Получение событий с Windows устройств при помощи KES

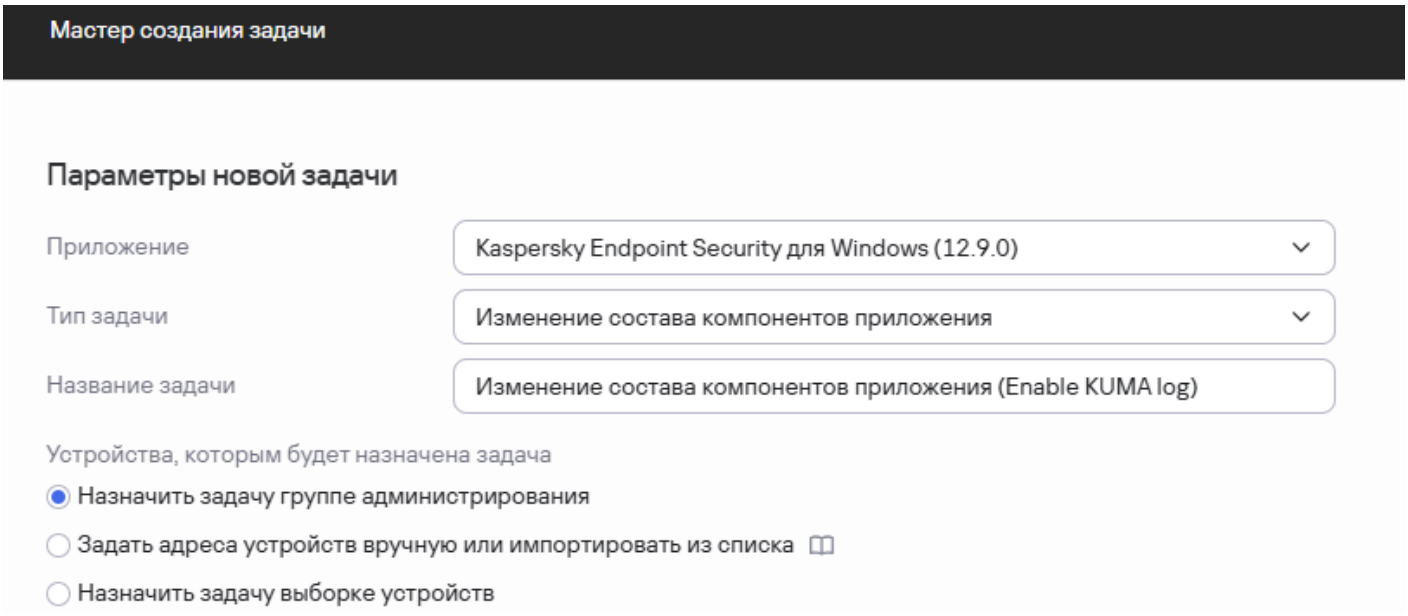
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Официальная документация

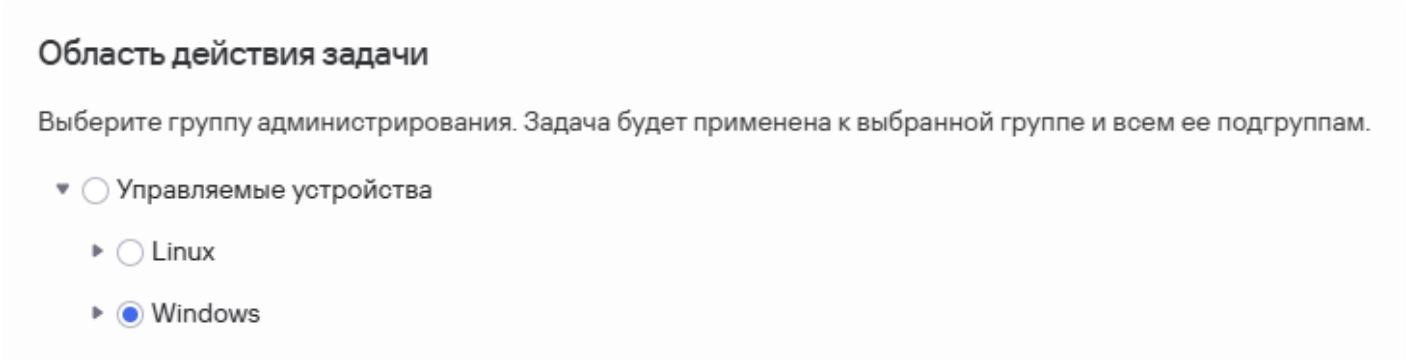
> Список передаваемых событий ограничен! Подробнее Приложение. События журналов Windows, отправляемые в KUMA

