КОД безопасности

Secret MDM

Инструкция

Работа в панели администратора

Почтовый адрес:	**115127, Россия, Москва, а/я 66 ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Введение

Инструкция предназначена для администраторов изделия "Программный комплекс Secret MDM" (далее — Secret MDM, комплекс). В ней содержатся сведения, необходимые для работы в панели администратора Secret MDM.

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru/.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training-courses/.

Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Пользовательский интерфейс панели администратора Secret MDM

Вход в Secret MDM

Для работы администратору необходимо иметь логин и пароль доступа к панели администратора Secret MDM.

Примечание.

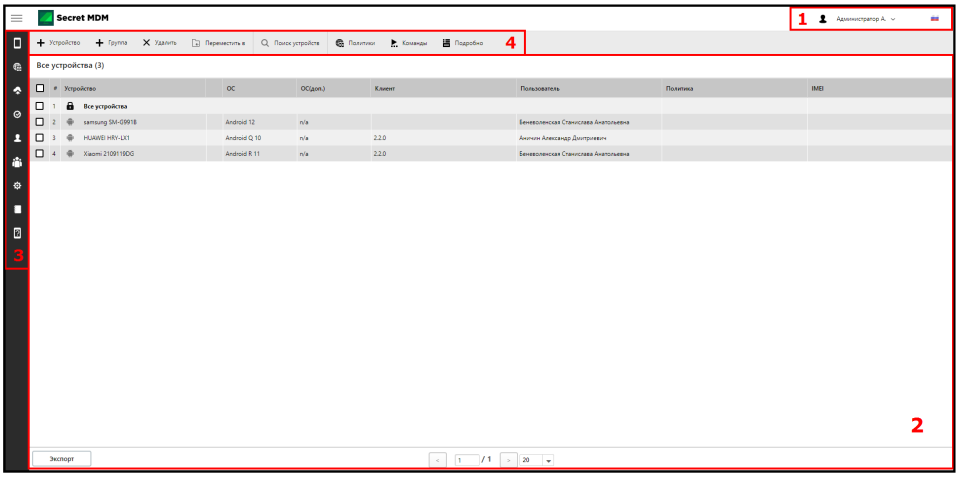
- Для работы с панелью администратора обновите браузер до последней версии.
- Адрес сервера, логин и пароль для доступа к панели администратора выдаются уполномоченным лицом предприятия – владельца сервера.

Для входа в Secret MDM:

1. Откройте веб-страницу панели администратора Secret MDM.

2. Введите логин и пароль и нажмите кнопку "Войти".

   После успешного входа появится окно панели администратора Secret MDM.



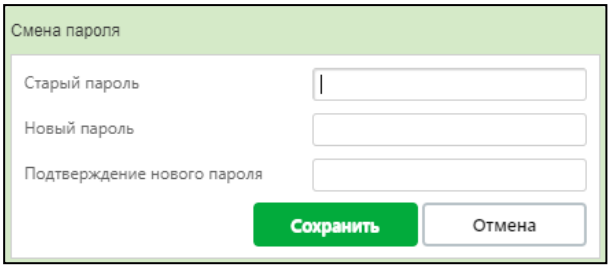
Панель администратора состоит из:

Обозначение	Описание
1	Меню для смены пароля и выхода из учетной записи
2	Область отображения информации раздела
3	Панель навигации
4	Панель инструментов

Для смены пароля:

1. В правом верхнем углу наведите курсор на значок справа от имени администратора .

2. Нажмите кнопку "Сменить пароль".
   На экране появится окно "Смена пароля".



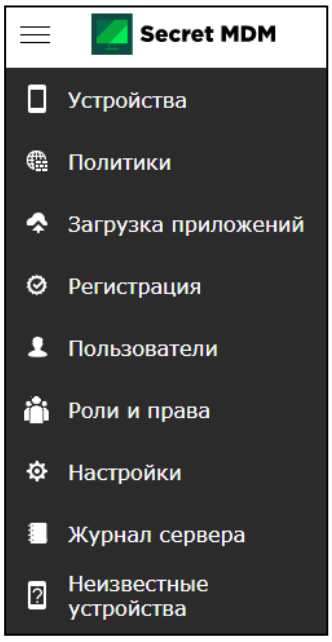
3. Введите старый и новый пароли в соответствующие поля.
4. Нажмите кнопку "Сохранить".
   На экране появится сообщение об успешной смене пароля.

Для выхода из аккаунта:

1. В правом верхнем углу наведите курсор на значок справа от имени администратора .
2. Нажмите кнопку "Выйти".
   Будет осуществлен выход из учетной записи администратора.
   Откроется страница входа в панель администратора Secret MDM.

Панель навигации

В левой части окна расположена панель навигации, на которой отображается список разделов панели администратора. Для переключения внешнего вида панели навигации используется кнопка .



Панели навигации Secret MDM содержит следующие разделы:

Значок	Название раздела	Описание
	Устройства	Раздел предназначен для управления работой мобильных устройств пользователей Secret MDM
	Политики	Раздел предназначен для управления политиками безопасности

Значок	Название раздела	Описание
	Загрузка приложений	Раздел предназначен для управления приложениями, которые добавляются в политики для управления их работой на устройстве
	Регистрация	Раздел предназначен для управления запросами на регистрацию устройства пользователя
	Пользователи	Раздел предназначен для управления учетными записями пользователей
	Роли и права	Раздел предназначен для просмотра доступных ролей привилегированных пользователей и редактирования прав администратора группы
	Настройки	Раздел предназначен для загрузки лицензий Secret MDM, просмотра версий компонентов системы и паролей сервисного режима
	Журнал сервера	Раздел предназначен для просмотра и экспорта событий, регистрируемых комплексом
	Неизвестные устройства	Раздел предназначен для управления устройствами, которые не поддерживаются комплексом

Управление устройствами

Раздел "Устройства" предназначен для управления устройствами пользователей Secret MDM и позволяет администратору:

- отправлять запросы на регистрацию устройств в Secret MDM (см. стр. **8**);
- создавать группы устройств (см. стр. **9**);
- удалять устройства или группы из Secret MDM (см. стр. **10**);
- перемещать выбранные устройства или группы устройств (см. стр. **9**);
- выполнять поиск устройств по заданным параметрам (см. стр. **10**);
- открывать панель со списком доступных для назначения на устройство политик (см. стр. **10**);
- выполнять команды на устройствах (см. стр. **11**);
- отображать журнал событий устройства, информацию о параметрах выбранного устройства, статусе его подключения к Secret MDM (см. стр. **15**).

Регистрация устройства пользователя

Приглашение на регистрацию отправляется администратором пользователю мобильного устройства. Идентификация пользователя осуществляется с помощью электронной почты.

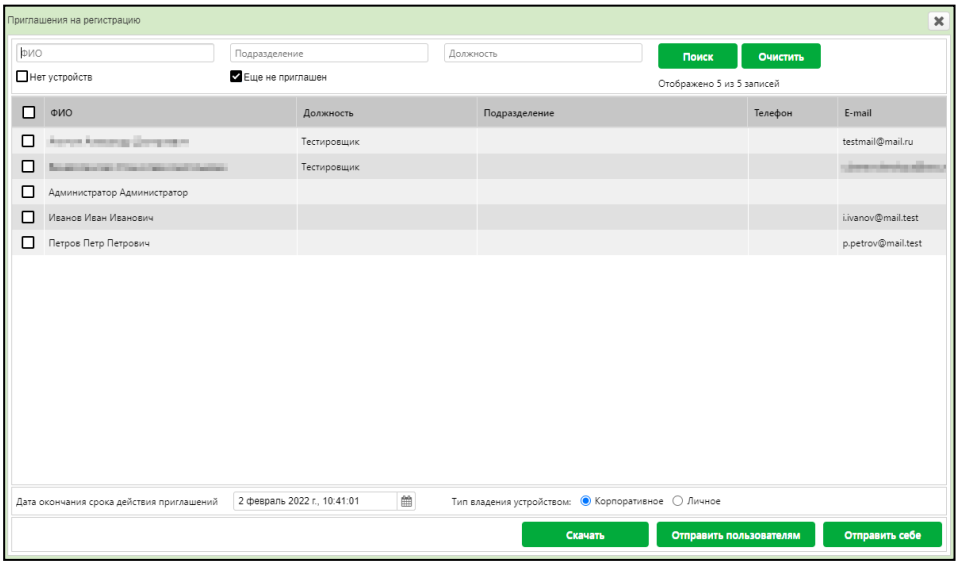
Администратору доступны:

- создание запроса на регистрацию устройства (см. ниже);
- просмотр статуса запроса (см. стр. **26**);
- удаление запроса на регистрацию пользователя (см. стр. **27**).

Для создания запроса на регистрацию устройства:

1. На панели навигации выберите раздел "Устройства".
2. На панели инструментов нажмите Устройство.

   Откроется окно "Приглашение на регистрацию".



