

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

Мастер создания задачи

Параметры новой задачи

Приложение

Kaspersky Endpoint Security для Windows (12.9.0)


Тип задачи

Изменение состава компонентов приложения

Название задачи

Изменение состава компонентов приложения (Enable KUMA log)

Устройства, которым будет назначена задача

- ☒ Назначить задачу группе администрирования
- ☐ Задать адреса устройств вручную или импортировать из списка 
- ☐ Назначить задачу выборке устройств

1.2 Выбираем группу устройств, к которой будет применена задача

Область действия задачи

Выберите группу администрирования. Задача будет применена к выбранной группе и всем ее подгруппам.

- ▼ ☐ Управляемые устройства
 - ▶ ☐ Linux
 - ▶ ☒ Windows

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.

Изменение состава компонентов приложения (Enable KUMA log)

Общие Результаты Параметры Параметры приложения Расписание История ревизий

- ☒ Адаптивный контроль аномалий
- ▼ ☐ Шифрование данных
 - ☐ Шифрование файлов
 - ☐ Полнодисковое шифрование
 - ☐ Управление BitLocker
- ▼ ☒ Detection and Response
 - ☐ Endpoint Detection and Response (KATA)
 - ☐ Endpoint Detection and Response Optimum
 - ☐ Endpoint Detection and Response Expert
 - ☐ Sandbox
 - ☐ Managed Detection and Response
 - ☐ Network Detection and Response (KATA)
 - ☒ Интеграция с KUMA

Настройки задачи

- ☒ Удалять несовместимые приложения сторонних производителей
- ☐ Использовать пароль для удаления Kaspersky Endpoint Agent и Kaspersky Security для Windows Server

Дополнительные настройки

- ☒ Использовать пароль для изменения состава компонентов приложения

- ☐ Использовать режим совместимости с Azure WVD

Неприменимо, если приложение используется в режиме Легкого агента. ⓘ

Имя пользователя

Пароль

Имя пользователя и пароль должны соответствовать значениям, заданным в политике.

2. Задачу добавления ключа в KSC

2.1 Создаём задачу как на скриншоте

Мастер создания задачи

Параметры новой задачи

Приложение

Kaspersky Endpoint Security для Windows (12.9.0) ▾

Тип задачи

Добавление ключа ▾

Название задачи

Добавление ключа (KUMA add-on)

Устройства, которым будет назначена задача

☒ Назначить задачу группе администрирования

2.2 Также определяем группу для которой будет запущена задача

Мастер создания задачи

Область действия задачи

Выберите группу администрирования. Задача будет применена к выбранной группе и всем ее подгруппам.

