Основные изменения

1. Доработана интеграция SafeMobile со службой каталогов Microsoft Active Directory:
   1.1. Синхронизация пользователей указанных администратором групп, начиная с указанного baseDN по команде администратора и/или автоматически с заданным администратором периодом. Импорт доменных пользователей с помощью файла больше не поддерживается. Если пользователи загружаются с помощью файла, они считаются локальными.
   1.2. Возможность использования групп безопасности при назначении профилей и приложений.
   1.3. Использование доменных групп для авторизации администраторов. Администраторы получают функциональные роли в зависимости от того, в какие доменные группы они входят.
   1.4. Для аутентификации доменных администраторов нужно вводить имя учётной записи в формате UPN (user principal name, с @). Создавать локальные учётные записи администраторов, в имени которых содержится @, не допускается.
   1.5. Автоматические действия с устройствами пользователя при отключении или блокировке его доменной учётной записи – блокировка, enterprise wipe или wipe.
   1.6. Оптимизирован способ отображения организационно-штатной структуры для быстрого отображения большого количества сотрудников.
   1.7. Изменён порядок регистрации мобильных устройств с использованием доменных учётных записей. Учётные записи доменных пользователей должны быть импортированы SafeMobile до того, как пользователи будут использовать их при регистрации мобильных устройств.
2. Внешние по отношению к SafeMobile системы могут запросить одноразовый код приглашения для регистрации мобильного устройства доменного пользователя с помощью API. Пользователь должен был предварительно импортирован в SafeMobile из домена. Если внешняя система – это корпоративный портал с доменной авторизацией, код приглашения можно использовать как второй фактор при регистрации устройств.

3. Настройка правил выявления несоответствия устройств требованиям безопасности (noncompliance). Если устройство не соответствует установленным требованиям, к нему могут быть применены одно или несколько действий.
   - 3.1. Доступные условия uncompliance:
     - 3.1.1. Принадлежность устройства – корпоративное или личное.
     - 3.1.2. Нахождение внутри или вне геозоны.
     - 3.1.3. Доменные группы, в которых должен быть пользователь или в которых его быть не должно.
     - 3.1.4. Нахождение iOS устройства в режиме supervised или не-нахождение устройства в этом режиме.
     - 3.1.5. Наличие или отсутствие на устройстве указанных приложений.
     - 3.1.6. Минимальная или максимальная версия мобильной ОС.
   - 3.2. Доступные действия uncompliance:
     - 3.2.1. Отправка email по указанному шаблону.
     - 3.2.2. Выполнение команд:
       - 3.2.2.1. Enterprise wipe.
       - 3.2.2.2. Wipe.
       - 3.2.2.3. Принудительное обновление iOS. Для Android принудительное обновление ОС настраивается с помощью профиля.
     - 3.2.3. Установка профиля. Профили uncompliance назначаются только через правила. Назначить такие профили на устройства или группы вручную нельзя.
   - 3.3. Пример использования:
     - 3.3.1. Пользователь подключает устройство с версией ОС ниже допустимой.
     - 3.3.2. Пользователю и администратору отправляется письмо о том, что ОС на устройстве необходимо обновить. Вместе с письмом на устройство отправляется команда или профиль для принудительного обновления ОС.
     - 3.3.3. Если через сутки устройство не обновляется, оно автоматически отключается от управления.
4. Добавлена возможность перевыпуска клиентских сертификатов:
   - 4.1. По команде администратора.

4.2. Автоматически после истечения 90% срока действия сертификата.

5. Возможность настройки альтернативного имени субъекта (SAN, subject alternative name) в сертификатах, выпускаемых с помощью SafeMobile на корпоративных центрах сертификации.
6. Автоматические формирование очереди событий безопасности и передача информации об этих событиях во внешние системы по Syslog. Например, в SIEM.
7. Динамическое формирование состава доступных для отправки на устройства команд. Например, для iOS не отображаются команды, которые можно отправить только на Android. Если одновременно выбраны устройства разных платформ, список доступных команд будет включать команды для всех выбранных мобильных платформ (iOS, Android, Аврора, Windows).
8. Новый отчёт “Правила управления (UID)”. С помощью отчёта можно для выбранного приложения найти все устройства, на которых не были применены актуальные правила, относящиеся к этому приложению. Например, после назначения новой версии приложения на несколько сотен устройств можно в несколько кликов посмотреть, на каких устройствах приложение пока ещё не установлено.
9. Автоматическое отключение от управления предыдущих записей об устройстве (комплектов) при его повторной регистрации. В результате на одно устройство всегда тратится только одна лицензия.

Новое в управлении Android

1. Новый режим киоска для Android с собственным лаунчером, который можно гибко кастомизировать. Администратор может (тэгом **новое** выделены возможности, которые не были доступны в предыдущем режиме киоска):
   1.1. Добавить в киоск приложения в двух режимах:
      1.1.1. Приложения, для которых есть иконки.
      1.1.2. **новое** Приложения, которые могут вызваны опосредованно. Например, пользователь скачал картинку в браузере и может открыть её с помощью галереи. У браузера есть иконка на рабочем столе, а у галереи нет.
   1.2. Настроить доступ пользователя к:
      1.2.1. Диалогу управления устройством – выключение, перезагрузка, экстренный режим.
      1.2.2. Кнопкам “Домой” и “Недавние”.
      1.2.3. Системной информации в строке состояния – дата, время, батарейка, подключение к сети.
      1.2.4. Экрану блокировки.
   1.3. **новое** Установить обои рабочего стола.
   1.4. **новое** Разрешить пользователю выбирать Wi-Fi сеть для подключения.
   1.5. **новое** Включить отображение в режиме киоска информации об устройстве – IMEI, серийный номер.
   1.6. **новое** Установить пароль для выхода из режима киоска непосредственно на устройстве.
   1.7. **новое** Разрешить пользователю настраивать яркость экрана.
2. Новый профиль управления обновлениями Android устройств, включающий:
   2.1. Откладывание обновления ОС до 30 дней.
   2.2. Настройку freeze-периодов, в которые запрещены обновления ОС. Freeze периоды настраиваются для диапазона календарных дат. Например, для праздников. Длительность одного периода до 90 дней, диапазон между периодами должен быть не менее 60 дней.
   2.3. Принудительного обновления ОС при доступности новой версии.