3. Выберите одного или нескольких пользователей, установив соответствующие отметки напротив нужных записей (при необходимости можно воспользоваться доступными фильтрами).
4. В поле "Дата окончания срока действия приглашений" укажите требуемое значение.
5. Для отправки запросов выполните одно из следующих действий:
   - нажмите кнопку "Отправить себе" для отправки QR-кодов на электронную почту администратора, указанную в учетной записи;
   - нажмите кнопку "Отправить пользователям" для отправки QR-кодов на электронную почту выбранным пользователям;
   - нажмите кнопку "Скачать" для скачивания QR-кодов на ПК администратора.
6. Нажмите кнопку "ОК".

После создания и отправления запроса в разделе "Регистрация" будет создана соответствующая запись.

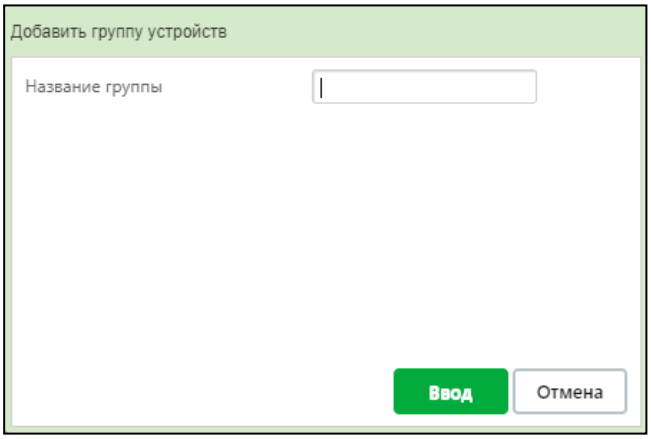
Примечание. Создать запрос на регистрацию устройства можно в разделе "Регистрация" (см. стр. 26).

Управление устройствами и группами устройств

Для создания группы устройств:

1. На панели навигации выберите раздел "Устройства".
2. На панели инструментов нажмите + Группа.

   Появится окно добавления группы устройств.



3. Введите название группы и нажмите кнопку "Ввод".

   Созданная группа появится в списке устройств.

Для добавления устройств в группу:

1. В разделе "Устройства" выберите устройство или существующую группу, установив соответствующие отметки напротив нужных записей.
2. На панели инструментов нажмите Переместить в.

   Окно "Выбор группы устройств" появится на экране.

3. Укажите нужную группу и нажмите кнопку "Выбрать".

   Соответствующие устройства или группы устройств будут перемещены в указанную группу.

Для удаления устройств из группы:

1. В разделе "Устройства" перейдите в необходимую группу.
2. Выберите устройство или группу, установив соответствующие отметки напротив нужных записей.
3. На панели инструментов нажмите Переместить в.
4. В появившемся окне выберите "Все устройства" и нажмите кнопку "Выбрать".

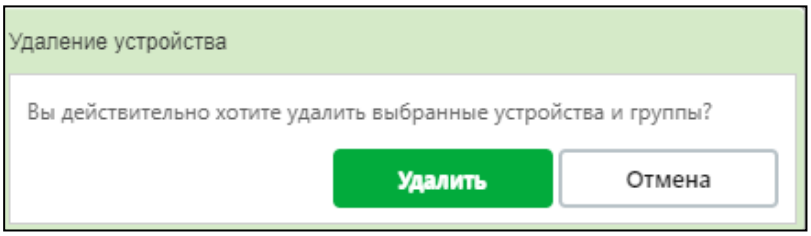
   Выбранные устройства будут удалены из группы и перемещены в общий список устройств.

Для удаления устройств и групп устройств:

Внимание! Перед удалением группы устройств необходимо удалить все устройства из удаляемой группы (см. выше).

1. В разделе "Устройства" выберите устройство и/или группу, установив соответствующие отметки напротив нужных записей.
2. На панели инструментов нажмите Удалить.

   На экране появится окно подтверждения удаления.



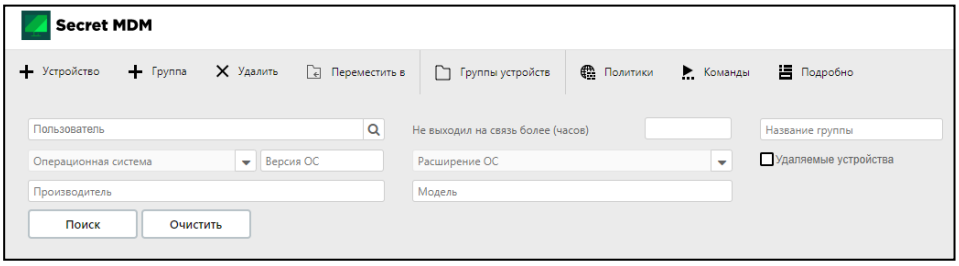
3. Нажмите "Удалить".

   Устройство или группа будут удалены из списка.

Для поиска устройства:

1. В разделе "Устройства" на панели инструментов нажмите Поиск устройств.

   Откроется окно поиска устройств.



2. Заполните поля в соответствии с необходимыми параметрами поиска и нажмите кнопку "Поиск".

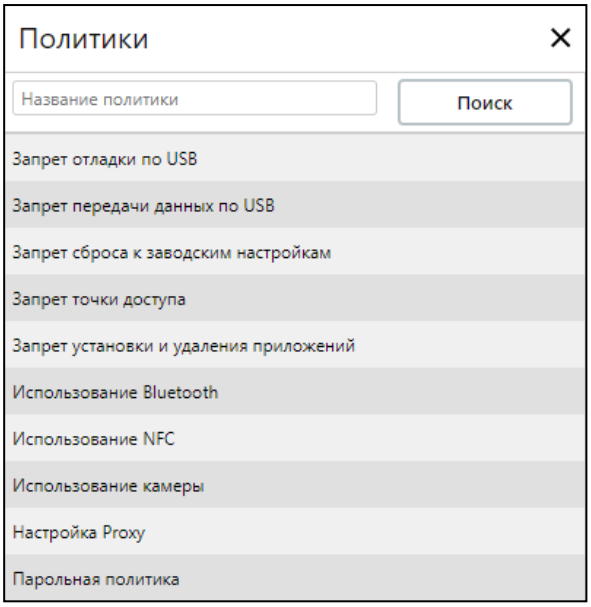
   На экране появится список устройств, соответствующих указанным параметрам.

Примечание. Для возврата к списку устройств нажмите кнопку "Группы устройств".

Для применения политик безопасности:

1. В разделе "Устройства" на панели инструментов нажмите Политики.

   Справа откроется панель со списком политик.



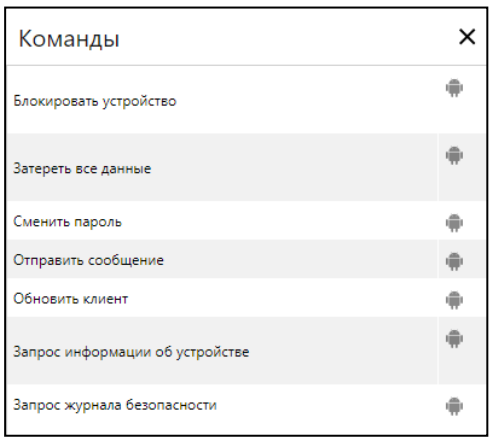
2. Выберите устройство и/или группу устройств, установив соответствующие отметки напротив нужных записей.
3. В панели со списком политик выберите нужную группу. При необходимости воспользуйтесь строкой поиска.
4. Нажмите кнопку "Назначить" внизу панели со списком политик.

   На экране появится соответствующее сообщение.
5. Нажмите кнопку "ОК".

   Назначенные политики начнут действовать на выбранных устройствах и/или группах устройств.

Команды управления работой устройства

Администратор может отправлять на устройство или группы устройств определенные команды, влияющие на его работу. На рисунке ниже представлен список команд управления работой мобильного устройства.



Блокировка устройства

На устройстве будет заблокирован экран. Пароль блокировки, сгенерированный на сервере, заменит текущий пароль. Устройство будет переведено в режим ожидания.

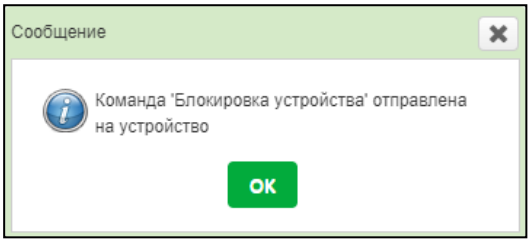
Примечание. Пароль блокировки будет неизвестен как пользователю, так и администратору Secret MDM. При этом он будет обладать стойкостью, исключающей подбор как ручными, так и автоматическими средствами. Разблокировать устройство сможет только администратор, прислав команду "Сменить пароль".

Для блокировки устройства:

1. На панели навигации выберите раздел "Устройства".
2. Выберите устройство и/или группу, установив соответствующие отметки напротив нужных записей.
3. На панели инструментов нажмите Команды.

