ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

Прикладное программное обеспечение «Аврора Центр» релиз 5.7.0

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Часть 3

Подсистема Платформа управления

Версия 1.2

Листов 425

2026

АННОТАЦИЯ

Настоящий документ является третьей частью руководства пользователя Прикладного программного обеспечения «Аврора Центр» (далее – ППО) релиз 5.7.0 и содержит описание функционирования подсистемы Платформа управления (ПУ), входящей в состав ППО.

ППО является прикладным программным обеспечением, предназначенным для:

– управления устройствами[1], а также приложениями[2] и их жизненным циклом;

– отправки push-уведомлений на устройства;

– обновления операционной системы (ОС) Аврора и ОС семейства Linux путем получения из доверенного хранилища пакетов с изменениями ОС (образа ОС) и их установки. При этом указанные процессы выполняются штатными средствами самой ОС, а ППО участвует лишь в их инициализации в ОС и не гарантирует их успешного завершения.

ПРИМЕЧАНИЯ:

✓ Подробная информация о составе и назначении ППО, а также требования к условиям выполнения приведены в документе «Руководство администратора»;

✓ Подробная информация об особенностях резервного копирования приведена в документе «Рекомендации по резервному копированию».

Описание интерфейсов подсистем, входящих в состав ППО, приведено в следующих документах:

– «Руководство пользователя. Часть 1. Подсистема безопасности»;

– «Руководство пользователя. Часть 2. Подсистема «Маркет»;

– «Руководство пользователя. Часть 3. Подсистема Платформа управления»;

– «Руководство пользователя. Часть 4. Подсистема управления тенантами»;

– «Руководство пользователя. Часть 5. Подсистема Сервис уведомлений».

Описание работы приложений приведено в документах:

– «Руководство пользователя. Часть 6. Приложение «Аврора Маркет» для операционной системы Аврора»;

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 8. Приложение «Аврора Маркет» для операционной системы Android»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android»;

[1] Определение термина «Устройство» приведено в таблице (Таблица 73).

2 Определение термина «Приложение» приведено в таблице (Таблица 73).

– «Руководство пользователя. Часть 10. Приложение «Аврора Маркет» для операционных систем семейства Linux»;

– «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

СОДЕРЖАНИЕ

1. Подготовка к работе 7
1.1. Описание принципов безопасной работы средства 7
1.1.1. Общая информация 7
1.1.2. Компрометация паролей 7
1.1.3. Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения 8
1.2. Начало сеанса работы 8
1.3. Описание интерфейса 10
1.3.1. Верхняя панель 10
1.3.2. Рабочая область 11
1.4. Работа с фильтрами 14
2. Работа в разделе «Управление» Консоли администратора ПУ 24
2.1. Общее описание карточек элементов управления 24
2.1.1. Работа с карточкой устройства 24
2.1.2. Работа с карточкой группы устройств 73
2.1.3. Работа с карточкой пользователя 77
2.1.4. Работа с карточкой группы пользователей 80
2.1.5. Работа с карточкой политики 83
2.1.6. Работа с карточкой офлайн-сценария 85
2.1.7. Работа с карточкой файла/папки 86
2.2. Подраздел «Устройства» 88
2.2.1. Добавление устройства в ПУ 90
2.2.2. Добавление группы устройств вручную 92
2.2.3. Добавление устройств или группы устройств с помощью CSV-файла 102
2.2.4. Добавление модели устройства 111
2.2.5. Приглашения на самостоятельную регистрацию устройства 113
2.2.6. Добавление множества 123
2.2.7. Экспорт списка устройств в CSV-файл 132
2.2.8. Привязка устройства к пользователю 133
2.2.9. Привязка устройств к группе устройств 135
2.2.10. Активация устройств 137
2.2.11. Применение оперативных команд 148
2.2.12. Отвязка (исключение) устройств из группы устройств 160
2.2.13. Архивирование устройства 161
2.2.14. Восстановление устройств из архива 162
2.2.15. Удаление устройства 164
2.2.16. Удаление группы устройств 166
2.2.17. Очистка устройств до заводских настроек 166

2.2.18. Вывод устройства из эксплуатации 167
2.3. Подраздел «Пользователи» 168
2.3.1. Добавление пользователя устройства вручную 169
2.3.2. Добавление группы пользователей вручную 171
2.3.3. Добавление пользователей или группы пользователей с помощью CSV-файла 173
2.3.4. Привязка пользователей к группе пользователей 182
2.3.5. Привязка пользователей к устройствам 185
2.3.6. Отвязать (исключить) пользователей из группы пользователей 186
2.3.7. Архивирование пользователя 187
2.3.8. Удаление группы пользователей 188
2.4. Подраздел «Политики» 189
2.4.1. Общее описание правил политик 199
2.4.2. Добавление политики вручную 294
2.4.3. Добавление политики на основе корпоративного шаблона 295
2.4.4. Назначение политики на группы устройств или группы пользователей 296
2.4.5. Добавление политики на основе существующей 299
2.4.6. Редактирование правила политики 300
2.4.7. Отвязка политики от группы устройств или группы пользователей 302
2.4.8. Удаление политики 304
2.5. Подраздел «Сценарии» 304
2.5.1. Добавление офлайн-сценария 306
2.5.2. Назначение офлайн-сценария на группы устройств или группы пользователей 311
2.5.3. Отвязка офлайн-сценарий от группы устройств/группы пользователей 313
2.5.4. Удаление офлайн-сценария 314
2.6. Подраздел «Файлы» 315
2.6.1. Работа с файлами (скриптами) 316
2.6.2. Работа с папками из git-репозитория 320
2.6.3. Доставка файла и выполнение скрипта на устройстве с помощью ПУ 322
3. Работа в разделе «Мониторинг» Консоли администратора ПУ в Подразделе «Индикаторы» 324
4. Работа в разделе «Администрирование» Консоли администратора ПУ 327
4.1. Подраздел «Настройки» 327
4.1.1. Доверенные корневые сертификаты 329
4.1.2. Категории пользовательских сертификатов 330
4.1.3. Приглашения 331
4.1.4. Платформа 336
4.1.5. Интеграция (информация о серверах) 339
4.1.6. Территории 359

4.1.7. Настройки правил политик 360
4.1.8. Переменные к подстановке 361
4.1.9. Экспорт/Импорт 367
4.2. Подраздел «Орг.структура» 369
5. Сообщения об ошибках и ограничения 371
5.1. Сообщения об ошибках 371
5.2. Ошибки импорта 384
5.2.1. Ошибки импорта устройств 384
5.2.2. Ошибки импорта пользователей 386
5.3. Ограничения 388
Перечень терминов и сокращений 389
Приложение 1 391
Приложение 2 393
Приложение 3 396
Приложение 4 398
Приложение 5 404
Приложение 6 406
Приложение 7 408
Приложение 8 410
Приложение 9 411
Приложение 10 413

1. ПОДГОТОВКА К РАБОТЕ

ПРИМЕЧАНИЕ. Для работы пользователей с интерфейсом ППО необходимо выполнение следующих условий:

– наличие веб-браузера с поддержкой технологий: TLS, CSS3, HTML5, ECMAScript 5 и Cookie. Рекомендуется использовать веб-браузер Chrome версии 90 или выше;

– разрешение экрана монитора не менее 1280x960 px.

1.1. Описание принципов безопасной работы средства

1.1.1. Общая информация

ППО реализует следующие функции безопасности:

– идентификация и аутентификация субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– регистрация событий безопасности.

При использовании ППО необходимо выполнение следующих мер по защите информации от несанкционированного доступа:

– соблюдение парольной политики;

– соблюдение требования, согласно которому пароль не должен включать в себя легко вычисляемые сочетания символов;

– отсутствие у пользователя права передачи личного пароля третьим лицам;

– обязанность пользователя при вводе пароля исключить возможность его перехвата третьими лицами и техническими средствами.

При эксплуатации ППО запрещается:

– оставлять без контроля незаблокированные программные средства и/или ППО;

– разглашать пароли, выводить их на экран, принтер или иные средства отображения информации.

1.1.2. Компрометация паролей

Под компрометацией паролей необходимо понимать следующее:

– физическую утрату носителя с парольной информацией;

– передачу идентификационной информации по открытым каналам связи;

– перехват пароля при распределении идентификаторов;

– сознательную передачу информации третьим лицам.

ПРИМЕЧАНИЕ. При компрометации пароля пользователь обязан незамедлительно оповестить Администратора учетных записей.

1.1.3. Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения

Настройки параметров безопасности ППО доступны только пользователям с ролью Администратор учетных записей и заключаются в возможности управления ролями пользователей ППО.

Пользователям должны назначаться минимальные права и привилегии, необходимые для выполнения ими своих должностных обязанностей (функций).

1.2. Начало сеанса работы

ВНИМАНИЕ! Первоначальный вход в ППО осуществляется с помощью Консоли администратора ПБ и предустановленной учетной записи с ролью Администратор учетных записей. Подробная информация приведена в документе «Руководство администратора».

Для аутентификации в Консоли администратора ПУ необходимо выполнить следующие действия:

– в веб-браузере перейти по адресу Консоли администратора ПУ.

ПРИМЕЧАНИЕ. Для получения адреса Консоли администратора ПУ необходимо обратиться к системному администратору либо иному лицу, ответственному за установку и настройку системы;

– на странице аутентификации выполнить следующие действия:

- выбрать язык интерфейса (по умолчанию интерфейс отображается на языке браузера пользователя);
- заполнить поля «Логин» и «Пароль»;
- нажать кнопку «Войти» (Рисунок 1).

ПРИМЕЧАНИЕ. Данные для заполнения полей «Логин» и «Пароль» Администратору Платформы управления предоставляет Администратор учетных записей. Процесс создания учетной записи Администратора Платформы управления приведен в документе «Руководство пользователя. Часть 1. Подсистема безопасности».

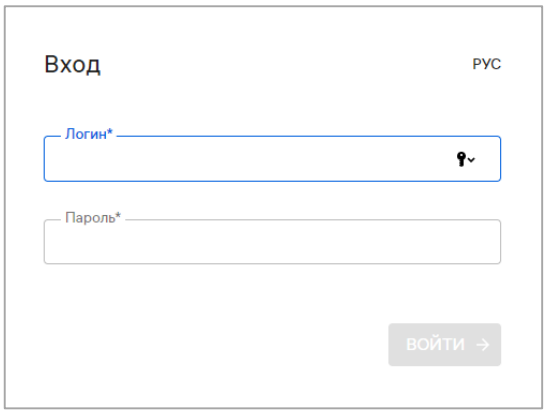


Рисунок 1

В целях безопасности при первом входе пользователю ПУ будет предложено сменить пароль. Для этого в открывшемся окне необходимо выполнить следующие действия (Рисунок 2):

– ввести текущий пароль;
– ввести новый пароль;
– повторно ввести новый пароль;
– выбрать язык интерфейса;
– нажать кнопку «Продолжить».

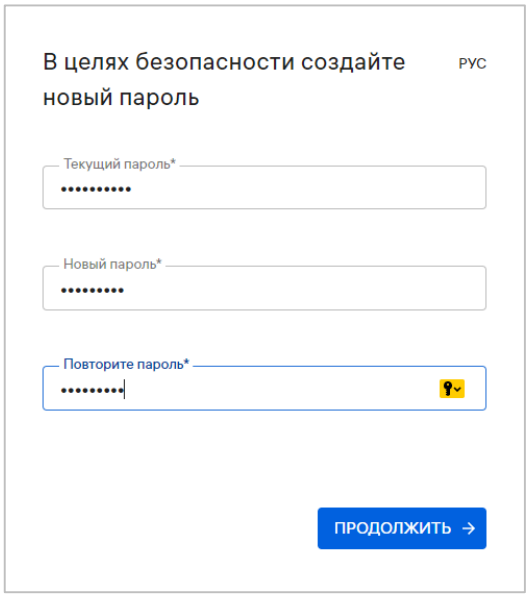


Рисунок 2

Новый пароль должен содержать:

– от 8 до 255 символов;
– заглавные буквы;
– строчные буквы;
– цифры;
– спецсимволы.

ПРИМЕЧАНИЕ. Срок действия пароля – 60 дней. По истечении указанного срока пароль необходимо сменить, при этом новый пароль должен отличаться от 3 ранее вводимых.

По умолчанию для каждого пользователя возможно не более двух одновременных (параллельных) сессий доступа.

При превышении допустимого количества сессий отобразится окно с информационным сообщением «Вы превысили количество допустимых сессий. Текущие сессии будут завершены», где необходимо выполнить одно из следующих действий:

– нажать кнопку «Подтвердить», в результате чего все текущие сессии завершатся и будет выполнен вход в Консоль администратора ПУ;

– нажать кнопку «Отмена», в результате чего все текущие сессии останутся активными и отобразится окно входа в Консоль администратора ПУ.

При успешной аутентификации отобразится страница Консоли администратора ПУ.

ПРИМЕЧАНИЕ. В случае изменения списка ролей необходимо пройти повторную аутентификацию.

Системным администратором могут быть установлены следующие настройки:

– автоматический выход из системы (в случае неактивности пользователя более 5 минут). Для продолжения работы необходимо повторно пройти аутентификацию;

– блокировка учетной записи пользователя (в случае неактивности пользователя в течение 45 дней). Для продолжения работы необходимо обратиться к системному администратору.

1.3. Описание интерфейса

Настоящий документ содержит описание работы ПУ и относящихся к ней подразделов верхней панели интерфейса.

1.3.1. Верхняя панель

Верхняя панель позволяет выполнить следующие действия:

1) Осуществлять навигацию между подсистемами ППО (Рисунок 3 [1]).

Работа в верхней панели Консоли администратора ПУ выполняется в следующих разделах:

– «Мониторинг» (раздел 3), включающем в себя подраздел «Индикаторы»;

– «Управление» (раздел 2), включающем в себя следующие подразделы:

- «Устройства» (подраздел 2.2);
- «Пользователи» (подраздел 2.3);
- «Политики» (подраздел 2.4);
- «Сценарии» (подраздел 2.5);
- «Файлы» (подраздел 2.6);

– «Администрирование» (раздел 4), включающем в себя следующие подразделы:

- «Настройки» (подраздел 4.1);
- «Орг.структура» (подраздел 4.2);

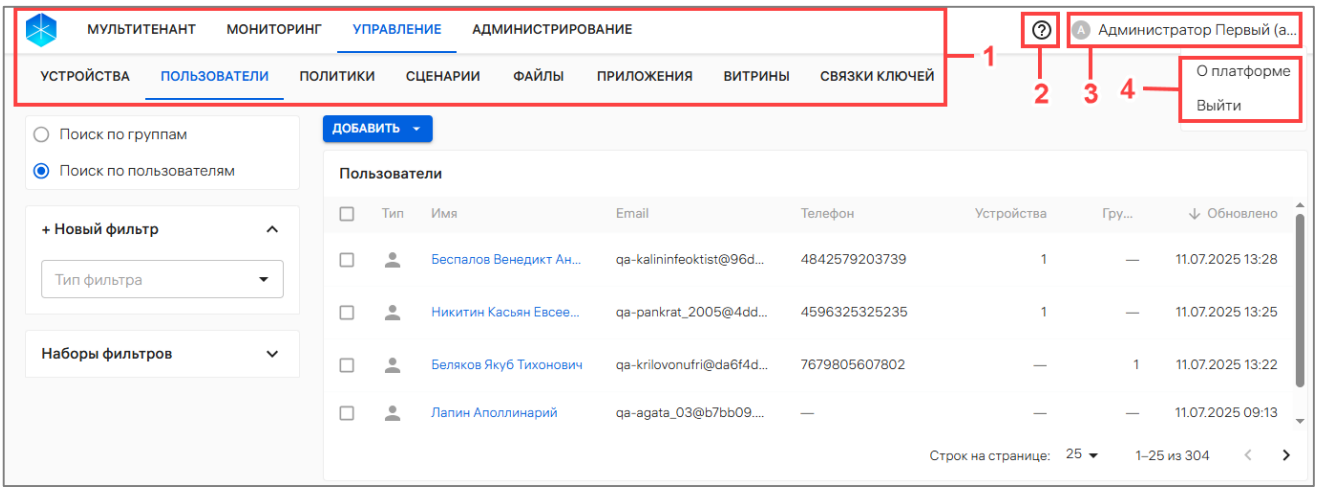


Рисунок 3

2) Получить доступ к справке с инструкцией и описанием работы в ППО нажатием значка (см. Рисунок 3 [2]);

3) Просматривать следующую информацию об учетной записи пользователя в меню текущего пользователя (см. Рисунок 3 [3]):

– имя;
– фамилия;
– Email;

4) Выбирать соответствующие пункты из раскрывающегося списка нажатием значка[3] в меню пользователя (см. Рисунок 3 [4]):

– «О платформе», содержащий:
  • список версий сервисов ППО;
  • кнопку «Скопировать сервисы» для копирования информации о сервисах в буфер обмена;
  • кнопку «Закрыть» для выхода из раздела «О платформе»;
– «Выйти» – пункт для завершения сеанса работы в ППО. В результате выхода отобразится Консоль входа пользователей (см. Рисунок 1).

1.3.2. Рабочая область

В рабочей области отображаются данные выбранного подраздела Консоли администратора ПУ и осуществляется работа с элементами его интерфейса (Рисунок 4 [1]), в частности:

– добавление устройства, групп устройств, пользователей или групп пользователей (вручную, с помощью CSV-файла);
– добавление приглашения на самостоятельную регистрацию устройства;
– привязка устройства к пользователю и его отвязка (вручную, с помощью CSV-файла);

[3] Внешний вид значка может отличаться от приведенного на рисунках в настоящем документе. На значке отображается первая буква имени пользователя.

– блокировка и разблокировка устройства;
– очистка содержимого устройства;
– блокировка и разблокировка камеры устройства;
– получение списка системных сообщений с устройства и событий безопасности;
– назначение и отслеживание политик, назначенных на пользователей, группу пользователей, устройства или группу устройств;
– создание и назначение на группу пользователей или группу устройств офлайн-сценариев;
– просмотр информации о текущем и целевом состоянии устройств;
– просмотр информации о назначенных оперативных командах, политиках и офлайн-сценариях на устройствах, а также о том, какие из них являются действующими в момент просмотра;
– мониторинг текущего состояния устройства;
– просмотр организационной структуры компании.

ВНИМАНИЕ! В зависимости от ОС доступность управляющих действий для устройств может быть ограничена.

В Консоли администратора ПУ элементы интерфейса, выделенные цветом (Рисунок 4 [2]), представляют собой активные ссылки, при нажатии на которые можно выполнить переход на страницу/карточку, где приведена более подробная информация и имеется возможность скопировать данные в буфер обмена.

Для упрощения взаимодействия Администратора Платформы управления с интерфейсом Консоли администратора ПУ предусмотрены всплывающие подсказки (Рисунок 4 [3]), которые отображаются при наведении курсора на соответствующий элемент, а также значки (Таблица 1), доступные в списке быстрых действий и позволяющие управлять выбранными элементами.

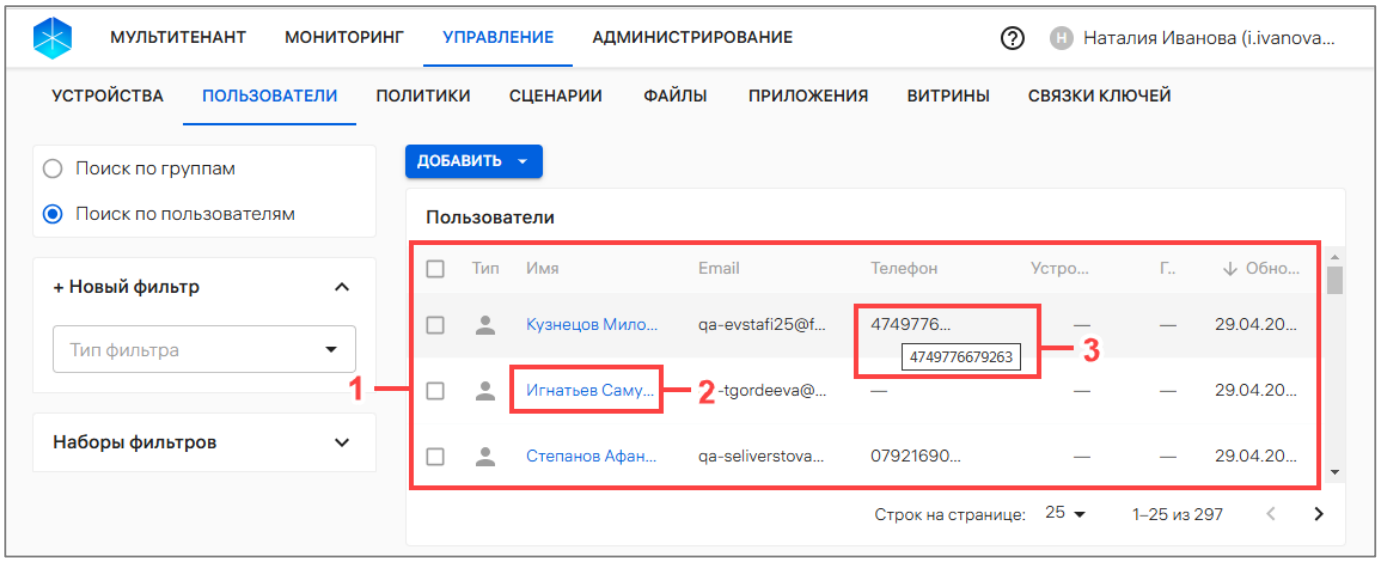


Рисунок 4

В таблице (Таблица 1) приведены возможные действия по каждому из подразделов раздела «Управление».

Таблица 1

Подраздел	Значок	Описание	Примечание
Устройства		Привязать устройства к пользователям	пп. 2.2.8.1
		Привязать устройства к группам	пп. 2.2.9.1
		Активировать	пп. 2.2.10.2
		Архивировать	пп. 2.2.13.1
		Удалить	пп. 2.2.15.2
Группы устройств		Активация устройств (активация с помощью JSON-файла)	пп. 2.2.10.4
Пользователи		Привязать пользователей к группам	пп. 2.3.4.1
		Привязать устройства к пользователям	пп. 2.3.5.1
		Архивировать пользователя	п. 2.3.7
Группы пользователей		Привязать пользователей к группам	пп. 2.3.4.1
Сценарии		Назначить офлайн-сценарии на группу пользователей	пп. 2.5.2.2
		Назначить офлайн-сценарии на группу устройств	пп. 2.5.2.2
		Удалить офлайн-сценарий	п. 2.5.4
Файлы		Удалить файл	пп. 2.6.1.6

Для доступа к списку быстрых действий необходимо установить галочку в чекбоксе напротив выбранного элемента управления (Рисунок 5).

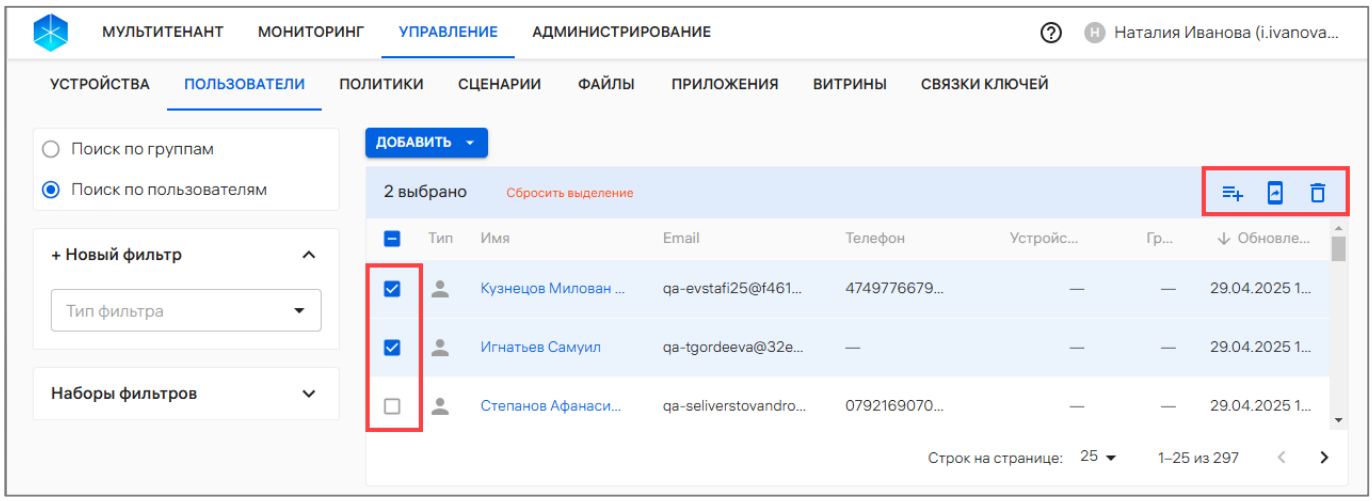


Рисунок 5

1.4. Работа с фильтрами

Область фильтров Консоли администратора ПУ позволяет выполнить поиск по критериям, доступным из раскрывающегося списка в следующих подразделах раздела «Управление»:

– «Устройства» – поиск устройств, групп устройств и событий безопасности устройств;

– «Пользователи» – поиск пользователей устройств, групп пользователей;

– «Политики» – поиск политик.

В таблице (Таблица 2) приведены фильтры для поиска информации в соответствующих разделах.

Таблица 2

Подраздел	Фильтры	Доступные значения
Поиск по устройствам		
Подраздел «Устройства» (поиск доступен также и внутри карточки группы устройств – предусмотрена возможность найти устройство, входящее в конкретную группу)	По идентификатору	Ввод значения с клавиатуры. Поиск по идентификатору устройства: – «По IMEI» – поиск по международному идентификатору устройства; – «По SN» – поиск по серийному номеру устройства; – «По Ethernet MAC» – поиск по MAC-адресу Ethernet устройства; – «По WLAN MAC» – поиск по MAC-адресу WLAN устройства. Например, «00:aa:00:00:a0:00»; – «По сетевому имени компьютера» – поиск по сетевому имени компьютера (hostname);

Подраздел	Фильтры	Доступные значения
		– «По IP-адресу устройства» – поиск устройств по IP-адресу; – «Имя устройства» - поиск по имени устройства. **ПРИМЕЧАНИЕ.** Доступно применение нескольких идентификаторов поиска одновременно
	По UUID	Поиск по идентификатору устройства. Ввод значения с клавиатуры
	Жизненный цикл	Поиск по статусу жизненного цикла устройства. Выбор значения из списка: – «Зарегистрировано»; – «В процессе активации»; – «Активировано»; – «Не активировано»; – «Очищено»; – «Архивное»
	Клиент АЦ	Поиск устройства по статусу наличия приложения «Аврора Центр» на устройстве. Выбор значения из списка: – «Установлен»; – «Удален»; – «Неизвестно»
	По соответствию политике	Поиск устройства по соответствию назначенным политикам. Выбор значения из списка: – «Соответствует»; – «Не соответствует»; – «Не управляется»
	По дате создания	Поиск по дате добавления устройства за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате обновления устройства за выбранный период. Выбор значения из календаря
	По дате подключения	Поиск по дате подключения устройства за выбранный период. Выбор значения из календаря

Подраздел	Фильтры	Доступные значения
	По модели	Выбор модели устройства из списка. Если нужной модели нет в списке, необходимо добавить ее (п. 2.2.4)
	По платформе	Выбор платформы: – «Аврора»; – «Android»; – «Linux»
	По группе	Поиск устройства по заданной группе. Ввод значения с клавиатуры
	По множеству	Поиск устройства по вхождению в множество. Ввод значения с клавиатуры
	По комментарию	Поиск устройства по комментарию. Ввод значения с клавиатуры
Поиск событий безопасности		
Подраздел «Устройства» → карточка устройства → вкладка «События безопасности»	По типу события	Поиск по типу события безопасности. Выбор значения из раскрывающегося списка: – «Информационное»; – «Отладочное»; – «Предупреждение»; – «Критическое»
	По имени события	Поиск по названию события безопасности. Выбор значения из списка
	По дате получения	Поиск по дате получения события безопасности за выбранный период. Выбор значения из календаря
	По дате возникновения	Поиск по дате возникновения события безопасности за выбранный период. Выбор значения из календаря
Поиск файлов		
Подраздел «Устройства» → карточка устройства → вкладка «Файлы»	По тэгу файла	Поиск диагностических отчетов

Подраздел	Фильтры	Доступные значения
Поиск событий журнала приложения «Аврора Центр»		
Подраздел «Устройства» → карточка устройства → вкладка «Журнал»	По результату	Поиск по статусу успешности события. Выбор значения из раскрывающегося списка: – «Успешно»; – «Неуспешно»
	По дате возникновения	Поиск по дате возникновения события безопасности. Выбор значений из календаря
Поиск учетных записей		
Подраздел «Устройства» → карточка устройства → вкладка «Учетные записи»	По типу учетной записи	Поиск учетных записей. Выбор значения из раскрывающегося списка: – «Системный»; «Несистемный»
Поиск приглашений		
Подраздел «Устройства» → «Приглашения»	По названию	Поиск по названию приглашения. Ввод значения с клавиатуры от двух символов или полное название приглашения
	По статусу	Доступные значения: – «Активно» - в списке отображаются только активные приглашения. **ВНИМАНИЕ!** По умолчанию при переходе во вкладку «Приглашения» автоматически применяется фильтр «Активно» и отображаются только активные приглашения. – «Отозвано» - в списке отображаются только отозванные приглашения. Если фильтр по статусу очищен, список отображается без ограничения по статусу
Поиск по группам устройств		
Подраздел «Устройства» → «Поиск по группам»	По названию	Поиск группы устройств по названию. Ввод значения с клавиатуры
	По принципу добавления	Поиск группы устройств по принципу добавления в группу. **ПРИМЕЧАНИЕ.** После применения фильтра в списке отображаются только динамические группы по выбранным критериям. Выбор значения из раскрывающегося списка:

Подраздел	Фильтры	Доступные значения
		– «Статус устройства» – поиск по статусу устройств. Выбор из списка: «Любое» или «Не задано»; – «Платформа устройства» – поиск по платформе устройств. Выбор из списка: «Любое» или «Не задано»; – «Объем жестких дисков» – поиск устройств по объему жестких дисков. Выбор из списка: «Любое» или «Не задано»; – «Количество процессорных ядер» – поиск устройств по количеству процессорных ядер. Выбор из списка: «Любое» или «Не задано»; – «Модель устройства» – поиск по модели устройств. Выбор из списка: «Любое» или «Не задано»; – «Тип устройства» – поиск по типу устройств. Выбор из списка: «Любое» или «Не задано»; – «Объем оперативной памяти» – поиск устройств по объему оперативной памяти. Выбор из списка: «Любое» или «Не задано»; – «Сетевое имя компьютера» – поиск устройств по сетевому имени компьютера. Выбор из списка: «Любое» или «Не задано»; – «Результат выполнения скрипта» – поиск устройств по результатам выполнения скрипта. Выбор из списка: «Любое» или «Не задано»; – «IP-адрес устройства» – поиск устройств по IP-адресу. Выбор из списка: «Любое» или «Не задано»; – «Производитель» – поиск устройств по названию производителя. Выбор из списка: «Любое» или «Не задано»; – «Программное обеспечение» – поиск устройств по наличию критерия программного обеспечения. Выбор из списка: «Любое» или «Не задано»;

Подраздел	Фильтры	Доступные значения
		– «Root-права» – поиск устройств по наличию root-прав. Выбор из списка: «Любое» или «Не задано»; – «Шифрование файлового хранилища» – поиск устройств по наличию шифрования файлового хранилища. Выбор из списка: «Любое» или «Не задано»; – «Версия ОС» – поиск по версии ОС на устройствах. Выбор из списка: «Любое» или «Не задано»; – «Сценарий по смене SIM» – поиск устройств по наличию сценария по смене SIM. Выбор из списка: «Любое» или «Не задано»; – «Директория LDAP» – поиск по директории LDAP. Выбор из списка: «Любое», «Не задано» или «Директория по названию из списка существующих директорий LDAP»
	По дате создания	Поиск по дате добавления группы устройств за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате обновления группы устройств за выбранный период. Выбор значения из календаря
Поиск по множествам		
Подраздел «Устройства» → «Поиск по множествам»	По названию	Поиск множеств по названию. Ввод значения с клавиатуры
	По UUID устройства	Поиск по идентификатору устройства. Ввод значения с клавиатуры
	По UUID группы	Поиск по идентификатору группы устройств/пользователей. Ввод значения с клавиатуры
	По дате создания	Поиск по дате создания множества. Выбор значений из календаря
	По дате обновления	Поиск по дате обновления множества. Выбор значений из календаря

Подраздел	Фильтры	Доступные значения
Поиск по пользователям		
Подраздел «Пользователи» → «Поиск по пользователям». (поиск доступен также и внутри карточки группы пользователей – предусмотрена возможность найти пользователя, входящего в конкретную группу)	По Email	Поиск по адресу рабочей почты пользователя
	По имени	Поиск по имени, фамилии, отчеству
	По фамилии	
	По отчеству	
	По дате создания	Поиск по дате добавления пользователя за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате обновления пользователя за выбранный период. Выбор значения из календаря
Поиск по группам пользователей		
Подраздел «Пользователи» → «Поиск по группам»	По названию	Поиск группы пользователей устройств по названию. Ввод значения с клавиатуры
	По типу группы	Поиск группы пользователей по типу группы: – «Группа пользователей»; – «Орг.подразделение»
	По принципу добавления	Поиск группы пользователей по принципу добавления в группу. Выбор значения из раскрывающегося списка: – «По дополнительным атрибутам пользователя LDAP»
	По дате создания	Поиск по дате добавления группы пользователей за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате обновления группы пользователей за выбранный период. Выбор значения из календаря
Поиск политик		
Политики	По названию	Поиск по названию. Ввод значения с клавиатуры
	По дате создания	Поиск по дате добавления политики за выбранный период. Выбор значения из календаря
	По дате обновления	Поиск по дате обновления политики за выбранный период. Выбор значения из календаря

Подраздел	Фильтры	Доступные значения
	По правилу политики	Поиск по правилу, добавленному в политику. Выбор значения из списка (доступные значения приведены в таблице (Таблица 45)
	По наличию переменной	Поиск по управляемой переменной. Выбор значения из раскрывающегося списка. ПРИМЕЧАНИЕ. Фильтр можно использовать для поиска политик сразу по нескольким управляемым переменным. Если задано более одной управляемой переменной, то поиск осуществляется с использованием логического оператора «И»
Поиск защищенных переменных		
Подраздел «Настройки» → «Перейти на страницу переменных к подстановке»	По названию	Поиск управляемой переменной по названию. Ввод значения с клавиатуры
	По защищенности	Поиск управляемой переменной по признаку защищенности. Выбор значения из раскрывающегося списка: – «Защищенная» - поиск защищенных переменных; – «Незащищенная» - поиск незащищенных переменных
	По блокировке	Поиск управляемой переменной по действию блокировки. Выбор значения из раскрывающегося списка: – «Действует» - поиск заблокированных переменных; – «Не действует» - поиск незаблокированных переменных

ВНИМАНИЕ! В данном пункте описаны общие принципы работы с фильтрами на примере подраздела «Пользователи».

Для поиска по заданным критериям требуется выполнить следующие действия:

– перейти в необходимый подраздел интерфейса ППО;

– выбрать из раскрывающегося списка «Тип фильтра» один из фильтров для поиска и задать параметры (Рисунок 6).

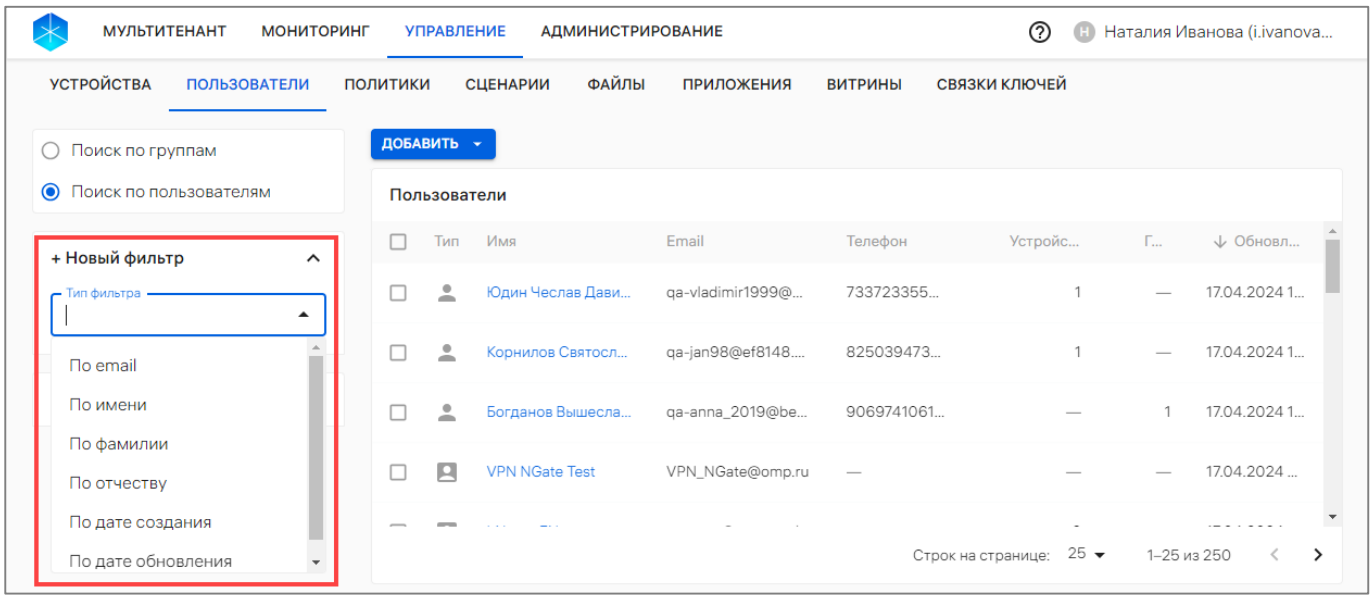


Рисунок 6

При вводе значения с клавиатуры (минимальная длина поискового запроса – 3 символа), а также выборе значения в календаре необходимо нажать соответствующую кнопку для применения фильтра, а при выборе значения из раскрывающегося списка фильтр будет применен автоматически.

Для формирования расширенного поиска по заданным критериям возможно задать несколько фильтров одновременно. В результате в рабочей области отобразится перечень элементов управления, сформированный на основании применения установленных фильтров. При необходимости для удаления фильтра следует нажать значок (Рисунок 7 [1]). Для сброса всех выбранных фильтров необходимо нажать кнопку «Сбросить все» (Рисунок 7 [2]).

Также при необходимости примененные фильтры можно сохранить в набор фильтров, выполнив следующие действия:

– нажать кнопку «Сохранить» (Рисунок 7 [3]);

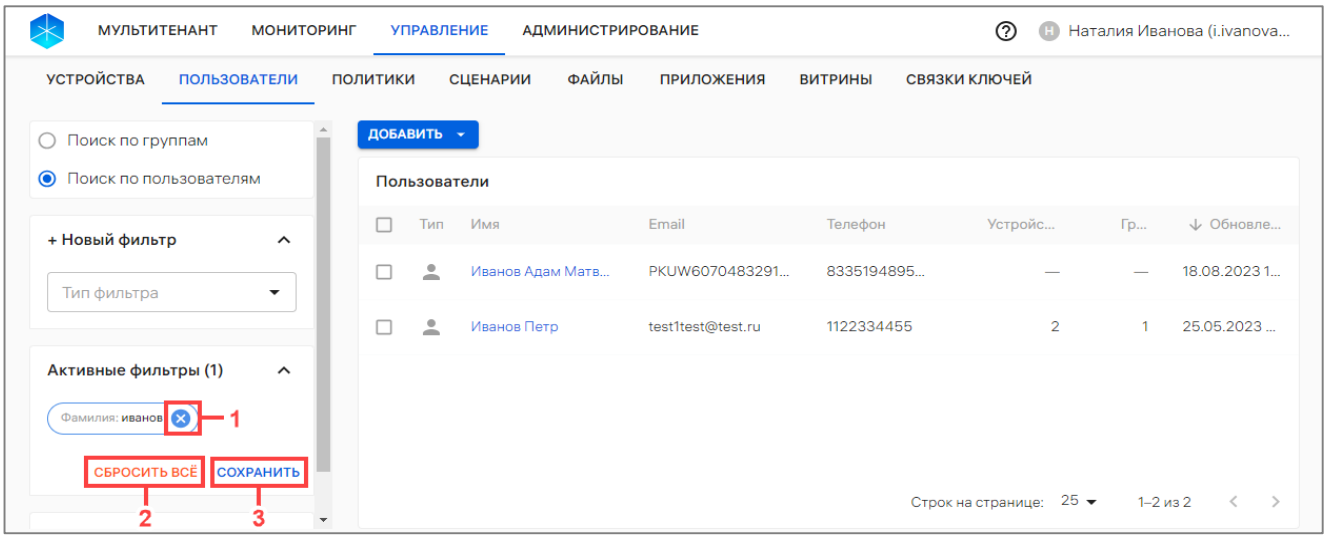


Рисунок 7

– в отобразившемся окне ввести имя набора фильтров;
– нажать кнопку «Создать».

В результате выбранная комбинация фильтров будет сохранена в набор фильтров, который при необходимости возможно удалить нажатием значка (Рисунок 8) или отредактировать его название нажатием значка .

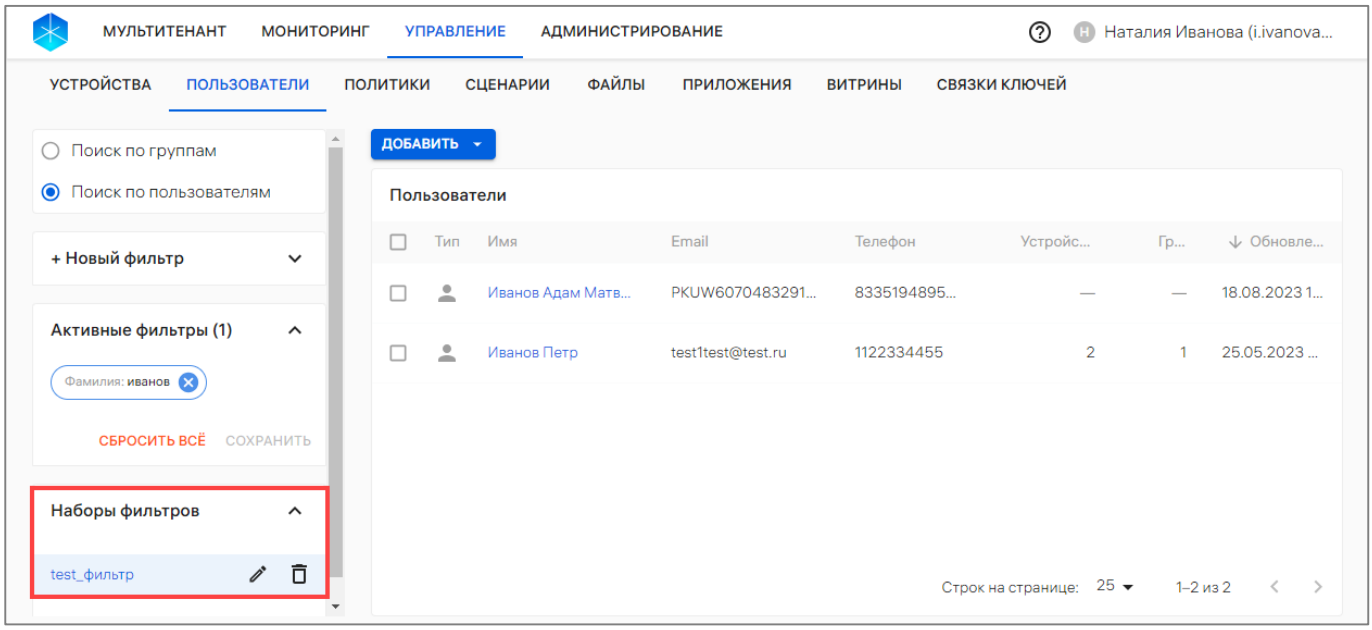


Рисунок 8

ПРИМЕЧАНИЕ. При выходе из Консоли администратора ПУ и повторном входе под этой же учетной записью сохраненные фильтры будут доступны.

2. РАБОТА В РАЗДЕЛЕ «УПРАВЛЕНИЕ» КОНСОЛИ АДМИНИСТРАТОРА ПУ

2.1. Общее описание карточек элементов управления

2.1.1. Работа с карточкой устройства

С помощью карточки устройства возможно выполнить следующие действия:

– просмотр детальной информации об устройстве;
– редактирование данных об устройстве;
– активация устройств;
– отправка оперативной команды на устройство;
– привязка к пользователю/группе устройств;
– удаленное подключение к рабочему столу устройства;
– просмотр событий безопасности устройств;
– архивирование устройств;
– удаление устройств.

Для просмотра карточки устройства необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;
– для отображения списка устройств выбрать в области фильтров «Поиск по устройствам»;
– нажать на значок в столбце «Карточка»;

В результате откроется карточка устройства, интерфейс которой включает:

– общую информацию об устройстве (Рисунок 9 [1]), состоящую из параметров, приведенных в таблице (Таблица 3);

Таблица 3

Параметр	Описание
Модель	– название модели устройства; – модель устройства (Приложение 1). **ПРИМЕЧАНИЕ.** Если устройство было импортировано из LDAP, то будет отображаться значение «LDAP устройство»
ID	Идентификатор устройства, который можно скопировать, нажав значок
IMEI	IMEI устройства, который можно скопировать, нажав значок
IP-адреса	IP-адрес устройства, который можно скопировать, нажав значок **ПРИМЕЧАНИЕ.** Параметр является инвентаризационным признаком. При наведении курсора на значок напротив параметра отобразится соответствующая подсказка

Параметр	Описание
Ethernet MAC	MAC-адрес Ethernet устройства, который можно скопировать, нажав значок
SN	Серийный номер устройства, который можно скопировать, нажав значок
WLAN MAC	MAC-адрес WLAN устройства, который можно скопировать, нажав значок
Сетевое имя	Сетевое имя компьютера, которое можно скопировать, нажав на значок . **ПРИМЕЧАНИЕ.** Параметр является инвентаризационным признаком (если устройство не подключено к корпоративной сети/не введено в домен). При наведении курсора на значок напротив параметра отобразится соответствующая подсказка
Имя	Имя устройства, которое можно скопировать, нажав на значок . **ПРИМЕЧАНИЕ.** Необязательный параметр «Имя устройства» является инвентаризационным признаком. В случае его отображения в карточке устройства, при наведении курсора на значок напротив параметра отобразится соответствующая подсказка
Статус	Статус жизненного цикла устройства/соответствия политике
Клиент АЦ (Аврора Центр)	Версия приложения «Аврора Центр» подсистемы ППО, которое установлено на устройство. **ПРИМЕЧАНИЕ.** Если приложение «Аврора Центр» было удалено с устройства, то будет отображено сообщение «Клиент удален». Если устройство не активировано, то отображается «—»
Клиент АМ (Аврора Маркет)	Версия приложения «Аврора Маркет» подсистемы ППО, которое установлено на устройство
Создано	Дата и время добавления устройства
Обновление	Дата и время внесения последних изменений в устройство (редактирование имени устройства, модели или комментария; привязка/отвязка к группам или пользователям; назначение/отвязка политики или офлайн-сценария на устройство)
Подключение	Дата и время последнего подключения устройства к ППО
Комментарий к устройству	Дополнительная информация об устройстве (заполняется при необходимости)

– оперативное управление (Рисунок 9 [4]), применение которого приведено в п. 2.2.11;

– вкладки карточки (Рисунок 9 [2]) с дополнительной информацией об устройстве:

- «Состояние» (пп. 2.1.1.1);
- «Управление» (пп. 2.1.1.2);
- «Пользователи» (пп. 2.1.1.3);
- «Группы» (пп. 2.1.1.4);
- «Политики» (пп. 2.1.1.5);
- «Сценарии» (пп. 2.1.1.6);
- «Удаленный доступ» (пп. 2.1.1.7);
- «События безопасности» (пп. 2.1.1.8);
- «Приложения» (пп. 2.1.1.9);
- «Карта» (пп. 2.1.1.10);
- «События восстановления» (пп. 2.1.1.11);
- «Файлы» (пп. 2.1.1.12);
- «Журнал» (пп. 2.1.1.13);
- «Учетные записи» (пп. 2.1.1.14).

При нажатии на значок ⋮ (Рисунок 9 [3]) будут доступны следующие действия:

– Редактировать данные (внести необходимые изменения);

– Активировать повторно (пп. 2.2.10.1);

– Архивировать (пп. 2.2.13.2);

– Удалить (п. 2.2.15).

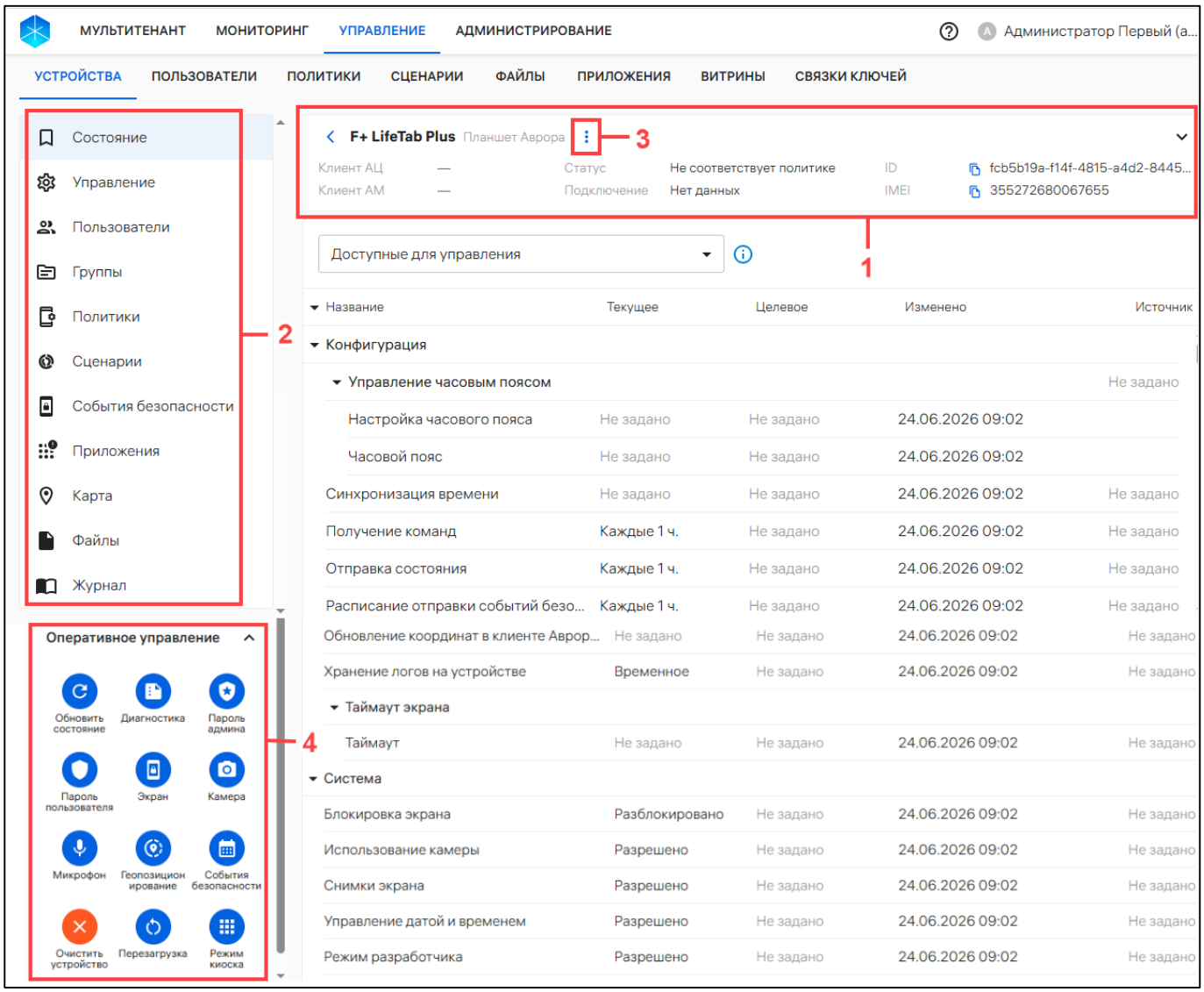

МУЛЬТИТЕНАНТ
МОНИТОРИНГ
УПРАВЛЕНИЕ
АДМИНИСТРИРОВАНИЕ
Администратор Первый (a...
УСТРОЙСТВА
ПОЛЬЗОВАТЕЛИ
ПОЛИТИКИ
СЦЕНАРИИ
ФАЙЛЫ
ПРИЛОЖЕНИЯ
ВИТРИНЫ
СВЯЗКИ КЛЮЧЕЙ
Состояние
Управление
Пользователи
Группы
Политики
Сценарии
События безопасности
Приложения
Карта
Файлы
Журнал
Оперативное управление
Обновить состояние
Диагностика
Пароль админа
Пароль пользователя
Экран
Камера
Микрофон
Геопозицион ирование
События безопасности
Очистить устройство
Перезагрузка
Режим киоска
F+ LifeTab Plus
Планшет Аврора
Клиент АЦ
Клиент АМ
Статус
Не соответствует политике
Подключение
Нет данных
ID
fcb5b19a-f14f-4815-a4d2-8445...
IMEI
355272680067655
Доступные для управления
Название
Текущее
Целевое
Изменено
Источник
Конфигурация
Управление часовым поясом
Не задано
Настройка часового пояса
Часовой пояс
Синхронизация времени
Получение команд
Каждые 1 ч.
Отправка состояния
Расписание отправки событий безо...
Обновление координат в клиенте Аврор...
Хранение логов на устройстве
Временное
Таймаут экрана
Таймаут
Система
Блокировка экрана
Разблокировано
Использование камеры
Разрешено
Снимки экрана
Управление датой и временем
Режим разработчика
24.06.2026 09:02
1
2
3
4

Рисунок 9

2.1.1.1. Вкладка «Состояние»

Во вкладке «Состояние» предусмотрена возможность управлять отображением полей состояния по следующим параметрам (Рисунок 10 [1]):

– «Все» – отображаются все параметры;

– «Доступные для управления» – отображаются параметры, которые изменяются при назначении команд оперативного управления, политик и офлайн-сценариев (значение выставлено по умолчанию);

– «Под управлением» – отображаются параметры, измененные назначенными командами оперативного управления, политиками и офлайн-сценариями, которые находятся под управлением политики или оперативной команды.

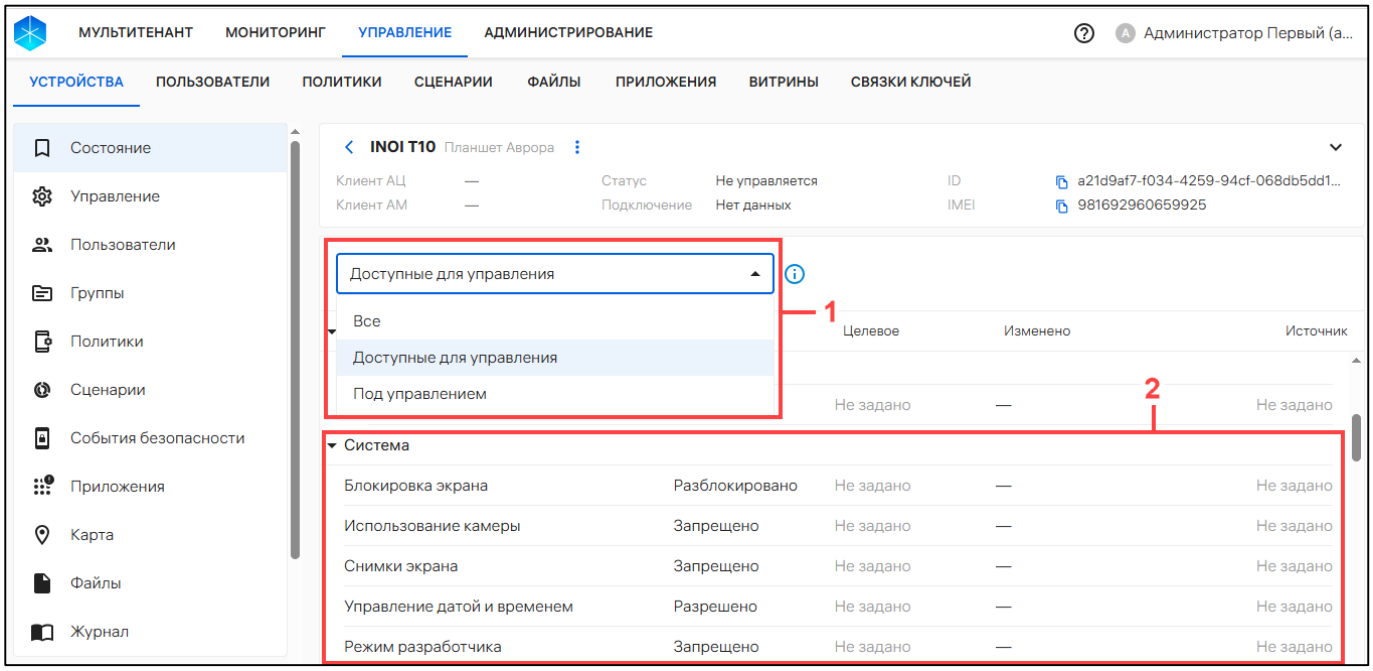


Рисунок 10

Для получения данных о состоянии активированного устройства в любом статусе необходимо создать и назначить на устройство политику отправки состояния или отправить оперативную команду «Обновить состояние». Подробное описание создания и назначения политики приведено в подразделе 2.4.

После получения данных о состоянии устройства отображается подробная информация о назначенных политиках и оперативных командах, а также параметры подключения к подсистеме Сервис уведомлений (ПСУ), входящей в состав ППО (если подключение к ПСУ зарегистрировано) в следующих столбцах (см. Рисунок 10 [2]):

– «Название» – название оперативных команд, группы политик или состояний;

– «Текущее» – последнее подтвержденное состояние устройства;

– «Целевое» – состояние, к которому устройство должно быть приведено;

– «Изменено» – дата и время изменения состояния устройства (например, после назначения (изменения) политики, офлайн-сценария или оперативной команды, перемещения устройства между группами и т.п.);

– «Источник» – источник целевого состояния (название политики, скомбинированная политика, оперативное управление).

ПРИМЕЧАНИЕ. При назначении на устройстве нескольких политик в столбце «Источник» отображаются все политики, из которых получена комбинированная политика. Например, если 3 политики назначены на устройство, при этом в 2 из них использование камеры запрещено, а в 1 – разрешено, то отобразятся политики с запретом использования камеры.

Если политика или оперативная команда не были получены на устройство, то текущее состояние и целевое состояние устройства не будут совпадать. Несоответствия выделяются красным цветом, и отображается значок .

Во вкладке «Состояние», в зависимости от версии ОС, возможно просмотреть и задать состояния на устройство, подробное описание которых приведено в таблице (Таблица 4).

ПРИМЕЧАНИЕ. Если значение целевого состояния устройства не отправлено, то в столбце «Текущее» будет отображаться «Не задано».

Таблица 4

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Свойства				
Серийный номер	Серийный номер, присвоенный устройству производителем. Может содержать от 1 до 20 символов	+	+	-
Производитель	Компания-производитель устройства	+	+	+
Модель	Модель устройства	+	+	+
Настройки Сервиса уведомлений				
ID приложения	Идентификатор приложения, с которым приложение «Аврора Центр» регистрируется в ПСУ	+	+	-
Адрес	Адрес Сервиса уведомлений для приложения «Аврора Центр»	+	+	-
Порт	Номер порта для подключения приложения «Аврора Центр»	+	+	-
SSL: Валидация сертификата	Включение или отключение валидации сертификата ПСУ. **ПРИМЕЧАНИЕ.** Поле отображается, только если настройка была добавлена в конфигурационный файл ППО. Возможные значения: – «Включено»; – «Выключено» Если устройство не зарегистрировано в ПСУ либо ПСУ отсутствует, по умолчанию выставлено значение «Не задано»	+	+	-
CRL: Интервал обновления в секундах	Временной интервал обновления списка отозванных сертификатов. **ПРИМЕЧАНИЕ.** Поле отображается, только если настройка была добавлена в конфигурационный файл ППО	+	+	-
CRL: Проверка отзыва сертификатов	Включение или отключение проверки наличия сертификата ПСУ среди списка отозванных сертификатов. **ПРИМЕЧАНИЕ.** Поле отображается, только если настройка была добавлена в конфигурационный файл ППО. Возможные значения: – «Включено»; – «Выключено». Если устройство не зарегистрировано в ПСУ либо ПСУ отсутствует, по умолчанию выставлено значение «Не задано»	+	+	-
SSL: Уровень валидации сертификата	Уровень валидации имени хоста, указанного в сертификате ПСУ. **ПРИМЕЧАНИЕ.** Поле отображается, только если настройка была добавлена в конфигурационный файл ППО. Возможные значения: – «Не проверяется»; – «Поддержка поддоменов»; – «Точное совпадение». Если устройство не зарегистрировано в ПСУ либо ПСУ отсутствует, по умолчанию выставлено значение «Не задано»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Настройки LDAP				
OIDC Клиент	Идентификатор клиента, необходимый для аутентификации в LDAP	+	+	-
Настройки проверки подключения к сети				
Адрес IPv4	Адрес IPv4 для проверки доступа к сети Интернет у устройства. **ПРИМЕЧАНИЕ.** Задается в конфигурационном файле ППО `(/var/ocs/config/subsystems/emm/applications/ocs-emm-state-manager-api/ocs-emm-state-manager-api.yml` параметр `networkCheckSettings.ipv4Url`) и передается на устройство при его активации или подключении к серверу	+	-	-
Адрес IPv6	Адрес IPv6 для проверки доступа к сети Интернет у устройства. **ПРИМЕЧАНИЕ.** Задается в конфигурационном файле ППО `(/var/ocs/config/subsystems/emm/applications/ocs-emm-state-manager-api/ocs-emm-state-manager-api.yml` параметр `networkCheckSettings.ipv6Url`) и передается на устройство при его активации или подключении к серверу	+	-	-
Настройки сервера времени				
Адреса	Список адресов серверов времени NTP. Например: `ntp1.vniiftri.ru, ntp2.niiftri.irkutsk.ru, vniiftri2.khv.ru.` **ПРИМЕЧАНИЕ.** Задаются в конфигурационном файле ППО `(/var/ocs/config/subsystems/emm/applications/ocs-emm-state-manager-api/ocs-emm-state-manager-api.yml` параметр `timeServerSettings.hosts`) и передается на устройство при его активации или подключении к серверу	+	-	-
Конфигурация				
Управление часовым поясом				
Настройка часового пояса	Режим настройки часового пояса на устройстве	+	-	-
Часовой пояс	Выбранный часовой пояс на устройстве	+	-	-
Синхронизация времени	Режим синхронизации времени на устройстве	+	-	-
Получение команд	Расписание на получение оперативных команд и заданных на устройствах политик и офлайн-сценариев. Значение в формате «Каждые [дд] дн. [чч] ч.»	+	+	+
Отправка состояния	Расписание отправки состояния устройства на ПУ. Значение в формате «Каждые [дд] дн. [чч] ч.»	+	+	+
Расписание отправки событий безопасности	Расписание отправки сообщений о событиях безопасности, произошедших на устройстве. Значение в формате «Каждые [дд] дн. [чч] ч.»	+	-	-
Исключения событий безопасности	Уровень событий безопасности процесса, который не будут отправляться в Аврора Центр	+	-	-
Обновление координат в клиенте Аврора Центр	Частота обновления координат в приложении «Аврора Центр». Значение в формате «Каждые [чч] ч. [мм] м [сс] с»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Хранение логов на устройстве	Тип хранения системных сообщений на устройствах. Возможные значения: – «Временное»; – «Постоянное»	+	-	-
Настройки правил политик (параметр отображается в ППО релиз 5.2.0 и выше)				
Запрет удаления приложений	Отображается одно из значений в текущем состоянии устройства в зависимости от выбранных настроек в разделе «Администрирование» → «Настройки» (п. 4.1.7). В целевом состоянии устройства отображается прочерк. Возможные значения: – «Действует»; – «Не действует»	+	+	+
Запрет удаления файлов		+	+	+
Запрет удаления скриптов		+	+	+
Создание точек восстановления				
Исключаемые директории	Директории, которые не попадут в точку восстановления	-	+	+
Интервал автоматического восстановления	Временной интервал. Если после применения политики, соответствующей режиму работы, связь с ППО оборвется более чем на указанный интервал, произойдет автоматический откат изменений на последнюю точку восстановления	-	+	+
Режим работы	Режим работы создания точек восстановления. Возможные значения: – «Всегда»; – «Только при применении правил, меняющих Файловую систему»	-	+	+
Статус	Статус создания точки восстановления. Например: «Создано»/«Не требуется»	-	+	+
Настройки прокси-сервера				
Хост	Хост прокси-сервера	-	-	+
Порт	Порт прокси-сервера	-	-	+
Имя пользователя	Имя пользователя для подключения через прокси-сервер	-	-	+
Хэш пароля	Хэш-сумма (sha256) пароля пользователя	-	-	+
Исключения из проксирования	Список хостов, которые будут исключены из проксирования	-	-	+
Таймаут экрана				
Таймаут	Время бездействия пользователя, после которого экран устройства блокируется	-	-	+
Корневые сертификаты (количество сертификатов)				
Название сертификата	В столбце «Текущее»/«Целевое» отображается цифровой отпечаток (Fingerprint) доверенного сертификата	+	+	-

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
	Удостоверяющий центр	Название удостоверяющего центра, выпустившего сертификат	+	+	-
	Дата выпуска	Дата выпуска сертификата	+	+	-
	Срок действия, до	Срок действия сертификата	+	+	-
	Таймаут экрана				
	Таймаут	Время бездействия пользователя, после которого экран устройства блокируется	+	+	-
Система					
Блокировка экрана		Разблокировка или блокировка экрана устройства, а также, в случае блокировки, сообщение, которое будет отображено на экране. Возможные значения: – «Разблокировано»; – «Заблокировано»	+	+	+
Использование камеры		Разрешение или запрет на использование камеры. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Снимки экрана		Разрешение или запрет на создание снимков экрана. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Управление датой и временем		Разрешение или запрет на внесение изменений в настройки даты и времени. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Режим разработчика		Разрешение или запрет на использование режима разработчика. Возможные значения: – «Доступен»; – «Недоступен»	+	+	-
Сброс к заводским настройкам		Разрешение или запрет на сброс устройства к заводским настройкам. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Использование микрофона	Разрешение или запрет на использование микрофона. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Отправка и получение SMS	Разрешение или запрет на отправку и получение SMS. Возможные значения: – «Разрешен(но)»; – «Запрещен(но)»	+	+	-
Root-права	Результат проверки устройства на наличие root-прав. Возможные значения: – «Не обнаружены»; – «—» (не известно); – «Неприменимо»	-	+	-
Шифрование файлового хранилища	Статус шифрования файлового хранилища. Возможные значения: – «Включено»; – «Выключено»; – «Не поддерживается»	-	+	-
Системные репозитории (сгруппированы по пронумерованным репозиториям)				
Параметры подключения	Информация о параметрах подключения к системному репозиторию	-	-	+
Требуется аутентификация	Определяет, требуется ли подключение к защищенному системному репозиторию. Возможные значения: – «Да»; – «Нет»	-	-	+
Flatpak репозитории (сгруппированы по пронумерованным репозиториям)				
Параметры подключения	Информация о параметрах подключения к flatpak репозиторию	-	-	+
Требуется аутентификация	Определяет, требуется ли подключение к защищенному flatpak репозиторию. Возможные значения: – «Да»; – «Нет»	-	-	+
Голосовые вызовы				
Исходящие вызовы	Разрешение или запрет выполнения исходящих звонков с устройства. Возможные значения: – «Разрешены»; – «Запрещены»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Входящие вызовы	Разрешение или запрет принятия входящих на устройства вызовов. Возможные значения: – «Разрешены»; – «Запрещены»	+	+	-
Параметры устройства				
Сетевое имя компьютера	Сетевое имя компьютера (hostname)	-	-	+
Тип устройства	Тип устройства – ПК/Ноутбук/Other	-	-	+
Серийный номер	Серийный номер, присвоенный устройству производителем. Может содержать от 1 до 20 символов	-	-	+
Объем жестких дисков	Общий объем жестких дисков на устройстве	-	-	+
Процессор				
Название	Название модели процессора	-	-	+
Частота	Частота процессора	-	-	+
Количество ядер	Количество ядер процессора	-	-	+
Звуковые устройства (список названий звуковых устройств ЭВМ). Получение информации о звуковых устройствах не поддерживается для ОС Astra Linux				
Название	Название звукового устройства ЭВМ	-	-	+
Мониторы, подключенные к устройству (сгруппированы по названиям мониторов). Получение информации о мониторах не поддерживается для ОС Astra Linux				
Интерфейс подключения	Информация о том, как подключен монитор к устройству	-	-	+
Размер матрицы	Размер матрицы монитора	-	-	+
Дата производства	Информация о дате производства монитора	-	-	+
Серийный номер	Серийный номер монитора	-	-	+
Память (список хранилищ устройств)				
Диски				
Тип физического диска	Тип физического диска. Возможные значения: HDD, SSD	-	-	+
Интерфейс физического диска	Интерфейс диска. Возможные значения: SATA, NVME	-	-	+
Серийный номер диска	Серийный номер диска	-	-	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Разделы (сгруппированы по названиям разделов). Разделы на физическом диске, доступные на устройстве				
Общий объем	Общий объем памяти раздела	+	+	+
Доступный объем	Доступный объем памяти раздела	+	+	+
Свободно	Свободный объем памяти раздела	+	+	+
Тип файловой системы	Тип файловой системы	-	-	+
Название раздела	Название партиции каталога	-	-	+
Название диска	Название диска, на котором присутствует этот каталог	-	-	+
ОЗУ (оперативная память устройства)				
Объем RAM	Объем оперативной памяти	-	-	+
Тип RAM	Тип оперативной памяти	-	-	+
Количество занятых слотов	Количество занятых слотов для оперативной памяти на устройстве	-	-	+
Количество свободных слотов	Количество свободных слотов для оперативной памяти на устройстве	-	-	+
Батарея (сгруппированы по элементам питания)				
Уровень заряда	Уровень заряда аккумулятора устройства	+	+	+
Заряжается	Заряжался ли аккумулятор устройства в момент отправки состояния. Возможные значения: – «Да»; – «Нет»	+	+	+
Износ батареи	Уровень износа элемента питания	+	+	+
Управление соединениями				
Управление авиарежимом	Разрешение или запрет на использование авиарежима. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-
Управление точкой доступа WLAN	Разрешение или запрет на изменение настроек мобильной точки доступа. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-
Использование браузера	Разрешение или запрет возможности использования браузера на устройстве. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Передача данных MTP	Разрешение или запрет возможности передачи данных по протоколу MTP. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-
Мобильная сеть				
Управление мобильной передачей данных	Разрешение или запрет на изменение настроек мобильной передачи данных	+	+	-
Точка доступа				
Имя	Имя точки доступа мобильной сети	+	+	-
APN	Хост точки доступа мобильной сети	+	+	-
MCC	Мобильный код страны	+	+	-
MNC	Код мобильной сети	+	+	-
Тип APN	По умолчанию значение «Интернет»	+	+	-
Тип аутентификации	По умолчанию значение «Нет»	+	+	-
Сетевые интерфейсы				
Название сетевого интерфейса				
Тип	Тип сетевого интерфейса	+	+	+
MAC	MAC-адрес сетевого интерфейса	+	+	+
IP-адрес	IP-адреса сетевого интерфейса	+	+	+
Метод получения IP	Информация о том, каким методом устройство получило IP-адрес	-	-	+
IP DHCP сервера	Информация об IP-адресе DHCP-сервера	-	-	+
DNS	Список IP-адресов, подключенных с помощью DNS	-	-	+
Шлюз	IP-адрес шлюз-сервера	-	-	+
WLAN				
Работа WLAN	Разрешение или запрет на использование сети WLAN. Возможные значения: – «Включен»; – «Выключен»	+	+	-
Управление WLAN	Разрешение или запрет изменения состояния адаптера сети WLAN. Возможные значения: – «Разрешено»; – «Запрещено»	+	+	-

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
Название WLAN		Название сети WLAN, к которой подключено устройство	+	+	-
MAC-адрес роутера		MAC-адрес роутера, к которому подключено устройство	+	+	-
	Подключения (созданные на устройствах подключения к сети WLAN, которые группируются по названиям подключений)				
	Название	Название беспроводной сети (Service Set Identifier) для подключения	+	+	-
	Скрытая сеть	Определяет, транслируется ли название беспроводной сети. Возможные значения: – «Да»; – «Нет»	+	+	-
	Автоподключение	Определяет, следует ли автоматически подключаться к беспроводной сети. Возможные значения: – «Да»; – «Нет»	+	+	-
	Настройка IP-адреса	Способ настройки/получения IP-адреса. Возможные значения: «Автоматически»	+	+	-
	Безопасность	Технология безопасности беспроводной сети. Возможные значения: – «WPA2»; – «WPA-EAP»	+	+	-
	Протокол	Протокол защиты беспроводной сети. **ПРИМЕЧАНИЕ.** Отображается для сети с WPA-EAP. Возможные значения: «TLS»	+	+	-
	Категория сертификата	Название категории, в рамках которой был выпущен пользовательский сертификат. **ПРИМЕЧАНИЕ.** Отображается для сети с WPA-EAP-TLS	+	+	-
	Тип аутентификации	Тип аутентификации пользователя. **ПРИМЕЧАНИЕ.** Отображается для сети с WPA-EAP-PEAP	-	+	-
	Идентификатор	Идентификатор пользователя для подключения к беспроводной сети. **ПРИМЕЧАНИЕ.** Отображается для сети с WPA-EAP-TLS и WPA-EAP-PEAP с типом идентификации по шаблону	+	+	-
	Логин	Логин пользователя для подключения к беспроводной сети. **ПРИМЕЧАНИЕ.** Отображается для сети с WPA-EAP-PEAP с типом идентификации по логину и паролю	-	+	-
	Хэш пароля	Хэш-значение пароля беспроводной сети (для WPA2) или пользователя (для WPA-EAP-PEAP). **ПРИМЕЧАНИЕ.** Отображается для сети с WPA2 и WPA-EAP-PEAP)	-	+	-

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
	VPN				
	Подключения (подключения VPN, созданные на устройстве с помощью политики)				
	Название (тип подключения)	Название подключения VPN. В скобках указывается тип подключения: – для устройств с ОС Аврора – КриптоПро NGate R2; – для устройств с ОС Android – Cisco AnyConnect/КриптоПро NGate R2	+	+	-
	Адрес сервера	Адрес сервера VPN	+	+	-
	Тип	Тип соединения VPN. Доступные значения: – КриптоПро NGate R2 – для ОС Аврора/ОС Android; – Cisco AnyConnect – для ОС Android	+	+	-
	Протокол (доступно для типа Cisco AnyConnect)	Протокол безопасности соединения VPN. Доступен только один протокол безопасности – SSL	-	+	-
	Категория сертификата (доступно для типа Cisco AnyConnect)	Название категории пользовательских сертификатов, в рамках которой выпущен сертификат для подключения VPN	-	+	-
	Тип аутентификации (доступно для типа КриптоПро NGate R2)	Тип аутентификации пользователя. Доступен только 1 тип аутентификации – «По логину и паролю»	+	+	-
	Логин (доступно для типа КриптоПро NGate R2)	Логин пользователя для подключения к VPN	+	+	-
	Автозапуск VPN (доступно для типа КриптоПро NGate R2)	Переключатель для автоматического подключения устройства к VPN	+	+	-
	Хэш серийного номера лицензии (доступно для типа КриптоПро NGate R2)	Хэш-значение серийного номера лицензии пользователя	+	+	-
	Bluetooth				
	Управление Bluetooth	Разрешение или запрет на внесение изменений в настройки и подключение к новым устройствам Bluetooth®. Возможные значения: – «Доступно»; – «Недоступно»	+	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Работа Bluetooth	Разрешение или запрет возможности использования Bluetooth®. Возможные значения: – «Включен»; – «Выключен»	+	+	-
NFC				
Управление NFC	Разрешение или запрет на изменение настроек NFC	+	+	-
Геопозиция				
Режим работы	Режим работы геопозиционирования. Возможные значения: – «Не задано»; – «Выключено»; – «Пользовательские настройки»; – «Сохранение заряда аккумулятора»; – «Только спутники»; – «Высокая точность»	+	+	-
Изменение настроек	Разрешение или запрет на внесение изменений в настройки геопозиционирования. Возможные значения: – «Разрешено»; – «Запрещено»	+	+	-
Работа геопозиции (GPS модуль)	Разрешение или запрет возможности внесения изменений в настройки геопозиции. Возможные значения: – «Включена»; – «Выключена»	+	+	-
AGPS	Наличие и отсутствие AGPS-модуля на устройствах. Возможные значения: – «Доступен»; – «Недоступен»	+	+	-
Активность AGPS	Активность AGPS-модуля при его наличии на устройствах. Возможные значения: – «Включен»; – «Выключен»	+	+	-
GPS-координаты	Географические координаты устройства (широта и долгота)	+	+	-
Время получения координат	Дата и время фиксации координат	+	+	-
Настройка LBS-сервиса				
LBS-сервис	Определяет, включен ли LBS-сервис	+	-	-

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
Выбор LBS-сервиса		Выбранный LBS-сервис	+	-	-
Переменная для API-ключа:					
	Переменная	Название управляемой переменной	+	-	-
	Версия переменной	Версия управляемой переменной	+	-	-
	Значение переменной	Значение управляемой переменной. Для защищенной переменной вместо значения отображается *****	+	-	-
	Блокировка переменной	Определяет, действует ли блокировка для управляемой переменной	+	-	-
Периодичность запросов		Интервал, с которым устройству необходимо обращаться к LBS- сервису	+	-	-
Режим экономии		Определяет, используется ли режим экономии LBS-запросов	+	-	-
Периодичность запросов в режиме экономии		Интервал, с которым устройству необходимо обращаться к LBS-сервису в режиме экономии	+	-	-
Настройка A-GNSS					
A-GNSS		Определяет, включен ли A-GNSS	+	-	-
Адрес сервера		Адрес SUPL-сервера. Например: supl.google.com	+	-	-
Порт		Порт SUPL-сервера	+	-	-
TLS-подключение		Определяет, защищено ли подключение по протоколу TLS	+	-	-
SIM-карты					
Слот SIM1 (то же для Слот SIM2)					
Номер телефона		Номер телефона, присвоенный оператором мобильной связи. Определяется на устройстве и передается в ППО только, если на устройство назначена политика с правилом «Мобильная сеть/Определение номера телефона (пп. 2.4.1.65)	+	+	-
IMEI		Уникальный номер SIM-карты	+	+	-
ICCID		Уникальный серийный номер SIM-карты	+	+	-
Активен		Активность SIM-карты. Возможные значения: – «Да»; – «Нет»	+	+	-
Защищена PIN-кодом		Защита SIM-карты PIN-кодом. Возможные значения: – «Да»; – «Нет»	+	+	-

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
	Голосовые вызовы	Разрешение или запрет голосовых вызовов. Возможные значения: – «Разрешена(ны)»; – «Запрещена(ны)»	+	+	-
	Мобильная передача данных	Разрешение или запрет на мобильную передачу данных. Возможные значения: – «Разрешена»; – «Запрещена»	+	+	-
Внешние накопители					
Использование USB-накопителей		Разрешение или запрет использования USB-накопителей. Возможные значения: – «Разрешено»; – «Запрещено»	+	-	+
Использование SD-карт		Разрешение или запрет использования SD-карт. Возможные значения: – «Разрешено»; – «Запрещено»	+	-	-
Проверки					
Наличие файлов и их содержимого (сгруппированы по путям к файлам). Для каждого файла отображается:					
Путь к файлу с шаблоном		Абсолютный путь до файла на устройстве, который содержит шаблон <<HOME>>	+	+	+
Найдено на устройстве		Определяет, есть ли файл на устройстве. Возможные значения: – «Не задано»; – «Да»; – «Нет»	-	+	+
Хеш MD5		Контрольная сумма MD5 файла	-	+	+
Комментарий		Комментарий к проверке наличия файла	-	+	+
	Проверка содержимого файла (сгруппированы по названиям проверок). Для каждого файла отображается:				
	Тип синтаксиса	Тип синтаксиса проверки	-	+	+
	Название параметра	Название параметра из проверяемого файла	-	+	+
	Название найдено в файле	Определяет, найдено ли название параметра в файле. Возможные значения: – «Не задано»; – «Да»; – «Нет»	-	+	+
	Значение параметра	Значение проверяемого параметра	-	+	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Значение найдено в файле	Определяет, найдено ли значение в файле. Возможные значения: – «Не задано»; – «Да»; – «Нет»	-	+	+
Символические ссылки (сгруппированы по путям к файлам со ссылками). Для каждого файла отображается:				
Путь к символической ссылке с шаблоном	Путь к символической ссылке, который содержит шаблон <<HOME>>	+	+	+
Статус	Статус проверки символической ссылки. Возможные значения: – «Успешно проверено»; – «Символическая ссылка не найдена»; – «Не является символической ссылкой»; – «Целевой путь не соответствует указанному»	-	-	+
Комментарий	Комментарий к проверке символической ссылки	-	-	+
Целевой путь	Целевой путь, к которому ведет символическая ссылка	-	-	+
Параметры безопасности (сгруппированы по путям к файлам или директориям). Для каждого файла или директории отображается:				
Путь с шаблоном	Путь до файла или директории, который содержит шаблон <<HOME>>	+	+	+
Найдено на устройстве	Определяет, есть ли файл или директория на устройстве. Возможные значения: – «Не задано»; – «Да»; – «Нет»	+	+	+
Комментарий	Комментарий к заданной проверке	+	+	+
Имя владельца	Имя владельца файла или директории на устройстве	+	+	+
Имя группы	Имя группы файла или директории на устройстве	+	+	+
Разрешения файловой системы	Разрешения элемента файловой системы	+	+	+
Базовые атрибуты	Базовые атрибуты файла или директории на устройстве	+	+	+
Расширенный атрибут N - расширенный атрибут файла или директории на устройстве:				
Ключ	Ключ расширенного атрибута файла или директории	+	+	+
Значение	Значение расширенного атрибута файла или директории	+	+	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Управление приложениями				
Установка приложений	Разрешение или запрет установки приложения на устройства. Возможные значения: – «Доступно»; – «Недоступно». Если значение целевого состояния устройства не отправлено, отображается «Не задано»	+	+	-
Установленные приложения (сгруппированы по названиям приложения)				
Статус	Статус установки приложения. Возможные значения: – «Установлено»; – «Ошибка скачивания приложения»; – «Ошибка установки приложения»; – «Неправильный хэш»; – «Тип приложения не поддерживается»; – «Не установлено: найдены критические уязвимости»; – «Внесено в запрещающий список»	+	+	+
Витрина	Название витрины приложения. В разделе текущего состояния отображается название витрины установленного приложения на устройстве. В разделе целевого состояния отображается название витрины приложения, указанного в политике, назначенной на устройствах	+	+	+
Наименование	Наименование приложения. В разделе текущего состояния отображается наименование установленного приложения на устройстве. В разделе целевого состояния отображается название приложения, указанного в политике, назначенной на устройствах	+	+	+
Версия	Версия приложения. В разделе текущего состояния отображается версия установленного приложения на устройстве. В разделе целевого состояния отображается версия приложения, указанного в политике, назначенной на устройствах	+	+	+
Автозапуск	Определяет включение автозапуска приложения. Возможные значения: – «Не задано»; – «Да»; – «Нет»	+	+	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Режим установки	Режим установки приложения на устройство. Возможные значения: – «Моментально»; – «По расписанию»	+	+	+
Период актуальности	Период актуальности установки приложения	+	+	+
Интервал установки	Время установки приложения на устройство (пример: с 14:00 до 15:00)	+	+	+
Часовой пояс	Часовой пояс, по времени которого будет выполнена установка приложения	+	+	+
Дата установки	Дата и время установки приложения на устройстве	-	+	+
Принудительное создание ярлыка	Статус создания ярлыка приложения (вынесение desktop-файлов устанавливаемого приложения на рабочий стол). Возможные значения: – «Не задано»; – «Создан»; – «Не создан»	+	-	-
Прикрепленные скрипты - информация о прикрепленных скриптах, которые должны выполниться после установки приложения (не действует для ОС Аврора и ОС Android)				
Перечень скриптов	Перечень скриптов, которые должны выполниться на устройстве после установки приложения	+	+	+
Информация по каждому прикрепленному скрипту	**ПРИМЕЧАНИЕ.** Информация указывается в группах, аналогичных группам из блока «Управление скриптами», приведенного ниже	+	+	+
Запрещенные приложения (сгруппированы по запрещенным пакетам)				
Название пакета	Название запрещенного пакета	+	+	+
Диапазон версий N	Диапазон запрещенных версий приложения (может быть несколько, N - номер диапазона). Если диапазон версий не был включен и задан при создании и назначении политики на группу устройств, то этот параметр не отображается	+	+	+
Статус	Статус присутствия приложения на устройстве. Возможные значения: – «Отсутствует на устройстве»; – «Присутствует на устройстве»	+	+	+
Дата удаления	Дата и время удаления приложения на устройстве	-	+	+
Дата установки	Дата и время установки запрещенного приложения. **ПРИМЕЧАНИ**Е. Параметр отображается только, если приложение из запрещенного списка было установлено на устройстве	-	-	+

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
	Авторизованные пользователи на дату установки	Пользователи, которые были авторизованы на устройстве на дату и время установки приложения из запрещенного списка. Пользователи сгруппированы по типу подключения (например: XRDP, SSH и другие): – **Пользователь N** – информация о логине пользователя. **ПРИМЕЧАНИЯ:** ✓ Список пользователей в формате .json можно скопировать в буфер обмена с помощью кнопки «Скопировать в буфер обмена». Если информации ни об одном пользователе не получено с устройства, в текущем состоянии отображается «Нет данных». В остальных случаях (например, для ОС Аврора и ОС Android) отображается прочерк; ✓ В списке не будут отображаться LDAP- пользователи, авторизованные через оболочку ОС с постфиксом или доменом; ✓ Сессии пользователя, которые были завершены аварийно (например, вследствие разрядки аккумулятора или отключения питания устройства), не будут учитываться при составлении списка авторизованных пользователей на дату установки запрещенного пакета	-	-	+
	Исключения из запрещенных приложений (сгруппированы по пакетам-исключениям из запрещенных)				
	Название пакета	Название пакета, исключенного из запрещенного списка	+	+	+
	Диапазон версий N	Диапазон версий приложения, исключенных из списка запрещенных (может быть несколько, N - номер диапазона). Если диапазон версий не был включен и задан при создании и назначении политики на группу устройств, то этот параметр не отображается	+	+	+
	Ограничение установки из источников				
	Ограничение установки приложений из источников	Возможные значения: – «Запрещено из любых источников»; – «Запрещено из неизвестных источников»; – «Разрешено из всех источников»	+	+	+
Подключенные витрины в клиенте Аврора Маркет					
	Название витрины	Для каждой витрины отображается: – «Идентификатор» - идентификатор подключаемой витрины; – «ApiURI» - ресурс для обращения приложения «Аврора Маркет» по API. **ПРИМЕЧАНИЕ.** В случае, если: – была задана подключаемая витрина с другого инстанса, то вместо названия витрины будет отображаться прочерк; – в настройках доступа подключаемой витрины в «Подключаемые Платформы управления» значение равное «Запрещено всем», то вместо названия витрины будет отображаться прочерк. **ВНИМАНИЕ!** Факт применения политики с подключением витрин посредством приложения «Аврора Центр» фиксируется в журнале независимо от итогового результата добавления данных приложением «Аврора Маркет». Например, приложение «Аврора Центр» успешно получает политику и сохраняет данные витрин в локальную базу данных, но при этом приложение «Аврора Маркет» не может добавить одну из витрин. Несмотря на это, в карточке устройства будет отображаться соответствие политикам	-	-	+

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
Диагностика ОС					
Проверка установленных пакетов на устройстве (сгруппированы по названиям пакетов). Для каждого пакета отображается:					
	Статус	Статус присутствия версии пакета на устройстве. Возможные значения: – «Установлена»; – «Не установлена»; – «Установлена версия не входящая в диапазон»; – «Хеш не соответствует»	+	+	+
	Диапазон версий N	Диапазон целевых версий пакета. Может быть несколько, N – номер диапазона. В целевом состоянии отображается диапазон целевых версий пакета. В текущем состоянии - номер версии пакета на устройстве. Если диапазон версий не был включен и задан при создании и назначении политики на группу устройств, то отображается значение «Все»	+	+	+
	Хеш MD5	Контрольная сумма MD5 пакета (версии пакета)	+	+	+
Управляемые конфигурации приложений (сгруппированы по названиям приложений). Для каждого приложения отображается:					
	Статус	Статус применения конфигурации приложения. Возможные значения: – «Не задано»; – «Успешно»; – «Неуспешно»	+	+	+
	Конфигурация	Конфигурация приложения в формате JSON	+	+	+
	Переменная N (информация об управляемой переменной). Отображается, если для конфигурации приложения была задана управляемая переменная				
	Переменная в конфигурации	Название переменной в конфигурации	+	+	+
	Переменная к подстановке	Управляемая переменная из Аврора Центр для подстановки при применении конфигурации	+	+	+
	Версия переменной к подстановке	Версия подставляемой управляемой переменной	+	+	+
	Выгружена на устройство	Статус получения устройством нужной версии управляемой переменной. Возможные значения: – «Да»; – «Нет»; – «Не задано»	+	+	+
	Значение переменной	Значение управляемой переменной. **ПРИМЕЧАНИЕ.** Для защищенной переменной вместо значения отображается *****	+	+	+

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
	Блокировка переменной	Действует ли блокировка для управляемой переменной	+	+	+
Управление доверенными источниками					
	Разрешить установку без доверенных источников	Определяет, разрешена ли на устройстве установка приложений без доверенных источников	+	+	+
	Доверенные источники	Доверенные источники, перечисленных через запятую	+	+	+
Управление контентом					
	Файлы (сгруппированы по названиям файлов)				
	Версия	Номер версии файла	+	+	+
	Директория	Директория на устройстве, в которую должен быть помещен файл	+	+	+
	Размер	Размер файла	+	+	+
	Комментарий	Комментарий к файлу	+	+	+
	Хэш файла (SHA-256)	Хэш содержимого файла	+	+	+
	Режим доставки	Режим доставки файла на устройство. Возможные значения: – «Моментально»; – «По расписанию»	+	+	+
	Период актуальности	Период актуальности доставки файла	+	+	+
	Интервал доставки	Время доставки файла на устройство (пример: с 14:00 до 15:00)	+	+	+
	Часовой пояс	Часовой пояс, по времени которого будет выполнена доставка файла	+	+	+
	Папки (сгруппированы по названиям папок)				
	Версия	Номер версии папки	-	+	+
	Директория	Директория на устройстве, в которую должна быть помещена папка	-	+	+
	Комментарий	Комментарий к папке	-	+	+
	Статус	Статус доставки папки на устройство. Возможные значения: – «Не задано»; – «Доставлена»; – «Не доставлена»	-	+	+

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
	Режим доставки	Режим доставки папки на устройство. Возможные значения: – «Моментально»; – «По расписанию»	-	+	+
	Период актуальности	Период актуальности доставки папки	-	+	+
	Интервал доставки	Время доставки папки на устройство (пример: с 14:00 до 15:00)	-	+	+
	Часовой пояс	Часовой пояс, по времени которого будет выполнена доставка папки	-	+	+
Файлы с устройства					
	Загружаемые файлы с устройства (сгруппированы по пути к папке с файлами на устройстве)				
	Директория	Папка на устройстве для отправки из нее файлов на сервер	-	+	+
	Проверять	Интервал проверки содержимого папки на наличие новых файлов	-	+	+
	Удалять на устройстве после отправки	Определяет, удалять ли файлы из папки устройства после загрузки на сервер приложения. Возможные значения: – «Не задан»; – «Да»; – «Нет»	-	+	+
	Статус	Статус отправки файлов. Возможные значения: – «Загружена»; – «Выполняется»; – «Ошибка загрузки»	-	+	+
	Сообщение	Сообщение с текстом ошибки при статусе «Ошибка загрузки»	-	+	+
	Дата последней проверки файлов	Дата и время последней проверки файлов в папке	-	+	+
Управление скриптами					
	Скрипты (сгруппированы по пути к файлам со скриптами)				
	Таймаут	Таймаут выполнения скрипта. Формат: [мм:сс]	+	+	+
	Частота запуска	Периодичность выполнения скрипта на устройстве	+	+	+
	Процент успешных выполнений	Процент успешных выполнений скрипта на устройстве	+	+	+
	Время выполнения	Время выполнения скрипта на устройстве после доставки. Отображается либо значение «Моментально», либо интервал выполнения. Пример: с 14:00 до 15:00	+	+	+
	Часовой пояс	Часовой пояс, по времени которого будет выполнен скрипт	+	+	+

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
	Количество успешных выполнений	Количество успешных выполнений скрипта на устройстве. Параметр отображается, если было хотя бы одно успешное выполнение	-	+	+
	Последнее успешное выполнение - информация о последнем успешном выполнении скрипта на устройстве.Параметр отображается, если было хотя бы одно успешное выполнение				
	Статус	Статус выполнения скрипта. Возможные значения: – «Успешно выполнено»; – «Не выполнен по заданному таймауту»; – «Не выполнен»; – «Не запущен»; – «Файл поврежден»; – «Не выполнен есть заблокированные переменные»; – «Выполнен: код <код из ответа>». Возможные значения кода из ответа: • 0 - при успешном выполнении; • 1 - скрипт выполнился, но в ходе выполнения произошла ошибка	-	+	+
	Результат выполнения скрипта	Результат выполнения скрипта. Передается, если в файл скрипта была добавлена переменная OMP_SCRIPT_RESULT_FILE. Подробнее в приложении (Приложение 3)	-	+	+
	Время	Дата и время последнего успешного выполнения скрипта. Формат: [дд].[мм].[гг] [чч]:[мм]	-	+	+
	Количество неуспешных выполнений	Количество неуспешных выполнений скрипта на устройстве. Параметр отображается, если было хотя бы одно неуспешное выполнение	-	+	+
	Последнее неуспешное выполнение - информация о последнем неуспешном выполнении скрипта на устройстве. Параметр отображается, если было хотя бы одно неуспешное выполнение				
	Статус	Статус выполнения скрипта. Возможные значения: – «Успешно выполнено»; – «Не выполнен по заданному таймауту»; – «Не выполнен»; – «Не запущен»; – «Файл поврежден»; – «Не выполнен есть заблокированные переменные»; – «Выполнен: код <код из ответа>». Возможные значения кода из ответа: • 0 - при успешном выполнении; • 1 - скрипт выполнился, но в ходе выполнения произошла ошибка	-	+	+

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
	Результат выполнения скрипта	Результат выполнения скрипта. Передается, если в файл скрипта была добавлена переменная OMP_SCRIPT_RESULT_FILE. Подробнее в приложении (Приложение 3)	-	+	+
	Время	Дата и время последнего неуспешного выполнения скрипта. Формат: [дд].[мм].[гг] [чч]:[мм]	-	+	+
	Переменная N - информация об управляемой переменной. Отображается, если для выполнения скрипта была задана управляемая переменная				
	Переменная в скрипте	Название переменной в скрипте	+	+	+
	Переменная к подстановке	Управляемая переменная из Аврора Центр для подстановки при выполнении скрипта	+	+	+
	Версия переменной к подстановке	Версия подставляемой управляемой переменной	+	+	+
	Выгружена на устройство	Статус получения устройством нужной версии управляемой переменной. Возможные значения: – «Да»; – «Нет»; – «Не задано»	+	+	+
	Значение переменной	Значение управляемой переменной. Для защищенной переменной вместо значения отображается *****	+	+	+
	Блокировка переменной	Действует ли блокировка для управляемой переменной	+	+	+
Дистрибутив ОС					
ОС		Название ОС	+	+	+
Версия ОС		Номер версии ОС	+	+	+
Вариант ОС		Название варианта ОС	+	+	+
К установке		Количество пакетов, которые будут установлены при обновлении ОС	+	+	+
К обновлению		Количество пакетов, которые будут обновлены при обновлении ОС	+	+	+
К удалению		Количество пакетов, которые будут удалены при обновлении ОС	+	+	+
Версия ядра доступная для обновления		Имя нового ядра, до которого можно обновиться	+	+	+
Интервал проверки обновлений		Частота проверки наличия обновлений в часах	+	+	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Дата обнаружения обновлений ОС	Дата и время, когда было обнаружено, что согласно политике обновления ОС устройство имеет возможность выполнить обновления (либо обновление пакетов, либо обновление ядра, либо двух – как задано в политике)	+	+	+
Планируемая дата обновления ОС	Дата и время планового обновления, которые были рассчитаны на устройстве в момент обнаружения возможных обновлений	+	+	+
Часовой пояс	Часовой пояс, по времени которого будет выполнено обновление ОС	+	+	+
Правило обновления	Временной период установки обновлений ОС. В скобках указана версия ОС	+	+	+
Пользователь может перенести обновление	Перенос обновления ОС пользователем (через уведомление на ЭВМ). Возможные значения: – «Нет»; – «Да, макс. N ч»; – «Не задано»	+	+	+
Дата установки	Дата установки дистрибутива ОС	+	+	+
Статус обновления	Статус установки обновлений ОС. Возможные значения: – «Нет данных»; – «Выполнено»; – «Не выполнено»; – «Запланировано»; – «Перенесено пользователем»; – «Ошибка»; – «Прервано»	+	+	+
Подготовка к обновлению				
Обновить пакеты	Определяет, требуется ли обновить пакеты ОС	+	+	+
Обновить ядро	Определяет, требуется ли обновить ядро ОС (и его модули)	+	+	+
Остановить обновления ядра, если хотя бы 1 модуль удаляется	Определяет, требуется ли остановить обновления ядра, если хотя бы 1 его модуль будет удален в процессе обновления	+	+	+
Предварительное скачивание обновлений	Определяет, включено ли предварительное скачивание обновлений (до начала запланированного периода обновлений). Возможные значения: – «Да»; – «Нет»	+	+	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Удалять дубликаты при предварительном скачивании	Определяет, включено ли удаление дубликатов пакетов при предварительном скачивании. Возможные значения: – «Да»; – «Не»	+	+	+
Выполнить скрипт до обновления	Путь к скрипту на устройстве, который необходимо выполнить до начала обновления	+	+	+
Выполнить указанный скрипт перед проверкой обновлений	Определяет, выполнять ли скрипт выше перед предварительным скачиванием пакетов для обновления ОС. Возможные значения: – «Да»; – «Нет»	+	+	+
Условия для обновления				
Минимальное свободное место на диске после обновления	Минимальное свободное место на диске после обновления в МиБ	+	+	+
Минимальная свободная оперативная память	Минимальная свободная оперативная память в МиБ	+	+	+
Максимальная загруженность процессора	Максимальная загруженность процессора в процентах	+	+	+
Обслуживание ОС перед выполнением обновления				
Удаление дубликатов до обновления ОС	Определяет, требуется ли удалить дубликаты пакетов до обновления ОС	+	+	+
Обслуживание ОС после выполнения обновления			+	+
Выполнить скрипт после обновления	Путь к скрипту на устройстве, который необходимо выполнить после успешного обновления ОС	+	+	+
Удаление ранее скачанных пакетов	Определяет, требуется ли удалить ранее скачанные пакеты после успешного обновления ОС	+	+	+
Удаление неиспользуемых пакетов	Определяет, требуется ли удалить неиспользуемые пакеты после успешного обновления ОС	+	+	+
Удаление старых ядер	Определяет, требуется ли удалить старые ядра после успешного обновления ОС	+	+	+
Перезагрузка ОС	Определяет, требуется ли выполнить перезагрузку ОС после успешного обновления	+	+	+
Пользователь может перенести перезагрузку	Перенос перезагрузки ОС пользователем (через уведомление на ЭВМ). Возможные значения: – «Нет»; – «Да, макс. N ч»; – «Не задано»	+	+	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Управление питанием				
Время перезагрузки	Дата и время начала последней перезагрузки устройства, выполненной с помощью команды оперативного управления	+	+	+
Расписание перезагрузки	Параметры перезагрузки устройство с помощью политики: – «Режим выполнения» - режим выполнения перезагрузки на устройстве («Однократно», «Многократно»); – «Дни недели» - дни недели, в которые будет выполняться перезагрузка; – «Интервал» - временной интервал, в который будет выполняться перезагрузка; – «Последняя перезагрузка» - дата и время начала последней перезагрузки устройства с помощью ППО	+	+	+
Управление принтерами (данные сгруппированы по названиям принтера)				
Имя принтера	Название принтера	+	-	-
Адрес подключения	Адрес подключения принтера	+	-	-
Принтер по умолчанию	Признак принтера для печати по умолчанию. Определяет, будет ли указанный принтер использоваться на устройстве по умолчанию	+	-	-
Последняя попытка обновления				
Дата обновления	Дата и время последней попытки обновления ОС	-	-	+
Результат обновления	Результат последней попытки обновления. Возможные значения: – «Успешно»; – «Неуспешно»; – «Перенесено пользователем»; – «Прервано»	-	-	+
Установлено	Количество установленных пакетов	-	-	+
Обновлено	Количество обновленных пакетов	-	-	+
Удалено	Количество удаленных пакетов	-	-	+
Этапы обновления	Отчет об обновлении ОС в виде списка этапов (`packageUpdate, kernelUpdate` ит.п.). Для каждой детали (этапа) отображается: – «Сообщение» - тело сообщения (произвольный текст); – «Тип сообщения» - важность сообщения. Возможные значения: • «Информационное»; • «Ошибка»; • «Предупреждение»	-	-	+

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Пользователь				
Управление сбросом пароля	Статус возможности сброса пароля на устройстве с помощью ПУ. Возможные значения: – «Активировано»; – «В ожидании подтверждения пароля»; – «В ожидании сброса устройства»; – «Не поддерживается»; – «Ошибка активации»; – «Неизвестно»	+	+	+
Требования к паролю	Отображается информация, используется ли пароль на устройстве. Если используется, то дополнительно отображается информация о требованиях к следующим параметрам пароля: – сложность пароля; – длина пароля; – срок истечения пароля. Возможные значения: – обычный: сложность – обычная (цифры), длина – от 7 до 10 символов; – сложный: сложность – высокая (цифры, буквы, символы, знаки пунктуации), длина – от 8 до 12 символов; – срок истечения пароля: 30, 60, 90, 120, 150, 180 дней (не зависит от сложности пароля)	+	+	+
Создание пользователя	Требование создания пользователя на устройствах. Возможные значения: – «Создание» – определяет, требуется ли создавать пользователя на устройстве; – «Сброс пароля Администратора» – определяет, требуется ли сбросить пароль Администратора на устройстве с ОС Аврора; – «Время сброса» – временной интервал, в течение которого нужно сбросить пароль Администратора и перезагрузить устройство	+	-	+
Пользовательские сессии				
Сессии пользовательских входов на устройстве	В текущем состоянии выводится ТОП-3 по наибольшему времени сессии пользователей, авторизованных на устройстве. Отображается логин и время сессии в минутах. **ВНИМАНИЕ!** ТОП-1 пользователь будет автоматически привязываться к устройству. Это означает, что если на группу, в которую входит ТОП-1 пользователь, назначена политика, то она начнет действовать на устройстве. Если пользователь был импортирован из LDAP-сервера, то будет отображаться его «UserPrincipalName». При определении суммарного времени пользовательских сессий и статуса активности учетных записей учитываются подключения по XRDP. **ПРИМЕЧАНИЯ:** ✓ Учитываются периоды неактивности сессий;	-	-	+

Название группы политик/состояний		Описание	Версии ОС		
			ОС Аврора	ОС Android	ОС семейства Linux
		✓ Если сессия была открыта, но не закрыта и при этом не является текущей активной сессией, то такая сессия не учитывается при подсчетах; ✓ Сессии пользователя, которые были завершены аварийно (например, вследствие разрядки аккумулятора или отключения питания устройства), не будут учитываться при составлении списка сессий; ✓ При первичном запуске приложения единоразово будет выполнен экспорт предыдущих XRDP сессий из файла `/var/lib/xrdp.log`			
	Сертификаты пользователей				
	Сертификат (информация о сертификатах пользователя, которые были выпущены и доставлены на устройства)				
	Категория	Название категории, в рамках которой был выпущен пользовательский сертификат	+	+	-
	Шаблон	Название шаблона для выпуска пользовательских сертификатов	+	+	-
	Фингерпринт	Цифровой отпечаток (Fingerprint) сертификата	+	+	-
	Хэш-алгоритм запроса	Алгоритм хэширования	+	+	-
	Тип шифрования и длина ключа	Алгоритм шифрования приватного ключа	+	+	-
	Subject	Список субъектов для сертификата. Каждый субъект состоит из набора параметров – название параметра (`key`) и его значения (`value`)	+	+	-
	Расширение	Дополнительные имена субъекта для сертификата. Отображается, если параметр «Subject Alt Name» указан в категории пользовательских сертификатов	+	+	-
Режим киоска					
Платформа		Платформы, для которой применяется режим киоска	+	+	-
Включен		Определяет, включен ли режим киоска	+	+	-
Тип		Тип режима киоска: – «Веб-ресурс»; – «Рабочий стол»; – «Приложение»	-	+	-
Отключение панели уведомлений		Настройка доступности панели уведомлений (верхнее меню) в режиме киоска	-	+	-
Код выхода из режима киоска		Код для выхода из режима киоска	-	+	-
Цвет шрифта		Настройка цвета шрифта в режиме «Рабочий стол». Возможные значения: – «По умолчанию»; – заданный цвет и HEX-код цвета в формате "#ffffff"	-	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Фон	Настройка цвета фона в режиме «Рабочий стол». Возможные значения: – «Системное изображение»; – заданный цвет и HEX-код в формате "#ffffff"	-	+	-
Приложения (список разрешенных приложений для режима киоска с типом «Рабочий стол»)				
Код приложения [№]	Названия пакетов приложений, которые будут доступны пользователю в режиме киоска	+	+	-
Ярлыки веб-страниц (для режима киоска с типом «Рабочий стол»)				
Название ярлыка	Название ярлыка веб-страницы	-	+	-
URL	Электронный адрес сайта/веб-страницы в формате URL	-	+	-
Путь к файлу иконки	Абсолютный путь к файлу иконки на устройстве	-	+	-
Панель навигации	Отображение кнопок «Назад»/«Вперед»/«Обновить» в режиме «Веб-ресурс»	-	+	-
Стартовая страница	URL-адрес ресурса, который должен открываться во весь экран в режиме «Веб-ресурс»	-	+	-
Запрещенные сайты	Электронные адреса запрещенных сайтов. Если отображается значение в виде звездочки (*), то запрещены все сайты, кроме указанных в исключениях	-	+	-
Исключения из запрещенных сайтов	Электронные адреса сайтов, которые исключены из запрещенных	-	+	-
Скрытые приложения	Список приложений, которые не отображаются пользователю, но разрешены для использования в режиме киоска (для типа «Приложение»)			
Приложение N	Название пакета скрытого приложения	-	+	-
Сервисы для автозапуска (список сервисов для автозапуска). Для каждого сервиса отображается:				
Имя пакета	Название пакета	-	+	-
Имя сервиса	Имя сервиса для автозапуска	-	+	-
Статус	Статус автозапуска сервиса. Возможные значения: – «Сервис запущен» - сервис успешно работает; – «Сервис недоступен» - в указанном пакете отсутствует сервис с заданным именем или сервис недоступен; – «Сервис не запущен» - сервис найден, но не работает; – «Пакет не найден» - приложение с указанным именем пакета отсутствует на устройстве; – «Не удалось определить состояние сервиса» - при проверке произошла неопределенная ошибка	-	+	-
Внешний вид				
Фон рабочего стола (информация об установленном фоне на рабочий стол устройства)				
Путь к файлу	Абсолютный путь к файлу изображения на устройстве	-	+	-

Название группы политик/состояний	Описание	Версии ОС		
		ОС Аврора	ОС Android	ОС семейства Linux
Отображение идентификаторов в клиенте Аврора Центр	Отображаются идентификаторы устройства в порядке, заданном в политике	+	+	+
Яркость	Информация о яркости на устройстве: – «Режим яркости» - информация о режиме яркости; – «Уровень яркости» - информация об уровне яркости; – «Управление яркостью» - запрет или разрешение управления яркостью на устройстве	-	+	-
Ориентация экрана	Информация об применяемой ориентации экрана на устройстве. Возможные значения: – «Автоматическая» - ориентация экрана изменяется автоматически в зависимости от положения устройства; – «Портретная» - ориентация экрана устройства фиксируется в вертикальном положении; – «Ландшафтная» - ориентация экрана устройства фиксируется в горизонтальном положении; – «Обратная портретная» - ориентация экрана фиксируется вверхом вниз в вертикальном положении; – «Обратная ландшафтная» - ориентация экрана фиксируется справа-налево в горизонтальном положении	-	+	-

2.1.1.2. Вкладка «Управление»

Во вкладке «Управление» отображается:

– перечень правил политик, офлайн-сценариев и оперативных команд, назначенных на устройство (доступные значения необходимо выбрать из раскрывающегося списка (Рисунок 11 [1]);

– информация о соответствии назначенных правил (в случае конфликта отображается действующее правило (Рисунок 11 [2]).

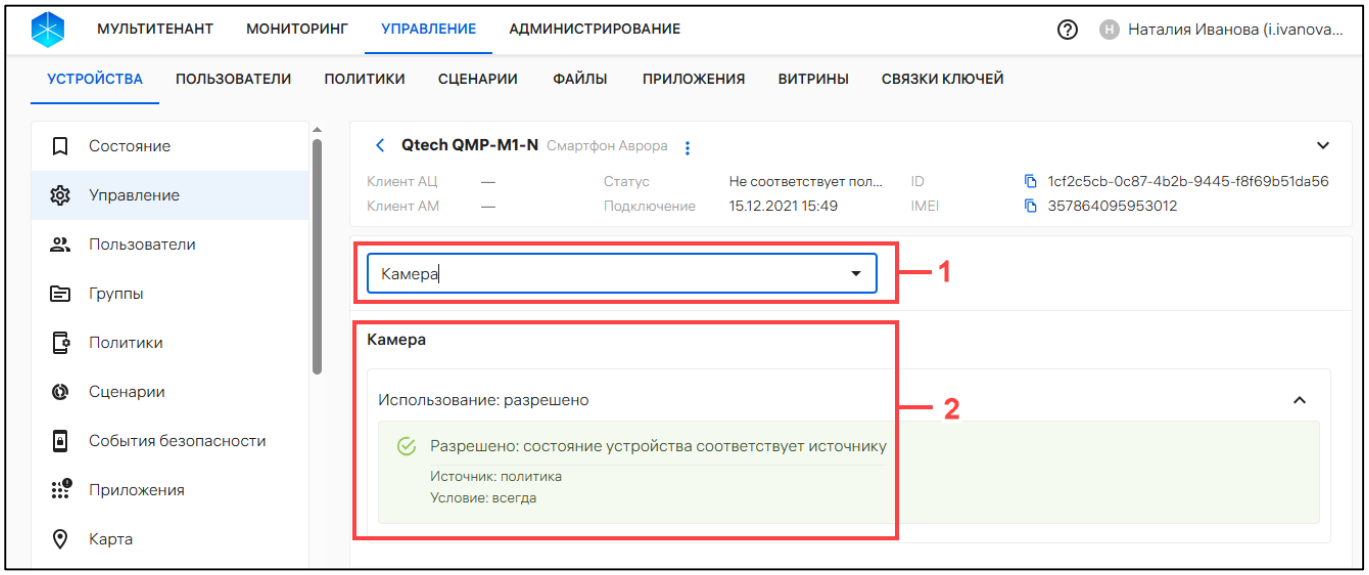


Рисунок 11

ПРИМЕЧАНИЕ. Одновременно назначенные на устройство правила имеют следующий приоритет:

1) Оперативная команда;
2) Офлайн-сценарий;
3) Политика.

