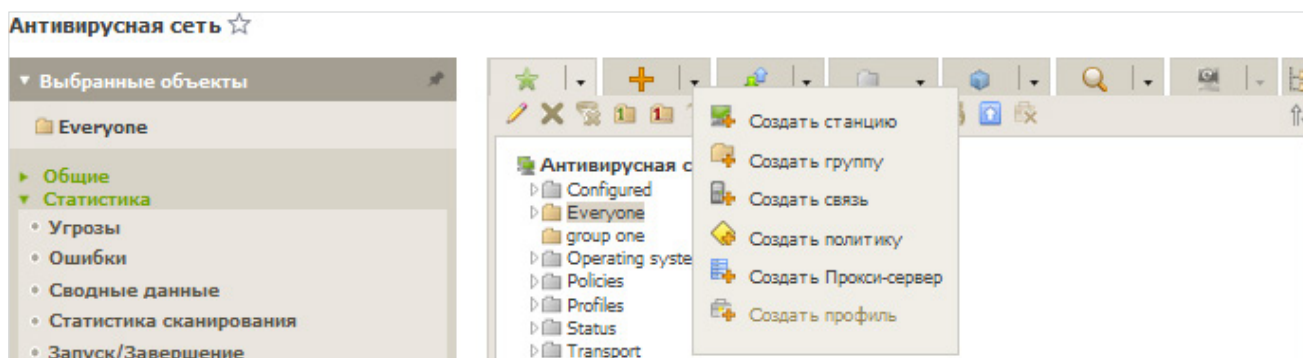
Профили определяют режим работы Контроля приложений. В связи с этим первым шагом настройки модуля **Контроль приложений** является создание нужного профиля — конфигурации работы модуля Контроль приложений для станций, групп станций, отдельных пользователей — которым они могут быть назначены.

Все профили размещаются в предустановленной группе **Profiles** дерева антивирусной сети.

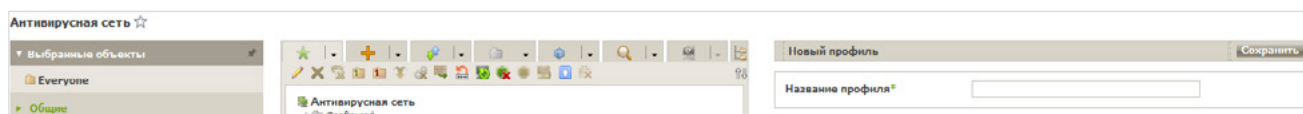


Чтобы создать профиль

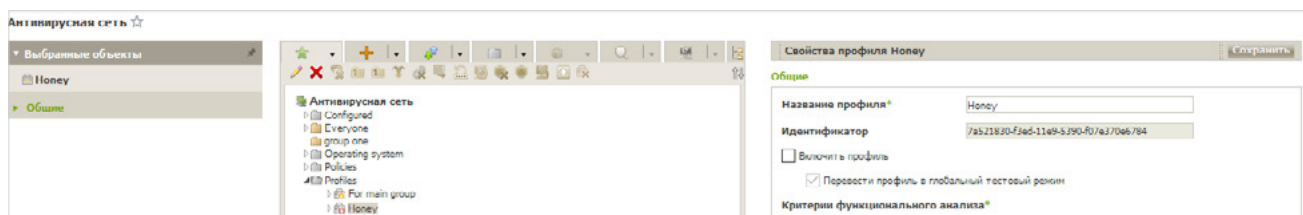
1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне на панели инструментов выберите пункт **Добавить объект сети** → **Создать профиль**.



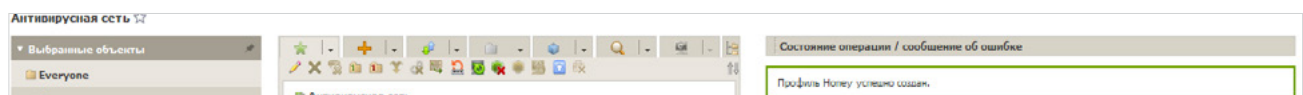
3. На открывшейся панели задайте **Название профиля**.



В дальнейшем имя профиля можно изменить в разделе настроек **Общие** свойств профиля.



4. Нажмите кнопку **Сохранить**.

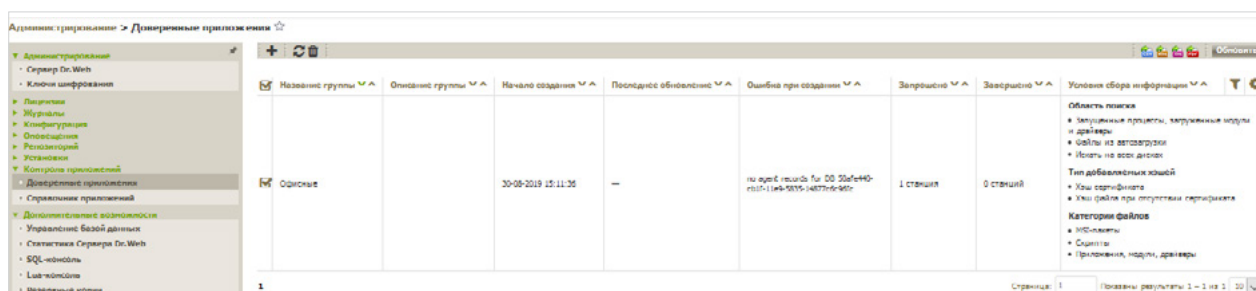


5. Новый профиль будет создан и помещен в группу **Profiles**.

### 1.3. Определение списка доверенных приложений

Доверенные приложения — списки приложений, запуск которых всегда разрешен на станциях с установленным компонентом **Контроль приложений**. Выбор разрешенных списков осуществляется в настройках профиля в разделе настроек Разрешающего режима. Для управления доверенными приложениями на Серверах, собирающих информацию, перейдите в раздел **Администрирование** → **Контроль приложений** → **Доверенные приложения**.

Таблица раздела содержит список всех актуальных групп доверенных приложений (белых списков) — приложений, собранных по заданным критериям с выбранной станции или группы станций.

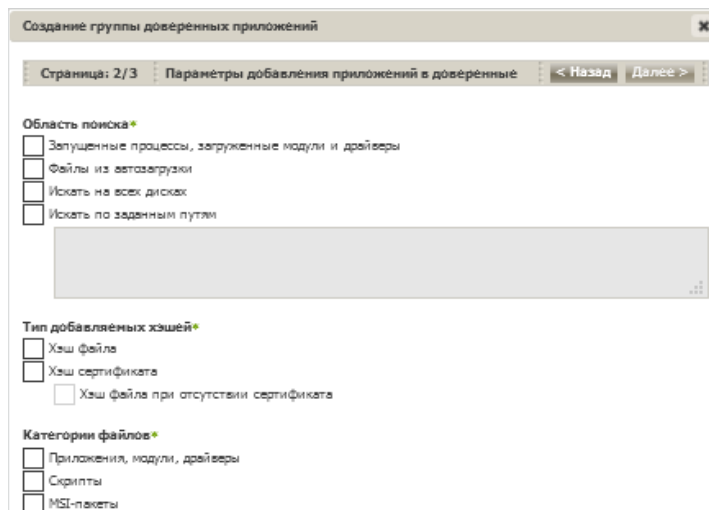


#### Чтобы создать новую группу доверенных приложений

1. В разделе **Доверенные приложения** нажмите на панели инструментов кнопку **+** (**Создать группу доверенных приложений**).
2. В открывшемся окне задайте **Название группы** (название создаваемой группы доверенных приложений), **Описание** (необязательное произвольное описание создаваемой группы).

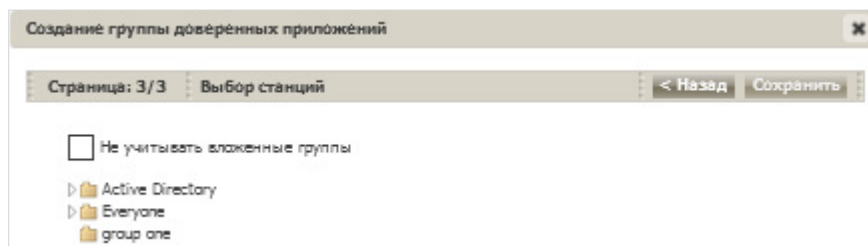


3. Нажмите **Далее** и задайте правила добавления приложений в доверенные, установив флаги, согласно которым приложения на станциях будут добавляться в создаваемую группу доверенных приложений.