   Справа появится список команд.
4. Выберите команду "Блокировать устройство" и нажмите кнопку "Выполнить команду".
5. В открывшемся диалоговом окне нажмите кнопку "Отправить".

   Появится сообщение о том, что команда отправлена на устройство.



6. Нажмите кнопку "ОК".

Обнуление устройства

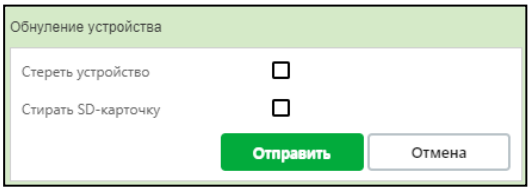
Из памяти устройства (кроме Samsung-устройств с Knox-контейнером) будут удалены все обновления, личные файлы, программы (в том числе Secret MDM), очищен раздел внутренней памяти данных пользователя (sdcard).

Для удаления данных с устройства:

1. На панели навигации выберите раздел "Устройства".
2. Выберите устройство и/или группу, установив соответствующие отметки напротив нужных записей.
3. На панели инструментов нажмите Команды.

   Справа появится список команд.
4. Выберите команду "Затереть все данные" и нажмите кнопку "Выполнить команду".

   На экране появится окно "Обнуление устройства".



5. Выберите нужные параметры и нажмите кнопку "Отправить".

   Появится сообщение о том, что команда отправлена на устройство.
6. Нажмите кнопку "ОК".

Смена пароля

На устройстве будет заблокирован экран. Пароль блокировки заменит текущий пароль. Устройство будет переведено в режим ожидания.

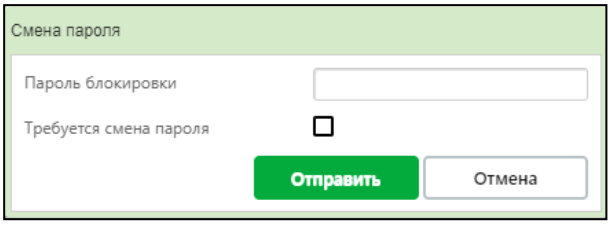
Для смены пароля и блокировки экрана:

1. На панели навигации выберите раздел "Устройства".
2. Выберите устройство или группу, установив соответствующие отметки напротив нужных записей.
3. На панели инструментов нажмите Команды.

Справа появится список команд.

4. Выберите команду "Сменить пароль" и нажмите кнопку "Выполнить команду".

   На экране появится окно "Смена пароля".



5. Заполните поля и нажмите кнопку "Отправить".

   Появится сообщение о том, что команда отправлена на устройство.

6. Нажмите кнопку "ОК".

Отправка сообщения

Команда позволяет администратору отправлять сообщения на устройство.

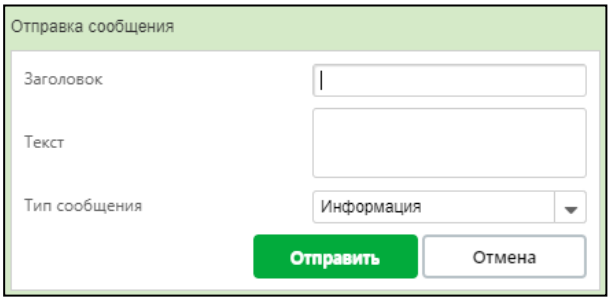
Для отправки сообщения:

1. На панели навигации выберите раздел "Устройства".
2. Выберите устройство и/или группу, установив соответствующие отметки напротив нужных записей.
3. На панели инструментов нажмите Команды.

   Справа появится список команд.

4. Выберите команду "Отправить сообщение" и нажмите кнопку "Выполнить команду".

   На экране появится окно "Отправка сообщения".



5. Заполните поля и нажмите кнопку "Отправить".

   Появится оповещение о том, что сообщение отправлено на устройство.

Обновление Secret MDM

Команда позволяет администратору обновить версию Secret MDM на устройстве пользователя.

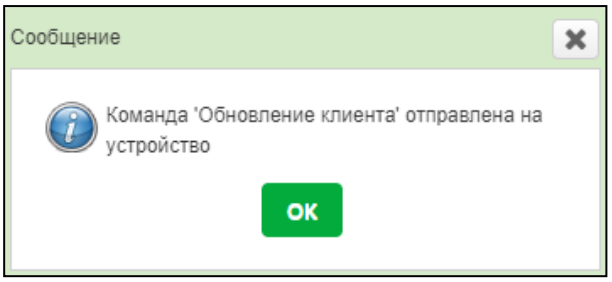
Для обновления Secret MDM на устройствах:

1. На панели навигации выберите раздел "Устройства".
2. Выберите устройство и/или группу, установив соответствующие отметки напротив нужных записей.
3. На панели инструментов нажмите Команды.

   Справа появится список команд.

4. Выберите команду "Обновить клиент" и нажмите кнопку "Выполнить команду".
5. В появившемся окне нажмите кнопку "Отправить".

Появится сообщение о том, что команда отправлена на устройство.



6. Нажмите кнопку "OK".

Запрос информации об устройстве

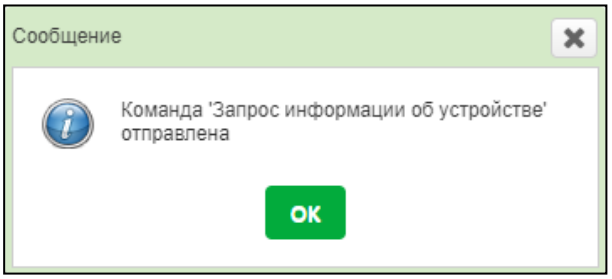
При запросе информации об устройстве администратор получает информацию о наличии root- прав у пользователя устройства, примененных политиках, установленных приложениях, точках доступа Wi-Fi и т.д.

Для запроса информации:

1. На панели навигации выберите раздел "Устройства".
2. Выберите устройство и/или группу, установив соответствующие отметки напротив нужных записей.
3. На панели инструментов нажмите Команды.

   Справа появится список команд.
4. Выберите команду "Запрос информации об устройстве" и нажмите кнопку "Выполнить команду".
5. В открывшемся диалоговом окне нажмите кнопку "Отправить".

   Появится сообщение о том, что команда отправлена на устройство.



6. Нажмите кнопку "OK".

Запрос журнала безопасности

Администратор Secret MDM отправляет на устройство запрос о предоставлении журнала событий, связанных с нарушением или изменением настроек безопасности. Для выполнения этой команды на устройстве должна действовать политика "Журнал событий". Оперативный ответ на запрос возможен, если устройство подключено к серверу. В противном случае информация о событиях безопасности поступит только тогда, когда устройство свяжется с сервером.

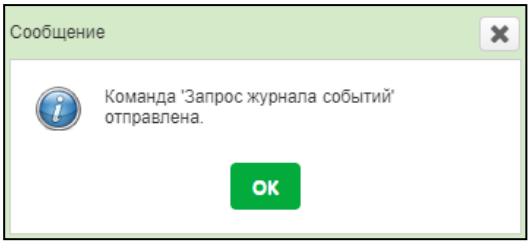
Для запроса журнала безопасности:

1. На панели навигации выберите раздел "Устройства".
2. Выберите устройство и/или группу, установив соответствующие отметки напротив нужных записей.
3. На панели инструментов нажмите Команды.

   Справа появится список команд.
4. Выберите команду "Запрос журнала безопасности" и нажмите кнопку "Выполнить команду".

5. В открывшемся диалоговом окне нажмите кнопку "Отправить".

   Появится сообщение о том, что команда отправлена на устройство.



6. Нажмите кнопку "OK".

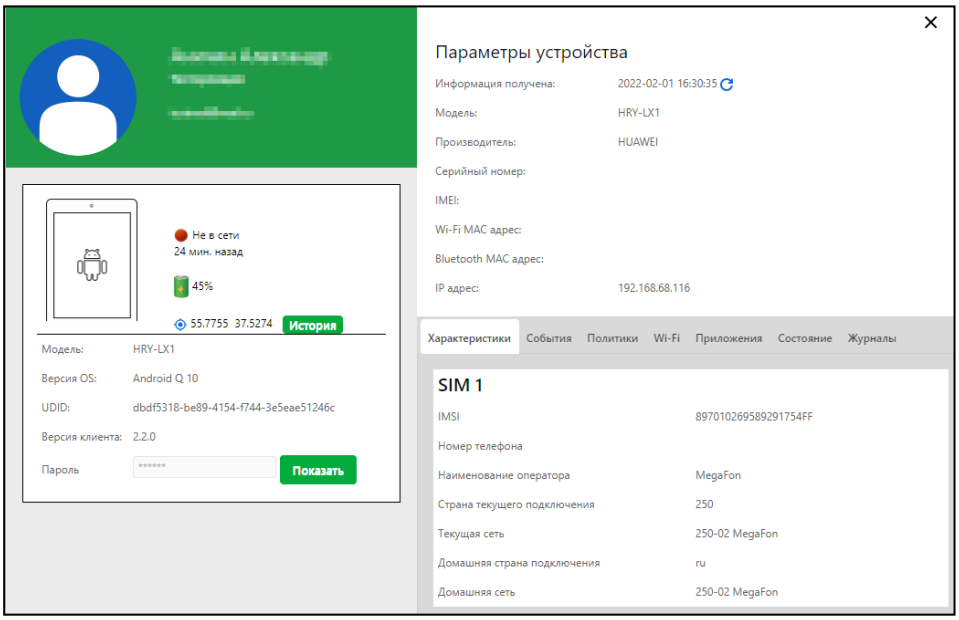
Информация об устройстве или группе устройств

Администратор может получить актуальную информацию о мобильном устройстве пользователя или о группах устройств.

