

КОМПЛЕКСНАЯ ЦИФРОВАЯ МУЛЬТИПЛАТФОРМА УПРАВЛЕНИЯ МОБИЛЬ-
НЫМИ СРЕДСТВАМИ КОММУНИКАЦИЙ
РУКОВОДСТВО АДМИНИСТРАТОРА



Москва

2026

СОДЕРЖАНИЕ

Перечень используемых терминов и сокращений	9
1 Введение	13
2 Описание действий при работе с APM Администратора SafeMobile.....	14
2.1 Аутентификация в APM Администратора SafeMobile	14
2.2 Обзор интерфейса APM Администратора SafeMobile	16
2.3 Панель ОШС.....	24
2.4 Главная таблица	27
2.5 Информационная таблица	32
2.6 Главное меню.....	33
2.6.1 Отчёт «Информация об устройстве»	36
2.6.1.1 Вкладка «Общее»	37
2.6.1.2 Вкладка «Клиентские сертификаты».....	43
2.6.1.3 Вкладка «Профили»	45
2.6.1.4 Вкладка «ПУП».....	48
2.6.1.5 Вкладка «Конфигурация приложений»	50
2.6.1.6 Вкладка «История смены сотрудников»	52
2.6.2 Раздел «Сообщения»	53
2.6.3 Раздел «Звонки»	55
2.6.4 Раздел «Местоположения».....	58
2.6.5 Раздел «Действия»	61
2.6.6 Раздел «События».....	64
2.6.7 Раздел «Команды»	81

2.6.8	Именованные команды.....	91
2.6.9	Раздел «Профили»	94
2.6.9.1	Создание профиля.....	96
2.6.9.2	Настройка параметров профиля	104
2.6.9.3	Задание условий применения профиля.....	107
2.6.9.4	Назначение профиля.....	112
2.6.9.5	Смена владельца сущности.....	113
2.6.9.6	Делегирование сущности	114
2.6.9.7	Применение профиля	115
2.6.9.8	Удаление профиля	119
2.6.10	Раздел «Правила несоответствия»	120
2.6.10.1	Добавление нового правила несоответствия.....	121
2.6.10.2	Задание условий применения правил несоответствия	125
2.6.10.3	Редактирование существующего правила несоответствия	125
2.6.10.4	Удаление существующего правила несоответствия	125
2.6.11	Раздел «Правила автомаркировки»	126
2.6.11.1	Создание нового правила автомаркировки	129
2.6.11.2	Особенности удаления и редактирования правил автомаркировки.....	130
2.6.12	Раздел «Установленные приложения»	132
2.6.13	Раздел «Правила управления»	134
2.6.13.1	Создание нового Правила управления приложениями	138
2.6.13.2	Задание условий применения ПУП	144
2.6.13.3	Назначение ПУП	144
2.6.13.4	Смена владельца сущности.....	144

2.6.13.5 Делегирование сущности	145
2.6.13.6 Управление разрешениями приложений (Android)	145
2.6.13.7 Применение ПУП	148
2.6.13.8 Особенности при удалении ПУП	149
2.6.13.9 Особенности обновления приложений	150
2.6.14 Раздел «Конфигурации»	152
2.6.14.1 Добавление конфигурации.....	153
2.6.14.2 Назначение конфигурации	159
2.6.14.3 Смена владельца сущности.....	160
2.6.14.4 Делегирование сущности	160
2.7 Построение отчётов (пункт меню «Отчёты»).....	161
2.7.1 Отчёт «Аудит»	161
2.7.2 Отчёт «Звонки и SMS»	165
2.7.3 Отчёт «События ИБ»	166
2.7.4 Отчёт «Перемещения»	167
2.7.5 Отчёт «Профили»	168
2.7.6 Отчёт «Правила управления».....	170
2.7.7 Отчет «Правила управления (UID)»	172
2.7.8 Отчет «Геозоны».....	175
2.7.9 Аудит SMAPI.....	177
2.7.10 Активность сотрудников	178
2.8 Управление объектами учёта (пункт меню «Объекты учёта»).....	180
2.8.1 Организационно-штатная структура	181
2.8.2 Сотрудники	184

2.8.2.1	Пакетное изменение атрибутов	189
2.8.3	Роли	192
2.8.4	Администраторы	196
2.8.4.1	Редактирование данных администратора	198
2.8.4.2	Добавить нового администратора	199
2.8.5	Ограничения администраторов	201
2.8.6	Парольные политики APM.....	206
2.8.7	Операционные системы	208
2.8.8	Приложения.....	210
2.8.8.1	Добавление записи о приложении в систему	212
2.8.8.2	Редактирование записи о приложении	215
2.8.8.3	Удаление записи о приложении	216
2.8.8.4	Создание шаблона конфигурации из записи о приложении	216
2.8.9	Шаблоны конфигураций	218
2.8.10	SIM-карты	219
2.8.11	Комплекты	222
2.8.11.1	Загрузка комплектов	225
2.8.11.2	Выгрузка комплектов	231
2.8.11.3	Отключение комплекта.....	232
2.8.11.4	Привязка SIM к комплектам	234
2.8.11.5	Перерегистрация устройства на другого сотрудника	236
2.8.12	Комплекты Linux.....	239
2.8.12.1	Добавить новый комплект Linux	240
2.8.12.2	Удаление комплекта Linux	240

2.8.13	Геозоны.....	241
2.8.14	Серверные сертификаты.....	244
2.8.15	Подключения к серверам	247
2.8.16	Удостоверяющие центры	255
2.8.17	Настройки SCEP	258
2.8.17.1	Добавление новой настройки SCEP.....	262
2.8.17.2	Удаление настроек SCEP.....	262
2.8.18	Клиентские сертификаты	264
2.8.19	Группы.....	268
2.8.20	Шаблоны писем.....	272
2.8.20.1	Добавление нового шаблона письма	274
2.8.20.2	Редактирование и удаление шаблона письма	275
2.8.21	Именованные условия применения	276
2.8.21.1	Добавление нового условия применения	277
2.8.21.2	Удаление условия применения	277
2.8.22	Метки устройств	278
2.8.22.1	Создание и удаление метки.....	279
2.8.23	Сервисные учетные записи.....	281
2.8.24	Модели устройств	284
2.8.25	Файлы	286
2.9	Синхронизация данных LDAP	288
2.9.1	Внешние каталоги	288
2.9.1.1	Создание нового подключения к службе каталогов.....	292
2.9.1.2	Удаление существующего подключения	294

2.9.1.3	Принудительная синхронизация с внешним каталогом LDAP	295
2.9.2	Пользователи	296
2.9.2.1	Изменение параметров существующего правила.....	300
2.9.2.2	Создание нового правила импорта пользователей	300
2.9.2.3	Удаление правила импорта пользователей	301
2.9.2.4	Создание правила импорта пользователей с помощью файла списка групп пользователей	301
2.9.2.5	Настройка приоритетов правила импорта пользователей.....	302
2.9.3	Группы.....	304
2.9.3.1	Изменение параметров существующего правила импорта	306
2.9.3.2	Добавить новое правило импорта групп пользователей.....	307
2.9.3.3	Удалить существующее правило импорта групп из списка.....	307
2.9.3.4	Создание правила импорта групп из файла, содержащего список групп внешнего каталога	309
2.9.4	Администраторы	311
2.9.4.1	Изменение параметров существующего правила.....	314
2.9.4.2	Добавить новое правило импорта администраторов	314
2.9.4.3	Удалить существующее правило импорта администраторов	314
2.9.4.4	Создание правила импорта администраторов из файла, содержащего список групп администраторов внешнего каталога.	315
2.9.5	Журнал.....	317
2.10	Регистрация устройств	318
2.10.1	Управление кодами приглашения (пункт меню «Загрузчик»)	318
2.10.1.1	Создание кода приглашения.....	322
2.10.2	Шаблоны QR	325

2.11	Корпоративный календарь рабочего времени (пункт меню «Календарь»).....	327
2.11.1	Создание правил.....	331
2.11.2	Изменение правил	334
2.11.3	Удаление правила	334
2.12	Контроль за лицензией на «UEM SafeMobile» (пункт меню «Лицензия»)	335
2.12.1	Отчет по подключенным устройствам.....	337
2.13	Управление пользовательским соглашением	339
2.14	Информация	340
2.14.1	Компоненты	340
2.15	Настройки	343
2.15.1	Дополнительные атрибуты	343
2.15.2	Периодическая очистка	346
2.15.3	Распределение ресурсов	349
2.15.4	Конфигурация компонентов	351
2.16	Завершение работы в «UEM SafeMobile».....	355
3	Частые вопросы	356
	Приложение А Установка MCK на платформе iOS в режим Supervised	359
	Приложение Б Перечень возможных ошибок при выполнении команд Администраторов.....	365
	Приложение В Приложения для мобильных устройств iOS.....	367
	Приложение Г Состав полномочий предустановленных ролей.....	371
	Приложение Д Подготовка устройства Windows для установки MCK	372
	Приложение Е Поддерживаемые платформы мобильных устройств	373
	Приложение Ж Взаимосвязи некоторых функций системы и стратегий подключения.....	377

Перечень используемых терминов и сокращений

Таблица 1 — Перечень терминов и сокращений

Сокращение	Полное наименование
ADEP	Программа управления корпоративная приложениями на устройствах Apple (Apple Developer Enterprise Program)
APN	Имя точки доступа (Access Point Name)
Auth-server	Сервер аутентификации SafeMobile. Отвечает за проверку сертификатов мобильных устройств, при доступе к серверу управления Android (socket-server).
CA	Удостоверяющий центр SafeMobile. Отвечает за выпуск сертификатов для мобильных устройств, используемых для авторизации в SafeMobile.
CHAP	Протокол аутентификации с косвенным согласованием (Challenge Handshake Authentication Protocol)
DN	Уникальное имя записи в внешнем каталоге LDAP (Distinguished Name)
DN базового подразделения	DN раздела каталога. Используется при импорте данных из внешнего каталога LDAP, в качестве «корня дерева» поиска объектов для импорта.
GPRS	Пакетная радиосвязь общего пользования (General Packet Radio Service) — служба передачи данных в мобильных сетях
GPS	Глобальная система спутникового позиционирования (Global Positioning System)
HTTP	Протокол передачи гипертекста (HyperText Transfer Protocol)
ICCID	Уникальный идентификатор SIM-карты (Integrated Circuit Card Identifier)
IMEI	Международный идентификатор мобильного оборудования (International Mobile Equipment Identity)
IMSI	Международный идентификатор мобильного абонента (International Mobile Subscriber Identity)
IP-адрес	Идентификатор (адрес) устройства, подключенного к сети (Internet Protocol Address)
KME	Облачный инструмент автоматической регистрации корпоративных мобильных устройств производства Samsung (Knox Mobile Enrollment)
Кнох	Технология управления смартфонами и планшетами от производителя Samsung
MCC	Мобильный код страны (Mobile Country Code)
MMS	Служба мультимедийных сообщений (Multimedia Messaging Service)
MNC	Код мобильной сети (Mobile Network Code)

Сокращение	Полное наименование
MTP	Протокол передачи мультимедиа (Media Transfer Protocol)
mTLS	Протокол взаимной аутентификации клиента и сервера (mutual TLS)
PAP	Протокол аутентификации, предусматривающий отправку имени пользователя и пароля на сервер удалённого доступа открытым текстом (Password Authentication Protocol)
PKI	Инфраструктура открытых ключей (Public Key Infrastructure)
PTP	Протокол передачи изображений (Picture Transfer Protocol)
SCEP	Протокол инфраструктуры PKI, который используется для упрощенного способа получения сертификатов (Simple Certificate Enrollment Protocol)
SDK	Комплект средств разработки для создания приложений для определенного ПО (Software Development Kit)
SIM	Модуль идентификации абонента (Subscriber Identification Module)
SIP-аккаунт	Учетная запись пользователя в системе интернет-телефонии
SMS	Служба коротких сообщений (Short Message Service)
SSID	Идентификатор сети (Service Set Identifier)
Supervised	Режим осуществления контроля над МСК на платформе iOS. Для перевода в режим контроля требуется перепрошивка МСК при помощи ПО Apple Configurator 2 на ПК с ОС MacOS с потерей данных пользователя (описание установки iOS-устройства в Supervised-режим приведено в приложении А)
TLS	Криптографический протокол, обеспечивающие защищённую передачу данных между узлами в сети Интернет (Transport Layer Security)
ToTp	Алгоритм создания одноразовых паролей для защищённой аутентификации (Time-based One-time Password Algorithm)
UDID	Уникальный идентификатор устройства (Unique Device Identifier)
UID	Идентификатор приложения (Unique Identifier)
UEM	Унифицированное управление конечными устройствами (Unified Endpoint Management)
USB	Последовательный интерфейс для подключения периферийных устройств (Universal Serial Bus)
USSD	Сервис в сотовых сетях, организующий интерактивное взаимодействие между абонентом сети и сервисным приложением (Unstructured Supplementary Service Data)
VPN	Виртуальная частная сеть — технология организации защищенных линий связи между абонентами по незащищенным каналам передачи данных (Virtual Private Network)

Сокращение	Полное наименование
WAP	Беспроводной протокол передачи данных (Wireless Application Protocol)
APM	Автоматизированное рабочее место
ЗУ	Зарядное устройство
ИБ	Информационная безопасность
Контейнер	Изолированная область на МСК, предназначенная для корпоративных приложений и данных. Для МСК на платформе Android производителя Samsung поддерживаются два типа контейнеров: Samsung KNOX и Work Profile.
КП	Конфигурация приложения
КРП	Корпоративный рабочий профиль
ЛРП	Личный рабочий профиль
Метаинформация	Дополнительная информация, раскрывающая сведения о признаках и свойствах, характеризующих какие-либо сущности, позволяющие автоматически искать и управлять ими в больших информационных потоках
Метка устройства	Маркер устройства, заданный пользователем. Объект учета.
МСК	Мобильное средство коммуникации (мобильный телефон, смартфон, планшетный компьютер)
ОС	Операционная система
ОШС	Организационно-штатная структура предприятия
ПК	Персональный компьютер
ПО	Программное обеспечение
Профиль	Совокупность значений и настроек ОС
ПУН	Приложение с управляемыми настройками
ПУП	Правило управления приложением
Режим киоска	Режим работы МСК, при котором разрешен запуск одного или нескольких определенных приложений.
Результирующий профиль	Профиль, который будет применен к устройству после учета всех политик и условий, профилей одного типа, назначенных на это же устройство.
Стратегия	Способ управления устройством Android. Стратегия задается администратором и определяет: чем и в каком объеме администратор сможет управлять на устройстве. Применяется при подключении устройства. Если монитор при подключении МСК не получит необходимых для исполнения заданной стратегии привилегий, то МСК не будет подключено

Сокращение	Полное наименование
Сущность	Именованный набор данных, который можно атомарно (целиком) назначить или снять с узла ОШС, сотрудника или МСК. К сущностям относятся профиль, ПУП и КП
УПАТС	Учрежденческо-производственная автоматическая телефонная станция
УЦ	Центр сертификации или удостоверяющий центр (англ. Certification authority, CA)
ФИО	Фамилия, имя и отчество

1 Введение

Настоящее руководство предназначено для Администраторов «UEM SafeMobile» (далее по тексту — система или SafeMobile) и содержит описание веб-интерфейса APM Администратора, а также действий по управлению комплексной цифровой мультиплатформой управления мобильными средствами коммуникаций посредством интерфейса, а именно в:

- регистрации МСК;
- настройке по применению политик безопасности на МСК, в том числе политик при смене SIM-карты устройства;
- удаленной настройке и управлении приложениями на МСК, в том числе в контейнере;
- удаленной блокировке и разблокировке мобильного устройства;
- удалённом отключении МСК от управления системой;
- управлении списком доверенных беспроводных точек доступа;
- осуществлении настройки доступа на МСК к электронной почте;
- управлении настройками ОС МСК, в зависимости от принадлежности устройства и его местонахождения;
- просмотре отчётов;
- выгрузке информации о МСК, включая реестр установленных на него корпоративных приложениях.

2 Описание действий при работе с APM Администратора SafeMobile

2.1 Аутентификация в APM Администратора SafeMobile

Для входа в APM Администратора SafeMobile необходимо открыть браузер (Mozilla Firefox или Google Chrome актуальной версии) и в адресной строке набрать адрес (например, <https://ip-address:8443>), по которому был размещен APM Администратора, после чего отобразится окно аутентификации в соответствии с рисунком 2.1.

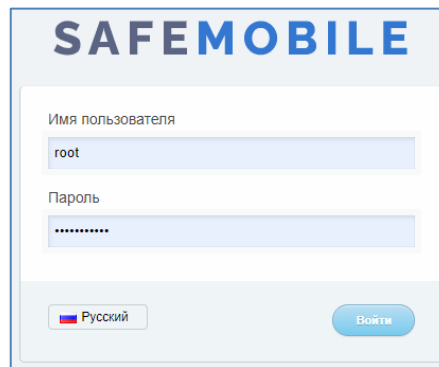




Рисунок 2.1 — Окно аутентификации

При первом входе необходимо ввести имя пользователя (*root*) и временный пароль (*change_on_install*) в соответствующие поля и нажать кнопку **«Войти»**. Временный пароль действует только при первом входе в систему. Сразу же после его успешного ввода потребуется сменить пароль на новый, в соответствии с параметрами парольной политики APMa, заданными в 2.8.5.

Примечание

*Если учетная запись администратора была импортирована из LDAP посредством «правил импорта администраторов», то для авторизации администратора необходимо вводить имя пользователя в формате UPN (*username@domain*) домена, из которого был произведен импорт учетной записи.*

В окне аутентификации доступно изменения языка интерфейса. При нажатии на кнопку  **Русский** интерфейс переключится на английский язык, при нажатии на кнопку  **English** интерфейс снова отобразится на русском языке.

После первого успешного входа в системе доступен только Суперадминистратор «**root**» с доступом к разделу «**Лицензия**». После ввода лицензии «**root**» **получает** неограниченные полномочия и доступ ко всем функциональным возможностям системы. Добавление новых пользователей системы, в том числе Администраторов ИТ и ИБ, осуществляется согласно разделу 2.8.4.

Отображение интерфейса в данном руководстве приведено для Суперадминистратора «**root**», для пользователей с ограниченными правами отображение интерфейса может отличаться.

В системе предусмотрен принудительный выход Администратора из системы, после которого потребуются повторный вход в систему. Принудительный выход Администратора из системы происходит в следующих случаях:

- если Администратор был заблокирован;
- если у Администратора изменился состав ролей;
- если у ролей Администратора изменился состав полномочий;
- если время сессии Администратора истекло (по умолчанию время сессии равно 30 минутам, время сессии является параметром настройки сервера веб-приложений SafeMobile).

В системе доступен контроль клиентских сессий, при котором возможен повторных вход с учетной записи уже подключенного Администратора (по умолчанию количество сессий одного пользователя равно двум, параметры контроля сессий устанавливаются при настройке сервера веб-приложений SafeMobile).

Набор доступных функций системы, а также соответствующий вид интерфейса АРМ, зависит от полномочий Администратора, от имени которого выполнен вход в систему.

2.2 Обзор интерфейса APM Администратора SafeMobile

Главное окно APM Администратора SafeMobile, открывающееся после аутентификации, состоит из следующих компонентов:

- главное меню навигации по разделам APM. Находится в левой части окна. Для того, чтобы скрыть главное меню следует нажать соответствующую кнопку (рисунок 2.2).

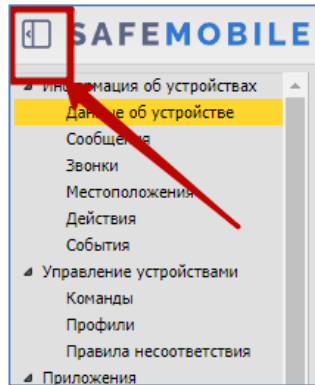


Рисунок 2.2 — Расположение кнопки «скрыть главное меню»

- панель организационно-штатной структуры (ОШС) организации в виде иерархического списка подразделений;
- главная таблица, содержащая список МСК сотрудников организации или подразделения, выбранного в панели ОШС;
- информационная таблица, которая находится в нижней части окна и отображает данные по МСК, выбранному в главной таблице;
- кнопка «Обновить» (рисунок 2.3), расположенная в правом верхнем углу окна, предназначена для обновления всей информации в главном окне, кнопки «Обновить» для главной и информационной таблиц расположены на панели внизу каждой из таблиц.

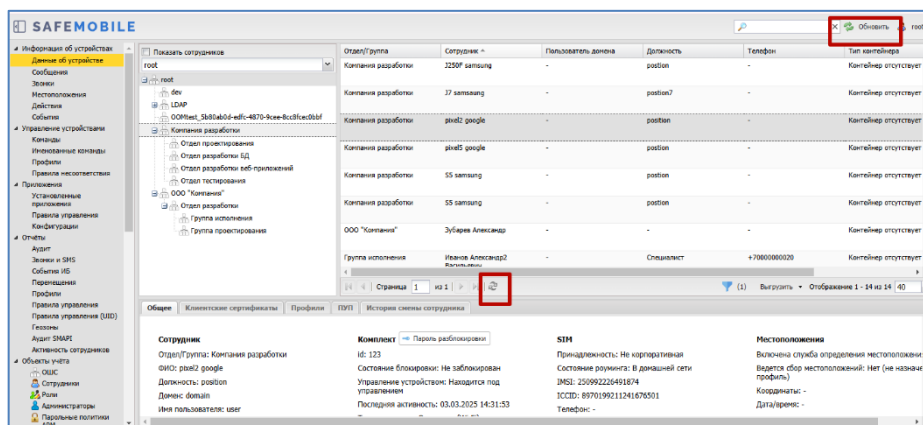


Рисунок 2.3 — Главное окно APM Администратора SafeMobile

В правом верхнем углу окна расположена также кнопка, отображающая имя пользователя (логин), под учётной записью которого выполнен вход в систему. Кроме того, нажатие на эту кнопку позволяет выбрать команду в раскрывающемся меню, а именно: **«Изменить пароль»**, введенный при аутентификации; выполнить **«Выход»** из APM Администратора SafeMobile; переключить интерфейс на английский язык, нажав на кнопку **Русский** (рисунок 2.4), после перехода на английский язык кнопка изменится на **English**.

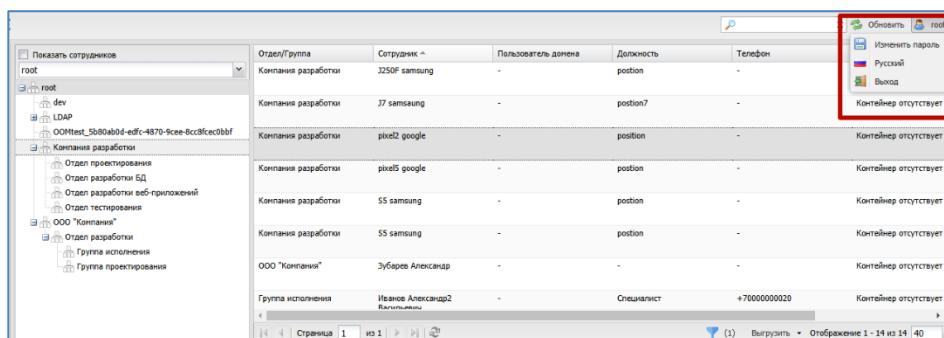


Рисунок 2.4 — Меню, отображающее имя пользователя (логин)

Для осуществления поиска в таблицах предназначена строка ввода поискового запроса и расположена в верхней части таблицы, в которой осуществляется поиск (рисунок 2.5). Поиск производится по различным колонкам, в зависимости от таблицы.

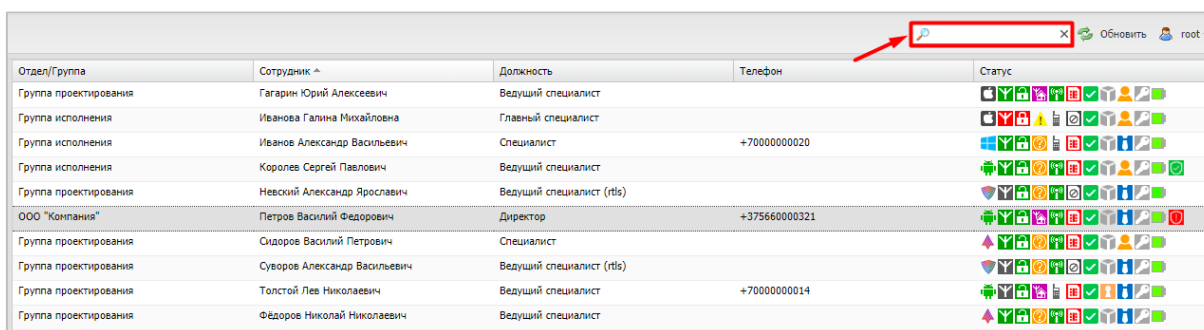


Рисунок 2.5 — Строка поиска в главной таблице

В APM Администратора SafeMobile существует возможность формирования отчета «Инвентаризация МСК» с учетом заданных параметров фильтрации для устройств подразделения, выбранного на панели ОШС. Для этого необходимо нажать кнопку **Выгрузить** на нижней панели главной таблицы, после чего в выпадающем меню выбрать параметр: «Без приложений/С приложениями» (рисунок 2.6). В отчет «Инвентаризация МСК» войдет имеющаяся в системе информация по МСК независимо от количества полей, отображаемых в главной таблице. Если задан параметр «С приложениями»,

то отчет сформируется с дополнительной информацией о приложениях (зарегистрированных в системе), установленных на МСК.

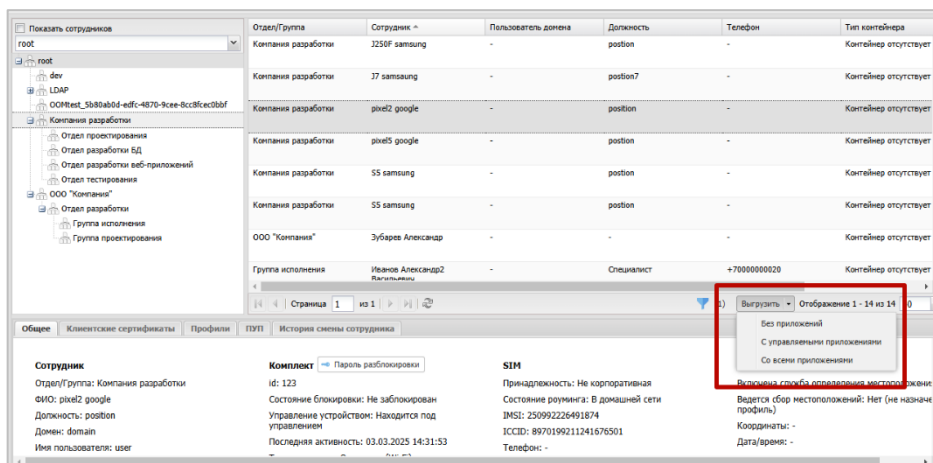


Рисунок 2.6 — Меню «Выгрузить» в главной таблице

При нажатии на кнопку **«Выгрузить»** на панели других таблиц (информационной таблицы и т.п.) отчет формируется с данными, отображаемыми в этих таблицах. Отчеты выгружаются в отдельном окне. Если отчет содержит менее 10000 записей, то выгрузка производится в формате XLSX. Если отчет содержит более 10000 записей, то выгрузка производится в формате CSV.

В таблицах APM Администратора SafeMobile имеются следующие возможности по управлению записями:

- изменение порядка столбцов путем перемещения заголовка столбца в нужное место с помощью мыши;
- сортировка записей таблиц по выбранному столбцу;
- изменение состава отображаемых столбцов в таблицах с помощью раскрывающегося меню в заголовках столбцов.

Записи в таблицах отображаются в постраничном режиме, количество отображаемых записей для удобства пользователя можно изменять (рисунок 2.7) в зависимости от объема информации.

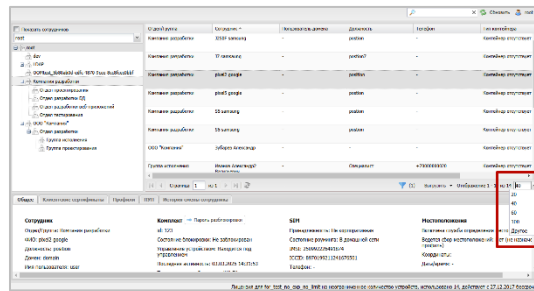


Рисунок 2.7 — Количество отображаемых записей в главной таблице

Для сортировки записей в таблице в порядке убывания или возрастания значений необходимо открыть раскрывающееся меню, нажав стрелку справа от заголовка выбранного столбца (рисунок 2.8) и выбрать требуемый порядок сортировки: «По возрастанию» или «По убыванию».

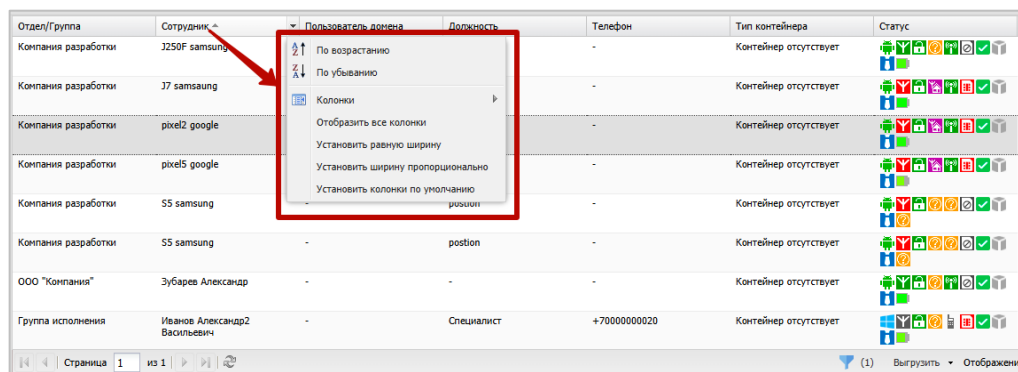


Рисунок 2.8 — Сортировка записей в столбце главной таблицы

Изменить состав отображаемых столбцов в таблицах можно с помощью раскрывающегося меню в заголовках столбцов (рисунок 2.9).

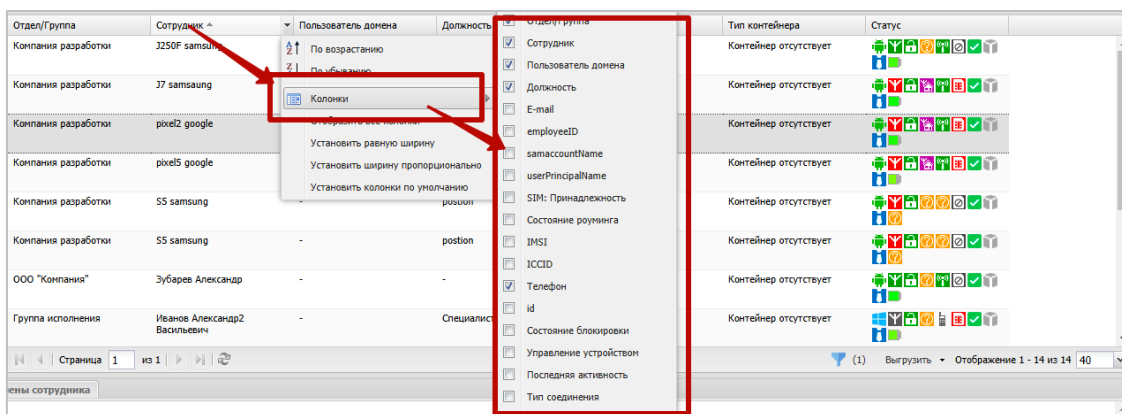


Рисунок 2.9 — Управление столбцами в главной таблице

Для включения столбцов в состав, отображаемых в таблице или исключения их необходимо открыть раскрывающееся меню, нажав стрелку справа от заголовка выбранного столбца, выбрать пункт меню **«Колонки»**, а затем отметить флажками те столбцы, которые требуется отобразить, или снять флажки с тех столбцов, которые требуется скрыть.

Система запоминает для каждого пользователя состав колонок, порядок расположения колонок, ширину колонок в следующих разделах системы:

- Информация об устройстве,
- Управлении устройствами:
 - Профили,
 - Правила несоответствия,
- Приложения,
- Отчеты:
 - Профили,
 - Правила управления,
- Объекты учета:
 - Комплекты,
 - Сотрудники,
 - Администраторы,
 - Клиентские сертификаты.

Для быстрого приведения этих параметров в исходное состояние следует нажать кнопку **«Установить колонки по умолчанию»** (рисунок 2.10). При её нажатии восстанавливаются первоначальные:

- состав колонок,
- порядок расположения колонок,
- ширина колонок.

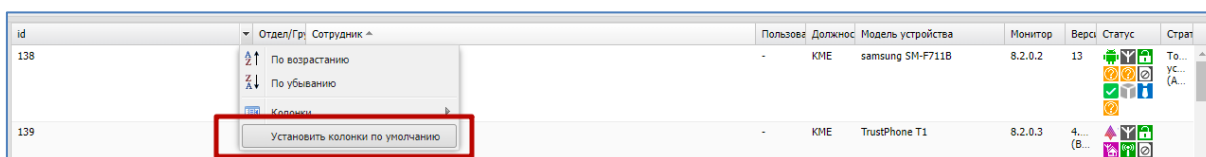


Рисунок 2.10 — Расположение кнопки «Установить кнопки по умолчанию»

Аналогичным образом осуществляется управление записями в информационной таблице. По умолчанию записи в главной таблице сортируются по возрастанию ФИО сотрудника.

Для задания в главной таблице фильтрации записей следует нажать кнопку фильтра (рисунок 2.11).



Рисунок 2.11 — Фильтрация записей в главной таблице

В окне фильтров отображаются три вкладки:

- Статусы,
- Платформа,
- Приложения,
- Метки,
- Регистрация,
- Последняя активность.

Во вкладке **«Статусы»** можно задать фильтрацию записей в главной таблице по статусу комплектов (рисунок 2.12).

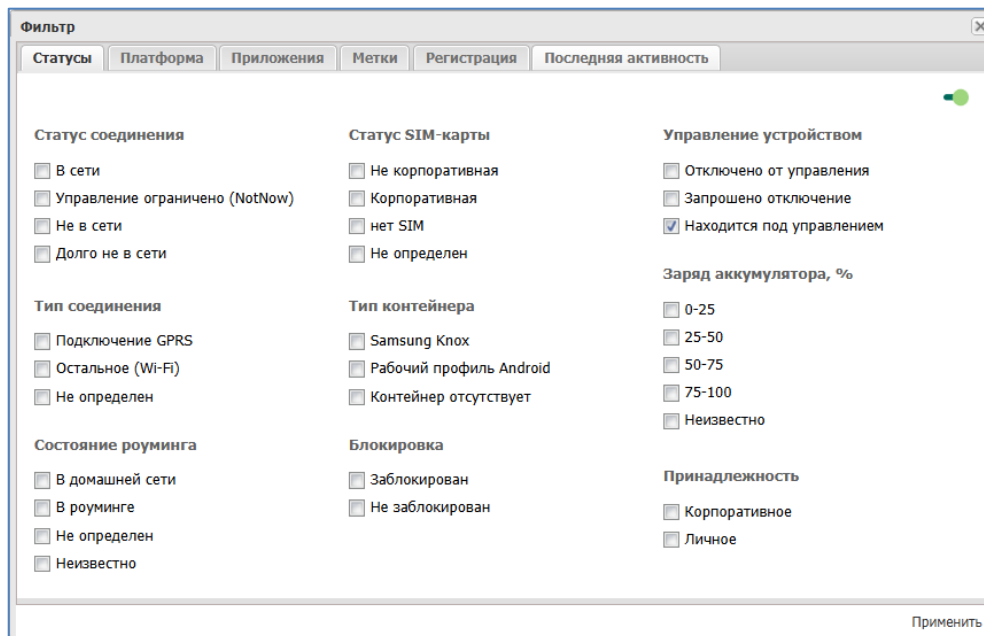


Рисунок 2.12 — Вкладка «Статусы»

По умолчанию установлен фильтр по статусу «Управление устройством», а именно: «Находится под управлением».

Во вкладке «Платформа» (рисунок 2.13) можно задать фильтрацию записей в зависимости платформы МСК. По умолчанию фильтр «Платформа» выключен.

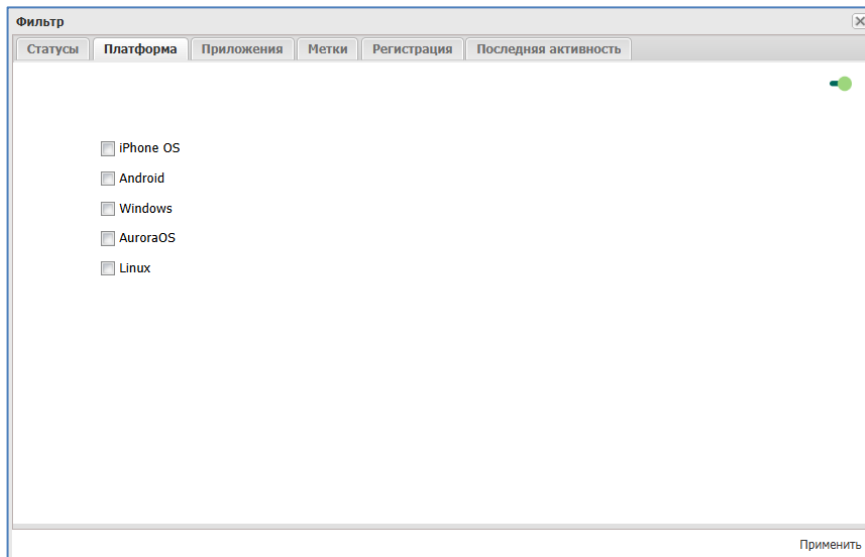


Рисунок 2.13 — Вкладка «Платформа»

Во вкладке «Приложения» можно задать фильтрацию записей в зависимости от установленных/неустановленных приложений на МСК (рисунок 2.14). По умолчанию фильтр «Приложения» выключен.

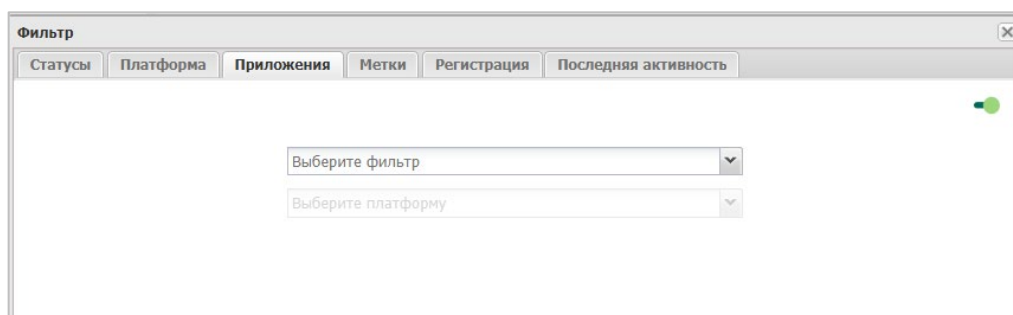


Рисунок 2.14 — Вкладка «Приложения»

Во вкладке «Метки» можно задать фильтрацию записей по наличию меток указанных в фильтре (рисунок 2.15). В окне фильтра отображается список заданных в системе меток. Для фильтрации записей по меткам следует отметить чекбоксы необходимых меток и нажать кнопку «Применить». Переключатель «Оставить только выбранные метки» позволяет отображать в списке только те метки, которые отметил пользователь. Через поисковую строку можно найти нужные метки.

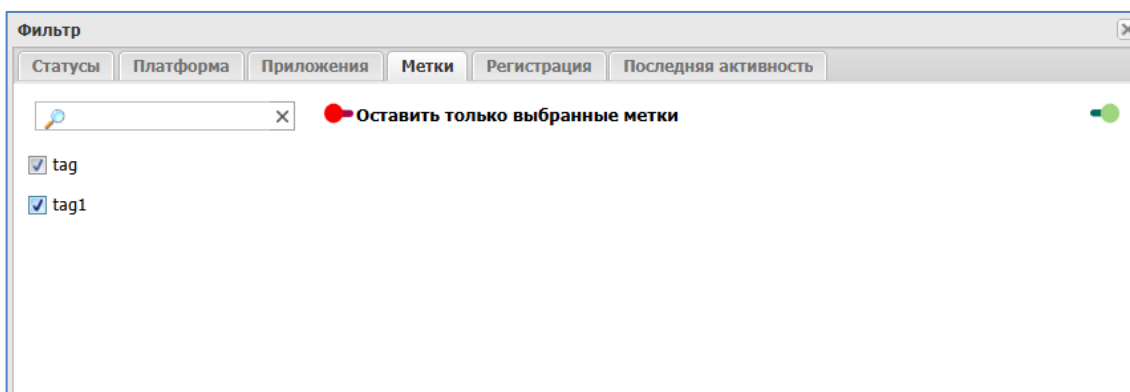




Рисунок 2.15 — Вкладка «Метки»

Для задания фильтрации следует выбрать требуемые параметры и нажать **«Применить»**. Рядом с кнопкой фильтра в панели инструментов отобразится количество установленных фильтров. Для отмены фильтров требуется переключатель  перевести в состояние «выключено» .

Во вкладке «Регистрация» можно задать диапазон даты и времени последней регистрации устройства (рисунок 2.16).

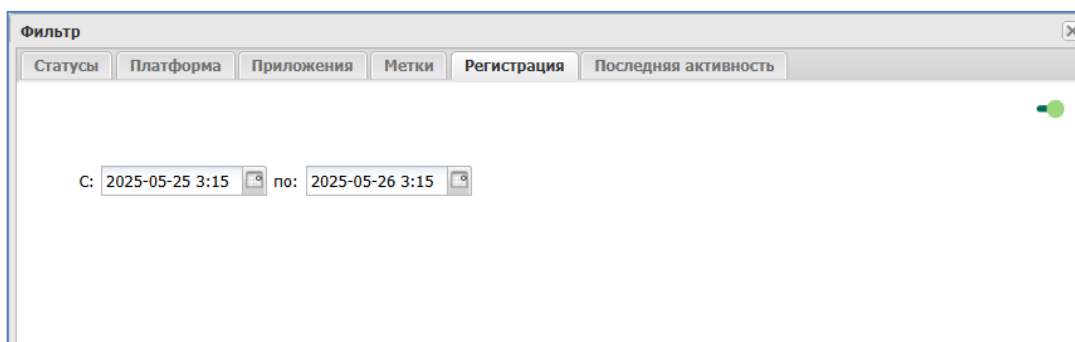


Рисунок 2.16 — Вкладка «Регистрация»

Во вкладке «Последняя активность» можно задать диапазон даты и времени последней активности устройства (рисунок 2.17).

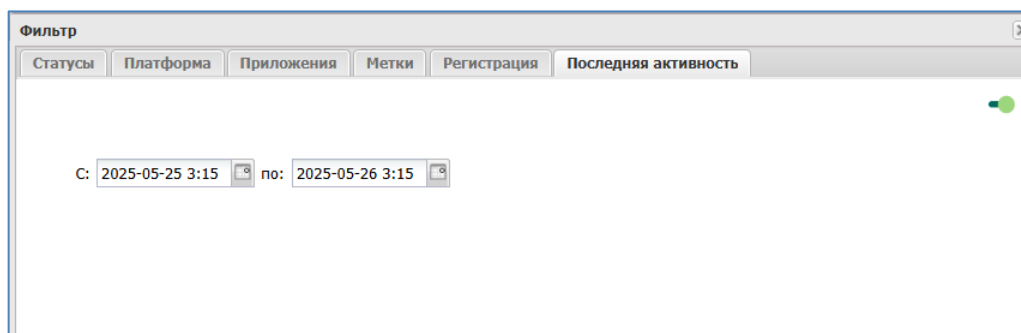


Рисунок 2.17 — Вкладка «Последняя активность»

2.3 Панель ОШС

В главном окне системы расположена панель, содержащая организационно-штатную структуру организации (ОШС) (рисунок 2.18).

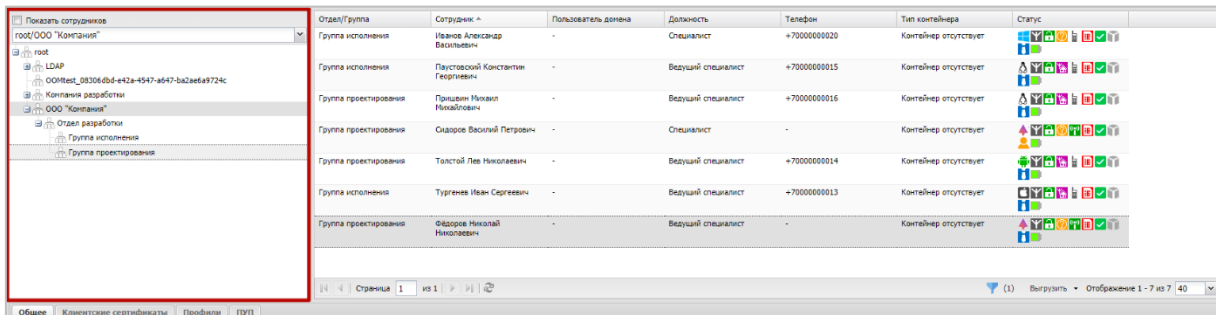


Рисунок 2.18 — Панель ОШС

Иерархический список подразделений позволяет выбрать подразделение, после чего в главной таблице справа отобразится список МСК, имеющихся у сотрудников этого подразделения. Кроме того, можно отобразить всех сотрудников и МСК организации, выбрав название всей организации в верхней строке ОШС (рисунок 2.19). Включение чек-бокса «Показать сотрудников» позволяет отобразить список сотрудников в дереве ОШС.

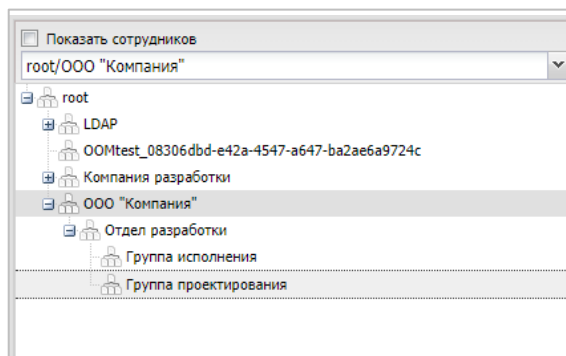


Рисунок 2.19 — Выбор корневого узла предприятия в панели ОШС

Строка пути ОШС отображает полный путь от корня, до выделенного пользователем объекта (рисунок 2.20)

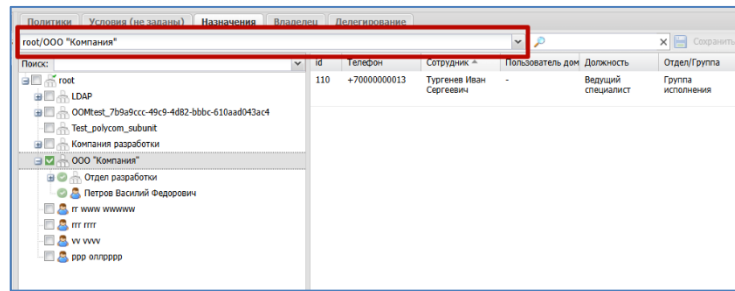


Рисунок 2.20 — Строка пути ОШС

Во вкладках «Назначение» присутствует строка поиска по дереву ОШС (рисунок 2.21).

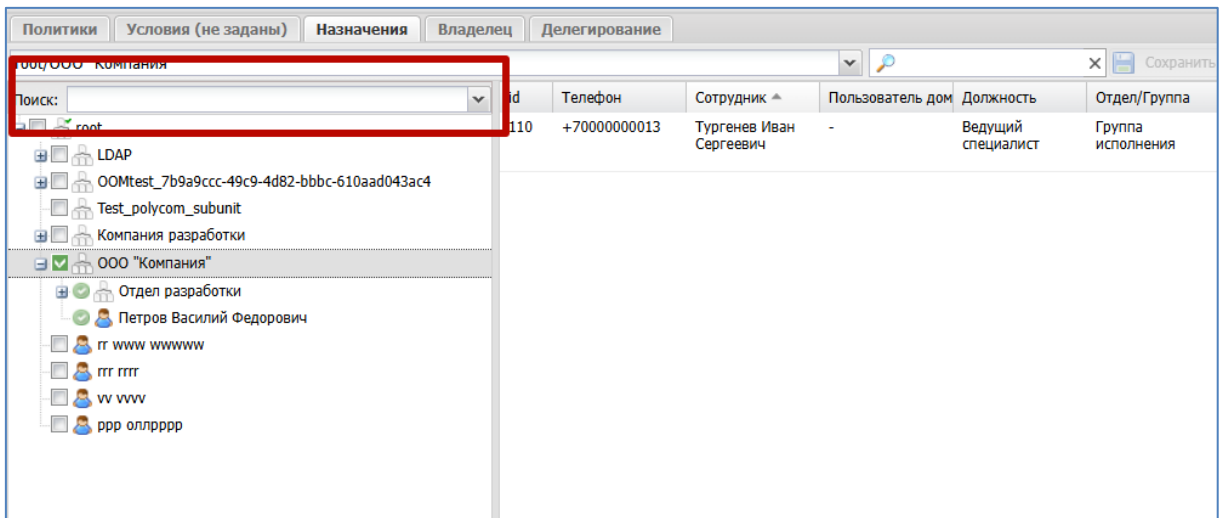


Рисунок 2.21 — Строка поиска по ОШС

При вводе данных в поисковую строку будет отображен выпадающий список с результатами совпадений поискового запроса с сотрудниками из ОШС (рисунок 2.22). При наведении на пиктограмму «?» отобразится путь к сотруднику в структуре ОШС. При выборе одного из результатов поиска система выделит его в дереве ОШС.

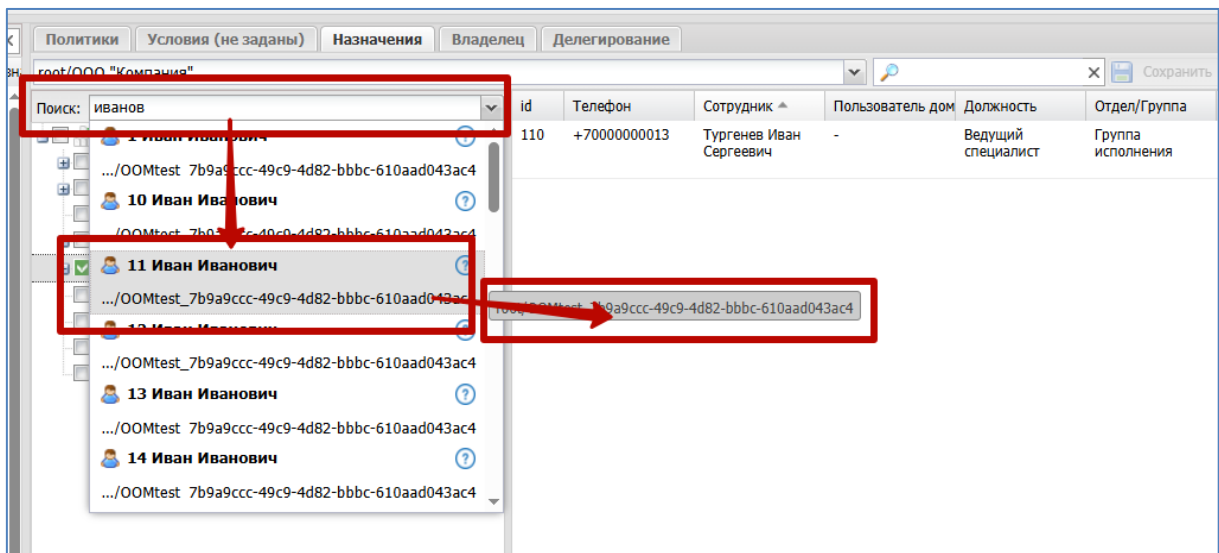


Рисунок 2.22 — Результат поискового запроса по ОШС

2.4 Главная таблица

В главной таблице (рисунок 2.23) отображается список и параметры комплектов, зарегистрированных в системе (хоть раз подключававшихся к серверу). Количество отображаемых комплектов зависит от выбранного в ОШС элемента — если выбран корневой элемент, в главной таблице отображается перечень всех комплектов предприятия; если выбран другой элемент ОШС (подразделение предприятия), в таблице будут показаны комплекты сотрудников и МСК этого подразделения.

При выборе комплекта в главной таблице подразделение, которому он принадлежит, выделяется в разделе ОШС жирным шрифтом, что упрощает поиск подразделения, в котором работает сотрудник с выбранным комплектом.

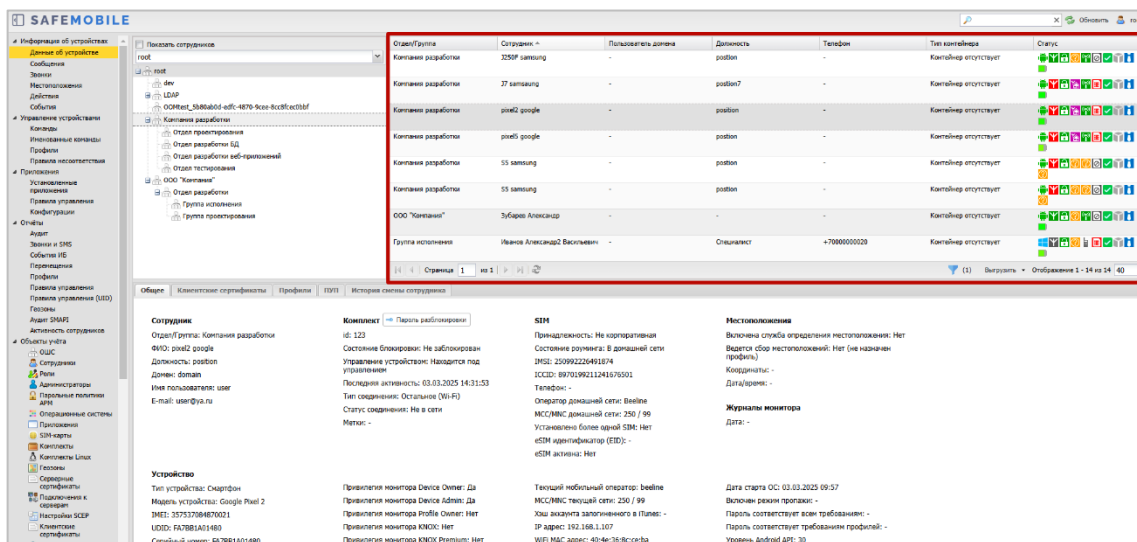


Рисунок 2.23 — Главная таблица

Главная таблица содержит следующие столбцы:

- Отдел/Группа — название подразделения, в котором работает сотрудник (по умолчанию, отображается в таблице);
- Сотрудник — ФИО сотрудника (по умолчанию, отображается в таблице);
- Пользователь домена — ФИО сотрудника или e-mail, если ФИО не было импортировано (по умолчанию, отображается в таблице);
- Должность — должность сотрудника (по умолчанию, отображается в таблице);
- E-mail — E-mail;
- employeeID — Импортированный из LDAP атрибут employeeID;
- samaccountName — Импортированный из LDAP атрибут samaccountName;










- userPrincipalName — Импортированный из LDAP атрибут userPrincipalName;
- SIM: Принадлежность — признак принадлежности SIM-карты организации, в которой работает сотрудник (корпоративная / не корпоративная/ нет SIM);
- Состояние роуминга — статус сети, к которой подключено МСК (в домашней сети / в роуминге / не определен / значение неизвестно);
- IMSI — международный идентификатор мобильного абонента (индивидуальный номер абонента);
- ICCID — уникальный серийный номер SIM-карты;
- Телефон — номер телефона комплекта (по умолчанию, отображается в таблице);
- id — уникальный идентификационный номер МСК в системе;
- Состояние блокировки — состояние телефона сотрудника для защиты данных (заблокирован / не заблокирован);
- Управление устройством — состояние подключения устройства к управлению «UEM SafeMobile» (отключено от управления / запрошено отключение / находится под управлением);
- Последняя активность — дата и время регистрации последнего нахождения МСК в системе;
- Тип соединения — тип подключения для передачи данных между МСК и системой (подключение GPRS / остальное (Wi-Fi) / не определен);
- Статус соединения — состояние соединения МСК с системой (в сети / не в сети / долго не в сети);
- IP адрес — только для МСК на платформе Android;
- Тип устройства — тип МСК, подключенного к системе (смартфон / планшет / иное);
- Модель устройства — модель МСК, подключенного к системе;
- Серийный номер — серийные номера МСК на платформе iOS и Android;
- Тип контейнера — тип созданного контейнера на устройстве (Samsung Knox / контейнер отсутствует);
- Заряд аккумулятора — уровень заряда батареи, %;
- Устройство: Принадлежность — признак собственности МСК (корпоративное / личное);
- Монитор — версия монитора, установленного на МСК;
- Платформа — мобильная платформа МСК;
- Версия — версия ОС МСК;
















- Статус — отображает значки состояния МСК сотрудника в системе, описание которых содержится в таблице 2.1 (по умолчанию, отображается в таблице);
- Стратегия — примененная на МСК стратегия управления;
- Метки — список меток на устройстве;
- Привязанные SIM (IMSI) — список привязанных SIM-карт к устройству.

ВАЖНО!

Таблицы, отображающие данные о сотрудниках и администраторах могут содержать поля, дополнительно заданные пользователем в разделе «Дополнительные атрибуты». Подробнее см. [2.15.1 — Дополнительные атрибуты](#).

Таблица 2.1 — Состояния мобильного средства коммуникации

Значок	Значение
Платформа	
	Android
	iOS
	Windows
	Аврора
Статус соединения	
	В сети
	Не в сети
	Долго не в сети
	Управление ограничено (NotNow) (см.примечание)
Блокировка	
	Заблокирован

Значок	Значение
	Не заблокирован
Состояние роуминга	
	В домашней сети
	В роуминге
	Неизвестно
	Не определен
Тип соединения	
	Подключение GPRS
	Остальное (Wi-Fi)
	Не определен
Статус SIM-карты в МСК	
	Корпоративная
	Не корпоративная
	SIM не определен
	Нет SIM
Тип контейнера	
	Samsung Knox
	Контейнер отсутствует
	Android for Work
Состояние батареи	

Значок	Значение
	Уровень заряда батареи
Управление устройством	
	Отключено от управления
	Запрошено отключение
	Находится под управлением
Принадлежность устройства	
	Корпоративное
	Личное
<p>Примечание</p> <p> Статус подключения NotNow — этот статус может быть только у устройстве iOS. Устройство в этом статусе соединения может принимать только команды блокировки и отключения от управления со сбросом к заводским настройкам. Команда синхронизации только обновит статус подключения устройства. Никакие профили, правила управления и конфигурации приложений не применяются. Данный статус может отображаться сразу после перезагрузки устройства, при низком заряде батареи и т.п.</p>	

2.5 Информационная таблица

В информационной таблице, расположенной в нижней части главного окна APM Администратора (рисунок 2.24) отображаются сведения по МСК, выбранному в главной таблице.

В информационной таблице воспроизводятся данные в зависимости от выбранных разделов главного меню. Детальное описание данных таблицы описано в разделе 2.6.1.

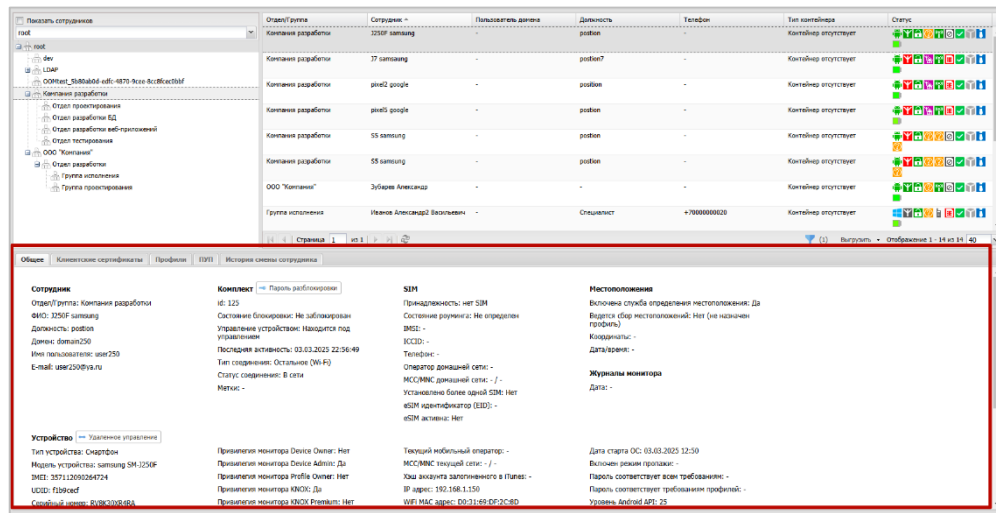


Рисунок 2.24 — Информационная таблица

2.6 Главное меню

В левой части главного окна APM Администратора SafeMobile (рисунок 2.25) расположена панель главного меню, содержащая следующие разделы:

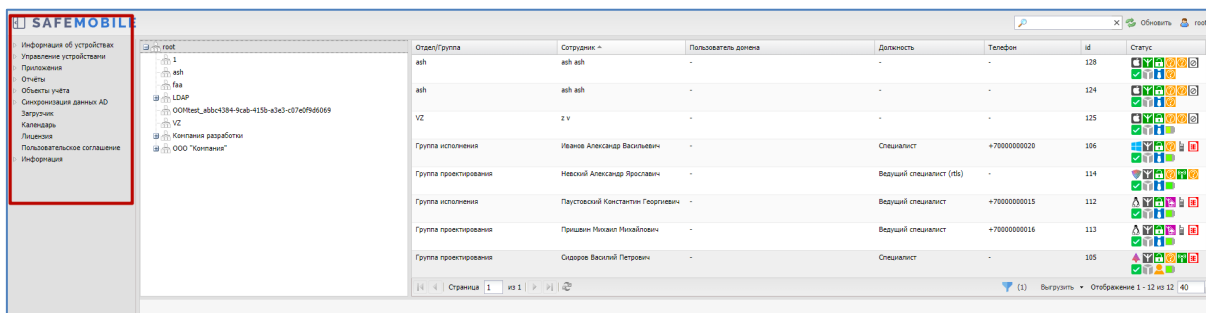


Рисунок 2.25 — Главное меню

- Информация об устройствах:
 - Данные об устройстве,
 - Сообщения,
 - Звонки,
 - Местоположения,
 - Действия,
 - События,
- Управление устройствами:
 - Команды,
 - Именованные команды,
 - Профили,
 - Правила несоответствия,
 - Правила автоматкировки,
- Приложения:
 - Установленные приложения,
 - Правила управления,
 - Конфигурации,
- Отчёты:
 - Аудит,
 - Звонки и SMS,
 - События ИБ,
 - Перемещения,

- Профили,
- Правила управления,
- Правила управления (UID),
- Геозоны,
- Аудит SMAPI,
- Активность сотрудников,
- Объекты учёта:
 - ОШС,
 - Сотрудники,
 - Роли,
 - Администраторы,
 - Ограничения администраторов,
 - Парольные политики APM,
 - Операционные системы,
 - Приложения,
 - Шаблоны конфигураций,
 - SIM-карты,
 - Комплекты,
 - Комплекты Linux,
 - Геозоны,
 - Серверные сертификаты,
 - Подключения к серверам,
 - Удостоверяющие центры,
 - Настройки SCEP,
 - Клиентские сертификаты,
 - Группы,
 - Шаблоны писем,
 - Условия применения,
 - Метки устройств,
 - Сервисные учетные записи,
 - Модели устройств,
 - Рассылаемые файлы,
- Синхронизация данных LDAP:
 - Внешние каталоги,
 - Пользователи,
 - Группы,
 - Администраторы,

- Журнал,
- Регистрация устройств:
 - Коды приглашения,
 - Шаблоны QR,
- Календарь,
- Лицензия,
- Пользовательское соглашение,
- Информация:
 - Компоненты,
- Настройки:
 - Дополнительные атрибуты,
 - Периодическая очистка,
 - Распределение ресурсов.

2.6.1 Отчёт «Информация об устройстве»

Для просмотра информации о параметрах комплекта следует нажать пункт **«Данные об устройстве»** главного меню и выбрать требуемый комплект в главной таблице (рисунок 2.26).

Группа исполнения	Сотрудник	Пользователь дочерня	Должность	Телефон	Тип контейнера	Статус
Группа исполнения	Иванов Александр Васильевич	-	Специалист	+70000000020	Контейнер отсутствует	[Иконки]
Группа исполнения	Паустовский Константин Георгиевич	-	Ведущий специалист	+70000000015	Контейнер отсутствует	[Иконки]
Группа проектирования	Прищипин Николай Михайлович	-	Ведущий специалист	+70000000016	Контейнер отсутствует	[Иконки]
Группа проектирования	Сидоров Василий Петрович	-	Специалист	-	Контейнер отсутствует	[Иконки]
Группа проектирования	Толстой Лев Николаевич	-	Ведущий специалист	+70000000014	Контейнер отсутствует	[Иконки]
Группа исполнения	Тургенев Иван Сергеевич	-	Ведущий специалист	+70000000013	Контейнер отсутствует	[Иконки]
Группа проектирования	Федоров Николай Николаевич	-	Ведущий специалист	-	Контейнер отсутствует	[Иконки]

Рисунок 2.26 — Информация о параметрах комплекта

После этого в нижней части АРМ отобразятся функциональные группы с параметрами сотрудника и его МСК.

Все данные разделены на следующие вкладки:

- **Общее** — сводные данные о сотруднике и параметры его МСК;
- **Клиентские сертификаты** — данные о сертификатах, полученных МСК пользователя;
- **Профили** — информация о профилях, применяемых к МСК;
- **ПУП** — информация о правилах управления приложениями, примененных к МСК;
- **История смены сотрудника** — история смены сотрудников, на которых было назначено устройство.

2.6.1.1 Вкладка «Общее»

- **Сотрудник:**

- Отдел/Группа,
- ФИО,
- Должность,
- Домен,
- Имя пользователя,
- E-mail,

- **Комплект:**

- Кнопка «Пароль разблокировки» — задает пароль разблокировки подключенного устройства (для Android, Аврора). Более подробно описано в «Инструкция по временной разблокировке устройства (Android)»;
- Id,
- Состояние блокировки (заблокирован/не заблокирован). Если устройство статусе «заблокировано», то дополнительно отображается причина блокировки:
 - командой администратора,
 - политикой,
 - меткой NFC,
 - прежней версией,
 - сменой пароля.

При наведении курсора на пиктограмму блокировки (в колонке «статус») в всплывающей подсказке будут отображены причины блокировки (рисунок 2.27).

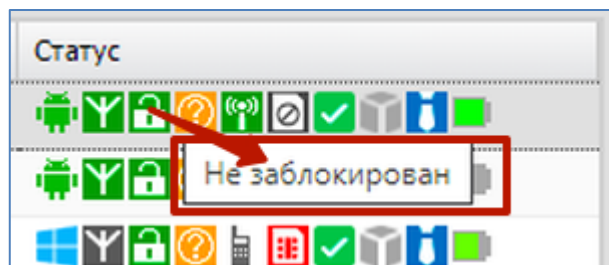


Рисунок 2.27 — Всплывающая подсказка, с информацией о блокировке

- Управление устройством (находится под управлением/отключен от управления/запрошено отключение);

- Последняя активность (дата и время);
- Тип соединения (GPRS/остальное (wi-fi)/не определен);
- Статус соединения:
 - В сети — Последняя активность была менее 15 минут назад. Если устройство iOS, то в последние 10 минут ни одна из команд протокола apple mdm НЕ завершилась со статусом NotNow;
 - Не в сети — Последняя активность была в диапазоне от 15 минут до 24 часов;
 - Долго не в сети — Последняя активность была более 24 часов назад;
 - Управление ограничено (NotNow) — Последняя активность была менее 15 минут назад и в последние 10 минут хотя бы одна из команд протокола apple mdm завершилась со статусом NotNow;
- Метки;
- Последняя регистрации устройства — дата и время последней регистрации устройства
- **SIM:**
 - Принадлежность (корпоративная, не корпоративная, нет SIM, есть SIM);
 - Состояние роуминга (в домашней сети/в роуминге/не определено/не известно);
 - IMSI;
 - ICCID;
 - Телефон (номер телефона);
 - Оператор домашней сети;
 - MCC / MNC домашней сети;
 - Установлено более одной SIM;
 - eSIM идентификатор (EID);
 - eSIM активна;
- **Местоположения:**
 - Включена служба определения местоположения (да/нет);
 - Ведется сбор местоположений: (+/-);
 - Источник данных — Значение политики «Источники данных местоположения» профиля «Настройки сбора местоположений Android» назначенного на устройство;
 - Координаты (последние зарегистрированные в системе координаты

- абонента);
- Дата/время (дата и время последней регистрации абонента в системе);
- **Устройство:**
 - Кнопка «Удаленное управление» (см руководство «Инструкция по удаленному управлению устройством»),
 - Тип устройства (смартфон/планшет/иное),
 - Модель устройства,
 - IMEI,
 - Кнопка «Добавить автомаркировку» (опционально).
 - UDID,
 - Кнопка «Добавить автомаркировку» (опционально).
 - Серийный номер (для МСК на платформе iOS и Android),
 - Кнопка «Добавить автомаркировку» (опционально).
 - Тип контейнера (Samsung Knox/Рабочий профиль Андроид/контейнер отсутствует),
 - Заряд аккумулятора (от 0 до 100 %),
 - Платформа,
 - Дистрибутив Linux,
 - Версия,
 - Версия ядра Linux,
 - Версия дистрибутива Linux
 - Принадлежность (корпоративное/личное),
 - Монитор (версия монитора),
 - Стратегия (устройство/устройство и контейнер KNOX/личный рабочий профиль/корпоративный рабочий профиль),
 - Привилегия монитора Device Owner (да/нет),
 - Привилегия монитора Device Admin (да/нет),
 - Привилегия монитора Profile Owner (да/нет),
 - Привилегия монитора KNOX (да/нет),
 - Привилегия монитора KNOX Premium (да/нет),
 - Привилегия монитора SYSTEM (да/нет),
 - Supervised,
 - Режим киоска (да/нет),
 - Наличие пароля (да/нет),
 - Текущий мобильный оператор,
 - MCC / MNC текущей сети,
 - Хэш аккаунта, залогиненного в iTunes,

- IP адрес,
- WiFi MAC адрес,
- SSID текущей WiFi сети,
- Bluetooth MAC адрес,
- Доступно RAM (Мб),
- Доступно на диске (Мб),
- Включено резервное копирование в облако,
- Шифрование хранилищ,
- Включен режим пропажи,
- Пароль соответствует всем требованиям — пароль соответствует не только требованиям парольных профилей системы (SafeMobile), но и требованиям всех парольных профилей, установленных на устройстве. Помимо профилей системы на устройство могут быть так же установлены профили Exchange и Apple Configurator. Только для МСК на платформе iOS:
- Пароль соответствует требованиям профилей (да/нет),
- Уровень Android API,
- Доступность Samsung KNOX API (да/нет),
- Версия Samsung KNOX API,
- Экран: высота (пиксели),
- Экран: ширина (пиксели),
- Уровень патча безопасности,
- Архитектура ОС,
- Дистрибутив Linux,
- Версия ядра Linux,
- Версия дистрибутива Linux,
- Заряд аккумулятора,
- Общий объём памяти (Мб),
- Имя устройства,
- Возможность сброса устройства,
- Идентификатор Exchange Active Sync,
- Устройство отображается в Find My (или в аналоге на Android),
- Включён режим «Не беспокоить»,
- Включён режим нескольких пользователей,
- Включена связанность устройств в сети,
- Присутствует активный аккаунт iTunes,
- Дата последнего бекапа в облако,
- Версия прошивки модема,

- Персональная точка доступа включена,
 - Имя продукта,
 - Идентификатор устройства для поиска обновления,
 - Какой тип обновлений отображается на устройстве,
 - Часовой пояс,
 - Способы аппаратного шифрования,
 - Корпоративный идентификатор устройства:
 - Кнопка «Добавить автомаркировку» (опционально).
 - Доступно обновление ОС,
 - Дата получения обновления ОС,
 - Дата старта ОС — только для Android и Аврора,
 - Привязанные SIM (IMSI) — список привязанных к устройству SIM-карт.
-
- **Журнал монитора:**
 - Дата — только для Android и Аврора. Отображает дату создания архива системных логов устройства, запрошенных администратором командой «Запрос журналов Монитора». При отсутствии архива дата не указывается.
 - Кнопка скачивания архива логов устройства. При отсутствии архива кнопка не отображается.
-
- **Дополнительные параметры (только для Android):**
 - Build Board,
 - Build Brand,
 - Build Fingerprint,
 - Build ID,
 - Build DISPLAY,
 - Build Tags,
 - Build Type,
 - Build Hardware,
 - Build Host,
 - Build Device,
 - Build Manufacturer,
 - Build Model,
 - Build Codename,
 - Build Incremental Version,

- Build Product,
- Build Supported Abist,
- Build User,
- IMEI для 2 слота,
- Оптимизация MIUI (фича ОС MIUI от Xiaomi),
- Серийный номер KNOX,
- Название KNOX версии,
- Установлена доверенная прошивка (KNOX Warranty Bit),
- Доступность Zebra Api,
- Устройство поддерживает PIN, графический ключ и пароль,
- NFC,
- Телефония,
- RFID сканер,
- Производитель процессора,
- Модель процессора.

2.6.1.2 Вкладка «Клиентские сертификаты»

Во вкладке отображаются клиентские сертификаты, полученные выбранным в главном окне устройством. По умолчанию отображаются сертификаты, действующие на момент просмотра данных, для просмотра всех сертификатов следует выключить чек-бокс «Показывать только действующие сертификаты» (рисунок 2.28).

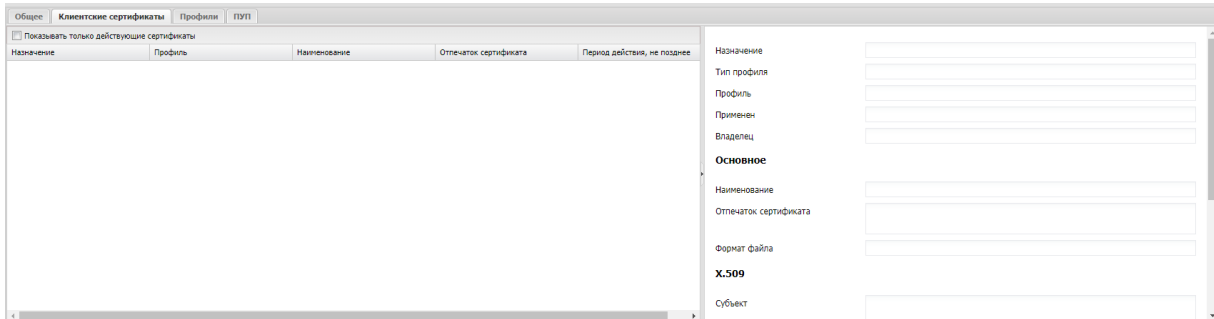


Рисунок 2.28 — Список клиентских сертификатов

Каждая строка списка содержит следующие данные:

- Назначение — принимает значения «Профиль» или mTls (отображается по умолчанию);
- Тип профиля — тип профиля, для которого был выписан сертификат, для mTls поле имеет значение «-»;
- Профиль — Наименование профиля, для которого был выписан сертификат (отображается по умолчанию);
- Флаг «Применен» — Для сертификатов с назначением профиля определяется по статусу применения профиля. Для mTLS по факту авторизации устройства с этим сертификатом;
- Наименование — (отображается по умолчанию);
- Отпечаток сертификата — (отображается по умолчанию);
- Формат файла;
- Субъект;
- Версия;
- Серийный номер;
- Издатель;
- Период действия:
 - Не ранее;
 - Не позднее — (отображается по умолчанию).
- Приватный ключ;
- Владелец.

В окне просмотра выбранного в списке сертификата отображается подробная информация о сертификате (рисунок 2.29).

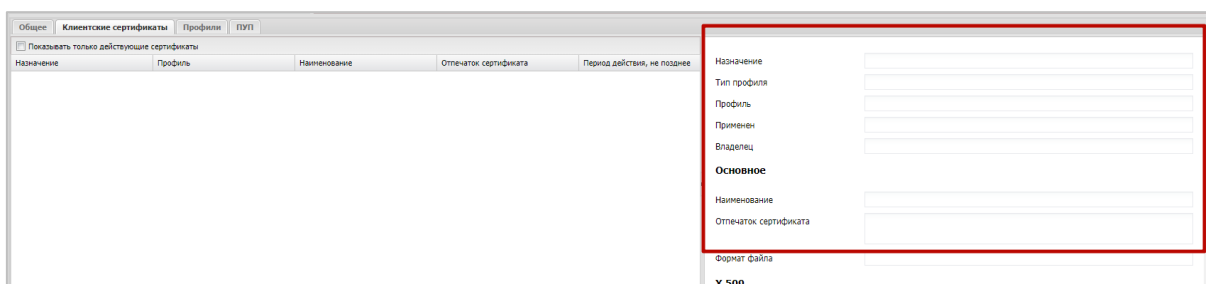


Рисунок 2.29 — Сводные данные о сертификате

2.6.1.3 Вкладка «Профили»

Во вкладке отображается список профилей, совпадающих с платформой устройства и назначенных на (подробнее о «Профилях» в разделе 2.6.8):

- Устройство,
- Пользователя,
- Одно из родительских подразделений пользователя (включая корень ОШС).

Профили в списке сгруппированы по результирующим профилям, результирующий профиль выделен жирным шрифтом (рисунок 2.30).

Тип/Наименование	Наименование ключа	Значение ключа	Приоритет	Назначен на	Условия соблюдения	Применен	Способ применения	Дата назначения	Дата применения
Точка доступа WiFi Android	Имя точки доступа (SSID)	ANY_CCNC				Нет	Раздельный	03.06.2024 09:33:05	
Профиль Android из точки доступа ANY_CCNC	Имя точки доступа (SSID)	ANY_CCNC	1	ООО "Компания"	Да	Нет	Раздельный	03.06.2024 09:33:05	
Точка доступа WiFi Android	Имя точки доступа (SSID)	ANY_CCNC_LDR				Нет	Раздельный	03.06.2024 09:33:05	
Профиль Android из точки доступа ANY_CCNC_LDR	Имя точки доступа (SSID)	ANY_CCNC_LDR	1	ООО "Компания"	Да	Нет	Раздельный	03.06.2024 09:33:05	
Точка доступа WiFi Android	Имя точки доступа (SSID)	MegaFon				Нет	Раздельный	03.06.2024 09:33:05	
Профиль Android из точки доступа MegaFon	Имя точки доступа (SSID)	MegaFon	1	ООО "Компания"	Да	Нет	Раздельный	03.06.2024 09:33:05	

Рисунок 2.30 — Результирующий профиль

Каждая строка списка содержит следующие данные:

- Тип/Наименование — (Отображается по умолчанию);
 - Для результирующего профиля отображается тип;
 - Для обычных профилей наименование;
- Наименование ключевой политики — (отображается по умолчанию);
 - Для профилей без ключевой политики отображается «-»;
- Значение ключевой политики — (отображается по умолчанию);
 - Для профилей без ключевой политики отображается «-»;
- Приоритет — (отображается по умолчанию);
- Назначен на — (отображается по умолчанию);
 - Для результирующего профиля не отображается;
 - Для обычных профилей:
 - «Устройство» — если ближайшее (по дереву ОШС) к устройству назначение профиля сделано на устройство;
 - «Сотрудник» — если ближайшее (по дереву ОШС) к устройству назначение профиля сделано на сотрудника;
 - Наименование ближайшего к устройству узла ОШС, на кото-

- рый сделано назначение профиля, если нет назначений профиля на сотрудника или устройство;
- Условия соблюдены — Принимает значения: «Да/Нет» (отображается по умолчанию). Профили, условия которых не соблюдены, выделены серым цветом;
 - Применен — (отображается по умолчанию):
 - Для результирующих профилей может принимать значения:
 - Да — если контрольная сумма результирующего профиля совпадает с контрольной суммой примененного профиля;
 - Применен устаревший профиль — если контрольная сумма результирующего профиля **не** совпадает с контрольной суммой примененного профиля;
 - Нет — в остальных случаях;
 - Для обычных отдельных профилей может принимать значения:
 - Да — если контрольная сумма обычного профиля совпадает с контрольной суммой примененного профиля;
 - Нет — в остальных случаях;
 - Для обычных совместных профилей может принимать значения:
 - Да — если контрольная сумма отображаемого профиля совпадает с контрольной суммой примененного профиля и результирующий профиль собран из одного профиля;
 - Частично — если контрольная сумма отображаемого профиля **не** совпадает с контрольной суммой примененного и результирующий профиль собран из двух и более профилей;
 - Нет — в остальных случаях;
 - Способ применения — Принимает значения: отдельно/совместно (отображается по умолчанию);
 - Дата назначения — (отображается по умолчанию);
 - Дата применения — (отображается по умолчанию).

В окне просмотра выбранного профиля отображаются следующие данные (рисунок 2.31):

- Политики — политики профиля (см. раздел 2.6.9);
- Условия — условия применения профиля, выбранного в списке (см. раздел 2.6.9.3).

Если результирующий профиль состоит из одного профиля, то политики и условия для него не отображаются. Для просмотра политик и условий применения следует выбрать тот профиль, который формирует результирующий.

Общие		Клиентские сертификаты		Профили		ПУП		Политики		Условия		
Тип	Наименование	Наименование к/л	Значение ключа	Приоритет	Назначен на	Условия соблюдения	Применен	Способ применения	Дата назначения	Дата применения	Имя	Значение
Точка доступа WiFi Android	Имя точки доступа (SSID)	ANY_CСMC				Нет		Раздельный	03.06.2024 09:33:05		Имя точки доступа (SSID)	"ANY_CСMC"
Профиль Android из точки доступа ANY_CСMC	Имя точки доступа (SSID)	ANY_CСMC	1	ООО "Компания"	Да	Нет		Раздельный	03.06.2024 09:33:05		Окрытая сеть	-
Точка доступа WiFi Android	Имя точки доступа (SSID)	ANY_CСMC_LDR				Нет		Раздельный	03.06.2024 09:33:05		Выполнить попытку автоматического подключения	-
Профиль Android из точки доступа ANY_CСMC_LDR	Имя точки доступа (SSID)	ANY_CСMC_LDR	1	ООО "Компания"	Да	Нет		Раздельный	03.06.2024 09:33:05		Адресация IP/С адреса	Не задано
Точка доступа WiFi Android	Имя точки доступа (SSID)	МегаФон				Нет		Раздельный	03.06.2024 09:33:05		Прокси	Не задано
Профиль Android из точки доступа МегаФон	Имя точки доступа (SSID)	МегаФон	1	ООО "Компания"	Да	Нет		Раздельный	03.06.2024 09:33:05		URL прокси-сервера	Не задано
											Порт прокси-сервера	-
											Тип безопасности	-
											Использовать PAC (Proxy Auto Config)	-
											Список хостов, для которых нужно исключить использование прокси-сервера при подключении. Можно использовать подстановочные символы, например: *.example.com	-
											Пароль	*****
											* Обязательно при использовании Android 13 и выше. Список доменов для проверки сертификата AAA-сервера (обычно RADIUS). Можно перечислить несколько доменов через ";". Если домен, указанный в сертификате сервера, не будет найден в этом списке то подключение к точке доступа будет заблокировано	
											Тип EAP	-
											Учётные данные (клиентский сертификат или настройки SCEP)	-

Рисунок 2.31 — Просмотр данных результирующего профиля

2.6.1.4 Вкладка «ПУП»

Во вкладке отображаются правила управления приложениями, совпадающими с платформой устройства и назначенными на:

- Устройство,
- Пользователя,
- Одно из родительских подразделений пользователя (включая корень ОШС).

ПУП сгруппированы по UID приложения и месту установки (рисунок 2.32).

Результирующие ПУП сортируются по наименованию приложения, в алфавитном порядке. Обычные ПУП — по приоритету, от меньшего к большему.

Общие										Настройки		Условия	
Приложение/ПУП	UID	Приоритет	Назначен на	Условия соблюдения	Применено	Контейнер	Цель	На устройстве	Включен	Настройка	Значение	Настройка	Условия
НММ - мы любим моду	com.him.goe				Да	Устройство	Некорпорат...	1.1	Включе	Название	com.him.goe		
com.him.goe	com.him.goe	1	Устройство	Да	Да	Устройство	Некорпоратив...	-	-	Платформа	iPhone OS		
Почта Mail.ru	ru.mail.mail				Нет	Устройство	Некорпорат...		Заблюк	Тип приложения	Некорпоративное		
ru.mail.mail	ru.mail.mail	1	ООО "Компания"	Да	Нет	Устройство	Некорпоратив...	-	-	UID	com.him.goe		
Приложение i 0	ru.application.name_i0				Нет	Устройство	1.0	1.1	Включе	Описание			
ru.application.name_i0	ru.application.name_i0	1	Устройство	Да	Нет	Устройство	1.0	-	-	Приложение должно быть установлено	Да		
afedutsov	ru.application.name_i0	2	root	Да	Нет	Устройство	Доступно в SafeStore	-	-	Приложение можно настроить удаленно	Да		
Приложение i 1	ru.application.name_i1				Нет	Устройство	1.1		Заблюк	Удалить с устройства при отключении от управления	Да		
ru.application.name_i1	ru.application.name_i1	1	ООО "Компания"	Да	Нет	Устройство	1.1	-	-	Запрещено резервное копирование данных	Да		
										Использовать VPN для приложений (Per-App VPN)	Нет		

Рисунок 2.32 — Список ПУП

Каждая строка таблицы содержит следующие данные:

- Приложение/ПУП — (отображается по умолчанию):
 - Для результирующего ПУП отображается — наименование приложения;
 - Для обычных ПУП — наименование ПУП;
- UID — (отображается по умолчанию);
- Приоритет — (отображается по умолчанию);
- Назначен на — (отображается по умолчанию):
 - Для результирующего ПУП не отображается;
 - Для обычных ПУП:
 - «Устройство» — если ближайшее (в ОШС) к устройству назначение ПУП сделано на устройство;
 - «Сотрудник» — если ближайшее (в ОШС) к устройству назначение ПУП сделано на сотрудника;
 - Наименование ближайшего к устройству узла ОШС, на который сделано назначение ПУП, если нет назначений ПУП на сотрудника или устройство.