Чтобы получать устройства с устройств Windows (с KES) нам понадобится:

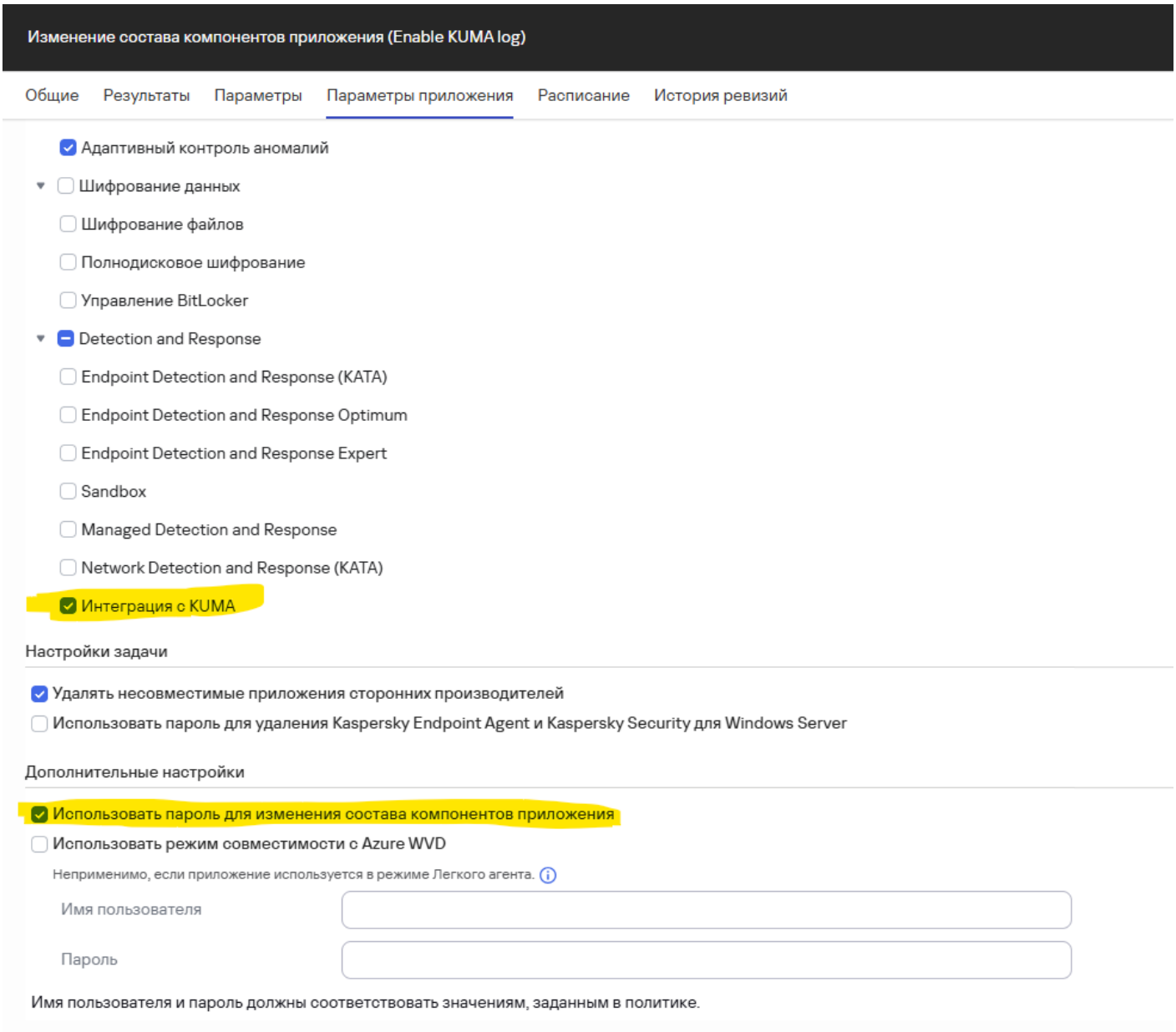
1. В KSC создать задачу на изменение состава компонентов приложения:
1.1 Создаём задачу с параметрами как на скриншоте