2.1.1.3. Вкладка «Пользователи»

Во вкладке «Пользователи» отображается список привязанных к устройству пользователей, а при его отсутствии отображается сообщение «Устройство не привязано ни к одному пользователю».

Устройство можно привязать к пользователю из карточки с помощью кнопки «Привязать пользователей», выполнив действия, приведенные в пп. 2.2.8.2.

Список пользователей сортируется по дате обновления информации о пользователях устройства.

Информация о пользователях отображается в столбцах, приведенных в таблице (Таблица 5).

Таблица 5

Параметр	Описание
Имя	Фамилия, имя и отчество пользователя (представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке пользователя (п. 2.1.3)
Email	Рабочая почта пользователя
Телефон	Номер телефона пользователя
Должность	Должность занимаемая пользователем
Назначено	Дата и время привязки устройства к пользователю

2.1.1.4. Вкладка «Группы»

Во вкладке «Группы» отображается список привязанных к устройству групп устройств.

Устройства можно привязать к группе устройств с помощью кнопки «Добавить в группы», выполнив действия, приведенные в пп. 2.2.9.2.

Информация о группах устройств отображается в столбцах, приведенных в таблице (Таблица 6).

Таблица 6

Параметр	Описание
Тип	Тип группы устройств (Приложение 1)
Группа устройств	– название группы устройств (представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке группы устройств; – комментарий – дополнительная информация (заполняется при необходимости)
Устройств	Количество устройств в данной группе устройств
Назначено	Дата и время добавления устройств в группу устройств

2.1.1.5. Вкладка «Политики»

Во вкладке «Политики» отображается список назначенных на устройство политик и их правил (Рисунок 12), а при отсутствии списка отображается сообщение «На устройство не назначено ни одной политики».

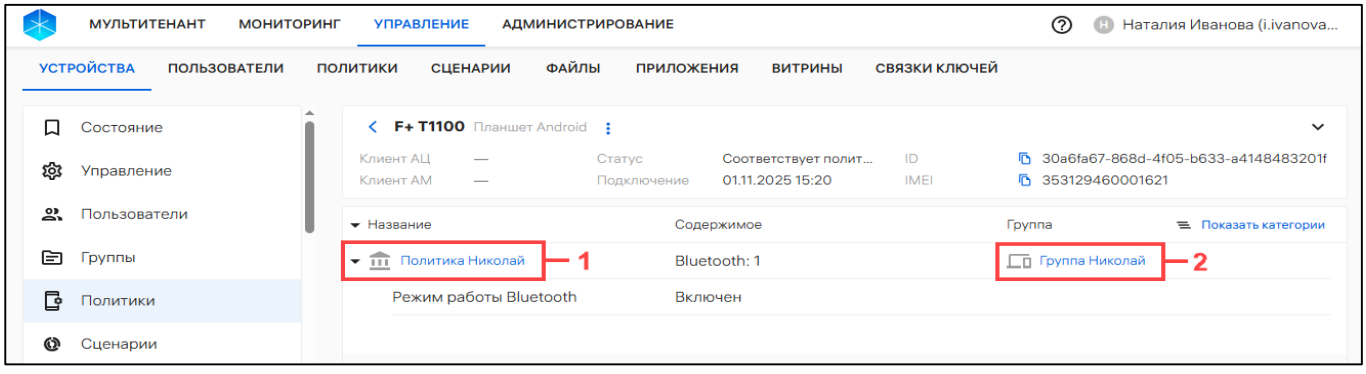


Рисунок 12

В случае пересечения с другими политиками отобразится полный список названий всех политик на группах устройств или группах пользователей.

Информация во вкладке «Политики» отображается в следующих столбцах, приведенных в таблице (Таблица 7).

Таблица 7

Параметр	Описание
Название	Название политики, назначенной на группу устройств/пользователей, в которую входит текущее устройство. Название политики выделено цветом и представляет собой активную ссылку (Рисунок 12 [1]), при нажатии на которую осуществляется переход к карточке политики
Содержимое	Краткая информация о правилах, добавленных в политику
Группа	наименование группы, на которую назначена политика. Название группы представляет собой активную ссылку (Рисунок 12 [2]), при нажатии на которую осуществляется переход к карточке группы

При отсутствии политик, назначенных на группу устройств/пользователей, в которую входит данное устройство, необходимо выполнить действия, приведенные в п. 2.4.4.

2.1.1.6. Вкладка «Сценарии»

Во вкладке «Сценарии» отображается следующий список:

– офлайн-сценарии, назначенные на устройство;
– бизнес-сценарии, выполняющиеся на устройстве.

В ППО доступен бизнес-сценарий по экстренному выводу устройства из эксплуатации (например, при утере или краже), при применении которого, устройство блокируется, затем очищается вместе со всеми данными (сбрасывается до заводских настроек (п. 2.2.17) и архивируется.

При отсутствии офлайн-сценариев, назначенных на группу устройств/пользователей, в которую входит данное устройство, отображается сообщение «На устройство не назначен ни один офлайн-сценарий». Подробное описание назначения офлайн-сценариев приведено в п. 2.5.2.

Информация об офлайн-сценариях и о бизнес-сценариях отображается в столбцах, приведенных в таблице (Таблица 8).

Таблица 8

Параметр	Описание
Офлайн-сценарии	
Название	Название офлайн-сценария, назначенного на группу устройств/пользователей, в которую входит текущее устройство. Название офлайн-сценария представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке офлайн-сценария

Параметр	Описание
Событие	Событие, по которому офлайн-сценарий должен сработать
Реакция	Реакция устройства, которая должна произойти при наступлении события офлайн-сценария
Группы	Наименование группы, на которую назначен офлайн-сценарий. Название группы представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке группы
Бизнес-сценарии, назначенные на устройства	
Название	Название бизнес-сценария, выполняющегося на устройстве
Статус	Статус выполнения бизнес-сценария
Назначено	Дата и время назначения бизнес-сценария на устройства

2.1.1.7. Вкладка «Удаленный доступ»

Во вкладке «Удаленный доступ» отображаются настройки RustDesk для удаленного подключения.

ПРИМЕЧАНИЕ. Для успешной работы удаленного доступа через ППО необходимо:

– чтобы был установлен сервер RustDesk и его настройки (адрес и ключ) заданы в конфигурационном файле ППО;

– ЭВМ администратора с:

- ОС Windows версии 11;
- ОС Ubuntu версии 22.04.

ПРИМЕЧАНИЕ. Удаленный доступ к устройству через ППО был протестирован только для перечисленных выше ОС. При необходимости возможно использовать другие ОС и приложения RustDesk (с официального сайта https://github.com/rustdesk/rustdesk/releases/tag/1.4.5), но следует учитывать, что корректная работа таких приложений не гарантируется. При взаимодействии с такими приложениями возможно возникновение обратного подключения к устройству пользователя;

– на ЭВМ администратора должен быть установлен и настроен desktop-клиент RustDesk (подробная информация приведена ниже).

– устройство пользователя с:

- ОС Android версии 7 и выше;
- ОС Astra Linux. Рабочая станция 10К и 11К;
- ОС Astra Linux 1.7SE и 1.8SE.

ПРИМЕЧАНИЕ. Удаленный доступ к устройству через ППО был протестирован только для перечисленных выше ОС. При необходимости возможно использовать другие ОС и приложения RustDesk (с официального сайта https://github.com/rustdesk/rustdesk/releases/tag/1.4.5), но следует учитывать, что корректная работа таких приложений не гарантируется;

– на устройстве пользователя должено быть установлено и настроено приложение RustDesk (подробная информация приведена ниже);

– на устройстве пользователя не была назначена и не действует политика с запрещающим правилом «Ограничение доступа/Снимки экрана».

Для удаленного подключения к рабочему столу активированного устройства, а также для обмена файлами с помощью ПУ, необходимо выполнить следующие действия:

1) Установить сервер RustDesk и зафиксировать его настройки в конфигурационном файле ПУ (подробнее в документе «Руководство администратора»);

2) Установить desktop-клиент RustDesk на ЭВМ.

ПРИМЕЧАНИЕ. В зависимости от версии ОС дистрибутив desktop-клиента расположен в следующей папке распакованного архива с дистрибутивом ППО:

– ОС Windows версии 11: /client-apps-android/thirdparty/rustdesk-fa/windows/;

– ОС Ubuntu 22.04: /client-apps-android/thirdparty/rustdesk-fa/ubuntu-22.04/.

ВНИМАНИЕ! Корректная работа desktop-клиента RustDesk на других версиях ОС не гарантируется;

3) Открыть настройки desktop-клиента RustDesk. Для этого необходимо открыть настройки desktop-клиента RustDesk (Рисунок 13), перейти в раздел «Сеть» и указать адрес и ключ сервера RustDesk, которые были получены на шаге 1.

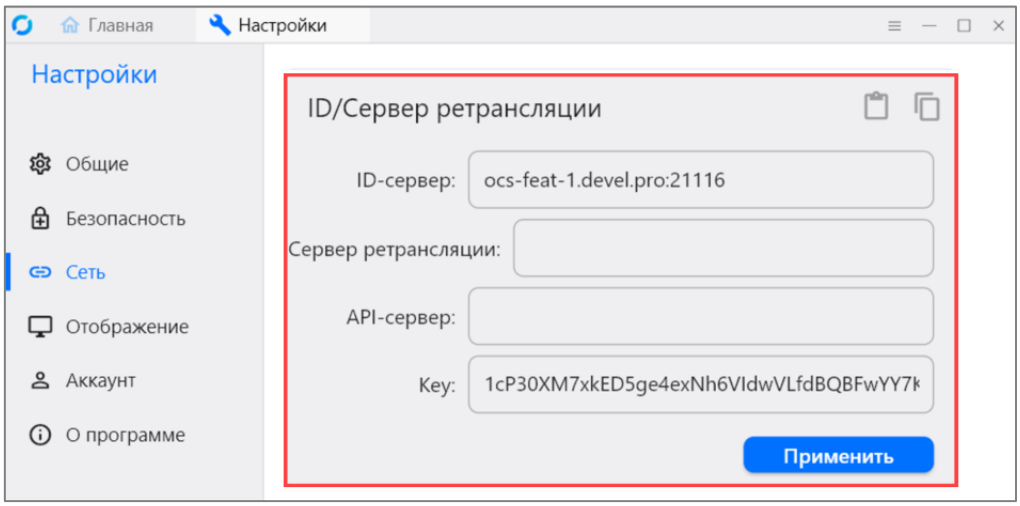


Рисунок 13

ПРИМЕЧАНИЕ. Для desktop-клиента RustDesk для ОС Windows необходимо также нажать кнопку «Установить» (Рисунок 14) на главной странице и следовать инструкциям из Wizard для установки RustDesk в системе;

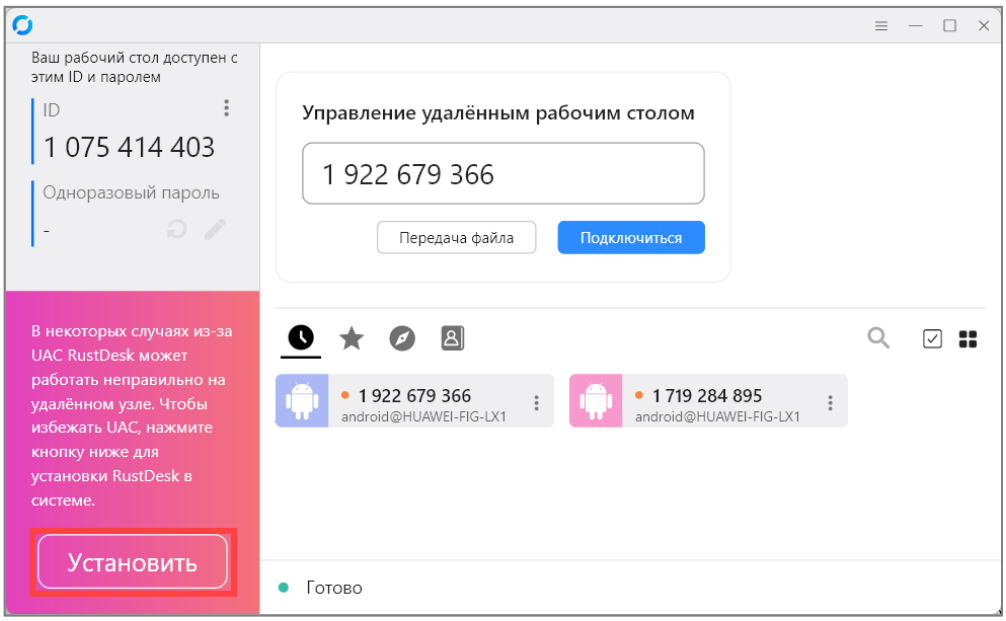


Рисунок 14

4) Установить приложение RustDesk на устройствах пользователя.

ВНИМАНИЕ! В зависимости от ОС, установленной на устройстве, дистрибутив приложения расположен в папке распакованного архива с ППО, а именно:

– **ОС Android версии 7 и выше**: `/client-apps-android/thirdparty/rustdesk/android/` (подготовка устройства к удаленному подключению приведена в приложении (Приложение 4).

Может быть доступна сборка приложения RustDesk, подписанная подписью производителя. Такая сборка позволяет осуществлять удаленное подключение к рабочему столу пользователя без запроса у пользователя отдельного разрешения (далее «бесшовное» подключение), при этом для нее характерно следующее:

– сборка располагается в архиве `client-apps-android-signed-vendor.tar.gz`, который входит в комплект поставки ППО;

– суффикс в названии APK-файла определяет производитель.

Особенности, характерные для производителя Chainway:

– приложение RustDesk располагается в папке: /client-apps-android/thirdparty/rustdesk/android/rustdesk-1.5.1+1-android.armeabi-v7a.chainway-4d.apk;

– используемые подписи зависят от модели устройства, например:

- для устройств на Qualcomm – подпись с суффиксом `4d`;
- для устройства C72 – подпись с суффиксом `cd`;

– **ОС Альт Linux версии 10К и 11К**: /client-apps-linux/thirdparty/alt-p10;

– **ОС Astra Linux версии 1.7 SE и 1.8SE**: /client-apps-linux/thirdparty/astra-se-1.7.

ВНИМАНИЕ! Рекомендуется установить приложение RustDesk, назначив политику «Приложения/Управление приложениями» (пп. 2.4.1.57).

Для установки приложения RustDesk с «бесшовным» подключением необходимо создать динамическую группу устройств по производителю (пп. 2.2.2.2) и затем назначить политику с правилом «Приложения/Управление приложениями», которая установит необходимое приложение в зависимости от производителя.

ПРИМЕЧАНИЕ. Если приложение RustDesk (из состава ППО релиз 5.0.0) версии 5.0.0.1+1 загружен в ПМ, то подгрузить к нему для обновления версию 1.5.1+1 и выше (ППО релиз 5.2.0) невозможно.

В этом случае необходимо создать новое приложение RustDesk под релиз 5.2.0 и затем переназначить его установку на устройства с использованием соответсвующей политики.

Прилжение RustDesk версии 1.10.0 для ОС Android из поставки ППО релиза 5.6.0 несовместим с более ранними версиями приложения «Аврора Центр»;

5) Если у пользователя устройство с ОС Android, необходимо подготовить устройство к удаленному подключению. Подробнее в приложении (Приложение 4);

6) Передать настройки на устройство и выполнить удаленное подключение через ПУ. Для этого в Консоли администратора ПУ в карточке устройства во вкладке «Удаленный доступ» нажать на кнопку «Конфигурировать сеанс», предварительно убедившись, что настройки сервера RustDesk заданы в настройках сети desktop-клиента RustDesk (см. Рисунок 13).

В результате настройки удаленного подключения будут переданы и применены на устройстве (это может занять некоторое время).

ПРИМЕЧАНИЯ:

✓ Поставляемое в дистрибутиве ППО приложение RustDesk для администратора в целях безопасности не поддерживает подключение к нему и может быть использовано только для подключения к управляемым устройствам;

✓ Если требуется удаленно подключаться к рабочему столу устройства в режиме киоска, то приложение RustDesk не нужно включать в список разрешенных приложений. В режиме киоска оно будет по умолчанию скрыто на экране устройства, при этом будет возможность удаленно подключиться к рабочему столу, выполнив шаги, приведенные выше.

Далее отобразится «Тип управления», в котором будут отображены (Рисунок 15 [1]):

– «ID клиента» – идентификатор клиента RustDesk на устройстве пользователя;
– «Пароль» – пароль для удаленного подключения.

ПРИМЕЧАНИЕ. Для устройств, функционирующих на ОС Android, перед выполнением удаленного подключения необходимо на устройствах вручную запустить службу RustDesk и выдать требуемые разрешения (Приложение 4).

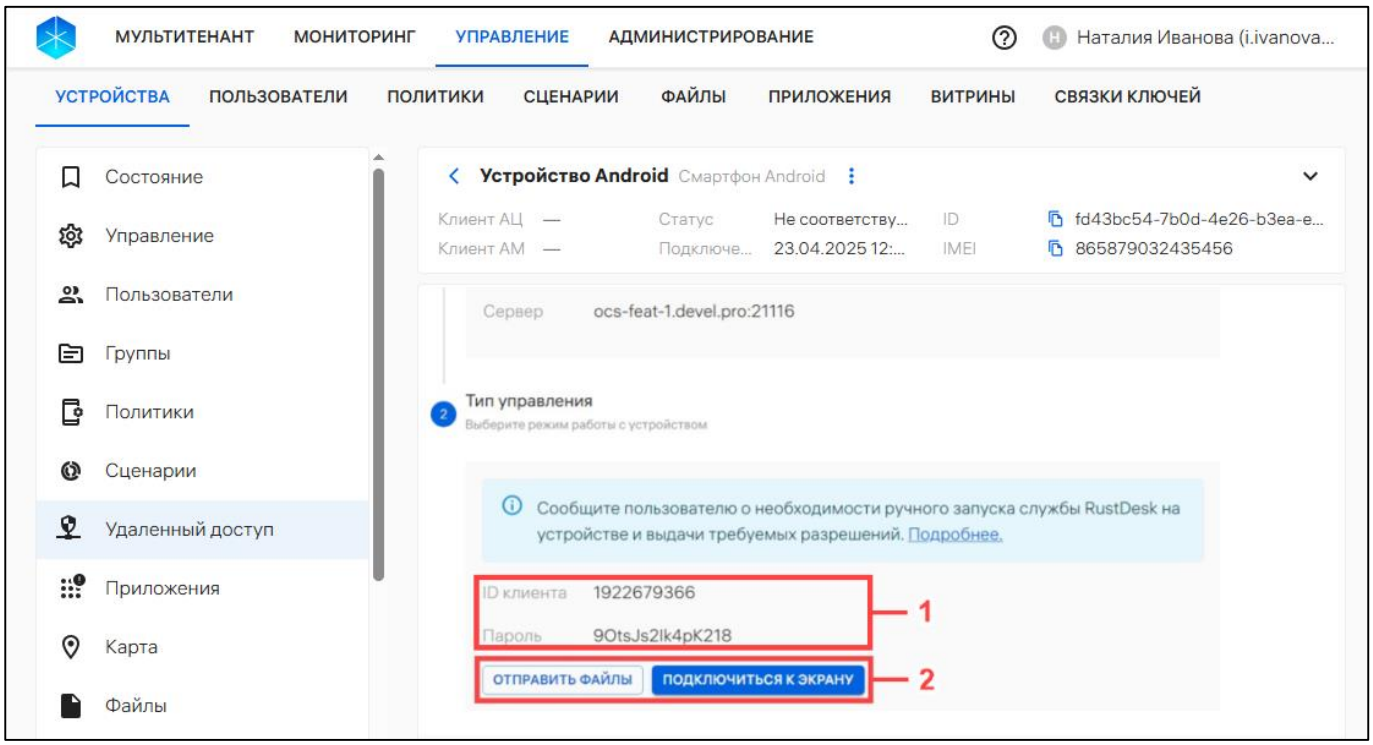


Рисунок 15

Если необходимо:

– подключиться к рабочему столу пользователя устройства, необходимо нажать кнопку «Подключиться к экрану» (см. Рисунок 15 [2]) и подтвердить подключение. Откроется окно desktop-клиента RustDesk с удаленным рабочим столом пользователя;

– передать на устройство или, наоборот, скопировать файлы с устройства, нажать «Отправить файлы» (см. Рисунок 15 [2]) и подтвердить подключение. Откроется окно desktop-клиента RustDesk для обмена файлами между ЭВМ и устройством пользователя.

В результате удаленное подключение к устройству пользователя будет настроено и выполнено.

2.1.1.8. Вкладка «События безопасности»

ПРИМЕЧАНИЕ. Оперативная команда «Расписание отправки событий безопасности» доступна только для устройств, функционирующих под управлением ОС Аврора.

Во вкладке «События безопасности» отображается список произошедших на устройстве событий безопасности, который при разборе инцидентов позволяет определить, что происходило на устройстве, а при отсутствии событий на устройстве отображается сообщение «Нет данных».

Для получения события безопасности необходимо воспользоваться оперативной командой «Расписание отправки событий безопасности» (п. 2.2.11) или политикой с правилом «Конфигурация/Расписание отправки событий безопасности» (пп. 2.4.1.26).

Список событий сортируется по дате произошедшего события, также возможно фильтровать по атрибутам, приведенным в таблице (см. Таблица 2).

Информация о событиях безопасности отображается в следующих столбцах, приведенных в таблице (Таблица 9).

Таблица 9

Параметр	Описание
Принято	Дата и время поступления события на устройствах
Произошло	Дата и время выполнения события на устройствах
Тип	Тип сообщения о событии в зависимости от важности (Приложение 1)
Процесс и роль	Роль отправителя события и полный путь к исполняемому файлу процесса отправителя события
Событие и подробности	Название события и дополнительная информация о нем
Инфо	Содержание сообщения. Для просмотра необходимо нажать значок «Содержание сообщения». Для копирования текста сообщения в буфер обмена необходимо нажать кнопку «Копировать». Для закрытия сообщения нажать кнопку «Закрыть»

2.1.1.9. Вкладка «Приложения»

Во вкладке «Приложения» отображается список приложений, установленных на устройстве.

ПРИМЕЧАНИЕ. На устройствах с ОС семейства Linux поиск установленных пакетов с типом `appimage` осуществляется в папках `/home, /tmp/.private/*`.

Информация о приложениях отображается в столбцах, приведенных в таблице (Таблица 10).

Таблица 10

Параметр	Описание
Приложение	Название приложения и его версия
Автозапуск	Определяет включение автозапуска приложения. Возможные значения: – ⊘ – Выключено; – ✓ – Включено. **ВНИМАНИЕ!** Автозапуск можно установить только для приложений с ОС Аврора. **ПРИМЕЧАНИЕ.** Если информация об автозапуске не была получена (например, автозапуск приложений отсутствует на устройстве на базе ОС Android), то ячейка не заполняется

Параметр	Описание
Разрешения	Автоматическое применение разрешений. Определяет, выдано ли приложению автоматическое применение требуемых разрешений. Возможные значения: – ⊘ – Выключено; – ✓ – Включено. **ПРИМЕЧАНИЕ.** Если информация о выданных разрешениях не была получена (например, для системных приложений в ОС Android), то ячейка не заполняется
Политика	Название политики, по правилу которой было установлено приложение. Название политики выделено цветом и представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке политики (п. 2.1.5). При отсутствии политик с правилом установки приложения отображается значок «—»
Пакетный менеджер	Источник установки пакета приложения. Например: `dpkg`, `rpm`, `appimage`, `snap` и другие. Если информация об источнике не была получена, то отображается значение «n/a»
Установлено	Дата и время установки пакета на устройстве. **ПРИМЕЧАНИЕ.** Дата и время установки отображаются только для пакетов с ОС Android и ОС семейства Linux
Получено	Дата и время получения информации о пакете
Инфо	Отображение дополнительной информации о пакете приложения при нажатии значка 👁 «Дополнительная информация»: – «Пакет» – название пакета; – «Путь» – путь к пакету на устройстве (только для `appimage` и `flatpak` пакетов

2.1.1.10.Вкладка «Карта»

Во вкладке «Карта» доступен просмотр местоположения активированного устройства на карте (Рисунок 16).

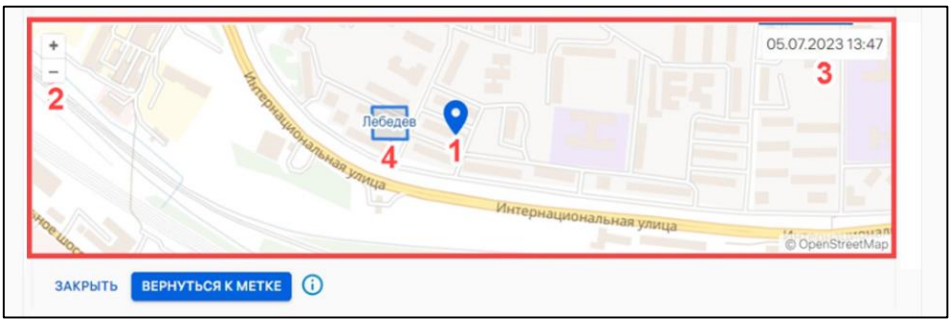


Рисунок 16

На карте отображены следующие элементы:

– метка с местоположением устройства (см. Рисунок 16 [1]);

– кнопки для увеличения или уменьшения масштаба карты (см. Рисунок 16 [2]);

– дата актуальности координат (см. Рисунок 16 [3]);

– территория (см. Рисунок 16 [4]) – если на устройство назначен офлайн-сценарий с событием «Нахождение на территориях, определяемых координатами» или «Нахождение вне территории, определяемой координатами», то на карте также отображаются территории из офлайн-сценария.

При наведении курсора на метку устройства отображается подсказка, содержащая следующую информацию (Рисунок 17 [1]):

– координаты устройства;

– дата актуальности координат;

– режим работы геопозиционирования.

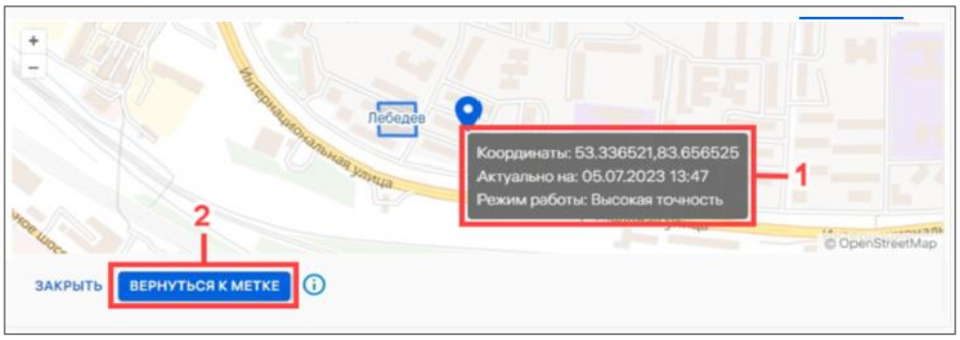


Рисунок 17

При необходимости возможно изменить масштаб и просматривать другие области карты. Чтобы вернуться к метке устройства в масштабе по умолчанию, необходимо нажать кнопку «Вернуться к метке» (см. Рисунок 17 [2]).

ПРИМЕЧАНИЯ:

✓ Координаты с устройства отправляются по расписанию отправки состояния;

✓ Актуальные координаты могут отсутствовать в состоянии, если устройство не определило их или определение отключено. Необходимо воспользоваться оперативным управлением для получения состояния устройства вне расписания;

✓ Точность определения координат устройства зависит от многих факторов, таких как: тип устройства, состояние сети, скорость, нахождение в здании или около высоких объектов, покрытие спутников, аппаратные и программные характеристики, уровень шума/помех и т.д;

✓ Местоположение устройства с ОС семейства Linux отображается, но точность может быть только на уровне города.

2.1.1.11.Вкладка «События восстановления»

Во вкладке «События восстановления» доступен просмотр списка событий восстановления ОС устройства.

ВНИМАНИЕ! Отображение событий восстановления доступно только для устройств с ОС семейства Linux.

ПРИМЕЧАНИЕ. Восстановление системы может быть выполнено:

– вручную с помощью команды оперативного управления «Откат на точку восстановления»;

– автоматически с помощью правила политики «Конфигурация/Создание точек восстановления».

Информация о событиях восстановления отображается в столбцах, приведенных в таблице (Таблица 11).

Таблица 11

Параметр	Описание
Дата восстановления	Дата и время, когда произошло восстановление ОС
Точка восстановления (локальное время устройства)	Имя точки восстановления (фактически локальные дата и время устройства). **ПРИМЕЧАНИЕ.** Если у устройства нет точек восстановления, созданных через ППО, отображается знак «—»
Режим	Режим восстановления. Возможные значения: – «Ручной»; – «Автоматический»
Статус	Статус восстановления. Возможные значения: – «Восстановлено»; – «Не восстановлено»
Сообщение	Сообщение от утилиты `timeShift`. Возможные значения: – «success» - если восстановление прошло успешно; – «[текст ошибки]» - если при восстановлении произошла ошибка. Текст ошибки отображается в том виде, в котором ее выдает `timeShift`. **ПРИМЕЧАНИЕ.** Перед сообщением доступна кнопка «Копировать», при нажатии на которую отобразится окно с возможностью копирования текста сообщения
Комментарий	Комментарий. **ПРИМЕЧАНИЕ.** Если был задан ручной режим восстановления, то отображается комментарий пользователя с причиной восстановления

2.1.1.12.Вкладка «Файлы»

Во вкладке «Файлы» возможно просмотреть список и скачать файлы, которые были загружены с устройства в ППО:

– с помощью правила политики «Файлы с устройства/Загрузка файлов с устройств» (пп. 2.4.1.47);

– с помощью команды оперативного управления «Диагностика» (п. 2.2.11).

Информация о файлах отображается в столбцах, приведенных в таблице (Таблица 12).

Таблица 12

Параметр	Описание
Название	Имя файла
Дата загрузки	Дата и время загрузки файла на сервер ППО. **ПРИМЕЧАНИЕ.** Доступна сортировка списка файлов по столбцу «Дата загрузки»
Тэг файла	Метка, определяющая назначение файла. При необходимости возможно отобразить в списке только диагностические отчеты, применив фильтр (подраздел 1.4). **ПРИМЕЧАНИЕ.** Доступна только метка «Диагностический отчет», которая присваивается файлам (отчетам) с логами устройства
Размер	Размер файла
Действия	Доступна кнопка «Скачать» для загрузки файла на локальный компьютер

2.1.1.13.Вкладка «Журнал»

Во вкладке «Журнал» отображается список событий журнала приложения «Аврора Центр».

Устройство отправит в ПУ записи:

– после успешной активации (п. 2.2.10);

– по расписанию раз в час (если устройство было активировано);

– при запросе состояния устройства (если устройство было активировано).

ПРИМЕЧАНИЯ:

✓ При каждой отправке высылается 150 последних событий. Если было больше событий, то они не отправятся. В этом случае необходимо запросить отчет с помощью оперативной команды «Диагностика» (п. 2.2.11), в который закладывается база данных приложения «Аврора Центр»;

✓ Данные о времени, когда произошло событие, хранятся в базе данных приложения «Аврора Центр» без информации о часовом поясе. Часовой пояс подставляется в момент забора информации из базы данных (например, для отображения в журнале приложения или отправки данных на сервер);

✓ Приложение «Аврора Центр» хранит записи за последние три месяца. Соответственно, в карточке устройства будут отображены события, которые не превышают этот срок.

Информация списка событий журнала приложения «Аврора Центр» отображается в столбцах, приведенных в таблице (Таблица 13).

Таблица 13

Параметр	Описание
Произошло	Дата и время события
Результат	Статус успешности события. Возможные значения: – «Успешно»; – «Неуспешно»
Сообщение	Сообщение события. При нажатии кнопки «Копировать» будет отображено окно с возможностью копирования полной информации события

Чтобы экспортировать список событий приложения «Аврора Центр» в файл формата `.csv` необходимо:

– нажать на кнопку «Экспорт» (при необходимости воспользоваться фильтром (подраздел 1.4), чтобы в списке отображались только нужные события приложения «Аврора Центр»);

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия.

После успешного завершения экспорта на ЭВМ будет скачан файл формата `.csv`, который будет содержать те же данные, что и в списке событий.

2.1.1.14.Вкладка «Учетные записи»

Во вкладке «Учетные записи» доступен просмотр локальных пользователей устройства с подробной информацией по ним.

ПРИМЕЧАНИЕ. Содержание вкладки обновляется при каждом получении состояния от устройства, в том числе если оно запрошено через команду оперативного управления.

ВНИМАНИЕ!

✓ Отображение локальных пользователей доступно только для устройств с ОС семейства Linux;

✓ Учитываются сессии по XRDP. Если пользователь, который вошел в систему по XRDP, сейчас подключен и не находится в режиме простоя (idle), тогда для этой учетной записи пользователя отображается статус «Онлайн»;

✓ Сессии пользователя, которые были завершены аварийно (например, вследствие разрядки аккумулятора или отключения питания устройства), не будут учитываться при составлении списка сессий.

Информация о локальных пользователях устройств отображается в столбцах, приведенных в таблице (Таблица 14).

Таблица 14

Параметр	Описание
Имя пользователя	Имя локального пользователя в ОС
Тип	Тип учетной записи. Возможные значения: – «Системный»; – «Несистемный». При необходимости для поиска воспользоваться фильтром по типу учетной записи (подраздел 1.4)
Статус	Статус нахождения пользователя в сети. Возможные значения: – «Офлайн»; – «Онлайн» **ПРИМЕЧАНИЕ.** Локальная учетная запись считается находящейся в статусе «Онлайн», если пользователь вошел в систему одним из следующих способов: – через интерактивный вход (login), включая вход через графический интерфейс (GUI); – через открытие сессии от своего имени с помощью `su`
Sudo	Доступ к sudo у данной учетной записи. Возможные значения: – «Да»; – «Нет»
Группы	Названия локальных групп на устройстве, в которые входит учетная запись. Для копирования названия группы в буфер обмена необходимо нажать кнопку «Скопировать»

2.1.2. Работа с карточкой группы устройств

С помощью карточки группы устройств можно просмотреть детальную информацию о группе устройств, выполнив следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– для отображения группы устройств в области фильтров выбрать «Поиск по группам»;

– нажать на название группы устройств.

В результате откроется карточка группы устройств, интерфейс которой включает:

– общую информацию о группе устройств (Рисунок 18 [1]), состоящую из параметров, приведенных в таблице (Таблица 15);

Таблица 15

Параметр	Описание
Название	Название группы устройств
Тип	Тип группы устройств (Приложение 1)

Параметр	Описание
ID	Идентификатор группы устройств, который можно скопировать, нажав кнопку «Копировать id группы в буфер обмена»
Создано	Дата и время добавления группы устройств
Обновление	Дата и время последнего обновления группы устройств
Комментарий	Дополнительная информация (заполняется при необходимости)

– вкладки карточки (Рисунок 18 [3]) с дополнительной информацией о группе устройств:

- «Устройства» (пп. 2.1.2.1);
- «Политики» (пп. 2.1.2.2);
- «Сценарии» (пп. 2.1.2.3).

При необходимости для поиска устройств возможно применение фильтров (см. Рисунок 18 [4]). Описание фильтров и процесса поиска приведено в подразделе 1.4.

При нажатии на значок (Рисунок 18 [2]) будут доступны следующие действия:

– Редактировать данные (внести необходимые изменения);

– Удалить (п. 2.2.16).

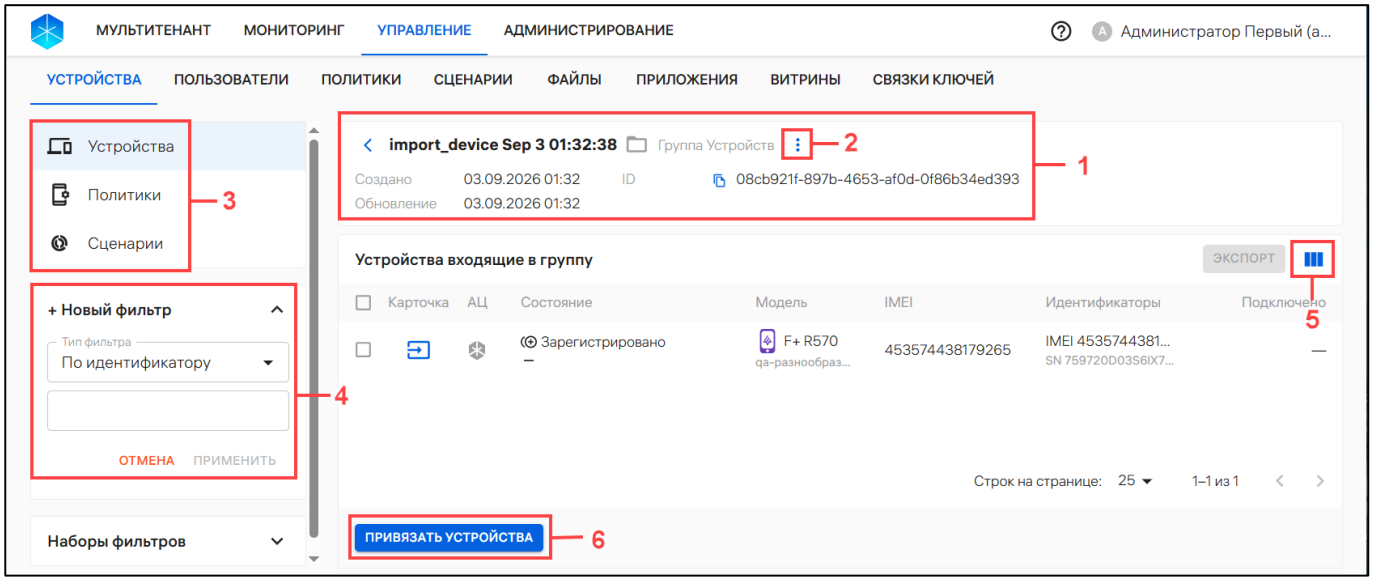


Рисунок 18

2.1.2.1. Вкладка «Устройства»

Во вкладке «Устройства» отображается список устройств, привязанных к группе устройств, а при его отсутствии отображается сообщение «Группа не содержит устройств».

Устройство возможно привязать к группе устройств с помощью кнопки «Привязать устройства» (см. Рисунок 18 [6]), выполнив действия, приведенные в пп. 2.2.9.3.

ПРИМЕЧАНИЕ. Указанный выше способ редактирования списка не применим для устройств из динамической группы. Кнопка «Привязать устройства» во вкладке «Устройства» у динамической группы устройств отсутствует.

Информация по каждому устройству отображается в столбцах, приведенных в таблице (Таблица 16).

ПРИМЕЧАНИЕ. Значение некоторых столбцов может быть отсортировано: от старых к новым, от новых к старым.

Таблица 16

Параметр	Описание
Карточка	Значок, при нажатии на который осуществляется переход к карточке устройства. Отображается по умолчанию. Не доступен для скрытия
АЦ	Значок со статусом приложения «Аврора Центр». Возможные значения: – «клиент АЦ установлен» - на устройстве установлено приложение «Аврора Центр», с помощью которого выполняется управление устройством; – «клиент АЦ удален» - на устройстве было удалено приложение «Аврора Центр»; – «нет данных о Клиенте» - ППО не получил данные об установленном приложении «Аврора Центр» на устройстве. Не отображается по умолчанию. Доступен для скрытия/отображения
Состояние	Статус жизненного цикла и соответствие назначенной политике (Приложение 1). Отображается по умолчанию. Не доступен для скрытия
Модель	– модель устройства; – комментарий – дополнительная информация (заполняется при необходимости). Столбец отображается по умолчанию. Доступен для скрытия/отображения
IMEI	Международный идентификатор устройства. Не отображается по умолчанию. Доступен для скрытия/отображения
Серийный номер	Серийный номер, который присвоен устройству производителем. Не отображается по умолчанию. Доступен для скрытия/отображения
Ethernet MAC	MAC-адрес Ethernet устройства. Не отображается по умолчанию. Доступен для скрытия/отображения
WLAN MAC	MAC-адрес WLAN устройства. Не отображается по умолчанию. Доступен для скрытия/отображения

Параметр	Описание
Сетевое имя устройства	Сетевое имя (hostname) устройства. Не отображается по умолчанию. Доступен для скрытия/отображения. ПРИМЕЧАНИЕ. В общем списке устройств и в списке устройств группы доступна сортировка списка устройств по столбцу «Сетевое имя устройства»
Идентификаторы	Идентификаторы устройства. Порядок отображения идентификаторов задается в настройках администрирования ППО (пп. 4.1.4.1). Отображается по умолчанию. Доступен для скрытия/отображения
Обновлено	Дата и время внесения последних изменений в устройство (редактирование имени устройства, модели или комментария; привязка/отвязка к группам или пользователям; назначение/отвязка политики или офлайн-сценария на устройство). Отображается по умолчанию. Доступен для скрытия/отображения. ПРИМЕЧАНИЕ. Доступна сортировка списка устройств по столбцу «Обновлено»
Подключено	Дата и время последнего подключения устройства к ППО. Отображается по умолчанию. Доступен для скрытия/отображения. ПРИМЕЧАНИЕ. Доступна сортировка списка устройств по столбцу «Подключено»

Чтобы скрыть/отобразить нужные столбцы в списке необходимо:

– нажать на значок «Управлять отображением столбцов» (см. Рисунок 18 [5]);

– установить или снять галочку в чекбоксе напротив названия тех столбцов, которые требуется отобразить или скрыть в списке, соответственно.

ВНИМАНИЕ! Если очистить localStorage браузера, то настройки отображения идентификаторов примут значения по умолчанию.

2.1.2.2. Вкладка «Политики»

Во вкладке «Политики» отображается список политик, назначенных на группу устройств, а при его отсутствии отображается сообщение «На группу не назначена ни одна политика».

Политика может быть назначена на группу устройств нажатием кнопки «Назначить политики» и выполнением действий, приведенных в пп. 2.4.4.2.

Информация о назначенных политиках отображается в следующих столбцах:

– «Название» – название политики, которая представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке политики (п. 2.1.5);

– «Дата назначения» – дата и время назначения политики на группу устройств.

2.1.2.3. Вкладка «Сценарии»

Во вкладке «Сценарии» отображается список офлайн-сценариев, назначенных на группу устройств, а при его отсутствии отображается сообщение «На группу не назначен ни один офлайн-сценарий».

ПРИМЕЧАНИЕ. Перед назначением офлайн-сценария на группу устройств необходимо убедиться, что добавлен хотя бы 1 офлайн-сценарий. Процесс добавления офлайн-сценариев приведен в п. 2.5.1.

При добавлении устройств в группу устройств все ранее назначенные на группу офлайн-сценарии будут применены на устройстве, в том числе при импорте устройства.

ПРИМЕЧАНИЕ. Процесс назначения офлайн-сценария на группы устройств и отвязки через карточку группы устройств приведен в пп. 2.5.2.3 и пп. 2.5.3.2 соответственно.

В рабочей области информация о назначенных офлайн-сценариях отображается в столбцах, приведенных в таблице (Таблица 17).

Таблица 17

Параметр	Описание
Название	– название офлайн-сценария; – комментарий – дополнительная информация (заполняется при необходимости)
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 53)
Реакция	Действие, которое должно произойти с устройством из группы устройств в результате назначения данного офлайн-сценария
Дата назначения	Дата и время назначения офлайн-сценария на группу устройств

2.1.3. Работа с карточкой пользователя

Для просмотра карточки пользователя необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– для отображения списка пользователей в области фильтров выбрать «Поиск по пользователям»;

– выбрать необходимого пользователя и нажать на имя.

В результате откроется карточка пользователя, интерфейс которой включает:

– общую информацию о пользователе (Рисунок 19 [1]), состоящую из параметров, приведенных в таблице (Таблица 18);

Таблица 18

Параметр	Описание
Пользователь	– фамилия, имя и отчество пользователя; – тип пользователя (Приложение 1)

Параметр	Описание
ID	Идентификатор пользователя, который можно скопировать, нажав кнопку «Копировать id пользователя в буфер обмена»
Должность	Должность, занимаемая пользователем
Email	Электронная почта пользователя
Тел. рабочий	Рабочий телефон пользователя
Создание	Дата и время добавления пользователя
Обновление	Дата и время последнего обновления информации о пользователе

– вкладки карточки (Рисунок 19 [2]) с дополнительной информацией о пользователе:

- «Устройства» (пп. 2.1.3.1);
- «Группы» (пп. 2.1.3.2);
- «Политики» (пп. 2.1.3.3).

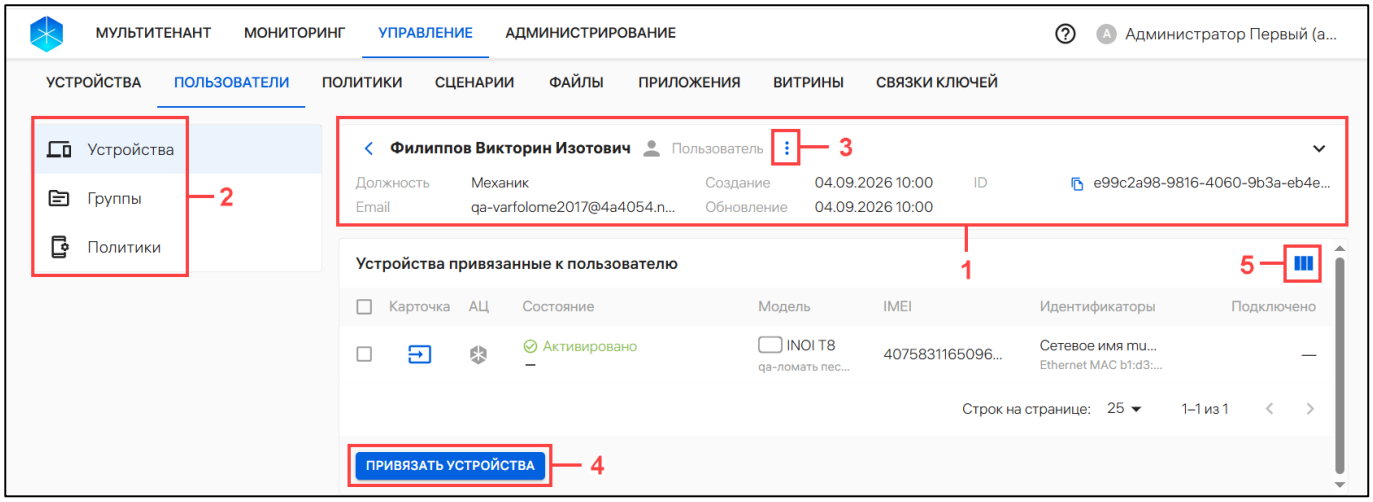


Рисунок 19

При нажатии на значок ⋮ (см. Рисунок 19 [3]) будут доступны следующие действия:

– Редактировать данные (внести необходимые изменения);

– Архивировать (п. 2.3.7).

ПРИМЕЧАНИЕ. Редактированию вручную подлежат данные только пользователей с типом «Пользователь». Для обновления данных пользователей с типом «Пользователь из орг.подразделения» необходимо повторно получить данные из LDAP.

2.1.3.1. Вкладка «Устройства»

Во вкладке «Устройства» отображается список устройств, привязанных к пользователю.

Для редактирования списка устройств во вкладке «Устройства» необходимо нажать кнопку «Привязать устройства» (см. Рисунок 19 [4]) и выполнить действия, приведенные в пп. 2.3.5.2.

ПРИМЕЧАНИЕ. На все привязанные и отвязанные устройства будут применены новые перекомбинированные политики и офлайн-сценарии.

Информация об устройствах отображается в столбцах, приведенных в таблице (см.Таблица 16). Описание возможности скрыть/отобразить нужные столбцы в списке приведено в пп. 2.1.2.1.

2.1.3.2. Вкладка «Группы»

Во вкладке «Группы» отображается список привязанных к пользователю групп пользователей, а при их отсутствии отображается сообщение «Пользователь не состоит ни в одной группе».

Для редактирования списка групп пользователей во вкладке «Группы» необходимо нажать кнопку «Добавить в группы» и выполнить действия, приведенные в пп. 2.3.4.2.

Название группы пользователей представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке группы.

Информация о группах пользователей отображается в столбцах, приведенных в таблице (Таблица 19).

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 19

Параметр	Описание
Тип	Тип группы пользователей (Приложение 1)
Группа пользователей	– название группы пользователей, к которой привязан данный пользователь; – комментарий – дополнительная информация (заполняется при необходимости)
Пользователей	Количество участников группы
Дата назначения	Дата и время привязки пользователя к группе

2.1.3.3. Вкладка «Политики»

Во вкладке «Политики» отображается список политик, назначенных на группу пользователей, к которой привязан данный пользователь (Рисунок 20 [2]), а при отсутствии назначенных политик отображается сообщение «На пользователя не назначено ни одной политики».

В случае пересечения с другими политиками отобразится полный список названий всех политик на группах устройств или группах пользователей.

Информация о политиках отображается в следующих столбцах (Рисунок 20):

– «Название» – название политики, назначенной на группу пользователей устройства, в которую входит текущий пользователь. Представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке (п. 2.1.5);

– «Содержимое» – краткая информация по правилам, добавленным в политику;

– «Группа» – наименование группы, на которую назначена политика.

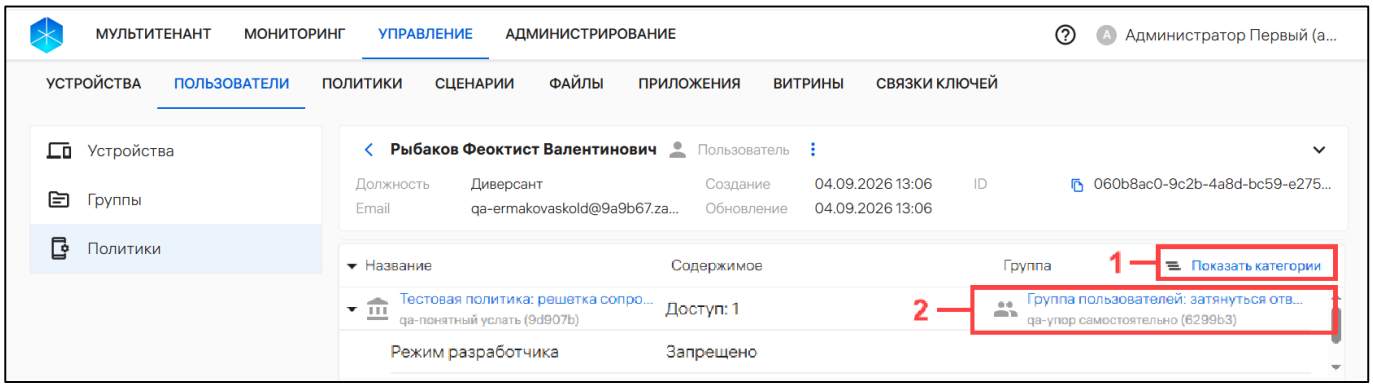


Рисунок 20

Для отображения категорий правил политик, назначенных на группу пользователей, необходимо нажать кнопку «Показать категории» (см. Рисунок 20 [1]).

Для просмотра вложенной информации о политике необходимо нажать значок , в результате чего откроется вложенная информация о политике.

2.1.4. Работа с карточкой группы пользователей

Для просмотра карточки группы пользователей необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название выбранной группы пользователей.

В результате откроется карточка группы пользователей, интерфейс которой включает:

– общую информацию о группе пользователей (Рисунок 21 [1]), состоящую из параметров, приведенных в таблице (Таблица 20);

Таблица 20

Параметр	Описание
Название	Название группы пользователей
Тип	Тип группы пользователей (Приложение 1)
ID	Идентификатор группы пользователей, который может быть скопирован нажатием кнопки «Копировать»
Создано	Дата и время добавления группы пользователей
Обновление	Дата и время последнего обновления группы пользователей
Комментарий	Дополнительная информация (заполняется при необходимости)

– вкладки карточки (Рисунок 21 [2]) с дополнительной информацией о группе пользователей:

- «Пользователи» (пп. 2.1.4.1);
- «Политики» (пп. 2.1.4.2);
- «Сценарии» (пп. 2.1.4.3).

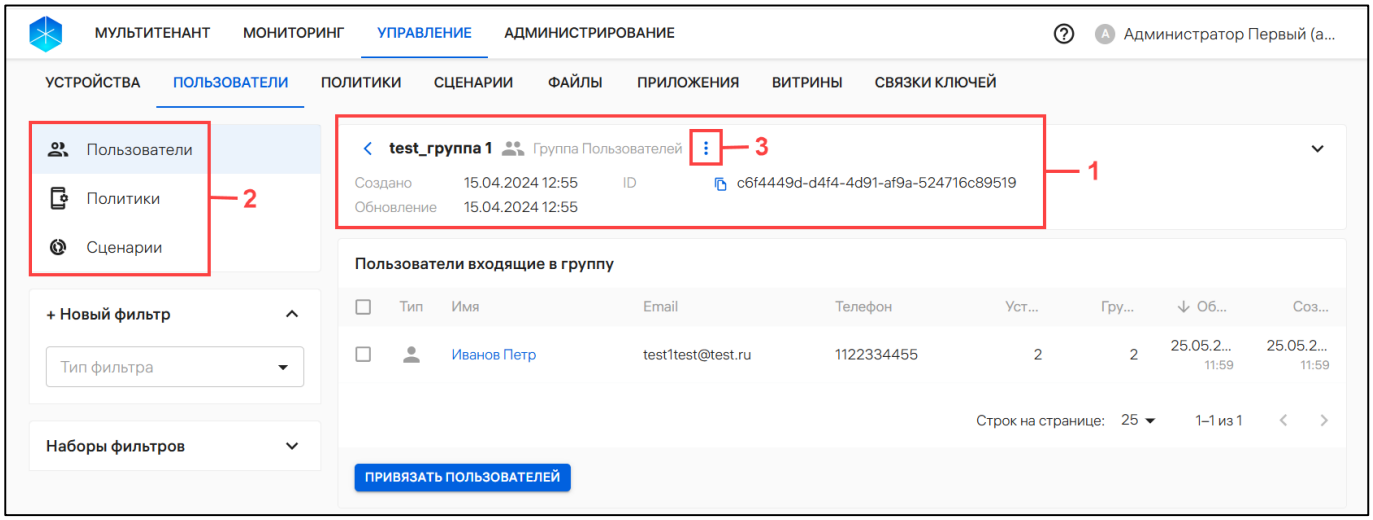


Рисунок 21

При нажатии на значок ⋮ (см. Рисунок 21 [2]) будут доступны следующие действия:

– Редактировать данные (внести необходимые изменения);

– Удалить (п. 2.3.8).

ПРИМЕЧАНИЕ. Редактирование группы с типом «Организационное подразделение» недоступно. Кнопки «Удалить», «Привязать пользователей» у такой группы неактивны.

2.1.4.1. Вкладка «Пользователи»

Во вкладке «Пользователи» отображается список пользователей для данной группы пользователей, а при отсутствии списка отображается сообщение «В группе нет пользователей».

Для редактирования списка пользователей необходимо нажать кнопку «Привязать пользователей» и выполнить действия, приведенные в пп. 2.3.4.3.

При необходимости для поиска устройств возможно применение фильтров. Описание фильтров и процесса поиска приведено в подразделе 1.4.

Информация о пользователях отображается в столбцах, приведенных в таблице (Таблица 21).

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 21

Параметр	Описание
Тип	Тип пользователей, входящих в группу (Приложение 1)
Имя	Фамилия, имя и отчество пользователя (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку пользователя (п. 2.1.3)
Email	Рабочая почта пользователя
Телефон	Номер телефона пользователя
Устройства	Количество устройств, привязанных к пользователю
Группы	Количество групп, в которые включен пользователь
Обновлено	Дата и время обновления данных пользователя

2.1.4.2. Вкладка «Политики»

Во вкладке «Политики» отображается список политик, назначенных на группу пользователей, а при отсутствии списка отображается сообщение «На группу не назначена ни одна политика».

Для редактирования списка политик необходимо нажать кнопку «Назначить политики» и далее выполнить действия, описанные в пп. 2.4.4.3.

Информация о политиках отображается в столбцах, приведенных в таблице (Таблица 22).

Таблица 22

Параметр	Описание
Название	Название политики, назначенной на группу пользователей (представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке политики (п. 2.1.5)
Дата назначения	Дата назначения политики

2.1.4.3. Вкладка «Сценарии»

Во вкладке «Сценарии» отображается список офлайн-сценариев, назначенных на группу пользователей, а при его отсутствии отображается сообщение «На группу не назначен ни один офлайн-сценарий».

ПРИМЕЧАНИЕ. Для назначения и отвязки офлайн-сценария необходимо нажать кнопку «Назначить сценарии» и выполнить действия, приведенные в пп. 2.5.2.4 и пп. 2.5.3.2.

ВНИМАНИЕ! Перед назначением офлайн-сценария на группу пользователей необходимо убедиться, что добавлен хотя бы 1 офлайн-сценарий. Процедура добавления офлайн-сценариев описана в п. 2.5.1.

При добавлении пользователей в группу пользователей, все ранее назначенные на группу офлайн-сценарии будут применены на пользователя, в том числе при импорте.

В рабочей области информация о назначенных офлайн-сценариях отображается в столбцах, приведенных в таблице (Таблица 23).

Таблица 23

Параметр	Описание
Название	– название офлайн-сценария (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку офлайн-сценария); – комментарий – дополнительная информация (заполняется при необходимости)
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 53)
Реакция	Действие, которое должно произойти с группой пользователей в результате назначения данного офлайн-сценария
Дата назначения	Дата и время назначения офлайн-сценария на группу пользователей

2.1.5. Работа с карточкой политики

В карточке политики отображается информация о правилах политики и списках групп пользователей, на которых данная политика назначена.

Для просмотра карточки политики необходимо выполнить следующие действия:

– перейти в подраздел «Политики» раздела «Управление»;

– нажать на название политики.

В результате откроется карточка политики, интерфейс которой включает:

– общую информацию о политике (Рисунок 22 [1], состоящую из параметров, приведенных в таблице (Таблица 24);

Таблица 24

Параметр	Описание
Название	Название политики
ID	Идентификатор политики, который можно скопировать, нажав кнопку «Копировать id политики в буфер обмена»
Создано	Дата и время создания политики
Обновление	Дата и время последнего обновления политики
Комментарий	Дополнительная информация (заполняется при необходимости)

– вкладки карточки (Рисунок 22 [2]) с дополнительной информацией о политике:

- «Правила» (пп. 2.1.5.1);
- «Группы» (пп. 2.1.5.2).

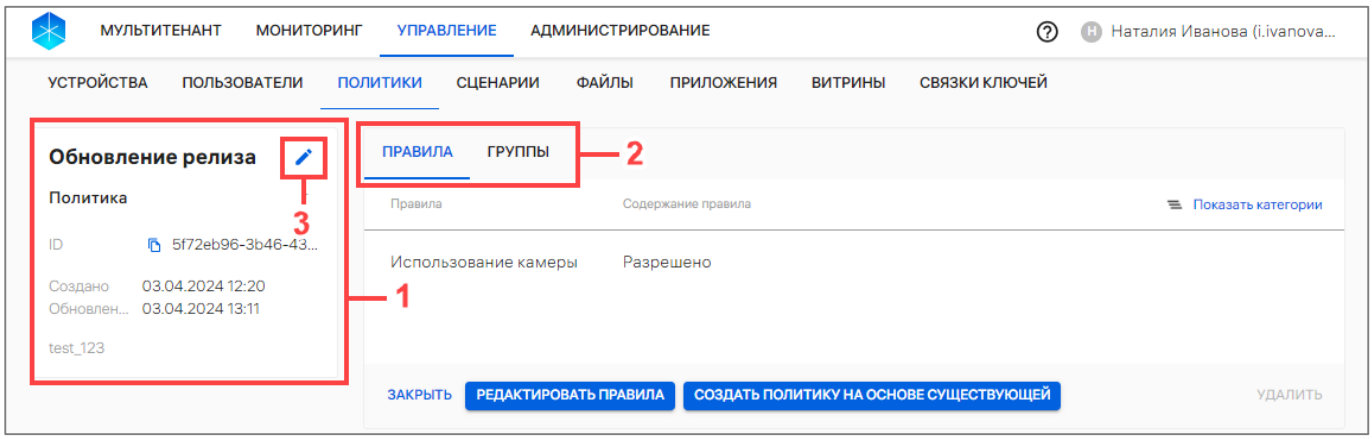


Рисунок 22

Для редактирования данных политики необходимо нажать на значок «Редактировать» (см. Рисунок 22 [3]) и внести необходимые изменения в следующие поля:

– «Наименование»;
– «Комментарий».

2.1.5.1. Вкладка «Правила»

Во вкладке «Правила» отображается список правил, добавленных в политику, с указанием их категории и содержания. Информация отображается в следующих столбцах (Рисунок 23):

– «Правила» – название правила;
– «Содержание правила» – краткая информация по правилам, добавленным в политику.

Для отображения категории правил необходимо нажать кнопку «Показать категории» (Рисунок 23).

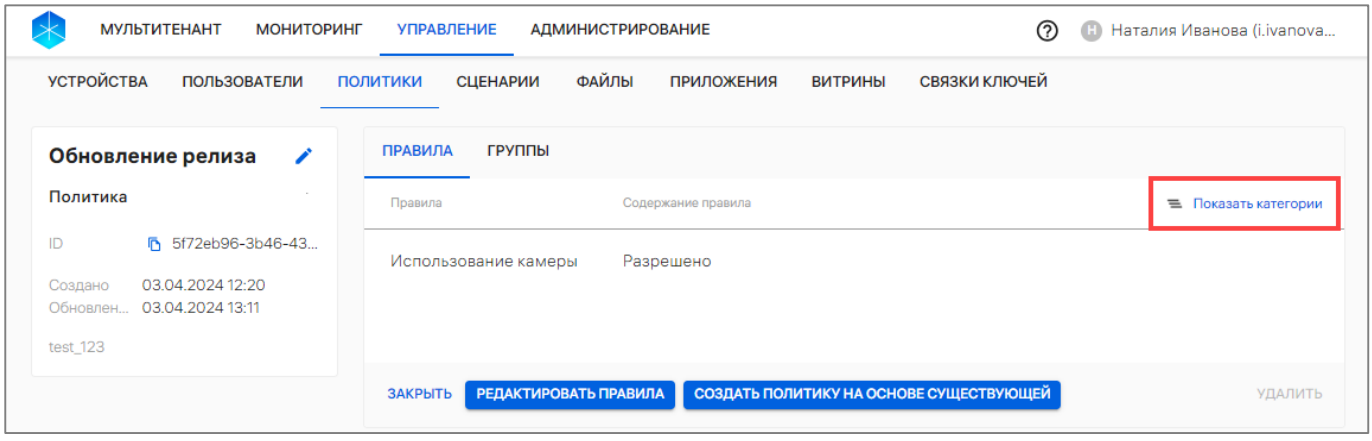


Рисунок 23

Для просмотра информации о каждой категории правил необходимо нажать значок в строке с категорией (Рисунок 24 [1]), в результате чего отобразится перечень правил, входящих в данную категорию.

Для перехода к списку правил необходимо нажать кнопку ☰ «Показать список» (Рисунок 24 [2]).

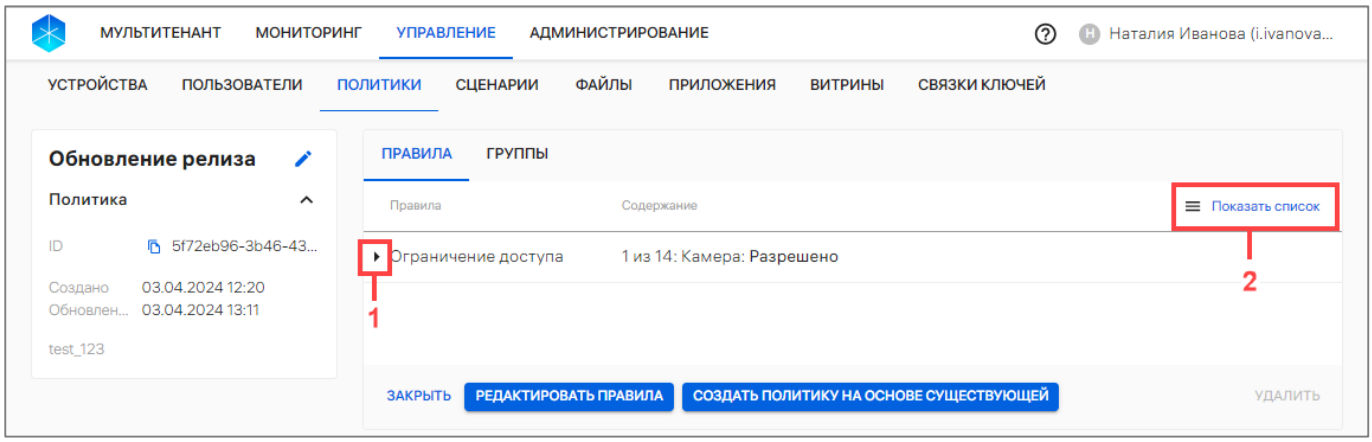


Рисунок 24

Набор правил политики подлежит редактированию. Процесс редактирования приведен в п. 2.4.6.

2.1.5.2. Вкладка «Группы»

Во вкладке «Группы» отображаются группы действия политик (списки групп устройств и групп пользователей), на которые назначена политика.

Для редактирования списка групп устройств или групп пользователей необходимо нажать кнопку «Редактировать группы» и далее выполнить действия, описанные в пп. 2.4.4.1 и пп. 2.4.7.1.

Информация о группах, на которые распространяется действие политики, отображается в столбцах, приведенных в таблице (Таблица 25).

Таблица 25

Параметр	Описание
Группа	– название группы устройств или группы пользователей, на которые назначена данная политика (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку группы); – комментарий – дополнительная информация (заполняется при необходимости)
Тип	Тип группы: – 👥 – группа пользователей; – 📱 – группа устройств
Дата назначения	Дата и время назначения политики

2.1.6. Работа с карточкой офлайн-сценария

В карточке офлайн-сценария отображаются параметры, заданные при создании сценария (событие, реакция, наименование, комментарий), а также группы устройств и пользователей, на которые сценарий назначен.

Для просмотра карточки сценария необходимо выполнить следующие действия:

– перейти в подраздел «Сценарии» раздела «Управление»;

– нажать на название офлайн-сценария.

В результате откроется карточка офлайн-сценария, интерфейс которой включает:

– общую информацию об офлайн-сценарии (Рисунок 25 [1]), состоящую из параметров, приведенных в таблице (Таблица 26);

Таблица 26

Параметр	Описание
Название	Название офлайн-сценария
ID	Идентификатор офлайн-сценария, который можно скопировать, нажав кнопку «Копировать id сценария в буфер обмена»
Создано	Дата и время создания офлайн-сценария
Комментарий	Дополнительная информация (заполняется при необходимости)

– вкладки карточки (Рисунок 25 [2]) с дополнительной информацией:

- «Событие и реакция» - действия (события) по срабатыванию;
- «Группы» - список групп устройств и групп пользователей, на которые назначен данный офлайн-сценарий.

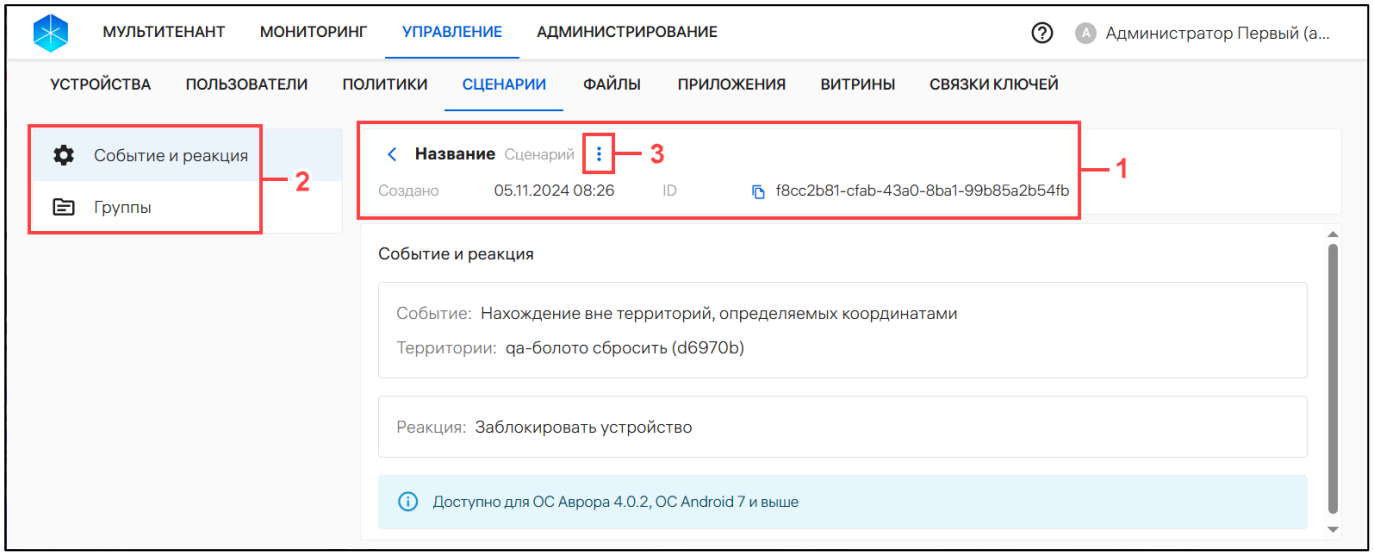


Рисунок 25

2.1.7. Работа с карточкой файла/папки

С помощью карточки файла/папки возможно выполнить следующие действия:

– просмотреть информацию о файле/папке;

– добавить, скачать и согласовать версию файла/папки;

– удалить версию файла/папки.

Для просмотра карточки файла/ необходимо выполнить следующие действия:

– перейти в подраздел «Файлы» раздела «Управление»;

– в области фильтров выбрать:

- раздел «Файлы», для отображения списка файлов;
- раздел «Папки из git-репозиториев», для отображения списка папок;

– нажать на название необходимого файла/папки.

В результате откроется карточка файла/папки, интерфейс которой включает:

– общую информацию о файле (Рисунок 26 [1], Рисунок 27 [1]), состоящую из параметров, приведенных в таблице (Таблица 27);

– версии файла/папок (Рисунок 26 [2], Рисунок 27 [2]).

Таблица 27

Параметр	Описание
ID	Идентификатор файла/папки, который можно скопировать, нажав значок
Источник	Источник откуда был загружен рабочий файл/папка
Ветка	Ветка в git-репозитории
Путь к файлу/ Путь к папке	Абсолютный путь к файлу/папке на устройстве
Папка	Название папки. **ПРИМЕЧАНИЕ.** Отображается только в карточке файла
Количество	Общее количество версий рабочего файла/папки
Создан	Дата и время создания файла/папки
Обновлен	Дата и время последнего обновления файла/папки
Комментарий	Дополнительная информация (заполняется при необходимости)

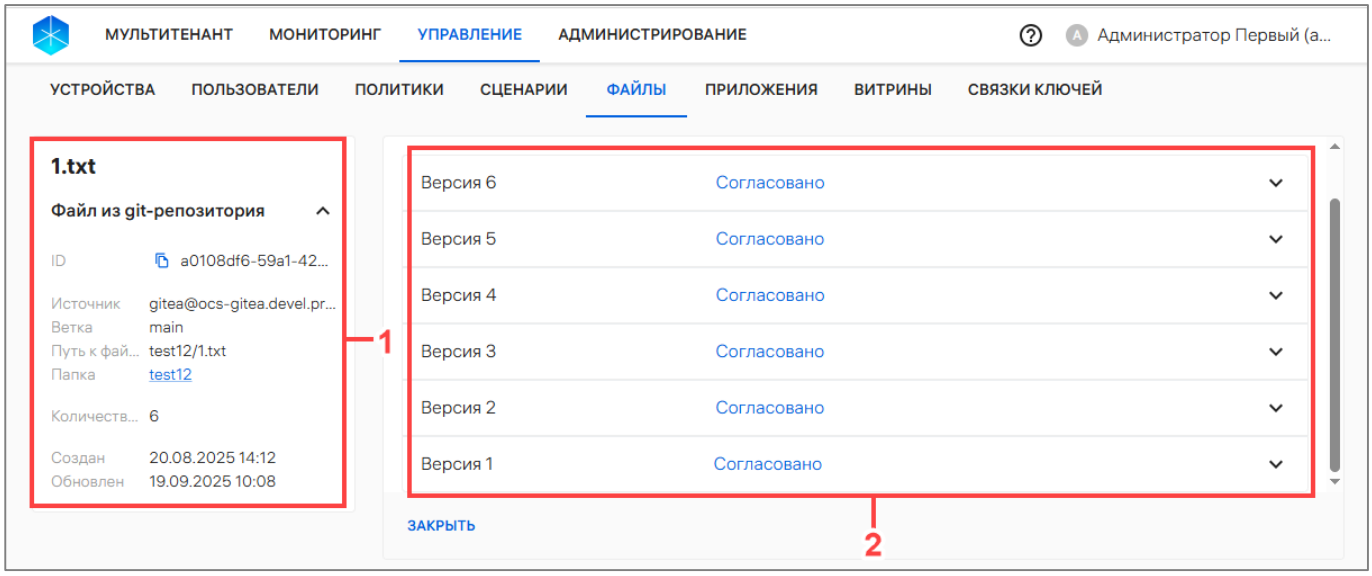


Рисунок 26

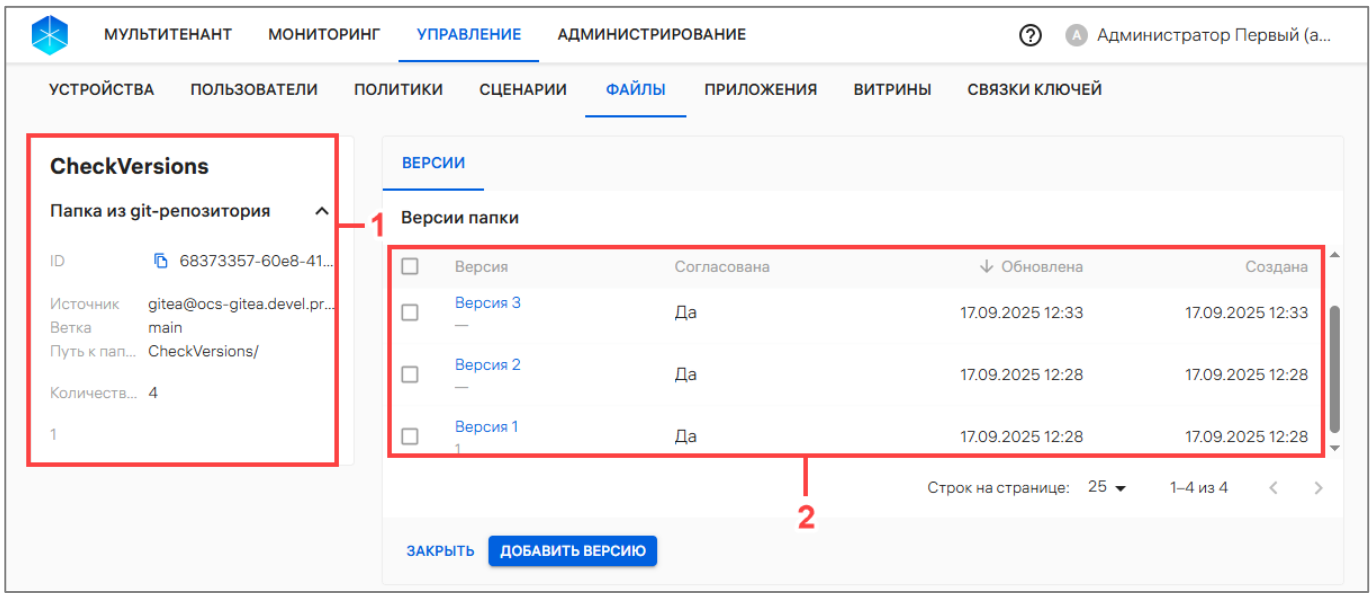


Рисунок 27

2.2. Подраздел «Устройства»

Подраздел «Устройства» Консоли администратора ПУ предназначен для работы с моделями устройств, списком устройств/групп устройств.

Для перехода в подраздел необходимо выбрать в верхней панели раздел «Управление», подраздел «Устройства». В результате в рабочей области отобразится список устройств/групп устройств (Рисунок 28 [2]).

Для отображения группы устройств необходимо в области фильтров выбрать «Поиск по группам» (Рисунок 28 [1]).

ПРИМЕЧАНИЕ. Архивные устройства отображаются в списке устройств только в случае, если включена соответствующая настройка (п. 4.1.3).

Для просмотра списка моделей устройств, зарегистрированных в ПУ, необходимо нажать кнопку «Модели устройств» (Рисунок 28 [3]).

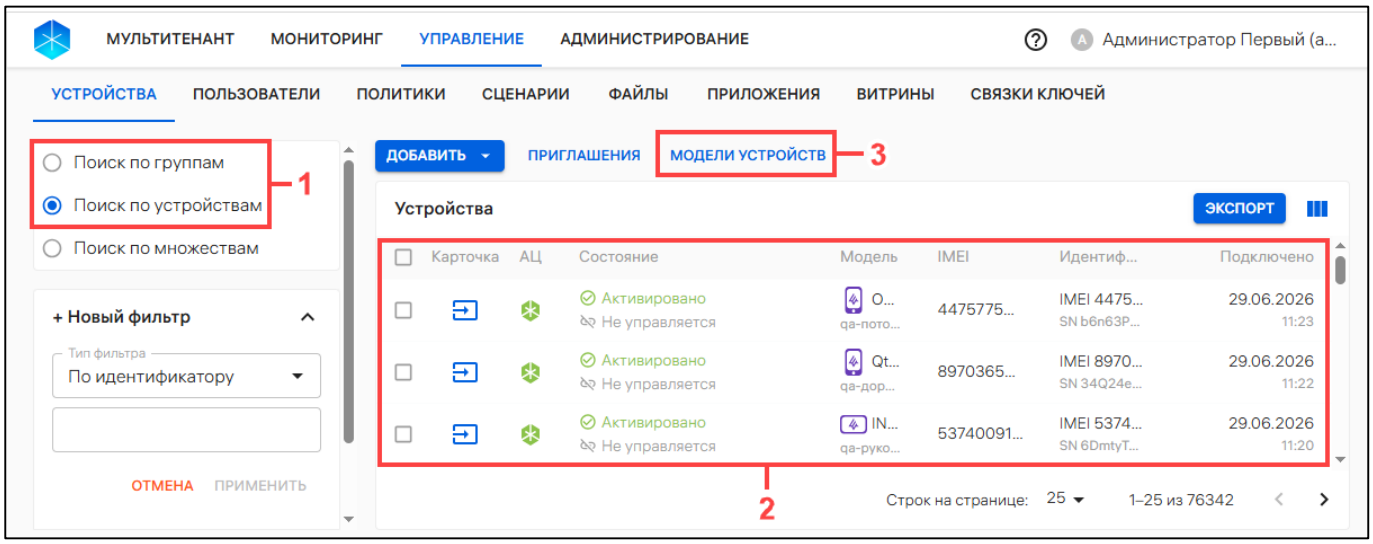


Рисунок 28

В рабочей области подраздела «Устройства» информация об устройствах отображается в столбцах, описания которых приведены в таблице (см. Таблица 16). При отсутствии информации о добавленных устройствах или групп устройств отображается сообщение «Нет данных».

При выборе в области фильтров «Поиск по группам» (см. Рисунок 28 [1]) информация о группах устройств в рабочей области отображается в столбцах, приведенных в таблице (Таблица 28).

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 28

Параметр	Описание
Тип	Тип группы устройств (Приложение 1)
Группа устройств	– название группы устройств (представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку группы устройств); – комментарий - дополнительная информация (заполняется при необходимости)
Принцип добавления	Значение, по которому устройства были добавлены в группу
Устройства	Количество устройств, привязанных к группе
Обновлено	Параметр сортировки по дате обновления политики

При переходе на страницу «Модели устройств» отобразится список моделей устройств, информация о которых отображается в столбцах, приведенных в таблице (Таблица 29).

ПРИМЕЧАНИЕ. Скрытые модели будут выделены серым цветом.

Таблица 29

Параметр	Описание
Название	Отображаемое в ПУ наименование производителя и модели устройства (например, Kozen P10)
Тип устройства	Тип устройств, к которому относится модель. Возможные значения: – «Планшет»; – «Смартфон»; – «КПК»; – «ПК»; – «ТСД»; – «POS-терминал»; – «Неизвестно»
Модель	Техническое название модели

Параметр	Описание
Комментарий	Произвольный комментарий к модели (при наличии)
Код модели	Уникальный код модели устройства. Может быть использован в шаблоне для импорта устройств (пп. 2.2.3.1)

В Консоли администратора ПУ предусмотрена возможность добавления устройств или групп устройств одним из следующих способов:

– вручную в соответствии с пп. 2.2.1.1 и п. 2.2.2;

– с помощью CSV-файла в соответствии с п. 2.2.2.2.1;

– с помощью приглашения на самостоятельную регистрацию устройства в соответствии с пп. 2.2.1.2.

2.2.1. Добавление устройства в ПУ

2.2.1.1. Добавление устройства вручную

Для добавления устройства вручную необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить устройство» (Рисунок 29);

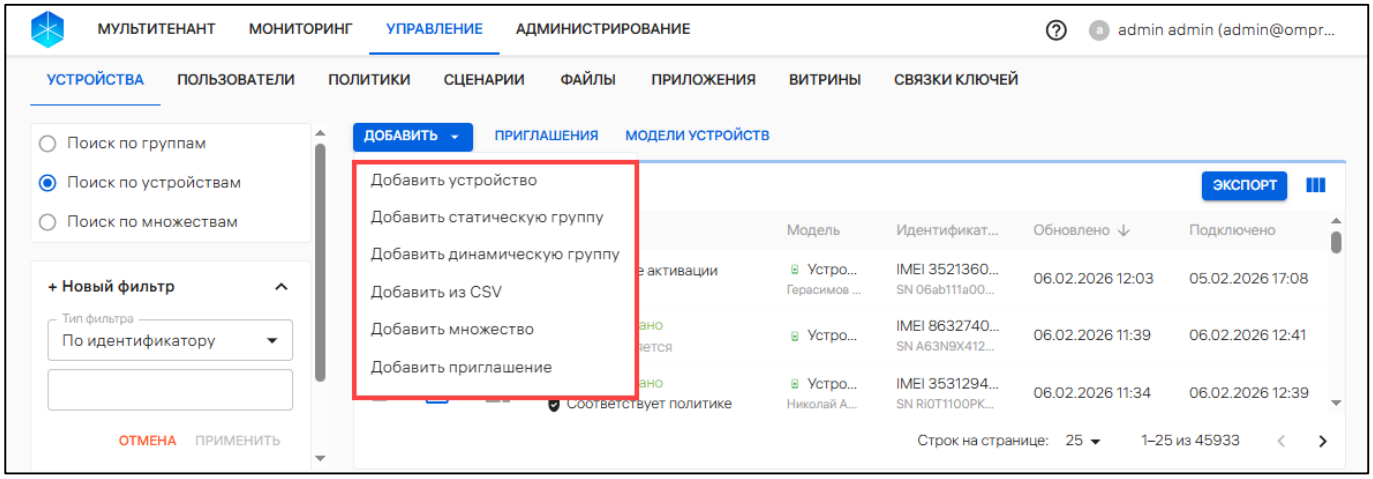


Рисунок 29

– в открывшемся окне заполнить поля, приведенные в таблице (Таблица 30).

ПРИМЕЧАНИЕ. Для отображения полей «IMEI», «Серийный номер», «Ethernet MAC», «WLAN MAC», «Имя устройства» необходимо установить галочку в чекбоксе напротив требуемого параметра. После ввода значения нажать «Enter» на клавиатуре и при необходимости добавить второе значение для полей: «IMEI», «Ethernet MAC», «WLAN MAC». При необходимость удалить параметр, нажать на значок справа от значения. Для полной очистки нажать на значок «Очистить» в конце поля.

ВИМАНИЕ! Рекомендуется заполнить все существующие идентификаторы устройства, чтобы уменьшить риск создания дублей;

– после ввода значений необходимо подтвердить либо отменить действия.

При успешном добавлении устройства отобразится соответствующее сообщение и откроется карточка добавленного устройства (п. 2.1.1).

Таблица 30

Параметр	Значения
IMEI	Ввести международный идентификатор мобильного оборудования. Ввод значения с клавиатуры. Количество символов – 15 цифр. **ПРИМЕЧАНИЕ.** Если устройство поддерживает работу 2 SIM-карт, в поле допускается ввод любого из 2 значений IMEI
Серийный номер	Ввести серийный номер, который присвоен устройству производителем. Может содержать от 1 до 20 символов
Ethernet MAC	Ввести MAC-адрес Ethernet устройства, который состоит из 6 пар символов, разделенных двоеточием
WLAN MAC	Ввести MAC-адрес WLAN устройства. Ввод значения с клавиатуры. Количество символов – 6 пар символов, разделенных двоеточием, например: «00:aa:00:00:a0:00»
Имя устройства	Ввод значения с клавиатуры. (Например, инвентарное имя устройства внутри компании). Может содержать от 1 до 16 символов. **ПРИМЕЧАНИЕ.** Поле не является обязательным для заполнения
Платформа	Выбор доступной платформы из списка: – Аврора; – Android; – Linux **ПРИМЕЧАНИЕ.** Поле обязательно для заполнения
Модель устройства	Выбор модели устройства из раскрывающегося списка. Если нужной модели нет в списке, необходимо добавить ее (подробнее в п. 2.2.4). **ПРИМЕЧАНИЕ.** Полное название типа устройств зависит от модели устройства
Комментарий	Ввод значения с клавиатуры. Максимальная длина – 512 символов. **ПРИМЕЧАНИЕ.** Поле не является обязательным для заполнения

2.2.1.2. Добавление и активация устройства в ПУ с помощью приглашения на самостоятельную регистрацию

С помощью приглашения возможно автоматически добавить новое устройство с любой из поддерживаемых ОС в ПУ и активировать его.

ВНИМАНИЕ! Повторная активация уже добавленного устройства в ПУ доступна в случаях если:

– устройство имеет статус «Очищено». В этом случае счетчик переактиваций для устройства (в день) не учитывается;

– задан счетчик переактиваций в приглашении, отличный от нуля, и если он для устройства не превышен, то можно использовать приглашение для переактивации устройства.

ПРИМЕЧАНИЕ. В случае неуспешной активации по приглашению, устройство будет автоматически повторять попытки активации с интервалом в 3 часа.

Для добавления и активации устройства в ПУ необходимо выполнить следующие действия:

– создать приглашение на самостоятельную регистрацию устройства (п. 2.2.4);

– установить приложение «Аврора Центр» на устройствах, описание которых приведено в следующих документах:

- «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;
- «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android»;
- «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux»;

– не переименовывая приглашение (файл должен иметь название `invite.json`), разместить JSON-файл на устройство:

- для ОС Аврора – `/etc/emm/`;
- для ОС Android – `files/plugins_data/emm/`;
- для ОС семейства Linux – `/etc/omp-uem-agent/`.

Далее на устройстве, в зависимости от версии ОС, выполнить следующие действия:

– для ОС Аврора/ОС Android, запустить приложение «Аврора Центр» и дождаться завершения процесса автодобавления и автоактивации устройства;

– для ОС семейства Linux дождаться завершения процесса автодобавления и автоактивации устройства (это может занять некоторое время) или перезапустить daemon клиента вручную с помощью команды:

```
sudo systemctl restart ru.omp.uem.service
```

В результате устройство будет добавлено и активировано в ПУ.

ПРИМЕЧАНИЕ. В случае неуспешной активации по приглашению, устройство будет автоматически повторять попытки активации с интервалом в 3 часа.

2.2.2. Добавление группы устройств вручную

При добавлении группы устройств в ручную доступно:

– добавление статической группы устройств (пп. 2.2.2.1);

– добавление динамической группы устройств (пп. 2.2.2.2).

2.2.2.1. Добавление статической группы устройств

ПРИМЕЧАНИЕ. Состав правил статической группы Администратор может редактировать вручную.

Для добавления статической группы необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить статическую группу» (см. Рисунок 29);

– в открывшемся окне заполнить поля, приведенные в таблице (Таблица 31);

– подтвердить либо отменить действия.

В результате успешного добавления статической группы отобразится соответствующее сообщение и откроется карточка добавленной группы (п. 2.1.1.13).

Таблица 31

Параметры	Описание
Имя группы	Ввод значения с клавиатуры. Поле обязательно для заполнения. Название группы устройств должно быть уникальным
Комментарий	Ввод значения с клавиатуры. Максимальная длина – 512 символов. Поле с дополнительной информацией не является обязательным для заполнения

2.2.2.2. Добавление динамической группы устройств

Динамическая группа устройств — группа с заданными условиями, при соблюдении которых устройства попадают в группу автоматически.

Для добавления динамической группы необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить динамическую группу» (см. Рисунок 29);

– в открывшемся окне раздела «Название, комментарий» (Рисунок 30 [1]) заполнить поля, приведенные в таблице (см. Таблица 31);

– в области фильтров выбрать и задать значения параметров, приведенных в таблице (Таблица 32), по которым устройства будут добавлены в динамическую группу (Рисунок 30 [2]), и далее подтвердить действия, нажав кнопку «Создать».

ПРИМЕЧАНИЯ:

✓ Возможно задать несколько параметров для динамической группы. В этом случае в динамическую группу попадут устройства, которые удовлетворяют всем заданным критериям;

✓ Для одного набора параметров можно создать только одну динамическую группу.

В результате успешного создания динамической группы устройств отобразится соответствующее сообщение и откроется карточка добавленной группы, которая будет включать все устройства, удовлетворяющие заданному критерию.

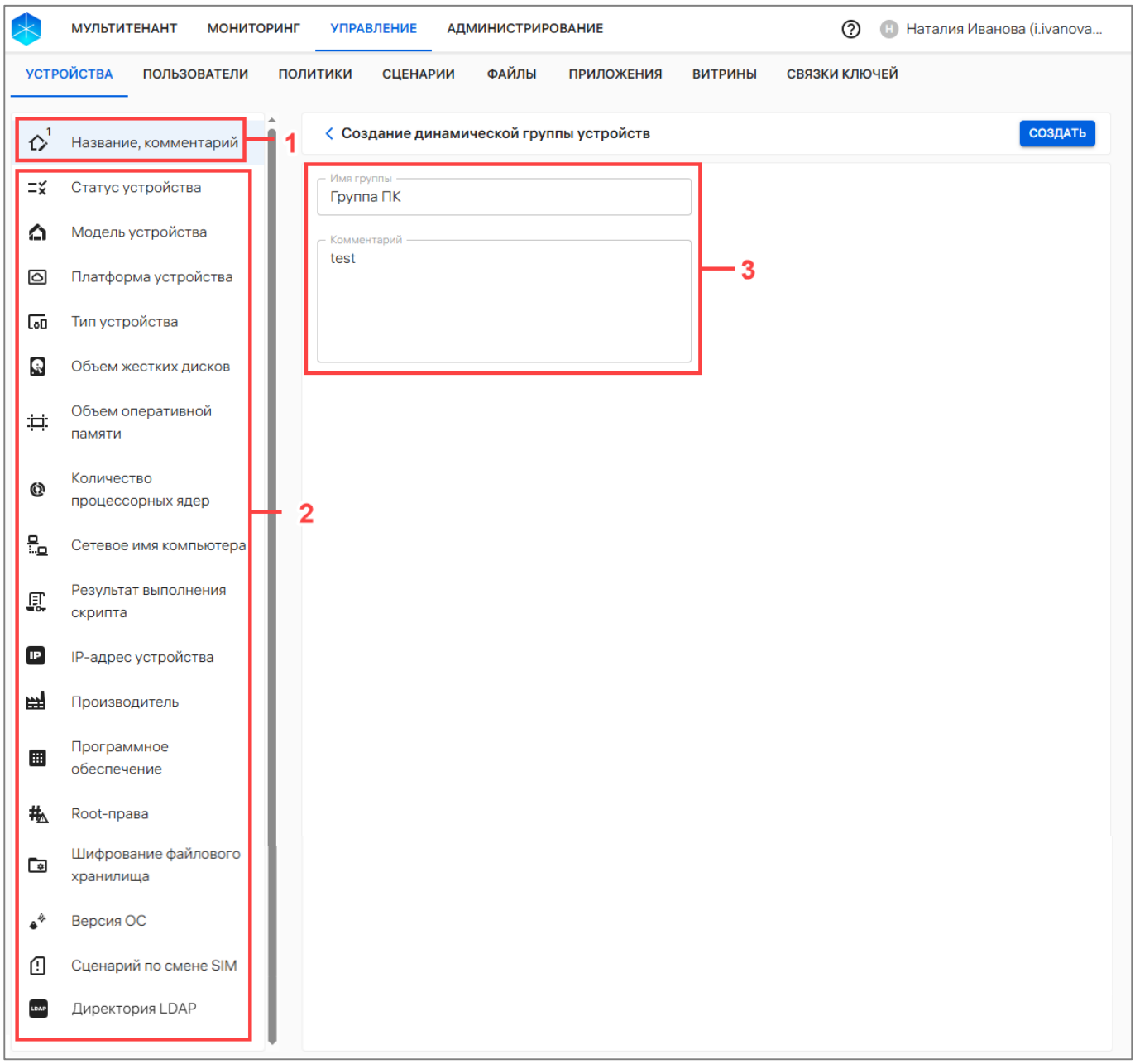

МУЛЬТИТЕНАНТ
МОНИТОРИНГ
УПРАВЛЕНИЕ
АДМИНИСТРИРОВАНИЕ
Наталия Иванова (i.ivanova...
УСТРОЙСТВА
ПОЛЬЗОВАТЕЛИ
ПОЛИТИКИ
СЦЕНАРИИ
ФАЙЛЫ
ПРИЛОЖЕНИЯ
ВИТРИНЫ
СВЯЗКИ КЛЮЧЕЙ
Название, комментарий
Статус устройства
Модель устройства
Платформа устройства
Тип устройства
Объем жестких дисков
Объем оперативной памяти
Количество процессорных ядер
Сетевое имя компьютера
Результат выполнения скрипта
IP-адрес устройства
Производитель
Программное обеспечение
Root-права
Шифрование файлового хранилища
Версия ОС
Сценарий по смене SIM
Директория LDAP
1
2
Создание динамической группы устройств
СОЗДАТЬ
Имя группы
Группа ПК
Комментарий
test
3

Рисунок 30

Таблица 32

Параметр	Значение
Статус устройства	Выбор значения из раскрывающегося списка: – «Активированные» – в динамическую группу будут автоматически попадать все активированные устройства; – «Не активированные» – в динамическую группу будут попадать все не активированные устройства
Модель устройства	Выбор модели устройства из раскрывающегося списка. Если нужной модели нет в списке, необходимо добавить ее (подробнее в п. 2.2.4)
Платформа устройства	Выбор значения из раскрывающегося списка: – «Аврора»; – «Android»; – «Linux»
Тип устройства	Выбор типа устройства из раскрывающегося списка: – «Планшет»; – «КПК»; – «ТСД»; – «POS-терминал»; – «Смартфон»; – «Неизвестный тип устройства»; – «ПК»
Объем жестких дисков. **ВНИМАНИЕ!** Данный параметр актуален для устройств ОС семейства Linux	Для ввода значений нажать кнопку «Диапазон». Указать объем жесткого диска устройств в формате: – «От» (МиБ); – «До» (МиБ). **ПРИМЕЧАНИЕ.** Верхняя граница «До» не включается в интервал.

Параметр	Значение
	При необходимости можно добавить еще один диапазон с другим интервалом, нажав на кнопку «Диапазон». При этом диапазоны в критерии не должны пересекаться. Для удаления диапазона нажать на значок «Удалить»
Объем оперативной памяти. **ВНИМАНИЕ!** Данный параметр актуален для устройств ОС семейства Linux	Для ввода значений нажать кнопку «Диапазон». Указать объем оперативной памяти устройств в формате: – «От» (МиБ); – «До» (МиБ). **ПРИМЕЧАНИЕ.** Верхняя граница «До» не включается в интервал. При необходимости можно добавить еще один диапазон с другим интервалом, нажав на кнопку «Диапазон». При этом диапазоны в критерии не должны пересекаться. Для удаления диапазона нажать на значок «Удалить»
Количество процессорных ядер. **ВНИМАНИЕ!** Данный параметр актуален для устройств ОС семейства Linux	Для ввода значений нажать кнопку «Диапазон». Указать количество процессорных ядер устройств в формате: – «От»; – «До». **ПРИМЕЧАНИЕ.** Верхняя граница «До» не включается в интервал. При необходимости можно добавить еще один диапазон с другим интервалом, нажав на кнопку «Диапазон». При этом диапазоны в критерии не должны пересекаться. Для удаления диапазона нажать на значок «Удалить»
Сетевое имя компьютера. **ВНИМАНИЕ!** Данный параметр актуален для устройств ОС семейства Linux	Ввести сетевое имя или маску сетевого имени компьютера, которое должно содержать хотя бы одну букву или цифру, и может включать буквы A-z, цифры 0-9, дефис (-), звездочки (*) и точки (.). Максимальная длина 253 символа, а длина от начала строки до первой точки не должна превышать 63 символа. Если необходимо ввести маску сетевого имени, необходимо ограничить ее звездочкой (*) в начале, внутри и/или в конце части сетевого имени. **ПРИМЕЧАНИЕ.** Возможно ввести несколько сетевых имен и/или масок сетевого имени компьютера

Параметр	Значение
Результат выполнения скрипта. **ВНИМАНИЕ!** Данный параметр актуален для устройств ОС Android и ОС семейства Linux	Для ввода значений нажать кнопку «Скрипт». Заполнить поля: – «Путь к скрипту» – ввести путь скрипта, который будет выполнен на устройстве после доставки; – «Результат выполнения скрипта» – ввести ожидаемый результат выполнения скрипта. Результат выполнения скрипта передается, если в файл скрипта была добавлена переменная `OMP_SCRIPT_RESULT_FILE`. Более подробная информация представлена в приложении (Приложение 3). При необходимости можно добавить еще один скрипт, выполнив шаги приведенные выше. Для удаления скрипта из критерия нажать на значок «Удалить»
IP-адрес устройства	Для ввода значений нажать кнопку «Диапазон». Указать интервал IP-адресов: – «Начальный адрес»; – «Конечный адрес». **ПРИМЕЧАНИЕ.** Конечный адрес не включается в интервал. При необходимости можно добавить еще один диапазон, нажав на кнопку «Диапазон». При этом диапазоны в критерии не должны пересекаться. Для удаления диапазона нажать на значок «Удалить»
Производитель	Названия производителя устройства. Ввод значения с клавиатуры. **ПРИМЕЧАНИЕ.** Возможно ввести несколько производителей
Программное обеспечение	**ПРИМЕЧАНИЯ:** ✓ Возможно создавать динамические группы с разными версиями одного приложения; ✓ Невозможно создать динамическую группу для того же приложения и версии «Любая», если динамическая группа с таким же приложением и с какой-либо версией уже создана (и наоборот).

	В раскрывающемся списке: – «Условие» – выбрать условие: • «Не применять условие» (по умолчанию). ПРИМЕЧАНИЕ. При создании динамической группы не используется поиск по наличию/отсутствию ПО; • «Установлено»; • «Не установлено»; – «Приложение» - выбрать приложение по коду приложения; – «Версия» – выбрать одну или несколько версий приложения. Значение «Любая», если версия приложения не имеет значения. При необходимости можно добавить диапазон версий, нажав кнопку «Диапазон версий» и задав интервал версий. При необходимости повторить шаг, чтобы добавить еще диапазон. Ввод нескольких диапазонов будет работать через логический оператор «ИЛИ». Диапазоны в критерии не должны пересекаться. Для удаления диапазона нажать на значок «Удалить». ВНИМАНИЕ! Для условия НЕ установленного ПО между версиями и диапазонами будет использоваться оператор «И», а не «ИЛИ» как для других условий и критериев. ПРИМЕЧАНИЯ: ✓ Можно создавать динамические группы с разными версиями/диапазонами версий одного приложения; ✓ Нельзя создать несколько динамических групп с одинаковыми значениями версий и/или диапазонов версий; ✓ Нельзя создать динамическую группу для того же приложения и версии «Любая», если динамическая группа с таким же приложением и с какой-либо версией/диапазоном версий уже создана (и наоборот), но если выбрать более одной версии и/или более одного диапазона версий, то группа будет создана, так как используется оператор OR (единый подход для всех критериев); ✓ Нельзя создать динамическую группу с пересечениями значений диапазонов и/или версий; ✓ В поля для ввода диапазона версий можно ввести только цифры и точки. При этом в итоговый список динамической группы попадут устройства с версиями, у которых основная часть (цифры и

Параметр	Значение
	точки) будет попадать в диапазон (например, если задать диапазон от 5.5, то в группу попадут устройства с версиями 5.5.2_arm, 5.5.2+1 и т.д.); ✓ Можно задать и версии, и диапазоны версий одновременно
Root-права	ПРИМЕЧАНИЕ. Проверка на наличие root-прав выполняется для устройств на базе ОС Android с периодичностью 1 раз в 1 час (или при запуске приложения «Аврора Центр»). Более подробная информация приведена в приложении (Приложение 5). Для устройств с другими ОС проверка неприменима. В раскрывающемся списке «Root-права» результат проверки устройства на наличие root-прав: – «Обнаружены» – в группу попадут устройства с ОС Android, у которых обнаружены root-права; – «Не обнаружены» - в группу попадут устройства с ОС Android, у которых не обнаружены root-права; – «Неизвестно» – в группу попадут устройства, у которых состояние root-прав неизвестно; – «Неприменимо» – в группу попадут устройства, для которых неприменима проверка на наличие root-прав (например, устройства с ОС Аврора или ОС семейства Linux)
Шифрование файлового хранилища	В раскрывающемся списке выбрать нужные значения (возможно выбрать более одного значения, выбор нескольких значений будет работать через логический оператор «ИЛИ»): – «Включено» – в динамическую группу будут попадать устройства, у которых в состоянии передается информация о том, что шифрование файлового хранилища включено; – «Выключено» – в динамическую группу будут попадать устройства, у которых в состоянии передается информация о том, что шифрование файлового хранилища выключено; – «Не поддерживается» – в динамическую группу будут попадать устройства, у которых в состоянии передается информация о том, что шифрование файлового хранилища не поддерживается

Параметр	Значение
Версия ОС	1) В раскрывающемся списке «Тип ОС» выбрать нужный тип ОС; 2) При необходимости: – в поле «Версия ОС» ввести значение и нажать «Enter» на клавиатуре. Можно ввести более одной версии. Ввод нескольких вариантов значений осуществляется посредством логического оператора «ИЛИ»; – нажать кнопку «Диапазон» и ввести диапазон версий ОС. При необходимости повторить шаг, чтобы добавить еще диапазон. Ввод нескольких вариантов значений осуществляется посредством логического оператора «ИЛИ». Диапазоны в критерии не должны пересекаться. Для удаления диапазона нажать на значок 🗑 «Удалить». **ПРИМЕЧАНИЯ:** ✓ Если выбран только тип ОС, то в динамическую группу попадут все устройства с выбранным типом ОС без учета версий; ✓ В поле для ввода версии ОС нельзя вводить кириллицу; ✓ В поля для ввода диапазона версий можно ввести только цифры и точки. При этом в итоговый список динамической группы попадут устройства с версиями, у которых основная часть (цифры и точки) будет попадать в диапазон (например, если задать диапазон от 5.5, то в группу попадут устройства с версиями 5.5.2_arm, 5.5.2+1 и т.д.); ✓ Можно задать и версии, и диапазон версий одновременно
Сценарий по смене SIM	В раскрывающемся списке «Сценарий по смене SIM» выбрать нужное значение: – «Сработал» – в динамическую группу попадут устройства, где зафиксировано событие смены SIM-карты, и офлайн-сценарий по смене SIM-карты сработал; – «Не сработал» – в динамическую группу попадут устройства, где событие не сработало (например, условия для срабатывания не выполнены); – «Не назначен» – в динамическую группу попадут устройства, на которые не назначен офлайн-сценарий по смене SIM-карты;

Параметр	Значение
	– «Не применимо» – в динамическую группу попадут устройства, не поддерживающие событие/механику смены SIM-карты. **ПРИМЕЧАНИЕ.** Устройство попадает в группу, когда начинает соответствовать выбранному статусу, например: – на устройство назначен офлайн-сценарий по смене SIM-карты (подробнее в п. 2.5.1); – произошла смена доверенной SIM-карты на несанкционированную (подробнее в приложении (Приложение 7); – приложение «Аврора Центр», установленное на устройстве, зафиксировало событие и передало информацию на сервер; – на сервере статус становится «Сработал». Устройство исключается из группы, когда перестает соответствовать условию. Например, для группы со значением «Сработал»: если после срабатывания вернули доверенную SIM-карту обратно, то устройство должно выйти из группы
Директория LDAP	В раскрывающемся списке «Директория LDAP» выбрать нужное значение. Существующие директории отображаются в соответствии с заданными настройками интеграции LDAP (подробнее в пп. 4.1.5.3.1 и пп. 4.1.5.3.2). **ПРИМЕЧАНИЯ:** ✓ В группу будут попадать только те устройства, которые были импортированы из выбранной директории; ✓ При удалении выбранной директории в настройках интеграции с LDAP, ранее добавленные устройства будут исключены из группы. **ВНИМАНИЕ!** Не рекомендуется назначать на динамические группы устройств политики с правилами, которые могут изменить состояние устройств, если по изменяемым значениям состояния формируется динамическая группа. Это может привести к нестабильному состоянию устройств из-за зацикливания применения политик в результате привязки или отвязки устройств от динамической группы

2.2.2.2.1. Редактирование динамической группы устройств

Для изменения названия и/или комментария к динамической группе устройств, а также изменения ее критериев необходимо:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы устройств для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок «Редактировать» и при необходимости в разделе «Название, комментарий» внести изменения в полях, приведенных в таблице (см. Таблица 31);

– в области фильтров выбрать раздел с критерием, по которому устройства будут добавляться в динамическую группу, и задать/изменить его значения согласно таблице (см. Таблица 32). Для применения изменений в составе группы необходимо внести уточнение как минимум в один из установленных критериев;

– нажать кнопку «Сохранить».

В результате изменения динамической группы будут применены. При изменении критериев состав группы устройств будет обновлен.

2.2.3. Добавление устройств или группы устройств с помощью CSV-файла

Добавление и обновление устройств или групп устройств, а также привязка устройств к группе в Консоли администратора ПУ, может выполняться с помощью подготовленного шаблона импорта устройств, который предоставляется в виде CSV-файла.

2.2.3.1. Шаблон CSV-файла

CSV-файл возможно создать вручную или скачать и заполнить шаблон.

Для загрузки шаблона CSV-файла необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить из CSV» (см. Рисунок 29);

– в открывшемся окне нажать «Шаблон .CSV» (Рисунок 31), в результате шаблон файла для импорта будет выгружен на ЭВМ. Требования к заполнению CSV-файлов приведены в таблице (Таблица 33).

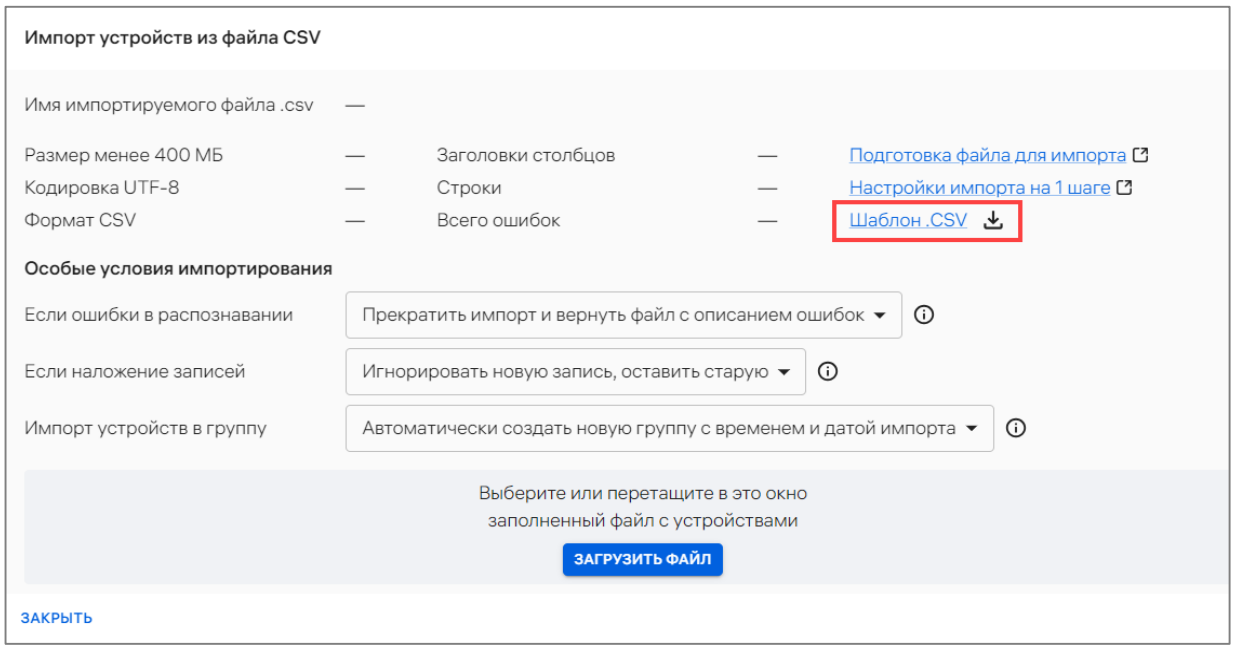


Рисунок 31

Пример заполненного CSV-файла:

```
GROUP,IMEI,IMEI,SN,ETHERNET_MAC,WLAN_MAC,MODEL_CODE,PLATFORM,COMMENT,STRATEGY
Группа 1,352132035783492,,6abcdg1,,,MIG C55,AURORA,Комментарий 1
Группа 2,350408012241197,,4gghdb6,,,MIG C55,AURORA,Комментарий 2
```

Также возможно заполнить CSV-файл в табличном виде (Рисунок 32).

