KSMG 2.0

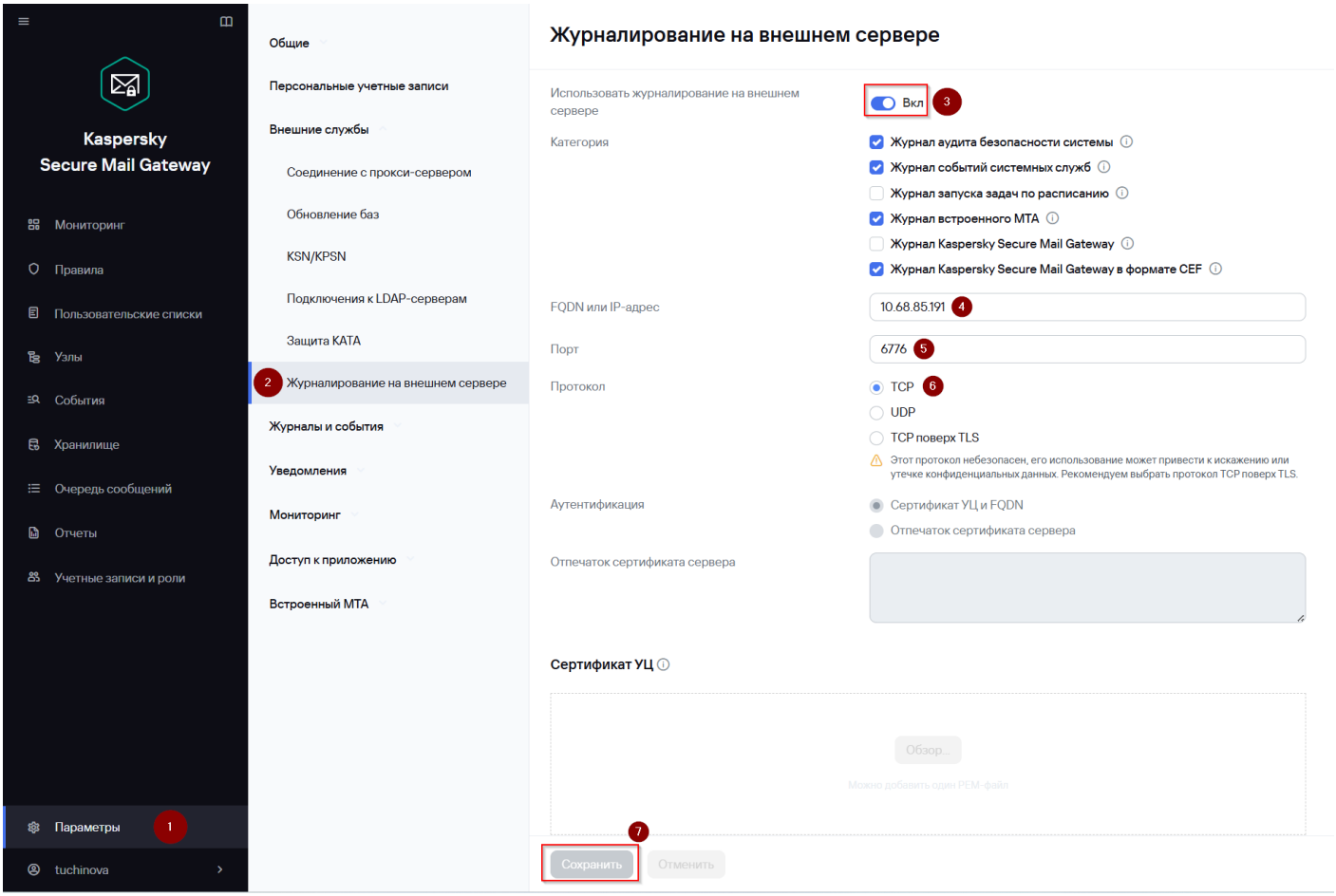
?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **НЕ** ???????? ??????????? ????????????? ???????.