1.2 Выбираем группу устройств, к которой будет применена задача

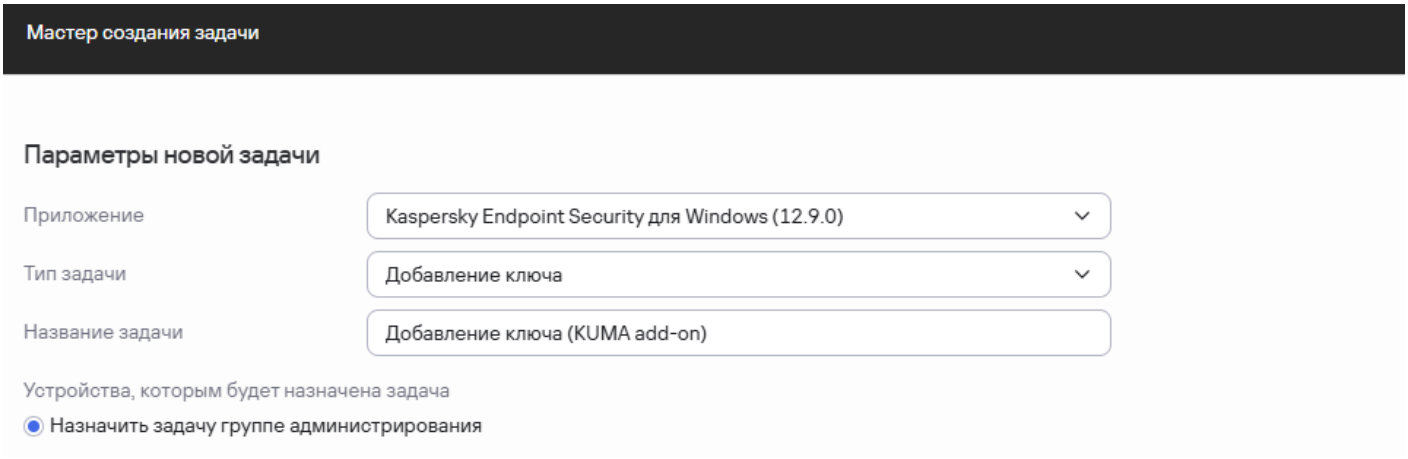


1.3 После создания задачи попадаем в свойства задачи, переходим в Параметры приложения и ставим галочку напротив "Интеграция с KUMA". Внимание, если у Вас используется пароль для удаления продукта - необходимо проставить галочку напротив "Использовать пароль для изменения состава компонентов приложения" и указать пользователя и пароль.

