Изменения в управлении Android

1. **Упрощение регистрации Android устройств**

   Использование приложения Loader, файлов и сертификатов skb для регистрации устройств больше не требуется. В любом сценарии для подключения достаточно наличие мобильного клиента SafeMobile (монитора).

   Поддерживаемые технологии и способы установки мобильного клиента SafeMobile для Android:

   1) Автоматическая регистрация с помощью технологии Samsung Knox Mobile Enrollment;
   2) Автоматизированная установка мобильного клиента при сканировании QR-кода в процессе первичной инициализации устройства. QR-код может быть общим для всех устройств или персональным для каждого сотрудника;
   3) Установка мобильного клиента SafeMobile без сброса устройств к заводским настройкам на личные устройства Samsung или корпоративные устройства Samsung с Android от 4.4 до 9 включительно;
   4) Самостоятельная регистрация пользователей с использованием доменных учётных записей корпоративного LDAP каталога;
   5) Регистрация устройств по IMEI. Администратор должен предварительно зарегистрировать IMEI корпоративных устройств на сервере SafeMobile.

2. **Контейнеры на любых устройствах Samsung, поддерживающих функции Knox Platform for Enterprise***

   С помощью контейнеров Knox Platform for Enterprise (KPE) можно безопасно разделить корпоративные и личные данные на мобильных устройствах Samsung. В отличие от контейнеров Android Enterprise, контейнеры KPE управляются SafeMobile напрямую, без взаимодействия с серверами Google.

   SafeMobile поддерживает следующие стратегии управления устройствами:

   1. Управление всем устройством. Эта стратегия предназначена для устройств, которые целиком управляются организацией. Один из примеров – это т.н. устройства целевого использования, где пользователю в режиме киоска доступно только одно или несколько приложений. Стратегия доступна для всех Android устройств.
   2. Управление устройством и контейнером. Стратегия доступна для устройств Samsung, выпущенных до Samsung Galaxy Note 10.

3. Управление контейнером. Компания управляет только контейнером, в котором размещаются приложения, нужные пользователю для работы. Доступа к данным вне контейнера компания не имеет. Возможности по настройке политик безопасности, действующих на всё устройство целиком, практически отсутствуют. Стратегия доступна для всех устройств Samsung с Android 7 и выше.
4. Управление корпоративным контейнером. Отличается от п.3 большим числом политик ограничений, которые можно настроить на все устройство целиком – и на контейнер, и на область вне его. Для реализации стратегии нужно, чтобы устройство подключалось к SafeMobile при первоначальной инициализации – при первом включении устройства или после его сброса к заводским настройкам. Стратегия доступна для устройств Samsung с Android 11 и выше.

Стратегию управления выбирает администратор перед тем, как устройство будет зарегистрировано на сервере. Для удобства предусмотрен механизм автоматического выбора наиболее подходящей стратегии в зависимости от способа подключения устройства к SafeMobile.

Новая версия корпоративного каталога приложений SafeStore адаптирована для возможности работы с любым из доступных вариантов контейнеров.

** Список устройств Samsung, которые поддерживают функции KPE можно найти на сайте производителя. Список устройств можно отфильтровать по наличию функций Knox Platform for Enterprise.*

3. Возможность принудительного добавления Android приложений в исключения по энергопотреблению

Android не будет автоматически закрывать такие приложения при повышенном энергопотреблении. Функция актуальна для VPN клиентов, мессенджеров и других энергоёмких приложений.

4. Возможность исправления ошибок в настройках подключения устройств

Если при изменении настроек подключения устройств допущена ошибка, из-за которой устройства не могут подключиться к серверу, мобильный клиент SafeMobile будет пытаться подключиться, используя предыдущие настройки подключения.

Если ошибки допущены многократно или предыдущие настройки подключения больше не актуальны, исправленные настройки можно доставить с помощью Firebase Cloud Messaging вместо того, чтобы переподключать устройства.

5. **Событие начала скачивания приложения**

   Мобильный клиент SafeMobile регистрирует информацию о том, когда он начал скачивать дистрибутив приложения, которое он должен установить. Эта информация помогает установить причины, по которым корпоративное приложение не было установлено на мобильном устройстве:

   1) Если клиент зарегистрировал несколько событий начала скачивания дистрибутива, значит дистрибутив приложения достаточно большой и текущая пропускная способность канала связи не позволяет его скачать;
   2) Если клиент не зарегистрировал событие начала скачивания приложений, значит он или давно не подключался к серверу, или считает, что установка приложения не требуется. В последнем случае нужно проверить состояние назначенных на устройства правил управления приложений в одноимённом отчёте. Если ошибка возникает при первоначальной настройке, скорее всего неверно настроены параметры подключения мобильных устройств к серверу SafeMobile.

6. **Шаблон для настройки Kaspersky Endpoint Security для Android**

   С помощью шаблона можно быстрее создать набор необходимых настроек, включая лицензионный ключ и параметры подключения устройств к Kaspersky Security Center.

Изменения в управлении iOS

1. **Запрет рандомизации MAC-адреса при подключении к Wi-Fi сетям для iOS 14 и выше**

   При настройке Wi-Fi сети с помощью SafeMobile 5.0 можно указать, чтобы управляемые устройства при подключении к этой сети не рандомизировали MAC-адреса. Если MAC-адреса не будут случайными, можно сформировать списки доступа к корпоративным Wi-Fi сетям по разрешённым MAC-адресам.