- Условия соблюдены — Принимает значения «Да/Нет» (отображается по умолчанию). ПУП, условия которых не соблюдены, выделены серым цветом;
- Применен — Вычисляется аналогично отчету «Правила управления» (см. раздел 2.7.6);
- Контейнер — (отображается по умолчанию);
- Цель — Вычисляется аналогично отчету «Правила управления» (см. раздел 2.7.6). (отображается по умолчанию);
- На устройстве — Вычисляется аналогично отчету «Правила управления» (см. раздел 2.7.6). (отображается по умолчанию);
 - Для обычных ПУП отображается «-»;
- Включено — Вычисляется аналогично отчету «Правила управления» (см. раздел 2.7.6). (отображается по умолчанию);
 - Для обычных ПУП отображается: «-»;
- Выбор пользователя — Вычисляется аналогично отчету «Правила управления» (см. раздел 2.7.6). (отображается по умолчанию);
 - Для обычных ПУП отображается «-»;
- Статус — Вычисляется аналогично отчету «Правила управления» (см. раздел 2.7.6). (отображается по умолчанию);
 - Для обычных ПУП отображается «-»;
- Дата назначения — Вычисляется аналогично отчету «Правила управления» (см. раздел 2.7.6). (отображается по умолчанию);
- Дата применения — вычисляется аналогично отчету «Правила управления» (см. раздел 2.7.6). (отображается по умолчанию).

В окне просмотра, выбранного в списке ПУПа, отображаются следующие данные (рисунок 2.33):

- Настройки — настройки ПУП выбранного в списке, в соответствии с платформой устройства (подробнее о настройках ПУП см. раздел 2.6.13);
- Условия — Условия применения, выбранного ПУП (подробнее об условиях применения ПУП см. раздел 2.6.13.2).

Имя ПУП	ID	Приоритет	Масштаб	Условия соблюдены	Применено	Контейнер	Цель	На устройстве	Включено	Настройки	Условия	Значение
Имя ПУП	ID	Приоритет	Масштаб	Условия соблюдены	Применено	Контейнер	Цель	На устройстве	Включено	Настройка	Условие	Значение
Имя ПУП	ID	Приоритет	Масштаб	Условия соблюдены	Применено	Контейнер	Цель	На устройстве	Включено	Настройка	Условие	Значение
Имя ПУП	ID	Приоритет	Масштаб	Условия соблюдены	Применено	Контейнер	Цель	На устройстве	Включено	Настройка	Условие	Значение
Имя ПУП	ID	Приоритет	Масштаб	Условия соблюдены	Применено	Контейнер	Цель	На устройстве	Включено	Настройка	Условие	Значение

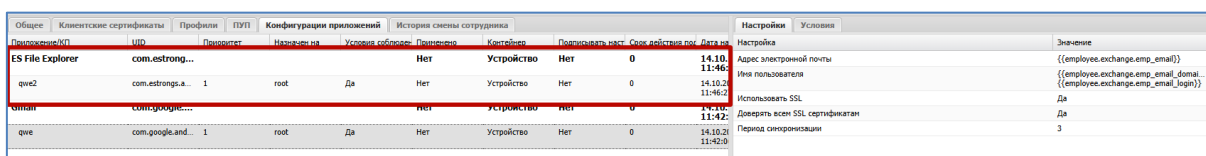
Рисунок 2.33 — Окно просмотра параметров ПУП

2.6.1.5 Вкладка «Конфигурация приложений»

Во вкладке отображаются конфигурации приложений заданные в разделе «Приложения — Конфигурации» и назначенные на:

- устройство,
- пользователя,
- одно из родительских подразделений пользователя (включая корень ОШС).

Конфигурации приложений сгруппированы по UID приложения и месту установки (рисунок 2.34). Группы сортируются по наименованию приложения, в алфавитном порядке. Конфигурации внутри групп — по приоритету, от меньшего к большему.



Приложение/КП	UID	Приоритет	Назначена на	Условия соблюдены	Применена	Категория	Получивать уведомления	Срок действия политики	Дата	Настройка	Условие	Значение
ES File Explorer	com.strong...			Нет	Устройство	Нет	0	14.10.11:46:0		Адрес электронной почты		{{employee.exchange_email}}
que2	com.strong.s...	1	root	Да	Нет	Устройство	Нет	0	14.10.21:46:2	Имя пользователя		{{employee.exchange_email_domain}} {{employee.exchange_email_login}}
Gmail	com.google...			Нет	Устройство	Нет	0	14.10.11:42:0		Использовать SSL		Да
que	com.google.and...	1	root	Да	Нет	Устройство	Нет	0	14.10.21:42:0	Доверять всем SSL сертификатам		Да
										Период синхронизации		3

Рисунок 2.34 — Приложения и конфигурации приложений

Каждая строка таблицы содержит следующие данные:

- Приложение/КП (отображается по умолчанию) — Для группы отображается наименование приложения, для конфигурации приложения — наименование КП.
- UID — UID приложения;
- Приоритет — (для группы не отображается) приоритет конфигурации ;
- Назначен на — (для группы не отображается) принимает значение:
 - устройство — если ближайшее к устройству назначение КП сделано на устройство;
 - сотрудник — если ближайшее к устройству назначение КП сделано на сотрудника;
 - наименование ближайшего к устройству узла ОШС, на который сделано назначение КП, если нет назначений КП на сотрудника или устройство;
- Условия соблюдены — (для группы не отображается) «Да»/«Нет». Конфигурации с невыполненными условиями выделяются цветом.
- Применена — статус применения конфигурации:
 - Для группы:
 - «Да» если контрольная сумма результирующей КП совпадает с применённой;
 - «Применена устаревшая КП» — если контрольные суммы не

совпадают;

- «Нет» — в остальных случаях.
- Для конфигурации приложения:
 - «Да» — если контрольная сумма КП совпадает с применённой;
 - «Нет» — в остальных случаях.
- Контейнер — место установки (Устройство/Контейнер),
- Подписывать настройки конфигурации приложения — «Да»/«Нет»;
- Срок действия подписи — (дни);
- Дата назначения (отображается по умолчанию);
- Дата применения (отображается по умолчанию).

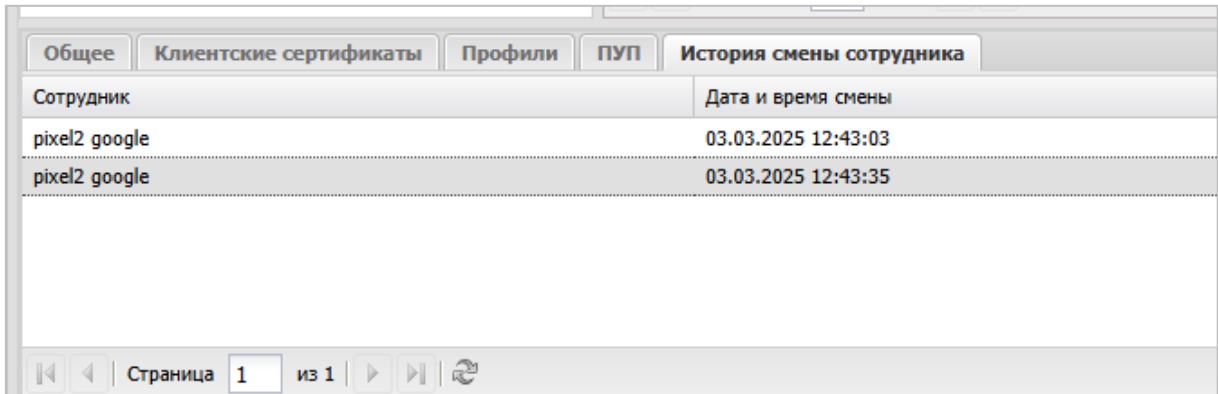
При выборе группы или конфигурации приложения отображается окно просмотра с закладками:

- Настройки — список настроек результирующей КП (для группы) или выбранной КП.
- Условия (только для конфигурации приложения) — список условий. Состав колонок:

2.6.1.6 Вкладка «История смены сотрудников»

Во вкладке отображается история смены сотрудников, на которых было назначено устройство в разделе «Комплекты». История событий смены сотрудников представлена в виде списка, в котором каждая строка содержит следующую информацию:

- ФИО сотрудника,
- Дата и время смены сотрудника (дд.мм.гг, чч.мм.сс).



Сотрудник	Дата и время смены
pixel2 google	03.03.2025 12:43:03
pixel2 google	03.03.2025 12:43:35

Рисунок 2.35 — История смены сотрудников на устройстве

2.6.2 Раздел «Сообщения»

Пункт главного меню «Сообщения» предназначен для отображения зарегистрированных сообщений на МСК (SMS).

Примечание

Информация о сообщениях доступна только для МСК на платформе Android версии не новее 9.0, при наличии у монитора привилегии владельца устройства (Device Owner).

Информационная таблица раздела «Сообщения» содержит следующие столбцы:

- Направление (входящее или исходящее);
- Абонент/телефон — ФИО сотрудника, если сообщение внутрикорпоративное (абонент зарегистрирован в «UEM SafeMobile»), и номер телефона, если сообщение внешнее;
- Текущий номер — номер телефона SIM-карты МСК (сотрудника, выбранного в главной таблице), с которого получено или на которое отправлено сообщение;
- Тип — тип сообщения: SMS;
- Время — время регистрации сообщения;
- Содержимое — в столбце отображается тип отправленного устройством сообщений (SMS);
- Блокировано — содержит «Да», если сообщение заблокировано политиками безопасности; содержит «Нет», если сообщение не заблокировано.

В информационной таблице имеется возможность отображения сообщений в соответствии с выбранным фильтром.

Чтобы открыть меню настройки фильтрации списка сообщений, следует нажать в нижней панели информационной таблицы кнопку **Настроить фильтры**, после чего раскроется меню со следующими пунктами:

Направление — установите этот флажок и выберите в появившемся списке, какие сообщения необходимо показать в таблице: Входящие и/или Исходящие.

После — установите этот флажок и укажите в появившемся календаре дату и время, чтобы отображать в списке сообщения, произошедшие после этой даты и времени.

До — установите этот флажок и укажите в появившемся календаре дату и время, чтобы отображать в списке сообщения, произошедшие до этой даты и времени.

По умолчанию в таблице показываються все сообщения без фильтрации (флажки в раскрывающемся меню «**Настроить фильтры**» сняты).

2.6.3 Раздел «Звонки»

В разделе «Звонки» отображаются сведения о зарегистрированных в системе звонках, выполненных с/на МСК, выбранное в главной таблице (рисунок 2.36).

ФИО	Тип	Категория	Направление	Текущий номер	Абонент/телефон	Время	Длительность	Емодирован
Фадорев Николай Николаевич	GSM	Телефон	Входящие		+70000000030	28.02.2024 12:23:00	0 с	Нет
Петров Василий Фадорович	GSM	Телефон	Входящие		+70000000011	28.02.2024 12:14:33	78 с	Нет
Фадорев Николай Николаевич	VoIP	SIP	Исходящие	41090	42090	22.02.2024 17:15:50	63 с	Нет
Петров Василий Фадорович	VoIP	SIP	Входящие	41090	2990	22.02.2024 17:01:26	11 с	Нет

Рисунок 2.36 — Раздел «Звонки»

Примечание

Информация о звонках доступна только для МСК на платформе Android версии не новее 9.0, при наличии у монитора привилегии владелец устройства (Device Owner).

Информационная таблица раздела «Звонки» содержит следующие столбцы:

- ФИО — фамилия, имя и отчество абонента, которому или от которого был выполнен звонок на МСК, выбранное в главной таблице;
- Тип — тип связи, использованный при выполнении звонка — GSM (для незащищенных звонков) или VoIP (для защищенных звонков);
- Категория — категория вызова: Телефон, SIP, УПАТС;
- Направление — входящий или исходящий звонок;
- Текущий номер — номер телефона SIM-карты МСК (сотрудника, выбранного в главной таблице), с которого или на который выполнялся вызов;
- Абонент/Телефон (номер вызываемого или позвонившего абонента) — отображается ФИО сотрудника, если звонок корпоративный (абонент зарегистрирован в «UEM SafeMobile»), и номер телефона, если звонок внешний. Если в столбце отображается ФИО, то при наведении на него курсора мыши отображается подсказка, содержащая номер телефона;
- Время — дата и время звонка;
- Длительность — продолжительность звонка в секундах;

- **Блокирован** — столбец содержит значок блокирования, если звонок был блокирован политиками безопасности, в противном случае отображается сообщение «Нет».

В информационной таблице имеется возможность отображения звонков в соответствии с выбранным фильтром (рисунок 2.37).

ФИО	Тип	Категория	Направление	Текущий номер	Абонент/телефон	Время	Длительность	Блокирован
Иванов Александр Васильевич	GSM	Телефон	Входящие	+70000000011	+37566000001	27.11.2018 14:52:44	9 с	Нет
Иванов Александр Васильевич	GSM	Телефон	Входящие	+375660000321	+70000000020	27.11.2018 11:36:03	9 с	Нет
Иванов Александр Васильевич	GSM	Телефон	Входящие	+375660000321	+70000000020	27.11.2018 11:30:25	89 с	Нет
Сидоров Василий Петрович	GSM	Телефон	Исходящие	+375660000321	+37566000001	27.11.2018 11:30:13	9 с	Нет
Сидоров Василий Петрович	GSM	Телефон	Исходящие	+70000000011	+70000000010	27.11.2018 11:24:28	80 с	Нет
Васечкин Петр Викторович	GSM	Телефон	Исходящие	+375660000321	+70000000003	25.11.2018 17:37:27	89 с	Нет
Васечкин Петр Викторович	GSM	Телефон	Исходящие	+375660000321	+70000000003	25.11.2018 17:28:48	87 с	Нет
Он, детали	Он, детали	Он, детали	Исходящие	Он, детали	Он, детали	22.11.2018 17:01:26	108 с	Нет
Сидоров Василий Петрович	VoIP	SIP	Исходящие	1990	31090	22.11.2018 17:01:26	108 с	Нет
Федоров Николай Николаевич	GSM	Телефон	Исходящие	+375660000321	+70000000030	22.11.2018 17:00:00	0 с	Нет
Сидоров Василий Петрович	GSM	Телефон	Исходящие	+375660000321	+70000000010	22.11.2018 17:00:00		Нет

Настройка фильтров:

- Направление
- Категория
 - Телефон
 - УПАТС
 - SIP
- Тип
- Блокировано
- После
- До

Рисунок 2.37 — Фильтрация звонков

Чтобы открыть меню настройки фильтрации списка звонков, следует нажать в нижней панели информационной таблицы кнопку «**Настроить фильтры**», после чего отобразятся меню со следующими пунктами:

- **Направление** — установите этот флажок и выберите в появившемся списке, какие звонки необходимо показать в таблице: **Входящие** и/или **Исходящие**.
- **Категория** — установите этот флажок и выберите в появившемся списке категорию звонков для отображения в таблице: **Телефон**, **УПАТС**, **SIP**.
- **Тип** — установите этот флажок и выберите в появившемся списке типы звонков, которые необходимо отобразить в таблице: GSM (незащищенные) или VoIP (защищенные);
- **Блокировано** — позволяет отображать записи о звонках в зависимости от признака их блокировки.
- **После** — установите этот флажок и укажите в появившемся календаре дату и время, чтобы отображать в списке звонки, выполненные после этой даты и времени.
- **До** — установите этот флажок и укажите в появившемся календаре дату и время, чтобы отображать в списке звонки, выполненные до этой даты и времени.

По умолчанию в таблице показываются все звонки без фильтрации (флажки в раскрывающемся меню «**Настроить фильтры**» сняты).

Вызовы, относящиеся к единому номеру абонента, отображаются в таблице звонков в виде сгруппированных элементов. В этом случае в столбцах «Категория» и «Абонент/телефон» отображается сообщение «См. детали» (рисунок 2.38).

ФИО	Тип	Категория	Направление	Текущий номер	Абонент/телефон	Время	Длительность	Блокирован
	GSM	Телефон	Исходящее	+70000000002	+70000000003	26.12.2016 17:56:27	87 сек.	Нет
	GSM	Телефон	Исходящее	+70000000002	+70000000003	26.12.2016 17:54:32	82 сек.	Нет
	GSM	Телефон	Исходящее	+70000000002	+375660000321	26.12.2016 17:53:29	28 сек.	Нет
	GSM	Телефон	Исходящее	+70000000002	+70000000011	26.12.2016 17:47:34	71 сек.	Нет
⊕	См. детали	См. детали	Исходящее	См. детали	См. детали	19.12.2016 14:01:26	89 сек.	Нет

Рисунок 2.38 — Звонок на единый номер в свернутом виде

Чтобы просмотреть дополнительные сведения обо всех звонках, содержащихся в едином звонке на номер абонента, нажмите значок ⊕, после чего записи о звонках будут развернуты в таблице (рисунок 2.39).

ФИО	Тип	Категория	Направление	Текущий номер	Абонент/телефон	Время	Длительность	Блокирован
	GSM	Телефон	Входящее	+70000000011	+375660000001	27.11.2018 14:52:44	9 с	Нет
Иванов Александр Васильевич	GSM	Телефон	Входящее	+375660000321	+70000000020	27.11.2018 11:36:03	9 с	Нет
Иванов Александр Васильевич	GSM	Телефон	Входящее	+375660000321	+70000000020	27.11.2018 11:30:25	89 с	Нет
Иванов Александр Васильевич	GSM	Телефон	Исходящее	+375660000321	+375660000001	27.11.2018 11:30:13	9 с	Нет
Сидоров Василий Петрович	GSM	Телефон	Исходящее	+70000000011	+70000000010	27.11.2018 11:24:28	80 с	Нет
Васечкин Петр Викторович	GSM	Телефон	Исходящее	+375660000321	+70000000003	25.11.2018 17:37:27	89 с	Нет
Васечкин Петр Викторович	GSM	Телефон	Исходящее	+375660000321	+70000000003	25.11.2018 17:28:48	87 с	Нет
⊕	См. детали	См. детали	Исходящее	См. детали	См. детали	22.11.2018 17:01:26	108 с	Нет
Сидоров Василий Петрович	VoIP	SIP	Исходящее	1990	31090	22.11.2018 17:01:26	108 с	Нет
Фадоров Николай Николаевич	GSM	Телефон	Исходящее	+375660000321	+70000000030	22.11.2018 17:00:00	0 с	Нет
Сидоров Василий Петрович	GSM	Телефон	Исходящее	+375660000321	+70000000010	22.11.2018 17:00:00	0 с	Нет

Рисунок 2.39 — Звонок на единый номер в развернутом виде

2.6.4 Раздел «Местоположения»

Раздел «Местоположения» отображает фрагмент карты, на которой в виде ломаной линии отображена информация о местоположении и перемещении абонента. Кроме того, эта информация выводится в виде таблицы с координатами абонента в определенный момент времени (рисунок 2.40).

В правой части информационной таблицы раздела «Местоположения» расположен реестр координат точек маршрута перемещений абонента МСК, а также время регистрации координат МСК в каждой указанной точке маршрута.

Для изменения масштаба карты (увеличения или уменьшения изображения) используется шкала масштабирования, расположенная в верхнем левом углу карты. Кроме того, масштаб изображения можно изменять, используя вращение колеса мыши, если курсор расположен в области карты.

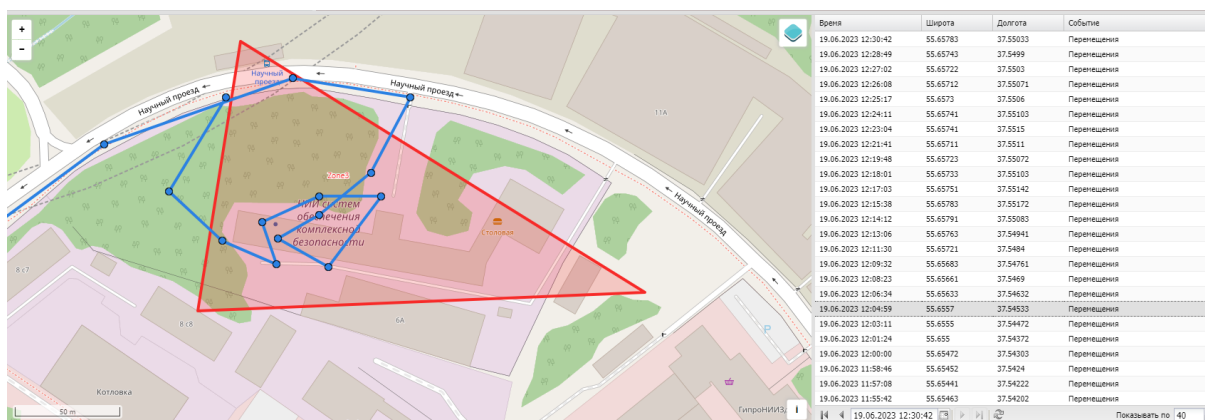



Рисунок 2.40 — Раздел «Местоположения»

При нажатии на значок  в правой верхней части карты отображается меню настройки отображения информации на карте (рисунок 2.41).

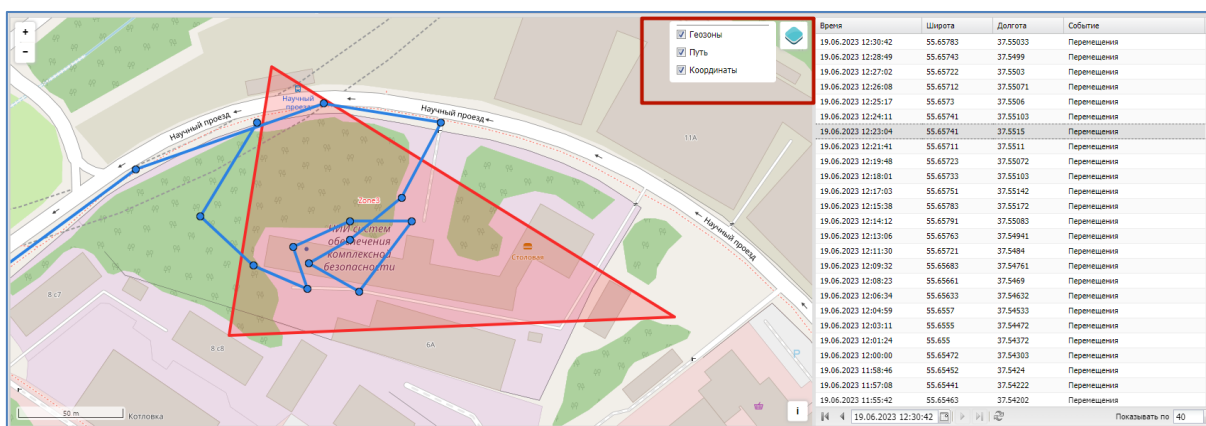


Рисунок 2.41 — Настройка режима отображения информации о местоположении абонента на карте

В меню расположены флажки, позволяющие выбрать слои отображения графической информации на карте (можно выбрать все параметры одновременно):

- Геозоны,
- Путь,
- Координаты.

При установленном флажке **«Геозоны»** на карте отображаются созданные области (описание приведено в 2.8.10), с установленными параметрами и ограничениями для применения на МСК. При установленном флажке **«Путь»** на карте отображается линия перемещения абонента. При установленном флажке **«Координаты»** в точках местоположения абонента выводятся координаты абонента.


Кроме того, меню позволяет выбрать источник картографической информации (сервер ГИС), который используется для отображения карты, по умолчанию: `openstreetmap.org`.

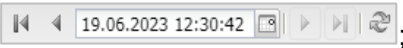
В информационной таблице имеется возможность отображения реестра координат местоположения абонента в соответствии с сортировкой по колонкам таблицы и настроек пагинации реестра (рисунок 2.42).

Время	Широта	Долгота	Событие
19.06.2023 12:30:42	55.65783	37.55033	Перемещения
19.06.2023 12:28:49	55.65743	37.5499	Перемещения
19.06.2023 12:27:02	55.65722	37.5503	Перемещения
19.06.2023 12:26:08	55.65712	37.55071	Перемещения
19.06.2023 12:25:17	55.6573	37.5506	Перемещения
19.06.2023 12:24:11	55.65741	37.55103	Перемещения
19.06.2023 12:23:04	55.65741	37.5515	Перемещения
19.06.2023 12:21:41	55.65711	37.5511	Перемещения
19.06.2023 12:19:48	55.65723	37.55072	Перемещения
19.06.2023 12:18:01	55.65733	37.55103	Перемещения
19.06.2023 12:17:03	55.65751	37.55142	Перемещения
19.06.2023 12:15:38	55.65783	37.55172	Перемещения
19.06.20		37.55083	Перемещения
19.06.20		37.54941	Перемещения
19.06.20		37.5484	Перемещения
19.06.20		37.54761	Перемещения
19.06.20		37.5469	Перемещения
19.06.20		37.54632	Перемещения
19.06.20		37.54533	Перемещения
19.06.20		37.54472	Перемещения
19.06.20		37.54372	Перемещения
19.06.20		37.54303	Перемещения
19.06.20		37.5424	Перемещения
19.06.20		37.54222	Перемещения
19.06.20		37.54202	Перемещения

Рисунок 2.42 — Фильтрация местоположений абонента

Настройки пагинации реестра координат позволяют просматривать записи изменения координат, с указанного времени и даты. Чтобы задать дату и время необходимо выполнить следующие действия:

1. Нажать кнопку , после чего откроется модальное окно выбора даты и времени;

2. Ввести дату и время. Так же ввести дату и время допустимо напрямую, в строке отображения даты и времени ;

3. Нажать кнопку «Принять», после чего реестр отобразит страницу данных изменения координат, совершенные после указанной даты и времени.

Для удобства работы со списком рекомендуется указывать необходимое количество записей на одной странице в соответствующем поле настройки пагинации.

Для просмотра отчётов о местоположении одного или нескольких абонентов в заданных интервалах времени следует использовать отчёт **«Перемещения»**, более подробные сведения о котором приведены в п. 2.7.4.

Примечание

Определение местоположения сотрудника и его комплекта выполняется только в рабочее время. Для того чтобы появилась такая возможность необходимо, чтобы у сотрудника или подразделения, в котором он работает, был настроен календарь рабочего времени в соответствующем разделе АРМ Администратора SafeMobile, более подробное описание которого приведено в п.2.11.

На карте имеется возможность просмотра местоположения сотрудника в выбранной точке траектории его передвижения. Для этого необходимо выбрать точку траектории, чтобы отобразить во всплывающем окне имя сотрудника и время его нахождения в этой точке местности (рисунок 2.43).



Рисунок 2.43 — Местонахождение сотрудника в выбранной точке траектории перемещения

2.6.5 Раздел «Действия»

Раздел «Действия» предназначен для просмотра команд, выполненных на выбранном МСК.

Для просмотра журнала действий следует выбрать пункт главного меню «Действия», а затем требуемое устройство в главной таблице. В информационной таблице отобразится журнал действий (рисунок 2.44).

Администратор	Команда	Параметры	Время создания	Время завершения	Результат	Отмена
demoadmin	Перегодочление	10	29.02.2024 08:41:22	н/д	Команда не поддерживается	X
demoadmin	Установка списка корпоративных SIM-карт		29.02.2024 08:41:22	н/д	Команда не поддерживается	X
demoadmin	Синхронизация времени устройства с сервером		29.02.2024 08:41:22	н/д	Команда не поддерживается	X
demoadmin	Запрос списка установленных приложений		29.02.2024 08:41:22	н/д	Команда не поддерживается	X
demoadmin	Запуск приложения	ru.application_name_w0	29.02.2024 08:41:22	н/д	Команда не поддерживается	X
demoadmin	Управление блокировкой устройства	F	29.02.2024 08:41:22	н/д	Команда не поддерживается	X
demoadmin	Управление блокировкой устройства	T	29.02.2024 08:41:22	н/д	Команда не поддерживается	X

Рисунок 2.44 — Раздел «Действия»

Информационная таблица раздела «Действия» содержит следующие столбцы:

- Администратор — имя пользователя (логин), который отправил команду на МСК, выбранное в главной таблице. Отсутствие имени пользователя (логина), указывает на то, что команда отправлена с МСК;
- Команда — команда, отправленная на МСК;
- Параметры — параметры команды (если есть);
- Время создания — время создания команды;
- Время завершения — время выполнения команды;
- Результат — результат выполнения команды;
- Отмена — в столбце отображается значок, позволяющий выполнить отмену отправленной на устройство команды, если значок отмены команды активен. Отменить команду можно пока не был получен её результат. Если команда завершена со статусом «Нормальное завершение» или завершена из-за ошибки (сбоя) устройства (или ПО), отменить команду невозможно (значок отмены неактивен).

В информационной таблице имеется возможность отображения журнала действий в соответствии с выбранным фильтром (рисунок 2.45).

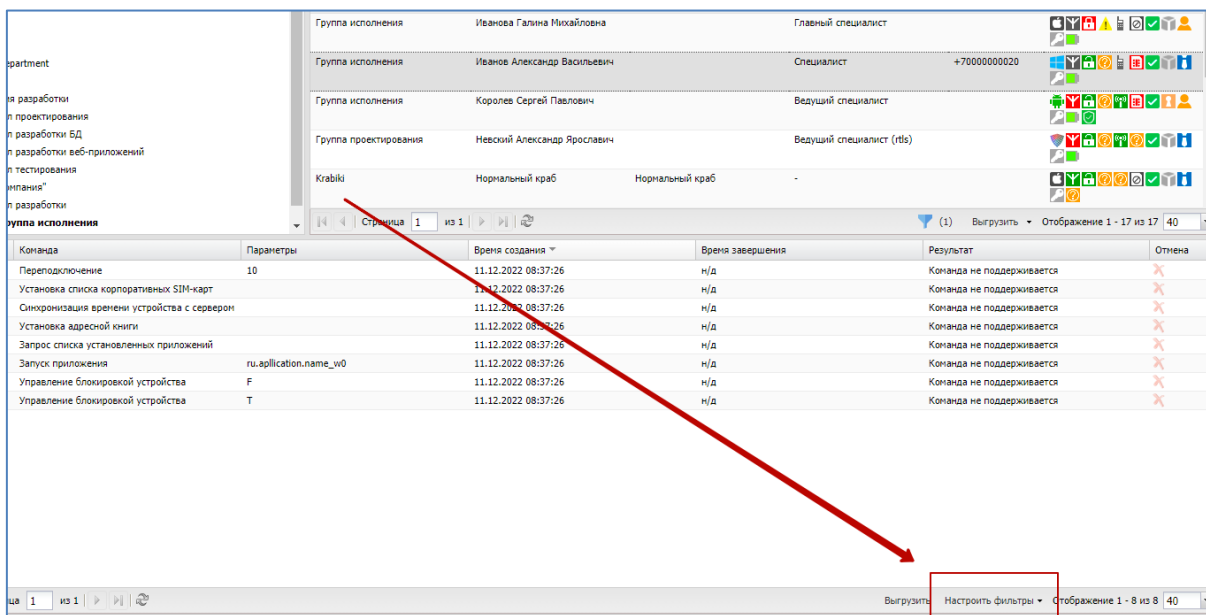
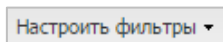


Рисунок 2.45 — Фильтрация действий

Чтобы открыть меню настройки фильтрации списка действий, нажмите кнопку



, после чего отобразятся следующие пункты меню:

Команда — установка флажка позволяет выбрать в появившемся списке команды, которые необходимо отобразить в таблице. В списке присутствуют команды, исключенные из полномочий системы, но сохраненные для обеспечения целостности журнала команд МСК;

Результат — установка флажка позволяет выбрать в появившемся списке результаты выполнения команд, которые необходимо отобразить в таблице;

Создано после — установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке действия, созданные после этой даты и времени;

Создано до — установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке действия, созданные до этой даты и времени;

Завершено после — установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке действия, завершённые после этой даты и времени;

Завершено до — установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке действия, завершённые до этой даты и времени.

По умолчанию в таблице показываются все действия без фильтрации (флажки в раскрывающемся меню «**Настроить фильтры**» сняты).

Перечень команд и описание их параметров приведены в п. 2.6.7.

Отправка команд на устройства осуществляется Администратором посредством раздела главного меню «**Команды**», описание которого приведено в п. 2.6.7.

2.6.6 Раздел «События»

Раздел «События» предназначен для просмотра журнала событий на выбранном МСК. Информационная таблица раздела «События» содержит следующие столбцы (рисунок 2.46):

Отдел/Группа	Сотрудник	Пользователь домена	Должность	Телефон	id	Статус
ash	ash ash	-	-	-	128	[Icons]
ash	ash ash	-	-	-	124	[Icons]
VZ	z v	-	-	-	125	[Icons]
Группа исполнения	Иванов Александр Васильевич	-	Специалист	+7000000020	106	[Icons]
Группа проектирования	Неволей Александр Ярославич	-	Ведущий специалист (HIS)	-	114	[Icons]
Группа исполнения	Паустовский Константин Георгиевич	-	Ведущий специалист	+7000000015	112	[Icons]
Группа проектирования	Прицаев Михаил Михайлович	-	Ведущий специалист	+7000000016	113	[Icons]
Группа проектирования	Сидоров Василий Петрович	-	Специалист	-	105	[Icons]

Порядок	Событие	Описание	Время
209	Подключение МСК		28.02.2024 08:43:58
208	Отключение МСК		28.02.2024 08:43:15
124	Нажатие тревожной кнопки		28.02.2024 08:43:15
123	Нажатие тревожной кнопки		28.02.2024 08:43:06
122	Время на МСК истекло		28.02.2024 08:42:49
121	МСК разблокировано		28.02.2024 08:41:40
120	МСК заблокировано		28.02.2024 08:41:31
119	Установка приложения	Приложение: Приложение n 0, версия 1.0, UID: ru.application.name_v0	28.02.2024 08:41:31
118	Состояние заряда батареи на МСК	Уровень заряда батареи МСК=80, Зарядка=Нет	28.02.2024 08:41:31
117	Подключение МСК		28.02.2024 08:41:31
116	Отключение МСК		28.02.2024 08:41:22
31	Состояние заряда батареи на МСК	Уровень заряда батареи МСК=90, Зарядка=Нет	28.02.2024 08:41:22
30	Оценка модели МСК	Модель: Hewlett-Packard HP ElitePad 1000 G2	28.02.2024 08:41:22
29	Подключение МСК		28.02.2024 08:41:22

Рисунок 2.46 — Раздел «События»

- Порядок — порядковый номер события в общем журнале событий;
- Событие — тип события;
- Описание — параметры события;
- Время — время и дата регистрации события.

В информационной таблице имеется возможность отображения журнала событий в соответствии с выбранным фильтром (рисунок 2.47).

Рисунок 2.47 — Фильтрация событий

Чтобы открыть меню настройки фильтрации списка событий, нажмите кнопку настройки фильтра (рисунок 2.48), после чего отобразятся следующие пункты меню:

Порядок	Событие	Описание	Время
209	Подключение МСК		28.02.2024 08:43:58
208	Отключение МСК		28.02.2024 08:43:15
124	Нажатие тревожной кнопки		28.02.2024 08:43:15
123	Нажатие тревожной кнопки		28.02.2024 08:43:06
122	Время на МСК изменено		28.02.2024 08:42:49
121	МСК разблокировано		28.02.2024 08:41:40
120	МСК заблокировано		28.02.2024 08:41:31

Страница 1 из 1

Выгрузить (0) Отображение 1 - 14 из 14 | 40

Рисунок 2.48 — Кнопка настройки фильтров

Типы событий — установка флажка позволяет выбрать в появившемся списке типы событий, которые необходимо отобразить в таблице. В списке отображаются только те события, которые хоть раз происходили с МСК;

После — установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке события, произошедшие после этой даты и времени;

До — установка флажка позволяет указать в появившемся календаре дату и время, чтобы отображать в списке события, произошедшие до этой даты и времени.

















По умолчанию в таблице показываются все события без фильтрации (флажки в раскрывающемся меню **«Настроить фильтры»** сняты).















Для выгрузки событий необходимо нажать кнопку **«Выгрузить»** на нижней панели инструментов. Если отчет содержит менее 10000 записей, то выгрузка производится в формате XLSX. Если отчет содержит более 10000 записей, то выгрузка производится в формате CSV. По завершении формирования отчета появится сообщение о готовности отчета, в котором будет необходимо нажать кнопку **«Скачать»**.

















В таблице 2.2 приводится краткое описание событий «UEM SafeMobile».


В столбце «Платформа» указаны значки платформ МСК, для которых актуально указанное событие «UEM SafeMobile».
















Таблица 2.2 — Краткое описание событий











Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Подключение МСК	Нет	   	Подключение МСК к «UEM SafeMobile»	Отсутствуют
Отключение МСК	Нет	   	Отключение МСК от «UEM SafeMobile»	Отсутствуют
Установка приложения	Нет	   	Приложение установлено на МСК	Название приложения, его версия и UID
Удаление приложения	Нет	   	Приложение удалено с МСК	Название приложения, его версия и UID

















Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Запуск монитора на МСК	Да	   	Мобильный клиент SafeMobile запущен на устройстве	Отсутствуют
Состояние заряда батареи на МСК	Нет	   	Отчёт об изменении уровня заряда батареи	Уровень заряда батареи в процентах от уровня полного заряда и признак подключенного ЗУ (Т — подключено, F— не подключено)
SIM-карта изменена	Да	   	На устройстве произошла смена SIM-карты	ICCID/IMSI старой SIM-карты, номер телефона (если определен), ICCID/IMSI новой SIM-карты, признак возможности блокировки МСК (Т — мобильный клиент заблокирует устройство, F— не заблокирует)
Время на МСК изменено	Нет	 	На устройстве изменено значение системного времени	Значение установленного времени (временная метка в миллисекундах от 1970 года по Гринвичу)

















Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Очистка БД от старых подключений	Нет	   	При завершении работы сервера управления SafeMobile (например, при его отключении) все МСК, подключенные к нему, остаются в подключенном состоянии. При следующем запуске сервера управления SafeMobile, эти МСК отмечаются в БД как отключенные (что представляет собой процедуру очистки БД от старых подключений)	Отсутствуют
Несоответствие IMSI/ICCID хранимому в БД	Да	   	Определено, что в БД для данного МСК хранится иной идентификатор SIM-карты	ICCID/IMSI старой SIM, ICCID/IMSI новой SIM
Смена модели МСК	Да	   	Определено, что в БД данному МСК соответствует иная модель устройства	Новая модель МСК
Ошибка при обработке пакета	Да	   	В ходе регистрации события, поступившего от МСК, произошла ошибка (сбой при обработке пакета, отправленного от МСК на сервер управления SafeMobile)	Отсутствуют










Событие		Платформа	Описание	Параметры события
	Событие ИБ			
SIM-карта извлечена	Нет	   	На устройстве произошло извлечение SIM-карты	ICCID/IMSI извлеченной SIM
SIM-карта установлена	Да	   	На устройстве произошла установка SIM-карты	ICCID/IMSI установленной SIM
МСК за пределами домашней сети GSM	Нет		Устройство переместилось за пределы домашней сети GSM (находится в роуминге)	ICCID/IMSI SIM
МСК в пределах домашней сети GSM	Нет		Устройство находится в домашней сети GSM (вернулось из роуминга)	ICCID/IMSI SIM
Принадлежность сети GSM не определена	Нет		Устройство не может определить, находится ли оно в домашней сети или в роуминге. Такая ситуация возможна сразу после установки новой SIM-карты в устройство	ICCID/IMSI SIM с нулевыми значениями
GSM не поддерживается	Нет		На устройстве отсутствует модуль GSM	ICCID/IMSI SIM с нулевыми значениями
МСК заблокировано	Да	   	Блокировка МСК по команде Администратора или применению политик работы с SIM-картами	Признаки блокировки по команде Администратора и по политикам работы с SIM

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
МСК разблокировано	Да	   	Разблокировка (удаленный сброс пароля) МСК по команде Администратора	Признаки блокировки по команде Администратора и по политикам работы с SIM
Сброс МСК к заводским настройкам	Да	   	Сброс МСК к заводским настройкам по команде Администратора «Отключение от управления со сбросом к заводским настройкам»	id и действие с командой удаления данных
Выход МСК из-под управления	Да		Отключение МСК от управления с удалением корпоративных данных средствами «UEM SafeMobile»	Отсутствуют
Взлом устройства	Да	 	Обнаружение признаков взлома (jailbreak — МСК iOS, root — МСК Android) мобильным клиентом SafeMobile. Способ отключения определяется политиками профиля монитора.	Отсутствуют
Изменение UDID устройства	Да	  	Изменение идентификатора при замене устройства в составе зарегистрированного в «UEM SafeMobile» комплекта	UDID старого устройства, UDID нового устройства
Установка профиля управления	Да		Установка профиля управления на МСК	Отсутствуют












Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Включение приложения	Нет		Включение установленного приложения на МСК	Название приложения, его UID, версия, состояние, флаг возможности отключения и удаления приложения
Отключение приложения	Нет		Отключение включенного приложения на МСК	Название приложения, его UID, версия, состояние, флаг возможности отключения и удаления приложения
Создание контейнера	Нет		Создание изолированной области на МСК для корпоративных приложений (данных)	Тип контейнера
Удаление контейнера	Нет		Удаление изолированной области на МСК для корпоративных приложений (данных)	Признак удаления контейнера
Установка приложения в контейнер	Нет		Приложение установлено в контейнер на МСК	Название приложения, его версия и UID
Удаление приложения из контейнера	Нет		Приложение удалено из контейнера на МСК	Название приложения, его версия и UID
Включение приложения в контейнере	Нет		Включение установленного приложения в контейнере на МСК	Название приложения, его UID, версия, состояние, флаг возможности отключения и удаления приложения
Отключение приложения в контейнере	Нет		Отключение включенного приложения в контейнере на МСК	Название приложения, его UID, версия, состояние, флаг возможности отключения и удаления приложения
Подтверждение пользовательского соглашения	Нет	 	Пользователь подтвердил согласие с условиями управления МСК «UEM SafeMobile»	Признак действия с соглашением: соглашение подтверждено / соглашение отклонено











Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Установка профиля	Нет	   	Установка на МСК заданных в профиле настроек ОС	Название профиля
Профиль не установлен (нет значения подстановки)	Нет	  	При установке на МСК настроек ОС произошла ошибка из-за отсутствия значения, заданного в профиле	Название профиля, причина ошибки, подстановка и ее значение
Ошибка формирования профиля (подстановки не соответствуют ограничениям)	Нет	  	При установке на МСК настроек ОС произошла ошибка из-за некорректного значения, заданного в профиле	Название профиля, причина ошибки, подстановка и ее значение
Ошибка установки профиля	Нет	   	При установке на МСК настроек ОС произошла ошибка из-за некорректного значения, заданного в профиле	Название профиля, причина ошибки
Удаление профиля	Нет	   	Удаление с МСК заданных в профиле настроек ОС	Название профиля



Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Ошибка удаления профиля	Нет	   	При удалении с МСК настроек ОС произошла ошибка из-за некорректного значения, заданного в профиле	Название профиля, причина ошибки
Ошибка установки политики	Нет	 	При установке на МСК настроек ОС произошла ошибка из-за некорректного значения, заданного в профиле	Тип профиля, название политики, причина ошибки
Установка конфигурации приложения	Нет	 	Установка на МСК заданных в конфигурации настроек приложения	Наименование ПУН (при наличии), UID ПУН, название КП
Ошибка формирования конфигурации приложения (подстановки не соответствуют ограничениям)	Нет	 	При установке на МСК настроек приложения произошла ошибка из-за некорректного значения, заданного в конфигурации	Наименование ПУН (при наличии), UID ПУН, название КП, причина ошибки, значение настройка, подстановка и ее значение
Ошибка установки конфигурации приложения	Нет	 	При установке на МСК настроек приложения произошла ошибка из-за некорректного значения, заданного в конфигурации	Наименование ПУН (при наличии), UID ПУН, название КП, причина ошибки
Удаление конфигурации приложения	Нет	 	Удаление с МСК заданных в конфигурации настроек приложения	Наименование ПУН (при наличии), UID ПУН, название КП
Ошибка удаления конфигурации приложения	Нет	 	При удалении с МСК настроек приложения произошла ошибка из-за некорректного значения, заданного в конфигурации	Наименование ПУН (при наличии), UID ПУН, название КП, причина ошибки













Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Активация лицензии Knox	Нет		Активация лицензии Knox на МСК посредством введения Knox ключей	Лицензия Knox активирована
Ошибка активации лицензии Knox	Нет		При активации лицензии Knox на МСК произошла ошибка при вводе ключа или пользователь МСК отклонил действие. Ошибка возникает также при отсутствии доступа к серверам Samsung	Причина ошибки
Ошибка создания контейнера	Нет		При создании контейнера на МСК произошла ошибка или пользователь отклонил действие. Если на МСК Samsung был установлен Knox warranty bit в результате проведения заводской прошивки, то создание контейнера будет невозможно, и в APM администратора отобразится ошибка	Тип контейнера, причина ошибки
Ошибка установки приложения	Нет	 	При установке приложения на МСК возникла ошибка	Название приложения, его версия и UID, причина ошибки
Ошибка удаления приложения	Нет	 	При удалении приложения с МСК возникла ошибка	Название приложения, его версия и UID, причина ошибки
Ошибка установки приложения в контейнер	Нет		При установке приложения в контейнер МСК возникла ошибка	Название приложения, его версия и UID, причина ошибки
Ошибка удаления приложения из контейнера	Нет		При удалении приложения из контейнера МСК возникла ошибка	Название приложения, его версия и UID, причина ошибки





Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Применение правила управления приложением	Нет	 	Применение правила управления приложением	Название приложения, его UID
Ошибка применения правила управления приложением	Нет	 	При применении правила управления приложения возникла ошибка	Название приложения, его UID, причина ошибки
Удаление правила управления приложением	Нет	 	Удаление правила управления приложением	Название приложения, его UID
Ошибка удаления правила управления приложением	Нет	 	При удалении правила управления приложения возникла ошибка	Название приложения, его UID, причина ошибки
Регистрация IP адреса	Нет	 	Определение IP адреса в сети сотового оператора	Название сотового оператора, IP адрес
Ошибка валидации Knox ключей	Нет		При валидации ключей произошла ошибка из-за некорректного значения ключа	Причина ошибки
Приложение не может быть добавлено в киоск	Нет	 	При добавлении приложения в киоск произошла ошибка	Название приложения, его версия и UID, причина ошибки
Пуш токен недействителен	Нет		Не поступают уведомления из-за некорректного значения пуш токена	Причина ошибки
Нет движения	Нет		На устройстве отсутствует информации о передвижении	

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Ошибка синхронизации	Нет		При получении устройством профиля/ПУП/КП произошла ошибка	Устройство / контейнер, причина ошибки
Ошибка скачивания приложения	Нет		При скачивании корпоративного приложения возникла ошибка	Название приложения, его версия и UID, причина ошибки
Ошибка определения SIM-карты	Нет		При определении параметров SIM карты возникла ошибка	Причина ошибки
Запрос SafeStore на установку приложения	Нет	 	Пользователь через приложение SafeStore запросил установку приложения	Название приложения, его UID.
Запрос SafeStore на удаление приложения	Нет	 	Пользователь через приложение SafeStore запросил удаление приложения	Название приложения, его UID.
Загрузка приложения	Нет		В процессе применения ПУП монитор скачивает корпоративное приложение	Название приложения, его версия и UID
Первая SIM зарегистрирована как корпоративная	Нет	 	В соответствии с политикой профиля настроек монитора первая установленная SIM карта зарегистрирована как корпоративная	IMSI: {{IMSI}}, ICCID: {{ICCID}}
Ошибка подключения к серверу	Нет		При подключении монитора к серверу системы произошла ошибка	Тип сервера, URL сервера, причина ошибки
Старт МСК	Нет	 	Время старта МСК	Дата и время

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Смена сотрудника	Нет		Событие фиксируется при смене сотрудника (владельца устройства).	Прежний сотрудник: ФИО, новый сотрудник: ФИО
Ошибка проверки настроек сбора местоположений	Нет		Монитор не смог получить доступ для чтения настроек сбора местоположений	Причина ошибки
Ошибка включения сервиса определения местоположения	Нет		Монитор не смог получить доступ для включения сервиса сбора местоположений	Причина ошибки
Обновление ОС	Нет		При успешном обновлении ОС по команде "Установить последнее обновление ОС"	Отсутствуют
Ошибка обновления ОС	Нет		В случае ошибки при выполнении команды "Установить последнее обновление ОС"	Причина ошибки
Обнаружено несоответствие	Да		К устройству было применено правило несоответствия	Наименование правила несоответствия
Несоответствие устранено	Да		Несоответствие устройства было устранено	Наименование правила несоответствия
Запрос сертификата авторизации устройства	Да	  	Устройство запросило сертификат авторизации устройства (mTLS) для подключения к системе	Отсутствуют

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Смена сертификата авторизации устройства	Да	  	Сертификат авторизации устройства (mTLS) был перевыпущен	Отсутствуют
Ошибка получения сертификата аутентификации устройств	Да	  	При получении сертификата авторизации устройства (mTLS) произошла ошибка	Причина ошибки
Комплект отключен (устройство зарегистрировалось повторно)	Нет	  	Устройство было подключено к системе, затем сброшено к заводским настройкам сотрудником (без отключения от управления). При повторной регистрации устройства прежний комплект будет переведен в статус "Отключен от управления"	Идентификатор нового комплекта на который зарегистрировано устройство
Установка профиля управления iOS	Нет		Установка профиля управления на устройство iOS	
Ошибка установки профиля управления iOS	Нет		При установке профиля управления на устройство iOS произошла ошибка	Причина ошибки
Первая SIM зарегистрирована как привязанная	Нет		В соответствии с политикой профиля настроек монитора первая установленная SIM карта зарегистрирована как корпоративная	IMSI, ICCID
МСК разблокировано паролем	Да		Состояние блокировки устройства было снято вводом пароля	Отсутствуют

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Статистика использования устройства	Да		Отправляется Раз в сутки в соответствии политиками профиля "Регистрация активности сотрудников Android"	Отсутствуют
Автоматическая маркировка	Да	  	При регистрации устройства сработало правило автоматической маркировки. На комплект проставлены метки, заданные в правиле	Наименование правила автоматической маркировки
Ошибка сброса к заводским настройкам	Да		При отключении от управления со сбросом к заводским настройкам произошла ошибка	Причина ошибки
Ошибка выпуска сертификата	Да	  	При отключении от управления со сбросом к заводским настройкам произошла ошибка	Причина ошибки
Успешная аутентификация	Да		При успешной аутентификации	Отсутствуют
Неудачная попытка аутентификации	Да		При не успешной аутентификации	Номер текущей неуспешной попытки входа
Ошибка ввода пароля выхода из киоска	Да		Ввод не верного пароля, при выходе из режима «Киоск».	Номер текущей неуспешной попытки ввода пароля
Исчерпано количество попыток ввода пароля выхода из киоска	Ла		Ввод не верного пароля 15 раз подряд, при выходе из режима «Киоск».	Отсутствуют

Событие		Платформа	Описание	Параметры события
	Событие ИБ			
Разблокирована учетная запись администратора устройства	Да	 	Разблокировка учетной записи администратора устройства.	Отсутствуют
Заблокирована учетная запись администратора устройства	Да	 	Заблокирована учетная запись администратора устройства	Отсутствуют

2.6.7 Раздел «Команды»

Раздел «**Команды**» предназначен для отображения списка команд и отправки требуемой команды на выбранное устройство.

Для отправки команды необходимо выбрать МСК в главной таблице, затем пункт меню «**Команда**» и требуемую команду в информационной таблице в соответствии с рисунком Рисунок 2.49.

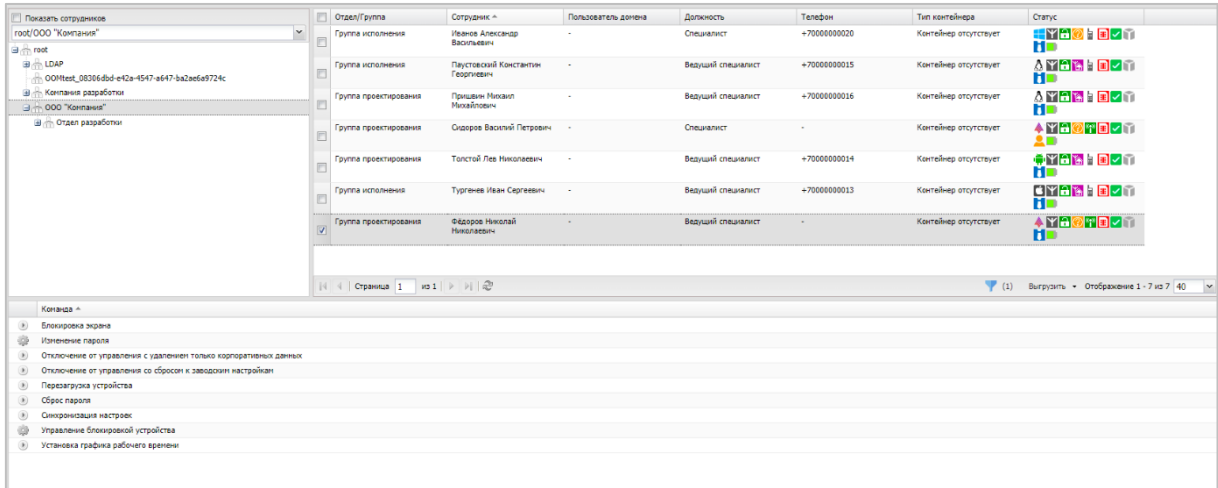


Рисунок 2.49 — Раздел «Команды»

Примечание

На выполнение команды может быть наложено ограничение в разделе «Объекты учета — Ограничения администратора». См. раздел 2.8.5

Если команда выполняется без параметров, слева от названия команды отображается значок . Для отправки команды на устройство необходимо нажать этот значок, после чего в появившемся окне уведомления нажать кнопку «**ОК**» (рисунок 2.50).

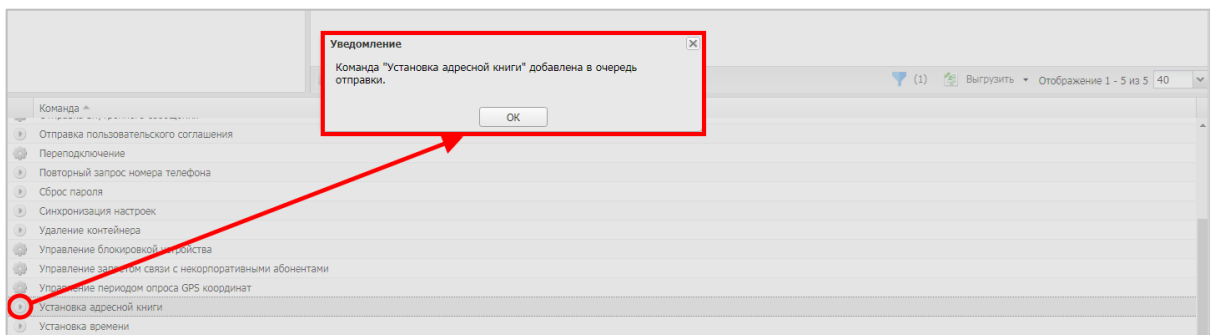



Рисунок 2.50 — Отправка команды без параметров

Если для выполнения команды требуется указать ее параметры, слева от названия команды отображается значок  (рисунок 2.51).

Для отображения параметров команды следует нажать этот значок, после чего в правой части таблицы появится перечень параметров команды. Чтобы отправить команду, установите требуемые значения параметров, нажмите кнопку **«Отправить»**, затем кнопку **«ОК»** в появившемся окне уведомления.



Рисунок 2.51 — Отправка команды с параметрами

Результат выполнения команды отображается в разделе главного меню **«Действия»**. В этом разделе можно также выполнить отмену отправленной на устройство команды. Если выполнение команды прошло успешно, в столбце **«Результат»** отобразится значение **«Нормальное завершение»**. В противном случае, будет отображена причина невыполнения команды.




Полный перечень возможных ошибок и их описание приведен в приложении Б.









В таблице 2.3 приводится краткое описание команд системы.







В столбце «Платформа» таблицы 2.3 указаны значки платформ МСК, для которых актуальна указанная команда системы.

Администратор может отправить из раздела главного меню «Установленные приложения» команды по работе с приложениями.









Таблица 2.3 — Краткое описание команд




Команда	Платформа	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
Управление блокировкой устройства	  	<p>При получении команды «Заблокировать устройство» осуществляется полная блокировка устройства с отображением сообщения о блокировке и передаче устройства администратору для разблокировки. Команда выполняется на устройствах в режиме Supervised, на других устройствах результатом выполненной команды будет «Нарушение защиты ОС».</p> <p>При получении команды «Заблокировать устройство» осуществляется блокировка доступа к пользовательскому интерфейсу МСК. Команда не выполняется на устройствах с действующими стратегиями КРП и ЛРП. Результатом выполнения команды на этих устройствах будет «Выполнение команды невозможно».</p> <p><i>Для Android:</i></p> <ul style="list-style-type: none"> • Если команда была дана к устройству, находящемуся в состоянии временной разблокировки (30 минут с момента ввода пароля разблокировки на МСК), то результатом выполнения команды будет ошибка «Устройство находится в режиме принудительной разблокировки». • Текст, отображаемый на экране заблокированного устройства может быть задан в политике «Текст на экране блокировки, отображаемый в случае блокировки устройства командой администратора» профиля «Настройки монитора Android». По умолчанию будет отображаться текст «Устройство заблокировано администратором». 	Заблокировать устройство	.T








Команда	Платформа	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
	  	<p>При получении команды «Разблокировать устройство» осуществляется разблокировка устройства. Команда выполняется на устройствах с Supervised.</p> <p>При получении команды «Разблокировать устройство» осуществляется снятие блокировки доступа к пользовательскому интерфейсу МСК.</p> <p><i>Для Android:</i> Если команда была дана к устройству, находящемуся в состоянии временной разблокировки (30 минут с момента ввода пароля разблокировки на МСК), то результатом выполнения команды будет ошибка «Устройство находится в режиме принудительной разблокировки».</p>	Разблокировать устройство	F
Блокировка экрана	  	<p>При получении команды осуществляется блокировка экрана паролем пользователя.</p> <p><i>Для Android:</i> Если команда была дана к устройству, находящемуся в состоянии временной разблокировки (30 минут с момента ввода пароля разблокировки на МСК), то результатом выполнения команды будет ошибка «Устройство находится в режиме принудительной разблокировки».</p>	Отсутствуют	
Запрос журналов Монитора	 	<p>На устройство (в том числе и на заблокированное) отправляется команда запроса системных логов устройства. После отправки команда встает в очередь на выполнение. Результатом работы команды является архив данных, который можно скачать в разделе «Информация об устройстве», в блоке «Журналы Монитора». Состав логов может быть задан в профиле «Настройки журналов Android». Подробное описание работы команды в руководстве «Инструкция по выгрузке логов».</p>	Отсутствуют	







Команда	Платформа	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
Переподключение		На устройство отправляется команда отключения и подключения заново мобильного клиента к серверу SafeMobile	Промежуток времени, указывающий, через сколько секунд МСК подключится к серверу заново после выполнения этой команды	
Установка списка разрешенных SIM-карт		На устройство отправляется актуальный список идентификаторов SIM, хранящихся в БД SafeMobile. Это действие применяется для обеспечения корректной работы устройств с установленной политикой смены SIM-карт	Отсутствуют	
Установка графика рабочего времени	  	На МСК отправляется команда установки графика рабочего времени для сотрудника-абонента МСК	Отсутствуют	
Синхронизация времени устройства с сервером*		На устройство отправляется команда установки текущего времени на сервере SafeMobile. <i>Если команда была дана к устройству, находящемуся в состоянии временной разблокировки (30 минут с момента ввода пароля разблокировки на МСК), то результатом выполнения команды будет ошибка «Устройство находится в режиме принудительной разблокировки».</i>	Отсутствуют	



* Команда актуальна для МСК производства Samsung до Android 11 включительно, а также для устройств Android начиная с версии– 9.0 при наличии у монитора прав DO или корпоративного рабочего профиля.

Команда	Платформа	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
Отключение от управления с удалением только корпоративных данных**	   	<p>На МСК отправляется команда отключения от управления средствами «UEM SafeMobile». В результате выполнения команды на МСК будет удалён профиль управления (на устройствах платформы iOS), а также все настройки (параметры Wi-Fi точек доступа, запрещающие правила доступа к интерфейсам, парольные политики, контейнер) и приложения, установленные «UEM SafeMobile». Личные данные сотрудника сохраняются.</p> <p><i>Для Android:</i></p> <ul style="list-style-type: none"> Если команда была дана к устройству, находящемуся в состоянии временной разблокировки (30 минут с момента ввода пароля разблокировки на МСК), то результатом выполнения команды будет ошибка "Устройство находится в режиме принудительной разблокировки". <p><i>После выполнения данной команды монитор останется с отключенным функционалом. Если приложение «Монитор» имел права Device Owner, пользователь не сможет удалить «Монитор» ничем кроме сброса к заводским настройкам. Если требуется удалить «Монитор» с правами Device Owner, рекомендуется отправлять команду «Отключение от управления со сбросом к заводским настройкам».</i></p>	Отсутствуют	
Отключение от управления со сбросом к заводским настройкам***	   	<p>На МСК отправляется команда отключения от управления средствами «UEM SafeMobile». В результате выполнения команды на МСК будут удалены корпоративные и личные данные (настройки, журналы звонков и сообщений, файлы, приложения, контейнер)</p> <p><i>Для Windows:</i></p> <ul style="list-style-type: none"> При наличии шифрования диска МСК с данными для ОС Windows 10. 	Отсутствуют	

Команда	Платформа	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
		<p><i>Для Android:</i></p> <ul style="list-style-type: none"> Если мобильный клиент Android не успел сообщить серверу об успешном завершении команды, тогда команда с результатом "Команда доставлена, ожидается результат" останется в системе на срок до 90 суток и будет удалена при периодической очистке БД. При повторном подключении устройства посредством КМЕ в указанный период команда отобразится с результатом «Нормальное завершение». Важно! На устройствах Samsung под управлением Android 14 (API 34, Кнох API 37) и выше команда не будет выполнена, если монитору назначены привилегии Device Administrator и KNOX! 		
Сброс пароля	 	<p>На устройство отправляется команда сброса пароля. Если к устройству платформы Android уже предъявлены требования парольной политики, а именно: минимальная длина пароля и категория сложности, перед сбросом пароля эти требования следует отменить. На МСК с ОС Android версий 8.0 и 8.1 команда не поддерживается производителем Samsung.</p> <p><i>Для Android:</i> Если команда была дана к устройству, находящемуся в состоянии временной разблокировки (30 минут с момента ввода пароля разблокировки на МСК), то результатом выполнения команды будет ошибка «Устройство находится в режиме принудительной разблокировки».</p>	Отсутствуют	
Изменение пароля		На устройство отправляется команда изменения текущего пароля на полученный.	Новый пароль	

Команда	Платформа	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
		<p>На MCK с ОС Android версий 8.0 и 8.1 команда не поддерживается производителем Samsung.</p> <p><i>Для Android:</i> Если команда была дана к устройству, находящемуся в состоянии временной разблокировки (30 минут с момента ввода пароля разблокировки на MCK), то результатом выполнения команды будет ошибка «Устройство находится в режиме принудительной разблокировки».</p>		
Изменение пароля контейнера		На устройство отправляется команда изменения текущего пароля контейнера на полученный новый пароль	Новый пароль	
Отправка пользовательского соглашения.	 	На устройство отправляется пользовательское соглашение по управлению MCK «UEM SafeMobile»	Отсутствуют	Порядковый номер пользовательского соглашения
Перезагрузка устройства	  	<p>На устройство отправляется команда перезагрузки устройства. Если устройство находится в состоянии звонка, то перезагрузка произойдет:</p> <ul style="list-style-type: none"> • после его окончания (для Android и iOS); • во время звонка (для Аврора). <p>Для Android — устройство должно удовлетворять требования:</p> <ul style="list-style-type: none"> • Android 7+ и наличие привилегии Device Owner или NKOX. <p>Для iOS — устройство должно работать в режиме Supervised.</p>	Отсутствуют	
Удаление контейнера		На устройство отправляется команда удаления изолированной области с корпоративными приложениями и данными.	Отсутствуют	

Команда	Платформа	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
Синхронизация настроек		На устройство отправляются актуальные настройки ОС и приложений, заданные в профилях и конфигурациях	Отсутствуют	
Повторный запрос номера телефона		МСК, получив команду, отправляет сообщение на номер телефона, заданный в профиле настроек монитора. По полученному сообщению, автоматически определяется номер телефона. На МСК, определяющий номер телефона, должен быть назначен профиль настроек монитора с политикой «Регистрировать SMS» = Да.	Отсутствуют	
Отправить файл	 	На устройство отправляется файл. По получении пользователь уведомляется и файл выкладывается в папку «Загрузки». Примечание <i>Для отправки файла на устройства IOS следует назначить ПУП для приложения EMM Client.</i>	Файл, предназначенный для отправки.	
Установить последнее обновление ОС		Команда позволяет установить последнее доступное для устройства обновление ОС. Примечание <i>Для устройств IOS, работающих в режиме unsupervised, нормальным результатом работы команды является оповещение «Команда не поддерживается».</i>	Отсутствуют	
Отправка уведомлений		Команда позволяет отправить на устройство уведомление, которое будет отображаться в модальном окне, поверх других окон устройства. По умолчанию заголовок уведомления «Уведомление от администратора SafeMobile»	Заголовок уведомления (не более 512 символов). Текст уведомления (не более 10 кб).	

Команда	Платформа	Описание	Параметр команды	
			В разделе «Команда»	В разделе «Действия»
Очистка данных приложения		Удаляет временные файлы (кэш), собранные приложением. Данные авторизации на сайтах (логины, пароли, cookies) очисткой не затрагиваются.	UID приложения	
Инвентаризация		При получении команды мобильное устройство (Android) отправляет на сервер промежуточный ответ о доставке и ожидании результата, затем выполняет сбор всех актуальных параметров инвентаризации, отправляет эти данные на сервер через специализированное событие инвентаризации и финализирует процесс отправкой итогового отчета о выполнении команды.	Отсутствуют	

2.6.8 Именованные команды

Раздел меню «Именованные команды» позволяет администратору применить одну команду сразу к нескольким устройствам, отвечающим требованиям. На одну команду может быть назначено подразделение применения в дереве ОШС и заданы условия применения.

Примечание

На применение именованной команды может быть наложено ограничение в разделе «Объекты учета — Ограничения администратора». См. раздел 2.8.5

Доступ к разделу определяется следующими полномочиями администратора:

- Просмотр команд.
- Добавление команд — доступна только при наличии полномочия «просмотр».
- Изменение команд — доступна только при наличии полномочия «просмотр».
- Удаление команд — доступна только при наличии полномочия «просмотр».
- Просмотр назначений команд — доступна только при наличии полномочия «просмотр».
- Изменение назначений команд — доступна только при наличии полномочия «просмотр» и «просмотр назначений».
 - Изменение назначений команд в дереве ОШС.
 - Изменение назначений команд в списке комплектов.
- Смена владельца команд.
- Отправка команд — доступна только при наличии полномочия «просмотр».
 - Состав полномочий должен быть идентичен разделу полномочий: «Управление устройствами — Команды». За исключением команды отправка логов.

Главный экран раздела отображает список заданных «Именованных команд» (рисунок 2.52) где каждая строка списка содержит следующие данные:

- Наименование — наименование «Именованной команды»;
- Платформа — ОС устройств на которых запускается команда;
- Команда — команда (из раздела «Команды») которая будет отправлена на

устройства;

- Владелец — владелец команды. Администратор может видеть только именованные команды, владельцы которых находятся в пределах его области управления.

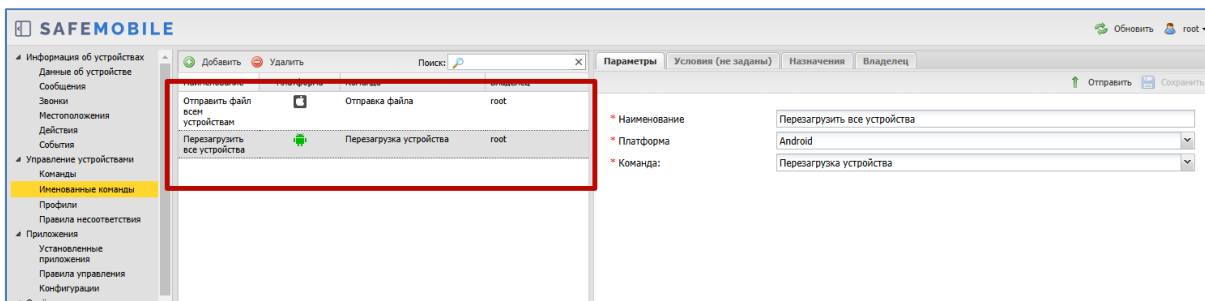


Рисунок 2.52 — Раздел «Именованные команды»

В верхней части рабочего экрана находятся кнопки:

- Добавить — добавить новую «Именованную команду»;
- Удалить — удалить существующую «Именованную команду», выбранную в списке.

Правая часть рабочего экрана отображает настройки «Именованной команды», выбранной в списке.

- Вкладка «Параметры»:
 - Наименование — название «Именованной команды»;
 - Платформа — ОС устройств на которых будет запускаться команда;
 - Команда — команда (из раздела «Команды») которая будет отправлена на устройства (кроме команды «Запрос журналов Монитора»);
 - Атрибуты команды. Например при выборе команды «Отправка файла» будет отображаться кнопка для загрузки файла. Полное описание работы команд см. в разделе 2.6.7 «Команды».
 - Кнопка «Сохранить» — при нажатии сохраняет новую команду или внесенные изменения в ее настройки;
 - Кнопка «Отправить» — при нажатии система запросит подтверждение действия, после чего отправляет сохраненную «Именованную команду» на устройства указанные во вкладке «Назначение». Если в одной из вкладок есть не сохраненные данные, то кнопка будет не доступна;
- Условия — содержит описание условий, при выполнении которых, команда

будет выполнена. Если ни одно из условий не задано, то команда выполняется безусловно;

- Назначения — назначение подразделения в дереве ОШС для которого будет выполняться команда.
- Владелец — позволяет сменить владельца команды выбрав его в дереве ОШС.

Для создания новой «Именованной команды» необходимо выполнить следующие действия:

1. Нажать кнопку «Добавить».
2. В правой части рабочего экрана заполнить обязательные поля параметров команды:
 - Наименование,
 - Платформа,
 - Команда и сопутствующие настройки выбранной команды,
3. Задать необходимые настройки во вкладках «Условия», «Назначения», «Владелец».
4. Нажать кнопку «Сохранить», после чего команда будет готова к отправке на устройства.

Для удаления команды следует выбрать ее в списке «Именованных команд», нажать кнопку «Удалить» и подтвердить свое действие в модельном запроса подтверждения.

2.6.9 Раздел «Профили»

Пункт меню «**Профили**» открывает окно (рисунок 2.53), предназначенное для создания, редактирования и удаления профилей, а также осуществления их назначений на МСК, сотрудника или подразделение.

В левой части окна «**Профили**» отображается форма с реестром созданных в системе профилей, таблица реестра содержит следующие столбцы:

- **Наименование** — название профиля (используется при поиске в таблице);
- **Тип** — разновидность политик ОС (используется при поиске в таблице);
- **Платформа** — платформа ОС;
- **Сущность** — инициатор сущности (собственный/делегированный);
- **Владелец** — узел ОШС, назначенный владельцем сущности (по умолчанию, не отображается, используется при поиске в таблице).

В правой части окна отображается форма для настройки параметров профиля с вкладками:

- **Политики** — содержит набор правил или настроек, в соответствии с которыми производится настройка рабочей среды устройства.
- **Условия/Условия (не заданы)** — содержит описание условий, при выполнении которых, политики профиля будут применены к устройству. Если ни одно из условий не задано политики профиля применяются безусловно.
- **Назначения** — содержит указание подразделения, пользователей или комплекты, на которые будет применен данный профиль. Если в «назначении» ничего не выбрано, профиль не будет применен;
- **Владелец** — содержит функционал назначения узла ОШС как владельца профиля. Каждый профиль принадлежит одному владельцу. Администратор узла «владельца» (а также, администратор вышестоящего узла ОШС) имеет права на редактирование настроек профиля;
- **Делегирование** –позволяет делегировать назначение профиля администраторам подчиненных подразделений.

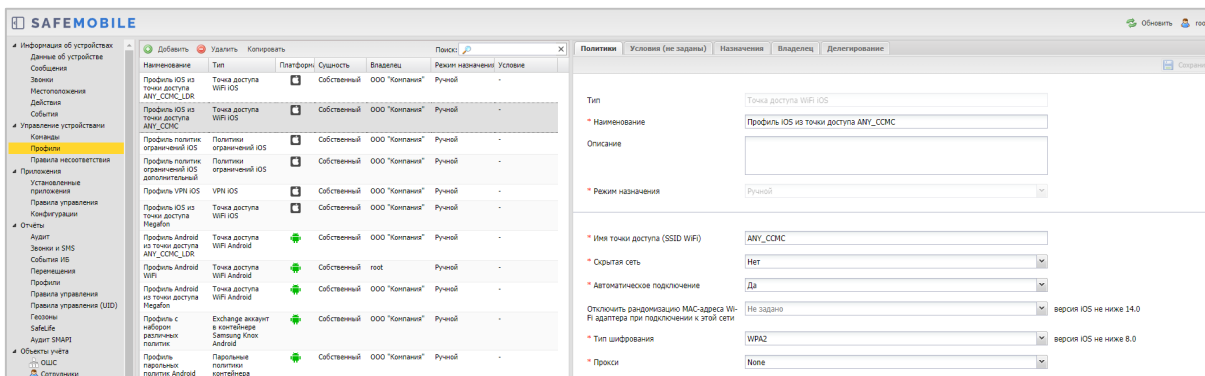


Рисунок 2.53 — Окно «Профили»

В верхней части таблицы находится панель инструментов со следующими кнопками:

- Добавить — предназначена для создания нового профиля;
- Удалить — предназначена для удаления уже созданного профиля;
- Копировать — предназначена для создания копии существующего профиля.

Примечание

С описанием политик ограничений от производителей устройств можно ознакомиться по ссылкам:

Для iOS:

<https://support.apple.com/ru-ru/guide/deployment/dep0f7dd3d8/1/web/1.0>

Для Android:

https://support.google.com/work/android/answer/9560920?hl=ru&ref_topic=9563482&sjid=14159055154926870826-EU#zippy=%2Срасширенные-функции

2.6.9.1 Создание профиля

Копирование существующего профиля

Для копирования существующего профиля необходимо выделить в списке профиль для копирования и нажать кнопку «Копировать», после чего будет создан идентичный профиль, кроме следующих изменений:

- Новый профиль будет иметь наименование исходного профиля, с добавлением слова «Копия» в начале наименования (Например «Копия Профиль iOS из точки доступа»);
- Копия не содержащий параметры «Условия» и «Назначения» исходного профиля.

Создание профиля с помощью кнопки «Добавить»

Для добавления нового профиля в реестр нажмите кнопку «Добавить», после чего появится всплывающее окно «Создание профиля» с перечнем типов профилей и иконками платформ в соответствии с рисунком 2.54.

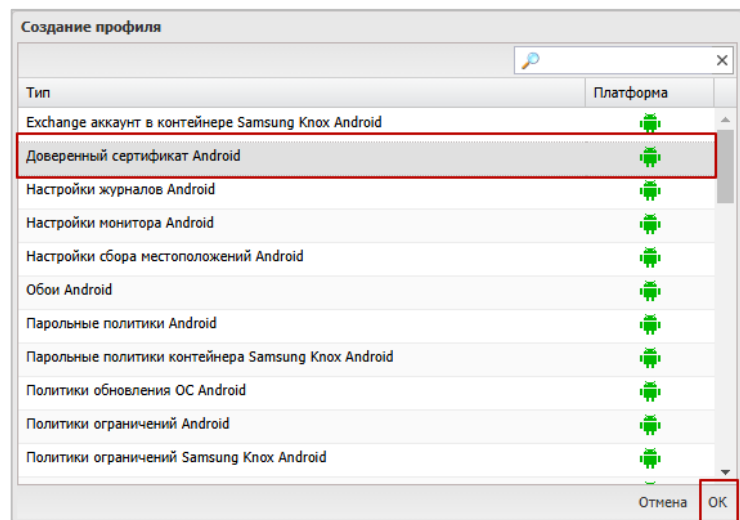


Рисунок 2.54 — Создание профиля

В системе поддерживаются следующие типы профилей:

- **Платформа Android:**
 - Exchange аккаунт в контейнере Samsung Knox Android — (работает с ЛРП и КРП);
 - Доверенный сертификат Android — (работает с ЛРП и КРП);

- Настройки автоматического отключения Android — (работает без ограничений). Профиль задает параметры автоматического отключения устройства от управления при длительном отсутствии связи с сервером. Ограничений по КРП и ЛРП нет. Но в ЛРП, будет выполнен не сброс к заводским настройкам, а только удаление рабочего профиля.;
- Настройки автоматической перезагрузки Android — Профиль задает разрешение автоматической перезагрузки устройства и ее и расписание;
- Настройки журналов Android — (работает без ограничений). Профиль определяет состав и объем логов собираемых «Монитором» для журналов трех типов:
 - журнал «Монитора»,
 - журнал событий безопасности,
 - журнал сетевых событий,
- Настройки монитора Android — (работает с ЛРП и КРП);
- Настройки сбора местоположений Android — (работает с КРП);

Примечание

Информация об источнике получения данных:

- *Точность и стабильность доставки координат монитору зависят от вендора устройства.*
- *«Только GPS» данные будут передаваться как в режиме низкого энергопотребления, так и в других режимах. Если на устройстве нет датчика GPS (физически), никакой ошибки возникать не будет, но БД не будет получать информацию о перемещении.*
- *В режиме работы стандартного api (не GMS) на версии 12+ в профиль можно передать показатель точности, но гарантия того, что координаты будут возвращены при вызове Монитору, есть только при выборе режима «высокого энергопотребления».*
- *В режиме работы, который использует стандартный api (не GMS) на версиях 11 и ниже, гарантию доставки параметром в профиле задать нельзя. На этой версии единственный способ получать данные местоположения —*

выбрать «Только GPS» или «... по нескольким источникам и GMS».

- *Местоположения могут не передаваться, если интервал запроса задан очень маленький. Чтобы повысить шанс приложению «Монитор» получить местоположение при вызове api (при любом источнике) — следует увеличить интервал в «Промежуток времени между попытками получения координат...».*

- Обои Android — (DO (Device Owner) и версия Android не ниже 7.0);
- Парольные политики Android — (работает с ЛРП и КРП);
- Парольные политики контейнера Samsung Knox Android;
- Политики обновления ОС Android — (работает с КРП, см. «примечание ****»);
- Политики ограничений Android — (работает с ЛРП и КРП);
- Политики ограничений Samsung Knox Android;
- Политики ограничений контейнера Samsung Knox Android;
- Политики смены сотрудника на устройстве Android — работает без ограничений;
- Политики сотовой сети (APN);
- Политики управления датой и временем Android;
- Политики фильтрации событий монитора Android — управление списком событий, отправляемых «Монитором» серверу;
- Регистрация активности сотрудников Android;
- Режим киоска Android;
- Режим киоска Android (устарел);
- Режим киоска Samsung Knox Android (устарел);
- Сертификат для приложений и VPN Android — работает без ограничений;
- Сетевые подключения Android;
- Точка доступа WiFi Android — (работает с ЛРП и КРП);
- Ярлык рабочего стола Android — (работает с ЛРП и КРП).

Примечание

**Для включения возможности входа и выхода из режима «киоск» необходимо:*

1. Назначить устройству профиль «Режим киоска Android»;
2. В настройках профиля «Режим киоска Android» разрешить «Выход из режима киоска по паролю»;
3. Установить пароль для выхода из режима «киоск».

****Для корректной работы ярлыков в режиме киоска, добавленных профилем «Ярлык рабочего стола Android» необходимо учитывать следующее:**

1. Если в профиле ярлыка **задан** «UID веб браузера, в котором необходимо открывать URL...», то этот же UID должен быть добавлен в политику «Список UID'ов отображаемых приложений» профиля «Режим киоска Android», примененного к данному устройству.
2. Если в профиле ярлыка **не задан** «UID веб-браузера, в котором необходимо открывать URL...», то ярлык будет открываться браузером «по умолчанию». Соответственно UID «браузера по умолчанию» должен быть добавлен в политику «Список UID'ов отображаемых приложений» профиля «Режим киоска Android», примененного к данному устройству.

*****Если на устройство назначен профиль парольных политик и текущий пароль устройства не соответствует этим политикам, то устройство блокируется окном смены пароля на пароль, соответствующий назначенным на устройство политикам. Для обеспечения безопасности в этом режиме так же блокируется обмен файлами с устройством и отладка по USB, даже если они не были запрещены политиками ограничений.**

****** Профиль «Политики обновления ОС Android» позволяет настроить отсрочку обновления системы. Обновления могут устанавливаться:**

- Сразу по получении,
- В день получения, но в указанные часы,
- Через 30 дней после получения обновления.

Помимо этого, профиль позволяет задать до 5-ти периодов «заморозки» обновлений в год. Если устройство получит обновление в период заморозки, то обновление будет отложено до завершения периода заморозки. Подобное поведение может быть востребовано для того, чтобы обновление не происходило бесконтрольно в праздничные дни. ОС позволяет отложить обновление не более чем на 90 дней.

Пример: Задана политика отсрочки на 30 дней и получено обновление. До завершения 30-дней, начался 90-дневный период заморозки. Обновление будет

установлено ОС через 90 дней с момента получения обновления. То, что период заморозки еще не завершен будет проигнорировано. Так же есть ограничение на минимальный промежуток времени между двумя периодами заморозки — 60 дней.

- **Платформа iOS:**

- Парольные политики. Требования к паролю доступа к МСК;
- Политики ограничений. Ограничение возможностей ОС и встроенных приложений;
- Exchange аккаунт iOS,
- Настройки автоматического отключения iOS — Профиль задает параметры автоматического отключения устройства от управления при длительном отсутствии связи с сервером.
- Политики сотовой сети (Cellular) iOS,
- Режим киоска iOS,
- Сертификат для браузера Safari iOS,
- Управляемые домены iOS,
- Точка доступа WiFi iOS,
- Доверенный сертификат,
- Настройки монитора iOS,
- Обои iOS,
- Ярлык рабочего стола iOS,
- VPN iOS,
- VPN для приложений (Per-App VPN) iOS,
- Фильтр web контента iOS.

Примечание

- *«Настройки автоматического отключения iOS» — Процедура отключения устройстве запускается планировщиком задач один раз в сутки, после 00:00. Это означает, что команда на отключение будет отправлена не в точный момент истечения таймаута, а во время следующего после этого момента ежедневного запуска.*

Пример:

- *Устройство перестало быть доступным в сети: 12.05.2025 в 12:00;*
- *Политика «Таймаут по истечению которого устройство будет отключено (дней)»: 3 дня;*

- Фактическое время отправки команды на отключение: 16.05.2025 после 00:00 (а не 15.05.2025 в 12:00).

- Политика «Управлять копированием и вставкой через буфер обмена» (1) (для профиля ограничений) работает только совместно с политиками «Разрешить открытие в неуправляемых приложениях документов, ранее открытых в управляемых приложениях» (2) и/или «Разрешить открытие в управляемых приложениях документов, ранее открытых в неуправляемых приложениях» (3).

Значение политики (1)	Значение политики (2)	Копирование данных через буфер обмена из управляемых в неуправляемые
Да	Нет	Запрещено
Да	Да	Разрешено
Да	Не задано	
Нет	Любое	
Не задано	Любое	

Значение политики (1)	Значение политики (3)	Копирование данных через буфер обмена из неуправляемых в управляемые
Да	Нет	Запрещено
Да	Да	Разрешено
Да	Не задано	
Нет	Любое	

	Не задано	Любое		
--	-----------	-------	--	--

- **Платформа Аврора**

- Политики ограничений Аврора,
- Настройки автоматического отключения Аврора — Профиль задает параметры автоматического отключения устройства от управления при длительном отсутствии связи с сервером;
- Настройки монитора Аврора,
- Парольные политики Аврора,
- Политики обновления ОС Аврора,
- Сертификат для приложений Аврора,
- Доверенный сертификат ОС Аврора,
- Точка доступа WiFi Aurora.

Примечание

Платформа «Аврора» существует в двух редакциях:

- *«Сертифицированная»: минимальная длина пароля — 7 символов, пароль генерируется системой.*
- *«Корпоративная»: минимальная длина пароля — 5 символов, пароль задаётся пользователем.*

Поскольку консоль управления (ЕММ) не различает редакции для конечных пользователей, в общей парольной политике установлено требование к минимальной длине 7 символов. Это гарантирует корректную работу для обоих вариантов «Авроры».

