



Описание функций

Kaspersky Secure Mobility Management

kaspersky

Решение Kaspersky Secure Mobility Management предназначено для защиты и управления корпоративными мобильными устройствами, а также личными мобильными устройствами, используемыми сотрудниками компании в корпоративных целях.

Возможности Kaspersky Secure Mobility Management:

Android

	Возможности по контролю за личным устройством сотрудника (BYOD)	Возможности по контролю за устройством с созданием изолированного контейнера для корпоративных данных (режим Profile Owner)	Возможности по контролю устройства, которым владеет компания (режим Device Owner)
Общие настройки			
Настройки периода синхронизации устройства с сервером	+	+	+
Настройка правил изменения статуса устройства	+	+	+
Настройки для событий безопасности устройства и функционирования решения			
Время хранения события	+	+	+
Уведомление администратора (почта, SMS, выполнение программы или скрипта)	+	+	+
Возможность интеграции с SIEM	+	+	+
Отправка команд на устройство			
Заблокировать устройство	+	+	+
Разблокировать устройство	+	+	+
Удалить корпоративные данные	+	+	+
Сбросить устройство к заводским настройкам	+	+	+
Определить местоположение устройства	+	+	+
Воспроизвести звуковой сигнал на устройстве	+	+	+
Сделать фото с фронтальной камеры устройства	+	+	+
Принудительно синхронизировать устройство	+	+	+
Защита устройства от зловредов и фишинга			
Real-time-protection файловой системы для защиты от вредоносных объектов	+	+	+
Сканирование по расписанию файловой системы для поиска вредоносных объектов	+	+	+

	Возможности по контролю за личным устройством сотрудника (BYOD)	Возможности по контролю за устройством с созданием изолированного контейнера для корпоративных данных (режим Profile Owner)	Возможности по контролю устройства, которым владеет компания (режим Device Owner)
Блокирование использования пользователем вредоносных объектов и приложений	+	+	+
Настройка действий при обнаружении вредоносных объектов (удалить, отправить в карантин, запросить действие у пользователя, пропустить)	+	+	+
Использование облачной службы KSN для детектирования объектов	+	+	+
Проверка и защита пользователя от вредоносных и фишинговых веб-страниц	+	+	+
Базовый контроль устройства			
Веб-контроль (по преднастроенным категориям, черный список, белый список веб-страниц)	+	+	+
Запрет использования Bluetooth	+	+	+
Запрет использования камеры устройства	+	+	+
Запрет использования Wi-Fi	+	+	+
Настройка подключения к Wi-Fi сетям	+	+	+
Контроль приложений (белый список, черный список, список обязательных приложений)	+	+	+
Silent установка и удаление приложений без вовлечения пользователя			+
Загрузка и распространение приложений без использования Play Market	+	+	+
Контроль соответствия (можно задать правило при невыполнении которого будет реакция на устройстве)	+	+	+
Определение root на устройстве	+	+	+
Добавление Web-Clip на рабочий стол	+	+	+
Настройка требований к паролю разблокировки устройства			
Минимальное количество символов	+	+	+
Минимальные требования к паролю разблокировки			+
Срок действия пароля	+	+	+
Количество дней, за которое уведомлять об истечении срока действия пароля			+
Количество неповторяющихся паролей в журнале	+	+	+
Период неактивности для блокировки устройств	+	+	+
Период разблокировки без пароля			+

	Возможности по контролю за личным устройством сотрудника (BYOD)	Возможности по контролю за устройством с созданием изолированного контейнера для корпоративных данных (режим Profile Owner)	Возможности по контролю устройства, которым владеет компания (режим Device Owner)
Разрешить биометрические методы разблокировки	+	+	+
Разрешить использование отпечатков пальцев	+	+	+
Разрешить распознавание лица	+	+	+
Разрешить распознавание по радужной оболочке глаза	+	+	+
Установить заданный пароль разблокировки	+	+	+
Возможность удаления данных после неудачных попыток ввода пароля	+	+	+
Контроль устройств Samsung с KNOX			
Настройка точки доступа к мобильному интернету (APN)	+	+	+
Настройка Firewall	+	+	+
Настройка VPN	+	+	+
Настройка Exchange ActiveSync	+	+	+
Создание KNOX контейнера	+	+	+
Режим Profile Owner (Android Work Profile)			
Запрет передачи данных из рабочего контейнера в личный		+	+
Запрет включения USB дебаггинга для приложений, установленных в рабочий профиль		+	+
Запрет установки приложений в рабочий профиль из недоверенных источников		+	+
Запрет удаления приложений, установленных в рабочий профиль		+	+
Включение правил веб-контроля только в рабочем профиле		+	+
Включение правил контроля приложений только в рабочем профиле		+	+
Корпоративный каталог приложений под самые распространенные платформы (Android, iOS, Win, Mac, Linux)			
Скачивание приложений из корпоративного каталога	+	+	+
Подключение устройства Android/iOS MDM пользователем самостоятельно	+	+	+
Режим Kiosk mode			
Режим одного приложения			+
Режим нескольких приложений			+