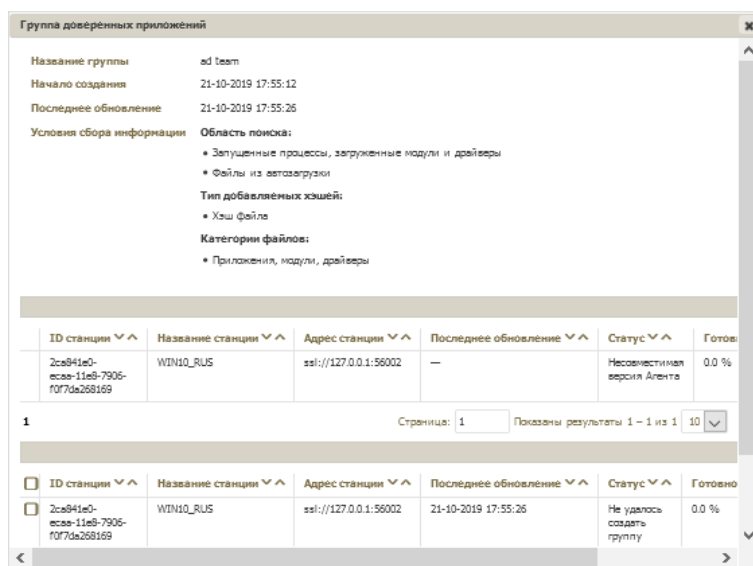
В поле **Искать по заданным путям** можно задать несколько путей для поиска приложений. Используйте ";" в качестве разделителя.

4. Нажмите **Далее** и в дереве сети выберите станции и группы станций, на которых будет осуществляться сбор информации о приложениях для включения их в список доверенных. Для выбора нескольких групп и станций используйте кнопки CTRL и SHIFT.




5. Нажмите кнопку **Сохранить**, начнется сбор информации о приложениях на станциях согласно заданным настройкам. Процесс может занять продолжительное время.


Информацию о состоянии и обновлении группы доверенных приложений можно увидеть как в основной таблице раздела **Доверенные приложения**, так и в дополнительной информации о группе, которая открывается при нажатии на строку, соответствующую группе в основной таблице раздела **Доверенные приложения**.



### Чтобы запустить обновление группы доверенных приложений

1. В разделе **Доверенные приложения** в таблице раздела установите флаги для групп, которые вы хотите обновить.
2. Нажмите на панели инструментов кнопку  (**Перезапустить создание группы доверенных приложений**).

### Чтобы удалить группу доверенных приложений

1. В разделе **Доверенные приложения** в таблице раздела установите флаги для групп, которые вы хотите удалить.
2. Нажмитена панели инструментов кнопку  (**Удалить группу доверенных приложений**).
3. Если группа не назначена на профили Контроля приложений, приложения данной группы будут удалены из списка разрешенных для запуска на станциях и сбор приложений для списка доверенных по критериям данной группы будет остановлен.

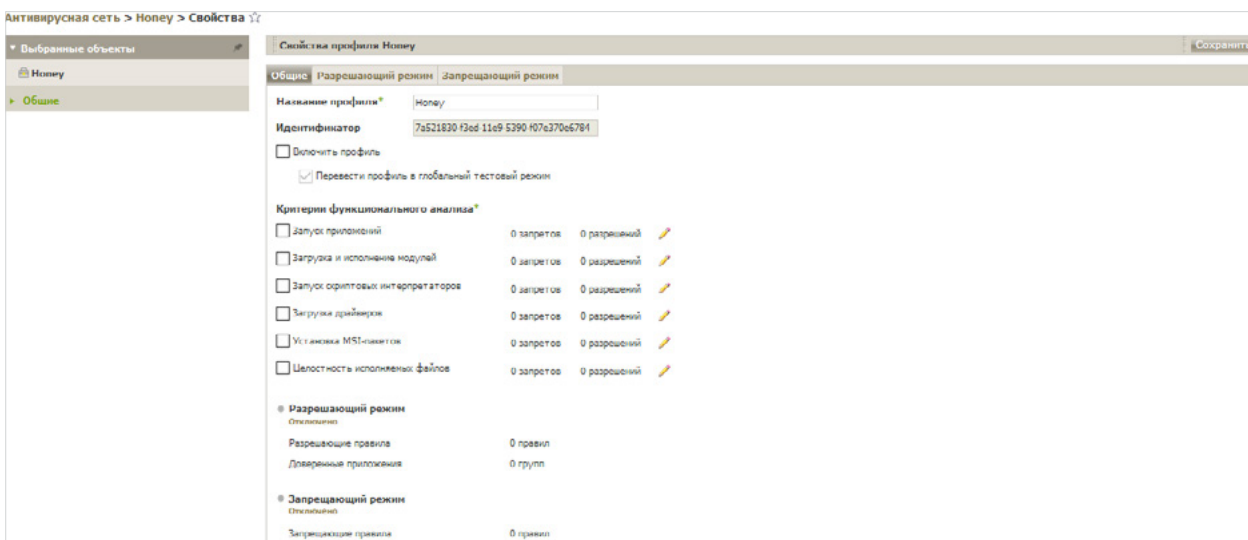
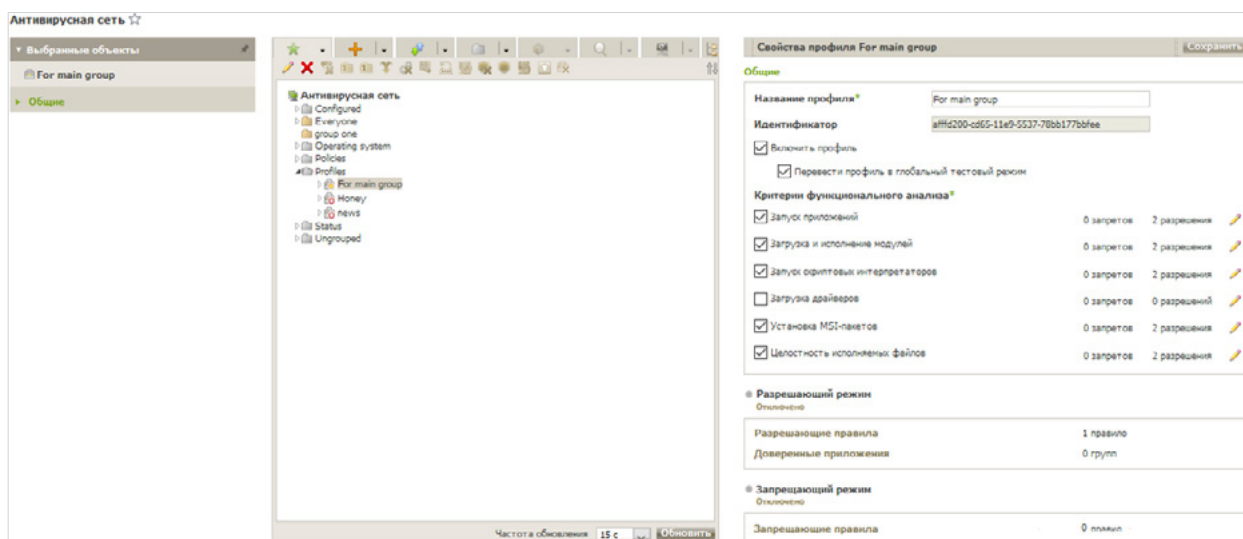
При удалении групп доверенных приложений создается новая ревизия в репозитории для продукта **Доверенные приложения** и распространяется на соседние Серверы. При



этом может быть нарушена работа профилей Контроля приложений, для которых эта группа назначена на соседних Серверах.

## 1.4. Установка режима работы Профиля Контроля приложений

1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. Нажмите на название профиля в иерархическом списке антивирусной сети (о 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).



3. В поле **Название профиля** можете изменить имя профиля.
4. 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.

Различают следующие режимы работы профилей:

- **Отключен** — профиль не активен, настройки профиля не применяются.
- **Активный** — профиль активен, настройки применяются для объектов, на которые

данный профиль распространен.