- **Платформа Windows**

- Парольные политики,
- Настройки bluetooth,
- Политики сетевых подключений,
- Политики ограничений,

- Политики использования камеры,
- Политики доступа к настройкам,
- Политики Defender,
- Настройки BitLocker.

Примечание

Для устройств производства Samsung:

- *если приложение «Монитор» не имеет привилегий DO или PO, следует применять «политики ограничений Samsung Knox».*

Для всех прочих случаев и устройств других производителей:

- *применять «политики ограничений Android».*

Для продолжения работы следует сделать выбор и нажать на кнопку **«ОК»** или **«Отмена»**. При нажатии на кнопку **«ОК»** откроется новая форма с настройками политик профиля — вкладка **«Политики»**, а созданный профиль отобразится в реестре профилей. При нажатии на кнопку **«Отмена»** окно создания профиля закроется без сохранения изменений.

2.6.9.2 Настройка параметров профиля

В форме настроек политик профиля (рисунок 2.55), следует указать требуемые значения.

Рисунок 2.55 — Форма с настройками политик профиля

Подстановки

В качестве значений строковых параметров можно использовать подстановки. Подстановки — строки специального вида, вместо которых перед применением подставляются персонифицированные данные.

В каждом строковом параметре допускается использование одной или нескольких подстановок.

Ключ подстановки в тексте должен начинаться с префикса «{{» без кавычек, а заканчиваться постфиксом «}}» без кавычек.

Например, для того чтобы значение параметра содержало домен\логин пользователя, нужно указать следующую строку:

{{employee.exchange.emp_email_domain}}\{{employee.exchange.emp_email_login}}

Список ключей подстановок:

- {{employee.surname}} — фамилия сотрудника;
- {{employee.name}} — имя сотрудника;
- {{employee.patronymic}} — отчество сотрудника;

- {{employee.exchange.emp_email}} — email сотрудника;
- {{employee.exchange.emp_email_login}} — логин сотрудника;
- {{employee.exchange.emp_email_domain}} — домен сотрудника;
- {{noncompliance_rule.name}} — наименование правила несоответствия;
- Импортированные атрибуты из LDAP:
 - {{company}},
 - {{department}},
 - {{displayname}},
 - {{distinguishedName}},
 - {{employeeID}},
 - {{givenName}},
 - {{mail}},
 - {{mailNickName}},
 - {{middleName}},
 - {{mobile}},
 - {{name}},
 - {{objectCategory}},
 - {{objectGuid}},
 - {{sAMAccountName}},
 - {{sn}},
 - {{telephoneNumber}},
 - {{title}},
 - {{userPrincipalName}}.

Примечание

- Подстановки могут быть использованы только в политиках типа «Строка» или «Массив строк».
- При отсутствии значения подстановки в необязательной политике подстановка заменяется на пустую строку удаляется из политики, после чего политика обрабатывается как валидная.
- Для обязательных политик отсутствие подстановки интерпретируется как сознательное действие администратора (например, в случае exchange, как отключение пользователя от корпоративной почты) и приводит к следующим действиям:
 - Отмену установки профиля.
 - Событие «Отсутствие значения обязательной политики».

Добавление идентификаторов приложений

Для ряда параметров профилей требуется указать идентификатор(ы) одного или нескольких приложений.

- Политики профиля **«Политики ограничений iOS»**
 - Список идентификаторов приложений, запуск которых разрешен;
 - Список идентификаторов приложений, запуск которых запрещен;

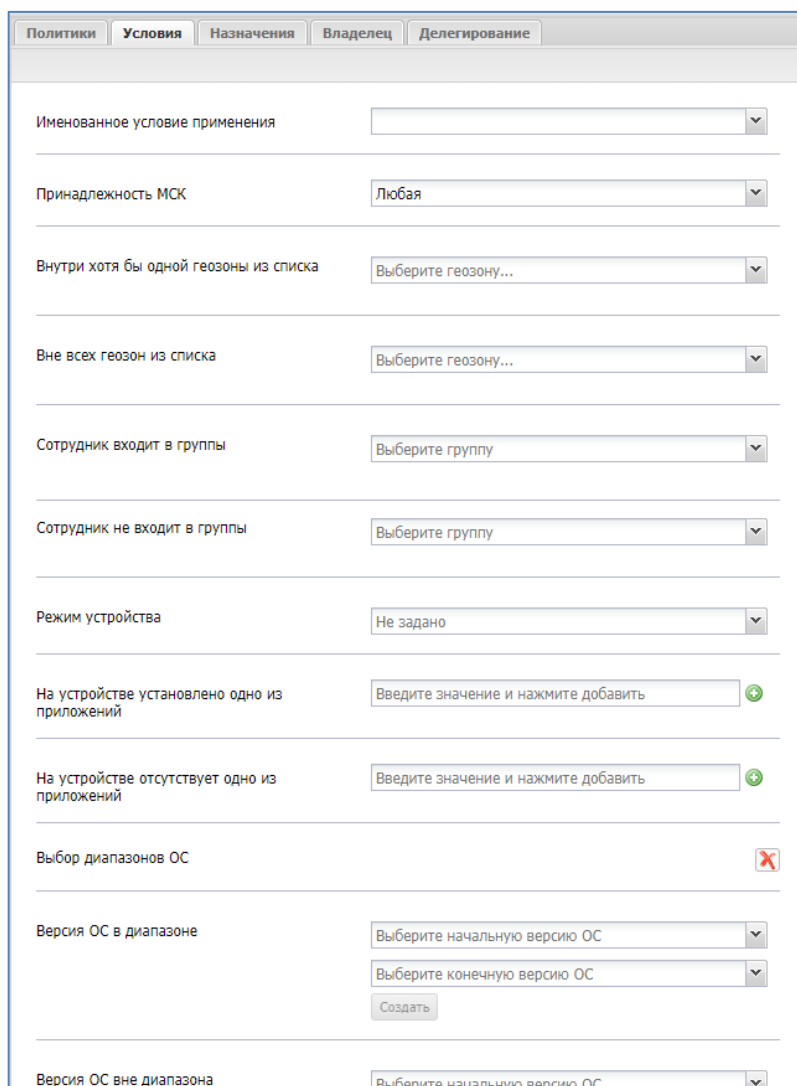
- Условия
 - На устройстве установлено одно из приложений;
 - На устройстве отсутствует одно из приложений.

Узнать идентификатор для конкретного приложения можно в столбце **«UID»** таблицы установленных приложений раздела **«Приложения / Установленные приложения»**.

Узнать идентификатор системного приложения для MCK производства iOS можно в столбце **«iOS Bundle ID»** приложения В.

2.6.9.3 Задание условий применения профиля

После заполнения формы профиля нажать кнопку **«Сохранить»** и, после подтверждения действия, выбрать вкладку **«Условия»** в соответствии с рисунком 2.56.



The screenshot shows the 'Условия' (Conditions) tab in the UEM SAFEMOBILE administrator interface. The form contains the following fields and options:

- Именованное условие применения**: A dropdown menu.
- Принадлежность МСК**: A dropdown menu with the value 'Любая' (Any).
- Внутри хотя бы одной геозоны из списка**: A dropdown menu with the value 'Выберите геозону...' (Select a geozona...).
- Вне всех геозон из списка**: A dropdown menu with the value 'Выберите геозону...' (Select a geozona...).
- Сотрудник входит в группы**: A dropdown menu with the value 'Выберите группу' (Select a group).
- Сотрудник не входит в группы**: A dropdown menu with the value 'Выберите группу' (Select a group).
- Режим устройства**: A dropdown menu with the value 'Не задано' (Not set).
- На устройстве установлено одно из приложений**: A text input field with a green plus icon and the placeholder 'Введите значение и нажмите добавить' (Enter a value and click add).
- На устройстве отсутствует одно из приложений**: A text input field with a green plus icon and the placeholder 'Введите значение и нажмите добавить' (Enter a value and click add).
- Выбор диапазонов ОС**: A section with a red 'X' icon, currently disabled.
- Версия ОС в диапазоне**: Two dropdown menus for 'Выберите начальную версию ОС' (Select initial OS version) and 'Выберите конечную версию ОС' (Select final OS version), followed by a 'Создать' (Create) button.
- Версия ОС вне диапазона**: A dropdown menu with the value 'Выберите начальную версию ОС' (Select initial OS version).

Рисунок 2.56 — Условия применения профиля

По умолчанию условия не заданы, после задания условий название закладки измениться на «Условия». Для задания условий применения следует в раскрывающемся списке выбрать параметр со значением:

- **Именованное условие применения** — применяет именованное условие применения, заданное в разделе «Объекты учета — Условия применения». После выбора условия из списка все остальные параметры в блоке становятся не доступны для изменения. Чтобы параметры стали доступны для редактирования необходимо в поле «Именованное условие применения» выбрать «Не заданно»;

- Принадлежность МСК (любая/личная/корпоративная);
- Стратегия управления устройством входит в список (только устройство/устройство и контейнер KNOX/личный рабочий профиль/корпоративный рабочий профиль) — **только для Android**;

Примечание

Для стратегий «личный рабочий профиль» и «корпоративный рабочий профиль»:

- *Передача файлов по usb на устройство и обратно недоступна.*
- *Политика «Запретить экспорт данных из рабочего профиля на устройство через буфер обмена» не распространяется на файлы.*

- Внутри хотя бы одной геозоны (название геозоны);
*Для возможности применения геозона должна быть активирована.
Описание работы с геозонами приведено в 2.8.11.*
- Вне всех геозон из списка (название геозоны);
Для возможности применения геозона должна быть активирована. Описание работы с геозонами приведено в 2.8.11.

Примечание

Если к устройствам Android применяются «условия применения» по геозонам, то необходимо выполнить следующие действия:

- 1. На устройство Android должен быть назначен профиль «Настройки сбора местоположений Android», который должен применяться безусловно.*
- 2. В профиле должны быть включены политики «Собирать информацию о местоположении (в рабочее время)» и «Системный сервис определения местоположения должен быть всегда включен».*

- Сотрудник входит в группы – список DN импортированных группы или наименование локальных;
- Сотрудник не входит в группы – список DN импортированных группы или наименование локальных;
- Режим устройства (supervised/unsupervised) — **только для iOS**;
- На устройстве установлено одно из приложений (UID приложения);
- На устройстве отсутствует одно из приложений (UID приложения);

Выбор диапазонов ОС

- Выбор диапазона разрешенных ОС: (Выберите начальную версию ОС / Выберите конечную версию ОС);
- Выбор диапазона запрещенных ОС: (Выберите начальную версию ОС / Выберите конечную версию ОС);

После выбора значений диапазона ОС следует нажать кнопку **«Создать»**.
Для сохранения внесенных изменений нажать кнопку **«Сохранить»**.

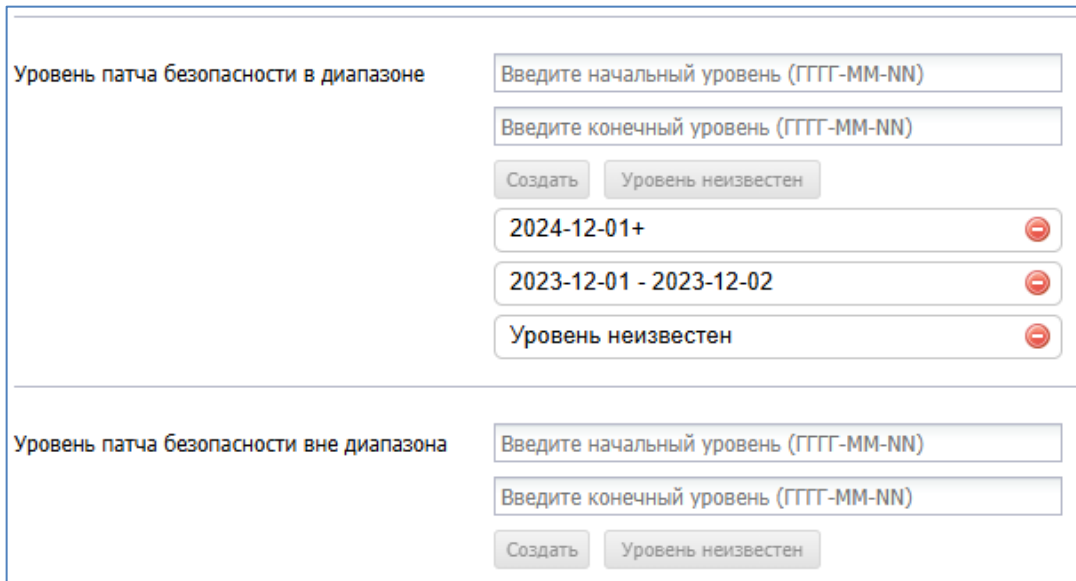
- Устройство имеет все перечисленные метки;
- У устройства есть хотя бы одна метка из перечисленных;
- У устройства нет ни одной из перечисленных меток;
- Модель устройства входит в список;
- Модель устройства отсутствует в списке;
- Тип устройства;
- Монитор имеет все перечисленные привилегии — **только для Android**;
- Монитор имеет хотя бы одну из перечисленных привилегий — **только для Android**;
- Монитор не имеет ни одной из перечисленных привилегий — **только для Android**;
- Наличие пароля или другого способа авторизации (пин-код, биометрия и т.п.) — **только для Android, iOS**;
- Пароль соответствует требованиям профилей — **только для Android, iOS, Аврора**;
- Уровень патча безопасности в диапазоне — **только для Android**.
Сущность применяется если патч безопасности находится в **заданном** диапазоне. Допускается указание нескольких диапазонов. Значения диапазонов не должны пересекаться. Диапазон задается в формате — ГГГГ-ММ-NN (рисунок 2.57):

- Начальный уровень,
- Конечный уровень,

Значение диапазона может быть задано как «Уровень неизвестен», данное значение может быть добавлено в список диапазонов только единожды. При таком значении диапазона условие срабатывает для устройств, у которых уровень патча безопасности не определен.

- Уровень патча безопасности вне диапазона — **только для Android**.
Сущность применяется если дата последнего обновления патча безопасности **выходит за пределы** указанного диапазона. Параметр имеет приоритет

над параметром «Уровень патча безопасности в диапазоне». Заполнение параметра данными аналогично параметру «Уровень патча безопасности в диапазоне».



Уровень патча безопасности в диапазоне	Введите начальный уровень (ГТТГ-ММ-NN)
	Введите конечный уровень (ГТТГ-ММ-NN)
	Создать
	Уровень неизвестен
	2024-12-01+
	2023-12-01 - 2023-12-02
	Уровень неизвестен

Уровень патча безопасности вне диапазона	Введите начальный уровень (ГТТГ-ММ-NN)
	Введите конечный уровень (ГТТГ-ММ-NN)
	Создать
	Уровень неизвестен

Рисунок 2.57 — Диапазон уровня патча безопасности

- Модель процессора входит в список — **только для Android**. Применяется, если модель процессора (SocModel) присутствует в указанном списке. Если список пуст, условие игнорируется.

Правила формирования списка:

- Модель можно добавить:
 - текстом (регистронезависимое сравнение).
 - регулярным выражением (с префиксом RegExp).
- Регулярное выражение должно быть валидным (иначе не добавляется).
- Одна модель или регулярное выражение не может входить в несколько списков. В противном случае системы выдаст ошибку: «Нельзя добавить одну модель процессора или регулярное выражение в оба списка».
- Модель процессора отсутствует в списке — **только для Android**. Применяется, если модель процессора (SocModel) отсутствует в указанном списке. Если список пуст, условие игнорируется. Правила формирования списка аналогичны пункту выше.

- Версия прошивки (Build Incremental Version) входит в список — **только для Android**. Применяется, если версия прошивки (BuildIncrementalVersion) есть в списке. Если список пуст, условие игнорируется.

Правила формирования списка:

- Модель можно добавить:
 - текстом (регистронезависимое сравнение).
 - регулярным выражением (с префиксом RegExp).
- Регулярное выражение должно быть валидным (иначе не добавляется).
- Одна модель или регулярное выражение не может входить в несколько списков. В противном случае системы выдаст ошибку: «Нельзя добавить одну модель процессора или регулярное выражение в оба списка».
- Версия прошивки (Build Incremental Version) отсутствует в списке — **только для Android**. Применяется, если версия прошивки (BuildIncrementalVersion) отсутствует в списке. Если список пуст, условие игнорируется. Правила формирования списка аналогичны пункту выше.
- Наличие модуля NFC на устройстве — **только для Android**. Проверяет наличие NFC (FeatureHardwareNFC). Если параметр не задан, условие игнорируется.
- Наличие модуля телефонии на устройстве — **только для Android**. Проверяет поддержку телефонии (FeatureHardwareTelephony). Если параметр не задан, условие игнорируется.
- Наличие сканера RFID на устройстве — **только для Android**. Проверяет наличие встроенного RFID-сканера (считывателя), который позволяет работать с RFID-метками или картами.

2.6.9.4 Назначение профиля

Для назначения профиля во вкладке **«Назначения»** (рисунок 2.58) в окне ОШС выбрать подразделение(я)/сотрудника(ов) или в главной таблице выбрать одно или несколько МСК сотрудников. Для удобства можно использовать поиск по следующим параметрам таблицы:

- id,
- Телефон,
- Сотрудник,
- Пользователь домена,
- Отдел/группа,
- Метка.

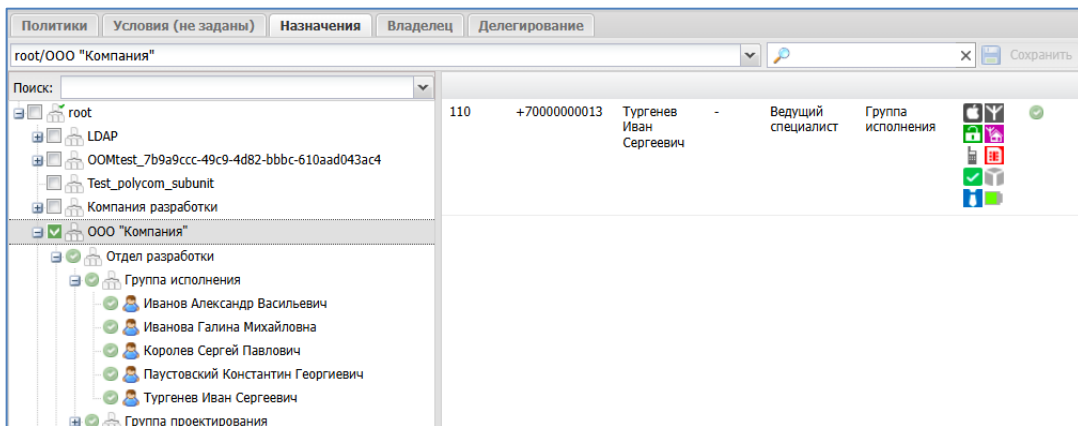




Рисунок 2.58 — Назначение профиля

Назначение сущности имеет два состояния:

-  — назначено;
-  — исключено.

Для сохранения назначения профиля в системе нажать на кнопку **«Сохранить»**.

2.6.9.5 Смена владельца сущности

Во вкладке **«Владелец»** администратор может сменить владельца сущности для подчиненного подразделения. Для этого следует выбрать требуемый узел ОШС в соответствии с рисунком 2.59 и нажать **«Сохранить»**. После подтверждения изменения владельцем сущности будет назначен указанный объект ОШС. Если сущность имеет назначения за пределами области управления нового владельца, то в интерфейсе отобразится ошибка в соответствии с рисунком 2.60 . У объекта ОШС может быть только один владелец для управления сущностями.

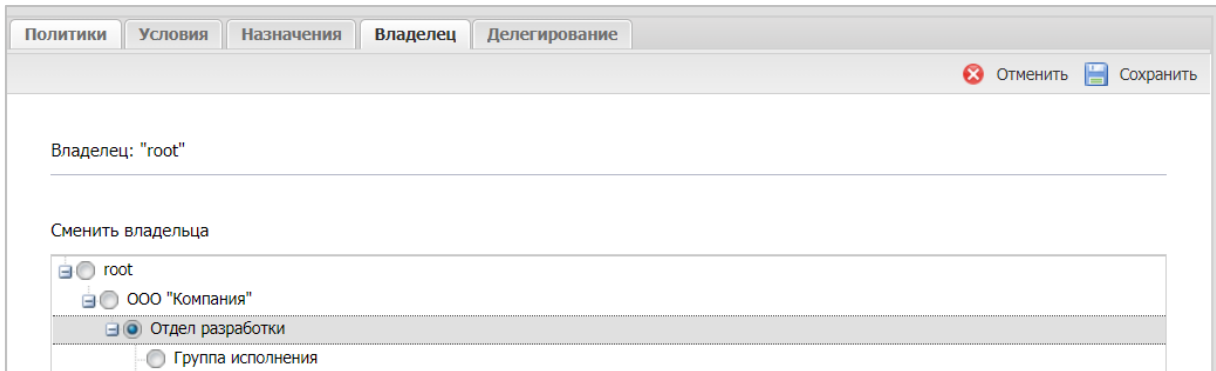


Рисунок 2.59 — Смена владельца сущности

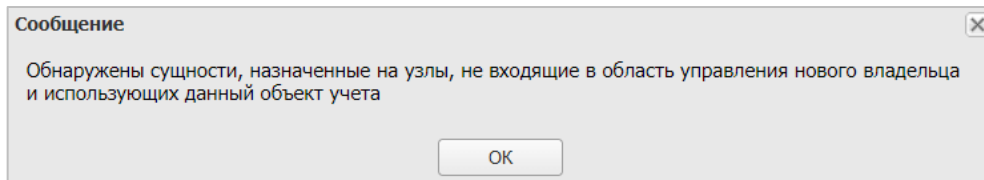


Рисунок 2.60 — Сообщение об ошибке при смене владельца сущности

Для отмены действия смены владельца сущности следует нажать **«Отменить»**, после чего кнопка **«Сохранить»** станет не активной.

2.6.9.6 Делегирование сущности

Во вкладке **«Делегирование»**, для передачи прав на управление назначением сущности администраторам узла ОШС (рисунок 2.61), владельцем является «root» требуется выбрать один или несколько объектов ОШС, нажать **«Сохранить»** и подтвердить действие. В этом случае, для администратора выбранного объекта ОШС данная сущность в АРМе в окне с реестром профилей будет отображаться как «Делегированная» в столбце «Сущность».

Для отмены делегирования следует нажать **«Отменить»**.

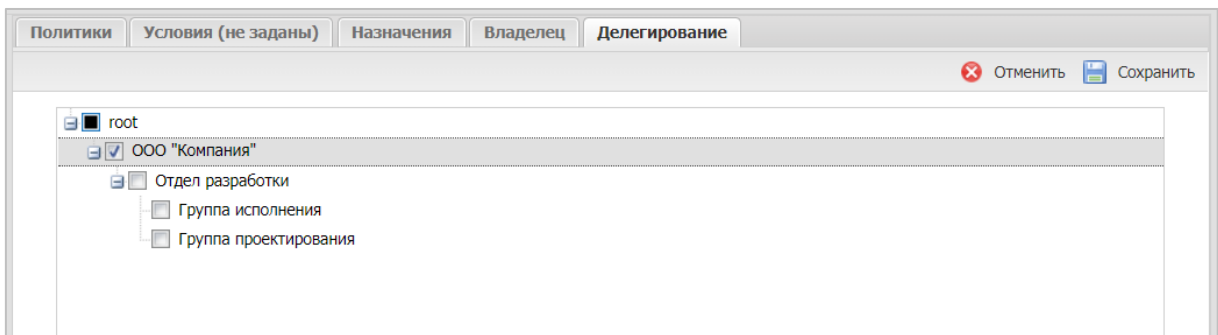


Рисунок 2.61 — Делегирование сущности

2.6.9.7 Применение профиля

Особенности применения на МСК платформы Android профилей парольные политики

Начиная с 10 версии Android, для управления парольными политиками устройства, Монитору **обязательно** нужны права Device Owner. Таким образом, если монитор был установлен на Android 9 без прав Device Owner (например, с правами Device Admin или лицензией KNOX), то после обновления устройства до Android 10 возможность управлять парольными политиками будет утрачена.

Особенности применения на МСК профилей различных типов

При добавлении профиля следует учитывать следующие особенности:

- При назначении нескольких профилей будут применяться политики назначенные на ближайшие к МСК родительские узлы в дереве ОШС. Для следующих типов профилей:
 - Парольные политики iOS,
 - Парольные политики Android,
 - Политики ограничений iOS,
 - Политики ограничений Android,
 - Политики ограничений Samsung Knox Android,
 - Политики ограничений контейнера Samsung Knox Android,
 - Парольные политики контейнера Samsung Knox Android,
- При назначении нескольких профилей на МСК будет применено то количество аккаунтов, которое было назначено. Для следующих типов профилей:
 - Exchange аккаунт в контейнере Samsung Knox Android,
 - Exchange аккаунт iOS,
 - доверенный сертификат iOS,
 - доверенный сертификат Android,
 - доверенный сертификат ОС Аврора,
 - точка доступа WiFi iOS,
 - точка доступа WiF Android,
 - политики Cellular iOS;
- Допустимо назначение нескольких, различных профилей «Политики сотовой сети (APN)», для разных сотовых операторов. После применения профилей APN блокируется возможность использования любых мобильных точек доступа, помимо заданных в профилях.

Особенности применения на МСК профилей одного типа

При назначении нескольких профилей одного типа непосредственно на МСК, пользователя или узел будут применяться политики из профиля, назначенного последним. Под **«последним»** понимается назначение, сделанное последним по времени.

Особенности применения профилей «Режим киоска...»

При добавлении профиля «Режим киоска...» для МСК будут применены следующие ограничения:

- Ограничение на количество приложений:
 - IOS — пользователю МСК доступно только одно приложение;
 - Android — доступно несколько режимов работы:
 - Режим одного приложения;
 - Режим нескольких приложений;
 - Режим одного WEB приложения;
- На устройстве применяются другие профили, кроме:
 - Профиль парольных политик контейнера Knox.
- На устройстве выполняются команды, кроме:
 - Установка пароля контейнера;

Чтобы в режиме киоска была возможность принимать и совершать звонки, а также получать и отправлять SMS, необходимо добавить в политику «Список UID'ов отображаемых приложений» следующие приложения:

- com.google.android.dialer;
- com.google.android.contacts,
- com.google.android.apps.messaging.

В зависимости от производителя и модели устройства состав приложений может отличаться. В частности, для устройств производителя Samsung необходимо добавлять приложения:

- com.samsung.android.dialer,
- com.samsung.android.app.contacts,
- com.samsung.android.incallui,
- com.samsung.android.messaging,
- com.android.server.telecom.

Состав необходимых приложений для конкретного устройства необходимо определять экспериментально.

Примечание:

В текущей версии поддерживается работа устаревших типов профилей на Android:

- *Режим киоска Android (устарел)*
- *Режим киоска Samsung Knox Android (устарел)*

Следует отказаться от их использования в дальнейшем и произвести миграцию на другие типы профилей.

В режиме работы «Киоск», при открытии файлов может отсутствовать диалоговое окно выбора приложения для открытия файла. При этом вне режима работы «Киоск» выбор приложения открытия файлов работает корректно. Это происходит потому, что приложение, которым следует открывать файл не прописано в политиках: «Список UID'ов отображаемых приложений» или «Дополнительный список UID'ов разрешенных приложений...» настроек профиля «Киоск», назначенного на МСК.

Чтобы выбор приложения отображался корректно необходимо выполнить следующие действия:

1. Вывести МСК из режима «Киоск»;
2. Запустить приложение, которое не отображается в диалоговом окне выбора приложения для открытия файла;
3. С помощью утилиты Android Debug Bridge выполнить команду:

```
adb shell dumpsys activity activities
```

4. В отображенных результатах работы команды находим информацию об открытом activity. Она должна иметь вид:

```
ActivityRecord{... com.application.package/CurrentActivity ...}.
```

Например:

```
ActivityRecord{cd11070          u0          ru.niisokb.mcc/.  
monitorui.presentation.view.MonitorRootActivity t194}
```

5. Найти UID целевого activity — часть строки с информацией об activity до значка «/»: com.application.package

Как в примере:

```
ru.niisokb.mcc
```

6. Добавить UDI в профиль «Киоск», в политику:
 - Список UID'ов отображаемых приложений — если требуется отображение иконки приложения на главном экране «Киоска»;

или

- Дополнительный список UID'ов разрешенных приложений... — если отображение иконки приложения не требуется.
7. Сохранить изменения. После чего приложение будет отображаться в диалоговом окне выбора приложения для открытия файлов на всех МСК, к которым применен данный профиль.

В режиме работы «киоск», на управление WiFi и яркостью экрана действуют не только политики «киоска», но и политики профиля ограничений Android, а именно:

- «Запретить добавлять новые точки доступа WiFi»;
- «Запретить изменять состояние WiFi»;
- «Запретить изменение настроек точек доступа Wi-Fi»;
- «Минимальный уровень безопасности Wi-Fi»;
- «Запретить регулировку яркости».

Особенность применения профиля «Политики ограничений Samsung Knox Android»

Одновременное назначение запрета на использование всех сетевых интерфейсов, перепрошивку устройства и сброс к заводским настройкам приведет к **нерабочему состоянию МСК без возможности восстановления его работоспособности**.

Пример такого назначения приведен ниже:

Разрешить перепрошивку устройства — Нет.

Разрешить сброс устройства к заводским настройкам — Нет.

Разрешить Wi-Fi (при запрете недоступны Wi-Fi Direct и S Beam) — Нет.

Разрешить мобильную передачу данных — Нет.

Разрешить использование Bluetooth — Нет.

Особенность применения профилей на МСК при его блокировке и разблокировке.

Если МСК на платформе Android было заблокировано, то после его разблокировки для применения назначенных профилей следует повторно отправить команду синхронизации настроек.

Условия создания контейнера Knox

При добавлении профиля Настройки монитора Android на МСК производства Samsung одной из задач является создание контейнера Knox. Но для достижения этой цели должны быть выполнены следующие условия:

- в параметрах профиля назначен действительный ключ Samsung Knox License (SKL);
- на МСК не был установлен Knox warranty bit в результате проведения заводской прошивки;
- пользователь МСК согласился с созданием контейнера;
- на момент активации лицензий Knox были доступны серверы Samsung.

Если указанные условия не выполнены, в системе воспроизведется ошибка (ошибка активации Knox ключей, ошибка создания контейнера) в соответствии с описанием в таблице 2.2.

2.6.9.8 Удаление профиля

Для удаления следует выбрать в реестре профиль и нажать кнопку **«Удалить»**. Данный профиль будет удален из подраздела **«Профили»**. Если удаленный профиль был назначен на МСК, то в подразделе **«Отчёты/Профили»** он отобразится в применённых профилях с записью **«удален»**. После синхронизации устройства с системой и удаления настроек с МСК профиль будет окончательно удален из интерфейса.

Примечание

На устройствах iOS, при удалении корпоративного профиля, приложение «Монитор» должно автоматически удаляться с устройства. Если этого не произошло, то устройство необходимо сбросить до заводских настроек.

2.6.10 Раздел «Правила несоответствия»

«Правила несоответствия» позволяет создавать, редактировать или удалять набор действий, которые система автоматически произведет при выполнении заданных условий (рисунок 2.62). Для каждого действия в правиле существует возможность указать задержку между выполнением условий и действием.

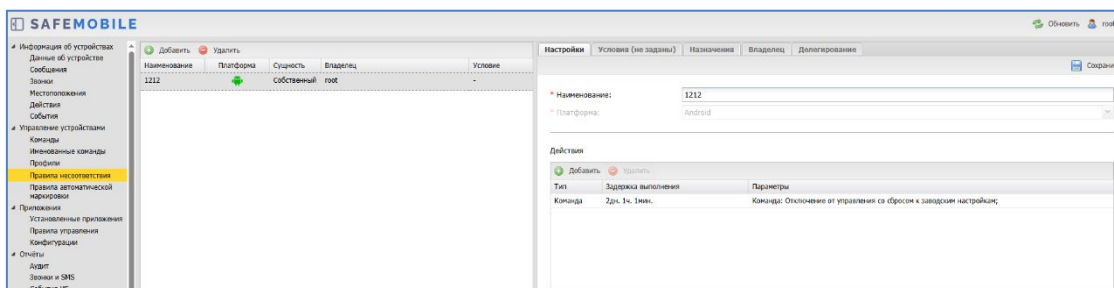


Рисунок 2.62 — Список правил несоответствия

В центральной части рабочего экрана отображается список правил, в котором каждая строка запись одного правила и содержит следующую информацию:

- Наименование — наименование правила;
- Платформа — iOS или Android;
- Сущность — тип сущности;
- Владелец — владелец правила в ОШС;
- Условие — именованные условия применения, заданные в правиле .

В боковом экране, рабочей области раздела отображаются параметры правила, выделенного в списке.

- Настройки — описание действия над МСК, при соответствии условий;
 - Наименование — наименование правила;
 - Платформа — платформа МСК, для которой назначается правило;
 - Действия — блок содержит список действий над устройством, выполняемых над МСК;
- Условия/Условия (не заданы) — содержит описание условий, при выполнении которых, настройки правила будут применены к устройству. Список условий идентичен [условиям применения профилей \(см. 2.6.8.3\)](#);

- Назначения — содержит указание подразделения, пользователей или комплекты, на которые будет применено данное правило;
- Владелец — содержит функционал назначения узла ОШС как владельца правила. Каждое правило принадлежит одному владельцу. Администратор узла «владельца» (а также администратор вышестоящего узла ОШС) имеет права на редактирование настроек правила;
- Делегирование — позволяет делегировать назначение правила администраторам подчиненных подразделений.

В верхней части таблицы находится панель инструментов со следующими кнопками:

- Добавить — предназначена для создания нового правила;
- Удалить — предназначена для удаления уже созданного правила.

2.6.10.1 Добавление нового правила несоответствия

Чтобы добавить новое правило несоответствия, необходимо выполнить следующие действия:

1. Перейти в раздел «Правила несоответствия»;
2. Нажать кнопку «Добавить»
3. В боковом блоке, рабочего экрана заполнить следующие поля:
 - Наименование
 - Платформа
4. В блоке «Действия» нажать кнопку «Добавить», после чего откроется модальное окно настройки действия правила.
5. Выбрать тип действия, после чего откроются дополнительные поля настроек:
 - Отправка e-mail — отправка e-mail сообщения (рисунок 2.63);
 - Получатель — список адресов email (разделитель — точка с запятой);
 - Копия — список адресов email (разделитель — точка с запятой);
 - Шаблон — шаблон письма. Выбирается из шаблонов писем в объектах учета;
 - Задержка выполнения — время задержки выполнения действия (дни, часы, минуты).

Примечание

При заполнении полей «Получатель» и «Копия» допускается использование подстановок, описанных в разделе [2.6.8.2 Настройка параметров профиля](#).

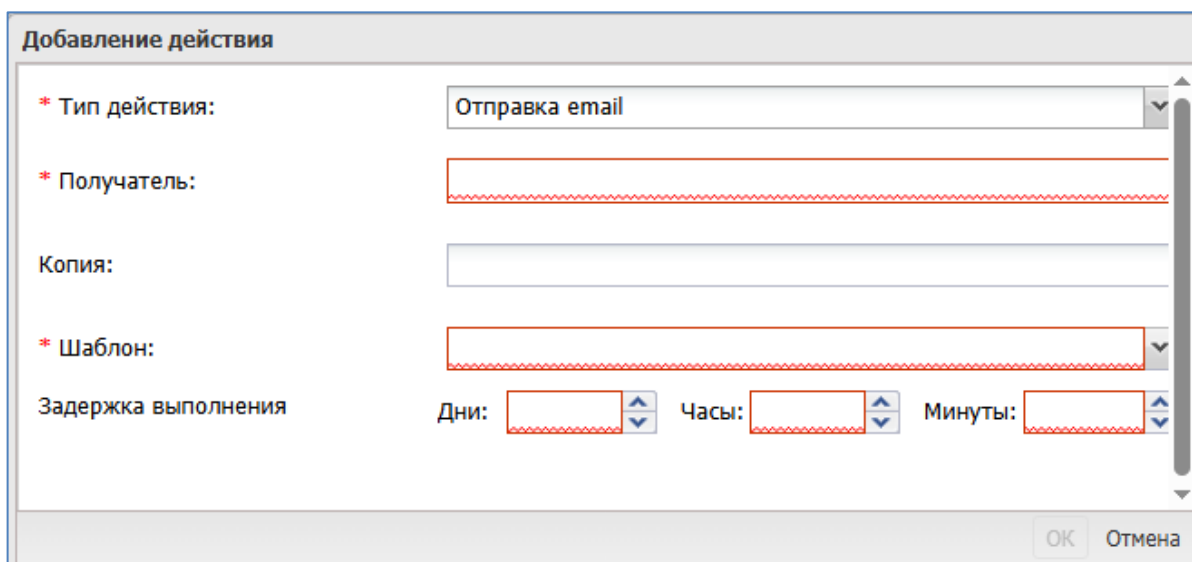


Рисунок 2.63 — Параметры действия «Отправка email»

- Команда — назначает выполнение заданной команды (рисунок 2.64);
 - Команда — выбор команды:
 - Синхронизация времени устройства с сервером;
 - Отключение от управления со сбросом к заводским настройкам;
 - Установка графика рабочего времени;
 - Повторный запрос номера телефона;
 - Отключение от управления с удалением только корпоративных данных;
 - Синхронизация настроек;
 - Отправка уведомления;
 - Очистка данных приложения.
 - Задержка выполнения — время задержки выполнения действия (дни, часы, минуты).

The screenshot shows a dialog box titled "Добавление действия" (Add Action). It contains the following fields:

- * Тип действия: Команда (dropdown menu)
- * Команда: (empty text input field)
- Задержка выполнения (Execution delay):
 - Дни: (spin box)
 - Часы: (spin box)
 - Минуты: (spin box)

Buttons "OK" and "Отмена" (Cancel) are located at the bottom right.

Рисунок 2.64 — Параметры действия «Команда»

- Профиль — назначение на устройство профиля (рисунок 2.65);
 - Тип профиля — выпадающий список выбора назначаемого типа профиля. В списке отображаются только типы профилей с режимом назначения «автоматический»;
 - Выбор — выбор профиля, соответствующего выбранному типу профиля;
 - Задержка выполнения — время задержки выполнения действия (дни, часы, минуты).

The screenshot shows a dialog box titled "Добавление действия" (Add Action). It contains the following fields:

- * Тип действия: Профиль (dropdown menu)
- * Тип профиля: (empty dropdown menu)
- * Выбор: (empty dropdown menu)
- Задержка выполнения (Execution delay):
 - Дни: (spin box)
 - Часы: (spin box)
 - Минуты: (spin box)

Buttons "OK" and "Отмена" (Cancel) are located at the bottom right.

Рисунок 2.65 — Параметры действия «Профиль»

- Метка назначение метки на правило несоответствия (рисунок 2.66).
 - Выбор — выпадающие список выбора заданных в системе меток;

- **Задержка выполнения** — время задержки выполнения действия (дни, часы, минуты).

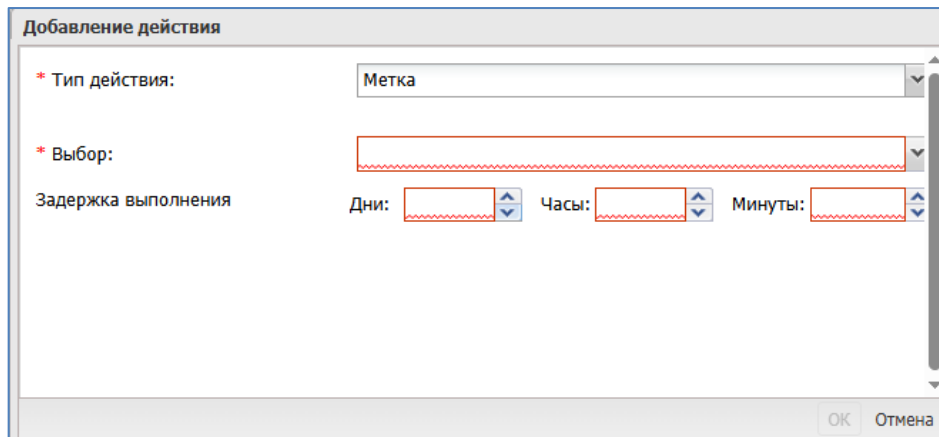


Рисунок 2.66 — Параметр действия «Метка»

6. Нажать кнопку «Ок», после чего действие будет добавлено в список действий правила;
7. Нажать кнопку «Сохранить» (рисунок 2.67);

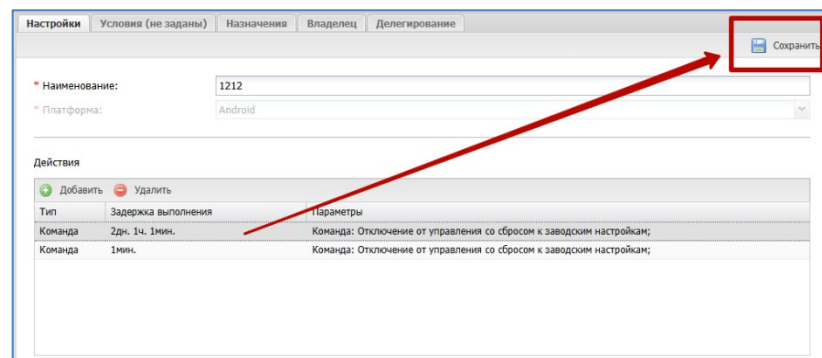


Рисунок 2.67 — Расположение кнопки «Сохранить»

8. Нажать кнопку «Да», в модальном окне подтверждения действия, после чего новое правило будет добавлено в список.

Примечание

- Если в «назначении» ничего не выбрано, то правило не будет применено;
- Если в период «задержки выполнения» устройство перестало удовлетворять условиям, то действие произведено не будет;
- Если ни одно из условий не задано, то правило применяется безусловно;

- *Настройки правила во вкладках «Условия», «Назначения», «Владелец», «Делегирование» доступны после завершения создания правила.*
- *Если в качестве действия задано применение профилей, то все профили, указанные в правиле несоответствия:*
 1. *Будут назначены непосредственно на устройство.*
 2. *Будут иметь более высокий приоритет по отношению к профилям назначенным администратором.*
 3. *В остальном будут подчиняться общим правилам применения профилей.*

2.6.10.2 Задание условий применения правил несоответствия

После создания правила станет доступна настройка условий его применения на вкладке **«Условия»**. Настройка осуществляется в соответствии с описанием задания условий применения профиля раздел 2.6.9.3.

2.6.10.3 Редактирование существующего правила несоответствия

Чтобы внести изменения в существующее правило несоответствия, необходимо выполнить следующие действия:

1. В списке правил выделить правило подлежащее редактированию;
2. В блоке настроек внести изменения в параметры правила;
(Изменить уже заданное действие, в блоке «Действия» нельзя. Допускается только удаление существующего и создание нового);
3. Нажать кнопку «Сохранить».

2.6.10.4 Удаление существующего правила несоответствия

Чтобы удалить существующее правило несоответствия, необходимо выполнить следующие действия:

1. В списке правил выделить правило подлежащее редактированию;
2. Нажать кнопку «Удалить» на центральном рабочем экране раздела;
3. В модальном окне подтверждения действия нажать кнопку «Да», после чего правило будет удалено.

2.6.11 Раздел «Правила автомаркировки»

Раздел «Правила автомаркировки» предназначен для автоматического назначения меток на устройства по их идентификаторам (серийный номер, IMEI, UDID, корпоративный идентификатор).

Основные задачи:

- Создание, редактирование и удаление правил автоматической маркировки.
- Управление списками идентификаторов устройств.
- Назначение правил на подразделения организационной структуры (ОШС).
- Контроль применения меток при изменении данных устройства.

Доступ и права для работы с разделом:

Просмотр, изменение, удаление — в зависимости от прав владельца.

Дополнительные полномочия:

- Изменение списков ID устройств правил автоматической маркировки.
- Смена владельца правил автоматической маркировки.
- Просмотр назначений на ОШС правил автоматической маркировки.
- Изменение назначений на ОШС правил автоматической маркировки.

В центральной части рабочего экрана (рисунок 2.68) отображается список правил автомаркировки, где каждая строка списка содержит:

- наименование правила,
- список меток (через запятую),
- владельца правила.

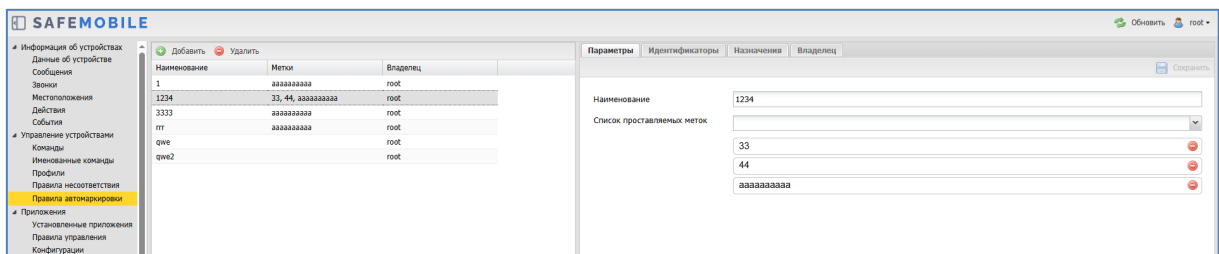


Рисунок 2.68 — Раздел «Правила автомаркировки»

В правой части рабочего экрана отображаются параметры и настройки правила выбранного в основной таблице. Параметры и настройки правила содержат следующие опции управления:

- Вкладка «Параметры»:
 - Наименование — наименование правила (уникальное, в пределах владельца);
 - Список проставляемых меток — список меток, состоящий из существующих меток;
- Вкладка «Идентификаторы» (рисунок 2.69):
 - Вкладка «Серийный номер» — список идентификаторов устройств по серийным номерам;
 - Поля ввода и кнопки управления списком идентификаторов (аналогичен для всех аналогичных вкладок раздела):
 - Поле ввода и кнопка «Добавить» — позволяет вручную добавить идентификатор в список.
 - Кнопка «Удалить» — удалить идентификатор, выбранный в списке.

Примечание

При добавлении идентификатора в список система проводит проверку на формат:

- *IMEI — 15ти-значный номер;*
- *UDID, серийный номер, корпоративный ID — длина ≤ 255 символов.*

- Вкладка «IMEI» — список идентификаторов устройств по IMEI;
- Вкладка «UDID» — список идентификаторов устройств по UDID;
- Вкладка «Корпоративный идентификатор устройства» — список устройств по корпоративным идентификаторам;
- Кнопка «Загрузить файл» — позволяет заполнить выбранную вкладку идентификатора из CSV файла;
- Кнопка «Выгрузить файл» — позволяет выгрузить существующий список из выбранной вкладки идентификаторов. Полученный файл может быть использован как шаблон для составления CSV файла загрузки идентификаторов.
- Кнопка «Очистить» — очистить список идентификаторов в выбранной

вкладке.

- Вкладка «Назначения» — назначение правила автомаркировки на узел ОШС (только на один узел, без делегирования).
- Вкладка «Владелец» — назначение владельца правила. Допускается смена владельца.

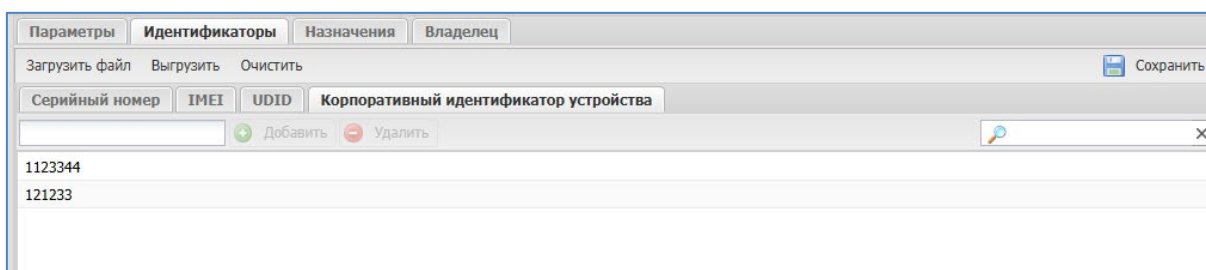
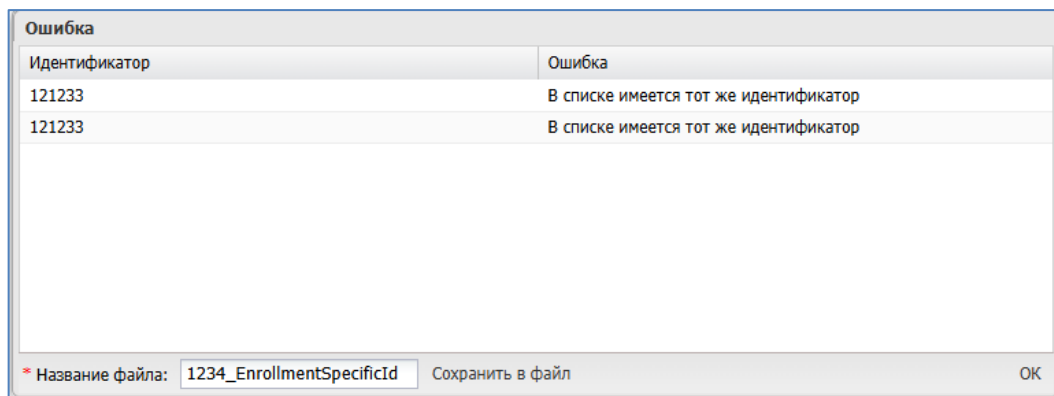


Рисунок 2.69 — Идентификаторы устройств

2.6.11.1 Создание нового правила автомаркировки

Чтобы создать новое правило необходимо выполнить следующие действия:

1. Выбрать раздел «Правила автомаркировки».
2. Нажать кнопку «Добавить»
3. Заполнить параметры:
 - Наименование — уникальное название правила (проверяется на уникальность).
 - Список меток — выбрать из списка метки, которые будут автоматически назначаться на устройства.
4. Добавить идентификаторы устройств.
 - Ручное добавление:
 - 4..1. Открыть вкладку индентификатора.
 - 4..2. Заполнить поле ввода.
 - 4..3. Нажать кнопку «Добавить».
 - Загрузка из CSV файла:
 - 4..1. Открыть вкладку индентификатора.
 - 4..2. Нажать кнопку «Загрузить файл».
 - 4..3. Загрузить выбранный файл.
 - 4..4. Система проверит данные из файла. При наличии ошибок будет показан отчет о не верных данных (рисунок 2.70). Отчет может быть сохранен в отдельный CSV файл. Идентификаторы с ошибками не импортируются.



Идентификатор	Ошибка
121233	В списке имеется тот же идентификатор
121233	В списке имеется тот же идентификатор

* Название файла:

Рисунок 2.70 — Ошибки при импорте идентификаторов

5. Открыть вкладку «Назначение» и назначить правило на нужный узел ОШС.
6. Во вкладке «Владелец» указать владельца.
7. Нажать кнопку «Сохранить».

2.6.11.2 Особенности удаления и редактирования правил авто-маркировки

Чтобы удалить правило автоматической маркировки необходимо выбрать нужное правило в общем списке правил и нажать кнопку «Удалить».

Чтобы отредактировать правило необходимо выбрать его с списке правил, внести изменения в параметры и нажать кнопку «Сохранить».

Для ручного добавления идентификатора **конкретного** устройства **в существующее правило** автомаркировки необходимо перейти в раздел «Информация об устройствах — Данные об устройстве». Если в системе существует хотя бы одно правило автоматической маркировки, доступное текущему администратору, рядом с каждым идентификатором устройства (серийный номер, IMEI, UDID и др.) будет отображаться кнопка «Добавить идентификатор» (рисунок 2.71). При нажатии на эту кнопку открывается диалоговое окно, содержащее список всех доступных правил автомаркировки, в которое можно добавить выбранный идентификатор текущего устройства. Доступ к этим кнопкам возможен при наличии полномочия «Расширение правил автоматической маркировки».

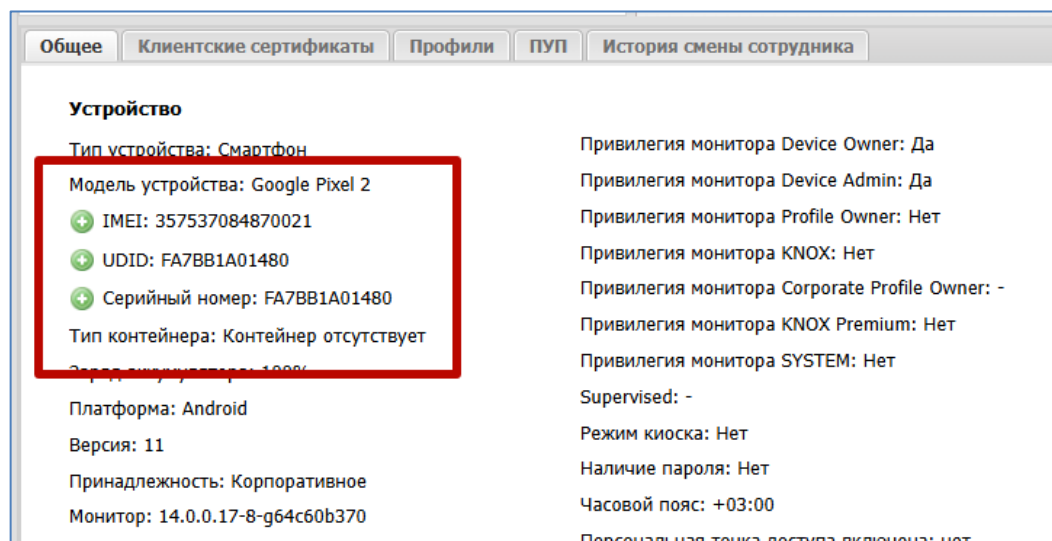


Рисунок 2.71 — Кнопка «Добавить идентификатор в правило»

Если, при редактировании правила происходит удаление уже установленных этим правилом меток (смена назначения, удаление идентификаторов), а так же при удалении правила система предоставит выбор действий (рисунок 2.72):

- «Снять метки с устройств» (по умолчанию).
- «Оставить метки на устройствах, поменяв способ назначения меток с автоматического на ручной».

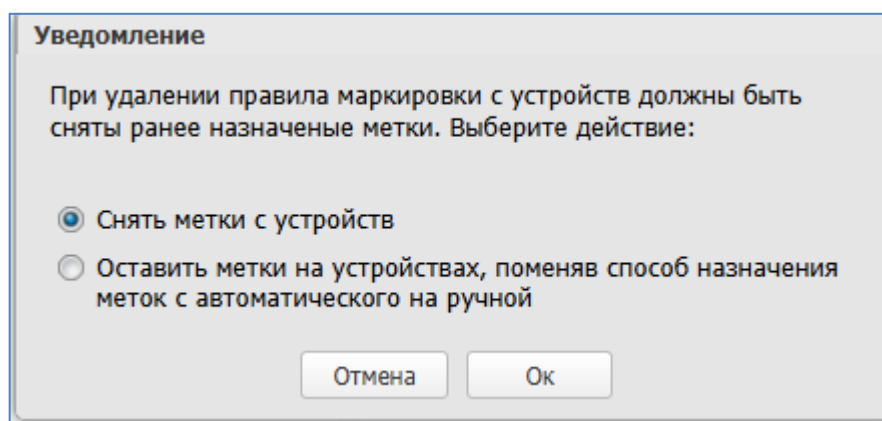


Рисунок 2.72 — Уведомление при удалении правила автомаркировки

Если, при смене владельца устройства или при перемещении сотрудника между подразделениями, устройство вышло из области действия правила автоматической маркировки, метки установленные правилом будут сняты.

2.6.12 Раздел «Установленные приложения»

Раздел «Установленные приложения» (рисунок 2.73) предназначен для осуществления контроля за приложениями, установленными на МСК пользователя, в том числе, установленными в контейнер, позволяет Администратору зарегистрировать приложение в «UEM SafeMobile», а также осуществить удаленный запуск выбранного приложения.

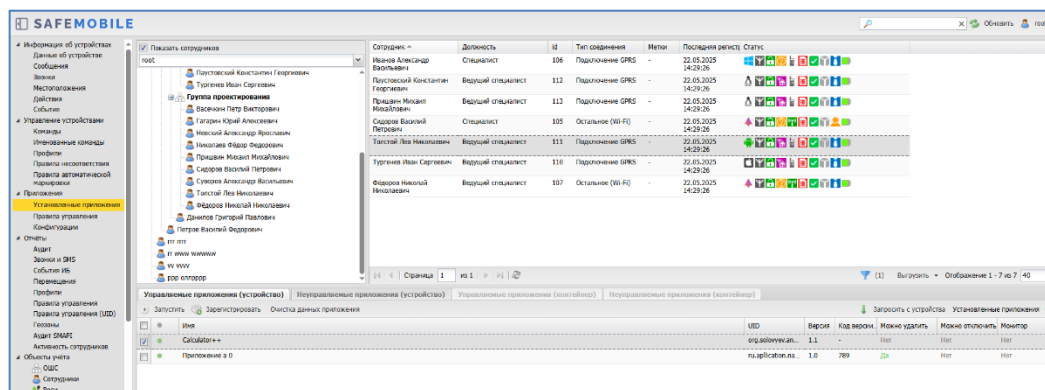


Рисунок 2.73 — Раздел «Установленные приложения»

В нижней части рабочего экрана отображаются установленные на МСК приложения. Список приложений разделен по вкладкам:

- Управляемые приложения (устройство),
- Неуправляемые приложения (устройство),
- Управляемые приложения (контейнер),
- Неуправляемые приложения (контейнер).

Каждая вкладка таблицы установленных приложений содержит следующие столбцы:

- — Состояние установленного приложения (— включено, — выключено);
- Имя — название установленного приложения;
- UID — уникальный идентификатор приложения;
- Версия — версия установленного приложения;
- Код версии — код установленной версии приложения;
- Можно удалить — возможность удаления приложения с МСК (Да/Нет);
- Можно отключить — возможность отключения приложения на МСК на платформе Android (Да/Нет);
- Монитор — мобильный клиент SafeMobile «Да/Нет»;

Отключение и удаление приложения осуществляется посредством создания ПУП в соответствии с 2.6.11.

Кнопки, расположенные на панели таблицы установленных приложений, позволяют Администратору отправить с АРМ на МСК команды, после чего будет выполнено следующее действие, а именно:

- **Запустить** — нажатие кнопки приводит к запуску выбранного приложения на устройстве. На МСК платформы Android нельзя удаленно запустить отключенное пользователем **системное** приложение. Если системное приложение было отключено на устройстве в разделе **«Настройки»**, то включить его можно только в **«Настройках»** устройства.
- **Запросить с устройства** — нажатие кнопки приводит к отправке команды-запроса на формирование списка всех установленных приложений на МСК, включая приложения, установленные до подключения устройства к системе.
- **Зарегистрировать** — нажатие кнопки выбранное некорпоративное приложение, установленное на МСК пользователя, регистрируется в «UEM SafeMobile» и будет доступно при назначении ПУП Администратором.
- **Очистка данных приложения** — (только для Android) при нажатии кнопки будут удалены данные выбранного приложения (очистка кэша). Операция доступна для вкладки «Управляемые приложения (устройство)» за исключением случая, когда выбрано устройство Android с привилегией РО. Для прочих вкладок операция доступна при наличии приложений в этих вкладках.

2.6.13 Раздел «Правила управления»

Раздел «Правила управления» предназначен для управления приложениями на МСК, а именно:

- Автоматическая установка, обновление и удаление приложений;
- Установка приложений из Google Play и App Store;
- Автоматическое перемещение приложений в контейнер Knox;
- Настройка режима киоска: пользователю доступно только одно приложение на МСК;
- Взятие под управление «UEM SafeMobile» некорпоративных приложений пользователя;
- Ограничение доступа пользователя к приложению посредством «черного» списка.

ПУП назначается на выбранное приложение, установленное на МСК пользователя и зарегистрированное в «UEM SafeMobile». Список зарегистрированных приложений отображается в разделе «Объекты учёта/Приложения».

В левой части окна «Правила управления» (рисунок 2.74) отображается список созданных в системе ПУП, оформленный в виде таблицы.

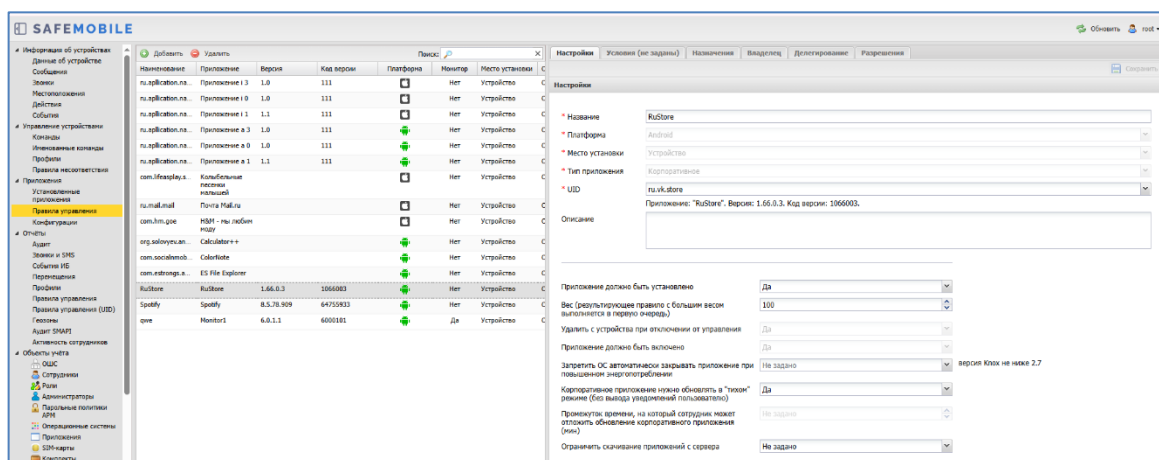


Рисунок 2.74 — Раздел «Правила управления»

Каждая строка списка содержит информацию об одном правиле для одного приложения. Таблица содержит следующие колонки данных:

- Колонки данных, отображающиеся по умолчанию:
 - Наименование — название правила;
 - Приложение — название приложения;

- Версия — версия приложения;
 - Код версии — «внутренний» номер версии приложения;
 - Платформа — платформа ОС;
 - Монитор — мобильный клиент SafeMobile (Да/Нет);
 - Место установки — Выбор места установки приложения доступен только для платформы Android (устройство / контейнер). Для прочих платформ место установки всегда — «устройство».
 - Сущность — инициатор сущности (собственный/делегированный);
 - Владелец — администратор узла ОШС, назначенный владельцем сущности;
 - Условие.
- Колонки данных опционального отображения:
 - UID — UID приложения;
 - Тип приложения — зависит от наличия дистрибутива в «UEM SafeMobile» (корпоративное/некорпоративное);
 - Приложение должно быть установлено — (Да/Нет/Не задано/Доступно в SafeStore);
 - Вес (результатирующее правило с большим весом выполняется в первую очередь);
 - Удалить с устройства при отключении от управления — Имеет значения «Да/Нет/Не задано»;
 - Приложение должно быть включено — только для МСК на платформе Android (Да/Нет/Не задано);

Примечание

Если для системного приложения задано значение «Нет», то на устройстве кнопка «Остановить» (в разделе настроек «Сведения о приложениях») будет оставаться активной несмотря на то, что приложение не запущено.

Если системное приложение отключено на устройстве через настройки пользователем, то оно не может быть включено средствами MDM.

- Приложение можно настраивать удалённо — только для МСК на платформе iOS (Да/Нет/Не задано);

- Запрещено резервное копирование данных — только для МСК на платформе iOS (Да/Нет/Не задано);
- Запретить закрытие приложения — Запретить ОС автоматически закрывать приложение при повышенном энергопотреблении. Только для МСК на платформе Android (Да/Нет);
- Использовать VPN для приложений (Per-App VPN) — только для МСК на платформе iOS (Название профиля Per-App VPN соединения/Нет);
- Корпоративное приложение нужно обновлять в «тихом» режиме (без вывода уведомлений пользователю);
- Промежуток времени, на который сотрудник может отложить обновление корпоративного приложения (мин);
- Получать обратную связь от приложения. Целевое приложение должно поддерживать механизм 'Applications Feedback';
- Отправлять данные обратной связи приложения не чаще чем один раз в (мин).

В верхней части таблицы находится панель инструментов с кнопками:

- Добавить — предназначена для создания нового ПУП;
- Удалить — предназначена для удаления, уже созданного ПУП.

Примечание

Единовременно на устройстве в контейнере и не в контейнере устройства может быть установлена только одна версия приложения.

Приложения, установленные пользователем на личном устройстве с рабочим профилем, могут влиять на управление приложениями в рабочем профиле через монитор и наоборот.

Таким образом, если на устройстве или в контейнере уже установлено целевое приложение, то при установке в другую управляемую область существуют следующие ограничения:

- Подписи приложений должны совпадать;
- Версии приложений должны совпадать, либо версия устанавливаемого приложения должна быть выше, чем у установленного.

2.6.13.1 Создание нового Правила управления приложениями

Чтобы создать новое «правило управления приложениями», необходимо выполнить следующие действия:

1. Перейти в раздел «Правила управления»;
2. Нажать кнопку «Добавить», после чего откроется форма создания нового правила (рисунок 2.75);

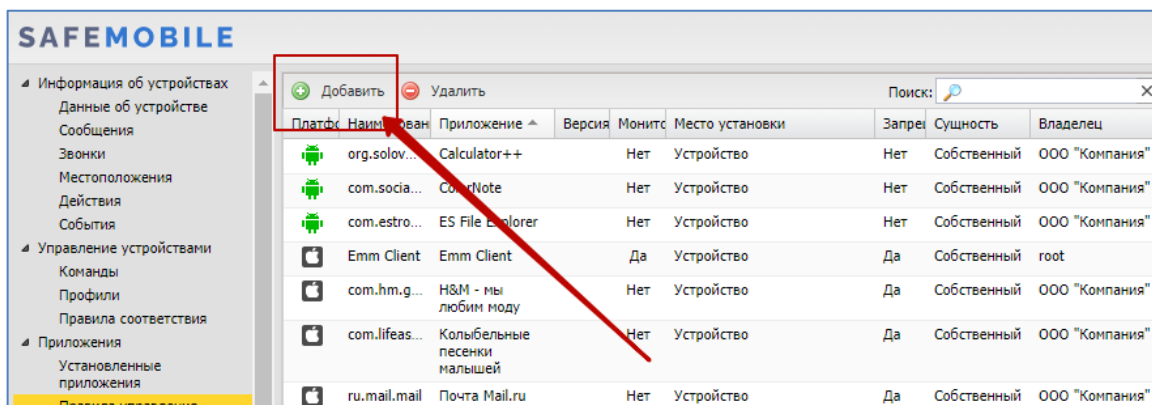


Рисунок 2.75 — Кнопка «Добавить» правило

3. Во вкладке «Настройки» заполнить все необходимые поля ввода данных;
4. Нажать кнопку «Сохранить», после чего новое правило будет сохранено в системе;
5. (Только для Android) При необходимости настроить разрешения для приложения (см. Управление разрешениями приложений 2.6.12.6);
6. Перейти во вкладку «Назначение»;
7. Выбрать пользователей, к которым будет применено новое правило;
8. Нажать кнопку «Сохранить», после чего новое правило становится действующим (см. 2.6.11.6. «Применение ПУП»).

В зависимости от того какие будут выбраны значения в полях «Платформа» и «Тип приложения» становятся доступны дополнительные поля ввода данных:

Поля ввода данных для платформы iPhone OS

- Приложение должно быть установлено:
 - Да,
 - Нет,
 - Не задано,
- Доступно в SafeStore (только для корпоративного приложения),
- Вес (результатирующее правило с большим весом выполняется в первую очередь) — по умолчанию 100;

- Приложение можно настраивать удаленно (всегда «ДА»);
- Удалить с устройства при отключении от управления;
Доступно для ввода, если:
 - Значение поля «Тип приложения» является «Не корпоративное»;
 - Значение поля «Приложение должно быть установлено» является «Да»;
- Запрещено резервное копирование данных — (доступно для ввода, если «Тип приложения» — Не корпоративное);
- Использовать VPN для приложений (Per-App VPN) — для версии iOS не ниже 14.0.

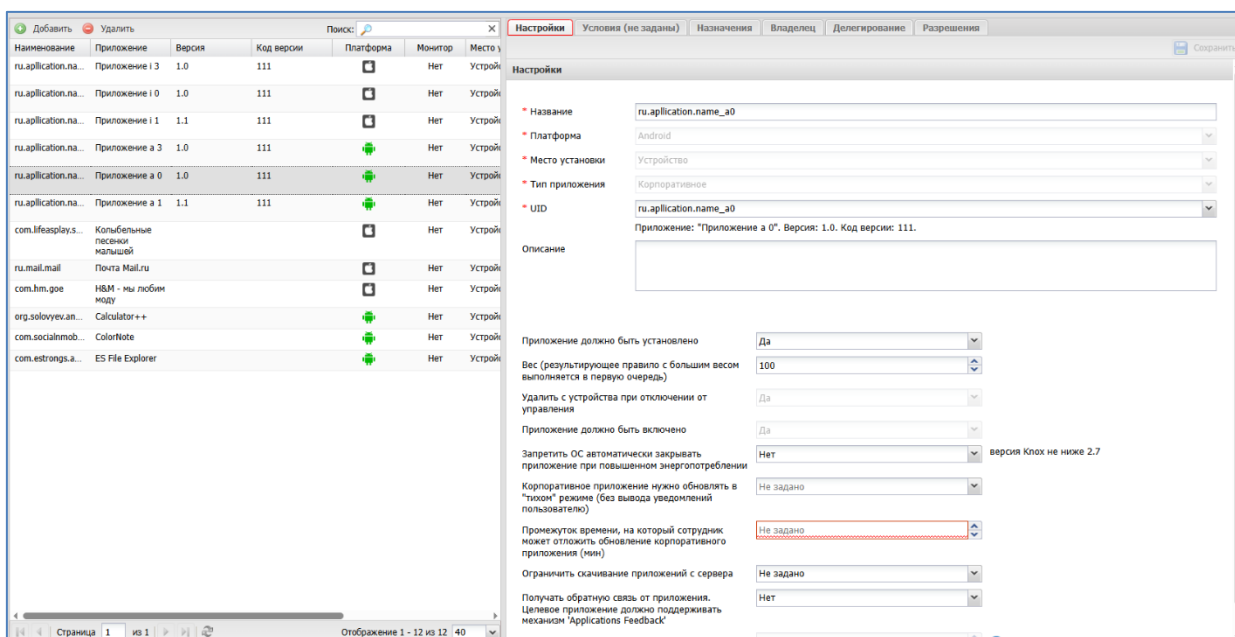


Рисунок 2.76 — Поля ввода данных для платформы iPhone OS

Поля ввода данных для платформы Android

- Приложение должно быть установлено:
 - Да,
 - Нет,
 - Не задано,
 - Доступно в SafeStore (только для корпоративного приложения),
- Вес (результатирующее правило с большим весом выполняется в первую очередь) — по умолчанию 100;
- Удалить с устройства при отключении от управления.
Доступно для ввода, если:

- Значение поля «Тип приложения» является «Не корпоративное»;
- Значение поля «Приложение должно быть установлено» является «Да» или «Не задано»;

Важно!

Данная политика не применима к приложению «Монитор».

- Приложение должно быть включено;
Доступно для ввода, если:
 - Значение поля «Тип приложения» является «Не корпоративное»;
- Запретить ОС автоматически закрывать приложение при повышенном энергопотреблении;
- Корпоративное приложение нужно обновлять в «тихом» режиме (без вывода уведомлений пользователю) — активно, если значение параметра «Приложение должно быть установлено» — «Да». При обновлении приложения пользователь получит соответствующее уведомление;
- Промежуток времени, на который сотрудник может отложить обновление корпоративного приложения (мин) — значение от 0 до 180. Активно, если приложение «корпоративное» и значение параметра «Приложение нужно обновлять в «тихом» режиме» — нет. Если задано значение не равное нулю, то система, в течение 2 минут будет ожидать от пользователя одно из следующих действий:
 - Обновить;
 - Отложить обновление на 10% от промежутка времени, заданного в ПУП в минутах. Отображается если 10% больше 5 мин.
 - Отложить обновление на 30% от промежутка времени, заданного в ПУП в минутах. Отображается только если 30% больше 5 мин.
 - Отложить обновление на промежуток времени, заданный в ПУП.
 - По истечении 2 минут, при отсутствии реакции пользователя приложение будет обновлено автоматически.
- Ограничить скачивание корпоративных приложений с сервера — устанавливает ограничения на скачивание приложения. Заданные в этих настройках значения, имеют больший приоритет, чем политики профиля «Сетевые подключения Android»:
 - Скачивать только по Wi-Fi,
 - Скачивать по Wi-Fi и в домашней сети,
 - Скачивать при любом подключении,

- Не задано.
- Получать обратную связь от приложения. Целевое приложение должно поддерживать механизм 'Applications Feedback' — позволяет приложениям отправлять на устройство уведомления о своем состоянии и событиях.
- Отправлять данные обратной связи приложения не чаще чем один раз в (мин).

Настройки	Условия	Назначения	Владелец	Делегирование	Разрешения
Настройки					
Название	ru.application.name_a0				
Платформа	Android				
Место установки	Устройство				
Тип приложения	Корпоративное				
UID	ru.application.name_a0				
Описание	Приложение: "Приложение а 0". Версия: 1.0. Код версии: 111.				
Приложение должно быть установлено	Да				
Вес (результатирующее правило с большим весом выполняется в первую очередь)	100				
Удалить с устройства при отключении от управления	Да				
Приложение должно быть включено	Да				
Запретить ОС автоматически закрывать приложение при повышенном энергопотреблении	Нет				
Корпоративное приложение нужно обновлять в "тихом" режиме (без вывода уведомлений пользователю)	Не задано				
Промежуток времени, на который сотрудник может отложить обновление корпоративного приложения (мин)	1				
Ограничить скачивание приложений с сервера	Не задано				
Получать обратную связь от приложения. Целевое приложение должно поддерживать механизм 'Applications Feedback'	Да				
Отправлять данные обратной связи приложения не чаще чем один раз в (мин)	60				

Рисунок 2.77 — Поля ввода данных для платформы Android

Поля ввода данных для платформы Windows

- Приложение должно быть установлено — всегда «Да»;
- Вес (результатирующее правило с большим весом выполняется в первую очередь) — по умолчанию 100;

Настройки | Условия (не заданы) | Назначения | Владелец | Делегирование

Настройки

* Название

* Платформа: Windows

* Тип приложения: Корпоративное

* UID

Описание

Приложение должно быть установлено: Да

Вес (результатирующее правило с большим весом выполняется в первую очередь): 100

Рисунок 2.78 — Поля ввода данных для платформы Windows

Поля ввода данных для платформы AuroraOS

- Приложение должно быть установлено:
 - Да,
 - Нет,
 - Доступно в SafeStore,
- Вес (результатирующее правило с большим весом выполняется в первую очередь) — по умолчанию 100;

Настройки | Условия (не заданы) | Назначения | Владелец | Делегирование

Настройки

* Название

* Платформа: AuroraOS

* Тип приложения: Корпоративное

* UID

Описание

Приложение должно быть установлено: Да

Вес (результатирующее правило с большим весом выполняется в первую очередь): 100

Рисунок 2.79 — Поля ввода данных для платформы AuroraOS

Поля ввода данных для платформ Linux (Altlinux, Astra, Debian)

- Приложение должно быть установлено:
 - Да,

- Нет,
- Вес (результатирующее правило с большим весом выполняется в первую очередь) — по умолчанию 100;
- Автоматически обновлять приложение;

Доступно для ввода, если:

- Значение поля «Тип приложения» является «Не корпоративное».

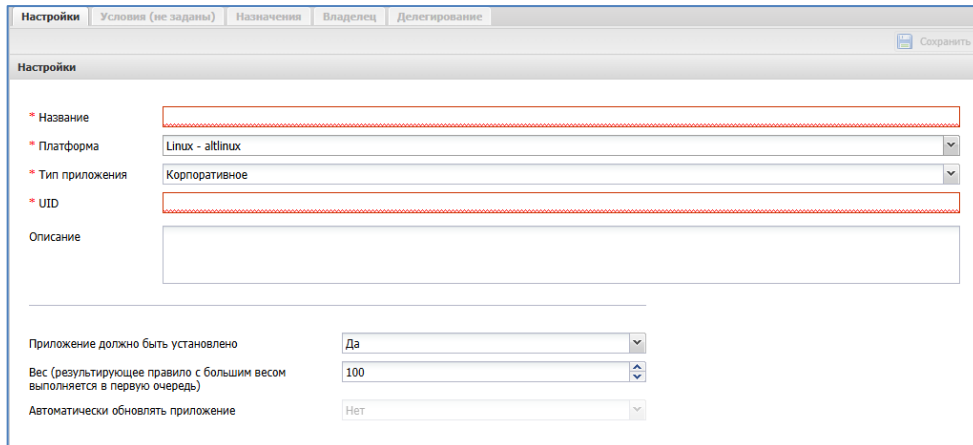


Рисунок 2.80 — Поля ввода данных для платформ Linux (Altlinux, Astra, Debian)

2.6.13.2 Задание условий применения ПУП

После заполнения формы ПУП и сохранения настроек выбрать условия применения ПУП во вкладке **«Условия»** в соответствии с описанием задания условий применения профиля раздел 2.6.9.3.

2.6.13.3 Назначение ПУП

Для назначения ПУП во вкладке **«Назначения»** (рисунок 2.81) в окне ОШС выбрать подразделение(я)/сотрудника(ов) или в главной таблице выбрать одно или несколько МСК сотрудников в соответствии с 2.6.8.4.

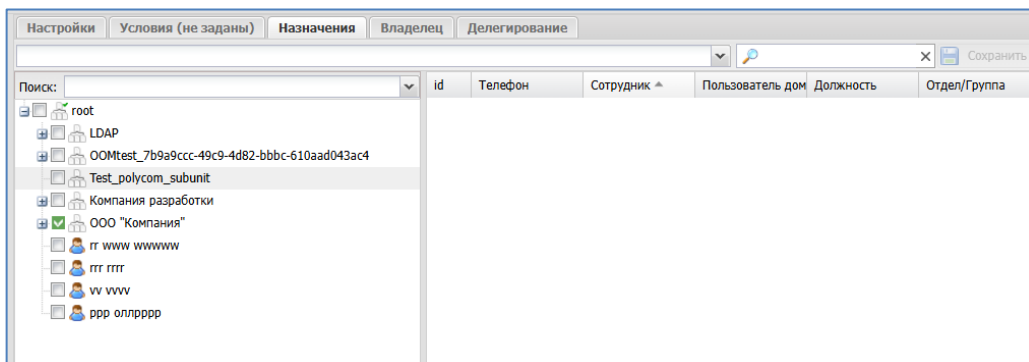


Рисунок 2.81 — Назначение ПУП

2.6.13.4 Смена владельца сущности

Для смены владельца сущности, во вкладке **«Владелец»** следует выбрать узел ОШС (рисунок 2.82) в окне ОШС в соответствии с 2.6.8.5.

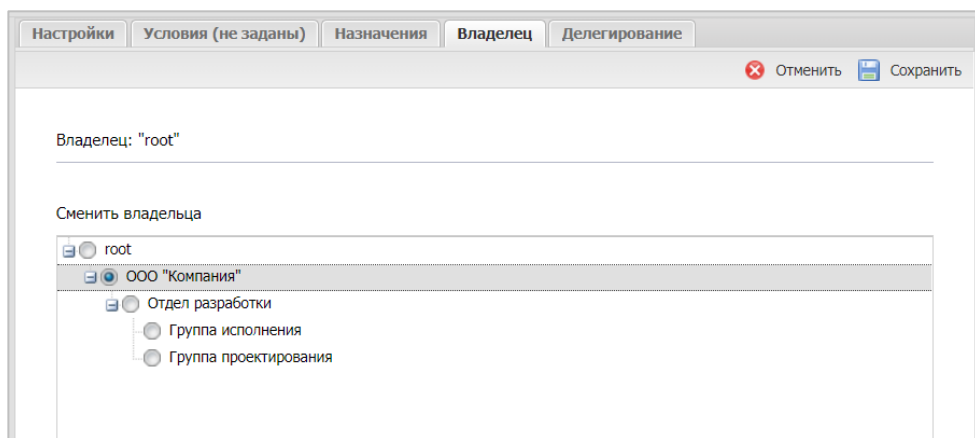


Рисунок 2.82 — Смена владельца сущности

2.6.13.5 Делегирование сущности

Для делегирования сущности, во вкладке «Делегирование» следует выбрать один или несколько объектов ОШС (рисунок 2.83) в окне ОШС в соответствии с 2.6.8.6.

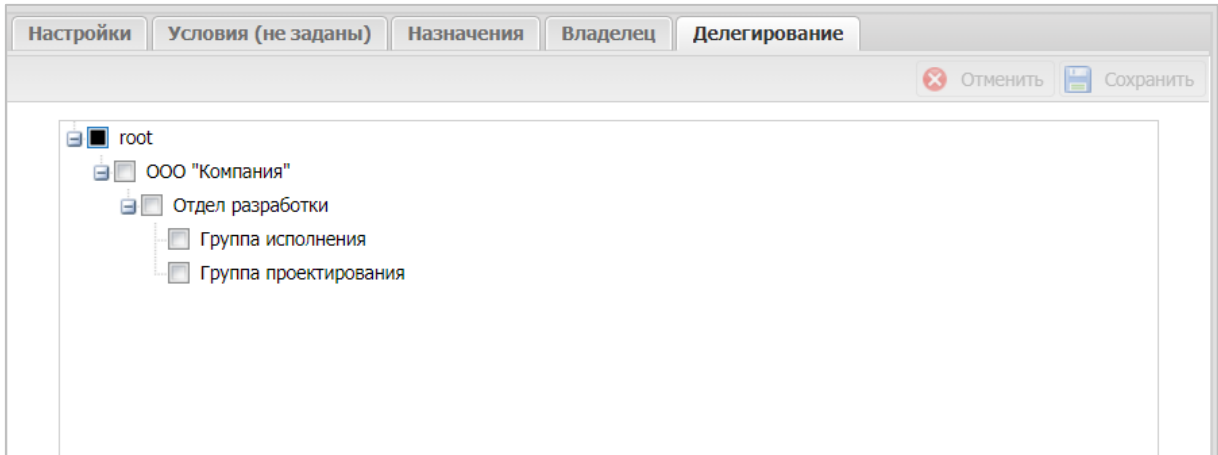


Рисунок 2.83 — Делегирование сущности

2.6.13.6 Управление разрешениями приложений (Android)

Вкладка «Разрешения» появляется после сохранения созданного правила управления приложениями (рисунок 2.84).

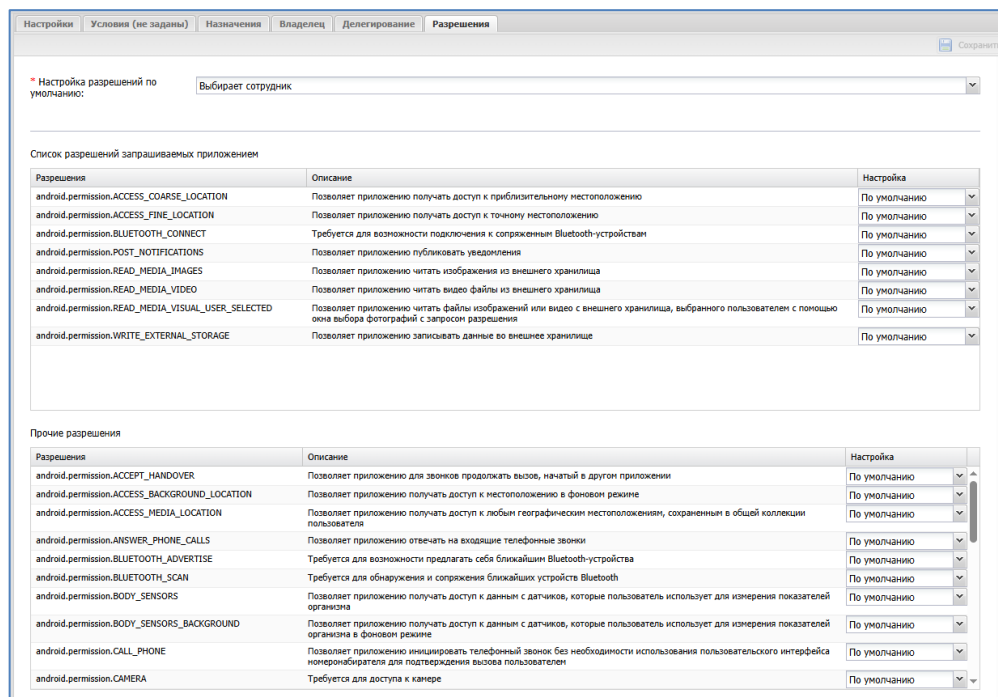


Рисунок 2.84 — Вкладка «Разрешения»

Вкладка содержит следующие настройки разрешений приложений:

- Настройка разрешений по умолчанию — задаёт значение разрешений, заданных «по умолчанию». Разрешениям «по умолчанию» могут быть заданы следующие значения:
 - Запретить,
 - Разрешить — устанавливается по умолчанию для корпоративных приложений;
 - Выбирает сотрудник — устанавливается по умолчанию для некорпоративных приложений;
- Таблица «Список разрешений запрашиваемых приложением» — содержит только опасные разрешения дистрибутива выбранного в ПУП. Отображается только для корпоративных приложений. Каждая строка списка должна содержать:
 - Разрешение — название разрешения;
 - Описание — описание разрешения;
 - Настройка — значение разрешения:
 - По умолчанию — это значение для настройки определяется в опции «Настройка разрешений по умолчанию»;
 - Запретить — запретить разрешение;
 - Разрешить — разрешить разрешение;
 - Выбирает сотрудник — разрешение устанавливает пользователь МСК;
- Таблица «Прочие разрешения» (для некорпоративных приложений имеет название «Разрешения»). Структура аналогична таблице «Список разрешений запрашиваемых приложением» и содержит следующие данные:
 - Для корпоративного приложения — содержит те разрешения из справочника опасных разрешений Android (<https://developer.android.com/reference/android/Manifest.permission>), которые не вошли в список разрешений запрашиваемых приложением;
 - Для некорпоративного приложения — содержит все разрешения из справочника опасных разрешений Android.

