

Запрет запуска программ с помощью Контроля приложений в Dr.Web Enterprise Security Suite 12.0



Dr.Web Enterprise Security Suite 12.0

Запрет запуска программ с помощью Контроля приложений

Чтобы создать правило для модуля **Контроль приложений** Центра управления Dr.Web Enterprise 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**.

Антивирусная сеть > Everyone > События Контроля приложений ☆

Выбранные объекты	Идентификатор	Станция	Тип события	Применимое действие	Название профиля	Название правила	Режим работы	Процесс
Everyone	7ca841e0-ec5a-11e8-7906-f97da260169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	IEFRAME.DLL
Общие	2ca841e0-ec5a-11e8-7906-f97da260169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	SMBWIMV2.DLL
Статистика	7ca841e0-ec5a-11e8-7906-f97da260169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	AppXDeploymentServer...
Угрозы	2ca841e0-ec5a-11e8-7906-f97da260169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	AppXDeploymentExtern...
Ошибки	7ca841e0-ec5a-11e8-7906-f97da260169	WIN10_RUS	Загрузка модуля	Неизвестно			Активный	AppXDeploymentExtern...
Сводные данные								
Статистика сканирования								
Запуск/Завершение								
Статистика угроз								
Состояние								
Задания								
Заблокированные устройства								
Продукты								
События Пресентивной защиты								
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.

Антивирусная сеть > Everyone > Windows > Агент Dr.Web ☆

Everyone. Заданы персональные настройки.

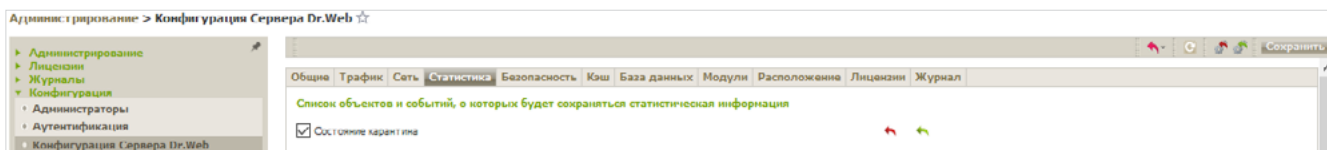
Общие	Мобильность	Журнал	Интерфейс	События
Задержка запуска Планировщика заданий (мин.)	1			
Периодичность отправки статистики (мин.)	60			
Интервал актуальности вирусных баз	1	дни		
Язык	Системный язык			
<input checked="" type="checkbox"/> Включить Microsoft Network Access Protection				
<input checked="" type="checkbox"/> Разрешить удаленное управление карантин				
<input checked="" type="checkbox"/> Собирать информацию о станциях				
Период сбора информации о станциях (мин.)	100			
<input checked="" type="checkbox"/> Отслеживать местоположение				
Периодичность в передаче координат	15	мин		
<input checked="" type="checkbox"/> Отслеживать события Контроля приложений				

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:

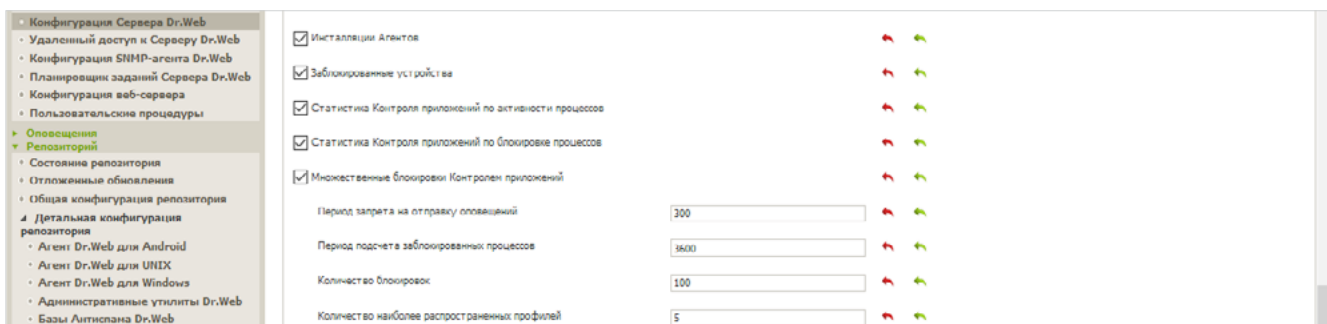
- **Статистика Контроля приложений по активности процессов**, чтобы получать и записывать информацию по любой активности всех процессов: как разрешенных для запуска, так и запрещенных Контролем приложений.

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.

