

Сценарии использования SMAPI

Внешнее API системы SafeMobile описано в [Swagger](#)-файле, содержащем подробную информацию о самих вызовах, но не об их последовательности. В [README](#) приведён синтаксис.

Настоящий документ дает представление об основных сценариях использования API и типичной последовательности вызовов, и предназначен для программистов, знакомых с APM.

Пониманию входных параметров поможет [Глоссарий](#) SMAPI.

1. [Как получить список устройств сотрудника](#)
2. [Как сгенерировать отчётность](#)
3. [Как переустановить приложение](#)
4. [Как добавить и установить свое приложение](#)
5. [Как получить географические координаты сотрудника](#)
6. [Как импортировать группу из Active Directory](#)
7. [Как изменить профиль или установить собственный](#)
8. [Как изменить ПУП или создать собственное](#)
9. [Как ограничить длину пароля сотрудников](#)
10. [Как по серийному номеру телефона получить информацию о сотруднике](#)
(список вопросов пополняется по Вашим заявкам...)

Как получить список устройств сотрудника?

1. `/api/v1/employee`

Запросите идентификатор сотрудника в SafeMobile `sm_employee_id` по его атрибутам в Active Directory `distinguished_name`, `employeeID` или `sAMAccountName`

2. `/api/v1/devices`

По `sm_employee_id` запросите список устройств, принадлежащих сотруднику. Это могут быть телефоны, планшеты, ноутбуки.

Среди множества параметров Вы получите не только телефонный номер и марку аппарата, но и информацию о eSIM, операционной системе, IMSI, а так же актуальном состоянии устройства.

В выдаче роута `/api/v1/devices`` будет находиться важный параметр ``mcc_id``. Это идентификатор устройства в SafeMobile. Пара ``sm_employee_id`` & ``mcc_id`` используется во всех адресуемых устройству API в качестве дополнительной авторизации.

Как сгенерировать отчётность?

Используйте роуты, имеющие в наименовании текстовый фрагмент «**list**». Все АПИ с этими роутами возвращают списки.

Длина списка задаётся параметром **limit**, но не может превышать 100 тыс. записей на страницу (по умолчанию).

Чтобы прочитать следующую страницу, необходимо повторить запрос, указав в нём значение **continuation_token**, взятое из предыдущей выдачи. Получение **continuation_token** не означает, что записи ещё имеются. Об их исчерпании Вы узнаете, только получив пустой список.

Для сокращения непроизводительной выдачи используйте фильтры, ограничивающие количество записей, например **start_date** и **end_date**.

Каждая запись списка - это словарь json, который можно распечатать в виде таблицы или преобразовать любым нужным способом. Содержимое словарей смотрите в [Swagger](#)-файле.

1. **/api/v1/employee/list**

Список всех сотрудников в системе с их основными параметрами (включая импортированные из Active Directory).

2. **/api/v2/kits/list**

Общий список всех комплектов (устройств) в системе. Каждая запись содержит идентификатор сотрудника **emp_id**, а так же ещё около ста полей, описывающие устройство и его состояние. У этого АПИ самая тяжёлая выдача, поэтому используйте фильтры и устанавливайте **limit**.

3. **/api/v1/assigned/profiles/list**

По разным причинам, Профиль управления устройством может не "долететь" до адресата. И тогда в АРМ он будет отображён как "назначенный", но фактически установлен на устройство не будет. Такое может быть при отсутствии связи с устройством.

Этот роут проверит систему и сообщит, какие профили на какие устройства не установились.

4. **/api/v1/coordinates/list**

Географические координаты всех устройств. Обновляются каждые 10 минут.

Можно узнать о перемещениях устройства, отфильтровав по **mcc_id** его владельца в выдаче **/api/v2/kits/list** (см. п.2 Отчётности).

5. **/api/v1/applist**

Покажет, какие приложения установлены на устройстве сотрудника.

6. **/api/v1/accesscode/list**

Список активных кодов приглашения выбранного сотрудника.