Примечание

Если при редактировании ПУП происходит смена дистрибутива, то система перестроит список опасных разрешений. Если состав разрешений изменится, то

вкладка «Разрешения» будет помечена красным цветом, а кнопка «Сохранить» станет не доступной.

Кнопка «Сохранить» будет разблокирована после перехода на вкладку «Разрешения», в которой зеленым цветом будут помечены изменения в разрешениях.

2.6.13.7 Применение ПУП

При создании и использовании ПУП необходимо учитывать следующую информацию:

Для всех платформ:

- Если при создании правила, в поле «Приложение должно быть установлено» стоит значение «Нет», то приложение, **установленное пользователем**, будет автоматически удалено с устройства, а при невозможности удаления — отключено;
- При добавлении ПУП следует учитывать, что профили имеют больший приоритет перед ПУП. Например, если в примененном профиле присутствуют политики, запрещающие отдельные приложения, а ПУП эти приложения разрешает, то в этом случае приложение будет запрещено.
- При изменении значения параметра ПУП **«Удалить с устройства при отключении от управления»** с «Да» на «Нет», а синхронизация настроек задержалась, например, из-за нахождения МСК в статусе «Не в сети», тогда будет применено первое значение и приложение удалится с устройства.

Для iPhone OS:

- Если при создании правила, в поле «Приложение должно быть установлено» стоит «ДА», при этом МСК не находится в режиме «supervised» (см. данные об устройстве), то для действия с ним будет запрошено подтверждение пользователя;
- Для исключения несанкционированного распространения корпоративных данных через некорпоративные приложения, при создании ПУП следует установить значения «Да» для параметров:
 - «Приложение можно настраивать удалённо»,
 - «Удалить с устройства при отключении от управления»,
 - «Запрещено резервное копирование данных».
- На МСК в режиме «supervised» версии iOS 14.0 и выше пользователь не сможет удалить приложение, установленное системой. На МСК без «supervised» пользователь может удалить приложение, но система будет пытаться повторно установить приложение, запрашивая у пользователя подтверждение.
- Для приложений на МСК платформы iOS после применения ПУП с параметром **«Приложение можно настраивать удалённо»**, невозможно обратное действие: сделать приложение неуправляемым.

Для Android:

- При установке корпоративных приложений на МСК платформы Android следует учитывать, что на время установки снимается блокировка установки из недоверенных источников.
- При установке корпоративного приложения на МСК платформы Android, приложение проверяется сервисом ОС «**Play Protect**». Если сервис посчитает приложение вредоносным, он может приостановить установку приложения и предложить пользователю удалить данное приложение. Монитор не может повлиять на статус приложения в сервисе. Так как сервис «**Play Protect**» является частью приложения «**Google Play**», то отключение магазина приложений позволяет отключать проверку приложений сервисом «**Play Protect**».
- В связи с тем, что платформа Android не допускает установку двух разных версий одного приложения и в контейнер, и на устройство, то в случае, если на МСК Android назначены два правила одного корпоративного приложения с разными местами установки, а версии приложения различаются, то будет произведена установка только в одно место: или в контейнер или на устройство.
- Если устройство подключено стратегиями «Личный рабочий профиль», либо «Корпоративный рабочий профиль», то приложение не будет автоматически удалено из контейнера устройства, а потребует подтверждение удаления приложения пользователем. Подтверждение необходимо выполнить в приложении «Монитор», вкладка «Приложения».

2.6.13.8 Особенности при удалении ПУП

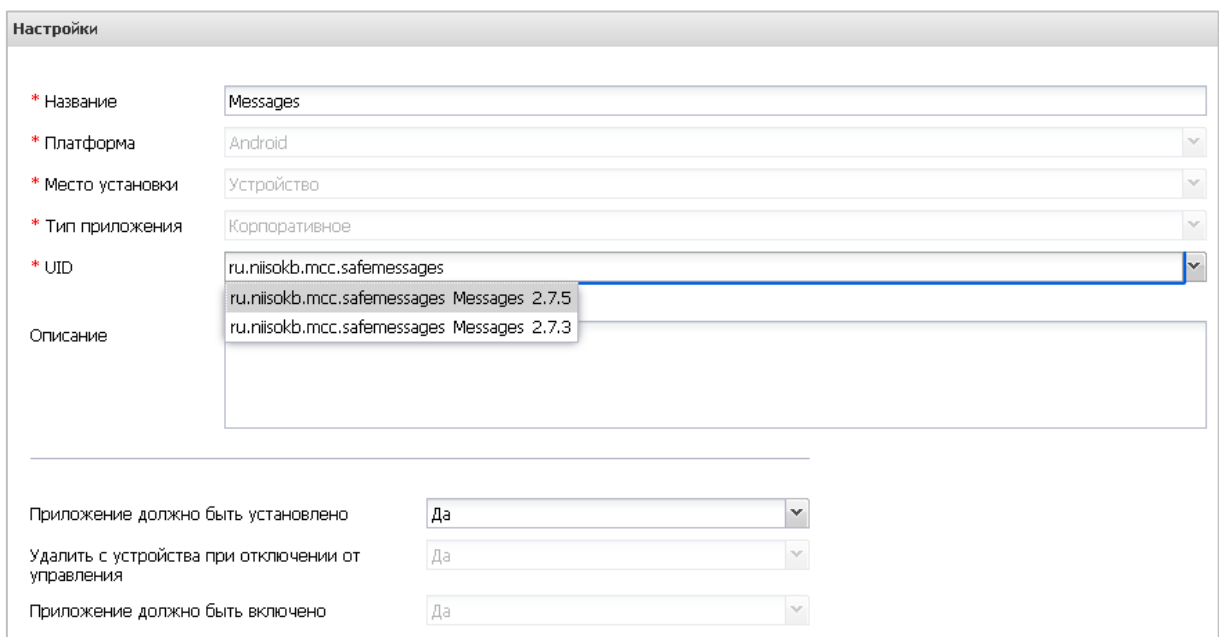
Для платформы Android.

Особенность корпоративного ПУП, предназначенного для обновления системного приложения (встроенного приложения от производителя устройства). Если удалить данное ПУП, то системное приложение удалено не будет. Но если монитор установлен с правами Device Owner в соответствии с разделом 2.6.8, в этом случае будет удалено обновление системного приложения.

2.6.13.9 Особенности обновления приложений

При необходимости обновить корпоративное приложение на устройствах, необходимо загрузить новую версию в раздел «**Приложения**» и определиться с ПУП.

- 1) Если новую версию необходимо сначала протестировать на ограниченном списке сотрудников, рекомендуется создать новое правило и назначить его на тестовые устройства. Произойдет обновление до новой версии приложения только на тестовых устройствах. После проведения всех проверок и подтверждения готовности новой версии к распространению, необходимо внести правки в основное правило для этого приложения, а временное правило потом можно будет удалить.
- 2) Если сразу или после тестирования новая версия готова к распространению, необходимо внести изменение в правило управления, созданное ранее для предыдущей версии. Тогда все **Назначения** сохранятся и произойдет автоматическое обновление приложения на всех целевых устройствах. Для внесения исправления в правило управления, необходимо через поле **UID** вызвать список доступных версий и выбрать новую в соответствии с рисунком 2.85.



Настройки

* Название: Messages

* Платформа: Android

* Место установки: Устройство

* Тип приложения: Корпоративное

* UID: ru.niisokb.mcc.safemessages

Описание: ru.niisokb.mcc.safemessages Messages 2.7.5
ru.niisokb.mcc.safemessages Messages 2.7.3

Приложение должно быть установлено: Да


Удалить с устройства при отключении от управления: Да

Приложение должно быть включено: Да

Рисунок 2.85 — Выбор версии приложения

- 3) Для приложений на МСК платформе Windows не поддерживается обновление приложений. При назначении новой версии возникнет ошибка установки. Для установки новой версии приложения необходимо снять назначение ранее установленной версии приложения.

Таблица 2.4 — Параметры ПУП

Платформа	Тип приложения	Параметры ПУП					
		Приложение должно быть установлено	Приложение можно настраивать удалённо	Удалить с устройства при отключении от управления	Запрещено резервное копирование данных	Приложение должно быть включено	Запретить ОС автоматически закрывать приложение при повышенном энергопотреблении
	Корпоративное	Да (по умолчанию) Не задано Доступно в SafeStore	Да	Да	Да	-	-
		Нет	Да	Нет	Нет		
	Некорпоративное	Да (по умолчанию) Не задано	Да	Да (по умолчанию) Нет	Да (по умолчанию) Нет		
		Нет	Да	Нет	Нет		
	Корпоративное	Да (по умолчанию) Не задано Доступно в SafeStore	-	Да	-	Да	Да
		Нет		Нет		Нет	
	Некорпоративное	Да (по умолчанию) Не задано		Да (по умолчанию) Нет		Да (по умолчанию) Нет	Да (по умолчанию) Нет Не задано
		Нет		Нет		Нет	Нет
	Корпоративное	Да (по умолчанию)	-	-	-	-	-

2.6.14 Раздел «Конфигурации»

Пункт меню «**Конфигурации**» открывает окно (рисунок 2.86), предназначенное для управления настройками приложений на МСК посредством созданных конфигураций. В данном окне доступно создание, редактирование и удаление конфигураций, а также осуществление их назначений на МСК, сотрудника или подразделение.

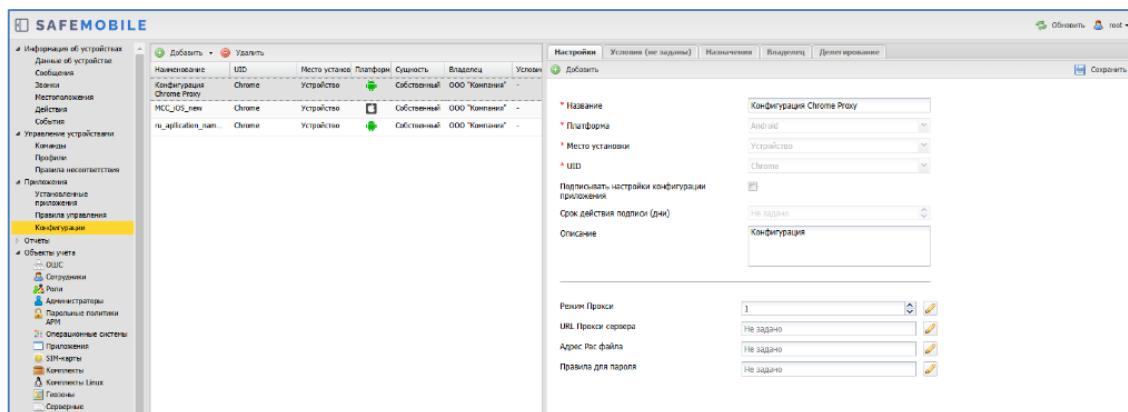


Рисунок 2.86 — Окно «Конфигурации»

Управление конфигурациями приложений осуществляется для МСК:

- на платформе iOS версий 10 и выше;
- на платформе Android для устройств Samsung с Knox версии 2.7, версия Android 5.0 и выше;
- на платформе Android для устройств других производителей, отличных от Samsung, версия Android 6.0 и выше».
- на платформе Аврора;
- на платформе Linux следующих дистрибутивов:
 - Linux — altlinux,
 - Linux — astra,
 - Linux — Debian.

В левой части окна «**Конфигурации**» отображается форма с реестром созданных в системе конфигураций приложений, таблица реестра содержит следующие столбцы:

- Наименование — название конфигурации приложения;

- UID — уникальный идентификатор приложения, к которому относится конфигурация;
- Версия — версия приложения;
- Код версии — код версии приложения;
- Место установки — контейнер (для МСК на платформе Android) или устройство;
- Платформа — платформа ОС;
- Сущность — инициатор сущности (собственный/делегированный/внешний);
- Владелец — администратор узла ОШС, назначенный владельцем сущности; по умолчанию, не отображается в форме;
- Условие.

В правой части окна отображается форма для настройки параметров конфигурации с вкладками:

- Настройки,
- Условия,
- Назначения,
- Владелец,
- Делегирование.

В верхней части таблицы находится панель инструментов со следующими кнопками:

- Добавить — предназначена для создания новой конфигурации;
 - Создать пустую конфигурацию;
 - Создать конфигурацию из шаблона;
- Удалить — предназначена для удаления уже созданной конфигурации.

2.6.14.1 Добавление конфигурации

Для добавления новой конфигурации раскройте выпадающий список справа от кнопки **«Добавить»** и выберите один из вариантов:

- Создать пустую конфигурацию;
- Создать конфигурацию из шаблона.

При выборе параметра **«Создать пустую конфигурацию»** откроется новая форма во вкладке **«Настройки»** в соответствии с рисунком 2.87. Поля, отмеченные * обязательные для заполнения.

- Название — Название конфигурации (обязательно для заполнения);
- Платформа — Выбор платформы МСК (обязательно для заполнения);
- Место установки — Доступно для изменения только для платформы Android. Для прочих платформ, значение поля автоматически устанавливается — «Устройство».

Для Android необходимо указать (обязательно для заполнения):

- «Устройство», если нужно применить Конфигурацию к приложению, размещенному на устройстве. Устройство должно быть подключено по стратегиям «Только устройство (Android)», либо «Устройство и контейнер KNOX (Samsung 5.0 — 9)»;
 - «Контейнер», если нужно применить Конфигурацию к приложению, размещенному в контейнере KNOX (Samsung 5.0 — 9) или рабочем профиле Android. Доступно только для МСК, подключенным по стратегиям «Устройство и контейнер KNOX (Samsung 5.0 — 9)», либо «Личный рабочий профиль (Android 7.0+)», либо «Корпоративный рабочий профиль (Android 11.0+)».
- UID — UID приложения, для которого настраивается конфигурация (обязательно для заполнения);
 - Подписывать настройки конфигурации приложения — Включение/выключение функции подписи конфигурации приложения. Позволяет приложению проверять подлинность конфигурации.

Примечание

*Для корректной работы данной настройки необходимо прописать в конфигурационный файл **mdm.yml** параметры **app_conf_cert** и **app_conf_key** (описание в **mdm_config.md**).*

*Для валидации подписи конфигурации можно использовать сервис **SMAPI**, в его конфигурационный файл **smapi.yml** (описание в **smapi_config.md**) должен быть добавлен параметр **app_conf_cert**.*

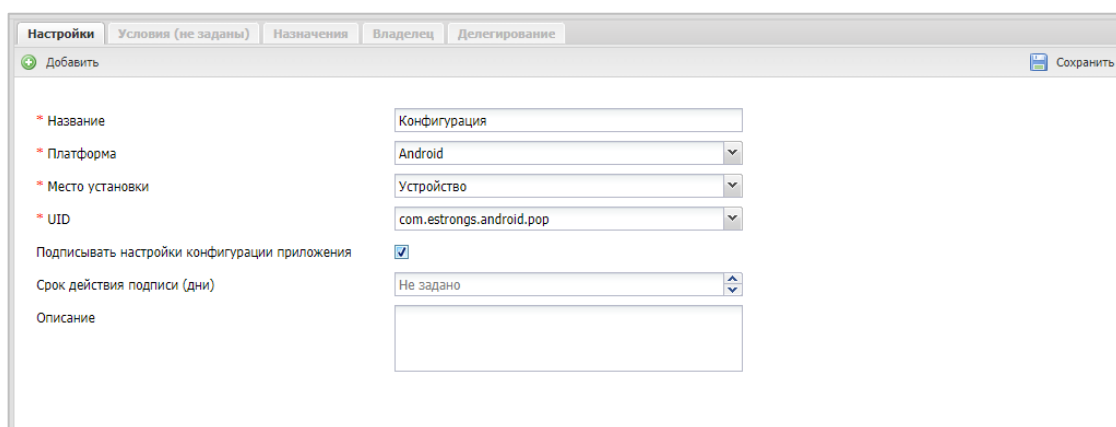
Описание параметров конфигурационных файлов указано в «Руководстве по установке и настройке Safe Mobile».

Если параметры отсутствуют или указаны неверно, то при попытке отправить подписанную конфигурацию приложения в логах MDM сервера будут указаны ошибки.

Пример записи об ошибке:

- `JWT not generated due to error`

- Срок действия подписи (дни) — Срок действия подписи, указывается в днях;
- Описание — Описание конфигурации.



The screenshot shows a web interface for adding a new configuration. At the top, there are tabs: 'Настройки' (selected), 'Условия (не заданы)', 'Назначения', 'Владелец', and 'Делегирование'. Below the tabs is a 'Добавить' button with a green plus icon and a 'Сохранить' button with a floppy disk icon. The form contains the following fields:

- * Название: Конфигурация
- * Платформа: Android
- * Место установки: Устройство
- * UID: com.estrongs.android.pop
- Подписывать настройки конфигурации приложения:
- Срок действия подписи (дни): Не задано
- Описание: (empty text area)

Рисунок 2.87 — Форма новой конфигурации

Для добавления параметров настройки приложения нажать кнопку **«Добавить»**, после чего отобразится форма создания настройки конфигурации (рисунок 2.88).

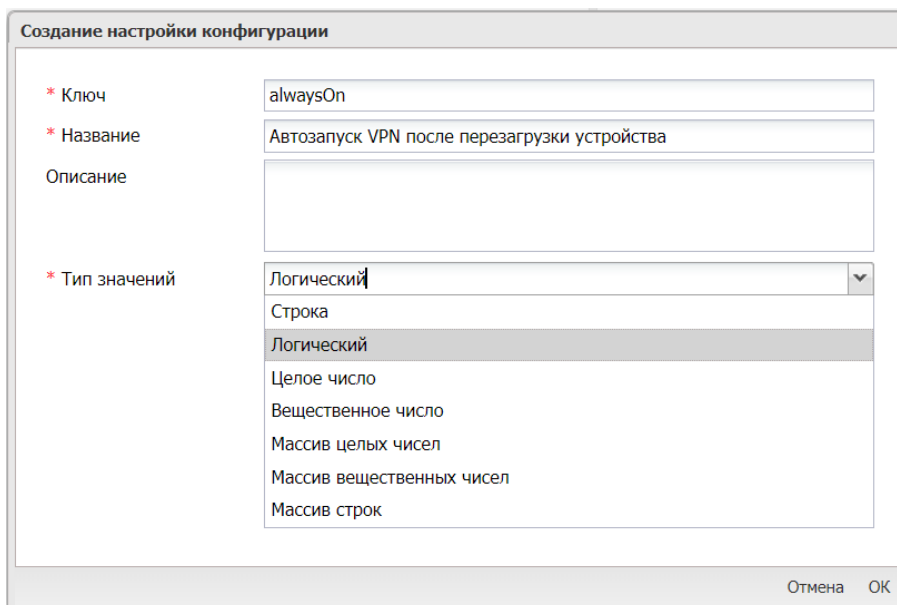


Рисунок 2.88 — Создание настройки конфигурации

Форма создания настройки конфигурации состоит из следующих полей:

- Ключ — обозначение настройки конфигурации, заданное разработчиком приложения МСК;
- Название — обозначение настройки в системе;
- Описание — краткое описание настройки;
- Тип значений — Строка / Логический / Целое число / Вещественное число / Массив целых чисел / Массив вещественных чисел / Массив строк.

В конфигурациях могут быть использованы подстановки, описанные в [«2.6.9.2 Настройка параметров профиля»](#).

Поля **«Ключ»**, **«Название»** и **«Тип значений»** обязательные для заполнения. После заполнения полей следует нажать кнопку **«ОК»**. Конфигурация может включать в себя одну или несколько настроек приложения.

Для добавления конфигурации из существующего шаблона следует нажать кнопку **«Добавить»** и выбрать вариант установки **«Создать конфигурацию из шаблона»**. После чего откроется окно выбора шаблона конфигураций приложений (рисунок 2.89). Шаблоны указанные в списке доступны в разделе **«Объекты учета — Шаблоны конфигураций»** ([см. раздел 2.8.9](#)).










Создание конфигурации приложения				
Приложение ^	UID	Версия	Код версии	Платформа
Платформа: Android				
CryptoPro NGate R2	ru.cprosp.NGateR2	-	-	
Gmail	com.google.android.gm	-	-	
Gmail	com.google.android.gm	-	-	
Gmail	com.google.android.gm	2025.08.25.800175820.Rele...	65311558	
HCL Verse	com.lotus.sync.traveler	-	-	
Kaspersky Endpoint Security	com.kaspersky.kes	-	-	
Outlook	com.microsoft.office.outlook	-	-	
Samsung Smart Switch Mobile	com.sec.android.easyMover	-	-	
Платформа: iPhone OS				
Outlook	com.microsoft.Office.Outlook	-	-	
Отмена <input type="button" value="OK"/>				

Рисунок 2.89 — Создание конфигурации приложения

В списке следует выбрать требуемый шаблон, нажать кнопку **«ОК»** для продолжения настроек конфигурации в форме (рисунок 2.90) и возможности редактирования параметров. Параметры конфигурации в форме будут зависеть от выбранного шаблона. В конфигурации созданной из шаблона присутствуют все доступные параметры, следовательно кнопка **«Добавить»** будет не активна.

После заполнения всех необходимых полей для сохранения настроек конфигурации нажать кнопку **«Сохранить»**.

После заполнения формы и сохранения настроек (опционально) следует задать условия применения конфигурации во вкладке **«Условия»** в соответствии с описанием задания условий применения профиля раздел 2.6.9.3.

Настройки | Условия (не заданы) | Назначения | Владелец | Делегирование

Добавить | Сохранить

* Название: Новая конфигурация

* Платформа: Android

* Место установки: Устройство

* UID: com.lotus.sync.traveler

Подписывать настройки конфигурации приложения:

Срок действия подписи (дни): 1

Описание:

* URL сервера Traveler: {{employee.exchange.emp_email}}

* ИД пользователя: {{employee.exchange.emp_email}}

Пароль: Не задано

Почта: Усекать почту до: Не задано

Заблокировать усечение почты: Нет

Почта: Автоматически загружать вложенные изображения размером до: Не задано

Заблокировать автоматическую загрузку вложенных изображений размером до: Нет

Почта: Автоматически загружать вложения размером до: Не задано

Заблокировать автоматическую загрузку вложений размером до: Нет

Почта: Удалить сообщения, которые хранятся дольше: Не задано

Рисунок 2.90 — Шаблон КП

2.6.14.2 Назначение конфигурации

Чтобы назначить конфигурацию, необходимо выполнить следующие действия:

1. Выбрать конфигурацию в списке, после чего в блоке настроек будут отображены параметры конфигурации;
2. Во вкладке «Назначения», выбрать объект назначения (рисунок 2.91):

- В окне ОШС — подразделение, сотрудник;
- В окне устройств выбрать одно или несколько МСК сотрудников в соответствии с 2.6.8.4;

Для удобства можно использовать поиск по следующим параметрам таблицы:

- id,
- Телефон,
- Сотрудник,
- Пользователь домена,
- Отдел/группа,
- Метка.

3. Нажать кнопку «Сохранить».

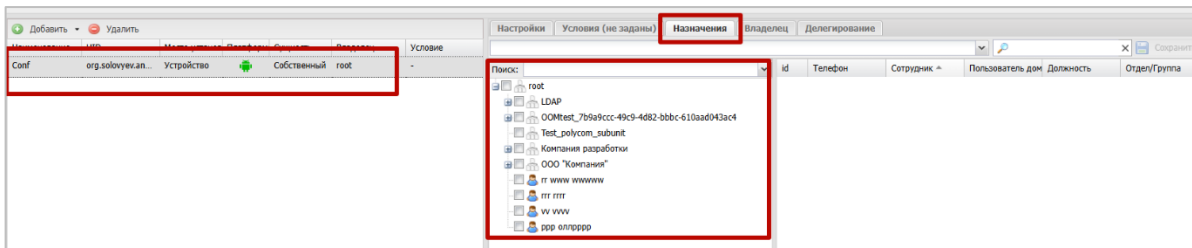


Рисунок 2.91 — Назначение конфигурации

2.6.14.3 Смена владельца сущности

Для смены владельца сущности во вкладке **«Владелец»** следует выбрать узел ОШС (рисунок 2.92) в окне ОШС в соответствии с 2.6.8.5.

Для сохранения изменений в системе следует нажать на кнопку **«Сохранить»**.

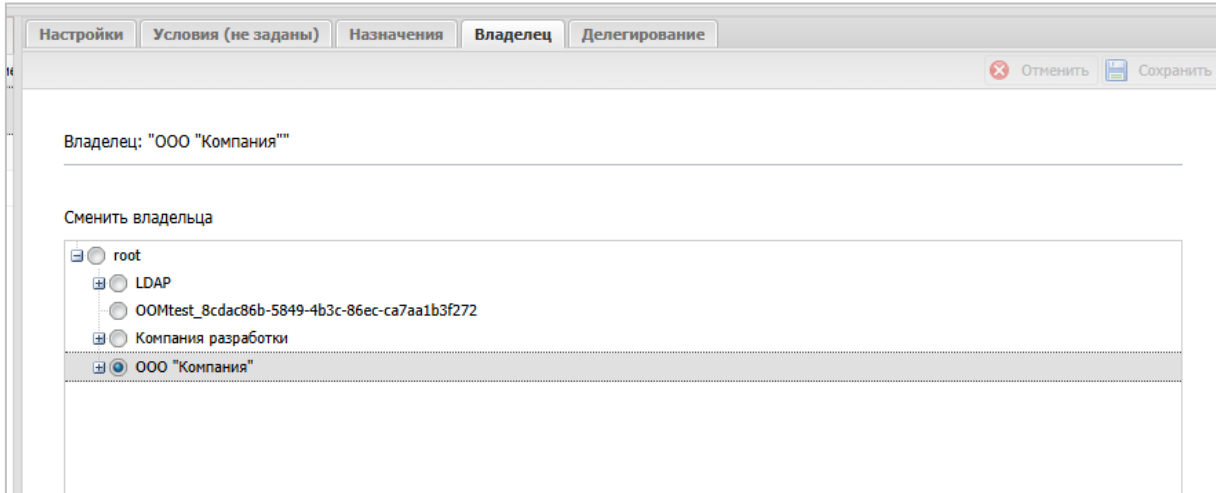


Рисунок 2.92 — Смена владельца сущности

2.6.14.4 Делегирование сущности

Для делегирования сущности во вкладке **«Делегирование»** следует выбрать один или несколько объектов ОШС (рисунок 2.93) в окне ОШС в соответствии с 2.6.8.6.

Для сохранения изменений в системе следует нажать на кнопку **«Сохранить»**.

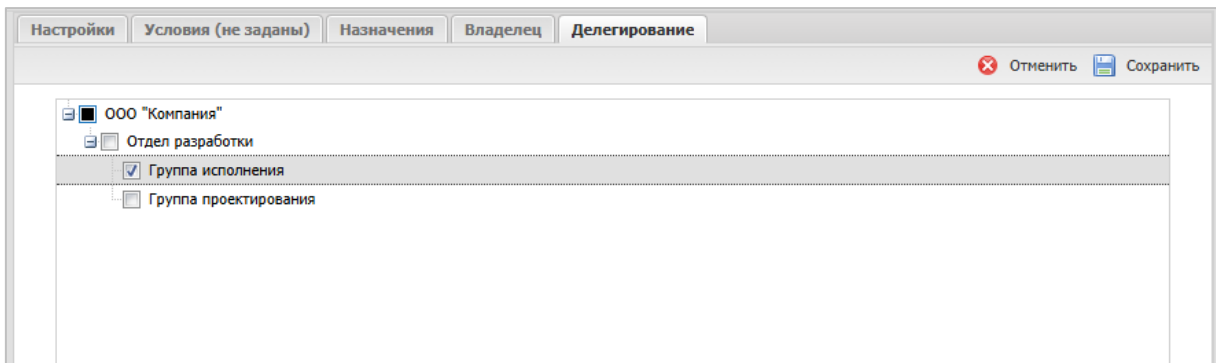


Рисунок 2.93 — Делегирование сущности

2.7 Построение отчётов (пункт меню «Отчёты»)

В разделе главного меню «Отчёты» формируются следующие отчёты:

- Аудит,
- Звонки и SMS,
- События ИБ,
- Перемещения,
- Профили,
- Правила управления,
- Правила управления (UID),
- Геозоны.

2.7.1 Отчёт «Аудит»

Для формирования отчёта выберите пункт главного меню «Аудит». В открывшемся окне отображается таблица с перечнем действий администраторов в АРМ «UEM SafeMobile», произошедших в заданном интервале времени, и их результатов в соответствии с рисунком 2.94.

Транзакция	Администратор	Пользователь, имя пользователя	Место работы	Должность	Область управления	Действие	Тип операции	Время	Результат
117914	Администра...	root			root	Запрос списка всех комплектов	Чтение	01.07.2025 13:45:55	Успешное завершение
117911	Администра...	root			root	Список меток устройств из справочника	Запись	01.07.2025 13:45:53	Успешное завершение
117904	Администра...	root			root	Запрос списка операционных систем	Чтение	01.07.2025 13:45:44	Успешное завершение
117897	Администра...	root			root	Список непосредственно подчинённых узлов дерева OHS	Запись	01.07.2025 13:45:44	Успешное завершение
117893	Администра...	root			root	Шаблон QR для OHS	Запись	01.07.2025 13:45:44	Успешное завершение
117888	Администра...	root			root	Список меток устройств из справочника	Запись	01.07.2025 13:45:43	Успешное завершение
117869	Администра...	root			root	Получение списка соединений с серверами EMM	Чтение	01.07.2025 13:45:43	Успешное завершение
117866	Администра...	root			root	Справочник параметров шаблона QR	Запись	01.07.2025 13:45:42	Успешное завершение
117863	Администра...	root			root	Список значений политики "UPM/IDM" профили с типом "URL" для приложений (One App UPM) iOS администраторов	Чтение	01.07.2025 13:45:41	Успешное завершение
117859	Администра...	root			root	Получение области управления администратора или поддерева OHS внутри области управления	Чтение	01.07.2025 13:45:40	Успешное завершение
117855	Администра...	root			root	Проверка наличия любого из удалённых внешнего каталога	Чтение	01.07.2025 13:45:40	Успешное завершение
117852	Администра...	root			root	Проверка необходимости смены пароля администратора	Чтение	01.07.2025 13:45:40	Успешное завершение
117847	Администра...	root			root	Регистрация результата логина администратора	Запись	01.07.2025 13:45:40	Успешное завершение


Рисунок 2.94 — Окно отчёта «Аудит»

Сформированный отчёт содержит следующие столбцы:

- Транзакция — номер операции в системе (по умолчанию, в таблице не отображается);
- Администратор — ФИО администратора, выполнившего действие в системе;
- Пользователь домена — Отображает ФИО администратора (отображает e-mail, если ФИО не было импортировано)
- Имя пользователя — имя пользователя (логин) администратора, выполнившего действие в системе;
- Место работы — место работы по штатному расписанию;

- Должность — должность по штатному расписанию;
- Область управления — узел поддерева ОШС, на который назначен администратор;
- Действие — действие, выполненное администратором в системе;
- Тип операции — вид операции с данными (чтение/запись);
- Время — дата и время выполнения действия;
- Параметры — параметры выполненного действия (по умолчанию, в таблице не отображается);
- Результат — результат выполнения действия, инициированного администратором;
- Код завершения — 0 — успешное завершение, 1 — ошибка (по умолчанию, в таблице не отображается).

Положительные результаты выполненных действий воспроизводятся зеленым цветом, а отрицательные — красным.

Для просмотра дополнительной информации по действию следует в столбце **«Администратор»** нажать значок  (при его наличии).

Для настройки отображаемых в отчёте сведений используется окно настроек (рисунок 2.95), открывающееся нажатием кнопки **«Настроить фильтры»** в верхней панели инструментов.

В окне настроек параметров отчёта можно выбрать период, для которого создаётся отчёт. Для этого используются поля ввода даты/времени **«Отчёт за период с»**, **«по»** (для начальной и конечной даты соответственно) в верхней части окна настроек. После нажатия на кнопку со значком календаря, выберите год, месяц, день и время начала и конца отчёта по аудиту действий администраторов в системе.

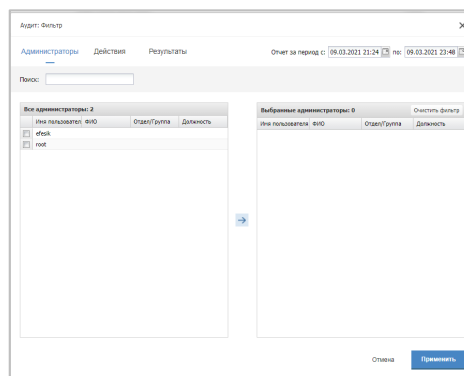


Рисунок 2.95 — Окно настроек параметров отчёта «Аудит»

Кроме того, в окне настроек отчёта можно настроить фильтры выводимых результатов на следующих вкладках:

Администраторы — позволяет выбрать администраторов, действия которых будут отображены в отчёте;

Действия — позволяет выбрать действия администраторов в системе, которые будут отображены в отчёте;

Результаты — позволяет выбрать результаты действий администраторов в системе, которые будут отображены в отчёте.

Чтобы выбрать требуемые позиции в реестрах **«Администраторы»**, **«Действия»** и **«Результаты»**, установите флажки в перечне слева и нажмите кнопку со стрелкой, после чего выбранные элементы появятся в перечне справа. Можно также просто перенести элемент из левого перечня в правый с помощью мыши. При выборе верхней строки в раскрывающихся реестрах, будут выделены все перечисления.

Окно настроек **«Действия»** (рисунок 2.96) содержит флажки **«Чтение»** и **«Запись»**. При установке флажка **«Запись»** в перечне отображаются действия администраторов с возможным редактированием данных, при установке флажка **«Чтение»** отображаются действия только с просмотром данных. Если установлены оба флажка, список содержит перечень всех имеющихся в системе действий администраторов.

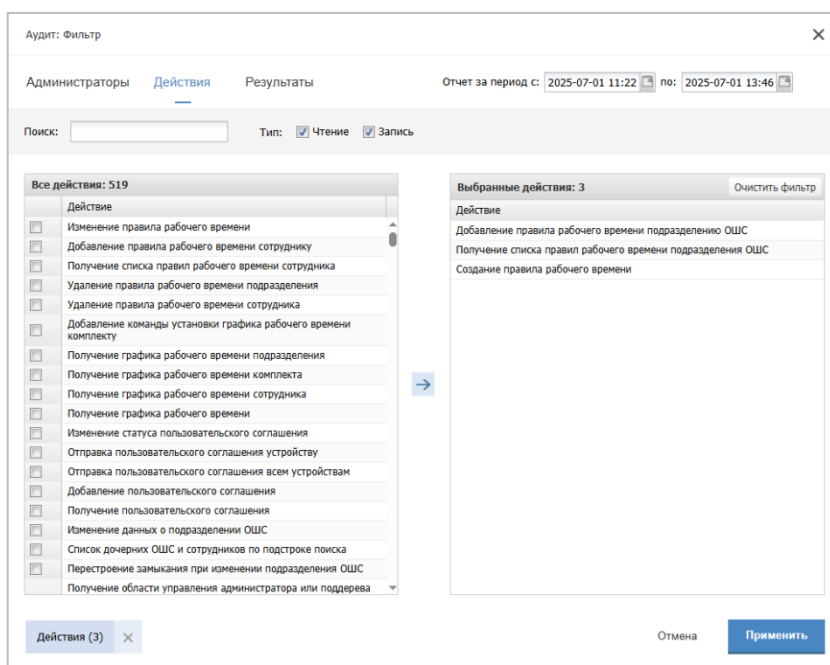


Рисунок 2.96 — Окно **«Действия»** в настройках параметров отчёта **«Аудит»**

Для осуществления поиска по ключевому слову в реестрах параметров отчёта «Аудит» предназначено окно «Поиск» (рисунок 2.97).

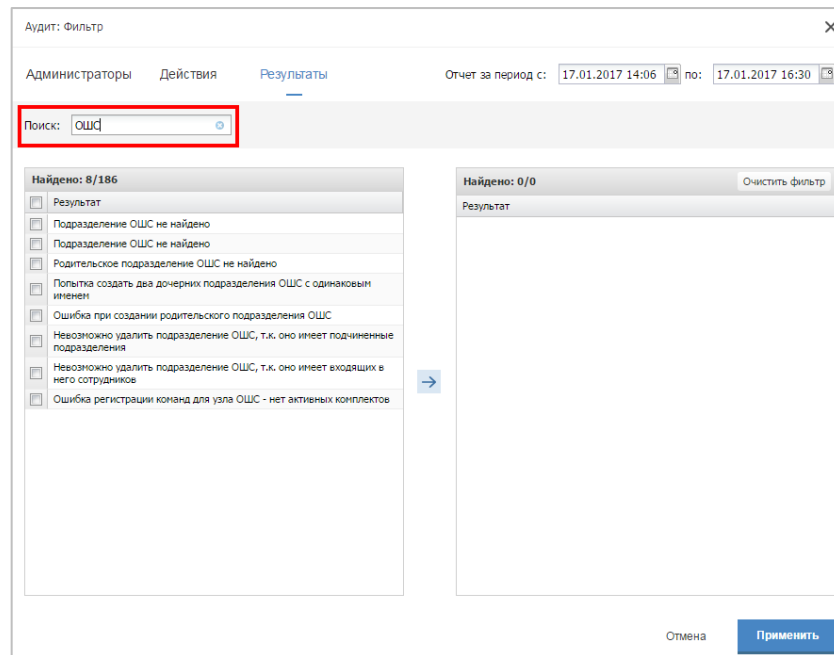


Рисунок 2.97 — Окно «Поиск» в настройках параметров отчёта «Аудит»

После настройки параметров отчёта по действиям Администраторов в «UEM SafeMobile» необходимо нажать кнопку **«Применить»** в нижней части окна настроек для перехода к сформированному отчёту согласно установленным фильтрам.

2.7.2 Отчёт «Звонки и SMS»

Для формирования отчёта выберите пункт главного меню «Звонки и SMS». В открывшемся окне (рисунок 2.98) отображается таблица с перечнем звонков и SMS-сообщений за заданный период времени.

Сотрудник	Пользователь домена	Телефон	Звонки ↑	Время разговоров (мин) ↑	SMS ↑	Звонки ↓	Время разговоров (мин) ↓	SMS ↓
Веселкин Петр Викторович			4	2	0	0	0	0
Петров Василий Фёдорович	+7000000011		32	40	8	24	18	16
Сидоров Василий Петрович			0	0	8	16	17	0
Фадорев Николай Николаевич			16	6	32	0	0	0

Рисунок 2.98 — Окно «Звонки и SMS»

Для выбора периода построения отчёта используются поля ввода даты/времени «Отчёт за период с», «по» (для начальной и конечной даты соответственно) в верхней панели инструментов. После нажатия на кнопку со значком календаря выберите год, месяц, день и время начала и завершения периода отчёта. После задания периода отчета нажмите кнопку «Запросить отчет».

Сформированный отчёт содержит следующие столбцы:

- id — номер устройства в системе (по умолчанию, в таблице не отображается);
- Сотрудник — фамилия, имя и отчество сотрудника-владельца устройства;
- Пользователь домена — ФИО сотрудника или e-mail, если ФИО не было импортировано;
- Телефон — номер телефона SIM-карты устройства;
- Звонки входящие — количество входящих звонков;
- Время разговоров (мин) — общая продолжительность входящих соединений;
- SMS — количество входящих SMS;
- Звонки исходящие — количество исходящих звонков;
- Время разговоров (мин) — общая продолжительность исходящих соединений;
- SMS — количество исходящих SMS.

2.7.3 Отчёт «События ИБ»

Для формирования отчёта выберите пункт главного меню «События ИБ». В открывшемся окне отображается таблица с перечнем событий информационной безопасности «UEM SafeMobile», произошедших в интервале времени, заданном Администратором в соответствии с рисунком 2.99.

id	Время	Описание	Сотрудник	Пользователь домена
103	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Васечкин Петр Викторович	
103	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Васечкин Петр Викторович	
103	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Васечкин Петр Викторович	
109	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Гагарин Юрий Алексеевич	
109	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Гагарин Юрий Алексеевич	
109	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Гагарин Юрий Алексеевич	
109	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Гагарин Юрий Алексеевич	
109	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Гагарин Юрий Алексеевич	
102	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Данилов Григорий Павлович	
102	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Данилов Григорий Павлович	
102	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Данилов Григорий Павлович	
102	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Данилов Григорий Павлович	
102	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Данилов Григорий Павлович	
102	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Данилов Григорий Павлович	
102	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Данилов Григорий Павлович	
102	28.02.2023 11:46:17	Сброс МСК к заводским настройкам	Данилов Григорий Павлович	

Рисунок 2.99 — Окно «События ИБ»

Для выбора периода построения отчёта используются поля ввода даты/времени «Отчёт за период с», «по» (для начальной и конечной даты соответственно) в верхней панели инструментов. Нажмите на кнопку со значком календаря в требуемом поле и в открывшемся календаре выберите год, месяц, день и время. После задания периода отчета нажмите кнопку «Запросить отчет».

Сформированный отчёт содержит следующие столбцы:

- id — номер устройства в системе;
- Время — время наступления события;
- Описание — название события;
- Сотрудник — фамилия, имя и отчество сотрудника, на устройстве которого это событие наступило;
- Пользователь домена — ФИО сотрудника или e-mail, если ФИО не было импортировано.

В отчёт попадают события ИБ, указанные в таблице 2.2.

2.7.4 Отчёт «Перемещения»

В отчёте отображается информация о перемещении абонентов «UEM SafeMobile» (в виде ломаных линий на карте) за указанный Администратором интервал времени. Для формирования отчёта следует выбрать пункт главного меню **«Перемещения»**.

Для выбора периода построения отчёта используются поля ввода даты/времени **«Отчёт за период с», «по»** (для начальной и конечной даты соответственно), для этого следует нажать на кнопку со значком календаря и выбрать год, месяц, день и время.

В поле **«Интервал (с)»** следует ввести интервал времени, на основе которого будут запрашиваться данные по координатам абонентов из базы данных.

В главной таблице необходимо выбрать сотрудника (сотрудников), отчёт о перемещении которых требуется сформировать. Затем нажать кнопку **«Запросить отчёт»**, чтобы отобразить линию перемещения абонента на карте, расположенную в информационной таблице, в соответствии с рисунком 2.100.

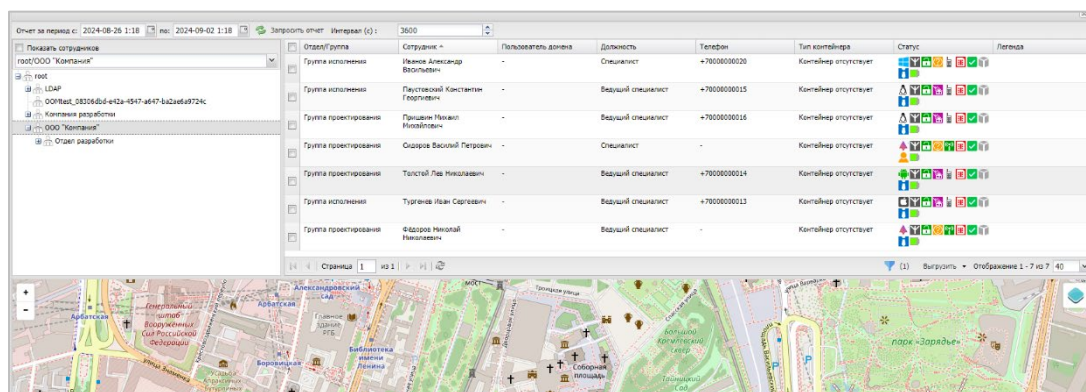


Рисунок 2.100 — Окно «Перемещения»

Если в таблице выбрано несколько сотрудников, траектории их перемещения отображаются разными цветами. Цвет траектории показывается в столбце **«Легенда»** главной таблицы.

Более подробные сведения об инструментах работы с картой приведены в разделе 2.6.4.

2.7.5 Отчёт «Профили»

В отчёте отображается информация о профилях, применённых на подключённых к системе МСК. Отчёт состоит из двух таблиц: верхняя таблица с реестром назначенных и применённых профилей; а в нижней таблице воспроизводятся установленные и применённые на МСК значения параметров политик выбранного профиля в соответствии с рисунком 2.101.

Название профиля	Тип	Назначен	Применен	Описание	Платформа	Назначено	Применено
Профиль политики ограниченный iOS	Политики ограниченный iOS	Да	Нет	Профиль. Содержит запрет окончания аккаунта / добавление друзей в Game Center / использование приложения подкасты		28.02.2023 11:46:17	-
Профиль iOS из точки доступа ANY_CСMС	Точка доступа WPA2 iOS	Да	Нет			28.02.2023 11:46:17	-
Профиль iOS из точки доступа Мербайн	Точка доступа WPA2 iOS	Да	Нет			28.02.2023 11:46:17	-
Профиль iOS из точки доступа ANY_CСMС_LDR	Точка доступа WPA2 iOS	Да	Нет			28.02.2023 11:46:17	-

Название политики	Установленное значение	Применённое значение	Дата
Имя точки доступа (SSID WPA2)	ANY_CСMС	-	
Скрытая сеть	Нет	-	
Автоматическое подключение	Да	-	
Тип шифрования	WPA2	-	
Протокол	None	-	
Тип безопасности	Personal	-	
Пароль	password	-	

Рисунок 2.101 — Окно отчёта «Профили»

Верхняя таблица отчёта содержит следующие столбцы:

- Название профиля — название созданного в системе профиля;
- Тип — разновидность политик ОС;
- Назначен — «Да/Нет»;
- Применен — «Да/Нет»;
- Описание — описание настроек ОС, заданных в профиле;
- Платформа — значок платформы МСК, на которое назначен профиль;
- Назначено — время назначения;
- Применено — время применения.

Нижняя таблица отчёта содержит следующие столбцы (данные отображаются при выборе МСК в верхней таблице):

- Название политики — название политики профиля;
- Установленное значение — значение параметра установленной на МСК политики;
- Применённое значение — значение параметра политики, которое было применено на МСК;
- Дата — дата/время, когда значение политики было применено на МСК.

Для просмотра отчёта необходимо в панели ОШС выбрать МСК сотрудника, а затем в верхней таблице интересующий профиль. В нижней таблице отобразится информация с установленными и применёнными на МСК значениями параметров политики назначенного профиля.

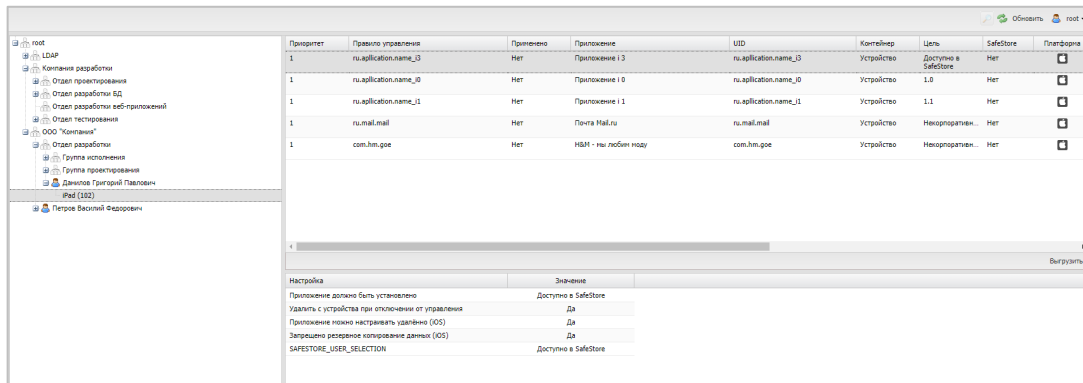
Сертификаты, выписанные через сервер SCEP, могут быть принудительно перевыпущены по команде администратора. Кнопка «перевыпуск сертификата» располагается в блоке отображения списка профилей, назначенных на МСК. Кнопка становится активной при следующих условиях:

- В дереве ОШС выбран МСК;
- Доступна для следующих типов профилей:
 - VPN iOS,
 - VPN для приложений (Per-App VPN) iOS,
 - Точка доступа WiFi iOS,
 - Точка доступа WiFi Android,
 - Exchange аккаунт iOS,
- В качестве учетных данных, в профиле выбраны настройки SCEP.

При нажатии кнопки начинается процесс перевыпуска сертификата.

2.7.6 Отчёт «Правила управления»

В отчёте отображается информация о ПУП, примененных на подключенных к системе МСК. Отчёт состоит из двух таблиц: верхняя таблица с реестром назначенных и применённых правил управления; а в нижней таблице воспроизводятся установленные и примененные на МСК значения параметров ПУП в соответствии с рисунком 2.102.



Приоритет	Правило управления	Применено	Приложение	UID	Контейнер	Цель	SafeStore	Платформа
1	ru.application.name_03	Нет	Приложение 1.3	ru.application.name_03	Устройство	Доступно в SafeStore	Нет	
1	ru.application.name_00	Нет	Приложение 1.0	ru.application.name_00	Устройство	1.0	Нет	
1	ru.application.name_01	Нет	Приложение 1.1	ru.application.name_01	Устройство	1.1	Нет	
1	ru.mail.mail	Нет	Почта Mail.ru	ru.mail.mail	Устройство	Некорпоративн...	Нет	
1	com.hm.goe	Нет	ИМН - my love! node	com.hm.goe	Устройство	Некорпоративн...	Нет	

Настройка	Значение
Приложение должно быть установлено	Доступно в SafeStore
Удалить с устройства при отключении от управления	Да
Приложение можно настраивать удалённо (IOS)	Да
Защищено резервное копирование данных (IOS)	Да
SAFESTORE_USER_SELECTION	Доступно в SafeStore

Рисунок 2.102 — Окно отчёта «Правила управления»

Верхняя таблица отчёта содержит следующие столбцы:

- Приоритет — если назначено несколько правил с одинаковым приложением, то применяется правило с приоритетом равным единице;
- Правило управления — название созданного в системе ПУП;
- Применено — Да / Нет;
- Приложение — название приложения;
- UID;
- Контейнер — приложение установлено в контейнере;
- Цель — цель назначения ПУП;
- Платформа — платформа МСК, на котором установлено приложение и назначен ПУП;
- Описание — описание настроек ОС;
- Условия — выполнено/не выполнено;
- На устройстве — версия приложения, установленного на устройстве.
- Включено — Включено / Заблокировано;
- Выбор пользователя — отображается при выборе МСК в ОШС;
- Статус — применено / не применено;
- Дата назначения;
- Дата применения.

Нижняя таблица отчёта содержит следующие столбцы:

- Настройка — описание параметров ПУП;
- Значение — Да / Нет.

Для просмотра отчёта необходимо в панели ОШС выбрать МСК сотрудника, а затем в верхней таблице интересующий ПУП. В нижней таблице отобразится информация с установленными и применёнными на МСК значениями параметров назначенного ПУП.

2.7.7 Отчет «Правила управления (UID)»

В отчёте отображается информация о ПУП одного приложения, примененного на подключенных к системе МСК. Страница отчета состоит из следующих блоков (рисунок 2.103):

- Блок поиска приложения, по которому будет сформирован отчет;
- Блок указания подразделения (дерево ОШС), к комплектам которого будет применен отчет;
- Блок со списком комплектов, на которых установлено заданное приложение;
- Блок вывода отчета о настройках ПУП, в выбранном комплекте.

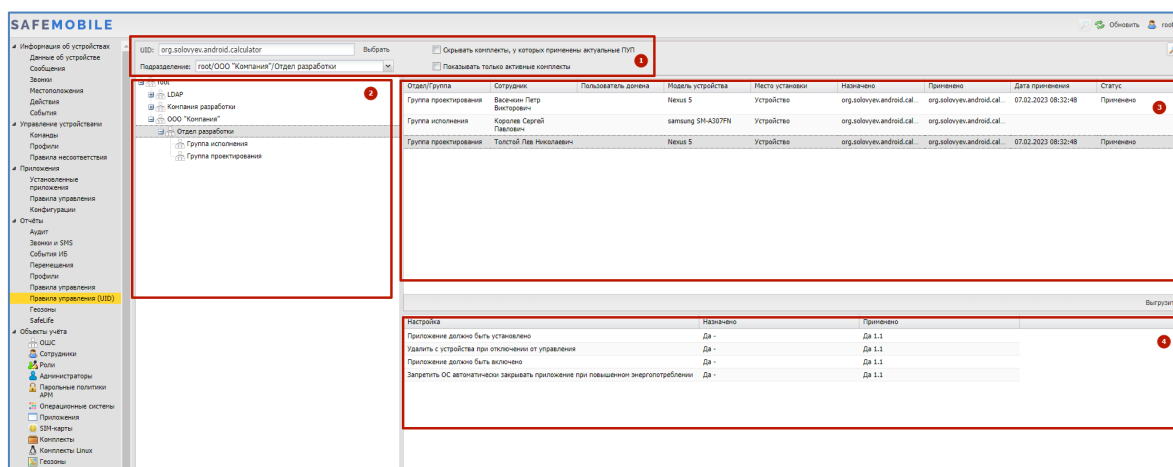


Рисунок 2.103 — Расположение блоков в разделе «Отчеты — Правила управления (UID)»

Блок поиска приложения состоит из следующих элементов:

- UID — Поле отображения UID выбранного приложения;
- Кнопка «Выбрать» — Открывает список приложений, установленных в комплектах системы и позволяет выбрать приложение для формирования отчета;
- Скрыть комплекты, у которых применены актуальные ПУП — фильтр (чекбокс). Если флаг фильтра включен, то из отчета будут исключены комплекты, на которые применен актуальный ПУП приложения;
- Показывать только активные комплекты — фильтр (чекбокс);
- Подразделение — поле отображения выбранного подразделения в структуре ОШС;

Блок списка комплектов представлен в виде таблицы, в которой каждая строка списка является информацией об одном комплекте, сгруппированной по следующим колонкам данных:

- Колонки таблицы, включенные по умолчанию;
 - Отдел/Группа — название группы в структуре ОШС, которой принадлежит пользователь (владелец МСК);
 - Сотрудник — ФИО сотрудника
 - Пользователь домена — ФИО сотрудника (или e-mail, если ФИО не было импортировано из LDAP);
 - Модель устройства;
 - Место установки — устройство или контейнер;
 - Назначено — наименование назначенного ПУП;
 - Применено — наименование примененного ПУП;
 - Дата применения — дата и время применения ПУП на комплект;
 - Статус правила — состояние или ошибка применения ПУП;
- Колонки таблицы, не включенные по умолчанию;
 - Должность,
 - SIM: Принадлежность,
 - Состояние роуминга,
 - IMSI,
 - ICCID,
 - Телефон,
 - Id,
 - Состояние блокировки,
 - Управление устройствами,
 - Последняя активность,
 - Тип соединения,
 - IP адрес,
 - Тип устройства,
 - IMEI,
 - UDID,
 - Серийный номер,
 - Тип контейнера,
 - Заряд аккумулятора,
 - Устройство: Принадлежность,
 - Монитор,
 - Платформа,
 - Версия,
 - Статус устройства,
 - Условия,
 - Стратегия.

- Кнопка «Выгрузить» — выгрузка отчета (excel).

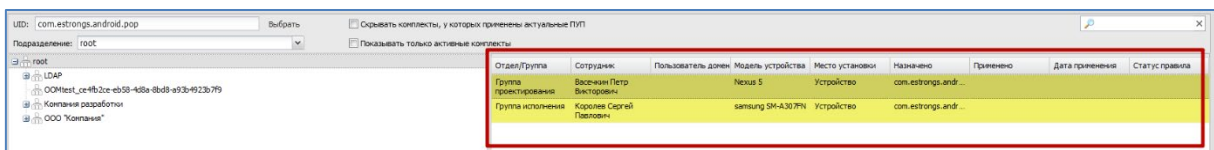
Блок отображения списка ПУП, выбранного комплекта представлен в виде таблицы, в которой каждая строка списка содержит информацию об одном «правиле управления приложениями» и распределена по следующим колонкам:

- Настройка — название настройки ПУП;
- Назначено — назначенное значение настройки ПУП;
- Применено — назначенное значение настройки ПУП, примененное на устройстве.

Чтобы сформировать отчет по ПУП, необходимо выполнить следующие действия:

1. В блоке выбора приложения нажать кнопку «Выбрать», после чего откроется список UID приложений, зарегистрированных в системе;
2. Выбрать в списке приложение, по которому необходимо сформировать отчет;
3. Установить фильтрам поиска необходимые значения (по умолчанию они включены);
4. В структуре ОШС указать подразделение, по комплектам которого будет сформирован отчет. Если ПУП с указанным приложением назначен или применен хотя бы на одном устройстве выбранного подразделения, то в соответствующем блоке будет отображен список комплектов, на которых установлено указанное приложение.
5. Выбрать в списке комплектов необходимый для просмотра значений настроек ПУП, после чего в соответствующем блоке будет отображен список значений назначенного и примененного на комплект ПУП.

Если у комплекта примененный и назначенный ПУП не совпадают, то строка в списке комплектов будет выделена цветом (рисунок 2.104).



Отдел/Группа	Сотрудник	Пользователь домен	Модель устройства	Место установки	Назначено	Применено	Дата применения	Статус правила
Группа проектирования	Васнецкий Пётр Викторович		Nexus 5	Устройство	com.estrongs.andr...			
Группа исполнения	Королев Сергей Павлович		samsung SM-A307N	Устройство	com.estrongs.andr...			

Рисунок 2.104 — Комплект с несовпадающими назначенными и примененными ПУПами

2.7.8 Отчет «Геозоны»

В отчете отображается информация о входе/выходе в/из геозоны абонентов «UEM SafeMobile» за указанный Администратором интервал времени. Для формирования отчёта следует выбрать пункт главного меню «Геозоны» (рисунок 2.105).

Отдел/группа	ФИО	Пользователь домена	Должность	IMEI	Серийный номер	Платформа	Дата/время	Название геозоны	Событие
ООО "Компания"	Петров Василий Фёдорович		Директор	358363100024595	R38M667L9SL	Android	27.02.2023 13:02:01	Zone3	Вход
ООО "Компания"	Петров Василий Фёдорович		Директор	358363100024595	R38M667L9SL	Android	27.02.2023 13:14:15	Zone3	Выход
ООО "Компания"	Петров Василий Фёдорович		Директор	358363100024595	R38M667L9SL	Android	27.02.2023 13:15:50	Zone3	Вход
ООО "Компания"	Петров Василий Фёдорович		Директор	358363100024595	R38M667L9SL	Android	27.02.2023 13:19:50	Zone3	Выход
ООО "Компания"	Петров Василий Фёдорович		Директор	358363100024595	R38M667L9SL	Android	27.02.2023 13:21:37	Zone3	Вход
ООО "Компания"	Петров Василий Фёдорович		Директор	358363100024595	R38M667L9SL	Android	27.02.2023 13:25:37	Zone3	Выход
Отдел разработки	Данилов Григорий Павлович		Начальник	990002078369549	HD52R85	iPhone OS	27.02.2023 09:29:30	Zone3	Вход
Отдел разработки	Данилов Григорий Павлович		Начальник	990002078369549	HD52R85	iPhone OS	27.02.2023 09:29:14	Zone3	Выход
Отдел разработки	Данилов Григорий Павлович		Начальник	990002078369549	HD52R85	iPhone OS	27.02.2023 09:31:16	Zone3	Вход
Отдел разработки	Данилов Григорий Павлович		Начальник	990002078369549	HD52R85	iPhone OS	27.02.2023 09:40:08	Zone3	Выход
Отдел разработки	Данилов Григорий Павлович		Начальник	990002078369549	HD52R85	iPhone OS	27.02.2023 09:40:26	Zone3	Вход
Отдел разработки	Данилов Григорий Павлович		Начальник	990002078369549	HD52R85	iPhone OS	27.02.2023 09:49:16	Zone3	Выход
Отдел разработки	Данилов Григорий Павлович		Начальник	990002078369549	HD52R85	iPhone OS	27.02.2023 09:50:49	Zone3	Вход
Группа проектирования	Васечкин Петр Викторович		Специалист	013327002453779	245377	Android	27.02.2023 13:26:25	Zone3	Вход
Группа проектирования	Васечкин Петр Викторович		Специалист	013327002453779	245377	Android	27.02.2023 13:27:28	Zone3	Выход
Группа проектирования	Васечкин Петр Викторович		Специалист	013327002453779	245377	Android	27.02.2023 13:29:13	Zone3	Вход
Группа проектирования	Васечкин Петр Викторович		Специалист	013327002453779	245377	Android	27.02.2023 13:41:13	Zone3	Выход
Группа проектирования	Васечкин Петр Викторович		Специалист	013327002453779	245377	Android	27.02.2023 13:43:53	Zone3	Вход
Группа проектирования	Васечкин Петр Викторович		Специалист	013327002453779	245377	Android	27.02.2023 13:45:34	Zone3	Выход

Рисунок 2.105 — Окно «Геозоны»

Для выбора периода построения отчёта используются поля ввода даты/времени «Отчёт за период с», «по» (для начальной и конечной даты соответственно) в верхней панели инструментов, для этого следует нажать на кнопку со значком календаря и выбрать год, месяц, день и время. После задания периода отчета нажмите кнопку «Выгрузить». Сформированный отчёт содержит следующие столбцы:

- Отдел/группа — подразделение организации, в котором работает сотрудник;
- ФИО — фамилия, имя и отчество сотрудника;
- Пользователь домена — ФИО сотрудника или e-mail, если ФИО не было импортировано;
- Должность — должность сотрудника;
- Тип устройства — тип МСК, подключенного к системе (по умолчанию, в таблице не отображается);
- Модель устройства — модель МСК, подключенного к системе (по умолчанию, в таблице не отображается);
- IMEI;
- UDID (по умолчанию, в таблице не отображается);
- Серийный номер — для МСК на платформе iOS и Android;
- Платформа — мобильная платформа МСК;
- Принадлежность — признак собственности МСК (по умолчанию, в таблице не отображается);
- Координаты — координаты регистрации события в системе (по умолчанию, в таблице не отображается);

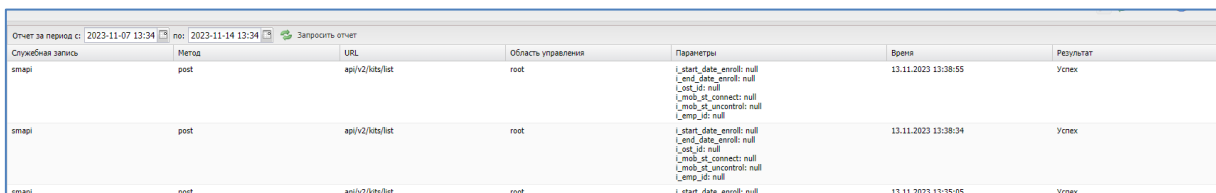
- Дата/время — дата и время регистрации события в системе;
- Название геозоны — название созданной и активированной в системе геозоны;
- Событие — вход/выход в/из геозоны.

2.7.9 Аудит SMAPI

Раздел отображает журнал данных по работе SMAPI через сервисные учетные записи. Доступ к журналу имеют администраторы назначенные на корень дерева ОШС и определяется полномочием на просмотр.

Данные отображаются в виде списке, каждая строка которого содержит информацию о подключениях через сервисные учетные записи (рисунок 2.106). Каждая строка содержит:

- Служебная запись — наименование сервисной учетной записи;
- Метод,
- URL,
- Область управления,
- Параметры — входные параметры запроса;
- Время — время регистрации обращения в БД;
- Результат.



Служебная запись	Метод	URL	Область управления	Параметры	Время	Результат
smapi	post	api/v2/kits/list	root	i_start_date_enroll: null i_end_date_enroll: null i_out_id: null i_mob_st_connect: null i_mob_st_uncontrol: null i_emp_id: null	13.11.2023 13:38:55	Успех
smapi	post	api/v2/kits/list	root	i_start_date_enroll: null i_end_date_enroll: null i_out_id: null i_mob_st_connect: null i_mob_st_uncontrol: null i_emp_id: null	13.11.2023 13:38:34	Успех
smapi	post	api/v2/kits/list	root	i_start_date_enroll: null	13.11.2023 13:35:05	Успех

Рисунок 2.106 — раздел «Аудит SMAPI»

По умолчанию журнал отображает данные за последние 7 календарных дней. Задать период отображения можно в фильтре по дате и времени над списком записей раздела. Для этого следует задать «дату и время начала — конца периода» и нажать кнопку «Запросить отчет», после чего данные в разделе будут сформированы в соответствии с установками фильтра.

2.7.10 Активность сотрудников

Раздел «Активность сотрудников» отображает статистические данные по использованию приложений и самого устройства сотрудниками (время разблокированного экрана). Включение регистрации активности сотрудника и настройку параметров сбора статистики производить в профиле «Регистрация активности Сотрудников Android». В настройках профиля указывается диапазон времени суток, в который один раз в день снимается статистика с устройства.

Рабочий экран раздела состоит двух частей (рисунок 2.107) :

- Дерево ОШС — выбор подразделения ОШС (или сотрудника) для формирования статистического отчета;
- Список статистических данных выбранного в ОШС подразделения (или сотрудника).

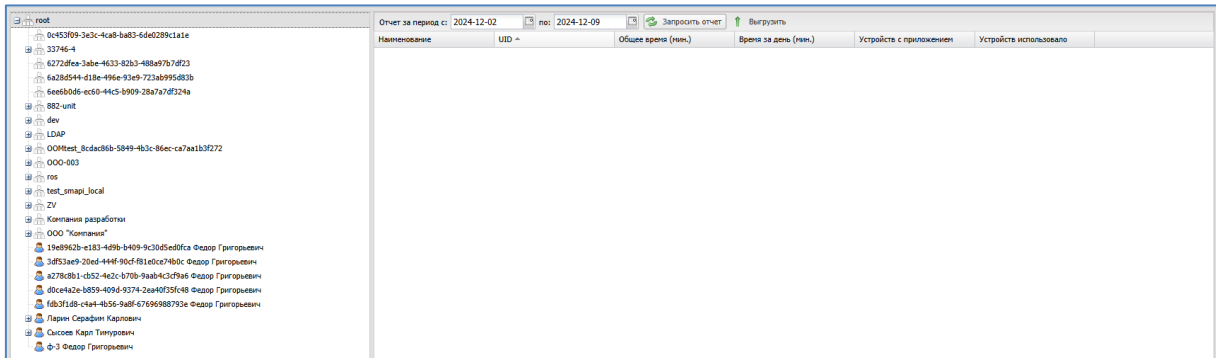


Рисунок 2.107 — Раздел «Активность сотрудников»

Область экрана отображения статистических данных состоит из следующих элементов:

- Диапазон дат сбора статистики — отчет за период с (дата в формате ГГГГ.ММ.ДД) по (дата в формате ГГГГ.ММ.ДД);
- Кнопка «Запросить отчет». При нажатии формируется статистический отчет за указанный период.
- Кнопка «Выгрузить». При нажатии формируется файл содержащий готовый статистический отчет в формате .xlsx.
- Таблица статистического отчета. Содержит данные, следующих типов:
 - Наименование — Название приложения (опционально);
 - UID — UID приложения;

- Общее время (мин) — общее время видимости приложения за указанный период;
- Время за день (мин) — время использования приложения за день;
- Устройств с приложением — количество устройств на которых установлено приложение;
- Устройств использовало — количество устройств которое использовало приложение за указанный период.

2.8 Управление объектами учёта (пункт меню «Объекты учёта»)

Пункт главного меню «Объекты учёта» предназначен для управления объектами учёта «UEM SafeMobile»:

- ОШС,
- Сотрудники,
- Роли,
- Администраторы,
- Парольные политики APM,
- Операционные системы,
- Приложения,
- SIM-карты,
- Комплекты,
- Комплекты Linux,
- Геозоны,
- Серверные сертификаты,
- Подключения к серверам,
- Настройки SCEP,
- Клиентские сертификаты,
- Группы,
- Шаблоны писем.

2.8.1 Организационно-штатная структура

Пункт меню «ОШС» открывает окно в соответствии с рисунком 2.108, в котором отображаются подразделения организации в виде иерархической структуры.

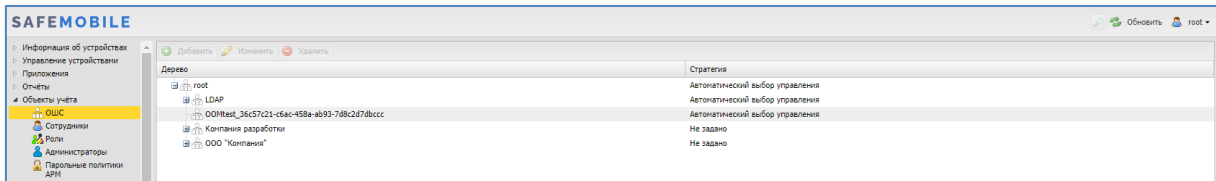


Рисунок 2.108 — Окно «ОШС»

В верхней части таблицы находится панель инструментов, содержащая следующие кнопки:

- **Добавить** — предназначена для добавления нового подразделения в структуру организации;
- **Изменить** — предназначена для изменения параметров подразделения, имеющегося в структуре организации;
- **Удалить** — предназначена для удаления подразделения, имеющегося в структуре организации.

Для добавления нового подразделения в структуру организации следует выбрать родительское подразделение и нажать кнопку «**Добавить**», после чего появится окно в соответствии с рисунком 2.109.

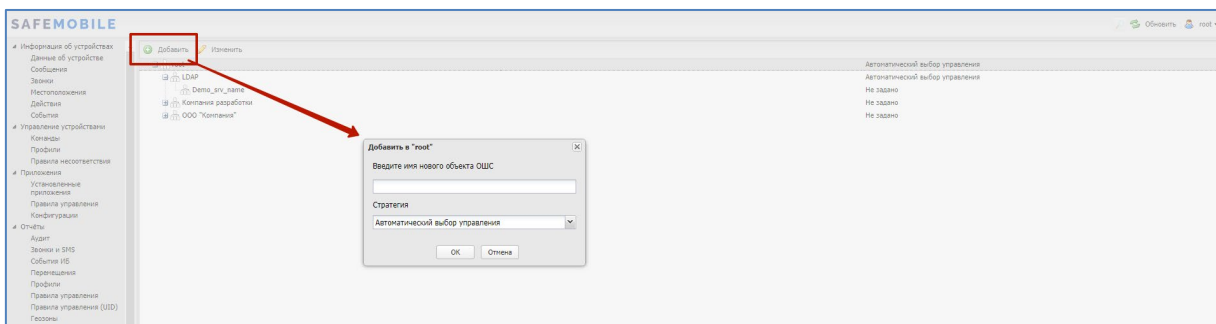


Рисунок 2.109 — Добавление подразделения в ОШС

В этом окне необходимо ввести название создаваемого подразделения. Опционально можно выбрать стратегию управления устройством Android по умолчанию. Если стратегию не выбрать, то будет использоваться стратегия, заданная в родительских

подразделениях. Затем нажать кнопку **«ОК»**. Для отмены создания подразделения необходимо нажать кнопку **«Отмена»**.

Стратегия по умолчанию будет автоматически выбираться при создании нового кода приглашения, при подключении МСК с авторизацией пользователя во внешнем каталоге (LDAP) и при подключении с использованием технологии КМЕ.

Добавление и изменения узлов ОШС

Если выбрать подразделение и нажать кнопку **«Добавить»**, новое подразделение будет добавлено в выбранное в качестве подчиненного.

Для изменения названия выбранного подразделения или стратегии по умолчанию нажмите кнопку **«Изменить»**, после чего появится окно в соответствии с рисунком 2.110. Для узлов ОШС, синхронизированных с внешним каталогом (LDAP), изменение названия подразделения недоступно.

Нажмите кнопку **«ОК»**, чтобы подтвердить изменение или кнопку **«Отмена»**, чтобы отменить его.

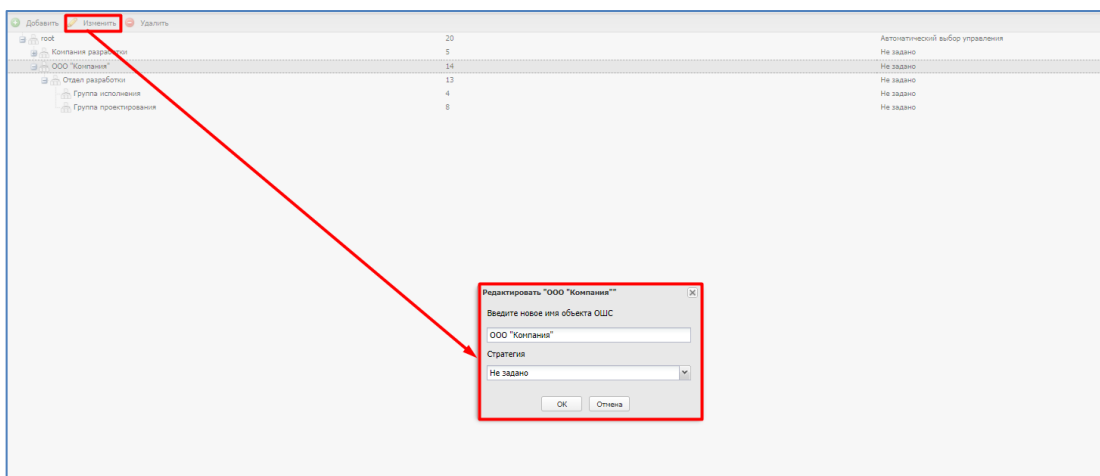


Рисунок 2.110 0 Изменение подразделения в ОШС

Удаление узлов ОШС

Объекты учета «ОШС» доступны для удаления, если соответствуют следующим требованиям:

- Удаляемый узел не является корневым,
- Не содержит «неудаляемых сотрудников»,
- Корневой узел для внешних каталогов (root/LDAP) доступен для удаления при отсутствии внешних каталогов и корневых узлов импорта;
- Корневой узел импорта (root/LDAP/«имя каталога») и целевой каталог (root/LDAP/«имя каталога»/«целевой каталог»), доступен для удаления при выполнении условий:

- Удален связанный с ним внешний каталог;
- Содержит только сотрудников доступных для удаления.

Для удаления выбранного узла из структуры организации нажмите кнопку **«Удалить»**, нажмите кнопку **«Да»**, чтобы подтвердить удаление. Далее система проводит проверку удаляемого узла ОШС на соответствие условиям удаления. Если, какой либо объект выбранного для удаления узла ОШС не подлежит удалению, то система выдаст сообщение об ошибке:

– Узел содержит комплекты: {{количество}} и/или сотрудников, связанных с внешним каталогом: {{количество}} и не может быть удален. Для удаления каталога необходимо удалить комплекты и правила импорта сотрудников».

Удаление узла и вложенных объектов будет отменено.

После проверки системой узла на возможность удаления, откроется окно содержащее список удаляемых объектов учета в выбранном узле ОШС. Каждая строка списка содержит:

- Тип — сотрудник или узел ОШС;
- Наименование — ФИО сотрудника или название узла ОШС.

Для подтверждение удаления необходимо ввести имя удаляемого подразделения в соответствующее поле окна, в соответствии с рисунком 2.111. После чего кнопка **«Удалить»** станет доступна для завершения удаления подразделения.

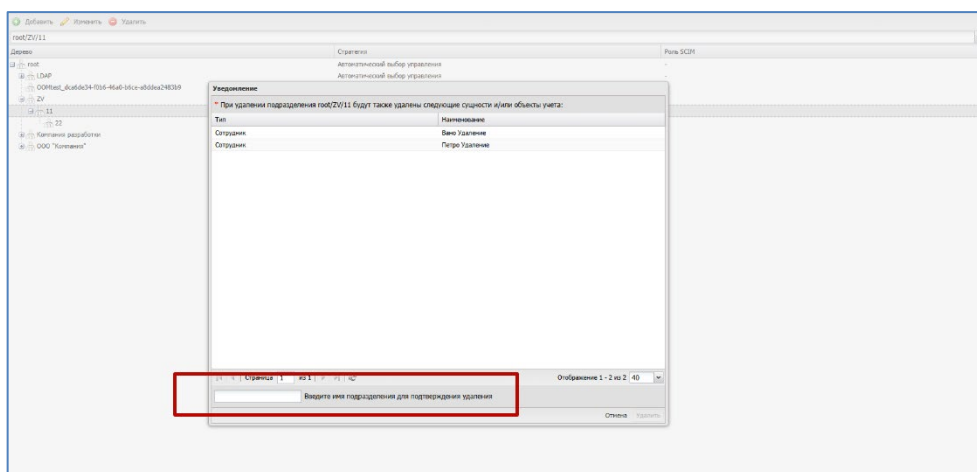


Рисунок 2.111 — Удаление подразделения в ОШС

2.8.2 Сотрудники

Раздел содержит справочник сотрудников и ведется для учёта абонентов МСК. Перед созданием комплектов МСК в «UEM SafeMobile» необходимо внести данные о сотрудниках организации

Страница раздела состоит из дерева ОШС, списка сотрудников подразделения ОШС, информации о сотруднике, выбранного в списке сотрудников подразделения (рисунок 2.112).

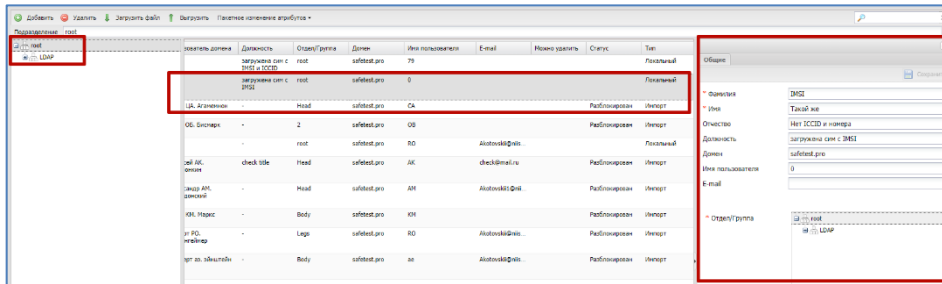


Рисунок 2.112 — Окно «Сотрудник»

Таблица списка сотрудников содержит следующие столбца данных:

- Столбцы, отображаемые по умолчанию:
 - ФИО — фамилия, имя и отчество сотрудника;
 - Пользователь домена — Отображает ФИО сотрудника (или e-mail, если ФИО не было импортировано);
 - Должность — должность сотрудника;
 - Отдел/Группа — подразделение организации, в котором работает сотрудник;
 - Домен — доменное имя организации пользователя;
 - Имя пользователя — имя пользователя (логин) в электронной почте;
 - E-mail — адрес электронной почты;
 - Можно удалить — отметка о том, что импортированного пользователя можно удалить из системы (Да/Нет);
 - Статус — статус блокировки пользователя (Заблокирован/Разблокирован/Не заданно);
 - Тип — тип пользователя (локальный/импорт);
- Столбцы, отображаемые опционально:
 - id — номер сотрудника с комплектом в системе,
 - objectGUID,
 - memberOf,

- name,
- givenName,
- middleName,
- sn,
- mail,
- mailNickName,
- mobile,
- telephoneNumber,
- distinguishedName,
- userPrincipalName,
- department,
- userAccountControl,
- lockoutTime,
- objectCategory,
- whenChanged,
- whenCreated,
- employeeID
- manager,
- title,
- company,
- samaccountName.

Блок с информацией о сотруднике отображает следующие данные:

- Общие:
 - Фамилия,
 - Имя,
 - Отчество,
 - Должность,
 - Домен,
 - Имя пользователя,
 - E-mail,
 - Отдел/Группа (подразделение в ОШС).

- Импорт:
(вкладка отображается только для импортированных пользователей)
 - Поля данных о пользователях, импортированных из внешнего каталога,
 - objectGUID,

- memberOf,
- name,
- displayName,
- givenName,
- middleName,
- sn,
- mail,
- mailNickName,
- mobile,
- telephoneNumber,
- distinguishedName,
- userPrincipalName,
- department,
- userAccountControl,
- lockoutTime,
- objectCategory,
- employeeID,
- manager,
- title,
- company,
- whenChanged,
- whenCreated,
- samaccountName.

Добавление сотрудника

Для добавления записи используется кнопка **«Добавить»**. Затем в правой части окна следует заполнить форму, содержащую информацию о сотруднике (рисунок 2.113). Для этого необходимо ввести сведения в обязательные поля: **«Фамилия»**, **«Имя»**. После заполнения формы нажать кнопку **«Сохранить»**, и запись о новом сотруднике будет добавлена в систему.

Кроме того, в списке ОШС, расположенном ниже поля **«Отдел/группа»**, выбрать подразделение, в котором работает сотрудник. **Изменение расположения доступно только для уже существующих записей о сотрудниках.**

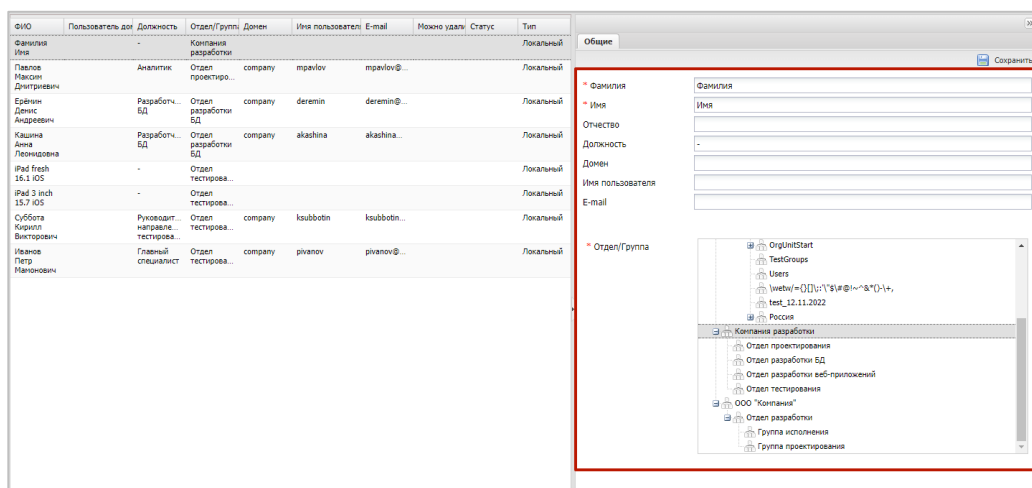


Рисунок 2.113 — Создание записи о сотруднике

После добавления нового сотрудника рекомендуется убедиться в наличии для него календаря рабочего времени в разделе **«Календарь»** (по умолчанию сотрудникам назначается календарь подразделения, если он задан). У Администратора появится возможность получать данные о местоположении сотрудника и его комплекта в рабочее время. Подробнее описание календаря приведено в п. 2.11, а об определении местоположения в п. 2.6.4.

Для редактирования необходимо выбрать в таблице запись о сотруднике и внести изменения в поля в правой части окна. В списке подразделений организации можно выбрать необходимый отдел и группу для перемещения туда редактируемой записи о сотруднике. При нажатии кнопки **«Сохранить»** внесенные изменения сохраняются в БД.

Удаление сотрудника

Объекты учета «Сотрудник» доступны для удаления, если соответствуют следующим требованиям:

- Локальный сотрудник не имеющий комплектов;
- Импортированный сотрудник не имеющий комплектов и не связанный с внешним каталогом. Импортированный сотрудник теряет связь с внешним каталогом в следующих случаях:
 - Объект учета выходит из области синхронизации,
 - Объект учета выходит из групп синхронизации,
 - Объект учета перестает удовлетворять условиям синхронизации, заданным во внешнем каталоге:
 - Сотрудник отключен во внешнем каталоге LDAP и во внешнем

каталоге задано — «отключение от управления при отключении в внешнем каталоге LDAP».

- При удалении внешнего каталога все ранее связанные с ним сотрудники помечаются как локальные.

Перед удалением система проверяет объект учета на соответствие условиям для удаления. Если объект учета не соответствует условиям, то система выдаст соответствующее сообщение об ошибке.

Для удаления объекта учёта необходимо выбрать в таблице (рисунок 2.114) соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждения выполняемого действия, выбранная запись удаляется из базы при отсутствии связанных объектов учёта, так же будут удалены все назначения на удаленного пользователя.

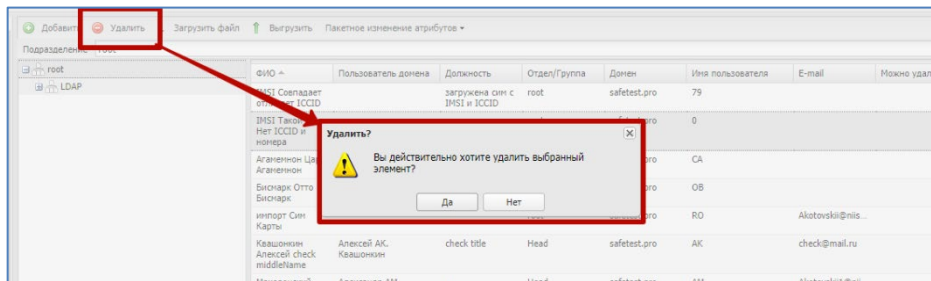


Рисунок 2.114 — Удаление сотрудника

Выгрузка списка сотрудников

Кнопка **«Выгрузить»** предназначена для выгрузки списка сотрудников в файл формата **«xlsx»** (рисунок 2.115).

