# KSMG 2.0

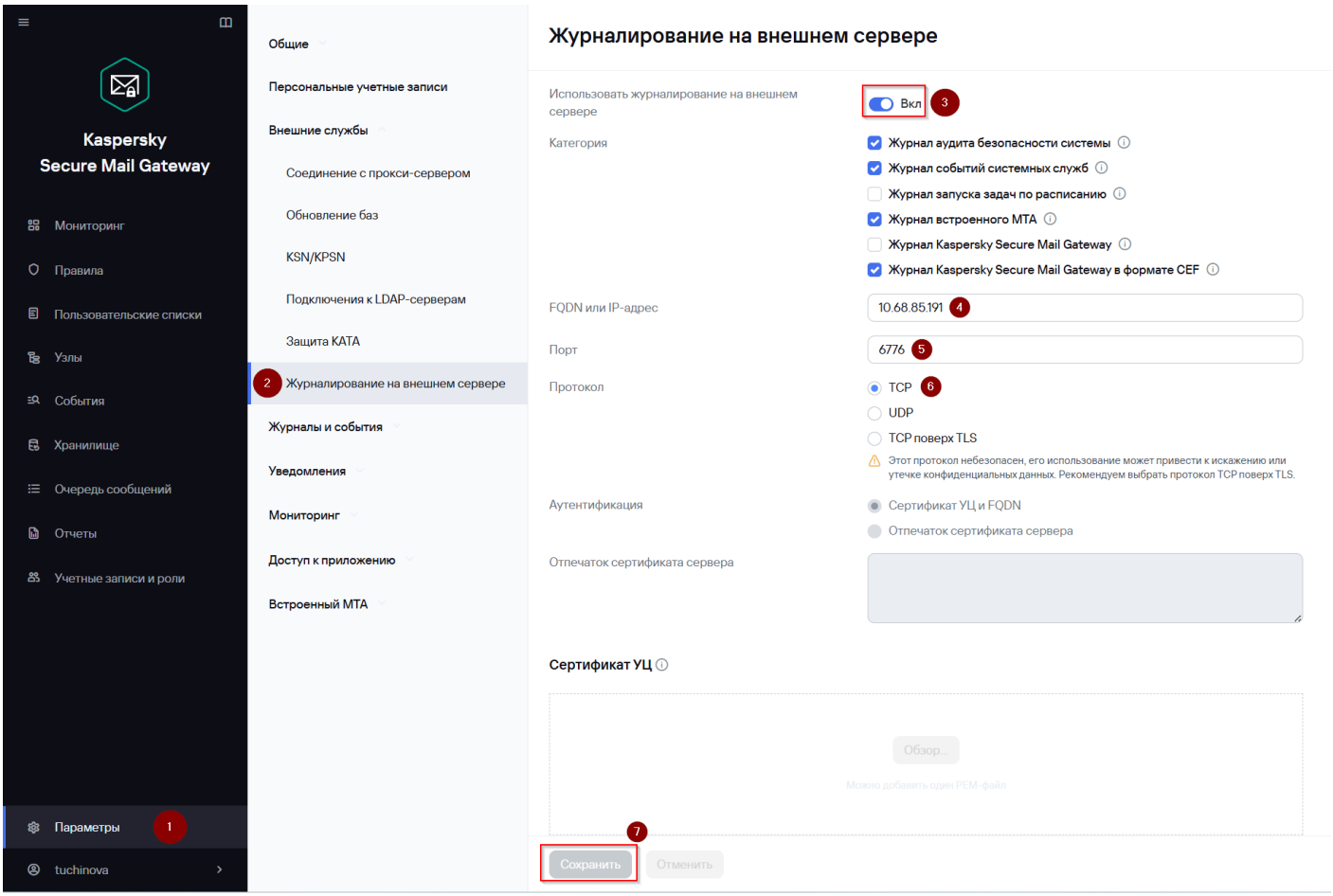
> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

# ????????? ???????? ??????? KSMG ? KUMA

> Настройка отправкм логов для актуальной версии KSMG 2.1.1VA доступно из справки - https://support.kaspersky.com/KSMG/2.1.1VA/ru-RU/218660.htm

> Данная инструкция применима для KSMG версии от 2.1.1VA и KUMA 4.0:

В меню KSMG необходимо перейти в "Параметры" -> Журналирование на внешнем сервере -> Поставить флажок в "Использовать журналирование на внешнем сервере" и далее настроить соответсвующие параметры для коннекта с KUMA, нажать сохранить.

