Основные изменения

1. Добавлена возможность сделать копию профиля. Копия профиля создаётся с теми же значениями политик. Назначения и условия применения профиля не копируются. Копии позволяют быстро создать профиль с небольшим числом отличий от оригинала.
2. Можно включить шифрование пароля сервисной доменной учётной записи, которая используется для синхронизации данных с каталогом Microsoft Active Directory.
3. В настройках сервера email уведомлений можно указать ограничение числа писем в минуту. Изменение правил выявления несоответствия требованиям безопасности (noncompliance) может приводить к отправке большого количества писем. Например, если повышается минимально допустимая версия мобильной ОС. Учётная запись, от имени которой SafeMobile отправляет email, может иметь ограничение на число писем в минуту. Теперь в настройках SafeMobile можно указать те же ограничения, что установлены на почтовом сервере, чтобы не допустить потери email уведомлений.
4. Добавлена автоматическая очистка старых файлов кэша сервера управления. Параметры очистки указываются в конфигурационном файле. В кэше хранятся дистрибутивы приложений, которые сервер отправлял мобильным устройствам. Переполнение кэша приведёт к отказу в работе.
5. В настройках образа nginx сервера управления и сервера администрирования добавлена настройка Content Security Policy.
6. В связи с окончанием срока поддержки PostgreSQL 9 и 10 рекомендуем нашим клиентам перейти на более новые версии PostgreSQL. Служба поддержки SafeMobile готова оказать помощь в миграции. Если вам актуальна миграция, оставьте заявку на портале поддержки https://service.niisokb.ru/.
7. В руководство по установке и настройке добавлена недостающая информация по новым серверным компонентам, добавленным в SafeMobile 7.
8. Разработан документ с описанием состава и формата событий, которые SafeMobile может передавать по Syslog. Документ можно запросить на портале технической поддержки.

Новое в управлении Android

1. Профили ИБ устанавливаются в процессе инициализации мобильного клиента SafeMobile – профиль парольных политик, профиль киоска и профили ограничений. Остальные профили и приложения устанавливаются, как и раньше, после первой регистрации события запуска мобильного клиента SafeMobile на устройстве.
2. Новые политики по управлению Wi-Fi для корпоративных устройств с Android 13:
   2.1. Минимальный уровень безопасности Wi-Fi, к которому может подключиться устройство – WPA3, WPA/WPA2 Enterprise, WPA/WPA2 Personal.
   2.2. Запрет использования устройства в режиме Wi-Fi точки доступа. На Android 12 и ниже политика доступна только для устройств Samsung.
   2.3. Запрет совместного использования Wi-Fi сетей, настроенных с помощью SafeMobile.
   2.4. Запрет Wi-Fi Direct. На Android 12 и ниже политика доступна только для устройств Samsung.
   2.5. Запрет добавления новых Wi-Fi точек доступа.
   2.6. Запрет изменения состояния Wi-Fi. Если Wi-Fi включен, пользователь не сможет его выключить.
3. В состав парольных политик Android добавлен запрет использования Smart Lock – возможность разблокировать устройство по известным Bluetooth устройствам, Wi-Fi сетям и т.д. Политика доступна для устройств с Android 6 и выше.
4. В интерфейсе мобильного клиента SafeMobile для Android (приложение «Монитор») отображается информация о выданных клиенту разрешениях. Если какое-то из необходимых разрешений не предоставлено или отозвано, можно инициировать повторный запрос, не переходя в приложение «Настройки».
5. Мобильный клиент SafeMobile регистрирует на сервере информацию о том, осуществляет ли он сбор координат устройства. Если клиент не выполняет сбор координат, хотя, казалось бы, должен, проверьте настройки календаря рабочего времени в разделе «Календарь» и период опроса координат в применённом на устройстве профиле настроек монитора.
6. Добавлена возможность установки приложений на ТСД Zebra с Android 5.1.

Новое в управлении iOS

Изменён способ добавления элементов в списки доменов в профиле per-app VPN для iOS. Раньше списки нужно было набирать вручную. Теперь списки загружаются с помощью текстовых файлов. Это удобнее, если списки большие или их нужно дублировать в нескольких профилях.

Новое в управлении Аврора

1. Настройка требований к паролям.
2. Команда сброса пароля.
3. Возможность запрета подключения USB-накопителей.
4. Возможность подключения устройств с помощью общего QR-кода аналогично Android. Перед этим нужно загрузить в веб-консоль администратора список IMEI или серийных номеров устройств.

Новое в DevSecOps

Обновлён базовый образ и внешние зависимости для устранения актуальных CVE.

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. **H2’23**. 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.