	A	B	C	D	E	F	G	H	I	M
1	Фамилия	Имя	Отчество	Должность	Домен	Имя пользователя	E-mail	Место работы 1	Место работы 2	ра
2				Директор				1.НИИ СОКБ		
3										
4										
5										

Рисунок 2.115 — Список сотрудников в файле формата «xlsx»

Структура колонок в файле должна быть следующая:

- Фамилия (обязательно для заполнения),
- Имя (обязательно для заполнения),

- Отчество,
- Должность (обязательно для заполнения),
- Домен
- E-mail
- Место работы 1 (обязательно для заполнения),
- Место работы 2,
- Место работы ...,
- Место работы 10.

Кнопка «**Загрузить файл**» предназначена для загрузки в систему списка сотрудников из файла. Формат и структура файла аналогичная файлу выгрузки.

2.8.2.1 Пакетное изменение атрибутов

Функционал «пакетное изменение атрибутов» позволяет выгрузить список сотрудников в файл формата CSV, для последующей обработки и загрузки обратно в систему. Кнопки загрузки и выгрузки атрибутов пользователей находятся в выпадающем списке, в верхней панели инструментов раздела «Сотрудники» (рисунок 2.116).

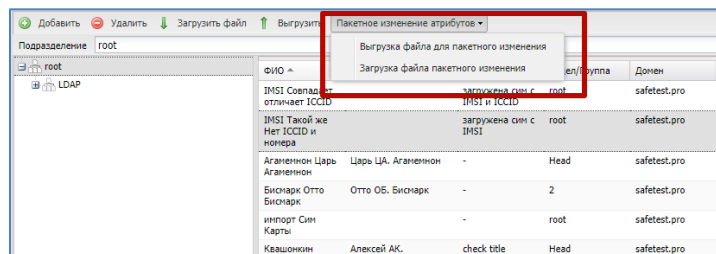


Рисунок 2.116 — Расположение кнопок загрузки и выгрузки, для пакетного изменения атрибутов

Для проведения пакетного изменения атрибутов списка сотрудников необходимо выполнить выгрузку файла, внесение изменений в файл, загрузку файла с измененными атрибутами сотрудников.

Для выгрузки файла необходимо выполнить следующие действия:

1. Перейти в раздел «Сотрудники».
2. В выпадающем списке «Пакетное изменение атрибутов» нажать кнопку «Выгрузка файла пакетного изменения».

3. Выбрать узел ОШС для выгрузки и нажать кнопку «ОК». Узлы из области синхронизации (каталог LDAP) не доступны для выбора.
4. Дождаться окончания формирования файла выгрузки и нажать кнопку «Скачать».

После чего внести изменения в полученный файл атрибутов сотрудников.

Примечание

При внесении изменений в файл следует учесть, что атрибут «id» изменить нельзя, т.к. по этому атрибуту выполняется поиск сотрудника для обновления атрибутов.

Для загрузки файла атрибутов сотрудников необходимо выполнить следующие действия:

1. В выпадающем списке «Пакетное изменение атрибутов» нажать кнопку «Загрузка файла пакетного изменения».
2. В диалоговом окне выбрать файл для загрузки и нажать кнопку «ОК».
3. Дождаться окончания обработки данных.
 - Для просмотра отчета по ошибкам нажать кнопку «Показать ошибки», после чего будет открыт отчет ошибок. Для сохранения отчета по ошибкам следует нажать кнопку «Сохранить в файл».
 - Если количество ошибок превысит 100, то загрузка будет прервана.
4. По завершении загрузки, системой будет предложено сохранить в файл список сотрудников, которых не удалось импортировать в результате ошибки. После исправления ошибок этот файл может быть использован для повторной загрузки.

Правила загрузки и выгрузки файла атрибутов сотрудников:

- Выгружаемый и загружаемый файл имеет формат csv, в кодировке UTF8, с разделителем «запятая».
- Выгружаемый список сотрудников содержит атрибуты:
 - Id,
 - Фамилия,
 - Имя,
 - Отчество (опционально),

- Должность (опционально),
 - Домен (опционально),
 - Имя пользователя (опционально),
 - E-mail (опционально).
- Опциональные атрибуты загружаемого файла могут быть пустыми, но должны присутствовать.
 - Первая строка загружаемого файла должна содержать заголовки атрибутов.
 - При любом нарушении формата файла или невозможности произвести парсинг загрузка будет невозможна, с ошибкой «Неверный формат файла».
 - При импорте удаляются все пробелы в начале и в конце каждого атрибута сотрудника.
 - Длина обязательных атрибутов должна быть не более 50 символов и содержать доступные для атрибута символы.
 - При успешном завершении проверок атрибутов импортируемых сотрудников будут произведены следующие действия системы:
 - Обновление значений атрибутов сотрудников.
 - Добавлена в очередь команда синхронизации для всех устройств сотрудника на платформах: Android и Аврора.
 - Смещение время следующей синхронизации на текущее для всех устройств сотрудника на платформе iOS.

2.8.3 Роли

Пункт меню **«Роли»** открывает окно (рисунок 2.117), предназначенное для управления ролями Администраторов «UEM SafeMobile».

В левой части таблицы в столбце **«Роль»** отображается список ролей Администраторов, а в правой части в столбце **«Полномочия»** — список полномочий, которые можно назначить каждой выбранной роли.

В верхней части таблицы находится панель инструментов, содержащая следующие кнопки:

- **Добавить** — предназначена для создания новой роли;
- **Изменить** — предназначена для изменения названия существующей роли;
- **Удалить** — предназначена для удаления выбранной роли.

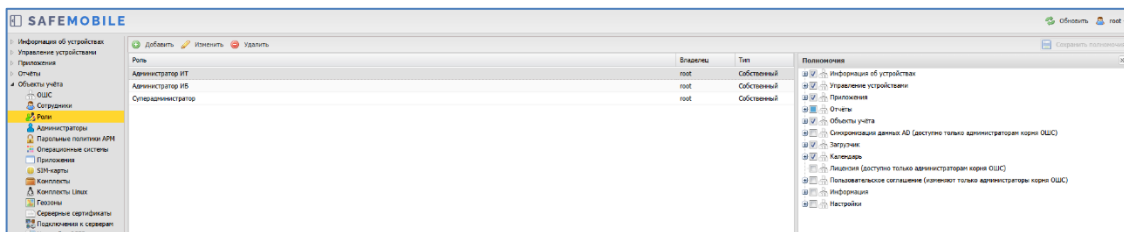


Рисунок 2.117 — Окно «Роли»

Для добавления новой роли в перечень ролей организации нажмите кнопку **«Добавить»** (рисунок 2.118), после чего появится следующее окно:

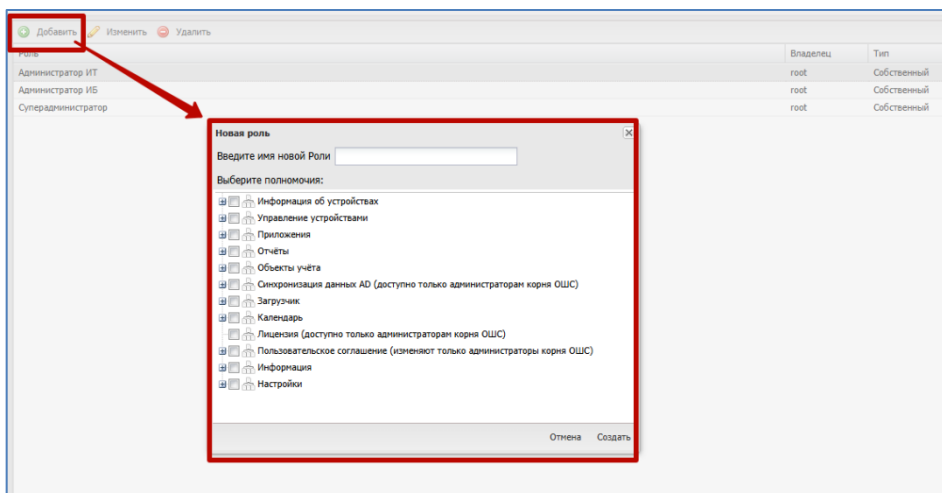


Рисунок 2.118 — Создание роли Администратора

После этого необходимо ввести имя и указать полномочия для новой роли, установив соответствующие флажки.

При добавлении новой роли следует учитывать, что для администраторов, назначенных не на корень дерева ОШС в иерархической структуре подразделений, действуют следующие ограничения:

1. Только администраторам, назначенным на корень дерева ОШС, доступны разделы:
 1. Парольные политики APM,
 2. Объекты учета:
 - Шаблоны писем,
 3. Синхронизация данных LDAP,
 4. Лицензия.
2. Только администраторы, назначенные на корень дерева ОШС, могут редактировать пользовательское соглашение. Прочие администраторы могут только его просматривать и рассылать.
3. Только администраторы, назначенные на корень дерева ОШС, могут редактировать информацию в разделах: «Настройки SCEP», «ОС», «Подключения к серверам».
4. Возможно назначение ограниченного доступа администратора к управлению назначениями для каждого типа сущностей и определяется полномочиями (профилей, правил несоответствия, правил управления приложениями, конфигураций приложений). Администратор сможет просматривать и/или изменять полномочия только для отдельных устройств:
 - Просмотр назначений.
 - Изменение назначений в дереве ОШС.
 - Изменение назначений в списке комплектов.

Для сохранения новой роли и назначенных ей полномочий необходимо нажать кнопку **«Создать»**, после чего она отобразится в списке слева, а также станет доступной для выбора в списке ролей в окне **«Администратор»**.

Для изменения названия роли следует нажать кнопку **«Изменить»**, после чего появится окно в соответствии с рисунком 2.119. После редактирования, для подтверждения изменения, необходимо нажать кнопку **«ОК»**.

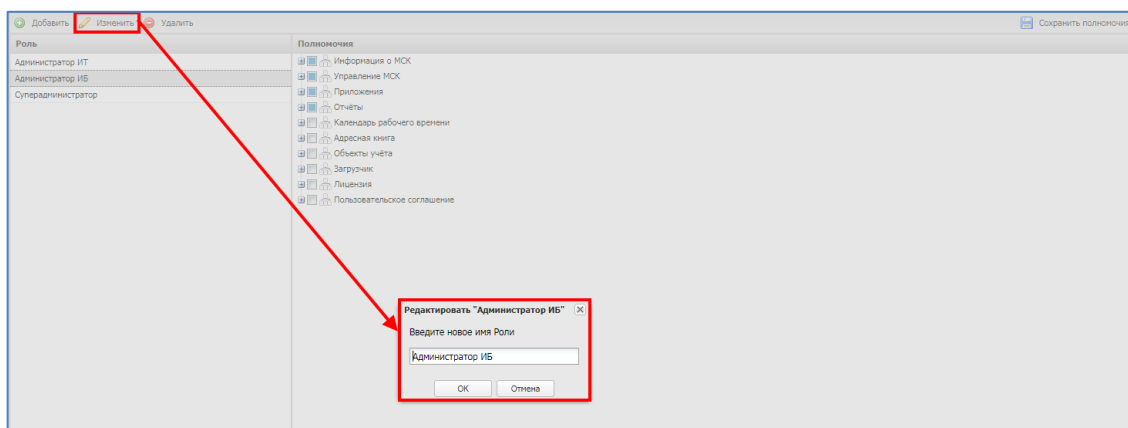


Рисунок 2.119 — Изменение роли Администратора

Для удаления существующей роли требуется нажать кнопку **«Удалить»**. После подтверждения действия (рисунок 2.120) роль будет удалена.

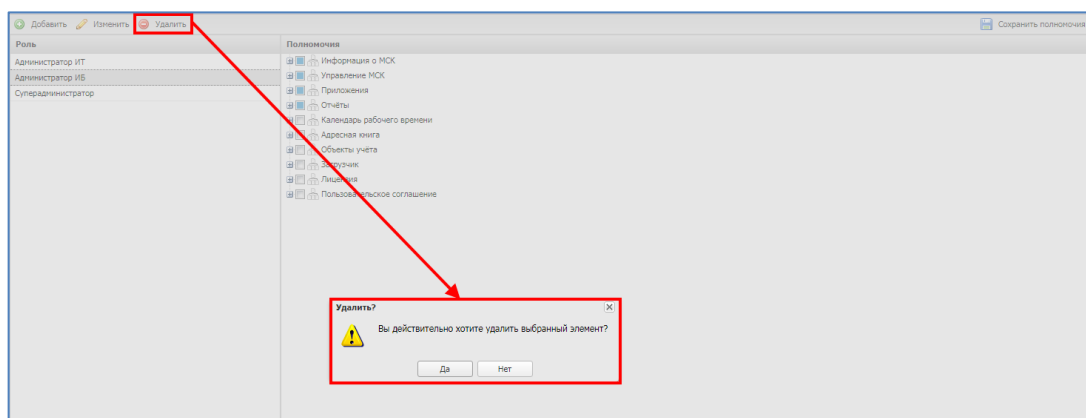


Рисунок 2.120 — Удаление роли Администратора

При удалении роли, которая является единственной назначенной для одного или нескольких администраторов будет выдано предупреждение.

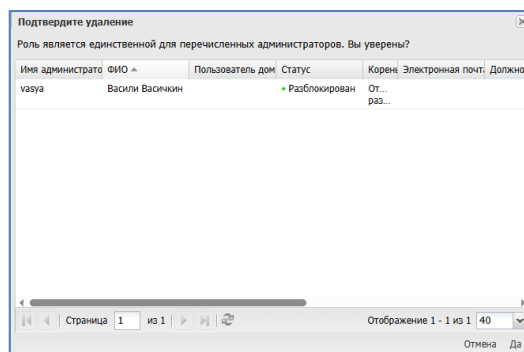


Рисунок 2.121 - Удаление единственной роли и Администратора

Примечания.

- 1. По умолчанию в системе имеется три роли, наделенные соответствующими полномочиями: Администратор ИБ, Администратор ИТ и Суперадминистратор. С полномочиями предустановленных ролей можно ознакомиться в приложении Г.*
- 2. Роль Суперадминистратор обладает максимальными полномочиями и не подлежит редактированию или удалению.*

2.8.4 Администраторы

Раздел содержит в себе справочник администраторов «UEM SafeMobile» и функционал по управлению справочником:

- Просмотр списка администраторов,
- Добавить/Удалить/Заблокировать администратора,
- Редактировать данные администратора,

Справочник представлен в виде списка администраторов и блока просмотра информации об администраторе (рисунок 2.122).

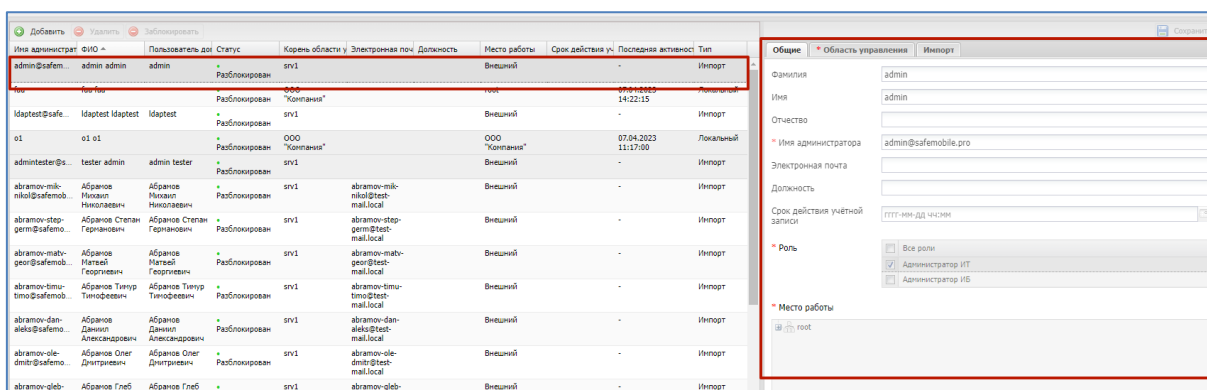


Рисунок 2.122 — Окно «Администратор»

В таблице в левой части окна отображаются следующие столбцы:

- Имя администратора — учетная запись администратора (логин);
- ФИО — фамилия, имя и отчество сотрудника, назначенного администратором;
- Пользователь домена — отображает ФИО администратора (или e-mail, если ФИО не было импортировано);
- Статус — состояние учётной записи администратора (заблокирована или не заблокирована). Статус администратора можно изменить с помощью кнопок «Заблокировать» и «Разблокировать». Изменение статуса допускается только для локальных администраторов;
- Корень области управления — начальный узел поддерева ОШС, на который назначен администратор;
- Электронная почта,
- Должность,
- Место работы,
- Срок действия учётной записи (дата и время),

- Последняя активность (дата и время),
- Тип — тип записи об администраторе (локальный/импорт).

В блоке просмотра информации об администраторе отображаются следующие данные:

- Общие:
 - Фамилия,
 - Имя,
 - Отчество,
 - Имя администратора,
 - Электронная почта,
 - Должность,
 - Срок действия учетной записи,
 - Кнопка «Изменить пароль»
(При нажатии открывается диалоговое окно запроса нового пароля для администратора),
 - Роль,
 - Место работы,
- Область управления:
 - Устанавливать область управления из правила синхронизации при каждой синхронизации (чекбокс) — только для импортированных администраторов (опционально);
 - Дерево ОШС,
- Импорт:
(вкладка отображается только для импортированных администраторов)
 - Поля данных об администраторах, импортированных из внешнего каталога.

В верхней части таблицы находится панель инструментов, содержащая следующие кнопки:

- Добавить — предназначена для добавления новой учётной записи Администратора;
- Удалить — предназначена для удаления выбранной учётной записи Администратора,
- Заблокировать — предназначена для блокирования выбранной учётной записи Администратора;
- Разблокировать — предназначена для разблокирования выбранной учётной записи Администратора;

записи Администратора (кнопка доступная только для заблокированных учётных записей).

2.8.4.1 Редактирование данных администратора

Чтобы изменить данные об администраторе, необходимо выполнить следующие действия:

1. Найти строку с записью об администраторе, подлежащего редактированию,
2. В блоке с информацией об администраторе внести необходимые изменения,
3. Нажать кнопку «Сохранить».

Примечание

1. Редактирование данных администраторов, импортированных из внешних каталогов не доступно.
2. Для администраторов любого типа допустимо изменить «Область управления».
3. Если у администратора не указано ни одной роли, то при сохранении записи об администраторе, система выдаст предупреждение о том, что этот администратор не сможет войти в систему.

2.8.4.2 Добавить нового администратора

Для добавления нового администратора нажмите кнопку **«Добавить»**, после чего следует заполнить форму в правой части окна, на вкладке «Администратор» выбрать роль администратора и область управления в соответствии с рисунком 2.123. Область управления — это поддерево ОШС, на которое администратор может влиять, начиная с узла, на который он назначен и заканчивая устройствами. В дальнейшем для администратора интерфейс будет отображаться только из своей области управления в соответствии с ролью и предоставленным правам. Обязательные для заполнения поля отмечены *.

Примечание

Имя пользователя Администратора должно начинаться с латинского символа. Может содержать латинские символы, цифры, точки, символы подчёркивания и тире. Использование других символов не допускается. Максимальная длина имени пользователя 32 символов.

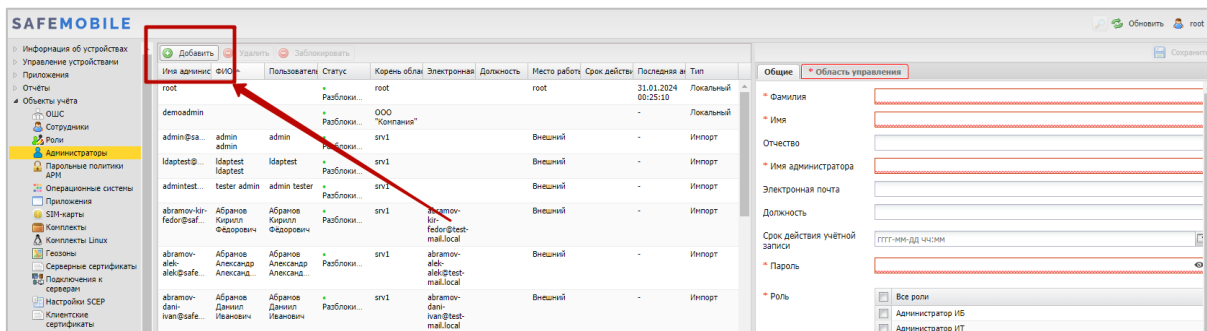


Рисунок 2.123 — Создание Администратора

Для сохранения записи об Администраторе, нажмите кнопку **«Сохранить»**, после чего новая запись отобразится в таблице Администраторов в левой части окна.

Для смены пароля имеющемуся Администратору необходимо выбрать его в списке слева, после чего нажать кнопку **«Изменить пароль»** (рисунок 2.124) в правой части окна на вкладке **«Администратор»**. Если пароль, на который осуществляется смена, не соответствует установленной парольной политике, то при первом входе Администратору потребуется его изменить.

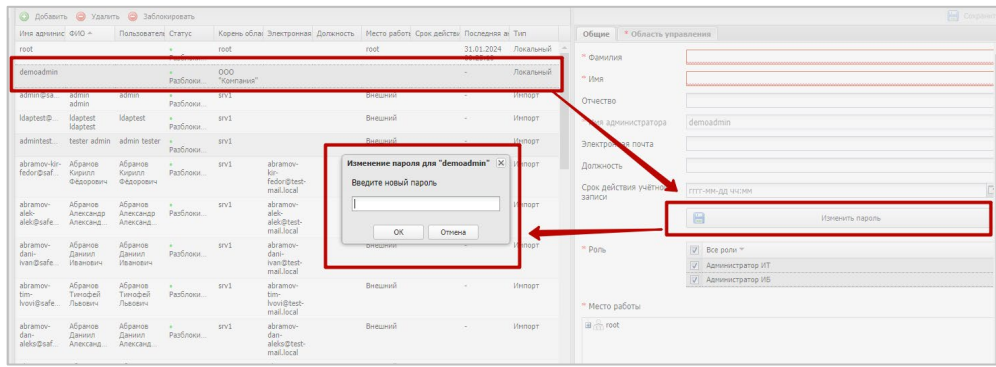


Рисунок 2.124 — Изменение пароля Администратора

2.8.5 Ограничения администраторов

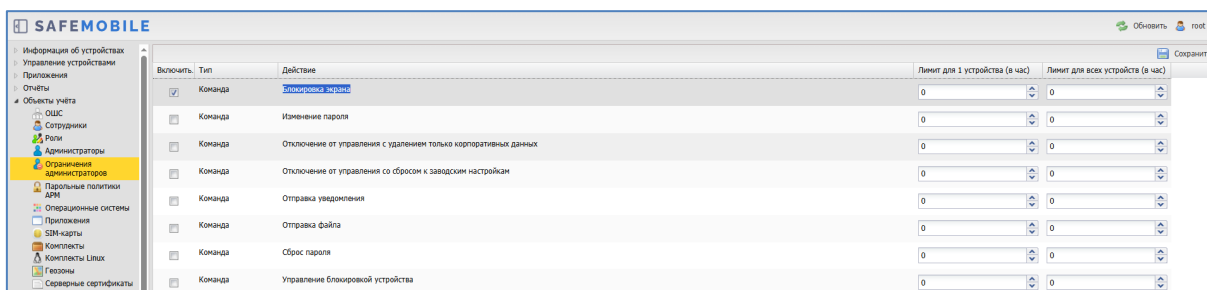
Раздел описывает систему лимитирования операционных действий администраторов, позволяющую устанавливать гибкие ограничения на количество выполняемых операций в час как для одиночных устройств, так и для всей зоны управления (с пропорциональным расчетом при выборе нескольких устройств). Лимиты применяются индивидуально к каждому типу действия, что предотвращает блокировку критически важных функций (например, управления профилями) при исчерпании квот на массовые операции (например, рассылку уведомлений). Действия без заданного лимита не ограничены, права администратора корня ОШС по умолчанию исключены из данной системы.

Доступ к разделу:

Доступ к разделу имеют администраторы назначенные на корень дерева ОШС и определяется полномочиями:

- Просмотр ограничений администраторов (доступно только администраторам корня ОШС).
- Изменение ограничений администраторов (доступно только администраторам корня ОШС).

В центральной части экрана содержится список команд (в том числе именованных), для которых выставляются лимиты выполняемых операций (рисунок 2.125).



Включить	Тип	Действие	Лимит для 1 устройства (в час)	Лимит для всех устройств (в час)
<input checked="" type="checkbox"/>	Команда	Блокировка экрана	0	0
<input type="checkbox"/>	Команда	Изменение пароля	0	0
<input type="checkbox"/>	Команда	Отключение от управления с удалением только корпоративных данных	0	0
<input type="checkbox"/>	Команда	Отключение от управления со сбросом к заводским настройкам	0	0
<input type="checkbox"/>	Команда	Отправка уведомления	0	0
<input type="checkbox"/>	Команда	Отправка файла	0	0
<input type="checkbox"/>	Команда	Сброс пароля	0	0
<input type="checkbox"/>	Команда	Управление Блокировкой устройства	0	0

Рисунок 2.125 — Раздел «Ограничения администраторов»

Каждая строка списка содержит:

1. Чекбокс – Включить/Выключить ограничение;
2. Тип действия;
3. Наименование действия:
 - Блокировка экрана,
 - Изменение пароля,

- Отключение от управления с удалением только корпоративных данных,
 - Отключение от управления со сбросом к заводским настройкам,
 - Отправка уведомления,
 - Отправка файла,
 - Сброс пароля,
 - Управление блокировкой устройства,
4. Лимит для 1 устройства (в час) — Ограничение значения:
- От 0 до 1000000, 0 – означает, что действие запрещено.
 - Лимит действий для всех устройств не должен превышать лимита для одного устройства;
5. Лимит для всех устройств (в час) — Ограничение значения:
- От 0 до 1000000, 0 – означает, что расчет количества разрешенных действий должен вестись на основании лимита для одного устройства.
 - Лимит действий для всех устройств не должен превышать лимита для одного устройства.

Примечание

Ограничения, заданные администратором, будут действовать на команды из разделов:

- *Управление устройствами — Команды;*
- *Управление устройствами — Именованные команды.*

Для назначения лимита действий необходимо:

1. Указать в нужной строке действия значения для «Лимит для 1 устройства (в час)» и/или «Лимит для всех устройств (в час)».
2. Отметить чекбокс «Включить».
3. Нажать кнопку «Сохранить».

Для отмены установленного лимита на действия необходимо снять чекбокс «Включить» со строки нужного действия и нажать кнопку «Сохранить».

Принцип работы управления лимитами запросов (Алгоритм «Корзина токенов»).

1. Назначение и цель

Данный механизм предназначен для контроля частоты отправки команд администраторами. Каждому администратору и каждой команде выделяется индивидуальный лимит запросов.

2. Ключевые параметры системы

- **Индивидуальная «корзина»:** Каждый администратор и каждая команда имеют свою собственную виртуальную «корзину токенов».
- **Емкость корзины: 36 000 000 токенов.** Это максимальный запас, который можно использовать одновременно.
- **Скорость пополнения: 36 000 000 токенов в час** (эквивалентно 10 000 токенов в секунду). Это означает, что даже полностью опустошенная корзина восстановит свой полный объем ровно за 1 час.

3. Расчет стоимости команды

Перед выполнением действия система автоматически рассчитывает его «стоимость» в токенах. Цель — привести заданные в системе лимиты к единой системе измерения (токенам). Используются две формулы:

3.1 Формула на основе лимита для одного устройства:

Применяется, когда установлен лимит "на одно устройство".

*Стоимость = (Емкость корзины / Лимит на 1 устройство в час) * Количество целевых устройств*

3.2 Формула на основе лимита для всех устройств:

Применяется, когда установлен глобальный лимит "на все устройства"

*Стоимость = (Емкость корзины / Общий лимит для всех устройств) * (Количество целевых устройств / Общее число устройств в зоне ответственности)*

3.3 Минимальная стоимость команды:

Стоимость действия не может быть меньше, чем стоимость одной одиночной команды:

Минимальная стоимость = (Емкость корзины / Лимит на 1 устройство в час)

Важно!

*Система всегда выбирает **меньшую** стоимость из рассчитанных по формулам на основе лимита. Если выбранная стоимость оказывается меньше минимальной, то стоимость действия принимается равной минимальной. Это позволяет гибко соблюдать оба типа ограничений, не блокируя операции излишне строго.*

4. Логика выполнения команды

Процесс выполняется автоматически для каждого действия:

1. Проверка остатка: Система проверяет текущее количество токенов в корзине администратора (или команды), инициирующего действие.
2. Расчет стоимости: Рассчитывается стоимость планируемой команды по алгоритму выше.
3. Принятие решения:
 - **Если токенов достаточно (остаток \geq стоимости):** Токены списываются, команда выполняется и отправляется на устройства.
 - **Если токенов недостаточно (остаток $<$ стоимости):** Команда полностью отклоняется и не отправляется ни на одно устройство. Частичное выполнение невозможно.

5. Практический пример для принятия управленческих решений

Сценарий действий:

- Установленный лимит: не более 1 000 команд в час на одно устройство.
- Администратор пытается отправить команду на 10 устройств одновременно.
- Глобальный лимит "на все устройства" не задан.

Расчет стоимости системой:

Стоимость = $(36\ 000\ 000 / 1\ 000) * 10 = 36\ 000 * 10 = 360\ 000$ токенов

Решение системы:

Команда будет выполнена, только если на момент запроса в корзине администратора имеется 360 000 или более токенов. В противном случае запрос будет заблокирован.

Управленческое значение для администратора:

При настройке лимитов администратор может оперировать привычными величинами (команды/час на устройство). Система внутренне конвертирует их в токены, чтобы обеспечить соблюдение лимитов для команд любой сложности и масштаба.

2.8.6 Парольные политики APM

Для настройки параметров пароля и учетной записи при входе в «UEM SafeMobile» следует открыть пункт меню «**Парольные политики APM**» (рисунок 2.126).

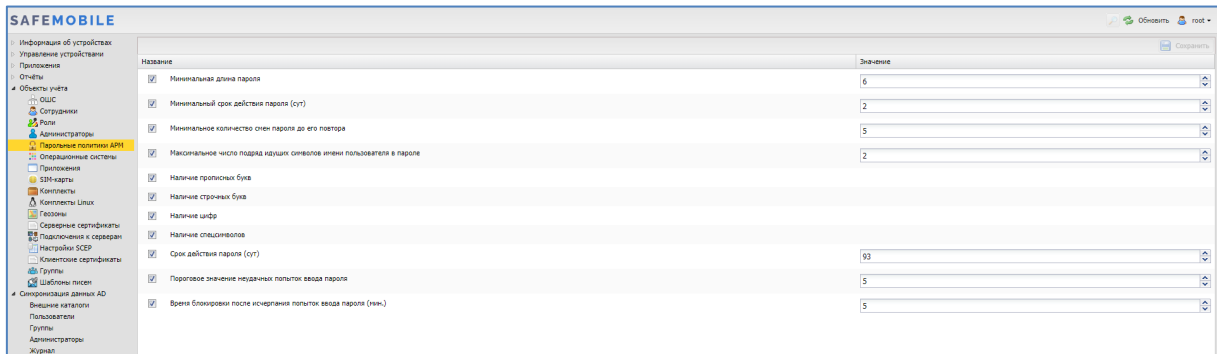


Рисунок 2.126 — Окно «Парольные политики APM»

Таблица парольных политик состоит из следующих столбцов:

- **Название** — название параметра парольной политики, который можно включить или отключить с помощью флажков;
- **Значение** — значение, которое необходимо для применения параметра парольной политики (при его наличии). После установки системы отображаются рекомендованные величины.

В таблице 2.5 указываются параметры парольных политик APM и рекомендованные значения.

Таблица 2.5 — Параметры парольной политики и рекомендованные значения

Название	Значение
Минимальная длина пароля	6
Минимальный срок действия пароля (сут)	2
Минимальное количество смен пароля до его повтора	5
Максимальное количество подряд идущих символов имени пользователя в пароле	2
Наличие прописных букв	Да
Наличие строчных букв	Да
Наличие цифр	Да

Название	Значение
Наличие спецсимволов	Да
Срок действия пароля (сут)	93
Пороговое значение неудачных попыток ввода пароля	5
Время блокировки после исчерпания попыток ввода пароля (мин.)	5

После выбора значений для сохранения параметров парольных политик нажмите кнопку **«Сохранить»**.

Примечание

- Парольные политики APM действуют только на локальных администраторов. На импортированных администраторов действуют доменные парольные политики.
- Спецсимволами являются следующие знаки: !\$#%@^&*()~/[]
Знаки «+» и «-» спецсимволами не являются.

2.8.7 Операционные системы

Справочник операционных систем ведется для учёта используемых мобильных платформ для связи приложений и ОС. Данные об ОС необходимо внести в соответствующий справочник до начала регистрации МСК в «UEM SafeMobile».

Чтобы открыть окно **«Операционные системы»**, необходимо выбрать соответствующий пункт главного меню АРМ, после чего отобразится таблица с перечнем операционных систем и их версий в соответствии с рисунком 2.127. Поле **«id»** с номером операционной системы (по умолчанию, в таблице не отображается).

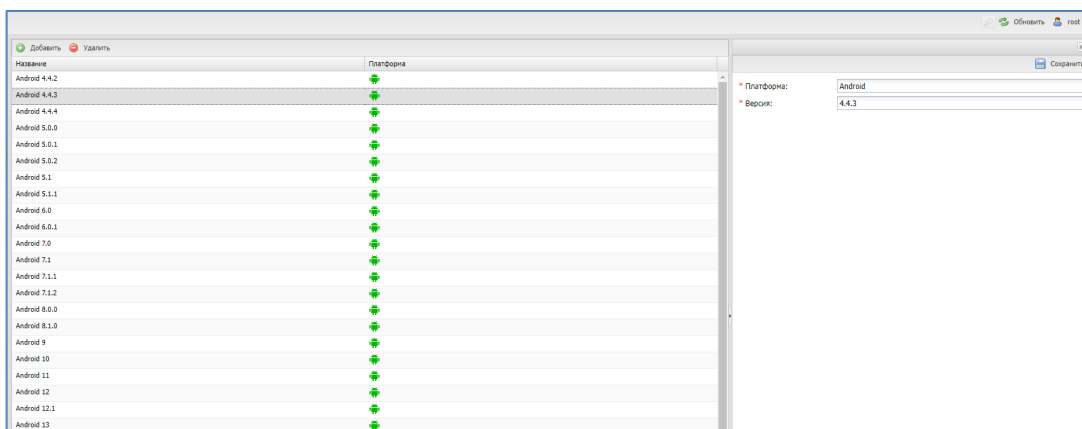


Рисунок 2.127 — Окно «Операционные системы»

Для добавления новой ОС в «UEM SafeMobile» используется кнопка **«Добавить»** в панели инструментов окна (рисунок 2.128), которая позволяет в правой части окна выбрать мобильную платформу в поле **«Платформа»** и указать версию добавляемой ОС в поле **«Версия»**.

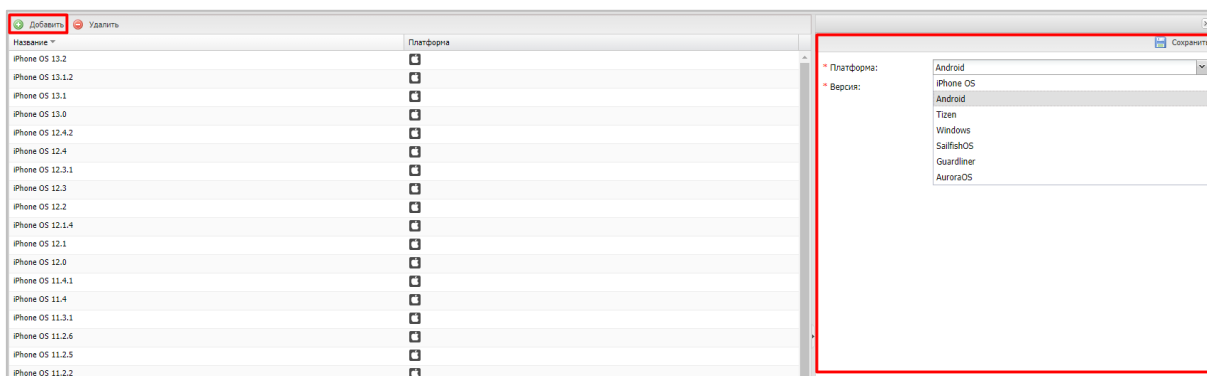


Рисунок 2.128 — Добавление ОС

После нажатия кнопки **«Сохранить»** созданная запись об ОС будет сохранена в системе.

Для удаления записи об ОС используется кнопка **«Удалить»**. При нажатии кнопки **«Удалить»** (рисунок 2.129) запрашивается подтверждение выполняемого действия, и выбранная запись об ОС удаляется из базы при отсутствии связанных объектов учёта.

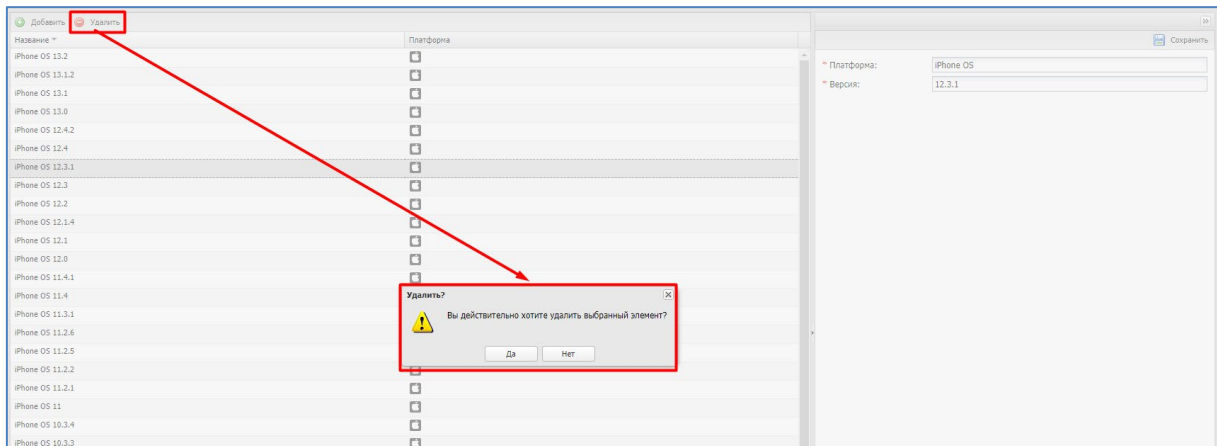


Рисунок 2.129 — Удаление ОС

2.8.8 Приложения

Репозиторий приложений ведётся для учёта и распространения приложений. Перечень приложений, зарегистрированных в «UEM SafeMobile», отображается в окне «Приложения» раздела «Объекты учёта» в соответствии с рисунком 2.130.

Таблица приложений содержит следующие столбцы:

- id — номер приложения в системе (по умолчанию; в таблице не отображается);
- UID — уникальный идентификатор приложения;
- Монитор — флаг отображает является ли приложение мобильным клиентом SafeMobile или нет. Определяется системой автоматически, изменить вручную нельзя;
- Тип — тип приложения: корпоративное (приложение; для которого загружен дистрибутив) /некорпоративное (любое другое приложение);
- Версия — версия приложения;
- Код версии— код версии приложения;
- Загружено — дата загрузки приложения в систему;
- Описание — текстовое описание приложения;
- Платформа — отображает значок платформы, на которой работает приложение;
- Владелец — администратор узла ОШС, назначенный владельцем сущности.

Имя	UID	Монитор	Тип	Версия	Код версии	Загружено	Описание	Платформа	Владелец
id									
Приложение # 0	ru.application.na...	Нет	Корпоративное	1.0	111	01.10.2025 15:06:45			ООО "Компания"
Приложение # 1	ru.application.na...	Нет	Корпоративное	1.1	111	01.10.2025 15:06:45			ООО "Компания"
MCC-Android-release	ru.nisobk.mcc.a...	Нет	Корпоративное	4.5.2	111	01.10.2025 15:06:45			ООО "Компания"
Google Play	com.android.ve...	Нет	Корпоративное	43.3.32-23 [0] [PR] 68969905	84333200	07.10.2025 17:29:24		root	
MCC-Android-release	ru.nisobk.mcc.a...	Нет	Корпоративное	5.0.1	111	01.10.2025 15:06:45			ООО "Компания"
Calculator++	org.solovjev.an...	Нет	Некорпоративн...	-	-	-	Калькулятор	root	
ColorNote	com.socialmob...	Нет	Некорпоративн...	-	-	-	Заточки	root	
ES File Explorer	com.estrongs.a...	Нет	Некорпоративн...	-	-	-	File Explorer	root	
WhatsApp	com.whatsapp	Нет	Корпоративное	2.25.2.85	250285003	06.10.2025 11:52:47		root	
Яндекс Карты	ru.yandex.yand...	Нет	Некорпоративн...	-	-	-		root	
Gmail	com.google.and...	Нет	Корпоративное	2025.08.25.800...	65311558	07.10.2025 08:48:37		root	
Telegram	org.telegram.m...	Нет	Корпоративное	11.12.0	59879	06.10.2025 11:52:02		root	
MCC-Android-release	ru.nisobk.mcc.a...	Нет	Корпоративное	5.0.0	111	01.10.2025 15:06:45			ООО "Компания"
Приложение # 3	ru.application.na...	Нет	Корпоративное	1.0	111	01.10.2025 15:06:45			ООО "Компания"

Рисунок 2.130 — Окно «Приложения»

По умолчанию, записи в реестре приложений группируются по платформам. Возможна также группировка по заданному полю. Сгруппировать по этому полю Для этого следует выбрать необходимый столбец и, при сортировке записей в раскрывающемся

меню, нажать на строку в соответствии с рисунком 2.131. В этом случае записи сгруппируются по версии приложений. Для разгруппировки записей приложений необходимо в раскрывающемся меню снять флажок в строке «Группировать».

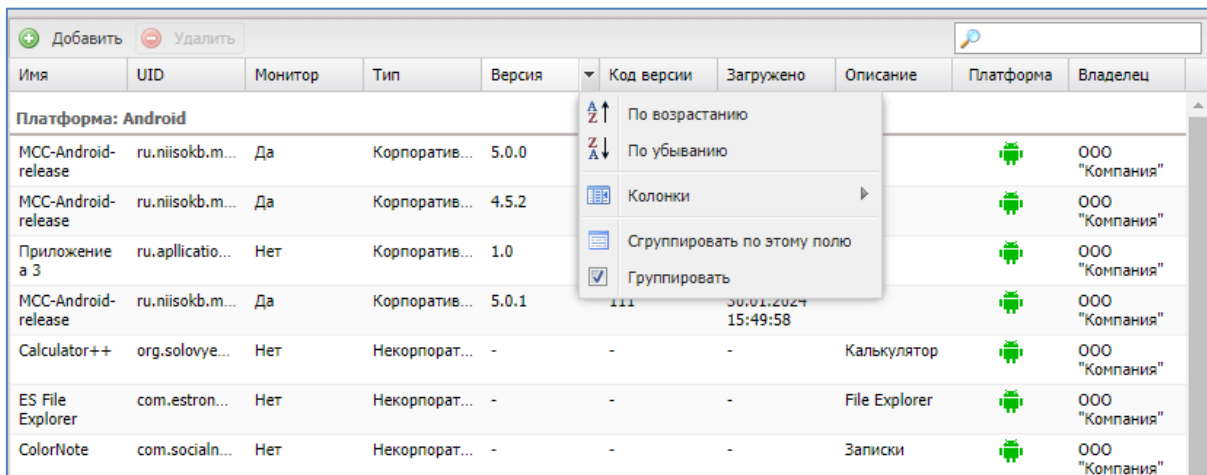


Рисунок 2.131 — Группировка приложений

В правой части рабочего экрана отображаются параметры, выбранного в списке приложения, а также критично важные разрешения запрашиваемые приложением (только для Android — см. Управление разрешениями приложений 2.6.12.6).

2.8.8.1 Добавление записи о приложении в систему

Для добавления в систему записи о приложении используется кнопка «**Добавить**» в верхней панели инструментов окна. Затем в правой части окна (рисунок 2.132) следует выбрать «**Тип приложения**».

Формы для корпоративных и некорпоративных приложений различны.

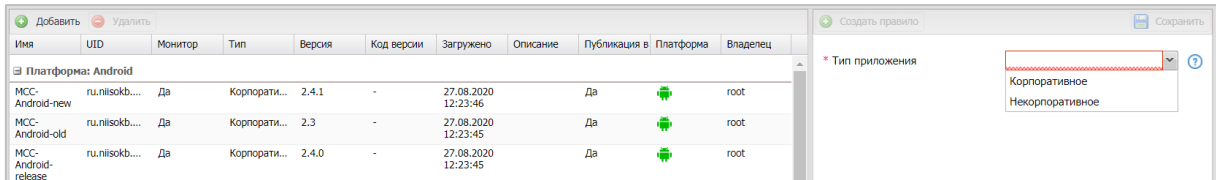


Рисунок 2.132 — Добавление приложения

2.8.8.1.1 Некорпоративное приложение

При добавлении **некорпоративного** приложения необходимо заполнить форму в соответствии с рисунком 2.133, содержащую перечень параметров добавляемого приложения. Поля, обозначенные * — обязательные для заполнения.

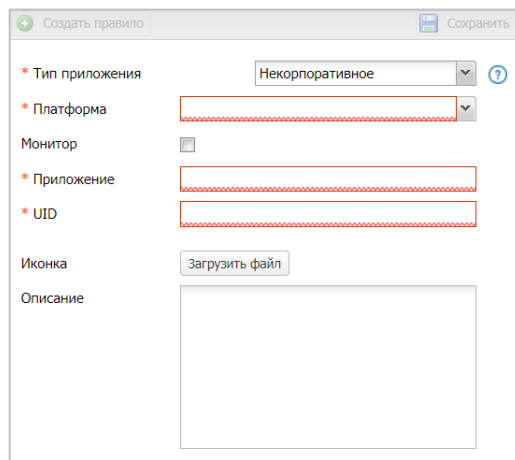


Рисунок 2.133 — Форма некорпоративного приложения

Если при заполнении формы поля не заполнились автоматически, то их нужно ввести вручную.

При добавлении приложения для МСК на платформе Android из Google Play UID приложения следует выбрать из адресной строки в соответствии с рисунком 2.134.

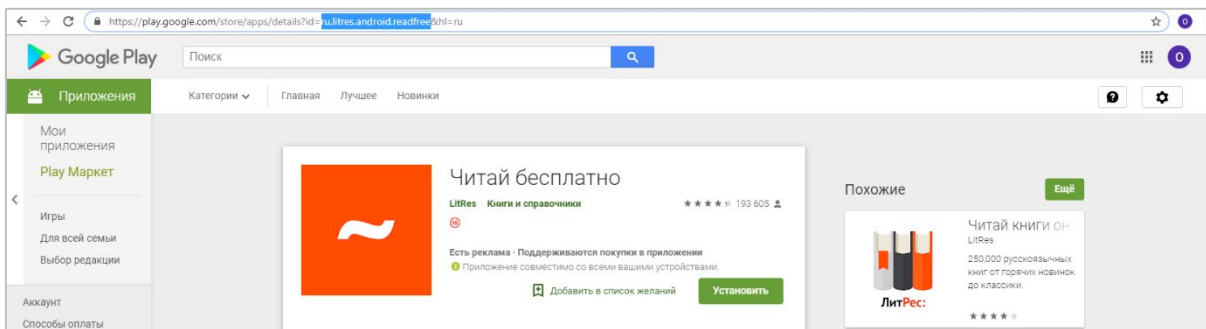


Рисунок 2.134 — Добавление приложения из Google Play

Для загрузки иконки нажать кнопку **«Загрузить файл»** и выбрать файл рисунка для приложения. Для продолжения работы нажать кнопку **«Сохранить»**.

После этого осуществляется запись в БД введенной информации, и запись о добавленном приложении воспроизведется в таблице в левой части окна. Приложение будет доступно для назначения ПУП, для этого следует нажать кнопку **«Создать правило»** и выполнить действия согласно описанию в 2.6.11.

Особенности создания записи о приложении для платформы Windows

Приложения на МСК платформы Windows загружаются в 2 этапа:

1. Необходимо подготовить файл с метаданными. На ПК с ОС Windows 10+ запустить **PowerShell** и выполнить команду:
 - `./msi-info.ps1 ./<приложение>.msi`
 - После выполнения команды, в той же папке появится файл `<приложение>.msi.meta.json`.
2. Загрузить msi-файл в соответствии с описанием, приведенном в данном разделе, как Корпоративное приложение: нажать кнопку **«Загрузить файл»** и загрузить файл с метаданными `<приложение>.msi.meta.json`, затем нажать кнопку **«Сохранить»**.

Сам скрипт **msi-info.ps1** можно скачать при загрузке первого msi-приложения (появится кнопка **«Скачать скрипт»**) и использовать в дальнейшем для последующих приложений.

Примечание

Если при первом выполнении скрипта возникает ошибка, извещающая об отсутствии у пользователя прав на выполнение ps-скриптов, необходимо один раз выполнить команду:

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope CurrentUser
```

Если некорпоративное приложение уже было установлено на МСК пользователя, то процедура добавления записи в систему аналогична процедуре в разделе «**Приложения/Управления приложениями**» при нажатии кнопки «**Зарегистрировать**».

2.8.8.1.2 Корпоративное приложение

При добавлении **корпоративного** приложения необходимо в строке «**Файл**» нажать кнопку «**Загрузить файл**», после чего в появившемся окне выбрать файл дистрибутива приложения. Загружаемые приложения имеют следующий формат:

- для устройств на платформе **iOS** — **IPA**;
- для устройств на платформе **Android** — **APK, APKS, XAPK, APKM**;
- для устройств на платформе **Windows** — **MSI** (только приложения в режиме автоматической установки);
- для устройств на платформе **Аврора** — **RPM**;
- для устройств на платформе **Linux** — **RPM**.

После загрузки дистрибутива его название, версия, код версии, UID, описание определяются автоматически и отразятся в соответствующих полях формы. Если поля не были заполнены автоматически, то их нужно ввести вручную. Поля, обозначенные * — обязательные для заполнения.

Примечание

- Для платформ *Linux* и *Аврора* необходимо указать платформу, вручную.
- Для платформ *Linux* необходимо указать «дистрибутив»
- Некорректное (ошибочное) заполнение поля *UID* приведет к воспроизведению ошибочных действий при установке приложения на МСК. Для МСК

платформы Windows такие действия приведут к невозможности удаления приложения средствами SafeMobile, т.к. регистрация установки была произведена для другого UID приложения.

Для завершения процесса создания в системе записи о приложении следует нажать кнопку **«Сохранить»**. После этого осуществляется запись в БД введенной информации и запись о добавленном корпоративном приложении воспроизведется в таблице в левой части окна. Приложение будет доступно для назначения ПУП, для этого следует нажать кнопку **«Создать правило»** и выполнить действия согласно описанию в 2.6.11.

2.8.8.2 Редактирование записи о приложении

Для приложения, выбранного в левой части окна, можно изменить параметры в соответствии с рисунком 2.135. После нажатия кнопки **«Сохранить»** внесенные изменения сохранятся в БД.

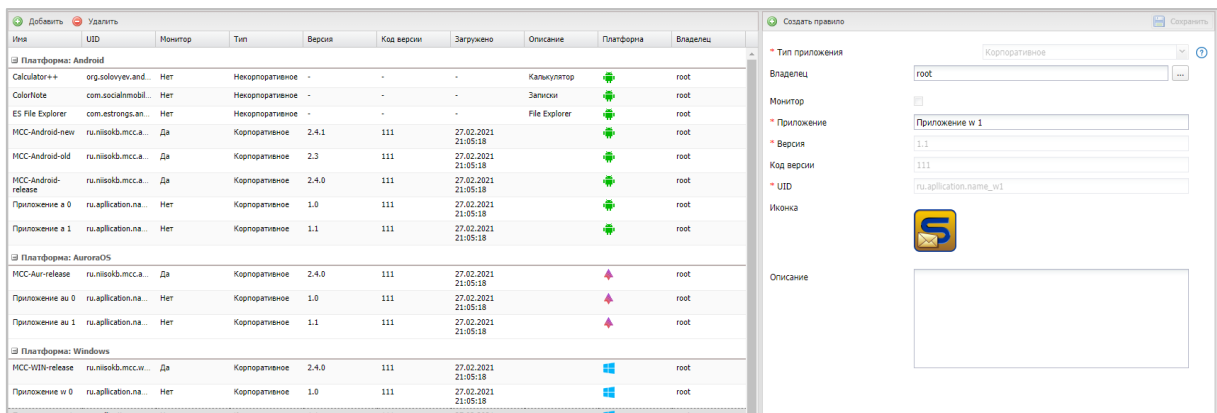


Рисунок 2.135 — Редактирование приложения

2.8.8.3 Удаление записи о приложении

Для удаления приложения необходимо выбрать в таблице соответствующую ему запись в соответствии с рисунком 2.136 и нажать кнопку «Удалить».

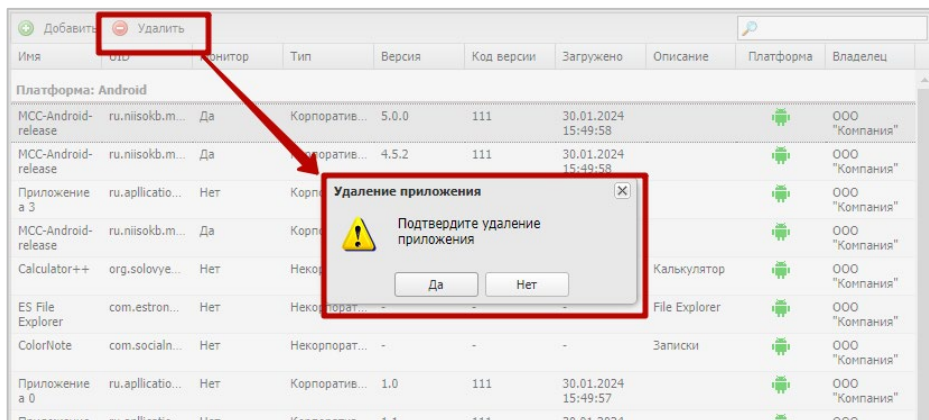


Рисунок 2.136 — Удаление приложения

После подтверждения выполняемого действия выбранная запись удалится из БД при отсутствии связанных объектов учёта.

2.8.8.4 Создание шаблона конфигурации из записи о приложении

Кнопка «Извлечь шаблон конфигурации» позволяет автоматически сгенерировать шаблон конфигурации приложения путем парсинга манифеста установленного приложения. Доступно только для приложений платформы Android.

Предварительные требования

- Приложение должно быть установлено в системе или его APK-файл должен быть доступен для анализа
- Пользователь должен иметь права администратора с полномочиями на создание шаблонов конфигураций
- Поддерживаемые платформы: Android

Для **создания шаблона** необходимо выполнить следующие действия:

1. Откройте раздел «Объекты учёта — Приложения».
2. Выбрать целевое приложение из списка.
3. Нажать кнопку «Извлечь шаблон конфигурации» (кнопка активна только для Android-приложений), после чего откроется модальное окно отображающее процесс создания шаблона.

Процесс извлечения и анализ:

1. Анализ манифеста приложения (для Android - APK).
2. Извлечение доступных настроек конфигурации.
3. Определение типа данных, ограничений и параметров отображения для каждой настройки.
4. Формирование структуры шаблона в соответствии с требованиями системы
5. После успешного завершения процесса система:
 - Создаст новый сгенерированный шаблон в разделе «Шаблоны конфигураций».
 - Автоматически заполнит все обязательные атрибуты:
 - Приложение,
 - UID,
 - Версия приложения,
 - Код версии,
 - Платформа,
 - Список настроек с типами, наименованиями и параметрами отображения.

Примечание

- *Извлечение возможно только если производитель приложения опубликовал настройки в манифесте.*
- *Некоторые приложения могут не иметь настроек в манифесте, даже если поддерживают управление конфигурациями.*

2.8.9 Шаблоны конфигураций

Раздел содержит список шаблонов конфигураций приложений, как встроенных, так и сгенерированных администратором (рисунок 2.137).

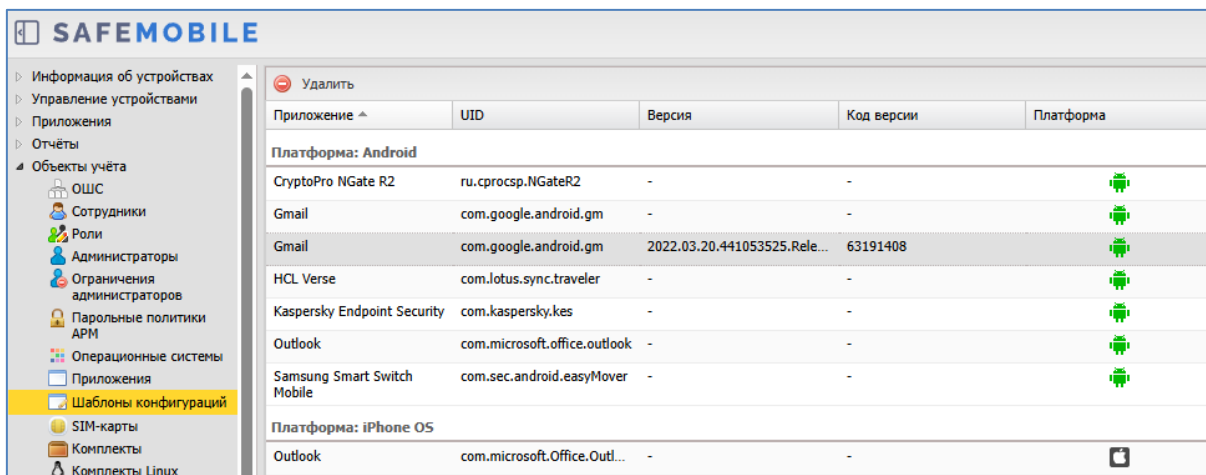


Рисунок 2.137 — Раздел «Шаблоны конфигураций»

Каждая строка списка содержит следующие данные:

- Приложение — название приложения;
- UID — UID приложения;
- Версия — версия приложения (только для сгенерированных шаблонов);
- Код версии — код версии приложения (только для сгенерированных шаблонов);
- Платформа.

Раздел позволяет удалять сгенерированные шаблоны. Для удаления шаблона следует выбрать нужный шаблон в списке и нажать кнопку «Удалить».

2.8.10 SIM-карты

Окно «**SIM-карты**» предназначено для управления записями о SIM-картах, используемых на устройствах. Чтобы открыть окно, выберите пункт «**SIM-карты**» в главном меню АРМ Администратора SafeMobile в соответствии с рисунком 2.138.

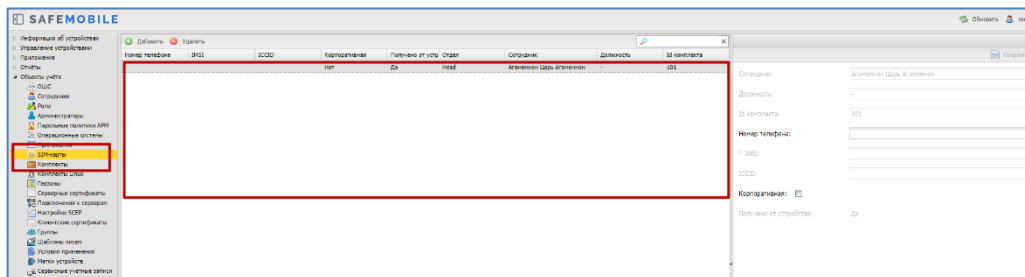


Рисунок 2.138 — Окно SIM-карты

Таблица зарегистрированных SIM-карт содержит столбцы:

- id — номер SIM-карты в системе (по умолчанию, в таблице не отображается);
- Номер,
- IMSI,
- ICCID,
- Корпоративная,
- Получено от устройства,
- Отдел,
- Сотрудник,
- Должность,
- Id комплекта.

SIM-карты регистрируются в системе автоматически (по данным подключенного МСК) или Администратором «вручную».

Администратор может назначить SIM-карте номер телефона или изменить признак её корпоративности при помощи соответствующего флажка (рисунок 2.139). Изменение полей IMSI и ICCID доступно для SIM зарегистрированных «вручную» администратором. После изменения параметров SIM-карты следует нажать кнопку «**Сохранить**».

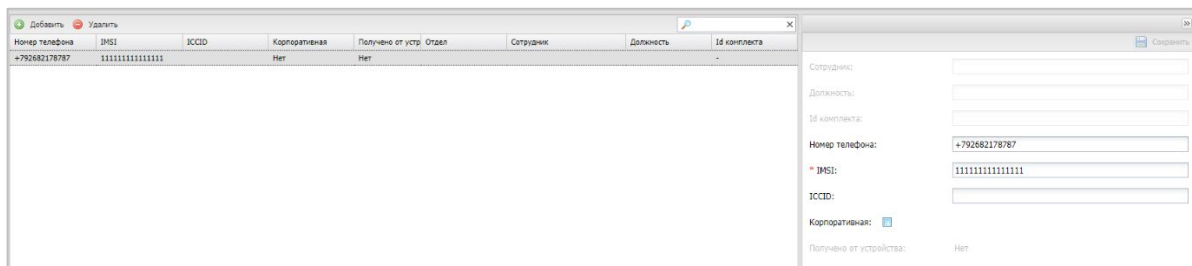


Рисунок 2.139 — Изменение записи о SIM-карте

Чтобы добавить новую SIM «вручную», необходимо выполнить следующие действия:

1. Перейти раздел системы «SIM-карты».
2. Нажать кнопку «Добавить».
3. Заполнить обязательное поле (IMSI).
4. Нажать кнопку «Сохранить» (рисунок 2.140).

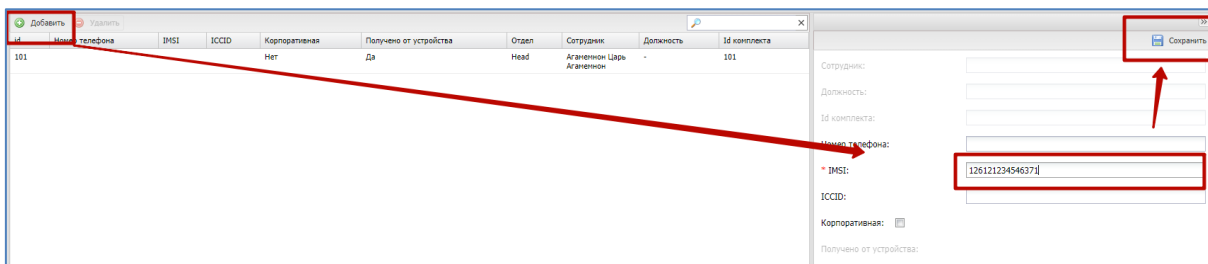


Рисунок 2.140 — Добавление новой SIM

5. Выделить в таблице созданную запись SIM и изменить номер телефона.
6. Нажать кнопку “Сохранить”

Для удаления SIM-карты следует выбрать ее в таблице и нажать кнопку «Удалить» (рисунок 2.141).

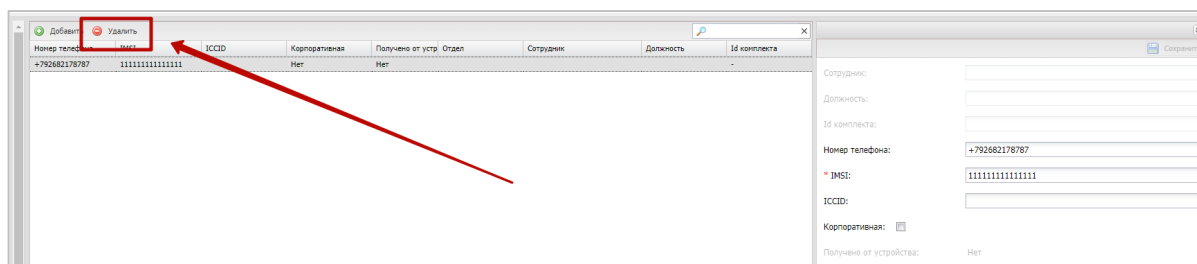


Рисунок 2.141 — Удаление записи о SIM-карте

Система запросит подтверждение удаления записи. Если у данной SIM-карты нет связанных объектов учета, она будет удалена из базы данных без запроса подтверждения действия.

Примечание

Для Android.

Если при регистрации SIM-карты номер телефона не был определен системой автоматически, необходимо выполнить следующие действия:

- 1. Применить к устройству администратора и к устройству пользователя (или ко всему дереву ОШС) профиль «Настройки монитора Android»,*
- 2. Включить политику «Регистрировать SMS»,*
- 3. В политике «Номер телефона для отправки SMS с параметрами SIM» указать номер администратора в формате +7XXXXXXXXXX. На телефоне администратора должен быть установлен «монитор».*

После чего на телефон администратора поступит техническое SMS с параметрами SIM-карты: ICCID и IMSI. По этим параметрам система сопоставит номер телефона отправителя смс с параметрами SIM-карт в системе, после чего номер телефона будет зарегистрирован.

2.8.11 Комплекты

Раздел отображает список всех комплектов в системе, (включая как те, что не подключались к системе). Здесь также можно создавать новые комплекты и редактировать параметры существующих.

Комплект является основным объектом учёта в системе. Комплект определяет абонента системы и устанавливает соответствие между SIM-картой, сотрудником и конфигурацией мобильного клиента SafeMobile. В таблице окна в соответствии с рисунком 2.142 имеются следующие столбцы:

Сотрудник	Пользователь домена	Загрузить файл	ИМЭИ	Свойный номер	Монитор	Статус
Сотрудник Петр Валерьевич	Пользователь домена	Загрузить файл	01232791024537	245377	3.0.0.9999	[Icons]
Гарин Юрий Александрович		Выгрузить комплект	9900020782895	8052285	1.20.0.9999	[Icons]
Данилов Григорий Павлович		Управление устройством	9900020782895	8052285	1.55.9999	[Icons]
Крикин Денис Андреевич		Служба разработки	0413268792124	-	-	[Icons]
Зубков Александр		Служба разработки БД	3530310108263	43941283801466	dev-1049-08-9308892	[Icons]
Новиков Александр Васильевич		Группа разработки	470800000020	0126951012483	124234	[Icons]
Новиков Петр Николаевич		Служба разработки	054220014223	-	-	[Icons]
Гаврилов Галина Николаевна		Группа разработки	013720194523	465224	1.20.0.9997	[Icons]
Климова Анна Леонидовна		Служба разработки БД	051240352968	-	-	[Icons]
Королев Сергей Павлович		Группа разработки	350301030245	23876107376	3.0.0.9-Dev	[Icons]
Новиков Александр Ярославич		Группа разработки	-	-	-	[Icons]
Новиков Федор Павлович		Группа разработки	3548000002454	471108661206	14.0.0.1_мобиль	[Icons]
Новиков Федор Павлович		Группа разработки	0675201212076	-	1.0.0.9996	[Icons]
Павлов Максим Дмитриевич		Служба разработки	9542201751245	-	-	[Icons]

Рисунок 2.142 — Окно «Комплекты»

- Сотрудник (по умолчанию, отображается в таблице),
- Пользователь домена — Отображает ФИО сотрудника или e-mail, если ФИО не было импортировано (по умолчанию, отображается в таблице);
- Отдел/Группа (по умолчанию, отображается в таблице),
- Должность,
- E-mail — E-mail,
- employeeID — Импортированный из LDAP атрибут employeeID;
- samaccountName — Импортированный из LDAP атрибут samaccountName;
- userPrincipalName — Импортированный из LDAP атрибут userPrincipalName;
- SIM: Принадлежность,
- Состояние роуминга,
- IMSI,
- ICCID,
- Телефон (по умолчанию, отображается в таблице),
- id,
- Состояние блокировки,
- Управление устройством,

- Последняя активность,
- Тип соединения,
- Статус соединения,
- IP адрес,
- Тип устройства,
- Модель устройства,
- IMEI (по умолчанию, отображается в таблице),
- UDID,
- Серийный номер (по умолчанию, отображается в таблице),
- Тип контейнера,
- Заряд аккумулятора,
- Устройство: Принадлежность,
- Монитор (по умолчанию, отображается в таблице),
- Платформа,
- Версия,
- Статус (по умолчанию, отображается в таблице),
- Стратегия,
- Метки,
- Привязанные SIM (IMSI).

В верхней части рабочего экрана расположены кнопки следующих функций:

- Добавить — добавить комплект,
- Удалить — удалить комплект,
- Отключить — отключить комплект от управления (кнопка доступна при наведении на подключенный комплект),
- Разблокировка:
 - Разблокировка устройств — вызывает окно разблокировки устройств. Позволяет разблокировать подключенные, отключенные и удаленные комплекты для Android. Более подробно в «Инструкция по временной разблокировке устройства (Android, Аврора)»;
 - Разблокировка администратора устройства — разблокировка учетной записи администратора на устройстве ОС Аврора. Функционал аналогичен «Разблокировка устройство» для Android;
- Дополнительно:
 - Загрузить файл — позволяет загрузить список комплектов из файла;
 - Скачать шаблон — позволяет скачать из системы шаблон списка комплектов;

- Выгрузить комплекты — позволяет выгрузить из системы список комплектов.

Перед созданием комплекта необходимо убедиться в том, что запись о сотруднике, которому планируется назначить создаваемый комплект, уже содержится в справочнике системы.

Для добавления нового комплекта используется кнопка **«Добавить»**, после нажатия которой отображается диалоговая форма в соответствии с рисунком 2.143, в которой необходимо выбрать ФИО сотрудника, которому будет назначен добавляемый комплект.

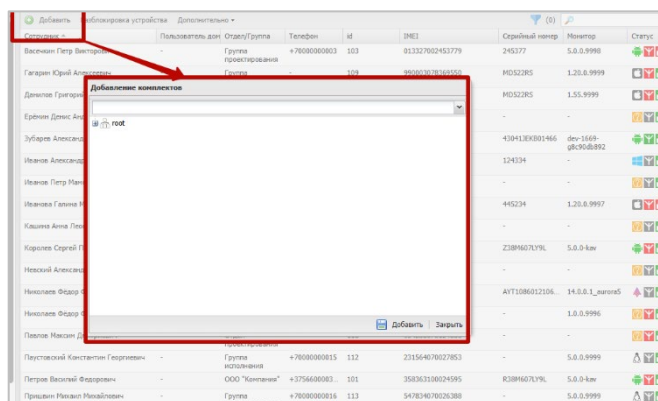



Рисунок 2.143 — Создание комплекта, вкладка «Сотрудник»

Для осуществления поиска, дополнительно к поисковой системе в главной таблице предназначена кнопка  в правом верхнем углу.

В верхней панели инструментов правой части окна расположена кнопка **«Сохранить»**, при нажатии которой осуществляется сохранение конфигурации комплекта. Кнопка **«Сохранить»** становится доступной только после выбора сотрудника на вкладке **«Сотрудник»**.

2.8.11.1 Загрузка комплектов

Кнопка «**Загрузить файл**» предназначена для добавления комплектов сотрудников:

- МСК которых были зарегистрированы посредством КМЕ в соответствии с «Руководством администратора по регистрации устройств в SafeMobile с помощью КМЕ».
- для МСК которых известны IMEI или серийные номера и которые планируется подключать со стратегией управления «Только устройство». После нажатия кнопки открывается диалоговая форма в соответствии с (рисунок 2.144). В которой необходимо выбрать подразделение, в которое будут импортированы комплекты и файл с комплектами.

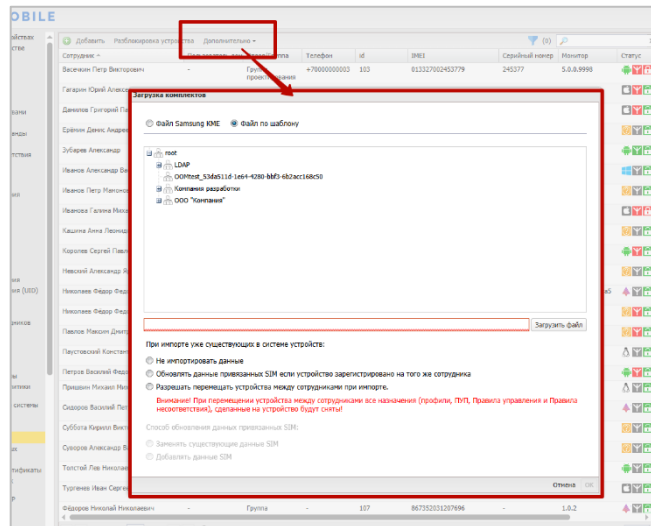


Рисунок 2.144 — Загрузка комплектов

Для импорта комплектов в систему необходимо выполнить следующие действия:

1. Перейти в раздел «Комплекты».
2. Нажать кнопку «Дополнительно — Загрузить файл».
3. Выбрать загружаемый тип файла:
 - Файл Samsung KME — загрузка файла формата CSV, выгружаемого из портала Knox Mobile Enrollment корпорации Samsung. Из файла импортируются колонки:
 - Файл по шаблону — загрузка файла соответствующего шаблону системы.

Примечание

Как образец шаблона можно использовать Выгружаемый файл.

4. Выбрать в структуре ОШС, раздел в который следует загрузить новые данные.

Примечание

Разделы ОШС из области синхронизации (LDAP) не доступны,

5. Нажать кнопку «загрузить файл» и выбрать файл для загрузки данных,
6. Задать условия импорта:
 - При импорте уже существующих в системе устройств:
 - Не импортировать данные,
 - Обновлять данные привязанных SIM если устройство зарегистрировано на того же сотрудника,
 - Разрешать перемещать устройства между сотрудниками при импорте.

Внимание!

При перемещении устройства между сотрудниками все назначения (профили, ПУП, Правила управления и Правила несоответствия), сделанные на устройство будут сняты!

- Способ обновления данных привязанных SIM:
 - Заменять существующие данные SIM,
 - Добавлять данные SIM.
7. Нажать кнопку «Ок».

Правила импорта комплектов:

- Файл Samsung KME должен иметь формат kme_devices.csv в кодировке UTF8 с разделителем «запятая».
 - Из файла импортируются только два столбца:
 - IMEI — целое число, длиной не более 16 знаков,
 - Serial Number.
 - Файл не содержит данных о сотрудниках,

- Все прочие столбцы могут отсутствовать или будут игнорироваться.
- При импорте комплекта с не существующим в системе сотрудником, будет создан фиктивный сотрудник со следующими параметрами:
 - Фамилия — значением поля IMEI из файла импорта.
 - Имя — КМЕ,
 - Должность — КМЕ,
 - Место работы — выбранное для загрузки подразделение ОШС.
- Загружаемый по шаблону файл может иметь формат CSV, в кодировке UTF8 с разделителем «запятая» или XLSX.
 - Опциональные поля могут быть пустыми, но должны присутствовать.
 - Количество листов в файле — не более двух. При наличии двух листов импорт производится со второго,
 - Первая строка должна содержать название колонок в следующем составе:
 - IMEI — (целое число, длиной не более 16 знаков) опционально, если задан Serial Number,
 - Serial Number — опционально, если задан IMEI,
 - Фамилия — обязательно,
 - Имя — обязательно,
 - Отчество — не обязательно,
 - Должность — не обязательно,
 - Домен — не обязательно,
 - Имя пользователя — не обязательно,
 - E-mail — не обязательно,
 - Место работы 1 — не обязательно,
 - Место работы 2 — не обязательно,
 - ...
 - Место работы 10 — не обязательно,
 - Номер телефона — не обязательно,
 - IMSI — обязателен, если задан номер телефона или ICCID,
 - ICCID — не обязательно.
- Не допускаются строки с одинаковыми заполненными: IMEI или Serial Number. Дубликаты не импортируются,

- Не допускаются строки с не заполненными: IMEI и Serial Number,
- Не допускаются строки с заполненным «Номер телефона» (или ICCID) и при этом не заполненным полем IMSI, 1
- Правила по которым загружаемое устройство, считается совпадающим с найденным:

	IMEI = X SN = Y	IMEI = X SN = не задан	IMEI = не задан SN = Y
IMEI = X SN = Y	•	•	•
IMEI = X SN = не задан	•	•	
IMEI = не задан SN = Y	•		•

- Если в системе обнаружено совпадающее устройство у которого не совпадает IMEI или серийный номер, то такая строка не будет импортирована,
- Загружаемая SIM считается «совпадающей с найденной в системе» в случае если у них совпадают IMSI,
- Если в системе обнаружена совпадающая SIM, у которой задан и не совпадает ICCID, то такая строка не будет импортирована,
- Место работы сотрудника:
 - не должно располагаться в области синхронизации ОШС,
 - если указано хотя бы одно место работы, то «Место работы 1» должно совпадать с корневым узлом области управления администратора,
 - «Место работы N» должны заполняться последовательно начиная с «Место работы 1». От родительских подразделений к дочерним. Например: «Место работы 1» — root, «Место работы 2» — Департамент разработки, «Место работы 3» — Отдел тестирования.
 - Если место работы не указано, то местом работы будет выбранное для загрузки устройств подразделение,
 - Если место работы указано, но с учётом иерархии не создано, тогда система создаст необходимую иерархию,
 - Если в подразделении уже есть сотрудник с совпадающими ФИО, то будет использована его запись.
 - Если в подразделении нет сотрудника с ФИО из списка, то будет создана запись о сотруднике,

- Если не найдено совпадающее устройство или производится перемещение устройств между сотрудниками, то:
 - Система создаст комплект **корпоративного** устройства для сотрудника,
 - Если заданы соответствующие параметры SIM, то:
 - система создаст **корпоративную** SIM, если в системе нет совпадающей SIM,
 - система изменит принадлежность SIM на **корпоративную**, если в системе есть совпадающая SIM и она некорпоративная
 - система привяжет SIM к комплекту.

Список возможных ошибок при импорте:

Текст ошибки	Описание
Неверный формат файла	Не верное расширение файла, кодировка, структура столбцов.
В файле имеется комплект с тем же IMEI или Серийным номером	В файле присутствует дублирование строк.
Должно быть заполнено хотя бы одно из полей: IMEI или Серийный номер	Пропущено одно из обязательных полей
Неправильный IMEI	Значение поля не соответствует правилам: <ul style="list-style-type: none"> • Значение в поле — целое число, • Длина числа в поле не превышает 16 символов, • Длина числа должна быть не менее 15 цифр.
В системе зарегистрирован комплект с таким IMEI или Серийным номером	При выборе параметра «не импортировать данные» строки не импортированных существующих, уже зарегистрированных устройств помечаются данной ошибкой.
Место работы не может располагаться в области синхронизации	Хотя бы одно из мест работы входит в область синхронизации.

Должны быть заполнены поля: Фамилия, Имя	Присутствуют строки с не заполненными обязательными полями.
Место работы должно заполняться последовательно. Начиная с колонки «Место работы 1» без пустых колонок до подразделения сотрудника	Если в строке заполнено хоть одно из полей Место работы, то должны быть заполнены все столбцы Место работы начиная с «Место работы 1» до последнего заполненного.
Поле «Место работы 1» должно совпадать с корневым узлом области управления администратора либо все поля «Место работы *» должны быть пустыми	Если в строке заполнено хоть одно из полей Место работы, то значение поля «Место работы 1» должно совпадать с корневым узлом области управления администратора.
Не заполнено поле IMSI	В строке заполнено поле «Номер телефона» или «ICCID», при этом не заполнена IMSI.
В системе обнаружена SIM с конфликтующими значениями IMSI={IMSI}, ICCID={ICCID}	В системе обнаружена совпадающая SIM, у которой задан и не совпадает ICCID.
В системе обнаружено устройство с конфликтующими значениями IMEI={IMEI}, Серийный номер={SN}	В системе обнаружено совпадающее устройство, у которого не совпадает IMEI или серийный номер.
Устройство уже зарегистрировано на сотрудника ФИО={ФИО}	При выборе параметра «Обновлять данные привязанных SIM если устройство зарегистрировано на того же сотрудника» устройство зарегистрировано на другого сотрудника (не совпадают ФИО или подразделение).
Количество ошибок превысило допустимое значение — 100	Превышено допустимое количество ошибок. При превышении допустимого количества ошибок загрузка прекращается.
Исчерпано количество устройств в лицензии	Количество зарегистрированных в системе комплектов превысило допустимое количество лицензий.

2.8.11.2 Выгрузка комплектов

Для выгрузки комплектов в файле формата XLSX, следует нажать кнопку «**Выгрузить комплекты**» в соответствии с рисунком 2.145.

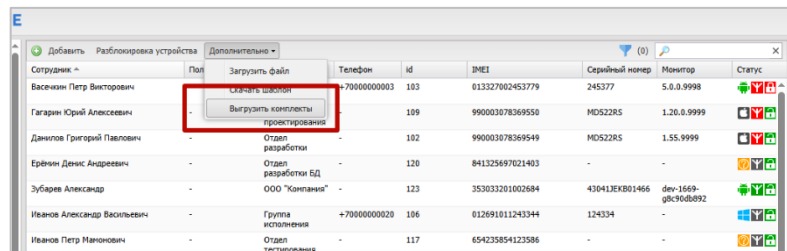


Рисунок 2.145 — Выгрузка комплектов

Примечание

Выгружаемый файл можно использовать в качестве образца для загружаемого файла.

2.8.11.3 Отключение комплекта

Для отключения комплекта от управления системой следует нажать кнопку «**Отключить**», после чего система предоставит выбор параметра отключения в соответствии с рисунком 2.146. Затем требуется подтвердить действие, нажав на кнопку «**Применить**».

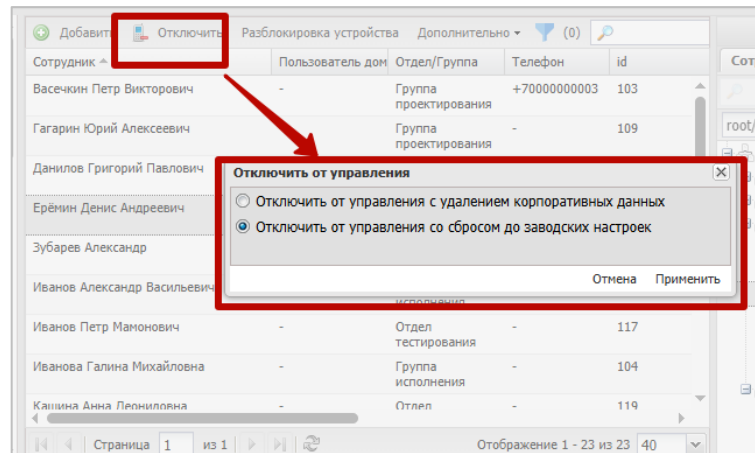


Рисунок 2.146 — Отключение комплекта от управления

После отключения от управления комплект можно будет удалить из системы. Для этого необходимо выбрать в таблице соответствующую ему запись, нажать кнопку «**Удалить**» (рисунок 2.147). Далее система запросит подтверждение действия удаления. После его подтверждения система выдаст уведомление о том, что следует проверить на самом устройстве его отключение от управления. Выбрав «**Всё равно удалить**» выбранная запись удалится из БД.

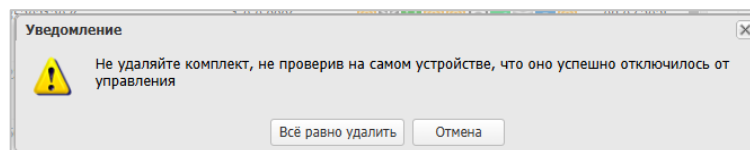


Рисунок 2.147 — Удаление комплекта

Удаление комплекта инициирует команду удаления данных с устройства. Такую операцию следует применять только в случае полного удаления пользователя из «UEM SafeMobile» (при увольнении сотрудника или утере устройства).

Примечание

- *Для корректного повторного использования МСК в системе необходимо удалить его комплект из АРМ Администратора SafeMobile. При этом выполняется очистка МСК путем отправки на МСК команды удаления данных и возврата его к заводским настройкам.*
- *Если очистка МСК была выполнена вручную непосредственно на устройстве (путём возврата МСК к заводским настройкам), то комплект также требуется удалить, используя АРМ, так как не удалённый комплект будет учитываться при лицензировании (при превышении допустимого количества таких комплектов невозможно будет подключить новые).*

2.8.11.4 Привязка SIM к комплектам

Привязка SIM-карт к комплекту задает список SIM-карт, разрешенных к использованию на МСК (Android). При использовании в МСК SIM-карты, не входящей в список «привязанных» устройство блокируется. Допускается привязка до 10 SIM-карт на один комплект, одна SIM-карта может быть привязана к нескольким комплектам.

Для привязки списка SIM-карт к комплекту необходимо выполнить следующие действия:

1. В разделе «Комплекты» найти (или создать) комплект, к которому необходимо совершить привязку одной или более SIM-карт, предварительно зарегистрированных в системе (см. раздел SIM-карты 2.8.8).
2. Выбрать необходимый комплект в списке комплектов, после чего в окне параметров комплекта перейти во вкладку «Привязанные SIM». (рисунок 2.148)

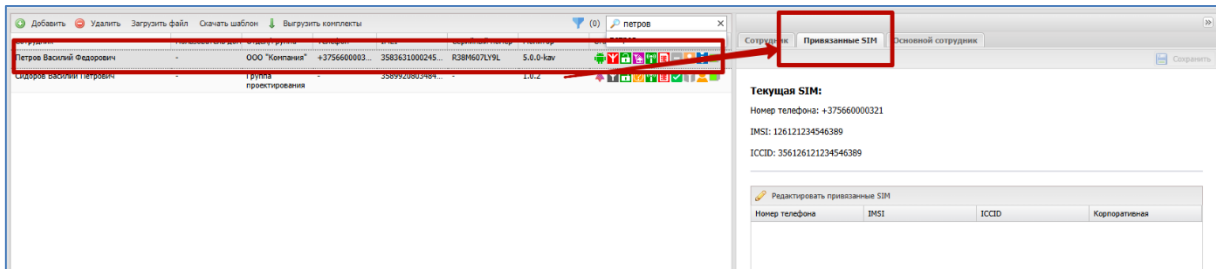


Рисунок 2.148 — Вкладка «Привязанные SIM»

3. В окне редактирования списка привязанных SIM-карт нажать кнопку «редактировать привязанные SIM», после чего откроется окно выбора SIM-карт (рисунок 2.149).

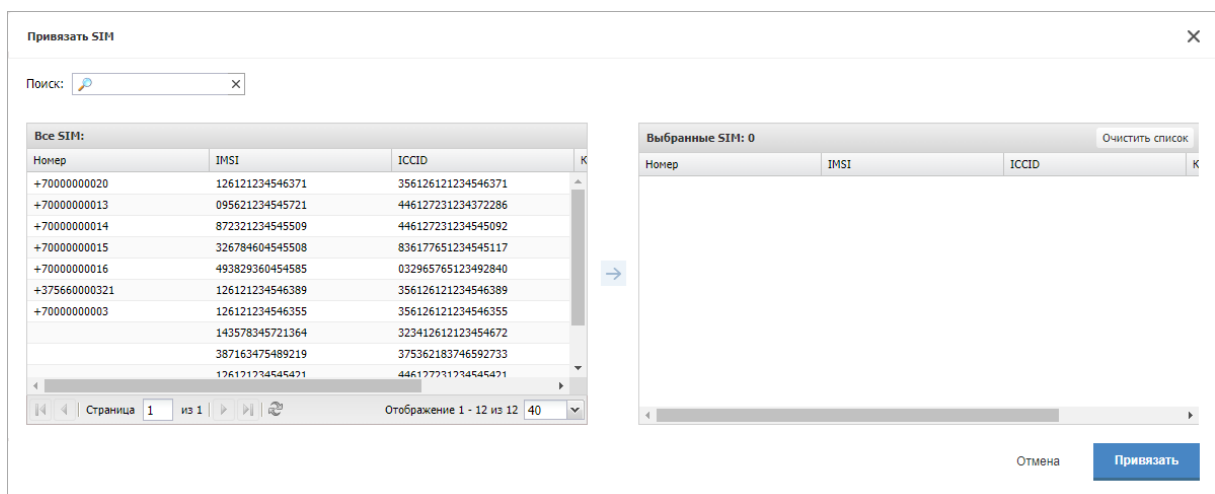


Рисунок 2.149 — Окно выбора SIM-карт для привязки

4. В левой части кона выбора SIM-карт представлен список SIM-карт зарегистрированных в системе. Список может быть отфильтрован по колонкам:
- Id,
 - Номер,
 - IMSI,
 - ICCID,
 - Корпоративная.

Так же для поиска необходимых SIM-карт можно воспользоваться строкой поиска и кнопками пагинации списка.

5. Выделить в списке необходимую SIM-карту и нажать кнопку перемещения в список «Выбранные SIM» (рисунок 2.150).

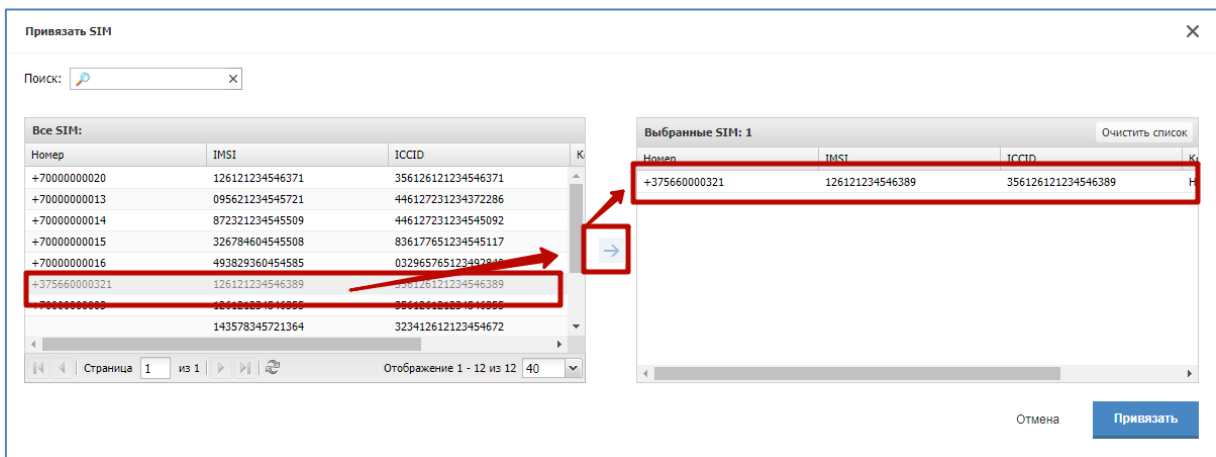


Рисунок 2.150 — Список «Выбранные SIM»

6. После окончания формирования списка нажать кнопку «Принять», после чего окно формирования списка будет закрыто, а в параметрах комплекта будут отражены привязанные SIM-карты.
7. Нажать кнопку «Сохранить», после чего привязка SIM-карт будет закончена.

Привязанные SIM-карты будут работать в соответствии с настройками политик профиля «Настройки монитора Android», указанными в блоке «telephony» (рисунок 2.151).

telephony

Разрешить личные звонки привилегия DO или DA

Разрешить внешние SIM привилегия DO или DA

Разрешить корпоративные или привязанные SIM. Если в системе есть корпоративные SIM и к устройству привязаны SIM, то на устройстве будут разрешены только привязанные SIM привилегия DO или DA

Разрешить работать без SIM привилегия DO или DA

Рисунок 2.151 — Политики профиля «Настройки монитора Android»

2.8.11.5 Перерегистрация устройства на другого сотрудника

Для устройств Android существует возможность замены сотрудника, за которым закреплен комплект. Если для комплекта переназначался сотрудник, то во вкладке «основной сотрудник» будет отображаться текущий «основной сотрудник» и его расположение в дереве ОШС (рисунок 2.152). В противном случае значение «Основной сотрудник» будет «не задано».

Историю смены сотрудников на устройстве можно просмотреть в разделе «Данные устройства», во вкладке «История смены сотрудника» выбранного в списке устройства.

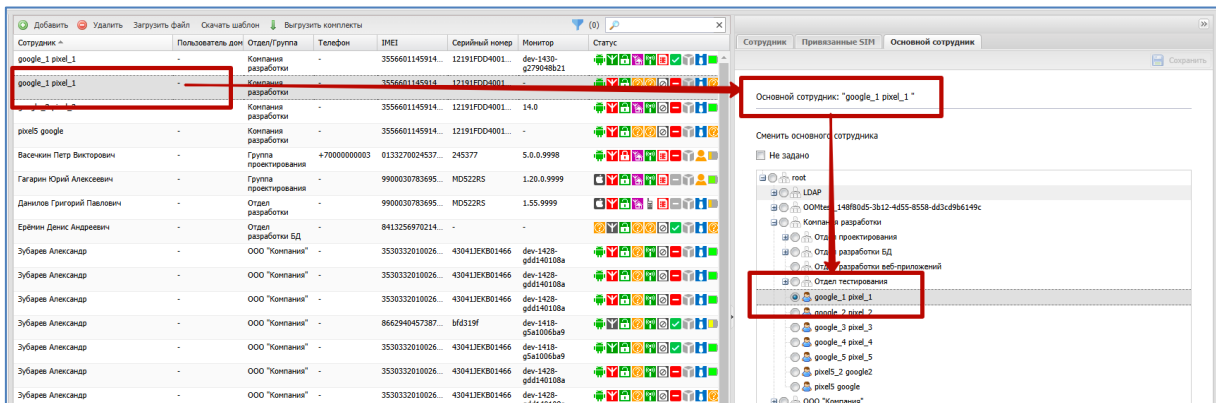


Рисунок 2.152 — Сотрудник переназначенный на комплект

При смене сотрудника комплекта могут быть задействованы политики профиля «Политики смены сотрудника на устройстве Android», который может быть назначен на комплект. В данном профиле настраиваются такие параметры как:

- Разрешить возврат устройства основному сотруднику — Да/Нет/Не задано;

- Разрешить смену сотрудника без отключения от управления — Да/Нет/Не задано;
- Сбрасывать пароль при смене сотрудника — Да/Нет/Не задано.

Чтобы перерегистрировать комплект на другого сотрудника необходимо выполнить следующие действия:

1. Выбрать комплект в списке комплектов, раздела «Комплекты».
2. В правой части рабочего экрана, во вкладке «Основной сотрудник» выключить чекбокс «Не задано», после чего дерево ОШС будет доступно для выбора сотрудника
3. Выбрать в дереве ОШС сотрудника, на которого будет переназначен комплект.
4. Нажать кнопку «Сохранить».

Примечание

Если сертификаты *mtls* выписываются на корпоративном удостоверяющем центре, то основной сотрудник должен принадлежать домену (иметь техническую учетную запись в домене, а в дереве ОШС он должен располагаться в каталоге LDAP).

Чтобы вернуть комплект сотруднику, на которого он был зарегистрирован первоначально необходимо во вкладке «Основной сотрудник» включить чекбокс «Не задано» и нажать кнопку «Сохранить» (рисунок 2.153).

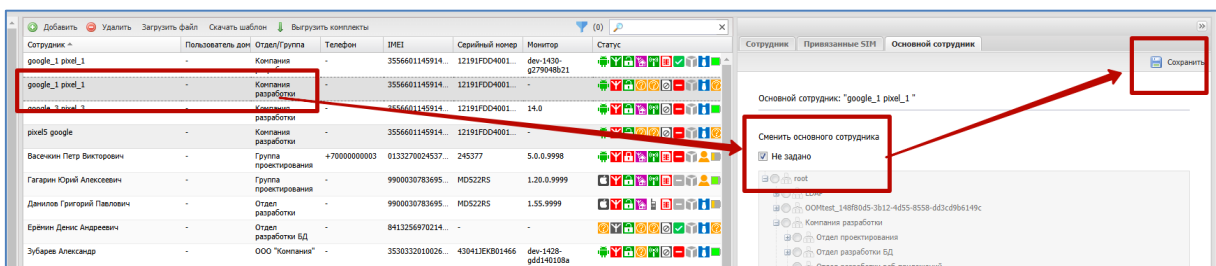


Рисунок 2.153 — Возврат комплекта первоначальному сотруднику

Примечание

Если в системе настроена синхронизация с LDAP и для выдачи mTLS сертификатов используется корпоративный УЦ, то основной сотрудник так же должен иметь доменную учетную запись с возможностью выпустить сертификат mTLS.

2.8.12 Комплекты Linux

В данном разделе задаются комплекты для устройств на платформе Linux.

Страница раздела состоит из следующих блоков и элементов управления:

- Подразделение — строка отображения названия подразделения, выбранного в структуре ОШС,
- Окно выбора подразделения — представлено в виде структуры ОШС,
- Список комплектов выбранного подразделения или пользователя — отображает список комплектов для выбранного подразделения или пользователя. Информации по каждому комплекту распределена по следующим колонкам таблицы (включенным по умолчанию):
 - Отдел/группа — наименование отдела/группы в структуре ОШС к которой принадлежит пользователь,
 - Сотрудник — ФИО пользователя,
 - Пользователь домена — отображает ФИО сотрудника (или e-mail, если ФИО не было импортировано),
 - Подключение SSH — параметры подключения по SSH,
 - Статус — статус устройства.
- Кнопка «Фильтр списка» — позволяет фильтровать список комплектов в соответствии с значениями колонок.
- Параметры комплекта — отображает параметры заданного комплекта. Для каждого комплекта могут отображаться следующие параметры:
 - Строка подключения по SSH к устройству в формате URI — помимо формата `ssh://user@hostname:22` допускается использовать IP адрес (например — `ssh://root@10.17.7.221:22`)
 - Сменить ключ — чекбокс. Если включен, то становятся доступны для редактирования поля смены ключа RSA:
 - Приватный RSA ключ SSH — поле ввода строки данных ключа,
 - Пароль RSA ключа — поле ввода пароля.
 - Кнопка «Сохранить» — сохранение изменений в настройках комплектов или сохранение данных о новом комплекте (доступна при внесении изменений или при создании нового комплекта).
- Кнопка «Добавить» — создать новый комплект,
- Кнопка «Отключить» — удаляет комплект из системы (кнопка появляется только при наведении на комплект, в блоке списка комплектов).

2.8.12.1 **Добавить новый комплект Linux**

Чтобы добавить новый комплект Linux, необходимо выполнить следующие действия:

1. Перейти в раздел «Объекты учета — Комплекты Linux»,
2. В структуре ОШС найти пользователя, для которого создается комплект,
3. Нажать кнопку «Добавить»,
4. В блоке параметров комплекта заполнить поля:
 - Строка подключения по SSH к устройству в формате URI. Например: `ssh://user@hostname:22` (обязательно для заполнения),
 - Приватный RSA ключ SSH подключения (обязательно для заполнения),
 - Пароль RSA ключа (опционально),
5. Нажать кнопку «Сохранить».

2.8.12.2 **Удаление комплекта Linux**

Чтобы удалить комплект Linux, необходимо выполнить следующие действия:

1. Перейти в раздел «Объекты учета — Комплекты Linux»,
2. В структуре ОШС найти пользователя, чей комплект необходимо удалить,
3. Выделить комплект в списке комплектов,
4. Нажать кнопку «Отключить».

2.8.13 Геозоны

Пункт меню «Геозоны» предназначен для создания и управления именованными областями на географической карте, которые используются для применения на МСК заданных ограничений и настроек ОС. В разделе отображается фрагмент карты и таблица с реестром геозон в соответствии с рисунком 2.154.

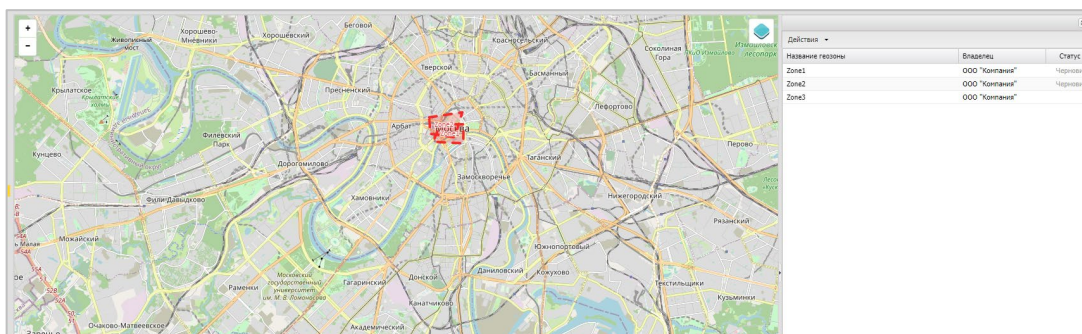



Рисунок 2.154 — Окно «Геозоны»

В правой части окна расположена таблица, в которой отображаются все созданные геозоны и их статус. В верхней части таблицы находится кнопка «Действия» при нажатии на которую выпадает меню с вариантами:

- Добавить — предназначена для создания новой геозоны;
- Удалить — предназначена для удаления уже созданной геозоны;
- Изменить — предназначена для внесения изменений в геозону только в статусе «Черновик»;
- Активировать — предназначена для активирования геозоны в системе и возможности использования ее при назначении профиля. Кнопка доступна только для геозон в статусе «Черновик»;
- Сменить владельца — предназначена для смены владельца геозоны.

В левой части окна расположен фрагмент карты, на которой отображаются созданные геозоны в форме многоугольника. Контур геозоны со статусом «Черновик» воспроизводится в виде пунктирной линии, а контур активированной геозоны — в виде сплошной линии.

Для изменения масштаба карты (увеличения или уменьшения изображения) используется шкала масштабирования, расположенная в верхнем левом углу карты. Кроме того, масштаб изображения можно изменять, используя вращение колеса мыши, если курсор расположен в области карты.

При нажатии на значок  в правой верхней части карты раскрывается меню настройки источника картографической информации (сервер ГИС), который используется для отображения карты: openstreetmap.org (рисунок 2.155).

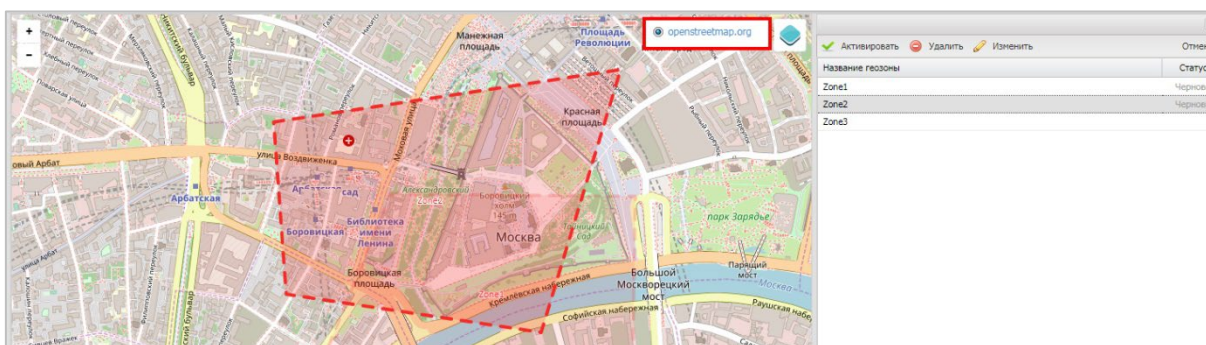


Рисунок 2.155 — Настройка режима отображения информации о геозонах на карте

Для создания геозоны следует нажать на кнопку «Действия», выбрать **«Добавить»** и, посредством мыши, нарисовать на выбранном участке карты необходимую область, повторный щелчок мыши завершит рисование. Для сохранения рисунка геозоны нажать на кнопку **«Сохранить черновик»**, затем в всплывающем окне в соответствии с рисунком 2.156 ввести имя новой геозоны, которое должно отличаться от уже созданных, и нажать **«ОК»**. Созданная геозона отобразится в реестре со статусом «Черновик».

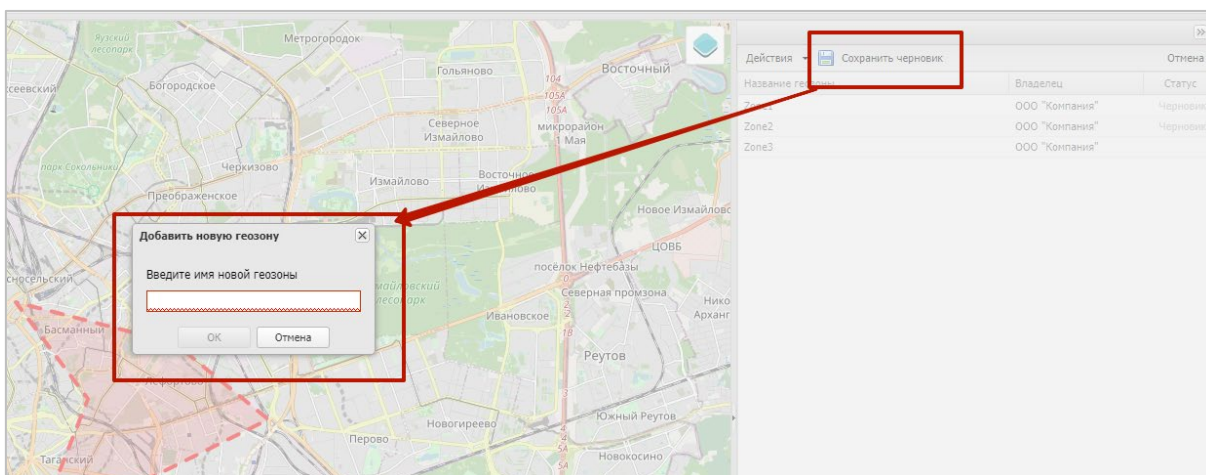


Рисунок 2.156 — Добавление геозоны

Для редактирования следует в реестре выбрать требуемую строку с названием геозоны и статусом «Черновик» и нажать кнопку «Действия», выбрать **«Изменить»**. Затем внести изменения в рисунок на карте, нажать кнопку **«Сохранить черновик»** и подтвердить название, нажав на кнопку **«ОК»**.

Для активирования геозоны необходимо в реестре выбрать требуемую строку с названием геозоны и статусом «Черновик» и нажать кнопку «Действия», выбрать **«Активировать»**. Активированная геозона в реестре отобразится без статуса и будет доступна в условиях применения профиля. После активирования геозоны ее редактирование будет **невозможно**.

Примечание

По отношению к активным геозонам доступны только два вида действий:

- Удаление,
- Смена владельца.

Для смены владельца геозоны необходимо в реестре выбрать требуемую строку с названием геозоны, нажать кнопку «действия», выбрать «Смена владельца», после чего откроется окно структуры ОШС. Выбрать владельца геозоны в структуре ОШС, нажать кнопку «Ок».

Для удаления геозоны требуется в реестре выбрать строку с ее названием и нажать кнопку «Действия», выбрать **«Удалить»**. После подтверждения действия геозона будет удалена из реестра. Если геозона активирована и является условием применения профиля, то при выборе **«Удалить»** воспроизведется предупреждение о невозможности ее удаления. Удаление возможно только для несвязанных геозон.

Для отмены действий следует нажать кнопку **«Нет»**.

2.8.14 Серверные сертификаты

Пункт меню «Серверные сертификаты» предназначен для учёта и распространения серверных сертификатов на МСК. Мобильные клиенты системы используют серверные сертификаты для аутентификации серверов системы. В разделе отображается таблица с перечнем сертификатов в соответствии с рисунком 2.157.

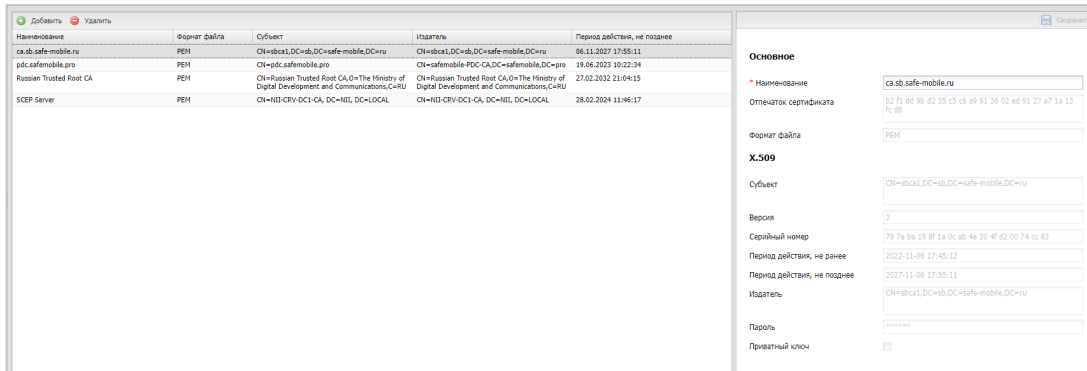


Рисунок 2.157 — Окно «Серверные сертификаты»

В таблице с перечнем сертификатов отображаются следующие столбцы:

- Наименование — наименование сертификата (по умолчанию отображается в таблице);
- Отпечаток сертификата — хэш сертификата, вычисляемый по всем данным сертификата и его подпись;
- Формат файла — формат файла сертификата (по умолчанию отображается в таблице);
- Субъект — информация о владельце сертификата (по умолчанию отображается в таблице);
- Версия — версия сертификата;
- Серийный номер — серийный номер сертификата;
- Издатель — информация об издателе сертификата (по умолчанию отображается в таблице);
- Период действия; не ранее — дата начала действия сертификата (приведено к локальному времени браузера);
- Период действия; не позднее — дата окончания действия сертификата (по умолчанию отображается в таблице; приведено к локальному времени браузера);
- Приватный ключ — (Да/Нет);
- Владелец — подразделение, владеющее сертификатом.

Для *добавления* нового серверного сертификата следует нажать кнопку **«Добавить»** в панели инструментов верхней части окна (рисунок 2.158).

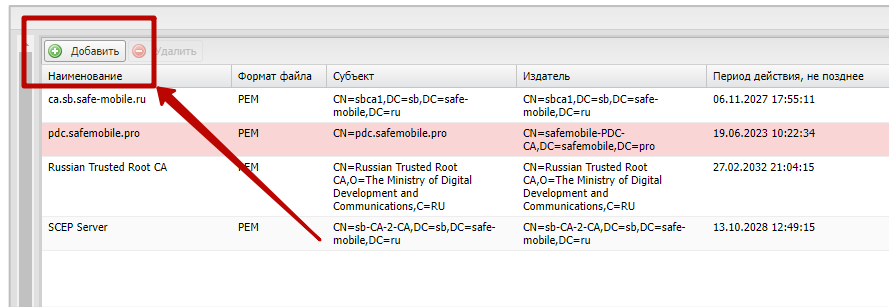


Рисунок 2.158 — Кнопка «Добавить» новый серверный сертификат

Затем в форме правой части окна ввести пароль (при необходимости) и загрузить файл, полученные от администратора системы. После загрузки файла отобразится форма с параметрами загруженного сертификата в соответствии с рисунком 2.159.

Основное

* Сертификат

* Наименование

Отпечаток сертификата

Формат файла

X.509

Субъект

Версия

Серийный номер

Период действия, не ранее

Период действия, не позднее

Издатель

Пароль

Приватный ключ

Рисунок 2.159 — Форма «Серверный сертификат»

Поле, обозначенное * — обязательное для заполнения. После заполнения формы нажать кнопку **«Сохранить»** и серверный сертификат отобразится в таблице с сертификатами.

Для *удаления* серверного сертификата необходимо выбрать в таблице (рисунок 2.160) соответствующую ему запись и нажать кнопку **«Удалить»**. После подтвержде-
 ние выполняемого действия, выбранная запись удалится из перечня с сертификатами
 при отсутствии связанных профилей.

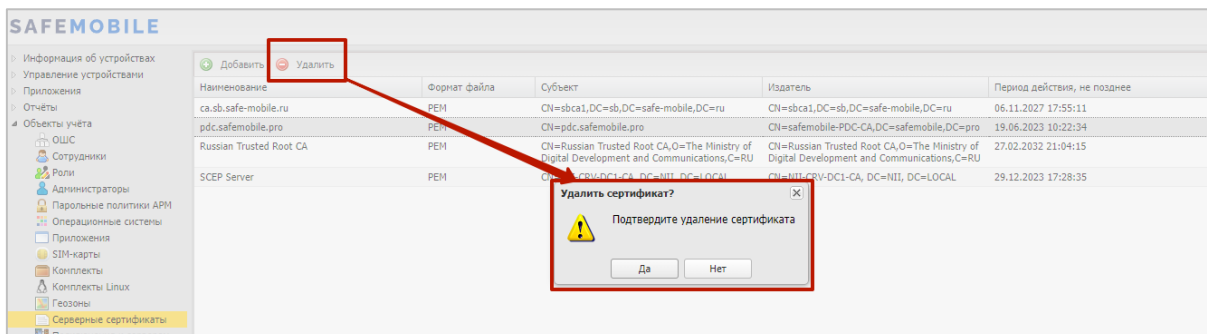


Рисунок 2.160 — Удаление серверного сертификата

2.8.15 Подключения к серверам

Пункт меню «Подключения к серверам» предназначен для настройки подключения МСК к серверам системы. Подключение МСК к серверам системы осуществляется по протоколу TLS. Серверный сертификат, указанный в настройках подключения будет использоваться МСК для аутентификации сервера. Если сервер использует сертификат TLS, выпущенный публичным центром сертификации, то указывать сертификат в настройках подключения не требуется.

Перед подключением первого МСК к системе должны быть выполнены следующие настройки:

- Настройка подключения к серверу команд **Command Server**. Сервер отвечает за отправку команд на МСК Android (для устройств с «монитором» версии 10.0 и выше):
 - Если управление МСК на платформе Android не планируется, настраивать подключение не требуется;
- **Enrollment Server** предназначен для регистрации мобильных устройств (Android, iOS и Aurora). Если Enrollment Server сервер расположен на том же физическом сервере, что и MDMServer, то его url адрес должен совпадать с адресом MDM сервера. В случае размещения портала регистрации на отдельном сервере необходимо обеспечить наличие сертификатов iosmdm.crt и iosmdm.key, идентичных используемым на сервере MDM, поскольку они применяются для подписи enrollment-профиля iOS.
- Настройка подключения к **MDMServer** — обязательна. MDMServer выполняет следующие функции:
 - Авторизации пользователя при регистрации МСК;
 - Отправка политик, приложений и конфигураций приложений (за исключением МСК на платформе Windows);
 - Отправка команд (за исключением МСК Android).

Примечание

Изменение URL MDMServer, при подключенных iOS устройствах, приведет к потере управления устройствами iOS.

- Настройка подключения к серверу команд **SocketServer**. Аналогичен Command Server, устаревший, для версии «Монитора» 9.x и ниже:
 - Если управление МСК на платформе Android не планируется, настраивать подключение не требуется;

- Настройка подключений к **WinMDM Enrollment** и **WinMDM Management** необходима при использовании MCK Windows:
 - Если управление MCK на платформе Windows не планируется, настраивать данное подключение не требуется;
 - Для упрощения регистрации MCK (пользователь введет свой e-mail вместо URL сервера) необходимо: в DNS зоне предприятия зарегистрировать имя сервера WinMDM Enrollment вида `enterpriseenrollment.<company.ru>`. Имя `enterpriseenrollment` зарезервировано и используется встроенным клиентом Windows при поиске сервиса регистрации устройства;
 - Если сертификаты серверов WinMDM Enrollment и WinMDM Management выпущены непубличным центром сертификации, то сертификат выпустившего их центра сертификации должен быть предварительно размещен на MCK, в хранилище: Компьютер -> Доверенные центры сертификации;
 - URL, которые необходимо указать для серверов WinMDM Enrollment и WinMDM Management зависят от следующих факторов:
 - выбрана ли при инсталляции системы установка WinMDM за внешний прокси сервер;
 - MDMServer и сервера WinMDM Enrollment и WinMDM Management размещены на одной машине или нет,
 - возможно ли добавить доменное имя третьего уровня в корпоративный DNS;

Значения URL в зависимости от этих факторов приведены в таблице **2.6**.

- Настройка подключения к **SCEPServer** обязательна. Подключение к серверу SCEP необходимо для получения устройствами на платформах iOS, Android и Аврора сертификатов mTLS. Сертификаты mTLS используются для авторизации устройств при подключении к серверу управления и серверу команд. Помимо mTLS настройка необходима при использовании доменной авторизации по клиентским сертификатам в приложениях;

- **TURN Server** обеспечивает подключение для удалённого управления мобильным устройством по протоколу TURN.

Примечание

Для УУ необходимо развернуть TURN сервер, для этого используйте документ:

Инструкция по установке и настройке TURN_STUN серверов

из состава документации SafeMobile.

- Настройка подключения **File Distribution Server**. Сервер предназначен для раздачи файлов и приложений. Если не используется внешний кэширующий сервер, то URL должен совпадать с URL **MDMServer**.

Правила назначения доменных имен для серверов

- Доменные имена в русской локализации **не поддерживаются**.
- Для SocketServer:
 - URL должен соответствовать RFC 3986, **без префиксов**: https://, http:// и т.п.
 - URL **не содержит** подстроку «127.0.0.1».
- Для TURN Server:
 - URL должен соответствовать RFC 3986, опционально могут присутствовать префиксы: turn:, turns:, stun:, stuns:.
 - Префикс **не содержит** «//».
- Для прочих серверов:
 - URL должен соответствовать RFC 3986, с **обязательным** префиксом: https://.
 - URL **не содержит** подстроку «127.0.0.1».

Если URL домена задан не верно, то система выдаст ошибку всплывающем сообщении, сохранение внесенных изменений в URL будет не доступно .

В разделе отображается таблица с перечнем серверов и подключенных к ним серверных сертификатов в соответствии с рисунком 2.161.

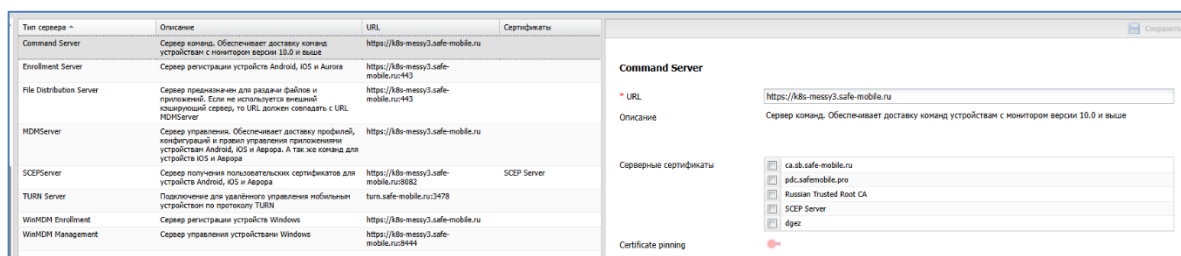


Рисунок 2.161 — Окно «Подключение к серверам»

Таблица подключения к серверам, по умолчанию, содержит столбцы:

- Тип сервера — наименование сервера системы (по умолчанию, отображается в таблице);
- Описание — описание назначения сервера;
- URL — электронный адрес (по умолчанию, отображается в таблице);
- Сертификат — наименование серверного сертификата (по умолчанию, отображается в таблице);
- Certificate pinning — закрепление сертификата. Доступно только для:
 - Command server (сервер для Android);
 - MDMServer (для Андроид, iOS и Аврора);
 - SCEP Server (для Андроид, iOS и Аврора);
 - Socket server (сервер для Android).

Примечание

Certificate pinning — подход, при котором доверенными УЦ (и их сертификатами соответственно) считаются не встроенные УЦ, а явно переданный список УЦ с цепочкой сертификатов. В таком случае доверенным сертификатом будет считаться тот и только тот сертификат, который содержится в переданном списке сертификатов.

ВАЖНО!

Подключение данной функции может привести к потере контроля над всеми устройствами.

Таблица 2.6 — Подключение к серверам

Внешний прокси	Правила на внешней прокси	Размещение	Встроенный nginx	Сервер	Регистрация в DNS	Настройка подключения
-	-	MDM и WinMDM на одной машине	example.com [x.x.x.1]	MDMServer	mdm.example.com -> x.x.x.1	mdm.example.com:443
				WinMDM Enrollment	enterpriseenrollment.example.com -> x.x.x.1	enterpriseenrollment.example.com:443
				WinMDM Management		enterpriseenrollment.example.com:8444
-	-	MDM и WinMDM на разных машинах	example.com [x.x.x.1]	MDMServer	mdm.example.com -> x.x.x.1	mdm.example.com:443
				WinMDM Enrollment	enterpriseenrollment.example.com -> x.x.x.2	enterpriseenrollment.example.com:443
			WinMDM Management	enterpriseenrollment.example.com:8444		
-	-	MDM и WinMDM на одной машине	example.com [x.x.x.1]	MDMServer	-	example.com:443
				WinMDM Enrollment		example.com:443
				WinMDM Management		example.com:8444
-	-	MDM и WinMDM на разных машинах	example.com [x.x.x.1]	MDMServer	-	example.com:443
				WinMDM Enrollment		example1.com:443
			WinMDM Management	example1.com:8444		
example.com [x.x.x.1]	mdm.example.com:443 -> y.y.y.1:443	MDM и WinMDM на одной машине	y.y.y.1:443	MDMServer	mdm.example.com -> y.y.y.1	mdm.example.com:443
	enterpriseenrollment.example.com:443 -> y.y.y.1:443		y.y.y.1:443	WinMDM Enrollment		enterpriseenrollment.example.com:443

Внешний прокси	Правила на внешней прокси	Размещение	Встроенный nginx	Сервер	Регистрация в DNS	Настройка подключения
	winmdm.example.com:p3 -> у.у.у.1:8444		у.у.у.1:8444	WinMDM Management	enterpriseenrollment.example.com ->у.у.у.1	enterpriseenrollment.example.com:8444
example.com [x.x.x.1]	mdm.example.com:443 -> у.у.у.1:443	MDM и WinMDM на разных машинах	у.у.у.1:443	MDMServer	mdm.example.com -> x.x.x.1	mdm.example.com:443
	enterpriseenrollment.example.com:443 -> у.у.у.1:443		у.у.у.2:443	WinMDM Enrollment	enterpriseenrollment.example.com -> x.x.x.2	enterpriseenrollment.example.com:443
	enterpriseenrollment.example.com:8444 -> у.у.у.1:8444		у.у.у.2:8444	WinMDM Management		enterpriseenrollment.example.com:8444
example.com [x.x.x.1]	example.com:443 -> у.у.у.1:443	MDM и WinMDM на одной машине	у.у.у.1:443	MDMServer	-	example.com:443
	example.com:443 -> у.у.у.1:443		у.у.у.1:443	WinMDM Enrollment		example.com:443
	example.com:p3 -> у.у.у.1:8444		у.у.у.1:8444	WinMDM Management		example.com:p3
example.com [x.x.x.1]	mdm.example.com:443 -> у.у.у.1:443	MDM и WinMDM на разных машинах	у.у.у.1:443	MDMServer	-	mdm.example.com:443
	enterpriseenrollment.example.com:443 -> у.у.у.2:443		у.у.у.2:443	WinMDM Enrollment	-	enterpriseenrollment.example.com:443
	enterpriseenrollment.example.com:8444 -> у.у.у.2:8444		у.у.у.2:8444	WinMDM Management	-	enterpriseenrollment.example.com:8444

Для настройки подключения МСК к серверу необходимо выполнить следующие действия:

1. В списке серверов выбрать сервер.
2. В форме правой части окна: ввести URL и установить флажок у тех серверных сертификатов, по которым МСК сможет аутентифицировать данный сервер (рисунок 2.162). В любой момент времени сервер использует только один сертификат.

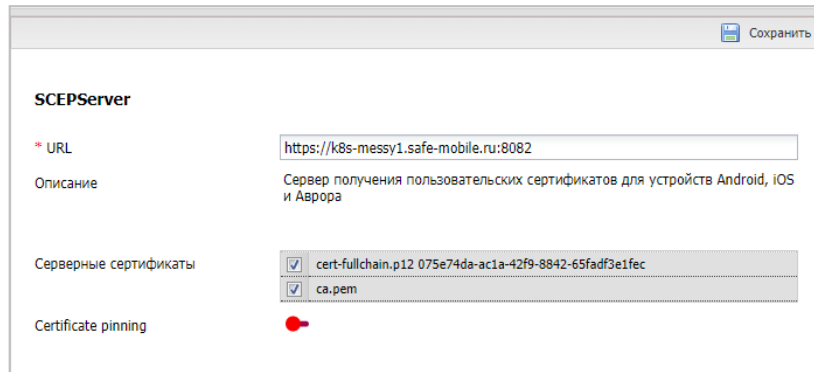


Рисунок 2.162 — Форма «Подключения к серверу»

3. Включить Certificate pinning для отмеченных серверных сертификатов (опционально).
 - При включении опции появится диалоговое окно предупреждения. Нажмите «ДА» (рисунок 2.163).

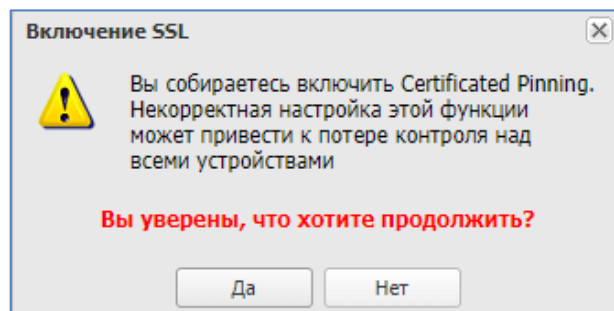


Рисунок 2.163 — Предупреждение о возможных последствиях

4. После заполнения формы нажать кнопку **«Сохранить»** и подключение отобразится в реестре.

Если Certificate pinning уже включен, и требуется добавить другие сертификаты, то следует отметить необходимые сертификаты и нажать «Сохранить».

До того момента как истечет время действия текущего сертификата, необходимо выписать новый серверный сертификат и распространить его на МСК. Для этого нужно новый сертификат добавить в список серверных сертификатов раздел 2.8.12, после чего включить его в список сертификатов, аутентифицирующих данный сервер.

2.8.16 Удостоверяющие центры

Раздел «Удостоверяющие центры» предназначен для управления удостоверяющими центрами (УЦ) в системе. Доступ к разделу осуществляется через меню «Объекты учета — «Удостоверяющие центры» (рисунок 2.164).

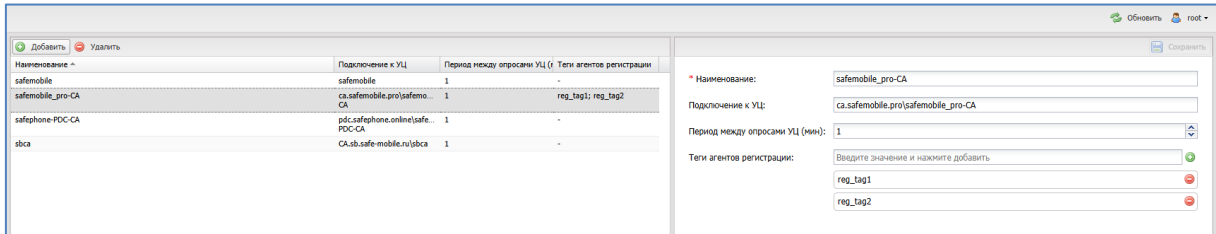


Рисунок 2.164 — Раздел «Удостоверяющие центры»

Основные операции:

- Просмотр списка УЦ,
- Добавление новых УЦ,
- Редактирование параметров УЦ,
- Удаление УЦ.

Раздел доступен при наличии полномочия:

- Просмотр:
 - Просмотр удостоверяющих центров.
- Создание и изменение УЦ:
 - Просмотр удостоверяющих центров
 - Изменение удостоверяющих центров (доступно только администраторам корня ОШС),
- Удаление УЦ:
 - Просмотр удостоверяющих центров,
 - Удаление удостоверяющих центров (доступно только администраторам корня ОШС).

Основной рабочий экран содержит список управляющих центров, в котором каждая строка содержит параметры одного УЦ.

Параметры удостоверяющего центра

Параметр	Обязательно для заполнения	Ограничения
Наименование	Да	1 ≤ длина ≤ 511 символов Должно быть уникальным
Подключение к УЦ	Нет	1 ≤ длина ≤ 2000 символов <имя домена><имя удостоверяющего центра>
Период между опросами УЦ (мин)	Нет	1 ≤ значение ≤ 2147483647 Значение по умолчанию: 60
Теги агентов регистрации	Нет	Ограничение для каждого тега: 1 ≤ длина ≤ 63 символов Каждый тег должен быть уникален (с учетом регистра) во всех УЦ. Наличие дублирующих тегов в одном УЦ недопустимо. Разделитель между тегами — «;».

Кнопки управления:

- Добавить — создание нового УЦ;
- Удалить — удаление выбранного УЦ;
- Сохранить — сохранение изменений.

Для **добавления нового УЦ** следует нажать кнопку «Добавить», заполнить параметры УЦ с учетом ограничений, нажать кнопку «Сохранить».

Для **удаления УЦ** следует выбрать его в списке, нажать кнопку «Удалить» и подтвердить действие. При удалении УЦ следует учитывать:

- Удаление УЦ используемого в настройках SCEP не возможно;
- Удаление УЦ, выпустившего действующие сертификаты, приведет к невозможности их отзыва в дальнейшем при снятии устройства с управления.

Примечание

В списке удостоверяющих центров присутствует УЦ устанавливаемый по умолчанию.

Параметры встроенного УЦ:

- *Идентификатор: -1,*
- *Наименование: Safemobile,*
- *Подключение к УЦ: safemobile,*
- *Период между опросами УЦ: 1 мин,*
- *Теги агентов регистрации: отсутствуют.*

Особенности работы:

- *Все параметры данной настройки являются неизменяемыми.*
- *Удаление встроенного УЦ невозможно.*
- *Данный УЦ может быть выбран только во встроенной настройке SCEP mTLS и недоступен для выбора в любых других настройках SCEP.*

2.8.17 Настройки SCEP

Раздел «**Настройки SCEP**» предназначен для учёта и распространения клиентских сертификатов с настраиваемыми параметрами посредством SCEP в соответствии с рисунком 2.165.

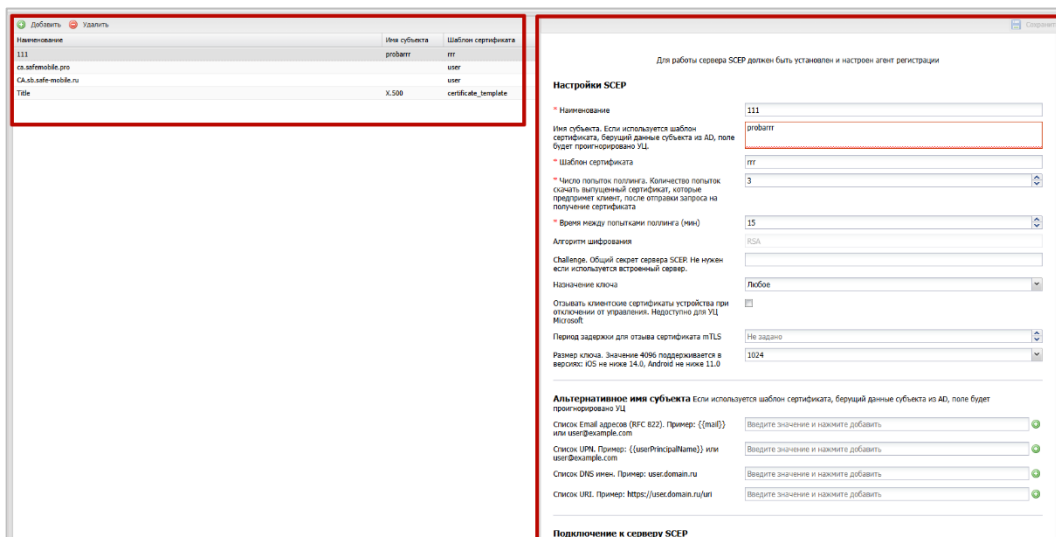


Рисунок 2.165 — Окно «Настройки SCEP»

В таблице с перечнем сертификатов отображаются следующие столбцы:

- Наименование — наименование сертификата (по умолчанию, отображается в таблице),
- Имя субъекта — формат сертификата (по умолчанию, отображается в таблице),
- Шаблон сертификата — шаблон используемого сертификата (по умолчанию, отображается в таблице).

В правой части рабочего экрана отображаются настройки, выбранной в таблице настройки SCEP и состоят из следующих полей данных:

- Настройки SCEP:
 - Наименование — наименование настройки;
 - Имя субъекта. Если используется шаблон сертификата, берущий данные субъекта из LDAP, поле будет проигнорировано УЦ — Отличительное имя (DN), содержащее идентифицирующую информацию об объекте, которому выдан сертификат. Имя субъекта

может быть создано из стандартных компонентов каталога LDAP, таких как общие имена и организационные подразделения. Эти компоненты определены в X.500. Поле не заполняется, если данные пользователя берутся из LDAP (см. примечание).

Пример:

```
/CN=user/OU=department/OU=root/DC=example/DC=com/E=user@example.com.
```

В имени субъекта могут быть использованы следующие подстановки:

1. `{{distinguishedname}}` — специальная подстановка (начинается с «/»), которую нужно использовать чтобы подставить полное имя пользователя.
2. `{{mail}}` — подстановка адреса электронной почты.

Пример использования подстановок:

```
/{{distinguishedname}}/E={{mail}}
```

- Шаблон сертификата — шаблон сертификата, по которому будут выпускаться сертификаты для устройств (должен быть заранее создан во внешнем каталоге (LDAP));
 - Число попыток поллинга. Количество попыток скачать выпущенный сертификат, которые предпримет клиент, после отправки запроса на получение сертификата. В зависимости от настроек, УЦ может выписывать сертификат не сразу, а после подтверждения администратором УЦ;
 - Время между попытками поллинга (мин) — интервал времени между обращениями монитора за готовым сертификатом,
 - Алгоритм шифрования — RSA (всегда);
 - Challenge. Общий секрет сервера SCEP. Не нужен если используется встроенный сервер;
 - Назначение ключа — доступны значения:
 - Шифрование, Подпись, Любое,
 - Отзывать клиентские сертификаты устройства при отключении от управления. Недоступно для УЦ Microsoft — (чекбокс);
 - Период задержки для отзыва сертификата mTLS;
 - Размер ключа. Значение 4096 поддерживается в версиях: iOS не ниже 14.0, Android не ниже 11.0,
- Альтернативное имя субъекта:
 - Список Email адресов (RFC 822). Пример: `{{mail}}` или `user@example.com`— один и более email адресов (не заполняется, если данные

- пользователя берутся из LDAP (см. примечание);
- Список UPN. Пример: {{userPrincipalName}} или user@example.com— один и более UserPrincipalName (не заполняется, если данные пользователя берутся из LDAP (см. примечание));
- Список DNS имен. Пример: user.domain.ru— один и более DNS (не заполняется, если данные пользователя берутся из LDAP (см. примечание));
- Список URI. Пример: https://user.domain.ru/uri — один и более Uniform Resource Identifier (не заполняется, если данные пользователя берутся из LDAP (см. примечание));
- Подключение к серверу SCEP:
 - Подключения к серверам — выбор из списка серверов SCEP;
- Корпоративный удостоверяющий центр:
 - Корпоративный удостоверяющий центр — выбор УЦ заданного в разделе «Удостоверяющие центры»;
 - Тег агента регистрации — тег выбирается из списка тегов выбранного корпоративного УЦ.
 - Если тег задан в конфиге Регистрационного агента (РА), то РА использует тег для получения задач на запрос и отзыв сертификатов.
 - Если тег не задан в конфиге РА, то РА использует URL УЦ из конфига для получения задач на запрос и отзыв сертификатов.

Примечание

- *В свойствах «шаблона сертификата» в УЦ должен быть указан источник данных пользователя: LDAP или запрос сертификата. Если в шаблоне указано, что брать данные следует из LDAP, то все, что введено в полях SN и SAN игнорируется и берется из LDAP. Если же указано брать из запроса сертификата, то нужно, чтобы в запросе было заполнено хотя бы одно из полей: SN или SAN иначе УЦ вернет ошибку создания сертификата.*
- *В поле «Имя субъекта» и полях блока «Альтернативное имя субъекта»*

допускается использование всех подстановок, указанных в «Руководстве администратора» 2.6.8.2 Настройка параметров профиля.

2.8.17.1 Добавление новой настройки SCEP

Чтобы добавить новые настройки SCEP, необходимо выполнить следующие действия.

1. Перейти в раздел «Настройки SCEP».
2. Нажать кнопку **«Добавить»** в панели инструментов верхней части окна. Затем заполнить форму в правой части окна (рисунок 2.166).

Для работы сервера SCEP должен быть установлен и настроен агент регистрации

Настройки SCEP

* **Наименование**
 Имя субъекта. Если используется шаблон сертификата, берущий данные субъекта из AD, поле будет проигнорировано УЦ.
 Пример: {{{distinguishedname}}}E= {{{mail}}} или /CN=user/OU=department/OU=root/DC=example/DC=com/E=user@example.com

* **Шаблон сертификата**
 Число попыток поллинга. Количество попыток оказавшихся неуспешными сертификаты, которые запрашивает клиент, после отправки запроса на получение сертификата

* **Время между попытками поллинга (мин)**

Алгоритм шифрования
 RSA

Challenge. Общий секрет сервера SCEP. Не нужен если используется встроенный сервер.

Назначение ключа
 Любое

Отзывать клиентские сертификаты устройства при отключении от управления. Недоступно для УЦ Microsoft

Период задержки для отзавы сертификата mTLS
 Не задано

Размер ключа. Значение 4096 поддерживается в версиях: iOS не ниже 14.0, Android не ниже 11.0

Альтернативное имя субъекта Если используется шаблон сертификата, берущий данные субъекта из AD, поле будет проигнорировано УЦ

Список Email адресов (RFC 822). Пример: {{{mail}}} или user@example.com

Список UPN. Пример: {{{userPrincipalName}}} или user@example.com

Список DNS имен. Пример: user.domain.ru

Список URI. Пример: https://user.domain.ru/uri

Подключение к серверу SCEP

* Подключения к серверам
 Выберите соединение с сервером...

Корпоративный удостоверяющий центр

Рисунок 2.166 — Форма с настройками SCEP

После заполнения формы нажать кнопку **«Сохранить»** и новые настройки SCEP отобразится в таблице.

2.8.17.2 Удаление настроек SCEP

Для удаления настроек SCEP необходимо выбрать в таблице (рисунок 2.167) соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждение выполняемого действия, выбранная запись удалится из перечня настроек SCEP (при отсутствии связанных профилей).

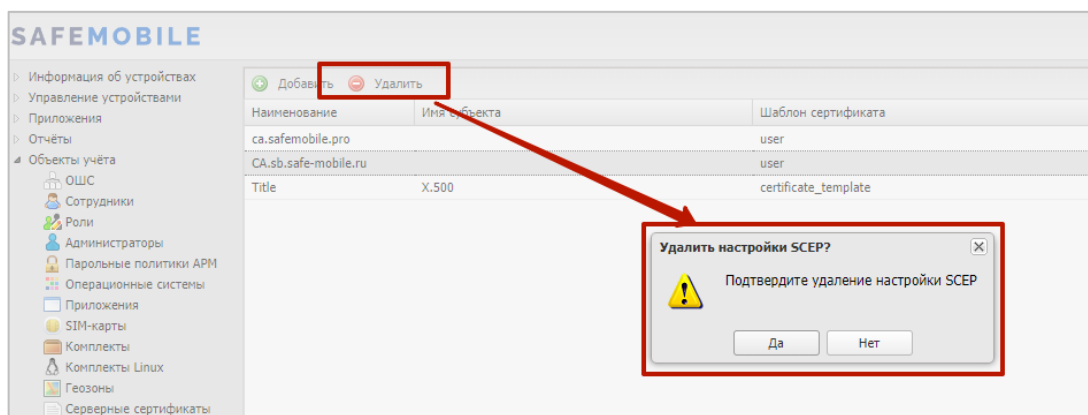


Рисунок 2.167 — Кнопка удаления настроек SCEP

2.8.18 Клиентские сертификаты

Пункт меню «Клиентские сертификаты» предназначен для учёта и распространения клиентских сертификатов, которые используются для:

- аутентификации устройства при подключении к системе с использованием протокола mTLS. Сертификаты mTLS выписываются встроенным в систему УЦ. По умолчанию имеют срок действия — 182 дня. Срок может изменен в файле конфигурации УЦ. Сертификаты обновляются автоматически, когда до истечения срока действия остается менее 50% времени. Если устройство не сможет обновить сертификат до истечения срока действия, то управление им будет потеряно, т.к. сервер не сможет аутентифицировать устройство;
- аутентификации сотрудника, при подключении к корпоративной сети WiFi;
- аутентификации сотрудника в VPN;
- аутентификации сотрудника на сервере Exchange.

В верхней части окна раздела в соответствии с рисунком 2.168 отображается таблица с перечнем сертификатов, а нижней части окна располагается главная таблица с комплектами МСК сотрудников, для которых эти сертификаты предназначены. Описание главной таблицы с комплектами приведено в разделе 2.4.

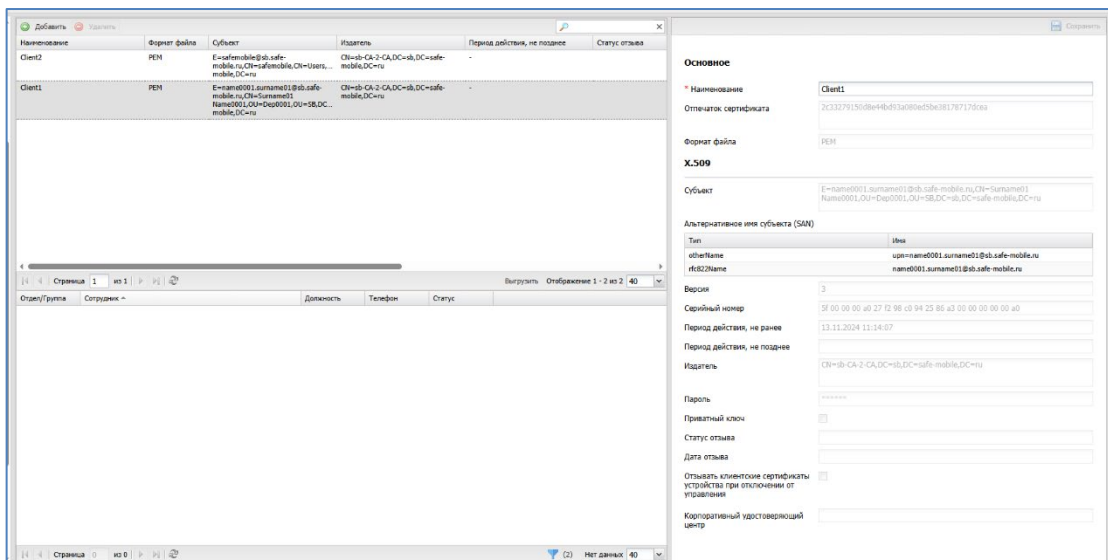


Рисунок 2.168 — Окно «Клиентские сертификаты»

В таблице с перечнем сертификатов отображаются следующие столбцы:

- Наименование — наименование сертификата (по умолчанию, отображается в таблице). У сертификатов, сгенерированных автоматически, в наименование добавляется назначение сертификата и идентификатор устройства;
- Отпечаток сертификата — информация о файле сертификата в формате base64;
- Формат файла — формат файла сертификата: X.509 для сертификата без закрытого ключа, PKCS12 для сертификата с закрытым ключом (по умолчанию, отображается в таблице);
- Субъект — информация о владельце сертификата (по умолчанию, отображается в таблице);
- Версия — версия сертификата;
- Серийный номер — серийный номер сертификата;
- Издатель — информация об издателе сертификата (по умолчанию, отображается в таблице);
- Период действия, не ранее — дата начала действия сертификата;
- Период действия, не позднее — дата окончания действия сертификата (по умолчанию, отображается в таблице);
- Приватный ключ — (Да/Нет);
- Владелец — администратор узла ОШС, назначенный владельцем сущности;
- Статус отзыва — может иметь следующие значения:
 - Запрошен отзыв,
 - Отозван,
 - Ошибка отзыва.
- Дата отзыва — дата отзыва сертификата;
- Отозвать при отключении — (Да/Нет);
- Период задержки — параметр задержки отзыва сертификата mTLS, указанный в настройках SCEP на момент сохранения сертификата.

Для **добавления** нового клиентского сертификата следует нажать кнопку **«Добавить»** в панели инструментов верхней части окна. Затем в форме в правой части окна ввести пароль от файла сертификата и загрузить файл сертификата в формате PKCS12, полученные от администратора удостоверяющего центра LDAP.

Примечание

Формат PKCS12 предназначен передачи и/или хранения закрытого ключа и цепочки доверия сертификата.

После загрузки файла отобразится форма с параметрами загруженного сертификата в соответствии с рисунком 2.169.

The screenshot shows a web form for configuring a client certificate. The form is titled "Основное" and includes the following fields and sections:

- Основное**
 - Наименование: Client2
 - Отпечаток сертификата: a04821351d5c7c8297993c5c9cfd3f9c5f8a55
 - Формат файла: PEM
- x.509**
 - Субъект: E=safemobile@sb.safemobile.ru,CN=safemobile,CN=Users,DC=sb,DC=safemobile,DC=ru
 - Альтернативное имя субъекта (SAN)

Тип	Имя
otherName	upn=safemobile@sb.safemobile.ru
rfc822Name	safemobile@sb.safemobile.ru
 - Версия: 3
 - Серийный номер: 5f 00 00 00 a0 27 f2 98 c0 94 25 86 a3 00 00 00 00 a0
 - Период действия, не ранее: 13.11.2024 11:05:04
 - Период действия, не позднее: (empty)
 - Издатель: CN=sb-CA-2-CA,DC=sb,DC=safemobile,DC=ru
 - Пароль: (masked)
 - Приватный ключ:
 - Статус отзыва: (empty)
 - Дата отзыва: (empty)
 - Отзывать клиентские сертификаты устройства при отключении от управления:
 - Корпоративный удостоверяющий центр: (empty)

Рисунок 2.169 — Форма «Клиентский сертификат»

Поле, обозначенное * — обязательное для заполнения. После заполнения формы нажать кнопку **«Сохранить»**.

Клиентский сертификат отобразится в таблице с сертификатами, а в главной таблице отобразятся комплекты МСК, которым данный сертификат назначен.

Для **удаления** клиентского сертификата необходимо выбрать в таблице соответствующую ему запись и нажать кнопку **«Удалить»**. После подтверждения выполняемого действия, выбранная запись удалится из перечня с сертификатами при отсутствии связанных профилей.

Примечание

Удаление доступно только для сертификатов, загруженных администратором вручную. Сертификаты, выписанные автоматически, через SCEP сервер — удалить нельзя.

2.8.19 Группы

В разделе отображается список групп сотрудников (рисунок 2.170). Назначение групп — использование в качестве фильтров во вкладке «Условия» при применении профилей, конфигураций приложений, правил управления приложениями, правил несоответствия.

Типы групп:

- Импортированные группы — формируются автоматически в результате синхронизации с внешним каталогом (LDAP).
- Локальные группы — создаются и управляются администратором вручную.

Права доступа:

Доступ администраторов к разделу определяется следующими привилегиями:

- Просмотр — базовое право, без него остальные привилегии недоступны.
- Создание — только для локальных групп.
- Изменение — только для локальных групп.
- Удаление — только для локальных групп.

Список групп:

В центральной рабочей области экрана отображается список групп, где каждая строка содержит запись об одной группе и содержит следующую информацию, упорядоченную по столбцам (отображаются по умолчанию):

- DN/Наименование:
 - для импортированной группы — **distinguishedName**,
 - для локальной — наименование группы.
- Тип — тип группы (импортированная или локальная).
- Владелец:
 - для импортированных групп владельцем становится корневой импортированный узел;
 - для локальных групп владелец из ОШС.
- ObjectGUID — идентификатор группы во внешнем каталоге (LDAP).
- Последняя синхронизация — дата и время последней успешной синхронизации в формате DD.MM.YY hh:mm:ss.

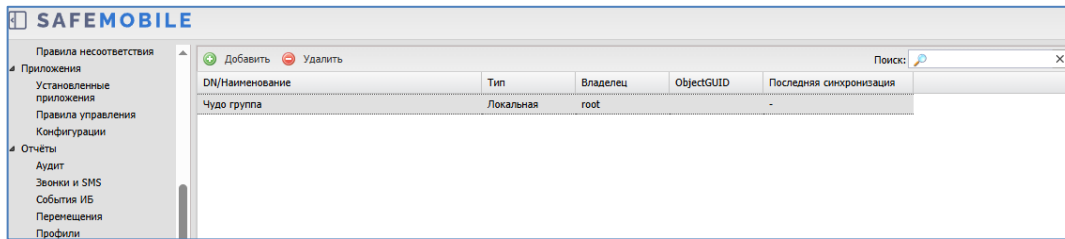


Рисунок 2.170 — Список групп

Поиск:

Поисковая выдача ограничивает список групп теми группами, у которых подстрока поиска содержится в DN/Наименовании или ObjectGUID.

Создание и удаление групп:

Для создания новой локальной группы необходимо выполнить следующие действия:

1. Нажать кнопку «Добавить», расположенную в центральной части рабочего экрана.
2. В правой части рабочего экрана заполнить поле «DN/Наименование группы».
3. Нажать кнопку «Сохранить», после чего новая локальная группа появится в общем списке и станет доступна для редактирования (изменение состава и владельца).

Для удаления локальной группы необходимо найти нужную группу в общем списке, нажать кнопку «Удалить» и подтвердить действие.

Примечание

Если группа используется в условиях применения, то при удалении группы система выдаст сообщение об ошибке.

Редактирование группы:

В правой части рабочей области отображается блок с настройками и информацией о выделенной в списке группе. Блок содержит следующие вкладки:

- Общие — сводные данные по группе:
 - DN/Наименование группы — уникальное для владельца группы.
 - Тип — импортированная или локальная (не доступно для изменения).
 - ObjectGUID — идентификатор во внешнем каталоге (LDAP) (только для импортированных).
 - Последняя синхронизация — дата/время (только для импортированных, формат DD.MM.YY чч:мм:сс).
- Члены группы — список сотрудников, входящих в группу. Каждая строка списка содержит информацию об одном сотруднике и упорядочена по следующим столбцам (отображаются по умолчанию):
 - ФИО — фамилия, имя и отчество;
 - Должность — должность сотрудника;
 - DN пользователя — **distinguishedName** пользователя во внешнем каталоге (LDAP);
 - ObjectGUID — идентификатор пользователя во внешнем каталоге (LDAP);

Действия, доступные во вкладке «Члены группы»:

- Кнопка «Добавить» — добавляет сотрудников в локальную группу. При нажатии открывается окно выбора сотрудников (рисунок 2.171). Окно содержит дерево ОШС и строку поиска по ФИО/должности.

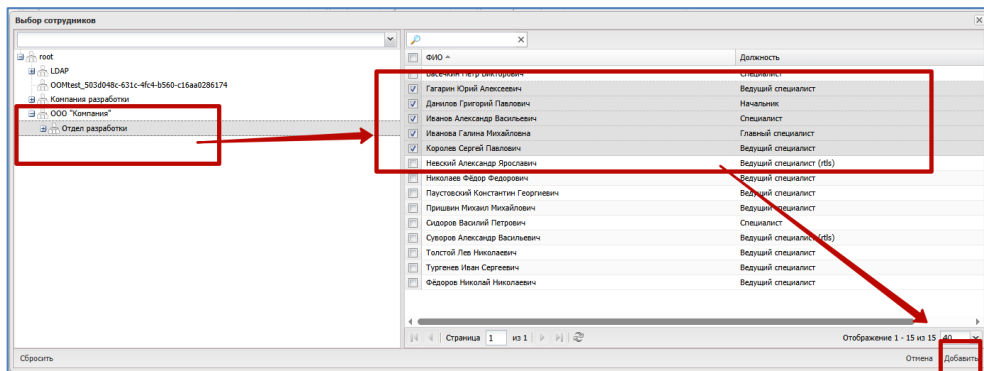


Рисунок 2.171 — Окно выбора сотрудников из ОШС

- Кнопка «Удалить» — удаляет сотрудников из локальной группы (рисунок 2.172).

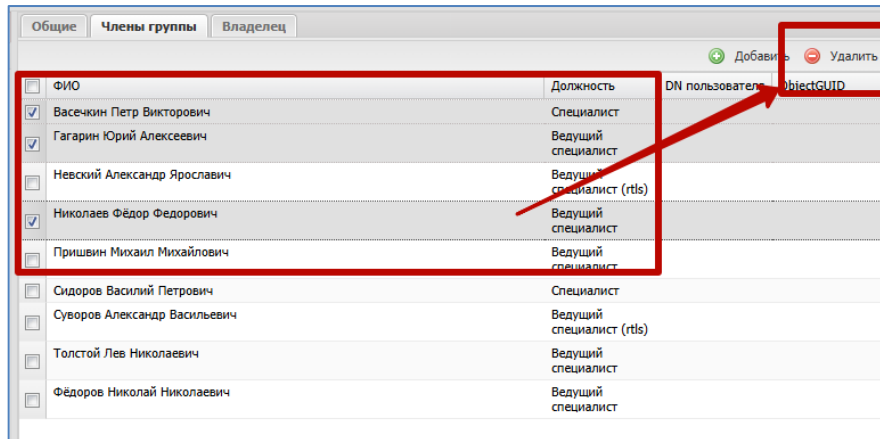


Рисунок 2.172 — Удаление сотрудника

Примечание

- *Перед сохранением система проверяет, что группа не содержит сотрудников, чьи владельцы не входят в область управления владельца группы. В противном случае система выдаст сообщение об ошибке.*
- *При изменении группы пересчитываются все назначения использующих ее сущностей.*

- Владелец — вкладка отображает владельца группы в ОШС и позволяет его сменить (для локальной группы). Для импортированных групп владельцем становится корневой импортированный узел.

2.8.20 Шаблоны писем

Раздел содержит список шаблонов писем для автоматической рассылки e-mail сообщений системой. Шаблоны писем применяются при создании правил несоответствия (рисунок 2.173).

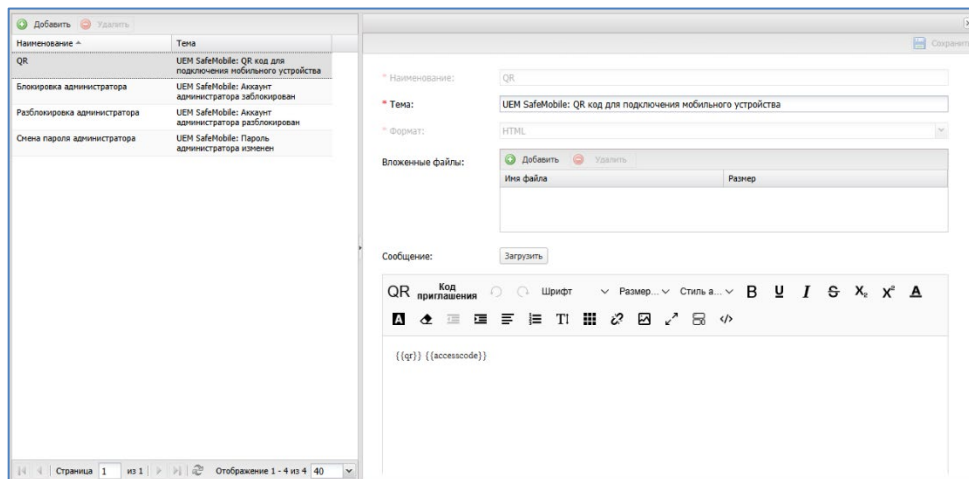


Рисунок 2.173 — Список шаблонов писем

В центральной части страницы раздела представлен список заданных шаблонов. Каждая строка списка содержит информацию об одном шаблоне и состоит из следующих полей данных:

- Наименование — наименование шаблона;
- Тема — тема сообщения, которая будет отображаться в сообщении.

По умолчанию в разделе присутствуют (не подлежащие удалению) следующие шаблоны:

- QR — тема сообщения «UEM SafeMobile: QR код для подключения мобильного устройства». Шаблон настроен на отправку адресатам сообщения содержащее QR-код подключения и код приглашения.
- Блокировка администратора — тема сообщения «UEM SafeMobile: Аккаунт администратора заблокирован».
- Разблокировка администратора — тема сообщения «UEM SafeMobile: Аккаунт администратора разблокирован».
- Смена пароля администратора — тема сообщения «UEM SafeMobile: Пароль администратора изменен».

В верхней части таблицы находятся кнопки:

- Добавить — добавить новый шаблон;
- Удалить — удалить выделенный в списке шаблон.

В правой части рабочего экрана отображаются настройки шаблона, выбранного в списке. Блок состоит из следующих полей данных и функциональных элементов:

- Наименование — наименование шаблона;
- Тема — тема сообщения;
- Формат — значение «HTML» или «простой текст»;
- Вложенные файлы — список файлов, добавленных в шаблон;
- Сообщение — окно просмотра и редактирования сообщения:
 - Если «Формат» задан как «простой текст», то поле сообщения позволяет задать сообщение обычным текстом (текст в кодировке UTF8);
 - Если «Формат» задан как «HTML», то поле сообщения включает в себя инструменты создания сообщений с использованием языка HTML, а также кнопки добавления в текст подстановок отправки QR-кода и кода приглашения для подключения устройств;
- Кнопка «Загрузить» — загрузка файла для создания сообщения. Формат файла определять по расширению:
 - Для формата «простой текст» — расширение «.txt» (текст в кодировке UTF8);
 - Для формата «HTML» — расширение «.html»;
 - При несоответствии расширения или невозможности распарсить формат будет выдана ошибка «Неверный формат файла».

2.8.20.1 Добавление нового шаблона письма

Чтобы добавить новый шаблон письма, необходимо выполнить следующие действия:

1. Перейти в раздел «Шаблоны писем».
2. Нажать кнопку «Добавить».
3. В блоке настроек шаблона заполнить следующие поля:
 - Наименование — после сохранения шаблона изменить нельзя;
 - Тема — будет отображаться как тема электронного письма;
 - Формат — после сохранения шаблона изменить нельзя;
 - Вложенные файлы (опционально, после сохранения шаблона изменить нельзя);
4. Задать тест сообщения в окне «Сообщение» или нажать кнопку «Загрузить», после чего откроется окно браузера ОС для выбора файла с шаблоном сообщения.
5. Нажать кнопку «Сохранить», после чего в списке шаблоном письма появится новый шаблон.

Примечание

- Допускается использование подстановок в поле ввода «Тема» и в сообщении (см. список подстановок в [2.6.8.2 Настройка параметров профиля](#)),

2.8.20.2 Редактирование и удаление шаблона письма

Чтобы **внести изменения** в существующий шаблон, необходимо выполнить следующие действия:

1. Найти в списке шаблон, подлежащий редактированию.
2. В блоке настроек внести изменения в параметры шаблона или заменить текст сообщения, через загрузку файла.
3. Нажать кнопку «Сохранить».

Чтобы **удалить** существующий шаблон, необходимо выполнить следующие действия:

1. Найти в списке шаблон, подлежащий редактированию,
2. Нажать кнопку «Удалить»,

В модальном окне подтверждения действия нажать кнопку «Да», после чего шаблон письма будет удален.

Примечание

- *Если шаблон уже используется в правилах несоответствия, то перед его удалением необходимо убрать использование этого шаблона в правилах несоответствия.*
- *При удалении шаблона, все не доставленные сообщения этого шаблона будут удалены.*
- *Шаблоны установленные в системе по умолчанию не могут быть удалены.*

2.8.21 Именованные условия применения

Для применения к устройству различных сущностей (конфигурации, правила управления, профили, правила несоответствия) устройство должно соответствовать заданным условиям. Администратор может создать именованное условие применения и далее использовать его в различных назначаемых сущностях. Если администратор изменит именованное условие применения, то все сущности, использующие это условие, будут применены заново с учетом сделанных изменений.

В разделе «Условия применения» администратор может создавать, редактировать и удалять именованные условия применения (рисунок 2.174). Каждая строка списка именованных условий применения отображает следующие данные:

- Наименование — название условия. **Обязательно для заполнения;**
- Платформа — платформа, для которой может быть применено условие. **Обязательно для заполнения. После сохранения изменить параметр будет нельзя;**
- Владелец — владелец условия применения в дереве ОШС. Задается при создании условия применения.

Для поиска по списку пользователю следует воспользоваться строкой ввода поискового запроса.

В правой части раздела отображаются параметры выбранного в списке условия применения. В верхней части таблицы раздела находится панель инструментов со следующими кнопками:

- Добавить — предназначена для создания нового условия применения,
- Удалить — предназначена для удаления уже созданного условия применения.

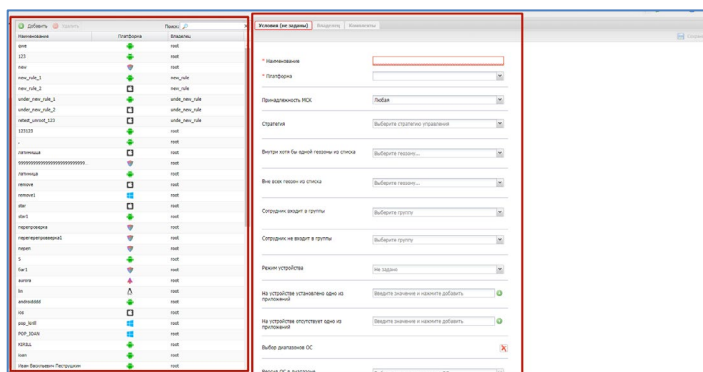


Рисунок 2.174 — Раздел «Условия применения»

2.8.21.1 Добавление нового условия применения

При добавлении нового условия применения необходимо задать его название в поле ввода «Наименование» и указать «Платформу». Описание работы с прочими параметрами условия описаны в [2.6.8.3 Задание условий применения профиля](#).

2.8.21.2 Удаление условия применения

Чтобы удалить условие применения необходимо выбрать его в списке условий и нажать кнопку «Удалить». Если условие не было применено ни к одной сущности, то условие будет удалено. Если условие было применено к сущностям (ПУП, конфигурация приложения, профиль, правило несоответствия), то система отобразит ошибку «Условия применения используются в назначаемых сущностях».

2.8.22 Метки устройств

Функционал маркировки устройств метками располагается в разделе «Объекты учета — Метки устройств». Пользователь имеет возможность маркировать одно или несколько устройств метками. К маркированным метками устройствам могут применяться условия применения назначаемых сущностей. На одно устройство может быть назначено произвольное количество меток.

Посмотреть список устройств и назначенные на них метки пользователь может в разделе «Информация об устройствах — Данные об устройстве», используя фильтр.

В центральной части раздела находится список меток. В правой части раздела отображаются свойства метки, выбранной в списке (рисунок 2.175).

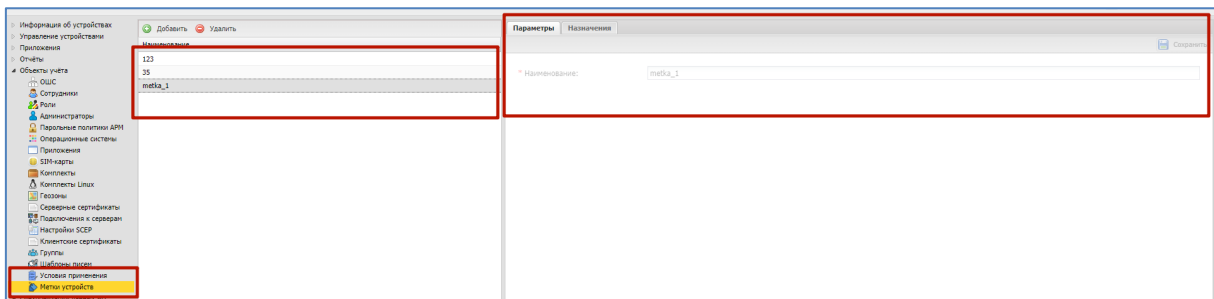


Рисунок 2.175 — Раздел «Метки устройств»

Свойства метки состоят из:

- Параметры:
 - Наименование — имя метки, задается пользователем при создании. Не может быть изменено;
- Назначения — Список устройств в ОШС, на которые можно назначить или снять назначение метки. Чтобы видеть список меток назначенных на устройства необходимо включить отображение колонки «Метки», в таблице (рисунок 2.176).

Отдел/Группа	Сотрудник	Пользователь доп	Должность	Телефон	Статус	Метки	Ручной	Автоматический (правилами несоответств)
ООО "Компания"	Зубарев Александр	-	-	-	Активен	tag_1, tag_2, tag_3	<input type="checkbox"/>	<input type="checkbox"/>
Отдел разработки БД	Ервин Денис Андреевич	-	Разработчик БД	-	Активен	tag_1, tag_2, tag_3	<input type="checkbox"/>	<input type="checkbox"/>
Отдел тестирования	Суббота Кирилл Викторович	-	Руководитель направления тестирования	-	Активен	tag_1, tag_2, tag_3	<input type="checkbox"/>	<input type="checkbox"/>
Компания разработки	google_1 rixel_1	-	postion1	-	Активен	tag_1, tag_2, tag_3	<input type="checkbox"/>	<input type="checkbox"/>
ООО "Компания"	Зубарев Александр	-	-	-	Активен	tag_1, tag_2, tag_3	<input type="checkbox"/>	<input type="checkbox"/>
Группа проектирования	Сидоров Василий Петрович	-	Специалист	-	Активен	tag_1, tag_2, tag_3	<input type="checkbox"/>	<input type="checkbox"/>
Группа проектирования	Федоров Николай Николаевич	-	Ведущий специалист	-	Активен	tag_1, tag_2, tag_3	<input type="checkbox"/>	<input type="checkbox"/>

Рисунок 2.176 — Отображение колонки «Метки»

Назначения меток администратором выполненных «в ручном режиме» отображаются в колонке «Ручной» и могут быть отредактированы. Назначения выполненные автоматически (с помощью правил не соответствия) отображаются в колонке «Автоматически (правилами несоответствия)» не могут быть изменены в ручную.

2.8.22.1 Создание и удаление метки

Чтобы создать метку необходимо выполнить следующие действия:

1. Перейти в раздел «Объекты учета — Метки устройств».
2. Нажать кнопку «Добавить».
3. В области параметров метки задать название метки.
4. Нажать кнопку сохранить. После чего в списке меток отобразится новая метка.

Примечание

При вводе названия метки следует учитывать:

- *Длина ограничена 20 символами,*
- *Допустимо использовать только латинские буквы, цифры, дефис, подчеркик, точку,*
- *Наименование должно быть уникальным (регистр не учитывается).*

Чтобы удалить метки необходимо выполнить следующие действия:

1. Перейти в раздел «Объекты учета — Метки устройств».
2. Выбрать метку в списке.
3. Нажать кнопку «Удалить». После чего метка будет снята со всех устройств, но останется в назначениях сущностей.
4. Перейти в раздел сущности, в которой использовалась удаленная метка (далее пример «Профили»). Профиль, в условиях которого использовалась удаленная метка, будет выделен красным (рисунок 2.177). В политике, в которой использовалась удаленная метка, будет указана дата и время удаления метки.

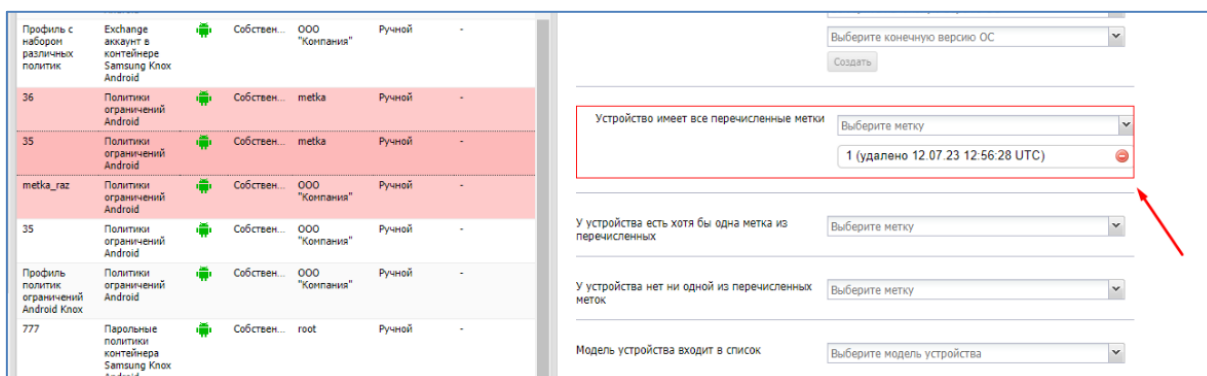


Рисунок 2.177 — Профиль с удаленной меткой в «условиях применения»

5. Выбрать профиль, перейти во вкладку «Условия».
6. Удалить метку из условий применения профиля.
7. Нажать кнопку «Сохранить», после чего профиль не будет выделяться красным в списке.

Примечание

Администратор может удалить метки только в своей области управления.

Удаление метки невозможно, если она используется в правилах автомаркировки.

2.8.23 Сервисные учетные записи

Сервисные учетные записи предназначены для управления доступом к SMAPI. Для каждой сервисной учетной записи создается токен, который в дальнейшем должен быть добавлен в заголовки http-запросов к SMAPI в виде параметра «X-Domain-Api-Token». Используя токены из раздела «Сервисные учетные записи» для авторизации при подключении к SMAPI, сервис подключившийся по токenu должен получать доступ:

- Только к области управления, заданной в учетной записи;
- Только URL, заданным в учетной записи.

Доступ к разделу «Объекты учета — Сервисные учетные записи» имеют администраторы назначенные на корень дерева ОШС и определяется полномочиями:

- Просмотр,
- Изменение и удаление. Только при наличии привилегии «Просмотр»;
- Просмотр токена. Только при наличии привилегии «Просмотр».

Раздел содержит список учетных записей в левой части рабочей области. Каждая строка списке содержит данные о названии учетной записи и области управления. В правой части рабочей области и отображает параметры выделенной в списке учетной записи. (рисунок 2.178)

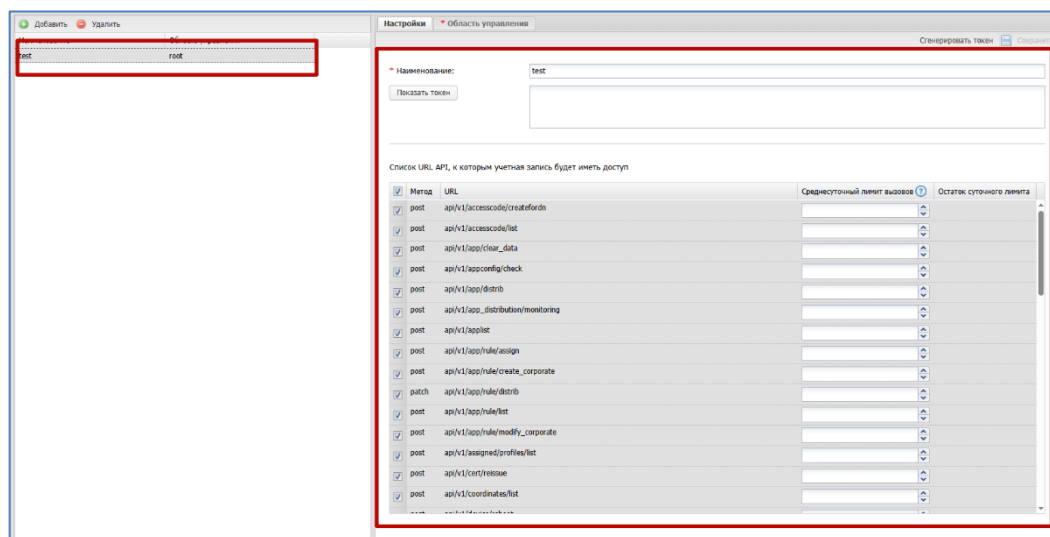


Рисунок 2.178 — Список сервисных учетных записей

Каждая сервисная учетная запись имеет следующие параметры и настройки.

- Наименование,
- Поле отображения токена — отображает токен учетной записи, после нажатия кнопки «Показать токен»;
- Кнопка «Сгенерировать токен» — При нажатии генерирует токен: 64 разряда в 16-ричном представлении. При замене токена, клиенты использовавшие прежний токен потеряют доступ к API;
- Список URL API к которым учетная запись будет иметь доступ:
 - Метод,
 - URL,
 - Среднесуточный лимит вызовов — максимальное количество обращений к методу SMAP, разрешенное в течение одних суток. Данный лимит устанавливается администратором системы. Метод, для которого этот параметр не задан может выполняться без ограничений;
 - Остаток суточного лимита — количество вызовов метода SMAP, которые еще можно совершить до истечения текущих суток;
 - чекбокс выделения с списке URL

Примечание

Описание принципов управления лимитами смотреть в разделе [2.8.5 «Ограничения администраторов»](#).

Для создания новой сервисной учетной записи необходимо выполнить следующие действия:

1. Нажать кнопку «Добавить».
2. В правой рабочей области заполнить поля:
 - Наименование,
 - Отметить чекбоксами URL для которых будет действовать учетная запись (опционально):
 - Указать «Среднесуточный лимит вызовов» (опционально).
3. Во вкладке «Область применения» задать область применения.
4. Нажать кнопку сохранить.
5. Нажать кнопку «Сгенерировать токен».

6. Задать «Область применения».

2.8.24 Модели устройств

Раздел «Модели устройств» позволяет просматривать список зарегистрированных в системе устройств. Устройства могут быть зарегистрированы в системе автоматически при регистрации устройства модели отсутствовавшей в списке ранее, а так же могут быть добавлены в ручную администратором. Модели устройств могут быть использованы в «условиях применения» при применении сущностей.

Основной экран раздела отображает список устройств, где каждая строка списка содержит следующие данные:

- Наименование — модель устройства;
- Тип устройства:
 - Смартфон,
 - Планшет,
 - Иное.

В верхней части рабочего экрана находятся кнопки:

- Добавить — добавить новое устройство;
- Удалить — удалить устройство из списка.

В правой части рабочего экрана отображается информация о выбранном в списке устройстве и ссылка на актуальный список протестированных устройств (рисунок 2.179).

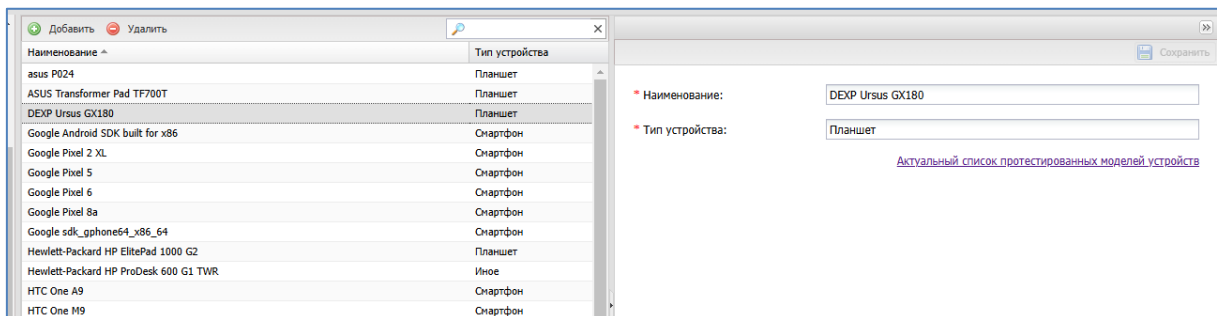


Рисунок 2.179 — Модели устройств зарегистрированных в системе

Чтобы добавить новое устройство в список необходимо выполнить следующие действия:

1. Нажать кнопку «Добавить».
2. Заполнить поля «Наименование» и «Тип устройства».

3. Нажать кнопку «Сохранить», после чего модель устройства будет добавлена в список и уже не может быть изменена.

Чтобы удалить устройство из списка необходимо выполнить следующие действия:

1. Убедиться, что модель не используется в комплектах и в условиях применения (именованных и не именованных), в противном случае удаление будет не возможно.
2. Выбрать в списке необходимую модель.
3. Нажать кнопку «Удалить».
4. Подтвердить действие, после чего запись о модели будет удалена из списка моделей устройств.

2.8.25 Файлы

Раздел «Файлы» позволяет загрузить файлы в систему, для последующей их отправки на устройства, в виде обоев рабочего стола (и/или киоска) и экрана блокировки. Установка файла на устройство в виде обоев осуществляется настройкой и назначением на устройство профиля «Обои» (см. раздел 2.6.9 Профили.)

Доступ к разделу имеют администраторы имеющие полномочия:

- Просмотр,
- Создание (только при наличии привилегии «Просмотр»),
- Изменение (только при наличии привилегии «Просмотр»),
- Удаление (только при наличии привилегии «Просмотр»).

В левой части раздела представлен список загруженных файлов, где каждая строка списка содержит следующие данные (рисунок 2.180):

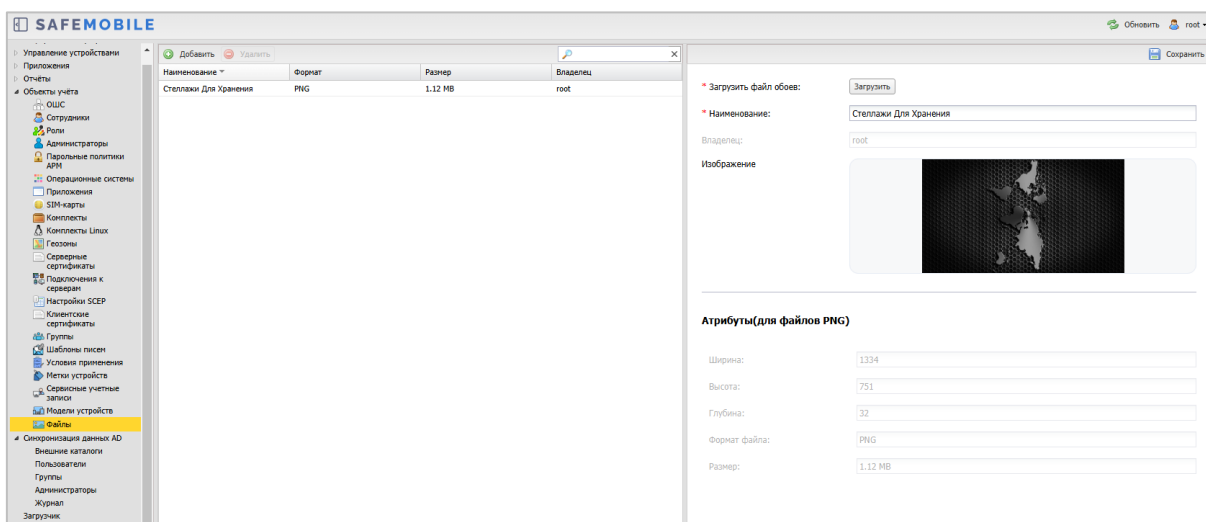


Рисунок 2.180 — Раздел «Файлы»

- Наименование — наименование загруженного файла;
- Формат — формат файла;
- Размер — размер файла;
- Владелец — корневой узел области управления администратора, загрузившего файл.

В правой части отображается информация о выбранном в списке файле, состоящая из следующих данных:

- Наименование — название загруженного файла;

- Владелец — корневой узел области управления администратора, загрузившего файл;
- Изображение — отображение загруженного файла;
- Атрибуты файла:
 - Ширина — ширина изображения (в пикселях);
 - Высота — высота изображения (в пикселях);
 - Глубина — глубина цвета (в битах);
 - Формат файла,
 - Размер — размер файла.

В верхней части рабочего экрана находятся кнопки:

- Добавить — загрузить в систему новый файл;
- Удалить — удалить из системы выбранный в списке файл.

Загрузка файла

Чтобы загрузить в систему новый файл необходимо выполнить следующие действия:

1. Проверить файл на соответствие следующим требованиям:
 - Формат файла должен быть PNG или JPG. Если файл имеет формат JPG, то после загрузки будет сконвертирован в PNG.
2. В разделе «Файлы» нажать кнопку «Добавить».
3. В правой части рабочего экрана нажать кнопку «Загрузить», после чего откроется окно выбора файла.
4. Выбрать файл, подтвердить загрузку.
5. Нажать кнопку «Сохранить», после чего файл будет загружен в систему.

Редактирование и удаление загруженного файла

Для редактирования названия файла следует выбрать файл с списке файлов, изменить значение поля «Наименование» и нажать кнопку «Сохранить».

Для удаления файла следует выбрать его в списке файлов, нажать кнопку «Удалить», подтвердить операцию удаления файла, после чего файл будет удален из системы.

2.9 Синхронизация данных LDAP

2.9.1 Внешние каталоги

В центральной части страницы раздела представлен список заданных подключений, к внешним каталогам LDAP.

Каждая строка списка содержит информацию об одном подключении и состоит из следующих полей данных (отображаются по умолчанию):

- **Наименование** — наименование подключения;
- **Тип LDAP** — тип внешнего каталога (по умолчанию «MS AD»);
- **Тег агента** — название компонента «агент синхронизации», предназначенного для синхронизации с внешним каталогом (LDAP);
- **Имя пользователя** — имя пользователя, для авторизации во внешнем каталоге (LDAP);
- **Синхронизация** — был ли каталог синхронизирован с актуальным набором параметров и правил. Возможные значения:
 - Успешно (дата и время),
 - Ошибка (дата и время),
 - Не синхронизировался,
- **Состояние синхронизации** — информация о синхронизации на текущий момент. Возможные значения:
 - Запланирована (дата и время),
 - В процессе (дата и время),
 - Не запланирована,
- **Последняя синхронизация** — информация о последней синхронизации. Возможные значения:
 - Успешно (дата и время),
 - Ошибка (дата и время),
- **Домен** — название домена;
- **Имя сервера** — доменное имя контроллера домена.

Справа, от списка подключений располагается блок настроек выбранного в списке подключения (рисунок 2.181).

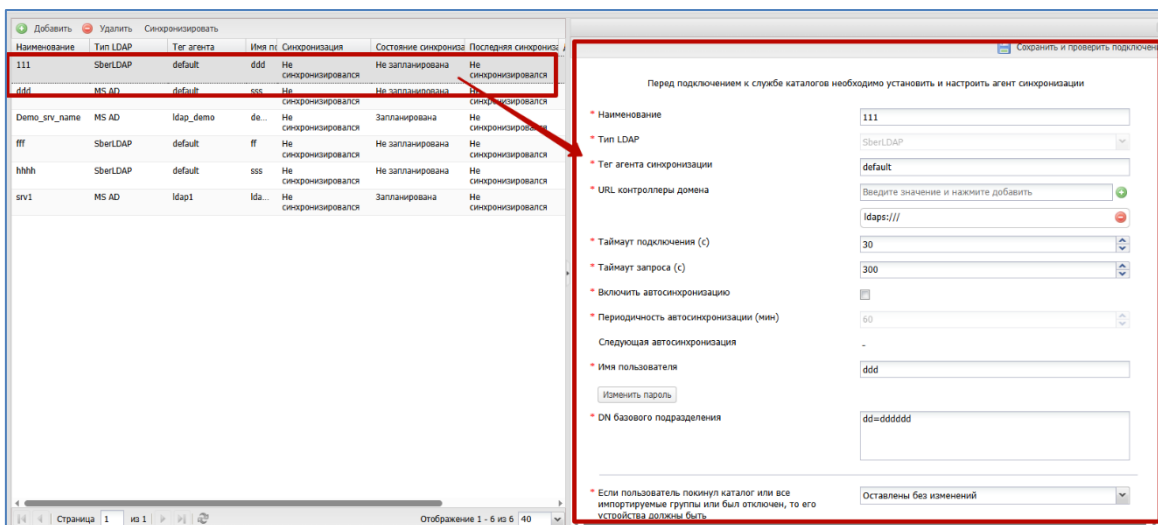


Рисунок 2.181 — Расположение блока настроек подключения

Блок настроек содержит следующие поля ввода, элементы управления и инфоблоки:

- **Наименование** — наименование подключения;
- **Тип LDAP** — тип внешнего каталога (по умолчанию «MS AD»). После первого сохранения параметр становится не доступен для изменения;
- **Тег агента синхронизации** — название компонента «агент синхронизации»; предназначенного для синхронизации с внешним каталогом LDAP. Тег агента должен совпадать с тегом, заданным в файле конфигурации агента синхронизации (по умолчанию имеет значение: default);
- **URL контроллера домена** — список из одного и более контроллеров домена. (Допускается заполнение как в виде доменного имени ldap://pdc.domain.com, так и в виде IP адреса);
- **Таймаут подключения (с)** — время ожидания восстановления подключения, до выдачи ошибки подключения. (заполняется в секундах);
- **Таймаут запроса (с)** — время ожидания ответа на запрос, до выдачи ошибки (заполняется в секундах);
- **Включить автосинхронизацию** — включить/выключить автоматическую синхронизацию с данным каталогом. При включенной автосинхронизации внешнего каталога изменение правил его синхронизации (Пользователи, Группы, Администраторы) невозможно;
- **Периодичность автосинхронизации (мин)** — период запуска автоматической

- синхронизации (задается в минутах);
- Следующая автосинхронизация — инфоблок с информацией о дате и времени следующей синхронизации с каталогом;
 - Имя пользователя — имя пользователя, для авторизации во внешнем каталоге (LDAP);
 - Пароль — пароль пользователя;
 - DN базового подразделения — заполняется в формате Distinguished Name;
 - Если пользователь покинул каталог или все импортируемые группы или был отключен, то его устройства должны быть (выбор варианта действия системы):
 - отключены от управление со сбросим к заводским настройкам;
 - отключены от управления с удалением корпоративных данных;
 - заблокированы,
 - оставлены без изменений,
 - Если пользователь заблокирован в каталоге, то его устройства должны быть (выбор действия системы):
 - отключены от управление со сбросим к заводским настройкам;
 - отключены от управления с удалением корпоративных данных;
 - заблокированы,
 - оставлены без изменений.

Примечание

Если в результате синхронизации определяется, что пользователь разблокирован в AD, то:

- *С сотрудника в системе снимается флаг «Заблокирован».*
- *Все устройства сотрудника, ранее заблокированные в результате синхронизации с AD, будут автоматически разблокированы.*

Инфоблок о состоянии подключения расположен в нижней части блока настроек подключения и содержащий следующие данные:

- Данные о проверке подключения, заполняются при нажатии кнопки «Сохранить и проверить подключение»:
 - Статус подключения — возможные значения «Успех», «Ошибка», «-»;

- Домен — название домена, записанное в формате Distinguished Name;
- Имя сервера — имя контроллера домена, записанное в формате Distinguished Name;
- Данные об актуальной, на текущий момент синхронизации:
 - Синхронизация — был ли каталог синхронизирован с актуальным набором параметров и правил. Возможные значения:
 - Успешно (дата и время),
 - Ошибка (дата и время),
 - Не синхронизировался,
 - Состояние синхронизации — информация о синхронизации на текущий момент. Возможные значения:
 - Запланирована (дата и время),
 - В процессе (дата и время),
 - Не запланирована,
 - Последняя синхронизация — информация о последней синхронизации. Возможные значения:
 - Успешно (дата и время),
 - Ошибка (дата и время),
 - Статус синхронизации — возможные значения «Успех», «Ошибка», «-»;
 - Время синхронизации — дата и время окончания синхронизации.

2.9.1.1 Создание нового подключения к службе каталогов

Чтобы создать подключение к внешнему каталогу LDAP, необходимо выполнить следующие действия:

1. Перейти в раздел «Внешние каталоги»,
2. Нажать кнопку «Добавить» (рисунок 2.182), после чего в блоке настроек подключения будут доступны поля для ввода данных о новом подключении,

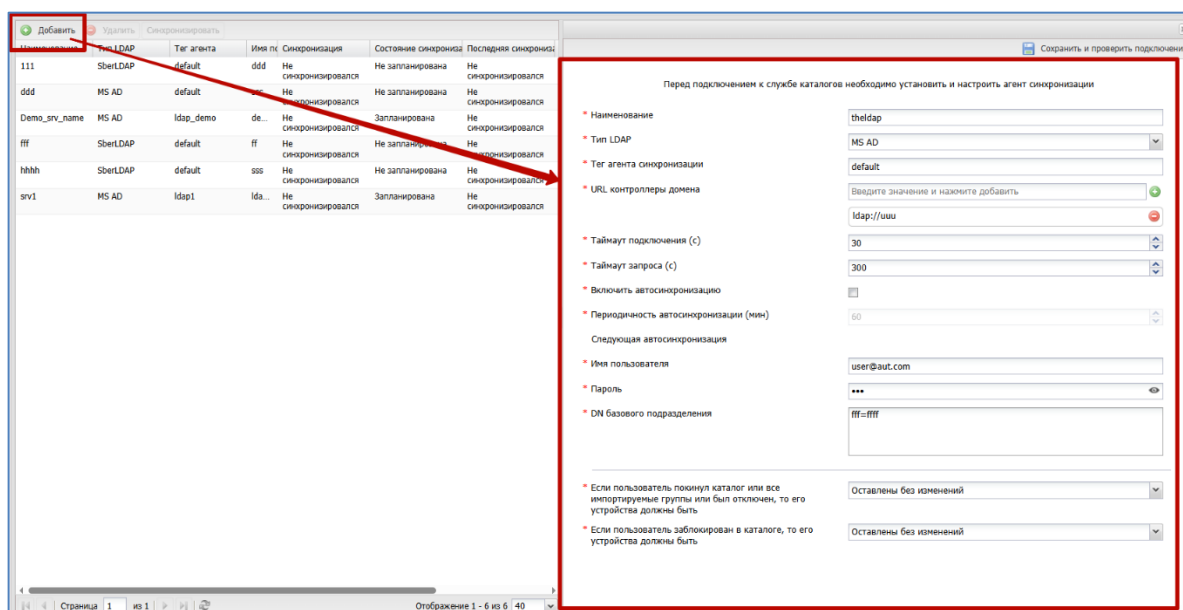


Рисунок 2.182 — Расположение кнопки «Добавить»

3. Заполнить все поля (Поле «Тег агента синхронизации» автоматически заполняется значением default),
4. Нажать кнопку «Сохранить и проверить подключение» (рисунок 2.183).

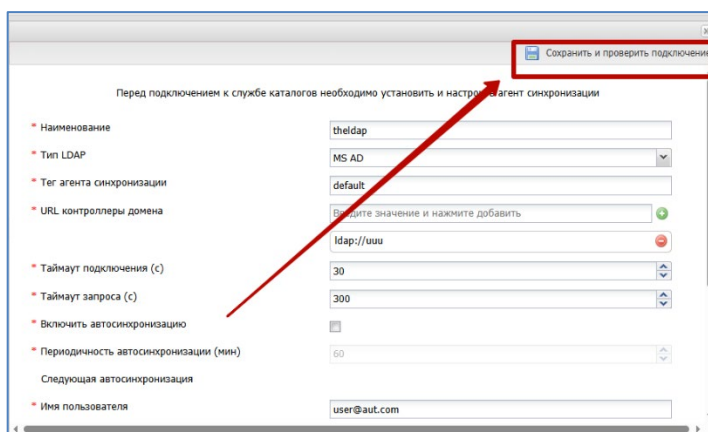


Рисунок 2.183 — Расположение кнопки «Сохранить и проверить подключение»

После нажатия кнопки «Сохранить и проверить подключение» в инфоблоке состояния подключения будет отображена информация о результатах проверки созданного подключения. (рисунок 2.184)

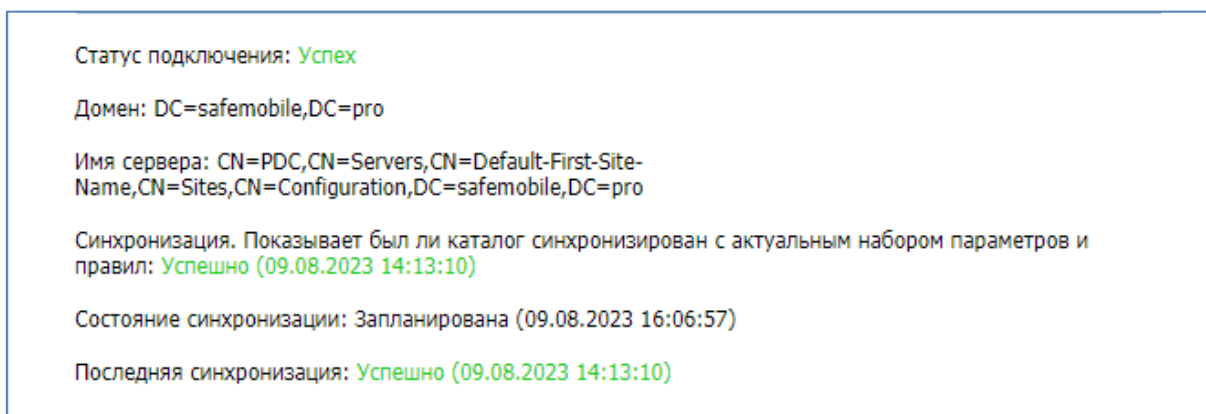
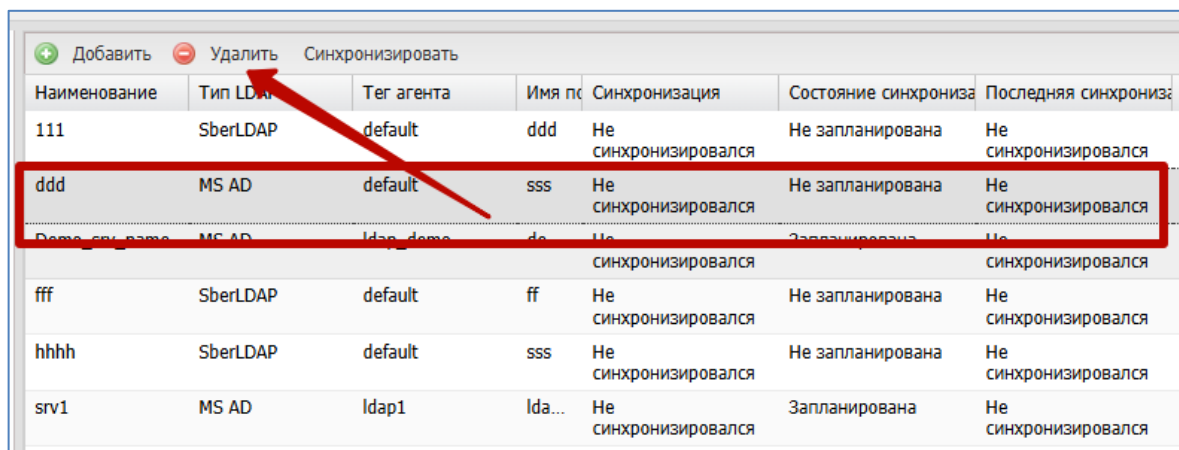


Рисунок 2.184 — Информационный блок состояния подключения

2.9.1.2 Удаление существующего подключения

Чтобы удалить существующее подключение к внешнему каталогу LDAP, необходимо выполнить следующие действия:

1. Перейти в раздел «Внешние каталоги».
2. Выделить в списке подключений строку, подлежащую удалению.
3. Нажать кнопку «Удалить» (рисунок 2.185).



Наименование	Тип LDAP	Тег агента	Имя по	Синхронизация	Состояние синхрониза	Последняя синхрониз
111	SberLDAP	default	ddd	Не синхронизировался	Не запланирована	Не синхронизировался
ddd	MS AD	default	sss	Не синхронизировался	Не запланирована	Не синхронизировался
Demo_srv_vame	MS AD	ldap_demo	da...	Не синхронизировался	Запланирована	Не синхронизировался
fff	SberLDAP	default	ff	Не синхронизировался	Не запланирована	Не синхронизировался
hhhh	SberLDAP	default	sss	Не синхронизировался	Не запланирована	Не синхронизировался
srv1	MS AD	ldap1	lda...	Не синхронизировался	Запланирована	Не синхронизировался

Рисунок 2.185 — Расположение кнопки «Удалить»

4. Подтвердить действие, после чего запись о подключении будет удалена.

Примечание

- Если удаляемое подключение ранее было успешно синхронизировано и у импортированных сотрудников имеются подключенные устройства, то система выдаст предупреждение о возможном отключении устройств пользователей от управления:
«Данный каталог ранее был успешно синхронизирован. Внесение изменений может привести к тому, что устройства сотрудников будут отключены от управления. Для подтверждения введите наименование внешнего каталога»,
- Пользователи и группы, импортированные с использованием удаляемого подключения, становятся доступны для удаления,
- Учетные записи администраторов, импортированных с использованием удаляемого подключения, удаляются,
- При удалении подключения с устройствами пользователей данного подключения будут произведены операции, описанные параметре «Если

пользователь покинул каталог или все импортируемые группы или был отключен, то его устройства должны быть».

2.9.1.3 Принудительная синхронизация с внешним каталогом LDAP

Чтобы запустить синхронизацию с внешним каталогом LDAP принудительно, необходимо выполнить следующие действия:

1. Перейти в раздел «Внешние каталоги».
2. Выделить в списке подключение, по которому необходимо сделать синхронизацию.
3. Нажать кнопку «Синхронизировать» (рисунок 2.186), после чего будет запущен процесс синхронизации с внешним каталогом LDAP.

Наименование	Тип LDAP	Имя агента	Имя пользователя	Синхронизация	Состояние синхронизации	Последняя синхронизация
111	SberLDAP	default	ddd	Не синхронизировался	Не запланирована	Не синхронизировался
ddd	MS AD	default	sss	Не синхронизировался	Не запланирована	Не синхронизировался
demo_ldap_name	MS AD	ldap_demo	demo	Не синхронизировался	Запланирована	Не синхронизировался

Рисунок 2.186 — Расположение кнопки «Синхронизировать»

Примечание

Срок запуска следующей автоматической синхронизации будет отсчитываться от времени запуска принудительной синхронизации.

2.9.2 Пользователи

В данном разделе задаются и настраиваются правила импорта пользователей из внешних каталогов LDAP. Результатом работы импорта пользователей является создание записи о пользователе (или списка пользователей) с атрибутами учетной записи внешнего каталога LDAP. Администратор может задать приоритет импорта. Если пользователь попадает под действие нескольких правил импорта, то он будет импортирован по правилу, у которого приоритет выше.

Пример:

Сотрудник попадает под правила с приоритетом 1 и 2, в правилах указаны разные подразделения, к которым принадлежит сотрудник. Сотрудник будет выгружен в то подразделение, которое указано в правиле с приоритетом 1.

Учетные записи пользователей, импортированные заданными правилами, отображаются в разделе:

- Объекты учета:
 - Сотрудники.

В центральной части раздела отображается список правил импорта пользователей системы из внешнего каталога LDAP (рисунок 2.187).

Приоритет	Целевое подразделение	DN группы	Внешний каталог	Базовый DN	Статус синхронизации	Время синхронизации
1	55		srv3	re=ity	-	-
2	33		srv3		-	-
2	11		srv2	dd=ll	-	-
2		CN=Крб, внутри салата,OU=...	faa	DC=safetest,DC=pro	Успех	17.01.2024 10:11:40

Рисунок 2.187 — Список правил синхронизации

Каждая строка списка является записью одного правила импорта, и содержит следующую информацию (отображается по умолчанию):

- Приоритет — приоритет правила импорта над другими правилами;

- Целевое подразделение — подразделение в древе ОШС; куда будет производиться импорт (опционально);
- DN группы — DN выбранной группы пользователей во внешнем каталоге LDAP ;
- Внешний каталог — наименование подключения к внешнему каталогу LDAP;
- Базовый DN — DN базового подразделения;
- Статус синхронизации — статус синхронизации; актуальной на момент просмотра;
- Время синхронизации — дата и время синхронизации с внешним каталогом LDAP, актуальной на момент просмотра.

В правой части рабочего экрана отображается блок параметров, выбранного в списке правила (рисунок 2.188).

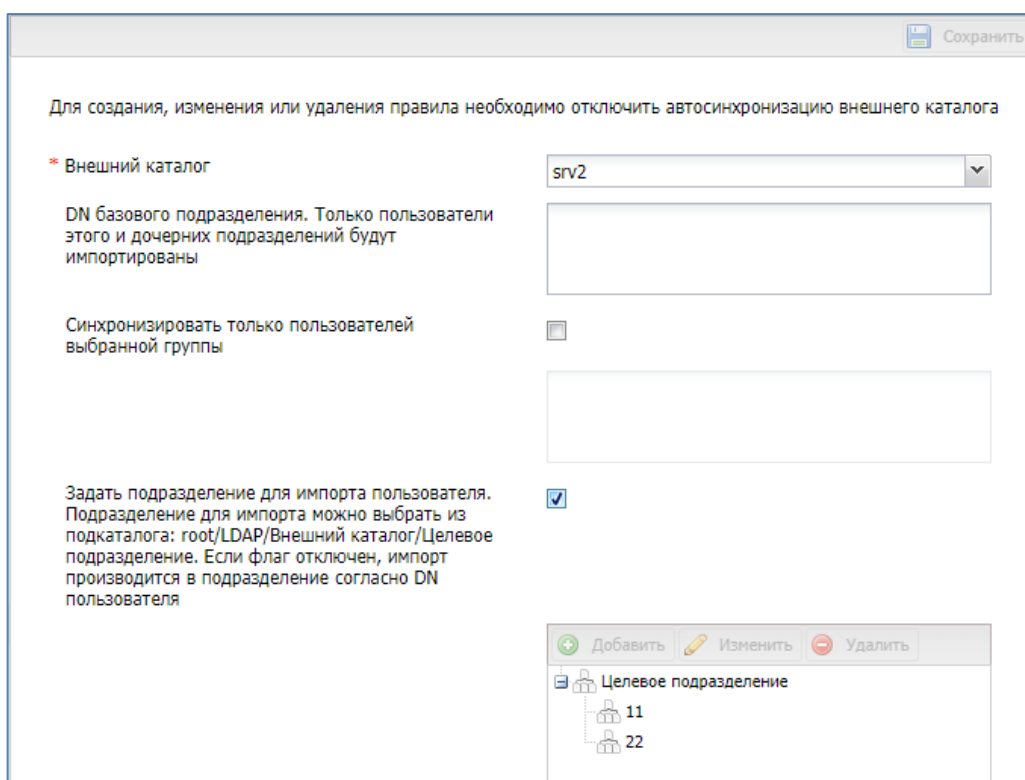


Рисунок 2.188 — Настройки правила синхронизации списка пользователей с внешним каталогом LDAP

Блок содержит следующие поля ввода:

- Внешний каталог — наименование подключения к внешнему каталогу LDAP. (Не доступен для изменения уже заданных правил);

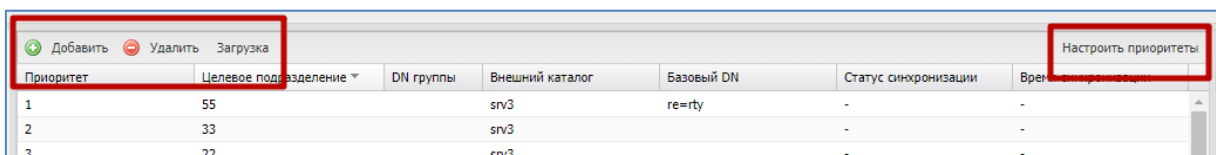
- DN базового подразделения. Только пользователи этого и дочерних подразделений будут импортированы — задается в формате DN. (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога);
- Синхронизировать только пользователей выбранной группы — флаг включает/выключает возможность добавления отдельной группы пользователей внешнего каталога LDAP, подлежащих импорту:
 - Поле ввода DN группы пользователей подлежащих импорту;
 - Включая пользователей подгрупп — при включении данного флага синхронизация затронет также пользователей всех подгрупп внутри указанной;
- Задать подразделение для импорта пользователя. Подразделение для импорта можно выбрать из подкаталога: root/LDAP/Внешний каталог/Целевое подразделение. Если флаг отключен, импорт производится в подразделение согласно DN пользователя — флаг включает/выключает возможность указания целевого подразделения:
 - Окно выбора целевого подразделения в структуре ОШС. В этом окне можно создать, изменить или удалить целевое подразделение. Так же целевое подразделение может быть задано заранее, в разделе «Объекты учета — ОШС»:
 - Создание целевого подразделения — процесс аналогичен созданию подразделения в структуре ОШС;
 - Удалить целевое подразделение:
 - Если есть правила импорта пользователей, которые используют данное целевое подразделение следует сначала удалить или правила или убрать целевое подразделение из этих правил. В противном случае при попытке удаления система выдаст сообщение об ошибке: *«Подразделение ОШС является целевым для импорта пользователей внешнего каталога»;*
 - Изменение целевого подразделения:
 - Для внесения изменений в целевое подразделение необходимо указать новое имя и выбрать стратегию управления.

Примечание

- *Импортированы будут только те пользователи, которые принадлежат базовому подразделению и непосредственно входят в указанную группу пользователей. Пользователи, входящие в подгруппы указанной группы, импортированы **не будут**.*
- *При включенной автосинхронизации.
Если у группы пользователей, используемой в правиле импорта сотрудников, изменился distinguishedName или базовое подразделение, то будет считаться, что сотрудники, импортированные этим правилом, покинули область источника импорта. С их устройствами будут произведены действия согласно настройкам во внешнем каталоге. Сотрудники станут доступным для удаления.*

В «шапке» списка правил синхронизации расположены кнопки вызова следующих функций (рисунок 2.189):

- Кнопка «Добавить» — добавить новое правило импорта,
- Кнопка «Удалить» — удалить правило импорта,
- Кнопка «Загрузить» — задать правило импорта пользователей с помощью файла, содержащего список групп пользователей,
- Кнопка «Настроить приоритеты» — открывает настройки приоритета для правил импорта.



Приоритет	Целевое подразделение	DN группы	Внешний каталог	Базовый DN	Статус синхронизации	Время синхронизации
1	55		srv3	re=rty	-	-
2	33		srv3		-	-
3	22		srv3		-	-

Рисунок 2.189 — расположение кнопок «Добавить», «Удалить», «Загрузить», «настроить приоритеты»

2.9.2.1 Изменение параметров существующего правила

Чтобы изменить параметры правила, необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи».
2. В списке правил синхронизации выделить правило подлежащее изменению.
3. В блоке параметров правила внести изменения.
4. Нажать кнопку «Сохранить» (рисунок 2.190).

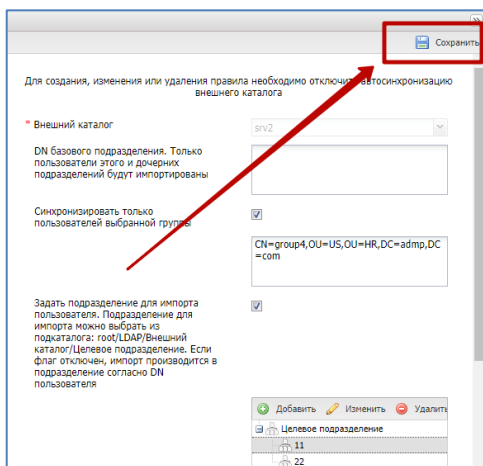


Рисунок 2.190 — Расположение кнопки «Сохранить»

2.9.2.2 Создание нового правила импорта пользователей

Чтобы создать новое правило импорта пользователей системы из списка пользователей внешнего каталога LDAP, необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи».
2. Нажать кнопку «Добавить».
3. В блоке параметров создаваемого правила заполнить необходимые поля.
4. Нажать кнопку «Сохранить».

Примечание

Импортированы будут только те пользователи, которые:

- принадлежат и базовому подразделению и указанной группе пользователей,
- у которых заполнен атрибут `displayName`, либо атрибуты `givenName` и `sn`

2.9.2.3 Удаление правила импорта пользователей

Чтобы удалить правило импорта пользователей, необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи».
2. В списке правил синхронизации выделить правило подлежащее удалению. После чего кнопка «Удалить» станет активной.
3. Нажать кнопку «Удалить».
4. Нажмите «Да», в диалоговом окне подтверждения действия (рисунок 2.191), после чего выбранное правило будет удалено.

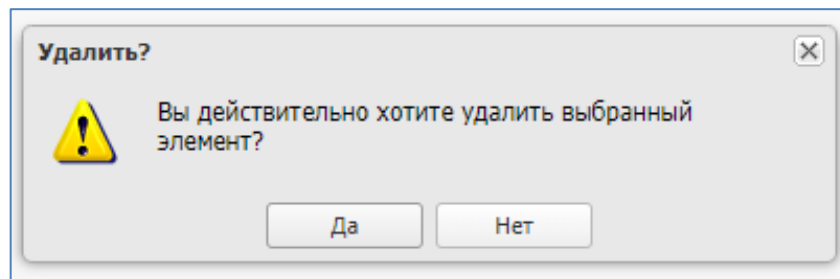


Рисунок 2.191 — Диалоговое окно подтверждения действия

2.9.2.4 Создание правила импорта пользователей с помощью файла списка групп пользователей

Данная функция используется для пакетного создания правил импорта пользователей из одного базового подразделения, но принадлежащих различным группам пользователей внешнего каталога LDAP. Для её использования необходимо иметь файл со списком DN имен групп пользователей внешнего каталога, подлежащих импорту. Формат файла — csv, кодировка — UTF-8.

Чтобы создать правило импорта пользователей с помощью файла, необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи».
2. Нажать кнопку «Загрузка», после чего откроется модальное окно с полями ввода параметров загрузки (рисунок 2.192).

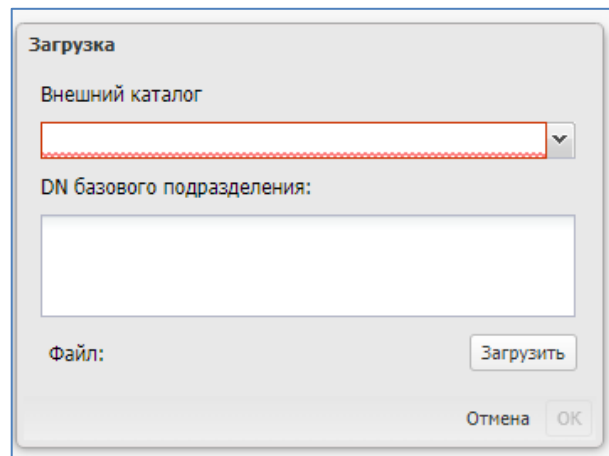


Рисунок 2.192 — Модальное окно с параметрами загрузки пользователей из файла

3. Заполнить поля:
 - Внешний каталог — название подключения к внешнему каталогу LDAP (выбор из выпадающего списка существующих подключений);
 - DN базового подразделения — название подразделения которому принадлежат импортируемые пользователи внешнего каталога (дается в формате DN). Если поле не задано, то за DN базового подразделения берется DN внешнего каталога;
4. Нажать кнопку «Загрузить», после чего откроется окно браузера ОС для выбора загружаемого файла, содержащего список групп пользователей.
5. Выбрать файл.
6. Нажать кнопку «Ок», после чего будут созданы новые правила импорта.

2.9.2.5 Настройка приоритетов правила импорта пользователей

Изменение приоритетов правил импорта доступно для серверов с отключенной автосинхронизацией. Перед внесением изменений следует убедиться, что автосинхронизация сервера отключена. В противном случае результаты настроек приоритетов сохранить будет невозможно.

Чтобы настроить приоритеты правила импорта необходимо выполнить следующие действия:

1. Перейти в раздел «Пользователи».
2. Нажать кнопку «Настроить приоритеты», после чего откроется окно настроек приоритетов правил импорта.
3. Выбрать внешний каталог, для правил которого требуется настроить приоритеты (рисунок 2.193).

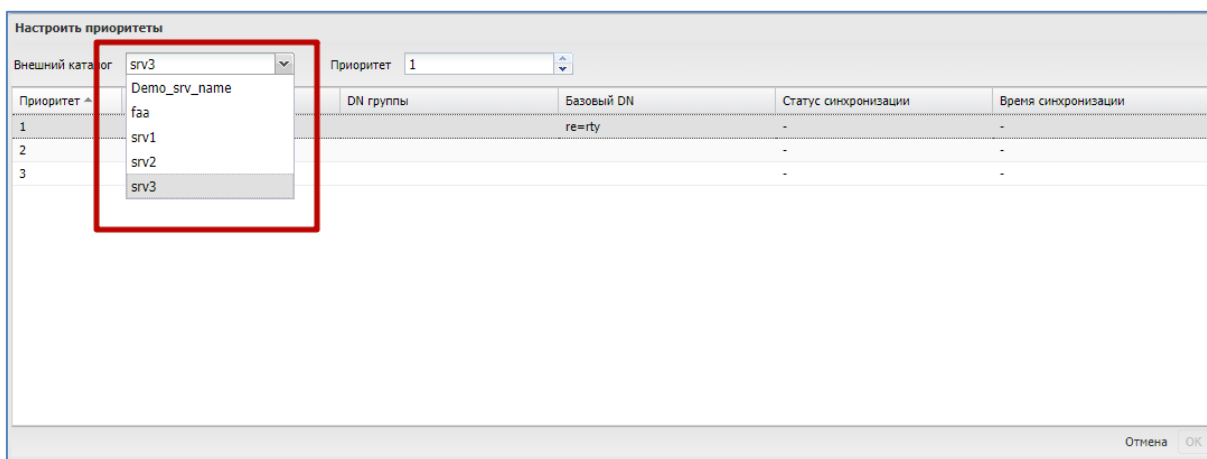


Рисунок 2.193 — Выбор внешнего каталога в настройках приоритетов импорта

4. Выбрать правило в списке и указать приоритет для данного правила (рисунок 2.194).

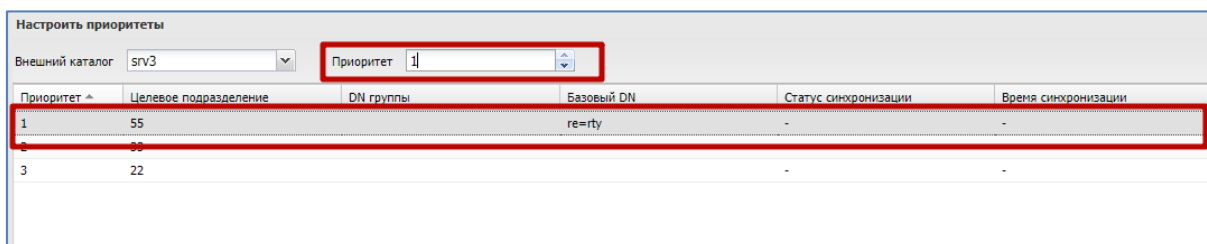


Рисунок 2.194 — Назначение приоритета на правило импорта

5. Нажать кнопку «Ок».

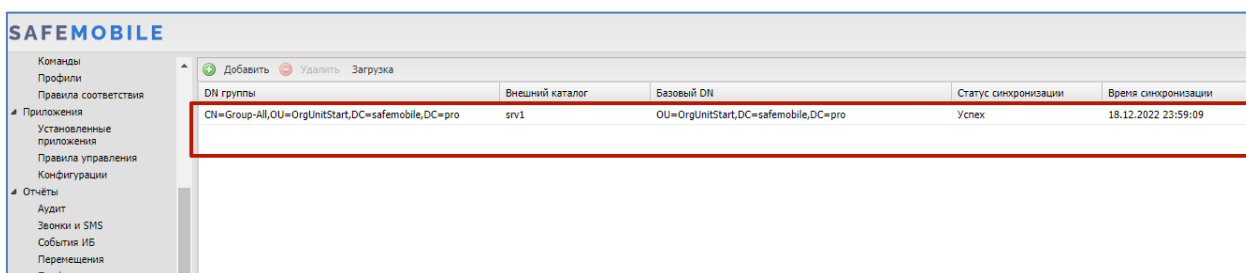
2.9.3 Группы

В разделе отображаются правила импорта групп пользователей из внешнего каталога LDAP. Результатом работы правил импорта групп пользователей является список DN групп и DN имена пользователей, принадлежащих этим группам.

Группы пользователей, импортированные по заданным правилам, отображаются в разделе:

- Объекты учета:
 - Группы.
- Используются при конфигурировании приложений и устройств, в разделах:
- Приложения:
 - Правила управления:
 - Вкладка «Условия»,
 - Конфигурации:
 - Вкладка «Условия»,
- Управление устройствами:
 - Правила несоответствия:
 - Вкладка «Условия»,
 - Профили:
 - Вкладка «Условия».

В центральной части раздела отображается список правил импорта групп пользователей внешнего каталога LDAP (рисунок 2.195).



DN группы	Внешний каталог	Базовый DN	Статус синхронизации	Время синхронизации
CN=Group-All,OU=OrgUnitStart,DC=safemobile,DC=pro	srv1	OU=OrgUnitStart,DC=safemobile,DC=pro	Успех	18.12.2022 23:59:09

Рисунок 2.195 — Список правил импорта групп

Каждая строка списка является записью одного правила импорта, и содержит следующую информацию (отображается по умолчанию):

- DN группы — DN выбранной группы пользователей в каталоге LDAP;
- Внешний каталог — наименование подключения к внешнему каталогу LDAP;
- Базовый DN — DN базового подразделения;

- Статус синхронизации — статус синхронизации, актуальной на момент просмотра;
- Время синхронизации — дата и время синхронизации с внешним каталогом LDAP, актуальной на момент просмотра.

В правой части рабочего экрана отображается блок параметров, выбранного в списке правила (рисунок 2.196).

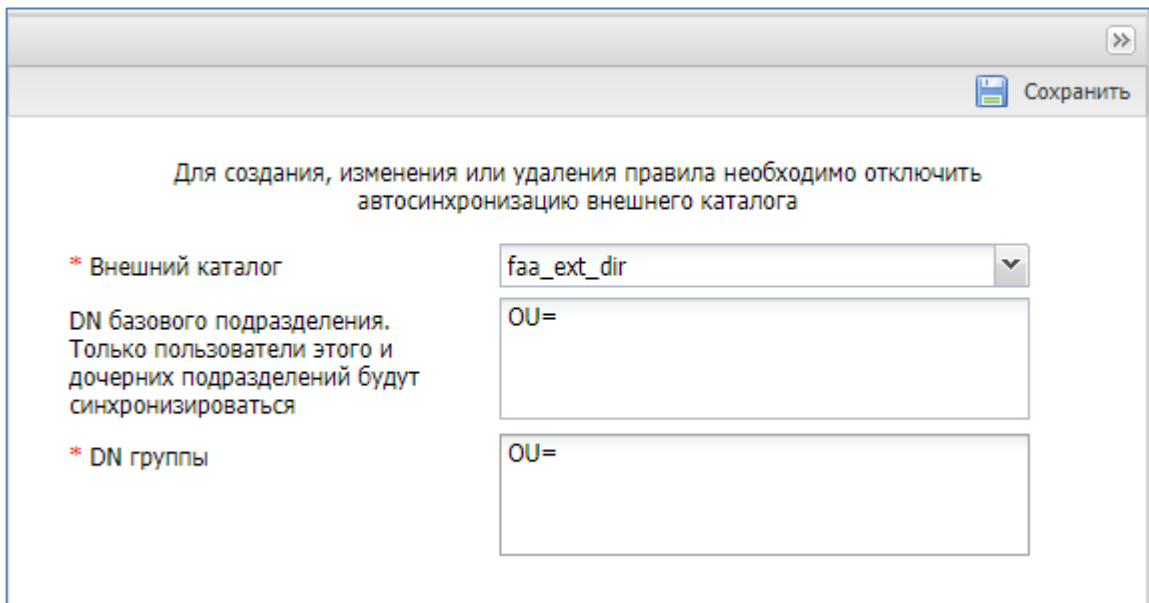


Рисунок 2.196 — Параметры правила импорта групп

Блок содержит следующие поля ввода:

- Внешний каталог — наименование подключения к внешнему каталогу LDAP. (Не доступен для изменения уже заданных правил);
- DN базового подразделения. Только пользователи этого и дочерних подразделений будут синхронизироваться — задается в формате DN; (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога);
- DN группы — DN имя группы, подлежащей импорту из внешнего каталога (обязательно для заполнения);
- Включая подгруппы — при включении данного флага синхронизация затронет также все подгруппы внутри указанной.

Примечание

- *Импортируются только названия групп, а не пользователи. Пользователи, импортированные из внешнего каталога, сопоставляются с импортированными группами и отображаются в разделе:*

Объекты учета

- **Группы**
 - **Вкладка «члены группы»**
- *При включенной автосинхронизации. Если у импортированной группы изменился distinguishedName (группа переименована или переименовано одно из родительских подразделений группы), то из импортированной группы будут удалены все сотрудники. Если импортированная группа использовалась в условиях применения профилей, правил управления, конфигурация приложений или правил несоответствия, то их назначения будут сняты с сотрудников, ранее входивших в группу.*

В «шапке» списка правил синхронизации расположены кнопки вызова следующих функций (рисунок 2.197):

- «Добавить» — добавить новое правило импорта;
- «Удалить» — удалить правило импорта из списка;
- «Загрузить» — задать правило импорта с помощью файла, содержащего список групп.

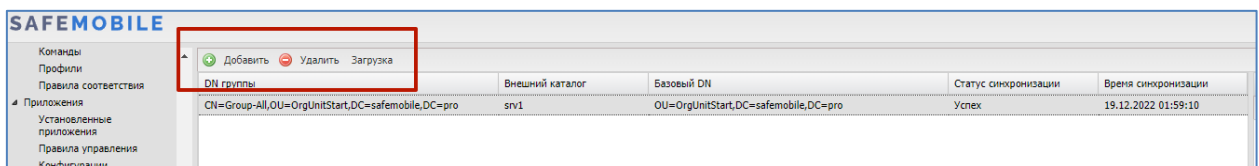


Рисунок 2.197 — Расположение кнопок «Добавить», «Удалить», «Загрузить»

2.9.3.1 Изменение параметров существующего правила импорта

Чтобы изменить параметры существующего правила импорта групп, необходимо выполнить следующие действия:

1. Перейти в раздел «Группы».
2. Найти и выделить в списке правило, подлежащее изменению параметров.

3. В блоке параметров правила внести изменения.
4. Нажать кнопку «Сохранить» (рисунок 2.198).

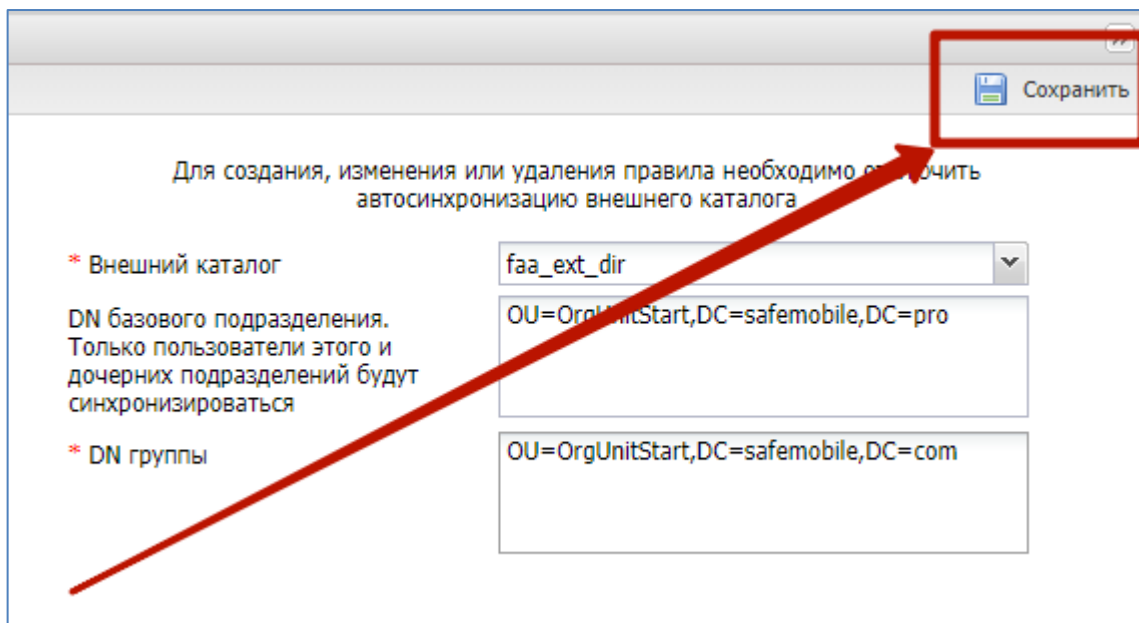


Рисунок 2.198 — Расположение кнопки «Сохранить»

2.9.3.2 Добавить новое правило импорта групп пользователей

Чтобы добавить новое правило импорта группы пользователей, необходимо выполнить следующие действия:

1. Перейти в раздел «Группы».
2. Нажать кнопку «Добавить».
3. В блоке параметров правила заполнить необходимые поля ввода.
4. Нажать кнопку «Сохранить».

2.9.3.3 Удалить существующее правило импорта групп из списка

Чтобы удалить правило импорта групп из списка, необходимо выполнить следующие действия:

1. Перейти в раздел «Группы».
2. В списке правил импорта выделить правило подлежащее удалению. После чего кнопка «Удалить» станет активной.
3. Нажать кнопку «Удалить».

4. Нажмите «Да», в диалоговом окне подтверждения действия (рисунок 2.199), после чего выбранное правило будет удалено.

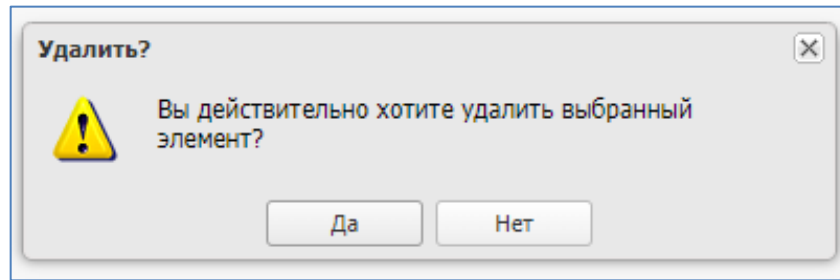


Рисунок 2.199 — Диалоговое окно подтверждения действия

При попытке удалить правило синхронизации групп система проверяет, используется ли импортированная правилом группа в условиях применения профилей, правил управления приложениями или конфигураций.

Если группа задействована в условиях, администратор увидит предупреждение:

- *«Группа используется в условиях применения сущностей. Удаление невозможно. Перевести импортированную группу в локальную?»*

При подтверждении удаления группа преобразуется в локальную и ей присваивается имя вида:

- <DN группы> (конвертирована в локальную <DD.MM.YY hh:mm:ss> UTC).
- При отказе правило удаляется вместе с группой.

При обновлении системы до версии 15.0 все импортированные группы, не связанные ни с одним правилом синхронизации, автоматически:

- переводятся в локальные, если используются в условиях применения сущностей (имя формируется аналогично);
- удаляются в противном случае.

2.9.3.4 Создание правила импорта групп из файла, содержащего список групп внешнего каталога

Данная функция используется для пакетного создания правил импорта групп внешнего каталога. Для её использования необходимо иметь файл со списком групп внешнего каталога, подлежащих импорту.

Чтобы создать правило импорта групп с помощью файла, содержащего список групп, необходимо выполнить следующие действия:

1. Перейти в раздел «Группы».
2. Нажать кнопку «Загрузка», после чего откроется модальное окно с полями ввода параметров загрузки (рисунок 2.200).

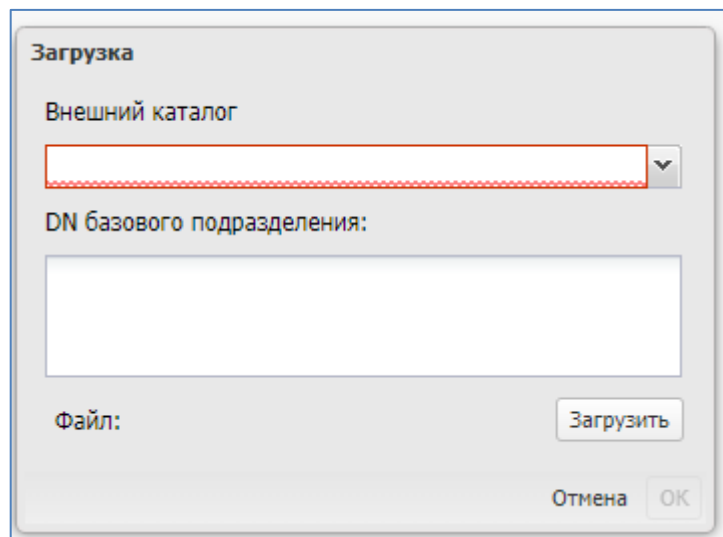


Рисунок 2.200 — Модальное окно с параметрами загрузки пользователей из файла

3. Заполнить поля:
 - Внешний каталог — название подключения к внешнему каталогу LDAP (выбор из выпадающего списка существующих подключений);
 - DN базового подразделения — название подразделения, которому принадлежит загружаемый список групп (задается в формате DN). (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога);
4. Нажать кнопку «Загрузить», после чего откроется окно браузера ОС для выбора загружаемого файла, содержащим список групп.
5. Выбрать файл.
6. Нажать кнопку «Ок», после чего будут созданы новые правила импорта.

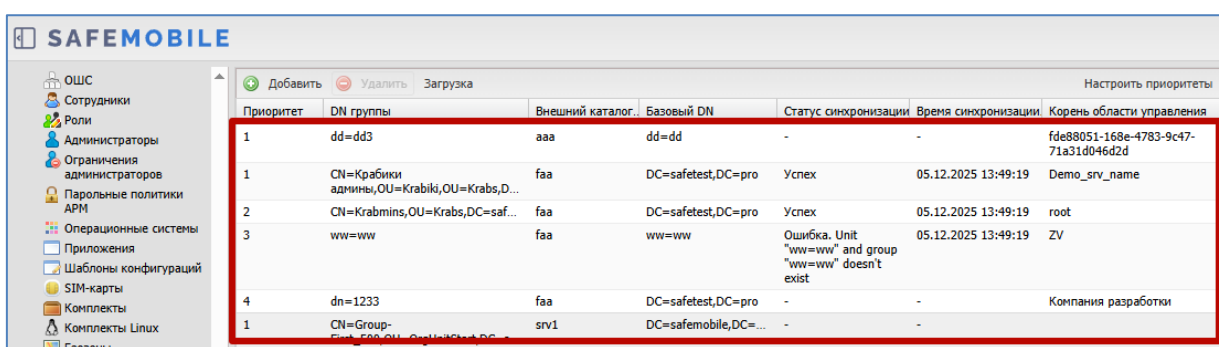
2.9.4 Администраторы

В данном разделе задаются правила импорта списка пользователей из внешнего каталога LDAP, подлежащих назначению администраторами в системе.

Список пользователей-администраторов, созданных с помощью правил импорта из внешнего каталога доступен в разделе:

- Объекты учета:
 - Администраторы

В центральной части раздела отображается список правил импорта администраторов из внешнего каталога LDAP (рисунок 2.201).



Приоритет	DN группы	Внешний каталог	Базовый DN	Статус синхронизации	Время синхронизации	Корень области управления
1	dd=dd3	aaa	dd=dd	-	-	fde88051-168e-4783-9c47-71a31d046d2d
1	CN=Крабика админы,OU=Krabiki,OU=Krabs,D...	faa	DC=safetest,DC=pro	Успех	05.12.2025 13:49:19	Demo_srv_name
2	CN=Krabmins,OU=Krabs,DC=saf...	faa	DC=safetest,DC=pro	Успех	05.12.2025 13:49:19	root
3	ww=ww	faa	ww=ww	Ошибка. Unit "ww=ww" and group "ww=ww" doesn't exist	05.12.2025 13:49:19	ZV
4	dn=1233	faa	DC=safetest,DC=pro	-	-	Компания разработки
1	CN=Group-...	srv1	DC=safemobile,DC=...	-	-	

Рисунок 2.201 — Список правил синхронизации

Каждая строка списка является записью одного правила импорта, и содержит следующую информацию (отображается по умолчанию):

- Приоритет — приоритет в порядке обработки правил импорта. 1 — наивысший;
- DN группы — DN выбранной группы пользователей в каталоге LDAP;
- Внешний каталог — наименование подключения к внешнему каталогу LDAP;
- Базовый DN — DN базового подразделения;
- Статус синхронизации — статус синхронизации, актуальной на момент просмотра;
- Время синхронизации — дата и время синхронизации с внешним каталогом LDAP, актуальной на момент просмотра;
- Корень области управления — верхний (родительский) узел в дереве организационно-штатной структуры (ОШС), на который администратору разрешено распространять свои полномочия.

В правой части рабочего экрана отображается блок параметров, выбранного в списке правила (рисунок 2.202).

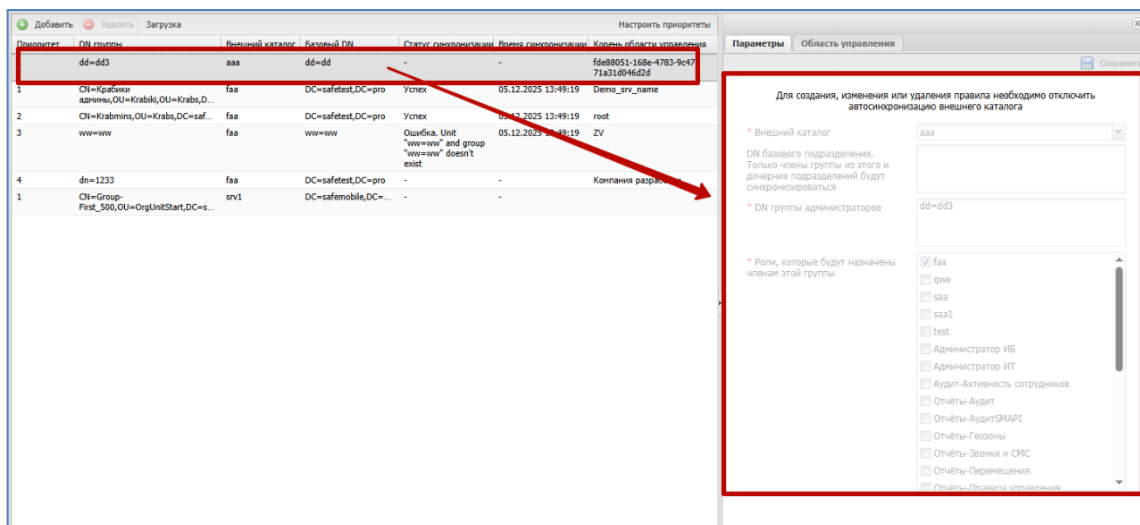


Рисунок 2.202 — Расположение блока параметров правила импорта

Блок содержит следующие данные:

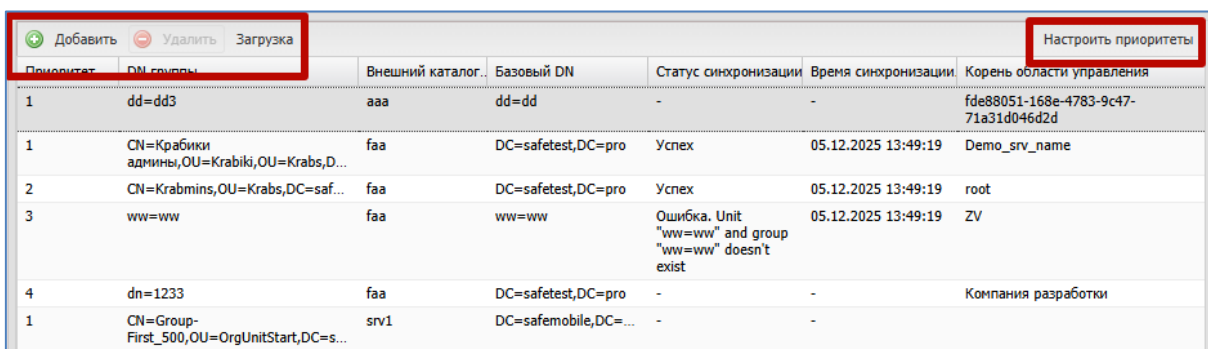
- Вкладка «Параметры»:
 - Внешний каталог — наименование подключения к внешнему каталогу LDAP. (Не доступен для изменения уже заданных правил);
 - DN базового подразделения. Только члены группы из этого подразделения и дочерних подразделений будут синхронизироваться — задается в формате DN. (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога);
 - DN группы администраторов — DN имя группы администраторов (обязательно для заполнения);
 - Роли, которые будут назначены членам этой группы — список ролей администраторов системы (обязательно для заполнения).
- Вкладка «Область управления» — задаёт, в какой части организационной структуры (ОШС) будет работать импортированный администратор.

Примечание

- Список ролей, отображаемый в параметрах правила задается в разделе: *Объекты учета — Роли.*
- При включенной автосинхронизации. если у группы, используемой в правиле импорта администраторов, изменился distinguishedName, то будет считаться, что администраторы, импортированные этим правилом, покинули область импорта LDAP. Администраторы будут удалены.

В «шапке» списка правил расположены кнопки вызова следующих функций (рисунок 2.203):

- Кнопка «Добавить» — добавить новое правило импорта;
- Кнопка «Удалить» — удалить правило импорта из списка;
- Кнопка «Загрузить» — задать правило импорта с помощью файла, содержащего список групп;
- Кнопка «Настроить приоритеты» — открывает диалог изменения порядка применения правил импорта внутри одного внешнего каталога. Работает аналогично приоритетам правил для пользователей (см. 2.9.2.5 Настройка приоритетов правила импорта пользователей).



Приоритет	DN группы	Внешний каталог	Базовый DN	Статус синхронизации	Время синхронизации	Корень области управления
1	dd=dd3	aaa	dd=dd	-	-	fde88051-168e-4783-9c47-71a31d046d2d
1	CN=Крабики админы,OU=Krabiki,OU=Krabs,D...	faa	DC=safetest,DC=pro	Успех	05.12.2025 13:49:19	Demo_srv_name
2	CN=Krabmins,OU=Krabs,DC=saf...	faa	DC=safetest,DC=pro	Успех	05.12.2025 13:49:19	root
3	ww=ww	faa	ww=ww	Ошибка. Unit "ww=ww" and group "ww=ww" doesn't exist	05.12.2025 13:49:19	ZV
4	dn=1233	faa	DC=safetest,DC=pro	-	-	Компания разработки
1	CN=Group-First_500,OU=OrgUnitStart,DC=s...	srv1	DC=safemobile,DC=...	-	-	

Рисунок 2.203 — Расположение кнопок «Добавить», «Удалить», «Загрузить», «Приоритеты».

2.9.4.1 Изменение параметров существующего правила

Для внесения изменения в правило импорта следует убедиться, что у внешнего каталога отключена «автосинхронизация».

Чтобы изменить параметры правила, необходимо выполнить следующие действия:

1. Перейти в раздел «Администраторы».
2. В списке правил синхронизации выделить правило подлежащее изменению.
3. В блоке параметров правила внести изменения.
4. Нажать кнопку «Сохранить».

2.9.4.2 Добавить новое правило импорта администраторов

Чтобы добавить новое правило импорта администраторов, необходимо выполнить следующие действия:

1. Перейти в раздел «Администраторы».
2. Нажать кнопку «Добавить».
3. Во вкладке правила «Параметры» заполнить необходимые поля ввода.
4. (Опционально) Во вкладке «Область управления» указать область управления для импортируемых администраторов.
5. Нажать кнопку «Сохранить».

Примечание

Импортированы будут только те пользователи, у которых заполнен атрибут `displayName`, либо атрибуты `givenName` и `sn`.

2.9.4.3 Удалить существующее правило импорта администраторов

Чтобы удалить правило импорта администраторов, необходимо выполнить следующие действия:

1. Перейти в раздел «Администраторы».
2. В списке правил выделить правило подлежащее удалению. После чего кнопка «Удалить» станет активной.
3. Нажать кнопку «Удалить».

4. Нажмите «Да», в диалоговом окне подтверждения действия (рисунок 2.204), после чего выбранное правило будет удалено.

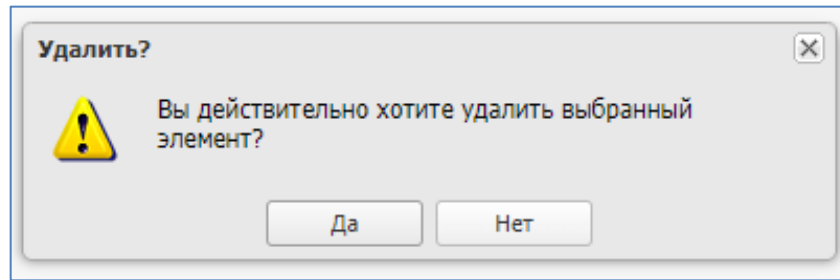


Рисунок 2.204 — Диалоговое окно подтверждения действия

2.9.4.4 Создание правила импорта администраторов из файла, содержащего список групп администраторов внешнего каталога.

Данная функция используется для пакетного создания правил импорта администраторов из нескольких групп пользователей внешнего каталога.

Для её использования необходимо иметь файл со списком групп пользователей внешнего каталога, подлежащих импорту.

Чтобы создать правило импорта групп с помощью файла, содержащего список групп, необходимо выполнить следующие действия:

1. Перейти в раздел «Администраторы».
2. Нажать кнопку «Загрузка», после чего откроется модальное окно с полями ввода параметров загрузки (рисунок 2.205).

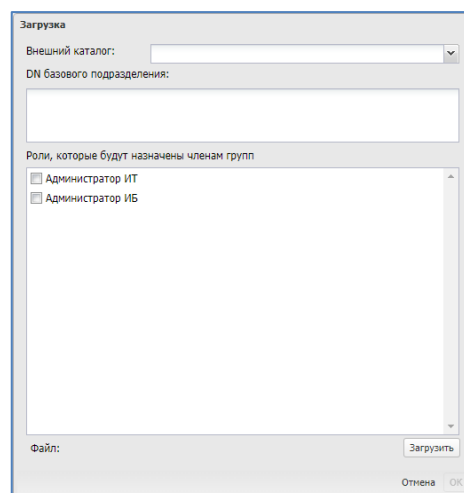


Рисунок 2.205 — Модальное окно с параметрами загрузки пользователей из файла

3. Заполнить поля:
 - Внешний каталог — название подключения к внешнему каталогу LDAP (выбор из выпадающего списка существующих подключений);
 - DN базового подразделения — название подразделения, которому принадлежит загружаемый список групп (задается в формате DN). (Если поле не задано, то за DN базового подразделения берется DN из внешнего каталога).
4. Роли, которые будут назначены членам групп — отметить флагами роли администраторов из списка.
5. Нажать кнопку «Загрузить», после чего откроется окно браузера ОС для выбора загружаемого файла, содержащим список групп.
6. Выбрать файл.
7. Нажать кнопку «Ок», после чего будет создано новое правило импорта.

2.9.5 Журнал

В разделе отображается список событий, связанных с импортом данных из внешних каталогов LDAP.

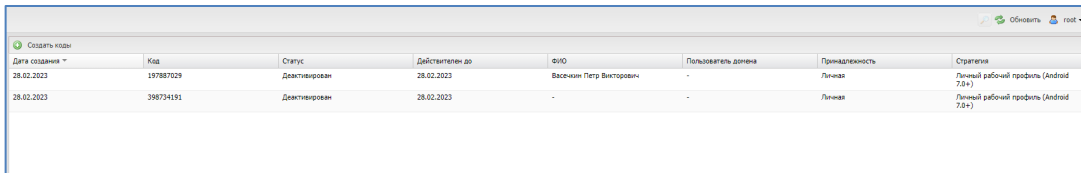
Каждая строка списка — запись о событии синхронизации одного правила импорта и содержит в себе следующие данные (отображаются по умолчанию):

- Тип — тип импортируемых данных (Пользователи, Группы, Администраторы);
- DN группы — DN группы импортируемых данных;
- Внешний каталог — название подключения к внешнему каталогу;
- Базовый DN — DN базового подразделения;
- Время начала — время начала синхронизации с внешним каталогом;
- Время завершения — время завершения синхронизации с внешним каталогом;
- Статус — статус операции, после ее завершения;
- Детали — детальная информация о возникших ошибках.

2.10 Регистрация устройств

2.10.1 Управление кодами приглашения (пункт меню «Загрузчик»)

«UEM SafeMobile» предоставляет возможность самостоятельной регистрации пользователей МСК при помощи кодов приглашений. Для управления кодами приглашений используется пункт меню **«Загрузчик»**. В окне отображается таблица кодов приглашений в соответствии с рисунком 2.206, которая состоит из следующих столбцов:



Дата создания	Код	Статус	Действителен до	ФИО	Пользователь домена	Принадлежность	Стратегия
28.02.2023	197867029	Действителен	28.02.2023	Басочин Петр Викторович	-	Личная	Личный рабочий профиль (Android 7.0+)
28.02.2023	398734191	Действителен	28.02.2023	-	-	Личная	Личный рабочий профиль (Android 7.0+)

Рисунок 2.206 — Окно «Загрузчик»

- Дата создания — отображает дату создания кода приглашения;
- Код — отображает значение кода;
- Статус — отображает состояние кода приглашения;
- Действителен до — отображает дату истечения срока действия кода приглашения;
- ФИО — отображает фамилию, имя и отчество сотрудника, которому присвоен код приглашения;
- Пользователь домена;
- E-mail,
- Принадлежность — признак собственности МСК (корпоративное / личное);
- Стратегия — способ управления устройством Android. Возможны варианты:
 - Автоматический выбор управления — монитор автоматически выбирает стратегию в зависимости от полученных привилегий;
 - Только устройство (Android) — требует наличия у монитора привилегий владельца устройства (Device Owner) или привилегий KNOX, и администратора устройства. Применима для всех поддерживаемых версий Android;
 - Устройство и контейнер KNOX (Samsung 5.0 — 9) — требует наличия у монитора привилегий KNOX и администратора устройства (Device Admin). Применима для МСК Samsung с версией Android начиная с 5.0 по 9.0;
 - Корпоративный рабочий профиль (Android 11.0+) — требует наличия у монитора привилегий владельца профиля (Profile Owner). Применима для МСК с версией Android 11.0 и выше. На МСК Samsung при

отсутствии у монитора привилегий KNOX Premium и MCK прочих производителей, применение правил управления приложениями, требует действий от пользователя. Требуется сброс устройства к заводским настройкам;

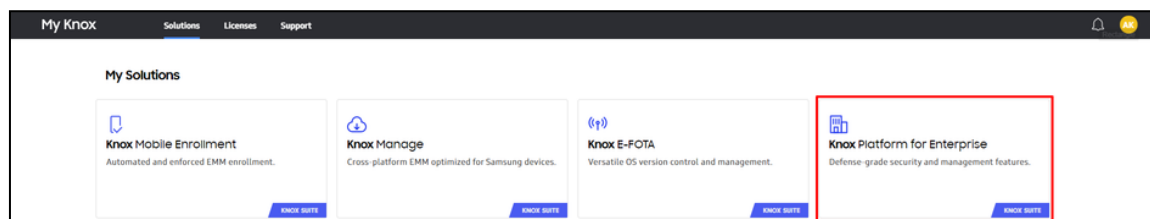
- Личный рабочий профиль (Android 7.0+) — требует наличия у монитора привилегий владельца профиля (Profile Owner). Применима для MCK с версией Android 7.0 и выше. На MCK Samsung при отсутствии у монитора привилегий KNOX Premium и MCK прочих производителей, применение правил управления приложениями, требует действий от пользователя.
- Шаблон QR — наименование шаблона QR.

Примечание

Чтобы получить привилегии KNOX Premium, необходимо выполнить следующие действия:

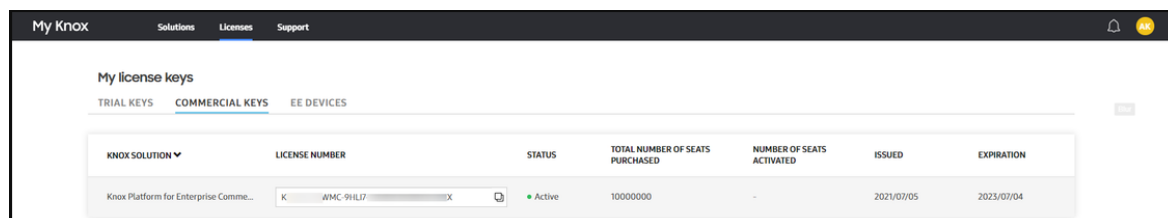
1. Перейти по ссылке: samsungknox.com со своей учетной записью, или создать новую (нужен рабочий email, публичные не принимаются).

2. Нажать на блок «Knox Platform for Enterprise».



3. Через некоторое время появится сообщение, что коммерческий ключ успешно сгенерирован.

4. Новый ключ отобразится на странице Licenses в разделе Commercial Keys.



В таблице имеется возможность отображения кодов приглашений в зависимости от статуса. Для этого следует нажать кнопку «Отображать со статусом», после чего раскрывается меню со следующими пунктами (рисунок 2.207):

- Новый код — созданный Администратором код, который пока не был использован сотрудником-абонентом МСК;
- Подготовка к установке — выполняется подготовка к установке мобильного клиента SafeMobile на МСК;
- Деактивирован — код деактивирован в результате истечения срока действия или принудительной деактивации Администратором;
- Клиент успешно установлен — мобильный клиент SafeMobile успешно установлен на МСК.

Для выбора статуса кода следует установить флажок в выбранной строке. По умолчанию в таблице показываются все коды приглашений без фильтрации (флажки в раскрывающемся меню «Отображать со статусом» сняты).

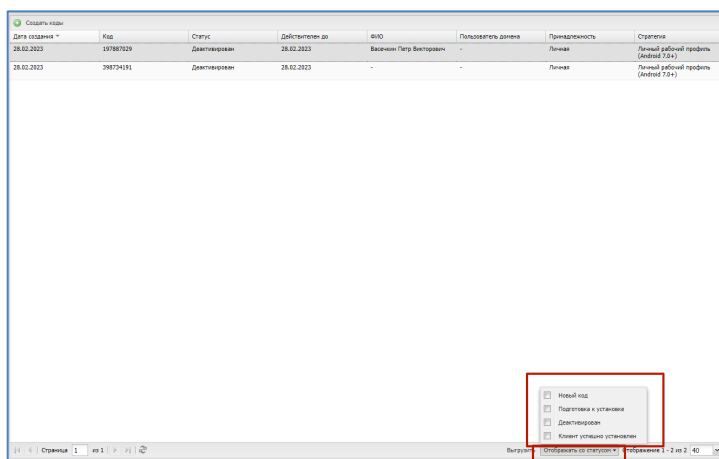


Рисунок 2.207 — Фильтрация по статусам кода приглашения

«UEM SafeMobile» позволяет настраивать коды приглашения по таким параметрам как:

- Длина кода,
- Наличие цифр,
- Наличие прописных букв (A-Z),
- Наличие строчных букв (A-Z),
- Наличие спецсимволов,
- Срок действия (минуты),
- Исключить символы.

Для изменения этих параметров следует нажать кнопку «Настройки кодов приглашения» в верхней части экрана, после чего откроется окно настроек кодов. При внесении изменений следует отслеживать результирующий показатель «Энтропия кода приглашения (бит)», он не должен быть ниже 30 бит. Показатель «Алфавит» отображает набор символов, который будет использоваться при генерации кода приглашения.

После внесения изменений в настройки кодов приглашения следует нажать кнопку «Сохранить», после чего настройки вступят в силу при генерации последующих кодов.

2.10.1.1 Создание кода приглашения

В верхней части окна расположена кнопка **«Создать коды»**, при нажатии которой открывается окно для создания кодов приглашений (рисунок 2.208)

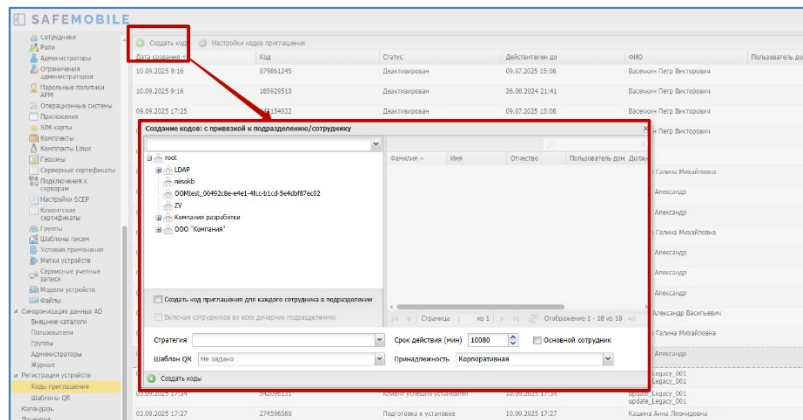


Рисунок 2.208 — Окно «Создание кодов»

Для создания кода приглашения для зарегистрированного сотрудника необходимо выполнить следующие действия:

1. Выбрать подразделение и сотрудника, для которого создается приглашение. С помощью «поиска» можно найти сотрудника по таким параметрам как:
 - Фамилия,
 - Имя,
 - Отчество,
 - Пользователь домена,
 - Должность.
2. Указать срок действия кода, после истечения которого действие кода будет прекращено (в поле **«Срок действия, мин»**).
3. Выбрать принадлежность и стратегию. Стратегия будет применяться только для MCK Android.
4. Выбрать шаблон QR, заданный в разделе «Шаблоны QR».
5. Включить чекбокс если выбранный сотрудник является основным.
6. Затем следует нажать кнопку **«Создать коды»**, расположенную в нижней части окна **«Создание кодов»** в соответствии с рисунком 2.209. После подтверждения действия будет создан новый код приглашения, и запись о нем добавится в таблицу кодов со статусом **«Новый код»**.

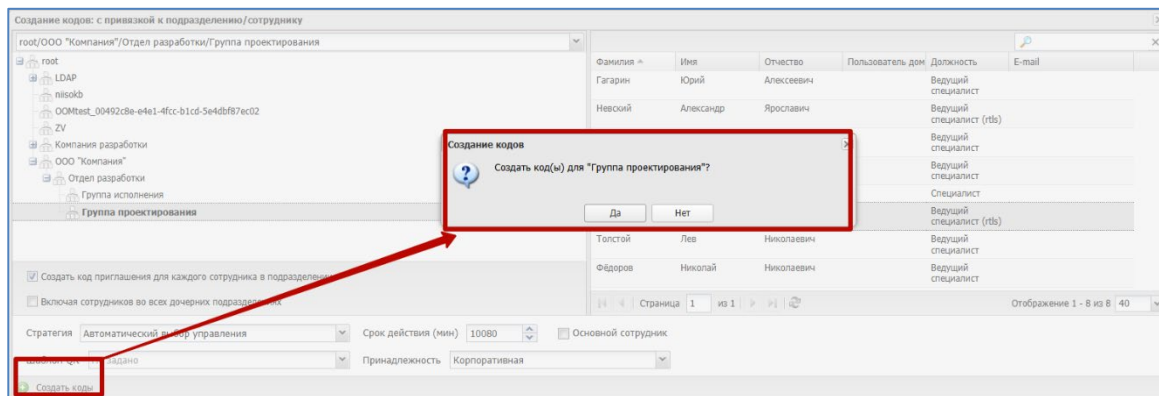


Рисунок 2.209 — Создание кодов с привязкой к сотруднику

«UEM SafeMobile» позволяет создавать коды приглашения для всех сотрудников, относящихся к одному подразделению или организации в целом. Для этого необходимо выбрать требуемое подразделение в списке слева и установить флажок **«Включая сотрудников во всех дочерних подразделениях»**, если требуется для всех подчиненных сотрудников (рисунок 2.210).

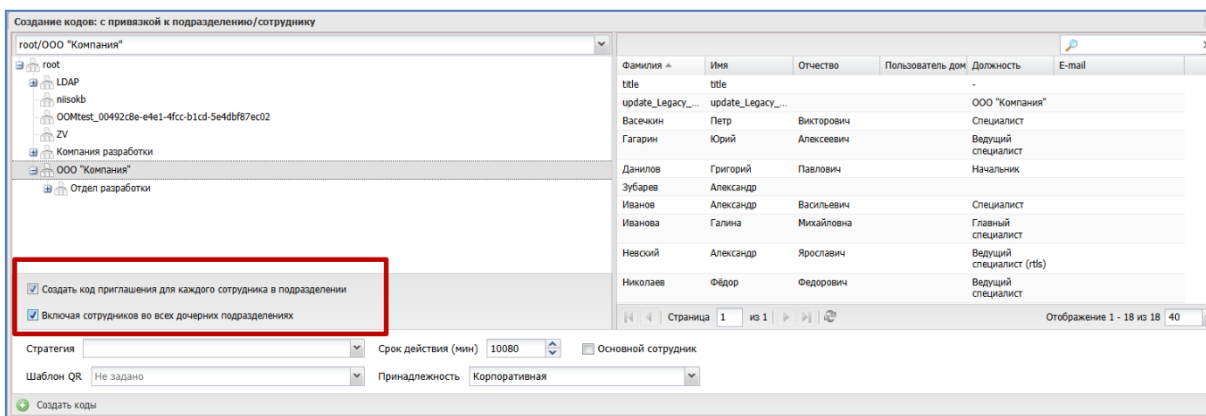


Рисунок 2.210 — Создание кодов с привязкой к подразделению

После нажатия кнопки **«Создать коды»** будут созданы новые коды приглашения и записи о них добавятся в таблицу кодов со статусом **«Новый код»**.

После этого Администратор выбирает запись с новым кодом в соответствии с рисунком 2.211, копирует QR-код (клик по картинке QR-кода) и сохраняет в файл (на рисунке QR-код приведен условно). Далее Администратор рассылает файлы с QR-кодами

требуемым сотрудникам и разрешает им выполнять самостоятельную регистрацию своих устройств в системе.

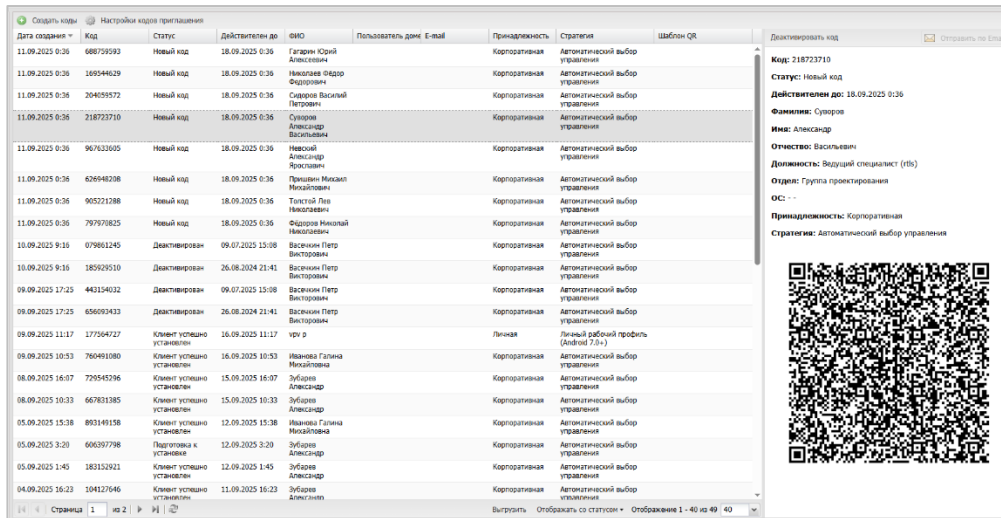


Рисунок 2.211 — Выбор записи с новым кодом

Во время регистрации Администратор следит за статусом этой операции в столбце **«Статус»**. В зависимости от статуса кода Администратор может осуществлять следующие действия, выбрав в таблице код приглашения (рисунок 2.212):

- Деактивировать код — действие доступно только кодов со статусом «Новый». При нажатии кнопки код перестает действовать и получает статус «Деактивирован»;
- Отправить по Email. Только для кодов в статусе «Новый код» и при наличии у сотрудника заполненного Email.

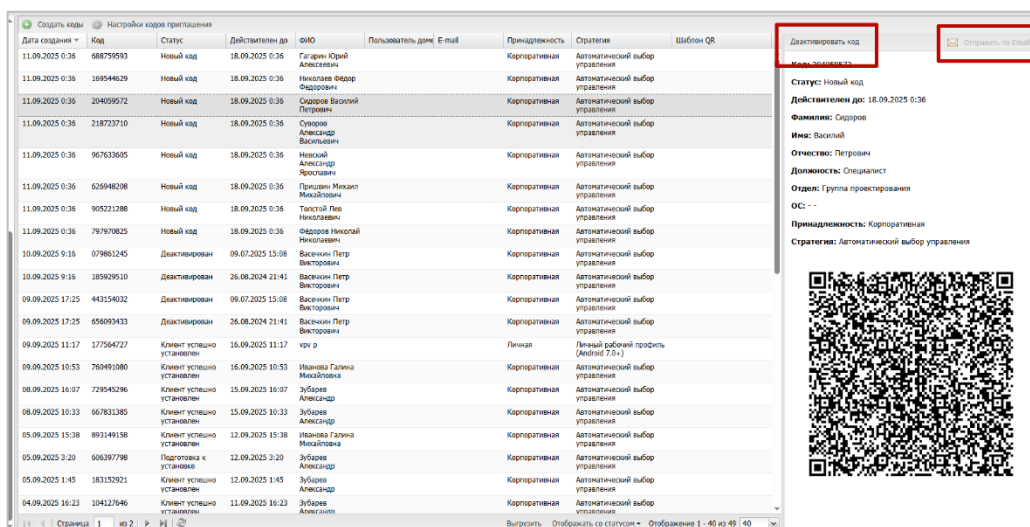


Рисунок 2.212 — Меню «Выбрать действие»

2.10.2 Шаблоны QR

Раздел предназначен для управления шаблонами QR-кодов используемых для регистрации устройств Android. В шаблоне определяются сетевые параметры, которые передаются устройству при сканировании кода. В зависимости от настроек шаблона, устройство может подключиться для регистрации:

- Через мобильный интернет (сеть оператора связи SIM-карты).
- Через беспроводную локальную сеть (Wi-Fi).

В центральной части экрана представлен список созданных шаблонов QR (рисунок 2.213).

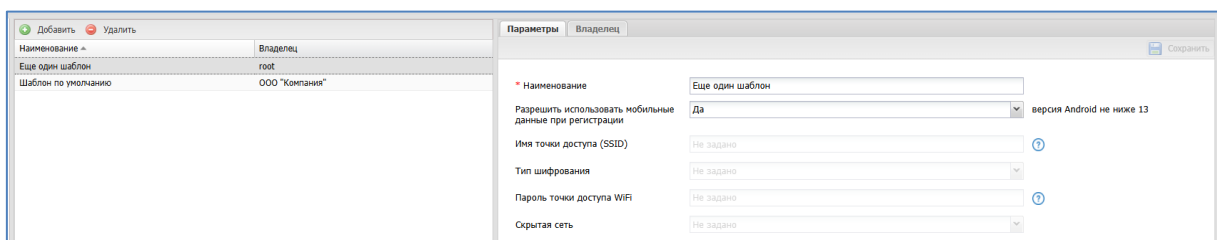


Рисунок 2.213 — Раздел «Шаблоны QR»

Каждая строка списка содержит:

- Наименование — наименование шаблона;
- Владелец — владелец шаблона в ОШС.

В правой части отображаются параметры выбранного в списке шаблона QR. Каждый шаблон имеет следующие настройки и параметры:

- Вкладка «Параметры»:
 - Наименование — наименование шаблона (обязательно для заполнения);
 - Разрешить использовать мобильные данные при регистрации (Да/Нет/Не задано) — параметр задает разрешение/запрет на использование мобильной сети устройства для регистрации;
 - Параметры сети Wi-Fi — доступны если параметр «Разрешить использовать мобильные данные при регистрации» указан как «Нет»:
 - Имя точки доступа (SSID),
 - Тип шифрования,
 - Пароль точки доступа WiFi,

- Скрытая сеть.
- Вкладка «Владелец» — позволяет указать/сменить владельца шаблона в дереве ОШС.

Для создания шаблона QR необходимо выполнить следующие действия:

1. В разделе «Шаблону QR» нажать кнопку «Добавить».
2. Заполнить параметры в правой части экрана.
3. Во вкладке «Владелец» указать узел ОШС как владельца шаблона (опционально).
4. Нажать кнопку «Сохранить».

Для удаления шаблона QR необходимо выбрать его в списке шаблонов и нажать кнопку «Удалить». После подтверждения операции шаблон будет удален. Если удаленный шаблон использовался в кодах приглашения, то в этих кодах параметр «Шаблон QR» будет указан как «не задано».

2.11 Корпоративный календарь рабочего времени (пункт меню «Календарь»)

Раздел главного меню «Календарь» позволяет создавать и назначать календарь рабочего времени как отдельному сотруднику, так и подразделению, а также настроить правила календаря.

Примечание

Создание календаря рабочего времени необходимо для определения местоположения сотрудников, которое может производиться только в рабочее время.

При выборе в главном меню раздела «Календарь» в левой части открывшегося окна отображается список подразделений организации и их сотрудников, а в правой части окна — календарь рабочего времени выбранного подразделения или сотрудника в соответствии с рисунком 2.214.

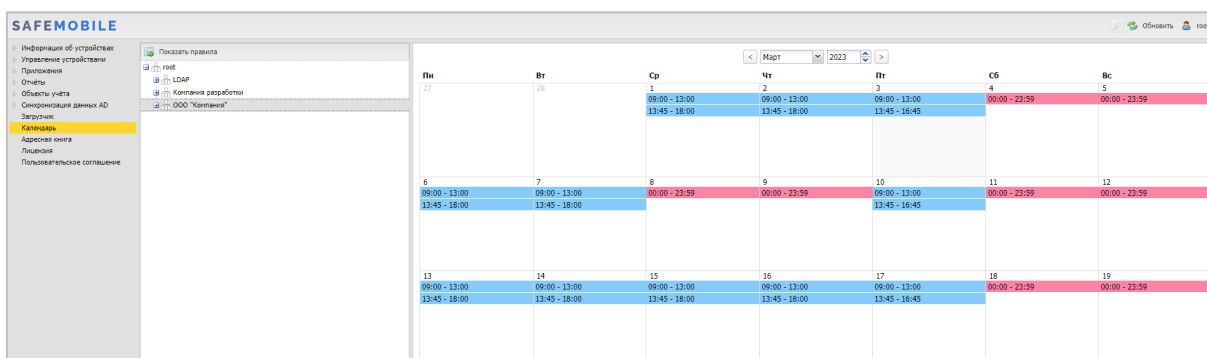



Рисунок 2.214 — Календарь рабочего времени

Для просмотра рабочего времени подразделения или сотрудника в текущем месяце выберите запись о сотруднике или подразделении в таблице слева, после чего в правой части окна отобразится календарь его рабочего времени. Для каждой даты в текущем месяце отображается диапазон рабочего времени (синим цветом) или нерабочее время (красным цветом).

Раскрывающийся список  в верхней части календаря позволяет выбирать требуемый месяц и год.

В системе предусмотрена возможность создания правил для формирования календаря рабочего времени сотрудника, подразделения или организации в целом. Чтобы

открыть окно создания правил и управления ими, нажмите кнопку «Показать правила» в верхней части списка сотрудников и кнопку, после чего отобразится окно в соответствии с рисунком 2.215.

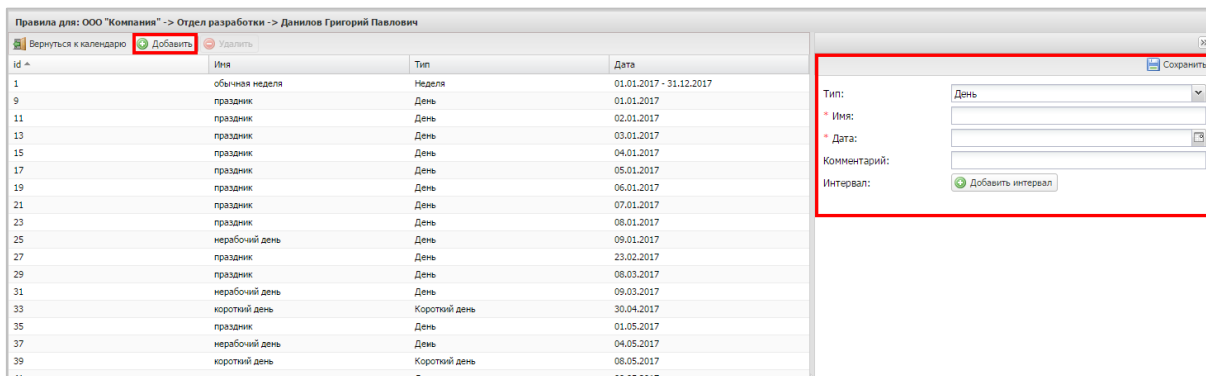


Рисунок 2.215 — Окно создания правил календаря рабочего времени

В левой части открывшегося окна расположена таблица, отображающая список правил, имеющихся в системе для выбранного сотрудника или подразделения. Для просмотра параметров правила выберите строку с правилом в таблице, после чего в правой части окна отобразятся параметры этого правила (рисунок 2.216).

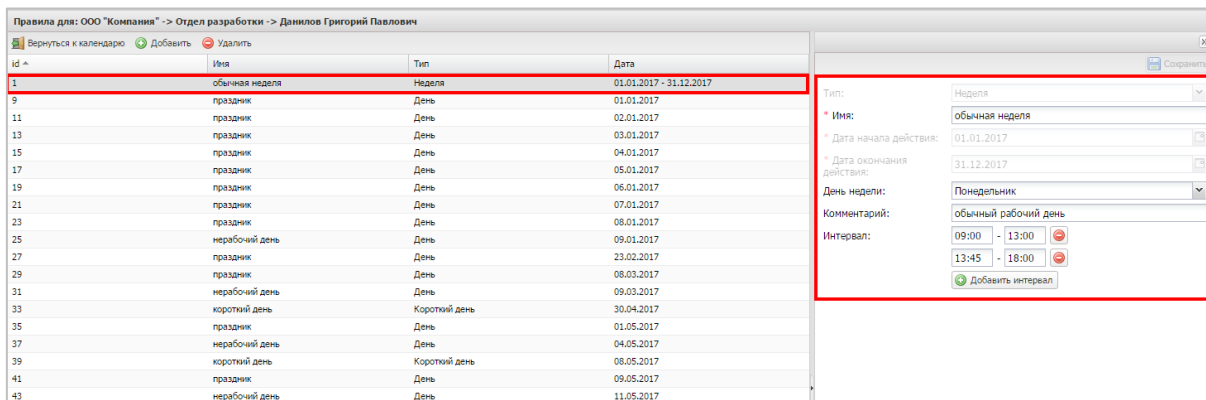


Рисунок 2.216 — Просмотр правила календаря рабочего времени

В системе предусмотрены три типа правил для формирования календаря рабочего времени:

Неделя (регулярное правило) — правило, которое описывает расписание для всей недели целиком. При его создании необходимо обязательно указать интервалы рабочего времени для всех семи дней недели. Каждое такое правило задаёт полное расписание на неделю. Если для одного и того же периода действует несколько правил "Неделя", то действующим будет считаться последнее из применённых правил, которое полностью перекрывает предыдущие правила "Неделя" для своего периода действия.

Такой тип правил применяется для быстрого указания стандартного рабочего времени на длительные промежутки, например, на год.

День (нерегулярное правило) — правила для конкретной даты или диапазона дат. Такой тип правил применяется для указания интервала рабочего времени, отличного от заданного при помощи регулярного правила. Например, когда необходимо обозначить в календаре время командировки, отпуска и т.д.

Короткий день (нерегулярное правило) — при применении этого правила для конкретной даты последний интервал рабочего времени сокращается на один час. Создание правил сокращенного дня для диапазона дат недоступно. Такой тип правил применяется для обозначения в календаре предпраздничных дней на конкретные даты.

Для каждого дня правила можно задать до четырёх интервалов рабочего времени.

Каждое правило имеет срок действия:

- для нерегулярных правил срок действия составляет один год, в рамках которого они заданы (от 01 января по 31 декабря);
- регулярные правила требуют явного указания даты начала и даты окончания действия.

Правила календаря рабочего времени применяются в следующей последовательности:

1. Правила рабочего времени применяются в соответствии с организационно-штатной структурой (ОШС) предприятия. Первыми применяются правила компаний (корневых узлов дерева ОШС). Затем последовательно накладываются правила подразделений. Последними применяются правила конкретных сотрудников.

2. При наличии нескольких правил для компании/подразделения/сотрудника, они применяются в соответствии со временем их добавления. Последние добавленные правила применяются последними.

3. Сначала применяются регулярные правила, затем — нерегулярные. То есть правила сотрудника применяются следующим образом:

- регулярные правила всех вышестоящих узлов ОШС, начиная с подразделения, в котором работает сотрудник (от старших к младшим),
- регулярные правила сотрудника,
- нерегулярные правила ОШС,
- нерегулярные правила сотрудника.

4. В процессе применения правил происходит их замещение. При этом одно правило замещает другое для каждой конкретной даты, а не для всего диапазона действия. В частности, правило типа "Неделя" замещает предыдущие регулярные правила для всех дней в рамках своего периода действия.

2.11.1 Создание правил

При создании правил необходимо указать к какому узлу ОШС (компания, подразделение) или сотруднику они относятся. Для этого нужно выбрать необходимый элемент в окне календаря.

Чтобы начать создание правила, нажмите кнопку **«Добавить»** в верхней панели инструментов, после чего в правой части окна отобразятся поля, предназначенные для заполнения в соответствии с рисунком 2.217. Целесообразно начинать создание правил для организации с создания недельного правила для корневого подразделения ОШС (головного подразделения организации), а затем можно создавать нерегулярные правила, приоритет которых выше.

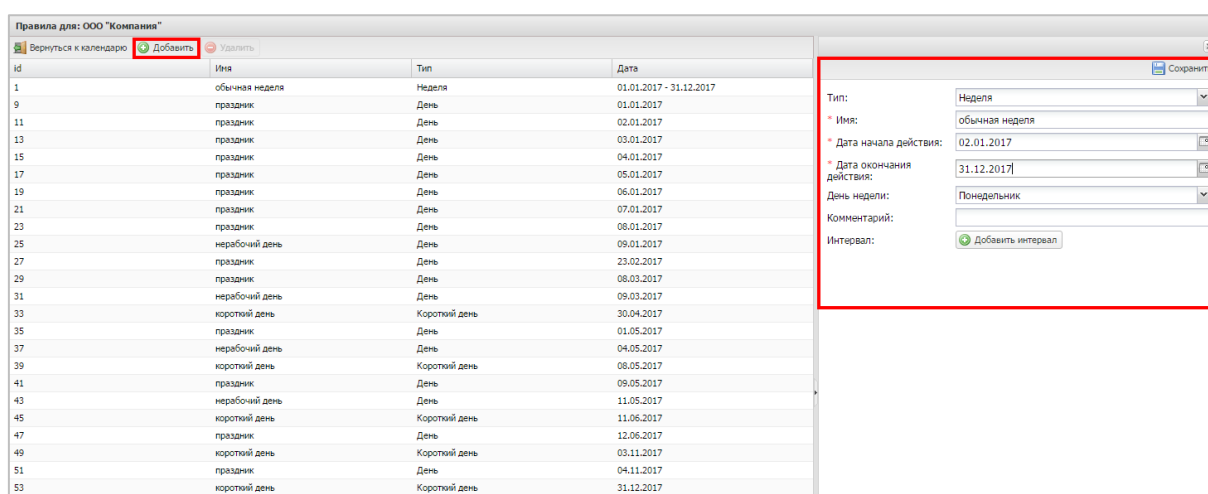



Рисунок 2.217 — Создание правила календаря рабочего времени типа «Неделя»

Для создания правила типа **«Неделя»** необходимо указать следующие обязательные параметры:

- Имя — наименование правила;
- Дата начала действия — выбрать в раскрывающемся календаре дату начала действия правила, например, день начала календарного года в организации;
- Дата окончания действия — выбрать в раскрывающемся календаре дату окончания действия правила, например, последний день календарного года в организации.

После указания и сохранения обязательных параметров правил календаря типа **«Неделя»** все дни указанного диапазона дат будут считаться выходными. Чтобы добавить рабочие дни в календарь, необходимо в раскрывающемся списке **«День недели»**

выбрать дни недели, которые будут рабочими (обычно это **Понедельник, Вторник, Среда, Четверг и Пятница**), и указать для каждого рабочего дня промежуток рабочего времени, например, с 10:00 до 19:00. Для добавления интервала времени используется кнопка **«Добавить интервал»**, после нажатия которой необходимо заполнить поля начала рабочего дня и его окончания. Для корректного заполнения этих полей время необходимо вводить в формате **«ЧЧ: ММ»**, при этом часы должны быть в диапазоне от 00 до 23, минуты — от 00 до 59. Разделитель часов и минут — символ двоеточия. Для удаления неиспользуемого диапазона времени используется кнопка .

При создании правила календаря можно добавить комментарий к нему. После завершения создания правила календаря его необходимо сохранить, нажав кнопку **«Сохранить»** в верхней панели инструментов.

При создании правила типа **«День»** (рисунок 2.218) необходимо указать следующие обязательные параметры:

- **Имя** — наименование правила;
- **Дата** — дата, к которой будет привязано правило.

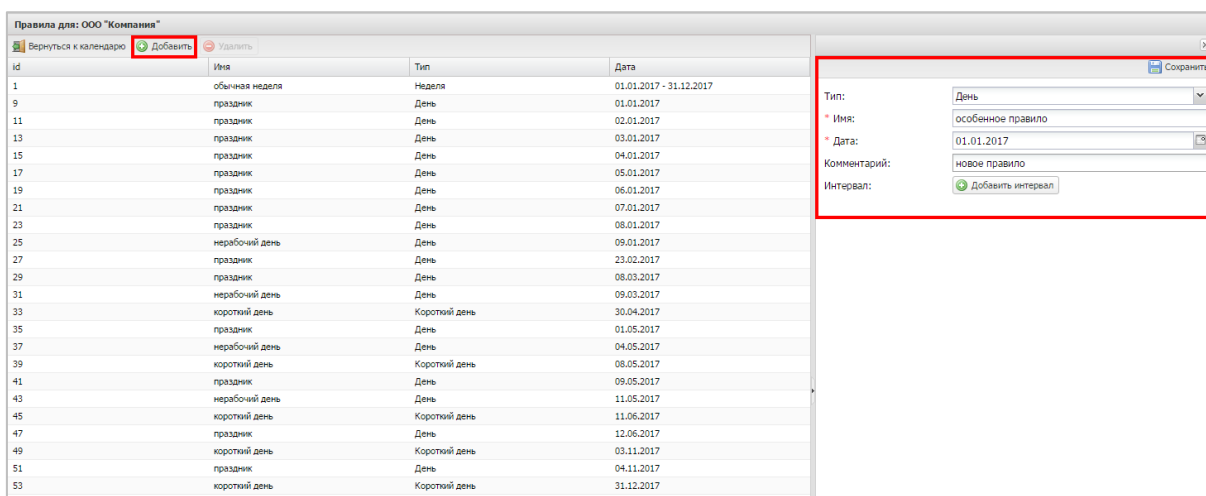


Рисунок 2.218 — Создание правила календаря рабочего времени типа «День»

Кроме того, можно записать комментарий в соответствующем поле и выбрать интервал времени (или несколько интервалов) в течение дня, когда будет действовать создаваемое правило.

Затем можно выбрать интервал времени (заполнив поле **«Интервал»**), если требуется указать в качестве нерабочего времени только часть дня.

Такой тип правил применяется для указания интервала рабочего времени, отличного от заданного при помощи регулярного правила (типа «**Неделя**»). Например, когда необходимо обозначить в календаре время командировки, отпуска и т.д.

Для создания правила типа «**Короткий день**» (рисунок 2.219) необходимо указать следующие обязательные параметры:

- **Имя** — название создаваемого правила;
- **Дата** — дата, к которой будет привязано правило.

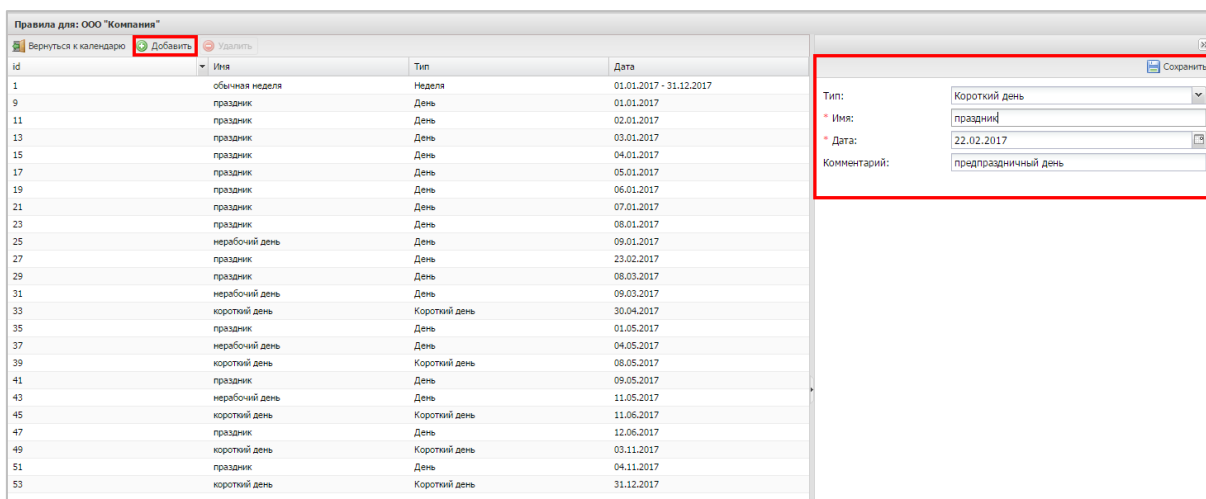


Рисунок 2.219 — Создание правила календаря рабочего времени типа «Короткий день»

Такой тип правил календаря позволяет указать в календаре дни, у которых последний интервал рабочего времени сокращён на один час.

Для сохранения созданного правила, нажмите кнопку «**Сохранить**».

2.11.2 Изменение правил

После создания правил с ними можно совершать следующие действия:

- изменить временной интервал,
- добавить новый интервал,
- удалить интервал,
- изменить наименование,
- добавить или изменить комментарий.

Примечание

Изменение правила приводит к его изменению в течение всего срока действия, независимо от даты внесения изменений. История изменений правил не поддерживается. Если изменить правило на третий день его действия, то для дней, в течение которых действовало неизменённое правило, будет отображаться правило с внесёнными изменениями. Тип правила и срок действия правила изменять после создания нельзя.

2.11.3 Удаление правила

Удаление правила приводит к удалению связи между правилом и элементом, к которому оно относится (компания/подразделение/сотрудник). Само правило при этом не удаляется.

Чтобы удалить выбранное правило календаря, нажмите кнопку **«Удалить»** в верхней панели инструментов в соответствии с рисунком 2.220.

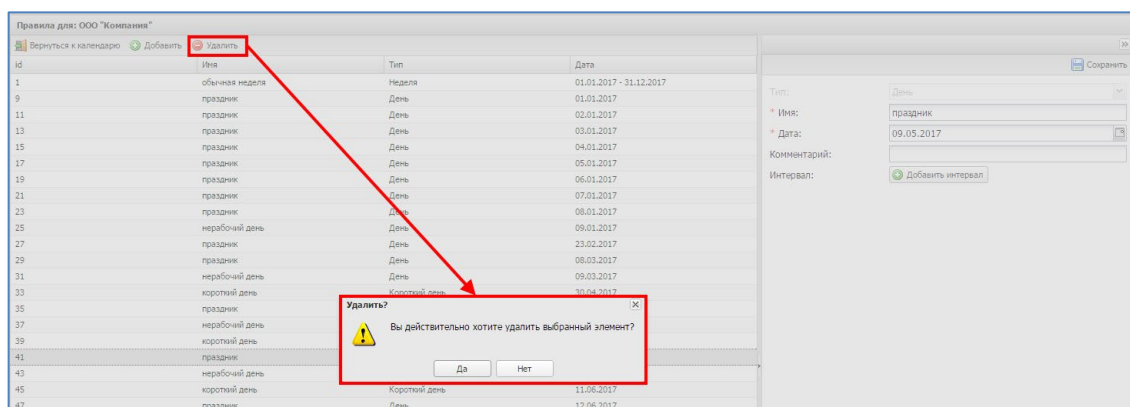


Рисунок 2.220 — Удаление правила календаря рабочего времени

После этого подтвердите действие, нажав **«Да»** в появившемся окне.

2.12 Контроль за лицензией на «UEM SafeMobile» (пункт меню «Лицензия»)

Пункт главного меню «**Лицензия**» предназначен для активации лицензии на использование системы и формирования отчета по числу подключенных устройств (см. раздел 2.14.1).

Для активации лицензии необходимо информацию из полученного лицензионного файла поместить в поле окна «**Лицензия**» (рисунок 2.221), которое является обязательным для заполнения. Затем нажать кнопку «**Сохранить**».

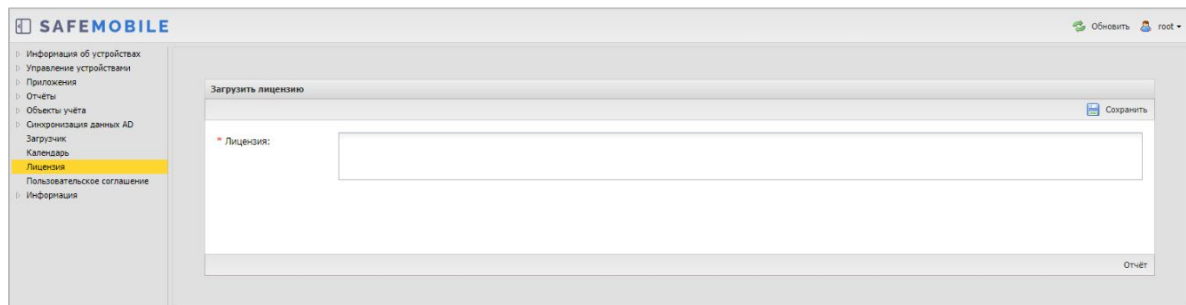


Рисунок 2.221 — Окно «Лицензия»

После проверки системой, при успешной загрузке лицензии, внизу интерфейса отобразится информация, например, «Лицензия для ООО «Кантор» на 100 устройств(а), использовано 10, действует с 30.10.2017 по 30.12.2018».

В случае нарушений условий лицензии или ее отсутствия интерфейс всех администраторов АРМ будет ограничен разделами «Лицензия» и «Управление устройствами — Команды», для возможности отключения устройств от системы. В нижней строке интерфейса отобразится предупреждающее сообщение красного цвета. Текст сообщения, в зависимости от предупреждения, может быть следующим (название юридического лица приведено условно):

- Отсутствует лицензия на использование системы. Для получения лицензии следует обратиться к поставщику,
- Лицензия для ООО «Кантор» действует с 30.10.2020 (в случае, если срок действия лицензии еще не наступил),
- Лицензия для ООО «Кантор» истекла 30.10.2019. Для продления лицензии обратитесь к поставщику.

Когда число подключенных комплектов достигнет числа комплектов в лицензии, подключение новых МСК будет блокироваться.

Когда до истечения срока действия лицензии остается 1 месяц, внизу интерфейса отобразится предупреждающее сообщение красного цвета: «Заканчивается срок действия лицензии, через 29 дней доступ в APM будет заблокирован».

Для обновления истекшей лицензии на лицензию с меньшим количеством устройств необходимо, чтобы на момент активации лицензии количество подключенных устройств не нарушало новое лицензионное соглашение. Если подключенных устройств будет больше, чем в лицензии, новая лицензия активирована не будет. Для активации лицензии необходимо отключить от управления избыточные комплекты.

2.12.1 Отчет по подключенным устройствам

Чтобы сформировать отчет о подключенных устройствах необходимо выполнить следующие действия:

1. В разделе «Лицензии» нажать кнопку «Отчет», после чего откроется диалоговое окно указания периода, за который следует сформировать отчет (рисунок 2.222).

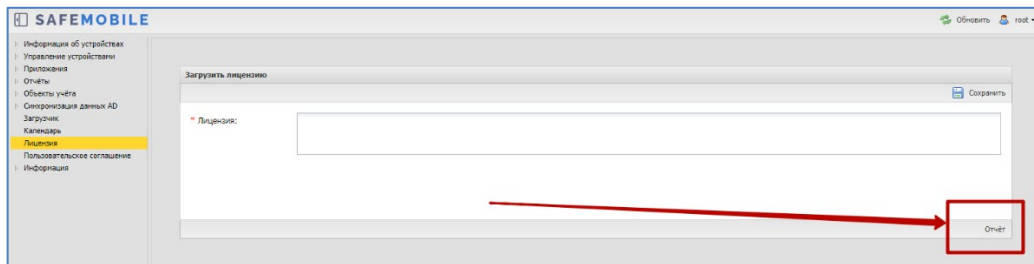


Рисунок 2.222 — Расположение кнопки «Отчет»

2. Указать даты начала и конца периода и нажать кнопку «Выгрузить» (рисунок 2.223).

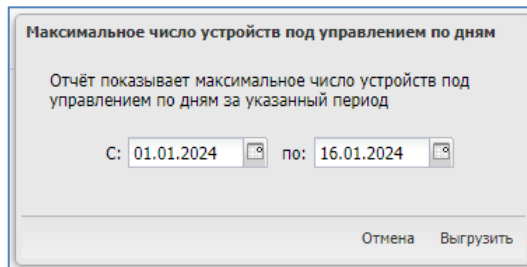


Рисунок 2.223 — Диалоговое окно указания периода формирования отчета

3. Дождаться сообщения о готовности файла и нажать кнопку «Скачать».

Отчет представлен в виде excel таблицы с вкладками:

- Параметры — сводные данные об отчете,
- Данные — данные о максимальном количестве подключений в день, за указанный период.

Примечание

Отчет не покажет данные в таких случаях как:

- *За период работы версии ниже 8.3.
При выгрузке отчета за период работы версии 8.2 для каждой даты подключения в отчете будет указано «нет данных».*
- *Устройства бывшие под управлением менее 1 часа не попадут в отчет, если их добавление пришлось с НН:01 по НН:59 (то есть не был совершен запрос со стороны БД).*

2.13 Управление пользовательским соглашением

Пункт главного меню **«Пользовательское соглашение»** предназначен для заключения с пользователем устройства соглашения об условиях управления системой МСК на платформах Android и iOS. Для этого необходимо текст пользовательского соглашения, длиной не более 100000 символов, поместить в поле окна **«Пользовательское соглашение»** (рисунок 2.224), затем установить флажок в строке **«Показывать ПС на портале регистрации пользователя»** и нажать кнопку **«Сохранить»**. В этом случае предложение о принятии условий пользовательского соглашения отобразится на устройстве пользователя при регистрации МСК в «UEM SafeMobile».

Если МСК уже зарегистрировано в системе или при изменениях в соглашении, после сохранения текста для отправки соглашения на МСК, следует нажать кнопку **«Отправить на устройства»**.

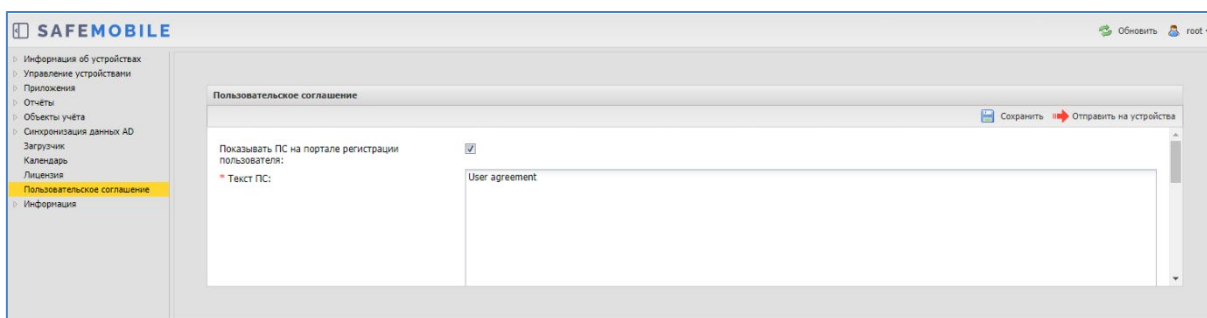


Рисунок 2.224 — Окно «Пользовательское соглашение»

2.14 Информация

2.14.1 Компоненты

В данном разделе отображается список подключенных к базе данных компонентов системы. Каждая строка списка отображает данные об одном экземпляре компонента и содержит следующие данные (рисунок 2.225):

Компонент	Версия	Время запуска	Последняя активн	Подключения	Идентификатор хост
adagent	14.0-1-g14671c2	21.07.2025 11:09:18	24.07.2025 15:40:51	2	10.17.2.250
apple-mdm-push	14.0-6-9a099458	22.07.2025 16:13:27	24.07.2025 15:40:48	2	10.17.2.196
apple-monitor-push	14.0-6-9a099458	22.07.2025 16:13:27	24.07.2025 15:40:48	2	10.17.2.196
art	14.0-1971-q1886e6	22.07.2025 12:31:57	24.07.2025 15:40:51	18	10.17.2.250
art	14.0-manual	24.07.2025 08:39:12	24.07.2025 15:40:48	41	10.17.2.254
art	14.0-manual	24.07.2025 08:39:12	24.07.2025 15:40:48	25	10.17.2.254
art	14.0-manual	24.07.2025 14:43:57	24.07.2025 14:43:59	18	10.17.2.238
art	14.0-manual	24.07.2025 14:59:50	24.07.2025 15:00:29	1	10.17.2.181
art	14.0-9586-q81dats	24.07.2025 15:22:46	24.07.2025 15:40:49	13	10.17.2.197
bgworker	14.0-1-94c0f32	21.07.2025 11:09:18	24.07.2025 15:40:51	10	10.17.2.250
ca	13.6-3-gf51107a	21.07.2025 11:09:21	24.07.2025 15:40:51	2	10.17.2.197
fcm-push	13.6-3-g880c565	21.07.2025 11:09:30	24.07.2025 15:40:51	2	10.17.2.197
file-distr-server	13.6-3-g01e1d87	21.07.2025 11:09:17	24.07.2025 15:40:50	2	10.17.2.196

Рисунок 2.225 — Подключенные компоненты

- Компонент — название компонента:
 - *adagent* — Агент синхронизации с контроллером домена LDAP;
 - *apple-mdm-push* — Сервис отправки пуш уведомлений клиенту MDM iOS;
 - *art* — Консоль управления администратора;
 - *bgworker* — Сервис асинхронной обработки событий (Android). А так же обеспечивает автоматическое удаление в БД устаревших данных;
 - *ca* — Сервис УЦ SafeMobile;
 - *fcm-push* — Сервис отправки пуш уведомлений FCM (Android);
 - *file-distr-server* — Сервер раздачи корпоративных приложения и файлов;
 - *mdm* — Сервер управления (Android, iOS, Windows и АврораОС);
 - *apple-monitor-push* — Сервис отправки пуш уведомлений монитору;
 - *lmsrv* — Сервер управления (Linux);
 - *mail-agent* — Сервис отправки почты;
 - *nginx*,
 - *regportal* — Портал саморегистрации устройств;
 - *sber-ca-agent* — Сервис подключения к корпоративному УЦ (SberCA);
 - *scer* — Сервер SCEP (устанавливается вместе с MDM и использует те же порты);
 - *bgworker* — Планировщик (периодическая очистка);
 - *sesl* — Сервис отправки системных логов;

- *smapi* — Сервер публичного API;
 - *command-server* — Сервер команд (Android);
 - *winmdm* — Сервер управления (Windows);
 - *scim* — Сервер SCIM.
-
- Время запуска — дата и время запуска экземпляра компонента;
 - Последняя активность — дата и время последних действий экземпляра компонента;
 - Подключения — количество подключений одного экземпляра компонента;
 - Идентификатор экземпляра — уникальный ID экземпляра. Идентификатор генерируется при каждом старте экземпляра компонента;
 - IP — IP адрес экземпляра,
 - Назначенная конфигурация — показывает название конфигурации, назначенной через APM.
 - Тег компонента — показывает тег конфигурации экземпляра (например, default).

Примечание

- *Если время работы компонента меньше 1 минуты, то допустимо кратковременное отсутствие компонента в списке. Если, при этом, время старта не меняется, то контейнер не перезагружался и проблем в соединении с БД у контейнера нет.*
- *Компоненты обслуживания windows и Linux не отображаются.*
- *Компоненты без заданного тега конфигурации не могут быть управляемыми через команды «Рестарт» и «Перезагрузка конфигурации».*
- *Система автоматически удаляет записи о неактивных экземплярах компонентов (неактивных более суток) для поддержания актуальности списка.*

Управление экземплярами компонентов

Для каждого экземпляра компонента доступны следующие команды управления:

Доступные команды:

- Рестарт — останавливает и автоматически перезапускает выбранный экземпляр компонента.

- Перегрузка конфигурации — применяет обновлённые настройки без перезапуска компонента (например, параметры логирования).

Условия выполнения команд:

1. В таблице выбран конкретный экземпляр компонента.
2. У экземпляра задан тег конфигурации (колонок «Тег компонента» не пустая).
3. Администратор имеет соответствующие права доступа:
 - «Информация → Компоненты → Рестарт»
 - «Информация → Компоненты → Перегрузка конфигурации»

Примечание

Если для экземпляра уже назначена команда, новая команда заменит предыдущую.

Просмотр конфигураций экземпляра

При выборе экземпляра компонента доступно окно просмотра конфигураций, содержащее две вкладки:

- Вкладка «Назначенная конфигурация»:
 - Отображает YAML-конфигурацию, назначенную через раздел «Настройки» → «Конфигурации компонентов».
- Вкладка «Применённая конфигурация»:
 - Показывает фактическую конфигурацию, которую использует экземпляр компонента.

Включает как настройки из назначенной конфигурации, так и параметры из файла конфигурации компонента (имеющие более высокий приоритет).

2.15 Настройки

2.15.1 Дополнительные атрибуты

Функционал данного раздела позволяет добавлять дополнительные поля (атрибуты) к записям о сотрудниках и администраторах. Поля, добавленные в этом разделе, будут отображаться (в таблицах и окнах редактирования) для следующих разделов системы:

Дополнительный атрибут для сотрудников:

- Информация об устройствах,
- Управление устройствами:
 - Команды,
 - Профили,
 - Правила несоответствия,
- Приложения:
 - Установленные приложения,
 - Правила управления,
 - Конфигурации,
- Отчеты:
 - Звонки и SMS,
 - События ИБ,
 - Перемещения,
 - Правила управления (UID),
 - Геозоны,
- Объекты учёта:
 - Сотрудники,
 - Комплекты,
 - Комплекты Linux,
 - Метки устройств,
- Загрузчик.

Дополнительный атрибут для администраторов:

- Объекты учёта:

○ Администраторы.

Основной рабочий экран раздела отображает список добавленных атрибутов к объектам учета — сотрудники или администраторы (рисунок 2.226). Каждая строка списка содержит следующие данные:

- Ключ — уникальный идентификатор поля в БД. После создания атрибута это параметр нельзя изменить;
- Наименование (рус) — название поля, в русской локализации, которое будет отображаться в системе;
- Наименование (анг) — название поля в английской локализации;
- Тип — тип данных, для данного поля (число или строка). После создания атрибута это параметр нельзя изменить;
- Обязательный — чекбокс, обязательно поле для заполнения или нет.

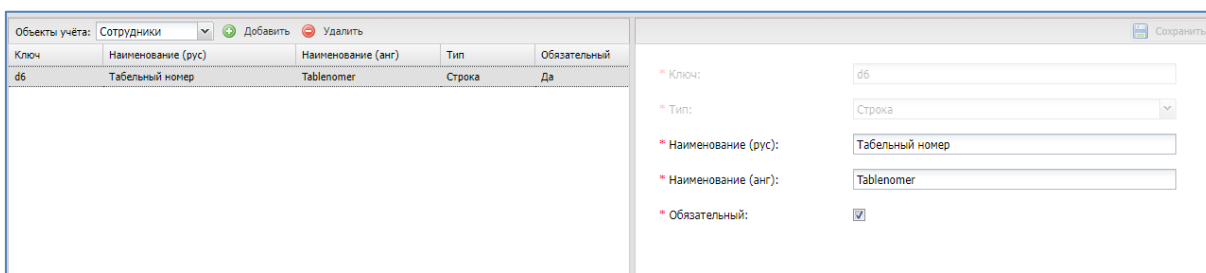


Рисунок 2.226 — Список дополнительных атрибутов для сотрудников

Чтобы добавить новый дополнительный атрибут, необходимо выполнить следующие действия:

1. Перейти в раздел «Дополнительные атрибуты».
2. Нажать кнопку «Добавить».
3. В правой части рабочего экрана заполнить поля данными.
4. Нажать кнопку «Сохранить», после чего дополнительный атрибут будет отображаться в соответствующих разделах системы (рисунок 2.227).

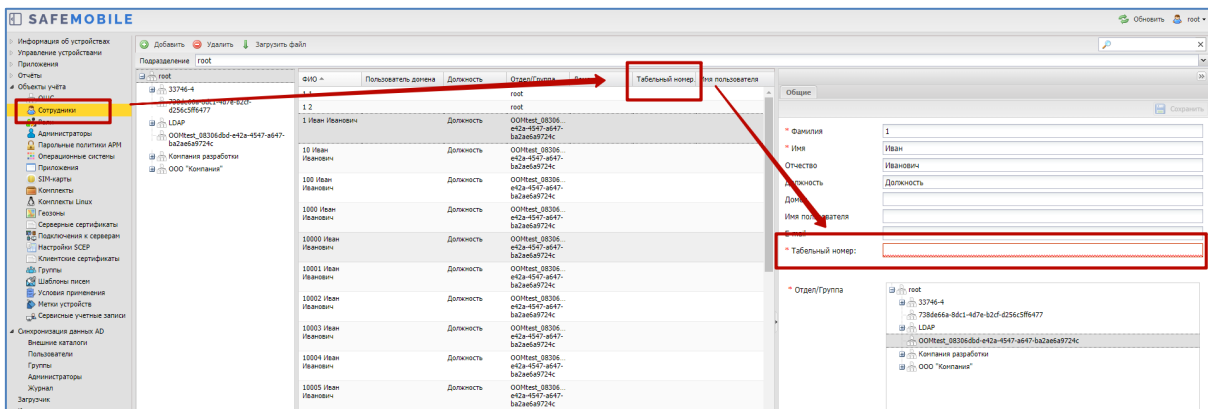


Рисунок 2.227 — Отображение дополнительного атрибута сотрудника в «Объектах учета»

Чтобы изменить параметры существующего атрибута, необходимо выбрать его в списке атрибутов, в правой части рабочего экрана внести изменения и нажать кнопку «Сохранить». Параметры доступны для редактирования:

- Наименование (рус),
- Наименование (ang),
- Обязательный.

Чтобы удалить дополнительный атрибут, необходимо выбрать его в списке основного рабочего экрана, нажать кнопку «Удалить» и подтвердить действие в модальном окне.

2.15.2 Периодическая очистка

Система предоставляет возможность выполнять автоматическую очистку базы данных, что позволяет не хранить в базе данных записи об устаревших событиях, произошедших в системе.

Настройка параметров автоматической очистки осуществляется в разделе «Периодическая очистка» (рисунок 2.228) и содержит следующие параметры:

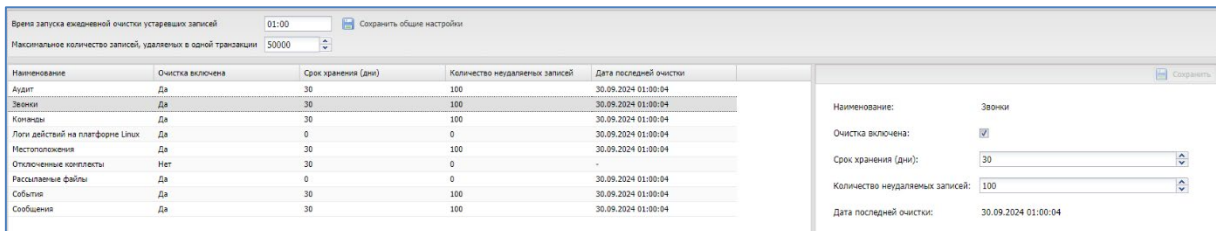


Рисунок 2.228 — раздел «Периодическая очистка»

Общие настройки:

- *Время запуска ежедневной очистки записей* — *Задается в виде «ЧЧ:ММ»;*
- *Максимальное количество записей, удаляемых в одной транзакции* — *по умолчанию 50000. Параметр может иметь значения от 1000 до 1000000;*
- *Кнопка «Сохранить общие настройки».*

Список типов записей и их настройки очистки:

- *Аудит,*
- *Журналы Монитора,*
- *Звонки,*
- *Истекшие клиентские сертификаты,*
- *Команды,*
- *Логи действий на платформе Linux,*

- Местоположения,
- Отключенные комплекты,
- Рассылаемые файлы,
- События,
- Сообщения,
- Статистика использования устройства,
- Удаленное управление устройством.

Настройки одного типа записей:

- *Наименование* — название настраиваемого типа записей;
- *Очистка включена* — (вкл/выкл). Включает или выключает очистку для данного типа записей;
- *Срок хранения (дни)* — записи старше заданного значения подлежат удалению;
- *Количество неудаляемых записей* — заданное количество последних записей должно сохраняться, игнорируя атрибут «Срок хранения». Параметр доступен для редактирования только при включенной очистке;
- *Дата последней очистки* — отображает дату последней успешной очистки.

Чтобы настроить очистку необходимо выполнить следующие действия:

1. Выбрать в таблице нужный тип записей.
2. В правой части рабочего экрана внести изменения в настройки для выбранного типа записей.
3. Нажать кнопку «Сохранить», после чего настройки вступят в силу.

Примечание

- Для следующих типов записей не редактируются параметры «Срок хранения» и «Количество неудаляемых записей»:
 - Логи действий на платформе Linux,
 - Рассылаемые файлы.
- Для типа записей «Отключенные комплекты» не редактируемый параметр «Количество неудаляемых записей».
- Для типа записей «Истекшие клиентские сертификаты» очистка за-

трагирует только просроченные клиентские сертификаты, за исключением:

- *последнего сертификата аутентификации;*
- *сертификатов, используемых в назначенных профилях.*

2.15.3 Распределение ресурсов

Раздел «Распределение ресурсов» позволяет настраивать распределение нагрузки на канал данных раздачи приложений. Настройки раздела позволяют задавать квоты на использование канала данных при раздаче приложений по параметрам «Ширина канала для раздачи приложений» и «Максимальное количество одновременных клиентов».

Доступ к разделу должны иметь администраторы назначенные на корень дерева ОШС и определяется полномочиями:

- Просмотр,
- Изменение (только при наличии привилегии «Просмотр»).

В рабочем экране раздела отображается нагрузка на канал раздачи приложений и настройки, регулирующие нагрузку на него:

- *Ширина канала для раздачи приложений (Мбит в секунду):*
 - *Объем ресурса — Задается в окне редактирования параметра. Если не задано, то квотирование ресурса не осуществляется;*
- *Максимальное количество одновременных клиентов:*
 - *Значение — Задается в окне редактирования параметра. Если не задано, то квотирование ресурса не осуществляется;*
- *Загрузка (%) — Текущая загрузка ресурса. Вычисляется в БД. Отображается только в случае, если осуществляется квотирование;*
- *Очередь ожидания — Объем очереди. Вычисляется в БД. Отображается только в случае, если осуществляется квотирование.*

Примечание

- *Параметр «Максимальное количество одновременных клиентов» работает следующим образом:*
 - *Если параметр «Максимальное количество одновременных клиентов» установлено в 1, то в момент когда первый клиент начал загрузку начинается ожидание окончания предполагаемого времени загрузки, которое вычисляется по ширине канала и размеру файла. После окончания загрузки, начнется загрузка для другого клиента.*

- *Если фактическое время заочки превысило ожидаемое, то ожидаемое время отображается как «0», до окончания загрузки текущего клиента.*
- *Для того, что бы квотирование канала данных работало следует задать оба параметра:*
 - *Ширина канала для раздачи приложений (Мбит в секунду),*
 - *Максимальное количество одновременных клиентов.*

2.15.4 Конфигурация компонентов

Система предоставляет возможность централизованно управлять настройками серверных компонентов через консоль администратора (APM), без необходимости перезапуска служб. Это позволяет оперативно изменять параметры работы компонентов, назначать разные конфигурации для разных экземпляров одного компонента и контролировать текущие настройки, применяемые в системе.

Настройки компонентов могут задаваться несколькими способами в порядке убывания приоритета:

1. Файл конфигурации компонента (наивысший приоритет).
2. Конфигурация, хранимая в базе данных и управляемая через APM.
3. Параметры командной строки.
4. Переменные окружения.

Параметры, заданные в файле конфигурации, имеют приоритет над настройками в БД и не могут быть переопределены через APM.

В данном разделе администратор может создавать, редактировать, копировать и удалять конфигурации компонентов, а также назначать их на экземпляры компонентов с использованием тегов конфигурации.

Доступ к разделу

Доступ к разделу «Конфигурации компонентов» и управление командами имеют только администраторы, назначенные на корень организационной структуры, с соответствующими правами:

- Просмотр конфигураций.
- Изменение конфигураций.
- Удаление конфигураций.
- Рестарт экземпляров.
- Перезагрузка конфигураций.

Раздел содержит (рисунок 229):

- Выпадающий список компонентов — выбор компонента из справочника доступных для настройки компонентов. При выборе отображается имя компонента и его описание.
- Таблица конфигураций — список конфигураций для выбранного компонента. Колонки:
 - Наименование конфигурации,
 - Компонент (по умолчанию скрыта),
 - Описание компонента,
 - Теги конфигурации (список тегов, разделённых точкой с запятой),
- Кнопки действий:
 - Создать,
 - Изменить,
 - Удалить,
 - Копировать,
 - Обновить список.

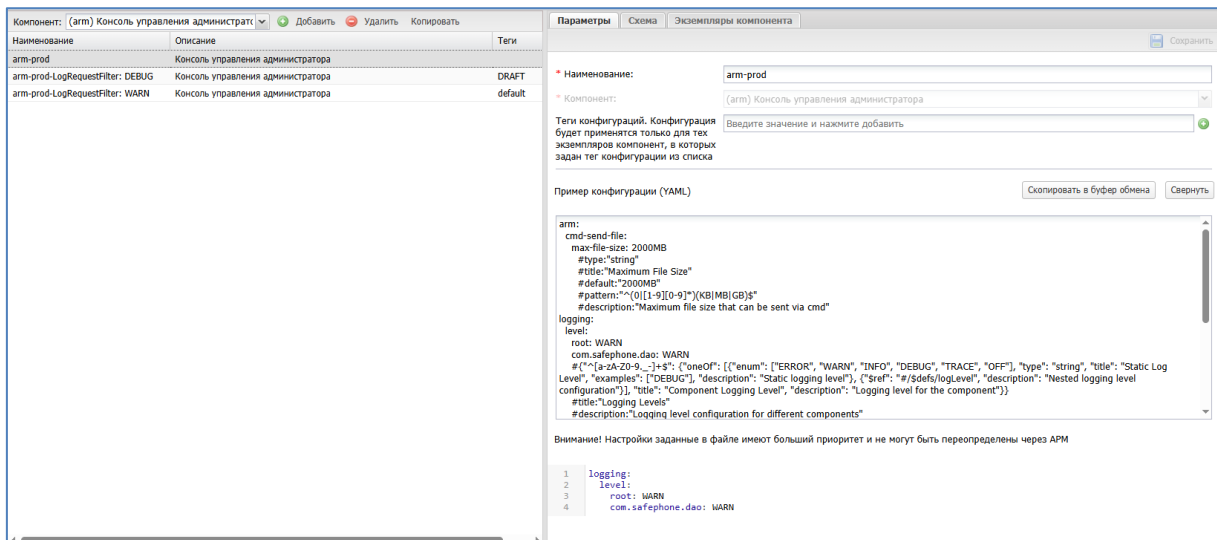


Рисунок 229 — Раздел "Конфигурации компонентов"

Редактирование конфигурации

Окно редактирования содержит следующие закладки:

1. Параметры:

- **Наименование** — уникальное в пределах компонента имя конфигурации (от 1 до 511 символов).
- **Компонент** — выбор компонента из справочника. После сохранения недоступен для изменения.
- **Теги конфигурации (опционально)** — список тегов, для которых данная конфигурация будет применена. Каждый тег:
 - Длиной от 1 до 63 символов.
 - Может содержать цифры, латинские буквы, дефис и нижнее подчеркивание.
 - Уникален (регистронезависимо) в пределах списка.

2. Конфигурация (YAML):

- YAML-редактор с подсветкой синтаксиса и проверкой формата.
Предупреждение: «Настройки, заданные в файле, имеют больший приоритет и не могут быть переопределены через APM.»

3. Схема:

- Отображение JSON-схемы конфигурации компонента (только для просмотра).
Схема форматирована аналогично Swagger UI.

4. Экземпляры компонента (опционально):

- Таблица экземпляров выбранного компонента с возможностью выполнения команд:
 - **Рестарт** — перезапуск экземпляра с применением новой конфигурации.
 - **Перезагрузка конфигурации** — обновление настроек без перезапуска компонента.

Правила работы с конфигурациями

- **Создание конфигурации:** При создании новой конфигурации необходимо выбрать компонент, указать уникальное имя и задать параметры в YAML-формате.
- **Копирование:** При копировании конфигурации к её имени автоматически добавляется префикс «Копия ».

- **Валидация:** При сохранении конфигурация проверяется по JSON-схеме компонента. При нарушении схемы выводится ошибка.
- **Назначение конфигурации:** Конфигурация применяется к тем экземплярам компонента, у которых задан соответствующий тег (или тег «default», если тег не указан).
- **Секретные параметры:** Параметры, содержащие секретные данные (например, пароли), исключаются из просмотра в APM.

Команды управления экземплярами компонентов

В разделе «Информация» → «Компоненты» добавлена возможность управлять экземплярами компонентов:

- Рестарт — остановка и автоматический перезапуск экземпляра компонента.
- Перезагрузка конфигурации — применение изменений в настройках без перезапуска.

Команды доступны при выполнении условий:

- Выбран экземпляр компонента.
- У экземпляра задан тег конфигурации.
- У администратора есть соответствующие полномочия.

Просмотр применённых конфигураций

Для каждого экземпляра компонента можно открыть окно с закладками:

Назначенная конфигурация — YAML-редактор с назначенной через APM конфигурацией (только для просмотра).

Применённая конфигурация — YAML-редактор с фактической конфигурацией, применяемой экземпляром (включая параметры из файла конфигурации).

2.16 Завершение работы в «UEM SafeMobile»

Для завершения сеанса работы пользователя с АРМ Администратора SafeMobile следует нажать кнопку **«Выход»** в верхней правой части основного окна. При этом происходит переход к окну аутентификации в соответствии с п. 2.1.

3 Частые вопросы

Вопрос 1:

Что делать, если при загрузке АРМ в браузере Firefox появляется окно: «*Внимание: сценарий не отвечает*», содержащее следующее сообщение «*Похоже, исполняемый на этой странице сценарий занят или не отвечает. Вы можете остановить его сейчас или продолжить и посмотреть, сможет ли он завершить свою работу*».

Ответ:

Для продолжения работы необходимо в настройках браузера Firefox увеличить значение параметра **dom.max_script_run_time**. Для этого следует выполнить действия:

1. В адресной строке набрать **about:config** и нажать на клавиатуре клавишу «Enter».
2. Может появиться страница предупреждения:

about:config «*Будьте осторожны, а то лишитесь гарантии!*».

Нажать кнопку «**Я обещаю, что буду осторожен!**», чтобы перейти на страницу **about:config**.

3. На странице **about:config** найти настройку **dom.max_script_run_time** и дважды нажать на нее.
4. Увеличьте исходное значение.
5. Нажать ОК.

Вопрос 2:

Что делать, если при смене пароля после успешной аутентификации появляется окно **Подтверждение смены пароля** с выбором пользователя (рисунок 3.1).

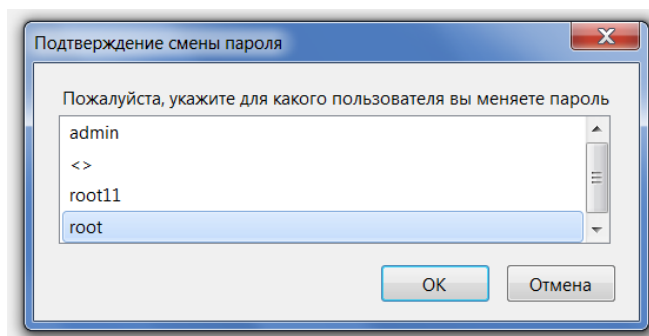


Рисунок 3.1 — Окно подтверждения смены пароля

Ответ:

Отключить автозаполнение и сохранение логинов и паролей в настройках браузера Firefox (рисунок 3.2).

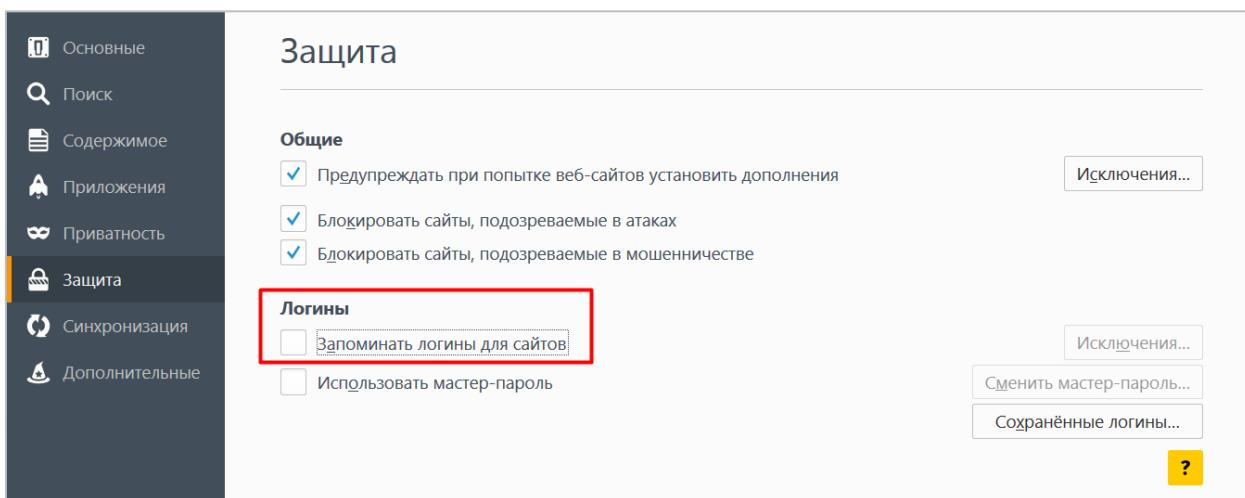


Рисунок 3.2 — Настройка отмены автозаполнения логина и пароля в браузере Firefox

Вопрос 3:

Что делать, если при открытии раздела главного меню «Администраторы» поле логин и пароль заполнено логином и паролем, сохраненным в окне аутентификации (рисунок 3.3)?

The screenshot shows a form with the following fields:

- * Имя пользователя:** Input field containing the text "admin".
- * Пароль:** Password input field filled with dots, with an eye icon to toggle visibility.
- Роль:** A list of roles with checkboxes:
 - Все роли
 - Администратор ИТ
 - Администратор ИБ
 - Суперадминистратор

Рисунок 3.3 — Автозаполнение пароля и логина в окне управления «Администраторы»

Ответ:

Отключить автозаполнение и сохранение логинов и паролей в настройках браузера Firefox (рисунок 3.4).

The screenshot shows the Firefox 'Защита' (Security) settings page. The 'Логины' (Logins) section is highlighted with a red box and contains the following options:

- Запоминать логины для сайтов (This option is currently unchecked).
- Использовать мастер-пароль

Other visible options in the 'Общие' (General) section include:

- Предупреждать при попытке веб-сайтов установить дополнения
- Блокировать сайты, подозреваемые в атаках
- Блокировать сайты, подозреваемые в мошенничестве

Buttons for 'Исключения...' (Exceptions) are present for the first two options. At the bottom right, there are buttons for 'Сменить мастер-пароль...' (Change master password...) and 'Сохранённые логины...' (Saved logins...), along with a yellow question mark icon.

Рисунок 3.4 — Настройка отмены автозаполнения логина и пароля в браузере Firefox

Приложение А Установка МСК на платформе iOS в режим Supervised

Перевод МСК на платформе iOS в режим Supervised с установкой требуемых параметров и ограничений для осуществления контроля над устройством, следует выполнять в соответствии со следующим регламентом:

1. Скачать и запустить ПО Apple Configurator 2.
2. Подключить iPhone (iPad) к ПК Mac.
3. Выбрать подключенное МСК и нажать кнопку «**Prepare**» (подготовить) в соответствии с рисунком А.1.

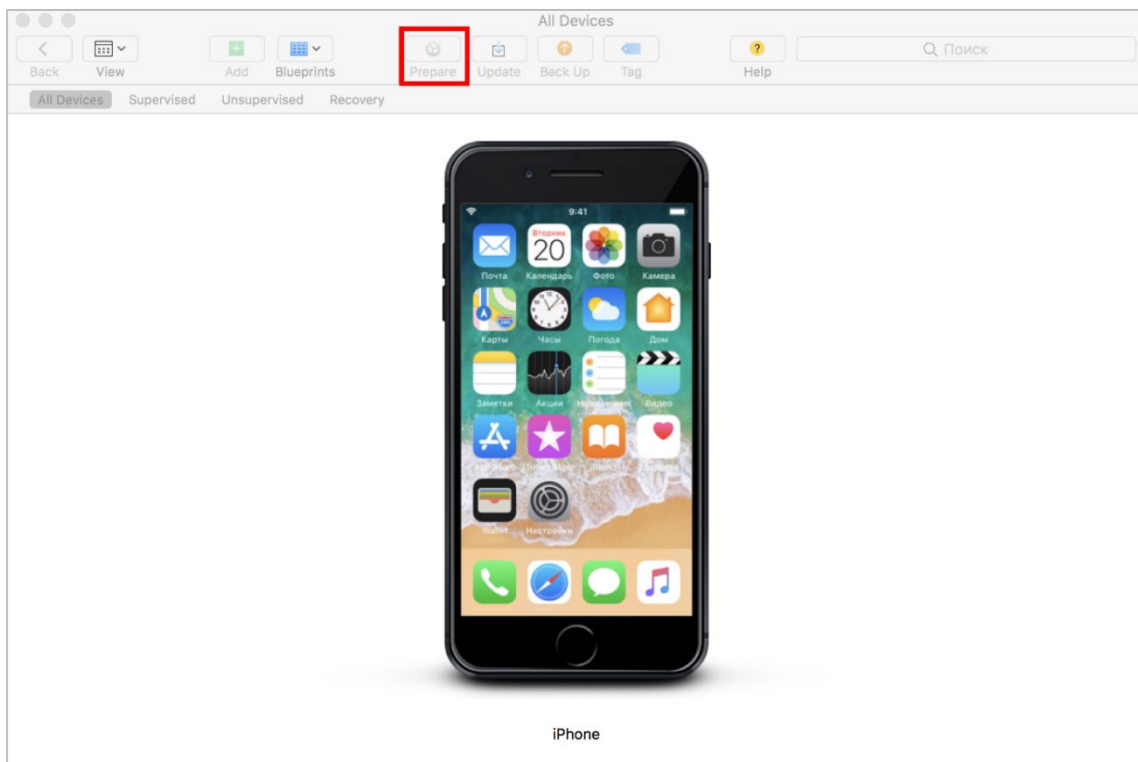


Рисунок А.1 — Окно подключенных устройств

4. В поле «**Prepare with**» в соответствии с рисунком А.2 выбрать значение по умолчанию «**Manual Configuration**» (установка конфигурации вручную). Для получения доступа к правам супервайзера поставить галочку напротив пунктов «**Supervise devices**» (контролировать устройства) и «**Allow devices to pair with other computers**» (разрешить устройствам соединяться с другими компьютерами), затем нажать кнопку «**Next**». При необходимости возврата в предыдущее меню следует нажать на кнопку «**Previous**».



Рисунок А.2 — Выбор режима подготовки устройства

5. В поле «**Server**» (рисунок а.3) выбрать значение «**Do not enroll in MDM**» (не регистрироваться в MDM) и нажать кнопку «**Next**».



Рисунок А.3 — Выбор MDM сервера

6. Нажать кнопку **«Skip»** (рисунок а.4),

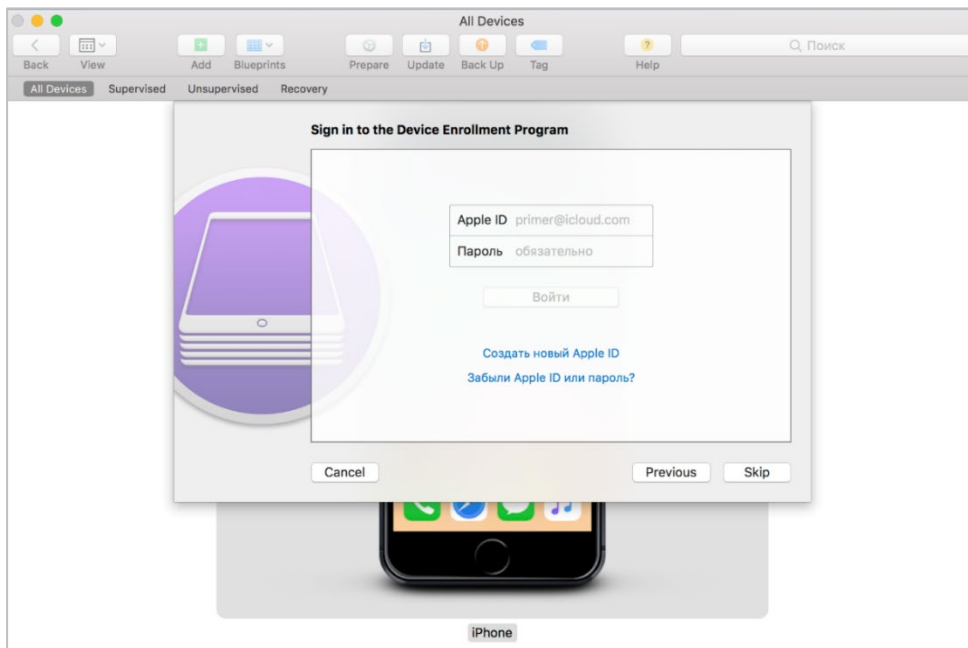


Рисунок А.4 — Аутентификация в ADEP

7. В поле **«Name»** (рисунок а.5) следует указать название организации, остальные поля можно оставить пустыми и нажать **«Next»**.



Рисунок А.5 — Создание записи о контролирующей организации

8. Если перевод в режим supervision осуществляется в первый раз, следует выбрать пункт **«Generate a new supervision identity»** (создать новый supervision-идентификатор) в соответствии с рисунком А.6, в противном случае выбрать пункт **«Choose an existing supervision identity»** (выберите существующий supervision-

идентификатор). Далее нажать «Next».



Рисунок А.6 — Выбор supervision-идентификатора

9. В поле «**Setup Assistant**» (рисунок а.7) выбрать значение «**Show all steps**» (показать все шаги). В этом случае все указанные параметры первоначальной конфигурации МСК будут доступны для настройки пользователю после перепрошивки устройства. Далее нажать «**Prepare**».

Примечание

Подробную информацию по настройке параметров конфигурации устройства посредством ПО Apple Configurator 2 можно получить на сайте производителя устройства на платформе iOS (apple.com).

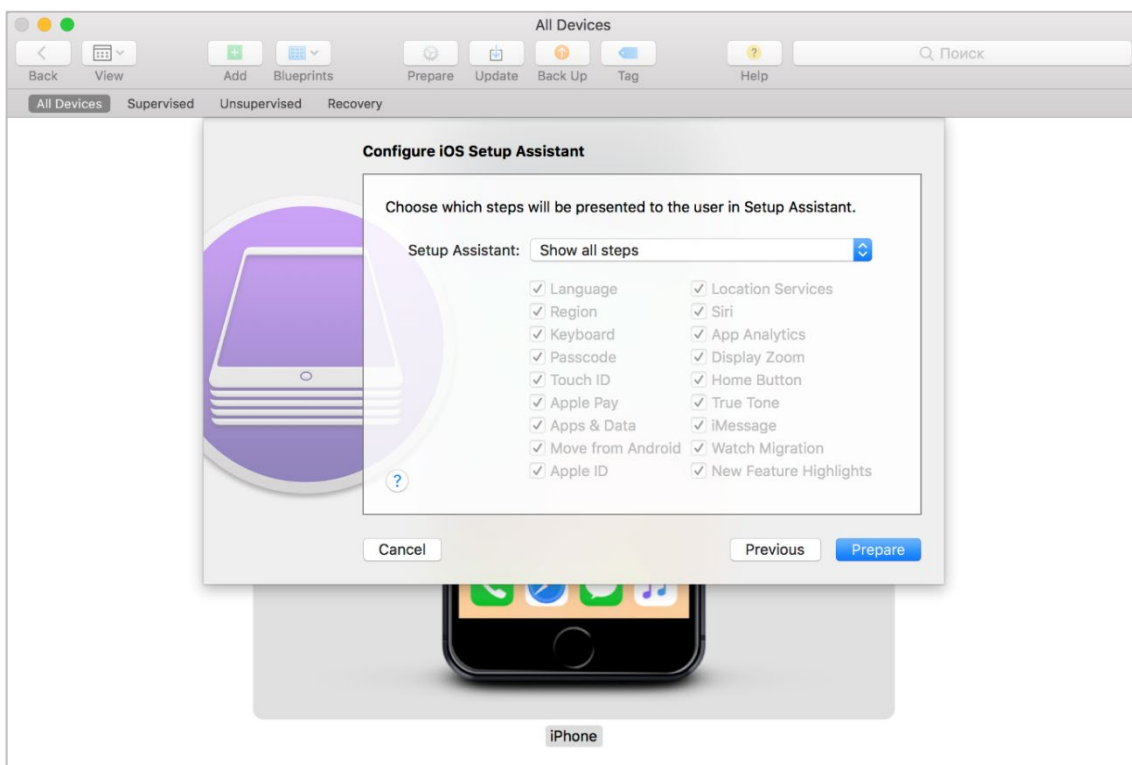


Рисунок А.7 — Выбор параметров первоначальной конфигурации МСК

Затем запустится процесс перепрошивки МСК и подготовки в соответствии с заданными параметрами конфигурации (рисунок а.8). МСК в ПО Apple Configurator 2 отобразится в разделе «**Supervised**».



Рисунок А.8 — Индикация процесса подготовки устройства

ВНИМАНИЕ!

Подготовка устройства может занять несколько минут. Попытка остановить или отменить процесс установки iOS после ее запуска или закрытие ПО Apple Configurator 2 может повредить устройство.

10. На МСК после перепрошивки и завершения настройки конфигурации в приложении **«Настройки»** отобразится сообщение об осуществлении контроля над устройством в соответствии с рисунком А.9.

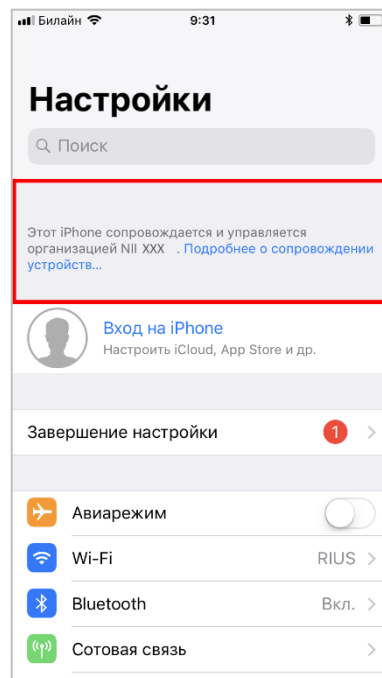


Рисунок А.9 — Сообщение о контроле над устройством в приложении «Настройки»

11. Для отмены контроля над устройством следует выполнить действия в соответствии с регламентом, но при выборе режима в п. А.4 снять галочку напротив пункта **«Supervise devices»** и продолжить подготовку устройства.

Приложение Б

Перечень возможных ошибок при выполнении команд Администраторов










Результат	Описание ошибки	Действие Администратора
Ошибка в ходе обработки ответа на команду	Ошибка обработки пакета клиента сервером	Повторно отправить команду
Команда была выдана на устройство, после чего устройство отключилось	Потеря соединения	Ожидать, пока устройство подключится к серверу, повторно отправить команду
Нарушение защиты ОС	Устройство получило команду, выполнение которой опасно для ОС	Действие не требуется
Данные, полученные от сервера SafeMobile, искажены (дистрибутив приложения)	Ошибка в ходе передачи пакета от сервера клиенту	Повторно отправить команду
Приложение уже установлено (или запущено)	Попытка установки уже установленного приложения	Действие не требуется
Недопустимое значение параметра команды	Параметр команды не поддерживается. При использовании GPRS точки доступа на MCK iOS	Изменить параметр команды и отправить команду повторно. Параметры команд приведены в п.2.6.6
Неизвестная ошибка	Ошибка в ходе выполнения команды	Повторно отправить команду













Результат	Описание ошибки	Действие Администратора
Сокет закрыт другой стороной	Потеря соединения	Ожидать, пока устройство подключится к серверу, повторно отправить команду
Истекло время ожидания ответа	Потеря соединения	Ожидать, пока устройство подключится к серверу, повторно отправить команду
Истекло количество попыток повторного доведения	Потеря соединения	Повторно отправить команду
Получен недействительный набор записей	Неверный параметр команды	Изменить параметр команды и отправить команду повторно
Пустой список точек доступа	В системе нет точек доступа, привязанных к комплекту	1) Создать одну или несколько точек доступа (раздел «Объекты учета/Точка доступа»), 2) Привязать точки доступа к комплекту на экранной форме комплекта (раздел «Объекты учета/Комплект»), 3) Повторно отправить команду












Приложение В








Приложения для мобильных устройств iOS

Данная информация была взята из сетевой документации производителя устройств iOS.

App	iOS Bundle ID
 Activity	com.apple.Fitness
 App Store	com.apple.AppStore
 Books	com.apple.iBooks
 Calculator	com.apple.calculator
 Calendar	com.apple.mobilecal
 Camera	com.apple.camera
 Clock	com.apple.mobletimer
 Compass	com.apple.compass
 Contacts	com.apple.MobileAddressBook

 FaceTime	com.apple.facetime
 Files	com.apple.DocumentsApp
 Find Friends	com.apple.mobileme.fmf1
 Find iPhone	com.apple.mobileme.fmip1
 Health	com.apple.Health
 Home	com.apple.Home
 iCloud Drive	com.apple.iCloudDriveApp
 iTunes Store	com.apple.MobileStore
 Mail	com.apple.mobilemail
 Maps	com.apple.Maps
 Measure	com.apple.measure
 Messages	com.apple.MobileSMS

 Music	com.apple.Music
 News	com.apple.news
 Notes	com.apple.mobilenotes
 Phone	com.apple.mobilephone
 Photo Booth	com.apple.Photo-Booth
 Photos	com.apple.mobileslideshow
 Podcasts	com.apple.podcasts
 Reminders	com.apple.reminders
 Safari	com.apple.mobilesafari
 Settings	com.apple.Preferences
 Stocks	com.apple.stocks

 Tips	com.apple.tips
 TV	com.apple.tv
 Videos	com.apple.videos
 Voice Memos	com.apple.VoiceMemos
 Wallet	com.apple.Passbook
 Watch	com.apple.Bridge
 Weather	com.apple.weather

Приложение Г

Состав полномочий предустановленных ролей

Роль	Назначенные полномочия
Администратор ИБ	1. «Информация об устройствах»: «Действия» (просмотр и отмена команд). 2. «Информация об устройствах»: «Данные об устройстве». 3. «Приложения / Установленные приложения»: «Просмотр установленных на устройстве приложений», «Запрос списка установленных на устройстве приложений», «Просмотр установленных в контейнере приложений». 5. Отчёты: «События ИБ», «Аудит»
Администратор ИТ	Все полномочия, кроме: отчётов «События ИБ» и «Аудит», разделов «Лицензия», «Пользовательское соглашение», «Информация», «Синхронизация данных LDAP»
Суперадминистратор	Все полномочия

Приложение Д Подготовка устройства Windows для установки МСК

Назначение и условие применения

Для регистрации МСК в системе необходимо, чтобы на МСК была установлена и активирована ОС Windows 10 версии не ниже 1703 в редакции Pro или Enterprise.

Для гарантированного уничтожения данных (в случае утраты устройства) необходимо, чтобы на всех несъемных накопителях МСК было включено шифрование данных посредством встроенного компонента BitLocker.

МСК не должно быть присоединено к домену Active Directory.

Для обеспечения возможности сброса к заводским настройкам должна быть включена среда восстановления (Windows Recovery Environment). Чтобы проверить состояние среды восстановления нужно запустить из-под учетной записи администратора консоль и выполнить команду: `reagentc /info`.