Пример:

GROUP	IMEI	IMEI	SN	ETHERNET_MAC	WLAN_MAC	MODEL_CODE	PLATFORM	COMMENT	STRATEGY
Группа 1	352132035783492		6abcdg1			MIG C55	AURORA	Комментарий 1	
Группа 2	350408012241197		4gghdb6			MIG C55	AURORA	Комментарий 2	

Рисунок 32

ПРИМЕЧАНИЕ. При больших значениях чисел (например, IMEI) необходимо выбрать числовой формат ячейки и количество десятичных знаков, равное 0.

Файл для импорта должен соответствовать следующим требованиям:

– размер файла не должен превышать 400 МБ. Для импорта файлов большего размера рекомендуемая скорость подключения к сети Интернет 100 Мбит/сек и выше. Если скорость подключения к сети Интернет менее 100 Мбит/сек, рекомендуется разделить файл на несколько частей и загружать их поочередно;

– формат файла – `.csv`;

– кодировка файла – UTF-8.

ПРИМЕЧАНИЕ. Скачанный шаблон CSV-файла имеет нужный формат и кодировку;

– первая строка файла должна содержать названия полей с разделителем (например, " GROUP,IMEI,IMEI,SN,ETHERNET_MAC,WLAN_MAC,MODEL_CODE,PLATFORM,COMMENT,STRATEGY").

ПРИМЕЧАНИЕ. После столбца COMMENT может быть добавлен необязательный столбец STRATEGY. Он заполняется если необходимо указать стратегию для конкретной строки (пп. 2.2.3.2). Стратегия в строке может отличаться от основной выбранной и будет являться приоритетной.

Разделитель для всех полей файла определяется по первой строке. В качестве разделителей может использоваться любой символ, кроме: \r, \n и символа замены Unicode (0xFFFD). Если в качестве разделителя используются буквы, то они должны заключаться в кавычки, например: «a».

Описание требований к значениям параметров приведены в таблице (Таблица 33).

Таблица 33

Параметр	Описание	Примечание
GROUP	Название группы устройств. Содержит от 2 до 64 символов	Параметр обязателен для заполнения, при: – создании группы устройств; – привязке устройств к группе
IMEI	Международный идентификатор мобильного оборудования. Должен содержать 15 цифр	Допустимо использовать не более 10 таких параметров. Параметр обязателен для заполнения, если не заполнены другие идентификаторы
SN	Серийный номер, который присвоен устройству производителем. Содержит от 1 до 20 символов	Допустимо использовать только 1 такой параметр. Параметр обязателен для заполнения, если не заполнены другие идентификаторы
ETHERNET_MAC	MAC-адрес Ethernet устройства. Содержит 6 пар символов, разделенных двоеточием	Допустимо использовать не более 10 таких параметров. Параметр обязателен для заполнения, если не заполнены другие идентификаторы
WLAN_MAC	MAC-адрес WLAN устройства. Содержит 6 пар символов, разделенных двоеточием, например: «00:aa:00:00:a0:00»	Допустимо использовать не более 10 таких параметров. Параметр обязателен для заполнения, если не заполнены другие идентификаторы
MODEL_CODE	Модель устройства. Содержит до 255 символов. Код нужной модели можно посмотреть в списке моделей устройств в столбце «Код	Параметр не обязателен для заполнения

Параметр	Описание	Примечание
	модели» (подробнее в подразделе 2.2)	
PLATFORM	ОС устройства. Доступные значения: – AURORA; – ANDROID; – LINUX	Параметр обязателен для заполнения
COMMENT	Дополнительная информация к устройству. Содержит до 512 символов	Параметр не обязателен для заполнения
STRATEGY	Правило разрешения конфликтующих записей. Доступные значения: – **SKIP** или **S** – в результате конфликтующая запись не будет перезаписана. Если файл содержит несколько одинаковых записей об устройстве, но с разными группами, то будут созданы все связи устройств с группами из файла; – **REPLACE** или **R** – в результате конфликтующая запись будет перезаписана. Если файл содержит несколько одинаковых записей об устройствах, но с разными группами, то устройство будет отвязано от всех групп, в которых оно состояло ранее в системе и привязано ко всем группам из файла	Параметр не обязателен для заполнения. Параметр имеет приоритет по сравнению с правилом разрешения конфликтов, выбранным в окне настройки импорта

2.2.3.2. Добавление устройства или группы устройств с помощью CSV-файла

Для импорта устройств, их группы и связи с группами в Консоли администратора ПУ необходимо выполнить следующие действия:

– подготовить CSV-файл для импорта (пп. 2.2.3.1);
– перейти в подраздел «Устройства» раздела «Управление»;
– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить из CSV» (см. Рисунок 29);

– в открывшемся окне задать особые условия импорта, приведенные в таблице (Таблица 34);

Таблица 34

Наименование полей	Описание	Примечание
Если ошибки в распознавании	Выбор правила импортирования (если CSV-файл будет содержать ошибки) из раскрывающегося списка (Рисунок 33 [1]): – **Прекратить импорт и вернуть файл с описанием ошибок** – при обнаружении ошибок будет остановлен импорт и сформирован файл с перечислением некорректных строк и указанием причин ошибок; – **Продолжить импорт и вернуть два файла с ошибками и без** – импорт продолжится с корректными записями, и после его завершения будут сформированы 2 файла: • файл с перечислением некорректных строк и указанием причин ошибок; • файл с указанием успешно импортированных устройств	В поле содержится подсказка, доступная для просмотра нажатием значка ⓘ. В результате отобразится текст подсказки следующего содержания: «При завершении импорта система предоставит 2 файла: список системных сообщений об ошибках распознавания и Журнал успешно импортированных устройств»
Если наложение записей	Выбор правила разрешения конфликтов при импорте из раскрывающегося списка (Рисунок 33 [2]): – **Игнорировать новую запись, оставить старую** – в результате конфликтующие записи не будут перезаписаны. Если файл содержит несколько одинаковых записей об устройствах, но с разными группами, то будут созданы все связи устройств с группами из файла; – **Перезаписывать новую строку поверх прежней** – в результате конфликтующие записи будут перезаписаны. Если файл содержит несколько одинаковых записей об	

Наименование полей	Описание	Примечание
	устройстве, но с разными группами, то устройство будет отвязано от всех групп, в которых оно состояло, и привязано ко всем группам из файла. **ПРИМЕЧАНИЕ.** Если в CSV-файле заполнен столбец «STRATEGY», правило разрешения конфликтов из этого столбца будет иметь приоритет над указанным правилом при настройке импорта. Процесс заполнения CSV-файла приведен в пп. 2.2.3.1	
Импорт устройств в группу	Выбор правила добавления импортируемых устройств в группы из раскрывающегося списка (Рисунок 33 [3]): – **Автоматически создать новую группу с временем и датой импорта** – в результате будет создана новая группа устройств (с типом «Группа устройств»), в которую будут включены все импортируемые устройства. Если в CSV-файле указана группа (значение в столбце «GROUP»), то такое устройство будет включено в новую группу и в указанную в файле группу; – **Не создавать группу** – в результате устройства будут добавлены только в группы, указанные в CSV-файле; – **Выбрать группу из имеющихся** – требуется выбрать из раскрывающегося списка группу, в которую необходимо включить устройство. Если в CSV-файле указана группа (значение в столбце «GROUP»), то устройство будет включено как в группу, указанную в файле, так и в группу, выбранную на этом шаге	В поле содержится подсказка, доступная для просмотра нажатием значка ⓘ. В результате отобразится текст подсказки следующего содержания: «В процессе импорта система может помещать все устройства в одну из имеющихся групп или создать новую»

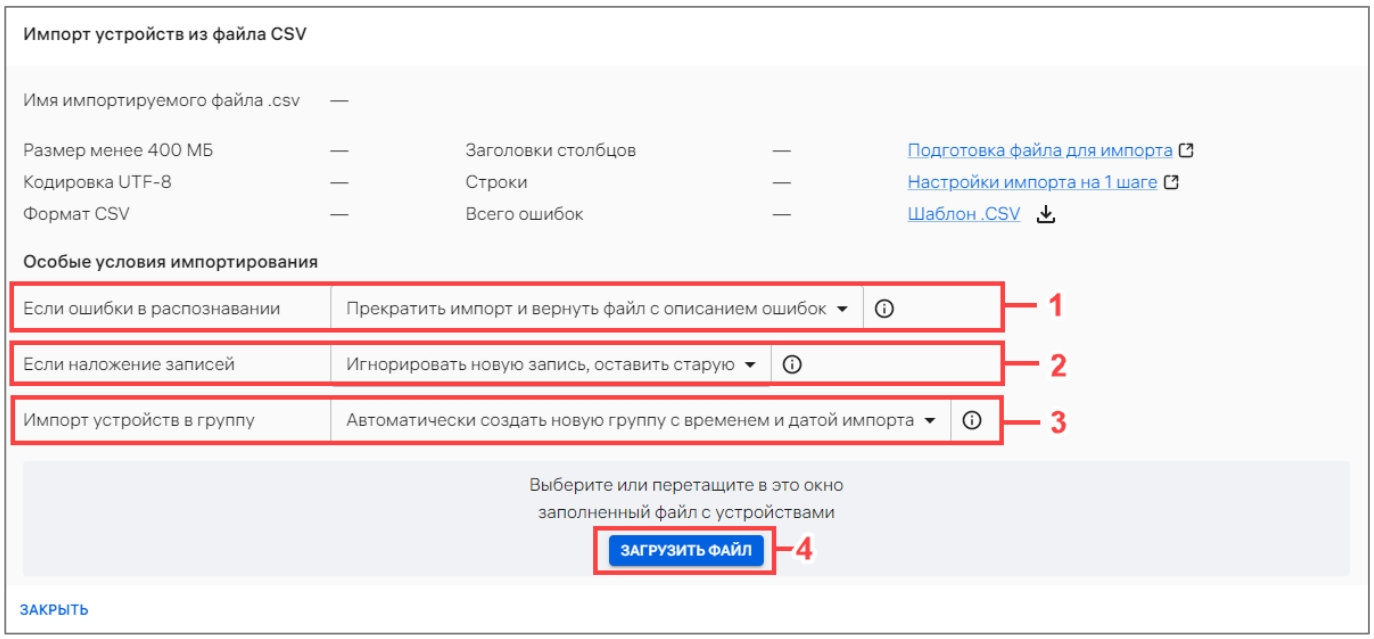


Рисунок 33

– далее необходимо загрузить CSV-файл одним из способов:
  - переместить CSV-файл в область загрузки;
  - нажать кнопку «Загрузить файл» (см. Рисунок 33 [4]) с последующим выбором файла для импорта;

– в результате будет запущен импорт устройств из CSV-файла и отобразится шкала загрузки импорта.

Если заполненный файл был загружен корректно или файл содержал ошибки, но при этом в особых условиях импортирования была выбрана опция «Продолжить импорт и вернуть 2 файла с ошибками и без», импорт будет завершен. В окне с результатами импорта шкала загрузки импорта будет заполнена до конца (Рисунок 34).

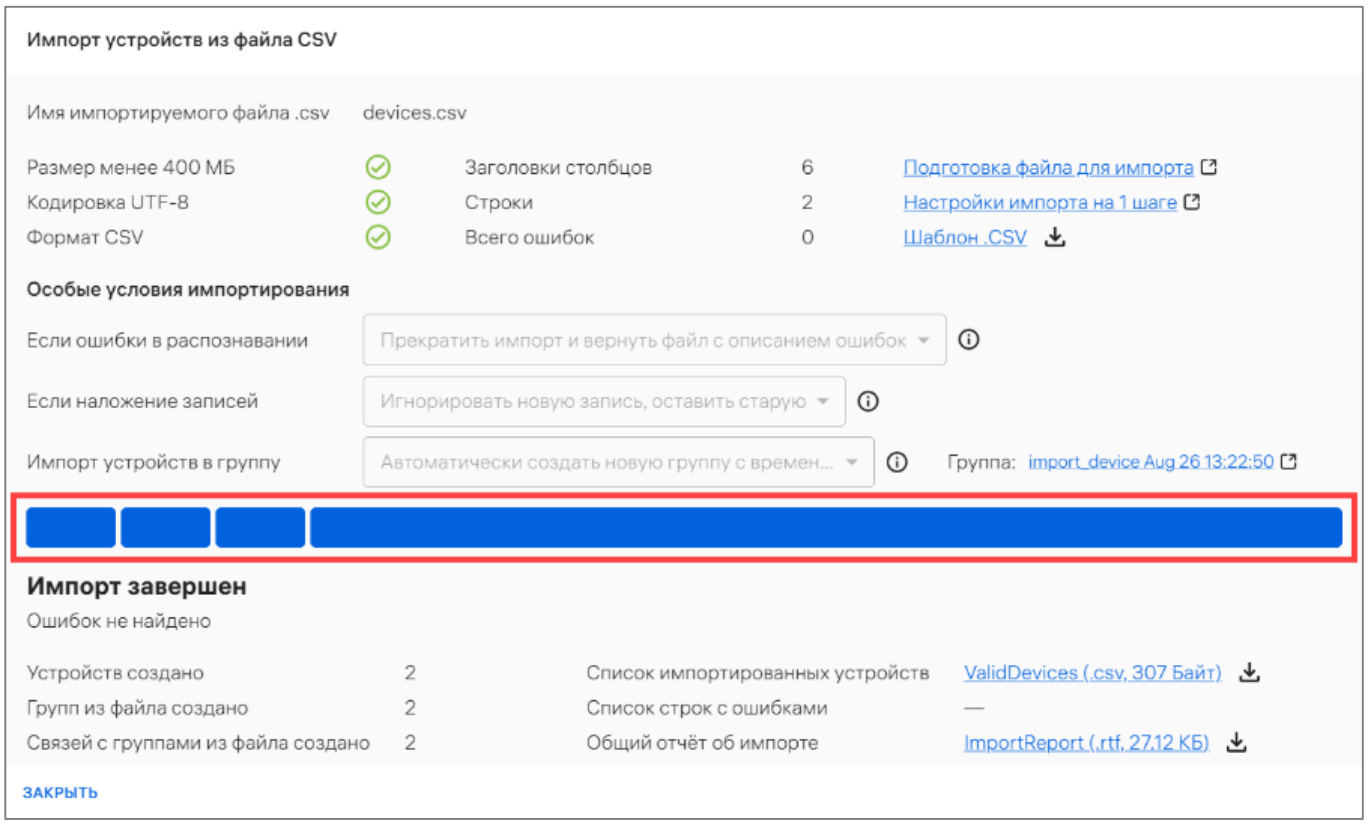


Рисунок 34

Если заполненный файл был загружен некорректно и при этом в особых условиях импортирования была выбрана опция «Прекратить импорт и вернуть файл с описанием ошибок», импорт будет остановлен. В окне с результатами импорта шкала загрузки импорта устройств будет прервана на этапе, где были обнаружены ошибки (Рисунок 35 [6]).

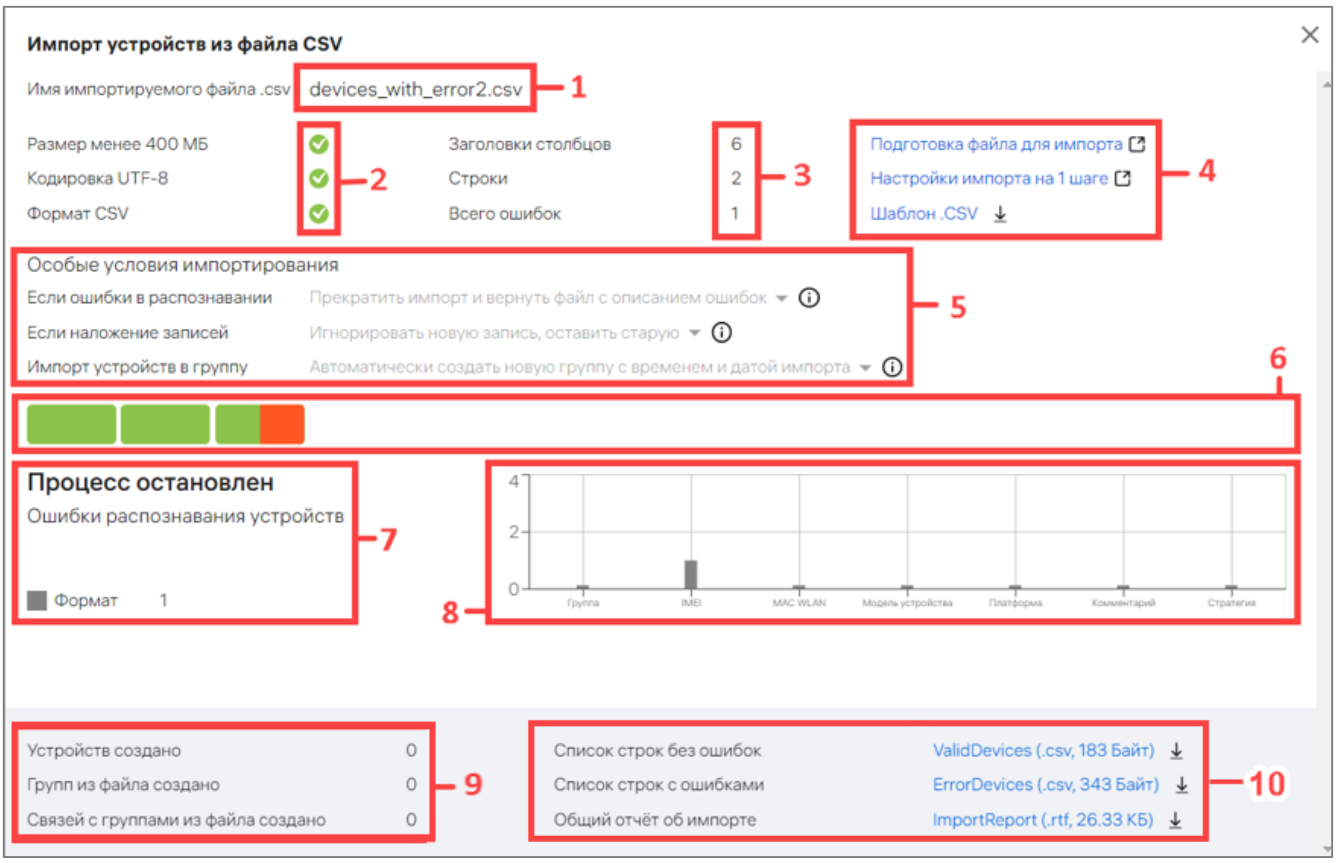


Рисунок 35

В окне с результатами импорта устройств отображается следующая информация:

– название импортируемого файла (см. Рисунок 35 [1]);

– соответствие импортируемого файла размеру, кодировке и формату (см. Рисунок 35 [2]);

– количество столбцов всех импортируемых строк и ошибок в файле (Рисунок 35 [3]);

– ссылки (см. Рисунок 35 [4]):

• **Подготовка файла для импорта**, при нажатии на которую произойдет переход на статью справки, описывающую требования и процесс подготовки CSV-файла для импорта устройств;

• **Настройки импорта на 1 шаге**, при нажатии на которую произойдет переход на статью справки, описывающую шаги импорта;

• **Шаблон .CSV**, при нажатии на которую произойдет скачивание шаблона CSV-файла для импорта устройств;

– особые условия импортирования (см. Рисунок 35 [5], см. Таблица 34);

– шкала прогресса импорта (см. Рисунок 35 [6]);

– сообщение о завершении импорта или прерывании процесса из-за ошибок (см. Рисунок 35 [7]);

– графическое распределение ошибок по столбцам параметров импорта (при обнаружении ошибок) (см. Рисунок 35 [8]);

– количество добавленных устройств, групп устройств и их связей (см. Рисунок 35 [9]);

– ссылки на скачивание отчетов (см. Рисунок 35 [10]):

- отчет со списком импортированных устройств. Формат отчета – `.csv`;
- отчет со списком ошибок, описание которых приведено в подразделе 5.2. Формат отчета – `.csv` (при отсутствии ошибок в импортированном файле данный отчет не будет сформирован);
- отчет с общей информацией об импорте. Формат отчета – `.rtf`.

Отследить процесс выполнения импорта также возможно в окне «Процессы» подраздела «Индикаторы» раздела «Мониторинг». Более подробная информация приведена в подразделе 3.

Для повторной загрузки CSV-файла необходимо нажать кнопку «К началу загрузки».

2.2.4. Добавление модели устройства

Для добавления модели устройства необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– нажать кнопку «Модели устройств» (см. Рисунок 28 [3]);

– в открывшемся окне нажать кнопку «Добавить модель» и заполнить поля, приведенные в таблице (Таблица 35);

Таблица 35

Параметр	Описание
Название	Наименование производителя и модель для отображения в ПУ (например, Kozen P10). Может содержать от 1 до 255 символов. Поле обязательно для заполнения
Тип устройства	Выбор значения из раскрывающегося списка: – «Планшет»; – «Смартфон»; – «КПК»; – «ПК»; – «ТСД»; – «POS-терминал»; – «Неизвестно». Поле обязательно для заполнения
Модель	Техническое название модели устройства (строго в том виде, как оно отображается на самом устройстве, например в разделе «Об устройстве»/«О телефоне»). Может содержать от 1 до 255 символов. Поле обязательно для заполнения
Комментарий	Ввод значения с клавиатуры. Максимальная длина до 512 символов. Поле не является обязательным для заполнения

При сохранении данных система проверяет уникальность полей «Название» и «Модель» среди уже существующих моделей. В случае обнаружения дубликатов система выдаст соответствующее уведомление, в результате чего создание модели будет прервано.

После успешного сохранения новая модель появится в списке и станет доступна в фильтрах и критериях динамических групп.

2.2.4.1. Редактировании модели устройства

При редактировании данных модели устройства необходимо:

– выбрать название модели устройства в списке;

– в открывшемся окне при необходимости внести изменения в полях, согласно таблице (см. Таблица 35);

– подтвердить или отменить действия.

ПРИМЕЧАНИЕ. При сохранении система проверяет:

– уникальность полей «Название» и «Модель»;

– при изменении в поле «Тип устройства» – не используется ли данная модель в динамической группе по критерию «Тип устройств». Если модель включена в динамическую группу, система не даст сохранить изменения и отобразится сообщение об ошибке.

ВНИМАНИЕ! Код модели при редактировании поля «Название» не меняется – это системный идентификатор.

После успешного сохранения обновленные данные отображаются в списке моделей и доступны для применения в фильтрах и динамических группах.

2.2.4.2. Скрытие/отображение модели устройства

Функционал скрытия модели устройств предусматривает возможность исключения отображения моделей устройств в интерфейсе ППО без удаления соответствующих записей из базы данных.

Скрытая модель будет недоступна для выбора:

– в фильтре «По модели» в списке устройств;

– в окне добавления/редактирования устройства;

– в критерии «Модель устройства» динамических групп.

Чтобы скрыть или отобразить модель устройства необходимо:

– выбрать необходимую модель устройства в списке, установив галочку в чекбоксе для доступа к списку быстрых действий.

ПРИМЕЧАНИЕ. За раз доступно скрыть/отобразить только одну модель устройства;

– для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок:

-  «Отобразить модель устройства», чтобы снова сделать модель доступной для выбора;
-  «Скрыть модель устройства» – скрыть модель из всех списков выбора.

Ограничения и поведение:

1) При выборе более одной модели кнопка скрытия/отображения становится неактивной;

2) После скрытия:

– строка модели в списке будет отображаться серым цветом и недоступна для редактирования;

– модель исчезает из списков выбора в фильтрах и критерии для создания динамической группы «Модель устройства».

2.2.5. Приглашения на самостоятельную регистрацию устройства

2.2.5.1. Добавление приглашения на самостоятельную регистрацию устройства

Для добавления приглашения на самостоятельную регистрацию устройства необходимо перейти в подраздел «Устройства» раздела «Управление» и выполнить одно из следующих действий:

1) Нажать кнопку «Добавить», в раскрывающемся списке выбрать пункт «Добавить приглашение» (см. Рисунок 29);

2) Перейти в список приглашений, нажав на кнопку «Приглашения» (Рисунок 36), и на отобразившейся странице нажать на кнопку «Добавить приглашение».

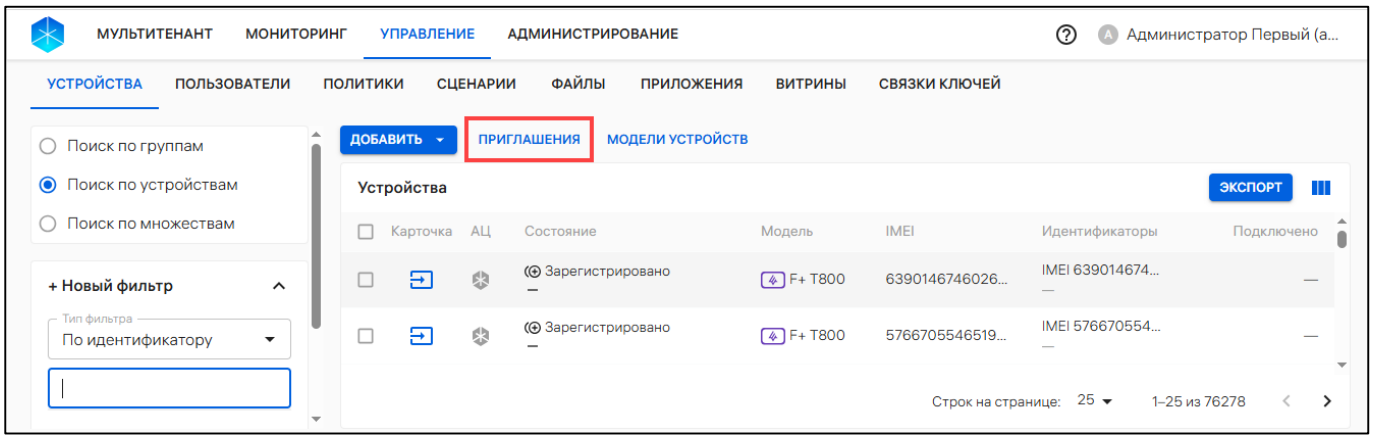


Рисунок 36

В результате в отобразившемся окне необходимо заполнить поля:

– «Название». Ввод значения с клавиатуры. Может содержать от 1 до 50 символов;

– «Лимит переиспользований в сутки». Ввести максимальное количество переиспользований приглашения для повторной активации устройства в сутки. Количество переиспользований считается для одного устройства и если оно превысит заданный лимит, то повторная активация устройства с помощью приглашения в текущие сутки не сработает. На следующие сутки счетчик переактиваций для устройства сбрасывается. Лимит может быть от 0 до 1000000. В случае 0 использовать приглашение для повторной активации устройства будет нельзя;

– если требуется отправлять на рассмотрение устройства из сетей, не входящих в список доверенных, необходимо перевести переключатель «Использовать доверенные сети» в положение «Включено». По ссылке «Подробнее» доступен переход в статью справки.

ПРИМЕЧАНИЕ. Для ОС Android в приглашении на самостоятельную регистрацию устройств возможно дополнительно указать:

1) Сеть WLAN, к которой устройство автоматически подключится в процессе самостоятельной регистрации. Для этого необходимо:

– перевести переключатель «Включить настройки WLAN» в положение «Включен»;

– в поле «Название сети (SSID)» ввести название беспроводной сети (Service Set Identifier) для подключения. Параметр обязателен для заполнения;

– с помощью переключателя «Скрытая сеть» указать транслируется ли название сети WLAN. Переключатель по умолчанию выключен;

– в раскрывающемся списке «Безопасность» необходимо выбрать технологию безопасности сети WLAN:

- WEP (выбрано по умолчанию);
- WPA;

– в поле «Пароль» ввести пароль сети WLAN. Параметр обязателен для заполнения;

2) Часовой пояс, который автоматически будет установлен на устройстве в процессе самостоятельной регистрации. Для этого необходимо:

– перевести переключатель «Настройки часового пояса» в положение «Включен»;

– в раскрывающемся списке «Часовой пояс» выбрать нужный часовой пояс. По умолчанию выбран часовой пояс Москва (GMT+03:00);

3) При необходимости возможно указать статические группы (максимум 5 групп), в которые устройства будут автоматически попадать сразу после активации по приглашению. Для этого необходимо:

– перевести переключатель «Добавление устройства в статические группы» в положение «Включено»;

– выбрать в раскрывающемся списке нужную группу. При необходимости воспользоваться фильтром по названию групп. Если необходимой группы нет в списке, ввести название новой группы в поле «Фильтр по названию группы» и нажать «Создать статическую группу».

ПРИМЕЧАНИЯ:

✓ Если активированное устройство отсканирует QR-код приглашения (или использует JSON-файл), то произойдет добавление устройства в группы, привязанные к приглашению. На данный момент при повторной активации устройства по QR-коду или JSON-файлу (которым оно было активировано ранее) с лимитом переиспользований в сутки 0 при ручном подтверждении устройство будет активировано, но не добавлено в группы;

✓ При удалении группы возможно посмотреть, в каких приглашениях она используется.

После выполнения указанных действий необходимо подтвердить или отменить действие.

Если приглашение успешно создано, отобразится карточка приглашения, на которой будут отображены:

– лимит переиспользований приглашения в сутки (Рисунок 37 [1]);

– использование доверенных сетей (Рисунок 37 [2]);

– название статических групп, в которые устройства будут автоматически попадать после активации по приглашению (Рисунок 37 [3]);

– QR-код (Рисунок 37 [4]), который необходимо отсканировать на устройстве с ОС Аврора/ОС Android для дальнейшей самостоятельной регистрации устройства (также доступно скачивание QR-кода при нажатии на значок при наведении на него курсора);

– кнопка «Скачать JSON» (Рисунок 37 [5]), при нажатии на которую будет скачен JSON-файл для дальнейшего размещения его на устройство для самостоятельной регистрации в ПУ (пп. 2.2.1.2).

ВНИМАНИЕ! При настройке ППО по умолчанию QR-код (и JSON-файл) приглашения генерируется на 60 дней. Настройку срока действия можно изменить в конфигурационном файле ППО: файл `/var/ocs/config/subsystems/auth/config.yml` параметр `ttl.capability_access_token`;

– при переходе со страницы приглашения отобразится предупреждающее сообщение, где необходимо подтвердить или отменить действие.

ПРИМЕЧАНИЕ. Необходимо убедиться, что QR-код или JSON-файл для саморегистрации устройства сохранен.

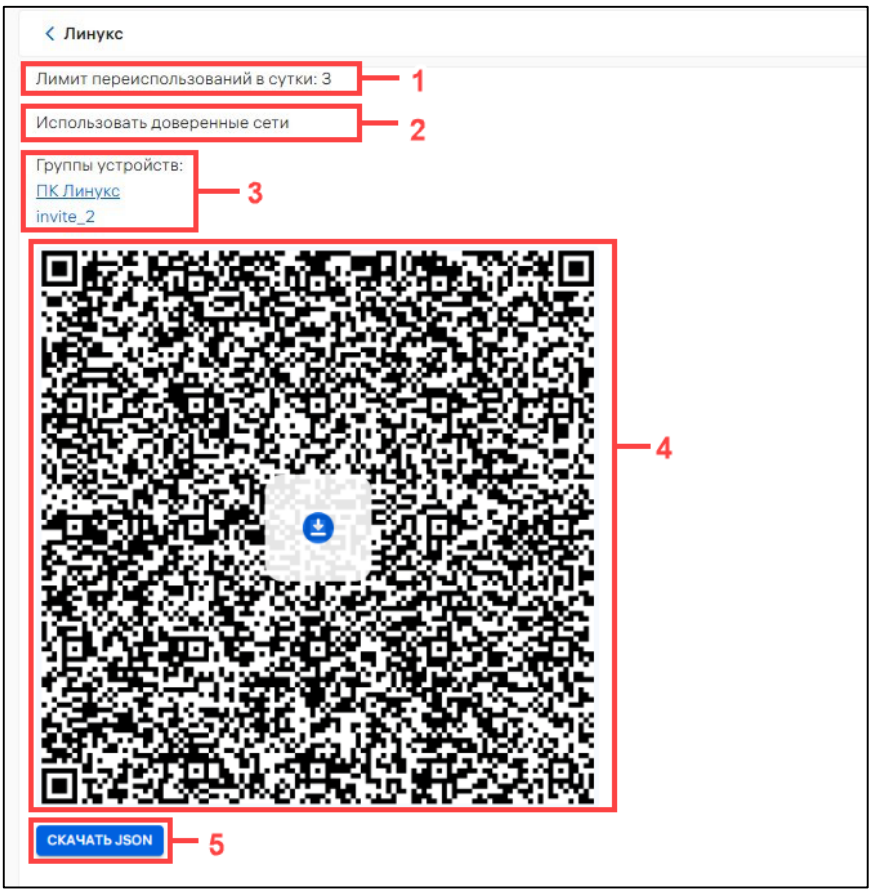


Рисунок 37

Приглашение имеет название `invite.json`.

Пример содержания JSON-файла:

{"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":{"accessToken":"CbSkUFQITgLiYIquSbqIgGuFXv1Hx2afHdBwQTNzstY.HezBPMQuVHb5UuAenMhS_wd3CGbc-wmnfuKM4MZIE30","inviteTakeupURL":"http://ocs-dev.ompcloud.ru/emm/mobile/api/deviceInvites/505381a3da794102b3a000da1c5df557/takeUp","trustedCerts":""},"android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":"http://ocs-dev.ompcloud.ru/emm/mobile/clientDownload","android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":"ru.omp.services/ru.omp.services.AdminReceiver","android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED":true,"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"bZ41Av7s6nrQpXjB2Pg5oKfKL5xPxhLevsESkkVLfg4","aurora.app.extra.PROVISIONING_DEVICE_ADMIN_APP_ID":"ru.omp.ac.uem"}

ВНИМАНИЕ!

✓ Пример приведен для ознакомления со структурой JSON-файла и может отличаться;

✓ Не рекомендуется изменять название и форматировать сгененированный JSON-файл (добавлять пробелы, табуляцию, переносы строк), так как это может привести к ошибкам при обработке JSON- файла в процессе добавления и активации устройств по приглашению.

Каждый параметр сопровождается двоеточием, пары ключ-значение разделяются запятой. Описание параметров из примера:

– **accessToken** – токен доступа;

– **inviteTakeURL** – URL, по которому устройство перейдет для начала процесса самостоятельной регистрации;

– **trustedCerts** – список цифровых отпечатков (`fingerprint`) корневых сертификатов для активации устройств, перечисленные через запятую;

– **android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME** – название компонента;

– **android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION** – ссылка на скачивание файла для установки приложения «Аврора Центр»;

– **android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM**– контрольная сумма подписи файла для установки приложения «Аврора Центр»;

– **android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED** – параметр, определяющий, включать ли полную установку системных приложений в процессе установки первоначальной настройки устройства с установкой приложения «Аврора Центр». По умолчанию установка всех системных приложений включена;

– **android.app.extra.PROVISIONING_WIFI_SSID** – название сети WLAN, к которой устройство автоматически подключится в процессе самостоятельной регистрации;

– **android.app.extra.PROVISIONING_WIFI_PASSWORD** – пароль сети WLAN, к которой устройство автоматически подключится в процессе самостоятельной регистрации;

– **android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE** – технология безопасности сети WLAN, к которой устройство автоматически подключится в процессе самостоятельной регистрации;

– **android.app.extra.PROVISIONING_WIFI_HIDDEN** – параметр, определяющий транслируется ли название сети WLAN, к которой устройство автоматически подключится в процессе самостоятельной регистрации;

– **android.app.extra.PROVISIONING_TIME_ZONE** – часовой пояс, который автоматически будет установлен на устройстве в процессе самостоятельной регистрации;

– **aurora.app.extra.PROVISIONING_DEVICE_ADMIN_APP_ID** – имя приложения на устройстве с ОС Аврора, в которое будут переданы активационные данные из QR-кода.

При выходе из карточки приглашения осуществится переход на страницу со списком приглашений в подразделе «Приглашения», на которой доступно отозвать созданное приглашение, нажав на значок ⊘ «Отозвать», а также возможно просмотреть информацию о каждом приглашении, которая отображается в следующих столбцах:

– «Название» – название приглашения;

– «Лимит» – лимит переиспользований приглашения в сутки;

– «Довер.сети» – использование доверенных для проверки IP-адреса устройства. Возможные значения:

- «Используются»;
- «Не используются»;

– «Группы» - группы, в которые будут включены устройства после успешного использования приглашения;

– «Статус» – статус активности приглашения. Возможные значения:

- «Активно»;
- «Отозвано»;

– «Создано» - дата создания приглашения;

– «Действует до» – дата, до которой действует токен доступа, соответствующий приглашению.

Список приглашений отсортирован по значениям столбца «Создано» в порядке убывания.

2.2.5.2. Заявки на активацию по приглашению

Для просмотра списка заявок на активацию устройств по приглашению необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– нажать на кнопку «Приглашения» (см. Рисунок 36);

– перейти в раздел «Заявки на активацию» (Рисунок 38 [1]);

– в рабочей области отобразится список заявок на активацию (Рисунок 38 [3]). Информация о заявках отображается в столбцах, приведенных в таблице (Таблица 36), и отсортирована по значениям столбца «Дата создания» в порядке убывания.

ПРИМЕЧАНИЕ. По умолчанию список заявок на активацию отображается в статусе «Требует согласования» (Рисунок 38 [2]). Для отображения списка заявок на активацию во всех статусах, нажать кнопку «Сбросить все». Далее в раскрывающемся списке «Тип фильтра» выбрать «Статус заявки» и выбрать нужный статус:

– «Требует согласования»;

– «Согласована»;

– «Отклонена».

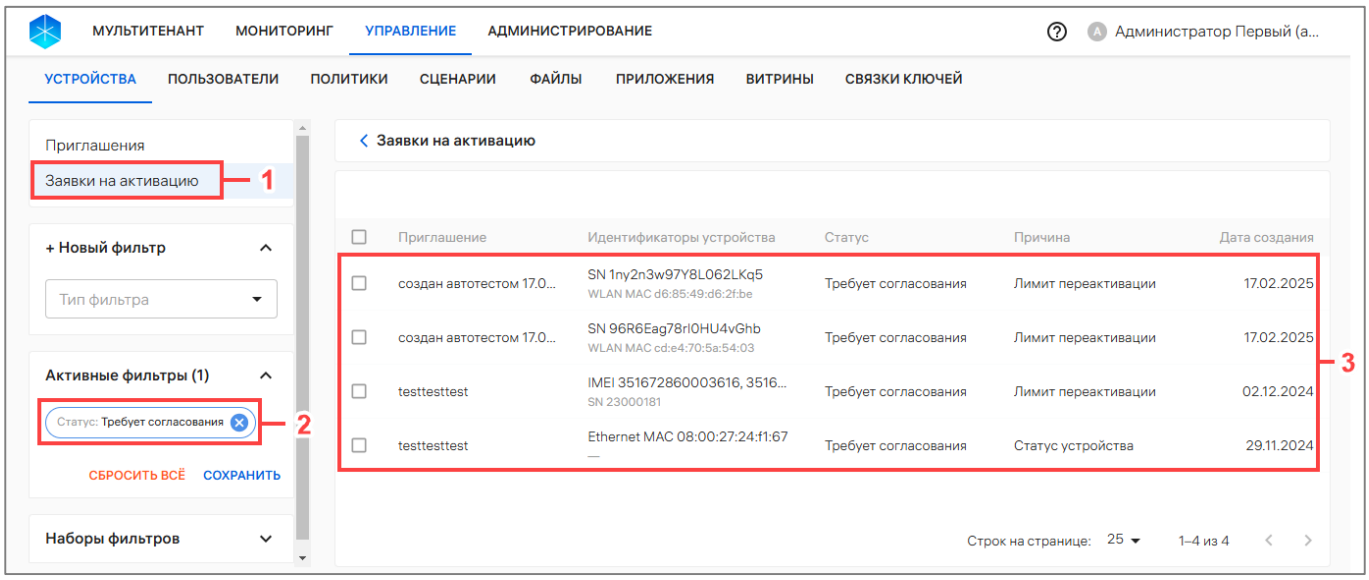


Рисунок 38

Таблица 36

Название столбца	Описание
Приглашение	Название приглашения
Идентификаторы устройства	Отображаются два имеющихся идентификатора устройства по приоритетам, выставленным в настройках администрирования ПУ (подробнее в п. 4.1.3)
Статус	Статус заявки на активацию. Возможные значения: – «Требует согласования»; – «Согласована»; – «Отклонена»; – «Выполнена»
Причина	Статус создания заявки. Возможные значения: – «Лимит переактивации»; – «Доверенная сеть». Дополнительно отображается IPv4-адрес, который передало устройство при использовании приглашения. **ПРИМЕЧАНИЕ.** Содержит значение, определяемое инфраструктурой, поэтому при неверной настройке инфраструктуры может содержать произвольное значение; – «Статус устройства»; – «Вручную»
Дата создания	Дата создания заявки на активацию

Чтобы согласовать или отклонить заявки на активацию по приглашению, необходимо:

– выбрать нужную заявку в списке, установив галочку в чекбоксе для доступа к списку быстрых действий. Для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок:

- «Согласовать» - для согласования заявки.

ПРИМЕЧАНИЕ. Для заявок с причиной «Пересечение идентификаторов» кнопка «Согласовать» недоступна. Для таких заявок необходимо выполнить разрешение конфликтов (подробнее в п.2.2.5.3);

- «Отклонить» - для отклонения заявки;

ПРИМЕЧАНИЯ:

✓ Согласовать заявки возможно только в статусах «Требует согласования» и «Отклонена»;

✓ Отклонить заявки возможно только в статусах «Требует согласования» и «Согласована»;

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия.

В результате успешного подтверждения, заявки будут согласованы или отклонены.

2.2.5.3. Разрешение конфликта устройств с пересекающимися идентификаторами из приглашения

Если при использовании приглашения ППО обнаружит, что устройства с идентификаторами из приглашения уже есть в системе, то будет создана заявка на активацию для разрешения конфликта.

Чтобы разрешить конфликт в заявке на активацию, необходимо:

1) Перейти в подраздел «Устройства» раздела «Управление»;

2) Нажать на кнопку «Приглашения» (см. Рисунок 36);

3) Перейти в раздел «Заявки на активацию» (см. Рисунок 38 [1]). По умолчанию будет отображен список заявок на активацию в статусе «Требует согласования». При необходимости с помощью области фильтров слева отобразить заявки на активацию в другом статусе или уточнить причину, или сбросить фильтр, чтобы отобразить в списке заявки на активацию во всех статусах;

4) Выбрать из списка одну заявку, у которой одна из причин «Пересечение идентификаторов», установив галочку в чекбоксе для доступа к списку быстрых действий;

5) В списке быстрых действий выбрать значок «Разрешить конфликт».

В отобразившемся окне будет приведена следующая информация:

– данные по существующим устройствам в ППО, с которыми есть пересечения в идентификаторах;

– данные по активируемому устройству, которое пришло в результате применения приглашения.

ПРИМЕЧАНИЕ. Пересечения в идентификаторах между существующими устройствами и активируемым устройством помечаются красно-оранжевым цветом;

6) В раскрывающемся списке «Стратегия разрешения конфликтов» выбрать нужное значение:

– **«Привязать новое устройство к одному из существующих»** (Рисунок 39) - активируемое устройство будет привязано к одному из выбранных существующих устройств в ППО. Дополнительно в раскрывающемся списке «Существующее устройство» выбрать существующее устройство для привязки. В результате данной привязки сохранятся пересекающиеся идентификаторы, а все остальные идентификаторы будут обновлены значениями, соответствующими новому активируемому устройству. При этом данные в карточке устройства не изменятся.

ПРИМЕЧАНИЕ. Для привязки можно использовать архивные и давно не подключавшиеся устройства. После применения стратегии такие устройства будут разархивированы и исключены из списка давно не подключавшихся.

Применение стратегии завершится ошибкой, если для привязки выбрано существующее устройство и:

– его `hostname` отличается от `hostname` активируемого устройства;

– у активируемого устройства есть `hostname`, а у существующего — нет;

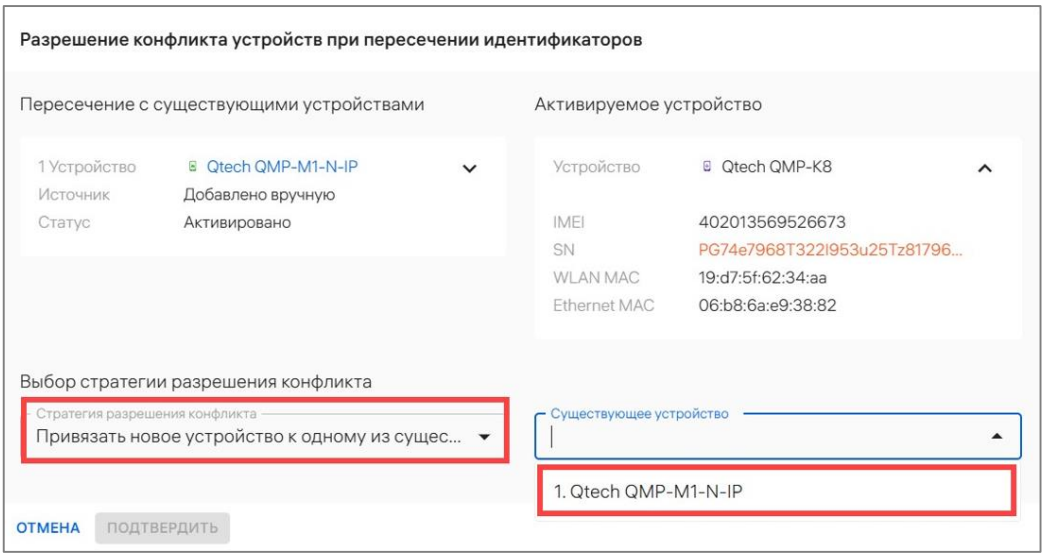


Рисунок 39

– **«Создать новое устройство, исключив пересекающиеся идентификаторы»** (Рисунок 40) - в результате применения этой стратегии будет создано новое устройство в ППО, но у него будут удалены пересекающиеся идентификаторы с другими существующими устройствами.

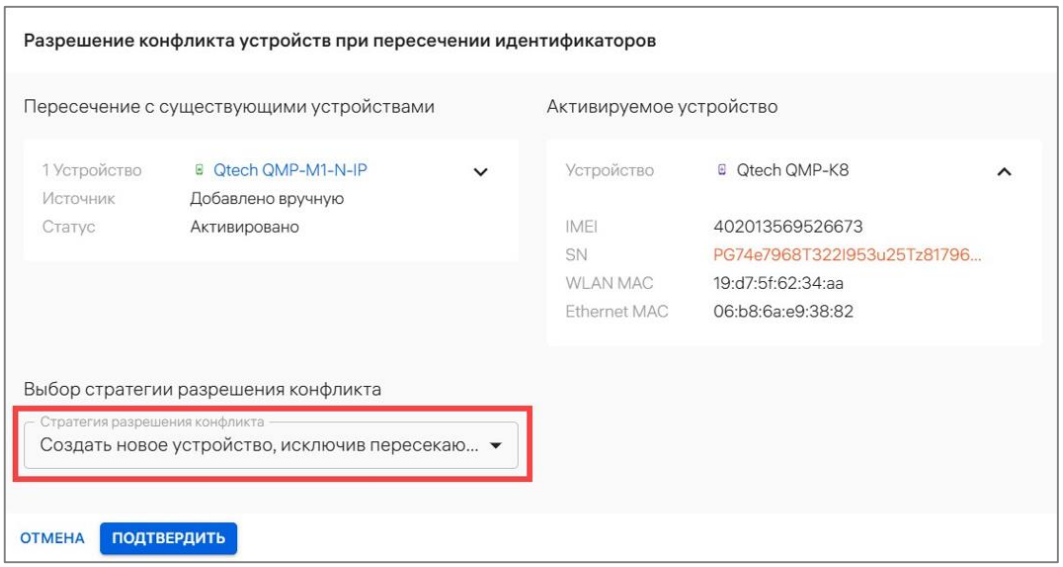


Рисунок 40

ПРИМЕЧАНИЕ. Применение стратегии завершится ошибкой, если у активируемого устройства не останется ни одного уникального идентификатора;

7) Нажать на кнопку «Подтвердить».

В результате успешного применения стратегии в открывшемся окне отобразится ссылка (Рисунок 41) на созданную или обновленную карточку устройства.



Рисунок 41

По результатам разрешения конфликта заявка на активацию будет полностью согласована, в дальнейшем устройство будет активировано.

ПРИМЕЧАНИЯ:

✓ Если заявка на активацию содержит несколько причин (например, пересечение идентификаторов и превышение лимита переактивации), то при разрешении конфликта по пересечению идентификаторов заявка будет автоматически полностью согласована;

✓ Если при применении стратегии разрешения конфликта у активируемого устройства не окажется пересечений с существующими устройствами, заявка станет неактуальной и перейдет в статус «Нерелевантная», после чего согласование или отклонение данной заявки будет невозможно;

✓ Если устройство при активации по приглашению попадает в заявки на активацию с одной из причин «Пересечение идентификаторов», то при ручном разрешении конфликтов в такой заявке необходимо задать основной идентификатор, на который необходимо ориентироваться в первую очередь. Стратегия, которую необходимо использовать, зависит от того, какие идентификаторы пересекаются у активируемого устройства с существующими устройствами.

Например, если у активируемого устройства совпадает основной идентификатор с существующим устройством, необходимо выбрать стратегию «Привязать активируемое устройство к одному из существующих», поскольку пришло то же самое устройство, но с другими вторичными идентификаторами. В случае, если у активируемого устройства совпадают вторичные идентификаторы, а не основной, с существующим устройством, рекомендуется применять стратегию «Создать новое устройство, исключив у него пересекающиеся идентификаторы», т.к. будет считаться другим устройством с другим основным идентификатором;

✓ Если в организации практикуется USB-донгл, который позволяет настраивать устройства без сетевого интерфейса, тогда рекомендуется выставить в настройках ППО режим автоматического разрешения конфликтов и выбрать стратегию «Создать новое устройство, исключив у него пересекающиеся идентификаторы», поскольку устройства при активации будут иметь одни и те же MAC-адреса, а ППО сможет самостоятельно разрешить данные конфликты;

✓ Рекомендуется отключить рандомизацию MAC-адресов на устройствах во избежание проблем при активации и разрешении конфликтов для таких устройств.

2.2.6. Добавление множества

Сущность «Множество» позволяет комбинировать в себе группы пользователей и устройств с помощью операторов «Объединение», «Пересечение» и «Разность».

Множество будет содержать:

– устройства из групп устройств множества;

– устройства, привязанные к пользователям из групп пользователей множества.

Для добавления множества необходимо:

1) Перейти в подраздел «Устройства» раздела «Управление»;

2) Нажать кнопку «Добавить», в раскрывающемся списке выбрать пункт «Добавить множество» (см. Рисунок 29);

3) В открывшемся окне заполнить поля (Рисунок 42 [1]), приведенные в таблице (Таблица 37);

Таблица 37

Параметр	Описание
Имя множества	Название множества. Поле обязательно для заполнения
Комментарий	Ввод значения с клавиатуры. Поле не является обязательным для заполнения

4) В разделе «Подмножества групп» (Рисунок 42 [2]) каждый блок должен содержать хотя бы один блок групп (подмножество):

– в раскрывающемся списке «Операция внутри блока» выбрать нужную операцию:

- «Объединение» - попадут все устройства, которые находятся хотя бы в одной из выбранных групп блока подмножества;

• «Разность» - попадут только те устройства, которые находятся в первой выбранной группе и отсутствуют в любой из остальных групп этого блока подмножеств;

• «Пересечение» - попадут только те устройства, которые находятся во всех выбранных группах блока подмножества;

5) Нажать на значок + и выбрать в раскрывающемся списке группу какого типа требуется добавить в блок (Рисунок 42 [3]): группа устройств или группа пользователей.

ПРИМЕЧАНИЕ. При добавлении группы пользователей во множество попадают не сами пользователи, а устройства, которые к ним привязаны;

6) Выбрать в раскрывающемся списке нужную группу. При необходимости воспользоваться фильтром по названию групп;

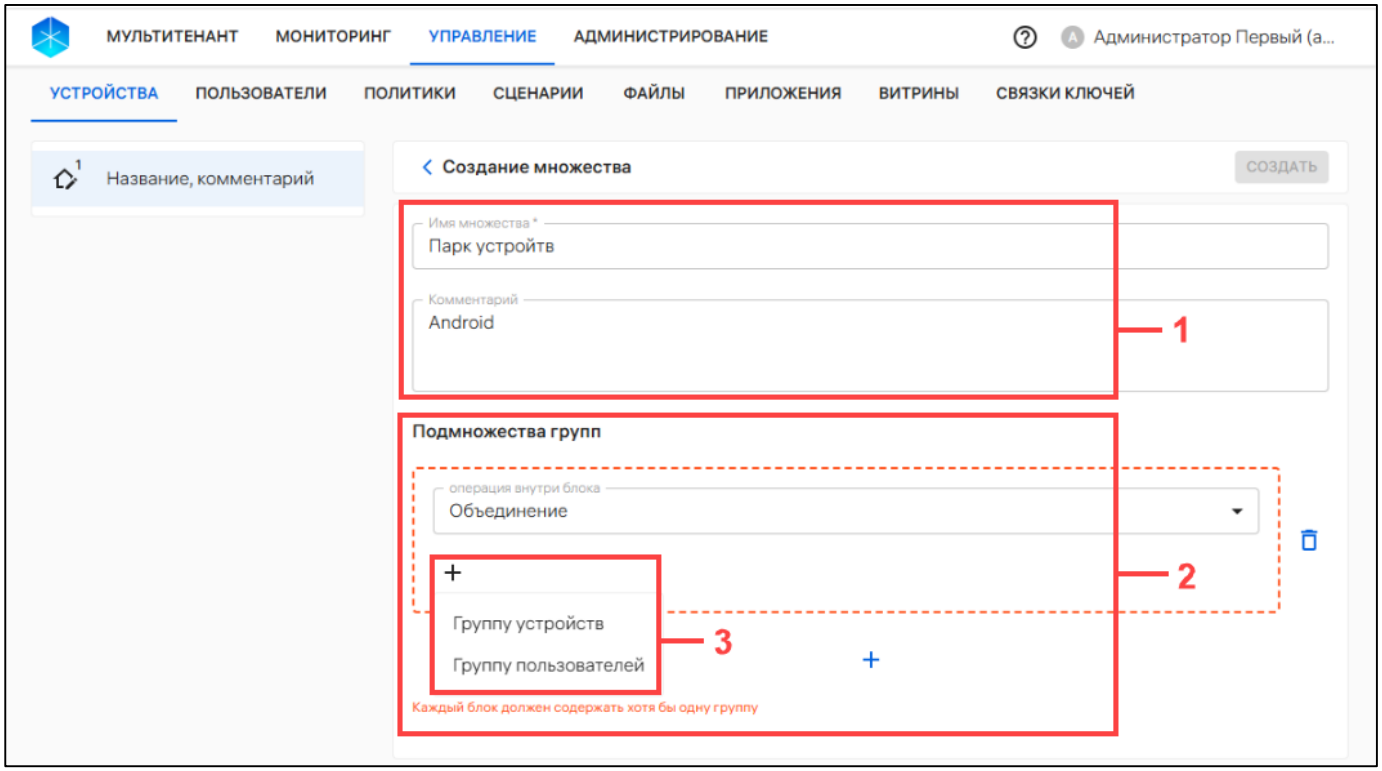


Рисунок 42

7) Чтобы добавить еще одну группу устройств или группу пользователей в блок (добавить в блок все необходимые группы), необходимо нажать на значок + (Рисунок 43 [1]) и повторить шаги 5 и 6;

8) Если требуется добавить еще один блок групп (подмножество) необходимо:

– нажать на значок + под первым блоком (Рисунок 43 [2]);

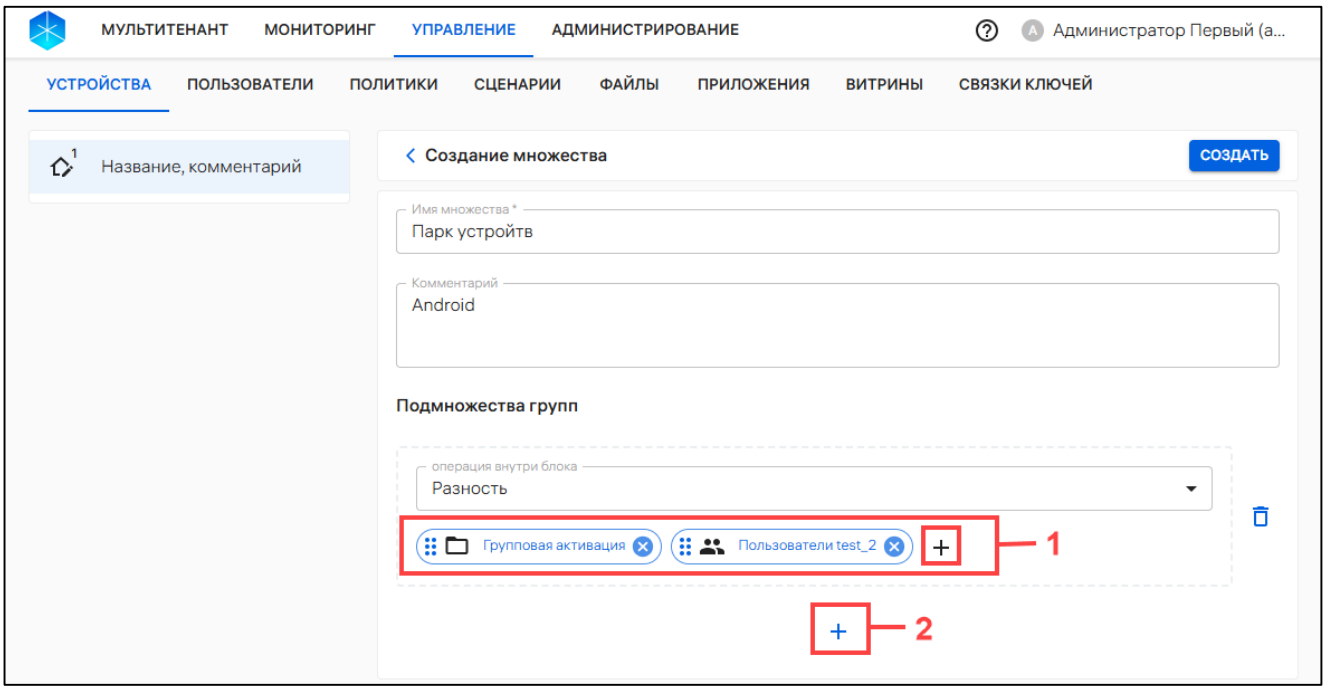


Рисунок 43

– в раскрывающемся списке «Операция между блоками» (см. Рисунок 44 [1]) выбрать нужную операцию:

- «Объединение» - попадут все устройства, которые находятся и в промежуточном вышестоящем результирующем выражении, и в нижестоящем добавляемом блоке подмножества;
- «Разность» - попадут только те устройства, которые находятся и в промежуточном вышестоящем результирующем выражении, и при этом не находятся в нижестоящем добавляемом блоке подмножества;
- «Пересечение» - попадут только те устройства, которые находятся и в промежуточном вышестоящем результирующем выражении, и в нижестоящем добавляемым блоком подмножества одновременно;

– во втором блоке выбрать операцию и группы по аналогии с заполнением блока на шаге 4;

9) Добавить необходимое количество блок групп (подмножеств), повторяя шаг 8;

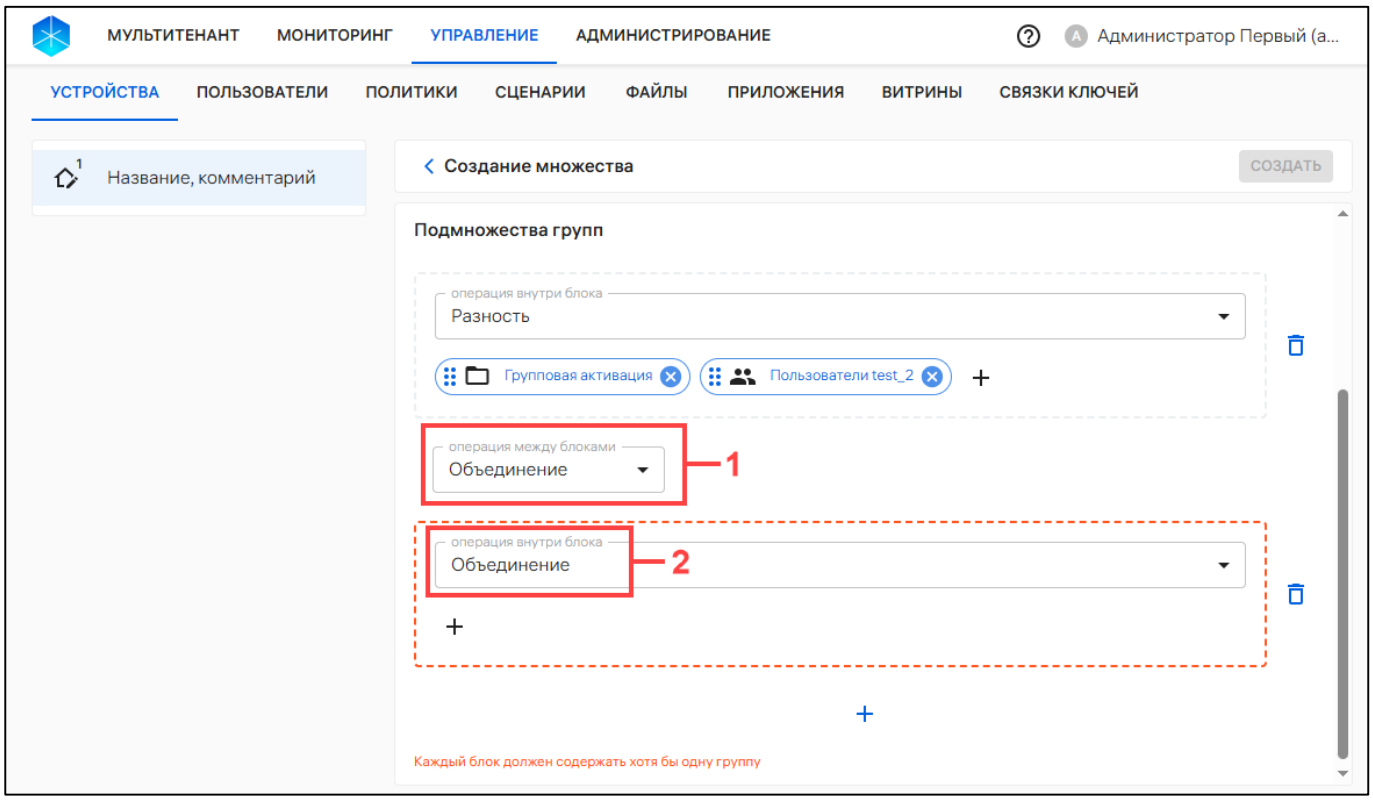


Рисунок 44

10) При необходимости возможно переместить группы из блока в блок (и внутри блока), удерживая нажатым значок перед названием группы (Рисунок 45);

11) Нажать кнопку «Создать» (Рисунок 45), в результате чего множество будет создано.

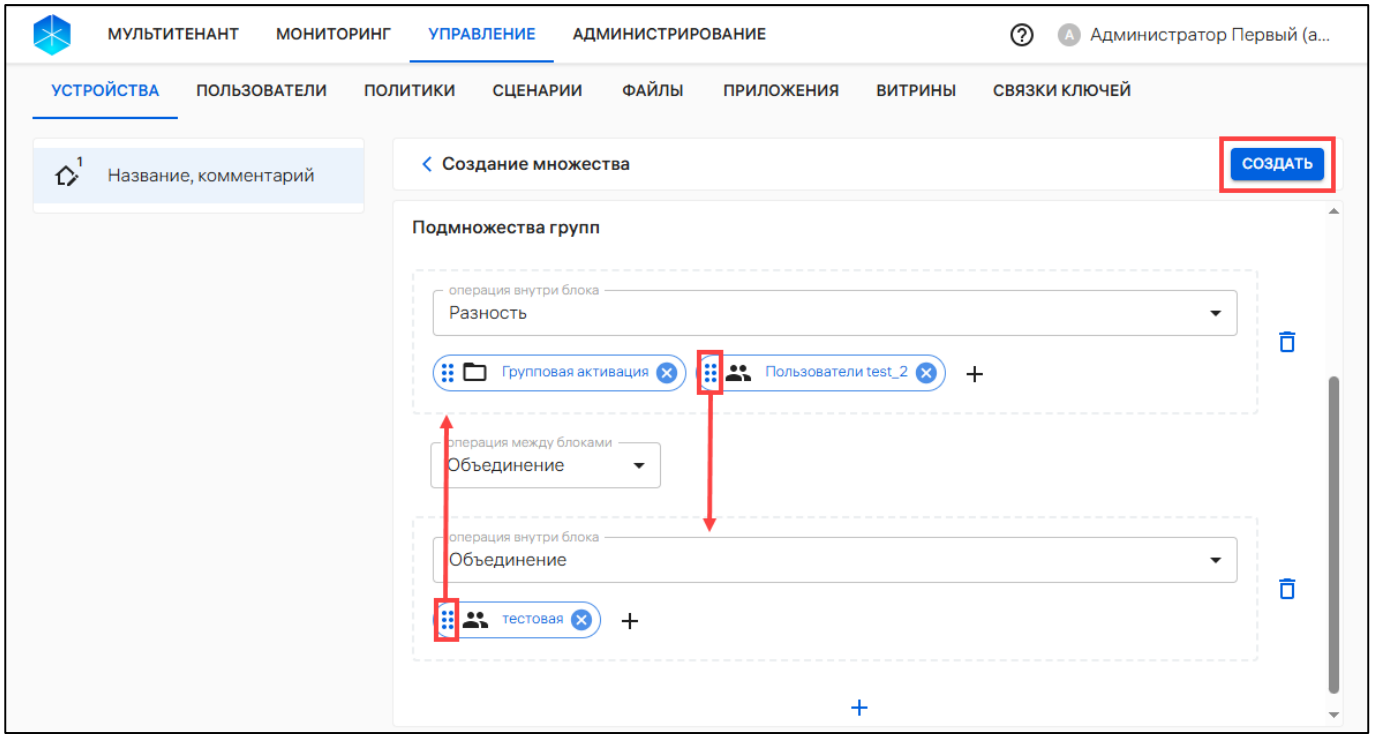


Рисунок 45

Наполнение и формирование результирующего множества выполняется в следующем порядке:

1) Сначала выполняются операции внутри блоков подмножеств;

2) Затем последовательно выполняются операции между блоками подмножеств сверху вниз.

Например, есть три блока подмножеств: 1, 2 и 3. Сперва выполнятся операции внутри блоков, затем выполнится операция между результатом блоков 1 и 2, затем этот полученный результат будет оперирован с результатом блока 3.

На вкладках карточки множества (Рисунок 46 [1]) отображается следующая информация:

– «Структура» (по умолчанию) – отображается информация о том, какие группы и с какими операциями используются в множестве;

– «Устройства» – отображается список устройств, принадлежащих множеству. Доступен поиск устройств с помощью фильтров (подраздел 1.4);

– «Политики» – отображается список политик, назначенных на множество. Можно назначать и отвязывать политики, назначенные на множество. При назначении политики отображается окно с информацией о пересечении политик (как в группах);

– «Сценарии» – отображается список офлайн-сценариев, назначенных на множество. Можно назначать и отвязывать офлайн-сценарии, назначенные на множество.

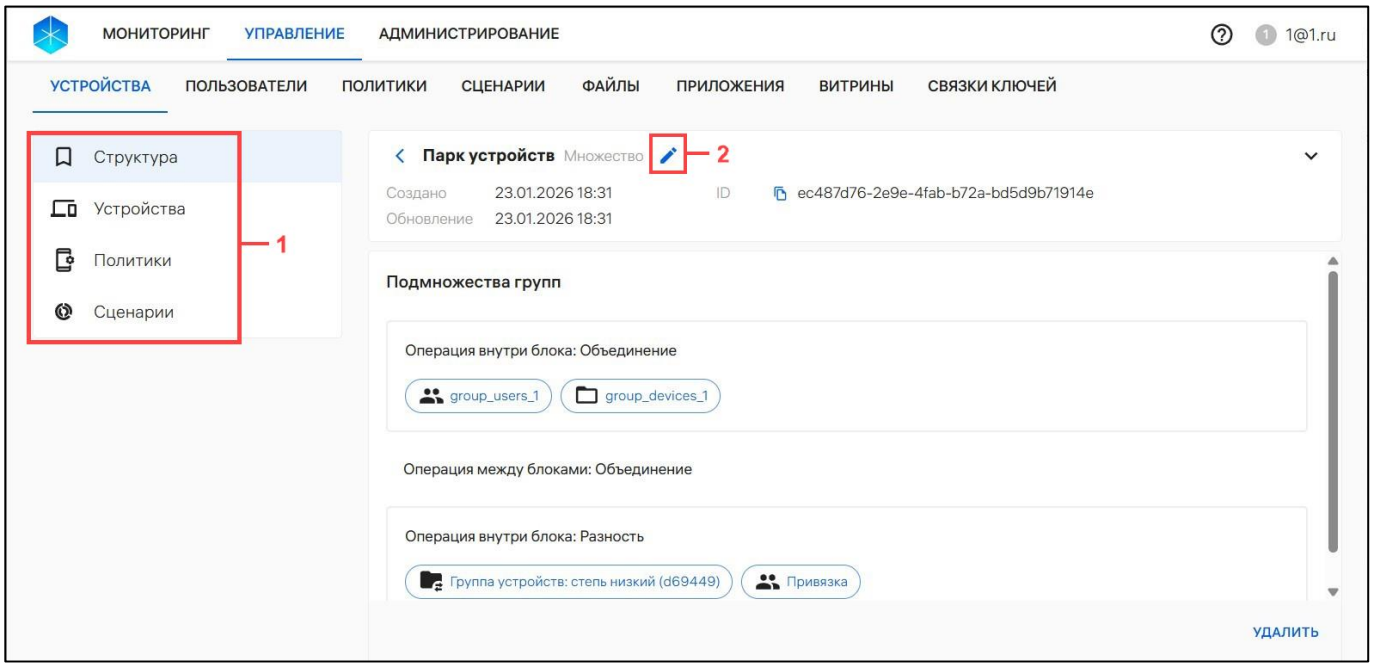


Рисунок 46

2.2.6.1. Редактирование множества

Для редактирования данных о множестве необходимо:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по множествам»;

– нажать на название нужного множества (при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок «Редактировать» (см. Рисунок 46 [2]) и внести необходимые изменения в следующие поля и разделы:

- в полях «Имя множества» и «Комментарий» согласно таблице (см. Таблица 37);
- в разделе «Подмножества групп»:

♦ изменить операцию между блоками групп (подмножеств), выбрав нужное значение в раскрывающемся списке «Операция между блоками» (подробнее в п. 2.2.6 шаг 8);

♦ изменить операцию внутри блока групп (подмножеств), выбрав нужное значение в раскрывающемся списке «Операция внутри блока» (подробнее в п. 2.2.6 шаг 4);

♦ изменить состав групп блока: для удаления группы необходимо использовать значок (Рисунок 47 [1]) справа от названия, для добавления группы устройств или пользователей необходимо использовать значок (Рисунок 47 [2]) в блоке. При добавлении группы пользователей во множество попадают не сами пользователи, а устройства, которые к ним привязаны;

♦ при необходимости переместить группы из блока в блок (и внутри блока), удерживая нажатым значок перед названием группы (см. Рисунок 45);

♦ для удаления блока, нажать на значок «Удалить» (Рисунок 47 [3]);

– если необходимо, добавить блок групп и операцию, связывающую с другими блоками, с помощью значка (Рисунок 47 [4]);

– нажать кнопку «Сохранить».

В результате изменения в множестве будут сохранены.

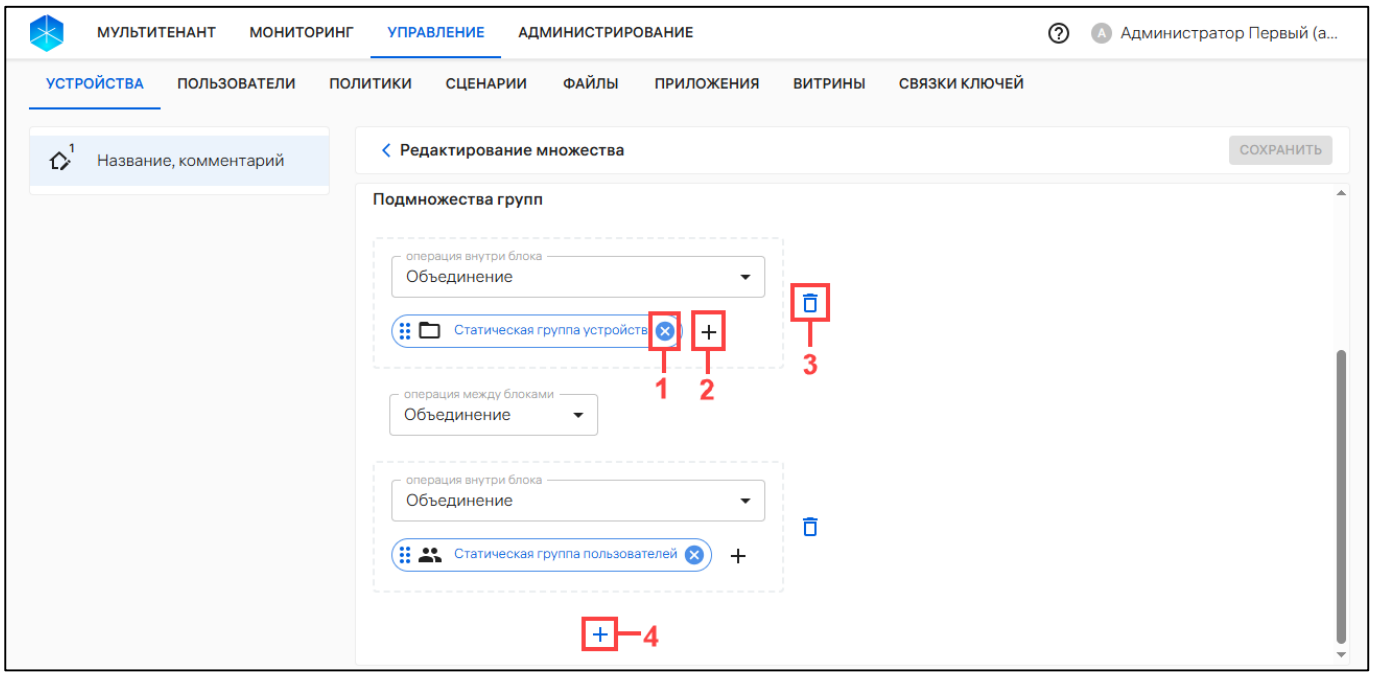


Рисунок 47

2.2.6.2. Удаление множества

Для удаления множества необходимо:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по множествам»;

– нажать на название нужного множества (при необходимости воспользоваться фильтром (подраздел 1.4);

– отвязать группу от всех политик (пп. 2.2.6.4) и офлайн-сценариев (пп. 2.2.6.6);

– нажать на кнопку «Удалить»;

– в отобразившемся окне подтвердить либо отменить действия;

В результате множество будет удалено.

2.2.6.3. Назначение политики на множество

Для назначения политики на множество необходимо:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по множествам»;

– нажать на название нужного множества (при необходимости воспользоваться фильтром (подраздел 1.4);

– перейти во вкладку «Политики» и нажать кнопку «Назначить политики» (Рисунок 48);

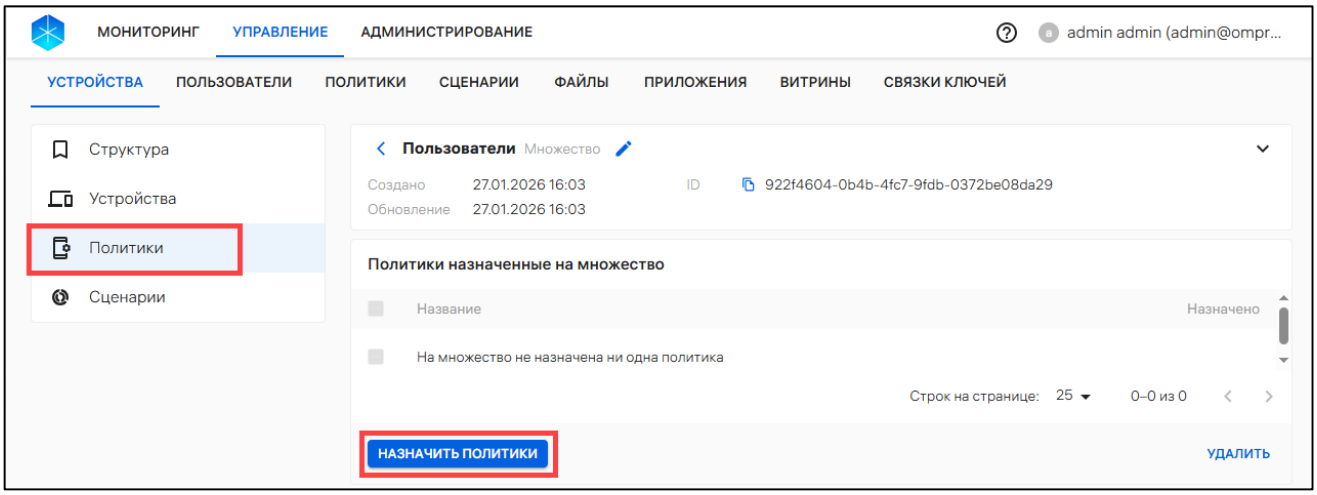


Рисунок 48

– выбрать в раскрывающемся списке нужную политику или воспользоваться фильтром по названию политики. Далее при необходимости возможно добавить дополнительную политику, выбрав ее из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранную политику, нажав значок «Убрать из списка» (Рисунок 49 [2]);

– нажать на кнопку «Назначить политики» (Рисунок 49 [1]).

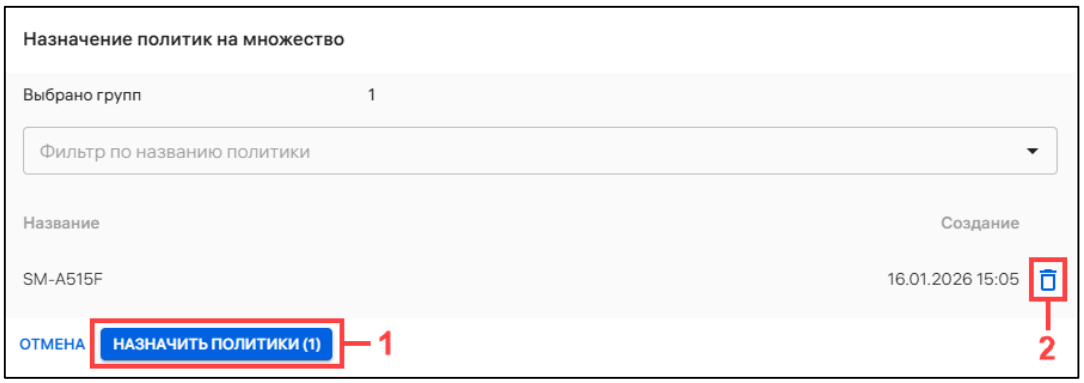


Рисунок 49

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Отобразится предупреждение о том, что это может занять некоторое время.

Для автоматического применения политики следует нажать кнопку «Назначить», не дожидаясь результата проверки, в результате политика с обновленными правилами будет назначена на все устройства.

Для просмотра пересечения политики с другими политиками и правилами из корпоративного шаблона необходимо дождаться завершения проверки. В результате будет отображен список названий пересекающихся групп и устройств (Рисунок 50), на которых пересекается политика, а также скомбинированная политика.

ПРИМЕЧАНИЕ. Перед применением скомбинированной политики следует помнить, что:

– приоритет имеют запрещающие правила;

– корпоративный шаблон дополняет скомбинированную политику правилами, которые указаны в нем, но не указаны в скомбинированной политике.

Для применения политики на все устройства необходимо нажать кнопку «Назначить» (Рисунок 50), в результате чего политика будет назначена на множество. Если устройство, входящее во множество, не было активировано, то после его активации на него будет назначена только последняя скомбинированная политика.

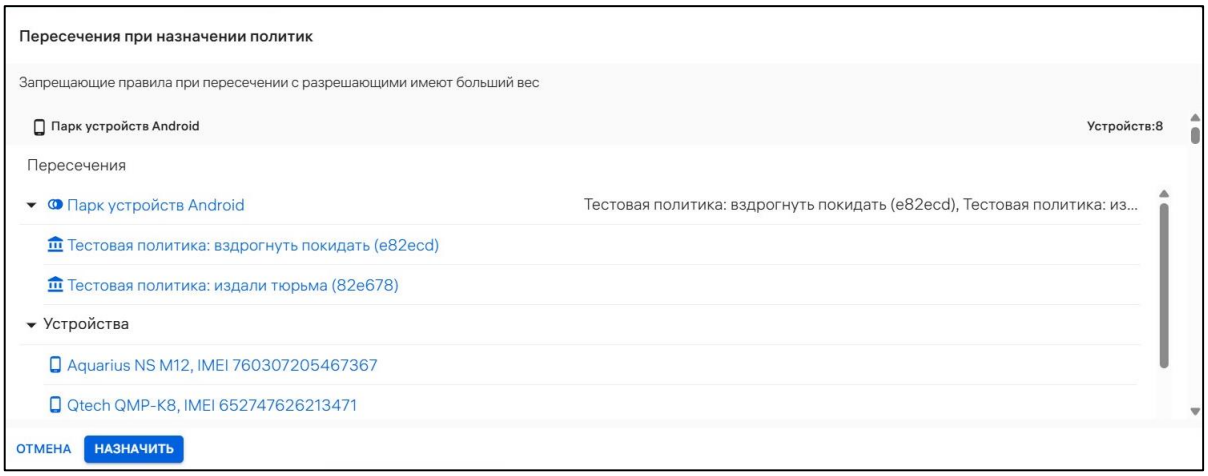


Рисунок 50

2.2.6.4. Отвязка множества от политики

Для отвязки множества от политики необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по множествам»;

– нажать на название нужного множества (при необходимости воспользоваться фильтром (подраздел 1.4);

– перейти во вкладку «Политики», выбрать необходимые политики в списке, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Отвязать политики от множества».

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в пп. 2.2.6.3.

В результате множество будет отвязано от политики.

ВНИМАНИЕ! Удаление запрещающего правила из политики, отвязка политики от множества или исключение устройства из группы множества не приведет к изменению состояния самого устройства (например, если правило политики запрещало использование камеры, то после снятия такой политики камера останется не доступной на устройстве). Для изменения состояния необходимо явно в политике установить целевое состояние. Также можно использовать корпоративный шаблон политики. Например, если в корпоративном шаблоне политики будет задано разрешающее правило политики на использование камеры, и при этом на устройстве будет назначена любая политика (даже пустая), тогда устройство приведется в состояние, указанное в корпоративном шаблоне политики.

Важно понимать, что корпоративный шаблон политики действует на все устройства, на которых действует хотя бы одна политика и регулирует только те правила, которые явно не заданы в политиках.

2.2.6.5. Назначение офлайн-сценария на множество

Для назначения офлайн-сценария на множество необходимо:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по множествам»;

– нажать на название нужного множества (при необходимости воспользоваться фильтром (подраздел 1.4);

– перейти во вкладку «Сценарии» и нажать кнопку «Назначить сценарии»;

– в открывшемся окне выбрать в раскрывающемся списке нужный офлайн-сценарий, при необходимости воспользовавшись фильтром по названию офлайн-сценария. Далее при необходимости возможно добавить дополнительный офлайн-сценарий, выбрав его из раскрывающегося списка либо воспользовавшись поиском по фильтру;

– добавленный офлайн-сценарий отобразится в списке. При необходимости возможно удалить добавленный офлайн-сценарий из списка, нажав значок «Убрать из списка»;

– нажать на кнопку «Назначить сценарий».

В результате применения офлайн-сценарий будет назначен на множество.

2.2.6.6. Отвязка множества от офлайн-сценария

Для отвязки множества от офлайн-сценария необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по множествам»;

– нажать на название нужного множества (при необходимости воспользоваться фильтром (подраздел 1.4);

– перейти во вкладку «Сценарии», выбрать необходимые офлайн-сценарии в списке, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Отвязать офлайн-сценарии от множества»;

– в отобразившемся окне подтвердить либо отменить действие.

В результате отвязки офлайн-сценарий будет удален со всех устройств множества.

ВНИМАНИЕ! Если результат данного офлайн-сценария уже применен на устройствах и при этом на устройствах не назначена политика с иным действием, после отвязки офлайн-сценария его результат не будет отменен.

2.2.7. Экспорт списка устройств в CSV-файл

Для экспорта списка устройств в файл формата `.csv` необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– выбрать в области фильтров «Поиск по устройствам»;

– нажать кнопку «Экспорт».

ПРИМЕЧАНИЕ. Также кнопка «Экспорт» доступна в карточке группы устройств (п. 2.1.2);

– в отобразившемся окне подтверждения экспорта устройств подтвердить либо отменить действия.

В результате подтверждения действия начнется процесс экспорта, который может занять несколько минут, после чего на ЭВМ будет скачан файл формата `.csv` с результатами экспорта.

Файл с результатами экспорта содержит следующие параметры устройств, разделенные запятой:

– **imeis** – международный идентификатор мобильного оборудования (состоит из 15 цифр). Если у устройства несколько IMEI, то они будут перечислены через точку с запятой;

– **sn** – серийный номер, который присвоен устройству производителем;

– **ethernetMACs** – MAC-адрес Ethernet устройства. Состоит из 6 пар символов, разделенных двоеточием. Если у устройства несколько MAC-адресов Ethernet, то они будут перечислены через точку с запятой;

– **wifiMACs** – MAC-адрес WLAN устройства. Состоит из 6 пар символов, разделенных двоеточием. Если у устройства несколько MAC-адресов WLAN, то они будут перечислены через точку с запятой;

– **modelName** – модель устройства;

– **platform** – ОС устройства;

– **status** – статус жизненного цикла устройства;

– **compliance** – соответствие устройства назначенной политике;

– **comment** – комментарий к устройству;

– **createdAt** – дата и время добавления устройства в Аврора Центр;

– **connectedAt** – дата и время последнего подключения устройства к Аврора Центр;

– **deviceGroups** – название группы, в которую входит устройство. Параметр заключен в кавычки. Если устройство входит в несколько групп, их названия будут перечислены через точку с запятой.

ВНИМАНИЕ! Одни и те же группы могут быть перечислены в разном порядке в разных строках. Для успешной работы с экспортированным CSV-файлом необходимо ознакомиться с рекомендацией, приведенной в приложении (Приложение 2).

2.2.8. Привязка устройства к пользователю

В Консоли администратора ПУ предусмотрена возможность привязки устройств к пользователю, которая может быть выполнена:

– с помощью быстрых действий в списке устройств (пп. 2.2.8.1);

– с помощью быстрых действий в списке пользователей (пп. 2.3.5.1);

– вручную через карточку устройства (пп. 2.2.8.2);

– вручную через карточку пользователя (пп. 2.3.5.2);

– с помощью импорта CSV-файла (п. 2.2.2.2.1);

– через интерфейс устройства с ОС Аврора или ОС Android (если добавлена интеграция ППО с LDAP-сервером, пп. 4.1.5.3.1);

– для устройств на базе ОС семейства Linux считается время пользовательских сессий на устройстве. В карточке устройства в текущем состоянии выводится ТОП-3 по наибольшему времени сессии пользователей, авторизованных на устройстве. ТОП-1 пользователь будет автоматически привязываться к устройству.

При привязке устройства к пользователю на устройстве будут действовать все офлайн-сценарии и политики, назначенные на группу пользователя либо скомбинированная политика, если политики были назначены на группу устройств, в которую входит устройство.

ПРИМЕЧАНИЕ. Перед привязкой устройства, необходимо убедиться, что добавлен хотя бы 1 пользователь. Процесс добавления пользователя приведен в п. 2.3.1 – 2.3.3.

2.2.8.1. Привязка устройства к пользователю с помощью списка быстрых действий

Для привязки устройства к пользователю с помощью списка быстрых действий необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по устройствам»;

– выбрать устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Привязать устройства к пользователям»;

– в отобразившемся окне выбрать пользователя из раскрывающегося списка или воспользоваться фильтром по ФИО, почте либо телефону пользователя. Далее, при необходимости, возможно добавить дополнительного пользователя, выбрав его из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также, возможно удалить из списка выбранных пользователей, нажав значок «Убрать из списка» справа от пользователя;

– нажать кнопку «Привязать пользователей».

В результате успешной привязки пользователей к устройству отобразится соответствующее сообщение.

Если на группу, в которую включен пользователь, назначена политика и/или офлайн-сценарий, они начнут действовать на привязанном устройстве (если оно активировано).

2.2.8.2. Привязка устройства к пользователю из карточки устройства

Для привязки устройства к пользователю из карточки устройства необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– для отображения списка устройств выбрать в области фильтров «Поиск по устройствам»;

– найти требуемое устройство, при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок в столбце «Карточка» для перехода в карточку устройства;

– перейти во вкладку «Пользователи»;

– нажать кнопку «Привязать пользователей»;

– в отобразившемся окне выполнить действия, описанные в пп. 2.2.8.1.

2.2.9. Привязка устройств к группе устройств

В Консоли администратора ПУ предусмотрены 2 типа групп устройств:

– динамическая – группа с заданными условиями, при соблюдении которых устройства автоматически попадают в группу. Например, в динамическую группу активированных устройств попадают все устройства, успешно прошедшие активацию. Редактирование или удаление динамической группы невозможно;

– статическая – группа, созданная Администратором Платформы управления. Состав группы изменяется Администратором Платформы управления.

Осуществить привязку устройств к статической группе можно с помощью:

– списка быстрых действий (пп. 2.2.9.1);

– карточки устройства (пп. 2.2.9.2);

– карточки группы устройств (пп. 2.2.9.3);

– заполненного CSV-файла в соответствии с пп. 2.2.3.1. После добавления устройств в группу с помощью импорта CSV-файла на устройства будут действовать все политики и офлайн-сценарии, назначенные на группу устройств.

Перед привязкой устройств необходимо убедиться, что добавлена хотя бы 1 группа устройств (п. 2.2.2).

2.2.9.1. Привязка устройств к группе устройств с помощью списка быстрых действий

Для привязки устройств к группе устройств с помощью списка быстрых действий необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по устройствам»;

– выбрать устройства в списке устройств, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Привязать устройства к группам»;

– в отобразившемся окне выбрать необходимую группу устройств из раскрывающегося списка или воспользоваться фильтром. Далее, при необходимости, возможно добавить дополнительную группу, выбрав ее из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранную группу, нажав на значок «Убрать из списка»;

– при отсутствии необходимой группы в списке, создать ее, введя название новой группы в поле «Фильтр по названию группы» и нажав кнопку «Создать статическую группу»;

– нажать кнопку «Добавить в группы».

В результате успешной привязки устройства к группе отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. На активированные устройства будут действовать все политики и офлайн-сценарии, назначенные на группу устройств.

2.2.9.2. Привязка устройств к группе устройств из карточки устройств

Для привязки устройств к группе из карточки устройств необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– для отображения списка устройств выбрать в области фильтров «Поиск по устройствам»;

– найти требуемое устройство, при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок в столбце «Карточка» для перехода в карточку устройства;

– перейти во вкладку «Группы»;

– нажать кнопку «Добавить в группы»;

– в открывшемся окне необходимо выполнить действия, описанные в пп. 2.2.9.1.

В результате успешной привязки устройства к группе отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. На активированном устройстве будут действовать все политики и офлайн-сценарии, назначенные на группу устройств.

2.2.9.3. Привязка устройств к группе устройств из карточки группы устройств

Для привязки устройств к группе устройств из карточки группы устройств необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке группы устройств перейти во вкладку «Устройства»;

– нажать кнопку «Привязать устройства» (см. Рисунок 18 [6]);

– в отобразившемся окне выбрать необходимое устройство из раскрывающегося списка или воспользоваться фильтром. Далее, при необходимости, возможно добавить дополнительное устройство, выбрав его из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранное устройство, нажав на значок «Убрать из списка»;

– нажать кнопку «Добавить устройства».

В результате на активированных устройствах будут действовать все политики и офлайн-сценарии, назначенные на группу устройств.

2.2.10. Активация устройств

Для активации устройств в Консоли администратора ПУ необходимо сгенерировать QR-код, после чего статус устройств с параметра «Жизненный цикл» поменяется на «В процессе активации». Для устройств во всех статусах доступна повторная генерация QR-кода (повторная активация).

При успешной активации на устройстве назначаются все политики, назначенные на:

– группы устройств, в которые входит устройство;

– на группу пользователей, к которым привязано устройство.

Если при активации устройства на него не были назначены политики, устройство в параметре «Жизненный цикл» примет значение «Активировано», а в параметре «Политики» – статус «Не управляется» и передаст свое состояние Консоли администратора ПУ.

Настроенные для работы устройства в параметре «Политики» имеют следующие статусы:

– «Не управляется»;

– «Соответствует политике»;

– «Не соответствует политике».

Порядок настройки устройств для работы с ПУ приведен в документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android»;

– «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

Активация устройств возможна следующими способами:

– вручную (пп. 2.2.10.1), если необходимо самостоятельно активировать 1 устройство;

– с помощью списка быстрых действий (пп. 2.2.10.2), если необходимо активировать несколько устройств;

– с помощью отправки QR-кода на Email (пп. 2.2.10.3), если необходимо, чтобы пользователи активировали свои устройства самостоятельно;

– с помощью загрузки JSON-файла (пп. 2.2.10.4), если необходимо активировать все устройства группы одним QR-кодом;

– с помощью приглашения на самостоятельную регистрацию устройства (пп. 2.2.1.2);

– при первом включении устройства (ускоренная активация), если для устройства были выполнены все условия ускоренной активации. Подробное описание процесса ускоренной активации на устройстве приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора».

2.2.10.1.Активация устройств вручную

Активация устройств вручную возможна из карточки устройства. Для этого необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– для отображения списка устройств выбрать в области фильтров «Поиск по устройствам»;

– найти требуемое устройство, при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок в столбце «Карточка» для перехода в карточку устройства;

– нажать на значок (см. Рисунок 9 [3]) и выбрать «Активировать».

ПРИМЕЧАНИЕ. При повторной генерации использовать предыдущий QR-код будет невозможно;

– отобразится окно активации устройств (Рисунок 51);

– если выбрано устройство, которое было активировано ранее (повторная активация), или устройство в статусе «В процессе активации», необходимо в чекбоксе установить галочку слева от статуса (Рисунок 51 [1]) и нажать кнопку «Дальше» (Рисунок 51 [2]);

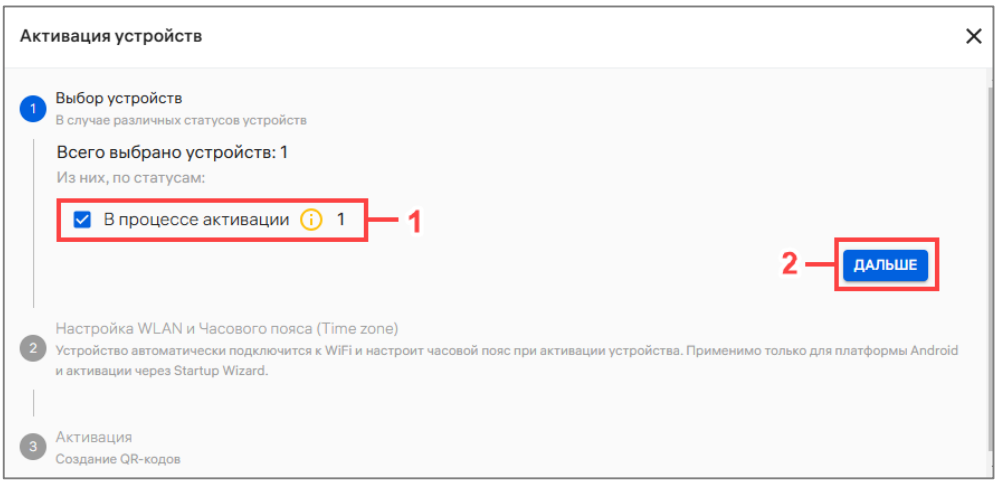


Рисунок 51

– для ОС Android в отобразившемся окне (Рисунок 52) возможно дополнительно указать сеть WLAN и часовой пояс, выполнив действия, приведенные в пп. 2.2.5.1 и нажать кнопку «Дальше»;

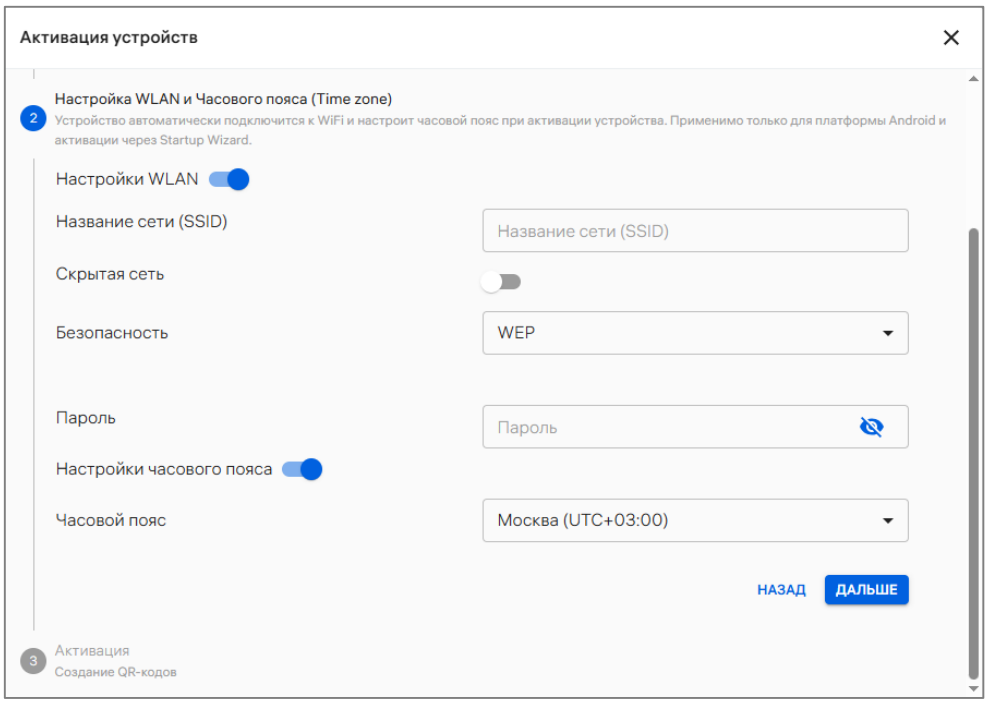


Рисунок 52

– откроется окно, где необходимо нажать кнопку «Активация вручную» (Рисунок 53);

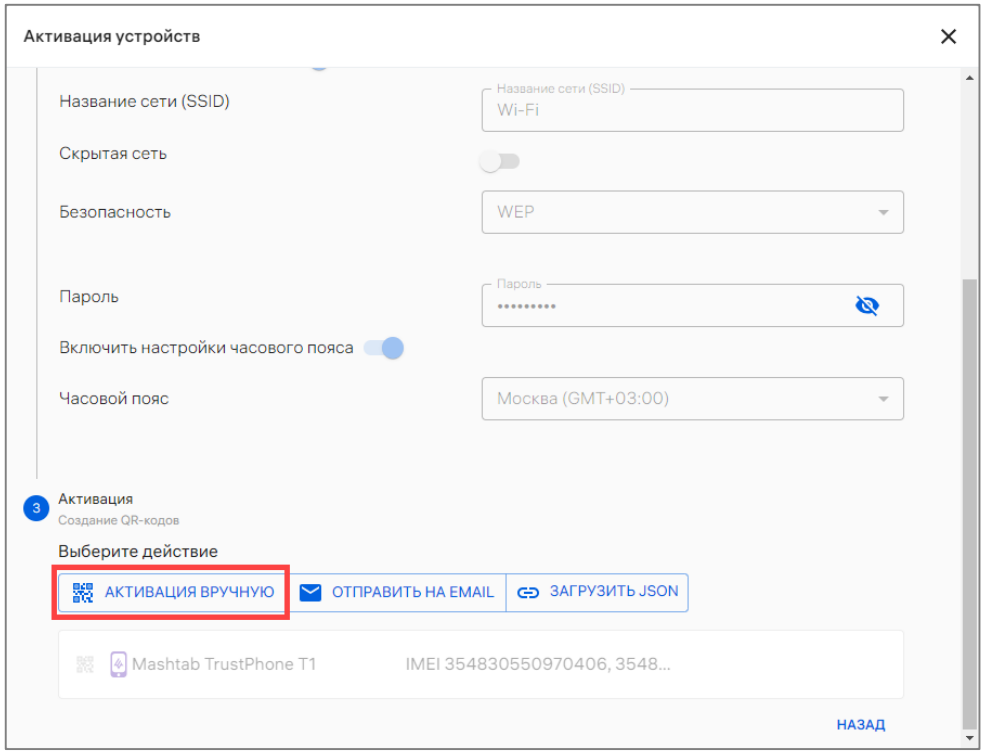


Рисунок 53

– в результате отобразится окно подтверждения создания QR-кода, где необходимо продолжить или отменить действия.

В результате успешного создания QR-кода будет отображена следующая информация (Рисунок 54):

– единый QR-код для установки приложения «Аврора Центр» и активации устройства, который необходимо отсканировать в приложении «Аврора Центр» на каждом устройстве;

– адрес процесса;

– пароль;

– дата истечения QR-кода.

ПРИМЕЧАНИЕ. По истечении срока действия сгенерированный QR-код будет недействителен;

– ссылка на скачивание пакета (APK-файла) для установки приложения «Аврора Центр»;

– часовой пояс.

ПРИМЕЧАНИЕ. Для отображения часового пояса необходимо в разделе «Настройка WLAN и Часового пояса» (Time zone)» (см. Рисунок 52) перевести переключатель «Настройки часового пояса» в положение «Включено» и в раскрывающемся списке выбрать необходимый часовой пояс;

– название компонента Android;

– контрольная сумма подписи пакета;

– название компонента Аврора;

– сумма MD5.

При успешной активации на устройство назначаются все политики и офлайн-сценарии, назначенные на:

– группу устройств, в которую входит устройство;

– на группу пользователей, к которым привязано устройство.

Если при активации устройства на него не были назначены политики, то устройство в параметре «Жизненный цикл» получит значение «Активировано», а в столбце «Соответствие политике» – статус «Не управляется» и передаст свое состояние в Аврора Центр.

ВНИМАНИЕ! При настройке ППО по умолчанию QR-код (и JSON-файл) генерируется на 5 минут. Этого времени может быть не достаточно для того, чтобы все устройства успели пройти активацию, если устройств много или QR-коды для активации отправляются на Email пользователей. Настройки срока действия QR-кода можно изменить в конфигурационном файле ППО: файл `/var/ocs/config/subsystems/emm/config.yml` параметр `qrCodeTtl`.

2.2.10.2.Активация устройств при помощи списка быстрых действий

Для активации устройств при помощи списка быстрых действий необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по устройствам»;

– выбрать устройства, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Активировать».

ПРИМЕЧАНИЕ. С помощью списка быстрых действий может быть выполнена активация одного или нескольких устройств;

– отобразится окно активации устройств (см. Рисунок 51);

– если выбрано устройство, которое было активировано ранее (повторная активация), или устройство в статусе «В процессе активации», необходимо в чекбоксе установить галочку слева от статуса устройства (см. Рисунок 51 [1]) и нажать кнопку «Дальше» (см. Рисунок 51 [2]);

– для ОС Android в отобразившемся окне (см. Рисунок 52) возможно дополнительно указать сеть WLAN и часовой пояс, выполнив действия, приведенные в п. 2.2.5.1 и нажать кнопку «Дальше»;

– в открывшемся окне необходимо нажать кнопку «Активация вручную» (см. Рисунок 53);

– отобразится окно подтверждения создания QR-кода, где необходимо продолжить или отменить действия.

В результате успешного создания QR-кода будет отображена следующая информация:

– единый QR-код для установки приложения «Аврора Центр» и активации устройства.

ПРИМЕЧАНИЕ. QR-код будет отображен для каждого из выбранных устройств (см. Рисунок 54 [1], см. Рисунок 54 [2]), который необходимо отсканировать в приложении «Аврора Центр» на каждом устройстве;

– адрес процесса;

– пароль;

– дата истечения QR-кода;

– ссылка на скачивание пакета (APK-файла) для установки приложения «Аврора Центр»;

– часовой пояс.

ПРИМЕЧАНИЕ. Для отображения часового пояса необходимо в разделе «Настройка WLAN и Часового пояса (Time zone)» (см. Рисунок 52) перевести переключатель «Настройки часового пояса» в положение «Включено» и в раскрывающемся списке выбрать необходимый часовой пояс;

– название компонента Android;

– контрольная сумма подписи пакета;

– название компонента Аврора;

– сумма MD5.

ПРИМЕЧАНИЕ. Установка приложения «Аврора Центр» и активация устройства будут автоматически выполняться при первоначальной настройке устройства с ОС Android (подробнее в документе «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android») и при корпоративной привязке устройства с ОС Аврора (подробнее в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора») к ПУ. В остальных случаях QR-код можно использовать только для активации устройства.

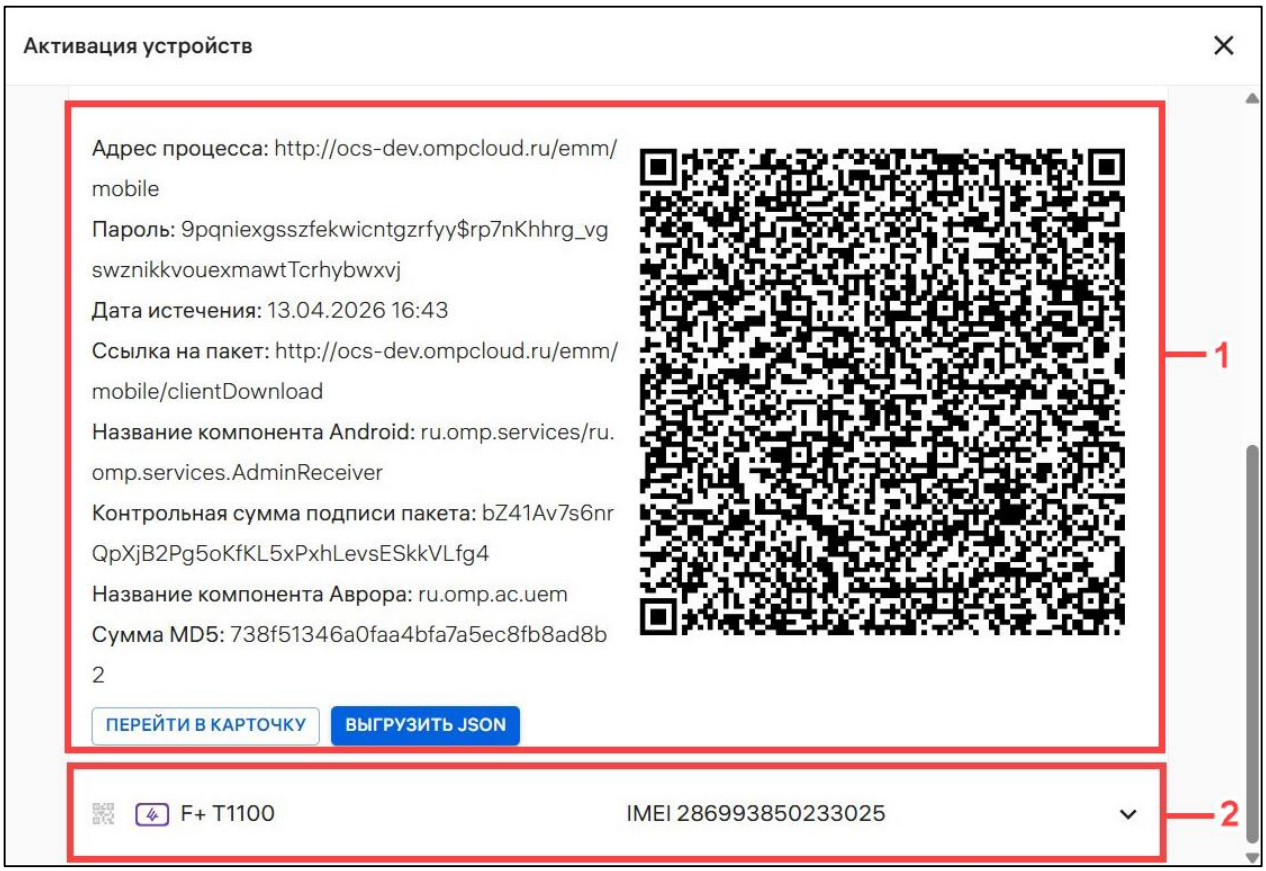


Рисунок 54

При успешной активации на устройство назначаются все политики и офлайн-сценарии, назначенные на:

– группу устройств, в которую входит устройство;
– на группу пользователей, к которым привязано устройство.

Если при активации устройства на него не были назначены политики, то устройство в параметре «Жизненный цикл» получит значение «Активировано», а в параметре «Соответствие политике» – статус «Не управляется» и передаст свое состояние в Аврора Центр.

ПРИМЕЧАНИЕ. Срок действия QR-кода указан в поле «Дата истечения». По истечении срока действия сгенерированный QR-код будет недействителен.

ВНИМАНИЕ! При настройке ППО по умолчанию QR-код (и JSON-файл) генерируется на 5 минут. Этого времени может быть не достаточно для того, чтобы все устройства успели пройти активацию, если устройств много или QR-коды для активации отправляются на Email пользователей. Настройки срока действия QR-кода

можно изменить в конфигурационном файле ППО: файл `/var/ocs/config/subsystems/emm/config.yml` параметр `qrCodeTtl`.

QR-код можно скопировать, нажав на него правой кнопкой мыши, и выбрать из списка пункт «Сохранить картинку как...», после чего QR-код можно отправить в виде изображения.

Далее пользователю необходимо отсканировать QR-код и выполнить активацию устройства. Подробное описание активации устройства приведено в документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android».

2.2.10.3.Активация устройств с помощью отправки QR-кода на Email

Для активации устройств с помощью Email на указанный адрес направляется электронное письмо с QR-кодом. Для этого необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по устройствам»;

– выбрать устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Активировать».

ПРИМЕЧАНИЕ. С помощью списка быстрых действий может быть выполнена активация одного или нескольких устройств;

– отобразится окно активации устройств (см. Рисунок 51);

– если выбрано устройство, которое было активировано ранее (повторная активация), или устройство в статусе «В процессе активации», необходимо в чекбоксе установить галочку слева от статуса (см. Рисунок 51 [1]) и нажать кнопку «Дальше» (см. Рисунок 51 [2]);

– для ОС Android в отобразившемся окне (см. Рисунок 52) возможно дополнительно указать сеть WLAN и часовой пояс, выполнив действия, приведенные в п. 2.2.5.1 и нажать кнопку «Дальше»;

– откроется окно, где необходимо нажать кнопку «Отправить на Email»;

– в результате отобразится окно отправки QR-кода на Email, где необходимо ввести Email для писем с активацией;

– нажать кнопку «Отправить».