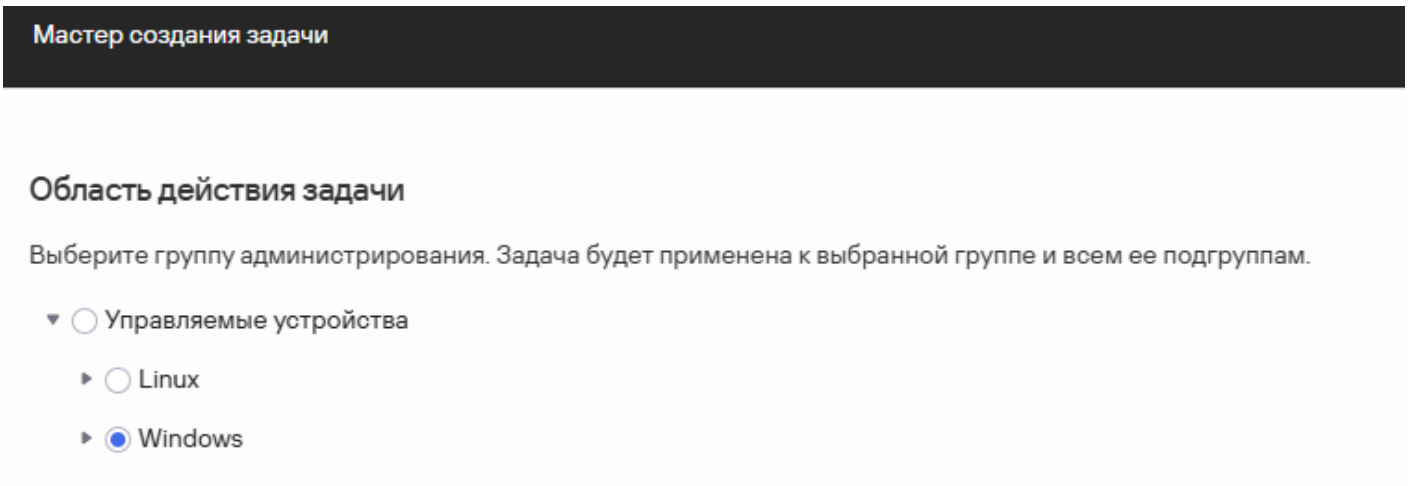


2. З**адачу добавления ключа в KSC**

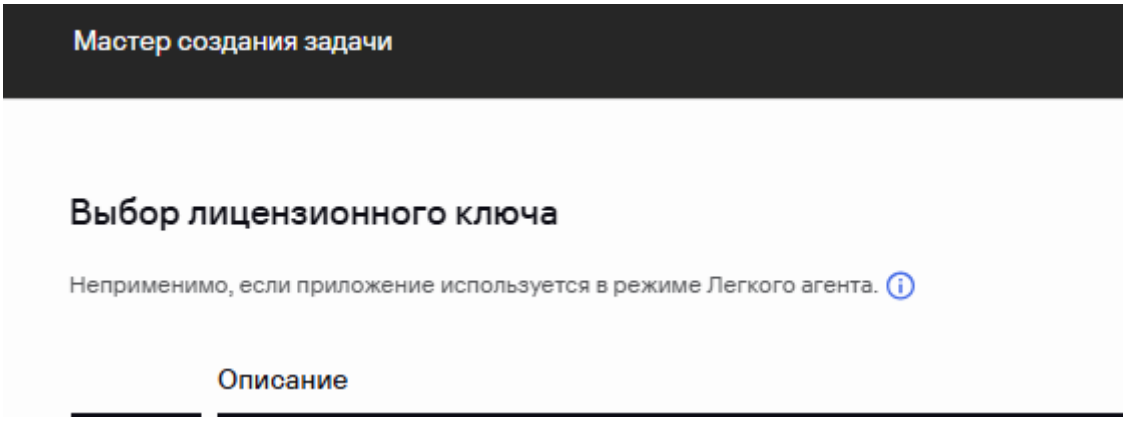
2.1 Создаём задачу как на скриншоте

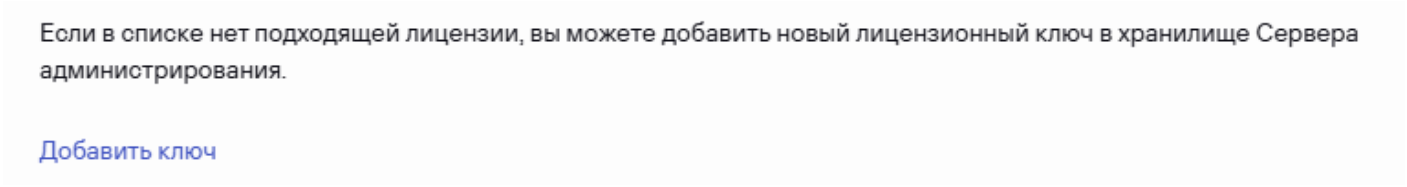


2.2 Также определяем группу для которой будет запущена задача



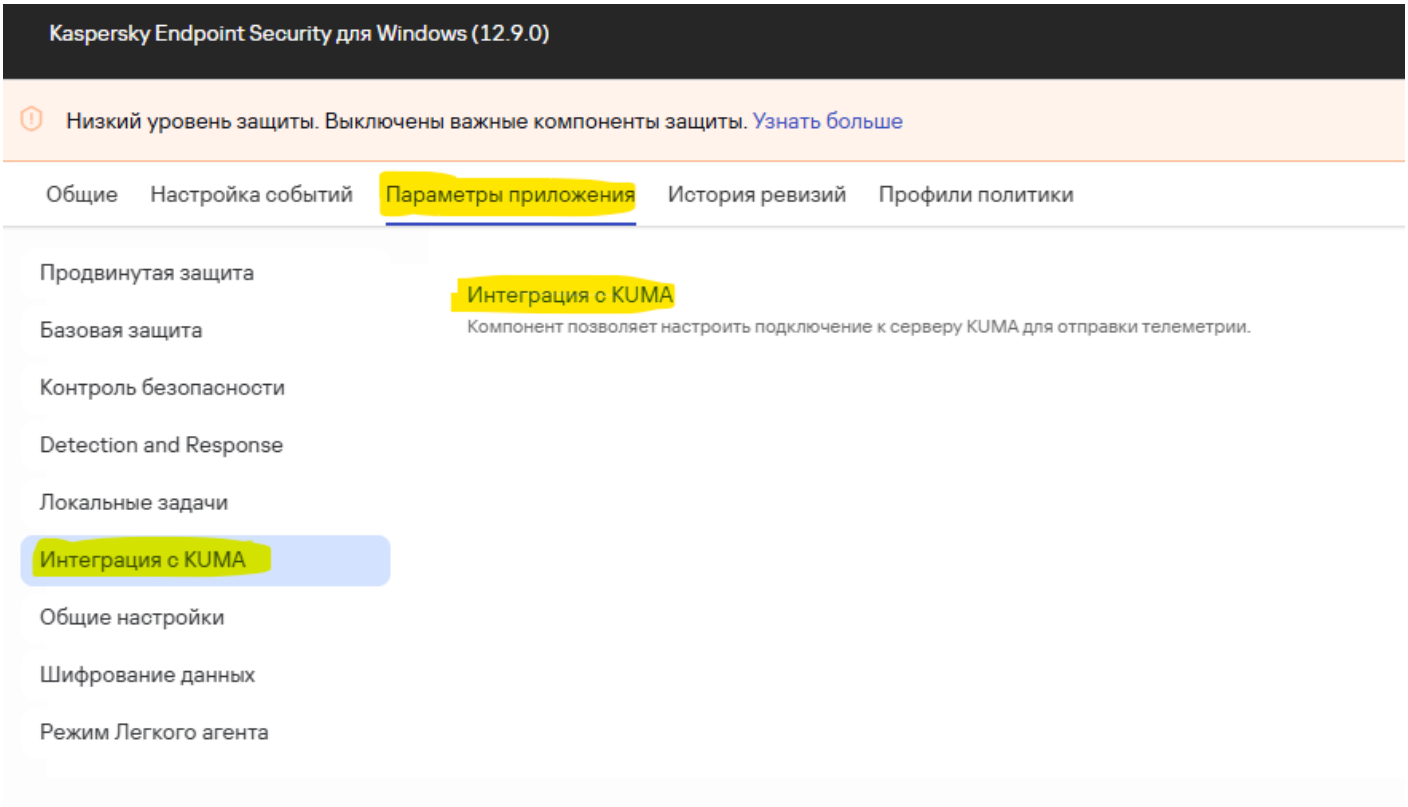
2.3 Подгружаем лицензионный ключ. Он должен идти вместе с ключём к KUMA. Описание какой ключ нам нужный будет находиться в файле CompatibilityList (идёт в архиве с лицензией). Нужный нам ключ указан в файле с описанием Kaspersky Endpoint Security 12 for Win KUMA Integration Add-on.
Нажимаем "Добавить ключ" и подгружаем файл