	Возможности по контролю за личным устройством сотрудника (BYOD)	Возможности по контролю за устройством с созданием изолированного контейнера для корпоративных данных (режим Profile Owner)	Возможности по контролю устройства, которым владеет компания (режим Device Owner)
Интеграция с Exchange ActiveSync			+
Интеграция со NDES/SCEP сервером			+
Настройка корневых сертификатов	+	+	+
Настройка пользовательских сертификатов			
Доставка и установка в системное хранилище пользовательского сертификата (VPN-сертификат)	+	+	+
Доставка и использование для конфигурации почтового клиента сертификата (Почтовый сертификат)	+	+	+
Интеграция с PKI при выпуске сертификатов	+	+	+
Ограничений функций устройства			
Запретить сброс к заводским настройкам			+
Запретить снимки экрана			+
Запретить исходящие звонки			+
Запретить отправку и получение SMS-сообщений			+
Запретить изменение учетных данных			+
Запретить строку состояния			+
Запретить безопасную загрузку (SafeBoot)			+
Принудительно включать экран при подключении к сетевому зарядному устройству			+
Принудительно включать экран при подключении к зарядному устройству USB			+
Принудительно включать экран при подключении к беспроводному зарядному устройству			+
Настройка ограничений для приложений			
Запретить использование камеры			+
Запретить переключение камеры			+
Запретить использование Google Play			+
Запретить использование Google Chrome			+
Запретить использование Google Assistant			+

	Возможности по контролю за личным устройством сотрудника (BYOD)	Возможности по контролю за устройством с созданием изолированного контейнера для корпоративных данных (режим Profile Owner)	Возможности по контролю устройства, которым владеет компания (режим Device Owner)
Запретить установку приложений из неизвестных источников			+
Запретить изменение приложений через Настройки			+
Запретить установку приложений			+
Запретить удаление приложений			+
Запретить отключение проверки приложения			+
Настройка ограничений для бэкапов, внешних носителей и отладки			
Запретить функции отладки			+
Запретить установку физических внешних носителей			+
Запретить передачу файлов через USB			+
Запретить сервис резервного копирования			+
Настройки ограничений сетевого взаимодействия			
Запретить использование Wi-Fi			+
Запретить использование Bluetooth			+
Запретить изменение настроек Wi-Fi			+
Запретить изменение предварительно настроенных сетей Wi-Fi			+
Запретить изменение настроек Bluetooth			+
Запретить изменение настроек VPN			+
Запретить изменение настроек мобильной сети			+
Запретить использование Android Beam через NFC			+
Запретить использование модема			+
Запретить обмен данными через Bluetooth			+
Настройки ограничений геолокации			
Запретить отслеживание местоположения			+
Запретить изменение настроек местоположения			+
Настройка правил обновления ОС			
Установить политику обновления ОС			+
Настроить периоды приостановки обновления ОС			+

	Возможности по контролю за личным устройством сотрудника (BYOD)	Возможности по контролю за устройством с созданием изолированного контейнера для корпоративных данных (режим Profile Owner)	Возможности по контролю устройства, которым владеет компания (режим Device Owner)
--	---	---	---

Управление Google Chrome

Настройки контента

Задать настройки файлов cookie по умолчанию			+
Разрешить файлы cookie на этих сайтах			+
Блокировать файлы cookie на этих сайтах			+
Разрешить файлы cookie на этих сайтах только для одного сеанса			+
Задать настройки JavaScript по умолчанию			+
Разрешить JavaScript на этих сайтах			+
Блокировать JavaScript на этих сайтах			+
Задать настройки всплывающих окон по умолчанию			+
Разрешить всплывающие окна на этих сайтах			+
Блокировать всплывающие окна на этих сайтах			+
Задать настройки отслеживания местоположения пользователей			+