Для получения информации об устройстве:

1. На панели навигации выберите раздел "Устройства".
2. Выберите устройство, установив соответствующую отметку напротив нужных записей.
3. На панели инструментов нажмите Подробно.

   На экране отобразится панель с информацией об устройстве.



Подробная информация об устройстве содержится на соответствующих вкладках панели:

Название	Описание
Характеристики	Информация о SIM-картах, установленных в устройстве пользователя
События	Информация о событиях безопасности на устройстве
Политики	Список политик, применяемых на устройстве, и их статус
Wi-Fi	Список используемых точек доступа Wi-Fi
Приложения	Список установленных на устройстве приложений
Состояние	Параметры состояния устройства
Журналы	Просмотр журнала клиента за определенный промежуток времени и комментариев клиента к записям журнала

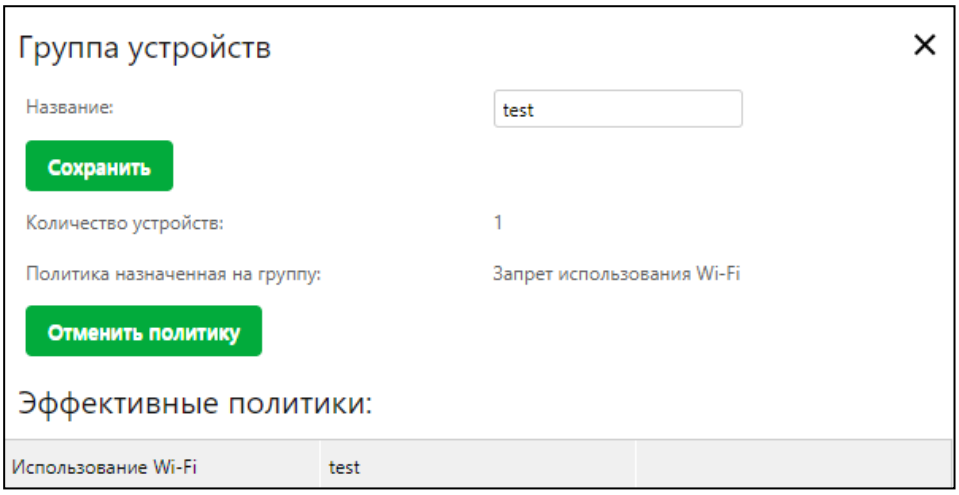
4. Для просмотра сведений о местоположении устройства нажмите кнопку "История" в левой части панели.

   Координатами или отметкой на карте будет обозначено местоположение устройств в данный момент времени.

Для получения информации о группах устройств:

1. В разделе "Устройства" выберите группу устройств, установив соответствующую отметку.
2. На панели инструментов нажмите Подробно.

   На экране отобразится панель "Группа устройств".



На панели выше содержится следующая информация:

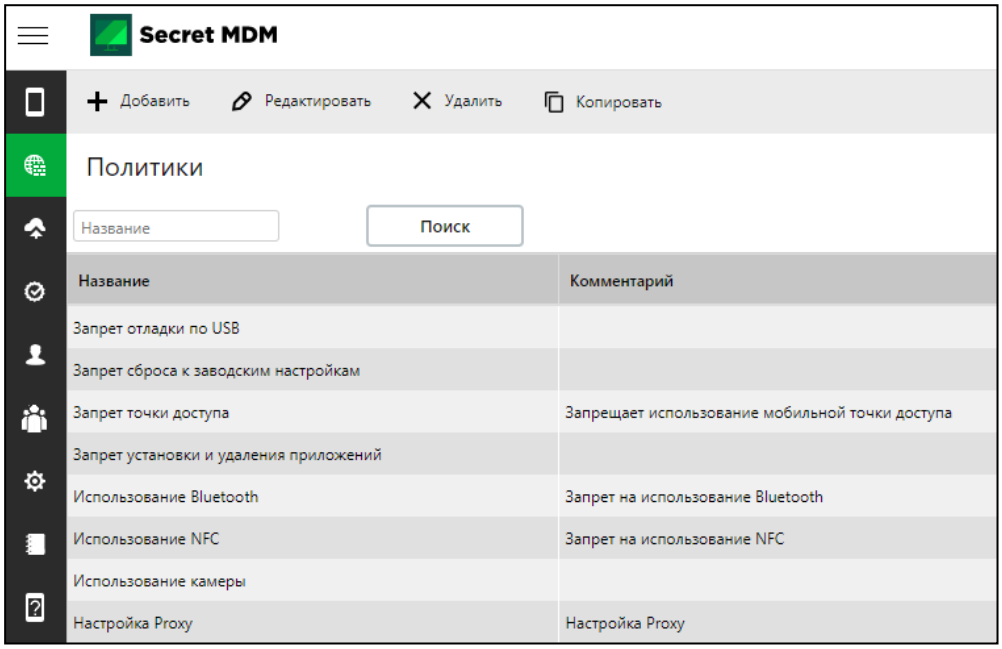
- название группы;
- количество устройств в группе;
- название назначенной группы политик;
- действующие эффективные политики — политики, входящие в сформированную группу политик.

Управление политиками

Управление устройствами обеспечивается применением политик безопасности. Политика — набор настроек для организации безопасной работы пользователей с мобильными устройствами.

Группы политик

Secret MDM позволяет сформировать и управлять списком групп политик, которые впоследствии могут быть применены на зарегистрированных устройствах и/или группах устройств.

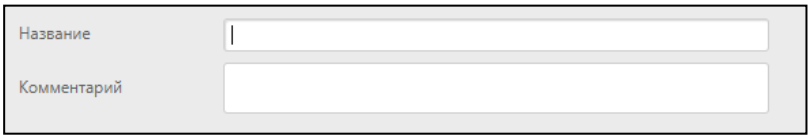


В разделе "Политики" доступны создание, редактирование, удаление и копирование политик безопасности.

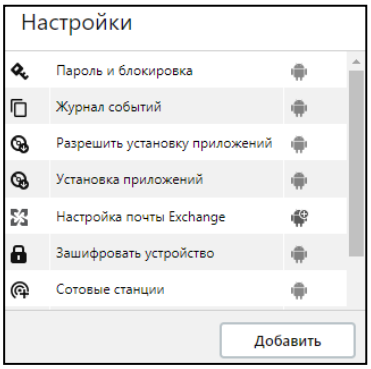
Для создания группы политик:

1. На панели навигации выберите раздел "Политики".
2. На панели инструментов нажмите Добавить.

   В центральной части экрана появится окно создания группы политик.
3. Введите название группы, при необходимости добавьте комментарий.



4. Добавьте требуемые политики в группу, выбрав их из списка справа.



5. После добавления всех необходимых политик в группу выполните настройку параметров политик и нажмите кнопку "Сохранить".

   Группа политик появится в списке. Окно создания политик закроется.

Для редактирования группы политик:

1. В разделе "Политики" выберите нужную группу политик из списка.
2. На панели инструментов нажмите Редактировать.

   В центральной части экрана появится окно редактирования группы политик.
3. Измените параметры политик, добавьте или удалите нужные политики.
4. После завершения редактирования нажмите кнопку "Сохранить" в нижней части экрана.

   Изменения будут сохранены. Окно редактирования политик закроется.

Для удаления группы политик:

1. В разделе "Политики" выберите в списке нужную группу политик.
2. На панели инструментов нажмите Удалить.

   На экране появится окно подтверждения удаления политики.
3. Нажмите "Да".

   Группа политик будет удалена из списка.

Для копирования группы политик:

1. В разделе "Политики" выберите нужную группу политик из списка.
2. На панели инструментов нажмите Копировать.

   В правой части экрана появится окно редактирования группы политик.
3. При необходимости измените название группы политик и отредактируйте параметры.
4. Нажмите кнопку "Сохранить" в нижней части экрана.

   В списке появится новая группа политик. Окно редактирования закроется.

