

# Dr.Web Enterprise Security Suite

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: [https://cdn-download.drweb.com/pub/drweb/esuite/13.0.1/documentation/html/ru/admin\\_manual/index.html?notifications\\_configure.htm](https://cdn-download.drweb.com/pub/drweb/esuite/13.0.1/documentation/html/ru/admin_manual/index.html?notifications_configure.htm)

## ?????????? ?? ???????? Dr.WEB Enterprise Security Suite

Настройка производится под встроенным УЗ admin в его разделе **Администрирование** → **Конфигурация оповещений**

У него два блока настроек оповещений:

- первый настроен под email;
- второй (SIEM KUMA) под Syslog.

Для настройки в этой версии сервера Dr.Web лучше прямо под встроенным УЗ admin в консоль заходить. У других админов этот блок может быть не всегда виден, либо не работать кнопка тестового события, либо ещё что-то.

Dr.WEB

Администрирование | Антивирусная сеть | Избранное

admin

Выход

СИЕМ KUMA

Метод отправки оповещений  
Syslog

Повторная отправка Сервером Dr.Web

Количество  
12

Тайм-аут  
300

Получатель  
udp://10.10.10.10:5140 IP:Port коллектора KUMA

Формат  
CEF (Common Event Format)

Тайм-аут подключения к получателю (с)  
5

Facility  
14

Отправитель  
drweb.local FQDN Dr. Web

**Администраторы**

- Неизвестный администратор
- Ошибка авторизации администратора

**Другое**

- Зафиксировано большое количество аварийно завершенных соединений
- Зафиксировано большое количество блокировок Контролем приложений
- Ошибка записи журнала Сервера Dr.Web
- Ошибка ротации журнала Сервера Dr.Web
- Соседний Сервер Dr.Web давно не подключался
- Статистический отчет
- Суммарный отчет Превентивной защиты
- Эпидемия в сети

**Лицензии**

- Достигнуто лицензионное ограничение по количеству станций в сети

**Станции**

- Аварийное завершение соединения
- Контроль приложений заблокировал процесс
- Контроль приложений заблокировал процесс из списка известных хешей угроз
- Критическая ошибка обновления станции
- Неизвестная станция
- Обнаружена угроза безопасности по известным хешам угроз
- Обнаружена угроза безопасности по известным хешам угроз
- Отчет Превентивной защиты
- Отчет Превентивной защиты об обнаружении угрозы по известным хешам угроз
- Ошибка авторизации станции
- Ошибка сканирования
- Ошибка сканирования при обнаружении угрозы по известным хешам угроз
- Ошибка создания учетной записи станции

Настройка коллектора KUMA по аналогии с этой главой (предварительно выберите тип коннектора **UDP**) - [ссылка](#)

Рекомендуемый парсер (без агрегации/склейки событий) для правил корреляции Community - **[2024-09-23] Dr. Web CEF** (из Community-Pack)

Revision #1

Created 2024-09-24 11:33:50 UTC by Boris RZR

Updated 2025-01-29 07:43:29 UTC by Boris RZR