```
PS C:\WINDOWS\system32> reagentc /info
Информация о конфигурации среды восстановления Windows и
сброса системы:

Состояние среды восстановления Windows:      Enabled
Расположение среды восстановления Windows:  \\?\GLOBALROOT\device\harddisk2\partition1\Recovery\WindowsRE
Идентификатор данных конфигурации загрузки: 40cc6258-1bdd-11ec-9dca-a0510bbcd256
Расположение образа для восстановления:
Индекс образа для восстановления:            0
Расположение пользовательского образа:
Индекс пользовательского образа:            0

REAGENTC.EXE: операция выполнена успешно.
PS C:\WINDOWS\system32>
```

Если среда восстановления выключена, то необходимо выполнить команду: `reagentc /enable`.

Эксплуатация устройства должна выполняться из-под учетной записи с ограниченными правами.

Подготовка к работе

Перед началом работы пользователю необходимо проверить корректность значений даты, времени и часового пояса на МСК. Если эти параметры установлены неверно, следует выключить на МСК автоматическое определение даты и времени, предоставляемое сетью, и осуществить настройку вручную.

Проверить наличие обновлений. Последние обновления ОС должны быть установлены и выполнена перезагрузка устройства.

Для того, чтобы на МСК, после подключения к Системе, имелась возможность установки публичных приложений, сотруднику необходимо аутентифицироваться в магазине публичных приложений Microsoft Store.

Приложение Е

Поддерживаемые платформы мобильных устройств

В текущей версии система поддерживает работу на устройствах следующих платформ:

1. iOS — версии от 11.0 и выше;
2. Android — версии от 5.0 и выше;
3. Windows — Windows 10 не ниже 1703 в редакции Pro или Enterprise;
4. Аврора — версии 4 и выше.

Для работы на устройствах платформ Android и Аврора требуется установка на МСК приложения «Монитор». В зависимости от типа устройства, версии платформы и метода установки приложения будут доступны различные стратегии управления устройством.

Выбор стратегии управления для Android

Стратегия управления устройством зависит от версии операционной системы и способа установки на него приложения «Монитор».

Монитор установлен на устройство как обычное приложение

Стратегия управления	Привилегии приложения «Монитор» на МСК, в зависимости от версии ОС				
	Samsung (Android 5-6)	Samsung (Android 7-11)	Samsung (Android 12+)	Android 5-6	Android 7+
Личный рабочий профиль	Стратегия не применима	Profile Owner, KNOX	Profile Owner, KNOX	Стратегия не применима	Profile Owner,
Корпоративный рабочий профиль	Стратегия не применима	Стратегия не применима	Стратегия не применима	Стратегия не применима	Стратегия не применима
Только устройство (Android)	Device Admin, KNOX	Device Admin, KNOX	Device Admin, KNOX (*)	Device Admin	Device Admin
Устройство и контейнер KNOX	Device Admin, KNOX	Device Admin, KNOX (**)	Device Admin, KNOX (*, **)	Стратегия не применима	Стратегия не применима

* — пользователю доступно управление частью разрешений монитора.

** — начиная с Android 10, Knox container доступен на ограниченном наборе устройств.

Монитор установлен на устройство через NFC

Стратегия управления	Привилегии приложения «Монитор» на МСК, в зависимости от версии ОС	
	Samsung (Android 5.0+)	Android 5.0+
Личный рабочий профиль	Стратегия не применима	Стратегия не применима
Корпоративный рабочий профиль	Стратегия не применима	Стратегия не применима
Только устройство (Android)	Device Owner, KNOX (опционально)	Device Owner, System
Устройство и контейнер KNOX	Device Admin, KNOX	Стратегия не применима

Монитор подключается по QR после сброса устройства к заводским настройкам (метод доступен, начиная с Android 7.0)

Стратегия управления	Привилегии приложения «Монитор» на МСК, в зависимости от версии ОС	
	Samsung (Android 7-10)	Android 11+
Личный рабочий профиль	Стратегия не применима	Стратегия не применима
Корпоративный рабочий профиль	Стратегия не применима	Corporate Profile Owner + KNOX (опционально)
Только устройство (Android)	Device Owner, KNOX (опционально)	Device Owner, KNOX (опционально)
Устройство и контейнер KNOX	Стратегия не применима	Стратегия не применима

Приложение Ж

Взаимосвязи некоторых функций системы и стратегий подключения

Функционал системы	Стратегии подключения			
	Device Owner	Кнох (устарел)	КРП	ЛРП
Определение местоположения	Да	Да	Да	Нет
Сброс к заводским настройкам	Да	Да	Да	Нет
Захват экрана	Да	Да	Да (не работают жесты)	В рабочей области (не работают жесты)
Политика использования камеры	Да	Да	Да	Нет
Безусловная установка корпоративных приложений	Да	Да	Нет	Нет

Регистрация звонков/СМС	Да	Да	Нет	Нет
Режим работы «Киоск»	Да	Да	Нет	Нет
Команда «Синхронизация времени»	Да	Да	Нет	Нет
Сетевые настройки	Да	Да	Нет	Нет
Команда «Перезагрузка устройства»	Да	Да	Нет	Нет
Команда «Блокировка устройства»	Да	Да	Нет	Нет