Параметры политик безопасности

Примечание. Политики назначаются как отдельным устройствам в группе, так и целиком группам устройств. Назначение политики группе устройств не отменяет действие политик, назначенных отдельным конкретным устройствам из этой группы, если они не противоречат друг другу.

Пароль и блокировка

Данная политика устанавливает минимальные требования к паролям и определяет порядок блокировки устройства пользователя. Пользователь имеет возможность использовать более стойкий пароль, чем предписано политикой.

Информация об обновлении парольной политики отображается в журнале Secret MDM на устройстве пользователя. Текущие значения парольной политики на устройстве приводятся в разделе "Политики".

Политика паролей состоит из следующих параметров:

- Тайм-аут экрана — период неактивности пользователя, по истечении которого экран будет выключен и заблокирован.
- Срок действия пароля — период действия пароля на устройстве. По истечении срока действия необходимо сменить пароль.
- Тип пароля — символьный или цифровой.
- Длина истории паролей — новый пароль проверяется на совпадение с предыдущими паролями.

Примечание. Если политика входит в группу политик, назначенных на устройство, при отмене данной политики будет отменена вся группа.

Журнал событий

Данная политика устанавливает срок хранения записей в журнале событий устройства и позволяет осуществлять отправку журналов событий.

Под сроком хранения записей понимается период времени, в течение которого будут сохраняться события в журнале.

Разрешить установку приложений

Данная политика позволяет разрешать/запрещать пользователю самостоятельно устанавливать и удалять приложения.

Если установка приложений запрещена, то при попытке установить или удалить какое-либо приложение как с помощью Google Play Store (или аналогичных сервисов), так и средствами настройки мобильного устройства на устройстве пользователя появится экран блокировки Secret MDM.

Примечание. Если запрещены установка и удаление приложений, произвести обновление Secret MDM будет невозможно.

Установка приложений

Данная политика позволяет сформировать список приложений, которые будут установлены на устройство пользователя при ее применении.

Если пользователь удалит приложение, включенное в список обязательных, через некоторое время на экране появится следующее системное сообщение: "Для работы требуется установить приложения", и так до тех пор, пока пользователь не установит все приложения из сформированного списка. Если пользователь удалит приложение, которое было добавлено в политику из раздела "Сторонние приложения", то оно будет снова установлено автоматически.

Примечание. Политики установки, удаления и блокировки приложений взаимосвязаны: если на устройство поступило несколько противоречащих друг другу политик, будет применена политика, полученная последней.

Для формирования списка приложений для установки:

1. В разделе "Политики" на центральной панели нажать кнопку "Выбрать приложение".
2. Заполнить политику приложениями из каталога.

   При выборе приложений из списка доступен текстовый поиск.

Удаление приложений

Данная политика позволяет сформировать список приложений, которые должны быть удалены с устройства пользователя при ее применении.

Если пользователь выполнит установку приложения, которое находится в данном списке, через некоторое время оно будет автоматически удалено.

Примечание. Политики установки, блокировки и удаления приложений взаимосвязаны: если на устройство поступило несколько противоречащих друг другу политик, то действовать будет политика, полученная последней.

Черный список приложений

При назначении данной политики на устройстве блокируется работа приложений, содержащихся в сформированном администратором списке.

При запуске заблокированных приложений на устройстве появится экран блокировки.

Примечание. Политики установки, блокировки и удаления приложений взаимосвязаны: если на устройство поступило несколько противоречащих друг другу политик, то действовать будет политика, полученная последней.

Использование Bluetooth

Данная политика разрешает или запрещает использование Bluetooth на устройстве.

При применении политики происходит блокировка кнопки активации Bluetooth и очистка списка доступных подключений. Если запрещающая политика была получена устройством в момент использования Bluetooth, в результате применения политики кнопка Bluetooth будет заблокирована, соединение разорвано, а список доступных подключений — очищен.

Использование звукозаписи

Данная политика позволяет администратору Secret MDM управлять микрофоном мобильного устройства пользователя. Если включен запрет на использование микрофона, то им будет невозможно пользоваться из сторонних приложений.

Примечание. Функция использования звукозаписи может не быть заблокирована данной политикой, при этом запись звука осуществляться не будет и в сохраненном аудиофайле звук будет отсутствовать.

Использование камеры

Данная политика позволяет заблокировать доступ пользователю к камере мобильного устройства из приложения "Камера" и из сторонних приложений, в том числе установленных в Knox-контейнере. При попытке разрешить доступ к камере с помощью настроек в журнале безопасности будет зарегистрировано соответствующее событие.

Использование Wi-Fi

Данная политика разрешает или запрещает использование на устройстве пользователя технологии Wi-Fi, а также регламентирует ее принудительное включение.

Примечание. Применение запрещающей политики не подразумевает запрет на передачу данных по протоколам 3G/4G.

При применении данной политики пользователь не сможет произвольно выключать Wi-Fi на устройстве. При попытке совершить данное действие подключение будет восстановлено автоматически, а на сервер будет отправлено соответствующее сообщение. Запись о событии появится на вкладке "События" панели информации об устройстве.

Если использование Wi-Fi-сетей разрешено, оно регулируется политиками, описанными ниже.

Настройка Wi-Fi-точек

Данная политика добавляет конкретные точки доступа Wi-Fi на устройстве или изменяет их настройки. Если в назначенной на устройство политике "Использование Wi-Fi" выбрана опция "Включить принудительно", при назначении на устройство данной политики:

- присланные администратором точки доступа Wi-Fi будут иметь приоритет для подключения. При наличии доступной настроенной сети подключение к иным точкам доступа будет заблокировано (устройство будет автоматически переключаться на одну из доступных сетей);
- при наличии нескольких доступных сетей будет выбрана сеть с наиболее сильным на момент подключения сигналом;
- при отсутствии доступа к приоритетным точкам доступа Wi-Fi устройство сможет подключаться к любым другим точкам.

Политика состоит из следующих параметров:

- SSID — идентификатор Wi-Fi-сети;
- пароль — пароль выбранной Wi-Fi-сети;

- тип авторизации — тип шифрования Wi-Fi-сети (WEP, WPA);
- адрес proxy;
- порт proxy.

Удаление Wi-Fi-точек

С помощью данной политики администратор может удалить точки доступа, добавленные на устройство политикой Secret MDM. Настройки точек доступа, добавленные пользователем вручную, удалены не будут, но подключение к этим точкам доступа будет заблокировано.

Для удаления Wi-Fi-точки необходимо внести SSID точки доступа.

Белый список Wi-Fi-точек

Данная политика устанавливает для устройств список точек доступа Wi-Fi, к которым разрешено подключение. Подключение к точкам вне списка будет заблокировано.

Для добавления в список Wi-Fi-точки необходимо внести SSID точки доступа.

Настройка Proxy

Данная политика устанавливает настройки глобального HTTP-proxy для всех точек доступа Wi-Fi. Если для какой-то из точек доступа HTTP-proxy был настроен ранее, он не будет заменен. Если какая-то из точек доступа, открытая для подключения, будет удалена пользователем, при следующей попытке подключения к сети она будет автоматически восстановлена, и HTTP-трафик будет проходить с использованием заданного Proxy-сервера.

Примечание. Данная политика влияет на процесс установки приложений из репозитория предприятия, поэтому корпоративное хранилище приложений должно быть доступно через заданный Proxy-сервер.

Настройка почты Exchange

Данная политика применяется для устройств с (установленной) ОС Android производства Samsung и определяет настройки почтового клиента, установленного на устройстве.

После применения политики на устройство пользователя поступят сообщение об обновлении настроек почтового аккаунта Exchange и предложение о настройке учетной записи пользователя.

Политика состоит из следующих параметров:

- домен;
- адрес сервера.

Примечание. Для Samsung-устройств, использующих Knox-контейнер, почта будет настроена внутри контейнера.

Зашифровать устройство

Данная политика обязывает пользователя зашифровать все данные на мобильном устройстве.

Сотовые станции

Данная политика отслеживает подключение к сотовым станциям из списка и, в случае попадания устройства пользователя в радиус действия сотовой станции, автоматически активирует работу следующих политик (если они входят в состав группы политик):

- использование Bluetooth (см. стр. **20**);
- использование звукозаписи (см. стр. **20**);
- использование камеры (см. стр. **20**);
- использование Wi-Fi (см. стр. **20**).

Активация данных политик происходит при включении на устройстве режима полета и/или в случае изъятия SIM-карты.

Деактивация политик происходит в следующих случаях:

- отключение от сотовой станции из списка;
- потеря сигнала сотовой связи;
- неисправность SIM-карты.

Использование NFC

Данная политика разрешает или запрещает передачу данных с использованием Android beam на устройстве. Остальные функции NFC, например, оплата банковской картой, остаются доступны.

Примечание. Для полной блокировки NFC необходимо подписать приложение Secret MDM тем же сертификатом, которым подписана ОС.

Использование VPN

Данная политика разрешает или запрещает использование VPN на устройстве. При попытке включить VPN в журнале безопасности будет зарегистрировано соответствующее событие.