На указанный адрес будет отправлено электронное письмо с QR-кодом для активации, который пользователю необходимо отсканировать на устройстве в приложении «Аврора Центр».

Подробное описание активации устройств приведено в документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android».

При успешной активации на устройстве назначаются все политики и офлайн-сценарии, назначенные на:

– группу устройств, в которую входит устройство;

– на группу пользователей, к которым привязано устройство.

Если при активации устройства на него не были назначены политики, то устройство в параметре «Жизненный цикл» получит значение «Активировано», а в параметре «Политика» – статус «Не управляется» и передаст свое состояние в Аврора Центр.

2.2.10.4.Активация группы устройств с помощью JSON-файла

Для активации устройств с помощью JSON-файла необходимо подготовить (пп. 2.2.10.4.1) и загрузить (пп. 2.2.10.4.2) JSON-файл.

Если первоначальная настройка устройств не осуществлялась, необходимо выполнить ускоренную активацию. Подробное описание приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора».

Если первоначальная настройка устройств была выполнена, необходимо отсканировать QR-код, сгенерированный для группы устройств, в которую входят устройства. Подробное описание приведено в документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android».

2.2.10.4.1. Подготовка JSON-файла

Активация устройств единым QR-кодом осуществляется с помощью JSON-файла, который можно сгенерировать в ПУ.

Для генерации JSON-файла необходимо выполнить действия, описанные в пп. 2.2.10.2, до этапа отображения окна активации устройств и отображения единого QR-кода, а затем нажать кнопку «Выгрузить JSON» (Рисунок 54 [1]).

В результате на ЭВМ будет выгружен JSON-файл.

Пример содержания JSON-файла:

{"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":{"accountDomain":"","clientID":"aurora-mobility-management","gatewayURI":"http://ocs-feat-1.ompcloud.ru/emm/mobile","password":"zo!xibhcqdhsonnokzndwGkbg8vktajuqOjigiim%dqosqovacwerfoorg5xozaf","trustedCerts":""},"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":"ru.omp.services/ru.omp.services.AdminReceiver","android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE

_DOWNLOAD_LOCATION":"http://ocs-feat-l.ompcloud.ru/emm/mobile/clientDownload","android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"bZ41Av7s6nrQpXjB2Pg5oKfKL5xPxhLevsESkkVLfg4","android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED":true,"android.app.extra.PROVISIONING_TIME_ZONE":"Asia/Krasnoyarsk","android.app.extra.PROVISIONING_WIFI_HIDDEN":"true","android.app.extra.PROVISIONING_WIFI_PASSWORD":"brn4872gdf3bue","android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE":"WEP","android.app.extra.PROVISIONING_WIFI_SSID":"liquidssid","aurora.app.extra.PROVISIONING_DEVICE_ADMIN_APP_ID":"ru.omp.ac.uem","expiredAt":"2026-04-03T16:46:07+03:00"}

ВНИМАНИЕ! Приведенный пример представлен для ознакомления с содержанием и структурой JSON-файла, и может отличаться от сгенерированного. Не рекомендуется форматировать сгенерированный JSON-файл (добавлять пробелы, табуляцию, переносы строк), так как это может привести к ошибкам при обработке JSON-файла в процессе установки приложения и активации устройств.

Каждый параметр сопровождается двоеточием «:», пары ключ/значение разделяются запятой «,».

Описание требований к значениям параметров из примера:

– **android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE** – содержимое JSON-файла:

- **password** – пароль, присваиваемый для созданной учетной записи устройства. Новый пароль может содержать:
  - от 8 до 255 символов;
  - не менее 2 заглавных букв;
  - не менее 2 строчных букв;
  - не менее 3 цифр;
  - не менее 2 спецсимволов.

ПРИМЕЧАНИЕ. При генерации JSON-файла создаются учетные записи устройств. Требования к паролю задаются администратором и могут отличаться от приведенных;

- **gatewayURI** – адрес сервера активации устройств;
- **accountDomain** – доменное имя аккаунтов учетных записей устройств, созданных в выбранном тенанте;
- **clientID** – идентификатор приложения в выбранном тенанте. Значение по умолчанию `aurora-mobility- management`;
- **trustedCerts** – список цифровых отпечатков (fingerprint) корневых сертификатов для активации устройств, перечисленные через запятую;

– **android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME** – название компонента;

– **android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM** – контрольная сумма подписи файла для установки приложения «Аврора Центр»;

– **android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION** – ссылка на скачивание файла для установки приложения «Аврора Центр»;

– **android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED** – параметр, определяющий, включать ли полную установку системных приложений в процессе установки первоначальной настройки устройства с установкой приложения «Аврора Центр» (актуально для устройств с ОС Android). По умолчанию установка всех системных приложений включена;

– **android.app.extra.PROVISIONING_WIFI_SSID** – название сети WLAN, к которой устройство автоматически подключится в процессе установки приложения «Аврора Центр» и активации устройства;

– **android.app.extra.PROVISIONING_WIFI_PASSWORD** – пароль сети WLAN, к которой устройство автоматически подключится в процессе установки приложения «Аврора Центр» и активации устройства;

– **android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE** – технология безопасности сети WLAN, к которой устройство автоматически подключится в процессе установки приложения «Аврора Центр» и активации устройства;

– **android.app.extra.PROVISIONING_WIFI_HIDDEN** – параметр, определяющий транслируется ли название сети WLAN, к которой устройство автоматически подключится в процессе установки приложения «Аврора Центр» и активации устройства;

– **android.app.extra.PROVISIONING_TIME_ZONE** – часовой пояс, который автоматически будет установлен на устройстве в процессе установки приложения «Аврора Центр» и активации устройства;

– **aurora.app.extra.PROVISIONING_DEVICE_ADMIN_APP_ID** – имя приложения на устройстве с ОС Аврора, в которое будут переданы активационные данные из QR-кода;

– **expiredAt** – срок действия QR-кода (дата истечения активации). После указанной даты сгенерированный QR-код будет недействителен.

2.2.10.4.2. Загрузка JSON-файл для активации группы устройств

Для активации группы устройств необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– выбрать группу устройств, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения следует нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Активация устройств»;

– перенести сгенерированный или подготовленный самостоятельно JSON-файл из файлового менеджера в поле загрузки (Рисунок 55);



Рисунок 55

– отобразится информация о загруженном JSON-файле, где необходимо нажать кнопку «Активация вручную» (Рисунок 56 [1]). Для удаления загруженного JSON-файла необходимо нажать кнопку «Удалить JSON» (Рисунок 56 [2]);



Рисунок 56

– в отобразившемся окне активации устройств необходимо нажать кнопку «Продолжить»;

– если были выбраны группы, содержащие активированные устройства или в статусе «В процессе активации», отобразится окно подтверждения операции, где необходимо подтвердить или отменить действия.

В чекбоксе «Не активировать ранее активированные устройства» следует установить галочку в случае отсутствия необходимости активировать ранее активированные устройства либо снять галочку, в случае наличия указанной необходимости.

В результате JSON-файл будет загружен, и отобразится QR-код для активации группы устройств.

Для завершения активации необходимо выполнить следующие действия:

– выполнить ускоренную активацию устройств, если их первоначальная настройка не осуществлялась. Описание процедуры ускоренной активации приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– отсканировать QR-код на каждом устройстве, если они уже прошли первоначальную настройку.

Для закрытия окна активации группы устройств необходимо нажать кнопку «Закрыть».

После загрузки JSON-файла для удобства работы с активацией в рабочей области раздела «Управление» подраздела «Устройства» отобразится индикатор активации (Рисунок 57). При нажатии на индикатор отобразится подробная информация об активации устройств: RequestID активации и количество готовых к активации устройств.

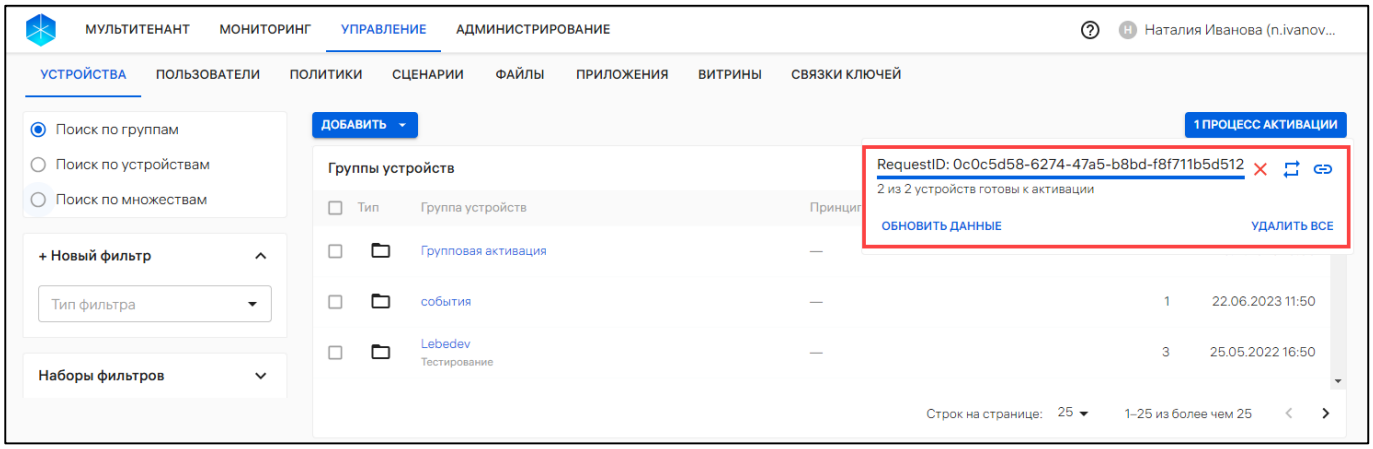


Рисунок 57

Для копирования ссылки процесса необходимо нажать значок «Скопировать ссылку процесса» (Рисунок 57). Для перезапуска процесса активации необходимо нажать значок «Перезапустить процесс». Для обновления информации об активации необходимо нажать кнопку «Обновить данные». Для закрытия индикатора следует нажать значок «Удалить процесс» или «Удалить все».

2.2.11. Применение оперативных команд

ВНИМАНИЕ! Применение оперативных команд доступно только для активированных устройств.

ПРИМЕЧАНИЕ. Для корректного управления устройством необходимо, чтобы на устройстве было выставлено корректное время и был задан часовой пояс.

Для применения команд оперативного управления необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– для отображения списка устройств выбрать в области фильтров «Поиск по устройствам»;

– найти требуемое устройство, при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок в столбце «Карточка» для перехода в карточку устройства;

– выбрать доступные оперативные команды (Рисунок 58 [1]), задать необходимые значения согласно таблице (Таблица 38) и далее подтвердить или отменить действия.

ПРИМЕЧАНИЕ. Действующие оперативные команды выделены цветным индикатором у соответствующего значка (Рисунок 58 [2]).

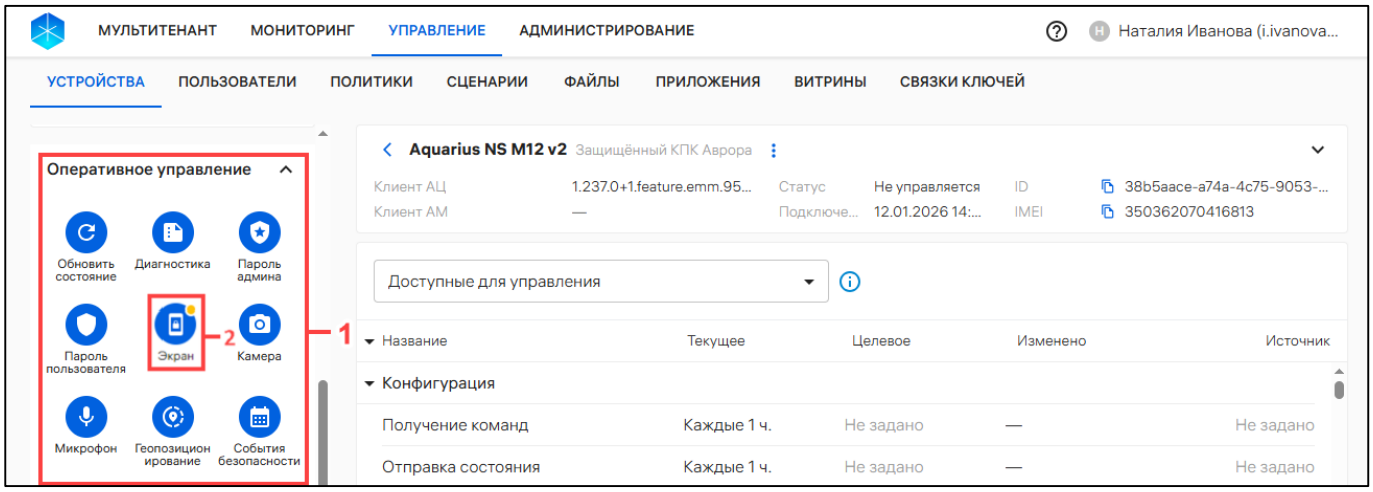


Рисунок 58

В результате успешной отправки оперативной команды отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Выбранная команда будет выполнена на устройстве в соответствии с установленным расписанием получения команд.

Если политика или оперативная команда не были получены на устройстве, то текущее и целевое состояния не будут совпадать. Несоответствия выделяются цветом, а в строке с названием группы политик/состояний отображается значок .

Таблица 38

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
Обновить состояние	Установка расписания обновления состояния устройства. Запрос получения текущего состояния устройства	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4
Диагностика	Получение диагностического отчета с активированного устройства с помощью команд оперативного управления. Для устройства на базе **ОС Аврора** будет отправлен запрос на формирование и получение отчета с логами. Для устройства на базе **ОС Android** необходимо: – предварительно настроить сбор через оперативную команду «Запустить сбор логов»; – установить галочку в чекбоксе «Отчет об ошибке». **ПРИМЕЧАНИЯ:** ✓Для сбора полных логов (logcat) приложению «Аврора Центр» требуются расширенные системные права. Необходимые права предоставляются с помощью вендорской подписи приложения. Без вендорской подписи автоматический сбор полных логов (logcat) без участия пользователя недоступен. Необходимость подтверждения пользователя зависит от версии ОС Android: – **ОС Android 13 и ниже**. Если приложение «Аврора Центр» подписано вендором, подтверждение пользователя не требуется; – **ОС Android 14 и выше**. Подтверждение пользователя требуется, в том числе если приложение «Аврора Центр» подписано вендором; ✓Если выбран «Отчет об ошибке», сформируется два архива: отчет об ошибке (`bugreport`) и диагностический отчет. В ином случае ППО сформирует только архив диагностического отчета; ✓Отчет об ошибке формируется с помощью стандартного механизма ОС Android. Для формирования отчета об ошибке требуется подтверждение пользователя на устройстве. Подтверждение требуется независимо от версии ОС Android и наличия у приложения «Аврора Центр» вендорской подписи После отправки команды на устройстве отображается системный запрос, который пользователь должен подтвердить. Запрос на подтверждение не отображается, если на устройстве активен режим с более высоким приоритетом, чем Киоск-режим, либо Киоск-режим настроен с отключенной панелью уведомлений. В этих случаях панель уведомлений недоступна, поэтому отчет об ошибке не формируется, при этом диагностический отчет будет сформирован;	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
	✓ Получение диагностического отчета во время активного сбора не останавливает сбор полных логов. После формирования отчета устройство продолжит собирать данные до окончания заданного периода. Например, если сбор полных логов был запущен в 10:00, а диагностический отчет запрошен в 12:00, в отчет войдут данные, собранные с 10:00 до момента формирования отчета. После этого сбор продолжится до времени окончания, указанного при запуске команды сбора логов(logcat). Для устройства на базе **ОС семейства Lin**ux необходимо: – задать параметры отчета «Период сбора логов с» и «Период сбора логов до» - ввести диапазон времени сбора логов. По умолчанию устанавливается диапазон в 24 часа от текущей даты и времени; – при необходимости указать диагностический скрипт, который был загружен и согласован в ППО. Для этого: • в раскрывающемся списке «Скрипт для диагностики» выбрать необходимый скрипт; • в раскрывающемся списке «Версия файла» выбрать нужную версию скрипта; • в поле «Таймаут» ввести максимальное время в формате [мм:сс], в течение которого скрипт должен выполниться на устройстве. При нажатии кнопки «Получить»: – устройство на базе **ОС Аврора** соберет логи приложения «Аврора Центр»: файл `omp-uem-agent.db` (база данных приложения «Аврора Центр»), файл `journalctl.log` (логи `journalctl`); – устройство на базе **ОС Android** соберет следующие данные: • папка emm: ♦ `omp-emm-client.db` (база данных приложения «Аврора Центр»); ♦ ompstorage2.ini; • папка push: ♦ applications.db; ♦ device_key; ♦ push-daemon.ini; ♦ `logcat.log` - вывод команды "logcat -d"; ♦ `getprop.txt` - вывод команды "getprop"; ♦ `storage.txt` - вывод команды "df -h"; ♦ `features.txt` - вывод команды "pm list features"; ♦ `packages.txt` - вывод команды "pm list packages -i"; ♦ `services.txt` - вывод команды "service list"; ♦ `processes.txt` - вывод команды "ps -e". **ПРИМЕЧАНИЕ.** В обычном режиме файл `logcat.log` содержит логи только приложения «Аврора Центр». Для получения логов всего устройства необходимо приложению «Аврора Центр» выдать специальный доступ и перезапустить устройство. Необходимо						

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
	использовать команду `adb shell "pm grant ru.omp.services android.permission.READ_LOGS"`. Команда выполняется через режим разработчика. Разница между logcat и отчетом об ошибке: ✓ **Logcat** представляет собой журнал сообщений устройства с ОС Android и приложений на нем. Сообщения расположены в хронологическом порядке, что помогает восстановить последовательность событий и выявить причино-следственную связь возникших проблем. ✓ **Отчет об ошибке** представляет собой снимок состояния устройства на момент формирования отчета. Он содержит более широкий набор сведений о системе, процессах, сервисах и сбоях. – устройство на базе **ОС семейства Linux** соберет данные: • логи приложения «Аврора Центр»: файл `omp-uem-agent.db` (база данных приложения «Аврора Центр»), файл `journalctl.log` (логи `journalctl` за выбранный период); • результат system-report; • версия ОС; • ядро; • подключенные репозитории; • информация о PCI устройствах; • данные о дисках; • результат диагностического скрипта (если был прикреплен); • для устройств с ОС Альт Linux, на которые было назначено правило политики по обновлению ОС (пп. 2.4.1.40), дополнительно будет сформирован список пакетов к установке, обновлению, удалению и список обновленных, установленных, удаленных пакетов за последние 30 дней. Файл формата CSV (`os-update- report.csv`). **ПРИМЕЧАНИЕ.** При формировании отчета по обновлению ОС «виртуальные» пакеты и их пакеты – провайдеры будут располагаться в разных строках. Поэтому могут быть ситуации, когда был запланирован к установке пакет-провайдер, а в результате установился «виртуальный» пакет и в отчете будут две строки с несоответствием в каждой. «Виртуальный» пакет - это пакет, который сам по себе не предоставляет контента, а используется для корректной установки/удаления «провайдящих» его пакетов. Например, виртуальный пакет mail «провайдит» пакеты gmail и supermail (и при установке виртуального пакета mail будет выбран пакет gmail или supermail). Подробнее о «виртуальных» пакетах см. Virtual packages). Архив загрузится во вкладку «Файлы» карточки устройства в течение нескольких минут. **ПРИМЕЧАНИЕ.** Подробная информация по работе со вкладкой «Файлы» приведена пп. 2.1.1.12						

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
Пароль админа	Установка одноразового пароля администратора для разблокировки устройства, если пользователь не знает или не может вспомнить пароль. Пароль должен содержать от 7 до 12 символов. После установки пароля администратор должен загрузить устройство в режиме администратора, ввести одноразовый пароль на устройстве, затем выбрать предлагаемый устройством новый пароль или самостоятельно задать новый пароль. Если учетная запись администратора была заблокирована на устройстве (в процессе ускоренной активации при применении политики создания пользователя), после установки одноразового пароля учетная запись администратора будет разблокирована	4.0.2 и выше	-	-	-	-	-
Пароль пользователя	Установка одноразового пароля пользователя для разблокировки устройства, если пользователь не знает или не может вспомнить пароль. Пароль должен соответствовать требованиям парольной политики и содержать от 7 до 12 символов. После установки пароля пользователю необходимо выполнить вход под своей учетной записью, ввести одноразовый пароль, затем выбрать предлагаемый устройством новый пароль или самостоятельно задать новый пароль	4.0.2 и выше	-	-	-	-	-
Экран	Блокировка экрана устройства для предотвращения его использования посторонними лицами в случае утери или кражи. **ВНИМАНИЕ!** Автоматической разблокировки/блокировки устройства по истечении установленного времени не предусмотрено. Для того чтобы по истечению счетчика оперативной команды устройство возвратилось в исходное состояние, необходимо предварительно создать и назначить политику на устройство с противоположным действием. **ПРИМЕЧАНИЕ.** Для устройств на базе ОС семейства Linux функционал приведен в документе «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux». Выбор значения из списка: – «Временная блокировка» – указание периода блокировки устройства. Ввод значения с клавиатуры в формате: «[дд] : [чч] : [мм]». Также доступна возможность ввода сообщения в поле «Сообщение при блокировке», которое будет отображаться на экране заблокированного устройства; – «Временная разблокировка» – период разблокировки устройства. Ввод значения с клавиатуры в формате: «[дд] : [чч] : [мм]». В результате блокировки устройства на экране блокировки отображается сообщение: «Заблокировано при помощи Aurora Device Manager. Заблокировано администратором». Использование устройства до разблокировки невозможно, кроме совершения экстренного вызова.	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
	ВНИМАНИЕ. После окончания периода действие оперативной команды сохраняется. Поэтому необходимо убедиться, что на устройство назначена политика (или действующий офлайн-сценарий) с противоположным эффектом						
Камера	Установка запрета/разрешения использовать камеру на устройствах. **ВНИМАНИЕ!** Автоматической разблокировки/блокировки камеры по истечении установленного времени не предусмотрено. Для того чтобы по истечению счетчика оперативной команды устройство возвратилось в исходное состояние, необходимо предварительно создать и назначить политику на устройство с противоположным действием. Выбор значения из списка: – «Временно запретить» – указать временной интервал, в течение которого использование камеры на устройстве будет запрещено. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]»; – «Временно разрешить» – указать временной интервал, в течение которого использование камеры на устройстве будет разрешено. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]». **ВНИМАНИЕ.** После окончания периода действие оперативной команды сохраняется. Поэтому необходимо убедиться, что на устройство назначена политика (или действующий офлайн-сценарий) с противоположным эффектом	4.0.2 и выше	7 и выше	-	-	-	-
Микрофон	Установка запрета/разрешения использование микрофона на устройствах. **ВНИМАНИЕ!** Автоматической разблокировки/блокировки микрофона по истечении установленного времени не предусмотрено. Для того чтобы по истечению счетчика оперативной команды устройство возвратилось в исходное состояние, необходимо предварительно создать и назначить политику на устройство с противоположным действием. Выбор значения из списка: – «Временно запретить» – указать временной интервал, в течение которого использование микрофона на устройстве будет запрещено. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]». **ПРИМЕЧАНИЕ.** При запрещающей команде микрофон будет недоступен для записи звука во всех приложениях и внешних устройствах, которые управляют им (наушники, гарнитуры и т.п.), но будет доступен для исходящих и входящих вызовов; – «Временно разрешить» – указать временной интервал, в течение которого использование микрофона на устройстве будет разрешено. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]». **ВНИМАНИЕ.** После окончания периода действие оперативной команды сохраняется. Поэтому необходимо убедиться, что на устройство назначена политика (или действующий офлайн-сценарий) с противоположным эффектом	4.0.2 и выше	-	-	-	-	-

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
События безопасности	Установка расписания отправки сообщений о произошедших на устройствах событиях безопасности. Выбор значения из списка: – «Временная установка» – сообщения доставляются по заданному расписанию и в течение указанного периода. Ввод значений с клавиатуры в формате: «[дд] : [чч] : [мм]»; – «Отменить отправку» – на устройствах применяются назначенные политики или настройки по умолчанию, если политик не назначено	4.0.2 и выше	-	-	-	-	-
Очистить устройство	Очистка всех данных пользователя для сохранения конфиденциальности данных в случае утери или кражи устройства. **ВНИМАНИЕ!** ✓ Перед очисткой устройства с ОС Android необходимо удалить все аккаунты в настройках устройства вручную. В противном случае после очистки и первоначальной настройки устройства ОС может запросить ввод PIN-кода, которым устройство было защищено до очистки; ✓ Не рекомендуется прерывать процесс очистки, т.к. для последующего включения устройства потребуется переустановка ОС; ✓ Данные с внешнего носителя (карты памяти MicroSD) будут удалены в случае, если это позволяет ОС. После завершения очистки на устройстве восстанавливаются заводские настройки. При активации устройства после полной очистки на него будут распространяться все политики, ранее назначенные на группы устройств или группы пользователей, в которые входит данное устройство	4.0.2 и выше	7 и выше	-	-	-	-
Откат на точку восстановления	**ПРИМЕЧАНИЯ:** ✓ Команда оперативного управления «Откат на точку восстановления» доступна только для устройств ОС семейства Linux (кроме ОС Astra Linux) и применима только для устройств с файловой системой BTRFS; ✓ Откат можно выполнить только на точки, созданные приложением «Аврора Центр»; ✓ Команда сработает только при наличии связи с приложением «Аврора Центр» на устройстве. Заполнить следующие поля: – «Причина отката» – ввести причину отката (например: «Ошибочное назначение политики с обновлением версии Приложения»). Поле обязательно для заполнения; – «Дата нужной точки отката» – ввести дату нужной точки отката в формате ДД.ММ.ГГГГ. По умолчанию установлена текущая дата; – «Время нужной точки отката» – ввести время нужной точки отката в формате ЧЧ:ММ. По умолчанию установлено текущее время.	-	-	Рабочая станция 10К и 11К	-	22 LTS	7.3.4

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
	После введения данных нажать на кнопку «Активировать изменения» и при наличии связи сервера с приложением «Аврора Центр» устройство найдет нужную точку восстановления и начнет делать откат на нее. **ВНИМАНИЕ!** Откат не произойдет точно на выбранные дату и время, вместо этого устройство выберет точку восстановления, максимально близкую к введенным значениям. **Логика создания точек восстановления.** При создании точки восстановления система автоматически записывает локальные дату и время устройства. Если на момент создания точки восстановления дата и время устройства были изменены вручную, в дальнейшем это может привести к некорректному откату на такие точки. Это связано с тем, что при формировании оперативной команды система «вписывает» значение серверного времени, но точка создается по локальному времени устройства. Например, если на устройстве вручную выставлено 17.03.2024, а серверная дата 17.03.2025, то это резервное копирование данных станет «актуальным» через год. **Логика выбора времени и даты точки восстановления при откате.** Если дата и время устройства не были изменены вручную при создании точек восстановления, логика выбора будет следующей: – на устройстве установлен часовой пояс UTC+7 (+4 к московскому времени), а дата и время синхронизированы с сервером; – на устройстве созданы две точки восстановления: • 17.03.2025-05:00 (по времени устройства, что соответствует 01:00 по Москве); • 17.03.2025-09:00 (по времени устройства, что соответствует 05:00 по Москве). Если администратор, находящийся в часовом поясе UTC+3, отправляет команду с указанием времени **17.03.2025-05:00**, система выполнит откат на точку **17.03.2025-09:00**, так как это соответствует указанному администратором времени с учетом разницы в часовых поясах						
Геопозиционирование	Временное выключение или включение геопозиционирования (с высокой точностью) на устройстве. **ВНИМАНИЕ!** Автоматического возвращения геопозиционирования в начальное состояние по истечении установленного времени не предусмотрено. Для того чтобы по истечению счетчика оперативной команды устройство возвратилось в исходное состояние, необходимо предварительно создать и назначить политику на устройство с противоположным действием. Для применения команды необходимо выполнить следующие действия: 1) В раскрывающемся списке «Состояние геопозиционирования» выбрать одно из значений: – «Временно включить геопозиционирование с высокой точностью».	4.0.2 и выше	7 и выше	-	-	-	-

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
	ВНИМАНИЕ! При использовании режима «Геопозиционирование с высокой точностью» расход заряда аккумулятора увеличен; – «Временно выключить». При инициировании команды выбрано по умолчанию; 2) В поле «Время действия» указать временной интервал (в формате: [дд] : [чч] : [мм]), в течение которого будет действовать выбранная опция; 3) Нажать «Активировать изменения». В результате геопозиционирование на устройстве будет включено или выключено (согласно выбранной опции) на указанный период времени. **ВНИМАНИЕ!** После окончания периода эффект команды оперативного управления сохраняется. При необходимости убедиться, что на устройство назначена политика с противоположным эффектом. **ПРИМЕЧАНИЯ**: ✓ Скорость определения геопозиции устройством зависит от факторов, на которые система не может повлиять; ✓ Получить текущую геопозицию устройства после применения оперативной команды возможно: – обновив состояние вручную через оперативное управление; – автоматически по расписанию при обновлении состояния устройства						
Сбросить пароль	Выключение пароля на устройстве подразумевает под собой сброс пароля. После успешного сброса пароля, если на устройство не была назначена политика с требованиями к паролю, будут установлены требования к паролю по умолчанию: – сложность – обычная; – количество символов – 7; – количество дней – 180. **ВНИМАНИЕ!** Выключение пароля (сброс пароля) доступно только для устройств с ОС Android версии 8 и выше. Возможность сброса пароля администратором зависит от того, когда было установлено приложение «Аврора Центр» и когда был задан пароль. Просмотр возможности сброса пароля доступен в карточке устройства. Для этого во вкладке «Состояние» необходимо выбрать «Все» и в разделе «Пользователь» проверить наличие параметра «Управление сбросом пароля». Возможные значения: – «Активировано». Отображается, если приложение «Аврора Центр» установлено и запущено до установки пароля. В таком случае функция сброса пароля активируется автоматически; – «В ожидании подтверждения пароля». Пароль на устройстве был установлен во время начальной настройки устройства (Startup Wizard) после установки приложения «Аврора Центр» через QR-код. Тогда токен безопасности не успевает активироваться. В журнале приложения «Аврора Центр» появится сообщение «Ошибка активации функции сброса	-	8 и выше	-	-	-	-

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
	пароля». На устройстве отобразится несбрасываемое уведомление «Требуется подтверждение пароля». Для активации функции сброса пароля необходимо нажать на уведомление и ввести текущий пароль устройства; – «В ожидании сброса устройства». Пароль на устройстве был установлен до установки приложения «Аврора Центр». В этом случае регистрация токена сброса пароля невозможна. Единственный способ сброса пароля — сброс устройства до заводских настроек с последующей установкой приложения «Аврора Центр» перед установкой нового пароля; – «Не поддерживается». Отображается для устройств, функционирующих на ОС Аврора, ОС Android либо ОС семейства Linux версии 7 и ниже; – «Ошибка активации» – отображается при возникновении ошибок во время активации функции сброса пароля. В этом случае необходимо собрать системные сообщения с устройства (подробнее в приложении документа «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android») и отправить их в запросе в техническую поддержку пользователя или в техническую поддержку компании ООО «Открытая мобильная платформа»; – «Неизвестно». Отображается при неудачных попытках чтения записей из базы данных. В этом случае необходимо собрать системные сообщения с устройства (подробнее в приложении документа «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android»)						
Перезагрузка	Для применения команды необходимо: – в поле «Максимальное время выполнения команды» указать временной интервал (в формате: [чч] : [мм]), в течение которого необходимо запустить перезагрузку устройства. По умолчанию установлена 1 минута; – нажать «Перезагрузить». В результате команда по перезагрузке будет отправлена на устройство. Начнется отсчет времени на ее выполнение. Если максимальное время выполнения команды не превышено, то перезагрузка будет выполнена сразу после доставки и обработки команды на устройстве. **ПРИМЕЧАНИЕ**. Активный входящий и исходящий вызов препятствует выполнению перезагрузки. **ВНИМАНИЕ!** Выделенного времени в одну минуту может оказаться недостаточно для завершения команды перезагрузки, поскольку способность устройства обрабатывать и выполнять данную операцию зависит от его технических характеристик и скорости работы. В этом случае перезагрузка не будет выполнена, будет получена ошибка «Истекло максимальное время на операцию». Это необходимо учитывать при выставлении максимального времени выполнения перезагрузки в команде оперативного управления	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4

Оперативная команда	Описание	Версии ОС					
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС
Режим киоска	Временное отключение режима киоска на устройстве. Для применения команды необходимо: – в раскрывающемся списке «Действие» выбрать «Временно выключить»; – в поле «Время действия» ввести временной интервал, на который нужно выключить режим киоска, в формате [чч] : [мм] (по умолчанию установлена 1 минута); – нажать «Активировать изменения». В результате режим киоска будет выключен на устройстве в течение указанного времени. Чтобы отменить временное выключение режима киоска, необходимо в раскрывающемся списке «Действие» выбрать «Отменить выключение» и нажать «Активировать изменения». Временное выключение режима киоска будет отменено. **ВНИМАНИЕ!** Автоматического включения режима киоска по истечении установленного времени или после отмены действия оперативной команды не предусмотрено. Чтобы по истечению счетчика (или после отмены) оперативной команды устройство вернулось в режим киоска, необходимо предварительно создать и назначить политику на устройство с включенным режимом киоска	5.2.0 и выше	7 и выше	-	-	-	-
Запустить сбор логов	**ВНИМАНИЕ!** Получение архива полного отчета об ошибках(запущенный logcat) осуществляется через оперативную команду «Диагностика». Сбор логов (logcat) – это системный журнал на ОС Android. Он содержит расположенные в хронологическом порядке сообщения операционной системы, системных сервисов и приложений. Журнал не ограничивается событиями мобильного приложения «Аврора Центр». Сбор логов позволяет сохранить данные за заданный период и включить их в диагностический отчет. Сбор начинается после получения команды устройством и продолжается до окончания указанного периода. Для применения команды необходимо: – в поле «Период сбора» ввести диапазон времени сбора «С» и «До». По умолчанию устанавлен диапазон в 24 часа от текущей даты и времени; **ПРИМЕЧАНИЯ:** ✓ Сбор логов начнется только после получения оперативной команды устройством. Данные за предшествующий период получены не будут; ✓ Период сбора должен состалять не меньше 1 минуты и больше 1 недели (или же 168 часов). – в поле «Максимальный объем лога, МБ» указать максимальный размер сохраняемых логов. По умолчанию устанавлен объем равный 1024 МБ (доступный объем от 1 до 4096 МБ). **ВНИМАНИЕ!** Если объем логов достиг указанного максимального значения до окончания периода сбора, применяется механизм ротации: новые записи продолжают сохраняться, а ранее собранные данные начинают перезаписываться. Например, если максимальный объем установлен равным 4096 МБ, что равно 4 ГБ и этот объем достигнут до окончания периода сбора, устройство продолжит сбор логов с перезаписью ранее сохраненных данных. В диагностический отчет войдут данные, которые сохранились на устройстве к моменту формирования отчета.	-	7 и выше	-	-	-	-

2.2.12. Отвязка (исключение) устройств из группы устройств

ВНИМАНИЕ! Невозможно исключить устройства из динамической группы устройств.

Для динамической группы устройств исключение устройств происходит автоматически в случае нарушения условий пребывания в группе.

Исключить устройства из статической группы возможно через:

– карточку устройства (пп. 2.2.12.1);

– каточку группы устройств (пп. 2.2.12.2).

2.2.12.1.Исключение устройства из группы устройств через карточку устройства

Для исключения устройства из группы устройств через карточку устройства необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– для отображения списка устройств выбрать в области фильтров «Поиск по устройствам»;

– найти требуемое устройство, при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок в столбце «Карточка» для перехода в карточку устройства;

– перейти во вкладку «Группы»;

– выбрать группу устройств, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение»;

– в списке быстрых действий нажать значок «Исключить устройство из группы»;

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия.

В результате успешного подтверждения, политики будут перекомбинированы таким образом, что для устройства будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.2.12.2.Отвязка устройств от группы устройств через карточку группы устройств

В статической группе устройств отвязать устройство возможно через карточку группы устройств, выполнив следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в карточке группы устройства перейти во вкладку «Устройства»;

– выбрать устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение»;

– в списке быстрых действий нажать значок «Отвязать устройства от группы»;

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия.

В результате успешной отвязки устройства от группы отобразится соответствующее сообщение, политики будут перекомбинированы таким образом, что для устройств будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.2.13. Архивирование устройства

Под архивированием подразумевается удаление из списка добавленных устройств, после чего устройство повторно добавить в Консоль администратора ПУ невозможно, а возможно только восстановить. Подробное описание восстановления устройства из архива приведено в пп. 2.2.14.

Перед архивированием активированного устройства необходимо очистить его с помощью оперативных команд (п. 2.2.11).

Архивирование устройства может быть выполнено:

– в подразделе «Устройства» с помощью списка быстрых действий (пп. 2.2.13.1);

– с помощью карточки устройства (пп. 2.2.13.2).

2.2.13.1.Архивирование устройства с помощью списка быстрых действий

Для архивирования устройства необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по устройствам»;

– выбрать устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Архивировать»;

– если выбранные устройства были очищены, то отобразится окно подтверждения операции, где необходимо нажать кнопку «Архивировать».

Если одно или несколько устройств не очищены, отображается сообщение, в котором необходимо выбрать соответствующую кнопку:

– для архивирования только очищенных устройств нажать кнопку «Архивировать только очищенные»;

– для архивирования без очистки необходимо:

- установить галочку в чекбоксе «Я хочу архивировать все без очистки»;
- нажать кнопку «Архивировать все».

В результате успешного архивирования устройства отобразится соответствующее сообщение, учетные записи устройства будут заблокированы.

ПРИМЕЧАНИЕ. Архивные устройства будут отображаться в списке устройств, если включена соответствующая настройка (п. 4.1.3).

2.2.13.2.Архивирование устройства из карточки устройства

Для архивирования устройства из карточки необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– для отображения списка устройств выбрать в области фильтров «Поиск по устройствам»;

– найти требуемое устройство, при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок в столбце «Карточка» для перехода в карточку устройства;

– перейти во вкладку «Состояние»;

– нажать на значок (см. Рисунок 9 [3]) и выбрать «Архивировать»;

– если устройство не очищено, отобразится соответствующее сообщение. Для подтверждения архивирования необходимо нажать кнопку «Архивировать».

В результате успешного архивирования устройства отобразится соответствующее сообщение, учетные записи устройства будут заблокированы.

ПРИМЕЧАНИЕ. Архивные устройства будут отображаться в списке устройств, если включена соответствующая настройка (п. 4.1.3).

2.2.14. Восстановление устройств из архива

Для отображения архивных устройств в подразделе «Устройства» в настройках должен быть активен переключатель «Отображать архивные устройства» (п. 4.1.3).

При восстановлении устройств из архива восстанавливаются все его связи с группами и пользователями.

Для восстановления устройства из архива необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– выбрать архивное устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– выбрать значок «Активировать»;

– в отобразившемся окне активации устройств установить галочку в чекбоксе «Перенесено в архив» (Рисунок 59 [1]) и нажать кнопку «Дальше»(Рисунок 59 [2]);

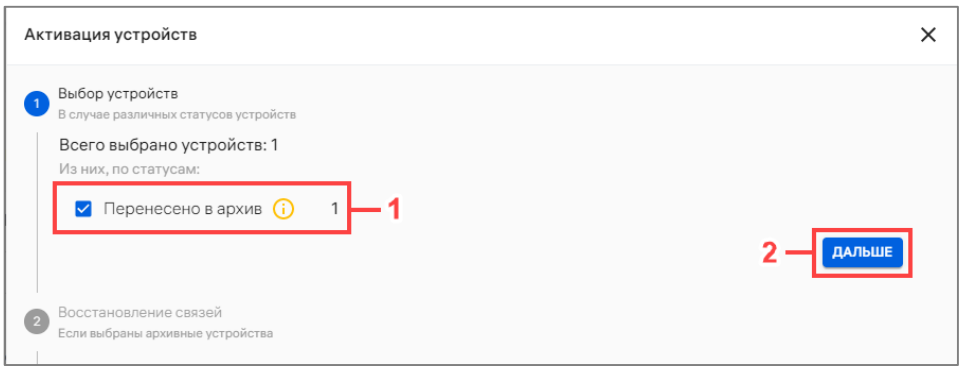


Рисунок 59

– при наличии у устройств связей со статистическими группами и/или пользователями на шаге «Восстановление связей» необходимо подтвердить восстановление связей, установив галочку в чекбоксе (Рисунок 60 [1]), и нажать кнопку «Дальше» (Рисунок 60 [2]). Данный шаг подразумевает восстановление связей с группами устройств и пользователями и применение соответствующих политик и офлайн-сценариев. При отсутствии необходимости восстановления связей, установка галочки в чекбоксе на «Восстановить все связи» не является обязательной;



Рисунок 60

– для ОС Android в отобразившемся окне (см. Рисунок 52) возможно дополнительно указать сеть WLAN и часовой пояс, выполнив действия, приведенные в п. 2.2.4 и нажать кнопку «Дальше».

Далее активировать устройства возможно одним из способов:

– нажать кнопку «Активация вручную» (Рисунок 61 [1]) и далее нажать кнопку «Продолжить»;

– нажать кнопку «Отправить на Email» (Рисунок 61 [2]), в открывшемся окне ввести адрес электронной почты и далее нажать кнопку «Отправить».

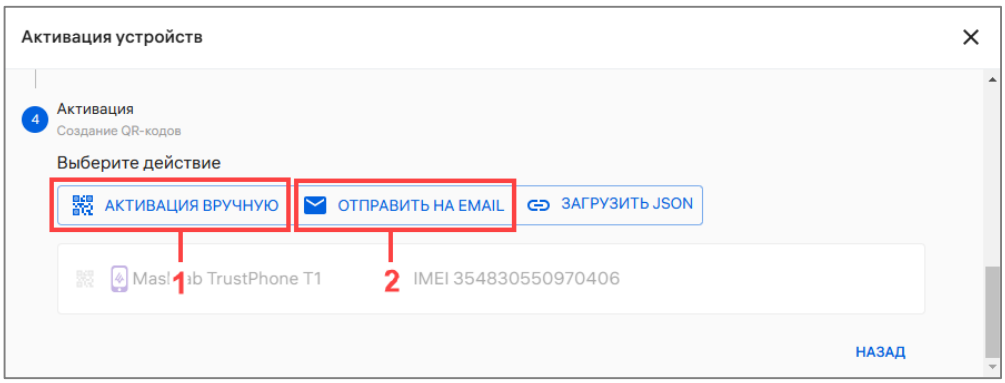


Рисунок 61

В результате будет сгенерирован и отображен QR-код для активации и отобразятся сообщения «Связи архивных устройств восстановлены» и «Процесс создания учетных записей устройств запущен».

Для завершения активации необходимо отсканировать QR-код на устройстве. Описание процесса активации устройств приведено в документах:

– «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора»;

– «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android».

2.2.15. Удаление устройства

ПРИМЕЧАНИЕ. Удаление устройства из ПУ доступно только для пользователей с ролью «Администратор Платформы управления» или «Администратор устройств Платформы управления» или «Специалист технического обслуживания устройств Платформы управления».

В Консоли администратора ПУ предусмотрена возможность удаления устройства одним из следующих способов:

– вручную из карточки устройства (пп. 2.2.15.1), если необходимо удалить одно устройство;

– с помощью списка быстрых действий, если требуется удалить сразу несколько устройств (п. 2.2.15.2).

2.2.15.1.Удаление устройства из карточки устройства

ПРИМЕЧАНИЕ. Перед удалением устройства необходимо выполнить его очистку с помощью оперативной команды «Очистить устройство» (п. 2.2.11). Это позволит избежать утечки конфиденциальных данных с устройства.

Для удаления устройства из карточки необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– для отображения списка устройств выбрать в области фильтров «Поиск по устройствам»;

– найти требуемое устройство, при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок в столбце «Карточка» для перехода в карточку устройства;

– перейти во вкладку «Состояние»;

– нажать на значок (см. Рисунок 9 [3]) и выбрать «Удалить»;

– если устройство:

- очищено, то для подтверждения удаления нажать «Удалить»;
- не очищено, то для подтверждения удаления установить галочку в чекбоксе «Я хочу удалить все без очистки» и нажать «Удалить все».

В результате успешного удаления устройство будет удалено из ПУ.

Удаление устройства выполняется в два этапа (при такой реализации до выполнения второго этапа информация об устройстве частично может остаться в Консоли администратора ПУ и отчетах в Grafana):

– на первом этапе выполняется удаление основной информации об устройстве и данных из ПБ, которые могут помешать повторной активации устройства;

– на втором этапе выполняется полное удаление всех оставшихся данных, связанных с устройством. Второй этап выполняется в зависимости от настроек в файле конфигурации (по умолчанию через 24 часа).

ПРИМЕЧАНИЕ. Если существует требующая согласования «Заявка на активацию» с удаляемым устройством, которое имеет идентификатор, пересекающийся с идентификатором активируемого устройства, и это единственное устройство с пересечениями из заведенных в ПУ устройств, тогда при удалении устройства заявка на активацию автоматически будет переведена в статус «Нерелевантная».

2.2.15.2.Удаление устройства с помощью списка быстрых действий

ПРИМЕЧАНИЕ. Перед удалением устройства необходимо выполнить его очистку с помощью оперативной команды «Очистить устройство» (п. 2.2.11). Это позволит избежать утечки конфиденциальных данных с устройства.

Для удаления устройства необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по устройствам»;

– выбрать устройство, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Удалить»;

– если устройство:

- очищено, то для подтверждения удаления нажать «Удалить»;
- не очищено хотя бы одно из выбранных устройств, то отобразится соответствующее сообщение.

Если требуется:

– удалить только очищенные, то нажать «Удалить только очищенные»;

– удалить все выбранные устройства, то установить галочку в чекбоксе «Я хочу удалить все без очистки» и нажать «Удалить все».

В результате успешного удаления устройство будет удалено из ПУ.

Удаление устройства выполняется в два этапа (при такой реализации до выполнения второго этапа информация об устройстве частично может остаться в Консоли администратора ПУ и отчетах в Grafana):

– на первом этапе выполняется удаление основной информации об устройстве и данных из ПБ, которые могут помешать повторной активации устройства;

– на втором этапе выполняется полное удаление всех оставшихся данных, связанных с устройством. Второй этап выполняется в зависимости от настроек в файле конфигурации (по умолчанию через 24 часа).

ПРИМЕЧАНИЕ. Если существует требующая согласования «Заявка на активацию» с удаляемым устройством, которое имеет идентификатор, пересекающийся с идентификатором активируемого устройства, и это единственное устройство с пересечениями из заведенных в ПУ устройств, тогда при удалении устройства заявка на активацию автоматически будет переведена в статус «Нерелевантная».

2.2.16. Удаление группы устройств

ПРИМЕЧАНИЕ. Перед удалением группы устройств необходимо:

– предварительно исключить все устройства из группы (п. 2.2.12), а также удалить ее из всех множеств (пп. 2.2.6.1) – для статической группы устройств;

– отвязать группу устройств от всех политик (п. 2.4.7) и офлайн-сценариев (п. 2.5.3) – для динамической группы.

После выполнения условий, приведенных выше, статическая/динамическая группа может быть удалена из ПУ. Для этого необходимо:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы устройств для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в карточке группы устройств нажать на кнопку «Удалить»;

– в отобразившемся окне подтвердить либо отменить действия.

В результате успешного удаления отобразится соответствующее сообщение.

2.2.17. Очистка устройств до заводских настроек

ПРИМЕЧАНИЕ. Бизнес-сценарий по экстренному выводу устройства из эксплуатации недоступен для устройств на базе ОС семейства Linux.

Для сброса устройства до заводских настроек необходимо назначить оперативную команду «Очистка устройства» (см. Таблица 38) в соответствии с п. 2.2.11, в результате чего отобразится окно подтверждения операции, где необходимо нажать кнопку «Очистить».

В результате успешной очистки все данные пользователя устройства, включая данные с внешнего носителя (карта памяти microSD), удалятся.

ВНИМАНИЕ! Не рекомендуется прерывать очистку устройства, т.к. для последующего включения потребуется переустановка ОС.

После завершения очистки на устройстве будут восстановлены заводские настройки. Для управления очищенным устройством следует активировать его повторно (п. 2.2.10).

При активации устройства после полной очистки на нем будут действовать все политики, ранее назначенные на группы устройств или пользователей, в которые входит это устройство.

2.2.18. Вывод устройства из эксплуатации

ВНИМАНИЕ! Вывод из эксплуатации доступен для устройств в статусе жизненного цикла «Активировано». В иных случаях кнопка «Вывести из эксплуатации» будет не активна.

Для экстренного вывода устройства из эксплуатации необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– для отображения списка устройств выбрать в области фильтров «Поиск по устройствам»;

– найти требуемое устройство, при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок в столбце «Карточка» для перехода в карточку устройства;

– перейти во вкладку «Сценарии»;

– нажать кнопку «Вывести из эксплуатации»;

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия.

В результате успешного вывода устройства из эксплуатации в течение некоторого времени на устройстве будут выполнены следующие операции:

1) На устройствах с ОС Аврора и ОС Android:

– блокировка экрана (с выведением сообщения «Устройство выведено из эксплуатации»);

– очистка устройства (сброс к заводским настройкам);

– архивирование устройства (удаление из списка устройств);

2) На устройствах с ОС семейства Linux:

– если учетная запись пользователя создана через ППО (пользователь acuser), то происходит блокировка экрана (с сообщением «Устройство выведено из эксплуатации»). Иначе экран не блокируется;

– запуск очистки в 3 этапа:

• отмонтирование сетевых папок. Система отключает все подключенные сетевые ресурсы (NFS, SMB/CIFS и др.);

• затирание данных на всех найденных разделах `home` с использованием алгоритма `shred`;

• полная очистка дисков (`dd`). Все диски устройства перезаписываются нулями (`dd if=/dev/zero`) до тех пор, пока не очистятся критичные для работы ОС директории;

– архивирование (удаление из списка устройств).

ПРИМЕЧАНИЕ. В отличие от ОС Аврора и ОС Android, очистка устройства с ОС семейства Linux подразумевает полное удаление данных с устройства, в том числе ОС.

2.3. Подраздел «Пользователи»

Подраздел «Пользователи» Консоли администратора ПУ предназначен для управления пользователями или группами пользователей.

Для перехода в подраздел необходимо в верхней панели выбрать раздел «Управление», подраздел «Пользователи», в результате чего в рабочей области отобразится информация о пользователях или группах пользователей.

ПРИМЕЧАНИЕ. Для отображения группы пользователей необходимо в области фильтров выбрать «Поиск по группам».

В рабочей области информация о пользователях и группах пользователей отображается в столбцах, приведенных в таблице (Таблица 39), а при отсутствии добавленных пользователей или групп пользователей отображается сообщение «Нет данных».

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 39

Параметр	Описание
Пользователи	
Тип	Тип пользователя (Приложение 1)
Имя	Фамилия, имя и отчество пользователя (представляет собой активную ссылку, при нажатии на которую происходит переход к карточке пользователя)
Email	Электронная почта пользователя
Телефон	Номер телефона пользователя
Устройства	Количество устройств, привязанных к пользователю

Параметр	Описание
Группы	Количество групп, к которым привязан пользователь
Обновлено	Дата обновления
Группа пользователей	
Тип	Тип группы пользователей (Приложение 1)
Группа пользователей	– название группы пользователей (представляет собой активную ссылку, при нажатии на которую происходит переход к карточке группы пользователей); – комментарий – дополнительная информация (заполняется при необходимости)
Принцип добавления	Значение, по которому пользователи были добавлены в группу
Пользователей	Количество пользователей, привязанных к группе
Устройств	Количество уникальных устройств, привязанных к пользователям группы
Обновлено	Дата обновления группы

В Консоли администратора ПУ предусмотрена возможность добавления пользователей или групп пользователей одним из следующих способов:

– вручную (п. 2.3.1 и п. 2.3.2);
– с помощью импорта CSV-файла (п. 2.3.3);
– с помощью импорта из LDAP-сервера (пп. 4.1.5.3.1.1).

2.3.1. Добавление пользователя устройства вручную

Для добавления пользователя вручную необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;
– нажать кнопку «Добавить»;
– в раскрывающемся списке выбрать пункт «Добавить пользователя» (Рисунок 62);

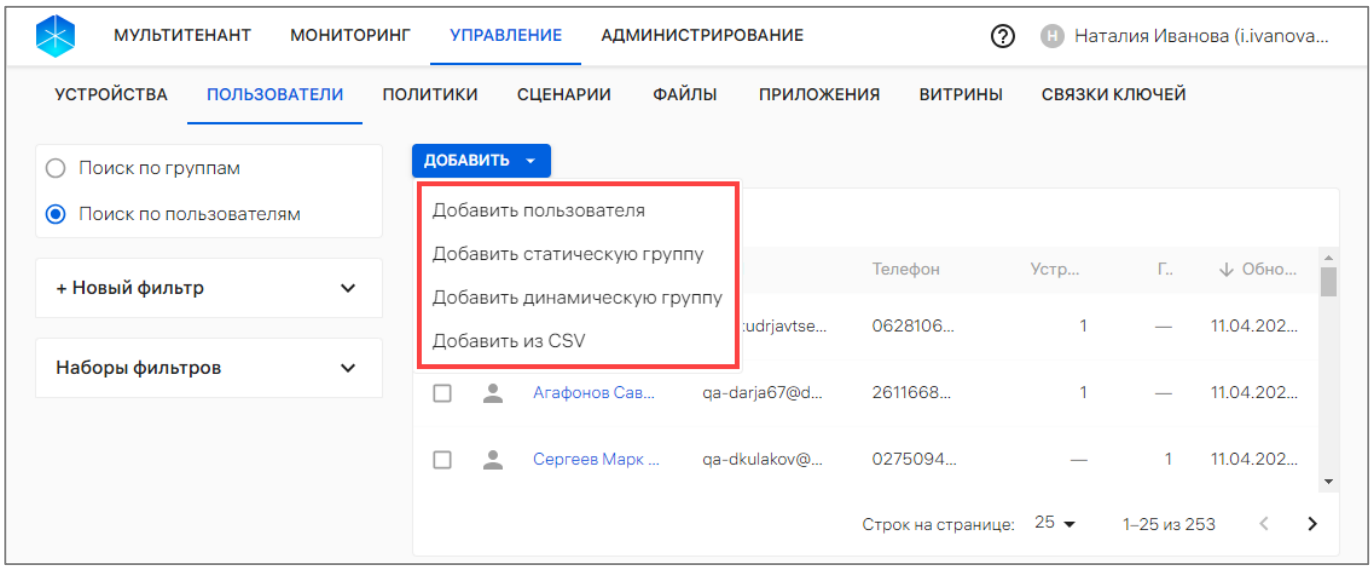


Рисунок 62

– в открывшемся окне ввести данные о пользователе (Таблица 40);

Таблица 40

Поле ввода	Значение	Примечание
Фамилия	Фамилия пользователя	Поле не обязательно для заполнения. Может содержать буквы, цифры и спецсимволы
Имя	Имя пользователя	Поле не обязательно для заполнения. Может содержать буквы, цифры и спецсимволы
Отчество	Отчество пользователя	Поле не обязательно для заполнения. Может содержать буквы, цифры и спецсимволы
Почта рабочая	Рабочий email пользователя	Поле обязательно для заполнения и является идентификатором пользователя Аврора Центр
Должность	Должность, занимаемая пользователем в компании	Поле не обязательно для заполнения
Телефон рабочий	Номер рабочего телефона пользователя	Поле не обязательно для заполнения

– после заполнения полей подтвердить либо отменить создание пользователя.

В результате успешного добавления пользователя отобразится соответствующее сообщение и откроется его карточка. Описание процесса работы с карточкой пользователя приведено в п. 2.1.3.

2.3.2. Добавление группы пользователей вручную

При добавлении группы пользователей вручную доступно:
– добавление статической группы пользователей (пп. 2.3.2.1);
– добавление динамической группы пользователей (пп. 2.3.2.2).

2.3.2.1. Добавлене статической группы пользователей

ПРИМЕЧАНИЕ. Состав правил статической группы Администратор может редактировать вручную.

Для добавления статической группы пользователей необходимо выполнить следующие действия:
– перейти в подраздел «Пользователи» раздела «Управление»;
– нажать кнопку «Добавить»;
– в раскрывающемся списке выбрать пункт «Добавить статическую группу» (см. Рисунок 62);
– в открывшемся окне заполнить поля (Таблица 41).

Таблица 41

Поле ввода	Значение	Примечание
Имя группы	Название группы пользователей	Поле обязательно для заполнения. Название группы пользователей должно быть уникальным
Комментарий	Дополнительная информация к группе пользователей	Поле не обязательно для заполнения

– нажать кнопку «Создать».

В результате успешного создания группы пользователей отобразится соответствующее сообщение и откроется карточка добавленной группы пользователей. Подробное описание работы с карточкой группы пользователей приведено в п. 2.1.4.

2.3.2.2. Добавление динамической группы пользователей

Динамическая группа – группа с заданными условиями, при соблюдении которых пользователи попадают в группу автоматически.

ПРИМЕЧАНИЕ. Нельзя создать несколько динамических групп с одинаковыми условиями. В случае попытки создания еще 1 динамической группы отобразится сообщение об ошибке. Такую группу невозможно удалить (кнопка «Удалить» неактивна).

ПРИМЕЧАНИЕ. Перед тем, как создать динамическую группу пользователей, необходимо настроить интеграцию с сервером LDAP (пп. 4.1.5.3).

Для добавления динамической группы необходимо выполнить следующие действия:

1) Перейти в подраздел «Пользователи» раздела «Управление»;
2) Нажать кнопку «Добавить»;

3) В раскрывающемся списке выбрать пункт «Добавить динамическую группу» (см. Рисунок 62);

4) В открывшемся окне заполнить поля, приведенные в таблице (см. Таблица 41);

5) В блоке «Принцип добавления в группу» в раскрывающемся списке «Атрибут пользователя LDAP» выбрать нужный атрибут и затем задать его значение одним из способов:

– если требуется выполнить поиск по точному совпадению атрибута, в поле «Значение» ввести необходимое значение атрибута;

– если требуется задать регулярное выражение для поиска, установить галочку в чекбоксе «Регулярное выражение» и в поле «Значение» ввести необходимое регулярное выражение.

ВНИМАНИЕ! При использовании регулярного выражения необходимо учитывать следующие ограничения:

– регулярное выражение должно быть задано по POSIX стандарту;

– возможен отказ в обслуживании с помощью регулярного выражения (https://en.wikipedia.org/ wiki/ReDoS) посредством Администратора Платформы управления;

– не определена производительность создания динамических групп пользователей с помощью регулярного выражения, например, при наличии в базе данных десятков тысяч пользователей;

6) Нажать кнопку «Создать».

В результате успешного создания группы пользователей отобразится соответствующее сообщение и откроется карточка добавленной группы пользователей. Подробное описание работы с карточкой группы пользователей приведено в п. 2.1.4.

2.3.2.2.1. Редактирование динамической группы пользователей

Для изменения названия и/или комментария к динамической группе пользователей, а также изменения ее критериев необходимо:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– нажать на значок ✎ «Редактировать» и при необходимости внести изменения в полях, приведенных в таблице (см. Таблица 41);

– в раскрывающемся списке «Атрибут пользователя LDAP» выбрать нужный атрибут и затем задать его значение одним из способов:

- в поле «Значение» ввести необходимое значение атрибута, если требуется выполнить поиск по точному совпадению атрибута;

- установить галочку в чекбоксе «Регулярное выражение» и в поле «Значение» ввести необходимое регулярное выражение, если требуется задать регулярное выражение для поиска.

ВНИМАНИЕ! При использовании регулярного выражения необходимо учитывать следующие ограничения:

✓ Регулярное выражение должно быть задано по POSIX стандарту;

✓ Возможен отказ в обслуживании с помощью регулярного выражения (https://en.wikipedia.org/wiki/ ReDoS) посредством Администратора Платформы управления;

✓ Не определена производительность создания динамических групп пользователей с помощью регулярного выражения, например, при наличии в базе данных десятков тысяч пользователей;

– нажать кнопку «Сохранить».

В результате изменения динамической группы будут применены. При изменении критериев состав группы пользователей будет обновлен.

2.3.3. Добавление пользователей или группы пользователей с помощью CSV-файла

Добавление и обновление, а также привязку пользователей или групп пользователей в ПУ, можно выполнить с помощью подготовленного шаблона импорта. Шаблон предоставляется в виде CSV-файла.

2.3.3.1. Шаблон CSV-файла

CSV-файл возможно создать вручную или скачать и заполнить шаблон.

Для загрузки шаблона CSV-файла необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить из CSV» (см. Рисунок 62);

– в открывшемся окне нажать «Шаблон .CSV ⭳» (Рисунок 63), в результате шаблон файла для импорта будет выгружен на ЭВМ. Требования к заполнению CSV-файлов приведены в таблице (Таблица 42).

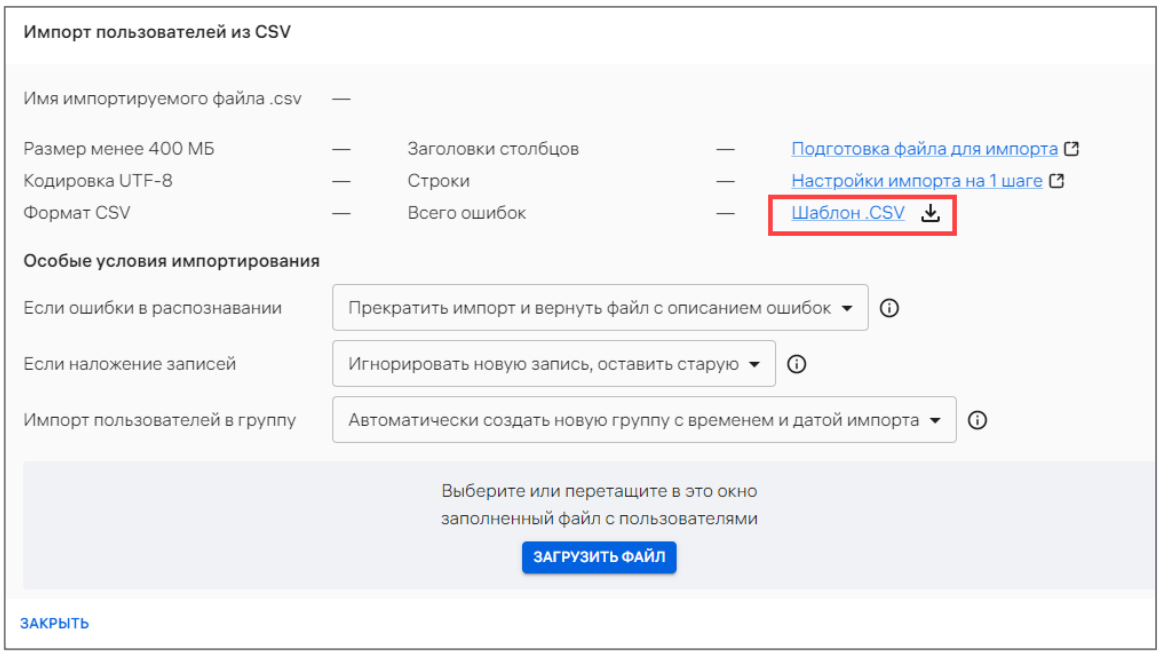


Рисунок 63

Пример заполненного CSV-файла:

```
GROUP,EMAIL,FIRST_NAME,LAST_NAME,PATRONYMIC,JOB_TITLE,PHONE_NUMBER,IMEI,SN,ETHERNET_MAC,WLAN_MAC
Пользователи INOI T10,i.ivanov@doc.ru,Игорь,Иванов,,Дежурный,9000900000,350081328638495,,,
Пользователи MIG C55,d.dolin@doc.ru,Дмитрий,Долин,,Руководитель,9000100000,350422453760656,,,
```

Также возможно заполнить CSV-файл в табличном виде (Рисунок 64).

Пример:

GROUP	EMAIL	FIRST_NAME	LAST_NAME	PATRONYMIC	JOB_TITLE	PHONE_NUMBER	IMEI	SN	ETHERNET_MAC	WLAN_MAC
Пользователи INOI T10	i.ivanov@doc.ru	Игорь	Иванов		Дежурный	9000900000	350081328638495			
Пользователи MIG C55	d.dolin@doc.ru	Дмитрий	Долин		Руководитель	9000100000	350422453760656			

Рисунок 64

ПРИМЕЧАНИЕ. При больших значениях чисел (например, IMEI) необходимо выбрать числовой формат ячейки и количество десятичных знаков, равное 0.

Файл для импорта должен соответствовать следующим требованиям:

– размер файла не должен превышать 400 МБ. Импортировать файл размером 400 МБ рекомендуется при скорости подключения к сети Интернет 100 Мбит/сек и выше. Если скорость подключения к сети Интернет менее 100 Мбит/сек, рекомендуется разделить файл на насколько частей и загружать их поочередно;

– формат файла – `.csv`;

– кодировка файла – UTF-8.

ПРИМЕЧАНИЕ. Скачанный шаблон CSV-файла имеет нужный формат и кодировку;

– первая строка файла должна содержать названия полей с разделителем (например, "GROUP,EMAIL,FIRST_NAME,LAST_NAME,PATRONYMIC,JOB_TITLE,PHONE_NUMBER,IMEI,SN,ETHERNET_MAC,WLAN_MAC,STRATEGY").

ПРИМЕЧАНИЕ. После столбца WLAN_MAC может быть добавлен необязательный столбец STRATEGY. Он заполняется в случае необходимости указать стратегию разрешения конфликтов для конкретной строки. Подробнее см. в описании столбца ниже.

Разделитель для всех полей файла определяется по первой строке. В качестве разделителей может использоваться любой символ, кроме: \r, \n и символа замены Unicode (0xFFFD). Если в качестве разделителя используются буквы, то они должны заключаться в кавычки, например: «a».

Описание требований к значениям параметров приведено в таблице (Таблица 42).

Таблица 42

Параметр	Описание	Примечание
GROUP	Название группы пользователей, к которой необходимо привязать пользователя. Содержит от 2 до 64 символов	Параметр обязателен для заполнения при: – создании группы пользователей; – привязке пользователя к существующей группе. **ПРИМЕЧАНИЕ.** Если в окне настройки импорта в особых условиях выбрана опция «Автоматически создать новую группу с временем и датой импорта» или «Выбрать группу из имеющихся», пользователь будет привязан и к новой/выбранной в опции группе, и к группе, указанной в файле
EMAIL	Рабочая почта пользователя. Должна быть уникальной для каждого пользователя и содержать 1 до 256 символов	Параметр обязателен для заполнения при: – добавлении нового пользователя; – привязке пользователя к группе
FIRST_NAME	Имя пользователя. Может содержать буквы, цифры и спецсимволы. Длина от 2 до 64 символов.	Параметр не обязателен для заполнения

Параметр	Описание	Примечание
LAST_NAME	Фамилия пользователя. Может содержать буквы, цифры и спецсимволы. Длина от 2 до 64 символов	Параметр не обязателен для заполнения
PATRONYMIC	Отчество пользователя. Может содержать буквы, цифры и спецсимволы. Длина от 2 до 64 символов	Параметр не обязателен для заполнения
JOB_TITLE	Должность пользователя в компании. Содержит следующие буквы и символы: а-я, А-Я, a-z, A- Z, дефис (-), апостроф (') и пробел. Длина от 2 до 64 символов	Параметр не обязателен для заполнения
PHONE_ NUMBER	Номер рабочего телефона пользователя. Содержит только цифры. Длина от 2 до 64 символов	Параметр не обязателен для заполнения
IMEI	Международный идентификатор мобильного оборудования. Содержит 15 цифр	Параметр обязателен для заполнения, если устройство с указанным IMEI необходимо привязать к пользователю
SN	Серийный номер, который присвоен устройству производителем. Содержит от 1 до 20 символов	Параметр обязателен для заполнения, если устройство с указанным серийным номером необходимо привязать к пользователю
ETHERNET_ MAC	MAC-адрес Ethernet устройства. Содержит 6 пар символов, разделенных двоеточием	Параметр обязателен для заполнения, если устройство с указанным MAC-адресом Ethernet необходимо привязать к пользователю
WLAN_MAC	MAC-адрес WLAN устройства. Содержит 6 пар символов, разделенных двоеточием, например: «00:aa:00:00:a0:00»	Параметр обязателен для заполнения, если устройство с указанным MAC-адресом WLAN необходимо привязать к пользователю

Параметр	Описание	Примечание
STRATEGY	Правило разрешения конфликтующих записей. Доступные значения: – **SKIP** или **S** – в результате конфликтующая запись не будет перезаписана. Если файл содержит несколько одинаковых записей о пользователе, но с разными группами, то будут созданы все связи пользователя с группами из файла; – **REPLACE** или **R** – в результате конфликтующая запись будет перезаписана. Если файл содержит несколько одинаковых записей о пользователе, но с разными группами, то пользователь будет отвязан от всех групп, в которых он состоял ранее в системе, и привязан ко всем группам из файла	Параметр не обязателен для заполнения. Параметр имеет приоритет по сравнению с правилом разрешения конфликтов, выбранным в окне настройки импорта

2.3.3.2. Добавление пользователей или группы пользователей с помощью CSV-файла

Для импорта пользователей и группы пользователей, а также привязки пользователей к группе пользователей в Консоли администратора ПУ необходимо выполнить следующие действия:

– подготовить CSV-файл для импорта (пп. 2.3.3.1);

– перейти в подраздел «Пользователи» раздела «Управление»;

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить из CSV» (см. Рисунок 62);

– в открывшемся окне задать особые условия импортирования, приведенные в таблице (Таблица 43);

Таблица 43

Наименование полей	Описание	Примечание
Если ошибки в распознавании	Выбор правила импортирования (если CSV-файл будет содержать ошибки) из раскрывающегося списка (Рисунок 65 [1]):	В поле содержится подсказка, доступная для

Наименование полей	Описание	Примечание
	– **Прекратить импорт и вернуть файл с описанием ошибок** – при обнаружении ошибок будет остановлен импорт и сформирован файл с перечислением некорректных строк и указанием причин ошибок; – **Продолжить импорт и вернуть два файла с ошибками и без** – импорт продолжится с корректными записями, и после его завершения будут сформированы 2 файла: • файл с перечислением некорректных строк и указанием причин ошибок; • файл с указанием успешно импортированных устройств	просмотра при наведении курсора на значок (Рисунок 65 [1],[2]). В результате отобразится текст подсказки следующего содержания: «При завершении импорта система предоставит 2 файла: список системных сообщений ошибок распознавания и Журнал успешно импортированных устройств»
Если наложение записей	Выбор правила разрешения конфликтов при импорте из раскрывающегося списка (Рисунок 65 [2]): – **Игнорировать новую запись, оставить старую** – в результате конфликтующие записи не будут перезаписаны. Если файл содержит несколько одинаковых записей о пользователе, но с разными группами, то будут созданы все связи пользователя с группами из файла; – **Перезаписывать новую строку поверх прежней** – в результате конфликтующие записи будут перезаписаны. Если файл содержит несколько одинаковых записей о пользователе, но с разными группами, то пользователь будет отвязан от всех групп, в которые он входил, и привязан ко всем группам из файла. **ПРИМЕЧАНИЕ.** Если в CSV-файле заполнен столбец «STRATEGY», правило разрешения конфликтов из этого столбца будет иметь приоритет над указанным правилом при настройке импорта. Описание процесса	

Наименование полей	Описание	Примечание
	заполнения CSV-файла приведено в пп. 2.3.3.1	
Импорт пользователей в группу	Выбор правила добавления импортируемых устройств в группы из раскрывающегося списка (Рисунок 65 [3]): – **Автоматически создать новую группу с временем и датой импорта** – в результате будет создана новая группа пользователей (с типом  «Группа пользователей»), в которую будут включены все импортируемые пользователи. Если в CSV-файле для пользователя указана группа (значение в столбце «GROUP»), то такой пользователь будет включен в новую группу и в указанную в файле группу; – **Не создавать группу –** в результате пользователи будут добавлены только в группы, указанные в CSV-файле; – **Выбрать группу из имеющихся** – выберите из раскрывающегося списка группу, в которую необходимо включить импортированных пользователей. Если в CSV-файле для пользователя указана группа (значение в столбце «GROUP»), то пользователь будет включен как в группу, указанную в файле, так и в группу, выбранную на этом шаге	В поле содержится подсказка, доступная для просмотра при наведении курсора на значок  (Рисунок 65 [3]). В результате отобразится текст подсказки следующего содержания: «В процессе импорта система может помещать все устройства в одну из имеющихся групп или создать новую»

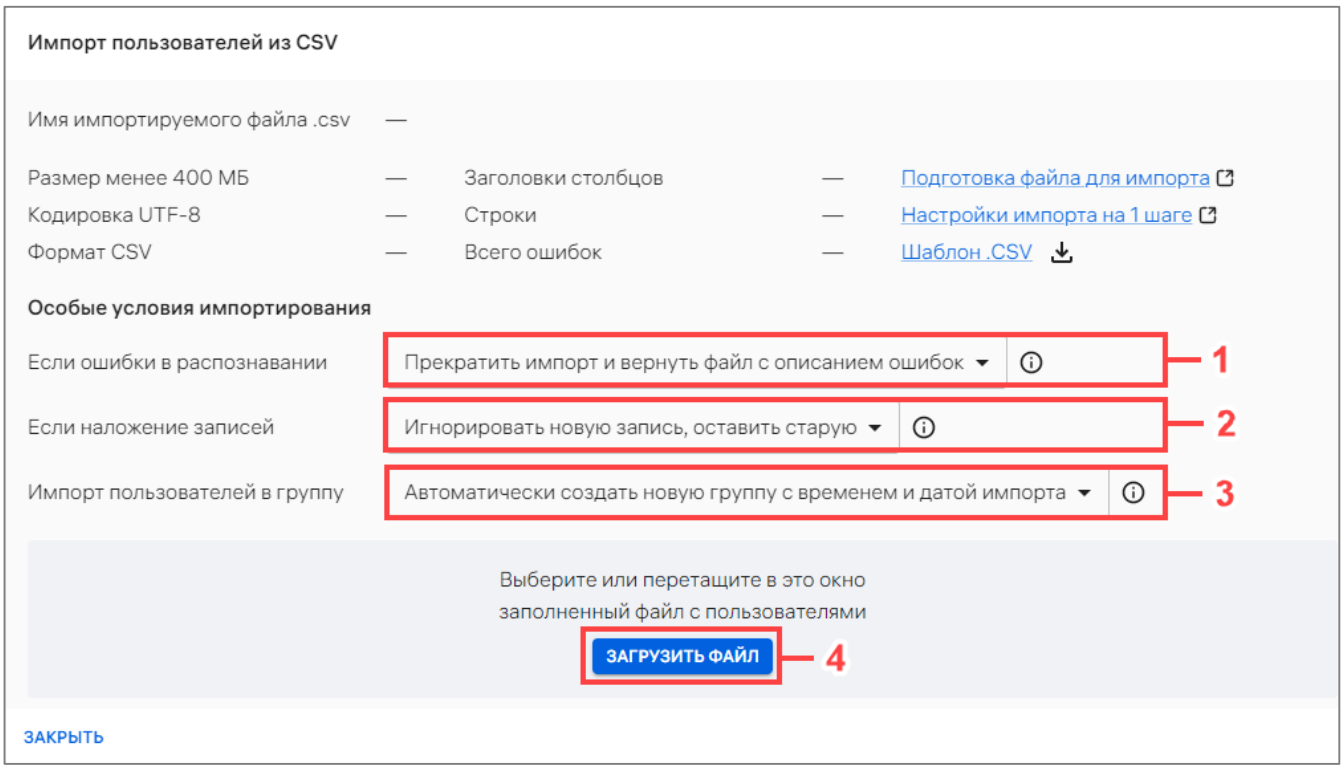


Рисунок 65

– далее необходимо загрузить CSV-файл одним из способов:

- переместить CSV-файл в область загрузки;
- нажать кнопку «Загрузить файл» (см. Рисунок 65 [4]) с последующим выбором файла для импорта;

– в результате будет запущен импорт пользователей из CSV-файла и отобразится шкала загрузки импорта.

Если заполненный файл был загружен корректно или файл содержал ошибки, но при этом в особых условиях импортирования была выбрана опция «Продолжить импорт и вернуть 2 файла с ошибками и без», импорт будет завершен. В окне с результатами импорта шкала загрузки импорта будет заполнена до конца (Рисунок 66).

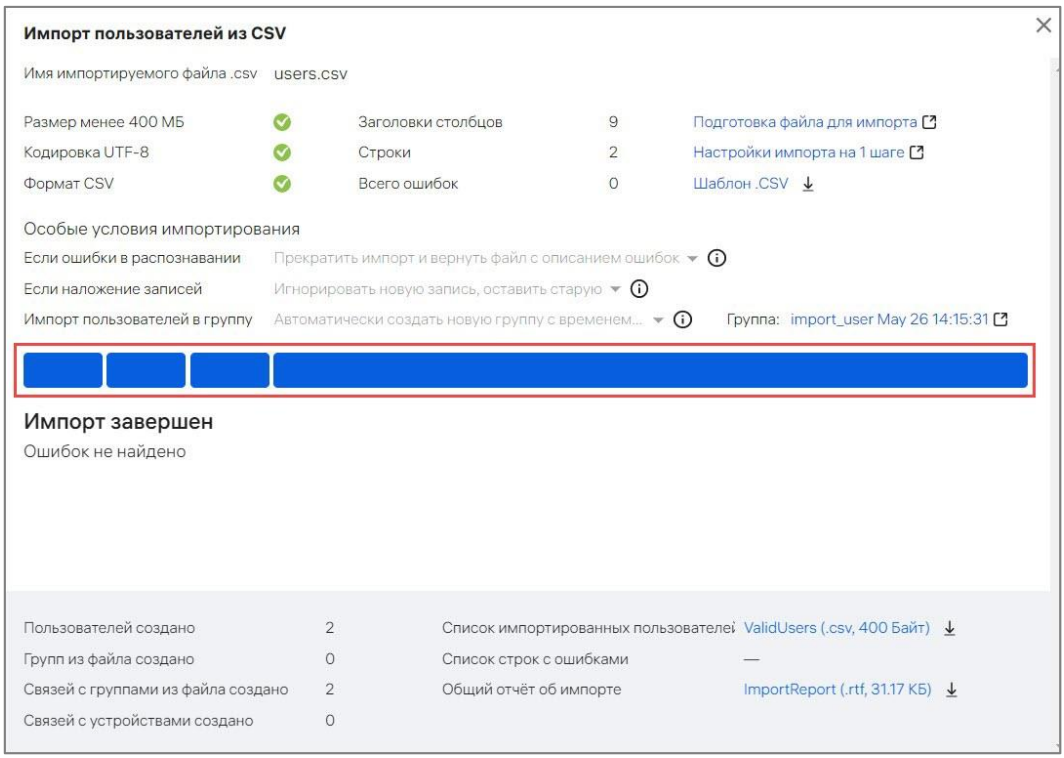


Рисунок 66

Если заполненный файл был загружен некорректно и при этом в особых условиях импортирования была выбрана опция «Прекратить импорт и вернуть файл с описанием ошибок», импорт будет остановлен. В окне с результатами импорта шкала загрузки импорта устройств будет прервана на этапе, где были обнаружены ошибки (Рисунок 67 [6]).

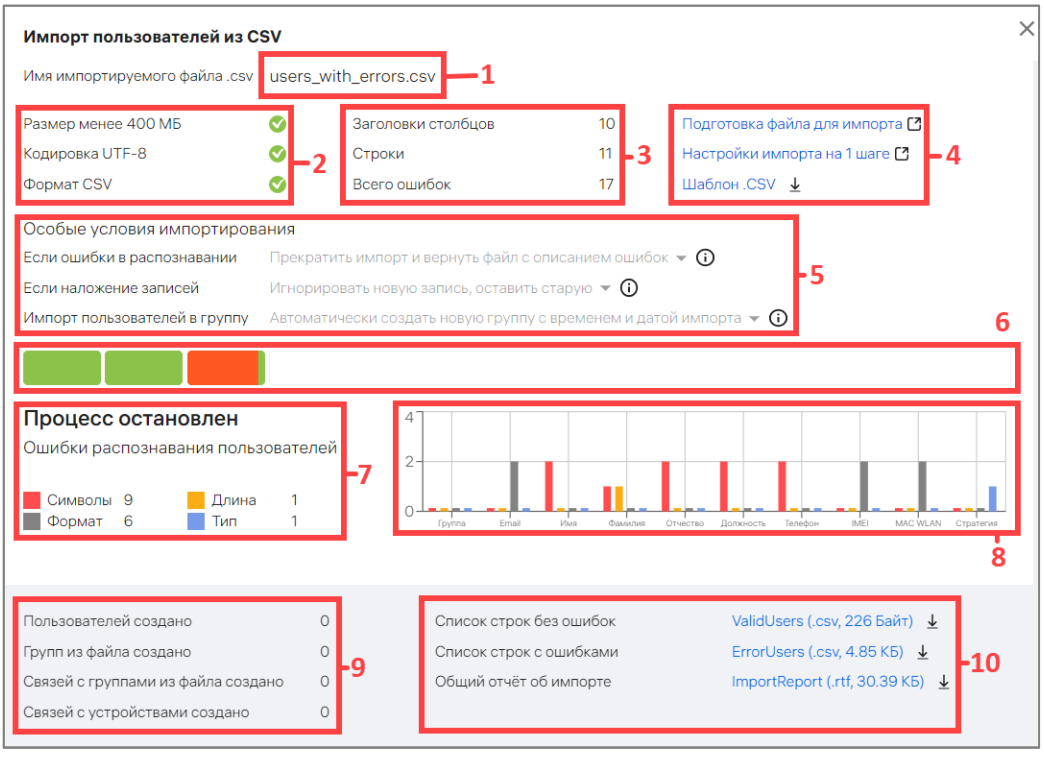


Рисунок 67

В окне с результатами импорта пользователей отображается следующая информация:

– название импортируемого файла (см. Рисунок 67 [1]);

– соответствие импортируемого файла размеру, кодировке и формату (см. Рисунок 67 [2]);

– количество столбцов, всех импортируемых строк и ошибок в файле (при их наличии) (см. Рисунок 67 [3]);

– ссылки (см. Рисунок 67 [4]):

• Подготовка файла для импорта, при нажатии на которую произойдет переход на статью справки, описывающую требования и процесс подготовки CSV-файла для импорта пользователей;

• Настройки импорта на 1 шаге, при нажатии на которую произойдет переход на статью справки, описывающую шаги импорта;

• Шаблон .CSV, при нажатии на которую произойдет скачивание шаблона CSV-файла для импорта пользователей;

– особые условия импортирования (см. Рисунок 67 [5]), см. Таблица 43);

– шкала прогресса импорта (см. Рисунок 67 [6]);

– сообщение о завершении импорта или прерывании процесса из-за ошибок (см. Рисунок 67 [7]);

– графическое распределение ошибок по столбцам параметров импорта (при обнаружении ошибок) (см. Рисунок 67 [8]);

– количество созданных пользователей, групп пользователей, связей пользователей с группами и устройствами (см. Рисунок 67 [9]);

– ссылки на скачивание отчетов (см. Рисунок 67 [10]):

• отчет со списком импортированных пользователей. Формат отчета – `.csv`;

• отчет со списком ошибок, описание которых приведено в подраздел 5.2. Формат отчета – `.csv` (при отсутствии ошибок в импортированном файле данный отчет не будет сформирован);

• отчет с общей информацией об импорте. Формат отчета – `.rtf`.

Отследить процесс выполнения импорта также возможно в окне «Процессы» подраздела «Индикаторы» раздела «Мониторинг». Более подробная информация приведена в разделе 3.

2.3.4. Привязка пользователей к группе пользователей

В Консоли администратора ПУ предусмотрена возможность привязки пользователя к группе пользователей, которая может быть выполнена:

– с помощью списка быстрых действий (пп. 2.3.4.1);

– вручную через карточку пользователя (пп. 2.3.4.2);

– вручную через карточку группы пользователей (пп. 2.3.4.3);

– с помощью импорта CSV-файла (п. 2.3.3);

– с помощью импорта из LDAP-сервера (пп. 4.1.5.3.1.1).

2.3.4.1. Привязка пользователей к группе пользователей с помощью списка быстрых действий

Привязка пользователей к группам с помощью списка быстрых действий возможна одним из способов:

– через список пользователей;

– через список групп пользователей.

Для этого необходимо:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать:

• «Поиск по пользователям» – для привязки пользователей через список пользователей;

• «Поиск по группам» – для привязки пользователей через список групп пользователей;

– выбрать пользователей с типом «Пользователь»/ «Группа пользователей», установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок или «Привязать пользователей к группам»;

– в отобразившемся окне выбрать необходимую группу пользователей или пользователя из раскрывающегося списка или воспользоваться фильтром. Далее при необходимости возможно добавить дополнительную группу/пользователя, выбрав из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка, нажав значок «Убрать из списка» справа от названия группы пользователей/пользователя.

ПРИМЕЧАНИЕ. Группы с типом «Организационное подразделение» недоступны в списке для выбора, т.к. их состав невозможно изменить вручную;

– при отсутствии необходимой группы в списке, создать ее, введя название новой группы в поле «Фильтр по названию группы» и нажав кнопку «Создать группу». В результате успешного создания группы отобразится соответствующее сообщение;

– нажать кнопку «Добавить в группы» или «Добавить пользователей». В результате успешной привязки пользователей к группам отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если на группу пользователей назначена политика и/или офлайн-сценарий, они начнут действовать для устройств, привязанных к пользователям.

2.3.4.2. Привязка пользователей к группе пользователей через карточку пользователя

Для привязки к пользователю группы пользователей через карточку пользователей необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– выбрать в области фильтров «Поиск по пользователям»;

– нажать на имя пользователя для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке пользователя перейти во вкладку «Группы»;

– нажать кнопку «Добавить в группы»;

– в отобразившемся окне выбрать необходимую группу пользователей из раскрывающегося списка или воспользоваться фильтром. Далее при необходимости возможно добавить дополнительную группу, выбрав из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка, нажав значок «Убрать из списка» справа от названия группы пользователей/пользователя.

ПРИМЕЧАНИЕ. Группы с типом «Организационное подразделение» недоступны в списке для выбора, т.к. их состав невозможно изменить вручную;

– при отсутствии необходимой группы в списке, создать ее, введя название новой группы в поле «Фильтр по названию группы» и нажав кнопку «Создать группу». В результате успешного создания группы отобразится соответствующее сообщение;

– нажать кнопку «Добавить в группы». В результате успешной привязки пользователей к группам отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если на группу пользователей назначена политика и/или офлайн-сценарий, они начнут действовать для устройств, привязанных к пользователям.

2.3.4.3. Привязать пользователей к группе пользователей через карточку группы пользователей

ПРИМЕЧАНИЕ. В группы с типом «Группа пользователей» возможно добавить только пользователей с типом «Пользователь».

Для привязки одного или нескольких пользователей к группе пользователей через карточку группы пользователей необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– выбрать в области фильтров «Поиск по группам»;

– нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке группы перейти во вкладку «Пользователи»;

– нажать кнопку «Привязать пользователей»;

– в отобразившемся окне выбрать пользователя из раскрывающегося списка или воспользоваться фильтром по ФИО, почте или номеру телефона (Рисунок 68 [1]). Далее при необходимости возможно добавить дополнительного пользователя, выбрав его из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранного пользователя, нажав значок «Убрать из списка» (Рисунок 68 [3]).

ПРИМЕЧАНИЕ. В списке отображаются только пользователи с типом «Пользователь»;

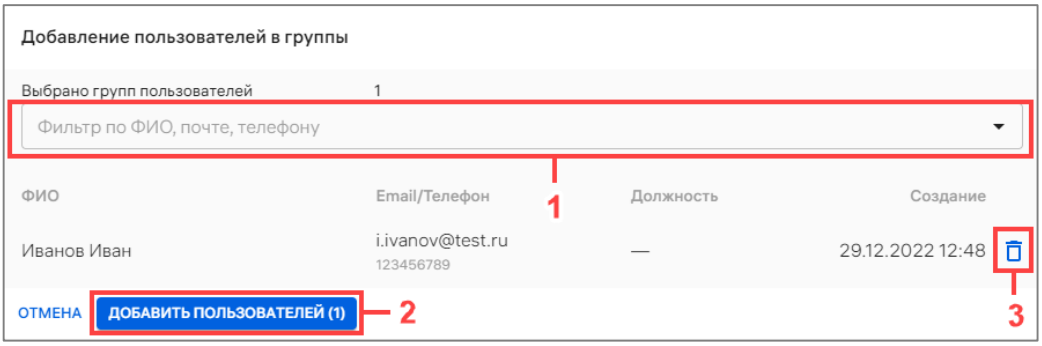


Рисунок 68

– далее нажать кнопку «Добавить пользователей» (см. Рисунок 68 [2]). В результате успешной привязки пользователя к группе отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если на группу пользователей назначена политика и/или офлайн-сценарий, они начнут действовать для активированных устройств, привязанных к пользователям.

2.3.5. Привязка пользователей к устройствам

2.3.5.1. Привязка пользователей к устройствам с помощью списка быстрых действий

Для привязки пользователей к устройствам с помощью списка быстрых действий необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по пользователям»;

– выбрать пользователя, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Привязать устройства к пользователям»;

– в отобразившемся окне выбрать устройства из раскрывающегося списка или воспользоваться фильтром по идентификатору или комментарию. Далее при необходимости возможно добавить дополнительные устройства, выбрав их из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также

возможно удалить из списка выбранные устройства, нажав значок «Убрать из списка» справа от устройства;

– нажать кнопку «Привязать устройства».

В результате успешной привязки устройства отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если на группу, в которую включен пользователь, назначены политика и/или офлайн-сценарии, они начнут действовать на устройстве (если оно активировано).

2.3.5.2. Привязка пользователей к устройствам через карточку пользователя

Для привязки пользователей к устройствам через карточку пользователя необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по пользователям»;

– нажать на имя пользователя для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке пользователя перейти во вкладку «Устройства»;

– нажать кнопку «Привязать устройства»;

– в отобразившемся окне выбрать устройства из раскрывающегося списка или воспользоваться фильтром по идентификатору или комментарию. Далее при необходимости возможно добавить дополнительные устройства, выбрав их из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранные устройства, нажав значок «Убрать из списка» справа от устройства;

– нажать кнопку «Привязать устройства».

2.3.6. Отвязать (исключить) пользователей из группы пользователей

Исключить пользователей с типом «Пользователь» из групп с типом «Группа пользователей» возможно вручную.

Исключить пользователей с типом «Пользователь из орг. подразделения» из группы с типом «Организационное подразделение» возможно только через синхронизацию с LDAP-сервером.

Исключить пользователя из группы с типом «Группа пользователей» возможно через:

– карточку пользователя (пп. 2.3.6.1);

– каточку группы пользователей (пп. 2.3.6.2).

2.3.6.1. Исключение пользователя из группы пользователей через карточку пользователя

Для исключения пользователя из группы пользователей через карточку пользователя необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по пользователям»;

– нажать на название устройства для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в карточке пользователя перейти во вкладку «Группы»;

– выбрать группу пользователей, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение»;

– в списке быстрых действий нажать значок  «Исключить пользователя из группы»;

– в отобразившемся окне подтверждения операции подтвердить либо отменить действия.

В результате успешного исключения пользователя из группы политики будут перекомбинированы таким образом, что для устройства, привязанного к пользователю, будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.3.6.2. Отвязка пользователя от группы пользователей через карточку группы пользователей

Отвязать пользователя возможно через карточку группы пользователя, выполнив следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в карточке группы пользователей перейти во вкладку «Пользователи»;

– выбрать пользователя, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения нажать кнопку «Сбросить выделение»;

– в списке быстрых действий нажать значок  «Отвязать пользователей от группы»;

– в отобразившемся окне подтвердить либо отменить действия;

В результате успешной отвязки пользователя от группы, политики будут перекомбинированы таким образом, что для устройства, привязанного к пользователю, будут действовать только политики, назначенные на группы устройств и группы пользователей, в которые входит устройство.

2.3.7. Архивирование пользователя

Администратор Платформы управления имеет возможность архивировать пользователя, который был добавлен вручную или с помощью импорта CSV-файла. Пользователь будет заархивирован со всеми его связями с группами и устройствами.

ВНИМАНИЕ!

✓ Архивирование пользователей с типом «Пользователь из орг. подразделения» возможно только через синхронизацию с LDAP-сервером;

✓ Пользователи с типом «Пользователь» не подлежат восстановлению из архива.

Архивировать пользователя возможно одним из следующих способов:

1) Через карточку пользователя. Для это необходимо:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по пользователям»;

– выбрать из списка пользователя с типом «Пользователь», при необходимости воспользовавшись фильтром (подраздел 1.4), и перейти в карточку пользователя;

– в открывшейся карточке пользователя перейти во вкладку «Устройства» и нажать кнопку «Архивировать»;

– в отобразившемся окне подтвердить либо отменить действия;

2) С помощь списка быстрых действий. Для это необходимо:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по пользователям»;

– выбрать пользователя с типом «Пользователь», установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Архивировать пользователя»;

– в отобразившемся окне подтвердить либо отменить действия.

В результате успешного архивирования отобразится соответствующее сообщение. Заархивированные пользователи не будут отображаться в списке пользователей.

2.3.8. Удаление группы пользователей

ВНИМАНИЕ! Удаление группы пользователей с типом «Организационное подразделение» возможно только через синхронизацию с LDAP-сервером (пп. 4.1.5.3.3).

Удаление группы пользователей с типом «Группа пользователей» и «Динамическая группа» возможно вручную. Для этого необходимо:

– предварительно исключить всех пользователей из группы (п. 2.3.6), а также удалить ее из всех множеств (пп. 2.2.6.1) – для группы с типом «Группа пользователей» (п. 2.3.6);

– отвязать группу пользователей от всех политик (п. 2.4.7) и офлайн-сценариев (п. 2.5.3) – для динамической группы.

После выполнения условий, приведенных выше, группа с типом «Группа пользователей» и «Динамическая группа» может быть удалена из ПУ. Для этого необходимо:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);
– в открывшейся карточке нажать кнопку «Удалить»;
– в открывшемся окне подтвердить либо отменить действия.

В результате успешного удаления отобразится соответствующее сообщение.

2.4. Подраздел «Политики»

Подраздел «Политики» Консоли администратора ПУ предназначен для работы и управления политиками и корпоративным шаблоном политик, которые могут быть назначены на группы устройств или группы пользователей.

ПРИМЕЧАНИЕ. Для корректного управления устройством необходимо, чтобы:
– на устройстве было выставлено корректное время и был задан часовой пояс;
– версия ППО совпадала с версией приложения «Аврора Центр» на устройстве (важно, после обновления ППО обновить также и версию приложения на устройстве).

Для управления устройством на базе ОС Аврора необходимо перевести устройство в режим администратора.

ПРИМЕЧАНИЕ. Если устройство в режиме пользователя, необходимо назначить и дождаться применения на устройстве политики с правилом «Настройки пользователя/Создать пользователя».

Для перехода в подраздел «Политики» необходимо в верхней панели раздела «Управление» выбрать подраздел «Политики». В результате отобразится список политик, а при их отсутствии отображается сообщение «Нет данных».

В рабочей области подраздела «Политики» информация о политике отображается в столбцах, приведенных в таблице (Таблица 44).

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 44

Название столбца	Значение		Описание
Название	Название политики		Представляет собой активную ссылку, при нажатии на которую происходит переход к карточке политики
	Комментарий		Дополнительная информация к политике. Заполняется при необходимости
Содержимое	Категория правил в политике		Ограничение доступа
			Голосовые вызовы
			Конфигурация WLAN
			Конфигурация VPN
			Конфигурация NFS

Название столбца	Значение		Описание
			Конфигурация Bluetooth®
			Конфигурация
			Конфигурация репозиториев
			Система
			Настройки пользователя
			Геопозиционирование
			Файлы
			Файлы с устройства
			Скрипты
			Внешний вид
			Приложения
			Мобильная сеть
	Количество правил		Количество правил в категории
Обновлено	Дата и время последнего обновления политики		

Добавление политики возможно одним из следующих способов:

– вручную (п. 2.4.2);

– на основе корпоративного шаблона (п. 2.4.3);

– на основе существующей политики (п. 2.4.4).

Существует возможность добавления в политику правил как во время, так и после ее создания.

Список правил политик, доступных для каждой версии ОС, приведен в таблице (Таблица 45).

Приложение «Аврора Центр» с периодичностью раз в час проверяет, какие политики, офлайн-сценарии и команды оперативного управления назначены на устройство (если политикой не задана другая периодичность). В случае несовпадения текущего и целевого состояния устройства, перепримeняет необходимые опции управления.

ПРИМЕЧАНИЕ. В связи с использованием более ранних версий программного интерфейса (API), в управлении устройствами с ОС Android версий 7-8 выделяют следующие особенности:

– пользователь может вручную отключить геолокацию, которая включена перманентно на управляемых устройствах с ОС Android;

– режим киоска, блокировка экрана и установка приложений работают с особенностями (подробное описание приведено в таблице (Таблица 45).

Таблица 45

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
1	Ограничение доступа/Блокировка экрана	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.1
2	Ограничение доступа/Использование камеры	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.2
3	Ограничение доступа/Снимки экрана	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.3
4	Ограничения доступа/Режим разработчика	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.4
5	Ограничение доступа/Управление авиарежимом	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.5
6	Ограничение доступа/Управление точкой доступа WLAN	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.6
7	Ограничение доступа/Управление Bluetooth	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.7
8	Ограничение доступа/Использование браузера	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.8
9	Ограничение доступа/Управление датой и временем	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.9

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
10	Ограничение доступа/Передача данных MTP	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.10
11	Ограничение доступа/Использование микрофона	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.11
12	Ограничение доступа/Сброс к заводским настройкам	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.12
13	Ограничение доступа/Использование USB-накопителей	4.1.0 и выше	-	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.13
14	Ограничение доступа/Использование SD-карт	4.1.0 и выше	-	-	-	-	-	пп. 2.4.1.14
15	Ограничение доступа/Отправка и получение SMS	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.15
16	Ограничение доступа/Режим киоска	5.2.0 и выше	7 и выше	-	-	-	-	пп. 2.4.1.16
17	Голосовые вызовы/Исходящие вызовы	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.17
18	Голосовые вызовы/Входящие вызовы	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.18
19	Конфигурация WLAN/Режим работы WLAN	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.19

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
20	Конфигурация WLAN/Подключения к сети WLAN	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.20
21	Конфигурация VPN/Подключения VPN	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.21
22	Конфигурация NFC/Управление NFC	5 и выше	-	-	-	-		пп. 2.4.1.22
23	Конфигурация Bluetooth/Режим работы Bluetooth	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.23
24	Конфигурация/Расписание получения команд	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.24
25	Конфигурация/Расписание отправки состояния	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.25
26	Конфигурация/Расписание отправки событий безопасности	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.26
27	Конфигурация/Исключения событий безопасности	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.27
28	Конфигурация/Хранение логов на устройстве	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.28
29	Конфигурация/Обновление координат в клиенте Аврора Центр	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.29

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
30	Конфигурация/Создание точек восстановления	-	-	Рабочая станция 10К и 11К	-	22 LTS	7.3.4	пп. 2.4.1.30
31	Конфигурация/Управление часовым поясом	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.31
32	Конфигурация/Синхронизация времени	4.0.2 и выше	-	-	-	-	-	пп. 2.4.1.32
33	Конфигурация/Расписание перезагрузки	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.33
34	Конфигурация/Настройка прокси-сервера	4.0.2 и выше	-	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.34
35	Конфигурация/Таймаут экрана	5.1.3 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.35
36	Конфигурация принтеров/Управление принтерами	5.2.0	-	-	-	-	-	пп. 2.4.1.36
37	Конфигурация репозиториев/Подключение системных репозиториев	-	-	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.37

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
38	Конфигурация репозиториев/Подключение flatpak репозиториев	-	-	Рабочая станция 10К и 11К	-	22 LTS	7.3.4	пп. 2.4.1.38
39	Конфигурация хранилища/Шифрование файлового хранилища	-	7 и выше	-	-	-	-	пп. 2.4.1.39
40	Система/Обновление ОС	4.0.2 и выше	-	Рабочая станция 10К и 11К	-	-	-	пп. 2.4.1.40
41	Настройки пользователя/Требования к паролю	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.41
42	Настройки пользователя/Создать пользователя	4.0.2 и выше	-	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.42
43	Настройки пользователя/Сертификаты пользователя	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.43
44	Геопозиционирование/ Настройки LBS-сервиса	5.2.0 и выше	-	-	-	-	-	пп. 2.4.1.44
45	Геопозиционирование/ Настройки A-GNSS	4.1.0 и выше	-	-	-	-	-	пп. 2.4.1.45

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
46	Контент/Доставка на устройство	5.2.0 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.46
47	Файлы с устройства/Загрузка файлов с устройств	5.2.0 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.47
48	Проверки/Наличие файлов и их содержимого	-	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.48
49	Проверки/Символические ссылки	-	-	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LT	7.3.4	пп. 2.4.1.49
50	Проверки/Параметры безопасности	-	-	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LT	7.3.4	пп. 2.4.1.50
51	Диагностика ОС/Проверка установленных пакетов на устройстве	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.51
52	Скрипты/Выполнение на устройстве	-	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.52

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
53	Геопозиционирование/ Настройки режима работы геопозиционирования	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.53
54	Внешний вид/Установка фона рабочего стола	-	7 и выше	-	-	-	-	пп. 2.4.1.54
55	Внешний вид/Отображение идентификаторов в клиенте Аврора Центр	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.55
56	Внешний вид/Управление яркостью	-	9 и выше	-	-	-	-	пп. 2.4.1.56
57	Внешний вид/Ориентация экрана	-	9 и выше	-	-	-	-	пп. 2.4.1.57
58	Приложения/Управление приложениями	4.0.2 и выше	7 и выше	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	22 LTS	7.3.4	пп. 2.4.1.58
59	Приложения/Управление доверенными источниками	5.1.0 и выше	-	-	-	-	-	пп. 2.4.1.59
60	Приложения/Ограничение установки из источников	-	7 и выше	-	-	-	-	пп. 2.4.1.60
61	Приложения/Управляемые конфигурации	5.1.5 и выше	7 и выше	-	-	-	-	пп. 2.4.1.61
62	Приложения/Подключение витрин в клиенте Аврора Маркет	-	-	Рабочая станция 10К и 11К	1.7 SE, 1.8 SE	-	-	пп. 2.4.1.62

№ п/п	Название правила политики	Версии ОС						Описание
		ОС Аврора	ОС Android	ОС Альт Linux	ОС Astra Linux	ОС Ubuntu	РЕД ОС	
63	Мобильная сеть/Точка доступа	4.0.2 и выше	9 и выше	-	-	-	-	пп. 2.4.1.63
64	Мобильная сеть/Управление мобильной передачей данных	4.0.2 и выше	7 и выше	-	-	-	-	пп. 2.4.1.64
65	Мобильная сеть/Определение номера телефона	-	7 и выше	-	-	-	-	пп. 2.4.1.65

2.4.1. Общее описание правил политик

2.4.1.1. Ограничение доступа/Блокировка экрана

Правило позволяет разблокировать или заблокировать экран устройства с выводом сообщения.

ПРИМЕЧАНИЕ. Особенности работы правила политики для устройств на базе ОС семейства Linux приведены в документе «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

Выбор значения из списка:

– «Заблокирован» – данное значение выбрано по умолчанию при добавлении правила, а также доступно поле для ввода сообщения, которое будет отображаться на заблокированном экране. Экстренные вызовы остаются доступны;

– «Разблокирован».

ВНИМАНИЕ! На устройствах на базе ОС Android:

– при блокировке экрана также блокируется передача данных по MTP и исходящие вызовы (кроме экстренных). Поэтому если на устройство назначена политика с разрешением передачи данных по MTP и/или исходящих вызовов, то в карточке устройств будет отображаться статус «Не соответствует политике»;

– в зависимости от производителя и версии ОС Android поведение блокировки экрана может отличаться, например:

- если устройство защищено PIN-кодом, то после перезагрузки на экране ввода PIN-кода может быть доступно верхнее меню;
- перезагрузка устройства касанием соответствующей кнопки в интерфейсе может быть недоступна (например, данное поведение наблюдается на устройстве Samsung). В этом случае осуществлять перезагрузку устройства данного производителя следует с помощью комбинации кнопок на корпусе (в соответствии с документацией производителя);
- на устройствах Huawei на базе ОС Android версии 9 выявлена следующая проблема: если в окне вызова вручную ввести номер, отличный от экстренного, и попытаться совершить вызов, то вызов не произойдет ни в этом случае, ни после изменения номера на экстренный. Для решения проблемы следует вернуться на Экран блокировки и повторить экстренный вызов.

ПРИМЕЧАНИЕ. На устройствах с ОС Android версии 7.0, 7.1, 8.0.0, 8.1.0:

– в режиме блокировки необходимо вводить пароль при каждом включении экрана, если устройство защищено паролем;

– при попытке выключить устройство будет отображено окно, в котором возможно не только выключить или перезагрузить устройство, но и включить авиарежим, несмотря на запрещающее правило политики. Если включить авиарежим, то будет отображено окно с уведомлением и инструкцией как отключить авиарежим (Рисунок 69).

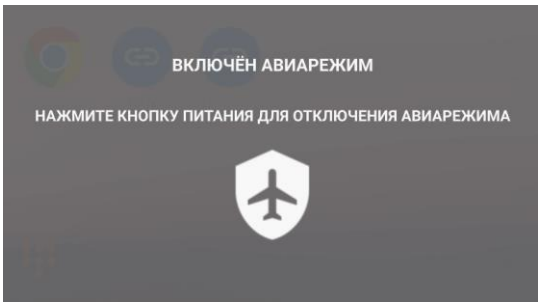


Рисунок 69

2.4.1.2. Ограничение доступа/Использование камеры

Правило разрешает или запрещает использование камеры на устройствах.
Выбор значения из списка:
– «Разрешено»;
– «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.3. Ограничение доступа/Снимки экрана

Правило разрешает или запрещает создание скриншотов с экрана устройства.
Выбор значения из списка:
– «Разрешено»;
– «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.4. Ограничения доступа/Режим разработчика

Правило разрешает или запрещает активировать режим разработчика на устройстве.

Доступные значения:
– «Разрешено» - в результате на устройстве в зависимости от ОС:
- Аврора: будет доступна возможность включить режим разработчика;
- Android: станет активным меню режима разработчика. Далее настройка на стороне пользователя;

– «Запрещено» (при добавлении правила значение выбрано по умолчанию) - в результате на устройстве в зависимости от ОС:
- Аврора: будет зафиксировано текущее состояние режима разработчика на устройстве и будет запрещено вносить изменения в зафиксированное состояние;
- Android: будет принудительно отключен режим разработчика на устройстве и пропадет возможность его активировать.

2.4.1.5. Ограничение доступа/Управление авиарежимом

Правило разрешает или запрещает использование авиарежима на устройствах.
Выбор значения из списка:
– «Разрешено»;
– «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.6. Ограничение доступа/Управление точкой доступа WLAN

Правило фиксирует текущее состояние точки доступа WLAN. Разрешает или запрещает вносить изменения в настройки точки доступа WLAN.

ПРИМЕЧАНИЕ. Для устройств Huawei и Honor на базе ОС Android при запрещающем правиле раздача интернета в режиме модема отключается, но пользователь может вручную включить и отключить точку доступа, а также изменить ее настройки.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.7. Ограничение доступа/Управление Bluetooth

Правило фиксирует текущее состояние Bluetooth®. Запрещает или разрешает вносить изменения в настройки Bluetooth®.

ВНИМАНИЕ! Для устройств на базе ОС Android версии 9, если Bluetooth® был включен, то после применения правила он может отображаться как выключенный в настройках, но при этом Bluetooth® продолжит работать.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (при добавлении правила значение выбрано по умолчанию) – будет запрещено создавать новые сопряжения с управляемого устройства (невозможно посмотреть доступные для подключения Bluetooth® и подключиться). При этом с другого устройства можно к будет подключиться к управляемому устройству.

2.4.1.8. Ограничение доступа/Использование браузера

Правило разрешает или запрещает использование браузера на устройствах.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.9. Ограничение доступа/Управление датой и временем

Правило фиксирует текущие дату и время на устройствах. Разрешает или запрещает вносить изменения в дату и время.

ПРИМЕЧАНИЯ:

✓ Для устройств на базе ОС Аврора и ОС Android изменение времени в меньшую сторону от реального может привести к тому, что записи о произошедших операциях перестанут отображаться в журнале приложения «Аврора Центр». Поэтому рекомендуется назначить политику с правилом по запрету управления датой и временем;

✓ Для некоторых устройств на базе ОС Android правило по запрету изменения даты и времени может оставлять возможность изменения часового пояса (в частности, на Huawei Y9).

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.10.Ограничение доступа/Передача данных MTP

Правило разрешает или запрещает передачу данных между устройством и ЭВМ при подключении по USB.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (при добавлении правила значение выбрано по умолчанию).

ПРИМЕЧАНИЕ. При запрете передачи данных по USB возможно следующее поведение устройства:

– при подключении к ЭВМ устройство не появляется как съемный накопитель в проводнике;

– зарядка и другие режимы USB работают;

– физические USB-накопители (флешки), подключенные через OTG, могут определяться и использоваться на самом устройстве (если не запрещено отдельной политикой);

– приложения на устройстве могут получать доступ к файлам на подключенной флешке (если не запрещено отдельной политикой).

2.4.1.11.Ограничение доступа/Использование микрофона

Правило запрещает или разрешает использование микрофона для записи звука на устройствах.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (микрофон будет недоступен для записи звука во всех приложениях и внешних устройствах, которые управляют им (наушники, гарнитуры и т.п.), но будет доступен для исходящих и входящих вызовов). При добавлении правила значение выбрано по умолчанию.

2.4.1.12.Ограничение доступа/Сброс к заводским настройкам

Правило запрещает или разрешает сброс к заводским настройкам.

Выбор значения из списка:

– «Разрешен»;

– «Запрещен» (при добавлении правила значение выбрано по умолчанию). При назначении правила пользователю становится недоступен сброс устройства к заводским настройкам стандартными средствами ОС.

ВНИМАНИЕ! Ограничение не предотвращает сброс через режим восстановления (ограничение ПУ). После сброса устройство потребуется заново поставить под управление.

2.4.1.13.Ограничение доступа/Использование USB-накопителей

Правило запрещает или разрешает использование USB-накопителей.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (при добавлении правила значение устанавливается по умолчанию).

