

KSC: увеличение лимита экспорта событий в 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, ??? ? ?? ??? ?????.