

Выгрузка логов с устройства

Отправка команды «Запрос журналов Монитора» на устройства Android позволяет получить файл архив, содержащий логи устройства следующих типов:

- *Логи «Монитора» – фиксируются все события работы с системой «SafeMobile». Максимальный уровень логирования Verbose. Файлы логов располагаются в папке /logs.*
- *Security – лог событий безопасности в ОС Android устройства. Максимальный уровень логирования Info. Файлы логов располагаются в папке /devicelogs/security.*
- *Network – лог сетевых событий в ОС Android устройства. Уровень логирования задать нельзя. ОС Android кеширует и отдает в «SafeMobile» с задержкой, о величине задержки узнать можно только экспериментальным путем. Если перезагрузить устройство, то устройство выдаст логи без задержки. Файлы логов располагаются в папке /devicelogs/network.*
- *Logcat – лог событий в ОС Android устройства. Уровень логирования задать нельзя, логи закольцованы, по принципу FIFO. Файл расположен в папке /logs.*

Чтобы получить файл архив с логами устройства следует выполнить следующие действия:

1. Перейти в раздел «Управление устройствами – Команды».
2. В списке устройств найти устройство, с которого необходимо получить файл архив логов. И отправить на него команду «Запрос журналов Монитора» (Рисунок 1). Команда будет выполнена когда устройство будет включено. При выполнении команды предыдущий файл в логах в системе заменяется новым.

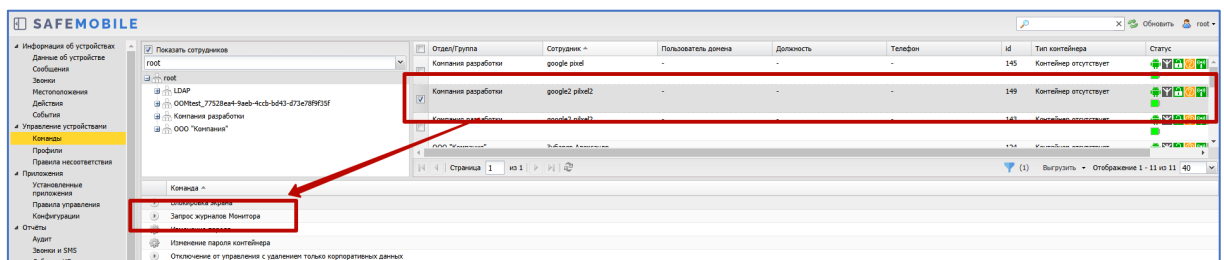


Рисунок 1 - Команда "Запрос журнала Монитора"

3. Скачать архив содержащий логи в разделе «Информация об устройствах – Данные устройства». Кнопка скачивания файла находится во вкладке «Общие», блок информации «Журналы монитора» (Рисунок 2) и будет доступна после выполнения команды устройством.

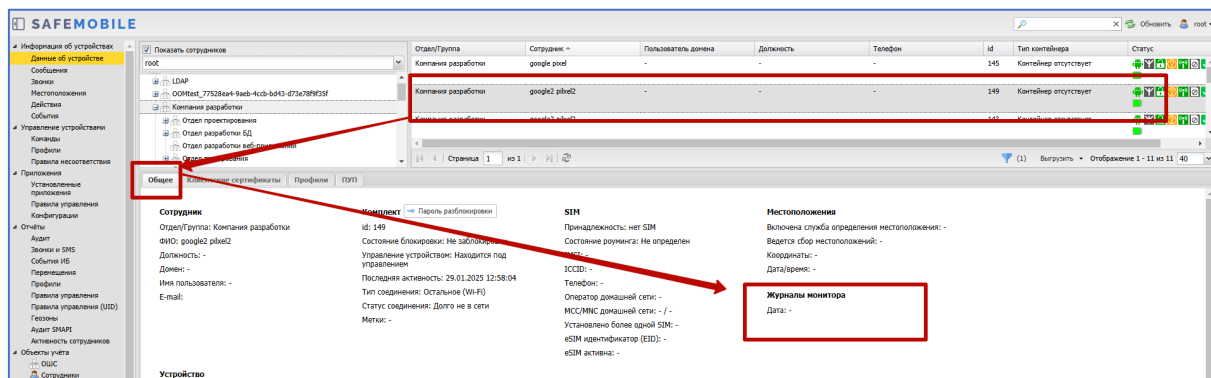


Рисунок 2 - Расположение кнопки скачивания файла

Настройка состава и размеров логов осуществляется настройкой профиля «Настройки журналов Android» и назначением его на устройство. Позволяет задавать такие параметры как:

- Вести журнал Монитора – Да/Нет;
 - Уровень логирования журнала Монитора – Verbose, Debug, Info, Warning, Error, Fatal Error, Не задано;
 - Максимальное число файлов журнала Монитора;
 - Максимальный размер одного файла журнала Монитора (Кбайт);
 - Интервал ротации файлов журнала (минуты);
- При выгрузке логов включать журнал logcat – Да/Нет;
- Вести журнал событий безопасности системы – Да/Нет;
 - Уровень логирования журнала событий безопасности системы - Info, Warning, Error, Не задано;
 - Максимальное число файлов журнала событий безопасности системы;
 - Максимальный размер одного файла журнала событий безопасности системы (Кбайт);
 - Сохранять события безопасности непосредственно перед последней перезагрузкой системы (поддерживается не всеми устройствами) – Да/Нет;
- Вести журнал сетевых событий системы – Да/Нет;
 - Максимальное число файлов журнала сетевых событий;
 - Максимальный размер одного файла журнала сетевых событий (Кбайт).

Ограничения в использовании:

Для скачивания файла логов администратор должен обладать полномочиями «Выгрузка журналов Монитора».

Для получения логов событий устройства должны соответствовать следующим требованиям (версия ОС Android и стратегии подключения устройства):

Сетевые события (Network logs):

- Android 8 + Device Owner;
- Android 12 + (Device Owner | Profile Owner).

События безопасности (Security logs):

- Android 7 + (Device Owner | Profile Owner);
- Фильтрация по LogLevel доступна начиная с Android 9

Отправка логов в агрегатор осуществляется по протоколу OTLP. Это необходимо учитывать в архитектуре системы.

Дополнительная информация по журналам «Security logs» и «Network logs»:

<https://developer.android.com/work/dpc/logging?hl=ru>

<https://developer.android.com/reference/android/app/admin/SecurityLog>