- **Тестовый глобальный** — профиль активен, но работает в глобальном тестовом режиме.
- **Тестовый для правил** — профиль активен, но на объекты распространяются только настройки функционального анализа.

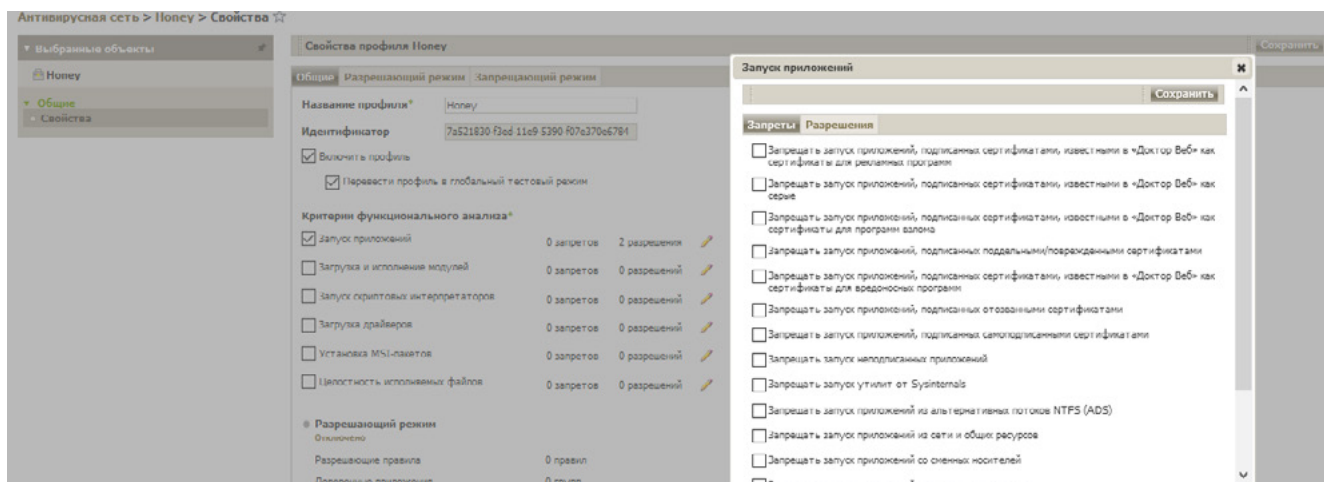
Разрешающие и запрещающие правила работают в тестовом режиме: их настройки на объекты не распространяются, но результат работы записывается в журнал активности (раздел статистики **События Контроля приложений**).

Тестовый режим для правил включается и отключается в разделе настроек запрещающих и разрешающих правил.

5. В разделе **Критерии функционального анализа** установите флаги для критериев, которые вы хотите использовать, и задайте наборы предустановленных правил, по которым запуск приложений будет разрешаться или запрещаться.

Если вы настраиваете профиль впервые, то при включении каждого из критериев автоматически включаются его разрешающие категории в расширенных настройках. В дальнейшем при необходимости вы можете отключить эти разрешающие категории в расширенных настройках.

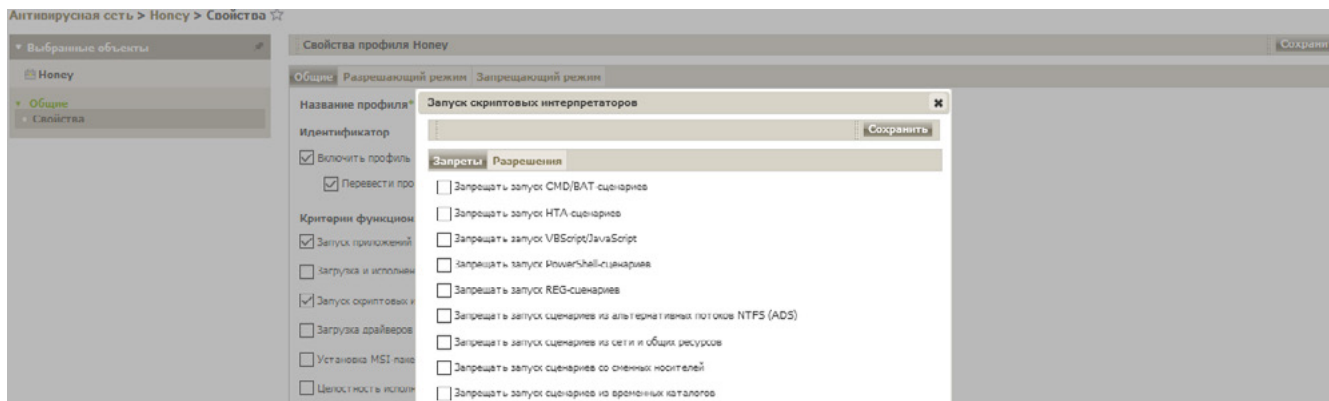
Для задания расширенных настроек по выбранному критерию нажмите **Редактировать** напротив соответствующего критерия. Откроется окно со списком настроек.



Настройки функционального анализа могут быть как запрещающими, так и разрешающими. Установите флаги для тех настроек, которые должны выполняться.

Если вы включите использование какого-либо из критериев, 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. Например:

- Если задан критерий **Запуск скриптовых интерпретаторов**, но не заданы его расширенные настройки, то будет контролироваться запуск всех скриптовых интерпретаторов в соответствии с настройками, заданными для разрешающего или запрещающего режимов.
- Если задан критерий **Запуск скриптовых интерпретаторов** и задана его расширенная настройка **Запрещать запуск сценариев со сменных носителей**, то будет запрещен только запуск сценариев со сменных носителей.



**Внимание!** Если вы зададите расширенные настройки, но не включите использование самого критерия, то ни расширенные настройки, ни сам критерий выполняться не будут.

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

**Внимание!** Если не включен ни один критерий в разделе **Критерии функционального анализа**, то сам профиль будет отключен.



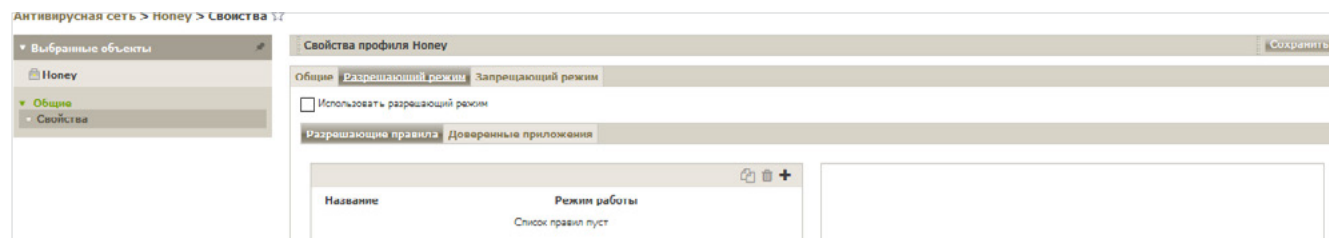
**Внимание!** Если ни для одного из критериев в разделе **Критерии функционального анализа** не заданы расширенные настройки и отключены запрещающий и разрешающий режимы, то сам профиль будет отключен.

6. Чтобы применить настройки, заданные в разделе **Общие**, нажмите **Сохранить** в настройках профиля.

7. В разделе **Разрешающий режим** окна свойств профиля приведена общая сводка по настройкам режима: количество созданных разрешающих правил и групп доверенных приложений, назначенных на данный профиль.

**Разрешающий режим** подразумевает, что на всех контролируемых станциях разрешается запуск только приложений из списка **Доверенные приложения** и приложений, которые соответствуют разрешающим правилам. Все остальные приложения блокируются.


Чтобы включить или отключить режим, а также настроить правила и доверенные приложения, перейдите в раздел **Разрешающий режим** для перехода в соответствующий раздел.