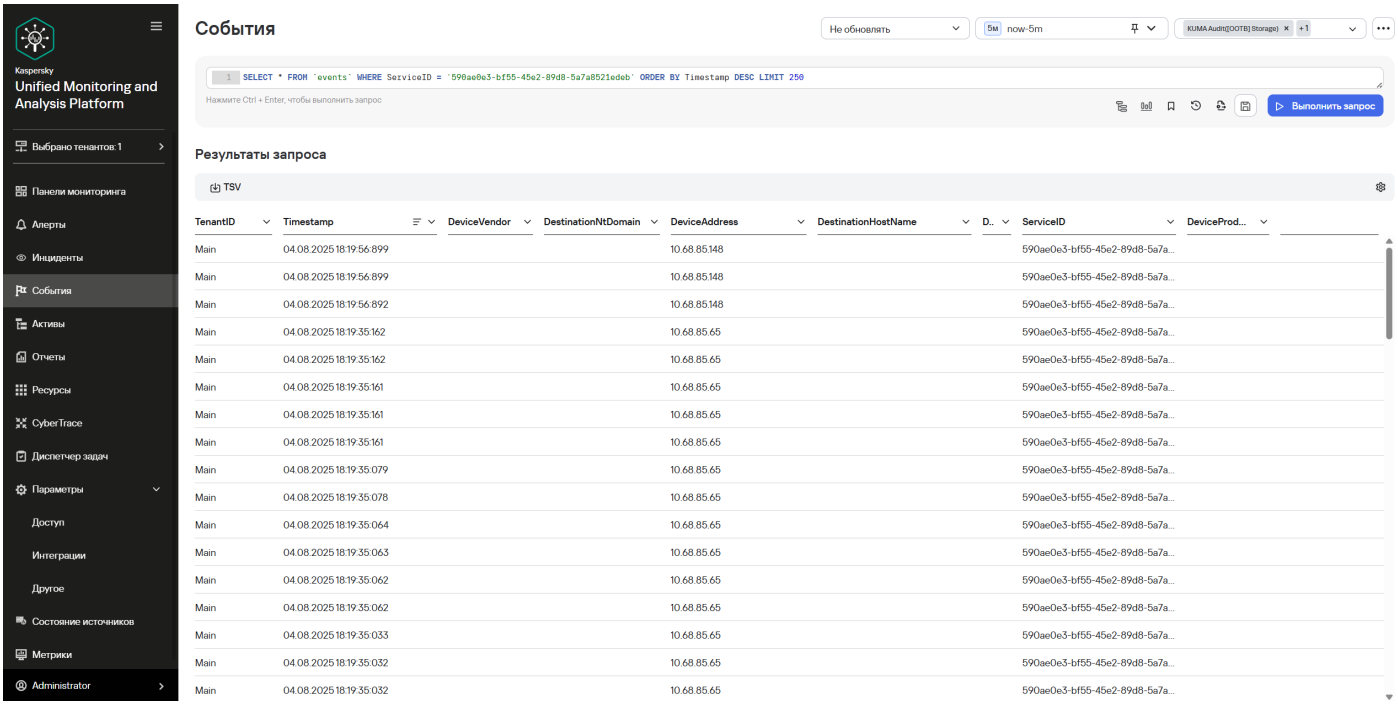


**Возможные категории: событий**

- Журнал аудита безопасности системы (authpriv).
- Журнал событий системных служб (daemon).
- Журнал запуска задач по расписанию (cron).
- Журнал встроенного MTA (mail).
- Журнал Kaspersky Secure Mail Gateway (local1).
- Журнал Kaspersky Secure Mail Gateway в формате CEF (local2).

