Термины и сокращения

1. **AD** – служба каталогов Microsoft Active Directory.
2. **Монитор** – мобильный клиент UEM SafeMobile для платформы Android.
3. **Назначаемая сущность** – сущности UEM SafeMobile, которые можно назначать: профили, правила управления приложениями, конфигурации приложений, правила несоответствия.
4. **УЦ** – удостоверяющий центр.

Основные изменения

1. Добавлена возможность проставлять устройствам метки и использовать эти метки в условиях применения назначаемых сущностей.
2. Добавлены именованные условия применения. Именованные условия позволяют не дублировать одинаковые условия в разных в назначаемых сущностях. В совокупности с метками устройств именованные условия применения реализуют функционал смарт-групп.
3. Список условий применения назначаемых сущностей дополнен следующими:
   3.1. Устройство имеет все перечисленные метки.
   3.2. У устройства есть хотя бы одна из перечисленных меток.
   3.3. У устройства нет ни одной из перечисленных меток.
   3.4. Модель устройства входит в список.
   3.5. Модель устройства отсутствует в списке.
   3.6. Тип устройства – смартфон или планшет.
   3.7. Монитор имеет все перечисленные привилегии[1]. Только Android.
   3.8. Монитор имеет хотя бы одну из перечисленных привилегий. Только Android.
   3.9. Монитор не имеет ни одной из перечисленных привилегий. Только Android.
4. Добавлена аутентификация доступа устройств iOS, Android и Аврора к серверам управления по клиентским сертификатам (mutual TLS, mTLS). Это исключает возможность одного устройства выдать себя за другое.
5. Для реализации mTLS в состав серверных компонентов добавлен встроенный УЦ и сервис аутентификации. Встроенный УЦ используется для выпуска

[1] Привилегии определяют возможности монитора. Примеры привилегий – device admin, device owner, profile owner.

клиентских сертификатов для аутентификации устройств через mTLS[2]. Сервер аутентификации нужен для реализации mTLS в сервере команд Android.

6. Добавлены дополнительные команды, которые можно использовать в качестве реакции на несоответствие устройств настроенным администратором правилам:
   6.1. Синхронизация настроек.
   6.2. Установка графика рабочего времени.
   6.3. Повторный запрос номера телефона. Только Android.
   6.4. Установка списка корпоративных SIM-карт. Только Android.
   6.5. Синхронизация времени устройства с сервером. Только Android.
7. Возможность сохранить порядок и ширину отображаемых колонок в главном окне АРМ Администратора.
8. Добавлена возможность поиска в назначениях, в списке профилей и правил управления приложениями, при создании кода приглашения. При большом количестве элементов администратору будет легче находить нужные записи.
9. Добавлен контроль версий компонентов. БД проверяет версию компонента при подключении. Если его мажорная версия (X.Y) не совпадает с версией БД, компонент работать не будет. Это сделано для исключения работы несовместимых версий БД и компонентов и упрощения диагностики.
10. Переработан механизм синхронизации с AD:
    10.1. Добавлен учёт переименований и перемещений OU или групп. Это позволило исправить ошибку появления дубликатов пользователей при перемещении пользователя между подразделениями в AD.
    10.2. Добавлена возможность импорта основной группы пользователя AD.
    10.3. Возможна синхронизация с DN, содержащим «,» и спец. символы. Такие символы могут использоваться в ФИО сотрудников и технических учётных записях.
    10.4. Агент синхронизации AD фиксирует в логах недоступность домена.
    10.5. Синхронизация каталога теперь происходит целиком, начиная с указанного администратора baseDN, а не по отдельным правилам.

[2] Использование встроенного УЦ является опциональным. При необходимости клиентские сертификаты могут выпускаться на корпоративном УЦ заказчика на базе Microsoft CA.

Ошибка в любом правиле приведет к остановке всей синхронизации, чтобы не привести к непоправимым последствиям.