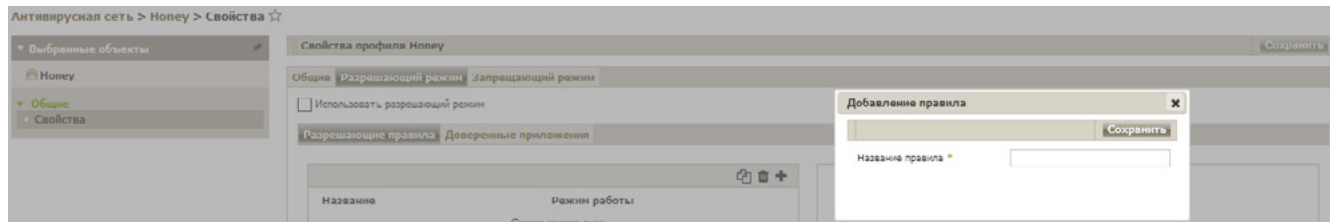


Чтобы использовать разрешающий режим

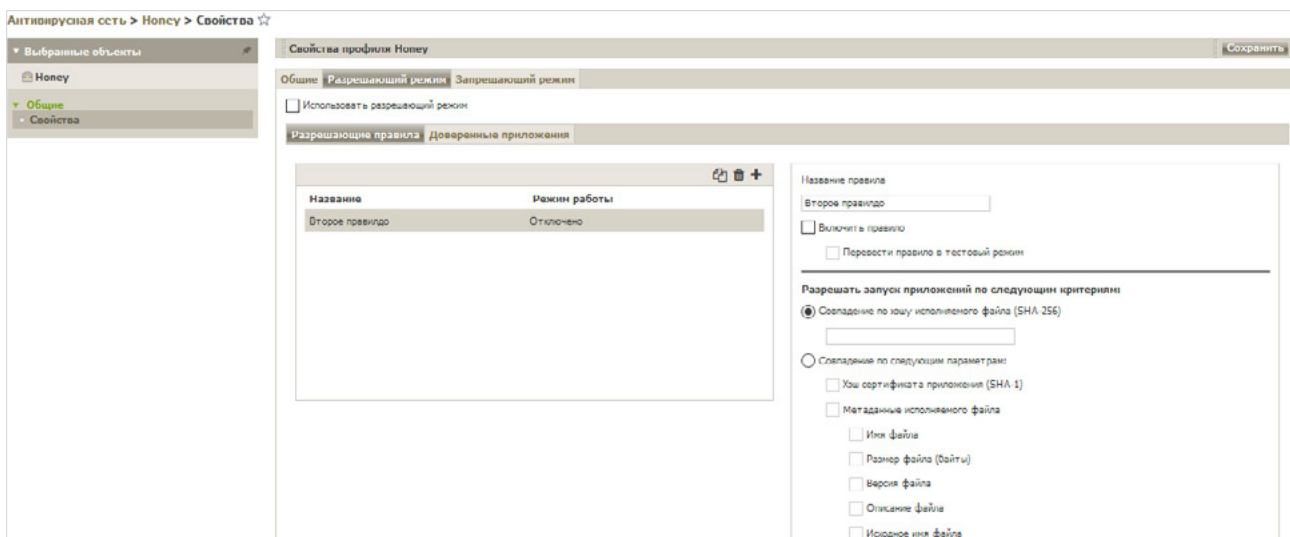
1. Установите флаг **Использовать разрешающий режим** на вкладке **Разрешающий режим**.
2. Задайте настройки в разделах **Разрешающие правила** и/или **Доверенные приложения**.

Чтобы создать новое разрешающее правило

- a. В разделе **Разрешающие правила** нажмите на панели инструментов кнопку  (**Создать правило**).
- b. В окне **Добавление правила** задайте **Название правила** и нажмите **Сохранить**.





- c. В списке правил выберите созданное правило и задайте его настройки на открывшейся панели свойств:
  - i. Установите флаг **Включить правило**, чтобы начать использовать это правило.



- ii. Если вы хотите проверить работу правила без применения его на станциях, установите флаг **Перевести правило в тестовый режим**.
  - iii. В разделе **Разрешать запуск приложений по следующим критериям** выберите опции, согласно которым запуск приложений на станциях будет разрешен. Также вы можете создавать разрешающие правила из разделов **События Контроля приложений** и **Справочник приложений** Центра управления на основе данных, полученных со станций.
- d. Нажмите **Сохранить**.

Чтобы создать дубликат разрешающего правила

- a. В разделе **Разрешающие правила** в таблице правил выберите правило, которое вы хотите продублировать для этого профиля.
- b. Нажмите на панели инструментов кнопку  (**Дублировать правило**).
- c. В таблице правил появится новое правило, настройки которого будут полностью скопированы из правила, выбранного на шаге 1. В имени правила добавится цифра **1**. Чтобы удалить разрешающее правило, в таблице правил выберите правило, которое вы хотите удалить из профиля, и нажмите на панели инструментов кнопку  (**Удалить правило**).


Для редактирования доверенных приложений для конкретного профиля необходимо перейти на закладку **Доверенные приложения**, таблица которого содержит список всех

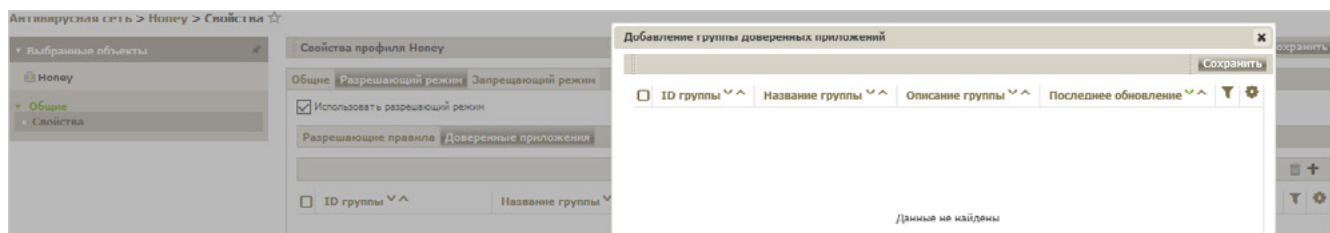
групп доверенных приложений (белый список приложений), назначенных для данного профиля. Белый список приложений представляет собой список приложений, собранных по заданным критериям с выбранной станции или группы станций.

Эти приложения разрешены для запуска на станциях антивирусной сети, для которых назначен данный профиль при работе в разрешающем режиме.

Если ваш Сервер получает доверенные приложения по межсерверной связи, то таблица групп может содержать записи со значком **Группа доверенных приложений отсутствует в репозитории Сервера**. Данные записи актуальны для групп приложений, которые были добавлены из предыдущей ревизии продукта **Доверенные приложения**, после чего была получена новая ревизия, в которую данная группа не входит. Чтобы предотвратить нарушения работы профиля, рекомендуется удалить такие группы из его настроек.


**Чтобы добавить группу доверенных приложений в профиль**

- a. В разделе **Доверенные приложения** нажмите на панели инструментов кнопку  (**Добавить группу доверенных приложений в профиль**).
- b. Откроется окно со списком всех доступных групп доверенных приложений.



- c. При настройке разрешающего режима группы доверенных приложений выбираются из списка групп, доступных в репозитории для продукта **Доверенные приложения**.
- d. Установите флаги напротив тех групп приложений, которые вы хотите добавить в профиль.
- e. Нажмите **Сохранить**.

**Чтобы удалить группу доверенных приложений из профиля**

- a. В разделе **Доверенные приложения** установите в таблице флаги для групп, которые вы хотите удалить из профиля.
- b. Нажмите на панели инструментов кнопку  (**Удалить группу доверенных приложений**).
- c. Приложения данной группы будут удалены из списка разрешенных для запуска на станциях, для которых назначен данный профиль.

При удалении из профиля сама группа доверенных приложений не удаляется. Группа остается доступна в репозитории и может быть добавлена как в данный, так и в другие профили.

Чтобы использовать доверенные приложения, выполните одно из следующих действий:

- a. Если сбор доверенных приложений будет осуществляться на вашем Сервере, активируйте сбор доверенных приложений в разделе Центра управления **Администрирование** → **Контроль приложений** → **Доверенные приложения**.
- b. Если доверенные приложения будут передаваться на ваш Сервер по межсерверной связи с соседнего Сервера, задайте соответствующие настройки в репозиториях Серверов, отправляющих и получающих продукт **Доверенные приложения**.

3. Нажмите **Сохранить**.