7. **/api/v1/app/rule/list**

Помогает понять, какие правила управления установлены для различных приложений.

8. **/api/v2/email/template/list**

Выдает список шаблонов электронной почты вместе с текстом шаблона, закодированном в base64.

9. **/api/v1/group/list**

Возвращает по distinguished_name идентификаторы группы в SM (**sg_id**, **sg_name**, **sg_type**), либо список идентификаторов всех групп системы, если distinguished_name опущен.

10. **/api/v1/safestore/applist**

Возвращает для устройства список ПУП, разрешающих пользователю самостоятельную установку приложений, доступных в SafeStore, из SMAPI.

11. **/api/v1/distrib/list**

Возвращает список всех приложений, дистрибутивы которых загружены в SM.

12. **/api/v1/ldap/list**

Возвращает список подключенных внешних каталогов, из которых производится импорт

сотрудников (AD, LDAP). Без параметров.

13. **/api/v1/profile/list**

Метод возвращает профили с политиками и условиями применения. Входящие параметры выполняют функции фильтра. Поддерживается пагинация.

Как переустановить приложение?

1. **Получите список устройств сотрудника** и сохраните идентификатор сотрудника

`sm_employee_id`.

Выберете устройство, на котором будете переустанавливать приложение, и сохраните идентификатор устройства `mcc_id`.

2. **/api/v1/applist**

Получите список приложений, установленных на устройстве, и выберите UID целевого приложения `app_uid`.

3. **/api/v1/reinstall/app**

Запросите переустановку выбранного приложения на данном устройстве по идентификаторам устройства, сотрудника и UID приложения.

Команда на переустановку будет добавлена в очередь команд.

Как добавить и установить свое приложение?

1. **/api/v1/app/distrib**

Загрузите в SM дистрибутив своего приложения (Android, Аврора, iOS).

Впоследствии Ваше приложение будет передаваться на устройство не только по Wi-Fi, но и по мобильной сети, поэтому размер имеет значение.

В выдаче АПИ помимо прочего Вы получите `appd_id` - это идентификатор Вашего приложения в SM, он пригодится на четвёртом шаге.

2. **/api/v2/app/rule/list**

Используя фильтр `app_uid`, запросите список ПУП (правил управления своим приложением).

В списке найдите и сохраните `appr_id` - это идентификатор ПУП в SM.

3. **/api/v1/app/rule/create_corporate**

Если нужного ПУП нет, предварительно создайте его, указав при необходимости условия применения.

Вы получите идентификатор созданного ПУП `appr_id`, он необходим на последнем шаге.

/api/v1/group/list,

По `distinguished_name` получите ИД группы для назначения ПУП `ot_id`

/api/v1/app/rule/assign

Назначьте ПУП по `appr_id` на подразделение ОШС по `ot_id`.

4. **/api/v1/app/rule/distrib**

В ПУП с идентификатором `appr_id`, замените ИД приложения на `appd_id`.

Если ПУП назначен на устройства, это вызовет массовую замену версии приложения.

Как получить географические координаты сотрудника?

1. **Получите список устройств сотрудника**

Выберете устройство для пеленгации и сохраните его идентификатор `mcc_id`.

2. **`/api/v1/coordinates/list`**

По фильтру `mcc_id` получите координаты устройства.

Координаты обновляются с 10-ти минутным интервалом.

Интервал можно изменить в профиле "Настройки сбора местоположений Android".

Как импортировать группу из Active Directory

1. **`/api/v1/ldap/list`**

Запросите список внешних каталогов (APM - Синхронизация данных AD - Внешние каталоги).

Сохраните ИД каталога `ldaps_id`.

2. **`/api/v1/ldap/set_sync_state`**

По `ldaps_id` выключите синхронизацию того каталога, откуда Вы будете импортировать сотрудников.

3. **`/api/v1/group_rule/create`**

Создайте правило импорта для Вашей группы по её DN (APM - Синхронизация данных AD - Группы).