Отладка по USB

Данная политика разрешает или запрещает отладку устройства по USB.

Передача данных по USB

Данная политика разрешает или запрещает передачу с устройства данных по USB. При применении этой политики при подключении устройства по USB передача файлов будет недоступна.

Сброс настроек

Данная политика разрешает или запрещает сброс устройства к заводским настройкам. При попытке выполнить сброс настроек в журнале безопасности будет зарегистрировано соответствующее событие.

Запрет исходящих звонков

Данная политика позволяет заблокировать доступ пользователю к функции звонков из приложения "Телефон" и/или сторонних приложений, в том числе установленных в Knox-контейнере.

Примечание. Осуществление звонков на номера экстренных служб остается доступным.

Данная политика не блокирует возможность набора номера — блокируется осуществление вызова. Для блокировки входящих звонков необходимо подписать приложение Secret MDM тем же сертификатом, которым подписана ОС.

Встроенный браузер

Данная политика разрешает или запрещает использование на устройстве встроенного браузера. При использовании другого браузера встроенный пропадает из списка приложений и становится недоступен для использования.

Мобильные данные

Данная политика разрешает или запрещает передачу данных с использованием протоколов 3G/4G.

Примечание. Применение запрещающей политики не подразумевает запрет на передачу данных по Wi-Fi.

При применении данной политики пользователь не сможет произвольно выключать передачу мобильных данных на устройстве. При попытке совершить данное действие подключение будет восстановлено автоматически, а на сервер будет отправлено соответствующее сообщение. Запись о событии появится на вкладке "События" панели информации об устройстве.

Хранилище данных

Данная политика разрешает или запрещает использование внешнего хранилища данных.

Примечание. Если внешний накопитель (SD-карта) уже установлен в устройстве, применение запрещающей политики не заблокирует возможность использования этого накопителя.

SMS

Данная политика позволяет заблокировать доступ пользователю к приложению для отправки SMS-сообщений, в том числе установленных в Knox-контейнере. Кроме того, блокируется получение входящих SMS-сообщений.

Мобильная точка доступа

Данная политика разрешает или запрещает использование на устройстве мобильной точки доступа.

Предоставление всех разрешений приложениям

Данная политика разрешает или запрещает предоставление разрешений всем приложениям.

Частота обмена данными

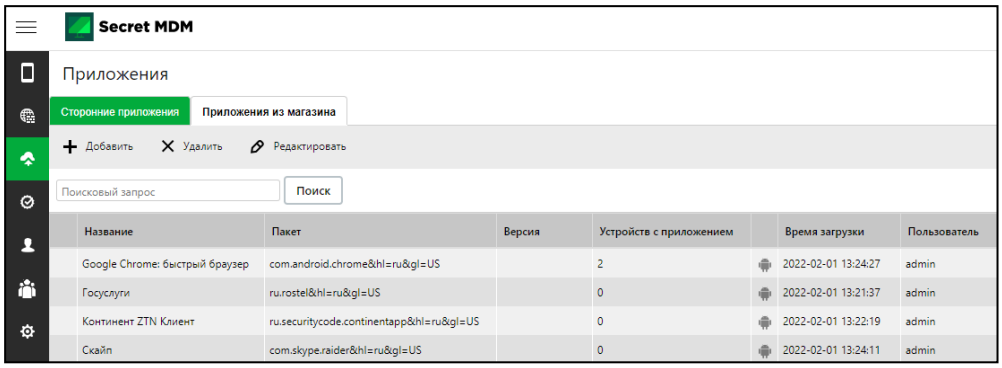
Данная политика регулирует частоту обмена данными с сервером.

Блокировка устройства при смене SIM-карты

Данная политика разрешает или запрещает блокировку устройства при смене SIM-карты.

Управление приложениями

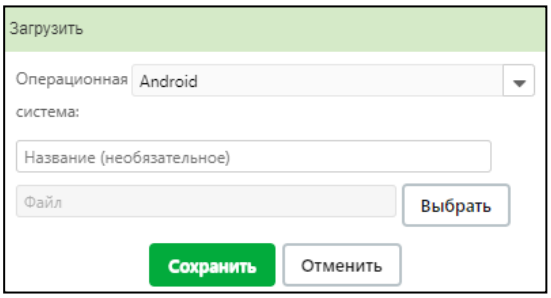
Secret MDM позволяет создать список приложений, которые впоследствии могут быть установлены на устройствах или группах устройств. Приложения в каталог можно добавлять как из магазина Google Play Store, так и загружая apk-файл.



Для добавления стороннего приложения:

1. На панели навигации выберите раздел "Загрузка приложений".
2. В верхней части окна перейдите на вкладку "Сторонние приложения".
3. На панели инструментов нажмите Добавить.

   На экране появится окно для загрузки стороннего приложения.



4. Заполните необходимые поля.
5. Нажмите кнопку "Выбрать".

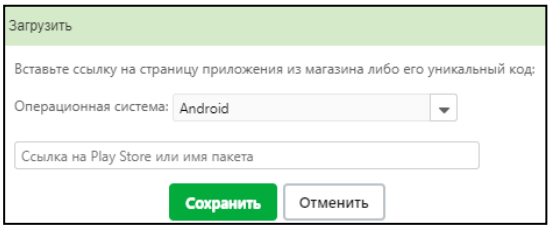
   В появившемся окне выберите нужный файл и нажмите кнопку "Открыть".
6. Нажмите кнопку "Сохранить".

   Диалоговое окно закроется. Новое приложение появится в списке.

Для добавления приложения из магазина:

1. В разделе "Загрузка приложений" в верхней части окна перейдите на вкладку "Приложения из магазина".
2. На панели инструментов нажмите Добавить.

   На экране появится окно для загрузки приложения из магазина.



3. Укажите ссылку на приложение.
4. Нажмите кнопку "Сохранить".

   Диалоговое окно закроется. Новое приложение появится в списке.

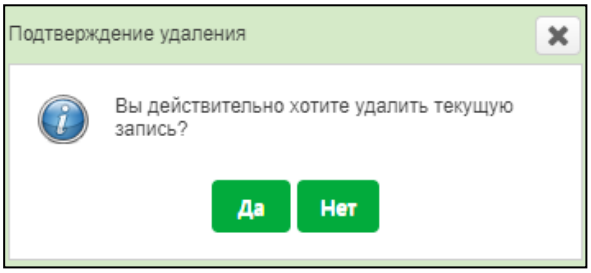
Для редактирования записи о приложении:

1. В разделе "Загрузка приложений" выберите приложение из списка и нажмите Редактировать на панели инструментов.
   На экране появится окно с настройками приложения.
2. Измените нужные параметры записи.
3. Нажмите кнопку "Сохранить".
   Диалоговое окно закроется. Запись о приложении будет отредактирована.

Для удаления приложения:

Внимание! Перед удалением приложения необходимо убедиться, что удаляемое приложение не включено в группу политик.

1. В разделе "Загрузка приложений" выберите приложение из списка и нажмите Удалить на панели инструментов.
   На экране появится окно подтверждения удаления.



2. Нажмите "Да".
   Диалоговое окно закроется. Приложение будет удалено из списка.

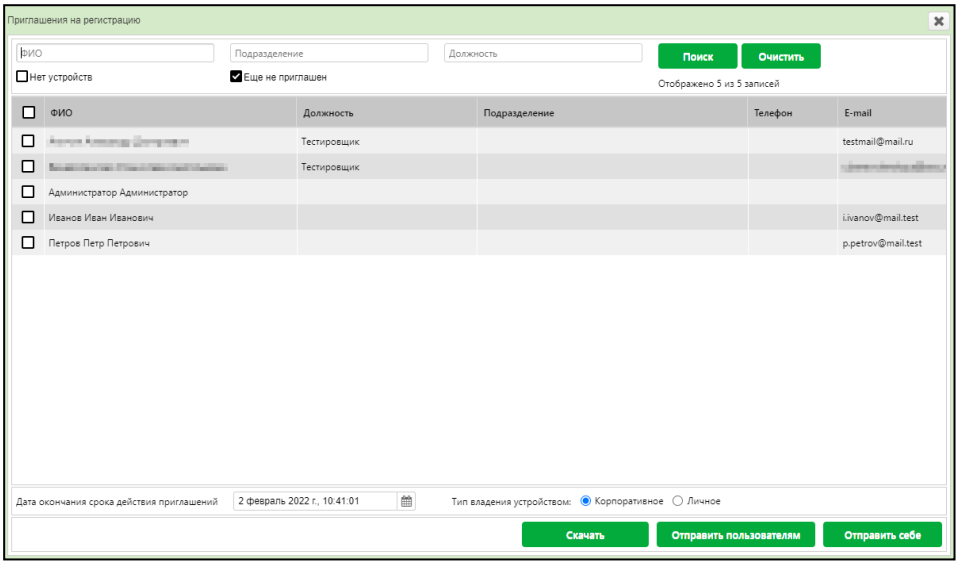
Управление запросами на регистрацию

Управление запросами на регистрацию устройств пользователей выполняется в разделе "Регистрация". Также из этого раздела администратор может узнать о статусе запроса на регистрацию.