Настройка передачи событий KSMG в KUMA

????????? ???????? ????? ??? ?????????? ?????? KSMG 2.1.1VA ???????? ?? ??????? - https://support.kaspersky.com/KSMG/2.1.1VA/ru-RU/218660.htm

?????? ?????????? ????????? ??? KSMG ?????? ?? 2.1.1VA ? KUMA 4.0:

? ???? KSMG ?????????? ??????? ? "??????????" -> ????????????? ?? ??????? ??????? -> ????????? ?????? ? "???????????? ????????????? ?? ??????? ???????" ? ????? ????????? ????????????? ????????? ??? ???????? ? KUMA, ?????? ?????????.

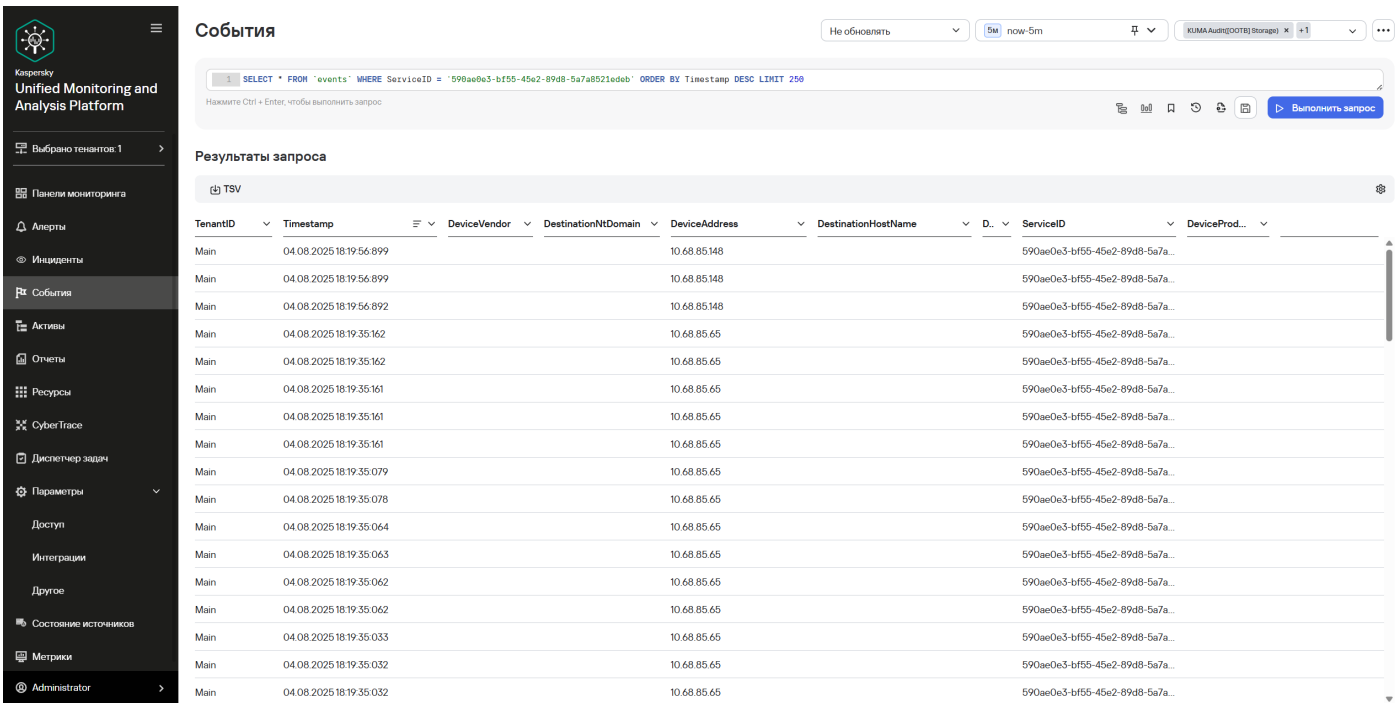


Возможные категории: событий

- ?????? ?????? ???????????? ??????? (authpriv).
- ?????? ??????? ????????? ????? (daemon).
- ?????? ??????? ????? ?? ?????????? (cron).
- ?????? ??????????? MTA (mail).
- ?????? Kaspersky Secure Mail Gateway (local1).
- ?????? Kaspersky Secure Mail Gateway ? ??????? CEF (local2).