▼ ☐ Управляемые устройства

▶ ☐ Linux

▶ ☒ Windows

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

Мастер создания задачи

Выбор лицензионного ключа

Неприменимо, если приложение используется в режиме Легкого агента. ⓘ

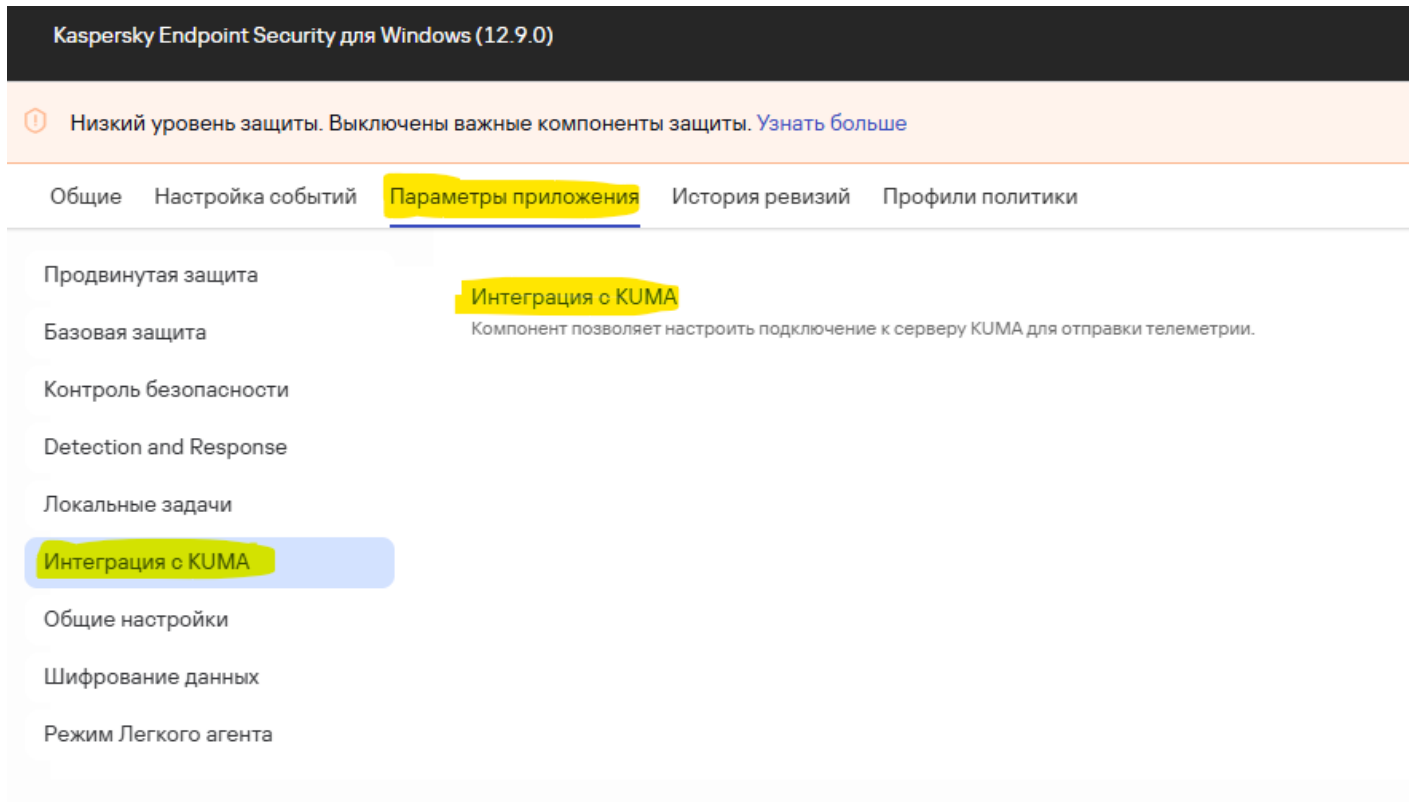
Описание

Если в списке нет подходящей лицензии, вы можете добавить новый лицензионный ключ в хранилище Сервера администрирования.

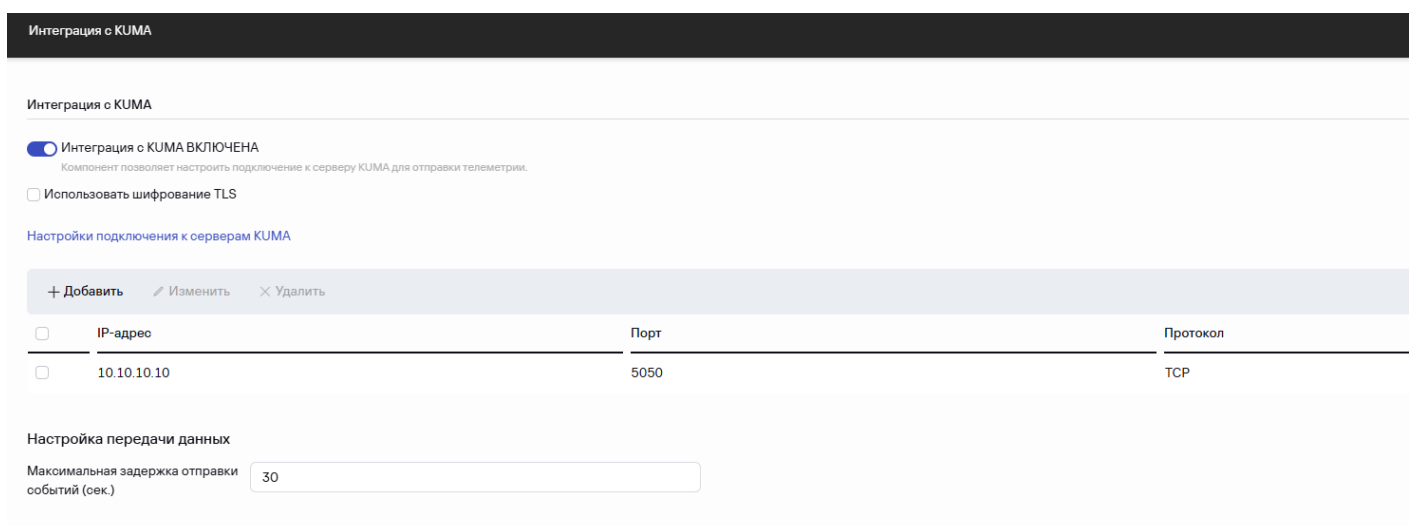
[Добавить ключ](#)

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 коллেকтора 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

Редактирование коллектора

Подключение источников

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры

Дополнительные параметры

Коннектор

Создать

Тип* ⓘ

top

URL* ⓘ

:5050

Auditd

☐

Разделитель

Выбираем нормализатор событий в разделе "Парсинг событий"

Редактирование

Основной парсинг событий

Подключение источника

Транспорт

Парсинг событий

Фильтрация событий

Агрегация событий

Обогащение событий

Маршрутизация

Проверка параметров

Схема нормализации

Обогащение

Нормализатор

[OOTB] Microsoft Products via KES WIN

Название*

[OOTB]-Microsoft-Products-via-KES-WIN

Метод парсинга* ⓘ

syslog

Сохранить исходное событие*

При возникновении ошибок

Сохранить дополнительные поля*

Нет

Примеры событий

+ Загрузить из файла

Сопоставление

+ Добавить строку

Удалить

Применить сопоставление по умолчанию

Исходные данные	Поле KUMA	Подпись	Примеры
<div><div>Иконка папки</div><div>Пусто</div></div>			

Сохранить

Отмена

Нормализатор можно использовать [OOTB] Microsoft Products via KES WIN

Указываем необходимые точки назначения и устанавливаем службу на необходимый сервер.