**Внимание!** Если не заданы ни разрешающие правила, ни доверенные приложения, разрешающий режим будет отключен.



8. В разделе **Запрещающий режим** окна свойств профиля приведена общая сводка по настройкам режима: количество созданных запрещающих правил.

**Запрещающий режим** подразумевает, что на всех контролируемых станциях запрещается запуск только тех приложений, которые соответствуют запрещающим правилам. Все остальные приложения разрешаются.

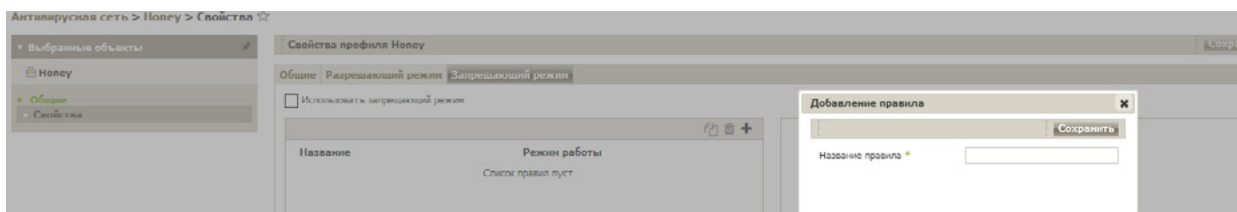
Чтобы включить или отключить режим, а также настроить правила, перейдите в раздел **Запрещающий режим** для перехода в соответствующий раздел.

1. Чтобы использовать запрещающий режим, установите флаг **Использовать запрещающий режим** на вкладке **Запрещающий режим**.

2. Создайте запрещающие правила.

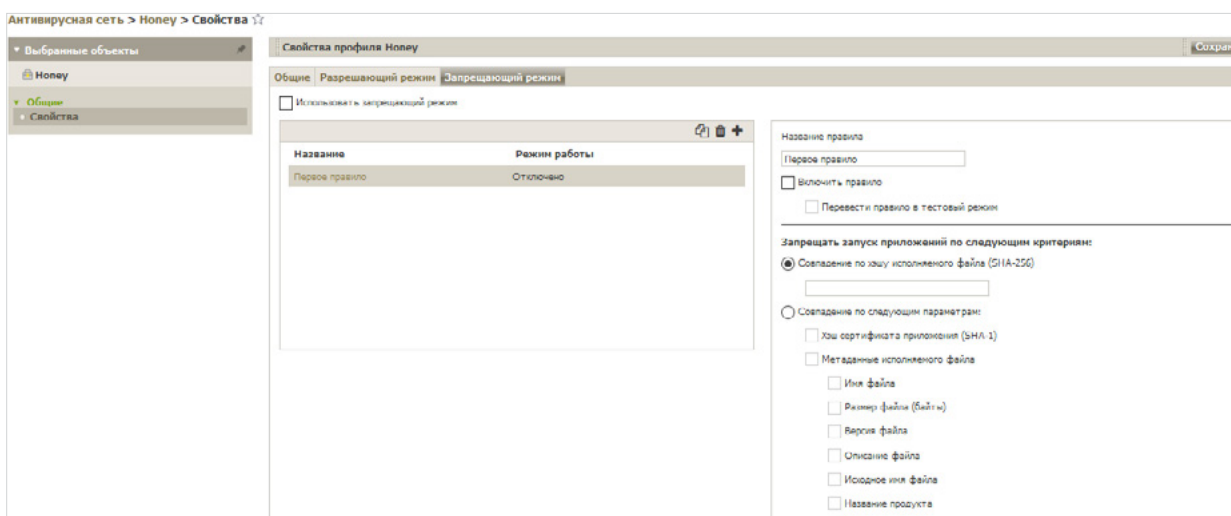
a. Нажмите кнопку **+** (**Создать правило**).

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.



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** выберите опции, согласно которым запуск приложений на станциях будет запрещен.

Также вы можете создавать запрещающие правила из разделов **События Контроля приложений** и **Справочник приложений** Центра управления на основе данных, полученных со станций.

d. Нажмите **Сохранить**.

4. Нажмите **Сохранить**.

## Чтобы создать дубликат запрещающего правила

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**.  
Чтобы удалить запрещающее правило, выберите правило, которое вы хотите удалить из профиля, и нажмите на панели инструментов кнопку  (**Удалить правило**).

**Внимание!** Если не заданы запрещающие правила, запрещающий режим будет отключен.

**Внимание!** Разрешающий и запрещающий режимы могут быть включены или отключены как вместе, так и по отдельности. Функциональный анализ должен быть всегда включен. Если все правила функционального анализа отключены, контроль запуска приложений не производится.

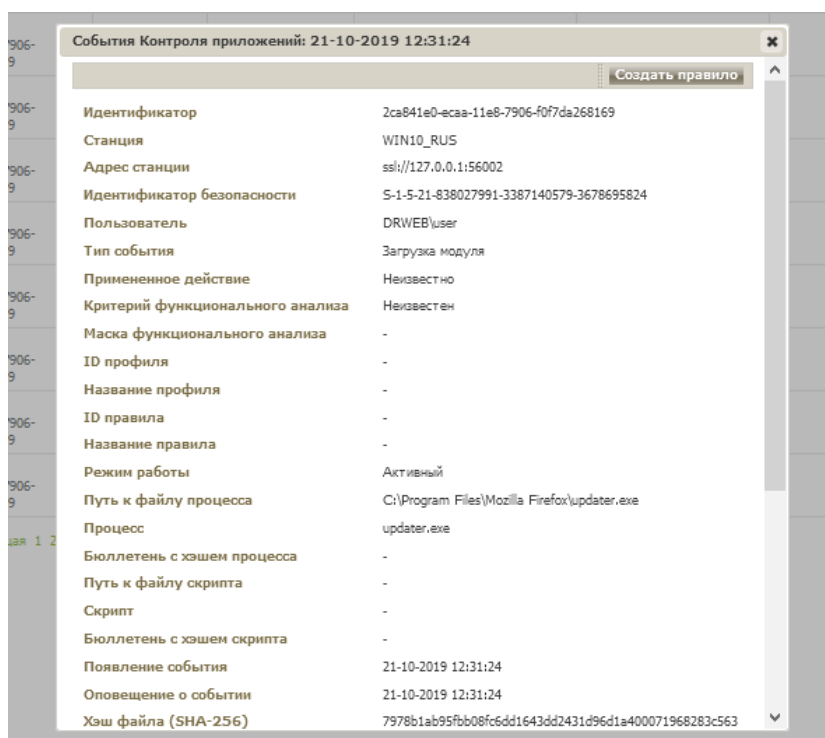
## 1.5. Настройка Профиля Контроля приложений

Чтобы контролировать запуск приложений на станциях, необходимо, чтобы для станции или пользователя станции был назначен хотя бы один активный профиль.

Так как все профили размещаются в предустановленной группе Profiles дерева антивирусной сети, то объекты, на которые назначен конкретный профиль, размещаются в дереве антивирусной сети в качестве элементов этого профиля.