Особенности применения политики на устройствах с ОС Аврора:

– если применить запрещающее правило в момент использования подключенного USB-накопителя (например, какой-либо файл с USB-накопителя открыт), то USB-накопитель не отключится. Также на устройстве могут возникнуть ошибки, после которых USB-накопитель останется доступен;

– если после применения запрещающего правила разрешить использование USB-накопителей, то устройство начнет видеть их через 1-2 минуты или после извлечения и повторного подключения USB-кабеля;

– при применении запрещающего правила на устройстве INOI P4903 сообщение о блокировке в пункте меню «Хранилище» в подразделе «Настройки» отображается не полностью.

Особенности применения политики на устройствах с ОС семейства Linux: если в момент применения запрещающего правила политики USB-накопитель подключен к устройству и на нем происходит чтение/запись, то будет производиться попытка размонтировки раз в час USB-накопителя и его блокировки, либо USB-накопитель будет запрещен после перезагрузки устройства.

2.4.1.14.Ограничение доступа/Использование SD-карт

Правило запрещает или разрешает использование SD-карт.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (при добавлении правила значение устанавливается по умолчанию).

ПРИМЕЧАНИЯ:

✓ В случае применении запрещающего правила в момент просмотра:

– каталога с SD-карты в приложении «Файлы», данный каталог будет доступен для просмотра до его закрытия;

– файла с SD-карты, данный файл будет доступен для просмотра до его закрытия;

✓ Если после запрета разрешить использование SD-карт, то устройство начнет видеть их после перезагрузки или после ручного включения в пункте меню «Хранилище» в подразделе «Настройки».

2.4.1.15.Ограничение доступа/Отправка и получение SMS

Правило разрешает или запрещает отправку и получение SMS-сообщений на устройстве.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (при добавлении правила значение устанавливается по умолчанию).

После назначения политики с правилом по запрету приема и отправки SMS:

1) Блокируется отправка сообщений на экстренные номера;

2) Стандартное приложение для отправки и получения SMS:

– на устройствах с ОС Аврора:

• ярлык приложения исчезнет. Если приложение было открыто и в этот момент пришла политика по запрету приема и отправки SMS, то пользователь останется в открытом приложении, но не сможет получать и отправлять новые SMS;

• если при получении вызова пользователь отвечает отправкой быстрого сообщения, то пользователь в истории сможет увидеть, что сообщение было отправлено, но не доставлено;

– на устройствах с ОС Android будет доступно для открытия, но недоступно для взаимодействия;

3) Только на устройствах с ОС Android при использовании сторонних приложений для SMS либо не будет возможности в него попасть, либо не будет возможности с его помощью отправить SMS;

4) При использовании нецелевых приложений для отправки сообщений (например, через приложение с вызовами, контактами, заметками и т.п.):

– на устройствах с ОС Android:

• будет неудачная попытка отправки;

• для некоторых версий ОС при попытке отправить сообщение через нецелевое приложение (например, «Контакты») данное приложение «зависнет» и для восстановления работоспособности необходимо перезапустить приложение;

– на устройствах ОС Аврора ничего не произойдет. Но при этом пользователь сможет ознакомиться с историей сообщений (через приложение «Контакты») и/или открыть приложение с сообщениями (такое же поведение может произойти после отправки SMS после завершения вызова);

5) В зависимости от ОС и прошивки запрет может распространяться также и на MMC-сообщения.

После снятия политики по запрету отправки и получения SMS в некоторых случаях:

– для **ОС Аврора** может потребоваться перезагрузка устройства для корректной работы с SMS. При этом сообщения, которые пользователь пытался отправить при запрете, невозможно будет отправить после снятия запрета, для их отправки необходимо пересоздать сообщения;

– для некоторых версий **ОС Android** созданные раннее SMS-диалоги могут исчезнуть.

2.4.1.16.Ограничения доступа/Режим киоска

Правило позволяет активировать на устройстве режим киоска, в котором в зависимости от ОС устройства доступны:

– **ОС Аврора** (пп. 2.4.1.16.1): только указанные приложения с возможностью их автозапуска;

– **ОС Android в режиме рабочего стола** (пп. 2.4.1.16.2): только указанные приложения, ярлыки веб-страниц и сайты. Также есть возможность отключить панель уведомлений («шторку»), настроить сервисы для автозапуска;

– **ОС Android в режиме веб-ресурса (моно-киоска)** (пп. 2.4.1.16.3): выбранная веб-страница во весь экран устройства с возможностью переходов только на разрешенные ресурсы, с возможностью управлять отображением панели навигации (кнопки «Назад»/«Вперед»/«Обновить») и настроить сервисы для автозапуска;

– **ОС Android в режиме запуска одного нативного приложения** (пп. 2.4.1.16.4): одно нативное приложение во весь экран устройства с возможностью указать список скрытых/разрешенных приложений и код выхода из режима киоска, настроить сервисы для автозапуска.

2.4.1.16.1. Создание правила для устройства с ОС Аврора

ВНИМАНИЕ! Создание правила для ОС Аврора доступно для устройств с версии 5.2.0 и выше.

ПРИМЕЧАНИЕ. Разрешенный (белый) список и автозапуск распространяются только на приложения с desktop-файлами.

Для создания правила необходимо:

1) В раскрывающемся списке «Платформа» выбрать «Аврора»;

2) При добавлении правила переключатель «Включен» находится во включенном положении. Если необходимо отключить режим киоска, то перевести переключатель в положение «Выключено»;

3) В блоке «Приложения» задать разрешенный (белый) список приложений, которые будут доступны в режиме киоска. Для этого:

– нажать на значок +;

– в раскрывающемся списке «Автозапуск» выбрать нужное значение:

• «Не задано» - пользователь может установить автозапуск приложения вручную. При добавлении правила значение выбрано по умолчанию;

• «Да» - приложение будет запускаться автоматически после загрузки ОС. Пользователь не сможет отменить автозапуск приложения вручную;

• «Нет» - приложение не будет запускаться автоматически после загрузки ОС. Пользователь не сможет установить автозапуск приложения вручную;

– ввести в поле «Название приложения» название пакета приложения. В случае отсутствия информации о названии пакета требуемого приложения, необходимо перейти в карточку устройства во вкладку «Приложения», столбец «Инфо». В списке отображаются названия всех пакетов со всех устройств, которые отправили свое состояние в ППО. При необходимости воспользоваться фильтром по названию пакета (ввести в поле «Название приложения» полное или частичное название пакета). Если нужного пакета нет в списке, ввести его точное название и в раскрывающемся списке выбрать «Добавить <название пакета>»;

– если необходимо добавить еще одно приложение, повторить шаг 3.

2.4.1.16.2. Создание правила для устройства с ОС Android в режиме рабочего стола

Если требуется, чтобы в режиме киоска отображались только разрешенные приложения и ярлыки сайтов/веб-страниц, необходимо:

1) В раскрывающемся списке «Платформа» выбрать «Android» (при добавлении правила выбрано по умолчанию);

2) С помощью переключателя «Включен» возможно включить или выключить режим киоска.

ПРИМЕЧАНИЕ. При добавлении правила переключатель по умолчанию включен;

3) Убедиться, что в раскрывающемся списке «Тип киоска» выбрано «Рабочий стол»;

4) В поле «Отключение панели уведомлений» выключить переключатель, если в режиме киоска требуется отключить верхнее меню.

ПРИМЕЧАНИЕ. При добавлении правила переключатель по умолчанию выключен.

ВНИМАНИЕ! Управление панелью уведомлений возможно для устройств с ОС Android 9 и выше;

5) В поле «Код выхода из режима киоска» ввести код, состоящий из 8 цифр. Также возможно сгенерировать код автоматически, нажав кнопку «Сгенерировать пароль» в правой части строки.

ПРИМЕЧАНИЕ. Поле обязательно для заполнения, если режим киоска включен;

6) Для параметра «Цвет шрифта» доступен выбор одного из значений:

– «По умолчанию» – цвет шрифта остается тот, который был в системе до назначения и применения плитики с правилом режима киоска;

– «Выбор цвета» – при выборе данного значения становится доступным:
- поле для ввода HEX-кода;
- окно с цветовой палитрой для выбора необходимого цвета;

7) Для параметра «Фон» доступен выбор одного из значений:

– «Системное изображение» — фон остается системным, который был до назначения и применения политики с правилом режима киоска;

– «Выбор цвета» – при выборе данного значения становится доступным:
- поле для ввода HEX-кода;
- окно с цветовой палитрой для выбора необходимого цвета;

8) В блоке «Укажите приложения/Приложения» указать приложения и их порядок расположения, которые будут доступны пользователю в режиме киоска. Для этого:

– нажать на значок +;

– в поле «Приложение N» ввести название пакета приложения (необходимые данные доступны для просмотра в карточке устройства в столбце «Инфо» (пп. 2.1.1.9). В списке отображаются названия всех пакетов со всех устройств, которые отправили свое состояние в ППО. При необходимости воспользоваться фильтров по названию пакета (ввест в поле «Название приложения» полное или частичное название пакета). Если нужного пакета нет в списке, то ввести его точное название и выбрать «Добавить <название пакета>» в раскрывающемся списке.

– если требуется добавить еще одно приложение, то необходимо нажать на значок + в левом нижнем углу и повторить шаг 8.

– если требуется изменить порядок расположения приложений необходимо воспользоваться кнопками ▲ ▼.

ПРИМЕЧАНИЕ. Поле обязательно для заполнения, если режим киоска включен, и в правило не добавлено ни одного ярлыка веб-страницы;

9) Добавить ярлыки веб-страниц, позволяющих открыть необходимые сайты, выполнив следующие действия:

– в блоке «Ярлыки веб-страниц/Укажите ярлыки веб-страниц» нажать на значок +;

– в поле «Название ярлыка» ввести название ярлыка (может содержать от 1 до 20 символов);

– в поле «URL» ввести электронный адрес необходимого сайта/страницы в формате URL. Например: https://www.omp.ru/;

– при необходимости задать иконку для ярлыка веб-страницы, выбрав в раскрывающемся списке «Путь к файлу иконки» путь к файлу иконки.

ПРИМЕЧАНИЯ:

✓ Выбор иконки возможен только при наличии правила по доставке контента в политике. Если в раскрывающемся списке «Путь к файлу иконки» нет нужного файла изображения, то необходимо нажать «добавить доставку контента» и заполнить параметры правила по доставке контента (пп. 2.4.1.46);

✓ Поле обязательно для заполнения, если режим киоска включен, и в правило не добавлено ни одного приложения;

✓ Возможно добавление нескольких ярлыков веб-страниц;

10) Настроить список разрешенных/запрещенных сайтов. Доступно, если в качестве браузера по умолчанию используется Chrome.

Для настройки списка разрешенных сайтов необходимо:

– перевести переключатель «Запретить все сайты» в положение «Включено»;

– в поле «Исключения из запрещенных сайтов» ввести электронный адрес разрешенного сайта в формате URL (например: https://www.omp.ru/) и нажать Enter.

ПРИМЕЧАНИЯ:

✓ С помощью кнопки «Добавить ярлыки в список исключений». Также возможно добавить в разрешенный список адреса сайтов из ярлыков, которые указаны на шаге 7;

✓ Возможно добавление нескольких разрешенных сайтов.

Для настройки списка запрещенных сайтов необходимо:

– убедиться, что переключатель «Запретить все сайты» находится в положении «Выключено»;

– в поле «Запрещенные сайты» ввести электронный адрес запрещенного сайта в формате URL (например: https://www.omp.ru/) и нажать «Enter».

ПРИМЕЧАНИЯ:

✓ Возможно добавление нескольких запрещенных сайтов;

✓ Необходимо добавлять в списки запрещенных/разрешенных сайтов только конечные URL. Например, если заблокировать все сайты, кроме https://www.omp.ru/, то после редиректа он станет https://omp.ru/ и разрешение не сработает;

11) При необходимости настроить автозапуск сервисов в режиме киоска.

ПРИМЕЧАНИЕ. Управление автозапуском сервисов возможно для устройств с ОС Android 10 и выше.

Автозапуск сервисов позволяет автоматически запускать фоновые компоненты, необходимые для работы кассовых, платежных, фискальных и других бизнес-приложений. Под сервисом подразумевается только тот сервис, который может работать в фоновом режиме. Например, основное приложение терминала может использовать отдельный платежный или фискальный сервис. После применения политики, включения или перезагрузки устройства ППО попытается автоматически запустить указанный сервис.

Для настройки запуска автосервисов необходимо:

– включить переключатель «Сервисы для автозапуска»;

– заполнить поля:

- в поле «Имя пакета» ввести или выбрать из списка название пакета приложения;

- в поле «Имя сервиса» ввести полное имя класса (например, com.example.app.MyService) или сокращенное, начиная с точки (например, .MyService), если класс находится внутри указанного пакета.

Если необходимо добавить еще один сервис для запуска, то необходимо нажать значок + и повторить шаги, приведенные выше.

ПРИМЕЧАНИЕ. Максимально можно добавить пять сервисов для автозапуска.

Сервис определяется сочетанием имени пакета и имени сервиса (подробнее в пп. 2.4.1.16.7).

2.4.1.16.3. Создание правила для устройства с ОС Android в режиме веб-ресурса (моно-киоска)

Если требуется отобразить нужную веб-страницу во весь экран устройства с возможностью переходов только на разрешенные ресурсы, необходимо:

1) В раскрывающемся списке «Платформа» выбрать «Android» (при добавлении правила выбрано по умолчанию);

2) Перевести переключатель «Включен» в положение «Выключено», если необходимо отключить режим киоска (при добавлении правила переключатель находится в положении «Включено»);

3) В раскрывающемся списке «Тип киоска» выбрать «Веб-ресурс»;

4) Перевести переключатель «Отключение панели уведомлений» в положение «Включено», если необходимо отключить в режиме киоска панель уведомлений («шторку»). При добавлении правила переключатель находится в положении «Выключено».

ВНИМАНИЕ! Управление панелью уведомлений возможно для устройств с ОС Android 9 и выше;

5) В поле «Код выхода из режима киоска» ввести код для выхода из режима киоска. Код должен состоять из 8 цифр. Также возможно сгенерировать код автоматически. Для этого в правой части поля нажать на кнопку «Сгенерировать пароль». Поле обязательно для заполнения, если режим киоска включен;

6) Перевести переключатель «Панель навигации» в положение «Включено», если необходимо включить в режиме киоска панель навигации (кнопки «Назад»/«Вперед»/«Обновить»). При добавлении правила переключатель находится в положении «Выключено»;

7) В поле «Стартовая страница» ввести URL веб-ресурса, который должен открываться во весь экран устройства.

ПРИМЕЧАНИЕ. Если в качестве дефолтного браузера используется Chrome, то возможно дополнительно настроить список разрешенных/запрещенных сайтов.

Настройка списка разрешенных сайтов:

– перевести переключатель «Запретить все сайты кроме разрешенных» в положение «Включено»;

– в поле «Исключения из запрещенных сайтов» ввести электронный адрес разрешенного сайта в формате URL (например: https://www.omp.ru/) и нажать «Enter»;

– если требуется добавить еще один разрешенный сайт, то повторить шаг выше.

Настройка списка запрещенных сайтов:

– убедиться, что переключатель «Запретить все сайты кроме разрешенных» находится в положении «Выключено»;

– в поле «Запрещенные сайты» ввести электронный адрес запрещенного сайта в формате URL(например: https://www.omp.ru/) и нажать «Enter»;

– если необходимо добавить еще один запрещенный сайт, то повторить шаг выше.

ВНИМАНИЕ! Необходимо добавлять в списки запрещенных/разрешенных сайтов только конечные URL. Например, если заблокировать все сайты, кроме https://www.omp.ru/, то после редиректа он станет https://omp.ru/ и разрешение не сработает;

8) При необходимости настроить автозапуск сервисов в режиме киоска.

ПРИМЕЧАНИЕ. Управление автозапуском сервисов возможно для устройств с ОС Android 10 и выше.

Автозапуск сервисов позволяет автоматически запускать фоновые компоненты, необходимые для работы кассовых, платежных, фискальных и других бизнес-приложений. Под сервисом подразумевается только тот сервис, который может работать в фоновом режиме. Например, основное приложение терминала может использовать отдельный платежный или фискальный сервис. После применения политики, включения или перезагрузки устройства ППО попытается автоматически запустить указанный сервис.

Для настройки запуска автосервисов необходимо:

– включить переключатель «Сервисы для автозапуска»;

– заполнить поля:

- в поле «Имя пакета» ввести или выбрать из списка название пакета приложения;
- в поле «Имя сервиса» ввести полное имя класса (например, com.example.app.MyService) или сокращенное, начиная с точки (например, .MyService), если класс находится внутри указанного пакета.

Если необходимо добавить еще один сервис для запуска, то необходимо нажать значок + и повторить шаги, приведенные выше.

ПРИМЕЧАНИЕ. Максимально можно добавить пять сервисов для автозапуска.

Сервис определяется сочетанием имени пакета и имени сервиса (подробнее в пп. 2.4.1.16.7).

2.4.1.16.4. Создание правила для устройства с ОС Android в режиме одного приложения (моно-киоск)

Если требуется запустить одно нативное приложение во весь экран устройства с возможностью указать список скрытых/разрешенных приложений и код выхода из режима киоска:

1) В раскрывающемся списке «Платформа» выбрать «Android» (при добавлении правила выбрано по умолчанию);

2) Перевести переключатель «Включен» в положение «Выключено», если необходимо отключить режим киоска (при добавлении правила находится в положении «Включено»);

3) В раскрывающемся списке «Тип киоска» выбрать «Приложение»;

4) Перевести переключатель «Отключение панели уведомлений» в положение «Включено», если необходимо отключить в режиме киоска панель уведомлений («шторку»). При добавлении правила переключатель находится в положении «Выключено».

ВНИМАНИЕ! Управление панелью уведомлений возможно для устройств с ОС Android 9 и выше;

5) В поле «Код выхода из режима киоска» ввести код для выхода из режима киоска. Код должен состоять из 8 цифр. Также возможно сгенерировать код автоматически. Для этого в правой части поля нажать на кнопку «Сгенерировать пароль». Поле обязательно для заполнения, если режим киоска включен;

6) Ввести в поле «Основное приложение» название пакета приложения, которое должно запускаться во весь экран устройства. В случае отсутствия информации о названии пакета требуемого приложения, необходимо перейти в карточку устройства во вкладку «Приложения», столбец «Инфо» (пп. 2.1.1.9). В списке отображаются названия всех пакетов со всех устройств, которые отправили свое состояние в ППО. При необходимости воспользоваться фильтром по названию пакета (ввести в поле «Основное приложение» полное или частичное название пакета). Если нужного пакета нет в списке, ввести его точное название и выбрать «Добавить <название пакета>» в раскрывающемся списке;

7) При необходимости указать список скрытых приложений — приложений, которые не будут отображаться пользователю, но будут разрешены для использования в режиме киоска. Для этого:

– перевести переключатель «Скрытые приложения» в положение «Включено» (по умолчанию он выключен);

– ввести в поле «Приложение N» название пакета приложения. В случае отсутствия информации о названии пакета требуемого приложения, необходимо перейти в карточку устройства во вкладку «Приложения», столбец «Инфо» (пп. 2.1.1.9). В списке отображаются названия всех пакетов со всех устройств, которые отправили свое состояние в ППО. При необходимости воспользоваться фильтром по названию пакета (ввести в поле «Название приложения» полное или частичное название

пакета). Если нужного пакета нет в списке, ввести его точное название и выбрать «Добавить <название пакета>» в раскрывающемся списке;

– если необходимо добавить еще одно приложение, то повторить шаг выше;

8) При необходимости настроить автозапуск сервисов в режиме киоска.

ПРИМЕЧАНИЕ. Управление автозапуском сервисов возможно для устройств с ОС Android 10 и выше.

Автозапуск сервисов позволяет автоматически запускать фоновые компоненты, необходимые для работы кассовых, платежных, фискальных и других бизнес-приложений. Под сервисом подразумевается только тот сервис, который может работать в фоновом режиме. Например, основное приложение терминала может использовать отдельный платежный или фискальный сервис. После применения политики, включения или перезагрузки устройства ППО попытается автоматически запустить указанный сервис.

Для настройки запуска автосервисов необходимо:

– включить переключатель «Сервисы для автозапуска»;

– заполнить поля:

- в поле «Имя пакета» ввести или выбрать из списка название пакета приложения;
- в поле «Имя сервиса» ввести полное имя класса (например, com.example.app.MyService) или сокращенное, начиная с точки (например, .MyService), если класс находится внутри указанного пакета.

Если необходимо добавить еще один сервис для запуска, то необходимо нажать значок + и повторить шаги, приведенные выше.

ПРИМЕЧАНИЕ. Максимально можно добавить пять сервисов для автозапуска.

Сервис определяется сочетанием имени пакета и имени сервиса (подробнее в пп. 2.4.1.16.7).

2.4.1.16.5. Особенности работы правила в режиме киоска

ВНИМАНИЕ! Не рекомендуется выбирать приложение «Аврора Центр» в качестве средства запуска (launcher) как при его установке, так и в дальнейшем. В противном случае выйти из режима киоска будет невозможно.

ПРИМЕЧАНИЯ:

✓ Блокировка экрана имеет приоритет над режимом киоска. При назначении политик с правилами включенной блокировки экрана и включенного режима киоска отобразится Экран блокировки, а в состоянии устройства – информация о включенной блокировке экрана и отключенном режиме киоска, вследствие чего в карточке устройства отобразится статус «Не соответствует политике»;

✓ Если в список разрешенных приложений добавить приложение по работе с файлами, то при открытии файлов будут запускаться обработчики этих файлов, даже если их нет в списке разрешенных приложений. Например, при открытии файла формата `.mp3` может запуститься медиаплеер (при его наличии на устройствах);

✓ В целях обеспечения экстренных вызовов в режиме киоска всегда доступно приложение для совершения вызовов. В случае необходимости запретить вызовы следует дополнительно назначить на устройство соответствующую политику;

✓ Ярлыки веб-страниц открываются через браузер, заданный по умолчанию. При этом:

– если заданный по умолчанию браузер выбран, то разрешенным в режиме киоска остается только он. При этом, если заданный по умолчанию браузер не добавлен в список приложений, то его иконка отображаться не будет;

– если заданный по умолчанию браузер не задан, то при открытии ярлыка пользователю будет предложено его выбрать;

✓ Адреса сайтов на кириллице необходимо добавлять в списки разрешенных/запрещенных сайтов в кодировке Punycode;

✓ При первом запуске режима киоска будет запрещен вход в безопасный режим (safeboot) на устройстве;

✓ Если устройство защищено паролем, то в режиме киоска необходимо вводить пароль при каждом включении экрана;

✓ На устройствах с ОС Android версии 7.0, 7.1, 8.0.0, 8.1.0, работающих в режиме киоска:

– при попытке выключить устройство будет отображено окно, в котором можно не только выключить или перезагрузить устройство, но и включить авиарежим, даже несмотря на запрещающее правило политики. Если включить авиарежим, то будет отображено окно с уведомлением и инструкцией как отключить авиарежим (см. Рисунок 69);

– переключение между окнами запущенных приложений запрещено;

– системные данные (время, заряд аккумулятора, уровень сигнала WLAN и т.п.) не отображаются в верхней строке состояния;

– панель уведомлений не отображается даже если отображение панели уведомлений разрешено в правиле политики;

✓ На устройствах с ОС Android версии 8.1 при включении режима киоска в момент блокировки экрана стандартным средством ОС, устройство будет не соответствовать политике в Аврора Центр, пока экран не будет разблокирован и устройство не отправит свое актуальное состояние;

✓ Особенности комбинирования политик, которые содержат разные правила режима киоска:

– пересечение приложений, ярлыков: в комбинированном варианте будут приложения и ярлыки из двух политик;

– пересечение запрещенных сайтов: в комбинированном варианте будут запрещенные сайты из двух политик;

– пересечение кодов выхода из киоска: код выхода будет отображен в окне комбинированной политики с перечнем доступных приложений, ярлыков, запрещенных ссылок, выбранного фона. Его необходимо запомнить;

✓ Чтобы отобразить в режиме киоска ярлыки к различным разделам настроек, необходимо в разделе «Приложения» в поле «Код приложения N» указать Activity нужной настройки:

– «Bluetooth»: com.android.settings/.Settings$BluetoothSettingsActivity;

– «Wi-Fi»: com.android.settings/.Settings$WifiSettingsActivity;

– «Мобильная передача данных»: com.android.settings/.Settings$WirelessSettingsActivity;

– «Геолокация»: com.android.settings/.Settings$LocationSettingsActivity;

– «Экран и яркость»: com.android.settings/.Settings$DisplaySettingsActivity;

– «Звуки и вибрация»: com.android.settings/.Settings$SoundSettingsActivity;

– «Настройки SIM», «APN»: com.android.settings/.Settings$ApnSettingsActivity.

При этом необходимо учитывать следующие ограничения, которые могут возникнуть на некоторых устройствах и версиях ОС:

– из окна с открытым разделом настроек будет возможность выйти в общие настройки;

– перечисленные выше Activity могут не сработать для открытия разделов настроек. В этом случае необходимо обратиться в техническую поддержку ООО «Открытая мобильная платформа» и в запросе указать проблемное Activity, модель и версию ОС устройства;

✓ При включенном режиме киоска (в раскрывающемся списке «Тип киоска» выбрано «Приложение») можно звонить и принимать входящие вызовы. Эта возможность будет удалена в следующих релизах ППО.

ВНИМАНИЕ! При необходимости возможно выйти из режима киоска на устройстве. Подробное описание приведено в документе «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android».

2.4.1.16.6. Комбинирование правил

Если правило «Режим киоска» включено хотя бы в одной политике, итоговая скомбинированная политика также будет считаться включенной.

Дальнейшее комбинирование выполняется только для тех политик, где режим киоска активирован.

Если среди применяемых политик есть политики для нескольких платформ (например, ОС Android и ОС Аврора одновременно), комбинирование не выполняется, и целиком выбирается правило «Режим киоска» из политики, которая была обновлена позже остальных.

Если среди включенных политик платформа одинаковая, для ОС Android действует следующий приоритет типов:

– «Приложение» выше, чем «Веб-ресурс»;

– «Веб-ресурс» выше, чем «Рабочий стол».

Это означает:

– если среди включенных политик есть хотя бы одна политика типа «Приложение», итоговая политика формируется как «Приложение», а настройки «Веб-ресурса» и «Рабочего стола» не применяются;

– если политик типа «Приложение» нет, но есть хотя бы одна политика типа «Веб-ресурс», итоговая политика формируется как «Веб-ресурс», а настройки «Рабочего стола» не применяются;

– если среди включенных политик есть только «Рабочий стол», итоговая политика формируется как «Рабочий стол».

Для типа «Приложение»:

– основное приложение берется из политики, которая была обновлена позже;

– список скрытых приложений объединяется без дубликатов;

– код выхода из режима киоска берется из политики, которая была обновлена позже остальных;

– правило отключения панели уведомлений имеет приоритет.

Для типа «Веб-ресурс»:

– стартовая страница берется из политики, которая была обновлена позже;

– панель навигации берется из политики, которая была обновлена позже;

– списки разрешенных и запрещенных ресурсов объединяются без дубликатов;

– код выхода из режима киоска берется из политики, которая была обновлена позже остальных;

– правило отключения панели уведомлений имеет приоритет.

Для типа «Рабочий стол»:

– цвет шрифта и фон берутся из политики, которая была обновлена позже;

– список приложений объединяется без дубликатов, при этом приложения из более новой политики идут первыми;

– ярлыки веб-страниц объединяются по URL;

– списки запрещенных сайтов и исключений из них объединяются;

– код выхода из режима киоска берется из политики, которая была обновлена позже остальных;

– правило отключения панели уведомлений имеет приоритет.

2.4.1.16.7. Сервисы для автозапуска

Сервис определяется сочетанием имени пакета и имени сервиса.

ПРИМЕЧАНИЕ. Для получения сервисов из APK-файла можно использовать команду:

```
aapt dump xmltree package-name AndroidManifest.xml | grep -A 2
"service"
```

где `package-name` - наименование APK-файла.

В одной политике можно указать не более 5 сервисов для автозапуска.

Ограничение введено для снижения нагрузки на устройство, так как приложение «Аврора Центр» периодически проверяет системные события, связанные с работой указанных сервисов. Увеличение количества отслеживаемых сервисов может повлиять на производительность приложения, энергопотребление устройства и выполнение других операций.

После применения политики устройство:

1) Применяет настройки выбранного типа киоска;
2) Получает список сервисов для автозапуска;
3) Пытается запустить каждый указанный сервис;
4) Сохраняет последний известный статус каждого сервиса;
5) Передает результат применения политики в ППО по общим правилам синхронизации состояния устройства.

Сервис запускается в фоновом режиме и не должен открывать пользовательский интерфейс поверх режима киоска.

ПРИМЕЧАНИЕ. Наличие приложения в списке «Разрешенные приложения» не приводит к автоматическому запуску его сервисов. Для автозапуска сервис необходимо отдельно добавить в блок «Сервисы для автозапуска».

Проверка состояния и перезапуск сервисов

После применения политики приложение «Аврора Центр» выполняет периодическую проверку состояния сервисов. Проверка инициируется с интервалом 1 минута.

Проверка выполняется в общей очереди задач приложения. Если устройство в этот момент выполняет другую длительную операцию, фактическая проверка может быть выполнена позднее.

Если приложение определяет, что сервис остановлен, оно пытается запустить его повторно. Для одного сервиса выполняется не более 3 попыток перезапуска. Если сервис успешно перезапущен, его статус обновляется на «Сервис запущен».

Если после 3 попыток сервис не удалось запустить, дальнейшие автоматические попытки прекращаются до следующего применения или переприменения политики.

Функциональность работает по принципу best effort:

– не гарантируется мгновенное обнаружение остановки сервиса;
– не гарантируется мгновенный перезапуск;
– проверка выполняется с интервалом 1 минута, но может быть отложена из-за выполнения других задач на устройстве.

Комбинирование политик

Если на устройство с ОС Android назначено несколько политик киоска, списки сервисов для автозапуска объединяются.

Одинаковым считается сервис, у которого совпадают:

– имя пакета;

– имя сервиса.

Одинаковый сервис включается в результирующую политику один раз.

Если имя пакета совпадает, а имя сервиса различается, сервисы считаются разными.

В результирующую политику может быть включено не более 5 сервисов для автозапуска.

ВНИМАНИЕ! Для автозапуска рекомендуется использовать сервисы, рассчитанные на продолжительную работу в фоновом режиме. Если сервис является кратковременным worker-сервисом, который запускается, выполняет операцию и штатно завершается, приложение может определить его как остановленный и выполнить повторную попытку запуска.

2.4.1.17.Голосовые вызовы/Исходящие вызовы

Правило разрешает или запрещает совершение исходящих вызовов с устройства.

Выбор значения из списка:

– «Разрешены»;

– «Запрещены» (при добавлении правила значение выбрано по умолчанию).

2.4.1.18.Голосовые вызовы/Входящие вызовы

Правило разрешает или запрещает входящие вызовы на устройство.

Выбор значения из списка:

– «Разрешены»;

– «Запрещены» (при добавлении правила значение выбрано по умолчанию). Входящие вызовы не будут отображаться пользователю, а звонящий абонент будет слышать гудки.

Особенности работы ограничения входящих вызовов на устройствах с ОС Android:

✓ При поступлении входящего вызова элементы интерфейса вызова могут кратковременно отображаться на экране устройства перед его ограничением;

✓ В режиме киоска возможно кратковременное появление окна входящего вызова, которое затем автоматически исчезает. Визуально это может проявляться как небольшое мерцание экрана;

✓ При работе устройства без режима киоска возможно кратковременное отображение уведомления или плашки входящего вызова, которая затем автоматически исчезает;

✓ Конкретное визуальное поведение зависит от модели устройства, версии ОС Android и используемого системного приложения для обработки вызовов. На отдельных устройствах кратковременное отображение интерфейса входящего вызова может отсутствовать;

✓ Кратковременное отображение элементов интерфейса входящего вызова не означает, что правило ограничения входящих вызовов не применилось.

2.4.1.19.Конфигурация WLAN/Режим работы WLAN

Правило позволяет:

– отключать или включать адаптер WLAN;

– зафиксировать текущее состояние адаптера WLAN.

Доступные значения для работы WLAN:

– «Не задано» – управление состоянием адаптера WLAN будет разблокировано (раскрывающийся список «Управление WLAN»);

– «Выключено» – адаптер WLAN будет выключен перманентно (включить его будет невозможно). При добавлении правила значение выбрано по умолчанию;

– «Включено» – адаптер WLAN будет включен перманентно (выключить его будет невозможно).

ВНИМАНИЕ! В зависимости от версии и прошивки ОС Android возможно наличие на устройствах пользовательских настроек, способных влиять на назначенную политику:

– журнал управления WLAN (встречается на устройствах Samsung). Позволяет запретить приложению «Аврора Центр» включать/отключать адаптер WLAN;

– автоматическое включение WLAN. Позволяет включать адаптер WLAN, когда устройство обнаружит поблизости одну из сохраненных сетей, и отключать его, если в течение некоторого времени не будет установлено соединение.

Доступные значения для управления состоянием адаптера WLAN:

– «Запрещено» – будет зафиксировано текущее состояние адаптера WLAN. При добавлении правила значение выбрано по умолчанию.

ВНИМАНИЕ! Для устройств на базе ОС Android версии 9 пользователь может вручную включить/отключить WLAN, даже если управление WLAN запрещено;

– «Разрешено» – пользователь может включать или отключать адаптер WLAN и изменять его настройки.

2.4.1.20.Конфигурация WLAN/Подключения к сети WLAN

Правило позволяет создать и настроить на устройствах подключения к сетям WLAN с технологиями безопасности WPA-EAP и WPA2. В результате устройство сможет подключаться к защищенным сетям WLAN без дополнительных действий.

ПРИМЕЧАНИЯ:

✓ Правило не сработает, если на устройствах выключен адаптер WLAN;

✓ На устройствах, функционирующих под управлением ОС Android, после включения адаптера WLAN и применения правила, момент непосредственного подключения к точке доступа зависит от версии и прошивки ОС. Если подключение к точке доступа не произошло, то следует перезагрузить устройство или выполнить подключение вручную.

Для создания правила необходимо:

1) В поле ввода «Название сети (SSID)» ввести название беспроводной сети (Service Set Identifier) для подключения. Параметр обязателен для заполнения. Название беспроводной сети должно быть уникальным в рамках правила.

ПРИМЕЧАНИЕ. Если разные политики содержат правила с одинаковым названием беспроводной сети, то при их назначении на устройстве будет применено правило с более поздней датой обновления.

ВНИМАНИЕ! Если название подключения WLAN в правиле содержит символ «/» (например, OMP/_test), то:

– на устройстве будет создано подключение WLAN в названии которого не будет указан данный символ (например, OMP_test), в результате чего устройство с символом «/» в названии не сможет подключиться к сети WLAN;

– в карточке устройства на вкладке «Состояние» будут отображены два подключения WLAN – с символом «/» в названии и без него. В результате чего устройство будет в статусе «Не соответствует политике»;

2) В поле «Скрытая сеть» при помощи переключателя возможно включить или отключить трансляцию названия беспроводной сети. При добавлении правила переключатель по умолчанию выключен;

3) В поле «Автоподключение» при помощи переключателя возможно включить или отключить автоподключение устройства к беспроводной сети. При добавлении правила переключатель по умолчанию включен.

ПРИМЕЧАНИЕ. Для устройств на базе ОС Android автоподключение работает следующим образом: в момент создания и настройки подключения будет произведена попытка подключения к точке доступа. В случае неудачи следующая попытка подключения будет произведена в соответствии с особенностями версии и прошивки ОС Android;

4) В поле «Настройка IP-адреса» по умолчанию выставлено значение «Автоматическая». Поле редактированию не подлежит;

5) Если необходимо создать подключение к беспроводной сети с технологией безопасности:

WPA2:

– в раскрывающемся списке «Безопасность» выбрать «WPA2». При добавлении правила значение выбрано по умолчанию;

– в поле «Пароль» ввести пароль беспроводной сети. Параметр не обязателен для заполнения. Если беспроводная сеть не защищена паролем, то необходимо оставить поле пустым.

ПРИМЕЧАНИЯ:

✓ Если пароль не задан, то на устройствах с ОС Android подключение не будет создано и в журнале приложения «Аврора Центр» отобразится запись об ошибке создания подключения, а на устройствах на базе ОС Аврора необходимо будет вручную ввести пароль для подключения к защищенной беспроводной сети;

✓ Пароль хранится в системе в нешифрованном виде. Просмотр пароля возможен:

– в карточке политики во вкладке «Правила» (пп. 2.1.5.1);

– в карточке устройства во вкладке «Политики» (пп. 2.1.1.5).

WPA-EAP:

Создать подключение к беспроводной сети с технологией безопасности WPA-EAP возможно по протоколу:

1. TLS (в дополнение к созданию подключения через протокол TLS будет выпущен и доставлен на устройства пользовательский сертификат для подключения к беспроводной сети).

Для подключения к беспроводной сети с технологией безопасности WPA-EAP по протоколу TLS необходимо:

– в раскрывающемся списке «Безопасность» выбрать «WPA-EAP»;

– в раскрывающемся списке «Протокол» выбрать «TLS»;

– в раскрывающемся списке «Категория сертификата» выбрать категорию пользовательских сертификатов, в рамках которой будет выпущен пользовательский сертификат. При отсутствии требуемой категории в списке необходимо добавить ее в настройках администрирования Аврора Центр (п. 4.1.2);

– в раскрывающемся списке «Идентификатор» выбрать динамическую перемененную, которая будет автоматически подставлять нужный идентификатор пользователя в подключение:

- `{{UserEmail}}` – email из карточки пользователя;
- `{{UserPrincipalName}}` – значение параметра «userPrincipalName» из LDAP-данных о пользователе.

2. PEAP.

Для подключения к беспроводной сети с технологией безопасности WPA-EAP по протоколу PEAP необходимо:

– в раскрывающемся списке «Безопасность» выбрать «WPA-EAP»;

– в раскрывающемся списке «Протокол» выбрать «PEAP»;

– в поле «2-й этап аутентификации» по умолчанию установлено значение «MSCHAPv2». Поле недоступно для редактирования;

– в раскрывающемся списке «Тип идентификации» выбрать, какой тип идентификации необходимо использовать:

• «Шаблон» – значение выбрано по умолчанию. Далее в поле «Идентификатор» в раскрывающемся списке выбрать динамическую перемененную, которая будет автоматически подставлять нужный идентификатор пользователя в подключение:

♦ `{{UserEmail}}` – email из карточки пользователя;

♦ `{{UserPrincipalName}}` – значение параметра «userPrincipalName» из LDAP-данных о пользователе;

♦ `{{sAMAccountName}}` – значение параметра «sAMAccountName» из LDAP-данных о пользователе.

ПРИМЕЧАНИЕ. Подключение к сети WPA-EAP PEAP будет создано с паролем по умолчанию (12345678). После создания подключения необходимо зайти в его настройки и вручную изменить пароль на корректное значение;

• «Логин и пароль». Далее для подключения ввести логин и пароль пользователя в соответсвующих полях. В случае незаданного пароля пользователь устройства должен будет ввести его самостоятельно.

ПРИМЕЧАНИЕ. Если требуется сменить пароль в режиме киоска (при отсутсвии прав на редактирование подключения), необходимо обратиться к администратору.

ВНИМАНИЕ!

✓ Для выпуска сертификата и корректной подстановки значения в динамическую переменную необходимо, чтобы устройство было привязано к пользователю;

✓ Если в ПУ к устройствам привязано несколько пользователей, то при создании подключения будут использоваться учетные данные пользователя, который был привязан к устройствам последним или который был получен из интеграции с LDAP. Если из LDAP получены данные нескольких пользователей, то будет выбран тот, который привязан к устройствам последним;

6) Если требуется создать подключение к сети WLAN, настроенной на прокси-сервер, необходимо перевести переключатель «Прокси-сервер» в положение  «Включено» и заполнить следующие поля:

– «Хост» – хост прокси-сервера. Поле обязательно для заполнения;

– «Порт» – по умолчанию задано значение 80. При необходимости доступно ввести другой номер порта. Поле обязательно для заполнения;

– «Исключения из проксирования» – при необходимости ввести через запятую хосты, которые будут исключениями из проксирования. Поле необязательно для заполнения.

ПРИМЕЧАНИЕ. Необходимо учитывать следующие особенности использования прокси-сервера в подключении:

– для устройств с ОС Android настроить прокси-сервер можно только в версиях 8 и выше;

– для устройств с ОС Аврора можно задавать более одного прокси-сервера на подключение. При получении настроек прокси-сервера от ОС, приложение «Аврора Центр» будет работать с прокси-сервером, который будет первым в списке серверов, полученных от ОС;

– если переключатель «Прокси-сервер» в правиле политики выключен, то это не влияет на соответствие устройства политике. После применения политики имеющиеся на устройстве настройки прокси-сервера будут удалены.

Если необходимо создать на устройствах еще одно подключение к сети WLAN, то необходимо нажать значок + внизу правила и повторить шаги, приведенные выше.

2.4.1.21.Конфигурация VPN/Подключения VPN

Правило позволяет создать подключение VPN в приложениях:

– Cisco AnyConnect для устройств ОС Android;

– КриптоПро NGate R2 для устройств на базе ОС Android и ОС Аврора.

Для создания правила необходимо:

1) В поле «Название» ввести название подключения VPN, которое должно быть уникальным в рамках правила. Параметр обязателен для заполнения.

ПРИМЕЧАНИЕ. Если разные политики содержат правила с одинаковым названием подключения VPN, то при их назначении на устройство будет применено правило с более поздней датой обновления;

2) В поле «Адрес сервера» ввести адрес сервера VPN. Параметр обязателен для заполнения;

3) В поле «Тип» выбрать одно из приложений, для которого необходимо создать подключение VPN:

– Cisco AnyConnect (при добавлении правила значение выбрано по умолчанию):

- в поле «Протокол» по умолчанию указан протокол безопасности SSL. Поле недоступно для редактирования;
- если требуется, чтобы вместе с созданием подключения VPN был выпущен и доставлен на устройство необходимый пользовательский сертификат, то в раскрывающемся списке «Категория сертификата» необходимо выбрать необходимую категорию пользовательских сертификатов, в рамках которой будет выпущен пользовательский сертификат. При отсутствии необходимой категории в списке, требуется добавить ее в подразделе «Настройки» раздела «Администрирование» (п. 4.1.2). Параметр не обязателен для заполнения;

– КриптоПро NGate R2:

- в поле «Тип аутентификации» указан тип «По логину и паролю». Поле заполнено по умолчанию и недоступно для редактирования;
- в раскрывающемся списке «Логин» необходимо выбрать динамическую перемененную, которая будет автоматически подставлять нужный логин пользователя в подключение:

- Не задано – пользователь самостоятельно вручную указывает логин на устройстве;
- `{{sAMAccountName}}` – логин пользователя (значение параметра «sAMAccountName» из LDAP о пользователе). Пример значения: ivanivanov. При добавлении правила значение выбрано по умолчанию;
- `{{UserEmail}}` – email из карточки пользователя. Пример значения: ivanov@mail.ru;
- `{{UserPrincipalName}}` – логин пользователя (значение параметра «userPrincipalName» из LDAP о пользователе). Пример значения: ivanivanov@mail.ru.

ВНИМАНИЕ! Если в ПУ к устройству привязано несколько пользователей, то при создании подключения будут использоваться учетные данные того пользователя, который был привязан к устройству позднее всех или данные пользователя, которые были получены из интеграции с LDAP. Если из LDAP получены данные нескольких пользователей, то будет выбран пользователь, который привязан к устройству позднее всех;

- в поле «Домен» необходимо ввести адрес, по которому приложение сможет построить полный адрес сервера. Домен должен быть согласованным с серверной конфигурацией, в противном случае приложение КриптоПро NGate R2 может переписать доменное имя в соответствии с серверной конфигурацией без учета данных из применяемого правила политики.

ВНИМАНИЕ! Домен поддерживается только для ОС Аврора;

- в поле «Автозапуск VPN» при помощи переключателя возможно включить или отключить автоподключение устройства к VPN. При добавлении правила переключатель по умолчанию включен.

ПРИМЕЧАНИЕ. Настройка автозапуска действует только для ОС Android;

- поле «Серийный номер лицензии» заполняется, если требуется передать в подключение VPN серийный номер лицензии. Параметр не обязателен для заполнения.

ПРИМЕЧАНИЕ. Передача серийного номера лицензии действует только для ОС Android.

Если необходимо создать еще одно подключение VPN в приложении Cisco AnyConnect для ОС Android, необходимо нажать на значок + внизу правила и повторить шаги, приведенные выше.

ВНИМАНИЕ! Для приложения КриптоПро NGate R2 можно создать только одно подключение VPN.

2.4.1.22.Конфигурация NFC/Управление NFC

Правило фиксирует текущее состояние NFC. Запрещает или разрешает вносить изменения в настройки NFC.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено» (при добавлении правила значение выбрано по умолчанию).

2.4.1.23.Конфигурация Bluetooth/Режим работы Bluetooth

Правило разрешает или запрещает возможность использовать Bluetooth®.

Выбор значения из списка:

– «Включен» – адаптер Bluetooth будет включен и пользователь сможет самостоятельно менять состояние;

– «Выключен» (при добавлении правила значение выбрано по умолчанию) – адаптер Bluetooth будет отключен и пользователь не сможет самостоятельно менять состояние.

2.4.1.24.Конфигурация/Расписание получения команд

Правило задает расписание на получение оперативных команд и политик.

Ввод значения с клавиатуры в формате: «Каждые [дд] дн. [чч] ч.».

2.4.1.25.Конфигурация/Расписание отправки состояния

Правило задает расписание отправки состояния устройства на ПУ.

Ввод значения с клавиатуры в формате: «Каждые [дд] дн. [чч] ч.».

2.4.1.26.Конфигурация/Расписание отправки событий безопасности

Правило задает расписание отправки в ПУ сообщений о событиях безопасности (`security.d journaling daemon`), произошедших на устройстве.

Ввод значения с клавиатуры в формате: «Каждые [дд] дн. [чч] ч.»

2.4.1.27.Конфигурация/Исключения событий безопасности

Правило позволяет исключить отправку определенных событий безопасности с устройств, фильтруя их по процессам и/или уровням.

Для фильтрации:

– по типу события безопасности всех процессов необходимо выбрать «Все процессы» и указать уровень событий, который следует исключить;

– по определенному событию безопасности необходимо ввести вручную путь к исполняемому файлу процесса отправителя события. Также представлена возможность дополнительно указать уровень события, которое следует исключить;

– по второму событию безопасности необходимо нажать на значок + внизу фильтра и также ввести вручную путь к исполняемому файлу процесса отправителя события. При необходимости дополнительно указать уровень события, которое следует исключить. Аналогично возможно сделать и для последующих событий безопасности, которые следует исключить.

2.4.1.28.Конфигурация/Хранение логов на устройстве

Правило позволяет задать способ хранения системных сообщений на устройствах.

Выбор значения из списка:

– «Постоянное» (значение выбрано по умолчанию) – системные сообщения хранятся в локальном хранилище устройства и сохраняются после перезагрузки устройства. Правило имеет приоритет в комбинированных политиках;

– «Временное» – системные сообщения хранятся в оперативной памяти устройства и удаляются при перезагрузке устройства.

2.4.1.29.Конфигурация/Обновление координат в клиенте Аврора Центр

Правило задает частоту обновления координат в приложении «Аврора Центр».

ВНИМАНИЕ! Обновление координат в приложении «Аврора Центр» не влияет на частоту актуализации координат самим устройством. Устройство актуализирует свои координаты независимо от того, как часто приложение «Аврора Центр» запрашивает координаты. На частоту актуализации координат устройства влияет режим работы геопозиционирования.

Ввод значения с клавиатуры в формате: «Каждые [чч] ч. [мм] м [сс] с».

ПРИМЕЧАНИЕ. При добавлении правила по умолчанию установлена частота 10 минут (значение: «Каждые [0] ч. [10] м [0] с»).

2.4.1.30.Конфигурация/Создание точек восстановления

ПРИМЕЧАНИЕ. ОС должна быть установлена на раздел BTRFS с разбивкой на подразделы @ и @home. Другие виды разделов не поддерживаются.

Правило регулирует создание точек восстановления при применении политик и автоматический возврат устройства на ранее созданные точки восстановления.

Для создания правила необходимо:

1) В поле «Исключаемые директории» (определяет директории, которые не будут включены в точку восстановления) в раскрывающемся списке выбрать необходимое значение:

– `/home` - данные из раздела `/home`, которые будут исключены только в случае, если для него выделен отдельный раздел на диске. Если раздел не выделен, исключение не произойдет, но работа системы не нарушится;

– пустое значение (выбрано по умолчанию) - исключаемые директории не будут заданы;

2) Если требуется, чтобы происходило автоматическое возвращение устройства на ранее созданные точки восстановления при отсутствии связи приложения «Аврора Центр» с сервером, необходимо перевести переключатель «Автоматическое восстановление» в положение  «Включено» и дополнительно в поле «Интервал» указать нужный временной интервал. По умолчанию переключатель выключен.

ПРИМЕЧАНИЕ. Если после применения политики, соответствующей режиму работы, связь с ПУ оборвется более чем на указанный интервал, произойдет автоматическое возвращение изменений на последнюю точку восстановления.

ВНИМАНИЕ!

✓ Крайне не рекомендуется выставлять значение интервала менее одного часа. В данный интервал входит не только время отсутствия связи при штатной работе, но и время перезагрузки устройства, установки обновлений и т.д.;

✓ По умолчанию проверка выполняется по доступности адреса http://ipv4.omprussia.ru/ . Однако ПУ может быть недоступен во время аварий и/или проведения технических работ. Для более безопасной работы автовосстановления требуется в конфигурационном файле `config/subsystems/emm/config.yml` найти параметр `networkCheckSettings` и указать в нем стабильный внутренний URL, который будет использоваться для проверки доступности сети. После этого связь будет проверяться по двум адресам, и если хотя бы один из них доступен, то автовосстановления не произойдет;

3) В раскрывающемся списке «Режим работы» выбрать необходимое значение:

– «Только при применении правил, изменяющих файловую систему» (выбрано по умолчанию). Точка восстановления будет создаваться только при применении хотя бы одного из следующих правил политики:

- «Система/Обновление ОС»;
- «Контент/Доставка на устройство»;
- «Скрипты/Выполнение на устройстве»;
- «Приложения/Управление приложениями»;

– «Всегда». Точка восстановления будет создаваться при каждом пересчете политик в приложении «Аврора Центр» (1 раз в час).

ВНИМАНИЕ! Точка восстановления будет создаваться только при наличии доступа к сети Интернет. Проверка выполняется по доступности адреса http://ipv4.omprussia.ru/. Для более безопасной проверки требуется в конфигурационном файле `/var/ocs/config/subsystems/emm/config.yml` найти параметр `networkCheckSettings` и указать в нем стабильный внутренний URL, который тоже будет использоваться для проверки доступности сети. После этого связь будет проверяться по двум адресам, и если хотя бы один из них доступен, то точка восстановления будет создана.

ПРИМЕЧАНИЯ:

✓ При создании точки восстановления система автоматически записывает локальные дату и время устройства. Если на момент создания точки восстановления дата и время устройства были изменены вручную, в дальнейшем это может привести к некорректному возвращению на такие точки. Это связано с тем, что при формировании оперативной команды система «вписывает» значение серверного времени, но точка создается по локальному времени устройства. Например, если на устройстве вручную выставлено 17.03.2024, а серверная дата 17.03.2025, то это резервное копирование данных станет «актуальным» через год;

✓ Создание точки восстановления будет происходить только при получении устройством новой версии комбинированной политики;

✓ В рамках опции «Автоматическое восстановление» связь с сервером будет проверяться однократно – при получении устройством новой версии комбинированной политики;

✓ При удалении правила «Создание точек восстановления» из политики действие этого правила будет снято с устройства.

2.4.1.31.Конфигурация/Управление часовым поясом

Правило позволяет управлять часовым поясом на устройствах с ОС Аврора, начиная с версии 4.0.2 и выше.

ПРИМЕЧАНИЕ. Для корректной работы правила рекомендуется запретить управление датой и временем, назначив правило «Ограничение доступа/Управление датой и временем» (пп. 2.4.1.9).

Для назначения часового пояс на устройство, необходимо в раскрывающемся списке «Настройка часового пояса» выбрать:

– «Определяется устройством» - для автоматического определения часового пояса устройством;

– «Ручная настройка» (при создании правила выбрано по умолчанию) - для назначения определнного часового пояс на устройство (по умолчанию выбрано значение UTC+03:00 (Москва, Волгоград, Киров, Симферополь). Дополнительно в раскрывающемся списке «Часовой пояс» выбрать нужный часовой пояс.

2.4.1.32.Конфигурация/Синхронизация времени

Правило позволяет задать режим синхронизации времени на устройствах с ОС Аврора, начиная с версии 4.0.2 и выше.

ПРИМЕЧАНИЕ. Для корректной работы правила рекомендуется запретить управление датой и временем, назначив правило «Ограничение доступа/Управление датой и временем» (пп. 2.4.1.9).

Для назначения определенного режима синхронизации на устройстве, необходимо в поле «Синхронизация времени» выбрать нужный режим:

– «Через Аврора Центр» (при создании правила выбрано по умолчанию) - синхронизация с временем серевера ППО. Синхронизация времени с сервером будет происходит раз в час;

– «Через NTP» - синхроинизация с помощью внешнего NTP-сервера;

ПРИМЕЧАНИЕ. Режим будет работать только в случае, если адреса NTP- серверов прописаны в конфигурационном файле ППО. Добавление данных адресов происходит при развертывании системы (подробнее в документе «Руководство администратора»);

– «Определяется устройством» - синхронизация времени остается на стороне устройства.

2.4.1.33.Конфигурация/Расписание перезагрузки

Правило позволяет установить расписание автоматической перезагрузки устройств без ручного вмешательства администратора.

Правило может использоваться, например, для освобождения оперативной памяти, сброса кэша или для выполнения требований стандарта PCI PED 4.

Правило позволяет настроить однократную перезагрузку устройств моментально или в заданный интервал времени.

Настройка моментальной перезагрузки

Для настройки правила с моментальной перезагрузкой устройств, необходимо:

– в раскрывающемся списке «Режим выполнения» выбрать значение «Однократно»;

– в поле «Период актуальности» указать дату и время начала и окончания действия команды;

– переключатель «Интервал» оставить в положении «Выключено».

Настройка перезагрузки в заданный интервал времени

Правило позволяет установить расписание автоматической перезагрузки устройств без ручного вмешательства администратора.

Правило может использоваться, например, для освобождения оперативной памяти, сброса кэша или для выполнения требований стандарта PCI PED 4.

Правило позволяет настроить однократную перезагрузку устройств моментально или в заданный интервал времени.

Настройка моментальной перезагрузки

Для настройки правила с моментальной перезагрузкой устройств, необходимо:

– в раскрывающемся списке «Режим выполнения» выбрать значение «Однократно»;

– в поле «Период актуальности» указать дату и время начала и окончания действия команды;

– переключатель «Интервал» оставить в положении «Выключено».

Настройка перезагрузки в заданный интервал времени

Для настройки правила с однократной перезагрузкой устройств, в заданный интервал времени необходимо:

– в раскрывающемся списке «Режим выполнения» выбрать значение «Однократно»;

– в поле «Период актуальности» указать дату и время начала и окончания действия команды;

– включить переключатель «Интервал»;

– в отобразившихся полях «с» и «до» указать временной интервал, в рамках которого должна быть выполнена перезагрузка;

Поля «Период актуальности» и «Интервал» задают разные ограничения:

– «Период актуальности» - общий период, в течение которого команда перезагрузки считается актуальной;

– «Интервал» - временной интервал внутри суток, в который устройство может выполнить перезагрузку.

Система проверяет корректность заполнения отдельных полей, например, в поле «Период актуальности» дата «До» не может быть меньше, чем дата «С», но не проверяет, пересекаются ли между собой «Период актуальности» и «Интервал». Это означает, что администратор может сохранить настройки, при которых фактически на устройстве не окажется подходящего времени для выполнения перезагрузки. В таком случае перезагрузка не будет выполнена.

Например:

Поле	Значение
Период актуальности	с 02.07.2026 15:00 до 02.07.2026 23:00
Интервал	с 14:47 до 14:12

Такой вариант может быть сохранен, так как система не выполняет кросс-проверку периода актуальности и интервала выполнения. При этом выполнение перезагрузки зависит от того, будет ли на устройстве момент времени, который одновременно входит и в период актуальности, и в интервал выполнения.

Например, если указаны следующие значения:

Поле	Значение
Период актуальности	с 02.07.2026 15:00 до 02.07.2026 23:00
Интервал	с 16:00 до 18:0

то устройство сможет выполнить перезагрузку только 02.07.2026 в период с 16:00 до 18:00.

В поле «Интервал» допускается указать значение, при котором время начала больше времени окончания.

Например:

Поле	Значение
Интервал	с 23:00 до 22:59

Такой интервал не блокируется системой. Его можно использовать для сценариев, в которых интервал выполнения переходит через границу суток.

Например, если нужно разрешить перезагрузку ночью, можно указать:

Поле	Значение
Период актуальности	с 02.07.2026 22:00 до 03.07.2026 03:00
Интервал	с 23:00 до 02:00

В этом случае у устройства будет возможность выполнить перезагрузку в ночной интервал, если оно получит правило и выполнит условия в рамках заданного периода актуальности

Настройка периодической перезагрузки

Для настройки правила с периодической перезагрузкой устройств, необходимо:

– в раскрывающемся списке «Режим выполнения» выбрать значение «Многократно»;

– при необходимости включить переключатель «Дни недели» и выбрать дни, в которые должна выполняться перезагрузка;

Для создания правила хотя бы один из переключателей «Дни недели» или «Интервал» должен быть включен и настроен.

Условия выполнения перезагрузки зависят от заполненных полей:

День недели	Интервал наполнения	Результат
Заполнено	Не заполнено	Перезагрузка выполняется один раз в каждый выбранный день недели в интервале с 00:00 до 23:59
Не заполнено	Заполнено	Перезагрузка выполняется ежедневно, один раз в течение заданного интервала
Заполнено	Заполнено	Перезагрузка выполняется в выбранные дни недели, один раз в течение заданного интервала
Не заполнено	Не заполнено	Правило нельзя сохранить

После успешной перезагрузки повторная перезагрузка в рамках этого же интервала не выполняется.

Настройка перезагрузки по дням недели

Для настройки перезагрузки по дням недели, необходимо:

– в раскрывающемся списке «Режим выполнения» выбрать значение «Многократно»;

– включите переключатель «Дни недели» и выбрать один или несколько дней, оставив поле «Интервал» незаполненным.

Например:

Поле	Значение
Дни недели	Понедельник, среда, пятница
Интервал выполнения	Не задан

В этом случае устройство будет выполнять одну перезагрузку по понедельникам, средам и пятницам в интервал с 00:00 до 23:59.

Настройка ежедневной перезагрузки в заданный интервал времени

Для настройки ежедневной перезагрузки в заданный интервал времени, необходимо:

– в раскрывающемся списке «Режим выполнения» выбрать значение «Многократно»;

– оставить переключатель «Дни недели» выключенным;

– включить переключатель «Интервал» и указать время начала и окончания интервала.

Например:

Поле	Значение
Дни недели	Не задан
Интервал выполнения	с 03:00 до 05:00

В этом случае устройство будет ежедневно выполнять одну перезагрузку в период с 03:00 до 05:00.

Настройка интервала, переходящего через границу суток

В поле «Интервал» допускается указать время начала, которое больше времени окончания. Такой интервал переходит через границу суток.

Если интервал начинается в выбранный день недели и заканчивается после 00:00, часть интервала после 00:00 относится к предыдущему дню — дню начала интервала.

Например:

Поле	Значение
Дни недели	Понедельник, вторник
Интервал выполнения	с 23:00 до 03:00

Для такого расписания формируются следующие интервалы выполнения:

День недели	Результат
Понедельник	с 23:00 понедельника до 03:00 вторника
Вторник	с 23:00 вторника до 03:00 среды

Устройство выполняет не более одной перезагрузки в рамках каждого интервала.

Например, если устройство выполнило перезагрузку во вторник в 01:00, эта перезагрузка относится к интервалу, начавшемуся в понедельник в 23:00. Повторная перезагрузка до окончания этого интервала в 03:00 не выполняется.

Следующая перезагрузка может быть выполнена во вторник с 23:00 до 03:00 среды, так как это отдельный интервал, относящийся ко вторнику.

Особенности выполнения правила

1) Если на устройстве активен входящий вызов, перезагрузка не будет выполнена;

2) Ограничения однократной перезагрузки:

– после успешной перезагрузки повторная перезагрузка по этому же правилу не выполняется;

– если устройство получило правило после окончания периода актуальности, перезагрузка не будет выполнена;

– если устройство не выполнило перезагрузку в указанный период актуальности или в заданный интервал выполнения, повторная попытка возможна только пока условия правила остаются актуальными;

3) Ограничения периодической перезагрузки:

– в рамках одного подходящего интервала устройство выполняет не более одной успешной перезагрузки. После успешной перезагрузки повторные попытки в рамках этого же интервала не выполняются;

– если устройство не выполнило перезагрузку в заданный день или интервал выполнения, следующая попытка возможна при наступлении следующих условий, соответствующих расписанию;

– если на устройстве активен входящий вызов, перезагрузка не будет выполнена. Повторная попытка выполняется только пока сохраняются условия, заданные в правиле. Например, если интервал выполнения задан с 03:00 до 05:00 и в момент попытки перезагрузки на устройстве активен входящий вызов, устройство сможет повторить попытку только до окончания заданного интервала. Если до 05:00 перезагрузка не будет выполнена, следующая попытка станет возможна при наступлении следующего периода, соответствующего расписанию.

Особенности расчета соответствия после перезагрузки через оперативное управление

Если на устройство назначено правило «Конфигурация/Расписание перезагрузки», система рассчитывает соответствие устройства политике с учетом времени последней выполненной перезагрузки.

Перезагрузка может быть выполнена не только по расписанию из политики, но и через команду оперативного управления. В этом случае время последней перезагрузки устройства обновляется.

Из-за этого возможна ситуация, при которой:

– устройство успешно выполнило перезагрузку по расписанию из политики;

– устройство находится в статусе соответствия политике;

– позже администратор выполнил перезагрузку устройства через оперативное управление;

– команда оперативного управления выполнилась успешно;

– после этого устройство может перейти в статус несоответствия политике, если время последней перезагрузки не попадает в условия правила расписания перезагрузки.

Такое поведение не означает ошибку выполнения команды оперативного управления или ошибку применения политики. Устройство переходит в несоответствие, потому что последняя зафиксированная перезагрузка была выполнена вне условий, заданных в правиле расписания перезагрузки.

Пример:

На устройство назначена политика с правилом «Конфигурация/Расписание перезагрузки». В правиле задан интервал выполнения перезагрузки: с 07:00 до 08:00.

Устройство выполнило перезагрузку по политике в 07:30. После этого устройство соответствует политике. Позже администратор перезагрузил это же устройство через оперативное управление в 12:00.

Так как последняя перезагрузка устройства теперь выполнена в 12:00, то есть вне интервала с 07:00 до 08:00, устройство может перейти в статус несоответствия политике.

При этом сама перезагрузка через оперативное управление считается успешно выполненной.

Для однократных правил рекомендуется удалять из политики правила перезагрузки, которые уже выполнились и больше не актуальны. Это позволит избежать ситуации, когда устройство отображается как несоответствующее политике из-за устаревшего правила.

2.4.1.34.Конфигурация/Настройка прокси-сервера

Правило позволяет настроить подключение к прокси-серверу.

Для создания правила необходимо заполнить следующие поля:

– «Хост» – ввести хост прокси-сервера. Поле обязательно для заполнения;

– «Порт» – по умолчанию задано значение 80. При необходимости ввести другой номер порта. Поле обязательно для заполнения;

– «Имя пользователя» – при необходимости ввести имя пользователя. Поле необязательно для заполнения;

– «Пароль» – ввести пароль пользователя. Поле обязательно для заполнения, если было введено имя пользователя.

ПРИМЕЧАНИЕ. Пароль хранится на сервере в незашифрованном виде;

– «Исключения из проксирования» – при необходимости ввести через запятую хосты, которые будут исключены из проксирования. Поле необязательно для заполнения.

После доставки политики для применения настроек прокси-сервера необходимо произвести повторную авторизацию на устройстве или перезагрузить устройство.

При назначении политики необходимо учитывать следующие особенности:

– пароль хранится на сервере в незашифрованном виде. При этом приложение «Аврора Центр» передает с устройства в «Текущее состояние» и ожидаемом состоянии пароль в виде хэша (sha256);

– для логина и пароля нельзя использовать специальные символы, т.к. устройство не сможет правильно прочитать настройки прокси-сервера из файла;

– если будет использоваться прокси-сервер с протоколами HTTPS или FTP, то сначала нужно настроить переадресацию на этом прокси-сервере, поскольку на устройство автоматически подставляется адрес прокси-сервера с использованием протокола HTTP.

2.4.1.35.Конфигурация/Таймаут экрана

Правило позволяет установить время бездействия пользователя, по истечении которого экран устройства будет заблокирован.

Для создания правила необходимо указать время таймаута в формате [количество минут] м. [количество секунд] с.

При добавлении правила в политику по умолчанию установлено время – 1 минута.

ПРИМЕЧАНИЯ:

✓ На устройствах с ОС Android по умолчанию переход в спящий режим и переход в режим блокировки совпадают, если не были изменены настройки, отвечающие за блокировку экрана;

✓ На устройствах с ОС Android доступны дискретные (фиксированные) значения времени, которые выбираются в интерфейсе. Если указанное в правиле значение не совпадает с одним из таких значений, поведение может зависеть от производителя устройства (вендора): один производитель может корректно обработать такое значение и отобразить его, другой — отобразить пустое значение или обработать его иначе. То, как отображаются значения, не входящие в набор предустановленных значений прошивки, определяется производителем устройства;

✓ Если требуется отключить блокировку устройства с ОС семейства Linux, указать в правиле – 0 м.0 с.

2.4.1.36.Конфигурация принтеров/Управление принтерами

Правило позволяет добавить конфигурацию принтера на устройство.

Для добавления принтер на устройство, необходимо:

– в поле «Имя принтера» ввести название принтера;

– в поле «Адрес подключения» нужно указать адрес подключения принтера;

– при необходимости перевсести переключатель «Принтер по умолчанию» в положение «Включено», в результате указанный принтер будет использоваться для печати по умолчанию.

ПРИМЕЧАНИЕ. Если имя принтера из правила совпадает с именем принтера на устройстве, то конфигурация такого принтера обновится.

2.4.1.37.Конфигурация репозиториев/Подключение системных репозиториев

Правило позволяет подключить корпоративные репозитории на платформе Linux, чтобы пользователь мог устанавливать/обновлять ПО из этих репозиториев.

Для создания правила необходимо заполнить следующие поля (Рисунок 70):

1) «Параметры подключения» – поле обязательно для заполнения. Ввести параметры подключения к системному репозиторию. Формат параметров зависит от ОС.

Примеры:

– ОС Альт Linux:

```
rpm https://repo.drweb.com/drweb/altlinux 11.0/x86_64 drweb
```

– ОС Astra Linux и ОС Ubuntu:

```
deb http://repo.drweb.com/drweb/debian 10.0.0 non-free
```

– РЕД ОС:

```
[drweb]
name=DrWeb - 11.0
baseurl=https://repo.drweb.com/drweb/el5/11.0/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```

В параметрах подключения возможно использовать:

– любой протокол, который поддерживает система, если настраивается подключение к незащищенному репозиторию;

– только протоколы http и https, если настраивается подключение к защищенному репозиторию. Подробная информация о защищенных репозиториях приведена ниже;

2) «Требуется аутентификация». Настройка отвечает за подключение к защищенному репозиторию.

Защищенные репозитории - корпоративные репозитории, доступ к которым необходимо обеспечить для устройств компании, которые находятся вне корпоративной сети, при этом возможность использовать их какими-либо другими внешними устройствами должна отсутствовать.

Если репозиторий:

– Не является защищенным, необходимо перевести переключатель «Требуется аутентификация» в положении «Выключен».

Пример настройки незащищенного репозитория `drweb` для ОС Альт Linux: в «Параметры подключения» ввести строку (с учетом формата, требуемого для данного дистрибутива ОС) rpm https://repo.drweb.com/ drweb/altlinux 11.0/x86_64 drweb, переключатель «Требуется аутентификация» должен быть в положении «Выключен»;

– Защищенный, перевести переключатель «Требуется аутентификация» в положение «Включен».

Правило «Подключение системных репозиториев» для защищенных репозиториев предполагает использование контент-серверов. Адрес проксируемого репозитория должен быть указан в конфигурационном файле ППО при развертывании (переменная `linuxRepoAddress`, подробнее о подключении репозитория для ОС семейства Linux через контент-сервер ППО приведено в документе «Руководство администратора»).

Пример настройки репозитория `drweb` для ОС Альт Linux (как защищенного): в «Параметры подключения» ввести строку (с учетом формата, требуемого для данного дистрибутива ОС) rpm http://content01.ocs-content.ompcloud.ru/pkgrepo/linux/drweb/altlinux 11.0/x86_64 drweb, где:

– `content01.ocs-content.ompcloud.ru` - адрес контент-сервера (адрес самого проксируемого репозитория `drweb` указывается в конфигурационном файле ППО при развертывании, переменная `linuxRepoAddress`);

– `pkgrepo/linux` - обязательный `base path` для репозиториев.

Переключатель «Требуется аутентификация» должен быть в положении «Включен».

Если требуется:

– добавить еще один репозиторий в политику, необходимо нажать на значок + и повторить шаги, приведенные выше;

– удалить репозиторий из правила, нажать на значок «Удалить» справа от названия репозитория.

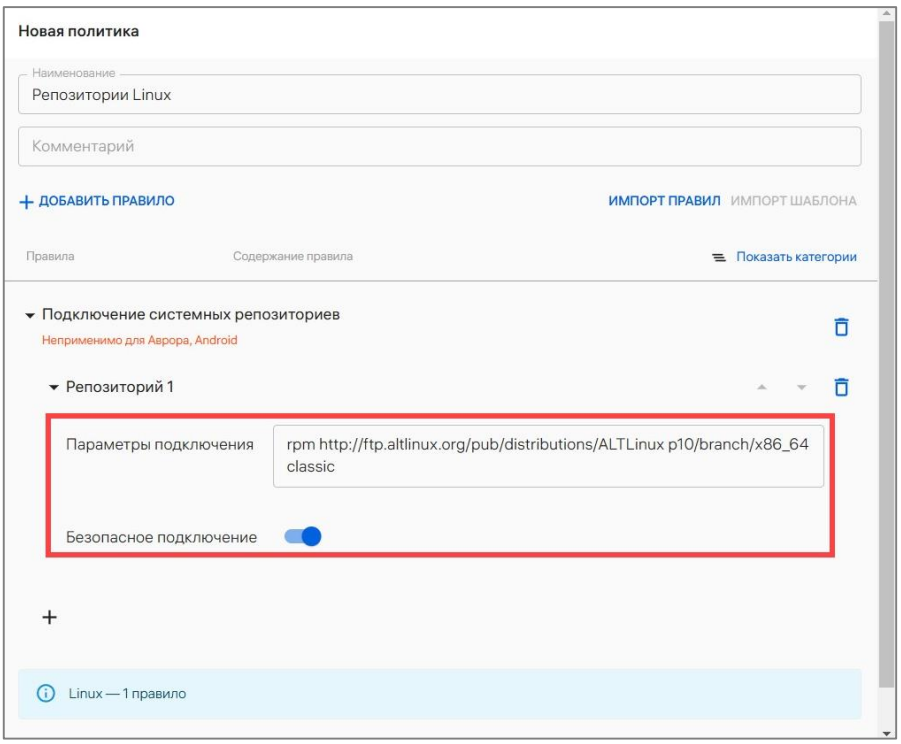


Рисунок 70

2.4.1.38.Конфигурация репозиториев/Подключение flatpak репозиториев

Правило позволяет подключить открытые и защищенные (требующие аутентификацию) flatpak репозитории, чтобы пользователь мог устанавливать/обновлять соответствующее программное обеспечение из этих репозиториев.

ПРИМЕЧАНИЕ. Защищенные репозитории - корпоративные репозитории, доступ к которым необходимо обеспечить для устройств компании, которые находятся вне корпоративной сети, при этом возможность использовать их какими-либо другими

внешними устройствами должна отсутствовать. Для корректного подключения к репозиторию требуется запросить у администратора, который разворачивал ППО, параметры подключения к репозиторию.

Для создания правила необходимо в поле «Параметры подключения» (Рисунок 71) ввести параметры подключения к flatpak репозиторию (поле обязательно для заполнения). Подробнее о параметрах подключения приведено ниже.



Рисунок 71

Если необходимо подключить:

– открытый flatpak репозиторий (не требующий аутентификации), то переключатель «Требуется аутентификация» должен находиться в положении «Выключено».

– защищенный flatplak репозиторий, то переключатель «Требуется аутентификация» должен находиться в положении «Включено».

Если требуется:

– добавить еще один репозиторий в политику, нажать на значок + внизу правила и повторить шаги, приведенные выше;

– удалить репозиторий из правила, нажать на значок 🗑 «Удалить» справа от названия репозитория.

ПРИМЕЧАНИЕ. При комбинировании политик:

– список репозиториев будет объединяться, при этом первыми в списке будут репозитории из политики, которая была обновлена позже;

– репозитории из более старых политик добавляются в конец списка, исключая дубликаты уже имеющихся репозиториев.

Подключение к открытому репозиторию.

Параметры подключения к репозиторию необходимо заполнять в формате: `<имя репозитория> <адрес конфигурационного файла>`.

ПРИМЕЧАНИЯ:

✓ Имя репозитория может быть любым, отображается только в списке подключенных репозиториев на устройстве. Поддерживаются только латиница и цифры;

✓ Имя репозитория должно отделяться одним пробелом от адреса конфигурационного файла.

```
flathub https://flatpak.elementary.io/repo.flatpakrepo
```

Подключение с аутентификацией (внутренние защищенные репозитории).

ВНИМАНИЕ! Для подключения к репозиторию с аутентификацией необходимо сделать предварительную настройку flatpack репозиториев. Подробнее в документе «Руководство администратора» в разделе по настройке подключения flatpak репозиториев.

Для подключения к репозиторию через политику в поле «Параметры подключения» (Рисунок 72) следует прописать строку, содержащую адрес контент-сервера. Пример:

```
<имя репозитория> https://<адрес контент
сервера>/pkgrepo/linux/flatpak/test-flatpak/<путь к файлу <имя
файла>.flatpakrepo>
```

ПРИМЕЧАНИЯ:

✓ Имя репозитория может быть любым, отображается только в списке подключенных репозиториев на устройстве. Поддерживаются только латиница и цифры;

✓ Контент-сервер при получении запроса проксирует его на `<адрес репозитория из config-файла>`.

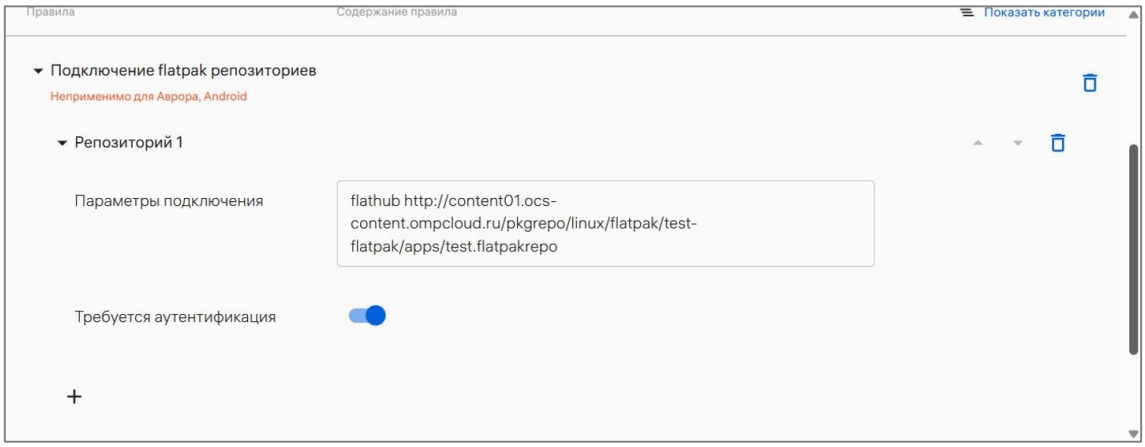


Рисунок 72

2.4.1.39.Конфигурация хранилища/Шифрование файлового хранилища

ВНИМАНИЕ!

✓ Некоторые версии ОС Android могут не поддерживать шифрование файлового хранилища. Поддержка шифрования файлового хранилища отображается в карточке устройства. Для этого во вкладке «Состояние» выбрать «Все» и в разделе «Система» проверить значение параметра «Шифрование файлового хранилища», в текущем состоянии которого передается одно из возможных значений: «Включено», «Выключено», «Не поддерживается»;

✓ На некоторых версиях ОС Android для обеспечения корректного процесса шифрования требуется выполнить следующие условия:

1) Зарядить полностью аккумулятор устройства;

2) Подключить устройство к заряду;

3) Возможно после назначения политики с шифрованием потребуется подтвердить процедуру на устройстве пользователя (Рисунок 73).

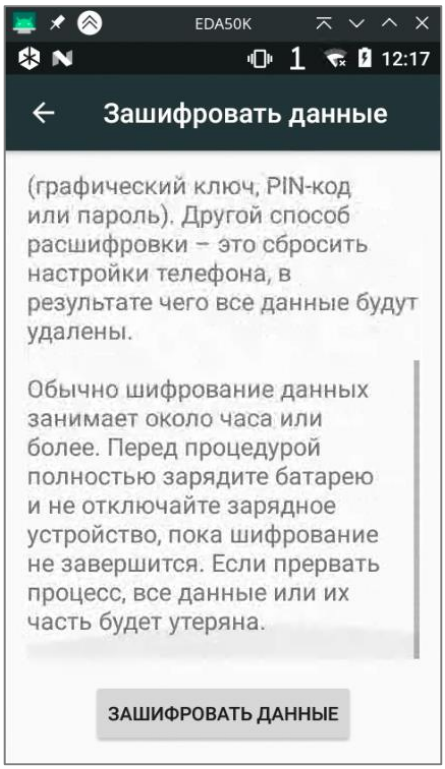


Рисунок 73

ПРИМЕЧАНИЯ:

✓ Устройство может перезагружаться до начала и окончания процесса шифрования;

✓ Не рекомендуется отключать устройство от зарядного устройства, чтобы шифрование выполнилось корректно;

✓ Процесс шифрования может занимать неопределенное время.

Также рекомендуется выполнить все описанные выше условия вне зависимости от версии ОС Android на устройстве.

Чтобы создать политику с правилом «Конфигурация хранилища/Шифрование файлового хранилища», необходимо добавить его в существующую или новую политику. При этом будет отображаться недоступный раскрывающийся список с одним значением «Включено» (Рисунок 74).

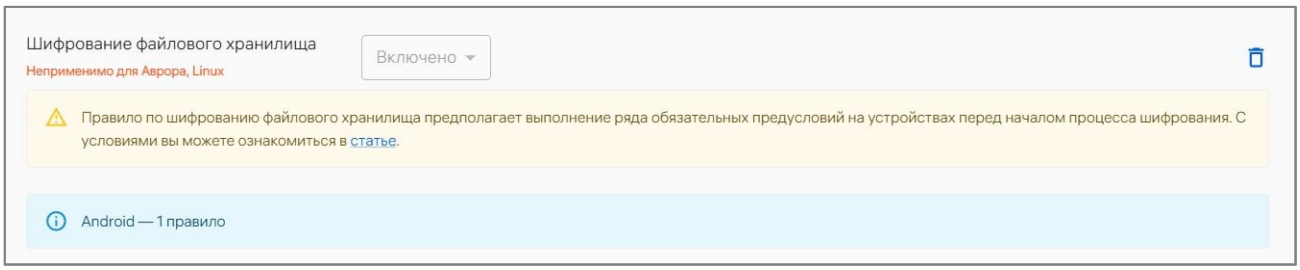


Рисунок 74

ВНИМАНИЕ! Если на устройство назначена политика с включенным режимом киоска, то для подтверждения и выполнения шифрования требуется добавить любое приложение с настройками в режим киоска (Рисунок 75). Например: `com.android.settings`.

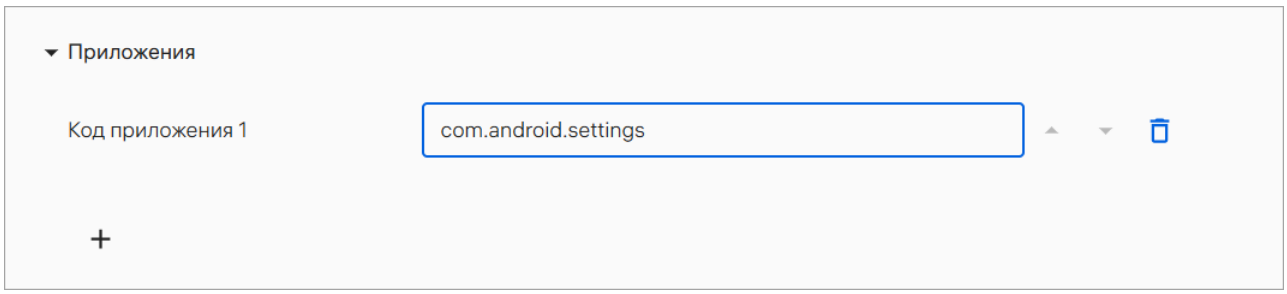


Рисунок 75

2.4.1.40.Система/Обновление ОС

Правило предназначено для обновления ОС на устройствах.

Правило задает:

– для ОС Аврора:

- версию ОС, которая будет установлена на устройстве. Список версий ОС заполняется в соответствии с версиями дистрибутивов в файловом хранилище ПООС. Описание ПООС приведено в документе «Руководство администратора»;
- временной интервал, в течение которого на устройство будет установлена указанная версия ОС;

– для ОС Альт Linux:

- объект обновления: пакеты и/или ядро;
- пред- и постнастройка с помощью выполнения необходимых скриптов (например, для переключения репозитория с одной версии ОС на другую);
- временной интервал, в течение которого на устройство будут установлены обновления ОС;
- частоту проверки доступных обновлений ОС на устройстве;
- предварительную загрузку пакетов для обновления ОС после их обнаружения;
- перенос пользователем ЭВМ начала обновления ОС и ее перезагрузку (после успешного обновления) с помощью уведомления на ЭВМ;

• опциональное обслуживание ОС до или после успешного обновления: удаление неиспользуемых пакетов, ранее скаченных пакетов, дубликатов пакетов, старых ядер; перезагрузка ОС;

• опциональные проверки устройства перед выполнением обновления: минимальная свободная оперативная память, минимальное свободное доступное место на диске после обновления, максимальная загруженность процессора.

Создание правила по установке версии ОС Аврора:

– в поле «Платформа» в раскрывающемся списке выбрать «Аврора». При добавлении правила это значение выбрано по умолчанию;

– в поле «Установить версию ОС» задать версию ОС, которая будет установлена на устройствах. Список версий ОС заполняется в соответствии с версиями дистрибутивов в файловом хранилище ПООС. Описание ПООС приведено в документе «Руководство администратора»;

– задать временной интервал, в течение которого на устройствах будет установлена указанная версия ОС. Выбор времени старта и завершения обновления в формате: «Установка с» [чч:мм] и «Установка до» [чч:мм]»;

– на устройство будет установлена указанная версия ОС. Если текущая версия ОС Аврора выше или соответствует версии из политики, обновление ОС Аврора не выполняется.

ПРИМЕЧАНИЕ. Под обновлением ОС понимается инициализация в защищенной ОС процессов получения пакетов с изменениями защищенной ОС (образа защищенной ОС) из доверенного хранилища и их установки. Получение пакетов с изменениями защищенной ОС и их установка осуществляется штатными средствами защищенной ОС. ППО не гарантирует успех получения пакетов с изменениями защищенной ОС и их установки;

Создание правила по установке версии ОС Альт Linux:

ВНИМАНИЕ! Не рекомендуется прерывать процесс установки обновления, особенно это важно при обновлении ядра и его модулей. Это может вызвать сбой ОС.

1) В поле «Платформа» в раскрывающемся списке выбрать «Linux» (Рисунок 76 [1]);

2) В разделе «Установить версию ОС» задать временной интервал, в течение которого на устройство будут установлены обновления ОС (Рисунок 76 [2]). Выбор времени старта и завершения обновления в формате: «Установка с» [чч:мм] и «Установка до» [чч:мм]».

ПРИМЕЧАНИЕ. В поле «Версия ОС» будет установлено значение «latest», которое нельзя изменить. Это означает, что будут установлены последние доступные версии пакетов и/или ядра;

3) В раскрывающемся списке «Тип установки» выбрать, по какому времени производить обновление ОС:

– «По локальному времени устройства». Выбрано по умолчанию;

– «По абсолютному времени». Дополнительно в раскрывающемся списке «Часовой пояс» выбрать часовой пояс, по времени которого нужно выполнить обновление ОС;

4) Перевести переключатель «Пробуждение устройств» (Рисунок 76 [3]) в положение «Включено» (по умолчанию он выключен), если требуется, чтобы устройство пробуждалось для обновления ОС в назначенный интервал.

ВНИМАНИЕ! Пробуждение устройств имеет ряд требований и особенностей, подробное описание приведено в приложении (Приложение 8);

5) В поле «Пользователь может перенести обновление» (Рисунок 76 [4]) по умолчанию включена опция с максимальным временем переноса 8 часов. При необходимости выключить опцию или изменить максимальное время переноса. При включенной опции пользователю ЭВМ будет показано уведомление о начале обновления с возможностью его отложить (при условии, что не превышено максимальное время переноса);

6) В поле «Интервал проверки обновлений» (Рисунок 76 [5]) ввести в часах частоту проверки доступных обновлений ОС на ЭВМ. По умолчанию задана частота 3 часа;

7) Перевести переключатели, отвечающие за объекты обновления (Рисунок 76 [6]), в положение «Включен» (по умолчанию они выключены):

– «Обновить пакеты» - будут обновлены пакеты, для которых в подключенных репозиториях есть доступные новые версии;

– «Обновить ядро» - будет обновлено ядро и его модули, если в подключенных репозиториях есть доступные новые версии;

8) Остановка обновления ядра при удалении модуля. При обновлении ядра может произойти ситуация, когда один или несколько его модулей будут удалены. Если в этом случае необходимо остановить обновление ядра, то перевести переключатель «Остановить обновления ядра, если хотя бы 1 модуль удаляется» (Рисунок 76 [7]) в положение «Включен» (по умолчанию он выключен и отображается, если «Обновить ядро» включено);

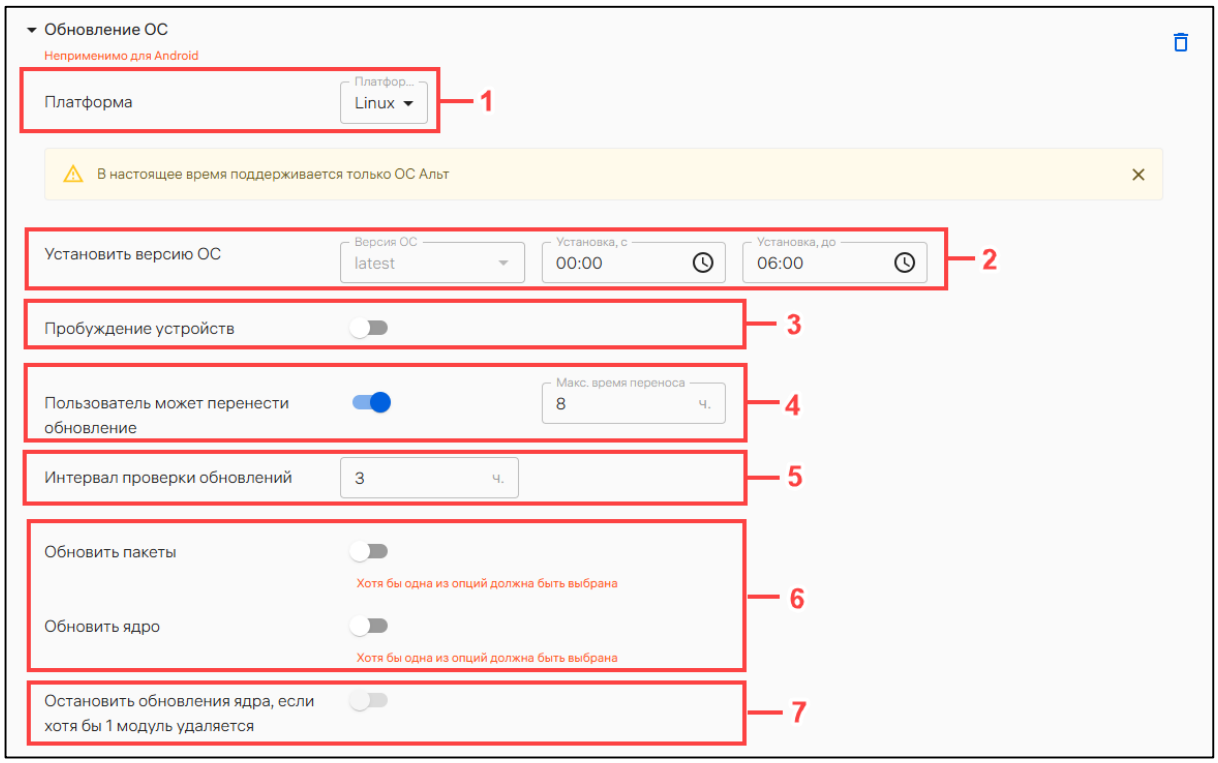


Рисунок 76

9) Если необходимо, чтобы доступные обновления ОС загрузились на ЭВМ до начала обновления ОС, то перевести переключатель «Предварительное скачивание обновлений» в положение «Включено» (Рисунок 77 [1]). По умолчанию он выключен;

10) Если необходимо, чтобы перед предварительным скачиванием обновлений ОС было выполнено удаление дубликатов пакетов, то перевести переключатель «Удалять дубликаты при предварительном скачивании» в положение «Включено» (Рисунок 77 [2]). По умолчанию он выключен и доступен для включения/выключения, если включен переключатель «Предварительное скачивание обновлений».

ВНИМАНИЕ! Наличие на устройстве дубликатов пакетов может быть причиной неудачного обновления ОС. Для их удаления можно использовать опцию «Удалять дубликаты при предварительном скачивании». Если она включена в правиле политики, то попытка удаления дубликатов будет выполняться перед предварительным скачиванием обновлений. Если попытка удаления дубликатов прошла неуспешно, то предварительное скачивание и обновление ОС не будет запущено. В этом случае необходимо удалить дубликаты пакетов вручную и затем повторить попытку обновления ОС;

11) При необходимости в поле «Выполнить скрипт до обновления» в раскрывающемся списке «Путь к файлу» выбрать путь к скрипту на устройстве (Рисунок 77 [3]), который необходимо выполнить до начала обновления. Путь к скрипту возможно выбрать только при наличии правила по доставке файлов/папок в политике. Если в раскрывающемся списке «Путь к файлу» нет нужного скрипта, нажать

«Добавить доставку на устройство» и заполнить параметры правила по доставке контента (пп. 2.4.1.46);

12) Если требуется, чтобы перед проверкой доступных обновлений ОС был выполнен скрипт, заданный на шаге 9, перевести переключатель «Выполнить указанный скрипт перед проверкой обновлений» в положение «Включено». По умолчанию он выключен и доступен для включения/выключения, если на шаге 9 был задан скрипт;

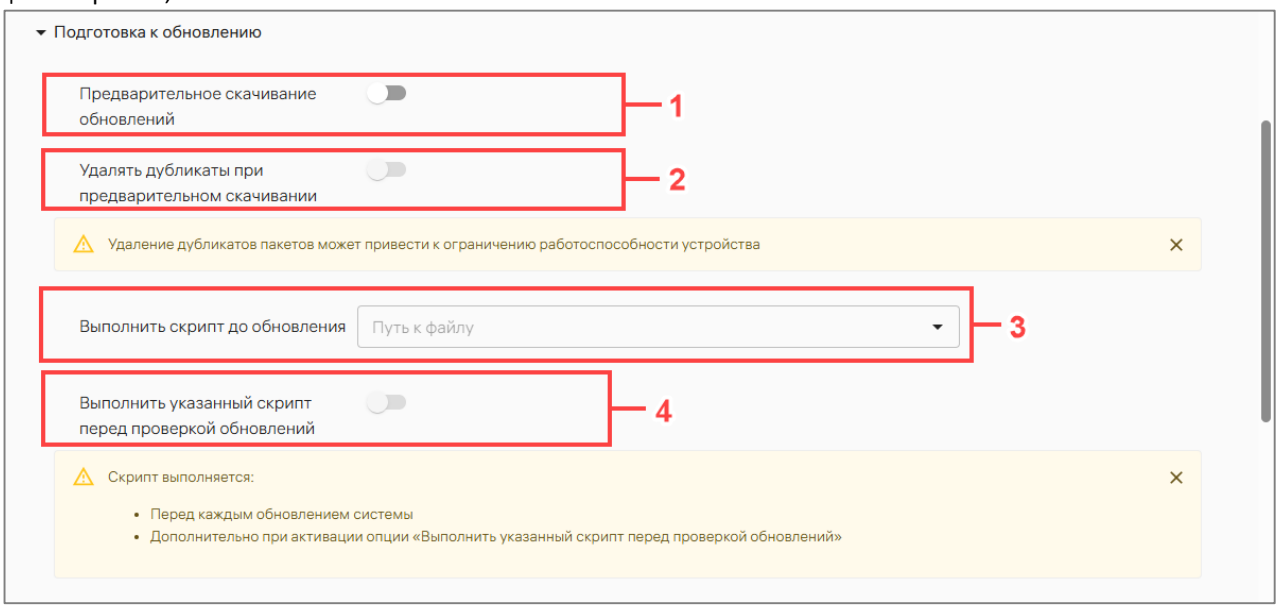


Рисунок 77

13) При необходимости в разделе «Условия для обновления» (Рисунок 78 [1]) задать условия, которые должны быть выполнены на устройстве для инициализации обновления:

– «Минимальное свободное место на диске после обновления» - ввести минимальное свободное место на диске после обновления в МиБ;

– «Минимальная свободная оперативная память» - ввести минимальную свободную оперативную память в МиБ;

– «Максимальная загруженность процессора» - ввести максимальную загруженность процессора в процентах;

14) Если необходимо, чтобы перед обновлением ОС было выполнено удаление дубликатов пакетов, то перевести переключатель «Удаление дубликатов до обновления ОС» в положение «Включено» (Рисунок 78 [2]). По умолчанию он выключен.

ВНИМАНИЕ! Наличие на устройстве дубликатов пакетов может быть причиной неудачного обновления ОС. Для их удаления можно использовать опцию «Удаление дубликатов до обновления ОС». Если она включена в правиле политики, то попытка удаления дубликатов будет выполняться перед установкой обновлений. Если попытка удаления дубликатов прошла неуспешно, то обновление ОС не будет запущено. В этом

случае необходимо удалить дубликаты пакетов вручную и затем повторить попытку обновления ОС;

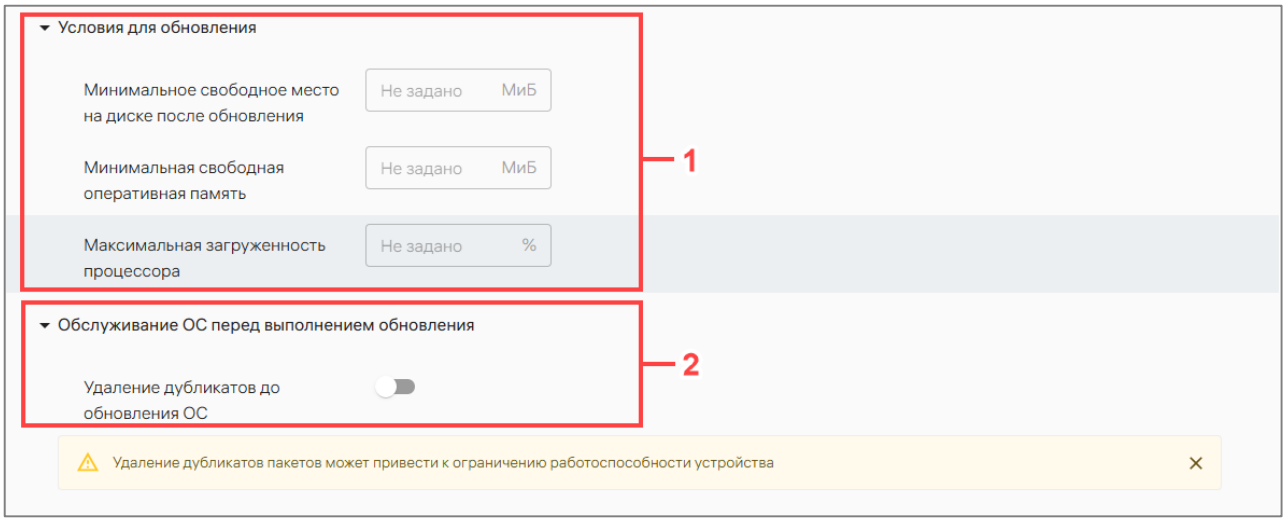


Рисунок 78

15) При необходимости в поле «Выполнить скрипт после обновления» (Рисунок 79 [1]) в раскрывающемся списке «Путь к файлу» выбрать путь к скрипту на устройстве, который необходимо выполнить после завершения обновления. Путь к скрипту возможно выбрать только при наличии правила по доставке файлов/папок в политике. Если в раскрывающемся списке «Путь к файлу» нет нужного скрипта, то необходимо нажать «Добавить доставку» на устройство и заполнить параметры правила по доставке контента;

16) В разделе «Обслуживание ОС после выполнения обновления» перевести нужные переключатели, отвечающие за объекты обновления, в положение «Включен» (Рисунок 79 [2]) (по умолчанию они выключены и отображаются, если «Обновить пакеты» или «Обновить ядро» включено):

– «Удаление ранее скачанных пакетов»;
– «Удаление неиспользуемых пакетов».

ПРИМЕЧАНИЕ. Наличие на устройстве повторов пакетов может быть причиной сбоя обновления ОС. Для их удаления возможно использовать опцию «Удаление дубликатов пакетов». Если она активирована в правиле политики, то попытка удаления повторов будет выполняться перед установкой обновлений. Если попытка удаления дубликатов прошла неуспешно, то обновление ОС не будет запущено. В этом случае необходимо удалить повторы пакетов вручную и затем повторить попытку обновления ОС;

– «Удаление старых ядер»;
– «Перезагрузка ОС»;
– «Пользователь может перенести перезагрузку». Опция доступна для включения/выключения, если включена опция «Перезагрузка ОС». Если включена опция «Перезагрузка ОС», то по умолчанию опция «Пользователь может перенести перезагрузку» включена с максимальным временем переноса 8 часов. При

необходимости доступно выключить опцию или изменить максимальное время переноса. При включенной опции после успешного обновления ОС пользователю ЭВМ будет показано уведомление о начале перезагрузки ОС с возможностью ее отложить (при условии, что не превышено максимальное время переноса).

ВНИМАНИЕ! Из-за проблемы в ОС Альт Linux после обновления с версии 10.4 на версию 11 может произойти сбой пользовательской сессии с отображением черного экрана. Чтобы избежать подобной ситуации при мажорном обновлении ОС с помощью ППО, в правиле политики «Система/Обновление ОС»:

– включить опцию «Перезагрузка ОС»;

– выключить опцию «Пользователь может перенести перезагрузку»;

– ознакомиться с рекомендациями в статье https://www.altlinux.org/Update/p11#4._Обновиться_до_p11.

ПРИМЕЧАНИЕ. Включенные опции обслуживания ОС будут выполнены только после успешной установки обновлений ОС.

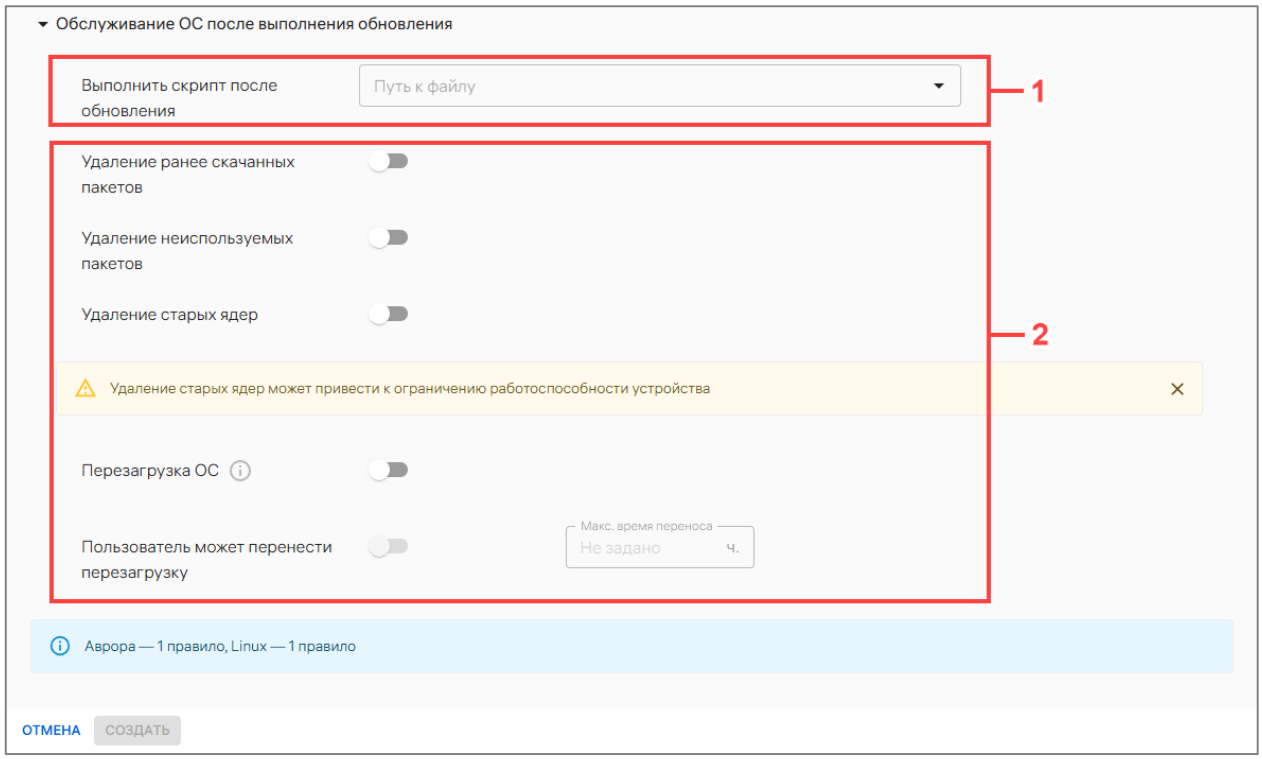


Рисунок 79

ПРИМЕЧАНИЕ. Особенности установки обновлений ОС Альт Linux приведены в документе «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

2.4.1.41.Настройки пользователя/Требования к паролю

Правило задает следующие параметры:

– сложность пароля для разблокировки устройства;

– срок действия пароля;

– включение/отключение пароля на устройстве (только для устройств с ОС Android версии 8 и выше).

Для создания правила необходимо:

1) Перевести переключатель «Использовать пароль» в нужное положение. При добавлении правила он включен по умолчанию.

ВНИМАНИЕ! Выключение пароля (сброс пароля) доступно только для устройств с ОС Android версии 8 и выше.

Возможность сброса пароля администратором зависит от того, когда было установлено приложение «Аврора Центр» и когда был задан пароль. Просмотр возможности сброса пароля доступен в карточке устройства. Для этого во вкладке «Состояние» необходимо выбрать «Все» и в разделе «Пользователь» проверить наличие параметра «Управление сбросом пароля». Возможные значения:

– «Активировано». Отображается, если приложение «Аврора Центр» установлено и запущено до установки пароля. В таком случае функция сброса пароля активируется автоматически;

– «В ожидании подтверждения пароля». Пароль на устройстве был установлен во время начальной настройки устройства (Startup Wizard) после установки приложения «Аврора Центр» через QR-код. Тогда токен безопасности не успевает активироваться. В журнале приложения «Аврора Центр» появится сообщение «Ошибка активации функции сброса пароля». На устройстве отобразится несбрасываемое уведомление «Требуется подтверждение пароля». Для активации функции сброса пароля необходимо нажать на уведомление и ввести текущий пароль устройства;

– «В ожидании сброса устройства». Пароль на устройстве был установлен до установки приложения «Аврора Центр». В этом случае регистрация токена сброса пароля невозможна. Единственный способ сброса пароля — сброс устройства до заводских настроек с последующей установкой приложения «Аврора Центр» перед установкой нового пароля;

– «Не поддерживается» – отображается для устройств, функционирующих на ОС Аврора, ОС Android либо ОС семейства Linux версии 7 и ниже;

– «Ошибка активации» – отображается при возникновении ошибок во время активации функции сброса пароля. В этом случае необходимо собрать системные сообщения с устройства (подробнее в приложении документа «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android») и отправить их в запросе в техническую поддержку пользователя или в техническую поддержку компании ООО «Открытая мобильная платформа»;

– «Неизвестно» – отображается при неудачных попытках чтения записей из базы данных. В этом случае необходимо собрать системные сообщения с устройства (подробнее в приложении документа «Руководство пользователя. Часть 9. Приложение «Аврора Центр» для операционной системы Android»);

2) Если перключатель «Использовать пароль» включен, то необходимо в раскрывающемся списке:

– «Сложность» – сложность пароля выбрать одно из значений:

• «Обычная» – позволяет задать пароль длиной от 7 до 10 символов. Может состоять только из цифр либо включать цифры, буквы и спецсимволы. При добавлении правила значение устанавливается по умолчанию;

• «Высокая» – позволяет задать пароль длиной от 8 до 12 символов и не менее заданной в правиле. Может включать цифры, буквы и спецсимволы. В зависимости от ОС, предъявляются следующие требования:

♦ для ОС Аврора: пароль должен содержать цифры, строчные буквы, прописные буквы и специальные символы;

♦ для ОС Android: пароль должен содержать цифры, специальные символы или строчные/прописные буквы;

– «Символов» - количество символов в пароле. Доступные значения зависят от выбранной сложности;

– «Срок, дней» - срок действия пароля в днях. Доступные значения: 30, 60, 90, 120, 150, 180 дней.

ВНИМАНИЕ! При назначении политики устанавливается запрет на изменение требований к паролю. Если после этого будет удалена политика «Требования к паролю», то запрет на изменения все еще будет действовать на устройстве.

ПРИМЕЧАНИЯ:

✓ Для ОС Аврора:

– в версии 4.0.2 и выше правило для пароля действует для учетной записи как пользователя, так и администратора устройства;

– за 6 дней до окончания срока действия пароля приходит уведомление о необходимости сменить пароль;

✓ Для ОС Android:

– не отображается уведомление с напоминанием о смене пароля;

– по истечении срока действия пароля отобразится уведомление о необходимости сменить пароль. При касании уведомления осуществляется переход в настройки ОС для смены пароля;

– если на устройстве были применены более строгие требования к паролю, то отобразится уведомление о необходимости сменить пароль. При нажатии на уведомление осуществляется переход в настройки ОС для смены пароля.

2.4.1.42.Настройки пользователя/Создать пользователя

Правило разрешает или запрещает создание пользователя, а также при необходимости задать временной интервал, в течение которого необходимо сбросить пароль Администратора и перезагрузить устройство.

Для создания правила необходимо:

1) В раскрывающемся списке «Создание» выбрать значение:

– «Создавать» – для создания пользователя `sfuser` (для ОС Аврора) или `acuser` (для ОС семейства Linux). При добавлении правила значение выбрано по умолчанию;

– «Не создавать» – чтобы не создавать пользователя;

2) Для устройств на базе ОС Аврора возможно дополнительно указать определенный временной интервал, в течение которого необходимо сбросить пароль Администратора и перезагрузить устройство. Для этого:

– перевести переключатель «Сброс пароля Администратора» в положение «Включено» (по умолчанию он выключен).

ПРИМЕЧАНИЕ. Переключатель «Сброс пароля Администратора» доступен для включения/выключения, если в раскрывающемся списке «Создание» выбрано значение «Создавать»;

– в полях «Сброс с» и «Сброс до» указать начало и конец временного интервала, в течение которого необходимо выполнить сброс пароля Администратора и перезагрузить устройство.

ПРИМЕЧАНИЯ:

✓ Время фактического сброса от заданного +3 минуты. То есть, если запланирован сброс с 14:50, то по факту сброс будет произведен в 14:53;

✓ Назначение времени сброса с 00:00 по 00:00 означает «Сбросить сейчас»;

✓ Если в правиле изменить условие с «Создавать» на «Не создавать», то устройство будет не соответствовать политике, пока `sfuser` на устройстве не будет удален. Также устройство будет не соответствовать политике, пока `sfuser`, на которого перезагрузилось устройство, не подключится к сети;

✓ Логин и имя пользователя `sfuser` должны быть одинаковыми, иначе будет ошибка создания роли пользователя. После применения политики имя пользователя можно менять свободно;

✓ Если нужно зайти на устройство под Администратором, то рекомендуется, находясь под `sfuser`, сбросить пароль на устройстве и дождаться синхронизации с сервером. Только потом переключиться на Администратора и ввести новый пароль.

2.4.1.43.Настройки пользователя/Сертификаты пользователя

Правило позволяет создать и передать на устройство сертификаты пользователя, необходимые для подключения к защищенным сетям WLAN.

Выбрать из раскрывающегося списка категорию пользовательских сертификатов, в рамках которой будет выпущен пользовательский сертификат. При отсутствии необходимой категории в списке, требуется добавить ее в подразделе «Настройки» раздела «Администрирование» (п. 4.1.2).

Для выпуска и доставки сертификата необходимо:

– привязать активированное устройство к пользователю (п. 2.2.8);

– выполнить одно из действий:

- привязать устройство к группе устройств (п. 2.2.9);
- привязать пользователя, к которому привязано устройство, к группе пользователей (п. 2.3.4);

– назначить политику с правилом «Настройки пользователя/Сертификаты пользователя» на группу устройств или пользователей, в которую входит устройство.

ПРИМЕЧАНИЯ:

✓ Если у устройств изменится пользователь, то сертификат не будет перевыпущен. Для выпуска сертификата другому пользователю необходимо создать новую категорию пользовательских сертификатов и применить ее в правиле;

✓ Если у пользователя изменились данные, используемые в сертификате, то сертификат не будет перевыпущен. Для выпуска нового сертификата необходимо пользователю создать новую категорию пользовательских сертификатов и применить ее в правиле;

✓ Если пользователь был отвязан от устройства, то пользовательский сертификат не удалится с устройства. Чтобы удалить сертификат с устройства, следует удалить правило из политики.

2.4.1.44.Геопозиционирование/Настройки LBS-сервиса

Правило позволяет отправить на устройство настройки для LBS-сервиса. Данное правило необходимо использовать в случае, когда необходимо настроить и улучшить определение геопозиции устройства.

ПРИМЕЧАНИЕ. LBS-сервис работает совместно с сервисом геопозиционирования.

ВНИМАНИЕ! Политика применяется всегда, но для работы LBS-сервиса требуется включение геопозиционирования с выбранным режимом «Высокая точность» или «Сохранение заряда аккумулятора» (пп. 2.4.1.53).

Для создания правила необходимо:

1) Убедиться, что переключатель «LBS-сервис», отвечающий за работу сервиса, находится в положении «Включен» (по умолчанию переключатель установлен в положении «Включен»);

2) В раскрывающемся списке «Выбор LBS-сервиса» выбрать необходимый LBS-сервис, в который будет обращаться устройство (по умолчанию выбран Яндекс.Локатор);

3) В раскрывающемся списке «Переменная для API-ключа» выбрать защищенную переменную, внутри которой будет передаваться API-ключ.

ПРИМЕЧАНИЕ. Если переменная отсутствует в списке, предварительно необходимо добавить ее во вкладке «Администрирование» в разделе «Настройки» (п. 4.1.8);

4) В поле «Периодичность запросов» указать интервал, с которым устройство должно обращаться к LBS-сервису (по умолчанию установлен интервал в 12 секунд);

5) В раскрывающемся списке «Режим экономии LBS-запросов» необходимо выбрать режим экономии запросов:

– «Включен»;

– «Выключен»;

– «Задаваемая переодичность» (выбрано по умолчанию при добавлении правила);

6) Поле «Периодичность запросов в режиме экономии» (отображается при выборе режима экономии «Заданная периодичность») необходимо задать интервал, с которым устройство должно обращаться к LBS-сервису.

ПРИМЕЧАНИЕ. Устройство при включенном режиме экономии запросов будет обращаться в LBS-сервис реже при выключенном экране. В поле «Периодичность запросов в режиме экономии» задается интервал запросов при выключенном экране.

2.4.1.45.Геопозиционирование/Настройки A-GNSS

Правило позволяет отправить на устройство настройки A-GNSS.

ВНИМАНИЕ! Для работы A-GNSS требуется включение геопозиционирования с выбранным режимом «Высокая точность».

Для создания правила необходимо:

1) Убедиться, что переключатель «A-GNSS», отвечающий за работу сервиса, находится в положении «Включено»;

2) Заполнить поля:

– «Адрес сервера» - ввести адрес SUPL-сервера;

– «Порт» - ввести порт SUPL-сервера;

3) По умолчанию опция «TLS-подключение» активирована. При необходимости, если требуется не защищенное соединение, перевести переключатель «TLS-подключение» в положение «Выключено».

2.4.1.46.Контент/Доставка на устройство

Правило позволяет выбрать один или несколько файлов/папок, которые необходимо доставить на устройство.

ПРИМЕЧАНИЯ:

✓ Для устройств с ОС Аврора действует только доставка файлов. Особенности доставки файлов на устройства с ОС Аврора описаны ниже;

✓ У доставляемого файла или папки должна быть хотя бы одна согласованная версия, если в настройках администрирования ПУ было задано количество администраторов для согласования файлов (подробнее в пп. 4.1.4.2).

ВНИМАНИЕ!

✓ ПУ позволяет добавлять сторонние файлы или папки в управляемую папку. При выборе исполняемого скрипта из папки в правиле «Скрипты/Выполнение на устройстве» рекомендуется писать скрипт так, чтобы он использовал в качестве зависимостей только те файлы, которые принадлежат управляемой папке, чтобы избежать ошибок;

✓ Если папка удаляется из ранее назначенной политики, то при переназначении с устройств будет удалено только управляемое ПУ содержимое в папке, т.е., по всему дереву будут удаляться только файлы, при этом папки будут оставаться, но они будут пустыми или в них будут сторонние файлы загруженные самим пользователем.

Для создания правила в случае, если требуется доставить файл на устройство, необходимо выполнить следующие действия:

1) В разделе «Укажите файлы к доставке» нажать на значок +;

2) Перевести переключатель «Общие настройки доставки» в положение «Включен» (Рисунок 80 [1]), если:

– требуется, чтобы все файлы из правила были доставлены на устройство сразу после получения политики устройством. Для этого необходимо в раскрывающемся списке «Режим доставки» выбрать значение «Моментально»;

– требуется, чтобы все файлы из правила были доставлены на устройство в заданный интервал времени. Для этого необходимо:

- в раскрывающемся списке «Режим доставки» выбрать значение «По расписанию»;
- если требуется настроить календарный период выполнения правила политики, перевести переключатель «Период актуальности» в положение «Включен» и указать дату и время начала и окончания действия правила политики;
- если требуется настроить интервал времени выполнения правила политики:
  - ♦ перевести переключатель «Интервал доставки» в положение «Включен» и указать начало и конец временного интервала, в течение которого нужно доставить файл;
  - ♦ в раскрывающемся списке «Тип доставки» выбрать, по какому времени производить доставку: «По локальному времени устройства» (выбрано по умолчанию) или «По абсолютному времени» (дополнительно в раскрывающемся списке «Часовой пояс» выбрать часовой пояс, по времени которого нужно выполнить доставку).

ПРИМЕЧАНИЯ:

✓ Для выполнения правила политики «По расписанию» необходимо, чтобы, как минимум одна из опций («Период актуальности», «Интервал доставки») была настроена. При этом, обе опции также могут быть настроены одновременно. В таком случае, правило политики будет выполняться в настроенный интервал времени с момента наступления начала периода актуальности и до его завершения;

✓ Для корректной настройки правила политики «По расписанию» необходимо соблюдать следующие ограничения:

– «Период актуальности» должен быть от 1 минуты до 3650 дней (10 лет без учета високосных годов);

– время начала и окончания «Интервала доставки» не должны совпадать;

✓ В поле «Период актуальности» отображается локальное время Администратора. При этом, действие выполняется на всех устройствах одновременно без учета локального часового пояса устройства;

✓ Если правило по доставке контента выполнено на устройстве, и истек его период актуальности и/или интервал доставки, то файл не будет удален с устройства.

Если требуется задать индивидуальное время доставки файла на устройство, необходимо:

– перевести переключатель «Общие настройки доставки» в положение «Выключен»;

– в раскрывающемся списке «Режим установки» ниже полей с данными файла выбрать нужный режим: «Моментально» или «По расписанию». Настройка режима «По расписанию» выполняется согласно шагам, приведенным выше;

3) Если требуется, чтобы устройство пробуждалось для доставки файла в назначенный интервал, перевести переключатель «Пробуждение устройств» (Рисунок 80 [2]) в положение «Включено» (по умолчанию он выключен).

ВНИМАНИЕ! Пробуждение устройств имеет ряд требований и особенностей, подробнее в приложении (Приложение 8);

4) В раскрывающемся списке «Файл» (Рисунок 80 [3])выбрать файл, который необходимо доставить на устройство, при необходимости воспользовавшись фильтром.

ПРИМЕЧАНИЕ. Если необходимого файла в списке нет, то следует добавить его, выполнив действия, описанные в пп. 2.6.1.1;

5) В раскрывающемся списке «Версия» (Рисунок 80 [4]) выбрать версию файла, которую необходимо доставить на устройство;

ПРИМЕЧАНИЕ. Если необходимой версии файла нет в списке, то следует добавить ее, выполнив действия, описанные в п. 2.6.1.2;

6) В поле «Директория» (Рисунок 80 [5]) ввести путь к папке на устройстве, в которую необходимо разместить файл.

7) Если необходимо добавить в правило еще один файл, то необходимо нажать на значок + в левом нижнем углу (Рисунок 80 [6]) и повторить действия, описанные выше;

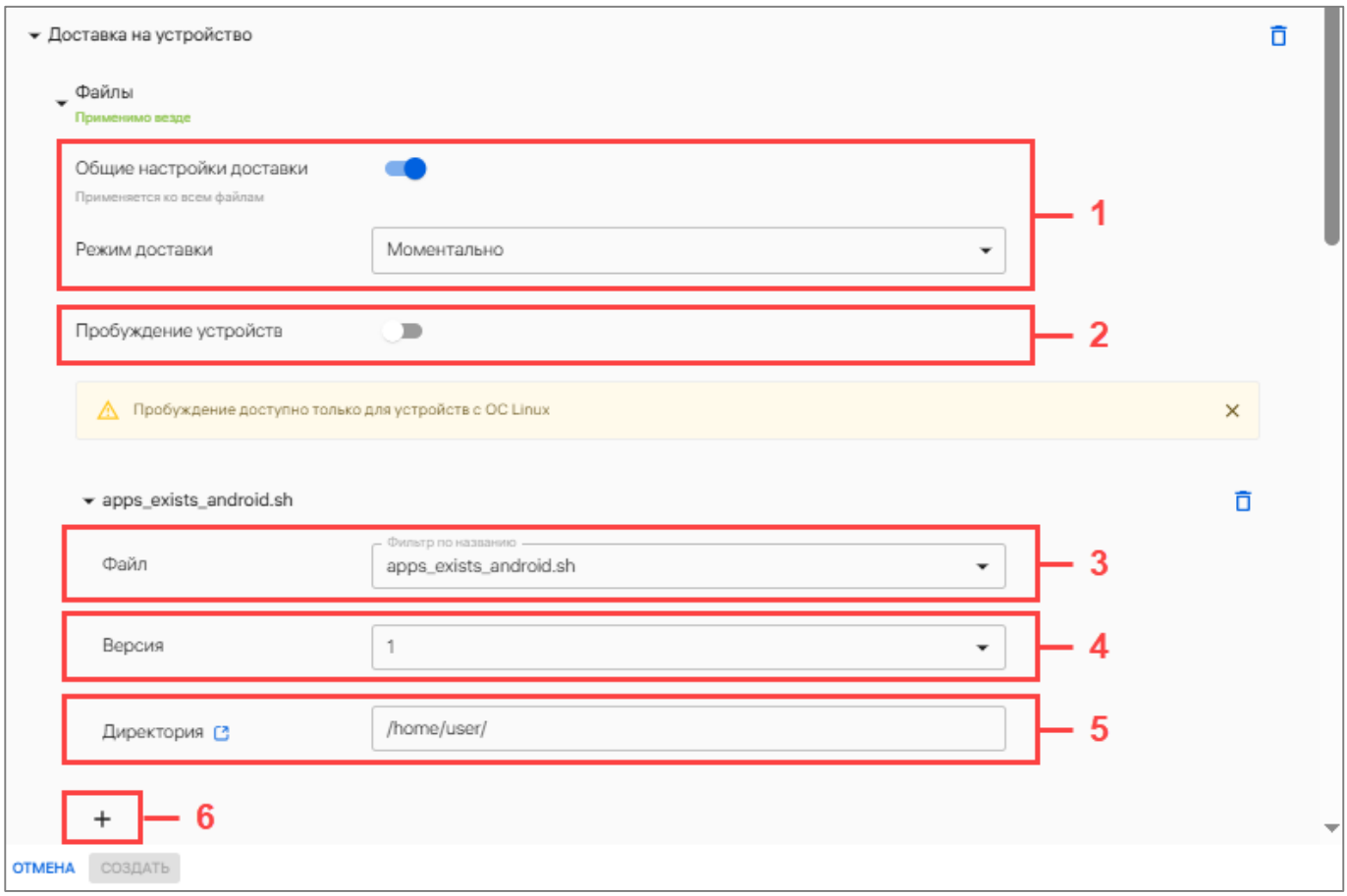


Рисунок 80

Для создания правила в случае, если требуется доставить папку, загруженную из git-репозитория, со всеми ее файлами на устройство, необходимо выполнить следующие действия:

1) В разделе «Укажите папки к доставке» нажать на значок +;

2) Перевести переключатель «Общие настройки доставки» в положение «Включен» (Рисунок 81 [1]), если:

– требуется, чтобы все папки из правила были доставлены на устройство сразу после получения политики устройством. Для этого необходимо в раскрывающемся списке «Режим доставки» выбрать значение «Моментально»;

– требуется, чтобы все папки из правила были доставлены на устройство в заданный интервал времени. Для этого необходимо:

- в раскрывающемся списке «Режим доставки» выбрать значение «По расписанию» (Рисунок 81 [1]);
- если требуется настроить календарный период выполнения правила политики, перевести переключатель «Период актуальности» в положение «Включен» и указать дату и время начала и окончания действия правила политики (Рисунок 81 [2]);
- если требуется настроить интервал времени выполнения правила политики (Рисунок 81 [2]):

♦ перевести переключатель «Интервал доставки» в положение «Включен» и указать начало и конец временного интервала, в течение которого нужно доставить папку;

♦ в раскрывающемся списке «Тип доставки» выбрать, по какому времени производить доставку: «По локальному времени устройства» (выбрано по умолчанию) или «По абсолютному времени» (дополнительно в раскрывающемся списке «Часовой пояс» выбрать часовой пояс, по времени которого нужно выполнить доставку).

ПРИМЕЧАНИЯ:

✓ Для выполнения правила политики «По расписанию» необходимо, чтобы, как минимум одна из опций («Период актуальности», «Интервал доставки») была настроена. При этом, обе опции также могут быть настроены одновременно. В таком случае, правило политики будет выполняться в настроенный интервал времени с момента наступления начала периода актуальности и до его завершения;

✓ Для корректной настройки правила политики «По расписанию» необходимо соблюдать следующие ограничения:

– «Период актуальности» должен быть от 1 минуты до 3650 дней (10 лет без учета високосных годов);

– время начала и окончания «Интервала доставки» не должны совпадать;

✓ В поле «Период актуальности» отображается локальное время Администратора. При этом, действие выполняется на всех устройствах одновременно без учета локального часового пояса устройства;

✓ Если правило по доставке контента выполнено на устройстве, и истек его период актуальности и/или интервал доставки, то папка не будет удалена с устройства.

Если требуется задать индивидуальное время доставки папки на устройство, необходимо:

– перевести переключатель «Общие настройки доставки» в положение «Выключен»;

– в раскрывающемся списке «Режим установки» ниже полей с данными папки выбрать нужный режим: «Моментально» или «По расписанию». Настройка режима «По расписанию» выполняется согласно шагам, приведенным выше;

3) Если требуется, чтобы устройство пробуждалось для доставки папки в назначенный интервал, перевести переключатель «Пробуждение устройств» (Рисунок 81 [3]) в положение «Включено» (по умолчанию он выключен).

ВНИМАНИЕ! Пробуждение устройств имеет ряд требований и особенностей, подробнее в приложении (Приложение 8);

4) В раскрывающемся списке «Папка» (Рисунок 81 [4]) выбрать папку, которую необходимо доставить на устройство, при необходимости воспользовавшись фильтром.

ПРИМЕЧАНИЕ. Если необходимой папки в списке нет, то следует добавить ее, выполнив действия, описанные в пп. 2.6.2.1;

5) В раскрывающемся списке «Версия» (Рисунок 81 [5]) выбрать версию папки, которую необходимо доставить на устройство.

ПРИМЕЧАНИЕ. Если необходимой версии папки нет в списке, то следует добавить ее, выполнив действия, описанные в п. 2.6.2.2;

6) В поле «Директория» (Рисунок 81 [6]) ввести путь к папке на устройстве, в которую необходимо разместить папку из git-репозитория;

7) Если необходимо добавить в правило еще одну папку, то необходимо нажать на значок + (Рисунок 81 [7]) в левом нижнем углу и повторить действия, описанные выше.

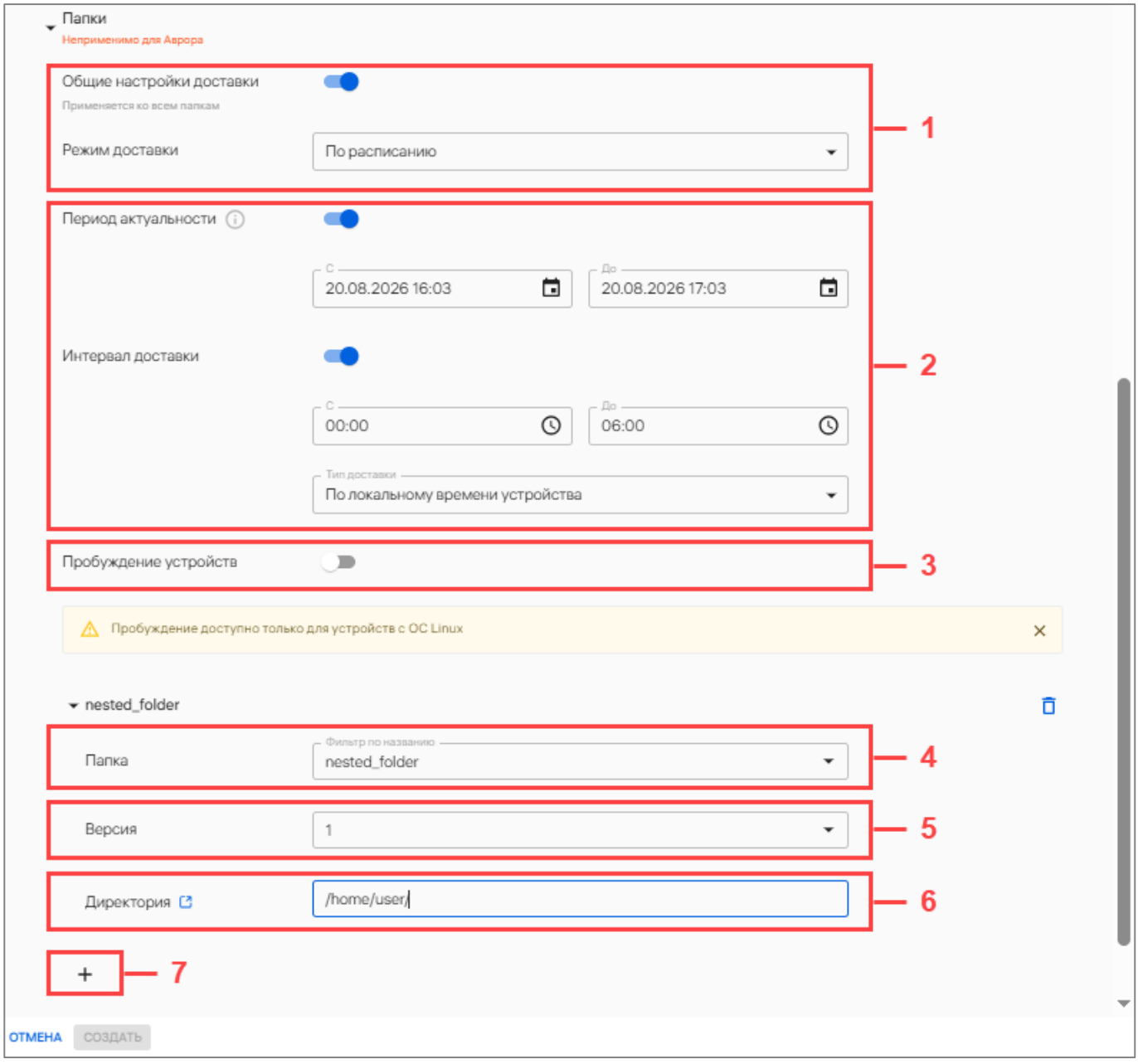


Рисунок 81

Особенности доставки файлов на устройства с ОС Аврора:

1) Максимальный размер файла - 100МБ;

2) Если в процессе доставки файлов пользователь укажет несуществующую папку внутри разрешенной директории, то папка создастся, однако это приведет к изменению прав для разрешенной директории. Пример:

– пользователь в политике указал путь: `/home/defaultuser/Downloads/SomeFolder/file.txt;`

– внутри разрешенной директории Downloads создалась новая папка SomeFolder (т.к. ее не было на устройстве) и в нее добавился `file.txt`;

– у разрешенной директории Downloads изменились права, выданные системой по умолчанию. На просмотр файлов внутри такой директории не влияет.

ПРИМЕЧАНИЕ. Если создать внутри разрешенной директории папку SomeFolder с файлом, а потом удалить файл через политику, то пустая директория SomeFolder тоже удалится.

Список разрешенных директорий: Desktop, Documents, Downloads, Music, Pictures, Playlists, Public, Templates, Videos.

Пример правильного пути для доставки файла: `/home/defaultuser/Downloads/file.txt`.

2.4.1.47.Файлы с устройства/Загрузка файлов с устройств

Правило позволяет указать папку на устройстве, из которой файлы будут загружаться на сервер ППО.

Для создания правила необходимо:

– в поле «Папка на устройстве» ввести путь до папки на устройстве, файлы из которой необходимо передавать на сервер Аврора Центр (поле обязательно для заполнения);

– в поле «Проверять каждые» ввести периодичность проверки новых файлов в папке в формате [дн:чч:мм] (по умолчанию установлена периодичность проверки в 1 час);

– перевести переключатель «Удалять на устройстве после отправки» в положение «Включено», если требуется, чтобы файлы после передачи на сервер Аврора Центр удалялись с устройства (по умолчанию переключатель установлен в положении «Включено»).

Если требуется:

– добавить еще одну папку в политику, нажать на значок + и повторить шаги, приведенные выше;

– удалить папку из правила, нажать на значок «Удалить» справа от названия папки.

Просмотреть список загруженных с устройства файлов, а также скачать их, возможно в карточке устройства во вкладке «Файлы» (пп. 2.1.1.12).

Для сохранения файлов на сервер будет использоваться папка Uploads (например, `/ocs/emm/uploads/default/`). Каждый загруженный файл будет в качестве названия использовать свой идентификатор, который ему присвоил Аврора Центр при сохранении на сервере. При этом каждый файл будет загружен в отдельную папку. Имя файла в папке будет совпадать с именем этого файла на устройстве.

Пример: при загрузке с устройства на сервер файлу был присвоен идентификатор 683bba5f-81c3-44e8-bac7- cb4bf021a284. Этот же идентификатор будет именем файла на сервере. Загруженный файл будет расположен на сервере по пути `/ocs/emm/uploads/default/68/3b/ba/5f/683bba5f-81c3-44e8-bac7-cb4bf021a284`.

ПРИМЕЧАНИЕ. Система размещения в 4-х подпапках, название каждой из которых - это разбитые по 2 первые 8 символов идентификатора файла (/68/3b/ba/5f/), необходима для успешного сохранения файла на сервере.

Если требуется открыть файл, необходимо скачать его с сервера и переименовать так, как он назывался на устройстве с указанием расширения (например, в `test.txt`). Затем открыть его подходящей программой.

ПРИМЕЧАНИЕ. Оригинальное название файла вместе с расширением доступно в базе данных `emm.applications.uploaded_files` в столбце `source_urn`.

Особенности загрузки файлов с устройств с ОС Аврора:

1) Максимальный размер файла - 50МБ;

2) Функционал удаления файла после загрузки не работает, т.к. предполагается, что файлы, загружаемые с устройства, созданы пользователем;

3) Если файлы для загрузки были ранее доставлены на устройство с помощью правила политики «Контент/Доставка на устройство», их удаление не требуется, т.к. достаточно отменить политику по доставке контента. Такие файлы доступны только для чтения, что исключает возможность их изменения пользователем. Следовательно, при загрузке с устройства будет использоваться та же версия файла, которая была первоначально доставлена.

2.4.1.48.Проверки/Наличие файлов и их содержимого

Правило позволяет проверять наличие файлов и их содержимое на устройстве.

Для создания правила необходимо заполнить поля, приведенные в таблице (Таблица 46).

Таблица 46

Наименование полей	Описание
Путь к файлу	Ввести абсолютный путь к файлу на устройстве. Поле обязательно для заполнения. Пример: `/home/user/tmp/nginx.config` **ПРИМЕЧАНИЕ.** Возможно использовать <<HOME>> в качестве шаблона для пути на устройстве, например: `<<HOME>>/test.txt`
Комментарий	При необходимости ввести комментарий для проверяемого файла

Если требуется добавить проверку контрольной суммы файла, необходимо:

– перевести переключатель «Проверять хеш» в положение «Включено» (по умолчанию он выключен);

– в поле «MD5» ввести значение контрольной суммы файла. Контрольная сумма должна быть с типом MD5.

Если требуется сделать проверку содержимого для проверяемого файла, необходимо:

1) Перевести переключатель «Проверка содержимого файла» (Рисунок 82 [1]) в положение «Включено» (по умолчанию он выключен);

2) В поле «Название проверки» ввести название проверки (Рисунок 82 [2]);

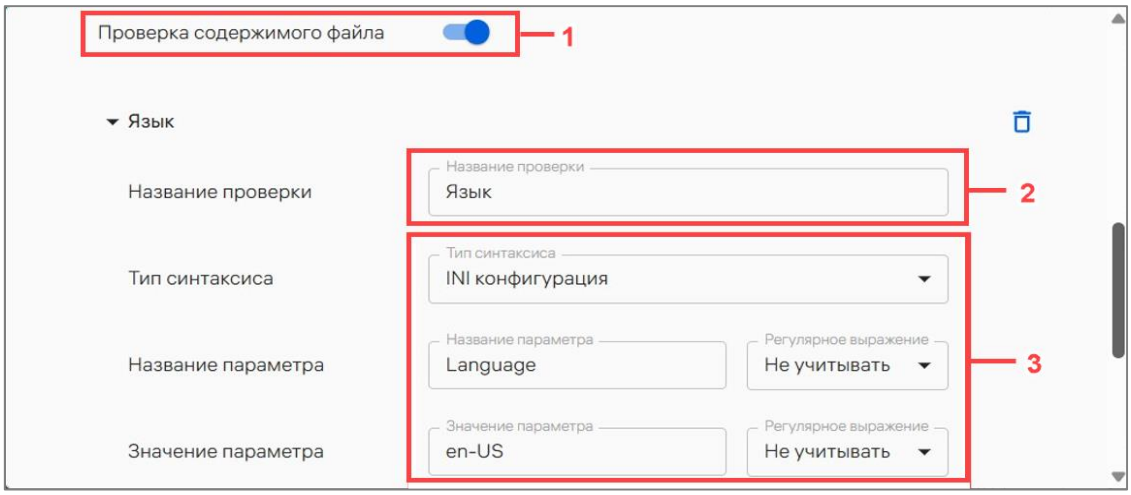


Рисунок 82

3) В раскрывающемся списке «Тип синтаксиса» (см. Рисунок 82 [3]) выбрать синтаксис, который используется в проверяемом файле:

– «Обычный текст» (plain text) - это формат писем, которые содержат только текст без форматирования, изображений, кнопок и других сложных элементов. Пример содержимого файла с типом синтаксиса plain text:

```
Hello, world!
```

– «INI-конфигурация» - это один из распространенных форматов текстовых файлов конфигурации, используемых различными приложениями. Этот формат позволяет хранить настройки приложения в виде набора секций, ключей и значений. Пример содержимого файла с типом синтаксиса INI:

```
[General]
Language=en-US
Theme=dark

[Database]
Server=localhost
Port=3306
Username=user
Password=secret
```

ВНИМАНИЕ! При использовании синтаксиса «INI-конфигурация» для приложения «Аврора Центр» секция «General» является секцией по умолчанию, поэтому для параметров, находящихся в ней, не стоит указывать секцию в виде префикса в политике;

– «Key-value конфигурация» - это формат текстовых файлов, используемых преимущественно в Unix - подобных системах, включая Linux, для хранения конфигурационных данных. Такие файлы состоят из пар ключ-значение, где каждая строка файла соответствует одной паре. Пример содержимого файла с типом синтаксиса key-value:

```
key1 val1 smt
```

ВНИМАНИЕ! Для синтаксиса «Key-value конфигурация» поддерживается только разделитель между ключом и значением в виде пробела, как показано на примере;

4) В поле «Название параметра» ввести название параметра. Если было использовано регулярное выражение в названии параметра, в раскрывающемся списке «Регулярное выражение» выбрать значение «Учитывать» (по умолчанию оно не учитывается).

ВНИМАНИЕ!

✓ Поле «Название параметра» отсутствует при выборе типа синтаксиса «Обычный текст»;

✓ Название при выборе синтаксиса «INI-конфигурация» должно содержать секцию и наименование параметра из этой секции. Например, `smt/key`, где `smt` - секция, а через "/" указан параметр `key`;

5) В поле «Значение параметра» ввести значение параметра. Если было использовано регулярное выражение в значении параметра, в раскрывающемся списке «Регулярное выражение» выбрать значение «Учитывать» (по умолчанию оно не учитывается).

ПРИМЕЧАНИЕ. Более подробная информация об использовании регулярных выражений приведена в приложении (Приложение 6).

Если требуется:

– добавить проверку, необходимо нажать «Добавить проверку» (Рисунок 83 [2]) и повторить шаги, приведенные выше.

ПРИМЕЧАНИЕ. Доступно добавление одной и более проверок для конкретного файла;

– удалить проверку, необходимо нажать на значок 🗑 «Удалить» (Рисунок 83 [1]).



Рисунок 83

2.4.1.49.Проверки/Символические ссылки

Правило позволяет проверять символические ссылки и целевые пути на устройстве.

Для создания правила необходимо заполнить поля, приведенные в таблице (Таблица 47).

Таблица 47

Наименование полей	Описание
Путь к символической ссылке	Ввести путь к символической ссылке. Поле обязательно для заполнения. Пример: `/home/user/tmp/nginx.link` **ПРИМЕЧАНИЕ.** Возможно использовать <<HOME>> в качестве шаблона для пути на устройстве, например: `<<HOME>>/nginx.link`
Целевой путь	Ввести абсолютный путь до файла или директорию, куда должна вести символическая ссылка. Поле обязательно для заполнения. Пример: /etc/nginx-launcher **ПРИМЕЧАНИЕ.** Возможно использовать <<HOME>> в качестве шаблона для пути, например: `<<HOME>>/nginx-launcher`
Комментарий	Ввести дополнительную информацию к проверке символической ссылки. Поле необязательно для заполнения

Если требуется добавить более одной проверяемой символической ссылки, нажать на значок + «Добавить» и повторить шаги, приведенные выше.

2.4.1.50.Проверки/Параметры безопасности

Правило позволяет проверять различные параметры безопасности элементов файловой системы на устройстве.

Для создания правила необходимо заполнить поля, приведенные в таблице (Таблица 48).

Таблица 48

Наименование полей	Описание
Путь на устройстве	Ввести абсолютный путь к файлу или директории на устройстве. Поле обязательно для заполнения. Пример: `/home/test.txt`. **ПРИМЕЧАНИЕ.** Возможно использовать <<HOME>> в качестве шаблона для пути на устройстве, например: `<<HOME>>/test.txt`
Комментарий	Ввести дополнительную информацию. Поле необязательно для заполнения
Имя владельца	Задать проверяемое имя владельца элемента файловой системы. Поле необязательно для заполнения. Допустимые символы: буквы (a-z, A-Z), цифры (0-9), специальные символы ('-', '_', '.'). Например: `mpendzhiev`
Имя группы	Задать проверяемое имя группы элемента файловой системы. Поле необязательно для заполнения. Допустимые символы: буквы (a-z, A-Z), цифры (0-9), специальные символы('-', '_', '.'). Например: domain-users
Разрешения файловой системы	Задать проверяемые разрешения элемента файловой системы. Поле необязательно для заполнения. Допустимые символы: цифры (0-7), не менее и не более 3 символов. Например: 777. Права доступа на файл или директорию следующие: u — права пользователя: r (4), w (2), x (1) g — правагруппы: r (4), w (2), x (1) o — прававсех остальных: r (4), w (2), x (1)
Базовые атрибуты	Задать проверяемые базовые атрибуты элемента файловой системы. Например: `ds`. Допустимые символы с поддерживаемыми базовыми атрибутами элементов файловой системы: – s – безопасное удаление (Secure_Deletion); – u – восстановление (Undelete); – S – синхронные обновления (Synchronous_Updates);

Наименование полей	Описание
	– D – синхронные обновления директорий (Synchronous_Directory_Updates); – i – неизменный (Immutable); – a – только добавление (Append_Only); – d – без создания дампа (No_Dump); – A – предотвращение обновление времени доступа (atime) файлов и каталогов при чтении (No_Atime); – c – требуемое сжатие (Compression_Requested); – E – зашифрованный (Encrypted); – j – данные, записанные в журнале (Journaled_Data); – I – индексированные директории (Indexed_directory); – t – в конце файла не будет фрагмента блока, который делится с данными другого файла(No_Tailmerging); – T – верхний уровень иерархии директорий (Top_of_Directory_Hierarchies); – e – последовательные физические блоки, которые описывают расположение данных в файловой системе Ext4 (Extents); – C – отключение функции копирования при записи (No_COW); – x – прямой доступ к файлам, хранящимся в постоянной памяти или на блочном устройстве (DAX); – F – игнорирование регистра букв при поиске файлов и директорий (Casefold); – N – опция файловой системы ext4, которая позволяет хранить данные файлов непосредственно в структуре индексного узла (Inline_Data); – P – команда иерархии проектов (Project_Hierarchy); – V – механизм защиты целостности данных, который реализуется через два модуля ядра: `fs-verity` и `dm- verity` (Verity); – m – без сжатия (Dont_Compress)

Если требуется добавить проверку расширенных атрибутов элемента файловой системы необходимо:

– нажать «Добавить расширенный атрибут»;

– в полях «Ключ» и «Значение» задать параметры, чтобы выполнить корректную проверку каждого добавляемого расширенного атрибута.

ВНИМАНИЕ. Ключ должен начинаться с «user.», «trusted.», «security.» или «system.»

Если требуется добавить еще один расширенный атрибут, необходимо нажать «Добавить расширенный атрибут» и повторить шаги, приведенные выше.

Если требуется добавить более одного проверяемого файла или директории на устройстве, необходимо нажать на значок + в левом нижнем углу и повторить действия, описанные выше.

ПРИМЕЧАНИЕ. Для успешного создания правила необходимо, чтобы был добавлен расширенный атрибут или заполнено одно из полей: «Имя владельца», «Имя группы», «Разрешения файловой системы» или «Базовые атрибуты».

2.4.1.51.Диагностика ОС/Проверка установленных пакетов на устройстве

Правило позволяет проверить, установлены ли все необходимые пакеты на устройстве.

Для создания правила необходимо:

1) В раскрывающемся списке «Название пакета» выбрать название пакета, который должен быть установлен на устройстве. В списке отображаются названия всех пакетов со всех устройств, которые отправили свое состояние в ПУ. При необходимости воспользоваться фильтром по названию пакета, для этого в поле «Название пакета» ввести полное или частичное название пакета. Если необходимого пакета нет в списке, ввести его точное название и выбрать «Добавить <название пакета>» в раскрывающемся списке;

2) Если требуется задать диапазон проверяемых версий пакета, необходимо:

– перевести переключатель «Диапазон версий» в положение «Включен»;

– в поле «Диапазон 1» ввести начало (поле «С») и/или конец (поле «До») нужного диапазона (верхняя граница «До» не включается в интервал).

ПРИМЕЧАНИЯ:

✓ По умолчанию будет проверяться наличие на устройстве любой версии пакета;

✓ Если заполнено только поле «С», тогда будут проверяться все версии пакета, начиная с нижней границы интервала. Если заполнено только поле «До», тогда будут проверяться все версии пакета до верхней границы интервала, не включая саму верхнюю границу.

Если требуется добавить еще один диапазон, необходимо нажать кнопку «Диапазон» и повторить шаги, приведенные выше;

3) Если требуется добавить проверку контрольной суммы пакета (версии пакета), необходимо:

– перевести переключатель «Проверять хеш» в положение «Включено» (по умолчанию он выключен);

– в поле «MD5» ввести значение контрольной суммы пакета (версии пакета). Контрольная сумма должна быть с типом MD5;

4) Если требуется добавить в правило еще один пакет, нажать на значок + в левом нижнем углу и повторить шаги, приведенные выше.

ПРИМЕЧАНИЕ. Ограничений на количество пакетов в правиле нет.

2.4.1.52.Скрипты/Выполнение на устройстве

Правило позволяет доставить и выполнить скрипт на устройстве.

Для создания правила необходимо:

1) Если требуется, чтобы все скрипты из правила политики были выполнены на устройстве сразу после получения политики устройством, убедиться что:

– переключатель «Общие настройки выполнения» находится в положении «Включен»;

– в раскрывающемся списке «Время выполнения» выбрано значение «Моментально»;

2) Если требуется, чтобы все скрипты из правила политики установились на устройстве в заданный интервал времени, необходимо:

– убедиться, что переключатель «Общие настройки выполнения» находится в положении «Включен»;

– в раскрывающемся списке «Время выполнения» выбрано значение «Интервал»;

– в поле «Интервал выполнения» указать начало и конец временного интервала, в течение которого можно доставить файлы. Если начало и конец интервала совпадают, то правило будет выполнено моментально;

– в раскрывающемся списке «Тип выполнения» выбрать, по какому времени производить выполнение:

- «По локальному времени устройства». Выбрано по умолчанию;
- «По абсолютному времени». Дополнительно в раскрывающемся списке «Часовой пояс» выбрать часовой пояс, по времени которого нужно выполнить скрипт;

3) Если требуется задать индивидуальное время выполнения скрипта на устройстве, необходимо:

– перевести переключатель «Общие настройки выполнения» в положение «Выключен»;

– в раскрывающемся списке «Время выполнения» выбрать:

- пункт «Моментально», если необходимо, чтобы скрипт был выполнен сразу после получения политики устройством;
- пункт «Интервал», если необходимо, чтобы скрипт был выполнен на устройстве в заданный интервал времени. И затем в поле «Интервал выполнения» указать начало и конец временного интервала, а также в раскрывающемся списке «Тип выполнения» выбрать, по какому времени производить запуск скрипта: «По локальному времени» (выбрано по умолчанию) или «По абсолютному времени» (дополнительно в раскрывающемся списке «Часовой пояс» выбрать часовой пояс, по времени которого нужно выполнить скрипт). Если начало и конец интервала совпадают, то правило будет выполнено моментально;

4) Если требуется, чтобы устройство пробуждалось для выполнения скрипта в назначенный интервал, перевести переключатель «Пробуждение устройств» в положение «Включено» (по умолчанию он выключен).

ВНИМАНИЕ! Пробуждение устройств имеет ряд требований и особенностей, подробнее в приложении (Приложение 8);

5) В раскрывающемся списке «Путь к файлу» выбрать путь к скрипту, который необходимо выполнить на устройстве после доставки.

ПРИМЕЧАНИЕ. Успешное создание правила по выполнению скриптов возможно только при наличии правила по доставке файлов в политике. Если в раскрывающемся списке «Путь к файлу» нет нужного скрипта, следует нажать на «добавить доставку на устройство» (Рисунок 84) и заполнить параметры правила по доставке контента (пп. 2.4.1.46);

6) В поле «Таймаут» необходимо ввести максимальное время в формате [мм:сс], в течение которого скрипт должен выполниться на устройстве после доставки. По умолчанию установлено время в 1 минуту;

7) Если требуется задать периодичность выполнения скрипта, необходимо в раскрывающемся списке «Периодичность выполнения» выбрать значения:

– «По умолчанию» – периодичность выполнения не задана, скрипт будет выполняться на устройстве каждый час. Данное значение задано по умолчанию;

– «Однократно» – скрипт будет выполнен на устройстве единожды;

– «С заданной периодичностью» – скрипт будет выполняться на устройстве с заданной частотой. Чтобы задать частоту, необходимо:

- в поле «Частота запуска» задать временной интервал между запусками скрипта. Минимальное значение - 1 минута;
- в поле «Процент успешных выполнений» задать минимальный процент успешных выполнений скриптов между отправками состояния устройством для соответствия политике. По умолчанию установлено 100%.

ПРИМЕЧАНИЕ. При добавлении устройств в динамическую группу с условием «Результат выполнения скрипта» будет учитываться только последний результат выполнения скрипта;

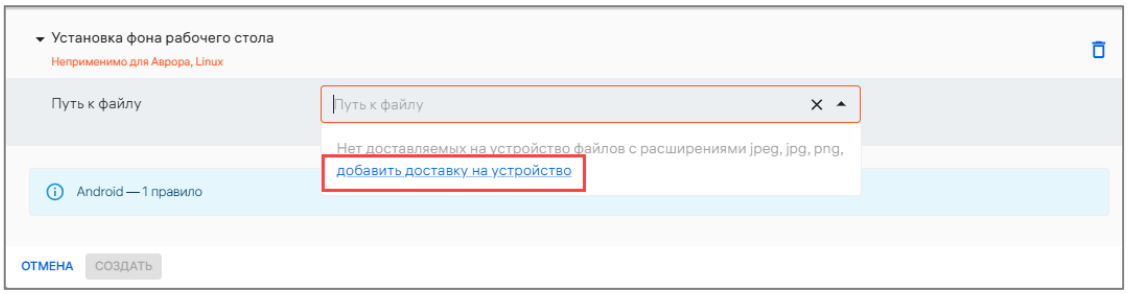


Рисунок 84

8) Нажать кнопку «Добавить переменную», если необходимо добавить в правило управляемые переменные для скрипта (защищенными являются переменными окружения, которые будут использованы в изолированной среде при выполнении скрипта), и заполнить следующие параметры:

– «Переменная в скрипте» - ввести идентичное название переменной из выбранного скрипта;

– «Переменная к подстановке» - выбрать в раскрывающемся списке нужную управляемую переменную для скрипта.

ПРИМЕЧАНИЯ:

✓ Если необходимой управляемой переменной нет в списке, необходимо добавить ее (п. 4.1.8);

✓ Если требуется добавить еще одну переменную для подстановки в скрипт, необходимо нажать на кнопку «Добавить переменную» и повторить шаги, приведенные выше.

ВНИМАНИЕ! ПУ позволяет добавлять сторонние файлы или папки в управляемую папку. При выборе исполняемого скрипта из папки в правиле «Скрипты/Выполнение на устройстве» рекомендуется писать скрипт так, чтобы он использовал в качестве зависимостей только те файлы, которые принадлежат управляемой папке, чтобы избежать ошибок.

Если необходимо добавить в правило еще один выполняемый скрипт, то необходимо нажать на значок + в левом нижнем углу и повторить действия, описанные выше.

ПРИМЕЧАНИЯ:

✓ Основным параметром на соответствие политике будет являться процент успешных выполнений. Результаты выполнения скриптов собираются по следующей логике:

– если заданный интервал выполнения скриптов МЕНЬШЕ, чем интервал отправки состояния, то результаты агрегируются за период между отправками состояния устройства по расписанию и затем сбрасываются;

– если заданный интервал выполнения скриптов БОЛЬШЕ, чем интервал отправки состояния, то результаты агрегируются за период между выполнениями скрипта и затем сбрасываются;

– интервал отправки состояния задается в правиле политики «Конфигурация/Расписание отправки состояния» и по умолчанию составляет один час;

✓ Если в раскрывающемся списке «Периодичность выполнения» выбрано значение «По умолчанию», то скрипт будет выполняться на устройстве каждый час. Также скрипт будет выполняться при применении новой или редактировании текущей политики. Также при создании скрипта необходимо учитывать другие особенности выполнения скриптов на устройстве (Приложение 3);

✓ После снятия политики скрипт перестанет выполняться на устройстве при условии, что в настройках администрирования ППО не включен переключатель «Запрет удаления скриптов с устройств» (раздел «Настройки правил политик»). Если переключатель «Запрет удаления скриптов с устройств» включен, то скрипт продолжит выполняться на устройстве каждый час (или с заданной периодичностью) даже при снятой политике;

✓ Перед выполнением скрипта приложение «Аврора Центр» выполняет сверку хэш-сумм файла скрипта, добавленного в ПУ, и файла скрипта, доставленного на устройство. При несовпадении хэш-сумм скрипт не будет выполнен.

Особенности запуска скрипта при задании частоты и временного интервала:

1) Скрипт запускается впервые в начале первого активного временного интервала, соответствующего заданному расписанию;

2) После завершения каждого выполнения скрипта, планируется его следующий запуск с учетом следующих условий:

– если момент следующего запуска (согласно заданной частоте) приходится на период активного интервала, скрипт будет запущен в пределах этого активного интервала согласно установленной частоте;

– если момент следующего запуска выходит за пределы активного интервала, скрипт будет запущен в начале ближайшего следующего интервала;

3) Если заданная частота запусков выше, чем длительность интервала (т.е., период между запусками короче самого интервала), то внутри одного активного интервала скрипт может быть выполнен несколько раз – до тех пор, пока очередной запланированный запуск попадает в границы этого же интервала.

Подробное описание о выполнении скриптов на устройстве приведено в пп. 2.6.1.2.

Примеры выполняемых скриптов с переменными окружения:

– BASH-скрипт на ОС Android:

```
#!/usr/bin/env sh
echo $LOGIN > /storage/emulated/0/Documents/test.txt echo $PASSWORD >>
/storage/emulated/0/Documents/test.txt
```

– BASH-скрипт на ОС семейства Linux:

```
#!/usr/bin/env sh
echo $LOGIN > test.txt echo $PASSWORD >> test.txt
```

2.4.1.53.Геопозиционирование/Настройки режима работы геопозиционирования

Правило задает следующие параметры:

– выключает или включает геопозиционирование;

– задает режим работы геопозиционирования;

– запрещает или разрешает вносить изменения в настройки геопозиционирования.

Доступные значения (для раскрывающегося списка «Режим работы»):

– «Не задано». Режим работы геопозиционирования не управляется ПУ. Если режим работы не задан, то запрет или разрешение изменения настроек задается вручную. Для этого необходимо выбрать необходимое значение из раскрывающегося списка «Изменение настроек»:

- «Запрещено» (при добавлении правила значение выбрано по умолчанию);
- «Разрешено»;

– «Выключено» (при добавлении правила значение выбрано по умолчанию):

- отключает геопозиционирование;
- устанавливает изменение настроек геопозиционирования в значение «Запрещено» и блокирует его.

ВНИМАНИЕ! Выключение режима работы геопозиционирования на устройствах с ОС Android может привести к сбою работоспособности следующих правил политик: «Конфигурация WLAN/Режим работы WLAN», «Конфигурация WLAN/Подключения к сети WLAN»;

– «Сохранение заряда аккумулятора»:

- активирует режим работы геопозиционирования, в котором для определения местоположения устройства используются поставщики сетевого местоположения и аппаратное позиционирование (например, с помощью триангуляции базовых станций), но не GPS;
- устанавливает изменение настроек геопозиционирования в значение «Запрещено» и блокирует его;

– «Только спутники»:

- активирует режим работы геопозиционирования, в котором для определения местоположения устройства используются GPS (Глобальная система позиционирования) и aGPS (Assisted GPS – технология, ускоряющая «холодный старт» GPS-приемника за счет предварительной загрузки в него необходимой информации не со спутников, а через более быстрые каналы связи, такие как WLAN, Bluetooth® и другие), а также аппаратное позиционирование (например, с помощью триангуляции базовых станций), но не поставщики местоположения;
- устанавливает изменение настроек геопозиционирования в значение «Запрещено» и блокирует его;

– «Высокая точность»:

- активирует режим работы геопозиционирования, в котором для определения местоположения устройства используются GPS, а также aGPS или какой-либо поставщик сетевого местоположения;
- устанавливает изменение настроек геопозиционирования в значение «Запрещено» и блокирует его.

ПРИМЕЧАНИЕ. Начиная с ОС Android версии 9 и выше режимы «Сохранение заряда аккумулятора», «Высокая точность» и «Только спутники» работают как один режим - «Геолокация включена». Все остальное определяет ОС в зависимости от того, какую точность координат запросило приложение использующее геолокацию.

2.4.1.54.Внешний вид/Установка фона рабочего стола

Правило позволяет доставить файл изображения и установить на фон рабочего стола устройства.

ПРИМЕЧАНИЯ:

✓ Правило не действует для устройств на базе с ОС Аврора и ОС семейства Linux;

✓ Правило поддерживает только файлы формата `.jpeg/.jpg/.png`;

✓ Для корректной установки и отображения обоев рабочего стола следует выбирать изображение с разрешением, аналогичным разрешению экрана используемого устройства, или остановиться на изображении с разрешением, значительно превосходящим разрешение экрана устройства.

Для создания правила необходимо в раскрывающемся списке «Путь к файлу» выбрать путь к файлу изображения, который необходимо установить фоном рабочего стола на устройстве после доставки.

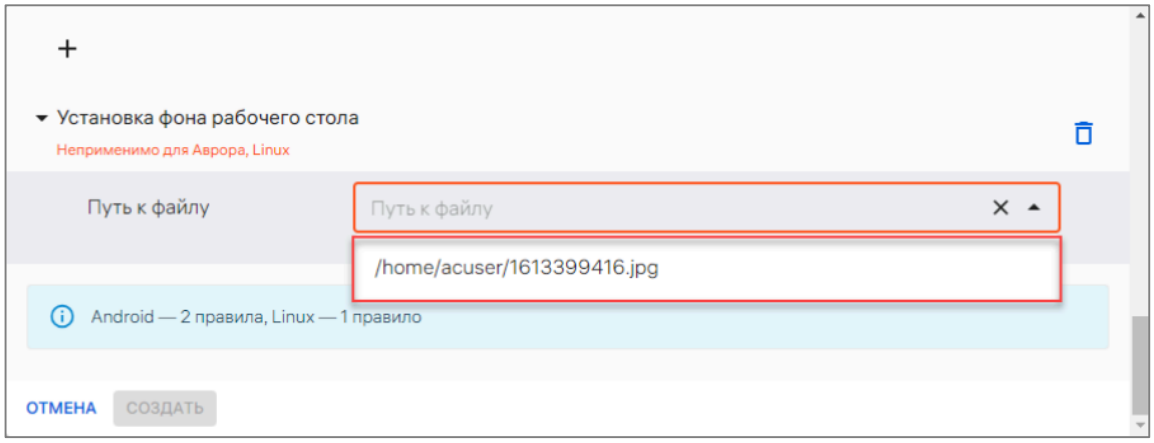


Рисунок 85

Успешное создание правила по установке фона рабочего стола возможно только при наличии правила по доставке файлов в политике с файлом в формате `.jpeg/.jpg/.png`.

Если в раскрывающемся списке «Путь к файлу» нет нужного файла изображения, то необходимо нажать «добавить доставку файлов» и заполнить параметры правила по доставке файлов (Рисунок 86).

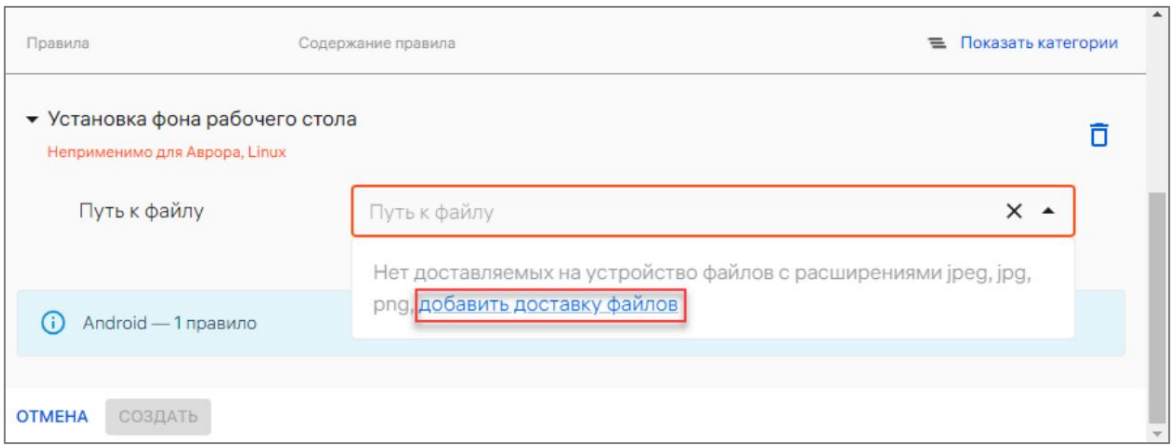


Рисунок 86

2.4.1.55.Внешний вид/Отображение идентификаторов в клиенте Аврора Центр

Правило позволяет задать порядок отображения идентификаторов в приложении «Аврора Центр».

Чтобы создать правило, в блоке «Порядок» необходимо расположить идентификаторы устройства в порядке уменьшения их значимости.

Первый и второй идентификаторы будут отображаться в приложении «Аврора Центр» для ОС Аврора и ОС Android (в том числе в режиме киоска) как основной и дополнительный (Рисунок 87, Рисунок 88), при их отсутствии будут отображаться менее приоритетные идентификаторы (третий, четвертый и т.д.).

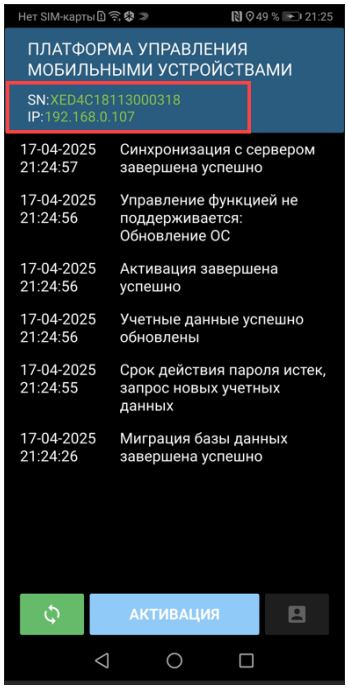


Рисунок 87

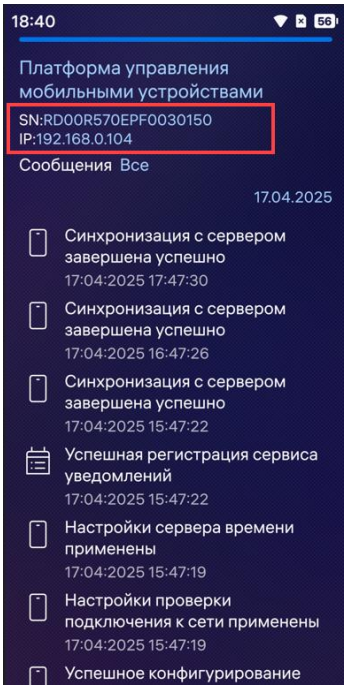


Рисунок 88

Правило также задаст порядок отображения идентификаторов в приложении «Аврора Центр» для ОС семейства Linux. Посмотреть идентификаторы в заданном порядке можно с помощью команды:

```
omp-uem-ctl get-device-identifiers
```

2.4.1.56.Внешний вид/Управление яркостью

Правило позволяет задавать яркость на устройстве и ограничивать доступ к управлению яркостью.

Для создания правила необходимо в раскрывающемся списке «Режим яркости» выбрать нужное значение:

– «Заданная яркость» (Рисунок 89) и далее в поле «Уровень яркости» с помощью слайдера настроить уровень яркости (изменить ее на устройстве будет невозможно). При добавлении правила уровень яркости выбран по умолчанию;

– «Автоопределение яркости». Будет включен режим автоопределения яркости (выключить его будет невозможно);

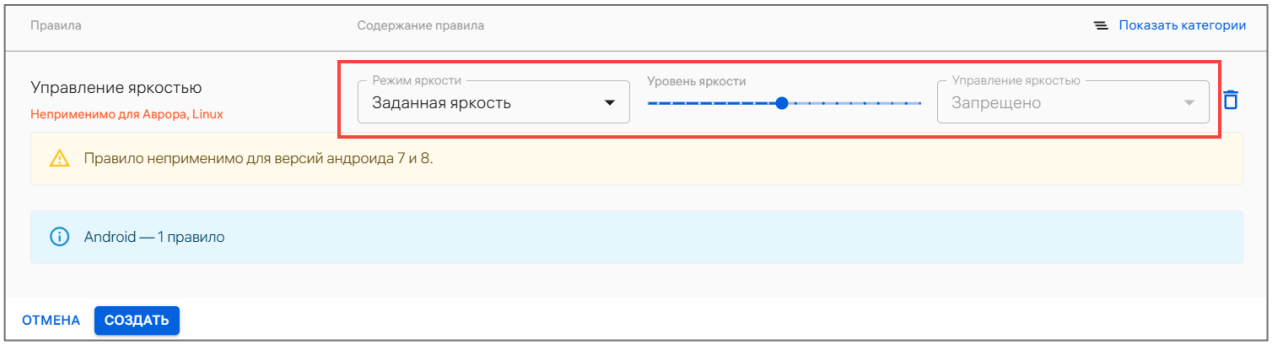


Рисунок 89

– «Не задано» (Рисунок 90). Раскрывающийся список «Управление яркостью» будет доступен для управления состоянием яркости. Доступные значения для управления яркостью:

- «Запрещено» – будет зафиксировано текущее состояние яркости. При добавлении правила значение выбрано по умолчанию;
- «Разрешено» – пользователь может изменять настройки яркости самостоятельно.

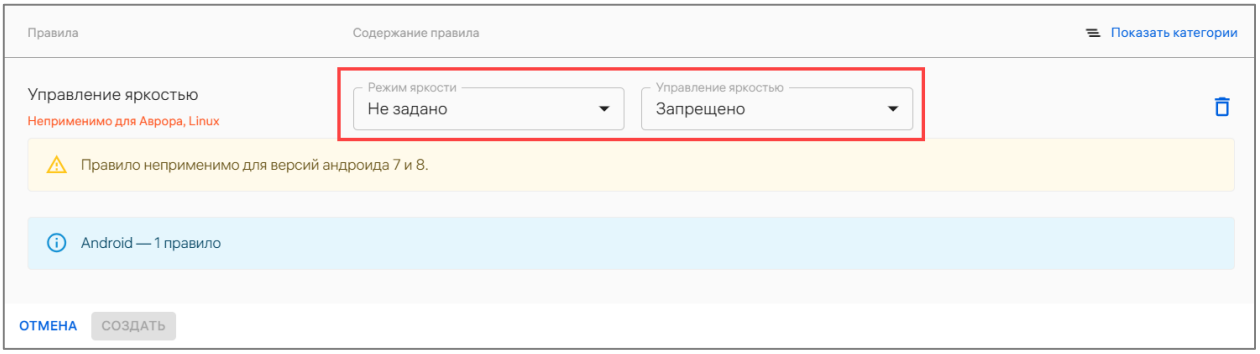


Рисунок 90

ПРИМЕЧАНИЯ:

✓ Яркость на устройстве может измениться при включении/выключении режима энергосбережения. Для получения максимальной яркости на устройстве убедиться, что режим энергосбережения выключен;

✓ Если на устройство назначены две и более политик с правилом, то комбинирование будет выполнено по режиму в следующем приоритете:

1) «Заданная яркость»;

2) «Автоопределение яркости»;

3) «Не задано». Правило с ограничением приоритетнее правила с разрешением;

✓ Значение яркости в процентах рассчитываются по разным алгоритмам (логарифмическая и линейная шкала). В связи с этим значение яркости в поле «Уровень яркости» в карточке устройства на кладке «Состояние» может отображаться некорректно. Также при использовании в правиле политики любого значения яркости, кроме минимального (0%) и максимального (100%), действительная яркость на устройстве может отличаться от ожидаемой. Это связано с изменениями на стороне ОС Android.

2.4.1.57.Внешний вид/Ориентация экрана

Правило позволяет управлять ориентацией экрана устройства.

Для создания правила необходимо в раскрывающемся списке «Ориентация экрана» выбрать одно из следующих значений:

– «Автоматическая». Ориентация экрана изменяется автоматически в зависимости от положения устройства;

– «Портретная». Ориентация экрана устройства фиксируется в вертикальном положении;

– «Ландшафтная». Ориентация экрана устройства фиксируется в горизонтальном положении;

– «Обратная портретная». Ориентация экрана фиксируется вверхом вниз в вертикальном положении;

– «Обратная ландшафтная». Ориентация экрана фиксируется справа-налево в горизонтальном положении.

При выборе режима, отличного от «Автоматическая», на устройстве отключается автоматический поворот экрана.

ПРИМЕЧАНИЯ:

✓ Если приложение самостоятельно фиксирует ориентацию экрана, например только вертикальную, установленная через ПУ ориентация может не применяться к такому приложению;

✓ На определенных моделях устройств поведение ориентации может зависеть от прошивки производителя.

2.4.1.58.Приложения/Управление приложениями

Правило позволяет:

– задать установки приложения выбранной витрины и версии на устройствах, а также позволяет обновлять и удалять установленные приложения (пп. 2.4.1.58.1). Приложений в политике может быть задано несколько;

– задать список запрещенных приложений (пп. 2.4.1.58.2), которых на устройстве быть не должно, вне зависимости от того, каким образом производилась установка на устройство (через ПУ или вручную).

– задать список исключений из запрещенного списка (пп. 2.4.1.58.3).

ПРИМЕЧАНИЕ. Особенности работы правила политики для устройств на базе ОС семейства Linux приведены в документе «Руководство пользователя. Часть 11. Приложение «Аврора Центр» для операционных систем семейства Linux».

Предусмотрена возможность задать дополнительные правила по добавлению нескольких приложений в политику, выполнив действия, описанные в п. 2.4.6.

Чтобы приложение было доступно для выбора, необходимо выполнение следующих условий:

– приложение должно быть добавлено и опубликовано в Подсистеме «Маркет» (ПМ) (подробная информация приведена в документе «Руководство пользователя. Часть 2. Подсистема «Маркет»);

– видимость витрины с приложением включена в настройках интеграции с Сервером приложений (пп. 4.1.5.1);

– приложения для ОС Аврора, ОС Android, ОС Альт Linux (и РЕД ОС) и ОС Astra Linux (и ОС Ubuntu) должны находиться в отдельных витринах (описание процесса создания витрины с приложением приведено в документе «Руководство пользователя. Часть 2. Подсистема «Маркет»).

ВНИМАНИЕ! При условии, что в ППО настроена интеграция с «РТК-Феникс», некоторые функции правила, а также индикация приложений, доступны только для пакетов формата `.rpm` для ОС Альт Linux. Подробная информация о настройке интеграции приведена в документе «Руководство администратора».

ПРИМЕЧАНИЯ:

✓ После установки, с помощью политики, приложению для ОС Android будут автоматически выданы все необходимые разрешения, которые пользователь не сможет отозвать;

✓ Приложение, которое подписано подписью разработчика, клиента и связкой ключей из ППО, невозможно установить через политику;

✓ Перед установкой приложения выполняется сверка хэш-сумм билда приложением «Аврора Центр», вычисленного в ПМ, и билда, полученного на устройстве для установки. При несовпадении хэш-сумм приложение не будет установлено;

✓ Для успешной установки snap-пакетов, требующих опцию `--classic`, на ОС Альт Linux и РЕД ОС необходимо сделать дополнительный симлинк с помощью команды:

```
n -s /var/lib/snapd/snap /snap
```

✓ Установка flatpak-пакетов не поддерживается в ОС Astra Linux.

Приложение будет удалено с устройства, если после установки оно удаляется из правила, заменяется другим приложением или устройство будет удалено из группы, на которую назначена политика.

ВНИМАНИЕ! Приложение, установленное через политику, будет запрещено для ручного удаления пользователем. При попытке удалить такое приложение пользователь увидит сообщение «Действие запрещено».

ПРИМЕЧАНИЕ. Для создания правила необходимо настроить хотя бы один список (устанавливаемых или запрещенных приложений).

Когда устройство успешно применит политику с запрещенным списком приложений:

– запрещенные версии приложений будут удалены с устройства (если были установлены);

– запрещенное приложение не будет установлено, если пользователь попытается установить его на устройстве;

– если на устройство назначена политика, которая содержит правило по установке приложения, но при этом это приложение в запрещенном списке, то такое приложение не будет установлено на устройство.

ПРИМЕЧАНИЕ. Если на устройстве с ОС Android версии 7.0, 7.1, 8.0.0, 8.1.0 установлен Google Play, то при первой установке приложения через политику может появиться окно с подтверждением (Рисунок 91).

После выдачи разрешения это окно не будет отображаться при последующих установках приложений с помощью политики.

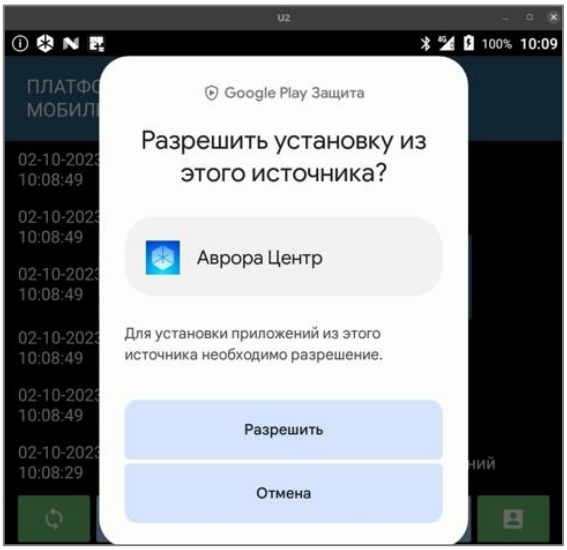


Рисунок 91

ПРИМЕЧАНИЯ:

✓ Начиная с версии ОС Аврора 5.1.0:

– поддерживается установка приложения с учетом архитектуры ОС: 32бита/64 бита (при условии, что сборка соответствующей архитектуры была загружена в ПМ);

– приложения, подписанные публичными/общедоступными ключами разработчика, можно устанавливать только при включенном режиме разработчика на устройстве;

– для успешной установки приложений через приложение «Аврора Маркет» необходимо его установить/обновить с помощью политики через ПУ, при этом приложение «Аврора Маркет» должно быть подписано подписью источника;

✓ На устройства с ОС семейства Linux возможно установить два приложения разных форматов, но с одинаковым именем;

✓ Установка на устройство:

– snap-пакетов – установить snap-менеджер при отсутствии его на устройстве. Обновить приложение со snap-пакетом с помощью политики можно только, если оно не запущено на устройстве;

– appimage-пакетов – после успешной установки appimage-приложение не имеет ярлыка на рабочем столе. Чтобы открыть приложение, необходимо зайти в папку установки `/opt/omp-uem-agent/appimages`;

– flatpak-пакетов – установить flatpak-менеджера при отсутствии его на устройстве. При установке flatpak-пакета может быть запрошена установка пакетов из общих репозиториев (необходимо настроить репозиторий).

Выделяют следующие особенности работы ППО с настроенной интеграцией с «РТК-Феникс»:

1) По умолчанию ПМ проверяет релизы на уязвимости:

– с периодичностью 1 раз в 1 час. При необходимости возможно изменить время в конфигурационном файле ППО (файл: `/var/ocs/config/subsystems/appstore/config.yml`, параметр: `verificationInterval`);

– при публикации релиза разработчиком;

2) Если релиз приложения был распространен на устройство через политику, то приложение «Аврора Центр» получит информацию о необходимости удалить или установить приложение с зависимостями при изменении статуса прохождения проверки безопасности от «РТК-Феникс» после синхронизации ППО и ПМ;

3) Устройство для дальнейшего удаления приложений и зависимостей выполняет проверку на наличие в активной витрине ПМ приложений с критическими уязвимостями в следующих случаях:

– автоматически 1 раз в 3 часа;

– при запуске приложения «Аврора Маркет»;

– при переключении активной витрины в приложении «Аврора Маркет»;

4) Если релиз приложения (в том числе системного) будет загружен в ПМ и будет отображаться в активной витрине, а в «РТК-Феникс» по нему будут найдены критические уязвимости, то:

– установленный на устройствах через политику или приложение «Аврора Маркет» релиз такого приложения и его зависимые пакеты будут удалены со всех устройств при совпадении имени пакета и версии, даже если включена опция «Запрет удаления приложений с устройств» в настройках администрирования ППО (раздел «Настройки правил политик»). При этом неважно, где были обнаружены критические уязвимости: в основном билде или в зависимом RPM-пакете;

– такой релиз будет недоступен для выбора к установке при создании правила политики «Приложения/Управление приложениями», а также будет не доступен для распространения через приложение «Аврора Маркет». При необходимости распространения данных релизов необходимо исключить их из проверок безопасности.

ПРИМЕЧАНИЯ:

✓ В случае ошибки проверки релиз приложения не будет удален с устройства, но будет не доступен для выбора при создании политики с правилом «Приложения/Управление приложениями», а также будет не доступен для распространения через приложение «Аврора Маркет»;

✓ Релизы приложений для ОС Альт Linux, загруженные до включения интеграции с «РТК-Феникс» без явного указания дистрибутива, перейдут в статус «Ошибка проверки уязвимостей», тем самым будут не доступны для дальнейшего распространения. При необходимости распространения данных релизов необходимо исключить их из проверок безопасности.

ВНИМАНИЕ! При включенной интеграции с «РТК-Феникс» для корректного функционирования приложений «Аврора Центр» и «Аврора Маркет» требуется добавлять все релизы этих приложений в список исключений для проверок в «РТК-Феникс». В противном случае при обнаружении критических уязвимостей или ошибках при проверке, возникнут проблемы с распространением и обновлением данных приложений.

Если была создана политика по установке приложения, в котором «РТК-Феникс» обнаружил критические уязвимости:

– в карточке политики на вкладке «Правила» для правила «Управление приложениями» справа от наименования и версии приложения будет отображаться индикатор (красная точка). При наведении на значение версии отобразится всплывающая подсказка, где к существующему тексту будет добавлено «найдены критические уязвимости» (Рисунок 92);

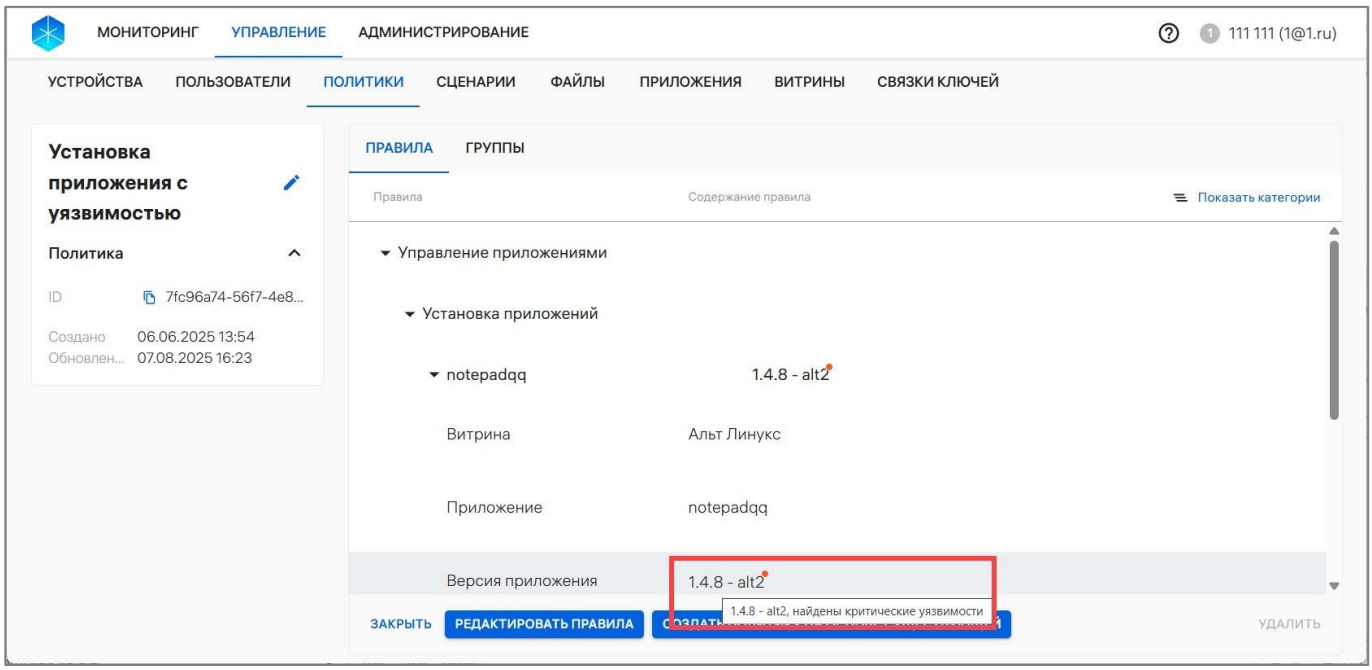


Рисунок 92

– в карточке редактирования правил политики для правила «Управление приложениями» справа от наименования и версии приложения будет отображаться индикатор (красная точка). При наведении на значение версии отобразится всплывающая подсказка, где к существующему тексту будет добавлено «найдены критические уязвимости» (Рисунок 93 [1]). Кнопка «Сохранить» будет не активна (Рисунок 93 [2]), пока не будет удалено или заменено данное приложение.

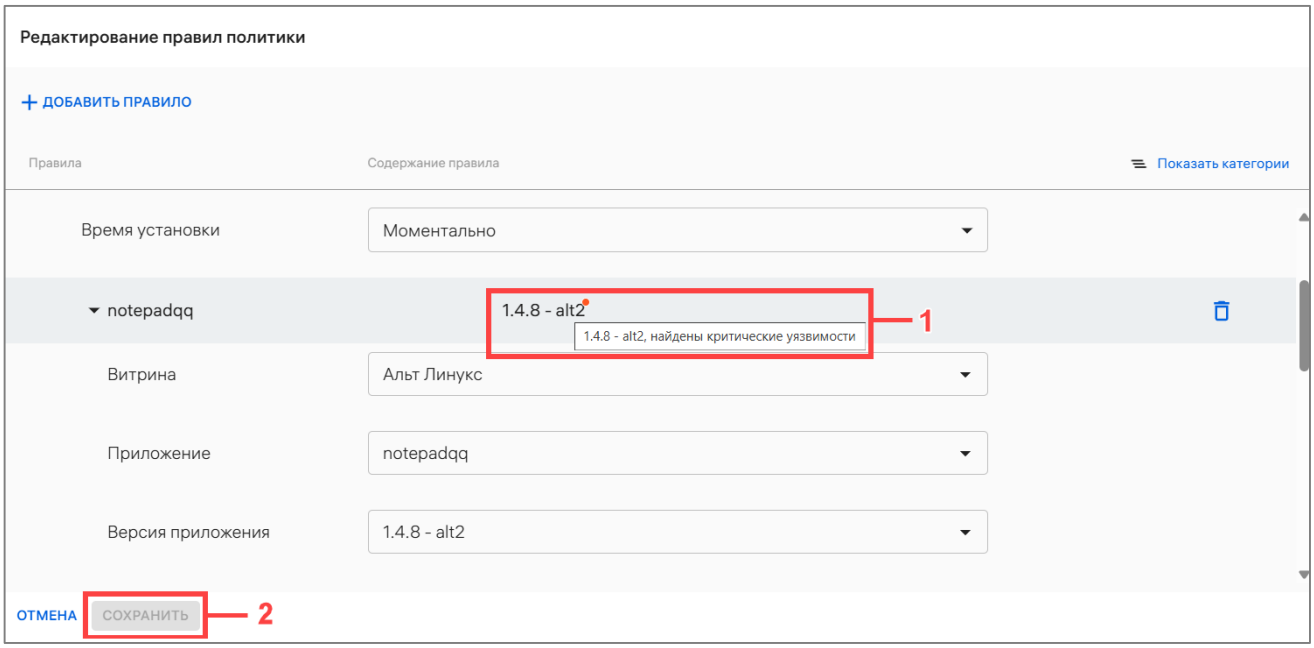


Рисунок 93

При примененной политике по установке приложения, в котором «РТК-Феникс» обнаружил критические уязвимости, в карточке устройства отобразится:

– статус «Не соответствует политике» (Рисунок 94 [1]);

– на вкладке «Состояние» в разделе «Управление приложениями» → «Установленные приложения» статус установки приложения «Не установлено: найдены критические уязвимости» (Рисунок 94 [2]);

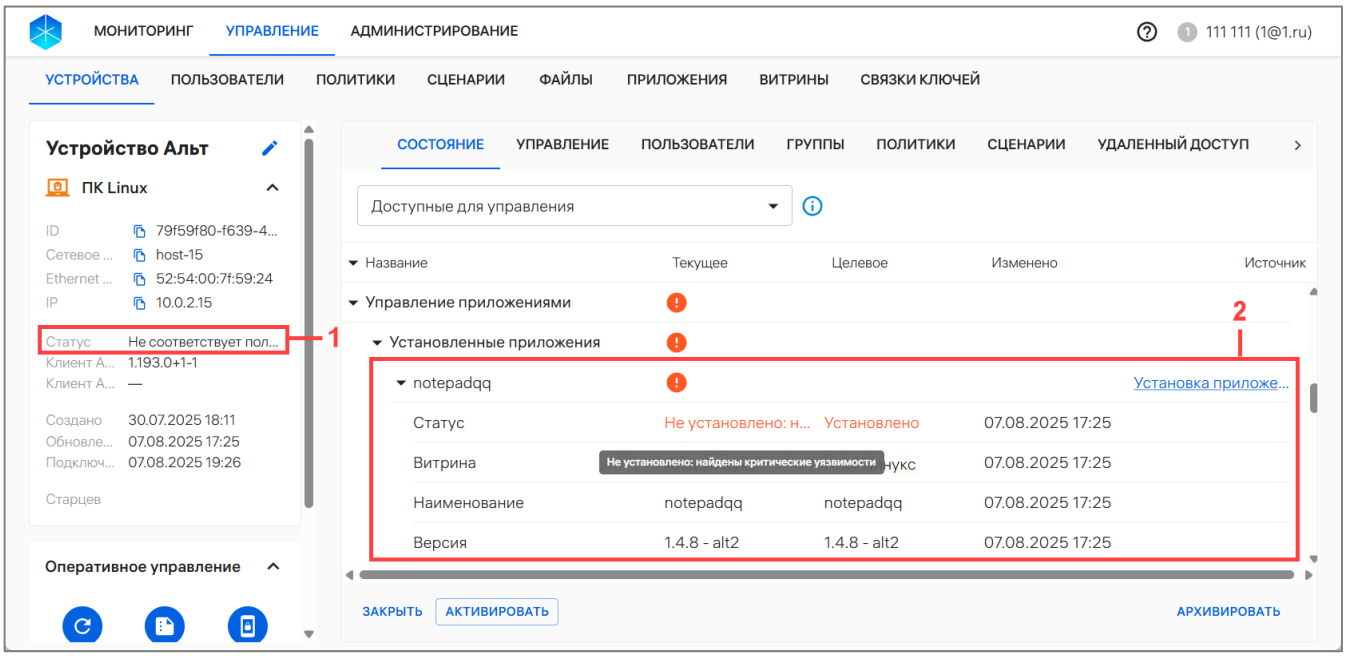


Рисунок 94

– на вкладке «Управление» в разделе «Приложения» для правила «Управление приложениями» несоответствие политике и статус установки приложения «Не установлено: найдены критические уязвимости» (Рисунок 95);

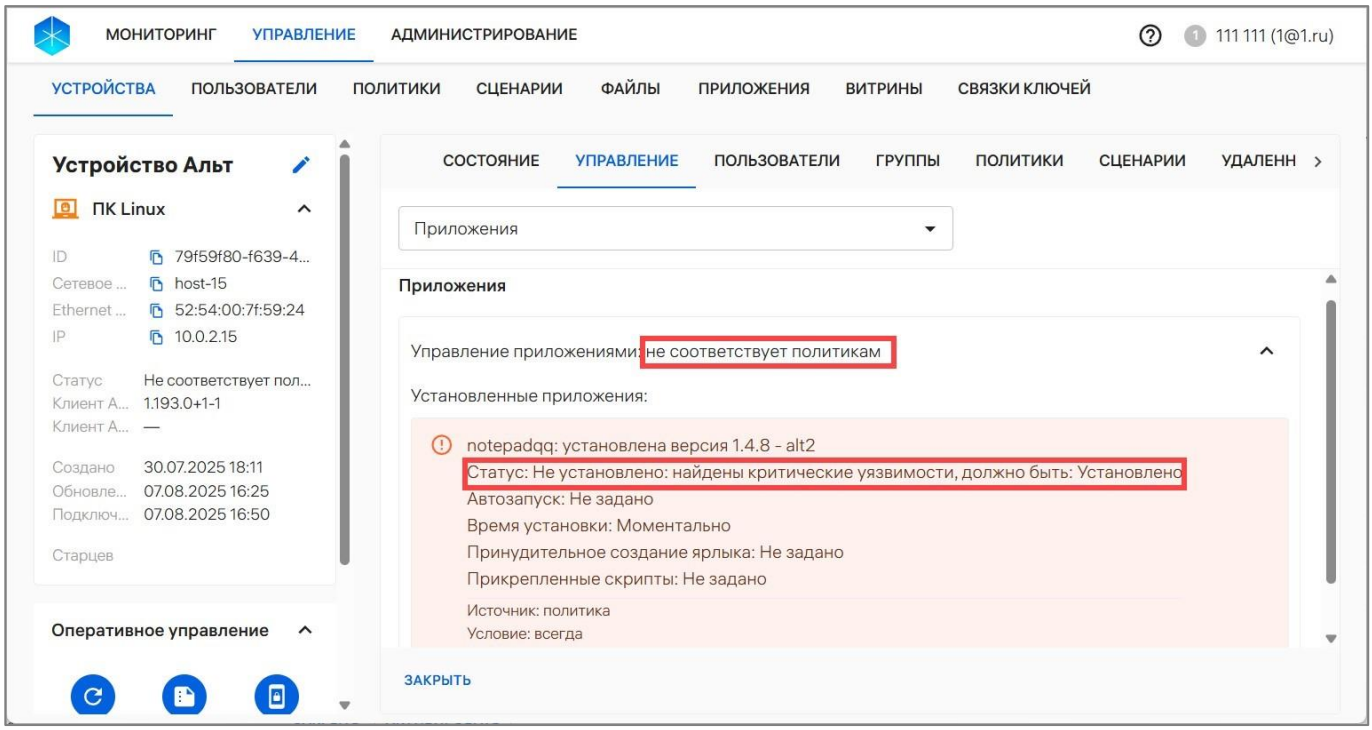


Рисунок 95

– на вкладке «Политики» для правила «Управление приложениями» справа от наименования и версии приложения индикатор (красная точка). При наведении на значение версии отобразится всплывающая подсказка, где к существующему тексту будет добавлено «найдены критические уязвимости» (Рисунок 96).

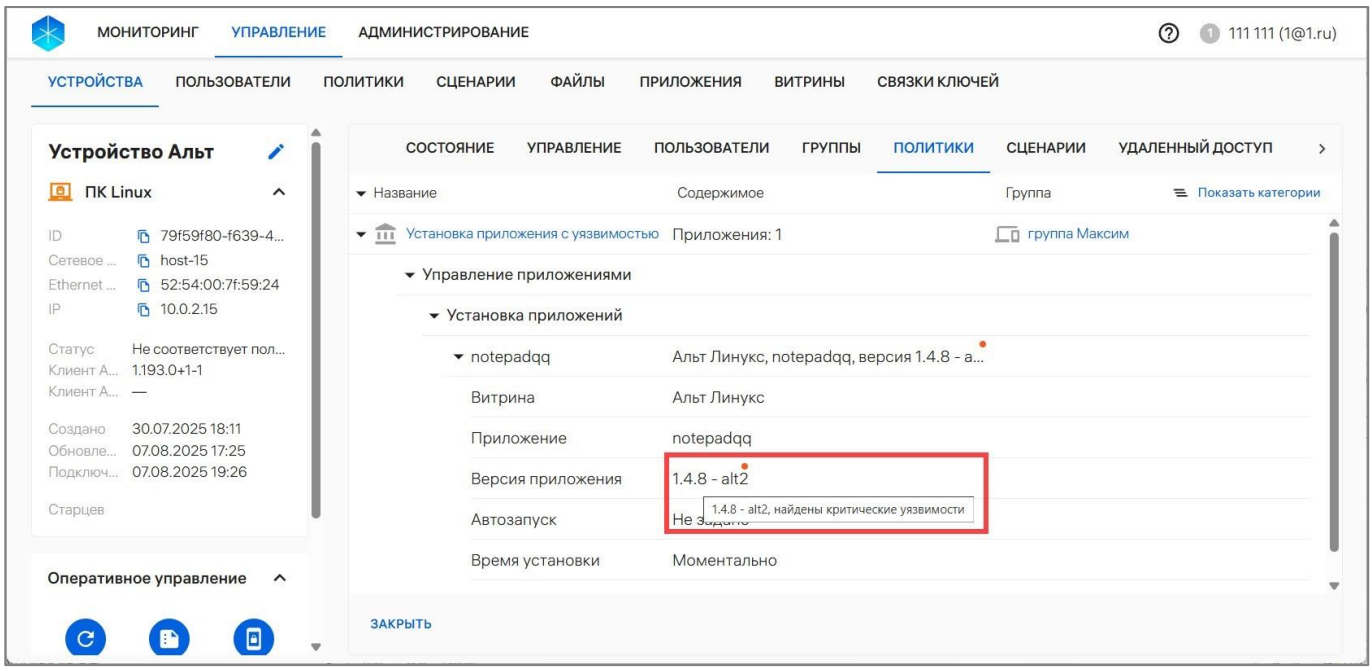


Рисунок 96

2.4.1.58.1. Приложения к установке

Для добавления в правило приложения для установки необходимо:

1) В разделе «Укажите приложения к установке» нажать на значок + «Добавить» (Рисунок 97 [1]);

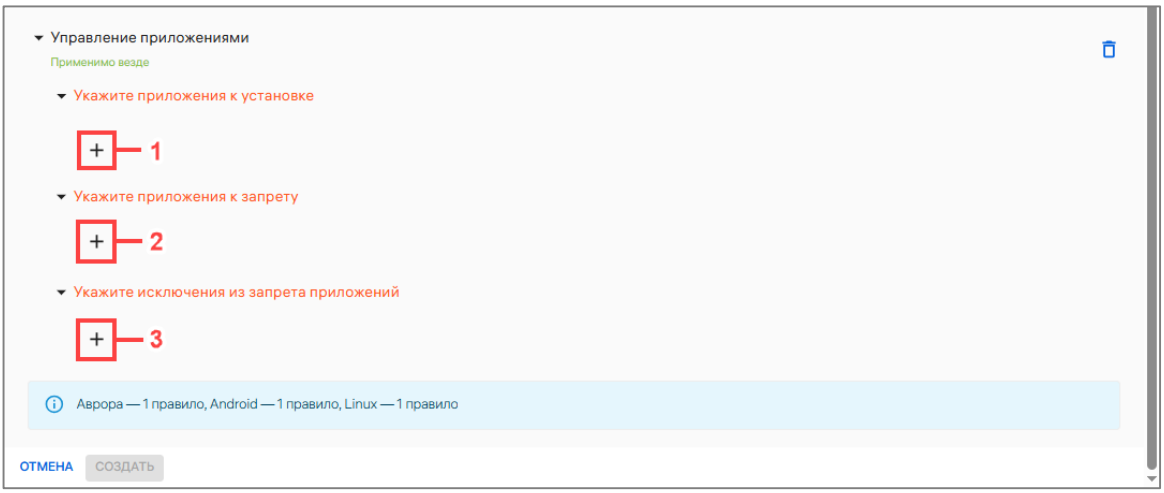


Рисунок 97

2) Если требуется, чтобы все приложения из правила установились на устройстве сразу после получения политики устройством, убедиться что:

– переключатель «Общие настройки установки» находится в положении «Включен»;

– в раскрывающемся списке «Режим установки» выбрано значение «Моментально»;

3) Если требуется, чтобы все приложения из правила установились на устройстве в заданный интервал времени, необходимо:

– убедиться, что переключатель «Общие настройки установки» находится в положении «Включен»;

– в раскрывающемся списке «Режим установки» выбрать значение «По расписанию»;

– если требуется настроить календарный период выполнения правила политики, установить переключатель «Период актуальности» в положение «Включен» и указать дату и время начала и окончания действия правила политики;

– если требуется настроить интервал времени выполнения правила политики:

- перевести переключатель «Интервал установки» в положение «Включен» и указать начало и окончание временного интервала, в течение которого нужно установить приложения;
- в раскрывающемся списке «Тип установки» выбрать, по какому времени будет производиться установка:
  - ♦ «По локальному времени устройства». Выбрано по умолчанию;
  - ♦ «По абсолютному времени». Дополнительно в раскрывающемся списке «Часовой пояс» выбратьчасовой пояс, по времени которого нужно выполнить установку.

ПРИМЕЧАНИЯ:

✓ Для выполнения правила политики «По расписанию» необходимо, чтобы, как минимум одна из опций («Период актуальности», «Интервал установки») была настроена. При этом, обе опции также могут быть настроены одновременно. В таком случае, правило политики будет выполняться в настроенный интервал времени с момента наступления начала периода актуальности и до его завершения;

✓ Для корректной настройки правила политики «По расписанию» необходимо соблюдать следующие ограничения:

– «Период актуальности» должен быть от 1 минуты до 3650 дней (10 лет без учета високосных годов);

– время начала и окончания «Интервала установки» не должны совпадать;

✓ В поле «Период актуальности» отображается локальное время Администратора. При этом, действие выполняется на всех устройствах одновременно без учета локального часового пояса устройства;

✓ Если правило по установке приложений выполнено на устройстве, и истек его период актуальности и/или интервал установки, то приложение не будет удалено с устройства.

Если требуется задать индивидуальное время установки приложения на устройстве, необходимо:

– перевести переключатель «Общие настройки установки» в положение «Выключен»;

– в раскрывающемся списке «Режим установки» ниже полей с данными приложения выбрать нужный режим: «Моментально» или «По расписанию». Настройка режима «По расписанию» выполняется согласно шагам, приведенным выше;

4) Перевести переключатель «Пробуждение устройств» в положение «Включено» (по умолчанию он выключен), если требуется, чтобы устройство пробуждалось для обновления ОС в назначенный интервал.

ВНИМАНИЕ! Пробуждение устройств имеет ряд требований и особенностей, подробное описание приведено в приложении (Приложение 8);

5) В полях с раскрывающимися списками выбрать:

– витрину, в которой размещено приложение;

– приложение, которое необходимо установить на устройства;

– номер версии приложения;

6) Для устройств, функционирующих на базе ОС Аврора, доступно задать автозапуск приложения. Для этого в раскрывающемся списке «Автозапуск» выбрать необходимое значение:

– «Не задано» – пользователь может установить автозапуск приложения вручную. При добавлении правила значение выбрано по умолчанию;

– «Да» – приложение будет запускаться автоматически после загрузки ОС. Пользователь не сможет отменить автозапуск приложения;

– «Нет» – приложение не будет запускаться автоматически после загрузки ОС. Пользователь не сможет установить автозапуск приложения;

7) Если требуется добавить скрипт, который будет выполняться на устройстве после установки приложения, в раскрывающемся списке «Связанные скрипты» необходимо выбрать нужный скрипт.

Для добавления еще одного связанного скрипта, необходимо повторить действия, приведенные выше. В этом случае все выбранные скрипты будут выполнены после установки приложения в произвольном порядке.

ПРИМЕЧАНИЯ:

✓ Параметр доступен только на устройствах с ОС семейства Linux;

✓ В списке отображаются только скрипты, которые добавлены в правиле по выполнению скриптов в той же политике. Если в раскрывающемся списке «Связанные скрипты» нет нужного скрипта, следует нажать «добавить выполнение скриптов» и заполнить параметры правила по выполнению скриптов (пп. 2.4.1.52);

✓ Если приложение из-за ошибки не будет установлено, то скрипт все равно выполнится на устройстве;

8) Если требуется, чтобы desktop-файлы устанавливаемого приложения были вынесены на рабочий стол, перевести переключатель «Принудительное создание ярлыка» в положение «Включен». По умолчанию он выключен.

ПРИМЕЧАНИЯ:

✓ Параметр доступен только на устройствах с ОС семейства Linux;

✓ Если в пакете приложения нет desktop-файлов, то ярлык не будет создан. При этом в карточке устройства будет статус политики «Не соответствует», пока в правиле не будет отключена опция «Принудительное создание ярлыка»;

✓ Если в пакете приложения несколько desktop-файлов, то они все будут вынесены на рабочий стол.

2.4.1.58.2. Приложения к запрету

ПРИМЕЧАНИЯ:

✓ Запрещенные приложения будут удалены с устройства, если были установлены. При этом с помощью запрещенного списка нельзя удалить системное ПО на устройствах с ОС Android;

✓ Запрещенное приложение не будет установлено, если пользователь попытается установить его на устройстве.

Для добавления в правило запрещенных приложений необходимо:

1) В разделе «Укажите приложения к запрету» нажать на значок + «Добавить»;

2) В раскрывающемся списке «Название пакета» выбрать название пакета запрещенного приложения. В списке отображаются названия всех пакетов со всех устройств, которые отправили свое состояние в ПУ. При необходимости воспользоваться фильтром по названию пакета, для этого в поле «Название пакета» ввести полное или частичное название пакета. Если необходимого пакета нет в списке, ввести его точное название и выбрать «Добавить <название пакета>» в раскрывающемся списке;

3) Если необходимо задать диапазон запрещенных версий приложения (по умолчанию запрещены все версии приложения):

– перевести переключатель «Диапазон версий» в положение «Включен»;

– в поле «Диапазон 1» ввести начало (поле «С») и/или конец (поле «До») нужного диапазона. Верхняя граница «До» не включается в интервал;

– нажать кнопку «Диапазон», если требуется добавить еще один диапазон, и повторить шаги, приведенные выше.

ПРИМЕЧАНИЕ. Если заполнено только поле «С», то будут запрещены все версии приложений начиная с нижней границы интервала. Если заполнено только поле «До», то будут запрещены все версии приложений до верхней границы интервала, не включая саму верхнюю границу. Оба условия работают в связке с запрещающим списком приложений.

2.4.1.58.3. Исключенные из запрета приложения

Для добавления в правило списка исключенных из запрета приложений, которые на устройстве должны быть разрешены к установке и дальнейшему использованию, вне зависимости от того, каким образом будет установлено приложение на устройство (через ПУ или вручную), необходимо:

1) В разделе «Исключения из запрета приложений» нажать на значок +;

2) В раскрывающемся списке «Название пакета» выбрать название пакета разрешенного приложения. В списке отображаются названия всех пакетов со всех устройств, которые отправили свое состояние в ПУ. При необходимости воспользоваться фильтром по названию пакета, для этого в поле «Название пакета» ввести полное или частичное название пакета. Если необходимого пакета нет в списке, ввести его точное название и выбрать «Добавить <название пакета>» в раскрывающемся списке;

3) Если необходимо задать диапазон разрешенных версий приложения (по умолчанию разрешены все версии приложения):

– перевести переключатель «Диапазон версий» в положение «Включен».

– в поле «Диапазон 1» ввести начало (поле «С») и/или конец (поле «До») нужного диапазона. Верхняя граница «До» не включается в интервал;

– нажать кнопку «Диапазон», если требуется добавить еще один диапазон, и повторить шаги, приведенные выше.

ПРИМЕЧАНИЯ:

✓ Если заполнено только поле «С», то будут разрешены все версии приложений начиная с нижней границы интервала. Если заполнено только поле «До», то будут разрешены все версии приложений до верхней границы интервала, не включая саму верхнюю границу. Оба условия работают в связке с запрещающим списком приложений;

✓ Раздел правила «Исключения из запрета приложений» работает в связке с разделом «Запрет приложений», но позволяет задавать в политиках список запрещенных и список исключенных из запрета приложений раздельно. Примеры:

1) Назначить на одну группу устройств запрещающий список с приложением «master-pdf» всех версий, далее назначить на вторую группу устройств (куда входят часть устройств из первой группы) исключающий из запрета список с тем же приложением «master-pdf» всех версий. В результате комбинирования политик на второй группе приложение «master-pdf» будет разрешено к установке и дальнейшему использованию всех версий на этих устройствах;

2) Назначить на одну группу устройств запрещающий список с приложением «master-pdf» с диапазоном версий: «С» 1 «До» 10, далее назначить на вторую группу устройств (куда входят часть устройств из первой группы) исключающий из запрета список с тем же приложением «master-pdf» с диапазоном версий: «С» 3 «До» 5. В результате комбинирования политик на второй группе приложение «master-pdf»

версий «С» 3 «До» 5 будет разрешено к установке и дальнейшему использованию этих версий на этих устройствах.

Также важно иметь ввиду:

– что для этих устройств в карточке устройства во вкладке «Состояние» из запрещающего списка:

- пропадет это приложение полностью, если все версии приложения, входящие в диапазон, исключены из запрета. Оно останется только в исключающем списке;
- пропадет только тот диапазон версий приложения, который входит в диапазон версий из исключающего списка запрещенных приложений;

– если запрещающий список был назначен раньше, чем исключающий из запрета список, то приложения все равно будут удалены, но их можно будет заново установить и после этого они не будут удаляться до тех пор, пока не будут исключены из исключающего из запрета списка.

2.4.1.59.Приложения/Управление доверенными источниками

Правило позволяет отправить на устройство список доверенных источников для установки приложений.

Для создания правила необходимо:

1) Перевести переключатель «Разрешить установку без доверенных источников» в положение «Включено», если необходимо разрешить на устройстве установку приложений без доверенных источников (по умолчанию выключен);

2) По умолчанию в поле «Доверенные источники» уже введен источник `source.rustore.ru`.

ПРИМЕЧАНИЕ. Для корректной работы политики на устройствах с ОС Аврора версии 5.2.1 необходимо также в поле «Доверенные источники» добавить значение `ru.omp.auroracenter`.

Чтобы:

– добавить еще один доверенный источник, откуда можно устанавливать приложения на устройство, ввести его и нажать «Enter» на клавиатуре. Требования к доверенному источнику для ввода:

- метки, разделенные точками (минимум одна);
- латинские символы, числа, символы "." и "-";
- не менее 3 символов (включая точку);
- максимум 255 символов;
- не допускается две и более точек подряд;
- не должен начинаться с числа или точки;
- не должен оканчиваться на точку;

– удалить доверенный источник из правила, нажать на значок крестика справа от доверенного источника.

В поле «Доверенные источники» необходимо указывать то название источника, которое было использовано при формировании запроса сертификата (подробная информация о работе со связками ключей в ПМ приведена в документе «Руководство пользователя. Часть 2. Подсистема «Маркет»).

2.4.1.60.Приложения/Ограничение установки из источников

Правило позволяет запретить установку приложений из всех или неизвестных источников.

Для создания правила необходимо в раскрывающемся списке выбрать нужное значение:

– **«Запрещено из любых источников» –** запрет установки приложений из любых источников, кроме Аврора Центр и приложения «Аврора Маркет». При добавлении правила значение выбрано по умолчанию;

– **«Запрещено из неизвестных источников» –** запрет установки приложений из неизвестных источников, кроме Аврора Центр и приложения «Аврора Маркет». Установка ПО из магазинов приложений на устройстве, которые являются известными (доверенными) для ОС (например, Play Market), будет разрешена.

ВНИМАНИЕ! Если магазин был предустановлен вендором, то он является доверенным. Если магазин был установлен пользователем (даже при наличии отметки пользователем, как доверенный), ОС не будет считать его доверенным и также попадет под действие политики;

– **«Разрешено из всех источников» –** разрешение установки приложений из любых источников, которые разрешены на устройстве.

ПРИМЕЧАНИЕ. Если на устройство назначены две и более политик с правилом «Приложения/Ограничение установки из источников», комбинирование будет выполнено по следующему приоритету:

1) Запрещено из любых источников;
2) Запрещено из неизвестных источников;
3) Разрешено из всех источников.

2.4.1.61.Приложения/Управляемые конфигурации

ПРИМЕЧАНИЕ. Правило применимо только для приложений, установленных на устройство (из любого источника), которые поддерживают `appconfig`.

Правило позволяет отправить на устройство и применить настройки приложений (`appconfig`). Данное правило следует использовать в случае, когда необходимо настроить приложение на парке устройств. `Appconfig` позволяет администраторам задавать параметры для конкретных приложений, без взаимодействия с приложением вручную.

Для создания правила необходимо:

1) В поле «Название пакета» (Рисунок 98 [1]) ввести название пакета, для которого нужно установить конфигурацию. При необходимости название пакета можно посмотреть в карточке устройства во вкладке «Приложения» в столбце «Инфо» (подробнее в пп. 2.1.1.9);

2) В поле «Конфигурация» (Рисунок 98 [2]) ввести в формате JSON конфигурацию пакета;



Рисунок 98

3) При необходимости чувствительные данные можно защитить с помощью подстановки управляемых(защищенные и незащищенные) переменных.

ПРИМЕЧАНИЕ. Защищенными являются переменные окружения, которые будут использованы визолированной среде при применении конфигурации приложения.

Для добавления управляемой переменной необходимо:

– нажать «Добавить переменную» (см. Рисунок 98 [3]);

– в поле «Переменная в конфигурации» (Рисунок 99) ввести идентичное название переменной, которое было введено в поле «Конфигурация»;

– в раскрывающемся списке «Переменная к подстановке» выбрать нужную управляемую переменную для подстановки в конфигурацию. Если нужной управляемой переменной нет в списке, необходимо добавить ее (подробнее в п. 4.1.8).

Если требуется добавить еще одну переменную для подстановки, необходимо нажать «Добавить переменную» (см. Рисунок 98 [3]) и повторить шаги, приведенные выше;

4) Если требуется добавить в правило конфигурацию для другого приложения, необходимо нажать на значок + в левом нижнем углу и повторить шаги выше.

Политика назначится, если на устройстве есть приложение, указанное в политике. Если сначала была создана политика с правилом конфигурации, а

приложение установили после, то конфигурация применится после установки приложения.

Для того чтобы указать место для подстановки переменной, необходимо заполнить JSON по примеру: `app:<<значение>>`.

ПРИМЕЧАНИЯ:

✓ Если переменная заблокирована, то конфигурация не применится в приложении на устройстве;

✓ При комбинировании политик будет применяется только правило «Приложения/Управляемые конфигурации» той политики, которая была обновлена позже других.

Пример применения конфигурации для приложения Trueconf.

В приложении Trueconf для ОС Android поддержаны следующие параметры (Таблица 49):

– автоматическое подключение к серверу;
– запрет снятия скриншотов и видео.

Таблица 49

Параметр	Тип	Описание
ServerURL	`string`	Адрес сервера, к которому подключается клиент
Recordingforbidden	`bool`	Запрет на снятие скриншотов и видео (`true/false`)

Для применения данной конфигурации необходимо в поле конфигурация ввести JSON вида (пример для версии 3.2.1.195):

```
{
"server_url": "vks.my.domain""recording_forbidden": true
}
```

После завершения настройки правила и применения политики на устройстве аппконфиг применится к приложению.

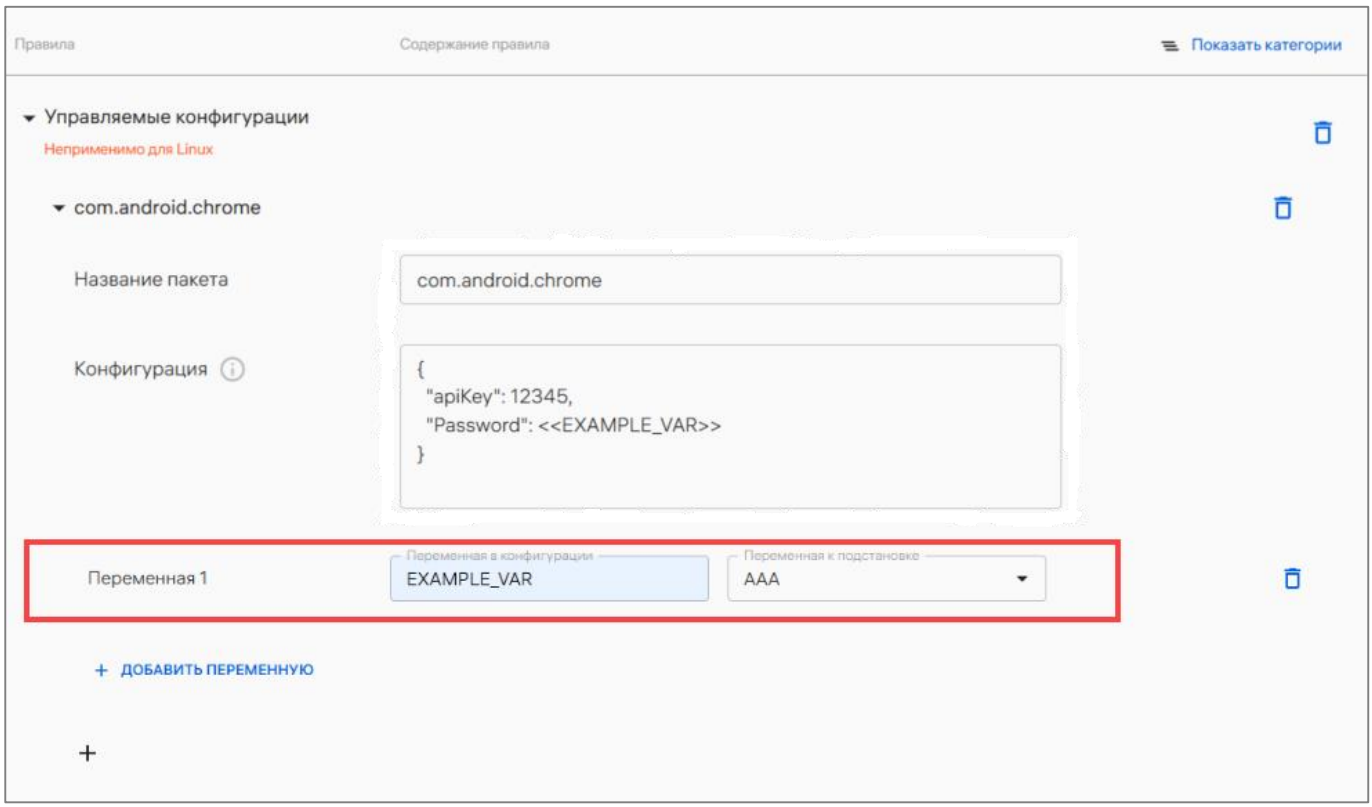


Рисунок 99

Для поиска нужных переменных (на примере приложения) необходимо выполнить следующие действия:

1) Разместить файлы `apktool.bat`, `apktool.jar` и приложения apk в одном каталоге;

2) Запустить командную строку и перейти в каталог с указанными файлами:

```
cd /d D:\Путь\К\Каталогу\с\файлами\
```

Например:

```
cd /d D:\Projects\apk\
```

3) Запустить распаковку приложения;

4) Перейти в распакованный каталог и найти файл (`/res/xml/app_restrictions.xml`);

5) В файле посмотреть доступные для изменения переменные android:key=:

```
<restrictions
xmlns:android="http://schemas.android.com/apk/res/android">

<restriction
android:description="@string/server_name_property_description"
android:title="@string/                    server_name_property"
android:key="server_url" android:restrictionType="string"/>

<restriction
android:description="@string/screen_recording_forbidden_description"
android:title="@string/                    screen_recording_forbidden"
```