Это же правило будет использоваться в дальнейшем и для синхронизации.

4. **`/api/v1/ldap/set_sync_state`**

Включите синхронизацию каталога. Начнётся импорт и синхронизация по вновь созданному и уже имеющимся правилам.

5. **`/api/v1/group/list`**

Проверяйте результат импорта - список групп (APM - Объекты учёта - Группы). Когда обнаружите группу со своим DN, это будет означать, что импорт прошёл успешно. Сохраните номер группы `sg_id`.

ВАЖНО

Полученный на последнем шаге номер группы можно далее использовать как *условие применения* ПУП-ов и профилей.

Как изменить профиль или установить собственный?

1. **`/api/v1/profile/list`**

Получите список установленных профилей и сохраните ИД профиля `prof_id` и тип профиля `pol_pt_id`

2. **`/api/v1/profile/modify`**

На основе полученных профилей и по [Swagger](#) составьте свой, укажите сохраненные на первом шаге `prof_id` и `pol_pt_id`

3. **`/api/v1/profile/create`**

Или создайте свой собственный профиль по [Swagger](#) с условиями применения.

Как изменить ПУП или создать собственное?

1. `/api/v1/app/rule/list`

Получите список установленных ПУП и сохраните ИД правила `appr_id` и ИД приложения `appd_id`

2. Если необходимо, [добавьте и установите свое приложение](#) и сохраните его `appd_id`

3. `/api/v1/app/rule/modify_corporate`

На основе полученных ПУП и по [Swagger](#) составьте своё правило, укажите сохраненные на предыдущих шагах `appr_id` и `appd_id`

4. `/api/v1/app/rule/create_corporate`


Или создайте своё собственное правило управления приложением по [Swagger](#) с условиями применения.

Как ограничить длину пароля сотрудников?


(использование меток для управления сущностями)

1. Предусловие: наличие нужного профиля с меткой


1. В APM создайте метку `set_len_pass` (имя произвольное)

Создание метки

2. Создайте профиль, ограничивающий длину пароля.

Создание профиля парольных политик

3. В условиях применения профиля задайте метку `set_len_pass`.

Метка в условиях применения профиля

2. `/api/v2/kits/list`

С помощью фильтров получите список устройств (комплектов) нужных сотрудников. ИД сотрудника это `emp_id`, а ИД устройства это `mcc_id`.

Альтернативно, пары ИД сотрудник-устройство можно получать [по имени сотрудника](#).

3. `/api/v1/set/tags`

По значению `mcc_id` установите на устройство метку `set_len_pass`. Профиль с этой меткой применится на устройстве и длина пароля будет ограничена.

Используйте метки для настройки Монитора, точек доступа Wi-Fi, установки обоев рабочего стола, сертификатов приложений и VPN, режима киоска, Exchange аккаунта и т.д. Имена меток произвольные, буквенно-цифровые плюс точка, подчёркивание и дефис.

Аналогично профилям можно использовать Правила Управления Приложением (ПУП) и Конфигурацию Приложения (КП).

Как по серийному номеру телефона получить информацию о сотруднике?

1. **api/v2/kits/list**

Запросите список информации о комплекте, используя фильтры, например `start_date_enroll` и `end_date_enroll`

2. **mob_ser_no**

В полученном списке произведите поиск по серийному номеру в поле `mob_ser_no`

В найденном элементе списка уже есть много данных о сотруднике: ФИО, должность, почта, `distinguished_name`, `emp_id`

3. **/api/v1/devices**

Поместите значение `emp_id`, полученное на предыдущем шаге, в параметр запроса `sm_employee_id` и получите список устройств, принадлежащих сотруднику.

В качестве исходного поискового параметра можно использовать не только серийный номер.

Это может быть UDID, IMEI, eSIM, IMSI, ICCID или просто номер телефона.

Подробнее см. swagger, параметры выдачи ``api/v2/kits/list``