НИИ СОКБ
ЦЕНТР РАЗРАБОТКИ

ИНСТРУКЦИЯ ПО НАСТРОЙКЕ СМЕНЫ СОТРУДНИКА НА МСК

SAFEMOBILE

Москва

2025

ИНСТРУКЦИЯ ПО НАСТРОЙКЕ СМЕНЫ СОТРУДНИКА НА МСК

В 12.0 появилась возможность передавать устройство между сотрудниками не отключая устройство от управления. Функция доступна для устройств на платформе Android, на которых монитор имеет права Device Owner (DO).

Настройка передачи устройства включает в себя следующие шаги:

1. Для того чтобы в процессе передачи данные прежнего владельца устройства не стали доступны новому, передача должна осуществляться через фиктивного владельца, не имеющего доступа к корпоративным данным. Тогда в процессе передачи данные предыдущего сотрудника будут очищены. Для этого необходимо создать фиктивную учётную запись (сотрудника), за которым будет числиться устройство в момент передачи между реальными сотрудниками. Эта технологическая учётная запись называется в SafeMobile основным сотрудником.
2. На этого фиктивного сотрудника нужно назначить профиль киоска, в котором будет разрешено только одно приложение - монитор SafeMobile.
3. Назначить устройству (комплекту) основного сотрудника можно на одноимённой вкладке в разделе «Комплекты» или при создании кода приглашения указать, что сотрудник, за которым изначально регистрируется устройство, является его основным.
4. Создать профиль «Политики смены сотрудника на устройстве», определяющий правила возврата устройства основному сотруднику. Его нужно назначить на подразделение, в котором предполагается разрешить передачу устройства без отключения от управления. В профиле необходимо:
    - Разрешить возврат устройства основному сотруднику.
    - Запретить смену сотрудника без отключения от управления. Это запретит прямую передачу устройства между реальными сотрудниками.
    - И включить сброс пароля при передаче устройства основному владельцу.
5. Создать профиль «Политики смены сотрудника на устройстве», определяющий правила передачи устройства от основного сотрудника реальному сотрудника. Его нужно назначить непосредственно на основного сотрудника. Политики этого профиля будут перекрывать политики профиля назначенного на подразделение. В профиле необходимо:
    - Запретить возврат устройства основному сотруднику. Так как профиль назначается непосредственно на основного сотрудника, то передача на основного сотрудника не имеет смысла.
    - Разрешить смену сотрудника без отключения от управления. Это разрешит передачу устройства от основного сотрудника реальному.

- Сброс пароля можно выключить. Предполагается, что после возврата основному сотруднику пароль уже будет сброшен чтобы любой сотрудник мог зарегистрировать устройство на себя.

Сотрудник может вернуть устройство основному сотруднику зайдя в приложение Монитор, открыв настройки аккаунта и нажав кнопку "Вернуть устройство основному сотруднику". Для выполнения возврата монитор должен иметь связь с сервером. Для комплекта должен быть задан основной сотрудник. Если на устройство не назначен профиль «Политики смены сотрудника на устройстве» и не включена политика, разрешающая возврат устройства, возврат устройства будет недоступен сотруднику.

Администратор может принудительно вернуть устройство основному владельцу в разделе **"Объекты учета" -> "Комплекты"**, выбрав комплект и нажав кнопку: **"Вернуть основному сотруднику"**. Для комплекта должен быть задан основной сотрудник. Если в данный момент устройство не имеет связи с сервером то, на устройстве возврат основному сотруднику произойдет после восстановления связи с сервером. В этом случае значение политик профиля будет проигнорировано.

Чтобы сотрудник мог зарегистрировать на себя устройство, принадлежащее основному сотруднику, он должен в приложении Монитор, открыть настройки аккаунта и нажать кнопку **"Сменить сотрудника"**. После необходимо выбрать способ регистрации. Доступна регистрация через QR-код или код приглашения.

При смене сотрудников на устройстве данные управляемых приложений очищаются. Сами приложения не удаляются каталоги типа Загрузок и Галереи не очищаются. Также не удаляются учётные записи. Их создание нужно блокировать с помощью профиля ограничений.

> ***Примечание***
>
> *Если в системе настроена синхронизация с AD и для выдачи mtls сертификатов используется корпоративный УЦ, то основной сотрудник так же должен иметь доменную учетную запись с возможностью выписать сертификат mtls.*