Настройки прокси

Задать настройки прокси			+
URL прокси-сервера			+
URL PAC-файла			+
Список исключений			+

Настройки поиска

Разрешить быстрый поиск			+
Включить поисковую систему по умолчанию			+
Название поисковой системы			+
Ключевое слово			+
URL поиска			+
URL запроса подсказок			+
URL значка			+
Кодировки			+
Дополнительные URL			+
URL изображений			+
URL страницы быстрого доступа			+
Параметры для запросов POST к URL-адресу для поиска			+

	Возможности по контролю за личным устройством сотрудника (BYOD)	Возможности по контролю за устройством с созданием изолированного контейнера для корпоративных данных (режим Profile Owner)	Возможности по контролю устройства, которым владеет компания (режим Device Owner)
Параметры для запросов POST к URL-адресу для поиска предложений			+
Параметры для запросов POST к URL-адресу для поиска изображений			+
Настройка страниц			
Включить дополнительные страницы с сообщениями об ошибках			+
Включить автозаполнение адресов			+
Включить автозаполнение данных кредитных карт			+
Другие настройки			
Включить печать			+
Задать настройки Безопасного просмотра Google			+
Отключить сохранение истории браузера			+
Отключить переход со страницы предупреждения Безопасного просмотра Google			+
Включить предварительное определение сети			+
Включить принудительное использование Безопасного поиска Google			+
Настроить Безопасный режим для YouTube			+
Настроить доступность режима инкогнито			+
Включить поисковые подсказки			+
Задать настройки Переводчика			+
Включить возможность изменения закладок			+
Управляемые закладки			+
Заблокировать доступ к этим URL			+
Разрешить доступ к этим URL (исключения для блокировки URL)			+
Задать минимально допустимую версию SSL			+

	Возможности по контролю за личным устройством сотрудника (non-supervised)	Возможности по контролю устройства, которым владеет компания (режим iOS-supervised)
Общие настройки		
Настройки периода синхронизации устройства с сервером	+	+
Настройка названия профиля, описания профиля и текста, который увидит пользователь при его установке на устройство	+	+
Настройки для событий безопасности устройства и функционирования решения		
Время хранения события	+	+
Уведомление администратора (почта, SMS, выполнение программы или скрипта)	+	+
Возможность интеграции с SIEM	+	+
Защита устройства от фишинга (посредством установки агента Security for iOS)	+	+
Проверка на наличие JailBreak (посредством установки агента Security for iOS)	+	+
Отправка команд на устройство		
Заблокировать устройство	+	+
Разблокировать устройство	+	+
Удалить корпоративные данные	+	+
Сбросить настройки до заводских	+	+
Принудительно синхронизировать	+	+
Настроить роуминг	+	+
Установить состояние Bluetooth (вкл/выкл)		+
Установить обновление ОС		+
Контроль соответствия (можно задать правило при невыполнении которого будет реакция на устройстве)	+	+
Управление приложениями		
Белый список приложений		+
Черный список приложений		+
Установить приложение (поддерживается распространение in-house приложений)	+	+
Удалить приложение	+	+
Настройка пользовательских сертификатов		
Доставка и использование для конфигурации VPN клиента сертификата (VPN-сертификат)	+	+

	Возможности по контролю за личным устройством сотрудника (non-supervised)	Возможности по контролю устройства, которым владеет компания (режим iOS-supervised)
Доставка и использование для конфигурации почтового клиента сертификата (Почтовый сертификат)	+	+
Интеграция с PKI при выпуске сертификатов	+	+
Настройка правил обновления ОС		+
Настройка корневых сертификатов	+	+
Контроль устройства (без режима Supervised)		
Настройка требований к паролю для разблокировки устройства	+	+
Single Sign On	+	+
Настройка точки доступа к мобильному интернету (APN) и мобильной сети	+	+
Настройка подключения к Wi-Fi сетям	+	+
Настройка VPN	+	+
Настройка per-app VPN	+	+
Настройка Proxу	+	+
Управление AirPlay	+	+
Управление AirPrint	+	+
Управление нативным клиентом для Email	+	+
Настройка Exchange ActiveSync	+	+
Настройка LDAP	+	+
Настройка календаря (CalDAV)	+	+
Настройка контактов (CardDAV)	+	+
Добавление Web-Clips	+	+
Интеграция со SCEP	+	+
Запрет использования камеры устройства	+	+
Запрет делать скриншоты и видео экрана	+	+
Запрет голосового набора на заблокированном устройстве	+	+
Запрет использования Siri (в том числе на заблокированном устройстве)	+	+
Запрет покупок в приложениях	+	+
Запрет подсказки пароля при покупках в iTunes	+	+
Запрет backup в iCloud	+	+
Запрет использования Apple KeyChain	+	+
Запрет хранения данных управляемых приложений в iCloud	+	+
Запрет backup enterprise books	+	+
Запрет синхронизации заметок и выделенных фрагментов в Enterprise Books	+	+