По умолчанию категория не выбрана.

Далее проверка событий через коллектор, который настроен на сбор событий с KSMG:




# ???????? ??????? KSMG < 2.1.1VA ? KUMA 3.4

1. Подключитесь к серверу KSMG по проколу SSH под учетной записью с правами администратора перейдите в меню Technical Support Mode.

2. Внесите следующие изменения в файл с параметрами экспорта событий `/opt/kaspersky/ksmg/share/templates/core_settings/event_logger.json.template`:

```
"siemSettings":
{
"enabled": true,
```

```
"facility": "Local2",
"logLevel": "Info",
"formatting":
}
```

Прочие параметры оставьте без изменений.

> Перед внесением изменений в файл `/etc/rsyslog.conf` рекомендуется сделать его резервную копию. Ошибка при редактировании файла может привести к некорректной работе системы.

3. В файле `/etc/rsyslog.conf` измените строку:

```
*.info;mail.none;authpriv.none;cron.none;local0.none;local1.none /var/log/messages
```

на

```
*.info;mail.none;authpriv.none;cron.none;local0.none;local1.none;local2.none /var/log/messages
```

4. Добавьте в файл `/etc/rsyslog.conf` следующую строку:

```
local2.* -/var/log/ksmg-cef-messages
```

5. Создайте файл `/var/log/ksmg-cef-messages` и настройте права доступа к нему. Для этого выполните команды:

```
touch /var/log/ksmg-cef-messages
chown root:klusers /var/log/ksmg-cef-messages
chmod 640 /var/log/ksmg-cef-messages
```

6. Настройте правила ротации файлов с экспортированными событиями. Для этого добавьте в файл `/etc/logrotate.d/ksmg-syslog` следующие строки:

```
/var/log/ksmg-cef-messages
{
size 500M
rotate 10
notifempty
sharedscripts
postrotate
/usr/bin/systemctl kill -s HUP rsyslog.service >/dev/null 2>&1 || true
```

```
endscript
}
```

7. Перезапустите сервис rsyslog с помощью следующей команды:

```
service rsyslog restart
```

> Если вам не требуется сохранять файлы локально, пропустите шаги 4–7 из инструкции выше

8. В веб-интерфейсе приложения в разделе **Параметры** → **Журналы и события** → **События** внесите изменение в значение любого параметра и нажмите на кнопку **Сохранить**.

Это необходимо для синхронизации параметров между узлами кластера и применения изменений, внесенных в конфигурационный файл. После этого вы можете вернуть исходное значение измененного параметра.

9. Внесите следующие изменения в файл `/etc/rsyslog.conf`:

```
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local2.* @<IP-адрес коллектора KUMA>:<порт коллектора>
```

Если вы хотите отправлять события по протоколу TCP, последняя строчка должна выглядеть следующим образом:

```
local2.* @@<IP-адрес коллектора KUMA>:<порт коллектора>
```

10. Перезапустите службу rsyslog. Для этого выполните команду:

```
service rsyslog restart
```

---

# ????????? KUMA

После того как параметры передачи событий настроены, требуется создать коллектор в веб-интерфейсе KUMA для событий KSMG.

1. На шаге **Транспорт** укажите тип и порт в соответствии с настройками на стороне KSMG.

2. На шаге **Парсинг** событий выберите нормализатор **[OOTB] KSMG**.

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.

> В случае если события не поступают перезапустите сервис rsyslog несколько раз

---

# ???????? ??????

Публикация событий в SIEM-систему (онлайн-справка KSMG):

https://support.kaspersky.com/KSMG/2.0.1/ru-RU/151504.htm

---

Revision #26
Created 2023-08-11 08:05:18 UTC by Koala
Updated 2026-03-11 10:37:04 UTC by Boris Rzr