Для создания запроса на регистрацию устройства:

1. На панели навигации выберите раздел "Регистрация".
2. На панели инструментов нажмите + Регистрация.

   Откроется список пользователей.



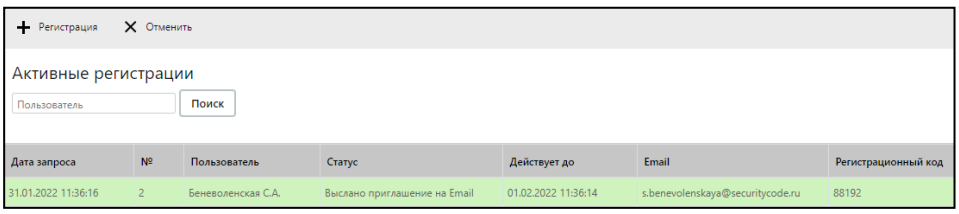
3. Выберите одного или нескольких пользователей, установив соответствующие отметки напротив нужных записей (при необходимости можно воспользоваться доступными фильтрами).
4. В поле "Дата окончания срока действия приглашений" укажите требуемое значение.
5. Для отправки запросов выполните одно из следующих действий:
   - нажмите кнопку "Отправить себе" для отправки QR-кодов на электронную почту администратора, указанную в учетной записи;
   - нажмите кнопку "Отправить пользователям" для отправки QR-кодов на электронную почту выбранным пользователям;
   - нажмите кнопку "Скачать" для скачивания QR-кодов на ПК администратора.
6. Нажмите кнопку "ОК".

После создания и отправления запроса в разделе "Регистрация" будет создана соответствующая запись.

Для просмотра статуса запроса:

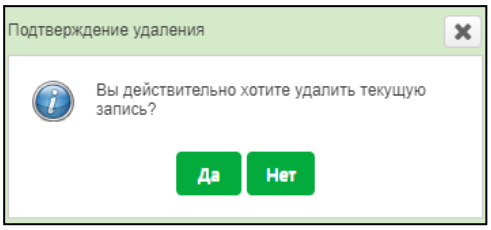
1. На панели навигации выберите раздел "Регистрация".

   На экране появится список активных запросов и их текущее состояние.



Для удаления запроса на регистрацию пользователя:

1. В разделе "Регистрация" в списке активных запросов выберите запрос, который хотите удалить, и нажмите Отменить.
   На экране появится окно подтверждения удаления.



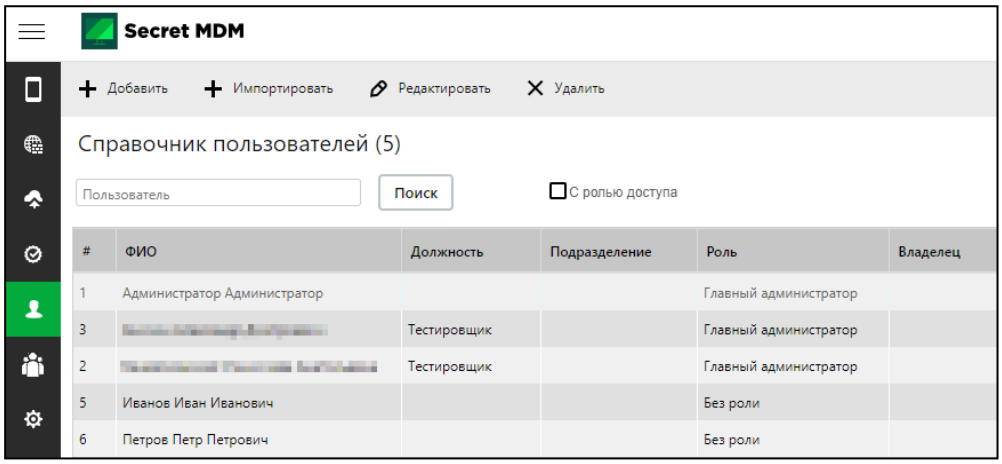
2. Нажмите "Да"
   Запрос будет удален из списка активных регистраций.

Управление пользователями

Раздел содержит список пользователей, зарегистрированных в Secret MDM. Главный администратор имеет право присваивать отдельным пользователям расширенные права доступа к функциям Secret MDM (назначать роли). Привилегированному пользователю может быть присвоена одна из четырех ролей:

- Главный администратор;
- Администратор;
- Администратор группы;
- Аудитор.

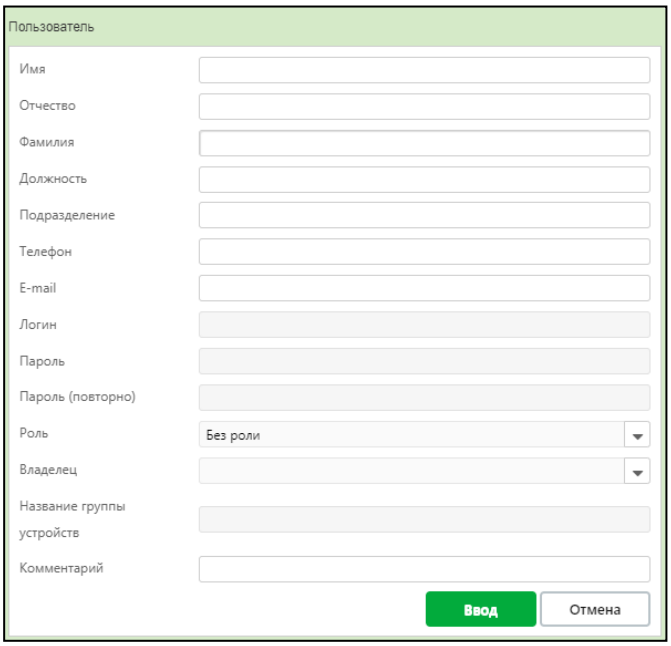
Роли различаются по уровню доступа и функциональным возможностям.



Для регистрации пользователя в системе:

1. На панели навигации выберите раздел "Пользователи".
2. На панели инструментов нажмите Добавить.

   Откроется окно "Пользователь".



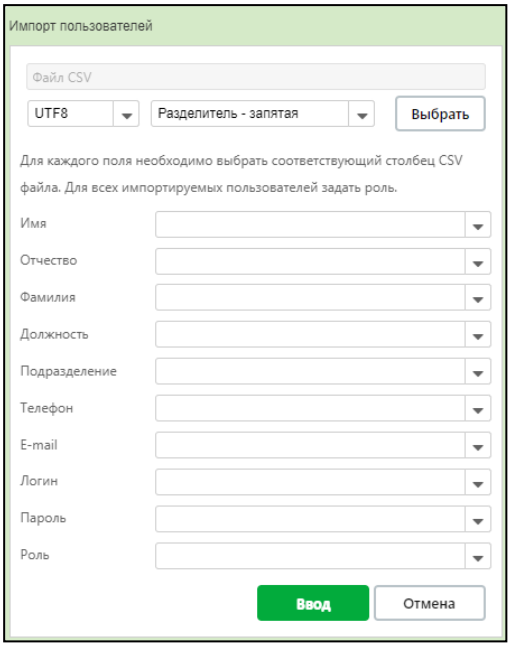
3. Заполните все необходимые поля и нажмите "Ввод".

Внимание! Поля "Фамилия" и "E-mail" являются обязательными для заполнения.

Пользователь будет зарегистрирован в Secret MDM, его учетная запись появится в списке пользователей.

Для импорта пользователей:

1. В разделе "Пользователи" на панели инструментов нажмите + Импортировать.
   Откроется окно "Импорт пользователей".



2. Выберите csv-файл, в котором содержится информация о пользователях.
3. Укажите кодировку файла и разделитель, который в нем используется.
4. Установите соответствие полей csv-файла и полей формы регистрации.

   Внимание! Поля "Фамилия" и "E-mail" являются обязательными для заполнения.

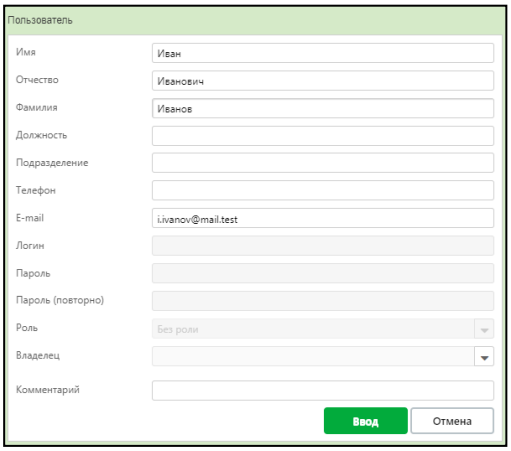
5. Укажите роль пользователя.
6. Для создания привилегированного пользователя задайте логин, пароль для входа в систему и подтверждение пароля.