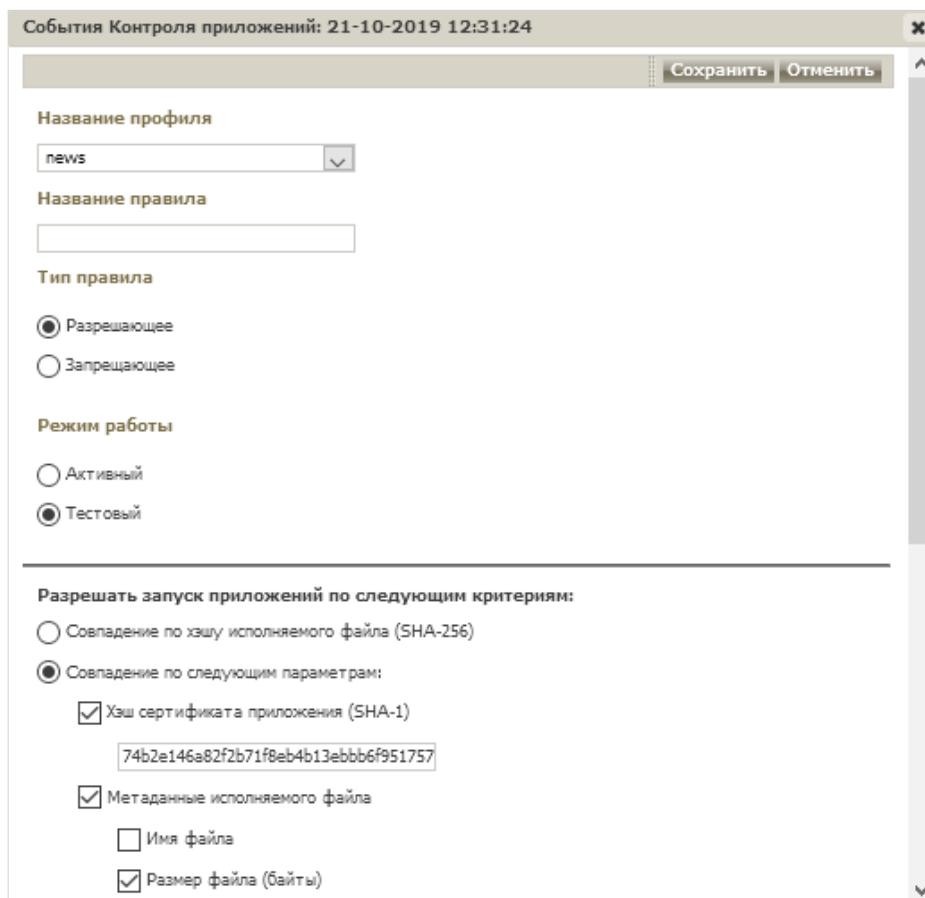
### 1.5.1. Создание правила на основе данных журнала активности

1. В разделе **Статистика** → **События Контроля приложений** нажмите на строку с событием о попытке запуска приложения, для которого вы хотите создать правило, контролирующее запуск.
2. В открывшемся окне с информацией о выбранном событии нажмите кнопку **Создать правило**.



3. В открывшемся окне задайте:

- a. В выпадающем списке **Название профиля** выберите профиль Контроля приложений, в котором будет создано правило.



- b. В поле **Название правила** задайте название для создаваемого правила.
- c. В разделе **Тип правила** выберите тип создаваемого правила: запрещающее или разрешающее.
- d. Для опции **Режим работы** выберите, в каком режиме будет работать созданное правило.

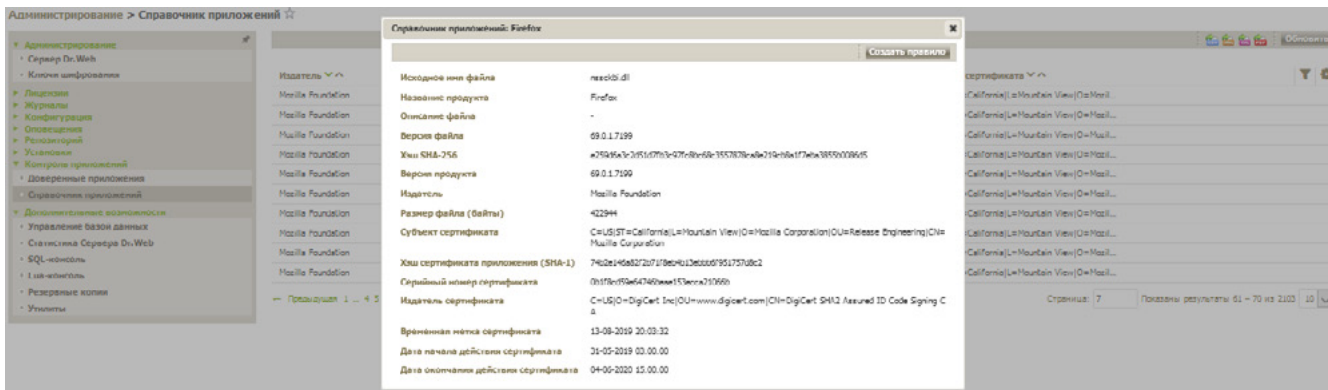
В режиме **Тестовый** приложения не будут блокироваться на станциях, однако будет осуществляться запись журнала активности, как при включенных настройках. Результаты потенциальных блокировок приложений по созданному правилу будут отображаться в разделе **События Контроля приложений**.

- e. В разделе **Запрещать запуск приложений по следующим критериям / Разрешать запуск приложений по следующим критериям** поля заполняются автоматически в соответствии с данными приложения, на основе которого создается правило. При необходимости данные можно отредактировать.

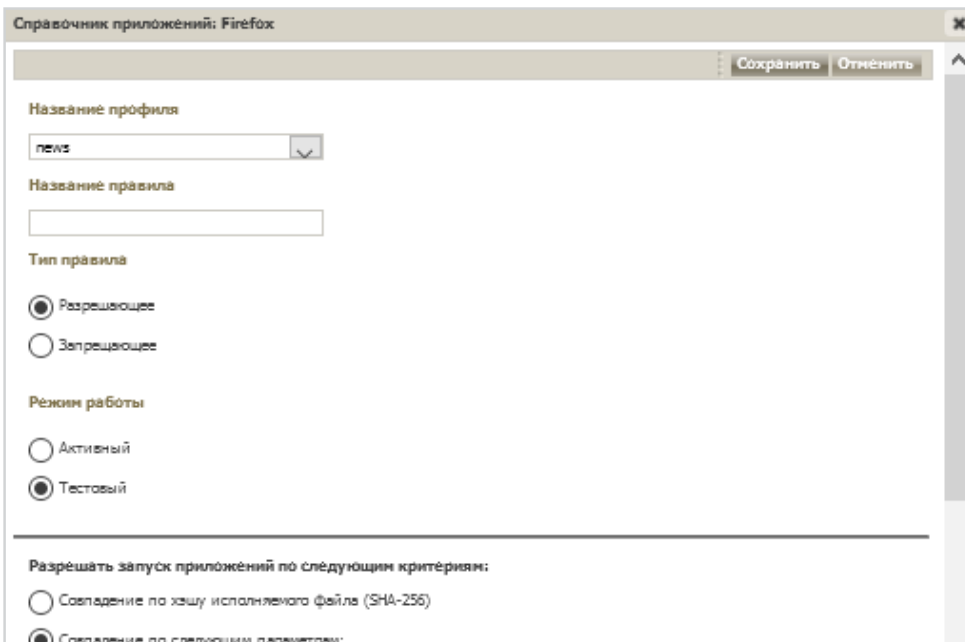
4. Нажмите **Сохранить**. Правило будет создано в заданном профиле Контроля приложений.

#### 1.5.2. Создание правила на основе данных справочника приложений

1. В разделе Справочник приложений выберите строку о приложении, для которого вы хотите создать правило, контролирующее запуск.
2. При нажатии на строку таблицы откроется окно с информацией о выбранном приложении.



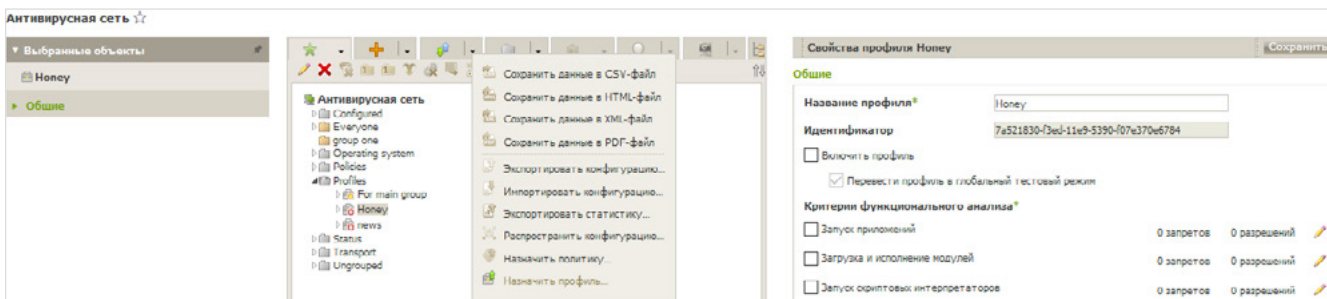
3. Нажмите кнопку **Создать правило**.
4. Откроется окно для создания нового правила. Задайте следующие настройки:
  - a. В выпадающем списке **Название профиля** выберите профиль Контроля приложений, в котором будет создано правило.