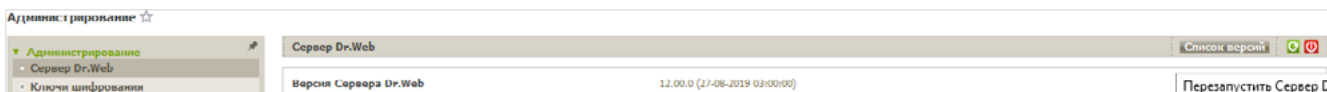
- **Статистика Контроля приложений по блокировке процессов**, чтобы получать и записывать информацию по активности всех процессов, запрещенных для запуска Контролем приложений.

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 единовременно 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**.

Администрирование > Справочник приложений

Идентификатор	Название продукта	Версия	Субъект сертификата
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...
VMware, Inc.	VMware Tools	10.0.6.54238	C=US ST=California L=Palo Alto O=VMware, I...

Теперь используем поиск на странице статистики.

Сегодня 28-10-2019 00:00:00 - 28-10-2019 23:59:59

Режим работы	Процесс	Скрипт	Появление события
Активный	OneDriveStandaloneUpdater.exe		
Активный	msiexec.exe		

Поиск:

Нажмите **Применить**.

Виртуальная сеть > Evergroup > События Контроля приложений

Идентификатор	Станция	Тип события	Применённое действие	Название профиля	Название правила	Режим работы	Процесс	Скрипт	Появление события
2c8b41e0-ecae-11e9-7906-0070a2581699	WIN10_RUS	Запуск процесса	Неизвестно			Активный	Far.exe		28-10-2019 14:48:47

Кликните по строке с информацией о запущенной программе.

События Контроля приложений: 28-10-2019 14:48:47

Идентификатор	2c8b41e0-ecae-11e9-7906-0070a2581699
Станция	WIN10_RUS
Адрес станции	ssl://127.0.0.1:49679
Идентификатор безопасности	S-1-5-21-838027991-3387140579-3678695824
Пользователь	DR\WEBuser
Тип события	Запуск процесса
Применённое действие	Неизвестно
Критерий функционального анализа	Неизвестно
Маска функционального анализа	-
ID профиля	-
Название профиля	-
ID правила	-
Название правила	-
Режим работы	Активный
Путь к файлу процесса	C:\Program Files (x86)\Manager\far.exe
Процесс	Far.exe
Биолетень с жжшем процесса	-
Путь к файлу скрипта	-
Скрипт	-
Биолетень с жжшем скрипта	-
Появление события	28-10-2019 14:48:47
Описание события	28 10 2019 14:48:47

Кликните **Создать правило**.

События Контроля приложений: 28-10-2019 14:48:47

Сохранить Отменить

Название профиля

For main group

news

Honey

For main group

Тип правила

Разрешающее

Запрещающее

Режим работы

Активный

Тестовый

Разрешать запуск приложений по следующим критериям:

Совпадение по хэшу исполняемого файла (SHA-256)

Совпадение по следующим параметрам:

Хэш сертификата приложения (SHA-1)

Метаданные исполняемого файла

Имя файла

Размер файла (байты)

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

События Контроля приложений: 28-10-2019 14:48:47

Запрещающее

Режим работы

Активный

Тестовый

Запрещать запуск приложений по следующим критериям:

Совпадение по хэшу исполняемого файла (SHA-256)

Совпадение по следующим параметрам:

Хэш сертификата приложения (SHA-1)

Метаданные исполняемого файла

Имя файла

Размер файла (байты)

Версия файла

= 3.0.5454.0

Описание файла

Исходное имя файла

Название продукта

Версия продукта

= 3.0.5454.0

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.

Запрещающее правило oldfar в профиле For main group успешно создано.

Идентификатор	Станция	Тип события	Примененное действие	Название профиля	Название правила	Режим работы	Процесс	Скринт	Появление события
3ca9f1e0-ec6e-11e8-7906-f0770a268109	WIN10_RUS	Запуск процесса	Неизвестно			Активный	OneDriveStandaloneUpdater.exe		28-10-2019 14:42:58
3ca9f1e0-ec6e-11e8-7906-f0770a268109	WIN10_RUS	Запуск процесса	Неизвестно			Активный	msiexec.exe		28-10-2019 14:48:16
3ca9f1e0-ec6e-11e8-7906-f0770a268109	WIN10_RUS	Запуск процесса	Неизвестно			Активный	File.exe		28-10-2019 14:48:47

Страница: 1 Показаны результаты: 1 - 3 из 3

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

Антивирусная сеть > For main group > Свойства

Свойства профиля For main group

Общие Разрешающий режим Запрещающий режим

Название профиля* For main group

Идентификатор a11f4200-e065-11e8-5537-79b6177b0f0e

Включить профиль

Переместить профиль в глобальный тестовый режим

Антивирусная сеть > For main group > Свойства

Свойства профиля For main group

Общие Разрешающий режим Запрещающий режим

Использовать запрещающий режим

Название	Режим работы
oldfar	Активный

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

Антивирусная сеть > For main group > Свойства

Свойства профиля For main group

Общие Разрешающий режим Запрещающий режим

Операция успешно завершена

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.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.

<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>