?? ????????? ????????? ?? ???????.

????? ???????? ??????? ????? ?????????, ??????? ???????? ?? ???? ??????? ? KSMG:



Передача событий KSMG < 2.1.1VA в KUMA 3.4

1. ???????????? ? ??????? KSMG ?? ??????? SSH ??? ??????? ??????? ? ??????? ????????????? ????????? ? ???? Technical Support Mode.

2. ??????? ????????? ????????? ? ???? ? ??????????? ???????? ??????? `/opt/kaspersky/ksmg/share/templates/core_settings/event_logger.json.template`:

```
"siemSettings":
{
"enabled": true,
"facility": "Local2",
"logLevel": "Info",
"formatting":
}
```

?????? ????????? ???????? ??? ?????????.

> ????? ????????? ????????? ? ???? `/etc/rsyslog.conf` ???????????? ??????? ??? ????????? ?????. ?????? ??? ????????????? ????? ????? ???????? ? ??????????? ?????? ???????.

3. ? ????? `/etc/rsyslog.conf` ???????? ??????:

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

??

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

4. ???????? ? ???? `/etc/rsyslog.conf` ????????? ??????:

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

5. ???????? ???? `/var/log/ksmg-cef-messages` ? ????????? ????? ??????? ? ????. ??? ????? ????????? ???????:

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

6. ????????? ??????? ??????? ?????? ? ???????????????? ?????????. ??? ????? ???????? ? ???? `/etc/logrotate.d/ksmg-syslog` ????????? ??????:

```
/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. ????????????? ?????? rsyslog ? ??????? ????????? ???????:

```
service rsyslog restart
```

> ???? ??? ?? ????????? ????????? ????? ????????, ?????????? ???? 4–7 ?? ?????????? ????

8. ? ???-?????????? ?????????? ? ??????? **Параметры** ? **Журналы и события** ? **События** ??????? ????????? ? ???????? ?????? ????????? ? ??????? ?? ?????? **Сохранить**.

??? ?????????? ??? ????????????? ????????? ????? ?????? ???????? ? ????????? ????????, ????????? ? ??????????????? ????. ????? ????? ?? ?????? ??????? ???????? ???????? ?????????? ?????????.

9. ??????? ????????? ????????? ? ???? `/etc/rsyslog.conf`:

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

???? ?? ?????? ?????????? ??????? ?? ????????? TCP, ????????? ??????? ?????? ????????? ????????? ???????:

```
local2.* @@<IP-????? ?????????? KUMA>:<???? ??????????>
```

10. ????????????? ?????? rsyslog. ??? ????? ????????? ???????:

```
service rsyslog restart
```

Настройка KUMA

????? ???? ??? ????????? ???????? ??????? ?????????, ????????? ??????? ????????? ? ???-?????????? KUMA ??? ??????? KSMG.

1. ?? ???? **Транспорт** ??????? ??? ? ???? ? ??????????? ? ??????????? ?? ??????? KSMG.

2. ?? ???? **Парсинг** ??????? ???????? ???????????? **[OOTB] KSMG**.

3. ?? ???? **Маршрутизация** ?????????, ??? ? ????? ???????? ?????????? ????????? ????????? ????? ??????????:

- Хранилище. ??? ???????? ??????????? ??????? ? ?????????.

- Коррелятор. ??? ???????? ??????????? ??????? ? ??????????.

???? ????? ?????????? **Хранилище** ? **Коррелятор** ?? ?????????, ???????? ??.

4. ?? ???? **Проверка параметров** ??????? **Сохранить и создать сервис**.

5. ?????????? ??????????? ??????? ??? ????????? ?????????? KUMA.

? ?????? ???? ??????? ?? ????????? ????????????? ?????? rsyslog ????????? ???

Полезные ссылки

?????????? ??????? ? SIEM-??????? (??????-??????? 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