

KATA

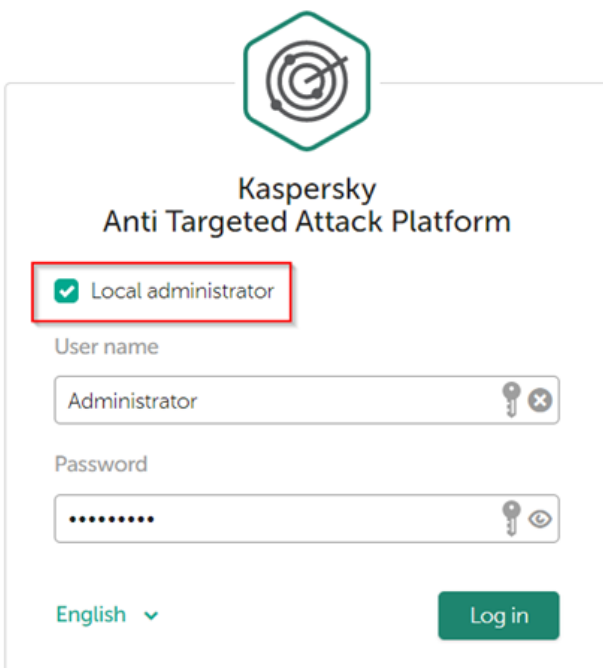
Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/help/KUMA/3.2/ru-RU/240690.htm>

?????????? KATA

Для настройки пересылки событий из KATA в SIEM KUMA необходимо выполнить следующие действия:

1. Перейти в веб-консоль центрального узла Kaspersky Anti Targeted Attack из-под учетной записи Администратора, предварительно отметив параметр **Local administrator**



The screenshot shows the login page for the Kaspersky Anti Targeted Attack Platform. At the top is a target icon. Below it, the text reads 'Kaspersky Anti Targeted Attack Platform'. There is a checkbox labeled 'Local administrator' which is checked and highlighted with a red rectangular box. Below this are two input fields: 'User name' containing 'Administrator' and 'Password' containing a series of dots. To the right of the password field is a key icon and an eye icon. At the bottom left, there is a language dropdown menu set to 'English'. At the bottom right, there is a green 'Log in' button.

2. Перейти в раздел **Settings - SIEM System** и настроить параметры отправки событий в KUMA SIEM:

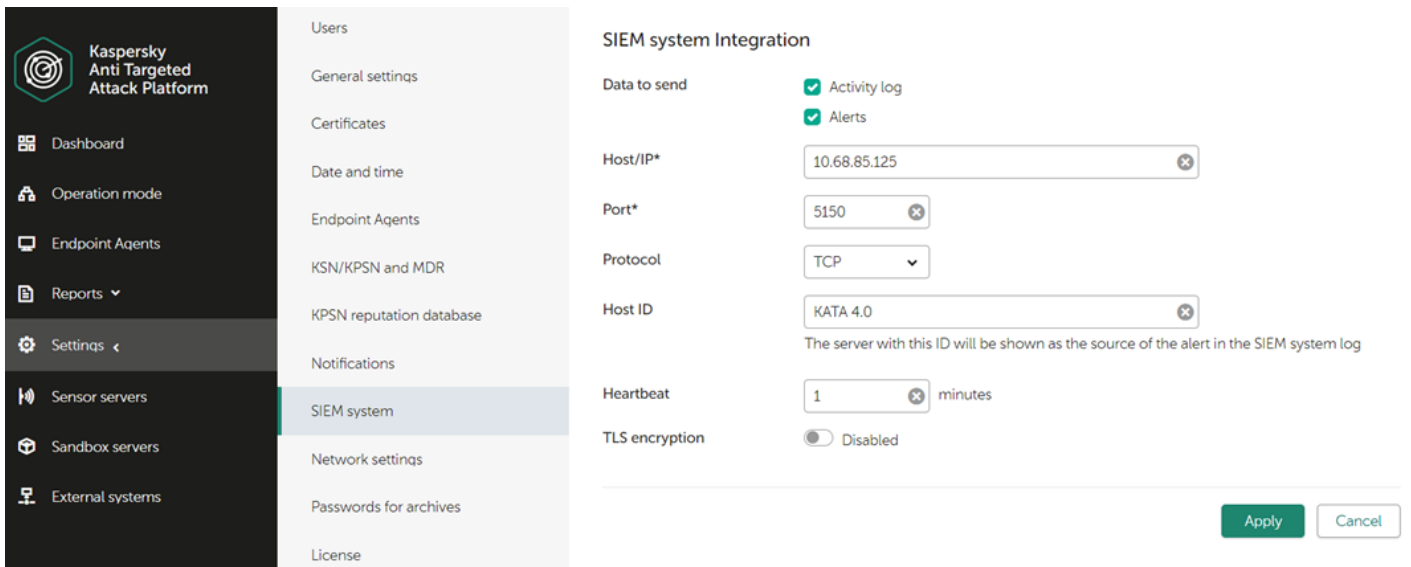
Host/IP: ip или fqdn адрес коллектора KUMA

Port: порт коллектора KUMA

Protocol: TCP или UDP

Host ID: напр., kata-cn

Heartbeat: интервал в минутах



????????? KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий Kaspersky Anti Targeted Attack Platform.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне KATA.
2. На шаге **Парсинг** событий выберите нормализатор **[ООТВ] KATA**.
3. На шаге **Маршрутизация** проверьте, что в набор ресурсов коллектора добавлены следующие точки назначения:

- **Хранилище**. Для отправки обработанных событий в хранилище.
- **Коррелятор**. Для отправки обработанных событий в коррелятор.

Если точки назначения **Хранилище** и **Коррелятор** не добавлены, создайте их.

4. На шаге **Проверка параметров** нажмите **Сохранить и создать сервис**.
5. Скопируйте появившуюся команду для установки коллектора KUMA.

????????? ???????

Настройка получения событий KATA/EDR (онлайн-справка KUMA):

<https://support.kaspersky.com/help/KUMA/3.2/ru-RU/240690.htm>

Updated 2026-03-11 08:40:09 UTC by lerat