3. Возможность массовой регистрации Android устройств по серийным номерам с помощью общего QR-кода. Для этого администратору необходимо предварительно загрузить в SafeMobile список серийных номеров устройств.
4. Принудительное включение служб геолокации на Android устройствах по запросу администратора. В предыдущих версиях Android клиент SafeMobile автоматически включал службу геолокации в рабочее время, если было настроено определение местоположения. Теперь можно принудительно включить геолокацию для других приложений, не осуществляя при этом сбор координат с помощью SafeMobile.

Новое в управлении iOS

1. Команда принудительного обновления iOS устройств в режиме supervised.
2. Новый профиль фильтрации контента для iOS, с помощью которого на устройствах в режиме supervised можно настроить чёрные и белые списки сайтов. Для удобства формирования списков из большого числа элементов реализована загрузка списка с помощью файла.
3. Настройка Exchange аккаунта на iOS с аутентификацией по клиентскому сертификату. Выпуск клиентских сертификатов на удостоверяющем центре может быть автоматизирован. Поддерживаются удостоверяющие центры Microsoft CA и SberCA.
4. Настройка встроенного VPN клиента iOS по протоколу IKEv2 с возможностью автоматического выпуска клиентского сертификата для аутентификации.
5. Настройка per-app VPN на устройствах iOS для:
   5.1. Доменов Safari.
   5.2. Указанных администратором приложений.
6. Добавлена возможность обновления информации об iOS устройствах и отправка на них команды сброса к заводским настройкам, если пользователь включил устройство, но ещё не ввёл на нём пароль.

Новое в управлении Аврора

1. Скачивание мобильного клиента с веб-портала регистрации устройств.
2. Регистрация устройств с помощью персональных QR-кодов и доменных учётных записей.
3. Установка и обновление приложений на устройствах с ОС Аврора 4.0.2.

Управление устройствами на базе Alt Linux и Astra Linux

1. Регистрация устройств.
2. Установка и обновление приложений.
3. Централизованное распространение конфигурационных файлов.

Новое в DevOps, DevSecOps

1. Обновлены версии используемых библиотек и базовых образов для устранения актуальных CVE.
2. Планируется организация выпуска новых версий серверных компонентов с устранением CVE уровня medium и выше по данным trivy в течение месяца с даты выпуска исправления.
3. Компоненты SafeMobile в docker образах не запускаются от имени суперпользователя (root).
4. Авторизованные заказчики могут получить доступ к образам серверных компонентов SafeMobile в docker registry, чтобы упростить процесс их развёртывания.
5. Подготовлены примеры конфигурационных файлов для развёртывания образов SafeMobile в среде k8s. Примеры предоставляются по запросу.

Известные ограничения

1. Начиная с SafeMobile 7, больше не поддерживается:
   1.1. Управление мобильными устройствами с Android версии 4.4.
   1.2. Установка мобильного клиента на устройства с iOS версии ниже 11. Для регистрации устройств с iOS в SafeMobile нужно использовать веб-портал.
2. Обои рабочего стола в режиме киоска Android устанавливаются не с помощью загрузки файла в веб-консоль администрирования, а с помощью указания URL, откуда устройство должно скачать обои. Это должен быть URL для прямого скачивания файла без дополнительных согласий и т.п.
3. Обновление мобильного клиента SafeMobile для Android требует отключения режима киоска. Отключение киоска на время обновления мобильного клиента может выполняться автоматически.
4. **H2’23**[1]. В режиме киоска Android нельзя добавить ярлык для быстрого доступа к указанному администратору URL в веб-браузере.
5. **H2’23**. Поведение при обнаружении признаков root или jailbreak не настраивается. Выполняется автоматический enterprise wipe.
6. **H2’23**. Нет статусов устройств compliant и compromised. Статусы будут добавлены вместе с API для получения информации по ним в H2’23.
7. Нельзя изменить период применения правил выявления несоответствия устройств требованиям безопасности (noncompliance). Правила применяются:
   7.1. При регистрации устройства.
   7.2. При назначении правила.
   7.3. Периодически каждый час.
   7.4. Перед выполнением каждого действия, предписанного правилом.

   Пример: если в правиле написано выполнить сброс устройства к заводским настройкам через 30 мин после обнаружения на нём нежелательного приложения и пользователь его за эти полчаса удалил, устройство не будет сброшено.
8. Шаблоны писем указываются в виде plain text. Загрузка шаблона тела письма осуществляется с помощью текстового файла в кодировке UTF-8. Это сделано, чтобы в будущем добавить загрузку html шаблонов.

[1] Здесь и далее так показан планируемый срок доработки

9. В разделе Объекты учёта / Клиентские сертификаты, где отображаются выписанные с помощью SafeMobile клиентские сертификаты, не отображается SAN сертификатов.
10. Срок автоматического перевыпуска сертификата всегда равен 90% от срока действия сертификата и этот % не настраивается.