2. **Запрет удаления управляемых приложений* в iOS 14 и выше**

   На устройствах с iOS 14 и выше все приложения, которыми управляет SafeMobile 5.0, защищены от удаления пользователем. Запрет удаления не требует режима supervised.

   До iOS 14 можно запретить удаление только всех приложений сразу – как управляемых, так и неуправляемых. Для запрета удаления всех приложений нужно, чтобы устройство находилось в режиме supervised.

   ** Управляемые iOS приложения – это приложения, которые установлены с помощью SafeMobile, или приложения, которые взяты под управление, чтобы настроить или запретить резервное копирование.*

3. **Новые политики ограничений**

№	Политика	iOS не ниже	Требует supervised
1	Запрет персонализированной рекламы Apple	14.0	**Нет**
2	Запрет подключения к сетевым дискам в приложении Файлы	13.1	**Да**
3	Запрет подключения к USB устройствам в приложении Файлы	13.1	**Да**
4	Запрет доступа Find My Friends в приложении Find My	13.0	**Да**
5	Запрет доступа Find My Device в приложении Find My	13.0	**Да**
6	Запрет NFC	14.2	**Да**
7	Запрет автозаполнения паролей	12.0	**Да**
8	Запрет запроса пароля у устройств поблизости	12.0	**Да**
9	Запрет обмена паролями с помощью Airdrop Passwords	12.0	**Да**

№	Политика	iOS не ниже	Требует supervised
10	Запрет изменения настроек режима модема	12.2	**Да**
11	Запрет подключения к USB-устройствам, когда устройство заблокировано	11.4.1	**Да**
12	Включение автоматической синхронизацию даты и времени, без возможности отключения пользователем	12.0	**Да**
13	Запрет подключения к серверам Siri для распознавания речи	14.5	**Нет**
14	Запрет подключения к серверам Siri для перевода	15.0	**Нет**
15	Включение Wi-Fi, без возможности отключения пользователем, в том числе с помощью включения режима полёта. При этом у пользователя сохраняется возможность выбирать Wi-Fi сеть, к которой будет подключаться устройство	13.0	**Да**
16	Включить управляемый буфер обмена. Если он включен, на операции копирование и вставки будет распространяться действие политики запрета передачи данных между управляемыми и неуправляемыми приложениями и аккаунтами	15.0	**Нет**
17	Запрет добавлять и удалять App Clips	14.0	**Да**
15	Запрет загрузки в режим восстановления с несопряженного устройства	14.5	

Изменения в управлении Аврора

1. **Поддержка Аврора 4**

   С помощью SafeMobile 5.0 можно управлять мобильными устройствами на базе ОС Аврора версии 4.

2. **Дистанционная блокировка устройств или сброс к заводским настройкам**

   В случае потери или кражи устройства администратор может отправить на него команду блокировки или команду сброса к заводским настройкам. Заблокированное устройство можно попытаться найти по данным о его местоположении. Если поиск устройства невозможен или его координаты неизвестны, рекомендуется дистанционно стирать с устройства все данные.

3. **Удалённое изменение пароля доступа к устройству**

   Если пользователь забыл пароль, администратор может его дистанционно изменить.

4. **Инвентаризация установленных приложений**

   Администратор может запросить с устройства список установленных приложений и просмотреть его в веб-консоли.

5. **Дистанционный запуск приложений**

   Если пользователь не может найти нужное приложение, администратор может запустить его удаленно.

Изменения в управлении Windows 10

1. **Автоматическое определение названия приложения в msi**

   Вместе с msi дистрибутивом нужно загрузить файл метаинформации. Файл нужно сформировать с помощью PowerShell скрипта, поставляемого в составе SafeMobile 5.0.

   Файл метаинформации содержит название приложения, которое будет отображаться на клиентском устройстве. Это название нужно, чтобы иметь возможность сопоставить действия администратора с событиями установки приложений.

Другие изменения

1. **Улучшения в работе со срочными лицензиями**

   При использовании срочных лицензий администратору при входе в консоль управления выводится предупреждение за 30 дней и за сутки до истечения срока лицензии. После истечения срока администратор может только загрузить новую лицензию или отключить устройства от управления. При этом клиенты SafeMobile на управляемых устройствах продолжают работать в полном объёме, кроме возможности получить от сервера обновления приложений и политик безопасности.

2. **Отключена поддержка небезопасных версий TLS**

   Серверные компоненты SafeMobile 5.0 по умолчанию не принимают запросы с TLS версий 1.0 и 1.1. При необходимости управления устройствами с Android 4.4, которые могут не поддерживать TLS версии 1.2, поддержку старых версий TLS можно включить в настройках.

3. **Длительное хранение последних данных об устройствах**

   SafeMobile хранит информацию о мобильных устройствах в течение заданного времени, включая информацию о событиях, местоположении и выполненных командах. Теперь последние 100 записей каждого типа не будут удаляться. Это позволит посмотреть последнюю информацию о любых устройствах, которые когда-либо управлялись в компании с помощью SafeMobile.