```
android:key="recording_forbidden"          android:defaultValue="false"
android:restrictionType="bool"/> </restrictions>
```

Пример: "server_url" (может иметь текстовое значение (Type="string") и "recording_forbidden" (Может иметь значение true/false (Type="bool") "server_url": "vks.my.domain" "recording_forbidden": true

2.4.1.62.Приложения/Подключение витрин в клиенте Аврора Маркет

Правило позволяет задавать нужное количество витрин для их дальнейшего подключения на устройствах в приложении «Аврора Маркет».

ПРИМЕЧАНИЯ:

✓ Для корректного применения политики рекомендуется сохранить исходную ссылку на витрину для подключения без изменений;

✓ Витрины, подключаемые в приложении «Аврора Маркет» через политику, управляются через ПУ и недоступны для удаления вручную;

✓ Если подключаемая витрина из политики уже ранее была добавлена вручную, то ПУ берет ее под управление и она становится недоступной для удаления вручную.

Для создания правила необходимо в поле «Витрина 1» вставить скопированную в карточке витрины ПМ ссылку для подключения к витрине (подробнее в документе «Руководство пользователя. Часть 2. Подсистема «Маркет») и нажать на кнопку «Создать».

Если требуется указать более одной подключаемой витрины, необходимо нажать на значок + и вставить скопированную в ПМ ссылку.

ВНИМАНИЕ! Если подключаемая витрина имеет настройки доступа по входу с логином и паролем и:

– разрешена всем пользователям приложения «Аврора Маркет», то такая витрина будет добавлена, но для отображения и получения доступа к приложениям из этой витрины пользователю потребуется пройти авторизацию;

– запрещена всем пользователям приложения «Аврора Маркет», то такая витрина будет добавлена, однако попытка авторизации завершится ошибкой, вследствие чего приложения из данной витрины не будут отображаться и не будут доступны для скачивания и установки.

ПРИМЕЧАНИЕ. Более подробная информация о работе с витринами приведена в документе «Руководство пользователя. Часть 2. Подсистема «Маркет».

Когда приложение «Аврора Маркет» подключит витрины из назначенной политики, пользователь увидит уведомление о необходимости перезапустить приложение, чтобы подключенные витрины отобразились для дальнейшей работы с ними.

2.4.1.63.Мобильная сеть/Точка доступа

Правило позволяет создать и настроить на устройстве точку доступа мобильной сети (APN).

Для создания правила необходимо заполнить поля, приведенные в таблице (Таблица 50).

Таблица 50

Наименование полей	Описание
Имя	Ввести имя точки доступа мобильной сети. Поле обязательно для заполнения. Может содержать от 1 до 256 символов
APN	Ввести хост точки доступа мобильной сети. Поле обязательно для заполнения. Требования к заполнению: – длина строки от 1 до 253 символов; – длина каждого сегмента (если разрезать строку по точкам) от 1 до 63 символов; – каждый сегмент содержит только латинские буквы, цифры, тире, при этом первый знак каждого сегмента не может быть тире либо нижнее подчеркивание
Тип APN	При добавлении правила значение по умолчанию «Интернет». Поле недоступно для редактирования
Тип аутентификации	При добавлении правила значение по умолчанию «Нет». Поле недоступно для редактирования
MCC	Ввести мобильный код страны. Поле обязательно для заполнения. Может содержать номер от 001 до 999
MNC	Ввести код мобильной сети. Поле обязательно для заполнения. Может содержать код от 01 до 999

ПРИМЕЧАНИЕ. При назначении политики следует учитывать следующие особенности:

– ОС Аврора и ОС Android:

- нет методов получения данных об MCC и MNC. Поэтому эти данные берутся из OperatorNumeric (для ОС Android) и IMSI (для ОС Аврора) по следующему принципу: MCC – первые 3 символа, MNC – 4 и 5 символ. Поскольку MNC в России двузначный – для других стран MNC может быть трехзначным и это надо учитывать, если SIM-карта и оператор сотовой связи будет из других стран;

– ОС Android:

- создание точки доступа мобильной сети возможно на ОС Android с версией 9 и выше;

- настройки точки доступа мобильной сети, выставленные через приложение «Аврора Центр», нельзя посмотреть и/или изменить на устройстве вручную;
- создание точки доступа мобильной сети работает некорректно на устройстве Huawei POT-LX1 с ОС Android версии 10;

– ОС Аврора:

- из-за ограничений MDM API нельзя выставить MCC и MNC;
- выставлять настройки точки доступа мобильной сети можно только применительно к конкретной SIM-карте, при этом, после выставления настроек эта SIM-карта становится картой по умолчанию для интернет-соединения (ограничение MDM API);
- выставлять настройки точки доступа мобильной сети можно только применительно к конкретной SIM-карте, соответственно, поддерживаются устройства, в которых вставлена одна SIM-карта. Если на устройстве более одной SIM-карты, то поведение будет неопределенным, поскольку настройки будут выставлены на ту SIM-карту, значение IMSI которой меньше в результате лексикографической сортировки;
- после удаления правила политики для настройки параметров точки доступа к мобильной сети эти значения не удаляются с устройства – значения по умолчанию не сбрасываются до первоначальных (ограничение MDM API). Как следствие этого поведения, если на устройство назначить правило политики с точно такими же настройками, какие уже выставлены в ОС, то в журнале приложения «Аврора Центр» не будет сообщения о создании точки доступа мобильной сети, поскольку она уже создана на устройстве.

2.4.1.64.Мобильная сеть/Управление мобильной передачей данных

Правило запрещает/разрешает конфигурировать мобильную передачу данных. В случае назначения запрещающего правила:

– для устройств с ОС Аврора правило запрещает/разрешает конфигурировать мобильную передачу данных. Также запрещается выключение/включение мобильной передачи данных. Параметр фиксируется в том состоянии, в котором был до применения политики с этим правилом;

– для устройств с ОС Android правило запрещает/разрешает конфигурировать мобильную передачу данных. При этом не запрещается выключение/включение мобильной передачи данных. Однако у некоторых производителей устройств с ОС Android данное правило может запрещать выключение/включение мобильной передачи данных, что является устройство-специфичным поведением.

Выбор значения из списка:

– «Разрешено»;

– «Запрещено». При добавлении правила значение выбрано по умолчанию.

2.4.1.65.Мобильная сеть/Определение номера телефона

Правило позволяет включить/отключить определение номера телефона на устройстве и его передачу в ППО.

Выбор значения из списка:

– «Выключено». При добавлении правила значение выбрано по умолчанию.

– «Включено».

Особенности получения номера телефона на устройствах с ОС Android:

1) Для устройств с ОС Android 7 номер будет передан в Аврора Центр только, если оператор передал номер на SIM-карту или номер прописан в настройках SIM-карты;

2) Для устройств с ОС Android 8 и выше для получения номера используется USSD-запрос. Запрос номера выполняется при перезапуске приложения «Аврора Центр» (например, при перезагрузке устройства), либо при смене SIM-карты при включенном устройстве.

ПРИМЕЧАНИЕ. На некоторых устройствах (например, если на устройстве SIM-карты расположены в раздельных слотах) смена SIM-карты может быть не распознана в качестве триггера для нового USSD-запроса. В этом случае необходимо перезапустить приложение «Аврора Центр» (например, сделать перезагрузку устройства);

3) USSD-команды операторов мобильной связи для получения номера SIM:

– **МТС**: *111*0887#;

– **Мегафон**: *205#;

– **Билайн**: *110*10# - сведения о номере и его возможностях;

– **Tele2**: *201#;

– **Yota**: *103#;

– **Тинькофф Мобайл**: *100# - информация о балансе, остатках пакетов, а также о номере абонента;

– **Сбер Мобайл:** *200#;

– **Ростелеком** (Tele2): *201#;

– **ВТБ Мобайл**: *200#;

4) При запросе состояния устройства будет передан номер, полученный ранее;

5) Отправка USSD-кодов не работает, если включен режим мобильной сети «Только LTE»;

6) В ответ на USSD-запрос может прийти:

– уведомление с номером телефона (10 сек. на ожидание). В этом случае номер будет отправлен сразу вместе с состоянием;

– SMS с номером телефона. В случае задержки ответного SMS вместе с состоянием не будет отправлен номер телефона. Он будет извлечен по факту получения SMS и отправлен при следующем запросе состояния;

7) Если в ответ на USSD-запрос пришло SMS и в устройстве две активных SIM-карты, то осуществляется дополнительная проверка на принадлежность SMS (с номером телефона) SIM-карте. В результате в карточке устройства будет отображен номер телефона в той секции SIM-карты, на которую пришло SMS;

8) Для виртуальной SIM-карты (eSIM) действуют тебе же правила определения номера, что и для физической SIM-карты.

2.4.2. Добавление политики вручную

Для добавления политики вручную необходимо выполнить следующие действия:

– перейти в подраздел «Политики» раздела «Управление»;

– нажать кнопку «Добавить» и выбрать из раскрывающегося списка «Добавить политику» (Рисунок 100);

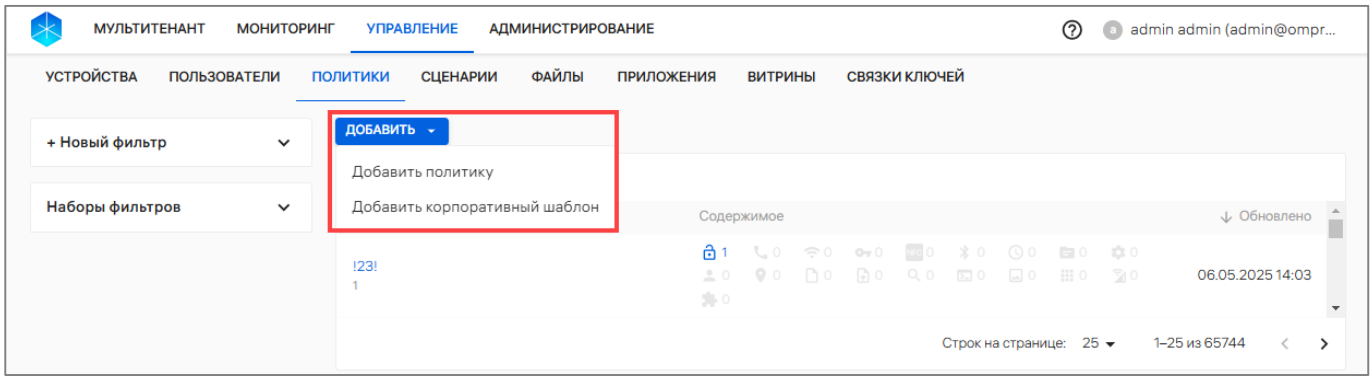


Рисунок 100

– в открывшемся окне:

- ввести название политики – название политики должно быть уникальным. Поле обязательно для заполнения;
- ввести комментарий – при необходимости ввести дополнительную информацию к политике;
- нажать кнопку «Добавить правило» и выбрать правило политики из раскрывающегося списка;
- задать параметры правила. Описание правил для политик приведено в таблице (см. Таблица 45).

В случае необходимости создать политику из нескольких правил следует повторить действия, описанные выше.

В случае необходимости удалить правило следует нажать значок «Удалить» справа от правила.

После выполнения действий, описанных выше, необходимо подтвердить либо отменить действия.

В результате успешного сохранения политики отобразится соответствующее сообщение и откроется карточка добавленной политики (п. 2.4.6).

2.4.3. Добавление политики на основе корпоративного шаблона

При необходимости на этапе добавления политики вручную возможно воспользоваться функционалом импорта шаблона.

ПРИМЕЧАНИЕ. Импорт шаблона возможно выполнить при условии, что корпоративный шаблон политик уже создан (пп. 2.4.3.1).

Для добавления политики на основе корпоративного шаблона необходимо в окне ввести:

– название политики (название политики должно быть уникальным. Поле обязательно для заполнения);

– комментарий (при необходимости ввести дополнительную информацию к политике);

– нажать кнопку «Импорт шаблона», в результате чего правила из корпоративного шаблона будут импортированы в новую политику.

При необходимости, в соответствии с п. 2.4.1, импортированные правила возможно:

– изменить. Описание правил для политик приведено в таблице (см. Таблица 45);

– добавить правило в политику;

– удалить правило.

После выполнения действий, описанных выше, необходимо подтвердить либо отменить действия.

В результате успешного добавления политики отобразится соответствующее сообщение и откроется карточка добавленной политики.

2.4.3.1. Добавление корпоративного шаблона

Корпоративный шаблон политик содержит стандартный для организации набор правил. Указанные значения будут использованы для последующего применения на устройствах, если они не определены создаваемой политикой. Шаблон политики освобождает Администратора Платформы управления от манипуляций с повторяемыми опциями на этапе создания новых политик.

Корпоративный шаблон политик включает в себя все опции, доступные для управления в момент создания шаблона. При создании корпоративного шаблона Администратор Платформы управления указывает значения опций «по умолчанию» и получает возможность создавать политики на основе этого шаблона.

Для добавления корпоративного шаблона необходимо выполнить следующие действия:

– перейти в подраздел «Политики» раздела «Управление»;

– нажать кнопку «Добавить»;

– выбрать из раскрывающегося списка пункт «Добавить корпоративный шаблон» (см. Рисунок 100).

ВНИМАНИЕ! Предусмотрена возможность создания только одного корпоративного шаблона. Пункт меню «Добавить корпоративный шаблон» отсутствует, если корпоративный шаблон политик уже создан. Вместо него отображается пункт меню «Редактировать корпоративный шаблон»;

– в открывшемся окне возможно выполнить следующие действия:

• при необходимости изменить комментарий к корпоративному шаблону (наименование корпоративного шаблона проставляется автоматически);

• добавить правила в корпоративный шаблон, нажав на кнопку «Добавить правило». Добавление правила выполняется в соответствии с п. 2.4.1.

ПРИМЕЧАНИЕ. По умолчанию корпоративный шаблон не содержит ни одного правила;

– подтвердить либо отменить действия.

В результате успешного создания корпоративного шаблона политики отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если корпоративный шаблон политик не создан, то в подразделе «Аудит» раздела «Мониторинг» отобразится ошибка «404» для следующих событий:

– переход в подраздел «Политики»;

– комбинирование политик.

2.4.3.2. Редактирование корпоративного шаблона

Созданный шаблон политики доступен для редактирования.

Редактирование предполагает изменение (в том числе удаление или дополнение) существующих правил шаблона.

Для редактирования корпоративного шаблона необходимо выполнить следующие действия:

– перейти в подраздел «Политики» раздела «Управление»;

– нажать кнопку «Добавить»;

– выбрать из раскрывающегося списка пункт «Редактировать корпоративный шаблон»;

– в открывшемся окне внести изменения, выполнив действия, приведенные в пп. 2.4.3.1.

В результате успешного сохранения внесенных в корпоративный шаблон изменений отобразится соответствующее сообщение.

ВНИМАНИЕ! После редактирования корпоративного шаблона для его вступления в силу необходимо отредактировать и применить текущую политику либо отвязать ее и снова применить.

2.4.4. Назначение политики на группы устройств или группы пользователей

Назначить политику на группу устройств и/или группу пользователей возможно через:

– карточку политики (пп. 2.4.4.1);
– карточку группы устройств (пп. 2.4.4.2);
– карточку группы пользователей (пп. 2.4.4.3).

2.4.4.1. Назначение политики на группы устройств и/или группы пользователей через карточку политики

Для назначения политики на группы устройств и/или группы пользователей необходимо выполнить следующие действия:

– перейти в подраздел «Политики» раздела «Управление»;
– нажать на название политики для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);
– в открывшейся карточке политики перейти во вкладку «Группы»;
– нажать кнопку «Редактировать группы»;
– в открывшемся окне нажать кнопку «Добавить»;
– в раскрывающемся списке выбрать тип группы:
  • «Группу устройств»;
  • «Группу пользователей»;
– выбрать необходимую группу из раскрывающегося списка или воспользоваться фильтром по названию группы.

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешного назначения политики на группы устройств и/или группы пользователей отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. При наличии нескольких изменений политик, например: редактирование политик, назначение политик на группы устройств или группы пользователей, добавление устройств в группы устройств и т.д., на устройство будет назначена последняя скомбинированная политика.

2.4.4.2. Назначение политики на группу устройств через карточку группы

В Консоли администратора ПУ предусмотрена возможность контроля и отслеживания политик, назначенных на группу устройств. Политики содержат набор правил для применения на устройства.

ПРИМЕЧАНИЕ. Перед назначением политики на группу устройств необходимо убедиться, что добавлена хотя бы 1 политика. Добавление политик описано в п. 2.4.1 – 2.4.4.

Для назначения политик на группу устройств необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;
– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы устройств для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке группы устройств перейти во вкладку «Политики»;

– нажать кнопку «Назначить политики»;

– в отобразившемся окне выбрать необходимую политику из раскрывающегося списка или воспользоваться фильтром (Рисунок 101 [1]). Далее при необходимости возможно добавить дополнительную политику, выбрав ее из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранную политику, нажав значок «Убрать из списка» (Рисунок 101 [3]);

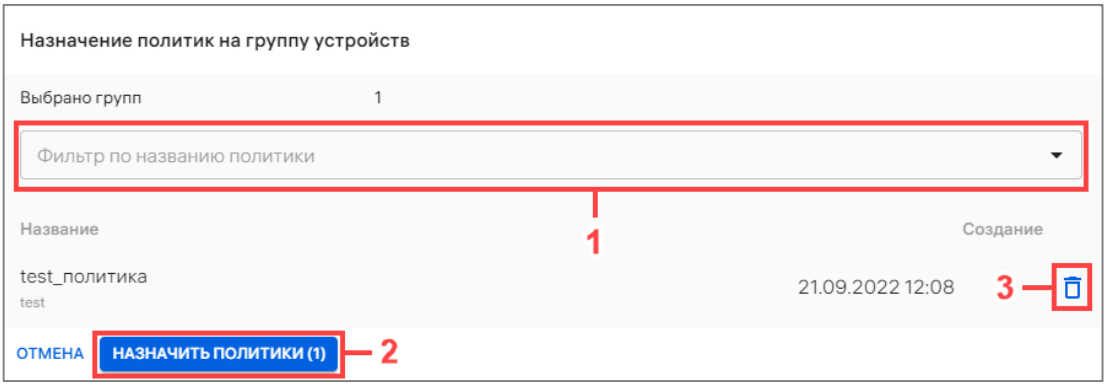


Рисунок 101

– нажать кнопку «Назначить политики» (см. Рисунок 101 [2]).

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешного назначения политики на группу устройств отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если устройство, входящее в группу, не было активировано, то после его активации на него будет назначена только последняя скомбинированная политика.

2.4.4.3. Назначение политики на группу пользователей через карточку группы

Для назначения политик на группу пользователей через карточку группы необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке группы пользователей перейти во вкладку «Политики»;

– нажать кнопку «Назначить политики»;

– в открывшемся окне (см. Рисунок 101) выполнить действия, приведенные в пп. 2.4.4.2.

В результате успешного назначения политики на группу пользователей отобразится соответствующее сообщение.

ПРИМЕЧАНИЕ. Если устройство, привязанное к пользователю из группы, не было активировано, то после его активации на него будет назначена только последняя скомбинированная политика.

2.4.5. Добавление политики на основе существующей

ПРИМЕЧАНИЕ. Добавление политики на основе существующей возможно только при условии, что добавлена хотя бы 1 политика (п. 2.4.2, 2.4.3).

Для добавления политики на основе существующей необходимо выполнить следующие действия:

– перейти в подраздел «Политики» раздела «Управление»;

– скопировать правила интересующей политики одним из следующих способов:

- выбрать политику в списке, при необходимости воспользовавшись фильтром, перейти в карточку выбранной политики и нажать кнопку «Создать политику на основе существующей»;

– в списке политик нажать кнопку «Добавить» или выбрать из раскрывающегося списка «Добавить политику» (см. Рисунок 100), а затем нажать кнопку «Импорт правил» (Рисунок 102 [1]). Из раскрывающегося списка выбрать правило политики, которое необходимо скопировать (при необходимости воспользоваться фильтром по названию политики) (Рисунок 102 [2]). В результате правила из выбранной политики будут импортированы в новую политику;

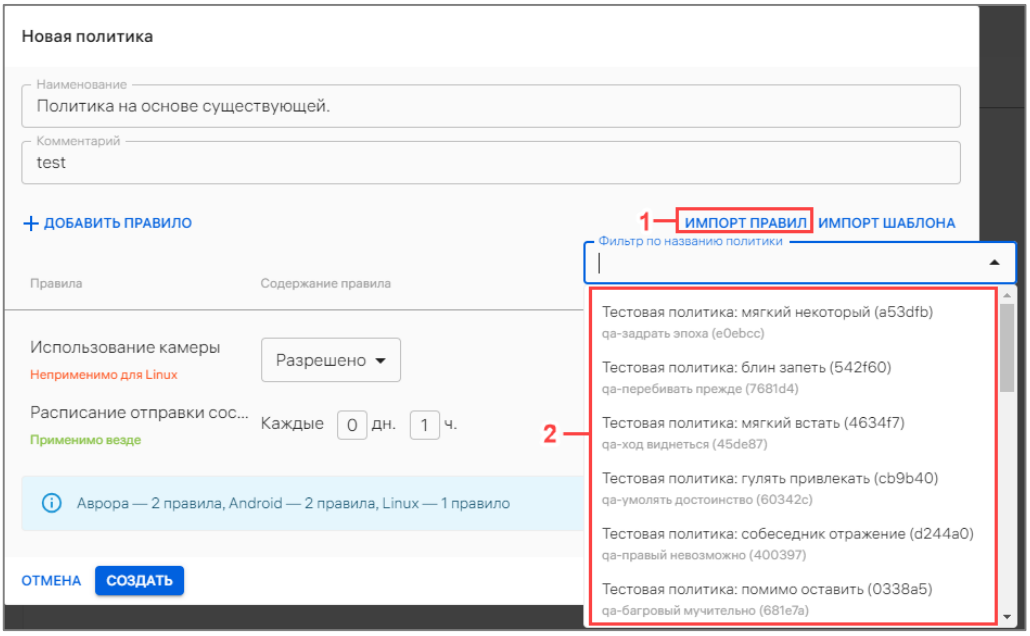


Рисунок 102

– в открывшемся окне:

• ввести название политики (название политики должно быть уникальным). Поле обязательно для заполнения;

• ввести комментарий (при необходимости ввести дополнительную информацию к политике);

• при необходимости изменить параметры импортированных правил (см. Таблица 45).

Если необходимо добавить правило в политику или удалить правило, следует выполнить действия, описанные в п. 2.4.2.

После выполнения действий, описанных выше, необходимо подтвердить либо отменить действия.

2.4.6. Редактирование правила политики

ВНИМАНИЕ! Удаление запрещающего правила из политики, отвязка политики от группы или исключение устройства из группы не приведет к изменению состояния самого устройства (например, если правило политики запрещало использование камеры, то после снятия такой политики камера останется не доступной на устройстве). Для изменения состояния необходимо явно в политике установить целевое состояние. Также можно использовать корпоративный шаблон политики (пп. 2.4.3.1). Например, если в корпоративном шаблоне политики будет задано разрешающее правило политики на использование камеры, и при этом на устройстве будет назначена любая политика (даже пустая), тогда устройство приведется в состояние, указанное в корпоративном шаблоне. Важно понимать, что корпоративный шаблон действует на всех устройствах, на которых действует хотя бы одна политика, и регулирует только те правила, которые явно не заданы в политиках.

Набор правил политики возможно отредактировать, выполнив следующие действия:

– перейти в подраздел «Политики» раздела «Управление»;

– выбрать политику из списка, при необходимости воспользовавшись фильтром (подраздел 1.4);

– перейти в карточку политики во вкладку «Правила»/«Группы»;

– нажать на значок ⋮ (Рисунок 103) и выполнить следующие действия:

• Редактировать данные (внести необходимые изменения);

• Создавать политику на основе существующей (п. 2.4.5);

• Удалить (п. 2.4.8);

– в открывшемся окне внести изменения в правилах политики (Рисунок 104 [2]) в соответствии с таблицей (см. Таблица 45);

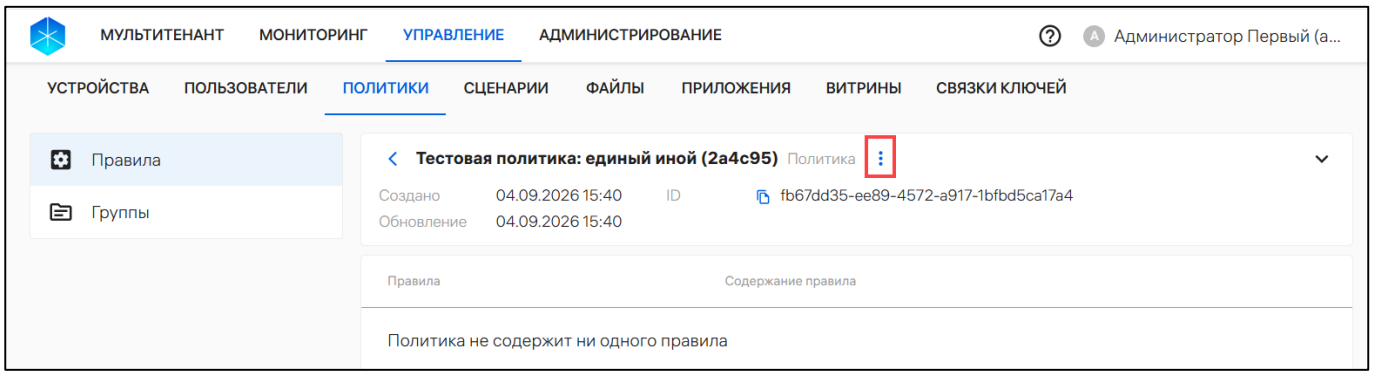


Рисунок 103

При редактировании данных:

– для добавления дополнительных правил нажать кнопку «Добавить правило» (Рисунок 104 [1]) и выбрать правило политики из раскрывающегося списка и задать его параметры (при необходимости);

– для удаления правил из политики нажать значок «Удалить» (Рисунок 104 [3]) справа от правила (при необходимости);

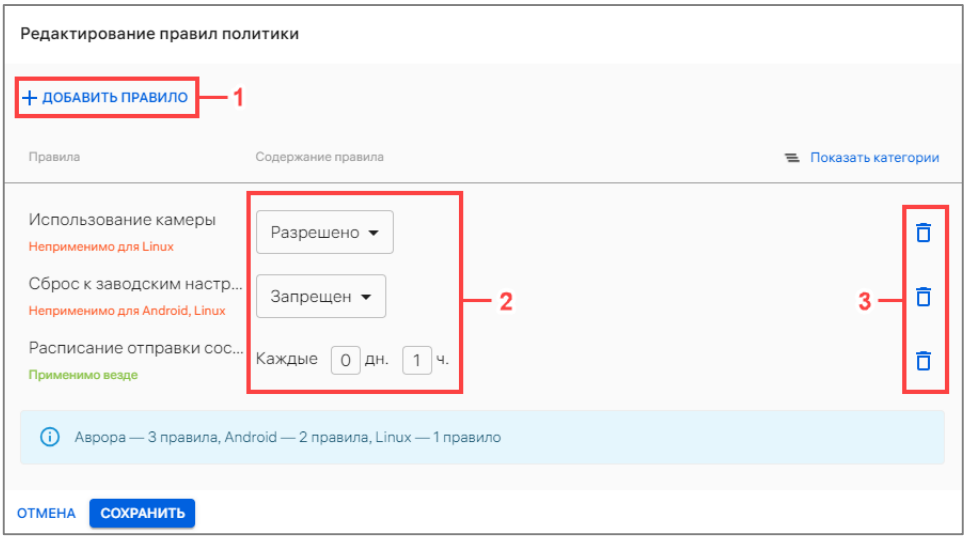


Рисунок 104

– сохранить изменения либо отменить действия.

При успешном сохранении изменений начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Отобразится предупреждение о том, что это может занять некоторое время.

Для автоматического применения политики следует нажать кнопку «Подтвердить», не дожидаясь результата проверки, в результате политика с обновленными правилами будет назначена на все устройства.

Для просмотра пересечения политики с другими политиками и правилами из корпоративного шаблона необходимо дождаться завершения проверки. В результате будет отображен список названий пересекающихся групп и устройств, на которых пересекается политика, а также скомбинированная политика.

Для применения политики на все устройства необходимо нажать кнопку «Подтвердить», в результате чего отобразится сообщение «Политика обновлена». Новые правила начнут действовать для всех активированных устройств, входящих в группы устройств или пользователей, на которые была назначена политика.

ПРИМЕЧАНИЕ. Перед применением скомбинированной политики следует учитывать следующее:

– приоритет имеют запрещающие правила;
– для правил с датами в приоритете правило с более поздней датой создания;
– для периодов – у наименьшего периода действия;
– для правил с версиями (обновление ОС и установка приложения) приоритет у последней версии (например, если версии 1.0.0 и 1.0.1 – будет установлена 1.0.1);
– для правила хранения системных сообщений приоритет у постоянного;
– корпоративный шаблон дополняет скомбинированную политику правилами, которые указаны в нем, но не указаны в скомбинированной политике.

2.4.7. Отвязка политики от группы устройств или группы пользователей

ВНИМАНИЕ! Удаление запрещающего правила из политики, отвязка политики от группы или исключение устройства из группы не приведет к изменению состояния самого устройства. (например, если правило политики запрещало использование камеры, то после снятия такой политики камера останется не доступной на устройстве). Для изменения состояния необходимо явно в политике установить целевое состояние. Также можно использовать корпоративный шаблон политики (пп. 2.4.3.1). Например, если в корпоративном шаблоне политики будет задано разрешающее правило политики на использование камеры, и при этом на устройстве будет назначена любая политика (даже пустая), тогда устройство приведется в состояние, указанное в корпоративный шаблон. Важно понимать, что корпоративный шаблон действует на все устройствах, на которых действует хотя бы одна политика и регулирует только те правила, которые явно не заданы в политиках.

Отвязать политики от группы устройств и/или группу пользователей возможно через:

– карточку политики (пп. 2.4.7.1);
– карточку группы устройств (пп. 2.4.7.2);
– карточку группы пользователей (пп. 2.4.7.3).

2.4.7.1. Отвязка политики от группы устройств и/или группы пользователей через карточку политики

Для отвязки политики от группы устройств и/или группы пользователей необходимо выполнить следующие действия:

– перейти в подраздел «Политики» раздела «Управление»;
– нажать на название политики для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке политики перейти во вкладку «Группы»;
– нажать кнопку «Редактировать группы»;
– в открывшемся окне нажать значок «Отвязать политику от группы».

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешной отвязки, политика будет отвязана от группы устройств или групп пользователей.

2.4.7.2. Отвязка политики от группы устройств через карточку группы

Для отвязки политики от группы устройств необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;
– в области фильтров выбрать «Поиск по группам»;
– нажать на название группы устройств для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);
– в открывшейся карточке группы устройств перейти во вкладку «Политики»;
– выбрать политику, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;
– в списке быстрых действий выбрать значок «Отвязать политики от группы».

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешной отвязки политики от группы устройств отобразится соответствующее сообщение.

2.4.7.3. Отвязка политики от группы пользователей через карточку группы

Для отвязки политик от группы пользователей через карточку группы необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;
– в области фильтров выбрать «Поиск по группам»;
– нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);
– в открывшейся карточке группы пользователей перейти во вкладку «Политики»;

– выбрать политику, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Отвязать политики от группы».

Начнется процесс проверки правил политики на пересечение с другими политиками, а также комбинирование с правилами из корпоративного шаблона политик, если он создан. Процесс проверки пересечения правил политик аналогичен приведенному в п. 2.4.6.

В результате успешной отвязки политики от группы пользователей отобразится соответствующее сообщение.

2.4.8. Удаление политики

ПРИМЕЧАНИЕ. Перед удалением политики необходимо предварительно отвязать ее от всех групп устройств или групп пользователей в соответствии с п. 2.4.7.

Для удаления политики из ПУ необходимо выполнить следующие действия:

– перейти в подраздел «Политики» раздела «Управление»;

– нажать на название необходимой политики для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в карточке политики нажать кнопку «Удалить»;

– в отобразившемся окне подтвердить либо отменить действия.

В результате политика будет успешно удалена.

2.5. Подраздел «Сценарии»

Подраздел «Сценарии» Консоли администратора ПУ предназначен для создания офлайн-сценариев и применения их на устройствах.

Офлайн-сценарии – правила, которые отправляются на устройства с указанием действия (события) по срабатыванию. Правила должны мгновенно примениться на устройстве по указанному событию, даже в случае, если в этот момент нет связи с сервером.

ПРИМЕЧАНИЯ:

✓ Для корректного управления устройством необходимо, чтобы на устройстве было выставлено корректное время и был задан часовой пояс;

✓ На группу устройств или группу пользователей может быть одновременно назначено несколько офлайн-сценариев.

Доступность событий и реакций офлайн-сценариев для разных версий ОС приведена в таблице (Таблица 51).

Таблица 51

Событие	Реакция					
	Заблокировать/ разблокировать устройство	Очистка устройства	Задать одноразовый пароль пользователя/ администратора	Задать период отправки событий безопасности	Разрешить/ запретить использование камеры	Разрешить/ запретить использование микрофона
Смена SIM-карты	– ОС Аврора; – ОС Android 7 и выше	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора	ОС Аврора	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора
Отсутствие соединения с Платформой Управления	– ОС Аврора; – ОС Android 7 и выше	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора	ОС Аврора	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора
Вне зоны действия WLAN	ОС Аврора	ОС Аврора	ОС Аврора	ОС Аврора	ОС Аврора	ОС Аврора
Нахождение в зоне WLAN	ОС Аврора	ОС Аврора	ОС Аврора	ОС Аврора	ОС Аврора	ОС Аврора
Нахождение на территории, определяемой NFC-метками	– ОС Аврора; – ОС Android 7 и выше	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора	ОС Аврора	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора
Нахождение вне территорий, определяемых координатами	– ОС Аврора; – ОС Android 7 и выше	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора	ОС Аврора	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора
Нахождение на территориях, определяемых координатами	– ОС Аврора; – ОС Android 7 и выше	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора	ОС Аврора	– ОС Аврора; – ОС Android 7 и выше	ОС Аврора
Обнаружены root-права	ОС Android 7 и выше	ОС Android 7 и выше	-	-	ОС Android 7 и выше	-

Для перехода в подраздел необходимо в верхней панели выбрать раздел «Управление», подраздел «Сценарии». В результате отобразится список сценариев.

В рабочей области подраздела «Сценарии» информация отображается в столбцах, приведенных в таблице (Таблица 52), а при их отсутствии отображается сообщение «Нет данных».

ПРИМЕЧАНИЕ. Значения столбцов могут быть отсортированы: ↑ от старых к новым, ↓ от новых к старым.

Таблица 52

Название столбца	Описание
Название	– название офлайн-сценария – представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку офлайн-сценария; – комментарий – дополнительная информация (заполняется при необходимости)
Событие	Событие офлайн-сценария (доступные значения описаны в таблице (Таблица 53). В поле содержится подсказка, доступная для просмотра при наведении курсора на значок ⓘ
Реакция	Действие, которое должно произойти с группой в результате назначения данного офлайн-сценария (доступные значения описаны в таблице (Таблица 53)
Обновлено	Дата и время последнего обновления офлайн-сценария

2.5.1. Добавление офлайн-сценария

ПРИМЕЧАНИЕ. Доступно добавление офлайн-сценариев со следующими параметрами:

– с разными событиями;

– с одним событием, но с разными реакциями (правилами);

– с одним событием («Нахождение в зоне WLAN» или «Вне зоны действия WLAN») и с одной реакцией, но с разными MAC-адресами (BSSID) точки доступа WLAN;

– с одним событием «Нахождение на территории, определяемой NFC-метками», при этом:

- одновременно один и тот же ID метки не может быть на входе и выходе;
- два офлайн-сценария с одинаковым ID метки входа или выхода не могут иметь одинаковую реакцию.

Для создания офлайн-сценария необходимо выполнить следующие действия:

– перейти в подраздел «Сценарии» раздела «Управление»;

– нажать кнопку «Добавить»;

– в открывшемся окне заполнить поля, приведенные в таблице (Таблица 53);

– подтвердить либо отменить действия.

При успешном создании офлайн-сценария отобразится соответствующее сообщение.

Таблица 53

Параметр	Значения
Название	Название офлайн-сценария. Поле обязательно для заполнения
Комментарий	Дополнительная информация к офлайн-сценарию. Поле необязательно для заполнения
Событие	Выбор значения из раскрывающегося списка. Событие, на которое среагирует устройство: – Смена SIM-карты – при смене SIM-карты на устройстве сработает реакция, выбранная из раскрывающегося списка «Реакция». Подробнее о проверке замены SIM-карты приведено в приложениии (Приложение 7); – Отсутствие соединения с Платформой Управления – при отсутствии соединения с сервером Аврора Центр на устройстве сработает реакция, выбранная из раскрывающегося списка «Реакция». Дополнительно необходимо указать временной интервал (формат: [ДД] : [ЧЧ] : [ММ]) отсутствия соединения с сервером, после наступления которого устройство среагирует. Отсчет таймера для указанного временного интервала начинает действовать как только устройство получило первую ошибку при попытке синхронизации с сервером ППО. ВНИМАНИЕ! Для устройств с ОС Android необходимо задавать интервал, кратный 1 часу. Если задать другой интервал, то при отсутсвии соединения с ПУ офлайн-сценарий сработает только при наступлении следуюшего часа. Пример: Задана реакция «Запретить использование камеры» с помощью офлайн-сценария с отуствием соединения с ПУ в 1 час 10 минут. Если в течение 1 часа и 10 минут связи устройства с ОС Android с ПУ не было, то использование камеры на устройстве станет недоступно только, когда пройдет 2 часа и соединение с ПУ так и будет отсутсовтвать; – Вне зоны действия WLAN – если устройство не обнаружит определенную сеть WLAN в доступных для подключения, то сработает реакция, выбранная из раскрывающегося списка «Реакция». ПРИМЕЧАНИЕ. При выборе события «Вне зоны действия WLAN» отображается дополнительное поле, в котором необходимо указать BSSID (Basic Service Set Identification или идентификатор) точки доступа WLAN;

	– **Нахождение в зоне WLAN** – если устройство обнаружит определенную сеть WLAN в доступных для подключения, то сработает реакция, выбранная из раскрывающегося списка «Реакция». **ПРИМЕЧАНИЕ.** При выборе события «Нахождение в зоне WLAN» отображается дополнительное поле, в котором необходимо указать BSSID (Basic Service Set Identification или идентификатор) точки доступа WLAN; – **Нахождение на территории, определяемой NFC-метками** (применение офлайн-сценария на состояние устройства определяется по NFC-метке) – при сканировании метки входа сработает реакция, выбранная из раскрывающегося списка «Реакция», и, наоборот, при сканировании метки выхода применение офлайн-сценария прекратится. **ВНИМАНИЕ!** После сканирования NFC-метки выхода на устройстве применяется правило из политики, похожее на реакцию офлайн-сценария. Если такое правило отсутствует в политике, то состояние устройства не изменится. Необходимо назначить на устройство политику с похожим правилом, чтобы состояние устройства изменялось после сканирования метки выхода. **Пример:** Задана реакция «Запретить использование камеры» с помощью офлайн-сценария с NFC-метками. При сканировании метки входа использование камеры будет недоступным. После сканирования метки выхода офлайн-сценарий прекратит действие на состояние устройства. При этом, если на устройство не была назначена политика с разрешением камеры, то запрет камеры на устройстве будет сохранен. Для разблокировки камеры необходимо назначить на устройство политику или отправить команду оперативного управления с разблокировкой камеры. При выборе события «Нахождение на территории, определяемой NFC-метками» дополнительно отображаются поля «ID меток входа» и «ID меток выхода», где необходимо указать уникальные идентификаторы меток входа и выхода, состоящие из 4, 7 или 8 пар символов, разделенных двоеточием. Доступно добавление нескольких идентификаторов меток. **ВНИМАНИЕ!** NFC-метка сканируется на устройствах: – на базе ОС Аврора при заблокированном/разблокированном телефоне и при включенном экране;

Параметр	Значения
	– на базе ОС Android при разблокированном устройстве и при включенном экране. На некоторых устройствах при включенной камере не срабатывает сканирование NFC; – **Нахождение вне территорий, определяемых координатами** – если местоположение устройства окажется вне заданной территории, то на состояние устройства начнет действовать офлайн-сценарий с реакцией, выбранной из раскрывающегося списка «Реакция». Дополнительно в раскрывающемся списке «Территория» необходимо выбрать требуемую территорию; – **Нахождение на территориях, определяемых координатами** – если местоположение устройства окажется внутри заданной территории, то на состояние устройства начнет действовать офлайн-сценарий с реакцией, выбранной из раскрывающегося списка «Реакция». Дополнительно в раскрывающемся списке «Территория» необходимо выбрать требуемую территорию. **ПРИМЕЧАНИЯ:** ✓ Если необходимой территории нет в списке, то требуется добавить ее (п. 4.1.6); ✓ Точность определения координат устройства зависит от многих факторов, а именно: тип устройства, состояние сети, скорость, нахождение в здании или около высоких объектов, покрытие спутников, аппаратные и программные характеристики, уровень шума/помех и т.д; ✓ Приложение «Аврора Центр» получает координаты устройства из ОС каждые 10 минут (ОС Аврора и ОС Android) или каждые 50 метров (ОС Android). При необходимости доступно изменение частоты обновления координат в приложении «Аврора Центр» с помощью правила политики «Конфигурация/Обновление координат в клиенте Аврора Центр» (пп. 2.4.1.29)
Обнаружены root-права	Если при проверке (осуществляется 1 раз в 1 час или при запуске приложения «Аврора Центр») обнаружены root-права на устройстве, то применится совместимая выбранная реакция. Подробная информация приведена в приложении (Приложение 5)

Параметр	Значения
Реакция	Выбор значения из раскрывающегося списка: – **Заблокировать устройство** – устройство будет заблокировано; – **Разблокировать устройство** – устройство будет разблокировано; – **Очистка устройства** – устройство будет очищено (до заводских настроек); – **Задать одноразовый пароль пользователя** – необходимо ввести пароль (от 7 до 12 символов), который пользователь сможет использовать для разблокировки устройства. Пароль должен соответствовать требованиям парольной политики; – **Задать одноразовый пароль администратора** – необходимо ввести пароль (от 7 до 12 символов), который администратор сможет использовать для разблокировки устройства. Пароль должен соответствовать требованиям парольной политики; – **Задать период отправки событий безопасности** – необходимо задать расписание отправки сообщений о событиях безопасности (security.d journaling daemon), произошедших на устройстве, в формате: [ДД] : [ЧЧ] : [ММ]; – **Разрешить использование камеры** – использование камеры на устройствах будет разрешено; – **Запретить использование камеры** – использование камеры на устройствах будет запрещено; – **Разрешить использование микрофона** – использование микрофона на устройствах будет разрешено; – **Запретить использование микрофона** – микрофон будет недоступен для записи звука во всех приложениях и внешних устройств, которые управляют им (наушники, гарнитуры и т.п.), но будет доступен для исходящих и входящих вызовов

2.5.2. Назначение офлайн-сценария на группы устройств или группы пользователей

Назначить офлайн-сценарии на группы устройств или пользователей возможно следующими способами:

– через карточку офлайн-сценария (пп. 2.5.2.1);
– с помощью списка быстрых действий (пп. 2.5.2.2);
– через карточку группы устройств (пп. 2.5.2.3);
– через карточку группы пользователей (пп. 2.5.2.4).

2.5.2.1. Назначение офлайн-сценария на группы устройств или группы пользователей через карточку офлайн-сценария

Для назначения офлайн-сценария на группы устройств или пользователей через карточку офлайн-сценария необходимо выполнить следующие действия:

– перейти в подраздел «Сценарии» раздела «Управление»;
– перейти в карточку офлайн-сценария (п. 2.1.6);
– для добавления группы устройств или пользователей в раскрывающемся списке выбрать «Добавить группы устройств» или «Добавить группы пользователей»;
– в открывшемся окне выбрать группу из списка, при необходимости воспользовавшись фильтром по названию группы (Рисунок 105 [1]);
– добавленная группа отобразится в списке. При необходимости возможно удалить добавленную группу из списка, нажав значок (Рисунок 105 [2]). Также доступна возможность отвязки офлайн-сценария от группы, описание которой приведено в п. 2.5.3;
– далее, для назначения офлайн-сценария на добавленные группы, нажать кнопку «Назначить на группы» либо отменить все последние действия нажатием кнопки «Отмена» (Рисунок 105 [3]).

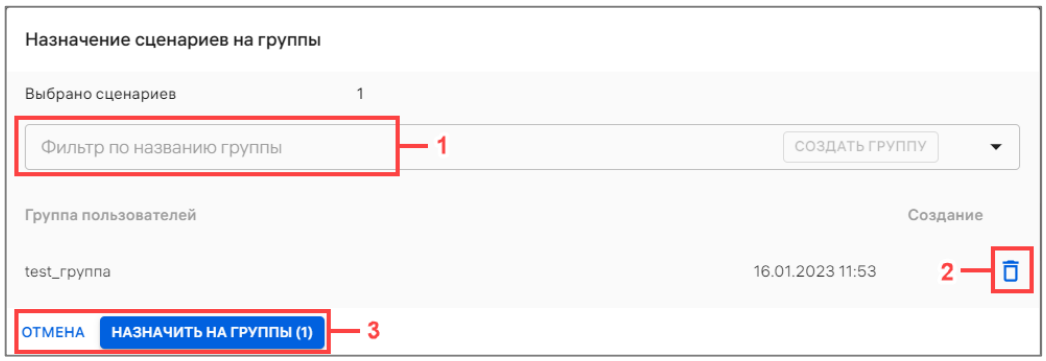


Рисунок 105

В результате применения офлайн-сценария отобразится соответствующее сообщение.

2.5.2.2. Назначение офлайн-сценария на группы устройств/группы пользователей с помощью списка быстрых действий

Для назначения офлайн-сценария на группы устройств/пользователей с помощью списка быстрых действий необходимо выполнить следующие действия:

– перейти в подраздел «Сценарии» раздела «Управление»;

– выбрать офлайн-сценарии, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать:

- значок для назначения офлайн-сценария на группу пользователей;
- значок для назначения офлайн-сценария на группу устройств;

– в открывшемся окне выполнить действия, приведенные в пп. 2.5.2.1.

2.5.2.3. Назначение офлайн-сценария на группы устройств через карточку группы

Для назначения офлайн-сценария на группу устройств через карточку группы необходимо выполнить следующие действия:

– перейти в подраздел «Устройства» раздела «Управление»;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название группы устройств для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке перейти во вкладку «Сценарии»;

– нажать кнопку «Назначить сценарии»;

– в отобразившемся окне выбрать офлайн-сценарий из раскрывающегося списка или воспользоваться фильтром (Рисунок 106 [1]). Далее, при необходимости, возможно добавить дополнительный сценарий, выбрав его из раскрывающегося списка либо воспользовавшись поиском по фильтру. Также возможно удалить из списка выбранные сценарии, нажав значок «Убрать из списка» (Рисунок 106 [3]);

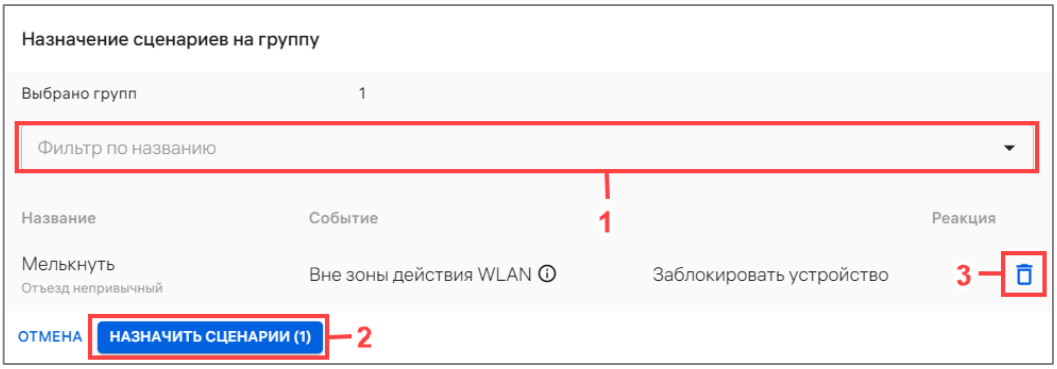


Рисунок 106

– нажать кнопку «Назначить сценарии» (см. Рисунок 106 [2]) либо кнопку «Отмена» для отмены действий.

В результате офлайн-сценарий будет назначен на группу устройств.

2.5.2.4. Назначение офлайн-сценария группы пользователей через карточку группы

Для назначения офлайн-сценария на группу пользователей через карточку группы необходимо выполнить следующие действия:

– перейти в подраздел «Пользователи» раздела «Управление»;

– выбрать в области фильтров «Поиск по группам»;

– нажать на название группы пользователей для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке перейти во вкладку «Сценарии»;

– нажать кнопку «Назначить сценарии»;

– в отобразившемся окне выполнить действия, описанные в пп. 2.5.2.3.

В результате офлайн-сценарий будет назначен на группу пользователей.

2.5.3. Отвязка офлайн-сценарий от группы устройств/группы пользователей

Отвязать офлайн-сценарии от группы устройств или группы пользователей возможно следующими способами:

– через карточку офлайн-сценария (пп. 2.5.3.1);

– через карточку группы устройств/группы пользователей (пп. 2.5.3.2).

2.5.3.1. Отвязка офлайн-сценария от группы устройств/группы пользователей через карточку офлайн-сценария

Для отвязки офлайн-сценарий от группы устройств/группы пользователей необходимо выполнить следующие действия:

– перейти в подраздел «Сценарии» раздела «Управление»;

– перейти в карточку офлайн-сценария;

– выбрать группу, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок  «Отвязать сценарий от группы»;

– в отобразившемся окне подтвердить либо отменить действие.

В результате отвязки офлайн-сценарий будет удален со всех устройств группы.

ВНИМАНИЕ! Если результат данного офлайн-сценария уже применен на устройствах и при этом на устройствах не назначена политика с иным действием, после отвязки офлайн-сценария его результат не будет отменен.

2.5.3.2. Отвязка офлайн-сценария от группы устройств/группы пользователей через карточку группы

Для отвязки офлайн-сценария от группы устройств/группы пользователей через карточку группы необходимо выполнить следующие действия:

– перейти:

- в подраздел «Устройства» раздела «Управление» – для отвязки группы устройств;
- в подраздел «Пользователи» раздела «Управление» – для отвязки группы пользователей;

– в области фильтров выбрать «Поиск по группам»;

– нажать на название необходимой группы для перехода в карточку (при необходимости воспользоваться фильтром (подраздел 1.4);

– в открывшейся карточке группы перейти во вкладку «Сценарии»;

– выбрать офлайн-сценарий, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения следует нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Отвязать сценарии от группы»;

– в отобразившемся окне подтвердить либо отменить действия.

В результате успешной отвязки офлайн-сценарий будет удален со всех устройств группы пользователей/устройств.

ВНИМАНИЕ! Если действие данного офлайн-сценария уже применено на устройствах и при этом на них не назначена политика с противоположным действием, после отвязки офлайн-сценария его действие не будет отменено.

2.5.4. Удаление офлайн-сценария

Удалить офлайн-сценарий возможно одним из следующих способов:

1) С помощь списка быстрых действий. Для это необходимо:

– перейти в подраздел «Сценарии» раздела «Управление»;

– выбрать офлайн-сценарии, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок ;

– в отобразившемся окне подтвердить либо отменить действия;

2) Через карточку офлайн-сценария. Для это необходимо:

– перейти в подраздел «Сценарии» раздела «Управление»;

– перейти в карточку офлайн-сценария (п. 2.1.6) во вкладку «Событие и реакция»/«Группы»;

– нажать на значок и выбрать Удалить;

– в отобразившемся окне подтвердить либо отменить действия.

В результате успешного удаления офлайн-сценария из системы отобразится соответствующее сообщение и будут удалены все связи офлайн-сценария с группами, а также он будет удален со всех устройств, на которые был назначен.

ВНИМАНИЕ! Если результат данного офлайн-сценария уже применен на устройствах и при этом на них не назначена политика с противоположным действием, после отвязки офлайн-сценария его результат не будет отменен.

2.6. Подраздел «Файлы»

Подраздел «Файлы» Консоли администратора ПУ предназначен для работы со списком файлов (скриптов) и/или папок с файлами, которые возможно добавить на устройства.

Для доставки на устройство файлов (скриптов) и/или папок с файлами, загруженных в ПУ из git-репозитория, необходимо добавить их в ПУ.

ПРИМЕЧАНИЕ. Если в настройках администрирования ПУ было задано количество администраторов для согласования файлов/папок (подробнее в пп. 4.1.4.2), то, чтобы версия файла была доступна для распространения через политику, она должна быть согласована заданным количеством администраторов. При этом администратор, который загрузил версию файла в ПУ, не может ее согласовать.

В Консоли администратора ПУ предусмотрена возможность добавления файлов (скриптов) и/или папок с файлами одним из следующих способов:

– добавление файла с локального компьютера (пп. 2.6.1.1).

ПРИМЕЧАНИЕ. Папку нельзя загрузить в ПУ с локального компьютера;

– добавление файла из git-репозитория (пп. 2.6.1.1.2);

– добавление папки для доставки на устройство из git-репозитория (пп. 2.6.2.1).

ПРИМЕЧАНИЕ. Возможно загрузить несколько версий одного файла/папки и при необходимости скачать, согласовать и удалить нужную версию, либо удалить все версии файла/папки.

ВНИМАНИЕ. Синхронизация с git-репозиторием для получения папок/файлов не будет работать, если в качестве хранилища в ППО выбрано S3.

Для перехода в подраздел необходимо:

– выбрать в верхней панели подраздел «Файлы» раздела «Управление»;

– в области фильтров выбрать:

- раздел «Файлы» для отображения списка файлов (скриптов), информация о которых отображается в столбцах, приведенных в таблице (Таблица 54), а при отсутствии добавленных файлов отображается сообщение «Нет данных»;

Таблица 54

Параметр	Описание
Название	– название файла (представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке файла); – комментарий – дополнительная информация (заполняется при необходимости)
Источник	Источник, откуда был загружен рабочий файл
Папка	Папка, добавленная из git-репозитория
Согласовано версий	Количество согласованных версий файла

Параметр	Описание
Обновлен	Дата обновления рабочего файла
Создан	Дата создания рабочего файла

• раздел «Папки из git-репозиториев» для отображения списка папок, информация о которых отображается в столбцах, приведенных в таблице (Таблица 55), а при отсутствии добавленных папок отображается сообщение «Нет данных».

Таблица 55

Параметр	Описание
Название	– название папки (представляет собой активную ссылку, при нажатии на которую осуществляется переход к карточке папки); – комментарий – дополнительная информация (заполняется при необходимости)
Источник	Источник, откуда была загружена рабочая папка
Согласовано версий	Количество согласованных версий папки
Обновлен	Дата обновления рабочей папки
Создан	Дата создания рабочей папки

2.6.1. Работа с файлами (скриптами)

2.6.1.1. Добавление файла (скрипта)

2.6.1.1.1. Добавление файла (скрипта) с компьютера

Для добавления файла (скрипта) с компьютера на устройство необходимо добавить его в ПУ, выполнив следующие действия:

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить файл с компьютера» (Рисунок 107);

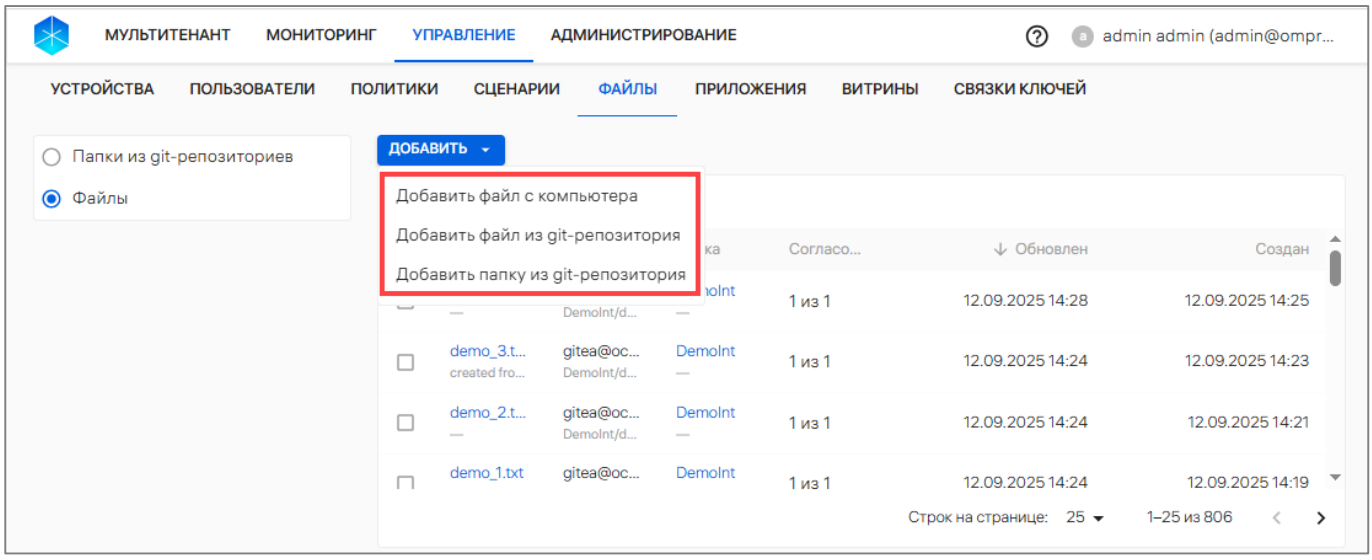


Рисунок 107

– в открывшемся окне добавить комментарий (при необходимости) и загрузить файл одним из способов:

- переместить файл в область загрузки;
- нажать кнопку «Загрузить файл» с последующим выбором файла для загрузки.

ПРИМЕЧАНИЕ. Максимальный размер загружаемого файла – 2048 МБ. Ограничений на формат файла нет;

– подтвердить либо отменить действия.

При успешном добавлении файл (скрипт) будет добавлен в ПУ и отобразится в списке файлов. Эта версия файла будет считаться первой. При необходимости возможно добавить другие версии файла (п. 2.6.1.1.2).

2.6.1.1.2. Добавление файла (скрипта) из git-репозитория

Для добавления файла (скрипта) из git-репозитория на устройство необходимо добавить его в ПУ, выполнив следующие действия:

– нажать кнопку «Добавить»;

– в раскрывающемся списке выбрать пункт «Добавить файл из git-репозитория» (см. Рисунок 107);

– в открывшемся окне заполнить поля приведенные в таблице (Таблица 56).

Таблица 56

Поле	Описание
Git-репозиторий	В раскрывающемся списке выбрать необходимый git-репозиторий. Если нужного git-репозитория нет в списке, добавить в ПУ интеграцию с ним (пп. 4.1.5.6)
Относительный путь к файлу	Ввести относительный путь к файлу в git-репозитории
Комментарий	Дополнительная информация (заполняется при необходимости)

При успешном добавлении, файл (скрипт) будет добавлен в ПУ и отобразится в списке файлов. Эта версия файла будет считаться первой. При необходимости возможно добавить другие версии файла (п. 2.6.1.1.2).

ВНИМАНИЕ! Файл не доступен для добавления в ПУ, если файл является частью уже ранее добавленной папки одного и того же git-репозитория, ветки и относительного пути.

2.6.1.2. Добавление версии файла (скрипта)

ПРИМЕЧАНИЕ. Если файл был добавлен из git-репозитория и в настройках интеграции с git-репозиторием была задана частота синхронизации, то ППО автоматически загрузит новую версию файла (при ее наличии) при следующей синхронизации. Если частота синхронизации не была задана, то для добавления новой версии файла необходимо выполнить действия, приведенные ниже.

Для добавления версии файла (скрипта) необходимо:

– перейти в подраздел «Файлы» раздела «Управление»;
– в области фильтров выбрать раздел «Файлы»;
– нажать на название необходимого файла для перехода в карточку (п. 2.1.7);
– нажать кнопку «Добавить версию;
– в отобразившемся окне:

• если файл был загружен с локального компьютера, необходимо перетащить файл в область загрузки или нажать «Загрузить файл» и выбрать необходимый файл (размер файла не должен превышать 2048 МБ);

• если файл из git-репозитория, то ПУ автоматически найдет новую версию файла;

• при необходимости в поле «Комментарий» ввести дополнительную информацию к версии файла;

– подтвердить либо отменить действия.

При успешном добавлении файла его версия будет добавлена в ПУ.

ПРИМЕЧАНИЕ. Если файл является частью добавленной папки из git-репозитория, то для такого файла запрещено добавлять новую версию. Чтобы обновить версию файла, принадлежащего папке из git-репозитория, необходимо добавить версию папки из git-репозитория (пп. 2.6.2.2).

2.6.1.3. Скачивание версии файла (скрипта)

Для скачивания версии файла (скрипта) из ПУ необходимо:

– перейти в подраздел «Файлы» раздела «Управление»;
– в области фильтров выбрать раздел «Файлы»;
– нажать на название необходимого файла для перехода в карточку (п. 2.1.7).

ПРИМЕЧАНИЕ. Также возможно перейти в карточку файла через папку из git-репозитория (если файл является частью добавленной папки из git-репозитория). Для этого необходимо перейти в карточку версии папки и нажать на название нужного файла;

– развернуть окно с информацией о версии файла и нажать на кнопку «Скачать файл версии».

В результате успешного скачивания файл будет скачан на ЭВМ.

2.6.1.4. Согласование версии файла (скрипта)

Для согласования версии файла (скрипта) из ПУ необходимо:

– перейти в подраздел «Файлы» раздела «Управление»;
– в области фильтров выбрать раздел «Файлы»;
– нажать на название необходимого файла для перехода в карточку (п. 2.1.7);

ПРИМЕЧАНИЕ. Также возможно перейти в карточку файла через папку из git-репозитория (если файл является частью добавленной папки из git-репозитория). Для этого необходимо перейти в карточку версии папки и нажать на название нужного файла.

– развернуть окно с информацией о версии файла и нажать на кнопку «Согласовать» (Рисунок 108).

В результате версия файла будет согласована.

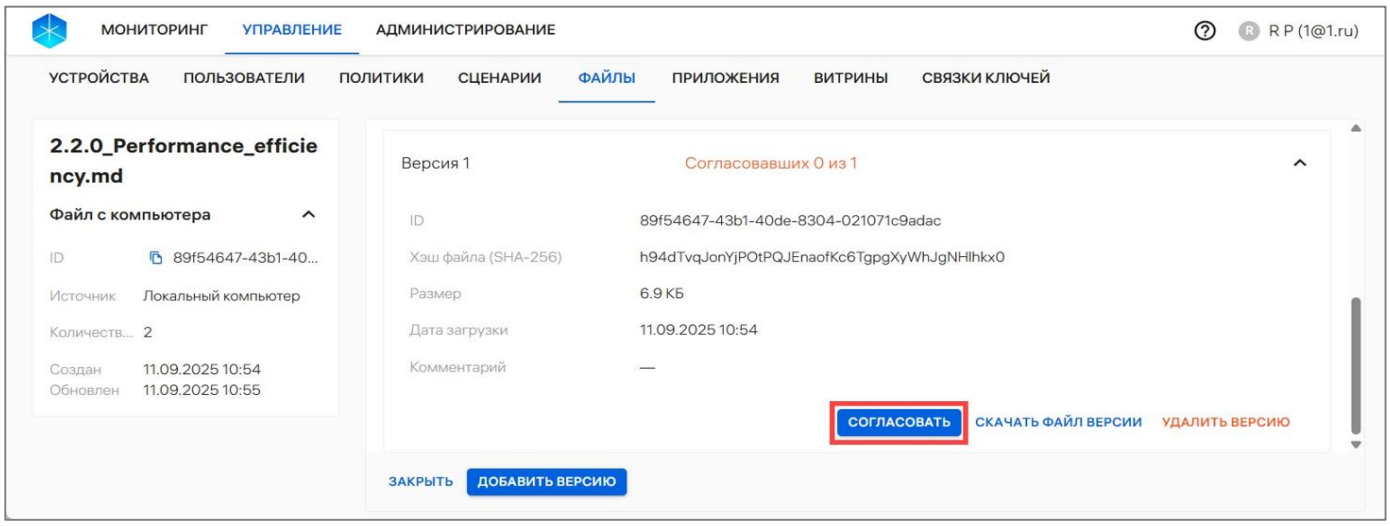


Рисунок 108

2.6.1.5. Удаление версии файла (скрипта)

ВНИМАНИЕ! Удалить версию файла из ПУ возможно, если она не добавлена ни в одну политику и файл не является частью добавленной папки из git-репозитория.

Для удаления версии файла (скрипта) из ПУ необходимо:

– перейти в подраздел «Файлы» раздела «Управление»;

– в области фильтров выбрать раздел «Файлы»;

– нажать на название необходимого файла для перехода в карточку (п. 2.1.7);

ПРИМЕЧАНИЕ. Также возможно перейти в карточку файла через папку из git-репозитория (если файл является частью добавленной папки из git-репозитория). Для этого необходимо перейти в карточку версии папки и нажать на название нужного файла.

– развернуть окно с информацией о версии файла и нажать на кнопку «Удалить версию»;

– в отобразившемся окне подтвердить либо отменить действия.

В результате успешного удаления версия файла будет удалена из ПУ.

ПРИМЕЧАНИЕ. Если файл является частью добавленной папки из git-репозитория, то для такого файла запрещено удалять версии. Необходимо удалить конкретную версию папки или папку со всеми ее версиями (пп. 2.6.2.4).

2.6.1.6. Удаление файла (скрипта) со всеми его версиями

ВНИМАНИЕ! Удалить файл (скрипт) из ПУ возможно, если ни одна его версия не добавлена ни в одну политику в ПУ и файл не является частью добавленной папки из git-репозитория.

Для удаления файла (скрипта) со всеми его версиями необходимо выполнить следующие действия:

– выбрать файл, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение».

ВНИМАНИЕ! Доступно удаление только одного файла за раз;

– в списке быстрых действий выбрать значок «Удалить файл»;

– в отобразившемся окне подтвердить либо отменить действия.

ПРИМЕЧАНИЕ. Если файл применен в политике «Контент/Доставка на устройство», отобразится предупреждающее сообщение о том, что удалить файл невозможно. Для удаления файла необходимо исключить файл из правила политики и выполнить шаги, указанные выше.

В результате файл будет успешно удален.

2.6.2. Работа с папками из git-репозитория

2.6.2.1. Добавление папки для доставки на устройство из git-репозитория

Для добавления папки из git-репозитория на устройство необходимо:

– нажать кнопку «Добавить» и в раскрывающемся списке выбрать пункт «Добавить папку из git-репозитория» (см. Рисунок 107);

– в открывшемся окне заполнить поля, приведенные в таблице (Таблица 57).

Таблица 57

Поле	Описание
Git-репозиторий	В раскрывающемся списке выбрать необходимый git-репозиторий. Если нужного git-репозитория нет в списке, добавить в ПУ интеграцию с ним (пп. 4.1.5.6)
Относительный путь к папке	Ввести путь к папке относительно git-репозитория
Комментарий	Дополнительная информация (заполняется при необходимости)

ВНИМАНИЕ! Если ранее был добавлен файл из такого же git-репозитория, такой же ветки и с таким же относительным путем, что и добавляемая папка из git-репозитория, то в результате добавления этой папки из git-репозитория ППО автоматически привяжет ранее добавленный файл из git-репозитория к добавленной папке из git-репозитория.

В результате успешного добавления папка будет добавлена в ПУ. Эта версия папки будет считаться первой. При необходимости возможно добавить другие версии папки (пп. 2.6.2.2).

2.6.2.2. Добавление версии папки из git-репозитория

ПРИМЕЧАНИЕ. Если папка была добавлена из git-репозитория и в настройках интеграции с git-репозиторием была задана частота синхронизации, то Аврора Центр автоматически загрузит новую версию папки (при ее наличии) при следующей синхронизации. Если частота синхронизации не была задана, то для добавления новой версии папки необходимо выполнить действия, приведенные ниже.

Для добавления версии папки необходимо:

– перейти в подраздел «Файлы» раздела «Управление»;
– в области фильтров выбрать раздел «Папки из git-репозиториев»;
– нажать на название необходимой папки для перехода в карточку;
– нажать кнопку «Добавить версию»;
– в отобразившемся окне:
  • если папка была загружена из git-репозитория, то ПУ автоматически найдет новую версию папки;
  • при необходимости в поле «Комментарий» ввести дополнительную информацию к версии файла;
– подтвердить либо отменить действия.

При успешном добавлении версия папки будет добавлена в ПУ.

2.6.2.3. Согласование версии папки из git-репозитория

Для согласования версии папки, загруженной другим администратором необходимо:

– перейти в подраздел «Файлы» раздела «Управление»;
– в области фильтров выбрать раздел «Папки из git-репозиториев»;
– нажать на название необходимой папки для перехода в карточку;
– нажать на кнопку «Согласовать версию папки»;
– подтвердить либо отменить действия.

В результате успешного согласования версия папки и файлы, входящие в папку, будут согласованы. Если ее согласовало количество администраторов, заданное в настройках администрирования ПУ, то версия папки и ее файлы станут доступными для доставки на устройство с помощью политики.

ПРИМЕЧАНИЯ:

✓ Версия папки считается согласованной, когда внутри версии согласованы все файлы;

✓ Для версии папки, добавленной с помощью автосинхронизации git-репозитория, необходимо согласование дополнительного администратора, помимо тех, которые указаны в настройках администрирования ПУ.

2.6.2.4. Удаление папки и версии папки, загруженных из git-репозитория

При необходимости возможно удалить версию папки и папку со всеми ее версиями из ПУ при условии, что версия папки и файлы из версии папки не используются в созданных политиках.

При удалении папки и версии папки:

– папка остается на устройстве;

– содержимое папки, загруженное на устройство вместе с самой папкой с помощью политики, удаляется;

– файлы, добавленные пользователем самостоятельно в папку на устройстве, остаются.

Для удаления папки и версии папки из ПУ необходимо:

– перейти в подраздел «Файлы» раздела «Управление»;

– в области фильтров выбрать раздел «Папки из git-репозиториев»;

– при удалении папки необходимо:

- выбрать нужную папку, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;
- в списке быстрых действий выбрать значок «Удалить папку».

ВНИМАНИЕ! Доступно удаление только одной папки за раз;

- в отобразившемся окне подтвердить либо отменить действия;
- при успешном удалении папка и входящие версии (вместе с их файлами) будут удалены из ПУ.

– при удалении версии папки необходимо:

- нажать на название необходимой папки для перехода в карточку папки;
- выбрать нужную версию папку, установив галочку в чекбоксе для доступа к списку быстрых действий. При необходимости для сброса выделения необходимо нажать кнопку «Сбросить выделение»;
- в списке быстрых действий выбрать значок «Удалить версию папку».

ВНИМАНИЕ! Доступно удаление только одной версии папки за раз;

- в отобразившемся окне подтвердить либо отменить действия;
- при успешном удалении версия папки и входящие в нее файлы будут удалены из ПУ.

2.6.3. Доставка файла и выполнение скрипта на устройстве с помощью ПУ

С помощью ПУ возможно доставлять файлы (в том числе и скрипты) и папки, загруженные в Аврора Центр из git-репозитория, на активированное устройство, функционирующее под управлением ОС Android и ОС семейства Linux, а также выполнять доставленные скрипты.

Для доставки файла и выполнения скрипта необходимо:

– добавить файл (скрипт) в ПУ (пп. 2.6.1.1);

– добавить папку из git-репозитория в ПУ (пп. 2.6.2.1);

– создать политику «Контент/Доставка на устройство» (пп. 2.4.1.46) и «Скрипты/Выполнение на устройстве» (пп. 2.4.1.52) или отредактировать существующую политику, добавив в нее новое правило по доставке файлов/папок или выполнению скриптов;

– назначить политику на группу, в которую входит устройство.

ВНИМАНИЕ! ПУ позволяет добавлять сторонние файлы или папки в управляемую папку. При выборе исполняемого скрипта из папки в правиле «Скрипты/Выполнение на устройстве» рекомендуется писать скрипт так, чтобы он использовал в качестве зависимостей только те файлы, которые принадлежат управляемой папке, чтобы избежать ошибок.

В результате:

– файл/папка с файлами будут доставлены на устройство и доступны только для чтения;

– скрипт будет доставлен и выполнен на устройстве.

ПРИМЕЧАНИЕ. Для успешного выполнения скрипта необходимо ознакомиться с особенностями выполнения скриптов на устройстве (Приложение 3).

3. РАБОТА В РАЗДЕЛЕ «МОНИТОРИНГ» КОНСОЛИ АДМИНИСТРАТОРА ПУ В ПОДРАЗДЕЛЕ «ИНДИКАТОРЫ»

Подраздел «Индикаторы» Консоли администратора ПУ предназначен для мониторинга показателей устройств и контроля их отклонений.

Для перехода в подраздел необходимо в верхней панели выбрать подраздел «Индикаторы» раздела «Мониторинг». В результате отобразится информация о устройствах в виде диаграмм и пояснений к ним, а также фоновый процесс импорта устройств, пользователей и их групп в следующих окнах (Рисунок 109):

– «Подключение устройств»;
– «Соответствие политикам»;
– «Активация устройств»;
– «Процессы»;
– «Статус клиента АЦ».

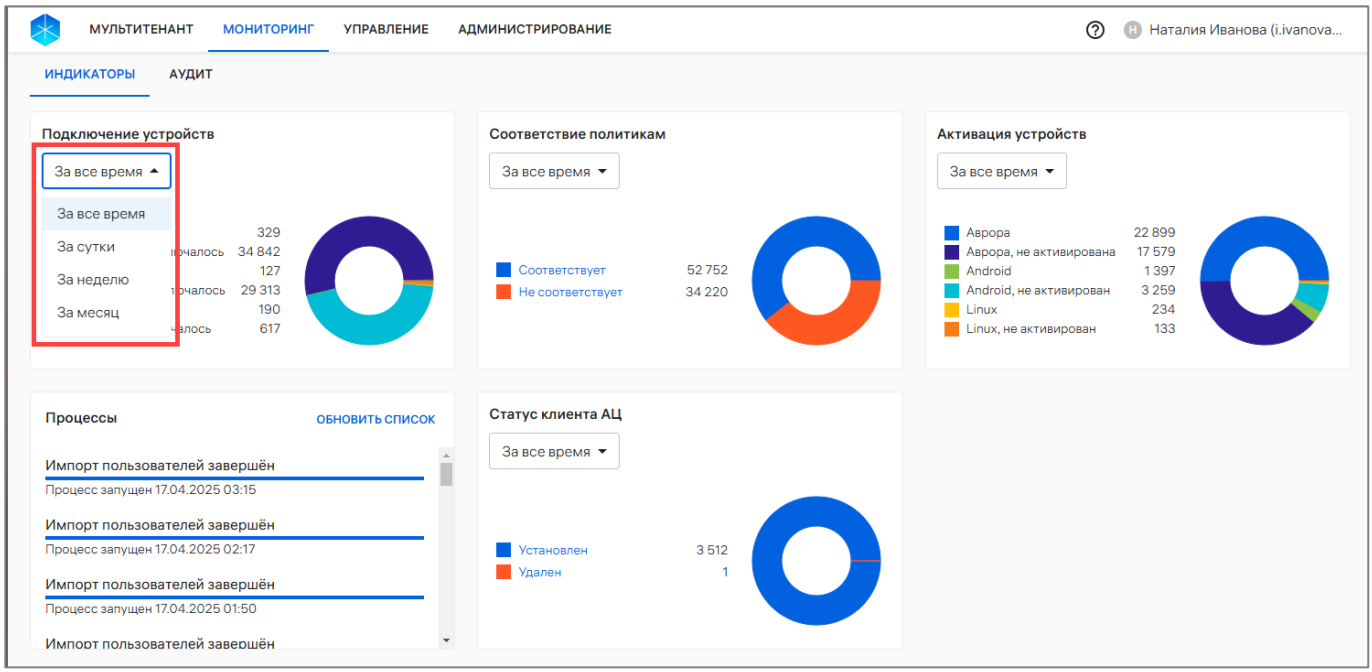


Рисунок 109

Возможно выбрать необходимый период отображения данных по устройствам из раскрывающегося списка:

– «За все время»;
– «За сутки» (установлено по умолчанию);
– «За неделю»;
– «За месяц».

Статистическая информация будет отображена за выбранный период времени.

В подразделе «Индикаторы» предусмотрена возможность просмотра подключений и активаций устройств для определенной платформы, а также соответствие политикам по следующим показателям:

– «Подключение устройств»:
  - «Аврора» - количество подключений устройств с ОС Аврора;
  - «Аврора, не подключалось» - количество устройств с ОС Аврора, которые добавлены в ППО, но еще не подключались к нему;
  - «Android» - количество подключений устройств с ОС Android;
  - «Android, не подключалось» - количество устройств с ОС Android, которые добавлены в ППО, но еще не подключались к нему;
  - «Linux» - количество подключений устройств с ОС семейства Linux;
  - «Linux, не подключалось» - количество устройств с ОС семейства Linux, которые добавлены в ППО, но еще не подключались к нему;
– «Соответствие политикам»:
  - «Соответствует» - количество устройств, соответствующих политикам. Представляет собой активную ссылку, при переходе будет отображен список устройств, отфильтрованный по статусу политик «Соответствует»;
  - «Не соответствует» - количество устройств, не соответствующих политикам. Представляет собой активную ссылку, при переходе будет отображен список устройств, отфильтрованный по статусу политик «Не соответствует».

ПРИМЕЧАНИЕ. В список устройств попадут не только активированные устройства, у которых целевое значение не совпадает с текущим, но и устройства в статусах «Зарегистрировано» и «В процессе активации», на которые назначена политика;

– «Активация устройств»:
  - «Аврора» - количество активаций устройств с ОС Аврора;
  - «Аврора, не активирована» - количество устройств с ОС Аврора, которые добавлены в ППО, но не активированы;
  - «Android» - количество активаций устройств с ОС Android;
  - «Android, не активирован» - количество устройств с ОС Android, которые добавлены в ППО, но не активированы;
  - «Linux» - количество активаций устройств с ОС семейства Linux;
  - «Linux, не активирован» - количество устройств с ОС семейства Linux, которые добавлены в ППО, но не активированы;
– «Статус клиента АЦ»:
  - «Установлен» - количество устройств, на которых было установлено приложение «Аврора Центр». Представляет собой активную ссылку, при переходе будет отображен список устройств, отфильтрованный по статусу приложения «Аврора Центр» «Установлен»;

- «Удален» - количество устройств, на которых было удалено приложение «Аврора Центр» (данная информация доступна только для устройств с ОС семейства Linux). Представляет собой активную ссылку, при переходе будет отображен список устройств, отфильтрованный по статусу приложения «Аврора Центр» «Удален».

В окне «Процессы» отображаются завершенные и текущие процессы импорта устройств, пользователей и их групп из CSV-файла. Возможны следующие статусы выполнения задач с запущенным импортом:

– завершен (импорт завершен успешно);

– в процессе (импорт/фоновый процесс выполняется);

– прервался (импорт прервался по какой-либо причине, например, если сервис недоступен).

Статус задачи не зависит от результата выполнения импорта, например, статус может быть завершен, но при этом загружен ошибочный файл.

Для просмотра состояния или результата импорта, необходимо нажать на интересующий процесс. В результате отобразится окно с информацией о состоянии импорта, если он еще выполняется, или с результатом импорта, если он завершен (даже с ошибкой) (см. Рисунок 34, Рисунок 35).

4. РАБОТА В РАЗДЕЛЕ «АДМИНИСТРИРОВАНИЕ» КОНСОЛИ АДМИНИСТРАТОРА ПУ

4.1. Подраздел «Настройки»

Подраздел «Настройки» Консоли администратора ПУ предназначен для:

– управления доверенными корневыми сертификатами на устройствах (п. 4.1.1, Рисунок 110 [1]);

– добавления и просмотра категорий пользовательских сертификатов (п. 4.1.2, Рисунок 110 [2]);

– разрешения конфликтов в заявках на активацию (пп. 4.1.3.1, Рисунок 110 [3]), добавления и удаления доверенных сетей (п. 4.1.3.2, Рисунок 110 [4]), а также настройки используемых типов идентификаторов (п. 4.1.3.3, Рисунок 110 [5]);

– управления отображением архивных устройств, настройки отображения списка устройств (пп. 4.1.4.1, Рисунок 110 [6]) и давно не подключавшихся устройств (пп. 4.1.4.2, Рисунок 110 [7]), согласования файлов (пп. 4.1.4.3, Рисунок 110 [8]),

– просмотра информации о (Рисунок 110 [9]):

- Сервере приложений (также представлена возможность включения/отключения витрин с приложением) (пп. 4.1.5.1);
- Обновлении ОС (пп. 4.1.5.2);
- Сервере LDAP (также представлена возможность добавления интеграции с сервером LDAP и настройки синхронизации данных с ППО) (пп. 4.1.5.3);
- Сервисе уведомлений (СУ) (также представлена возможность изменения настроек ПСУ) (пп. 4.1.5.4);
- Центрах сертификации (пп. 4.1.5.5);
- Git-репозитории (интеграция с удаленным git-репозиторием) (п. 4.1.5.6);

– просмотра и добавления территории на карте (п. 4.1.6, Рисунок 110 [10]);

– настройки правил политик (п. 4.1.7, Рисунок 110 [11]);

– просмотра и настройки управляемых переменных (п. 4.1.8, Рисунок 110 [12]);

– экспорта/импорта данных в формате JSON (п. 4.1.9, Рисунок 110 [13]).

Для перехода в подраздел необходимо в верхней панели перейти в раздел «Администрирование» и выбрать подраздел «Настройки».

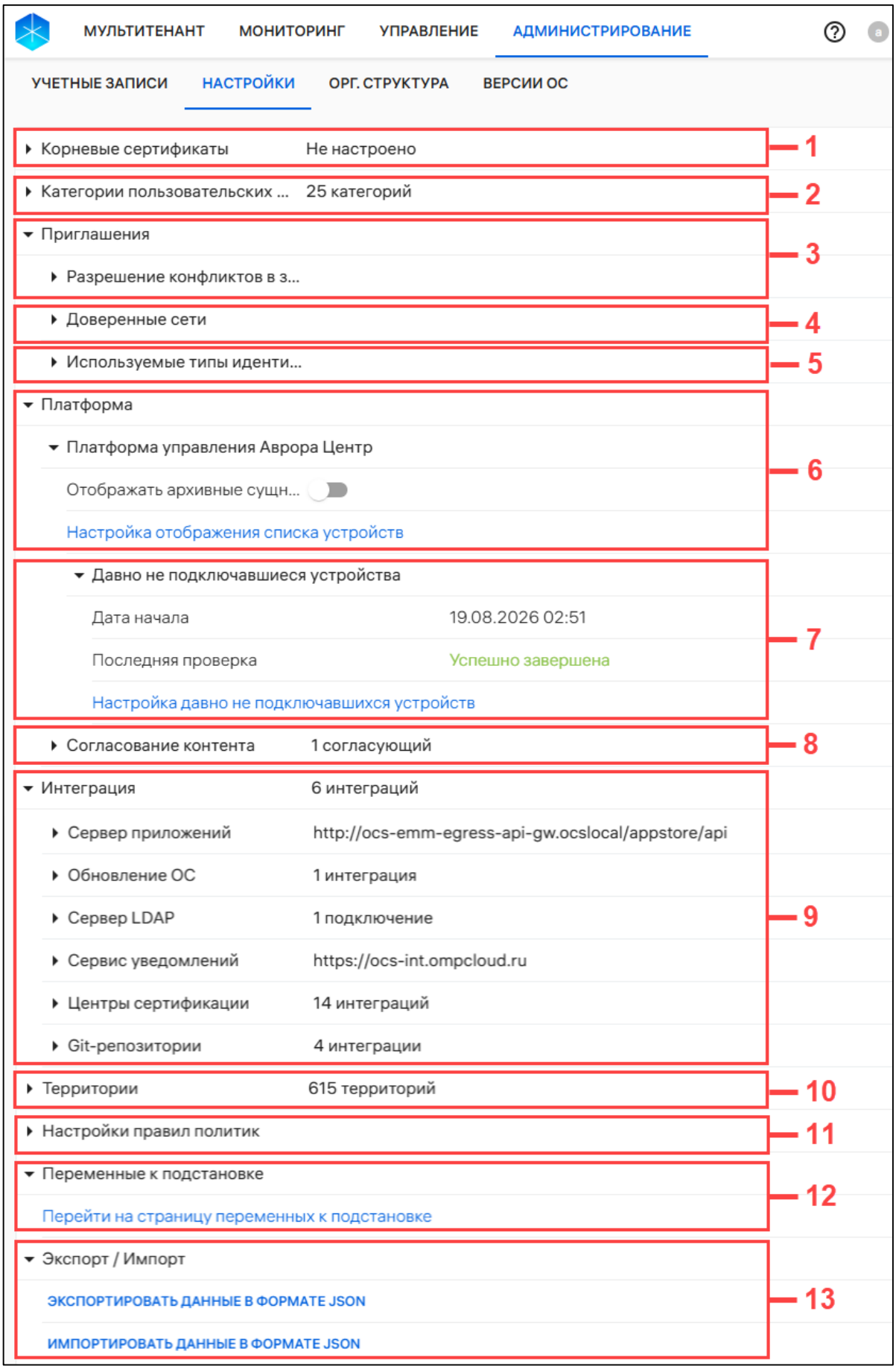

МУЛЬТИТЕНАНТ
МОНИТОРИНГ
УПРАВЛЕНИЕ
АДМИНИСТРИРОВАНИЕ
УЧЕТНЫЕ ЗАПИСИ
НАСТРОЙКИ
ОРГ. СТРУКТУРА
ВЕРСИИ ОС
Корневые сертификаты Не настроено
1
Категории пользовательских ... 25 категорий
2
Приглашения
Разрешение конфликтов в з...
3
Доверенные сети
4
Используемые типы иденти...
5
Платформа
Платформа управления Аврора Центр
Отображать архивные сущн...
Настройка отображения списка устройств
6
Давно не подключавшиеся устройства
Дата начала 19.08.2026 02:51
Последняя проверка Успешно завершена
Настройка давно не подключавшихся устройств
7
Согласование контента 1 согласующий
8
Интеграция 6 интеграций
Сервер приложений http://ocs-emm-egress-api-gw.ocslocal/appstore/api
Обновление ОС 1 интеграция
Сервер LDAP 1 подключение
Сервис уведомлений https://ocs-int.ompcloud.ru
Центры сертификации 14 интеграций
Git-репозитории 4 интеграции
9
Территории 615 территорий
10
Настройки правил политик
11
Переменные к подстановке
Перейти на страницу переменных к подстановке
12
Экспорт / Импорт
ЭКСПОРТИРОВАТЬ ДАННЫЕ В ФОРМАТЕ JSON
ИМПОРТИРОВАТЬ ДАННЫЕ В ФОРМАТЕ JSON
13

Рисунок 110

4.1.1. Доверенные корневые сертификаты

В раскрывающейся строке «Корневые сертификаты» при нажатии на значок (см. Рисунок 110 [1]) отображается список доверенных сертификатов, добавленных в ПУ.

Возможно установить или удалить на устройстве с помощью Платформы управления доверенные корневые сертификаты, которые необходимы для доступа к закрытым ресурсам компании.

Для активированных устройств доверенные сертификаты, добавленные в ПУ, будут доставлены на устройства и добавлены в ОС.

Чтобы использовать доверенные сертификаты в процессе активации, необходимо включить переключатель «Использовать в QR-коде при активации» при добавлении сертификата в ПУ (подробнее описано ниже). В этом случае цифровой отпечаток (fingerprint) сертификата будет добавлен в QR-код (JSON-файл) активации. При использовании цифрового отпечатка на устройстве приложение «Аврора Центр» будет проверять список доверенных отпечатков на наличие сертификата из цепочки, полученной с сервера в ходе запроса. В случае успешной проверки запрос будет обрабатываться далее. В противном случае запрос будет прерван.

После успешной активации приложение «Аврора Центр» отправит на сервер информацию об установленных доверенных сертификатах ОС. При отсутствии на ОС каких-либо сертификатов, которые были добавлены в ПУ, они будут доставлены и добавлены в ОС.

ПРИМЕЧАНИЕ. После добавления доверенных сертификатов в ОС их проверка при обработке запросов будет осуществляться средствами ОС.

Для просмотра информации о доверенном сертификате необходимо в раскрывающейся строке названия сертификата нажать значок , в результате чего отобразится следующая информация:

– название удостоверяющего центра;
– дата выпуска сертификата;
– срок действия сертификата;
– используется ли сертификат при активации и самостоятельной регистрации устройства.

Для добавления корневых сертификатов необходимо выполнить следующие действия:

– нажать кнопку «Добавить новый корневой сертификат»;
– в открывшемся окне в поле «Имя корневого сертификата» ввести название сертификата. Максимальная длина – 32 символа;
– перевести переключатель «Использовать в QR-коде при активации» в положение «Включено», если при помощи данного сертификата требуется пройти процесс активации (например, в закрытом контуре ППО).

ПРИМЕЧАНИЕ. Возможно добавление не более 3 сертификатов;

– нажать кнопку «Загрузить файл» для последующего выбора файла для загрузки. Допустимые форматы: `.crt`, `.cer`, `.pem`;

– подтвердить либо отменить действия.

При успешном добавлении сертификат отобразится в списке доверенных сертификатов.

При необходимости цифровой отпечаток (Fingerprint) сертификата возможно скопировать в буфер обмена нажатием значка «Копировать в буфер обмена» в строке с сертификатом.

Для удаления корневых сертификатов необходимо нажать значок «Удалить сертификат» в строке сертификатов и в открывшемся окне подтвердить либо отменить действие.

ПРИМЕЧАНИЕ. При следующем подключении устройства к Серверу приложений ПУ добавленные сертификаты будут установлены на устройстве, а удаленные сертификаты будут удалены с устройства.

4.1.2. Категории пользовательских сертификатов

Категории пользовательских сертификатов используются для выпуска разных типов сертификатов для разных подключений определенному пользователю.

ПРИМЕЧАНИЕ. Чтобы доставить на устройство сертификат созданной категории, необходимо привязать устройство к пользователю и назначить на группу, в которую входит устройство, политику с одним из правил:

– «Настройки пользователя/Сертификаты пользователя» (пп. 2.4.1.43);

– «Конфигурация WLAN/Подключения к сети WLAN» (пп. 2.4.1.20);

– «Конфигурация VPN/Подключения VPN» (пп. 2.4.1.21).

Список созданных категорий возможно посмотреть в раскрывающейся строке «Категории пользовательских сертификатов» при нажатии значка (см. Рисунок 110 [2]).

Для добавления категории пользовательских сертификатов необходимо выполнить следующие действия:

– нажать кнопку «Добавить категорию»;

– в отобразившемся окне заполнить поля, приведенные в таблице (Таблица 58);

– сохранить изменения либо отменить действия.

При успешном сохранении категория пользовательских сертификатов будет добавлена.

ВНИМАНИЕ! Удаление и редактирование категории сертификата недоступно. При необходимости доступно создать новую категорию пользовательских сертификатов.

Таблица 58

Параметр		Описание
Название категории		Ввод значения с клавиатуры. Может содержать только строчные буквы и дефис, максимальное количество символов – 50. Поле обязательно для заполнения
Центр сертификации		Выбор значения из раскрывающегося списка «Центр сертификации». При отсутствии необходимого центра сертификации в списке требуется добавить его (п. 4.1.4.2). Поле обязательно для заполнения
Название шаблона		Ввод значения с клавиатуры. Может содержать 255 символов. Поле обязательно для заполнения
Subject	key	Ввод значения с клавиатуры. Может содержать 255 символов. Поле обязательно для заполнения. Для добавления дополнительного субъекта для сертификата необходимо нажать кнопку «Добавить»
	value	Ввод значения с клавиатуры. Может содержать 255 символов. Значение шаблона {{...}} подставится автоматически из атрибутов пользователя устройства. Пример: для ключа C (`country`) значение должно состоять из 2 символов (например, RU). Для добавления дополнительного субъекта для сертификата необходимо нажать кнопку «Добавить»
Subject alt name		При необходимости доступен ввод дополнительных имен субъекта для сертификата. Каждое имя субъекта должно состоять из набора параметров – названия параметра (`key`) и его значения (`value`). Может содержать 1000 символов. Доступен выбор значений шаблона {{...}}, которые подставятся автоматически из атрибутов пользователя устройства. Пример заполнения Subject alt name: `email:{{UserEmail}},otherName:Microsoft User Principal Name;UTF8:{{UserPrincipalName}}`

4.1.3. Приглашения

4.1.3.1. Разрешение конфликтов в заявках на активацию

Возможно настроить специальные режимы и стратегии для разрешения конфликтов в заявках на активацию, которые могут появиться при пересечении идентификаторов у устройства при его активации через приглашения.

Для отображения текущего режима разрешения конфликтов, необходимо:

1) Развернуть строку «Разрешение конфликтов в заявках на активацию»;

2) Нажать на «Редактировать»;

3) Выбрать из раскрывающегося списка «Режим» одно из значений:

– «Ручное разрешение конфликтов» - выбрано по умолчанию. Все конфликты по пересечению идентификаторов в заявках на активацию будут уходить на ручное разрешение с дальнейшим согласованием (подробнее в пп. 2.2.5.3);

– «Автоматическое разрешение конфликтов» - при выборе данного значения все конфликты по пересечению идентификаторов в заявках на активацию будут автоматически разрешаться и согласовываться при помощи заданной стратегии.

ВНИМАНИЕ! Если заявка на активацию содержит несколько причин (например, пересечение идентификаторов и превышение лимита переактивации), то такая заявка не будет автоматически обработана и будет переведена в ручное разрешение конфликтов;

4) При выборе из раскрывающегося списка «Режим» значения «Автоматическое разрешение конфликтов», необходимо дополнительно выбрать в раскрывающемся списке «Стратегия разрешения конфликта» одно из значений:

– «Привязать новое устройство к одному из существующих» - активируемое устройство будет привязано к существующему устройству в ППО. В результате привязки пересекающиеся идентификаторы будут оставлены, а все остальные обновлены на те, что есть у нового активируемого устройства. При этом карточка устройства останется прежней.

ПРИМЕЧАНИЕ. Автоматическое применение данной стратегии при разрешении конфликта в заявке будет отменено и она перейдет в ручное разрешение с дальнейшим согласованием, если:

- более одного существующего устройства с пересечением;
- его `hostname` отличается от `hostname` активируемого устройства;
- у активируемого устройства нет `hostname`, а у существующего — есть;

– «Создать новое устройство, исключив пересекающиеся идентификаторы» - выбрано по умолчанию. В результате применения этой стратегии будет создано новое устройство в ППО, но у него будут удалены пересекающиеся идентификаторы с другими существующими устройствами.

ПРИМЕЧАНИЕ. Автоматическое применение данной стратегии при разрешении конфликта в заявке будет отменено и она перейдет в ручное разрешение с дальнейшим согласованием, если у активируемого устройства не останется ни одного уникального идентификатора.

После выполнения указанных выше действий необходимо подтвердить или отменить действие.

В результате успешного сохранения данных режим и стратегия для разрешения конфликтов в заявках на активацию будут установлены.

ПРИМЕЧАНИЕ. Заявки на активацию, созданные до выбора режима «Автоматическое разрешение конфликтов», будут автоматически обработаны, когда устройство попытается повторно активироваться по тому же приглашению.

4.1.3.2. Доверенные сети

Доверенные сети используются для проверки IP-адреса устройств, которые используют для самостоятельной регистрации в ПУ приглашение (если такая настройка была включена в приглашении), подробнее п. 2.2.4.

В раскрывающейся строке «Доверенные сети» при нажатии на значок  (см. Рисунок 110 [4]) отображается список доверенных сетей, добавленных в ПУ (Рисунок 111 [2]) с отображением следующей информации:

– «Имя» – название доверенной сети;
– «Адрес сети» – адрес доверенной сети;
– «Комментарий» – комментарий к доверенной сети.

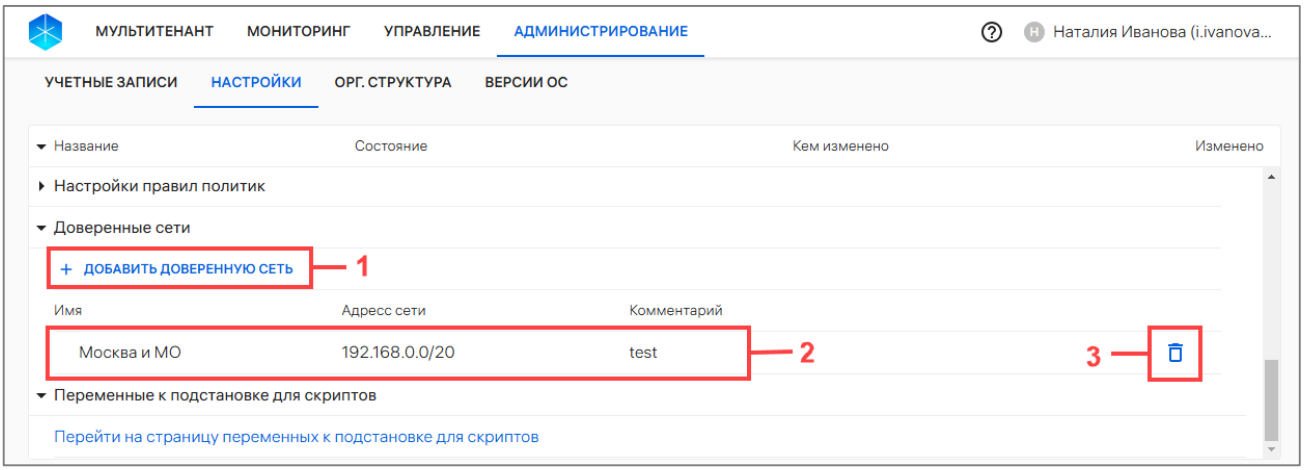


Рисунок 111

Для добавления доверенной сети, необходимо выполнить следующие действия:

– нажать кнопку «Добавить доверенную сеть» (см. Рисунок 111 [1]);
– в отобразившемся окне заполнить поля, приведенные в таблице (Таблица 59);
– после ввода значений необходимо подтвердить либо отменить действия.

Таблица 59

Параметр	Описание
Название	Название доверенной сети. Может содержать от 1 до 100 символов. Поле обязательно для заполнения
Сеть и маска	Адрес доверенной сети в формате IPv4/маска. Поле обязательно для заполнения
Комментарий	Дополнительная информация к доверенной сети. Может содержать до 1000 символов. Поле не обязательно для заполнения

Для удаления доверенной сети необходимо нажать на значок  «Удалить доверенную сеть» (см. Рисунок 111 [3]) и в открывшемся окне подтвердить либо отменить действие.

4.1.3.3. Используемые типы идентификаторов

Возможно настроить типы идентификаторов, которые будут использоваться ППО при активации устройств по приглашениям и в дальнейшем отображаться в интерфейсе.

ВНИМАНИЕ! По умолчанию данная настройка выключена, и ППО использует все типы идентификаторов, которые получает от устройства при активации по приглашениям.

В ППО поддерживаются и используются следующие типы идентификаторов:

– IMEI – при наличии для устройств с ОС Аврора и ОС Android;
– Серийный номер – при наличии для устройств с ОС Аврора и ОСAndroid;
– Ethernet MAC – при наличии для устройств с ОС семейства Linux;
– WLAN MAC – для устройств с ОС Аврора, ОС Android и ОС семейства Linux;
– Сетевое имя устройства – для устройств с ОС семейства Linux и только в том случае, если устройство подключено к корпоративной сети (введено в домен).

Для включения и настройки используемых типов идентификаторов необходимо:

1) Развернуть строку «Используемые типы идентификаторов» (см. Рисунок 110 [5]);

2) Нажать «Редактировать»;

3) Перевести переключатель «Настройка списка» в положение «Включено» (по умолчанию он выключен);

4) Нажать «Добавить тип идентификатора» и выбрать из раскрывающегося списка необходимый тип идентификаторов.

Если требуется добавить более одного типа идентификаторов, необходимо повторить данный шаг.

ПРИМЕЧАНИЕ. Следует добавлять только те типы идентификаторов, которые являются основными и действительно используются для устройств в организации;

5) При добавлении более одного типа идентификаторов будет доступна опция «Задать приоритетный идентификатор», активация которой позволяет задать приоритет применения идентификаторов. Для включения данной опции необходимо установить галочку в соответствующем чекбоксе (Рисунок 112).

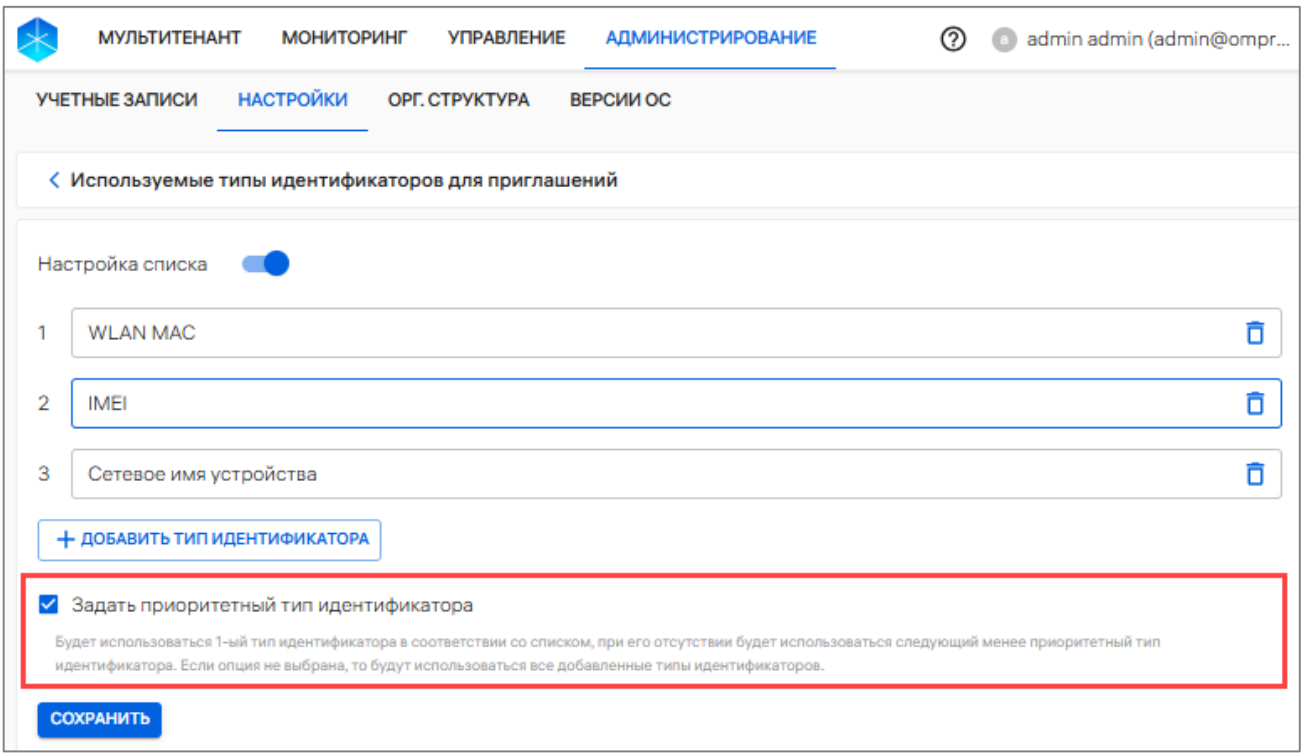


Рисунок 112

Например, в список были добавлены следующие типы идентификаторов:

1) IMEI;

2) WLAN MAC;

3) Сетевое имя устройства.

Затем, с помощью перемещения, выставлен следующий приоритет использования:

1) WLAN MAC;

2) IMEI;

3) Сетевое имя устройства.

Это означает, что при активации устройства по приглашению ППО будет использовать первый тип идентификатора (WLAN MAC) в соответствии с приоритетом в списке. При его отсутствии ППО будет использовать следующий по приоритету тип идентификатора из списка (IMEI).

Для использования всех добавленных типов идентификаторов необходимо оставить опцию выключенной.

ПРИМЕЧАНИЕ. Если были добавлены все типы идентификаторов и опция «Задать приоритетный идентификатор» выключена, то ППО будет работать с активацией устройств по приглашениям также, как и при настройке по умолчанию.

После сохранения настройка моментально применится и ППО начнет ее использовать при следующих активациях устройств по приглашениям.

ВНИМАНИЕ! В случае несоответствия полученных со стороны устройства типов идентификаторов заданному в настройках списку, активация по приглашению завершится с ошибкой: «Ошибка активации по приглашению. Типы идентификаторов не соответствуют заданному списку в настройках».

Если необходимо вернуть настройки по умолчанию, в раскрывающейся строке «Используемые типы идентификаторов» перевести переключатель «Настройка списка» в положение «Выключено» и сохранить изменения. После сохранения ППО будет использовать все поддерживаемые типы идентификаторов при активации устройств по приглашениям.

4.1.4. Платформа

В раскрывающейся строке «Платформа» доступно:

– управление отображением архивных устройств и настройка отображения списка устройств (пп. 4.1.4.1);

– согласование файлов (пп. 4.1.4.2).

4.1.4.1. Отображение архивных устройств и настройка отображения списка устройств

Для активации отображения архивных устройств (см. Рисунок 110 [6]) необходимо перевести переключатель в положение «Включено» . В результате в подразделе «Устройства» раздела «Управление» в списке устройств будут отображаться архивные устройства.

Для настройки отображения списка устройств необходимо нажать на одноименную кнопку. В результате откроется окно, где требуется выбрать платформу (ОС Аврора, ОС Android или ОС Linux и расположить идентификаторы устройства в порядке уменьшения их значимости и далее нажать кнопку «Сохранить».

В результате порядок отображения идентификаторов устройства в списке устройств будет изменен.

Первый и второй идентификаторы будут отображаться в списке устройств как основной и дополнительный, при их отсутствии будут отображаться менее приоритетные идентификаторы (третий, четвертый и т.д.).

ВНИМАНИЕ! Если очистить localStorage браузера, то настройки отображения идентификаторов примут значения по умолчанию.

По умолчанию идентификаторы устройства в списке устройств отображаются согласно следующим приоритетам:

– ОС Аврора, ОС Android:
  - IMEI;
  - Серийный номер;
  - WLAN MAC;
  - Ethernet MAC;
  - Сетевое имя;

- IP;
- Имя устройства;

– ОС семейства Linux:

- Сетевое имя;
- Ethernet MAC;
- IP;
- IMEI;
- WLAN MAC;
- Серийный номер;
- Имя устройства.

4.1.4.2. Настройка давно не подключавшихся устройств

Указанная настройка позволяет скрыть в ПУ все устройства, которые не подключались к серверу дольше указанного количества дней неактивности. Скрытые устройства будут доступны в списке устройств только при применении фильтра по жизненному циклу (подробнее в п. 1.4). Доступ к их карточкам для просмотра информации будет ограничен.

Чтобы скрыть давно не подключавшиеся устройства, необходимо:

– в разделе «Давно не подключавшиеся устройства» (см. Рисунок 110 [7]) нажать «Настройка давно не подключавшихся устройств»;

– перевести переключатель «Скрывать давно не подключавшиеся устройства» в положение «Включено» (по умолчанию он выключен);

– в поле «Количество дней неактивности» ввести количество дней неактивности устройства, после которого его необходимо скрыть. По умолчанию установлено 60 дней. Минимальное значение – 1 день. Максимальное значение - 730 дней;

– в поле «Интервал проверки неактивности» ввести частоту проверки неактивности устройств в формате «N дней M часов». По умолчанию установлено 1 день. Минимальное значение – 1 час;

– нажать кнопку «Сохранить»;

В результате ППО:

– проверит и переведет все устройства в статусе «Активировано», у которых разница между текущей датой и датой последнего подключения к ППО превышает «Количество дней неактивности» из настроек, в статус «Давно не подключалось»;

– исключит устройства со статусом «Давно не подключалось» из групп, в том числе из динамических;

– отвяжет устройства со статусом «Давно не подключалось» от пользователей;

– скроет в интерфейсе устройства со статусом «Давно не подключалось». Скрытые устройства будут доступны в списке устройств только при применении фильтра по жизненному циклу;

– будет проверять устройства на неактивность с частотой, заданной в настройке давно не подключавшихся устройств. Дата и статус последней проверки будут отображены в настройках администрирования ППО в разделе «Давно не подключавшиеся устройства».

При подключении к ППО давно не подключавшегося устройства система:

– восстанавливает связи устройства с группами и пользователями.