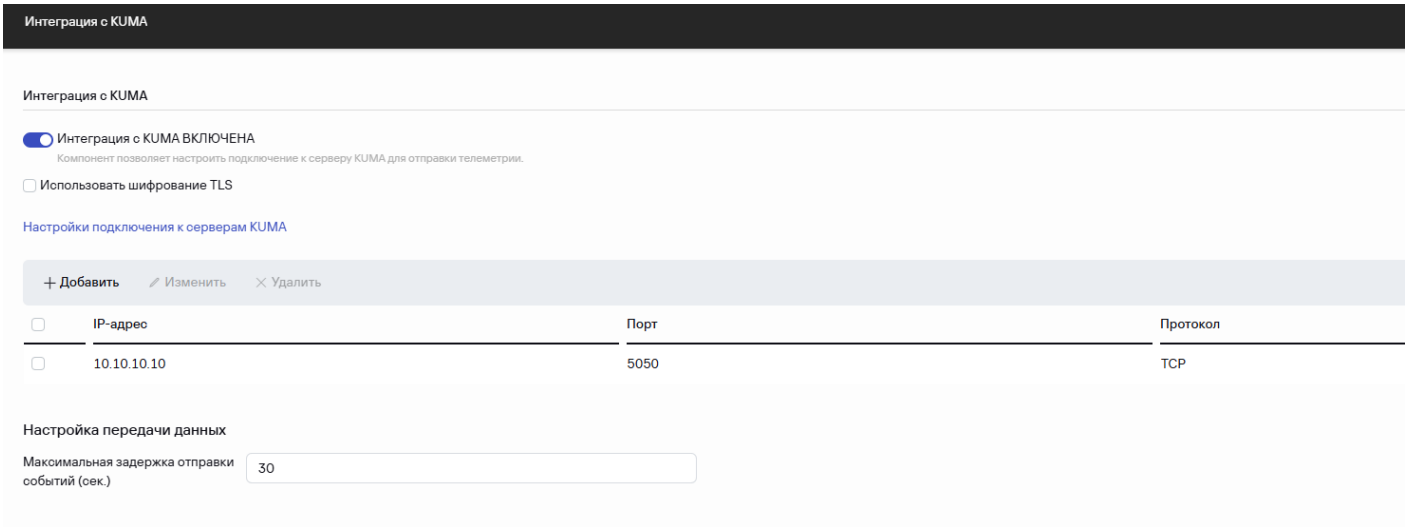


3. Правка политики

3.1 Переходим в политику Kaspersky Endpoint Security для Windows, далее в Параметры приложения выбираем интеграция с KUMA



