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

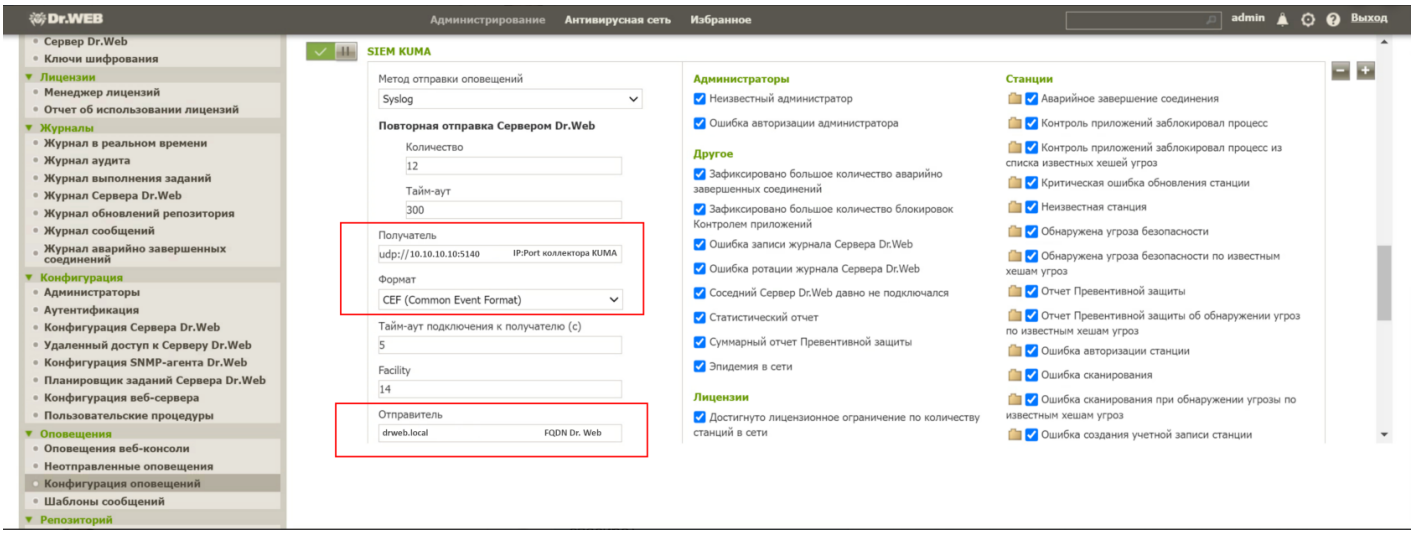
Настройка на стороне Dr.WEB Enterprise Security Suite

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.



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 24 September 2024 11:33:50 by Boris Rzr
Updated 24 September 2024 11:43:56 by Boris Rzr