- b. В поле **Название правила** задайте название для создаваемого правила.
  - c. Для опции **Тип правила** выберите тип создаваемого правила: запрещающее или разрешающее.
  - d. Для опции **Режим работы** выберите, в каком режиме будет работать созданное правило (соответствует флагу **Перевести правило в тестовый режим** при создании правила из профиля). Если вы хотите проверить работу правила без применения его на станциях, выберите режим **Тестовый**.
  - e. В разделе **Запрещать запуск приложений по следующим критериям / Разрешать запуск приложений по следующим критериям** (в зависимости от типа правила, выбранного на шаге d) будут автоматически заполнены поля в соответствии с приложением, на основе которого создается правило. При необходимости можете отредактировать значения настроек.
5. Нажмите **Сохранить**. Правило будет создано в заданном профиле Контроля приложений.

## 1.6. Назначение Профиля защищаемым объектам

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**.



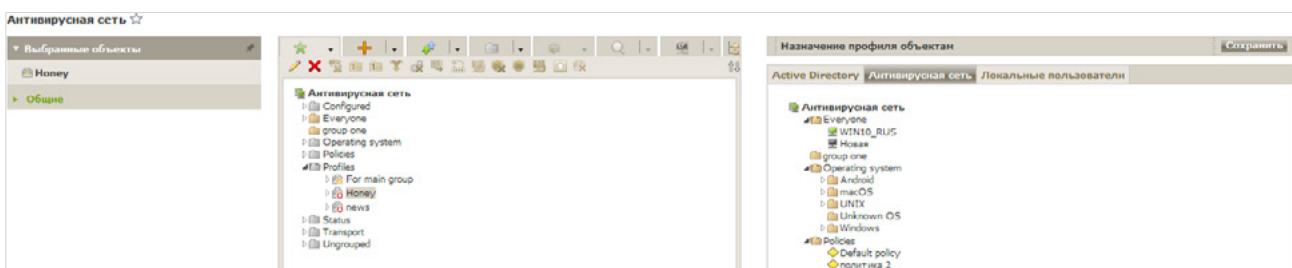
4. Выберите объект распространения настроек в открывшемся окне.

На вкладке **Active Directory** представлены списки, аналогичные списку в дереве антивирусной сети, обновляемые по заданию Синхронизация с Active Directory из расписания Сервера. Списки содержат идентичные объекты, но различаются по типу объектов, для которых будет назначен профиль:

- В списке **Станции Active Directory** вы можете выбрать группы станций или отдельные станции, зарегистрированные в домене Active Directory.
- В списке **Пользователи Active Directory** вы можете выбрать группы пользователей и отдельных пользователей, зарегистрированных в домене Active Directory.

Одни и те же объекты не должны быть выбраны в разных списках.

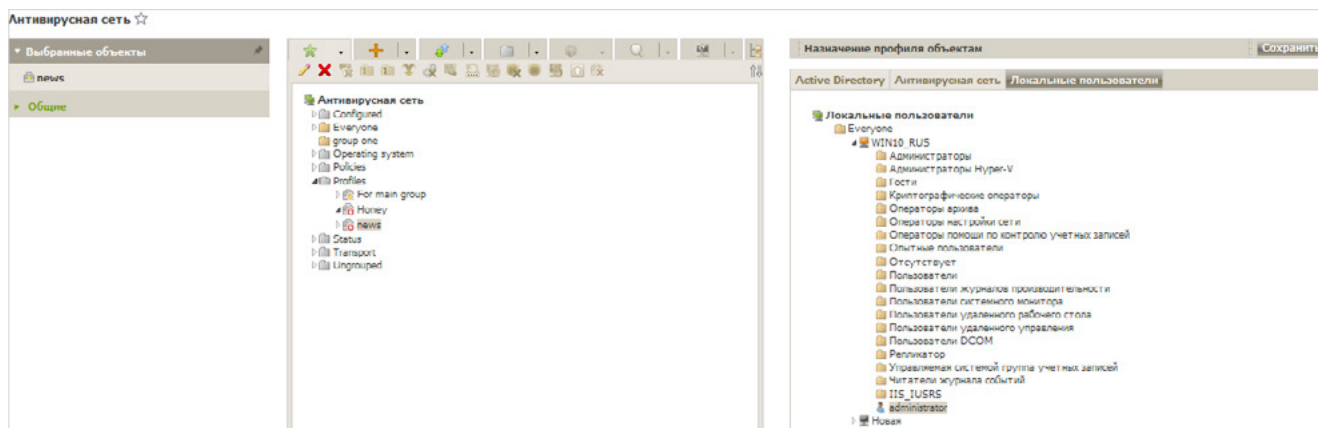
На вкладке **Антивирусная сеть** вы можете выбрать группы станций (настройки будут распространяться на учетные записи всех пользователей всех станций, входящих в данные группы) или отдельные станции в группах (настройки будут распространяться на учетные записи всех пользователей выбранных станций):



На вкладке **Локальные пользователи** вы можете выбрать следующие объекты:

- Станции. В этом случае настройки будут распространяться на учетные записи всех пользователей выбранных станций.
- Отдельных пользователей на станциях. В этом случае настройки будут распространяться только на учетные записи выбранных пользователей на этих станциях.



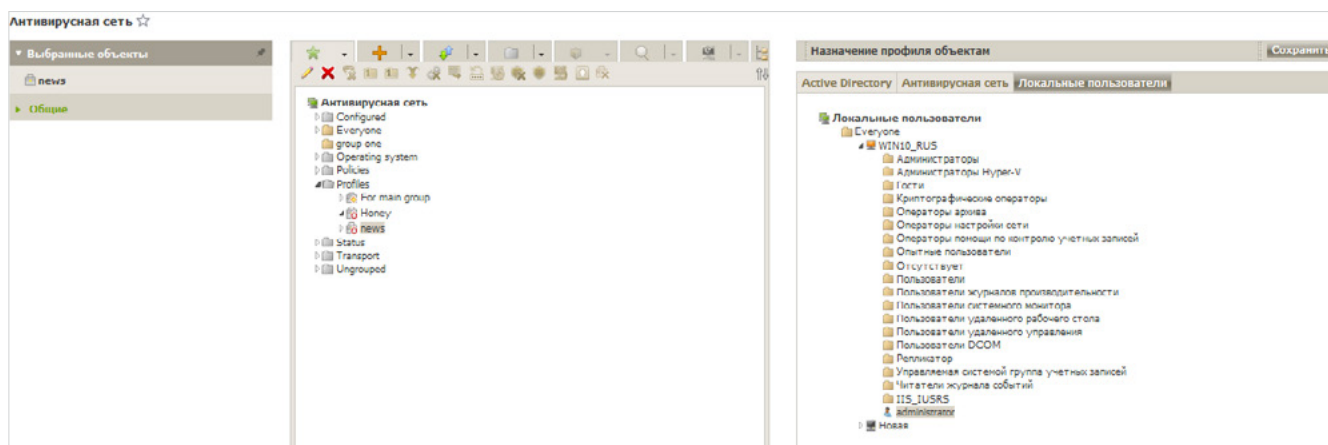


Настройки профилей Контроля приложений могут быть назначены не только на станции и группы станций, но также на отдельных пользователей и группы пользователей. При этом:

1. При наличии пользовательских настроек они обладают наивысшим приоритетом.
  2. При отсутствии пользовательских настроек приоритет отдается настройкам группы пользователей.
  3. Если не заданы настройки для пользователей и группы пользователей, наследование осуществляется по приоритету применения настроек для 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.