	Возможности по контролю за личным устройством сотрудника (non-supervised)	Возможности по контролю устройства, которым владеет компания (режим iOS-supervised)
Запрет iCloud Photo Sharing	+	+
Запрет iCloud Media Library	+	+
Запрет My Photo Stream	+	+
Запрет синхронизации в роуминге	+	+
Включение шифрование бэкапа	+	+
Ограничить трекинг для таргетированной рекламы	+	+
Запрет пользователю принимать недоверенные TLS сертификаты	+	+
Запрет пользователю автоматически обновлять доверенные сертификаты	+	+
Запрет неуправляемым приложениям использовать документы из управляемых	+	+
Запрет управляемым приложениям использовать документы из неуправляемых	+	+
Запрет использования AirDrop как управляемого приложения	+	+
Запрет HandOff	+	+
Запрет передачи диагностической информации в Apple	+	+
Запрет использования Touch ID и Face ID для разблокировки устройства	+	+
Запрет определения положения запястья для Apple Watch	+	+
Запрет подсказки пароля при первом подключении к AirPlay	+	+
Запрет уведомлений от Apple Wallet при заблокированном экране	+	+
Запрет показа Control Center когда экран заблокирован	+	+
Запрет показа Центра Уведомлений, когда экран заблокирован	+	+
Запрет показа Today, когда экран заблокирован	+	+
Запреты по потреблению контента	+	+
Контроль устройства в режиме Supervised		
Запрет изменения настроек Bluetooth		+
Запрет доступа к файлам на устройстве по USB		+
Запрет подключения к USB носителям при заблокированном устройстве		+
Запрет использования NFC		+
Запрет подключения к Wi-Fi сетям кроме заранее заданных		+
Запрет выключения Wi-Fi		+
Запрет создания профилей VPN		+

	Возможности по контролю за личным устройством сотрудника (non-supervised)	Возможности по контролю устройства, которым владеет компания (режим iOS-supervised)
Веб-контроль (черный список, белый список)		+
Запрет использования FaceID		+
Запрет шаринга экрана		+
Запрет AirDrop		+
Запрет iMessage		+
Запрет Apple Music и радио в Apple Music		+
Запрет модификаций настроек Bluetooth		+
Запрет фильтра нецензурной лексики и демонстрации контента пользователя в Siri		+
Запрет iBooks Store		+
Запрет Apple Configurator		+
Запрет AppStore		+
Запрет автоматической загрузки приложений		+
Запрет удаления приложений		+
Запрет хранения документов и данных в iCloud		+
Запрет full reset		+
Запрет установки конфигурационных профилей		+
Запрет изменения настроек аккаунта		+
Запрет изменения настроек мобильной сети		+
Запрет изменения имени устройства		+
Запрет изменения настроек Find My Friends		+
Запрет изменения настроек уведомлений		+
Запрет изменения пароля на устройстве		+
Запрет изменения настроек Touch ID и Face ID		+
Запрет изменения ограничений		+
Запрет изменения обоев		+
Запрет Non-configurator hosts		+
Запрет Spot Light suggestions		+
Запрет изменения настроек передачи диагностической информации в Apple		+
Запрет подключения к устройству Apple Watch		+
Запрет использования предиктивных подсказок на клавиатуре		+
Запрет использования keyboard shortcuts		+

	Возможности по контролю за личным устройством сотрудника (non-supervised)	Возможности по контролю устройства, которым владеет компания (режим iOS-supervised)
Запрет автоматической коррекции слов		+
Запрет проверки орфографии		+
Запрет поиска в словаре		+
Запрет использования iTunes		+
Запрет использования News		+
Запрет использования Podcasts		+
Запрет Game Center		+
Запрет использования Safari		+

kaspersky