10.6. Изменение значений атрибута whenChanged не приводит к повторной синхронизации объекта. Этот атрибут может обновляться в служебных целях и не приводить к изменению других доменных атрибутов, которые используются в SafeMobile.

10.7. Если включена автоматическая синхронизация, администратору запрещено изменять правила синхронизации. Для внесения изменения в правила нужно выключить автоматическую синхронизацию.

10.8. Из-за существенного изменения логики синхронизации с AD журнал синхронизации, отображаемый в АРМ администратора, будет очищен при обновлении.

10.9. Агент синхронизации AD фиксирует в логах недоступность домена.

11. В фильтр главного окна добавлен статус соединения устройств iOS «управление ограничено (NotNow)». Это внутренний статус iOS, который устройство может сообщить MDM серверу в ответ на одну из команд. Статус означает, что выполнение команды сейчас невозможно. Например, iOS для выполнения команды нужно, чтобы устройство было разблокировано, т.к. до ввода пользователем пароля файловая система устройства зашифрована. Добавление статуса NotNow делает управление iOS более прогнозируемым.

12. В журнале местоположений пагинация по числу записей заменена на пагинацию от начального времени. Это ускоряет отображение данных о перемещении в АРМ.

SafeMobile API

1. Список доступных функций SafeMobile API дополнен следующими:
   1.1. Получение списка действующих кодов приглашения.
   1.2. Получение идентификатора пользователя в SafeMobile по идентификаторам из AD.
   1.3. Получение списка устройств пользователя.
   1.4. Получение списка приложений, назначенных на устройство пользователя.
   1.5. Переустановка приложения. Только iOS.
   1.6. Получение списка Wi-Fi, VPN или почтовых[3] профилей, назначенных на устройство пользователя.
   1.7. Переустановка профиля. Только iOS.
   1.8. Перевыпуск клиентского сертификата для профиля, установленного на устройстве пользователя.
   1.9. Изменение пароля.
   1.10. Сброс пароля.
   1.11. Отключение от управления со сбросом к заводским настройкам.
   1.12. Отключение от управления с удалением только корпоративных данных.
   1.13. Отправка команда синхронизации.
   1.14. Получение количества регистраций устройств за интервал времени.
   1.15. Получение списка профилей, которые назначены устройствам, но не были применены на них.
   1.16. Отправка на устройство назначенного, но не применённого профиля.
   1.17. Получение списка всех устройств.
   1.18. Получение списка событий устройства.
   1.19. Получение списка координат устройства.
2. Доступ к SafeMobile API теперь не требует настройки интеграции SafeMobile с AD. Для доступа к API нужно создать сервисную учётную запись.
   2.1. Число сервисных учётных записей не ограничено.
   2.2. Перечень функций API, к которым имеет доступ сервисная учётная запись, можно настроить через APM администратора.

[3] Exchange аккаунт iOS.

2.3. У сервисной учёной записи можно настроить область управления, которая ограничит перечень устройств, к которым имеет доступ учётная запись с помощью API.

2.4. Действия сервисных учётных записей фиксируются в отдельном журнале, доступном администраторам системы.

Новое в управлении Android

1. Добавлена поддержка устройств с Android 13 и 14.
2. Добавлена возможность доставки клиентских сертификатов на устройство или в рабочий профиль[4]. Сертификат загружается в системное хранилище, откуда к нему могут получить доступ приложения на устройстве или в рабочем профиле. Можно доставить сертификаты, загруженные администратором, или настроить выпуск сертификатов на корпоративном УЦ.
3. Добавлена возможность установки некорпоративный приложений из сторонних магазинов. Например, RuStore и AppGallery.
4. В профиль Wi-Fi добавлена возможность указать домены серверов авторизации, которые будут использоваться при подключении устройств к корпоративным Wi-Fi сетям. На устройствах с Android 13 и выше использование политики обязательно при использовании сетей 802.1x, в которых присутствует сервер авторизации.
5. При отправке профиля Wi-Fi появилась возможность указать прокси-сервер. При подключении к Wi-Fi можно задать список адресов, подключение к которым будет происходить не через прокси-сервер.
6. Добавлена политика запрета рандомизации MAC-адресов при подключении к Wi-Fi. С помощью этой политики можно реализовать «белый» список доступа к корпоративным Wi-Fi по известным MAC-адресам. Список Wi-Fi MAC-адресов устройств, подключенных к UEM SafeMobile, можно получить с помощью API. Политика доступна для устройств с Android 13 и выше.
7. В информацию об устройстве добавлена информация о (об):
   7.1. Наличии новой версии операционной системы. Администраторы смогут увидеть наличие отложенного обновления безопасности на устройствах пользователей.