3.2 Задаём параметры коллектора KUMA

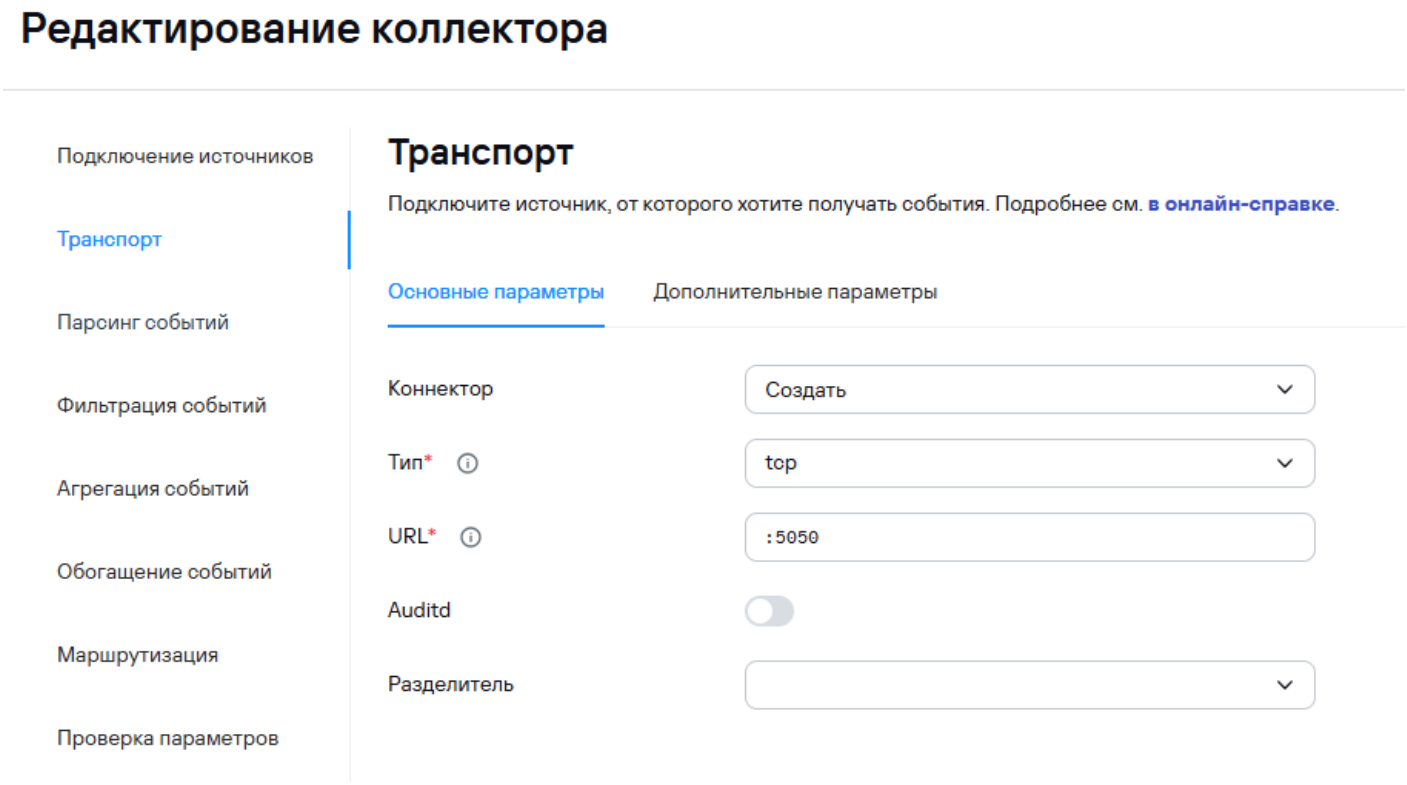


3.3 Жмём ОК - Сохранить и закрыть

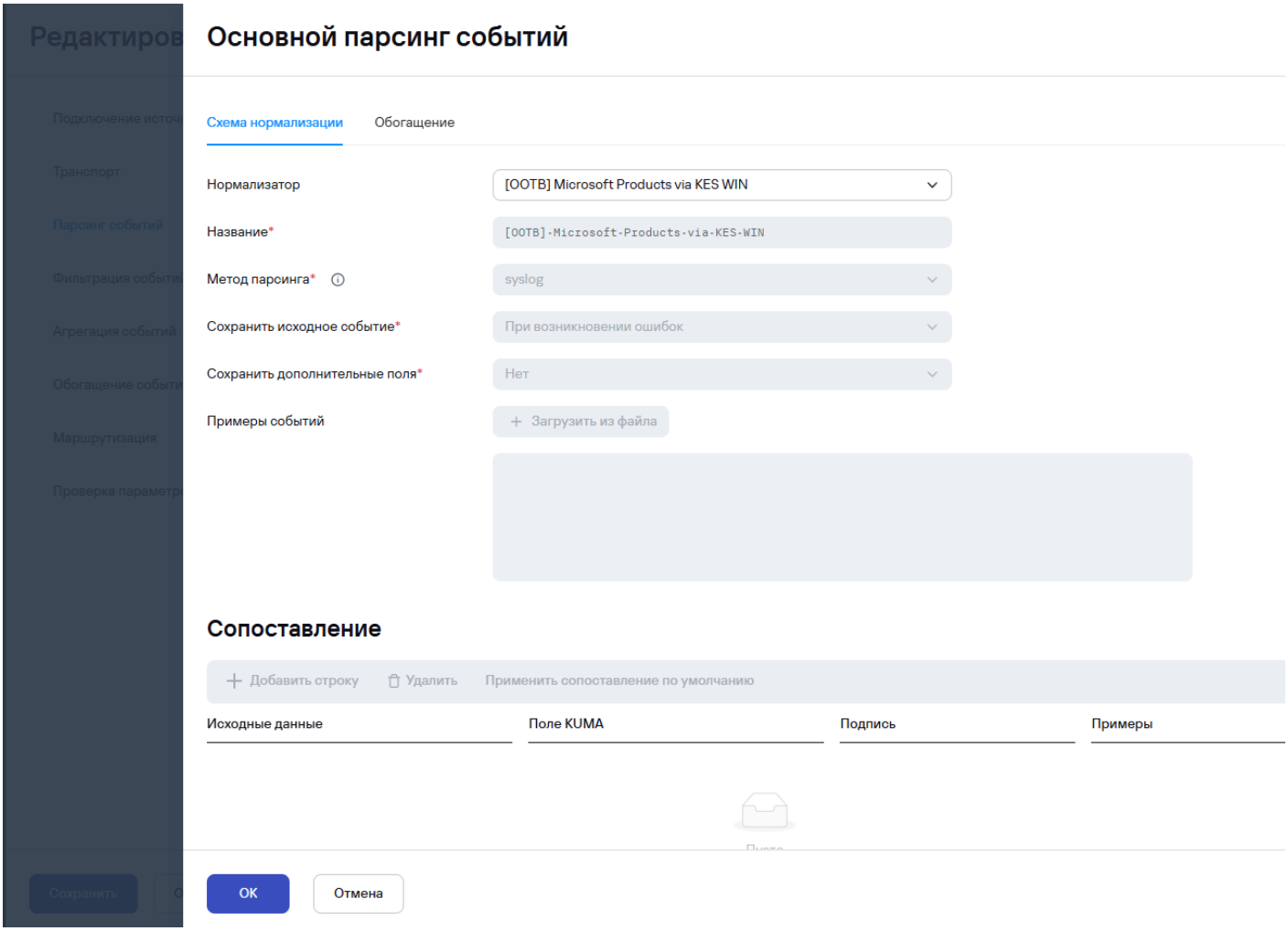
4. Возвращаемся в задачи и запускаем вручную задачи созданные в пунктах 1 и 2

5. В KUMA создаём коллектор для получения событий (параметры задали в этапе

3.2), в разделе транспорт



Выбираем нормализатор событий в разделе "Парсинг событий"



Нормализатор можно использовать [OOTB] Microsoft Products via KES WIN

Указываем необходимые точки назначения и устанавливаем службу на необходимый сервер.

Revision #5
Created 5 May 2025 14:24:02 by Anton
Updated 7 May 2025 11:39:01 by Anton