

# KSC: ?????????? ??????? ?????????? ?????????? ? SIEM (Syslog/CEF)

Официальная документация по настройке автоматического экспорта событий в SIEM-системы: <https://support.kaspersky.ru/ksc/14.2/151333>

?? ?????????? KSC ?????? ??????? ?? Syslog ?? ?????? 100 ????? ??????? 30 ??????. ??? ???????  
????????????? ?????????????? ??????????? ?/??? ?????????????????? ?????????? ?????? ?????????????? ??????????, ??????  
????????? ? KSC ?????? ?? ?????????? ?????????????????? ? SIEM, ? ?????? ?????????? ?????????? ?????????? ??  
??????????.

Изменить значение по экспорту событий, можно в реестре в системе с установленным Сервером администрирования.

Раздел:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

Флаги:

- KLSPLG\_READ\_MAX\_COUNT\_SF - количество событий, обрабатываемых в каждой итерации. Значение по умолчанию - 100 (в десятичной форме)
- KLSPLG\_READ\_DB\_PERIOD\_SF - скорость итерации в миллисекундах. По умолчанию 30000 (в десятичной форме).

?????????? ? ?????????? ?????????? ?? ?????????? ?????? ? ??????????????????. ?????????? ?????????? ??????  
?????????? ?? ?????? ?????????????????????????????? ??????????. ?????????????????? ?????????????? ??????????????  
??????????, ?????????????????? ?????? ??? ?? KSC, ??? ? ?? ??? ?????.