[4] Место доставки сертификата определяется местом размещения монитора.

7.2. Имени устройства, которое отображается в приложении «Настройки» на устройстве.

8. Изменён механизм ограничения доступа к Google Play. В новой версии управление Google Play осуществляется только через правила управления приложениями. Раньше этот запрет мог конфликтовать с политиками ограничений.
9. В меню первоначальной настройки монитора добавлена возможность выгрузки логов.

Новые возможности режима киоска Android

1. На рабочем столе устройств в режиме киоска можно добавлять ярлыки для быстрого доступа к веб-сайтам. Для доставки ярлыка нужно использовать профили типа «Ярлык рабочего стола Android».
2. Добавлена возможность запретить отключение экрана, если устройство в режиме киоска находится на зарядке.
3. Доработано управление Wi-Fi пользователем в режиме киоска. Актуальный перечень возможностей:
   3.1. Сканирование доступных Wi-Fi сетей.
   3.2. Включение / отключение Wi-Fi.
   3.3. Просмотр списка сохраненных Wi-Fi сетей.
   3.4. Подключение к выбранной Wi-Fi сети
   3.5. Отключение от текущей Wi-Fi сети.
   3.6. Добавление Wi-Fi сети.
   3.7. Удаление Wi-Fi сети.
   3.8. Изменение пароля Wi-Fi сети.
4. Для устройств в режиме киоска добавлена возможность устанавливать цветовую схему.

Новое в управлении iOS

1. В профиль «Политики ограничений iOS» добавлена политика запрета Handoff. Запрет Handoff позволяет запретить обмен данными на устройствах с одинаковым Apple ID в пределах действия Bluetooth.
2. Добавлены новые поля инвентаризации:
   2.1. Идентификатор клиента Exchange.
   2.2. Имя устройства, которое отображается в приложении «Настройки» на устройстве.
3. Добавлена возможность отключения от per-VPN при бездействии приложений. Когда приложение станет активно и ему потребуется VPN-подключение, оно будет установлено автоматически.

Изменения в управлении Аврора

1. Реализована политика безопасности «Запрет монтирования SD карт».
2. Добавлена возможность обновления ОС с помощью SafeMobile. Для устройств с сертифицированной редакцией ОС Аврора обновить ОС можно только с помощью MDM.
3. Добавлена возможность отправлять приложениям файлы настроек. Для доступа к настройкам, доставленным SafeMobile, приложению достаточно считать информацию из файла, размещённого в общедоступном каталоге.

DevSecOps

Обновлён базовый образ и внешние зависимости для устранения актуальных CVE.

Известные ограничения

1. Для устройств Android потребуется отключить управление Google Play через профили и создать необходимые правила управления приложением для корректной миграции.
2. Если используется внешний прокси-сервер, то он требует дополнительной настройки для работы mTLS. На внешнем прокси нужно настроить разрешение подключения с помощью не-публичных клиентских сертификатов и разрешить заголовки, где будут передаваться отпечаток и тело сертификата.

Окончание поддержки ряда функций и конфигураций

1. Минимальная версия PostgreSQL увеличена до 11.
2. Минимальная версия Android увеличена до 5.1.
3. Следующие функции в SafeMobile 8.2 предоставляются «как есть» и будут исключены в следующих релизах:
   3.1. Адресная книга.
   3.2. Отправка внутренних сообщения на Android с помощью приложения SafeMessage.