   Примечание. При создании Администратора группы в разделе "Устройства" будет автоматически создана подчиненная ему группа.

7. Нажмите кнопку "Ввод".
   Пользователи будут зарегистрированы в Secret MDM. Учетные записи появятся в списке пользователей.

Для редактирования информации о пользователе:

1. В разделе "Пользователи" выберите необходимого пользователя из списка.
2. На панели инструментов нажмите Редактировать.
   Откроется окно "Пользователь".



3. Внесите необходимые изменения.

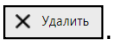
Примечание. Для передачи управления учетной записью пользователя без роли другому Администратору группы измените параметр "Владелец". Операция доступна только Главному администратору Secret MDM.

4. Нажмите "Ввод".

Окно закроется. Изменения отобразятся в списке пользователей.

Для удаления пользователя:

Внимание! Нельзя удалить пользователя с зарегистрированными устройствами.

1. В разделе "Пользователи" выберите из списка пользователя, которого хотите удалить.
2. На панели инструментов нажмите 

.

Откроется окно подтверждения удаления.

3. Нажмите кнопку "Да".

Пользователь будет удален из списка.

Управление ролями и правами

Управление комплексом осуществляют администраторы, обладающие разными уровнями доступа к разделам и функциям Secret MDM:

Главный администратор
Имеет доступ ко всем разделам и функциям комплекса (чтение, создание, удаление, редактирование, просмотр и управление журналами, управление настройками сервера, просмотр информации об устройствах). Только данная роль позволяет осуществлять: • просмотр списка привилегированных пользователей; • создание нового привилегированного пользователя; • удаление существующего привилегированного пользователя; • редактирование прав привилегированных пользователей; • изменение характеристик привилегированного пользователя
Администратор
Имеет доступ ко всем функциям комплекса и право управления всеми разделами, за исключением: • управления учетными записями привилегированных пользователей; • управления журналами; • просмотра вкладок в меню информации об устройстве, на которые отсутствуют права
Аудитор
Имеет право просмотра и управления журналами
Администратор группы
Имеет право: • отправлять диагностические журналы (если это право назначено Главным администратором Secret MDM); • создавать пользователей без роли; • управлять учетными записями и устройствами пользователей без роли, которые входят в группу Администратора группы; • просматривать информацию в меню устройства (если права на просмотр соответствующих вкладок назначены Администратором или Главным Администратором). Администратор группы не видит раздел "Журналы сервера", пользователей, которые не входят в группу Администратора группы, и их устройства

Управление настройками

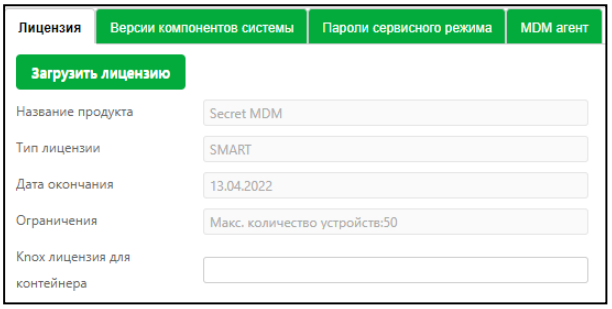
Раздел "Настройки" предназначен для загрузки лицензий Secret MDM, просмотра версий компонентов системы и паролей сервисного режима.

Лицензии

В Secret MDM существуют лицензионные ограничения на использование комплекса. Лицензия предоставляется потребителю в момент приобретения права на использование Secret MDM или предоставления временного права на ознакомление с возможностями комплекса.

Для смены лицензии Secret MDM:

1. На панели навигации выберите раздел "Настройки".
2. На вкладке "Лицензия" нажмите кнопку "Загрузить лицензию".



3. В появившемся окне выберите файл с лицензией Secret MDM и нажмите "Открыть".

   Параметры новой лицензии появятся в соответствующих полях.
4. Нажмите кнопку "Сохранить".

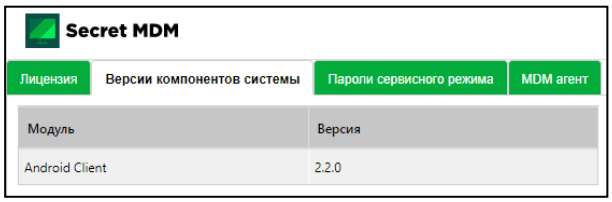
Примечание. Если не указана Knox-лицензия, использование Knox-контейнера на защищаемых Samsung-устройствах невозможно. За приобретением Knox-лицензии обращайтесь в представительство компании Samsung или к ее партнерам.

Для добавления Knox-лицензии:

1. В разделе "Настройки" на вкладке "Лицензия" в поле "Knox-лицензия для контейнера" укажите код Knox-лицензии.
2. Нажмите кнопку "Сохранить".

Версии компонентов системы

В разделе "Настройки" на вкладке "Версии компонентов системы" отображаются версии и наименования серверных компонентов. Версии компонентов меняются после загрузки обновлений.

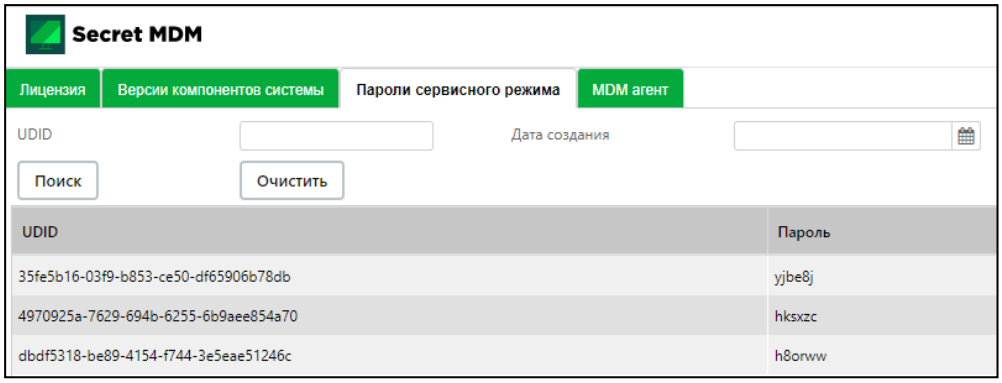


Пароли сервисного режима

Пароль сервисного режима генерируется автоматически при регистрации мобильного устройства. На вкладке создается запись, содержащая:

- информацию о UDID устройства;
- автоматически сгенерированный пароль.

Примечание. Если устройство (с одним и тем же UDID) регистрировалось несколько раз, пароль будет один и тот же. Если UDID устройства менялся, пароль будет соответствовать тому UDID, которым в настоящий момент обладает устройство.



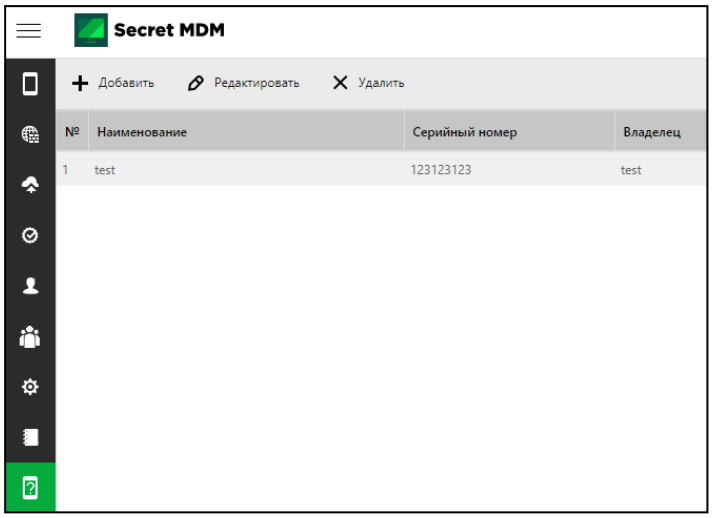
Пароль сервисного режима применяется пользователем для самостоятельного удаления приложения с устройства, если команда "Удалить устройство" не может быть исполнена. В таком случае администратор удаляет устройство из базы данных и любым доступным способом передает пароль, созданный для этого устройства, пользователю, после чего тот удаляет Secret MDM с устройства.

Для удаления записи с паролем:

- Нажмите кнопку ☒ в строке с удаляемой записью.

Управление неизвестными устройствами

Раздел "Неизвестные устройства" предназначен для регистрации устройств, не поддерживающих Secret MDM. К данному типу устройств относятся устройства с операционной системой, отличной от Android.



Примечание. Для получения актуальной информации обо всех зарегистрированных мобильных устройствах нажмите кнопку "Экспорт" в нижней части основного окна. Secret MDM сформирует csv-файл. Администратор может открыть файл для просмотра или сохранить его на компьютер.