#### Чтобы отменить назначение настроек профиля на объект

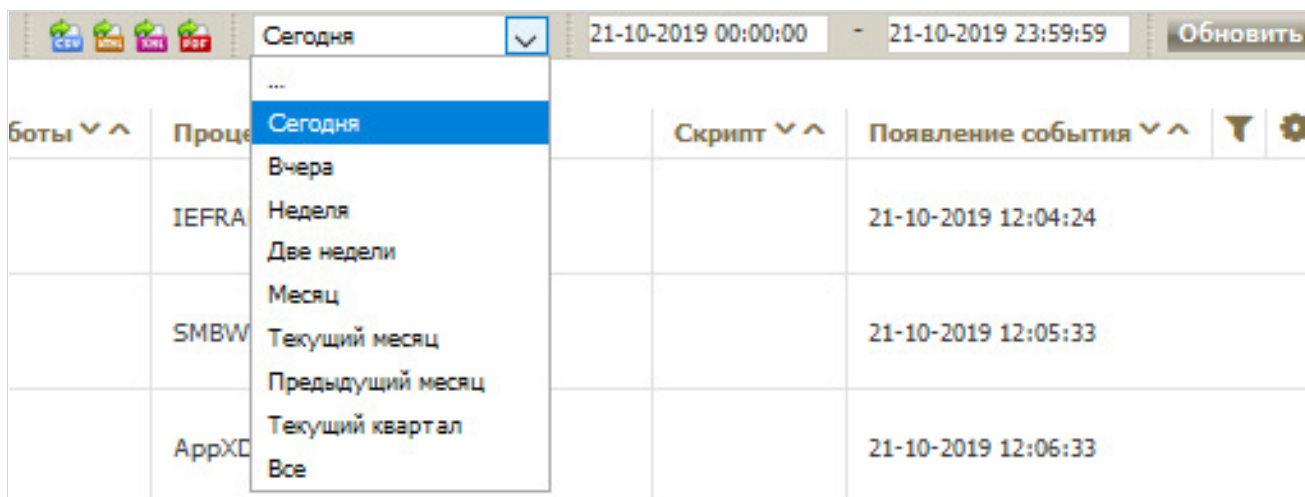
1. Выберите пункт **Антивирусная сеть** в главном меню Центра управления.
2. В открывшемся окне в иерархическом списке раскройте список объектов, вложенных в профиль, и выберите объект, для которого вы хотите отменить назначение профиля.
3. На панели инструментов нажмите **Общие** → **Отменить назначение профиля объектам**.



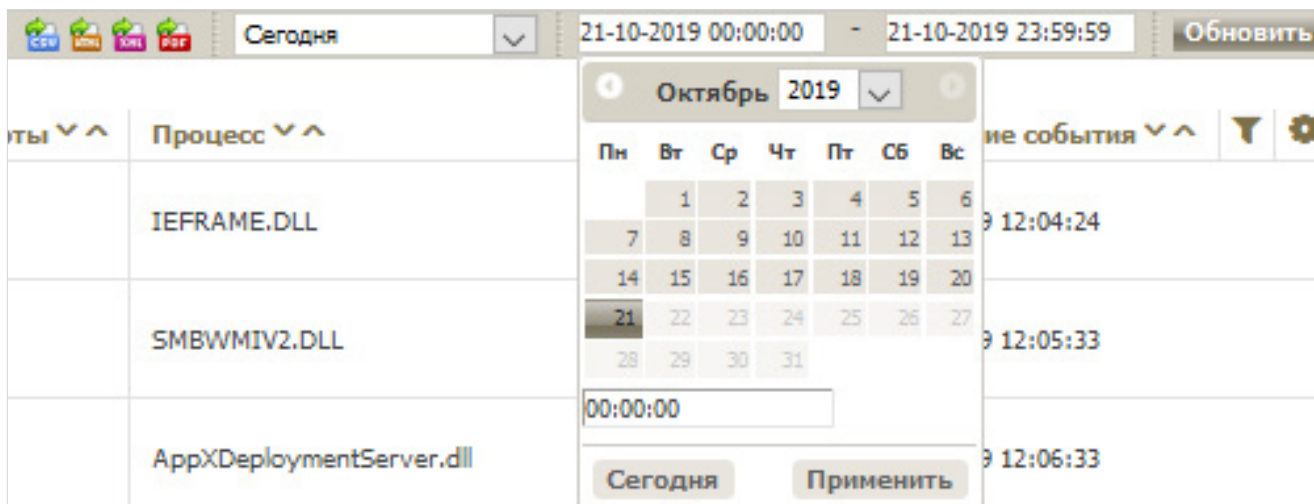
## 2. Просмотр статистики активности на защищаемых станциях

1. В иерархическом списке выберите станцию или группу.
2. В управляющем меню в разделе **Статистика** выберите пункт **События Контроля приложений**.
3. Откроется окно, содержащее список приложений, запуск которых был запрещен или разрешен на выбранных станциях.

По умолчанию отображается статистика за последние сутки. Для отображения данных за определенный период укажите диапазон времени относительно сегодняшнего дня из выпадающего списка.

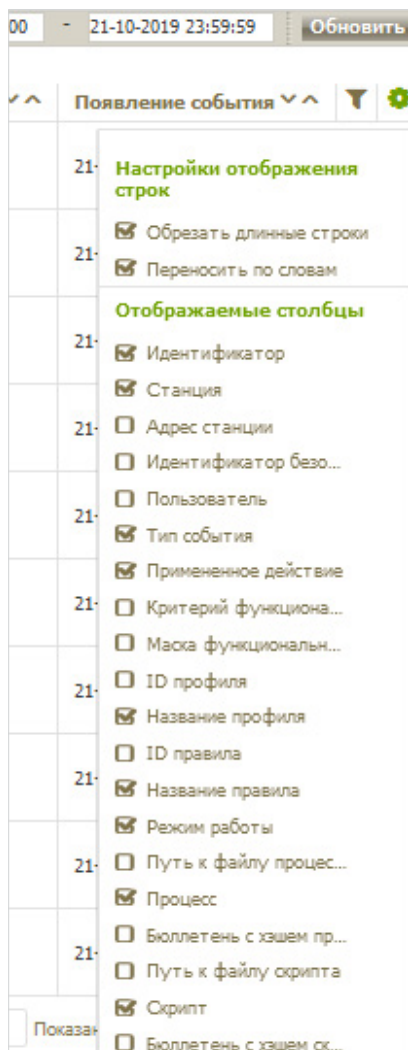


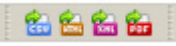
Для задания произвольного диапазона введите требуемые даты или нажмите на значки календаря рядом с полями дат.

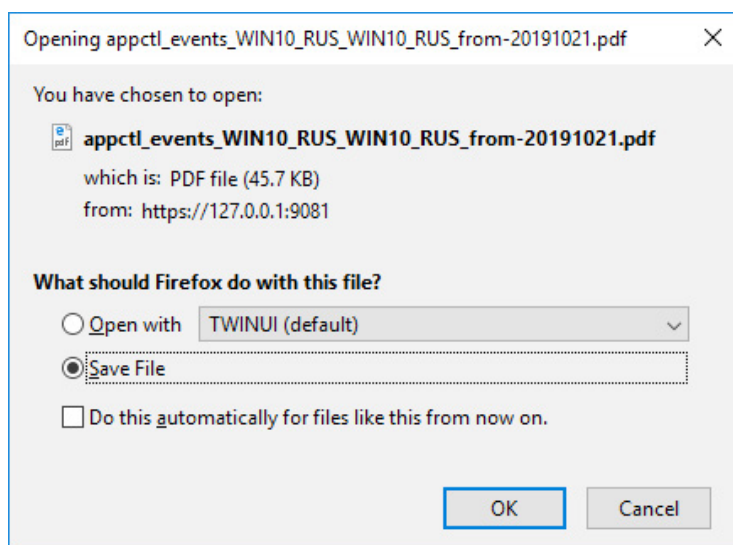


Для того чтобы отобразить данные, нажмите кнопку **Обновить**.

Состав показываемой информации также настраивается. Для того чтобы выбрать необходимые к показу поля таблицы, нажмите **⌵**.



Если необходимо сохранить таблицу статистики для распечатки или дальнейшей обработки, нажмите на одну из кнопок  (Сохранить данные в CSV-файл, Сохранить данные в HTML-файл, Сохранить данные в XML-файл, Сохранить данные в PDF-файл).



## 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 недеklarированных 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.

<u>Сертификаты</u> <u>ФСТЭК России</u>	<u>Сертификаты</u> <u>Минобороны России</u>	<u>Сертификаты</u> <u>ФСБ России</u>	<u>Все сертификаты</u> <u>и товарные знаки</u>
---	--	---	---

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



© ООО «Доктор Веб»,  
2003–2019

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>