ПРИМЕЧАНИЕ. Если пользователь или группа были удалены, пока устройство было в статуе «Давно не подключалось», их связь не будет восстановлена;

– переводит устройство в статус «Активировано»;

– возвращает учет устройства в критериях формирования динамических групп;

– отображает устройство в списке устройств (с измененным статусом «Активировано»).

ВНИМАНИЕ!

✓ Создание и редактирование настроек давно не подключавшихся устройств доступно только для роли «Администратор Платформы управления»;

✓ Перейти в статус «Давно не подключалось» могут только устройства из статуса «Активировано»;

✓ Переход в карточку давно не подключавшегося устройства недоступен;

✓ Для устройств в статусе «Давно не подключалось» доступна возможность архивирования и активации, как по QR-коду, так и по приглашению.

Для отображения давно не подключавшихся устройств, необходимо:

– перейти в настройки давно не подключавшихся устройств (см. Рисунок 110 [7]);

– перевести переключатель «Скрывать давно не подключавшиеся устройства» в положение «Выключено»;

– нажать кнопку «Сохранить».

В результате ППО:

– прекращает учитывать дату последнего подключения устройства к серверу для изменения статуса устройства;

– для каждого устройства в статусе «Давно не подключалось» восстанавливает связи устройства с группами и пользователями.

ПРИМЕЧАНИЕ. Если пользователь или группа были удалены, пока устройство было в статусу «Давно не подключалось», то их связь не будет восстановлена;

– возвращает все устройства из статуса «Давно не подключалось» в статус «Активировано»;

– возвращает учет устройства в критериях формирования динамических групп;

– отображает устройства в списке устройств (с измененным статусом «Активировано»).

4.1.4.3. Согласование контента

Для повышения безопасности в ППО реализована возможность согласования файлов и папок, в ПУ загружаемых, администраторами. Если файл/папка не был согласован или согласован меньшим количеством администраторов, чем задано в настройках ППО, то данный файл/папка недоступен для выбора в политике распространения файлов/папок.

Чтобы установить количество администраторов для согласования загружаемых файлов/папок, необходимо в раскрывающейся строке «Согласование контента» (см. Рисунок 110 [8]) в поле «Количество согласующих администраторов» ввести нужное количество администраторов для согласования файлов/папок и нажать на «Подтвердить».

В результате успешного подтверждения количество согласующих администраторов будет установлено.

4.1.5. Интеграция (информация о серверах)

Для просмотра детальной информации о серверах необходимо в раскрывающейся строке «Интеграция» нажать значок  напротив выбранной вкладки.

4.1.5.1. Сервер приложений

Сервер приложений – адрес Сервера приложений ПМ и список опубликованных витрин на Сервере приложений ПМ.

Переключатель  позволяет включать или отключать витрину. После отключения витрина становится недоступной в списке выбора витрины при создании правила «Приложения/Управление приложениями» в политике.

ПРИМЕЧАНИЕ. В случае, если приложения на устройствах установлены с помощью политики, они не будут удалены с устройств после отключения витрины.

Для просмотра детальной информации о витринах во вложенных строках, которые доступны созданному тенанту, следует нажать значок .

Список опубликованных приложений формируется в ПМ. При отсутствии на сервере опубликованных приложений отображается сообщение «Нет приложений, доступных для назначения».

Если необходимой витрины нет в списке, требуется добавить ее и/или выдать доступ к витрине (параметр «Подключаемые Платформы управления» в настройках витрины).

ПРИМЕЧАНИЕ. Процессы добавления и редактирования витрины приведены в документе «Руководство пользователя. Часть 2. Подсистема «Маркет».

4.1.5.2. Обновление ОС

Обновление ОС – адрес сервера обновления ОС.

Для просмотра версий ОС необходимо нажать значок  в строке «Обновление ОС».

4.1.5.3. Сервер LDAP

Сервер LDAP – адрес сервера LDAP. Во вкладке «Сервер LDAP» предусмотрена возможность просмотреть дату начала и статус синхронизации данных, а также возможность управлять интеграцией с сервером LDAP (добавлять, редактировать и удалять интеграцию).

4.1.5.3.1. Добавление интеграции с LDAP-сервером

Для синхронизации устройств, пользователей и групп с ПУ предусмотрена возможность добавления интеграции ПУ с одним и более LDAP-сервером Active Directory (AD). Синхронизация является односторонней – данные из ПУ не будут переноситься на LDAP-сервер.

ПРИМЕЧАНИЯ:

✓ Поддерживается интеграция со службами каталогов:

– MS AD, протестировано с версией Windows Server 2016;

– ALDPro, протестировано с версией 3.0.0;

– Samba DC (версии 4 и выше), протестировано с версией 4.19.4.

ВНИМАНИЕ! Интеграция может работать и с другими версиями LDAP-серверов, но возможны ограничения или некорректное поведение, не предусмотренное документацией;

✓ Предусматривается возможность добавления интеграции с LDAP-сервером для каждого тенанта;

✓ ПУ поддерживает синхронизацию с LDAP-серверами, в которых устройства, пользователи и группы безопасности хранятся в одном или разных организационных юнитах (`Organizational Unit`);

✓ Категории пользовательских сертификатов и Microsoft Active Directory должны использовать один и тот же центр сертификации AD CS.

Для добавления интеграции ПУ с LDAP-сервером необходимо:

– выполнить подключение ПУ к LDAP-серверу (пп. 4.1.5.3.1.1);

– если требуется синхронизировать:

- пользователей и их группы, настроить интеграцию пользователей (пп. 4.1.5.3.1.2);
- устройства и их группы, настроить интеграцию устройств (п. 4.1.5.3.1.3).

4.1.5.3.1.1. Подключение ПУ к LDAP-серверу

Для выполнения подключения ПУ к LDAP-серверу необходимо:

– во вложенном списке «Интеграция» нажать «Настроить»;

– в области фильтров во вкладке «Подключение к LDAP» задать настройки для подключения к LDAP-серверу согласно таблице (Таблица 60) и далее для проверки работоспособности подключения к LDAP-серверу с заданными настройками нажать кнопку «Проверить подключение».

Таблица 60

Поле	Описание
Тип подключения	Выбрать из раскрывающегося списка тип подключения: – MS AD/Samba DC; – ALD PRO
Использовать безопасное соединение (TLS/SSL)	Если необходимо использовать защищенное подключение к LDAP-серверу (с помощью SSL версии протокола LDAP – LDAPS), следует установить галочку в чекбоксе. По умолчанию галочка в чекбоксе не установлена (используется версия протокола без SSL – LDAP)/ ПРИМЕЧАНИЕ. Для корректной работы ППО с сервером LDAP по безопасному соединению необходимо на ОС установить соответствующий корневой сертификат в доверенные. Подробнее об установке в документе «Руководство администратора» (раздел «Добавление корневого сертификата в доверенные для настройки защищенного TLS/SSL соединения»)
Имя подключения	Ввести название подключения к LDAP-серверу
Адрес сервера	Ввести адрес LDAP-сервера
Порт	В поле задано значение по умолчанию: – 389, если в чекбоксе не установлена галочка «Использовать безопасное соединение (TLS/SSL)»; – 636, если в чекбоксе установлена галочка «Использовать безопасное соединение (TLS/SSL)». ПРИМЕЧАНИЕ. При необходимости можно ввести другой номер порта для подключения к LDAP-серверу. Например, ППО позволяет настроить подключения к LDAP по портам 3268/3269 для использования глобального каталога (Global Catalog)
Логин	Ввести логин для подключения к LDAP-серверу в одном из форматов: – логин без домена, например: «Admin»; – логин с доменом, например: «OMP/Admin»; – логин в виде E-mail, например: «Admin@omp.ru». ВНИМАНИЕ! Для настройки подключения к LDAP с типом ALD Pro необходимо ввести логин LDAP в формате Distinguished Name (DN)
Пароль	Ввести пароль для подключения к LDAP-серверу. Для просмотра/скрытия пароля необходимо использовать значок . После сохранения настроек просмотреть пароль будет невозможно

В случае успешной проверки отобразится сообщение «Подключение доступно».

В случае неудачного завершения проверки отобразится сообщение об ошибке (Рисунок 113[1]), которую необходимо устранить и повторить проверку или обратиться к системному администратору/администратору LDAP. После успешной проверки подключения нажать «Сохранить».

ПРИМЕЧАНИЕ. Для ознакомления с полным текстом ошибки следует нажать «Подробнее» (Рисунок 113 [2]).

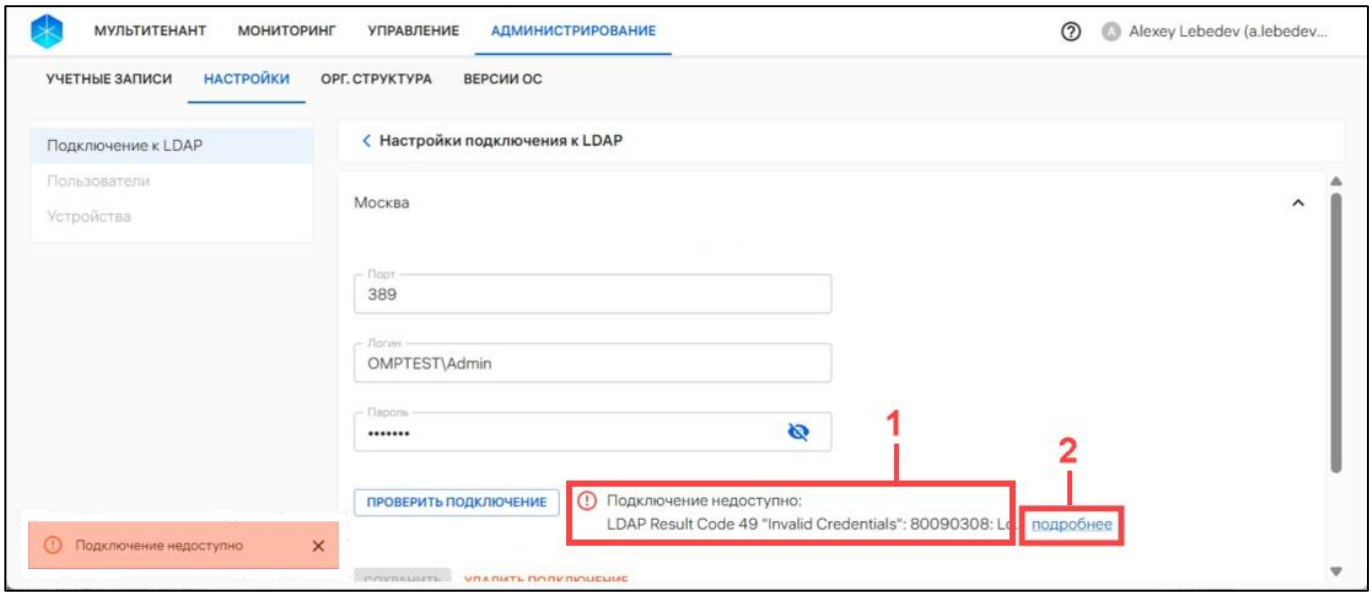


Рисунок 113

Если требуется добавить подключение к другому LDAP-серверу, необходимо нажать кнопку «Подключение» и повторить шаги, приведенные выше.

ПРИМЕЧАНИЕ. Не рекомендуется создавать подключение к Глобальному каталогу. Хотя в нем и содержатся объекты всего каталога (компьютеры, группы, пользователи), но только основные атрибуты этих объектов. Если в дальнейшем функциональность расширится, то не все атрибуты будут доступны и придется перенастраивать импорт, что может вызвать ошибки в синхронизации ППО и LDAP сервера.

4.1.5.3.1.2. Синхронизация пользователей и их групп

Для синхронизации пользователей и их групп необходимо в области фильтров во вкладке «Пользователи» задать настройки для интеграции пользователей согласно таблице (Таблица 61), данные из которой будут синхронизироваться с ППО.

Таблица 61

Поле	Описание
Base DN	Поле обязательно для заполнения. Максимально 1000 символов. Если организационные юниты, группы безопасности и пользователи хранятся: – в одном корне в иерархической структуре каталога, то в поле «Base DN» необходимо ввести это базовое отличительное имя этого корня;

Поле	Описание
	– в разных корнях, то в поле «Base DN» ввести все базовые отличительные имена корней, данные из которых необходимо синхронизировать. Например: `CN=Users, DC=mycompany, DC=com`. ВНИМАНИЕ! ✓ При импорте из ALD Pro, как пользователей, так и устройств в Base DN директории необходимо указать путь к корневому каталогу (так как в ALD Pro плоская структура хранения данных); ✓ Если интеграция с LDAP настроена только с типом подключения ALD PRO, то при редактировании директории и указании несуществующего/пустого корневого каталога, все ранее импортированные сущности будут удалены
Query	Поле необязательно для заполнения. При необходимости в поле «Query» ввести фильтр для выбора нужных записей из Base DN. Максимальное количество символов 10000. Фильтр будет применяться ко всем записям внутри введеных Base DN

ПРИМЕЧАНИЯ:

✓ В результате будут синхронизированы все доступные записи из указанных Base DN (группы с `objectClass = group`, пользователи с `objectClass = person`, организационные юниты с `objectClass = organizationalUnit`). Если `objectClass` для пользователей, групп и организационных юнитов на LDAP-сервере отличаются от указанных выше, следует изменить их в конфигурационном файле ППО;

✓ При импорте пользователей для каждой уникально заданной директории в ППО будут импортированы группы ее верхнего уровня, которые будут наполнены сущностями из «вложенных» групп. Сами же «вложенные» группы не будут импортированы в ППО.

Рекомендации по использованию фильтров:

1) Для корректной работы необходимо в `query` предусмотреть загрузку объектов типа OrganisationUnit. Пример: `(| (&(memberOf=CN=presales,OU=Presales,OU=Sales,OU=Departments,OU=Company,DC=profservice,DC=local) (objectClass=person))(objectClass=organizationalUnit))`.

В результате произойдет:

– обращение к группе (memberOf=CN=presales,OU=Presales,OU=Sales,OU=Departments,OU=Company,DC=profservice,DC=local);

– выгрузка из группы объектов только типа "Person" (&(memberOf=dn=*mygroup,CN=Users,DC=omptest,DC=local)(objectClass=person));

– итоговая конструкция добавляет к выгруженным данным орг. структуру;

2) Если для выбора необходимых пользователей и/или групп из юнита требуется задать несколько фильтров, то следует добавить еще одну директорию (как указано ниже), затем в каждой строке ввести одинаковый «Base DN» и задать нужный фильтр;

3) Если требуется синхронизировать в ПУ уволенных сотрудников, следует указать организационный юнит, в котором они хранятся, или задать фильтры для загрузки таких пользователей;

4) Если не требуется синхронизировать в ПУ уволенных сотрудников, следует задать в фильтрах правило, которое исключит таких сотрудников: если сотрудник имеет статус или параметр, определяющий его неактивность, то необходимо указать это в фильтре. Например: `!(employmentType=NEW)`.

При необходимости возможно добавить еще одну директорию для синхронизации. Для этого нажать кнопку «Добавить директорию» и заполнить для нее поля «Base DN» и «Query» и «Base DN» и «Query» согласно таблице (см. Таблица 61).

Далее необходимо развернуть расскрывающуюся строку «Настройки маппинга».

ВНИМАНИЕ! Для каждого подключения необходимо задавать свои настройки маппинга.

По умолчанию в блоке «Маппинг» в разделе «Основные атрибуты» заданы параметры маппинга атрибутов пользователя ППО и LDAP-сервера, основанные на часто используемых значениях в Active Directory. При необходимости следует ввести в поля другие атрибуты пользователя из LDAP-сервера, соответствующие названию полей, приведенных в таблице (Таблица 62).

Таблица 62

Название поля	Описание
Имя	Поле не обязательно для заполнения. Максимально 100 символов
Фамилия	Поле не обязательно для заполнения. Максимально 100 символов
Отчество	Поле не обязательно для заполнения. Максимально 100 символов. По умолчанию поле отличается в зависимости от типа подключения: для MS AD «middleName», для ALD Pro «rbtamidlename»
Должность	Поле не обязательно для заполнения. Максимально 100 символов
Почта рабочая	Поле обязательно для заполнения. Максимально 100 символов
Телефон рабочий	Поле не обязательно для заполнения. Максимально 100 символов

ВНИМАНИЕ! По указанному в маппинге параметру значения должны соответствовать требованиям к данным для пользователей и групп пользователей, содержащимся в Active Directory, которые приведены в таблице (Таблица 63).

Таблица 63

Параметр	Описание	Примечание
Название группы пользователей	Формат: от 2 до 64 символов	Поле обязательно для заполнения
Почта рабочая	Рабочая почта пользователя устройства. Формат: <логин>@<доменное_имя>, от 2 до 256 символов	Поле обязательно для заполнения. Рабочая почта пользователя должна быть уникальной
Имя	Имя пользователя устройства. Максимально 100 символов	Поле не является обязательным для заполнения
Фамилия	Фамилия пользователя устройства. Максимально 100 символов	Поле не является обязательным для заполнения
Отчество	Отчество пользователя устройства. Максимально 100 символов	Поле не является обязательным для заполнения
Должность	Должность, занимаемая пользователем устройства. Формат: от 2 до 256 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел	Поле не является обязательным для заполнения
Телефон рабочий	Номер телефона пользователя устройства. Формат: от 2 до 64 символов. Только цифры	Поле не является обязательным для заполнения

При необходимости в блоке «Маппинг» в разделе «Дополнительные атрибуты» возможно задать до 10 дополнительных атрибутов пользователя для маппинга.

Для этого необходимо выбрать нужный атрибут из раскрывающегося списка:

– `department` – название отдела;

– `employeeType` – статус работника (работает/уволен);

– `Manager` – ФИО непосредственного руководителя.

Если необходимого атрибута нет в списке, ввести название атрибута и нажать «Enter» на клавиатуре.

Далее необходимо развернуть расскрывающуюся строку «Синхронизация». Если необходимо импортировать сущности, вложенные в заданные Base DN, даже если они выходят за пределы области их видимости, установить переключатель «Расширенный поиск» в положение «Включено».

ПРИМЕЧАНИЯ:

✓ При применении данной настройки рекомендуется использовать подключение к глобальному каталогу, во избежание ошибок, связанных с невозможностью импорта сущности из другого домена для стандартного подключения к LDAP с портами 389/636;

✓ При использовании подключения к глобальному каталогу и включении настройки «Расширенный поиск», будут импортированы сущности только из групп с типом «Универсальная»;

✓ По умолчанию данные из LDAP-сервера будут синхронизироваться каждые 1 час 30 минут.

Если необходимо:

– отключить синхронизацию данных, то следует установить переключатель «Синхронизация по расписанию» в положение «Выключено»;

– изменить частоту синхронизации, то следует ввести нужный временной интервал в поле «Повторять каждые».

ВНИМАНИЕ! Перед архивированием тенанта необходимо отключить синхронизацию данных;

– нажать «Сохранить». Возможно сохранить настройки интеграции, если заполнена хотя бы одна директория по любому из подключений.

В результате будет добавлена интеграция пользователей ПУ с LDAP-сервером и запущена первая синхронизация данных.

Для просмотра даты начала синхронизации и ее статуса необходимо нажать значок  в раскрывающейся строке «Сервер LDAP».

В случае ошибки синхронизации данных для получения подробной информации об ошибке необходимо нажать кнопку «Подробнее» (Рисунок 114).

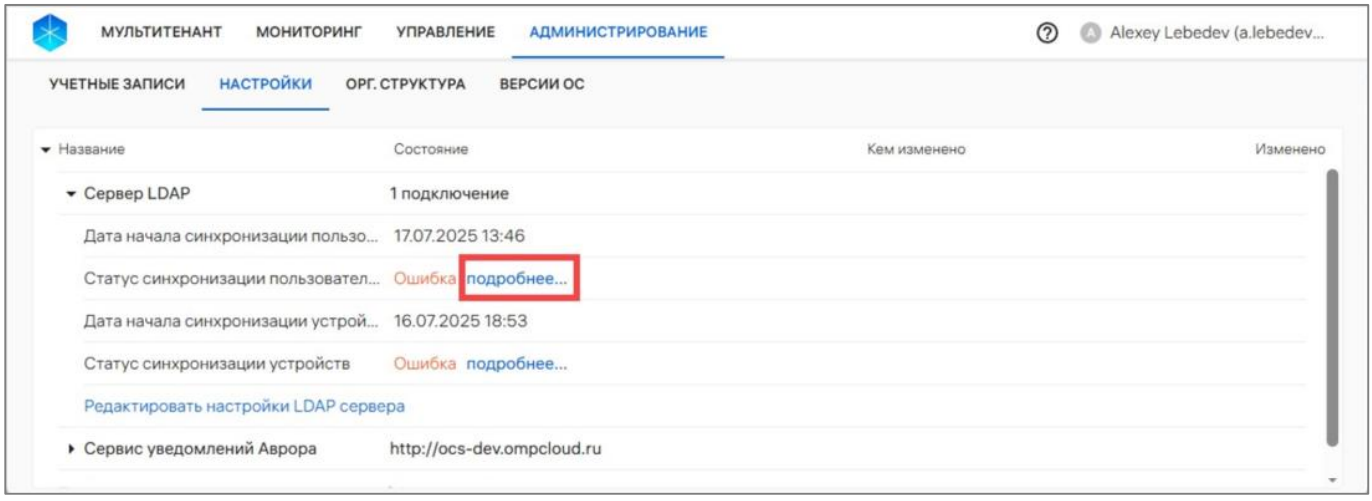


Рисунок 114

4.1.5.3.1.3. Синхронизация устройств и их групп

Для синхронизации устройств и их групп необходимо:

1) В области фильтров во вкладке «Устройства» (Рисунок 115 [1]) задать настройки для интеграции устройств согласно таблице (Таблица 64, Рисунок 115 [2]), данные из которой будут синхронизироваться с ППО;

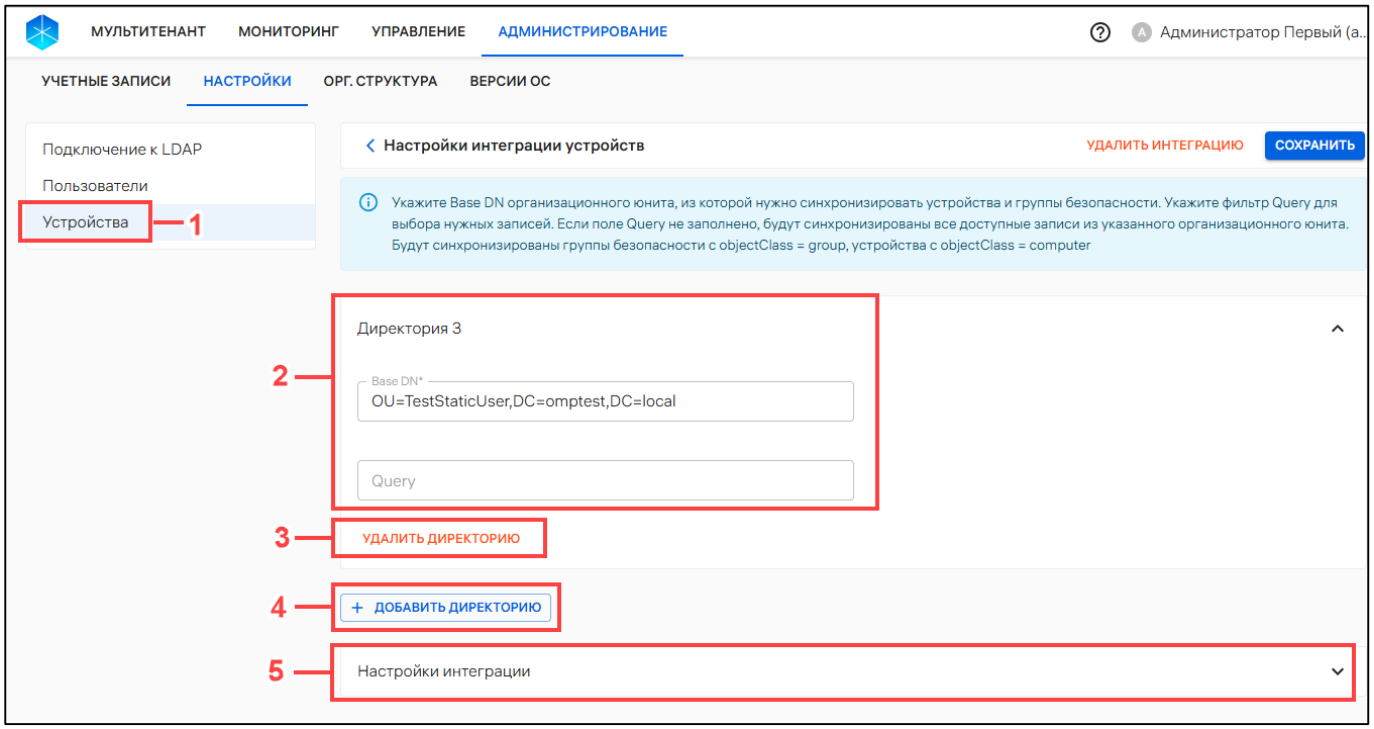


Рисунок 115

Таблица 64

Поле	Описание
Имя	Поле обязательно для заполнения. Ввести имя для директории, которое присвоится ей в ППО. В дальнейшем может использоваться в критерии «Директория LDAP» для формирования группы с устройствами, импортированными из данной директории (подробнее в пп. 2.2.2.2)
Base DN	Поле обязательно для заполнения. Максимально 1000 символов. Если группы безопасности и устройства хранятся: – в одном организационном юните, то в поле «Base DN» необходимо ввести этот юнит; – в разных организационных юнитах, то в поле «Base DN» ввести все организационные юниты, данные из которых необходимо синхронизировать. Например: `CN=Users, DC=mycompany, DC=com`. **ВНИМАНИЕ!** ✓ При импорте из ALD Pro, как пользователей, так и устройств в Base DN директории необходимо указать путь к корневому каталогу (так как в ALD Pro плоская структура хранения данных);

Поле	Описание
	✓ Если интеграция с LDAP настроена только с типом подключения ALD PRO, то при редактировании директории и указании несуществующего/пустого корневого каталога, все ранее импортированные сущности будут удалены
Query	Поле необязательно для заполнения. При необходимости в поле «Query» ввести фильтр для выбора нужных записей из организационных юнитов. Максимальное количество символов 10000. Фильтр будет применяться ко всем записям внутри организационных юнитов, введенных в поле «Base DN»

ПРИМЕЧАНИЯ:

✓ В результате будут синхронизированы группы безопасности с `objectClass = group`, устройства с `objectClass = computer`. Если `objectClass` для устройств и групп на LDAP-сервере отличаются от указанных выше, следует изменить их в конфигурационном файле ППО;

✓ При импорте устройств для каждой уникально заданной директории в ППО будут импортированы группы ее верхнего уровня, которые будут наполнены сущностями из «вложенных» групп. Сами же «вложенные» группы не будут импортированы в ППО.

Рекомендации по использованию фильтров:

– если для выбора необходимых устройств и/или групп из юнита требуется задать несколько фильтров, то следует добавить еще одну директорию (как указано ниже), затем в каждой строке ввести одинаковый «Base DN» и задать нужный фильтр;

– если требуется синхронизировать в ПУ удаленные устройства, следует указать организационный юнит, в котором они хранятся, или задать фильтры для загрузки таких устройств;

– если не требуется синхронизировать в ПУ удаленные устройства, следует задать в фильтрах правило, которое исключит такие устройства: если устройство имеет статус или параметр, определяющий его неактивность, то необходимо указать это в фильтре. Например: `!(deviceType=NEW)`;

2) Нажать кнопку «Добавить директорию» (см. Рисунок 115 [4]) и заполнить поля «Подключение», «Base DN» и «Query» согласно таблице (см. Таблица 64), если необходимо добавить еще одну директорию для синхронизации;

3) Если необходимо удалить директорию, нажать «Удалить директорию» (см. Рисунок 115 [3]);

4) Развернуть расскрывающуюся строку «Настройки интеграции» (Рисунок 115 [5]);

5) Переключатель «Сохранять десинхронизированные устройства» (Рисунок 116 [1]) оставить в положении «Включен», если требуется, чтобы устройства, которые должны будут заархивироваться в ПУ при синхронизации (удаленные на LDAP-сереверe), перемещались в группу `desynced_devices`. Если перевести переключатель в положении «Выключен», то удаленные на LDAP-сервере устройства при синхронизации перейдут в статус «Архивное»;

6) Если необходимо импортировать сущности, вложенные в заданные Base DN, даже если они выходят за пределы области их видимости, установить переключатель «Расширенный поиск» в положение «Включено».

ПРИМЕЧАНИЯ:

✓ При применении данной настройки рекомендуется использовать подключение к глобальному каталогу, во избежание ошибок, связанных с невозможностью импорта сущности из другого домена для стандартного подключения к LDAP с портами 389/636;

✓ При использовании подключения к глобальному каталогу и включении настройки «Расширенный поиск», будут импортированы сущности только из групп с типом «Универсальная»;

7) По умолчанию данные по устройствам из LDAP-сервера будут синхронизироваться каждый 1 час. Если необходимо:

– отключить синхронизацию данных, установить переключатель «Синхронизация по расписанию» в положение «Выключено» (Рисунок 116 [2]).

ВНИМАНИЕ! Перед архивированием тенанта необходимо отключить синхронизацию данных;

– изменить частоту синхронизации, ввести нужный временной интервал в поле «Повторять каждые» (Рисунок 116 [3]);

8) Нажать кнопку «Сохранить» (Рисунок 116 [4]). Возможно сохранить настройки интеграции, если заполнена хотя бы одна директория по любому из подключений.

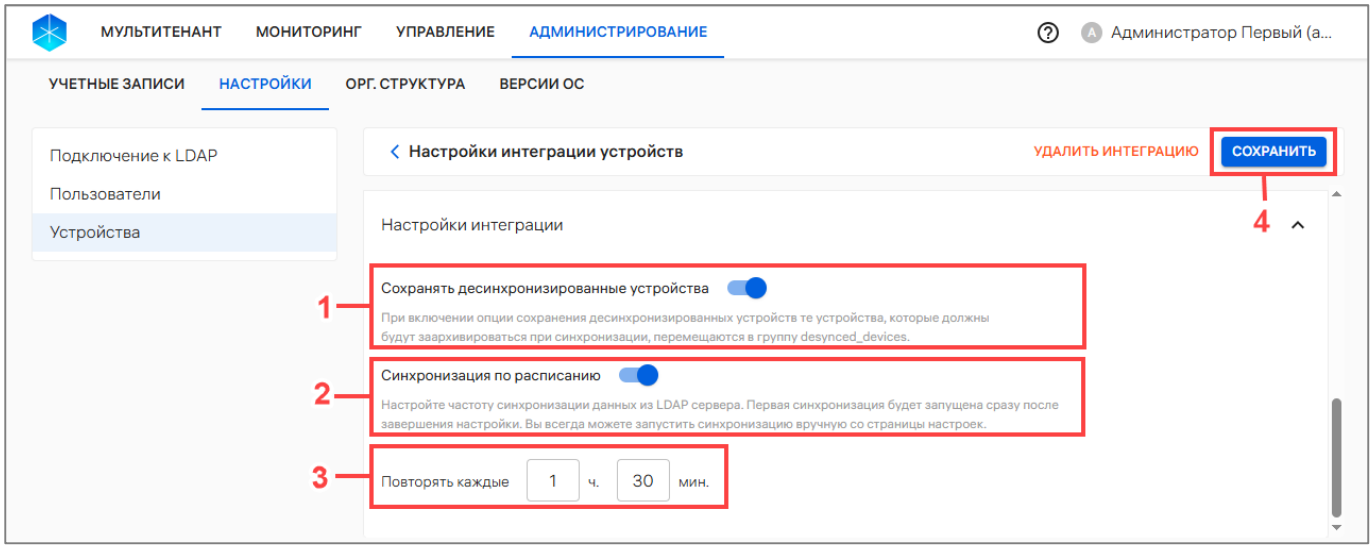


Рисунок 116

В результате будет добавлена интеграция устройств ПУ с LDAP-сервером и запущена первая синхронизация данных.

Для просмотра даты начала и статус синхронизации (Рисунок 117) необходимо нажать значок  в раскрывающейся строке «Сервер LDAP».

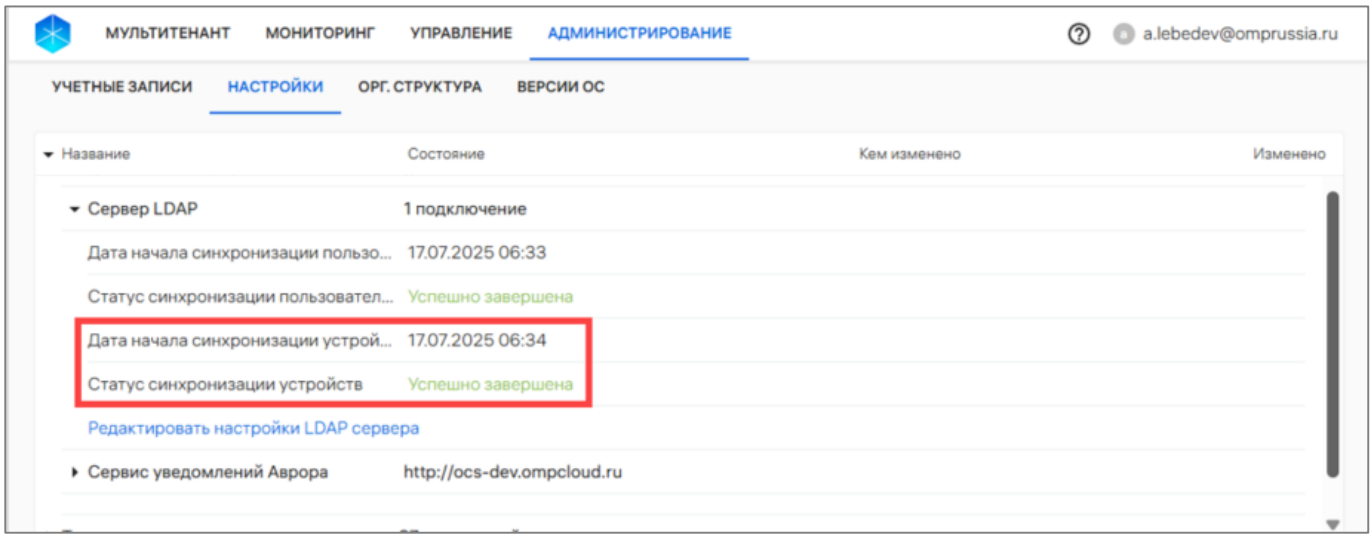


Рисунок 117

В случае ошибки синхронизации данных для получения подробной информации об ошибке необходимо нажать кнопку «Подробнее» (пример: см. Рисунок 114).

Доступно активировать устройства, синхронизированные из LDAP-сервера, с помощью сгенерированного QR-кода или приглашения на самостоятельную регистрацию. В качестве идентификатора устройства будет использовано сетевое имя (hostname) устройства.

ВНИМАНИЕ!

✓ При активации устройств, импортированных по LDAP, необходимо учитывать, что их сетевые имена будут содержать не более 15 символов в службе каталогов. Таким образом, устройства, у которых различаются только 16-й и далее символы, считаются как одно и то же устройство. Не рекомендуется использовать длинные сетевые имена, так как при передаче в ПУ они будут обрезаться (не более 15 символов);

✓ Сетевое имя устройства присылается приложением «Аврора Центр» с добавленным к нему названием домена. Например: для устройства «pc1» в домене «omp.ru» параметр будет содержать «pc1.omp.ru». Из этих же соображений не рекомендуется использовать точку «.» в названии устройства;

✓ При импорте пользователей из нескольких LDAP-подключений может возникать ситуация, при которой будет некорректно работать привязка устройства к пользователю по времени сессии (актуально для устройств с ОС семейства Linux): если в двух разных доменах существуют пользователи `user1@mos.rtk.ru` и `user1@spb.rtk.ru`, то если на устройстве работал `user1@mos.rtk.ru`, оно может

привязаться к user1@spb.rtk.ru. Причина - на устройстве невозможно получить данные о пользователях с их временем сессии, чтобы для пользователя был указан именно upn (user1@mos.rtk.ru). ППО имеет данные о домене, в который включено устройство, при этом пользователь из домена spb.rtk.ru может работать на устройстве из домена mos.rtk.ru.

4.1.5.3.2. Редактирование настроек подключений ПУ к LDAP-серверам

При необходимости возможно изменить настройки интеграции ПУ с LDAP-сервером Microsoft Active Directory (AD), после чего синхронизация также будет односторонняя – данные из ПУ не будут переноситься на LDAP-сервер.

Для редактирования настройки подключений ПУ к LDAP-серверам необходимо выполнить следующие действия:

– в раскрывающейся строке «Интеграция» развернуть строку «Сервер LDAP» и нажать «Редактировать настройки LDAP-сервера»;

– при необходимости изменить:

- настройки для подключения к LDAP-серверу в соответствии с описанием, приведенным в пп. 4.1.5.3.1.1. В результате успешного редактирования настройки подключения ПУ к LDAP-серверу будут изменены. Если была настроена интеграция пользователей и/или устройств, то начнется новая синхронизация данных;
- настройки интеграции пользователей в соответствии с описанием, приведенным в пп. 4.1.5.3.1.2. В результате успешного редактирования настройки интеграции пользователей будут изменены. Начнется новая синхронизация данных;
- настройки интеграции устройств в соответствии с описанием, приведенным в пп. 4.1.5.3.1.3. В результате успешного редактирования настройки интеграции устройств будут изменены. Начнется новая синхронизация данных.

4.1.5.3.3. Удаление интеграции с LDAP-сервером

При необходимости возможно удалить интеграцию пользователей и/или устройств ПУ с LDAP-сервером (пп. 4.1.5.3.3.1). В этом случае синхронизировать данные с ППО будет возможно, пока не будет добавлена новая интеграции с LDAP-сервером.

Также при необходимости возможно удалить настроенные подключения ПУ к LDAP-серверам (пп. 4.1.5.3.3.2).

4.1.5.3.3.1. Удаление интеграции пользователей и/или устройств

Для удаления интеграции с LDAP-сервером необходимо выполнить следующие действия:

– в раскрывающейся строке «Интеграция» развернуть строку «Сервер LDAP» и нажать «Редактировать настройки LDAP-сервера»;

– в области фильтров перейти во вкладку:

- «Пользователи» и нажать кнопку «Удалить интеграцию» для удаления интеграции пользователей;

• «Устройства» и нажать кнопку «Удалить интеграцию» для удаления интеграции устройств;

– в отобразившемся окне:

• при удалении интеграции пользователей подтвердить либо отменить действия;

• при удалении интеграции устройств, если требуется чтобы:

♦ синхронизированные ранее устройства были перенесены в группу `desynced_devices`, нажать кнопку «Сохранить устройства»;

♦ устройства были заархивированы, нажать кнопку «Удалить устройства».

В результате успешного удаления:

– интеграция пользователей будет удалена. Синхронизированные ранее пользователи будут заархивированы;

– интеграция устройств будет удалена. Синхронизированные ранее устройства будут заархивированы или перемещены в папку `desynced_devices` (в зависимости от того, что было выбрано в окне подтвержения.

Для синхронизации пользователей и/или устройств и групп с ПУ потребуется добавить новую интеграцию с LDAP-сервером (пп. 4.1.5.3.1).

4.1.5.3.3.2. Удаление подключения к LDAP-серверу

Для удаления подключения к LDAP-серверу необходимо:

– в настройках интеграции пользователей/устройств отвязать директории от подключения, которое необходимо удалить. Для этого либо удалить интеграции, выполнив действия, приведенные в пп. 4.1.5.3.3.1, либо отредактировать настройки интеграции (пп. 4.1.5.3.2);

– перейти во вкладку «Подключение к LDAP»;

– в блоке с нужным подключением нажать «Удалить подключение»;

– в результате отобразится окно подтверждения операции, где необходимо подтвердить или отменить действия.

В результате успешного подтверждения подключение к LDAP-серверу будет удалено.

Если небходимо удалить другое подключение к LDAP-серверу, повторить действия, приведенные выше.

4.1.5.4. Сервис уведомлений

Сервис уведомлений – настройка ПСУ.

С помощью ПСУ на устройства осуществляется оперативная доставка информации (текстовые сообщения и команды) в виде текстовых push-уведомлений.

Описание работы ПСУ приведено в документе «Руководство пользователя. Часть 5. Подсистема Сервис уведомлений».

Описание доставки push-уведомлений на устройства приведено в документе «Руководство пользователя. Часть 7. Приложение «Аврора Центр» для операционной системы Аврора».

Для просмотра настроек ПСУ необходимо нажать значок , в результате чего отобразятся параметры, приведенные в таблице (Таблица 65).

Таблица 65

Настройки	Описание
Интеграция с СУ	Определяет включение отправки настроек ПСУ для приложения «Аврора Центр»
Настройки устройства	
Адрес для мобильного клиента	Адрес ПСУ для приложения «Аврора Центр»
Порт для мобильного клиента	Порт уведомлений для приложения «Аврора Центр»
ID приложения	Идентификатор приложения «Аврора Центр», с которым оно регистрируется в ПСУ
Дополнительные параметры (отображаются в настройках ПСУ, только если они были добавлены в конфигурационный файл ППО, также они не учитываются на устройствах на базе ОС Android)	
CRL: Проверка отзыва сертификатов	Определяет, включена ли проверка наличия сертификата ПСУ среди списка отозванных сертификатов
CRL: Интервал обновления в секундах	Временной интервал обновления списка отозванных сертификатов
SSL: Валидация сертификата	Определяет, включена ли валидация сертификата ПСУ
SSL: Уровень валидации сертификата	Уровень валидации имени хоста, указанного в сертификате ПСУ. Возможные значения: – «Не проверяется»; – «Поддержка поддоменов»; – «Точное совпадение»
Настройки сервера	
Адрес API	Адрес API ПСУ для приложения «Аврора Центр»
ID проекта для отправки уведомлений	Идентификатор проекта в ПСУ для отправки уведомлений

Для изменения настроек ПСУ необходимо выполнить одно из следующих действий:

– нажать на название поля «Сервис уведомлений»;
– нажать «Редактировать настройки Сервиса уведомлений».

В результате выполнения одного из указанных действий будут доступны поля для редактирования настройки ПСУ одним из следующих способов:

– загрузка JSON-файлов с настройками нажатием кнопки «Загрузить файлы настроек»;

– внесение изменений вручную в соответствии с таблицей (Таблица 66).

После внесения уточнения в соответствии с таблицей (Таблица 66) необходимо подтвердить либо отменить действия.

Таблица 66

Поле	Описание
Интеграция с СУ	Данное поле предназначено для включения или выключения отправки настроек ПСУ для приложения «Аврора Центр» при помощи переключателя 
Мобильные устройства	
Имя хоста для мобильного клиента	IP-адрес или имя хоста ПСУ для приложения «Аврора Центр»
Порт для мобильного клиента	Номер порта уведомлений для приложения «Аврора Центр»
ID приложения мобильного клиента	Идентификатор приложения, с которым приложение «Аврора Центр» регистрируется в ПСУ
SSL (параметры SSL отображаются в настройках ПСУ, только если они были добавлены в конфигурационный файл ППО, также они учитываются на устройствах на базе ОС Android)	
Валидация соединения с сервером	Выбор из раскрывающегося списка значения, которое определяет, включена ли валидация сертификата ПСУ: – Выключено; – Включено
Уровень валидации имени хоста	Выбор из раскрывающегося списка уровеня валидации имени хоста, указанного в ПСУ: – Не выбрано; – Не проверяется; – Поддержка поддоменов; – Точное совпадение
CRL (параметры CRL отображаются в настройках ПСУ, только если они были добавлены в конфигурационный файл ППО, также они не учитываются на устройствах с ОС Android)	
Проверка отозванности сертификата	Выбор из раскрывающегося списка значения, определяющего, включена ли проверка наличия сертификата ПСУ среди списка отозванных сертификатов: – Выключено; – Включено

Поле	Описание
Период обновления	Ввод значения с клавиатуры временного интервала обновления списка отозванных сертификатов (в секундах)
Параметры сервера	
Адрес API	Адрес API ПСУ для приложения «Аврора Центр» (в виде `proto://host:port`). Параметр должен быть задан администратором в конфигурационном файле ППО. При изменении параметра вручную настройки ПСУ не меняются
ID проекта для отправки уведомлений	Ввод значения с клавиатуры: идентификатор проекта в ПСУ для отправки уведомлений
Параметры для авторизации	
Token URL	Ввод значения с клавиатуры: URL для получения токена авторизации
ClientID	Ввод значения с клавиатуры: идентификатор клиента технической учетной записи
KeyID	Ввод значения с клавиатуры: приватный ключ технической учетной записи. Параметр указывает, какой ключ используется на сервисе авторизации
Приватный ключ	Необходимо нажать «Обновить ключ» и ввести приватный ключ технической учетной записи
Audience	Ввод значения с клавиатуры: аудитория токена доступа после нажатия значка . Для удаления аудитории необходимо нажать значок  справа от его названия
Scopes	Ввод значения с клавиатуры: область (скоуп) для OIDC-клиента, используемая для аутентификации в ПСУ. Для ввода значения необходимо нажать значок . Для удаления области необходимо нажать значок  справа от ее названия
Интеграция	
Настроить интеграцию с внешним сервисом уведомлений	При нажатии «Настроить интеграцию с внешним сервисом уведомлений» произойдет выгрузка JSON-файла с настройками Аврора Центр для подключения к отдельно развернутому Сервису уведомлений. **ПРИМЕЧАНИЕ.** Процесс подключения к отдельно развернутому Сервису уведомлений приведен в документе «Руководство пользователя. Часть 5. Подсистема Сервис уведомлений»

4.1.5.5. Центры сертификации

В ППО доступна возможность добавить интеграцию с центром сертификации, который выпускает пользовательские сертификаты для подключения к беспроводным сетям.

ВНИМАНИЕ! ППО протестировано с интеграцией с центрами сертификации, имеющими тип сервера Microsoft Active Directory Certificate Services (AD CS) в Windows Server 2019.

Для просмотра списка интеграций с центрами сертификации необходимо нажать значок блока «Центры сертификации» (см. Рисунок 110 [9]). Для добавления центра сертификации необходимо выполнить следующие действия:

– нажать «Добавить центр сертификации»;
– заполнить поля ввода, приведенные в таблице (Таблица 67);
– нажать кнопку «Создать».

В результате интеграция с центром сертификации будет добавлена в ППО.

Таблица 67

Поле	Описание
Название	Название центра сертификации. Ввод значения с клавиатуры. Может содержать от 1 до 256 символов
URL веб-интерфейса центра сертификации	Ввести URL-адрес веб-интерфейса центра сертификации в формате https://<servername>/certsrv. Может содержать от 1 до 256 символов
Тип сервера	По умолчанию установлено значение Microsoft AD CS. Поле недоступно для редактирования
Логин	Логин для подключения к центру сертификации. Может содержать от 1 до 256 символов
Пароль	Пароль для подключения к центру сертификации. Может содержать от 1 до 256 символов

4.1.5.6. Git-репозитории

Для добавления в ПУ различных файлов скриптов/конфигураций для распространения на устройства доступно подключение удаленных репозиториев git. Для этого необходимо добавить интеграцию с git-репозиторием.

ВНИМАНИЕ. Синхронизация с git-репозиторием для получения папок/файлов не будет работать, если в качестве хранилища в ППО выбрано S3.

Для просмотра списка подключенных git-репозиториев, даты начала и статуса его синхронизации с ППО (Рисунок 118 [2]) необходимо нажать значок в строке «Git-репозитории».

Для подключения необходимо выполнить следующие действия:

– нажать на кнопку «Подключить git-репозиторий» (Рисунок 118 [1]);

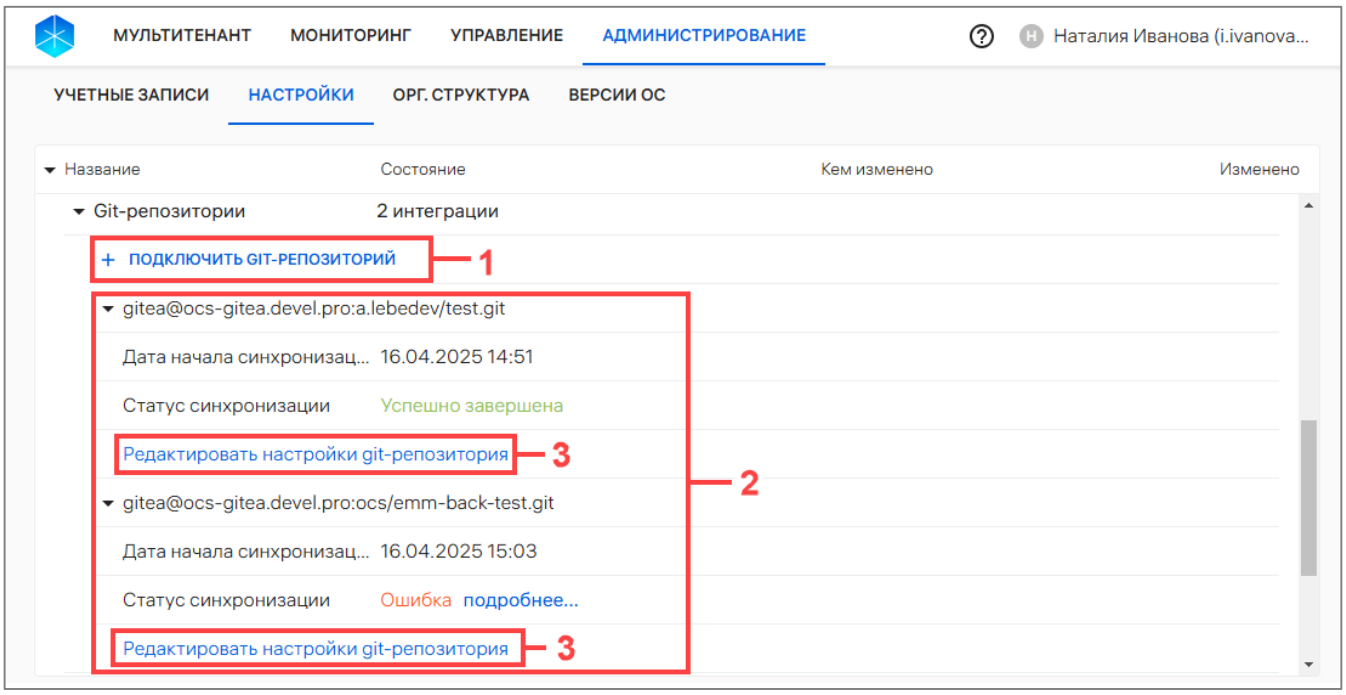


Рисунок 118

– в отобразившемся окне в поле «Публичный SSH-ключ» будет сгенерирован SSH-ключ, который необходимо скопировать с помощью кнопки (Рисунок 119 [2]) и добавить в git-репозиторий, который необходимо подключить;

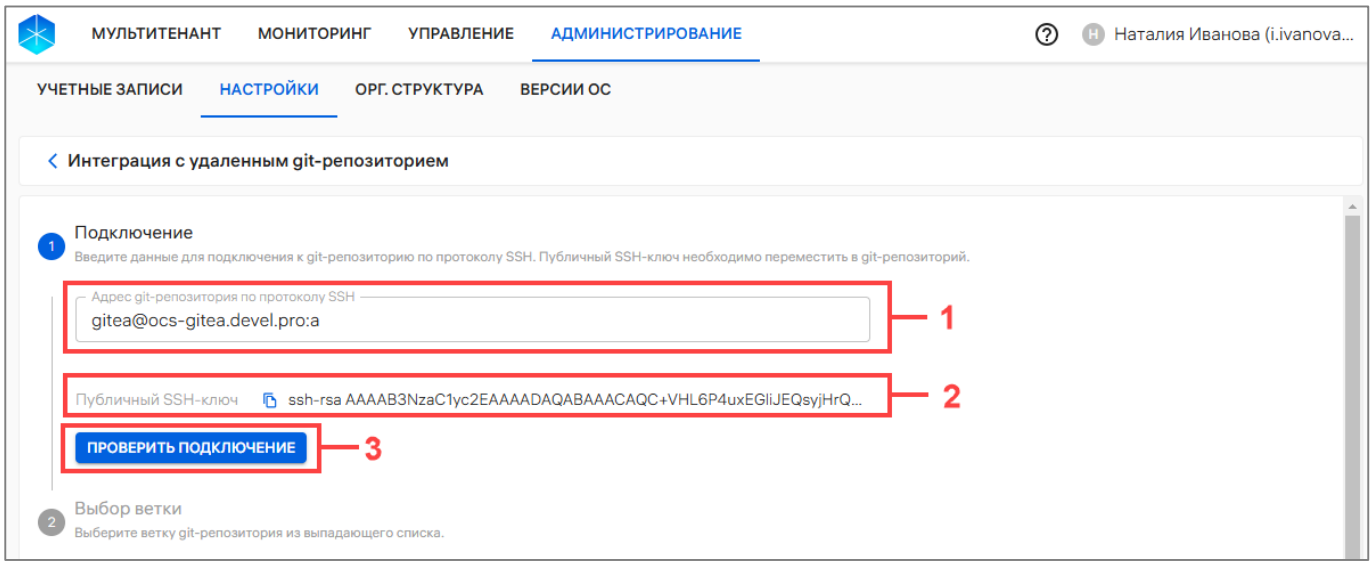


Рисунок 119

– в поле «Адрес Git-репозитория по протоколу SSH» (см. Рисунок 119 [1]) ввести адрес и нажать на кнопку «Проверить подключение» (см. Рисунок 119 [3]);

ВНИМАНИЕ! Если сервис для хостинга git-репозиториев использует нестандартный SSH-порт, то данный порт должен быть задан при создании интеграции с git. Для этого необходимо в строке подключения использовать следующую `scp-style` нотацию: `<user>@<host>:<port>:<path>`.

Например: `git@example.com:22222:path/to_repository.git`;

– в отобразившемся окне подтвердить либо отменить действия. При успешном подключении к git-репозиторию отобразится соответствующее сообщение;

– в раскрывающемся списке «Ветка» (Рисунок 120 [1]) выбрать ветку репозитория, файлы из которой требуется добавить в ПУ;

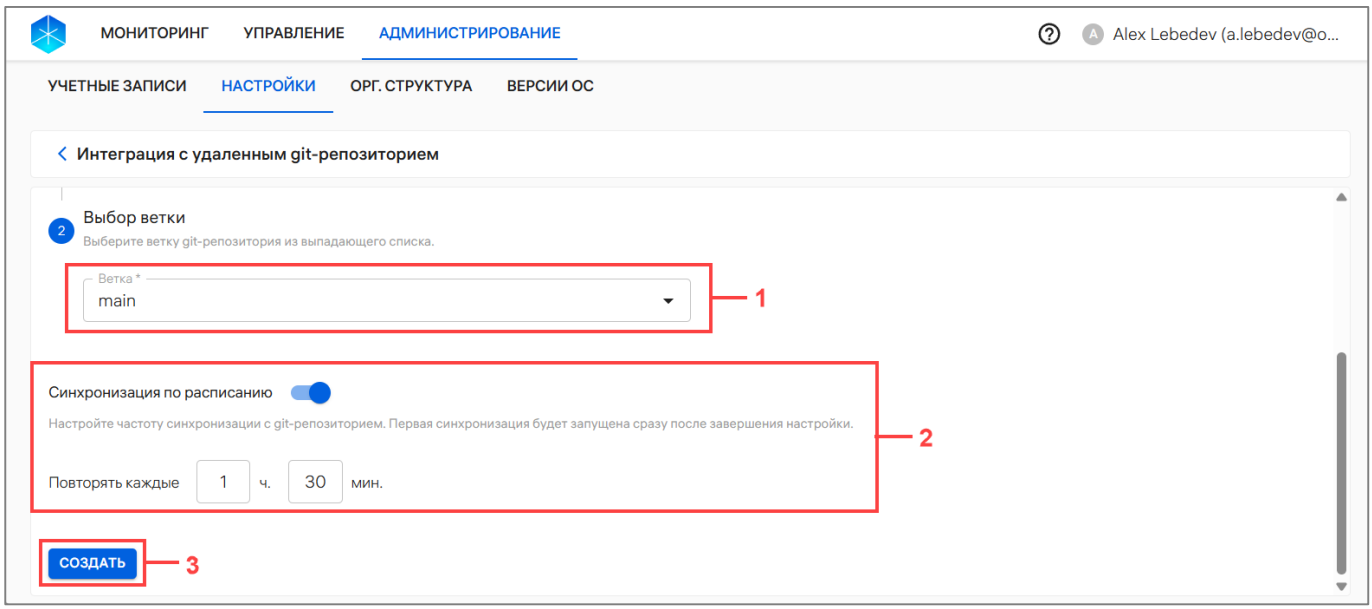


Рисунок 120

– перевести переключатель «Синхронизация по расписанию» (Рисунок 120 [2]) в положение «Включено», если требуется задать частоту синхронизации с git-репозиторием, а в поле «Повторять каждые» ввести частоту синхронизации. По умолчанию задана частота 5 минут.

ПРИМЕЧАНИЕ. При каждой синхронизации ППО будет проверять наличие новых версий загруженных файлов в git-репозитории, и, в случае их наличия, автоматически загрузит новые версии в ППО;

– нажать на кнопку «Создать» (см. Рисунок 120 [3]).

В результате git-репозиторий будет подключен к ППО и произойдет первая синхронизация.

Также для интеграции с git-репозиторием доступно редактирование (включение, отключение синхронизации, а также изменение ее частоты). Для этого в списке подключенных git-репозиториев необходимо нажать на «Редактировать настройки git-репозитория» (см. Рисунок 118 [3]).

В открывшемся окне редактирования:

– включить/выключить синхронизацию, для этого перевести переключатель «Синхронизация по расписанию» в нужное положение;

– изменить частоту синхронизации, для этого задать нужную частоту в поле «Повторять каждые»;

– нажать кнопку «Сохранить».

В результате настройки синхронизации с git-репозиторием будут изменены.

4.1.6. Территории

Территории используются для офлайн-сценариев с событиями «Нахождение на территориях, определяемых координатами»/«Нахождение вне территории, определяемой координатами». Территория может содержать один или несколько четырехугольных полигонов, нанесенных на карту.

В раскрывающейся строке «Территории» при нажатии на значок (см. Рисунок 110 [10]) отображается список территорий (Рисунок 121 [2]).

Если потребуется просмотреть территорию на карте, необходимо нажать на ее название.

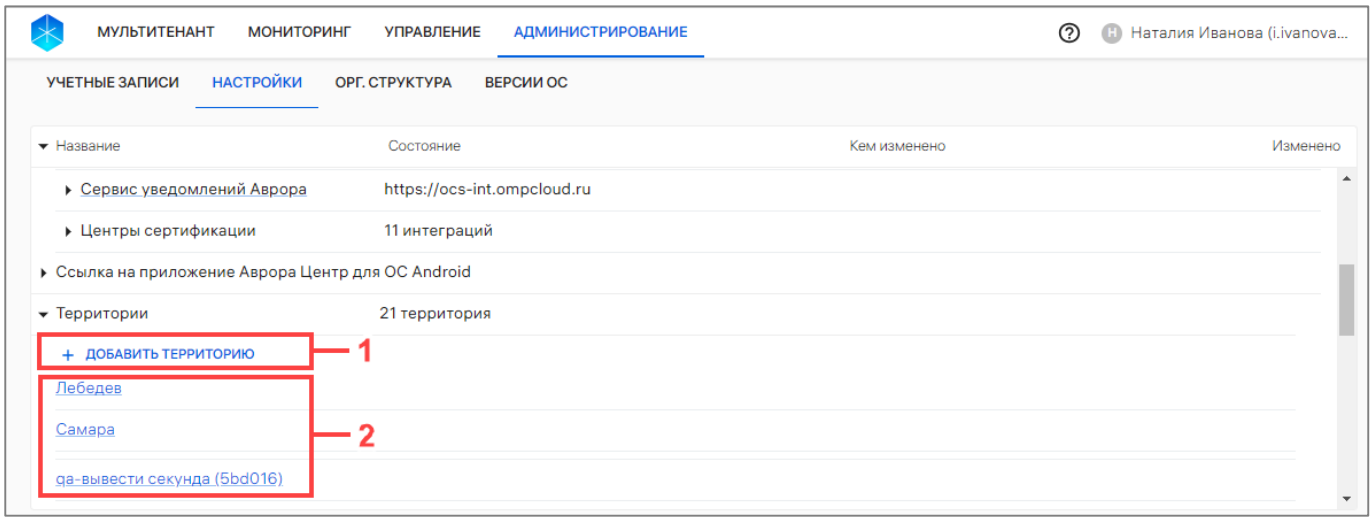


Рисунок 121

Для добавления территории необходимо выполнить следующие действия:

– нажать кнопку «Добавить территорию» (см. Рисунок 121 [1]);

– в отобразившемся окне необходимо ввести название территории в поле «Название» (Рисунок 122 [1]). Поле обязательно для заполнения и может содержать от 1 до 256 символов;

– добавить 1 или несколько полигонов на территории, выполнив следующие действия:

- выбрать объект на карте;
- нажать кнопку «Добавить полигон» (Рисунок 122 [3]);
- указать на карте 4 вершины полигина (Рисунок 122 [2]). С помощью перемещения вершин полигона возможно менять его форму. У полигона не может быть нулевой площади. Ребра одного полигона не должны пересекать друг друга. Территория должна содержать хотя бы один полигон.

ПРИМЕЧАНИЕ. Возможно добавление до 50 полигонов на территории;

– при необходимости доступно удаление полигонов, выделенных на карте. Для этого необходимо нажать на значок «Удалить полигон» и выбрать необходимый полигон (Рисунок 122 [4]);

– после ввода данных необходимо подтвердить либо отменить действие (Рисунок 122 [5]).

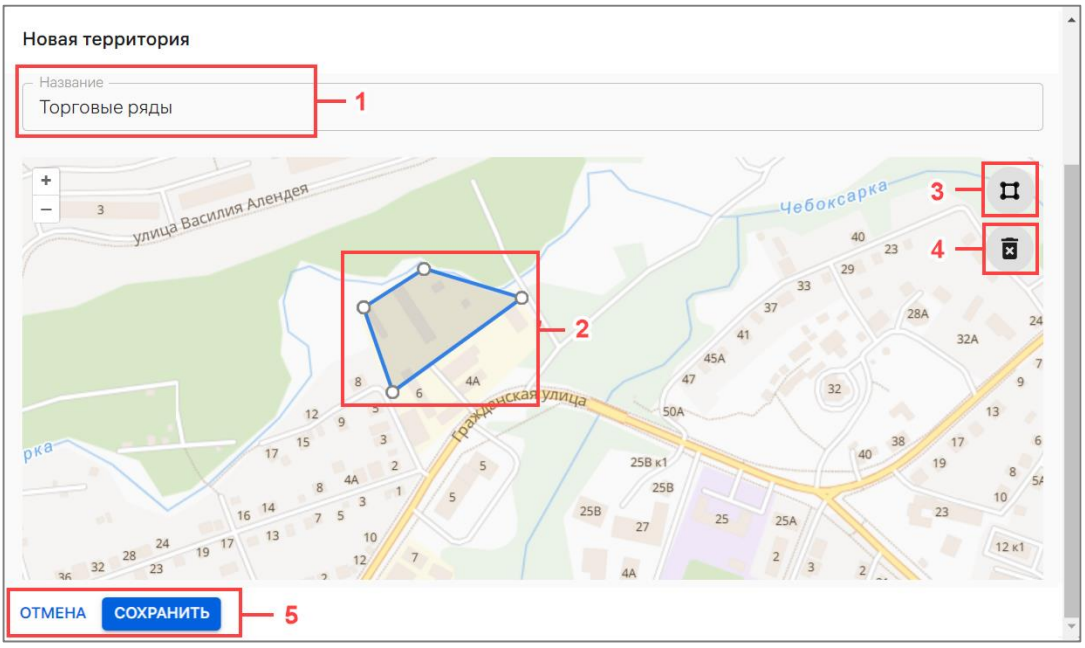


Рисунок 122

В результате успешного сохранения данных, территория будет добавлена в ППО и будет доступна при создании офлайн-сценариев с событиями «Нахождение на территориях, определяемых координатами»/«Нахождение вне территории, определяемой координатами».

4.1.7. Настройки правил политик

При настройке правил политики доступен:

– запрет удаления приложений с устройств при переведении переключателя в положение «Включено» (Рисунок 123 [1]) и с последующим сохранением при нажатии кнопки «Сохранить» (Рисунок 123 [4]). При включенном запрете на удаление приложений с устройств после снятия политики с группы устройств и переходе между другими группами устройств устанавливаемые и установленные ранее приложения:

- будут сохраняться на устройствах;
- не будут влиять на соответствие политике, которая больше не содержит правила по установке приложений.

ВНИМАНИЕ! Если на устройство была назначена политика с правилом по установке приложений с каким-либо интервалом установки, а затем из политики удалили правило по установке приложения и переназначили на устройство до момента наступления интервала установки, то устройство не установит это приложение даже при включенной настройке по запрету удаления приложений с устройств;

– запрет удаления файлов с устройств при переведении переключателя в положение «Включено» (Рисунок 123 [2]) и с последующим сохранением при нажатии кнопки «Сохранить» (Рисунок 123 [4]). При включенном запрете на удаление файлов с устройств после снятия политики с группы устройств и переходе между другими группами устройств доставляемые и доставленные ранее файлы:

- будут сохраняться на устройствах;
- не будут влиять на соответствие политике, которая больше не содержит правила по доставке файлов;

– запрет удаления скриптов с устройств при переведении переключателя в положение «Включено» (Рисунок 123 [3]) и с последующим сохранением при нажатии кнопки «Сохранить» (Рисунок 123 [4]). При включенном запрете на удаление скриптов с устройств после снятия политики с группы устройств и переходе между другими группами устройств выполняемые и выполненные ранее скрипты:

- будут сохраняться и выполняться на устройствах каждый час (или с заданной ранее в политике периодичностью);
- не будут влиять на соответствие политике, которая больше не содержит правила по выполнению скрипта.

ВНИМАНИЕ! При включении запрета на удаление скриптов с устройств автоматически включается запрет на удаление файлов с устройств.

ПРИМЕЧАНИЕ. После сохранения настройка запрета с соответствующим значением отправится на устройство при следующей синхронизации с сервером Аврора Центр.

Описанный выше результат будет действовать до тех пор, пока в настройках Аврора Центр самостоятельно не будет выключен запрет.

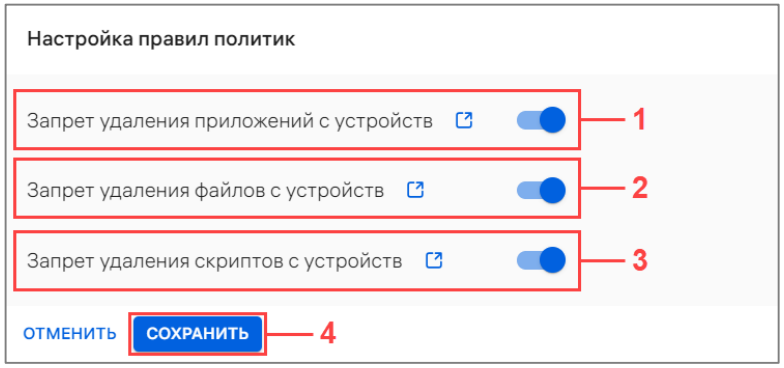


Рисунок 123

4.1.8. Переменные к подстановке

В Консоли администратора ПУ доступен просмотр списка всех управляемых переменных, которые существуют в ППО, а при отсутствии добавленных данных отображается сообщение «Нет данных».

Для просмотра данных необходимо:

– в разделе «Переменные к подстановке» нажать на «Перейти на страницу переменных к подстановке» (см. Рисунок 110 [12]);

– отобразится список управляемых переменных (Рисунок 124 [2]), информация о которых отображается в столбцах, приведенных в таблице (Таблица 68).

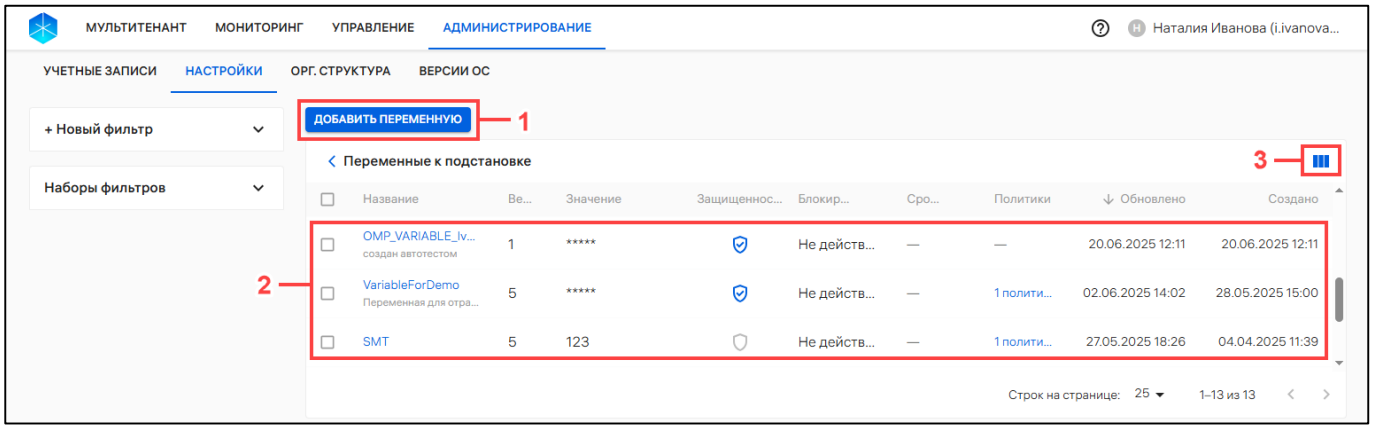


Рисунок 124

Таблица 68

Название столбца	Описание
Название	– название управляемой переменной, заданное при добавлении; – комментарий (при наличии), заданный при добавлении/редактировании. **ПРИМЕЧАНИЕ.** Отображается по умолчанию. Недоступен для скрытия
Версия	Номер версии управляемой переменной. **ПРИМЕЧАНИЕ.** Отображается по умолчанию. Недоступен для скрытия
Значение	Возможные значения: – открытое исходное значение переменной, если при добавлении/редактировании управляемойпеременной переключатель «Защищенность» был в положении «Выключен»; – 5 звезд, если при добавлении/редактировании управляемой переменной переключатель «Защищенность» был в положении «Включен». **ПРИМЕЧАНИЕ.** Отображается по умолчанию. Недоступен для скрытия
Защищенность	Возможные значения: – «Незащищенная переменная» - если при добавлении/редактировании управляемой переменной переключатель «Защищенность» был в положении «Выключен»;

Название столбца	Описание
	– «Защищенная переменная» - если при добавлении/редактировании управляемой переменной переключатель «Защищенность» был в положении «Включен». **ПРИМЕЧАНИЯ:** ✓Отображается по умолчанию. Недоступен для скрытия; ✓Режим защищенности обеспечивает защиту данных путем их шифрования как на сервере ППО, так и в локальном хранилище устройства. Если режим защищенности для переменной активирован, отключить его невозможно. Данный режим предназначен для передачи и безопасного хранения «чувствительной» информации с целью дальнейшего использования при выполнении скриптов с этими переменными
Блокировка	Возможные значения: – значение «Не действует», если управляемая переменная была добавлена впервые или в процессе редактирования переключатель «Блокировка» был переведен в положение «Выключен»; – значение «Действует», если при редактировании управляемой переменной переключатель «Блокировка» был переведен в положение «Включен». **ПРИМЕЧАНИЕ.** Отображается по умолчанию. Недоступен для скрытия
Срок жизни	Возможные значения: – «Истек», если у управляемой переменной закончился заданный срок жизни и она должна быть заблокирована. **ВНИМАНИЕ!** ✓ Управляемая переменная может автоматически блокироваться с задержкой в зависимости от заданного интервала массовой проверки срока жизни в конфигурационном файле сервиса; ✓ При принудительной или автоматической блокировке управляемой переменной ППО выключает срок жизни и сбрасывает количество заданных дней; – «N дн., M ч.», если у управляемой переменной идет заданный срок жизни, где «N» - число дней, «M» - количество часов. При нажатии на значение отображается новое окно с информацией о сроке жизни переменной; – прочерк, если для управляемой переменной нет заданного срока жизни. **ПРИМЕЧАНИЕ.** Отображается по умолчанию. Недоступен для скрытия

Название столбца	Описание
Политики	Возможные значения: – прочерк, если управляемая переменная не добавлена ни в одну из политик; – число политик с гиперссылкой на список политик, в которых присутствует управляемая переменная. Название политик представляет собой активную ссылку, при нажатии на которую осуществляется переход в карточку политики. **ПРИМЕЧАНИЕ.** Отображается по умолчанию. Доступен для скрытия/отображения
Обновлена	Дата и время обновления управляемой переменной в ППО. **ПРИМЕЧАНИЕ.** Отображается по умолчанию. Доступен для скрытия/отображения
Создана	Дата и время добавления управляемой переменной в ППО. **ПРИМЕЧАНИЕ.** Отображается по умолчанию. Доступен для скрытия/отображения

Чтобы скрыть/отобразить нужные столбцы в списке необходимо:

– нажать на значок  «Управлять отображением столбцов» (см. Рисунок 124 [3]);

– установить или снять галочку в чекбоксе (Рисунок 125) напротив названия тех столбцов, которые требуется отобразить или скрыть в списке соответственно.

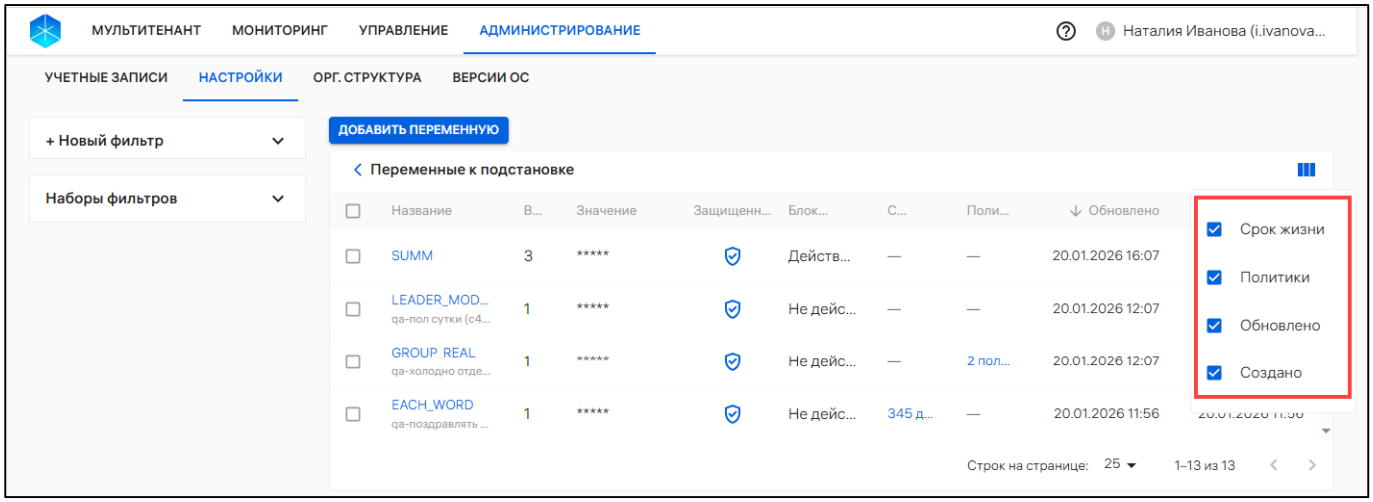


Рисунок 125

4.1.8.1. Добавление управляемой переменной

Для добавления новой управляемой переменной в ППО для дальнейшего использования в правиле политики «Скрипты/Выполнение на устройстве» (пп. 2.4.1.52) и «Приложения/Управляемые конфигурации» (пп. 2.4.1.61) необходимо нажать на кнопку «Добавить переменную» (см. Рисунок 124 [1]), заполнить параметры, приведенные в таблице (Таблица 69) и нажать на кнопку «Сохранить».

Таблица 69

Параметр	Описание
Название	Ввести название управляемой переменной с выполнением следующих условий: – допустимые символы:- a-z, A-Z, 0-9 и _; – первый символ в названии не должен содержать цифру; – название не должно быть меньше 1-ого и больше 255-ти символов. **ПРИМЕЧАНИЕ.** Поле обязательно для заполнения, не подлежит редактированию
Значение	Ввести значение управляемой переменной: – значение не должно быть меньше 1-ого и больше 4096-ти символов; – допускается многострочный ввод текста. Например, сертификат. **ПРИМЕЧАНИЕ.** Поле обязательно для заполнения. Не доступно для редактирования, если переменная заблокирована
Защищенность	Перевести переключатель «Защищенность» в положение «Включен», если требуется сделать управляемую переменную защищенной (по умолчанию он выключен). **ПРИМЕЧАНИЕ.** Режим защищенности обеспечивает защиту данных путем их шифрования как на сервере ППО, так и в локальном хранилище устройства. Если режим защищенности для переменной активирован, отключить его невозможно. Данный режим предназначен для передачи и безопасного хранения «чувствительной» информации с целью дальнейшего использования при выполнении скриптов с этими переменными
Срок жизни	Перевести переключатель «Срок жизни» в положение «Включен», если требуется задать срок жизни для управляемой переменной (по умолчанию он выключен). Затем в поле «ДД» ввести нужное количество дней (количество дней не должно быть больше 365-ти дней) и/или часов в поле «ЧЧ» (минимальное количество задаваемых часов - 1 ч., максимально количество задаваемых часов - 23 ч.), в результате отобразится предварительная дата и время блокировки переменной. **ПРИМЕЧАНИЕ.** Срок жизни обеспечивает безопасность и позволяет контролировать полный жизненный цикл переменной. После окончания указанного периода переменная автоматически блокируется. Это означает, что любые скрипты и конфигурации приложений, содержащие данную переменную и работающие согласно заданной политике, больше не будут выполняться на конечных устройствах пользователей. Для того, чтобы скрипты и

Параметр	Описание
	конфигурации приложений, содержащие данную переменную, вновь выполнялись на устройствах, нужно принудительно разблокировать переменную и при необходимости задать новый срок жизни для нее. **ВНИМАНИЕ!** Управляемая переменная может автоматически блокироваться с задержкой в зависимости от заданного интервала массовой проверки срока жизни в конфигурационном файле сервиса. **ПРИМЕЧАНИЯ:** ✓ При редактировании управляемой переменной, у которой есть действующий срок жизни, в поле «Время жизни» отображается изначально заданное количество дней и/или часов, а не оставшихся; ✓ Если отредактировать действующий срок жизни для управляемой переменной, тогда ППО сбросит счетчик и начнет действовать срок жизни с новым заданным количеством дней. При этом возможно задать новое количество дней/часов только меньше или больше изначального значения. Например: изначально было 30 дней, можно задать меньше и больше 30 дней в пределах допустимых значений
Комментарий	При необходимости ввести дополнительную информацию к управляемой переменной. Может содержать до 512 символов. **ПРИМЕЧАНИЕ.** Поле не обязательно для заполнения, подлежит редактированию

4.1.8.2. Редактирование параметров управляемой переменной

ПРИМЕЧАНИЕ. Для заблокированной переменной для редактирования доступно только поле «Комментарий».

Для редактирование параметров управляемой переменной необходимо:

– в списке управляемых переменных выбрать требуемую переменную (при необходимости воспользоваться фильтром);

– нажать на название нужной переменной;

– в отобразившемся окне внести изменения в полях, приведенных в таблице (см. Таблица 69).

ВНИМАНИЕ! Перед внесением правок убедитесь, что переменная не заблокирована;

– подтвердить либо отменить действия.

После успешного редактирования переменной ее версия будет увеличена (плюс 1 к предыдущей).

ПРИМЕЧАНИЯ:

✓ Если на устройство назначено 2 политики с одним и тем же выполняемым скриптом, но с разными управляемыми переменными, то при редактировании одной из этих управляемых переменных произойдет перекомбинирование политик, и на

устройстве будет действовать более поздняя назначенная политика;

✓ Если при включенной настройке по запрету удаления файлов и скриптов удалить правило по выполнению скрипта с управляемой переменной, то устройство не будет получать обновленные управляемые переменные, несмотря на включенную настройку по запрету удаления скрипта с устройства.

4.1.8.3. Принудительная блокировка/разблокировка управляемой переменной

Чтобы принудительно заблокировать/разблокировать управляемую переменную необходимо:

– в списке управляемых переменных выбрать переменную, установив галочку в чекбоксе для доступа к списку быстрых действий.

ПРИМЕЧАНИЕ. Принудительно заблокировать или разблокировать можно только одну управляемую переменную за раз;

– для сброса выделения необходимо нажать кнопку «Сбросить выделение»;

– в списке быстрых действий выбрать значок «Разблокировать переменную» или «Заблокировать переменную»;

– в отобразившемся окне подтверждения операции выбрать кнопку «Заблокировать»/«Разблокировать» либо отменить действия, нажав кнопку «Отмена».

В результате переменная будет заблокирована/разблокирована.

ВНИМАНИЕ! При принудительной или автоматической блокировке управляемой переменной ППО выключает срок жизни и сбрасывает количество заданных дней.

4.1.9. Экспорт/Импорт

4.1.9.1. Экспорт данных в формате JSON

Экспорт позволяет выгрузить данные из ППО в формате `.json` для дальнейшего переноса этой информации на другой инстанс (стенд) ППО.

ПРИМЕЧАНИЕ. Данный функционал доступен только для учетных записей с ролью «Администратор Платформы Управления».

ВНИМАНИЕ! Экспортируется только последняя загруженная в ППО версия каждого файла и каждой папки из git-репозиториев.

Чтобы экспортировать данные из ППО необходимо:

– нажать на «Экспортировать данные в формате JSON»;

– выбрать нужные данные для экспорта, установив галочку в чекбоксе:

- группы устройств;
- группы пользователей;
- файлы и папки из git-репозиториев;

– нажать на кнопку «Экспорт».

В результате начнется процесс экспорта, который может занять несколько минут (не закрывать окно до окончания загрузки).

После завершения экспорта:

1) Отобразится сводная информация о том, сколько объектов из каждой сущности были экспортированы;

2) В результате успешного скачивания сформированный файл из экспортированных данных будет скачан на ЭВМ.

4.1.9.2. Импорт данных в формате JSON

Импорт позволяет загрузить данные в ППО, которые ранее были экспортированы, например, из другого инстанса (стенда) ППО. Описание экспорта данных приведено в пп. 4.1.9.1.

ПРИМЕЧАНИЕ. Данный функционал доступен только для учетных записей с ролью «Администратор Платформы Управления».

ВНИМАНИЕ! Если требуется импортировать мета-данные о файлах и папках из git-репозиториев, то сначала необходимо настроить вручную интеграцию со всеми git-репозиториями, откуда были изначально загружены файлы и папки.

Чтобы импортировать данные в ППО из JSON-файла необходимо :

– нажать на «Импортировать данные в формате JSON»;

– перетащить JSON-файл в область загрузки или нажать «Загрузить файл» и выбрать необходимый файл (размер файла не должен превышать 100 МБ).

В результате начнется процесс импорта из JSON-файла, который может занять несколько минут (не закрывать окно до окончания загрузки).

В случае, если:

– в инстансе (стенде) ППО, в котором происходит импорт, будет обнаружена дублирующая информация, то они будут исключены из импорта;

– в импортируемом файле в сущности нет ни одного объекта, то импорт осуществлен не будет.

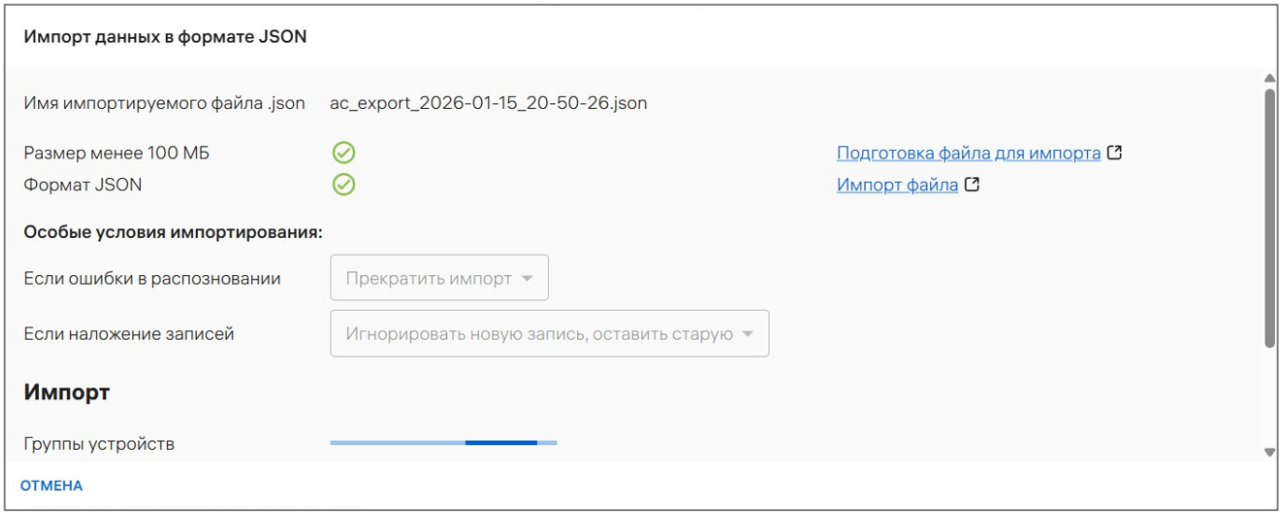


Рисунок 126

После завершения процесса импорта отображается сводная информация (Рисунок 127):

– с каким статусом завершен импорт по каждой сущности;
– количество успешно импортированных объектов по каждой сущности;
– количество обнаруженных ошибок при импорте по каждой сущности;
– файл в формате `.json` по каждой сущности, который содержит обнаруженные ошибки при импорте.

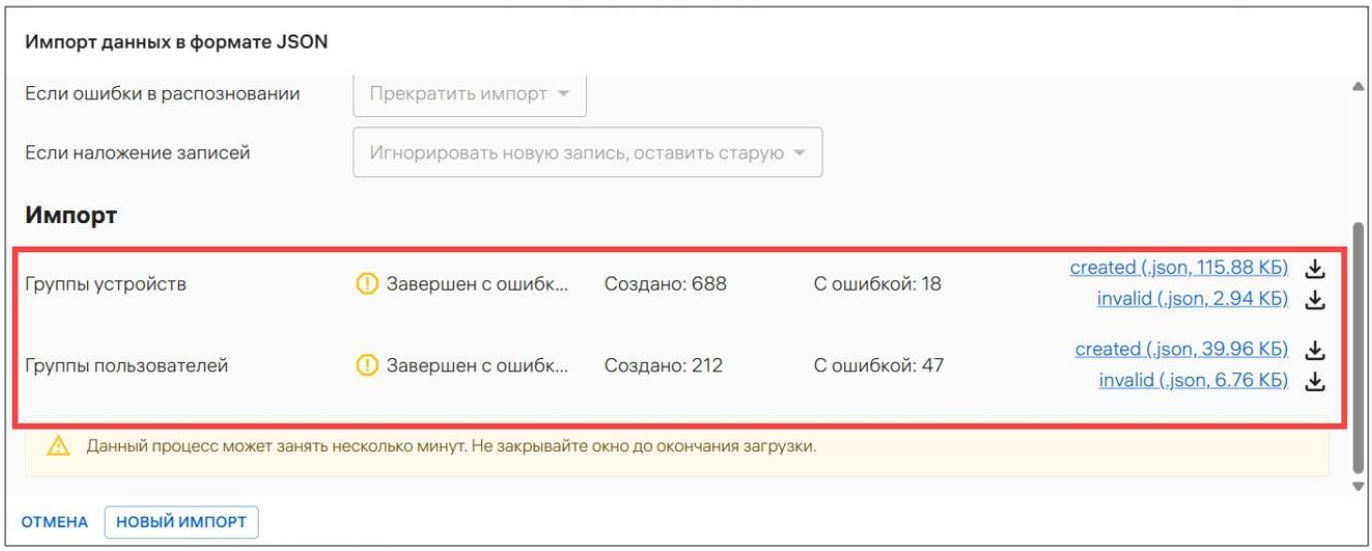


Рисунок 127

4.2. Подраздел «Орг.структура»

Подраздел «Орг.структура» Консоли администратора ПУ предназначен для просмотра организационной структуры компании, а также получения данных с сервера LDAP, с которым установлено соединение (пп. 4.1.5.3), а при отсутствии добавленных данных отображается сообщение «Нет данных». Заполнение подраздела данными производится с помощью импорта из Active Directory (LDAP) напрямую, если ПУ интегрирована с AD организации (пп. 4.1.5.3).

Для перехода в подраздел необходимо в верхней панели выбрать подраздел «Орг.структура» раздела «Администрирование». В результате отобразится основная информация о пользователях (сотрудниках) и о подразделениях пользователей в следующих столбцах:

– «Подразделение/Пользователь» – название группы или ФИО (при наличии) пользователя, представляющее собой активную ссылку, при нажатии на которую откроется карточка группы или пользователя;
– «Тип» – значок типа группы пользователей или пользователя. При наведении курсора появляется всплывающая подсказка с названием типа;
– «Email» – рабочая электронная почта пользователя. Для групп пользователей в этом столбце информация отсутствует;

– «Телефон» – рабочий телефон пользователя. Для групп пользователей в этом столбце информация отсутствует.

Для просмотра организационной структуры компании необходимо нажать значок  в строке с подразделением. В результате раскроется вложенный список (Рисунок 128) либо при его отсутствии отобразится «Нет дочерних элементов».

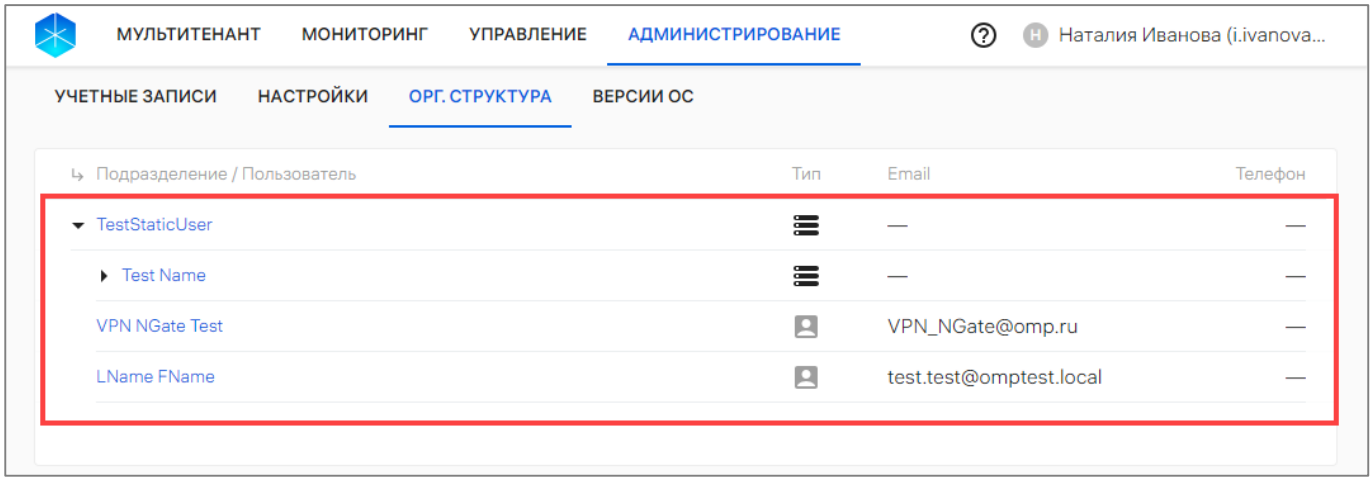


Рисунок 128

5. СООБЩЕНИЯ ОБ ОШИБКАХ И ОГРАНИЧЕНИЯ

5.1. Сообщения об ошибках

В ходе работы с компонентами ПУ пользователям могут выдаваться сообщения об ошибках, приведенные в таблице (Таблица 70).

Таблица 70

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
1	Произошла ошибка. Сообщите о ней системному администратору или смотрите подробности в логах на сервере	Необходимо обратиться к системному администратору или подробная информация в логах на сервере
2	Нет связи с сервером. Попробуйте повторить попытку позже	Необходимо обратиться к системному администратору, администратору LDAP или повторить попытку позже
3	В QR-коде может быть максимум 3 корневых сертификата	Необходимо удалить один из ранее загруженных корневых сертификатов, либо поменять у него свойство «Использовать в QR-коде при активации»
4	Не найдено	Попытка обращения к несуществующему элементу управления. Необходимо закрыть текущую экранную форму, с которой возникает ошибка
5	Для данной учетной записи доступ запрещен	У учетной записи пользователя нет необходимых прав доступа для просмотра выбранной страницы. Для назначения прав необходимо обратиться к администратору учетных записей
6	Истекло время действия активной сессии. Обновите страницу	Авторизованная сессия завершена. Необходимо обновить страницу браузера

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
7	Истек срок действия загруженного Вами QR-кода. Загрузите другой или сгенерируйте новый	Загружен JSON-файл с истекшем сроком действия (`expiredAt`). Необходимо загрузить JSON-файл с актуальным сроком действия
8	Произошла ошибка на стороне сервера. Сообщите о ней системному администратору или смотрите подробности в логах на сервере	Необходимо обратиться к системному администратору
9	Не удалось считать данные из JSON. Попробуйте другой JSON-файл или исправьте этот	Загрузка некорректного JSON-файла. Необходимо поверить корректность загружаемого файла
10	Не выбрано ни одного устройства для активации	При генерации QR-кода для группы устройств выбрана пустая группа. Необходимо выбрать группу, содержащую хотя бы 1 устройство
11	Загружен JSON-файл с параметрами активации, отличными от параметров текущей конфигурации	Необходимо сверить параметры JSON-файла с конфигурацией. Данная ошибка возникает при несоответствии конфигурации системы одному из значений: – `accountDomain`; – `gatewayURI`; – `clientID`
12	Группа с таким именем уже существует в системе	Попытаться создать группу устройств с существующим наименованием. Необходимо изменить значение в поле «Наименование»
13	Динамическая группа с такими условиями уже существует в системе	Необходимо заменить условия добавления в динамическую группу устройств/пользователей
14	Устройство с таким MAC WLAN уже есть в системе	Необходимо проверить корректность заполненных данных в CSV-файле
15	Устройство с таким IMEI уже есть в системе	Необходимо проверить корректность заполненных данных в файле
16	Устройство с таким Серийным номером уже есть в системе	Необходимо использовать существующее устройство

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
17	Устройство с таким Ethernet MAC уже есть в системе	Необходимо использовать существующее устройство
18	Данное устройство было удалено из системы	Необходимо обратиться к администратору
19	Нельзя удалить группу, созданную в Active Directory	Невозможно удалить группу, созданную в Active Directory
20	Нельзя удалить непустую группу	Попытка удалить группу с назначенными устройствами или пользователями. Необходимо исключить все дочерние элементы из группы, затем произвести удаление
21	В JSON-файле не указан ID активации (`enrollmentID`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным `enrollmentID`
22	В JSON-файле не указан пароль (`password`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным паролем
23	В JSON-файле не указан адрес активации (`gatewayURI`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с корректным адресом сервера активации
24	В JSON-файле не указан срок истечения (`expiredAt`)	Загружен некорректно заполненный файл активации. Необходимо загрузить файл с актуальным сроком действия
25	Импорт уже запущен. Дождитесь окончания процесса	Повторная попытка запуска импорта из LDAP при ранее запущенном импорте. Необходимо дождаться завершения выполнения импорта
26	Не удалось создать офлайн-сценарий. Вызов по этому событию уже существует	Попытка создания сценария с существующим событием. Необходимо использовать имеющийся сценарий либо выбрать другое событие
27	Не удалось создать офлайн-сценарий. Сообщите об этой ошибке администратору	Попытка создания сценария с невалидными параметрами. Необходимо обратиться к администратору

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
28	Корпоративный шаблон уже создан	Предусмотрена возможность создания только 1 корпоративного шаблона. Необходимо использовать шаблон, имеющийся в системе
29	Пользователь с указанным Email уже существует	Попытаться создать пользователя с существующим Email. Необходимо проверить корректность заполнения поля «Email»
30	Динамическая группа с такими условиями уже существует в системе	Попытаться создать динамическую группу с аналогичными условиями
31	Не удалось создать офлайн-сценарий. Пара событие/реакция уже существует	Офлайн-сценарий с заданными событием и реакцией существуют в системе. Необходимо удалить существующий сценарий перед созданием нового либо использовать существующий
32	Редактирование динамических групп не допускается	Динамическая группа не подлежит редактированию
33	Проверьте корректность заполнения правил	Необходимо проверить корректность заполнения правил
34	Политика с таким именем уже существует в системе	Попытка создать политику с существующим наименованием. Необходимо изменить значение в поле «Наименование»
35	Проверьте корректность заполнения названия политики	Попытка создать политику с пустым наименованием. Необходимо заполнить поле «Наименование»
36	В версиях не допускается использование букв кириллицы	При попытке ввести в диапазонах версиях буквы кириллицы
37	Допускается от 1 до 100 символов	При попытке ввести код приложения, которые превышают 100 символов
38	Файл не содержит данных. Убедитесь, что выбран нужный файл	Необходимо загрузить файл с заполненными данными
39	Неверный формат идентификатора записи (GUID)	Необходиом проверить корректность идентификаторов в загружаемом файле

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
40	Некорректный формат файла	Загружен файл в формате, отличном от `.ldif` или `.csv` необходимо импортировать файлы в указанных форматах
41	Ошибка при разборе файла. Убедитесь, что выбран нужный файл	Необходимо проверить корректность заполненных данных в файле
42	Некорректная структура файла. Проверьте файл на соответствие шаблону	Необходимо сверить заполненный CSV-файл с установленным шаблоном
43	Ошибка импорта устройства. В системе найдено устройство по одному из идентификаторов (IMEI или WLAN MAC), но второй идентификатор не совпадает. Найдите устройство в системе и проверьте указанные в файле данные на соответствие	Необходимо найти устройство в системе и проверить указанные в файле данные на соответствие
44	Ошибка валидации заголовка. Указаны некорректные названия колонок. Правильные названия колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта
45	Ошибка валидации заголовка. Указаны не все колонки. Количество колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта. Количество колонок необходимо взять из шаблона
46	Ошибка валидации заголовка. Неправильный порядок колонок. Правильный порядок колонок необходимо взять из шаблона	Необходимо проверить корректность заполнения заголовка CSV-файла для импорта. Правильный порядок колонок необходимо взять из шаблона
47	Некорректный статус устройства в системе	Необходимо обратиться к администратору

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
48	Не удалось создать QR-коды	Необходимо повторить попытку позже или обратиться к системному администратору
49	Удаленные устройства привязать к группе не удалось	Дополнительно не предусмотрено выполнение каких-либо действий. Все устройства кроме архивных успешно привязались к группе
50	HTTP ERROR 400	Необходимо очистить кэш и cookies веб-браузера и повторить запрос. В случае повторения ошибки следует обратиться к администратору
51	Не корректный ID согласующего	Указать корректное значение
52	Запрещенный ID согласующего	Указать корректное значение
53	Повторное согласование версии одним и тем же пользователем	Указать корректное значение
54	Не корректный ID файла	Указать корректное значение
55	Не корректный ID версии	Указать корректное значение
56	Значение параметра key превышает количество допустимых символов	Указать корректное значение
57	Значение параметра value превышает количество допустимых символов	Указать корректное значение
58	Значение параметра comment превышает количество допустимых символов	Указать корректное значение
59	Значение параметра key содержит недопустимые к использованию символы	Указать корректное значение
60	Значение защищенной управляемой переменной имеет недопустимую длину	Указать корректное значение
61	Правило управления скриптами имеет дублирующийся ключ скрипта	Указать корректное значение

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
62	Версия управляемой переменной является невалидной	Указать корректное значение
63	Новая добавляемая управляемая переменная является заблокированной	Указать корректное значение
64	Ошибка при изменении защищенной управляемой переменной на защищенную	Указать корректное значение
65	Заблокированную управляемую переменную невозможно изменить	Указать корректное значение
66	Срок жизни управляемых переменных должен составлять от 1 часа до 365 дней.	Указать корректное значение
67	Такой путь на устройстве уже есть в правиле	Указать корректное значение
68	Превышено количество допустим символов	Указать корректное значение
69	Введенные атрибуты являются невалидными	Указать корректное значение
70	Неподдерживаемая версия импортируемых данных по группам устройств	Указать корректное значение
71	Массив данных по группам устройств не содержит ни одного объекта	Указать корректное значение
72	Импортируемая группа устройств с таким же значением LDAP ID уже содержится в системе	Указать корректное значение
73	Массив данных по группам пользователей не содержит ни одного объекта	Указать корректное значение
74	Неподдерживаемая версия импортируемых данных по группам пользователей	Указать корректное значение

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
75	Параметр parentID не найден в одном из объектов импортируемого usersGroup	Указать корректное значение
76	Импортируемая группа пользователей с таким же значением LDAP ID уже содержится в системе	Указать корректное значение
77	Массив данных по файлам/папкам из git-репозитория \nне содержит ни одного объекта	Указать корректное значение
78	Не удалось распарсить ID файла	Указать корректное значение
79	Не удалось распарсить ID папки	Указать корректное значение
80	Импортируемый файл не из git-репозитория	Указать корректное значение
81	Импортируемая папка не из git-репозитория	Указать корректное значение
82	Импортируемый файл из git-репозитория не содержит версию	Указать корректное значение
83	Операция с архивной политикой запрещена	Обратиться к системному администратору
84	Интеграция с центром сертификации уже существует	Необходимо использовать существующую интеграцию с центром сертификации или добавить новую с другим центром сертификации
85	Название пусто или больше 256 символов	Необходимо ввести название, содержащее от 1 до 256 символов
86	Проверка формата URL не пройдена	Необходимо ввести электронный адрес в формате URL. Например: `https://www.omp.ru/`
87	Неподдерживаемый тип сервера	Необходимо указать тип сервера Microsoft Active Directory Certificate Services (AD CS), т.к. Аврора Центр поддерживает интеграцию с центрами сертификации, имеющим данный тип сервера
88	Логин пуст или больше 256 символов	Необходимо ввести логин, содержащий от 1 до 256 символов
89	Пароль пусто или больше 256 символов	Необходимо ввести пароль, содержащий от 1 до 256 символов

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
90	Ошибка при обработке полученных данных	Необходимо обратиться к системному администратору, администратору LDAP или повторить попытку позднее
91	Не удалось удалить настройки интеграции	Необходимо обновить страницу и повторить попытку или обратиться к системному администратору
92	Ошибка сохранения настроек интеграции	Необходимо обратиться к системному администратору, администратору LDAP или повторить попытку позднее
93	Подключение недоступно	Необходимо нажать «Подробнее», чтобы посмотреть полный текст ошибки (пп. 4.1.5.3.1.1). Обратиться к системному администратору, администратору LDAP или повторить попытку позднее
94	Неверное название территории при создании	Ввести название, содержащее от 1 до 256 символов
95	Неверное количество полигонов при создании территории	Ввести хотя бы один полигон для территории. Количество полигонов не должно превышать 50
96	Неверный идентификатор территории	Обратиться к системному администратору
97	Неверные параметры запроса тайла карты	Обратиться к системному администратору
98	Неверный масштаб запроса тайла карты	Обратиться к системному администратору
99	Ошибка получения тайла карты из источника	Обратиться к системному администратору
100	Тайл карты не найден	Обратиться к системному администратору
101	Название файла не должно быть пустым	Добавить файл с названием не больше 255 символов
102	В названии файла должно быть не больше 255 символов	Добавьте файл с названием не больше 255 символов
103	В названии файла должны быть только буквы, цифры и спецсимволы "-", ".", "_", а также пробелы	Добавить файл, в названии которого только буквы, цифры и спецсимволы "-", ".", "_", а также пробелы
104	Файл с таким именем уже существует в системе	Добавить файл с другим именем

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
105	Папка содержит файлы с пустым содержимым	Добавить файл с содержанием
106	Файл не может быть удален из хранилища	Обратиться к системному администратору
107	Файл не может быть удален, т.к. используется в политике	Удалить файл из политики
108	GIT-репозиторий с таким параметром remote не найден	Проверить правильность введенного адреса до удаленного git-репозитория по протоколу ssh
109	GIT-репозиторий недоступен для аутентификации	Обратиться к системному администратору, администратору git-репозитория или повторить попытку позднее
110	Ошибка при валидации длины параметра remote	Обратиться к системному администратору
111	Ошибка при валидации допустимых символов параметра remote	Обратиться к системному администратору
112	Ошибка при валидации допустимых значений параметра branch	Обратиться к системному администратору
113	Ошибка при валидации допустимых значений параметра sshKeyID	Обратиться к системному администратору
114	Пара SSH-ключей с таким ID не найдена. Генерация пары SSH-ключей не завершена до конца. Указанный файл не найден	Обратиться к системному администратору и повторить попытку позднее
115	Пара SSH-ключей с таким ID уже используется	Перегенерировать пару SSH-ключей, обновив страницу
116	GIT-репозиторий с таким параметром remote уже существует	Удалить интеграцию с существующим git-репозиторием или создать интеграцию с другим git-репозиторием
117	Ошибка при валидации стратегии архивации LDAP-ных устройств	Обратиться к системному администратору и повторить попытку позднее

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
118	Переменная с таким именем уже существует в системе	Необходимо добавить переменную с другим именем
119	Отсутствует содержимое файла	Повторить попытку выгрузки файла с устройства
120	Несоответствие хэш суммы	Повторить попытку выгрузки файла с устройства
121	Файл не найден	Повторить попытку выгрузки файла с устройства
122	Не валидный ID файла	Необходимо проверить правильность ID файла
123	Не валидный ID устройства	Необходимо проверить правильность ID устройства
124	Такая папка из git-репозитория не найдена	Обратиться к системному администратору
125	Версия папки не была найдена	Обратиться к системному администратору
126	Папка не может быть удалена т.к. файл из папки используется в политике	Обратиться к системному администратору
127	Папка с таким именем уже существует. Если хотите добавить версию папки, перейдите в карточку папки - название папки с гиперссылкой	Для добавления версии папки перейти в карточку папки
128	Путь папки пересекается с существующими папками в системе	Обратиться к системному администратору
129	Файл с таким именем принадлежит папке	Обратиться к системному администратору
130	Не обрабатываем такую ошибку, т.к. первее возникает ошибка выше	Обратиться к системному администратору
131	Не обрабатываем такую ошибку, т.к. у пользователя кнопка для удаления всего файла залочена	Обратиться к системному администратору
132	Запрет удаления последней версии	Обратиться к системному администратору
133	Папка используется в политике	Обратиться к системному администратору

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
134	Версия папки уже удалена	Обратиться к системному администратору
135	Указанная папка не найдена	Обратиться к системному администратору
136	Папка не должна быть пустой	Обратиться к системному администратору
137	Не удалось получить информацию по указанной папке	Обратиться к системному администратору
138	Версия папки с таким содержимым уже существует в системе	Обратиться к системному администратору
139	Невозможно изменить модель устройства: используется в динамических группах	Обратиться к системному администратору
140	Модель устройства с таким названием уже существует	Необходимо ввести уникальное название модели и повторить попытку
141	Модель устройства уже существует	Необходимо ввести уникальную модель и повторить попытку
142	Не обнаружена интеграция с git-репозиторием для импортируемых файлов/папок	Необходимо настроить интеграцию(-и) с git-репозиторием(-ями) и повторить импорт
143	Ветка настроенной интеграции с git-репозиторием отличается от ветки git-репозитория импортируемых файлов/папок	Обратиться к системному администратору
144	Невозможно импортировать файл, поскольку отсутствует папка к которой привязан этот файл	Обратиться к системному администратору
145	Неподдерживаемая версия импортируемых данных по файлам и папкам из git-репозитория	Обратиться к системному администратору
146	Не удалось удалить множество, снимите назначенные на него политики и сценарии и попробуйте снова	Обратиться к системному администратору

№ п/п	Ошибка/текст ошибки в интерфейсе	Действия для устранения
147	Нельзя удалить группу, которая используется в множестве. Измените состав множества и повторите попытку	Обратиться к системному администратору
148	Множество с таким именем уже существует в системе	Обратиться к системному администратору
149	Не указаны заявки на активацию	Обратиться к системному администратору
150	Некорректная стратегия заявки на активацию	Обратиться к системному администратору
151	Некорректный ID заявки на активацию	Обратиться к системному администратору
152	В заявке на активацию есть конфликт по пересечению идентификаторов	Обратиться к системному администратору
153	Попытка привязать устройство с пустым deviceID	Обратиться к системному администратору
154	Устройство не найдено	Обратиться к системному администратору
155	Не осталось ни одного уникального идентификатора	Обратиться к системному администратору
156	Такое сетевое имя уже используется	Обратиться к системному администратору
157	Попытка привязать устройство с другим сетевым именем к устройству из LDAP	Обратиться к системному администратору
158	Попытка привязать устройство без сетевого имени к устройству из LDAP	Обратиться к системному администратору

5.2. Ошибки импорта

5.2.1. Ошибки импорта устройств

Импорт устройств из CSV-файла может проходить с ошибками, описание которых приведено в таблице (Таблица 71).

Таблица 71

№ п/п	Текст ошибки	Действие для устранения ошибки
1	Модель устройства (MODEL_CODE). Ошибка валидации значения. Указанное значение не соответствует названию модели устройства в системе. Ознакомиться с корректными названиями моделей устройств можно в справке об импорте или в справочнике моделей при создании устройства	Указать корректное значение
2	Платформа (PLATFORM). Ошибка валидации значения. Указанное значение не соответствует названию платформы в системе. Ознакомиться с корректными названиями платформ можно в справке об импорте или в предложенном списке платформ при создании устройства	Указать корректное значение
3	Ошибка привязки устройства к группе. Указанная в файле группа является динамической группой в системе. К динамической группе нельзя привязывать устройства. Укажите другое название группы в файле	Указать другое название группы в файле
4	Группа (GROUP). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
5	Ошибка импорта группы. Группа с таким названием была помещена в архив. Восстановить ее невозможно, поэтому необходимо использовать другое название группы	Указать другое название группы в файле
6	IMEI. Ошибка валидации значения. IMEI необходимо переписать из параметров устройства	Указать корректное значение
7	SN. Ошибка валидации значения. SN необходимо переписать из параметров устройства	Указать корректное значение

№ п/п	Текст ошибки	Действие для устранения ошибки
8	Ethernet MAC. Ошибка валидации значения. Ethernet необходимо переписать из параметров устройства	Указать корректное значение
9	WLAN MAC. Ошибка валидации значения. WLAN MAC необходимо переписать из параметров устройства	Указать корректное значение
10	Ошибка импорта устройства. Устройство с таким идентификатором было помещено в архив. Необходимо найти его в архиве и восстановить	Найти устройство в архиве и восстановить
11	Ошибка импорта устройства. В системе найдено устройство по одному из идентификаторов, но другие идентификаторы не совпадают. Найдите устройство в системе и проверьте указанные в файле данные на соответствие	Найти устройство в системе и проверить на соответствие указанных в файле данных
12	Ошибка валидации строки. Система не смогла распознать содержимое строки. Проверьте корректность заполнения данных, воспользовавшись рекомендациями в справке об импорте	Проверить корректность заполнения данных (пп. 2.2.3.1, пп. 2.3.3.1)
13	Ошибка импорта. Загружен пустой CSV файл. Файл должен быть заполнен данными	Заполнить файл данными
14	Ошибка импорта устройства. Количество значений в строке не равно количеству колонок в заголовке. Разделители должны соответствовать разделителям первой строки	Необходимо проверить корректность заполненных данных в CSV-файле. Разделители должны соответствовать разделителям первой строки
15	Комментарий (COMMENT). Ошибка валидации значения. Длина должна быть до 512 символов	Длина должна быть до 512 символов
16	Ошибка привязки устройства к группе. Указанная в стратегии импорта группа удалена из системы. Устройство было добавлено в группу, указанную в файле. Если в файле отсутствовала группа, тогда устройство находится в системе без группы	Указать корректную группу
17	Ошибка импорта устройства. Указано слишком много идентификаторов одного типа. Идентификаторов одного типа должно быть не более 10	Указать не более 10 идентификаторов в файле

№ п/п	Текст ошибки	Действие для устранения ошибки
18	Ошибка импорта устройства. Указано слишком много идентификаторов одного типа для существующего устройства. Идентификаторов одного типа должно быть не более 10	Указать не более 10 идентификаторов в файле
19	Ошибка импорта устройства. Указаны дублирующиеся идентификаторы	Исключить дублирующие идентификаторы из файла
20	Стратегия (STRATEGY). Ошибка валидации значения. Тип должен быть SKIP или REPLACE	Указать корректное значение

5.2.2. Ошибки импорта пользователей

Импорт пользователей из CSV-файла может проходить с ошибками, описание которых приведено в таблице (Таблица 72).

Таблица 72

№ п/п	Текст ошибки	Действие для устранения ошибки
1	Ошибка поиска устройства. Указанные данные идентификаторов некорректны, либо по ним не удалось найти устройство	Указать корректное значение или добавить устройство в систему, в случае его отсутствия
2	Имя (FIRST_NAME). Ошибка валидации значения. Имя может содержать: а-я ё a-z A-Я Ё A-Z - ' пробел	Указать корректное значение
3	Фамилия (LAST_NAME). Ошибка валидации значения. Фамилия может содержать: а-я ё a-z A-Я Ё A-Z - ' пробел	Указать корректное значение
4	Отчество (PATRONYMIC). Ошибка валидации значения. Отчество может содержать: а-я ё a-z A-Я Ё A-Z - ' пробел	Указать корректное значение
5	Электронная почта (EMAIL). Ошибка валидации значения. Электронная почта состоит из двух частей (логина пользователя и доменного имени сервера), разделенных символом «@». Пример: example@example.ru	Указать корректное значение

№ п/п	Текст ошибки	Действие для устранения ошибки
6	Должность (JOB_TITLE). Ошибка валидации значения. Должность может содержать: а-я ё a-z A-Я Ё A-Z - пробел	Указать корректное значение
7	Номер телефона (PHONE_NUMBER). Ошибка валидации значения. Номер телефона должен состоять из цифр	Указать корректное значение
8	Имя (FIRST_NAME). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
9	Фамилия (LAST_NAME). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
10	Отчество (PATRONYMIC). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
11	Электронная почта (EMAIL). Ошибка валидации значения. Длина должна быть от 1 до 256 символов	Длина должна быть от 1 до 256 символов
12	Должность (JOB_TITLE). Ошибка валидации значения. Длина должна быть от 2 до 256 символов	Длина должна быть от 2 до 256 символов
13	Номер телефона (PHONE_NUMBER). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
14	Группа (GROUP). Ошибка валидации значения. Длина должна быть от 2 до 64 символов	Длина должна быть от 2 до 64 символов
15	WLAN MAC. Ошибка валидации значения. WLAN MAC необходимо переписать из параметров устройства	Указать корректное значение
16	IMEI. Ошибка валидации значения. IMEI необходимо переписать из параметров устройства	Указать корректное значение
17	Ethernet MAC. Ошибка валидации значения. Ethernet необходимо переписать из параметров устройства	Указать корректное значение

№ п/п	Текст ошибки	Действие для устранения ошибки
18	SN. Ошибка валидации значения. SN необходимо переписать из параметров устройства	Указать корректное значение
19	Ошибка импорта. Загружен пустой CSV файл. Файл должен быть заполнен данными	Заполнить файл данными
20	Ошибка импорта. Файл содержит только заголовок. Файл должен быть заполнен данными	Заполнить файл данными
21	Ошибка импорта пользователя. Количество значений в строке не равно количеству колонок в заголовке. Разделители должны соответствовать разделителям первой строки	Разделители должны соответствовать разделителям первой строки
22	Ошибка импорта пользователя. Пользователь получен из LDAP, изменение его данных недоступно. Для продолжения импорта удалите данную строку из файла	Для продолжения импорта необходимо удалить данную строку из файла
23	Стратегия (STRATEGY). Ошибка валидации значения. Тип должен быть SKIP или REPLACE	Указать корректное значение

5.3. Ограничения

В ходе работы с ПУ могут быть выделены различные ограничения в работе системы, информация о которых приводится в документе «Release Notes», для получения которого необходимо направить запрос на электронную почту info@omp.ru.

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 73).

Таблица 73

Термин/ Сокращение	Расшифровка
ОС	Операционная система
Офлайн-сценарий	Правило, которое отправляется с указанием события срабатывания на устройства и должно «мгновенно» примениться по этому событию (в том числе, если в этот момент нет связи с сервером)
ПБ	Подсистема безопасности
ПМ	Подсистема «Маркет»
ПО	Программное обеспечение
ПООС	Подсистема обновления ОС
ППО	Прикладное программное обеспечение «Аврора Центр»
Приложение	Приложением является: – мобильное приложение, функционирующее под управлением ОС Аврора/ОС Android; – приложение для ЭВМ, функционирующей под управлением ОС семейства Linux
ПУ	Подсистема Платформа управления
РТК-Феникс	Доверенный репозиторий, обеспечивающий возможность применения безопасных библиотек свободного ПО в проектах разработки ПО. Разработан ООО «РТК ИТ»
СУ	Сервис уведомлений
Устройство	Под устройством подразумевается мобильное устройство и/или ЭВМ, на которой функционируют соответствующие компоненты ППО
Чекбокс	Элемент управления, предоставляющий возможность осуществить выбор, а также вызвать список быстрых действий
ЭВМ	Электронно-вычислительная машина
Bluetooth®	Стандарт беспроводной связи, обеспечивающий обмен данными между устройствами на основе ультракоротких радиоволн
BSSID	Basic Service Set Id – 48-битный идентификационный номер в беспроводных сетях стандарта IEEE 802.11

Термин/ Сокращение	Расшифровка
CSV	Comma-Separated Values – текстовый формат, предназначенный для представления табличных данных
Fingerprint	Цифровой отпечаток (информация, собранная об удаленном устройстве для дальнейшей идентификации)
HTTP	HyperText Transfer Protocol – протокол прикладного уровня передачи данных (изначально – в виде гипертекстовых документов). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом
IMEI	Уникальный номер устройства, состоящий из 15 цифр
JSON	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
MTP	Media Transfer Protocol – основанный на PTP аппаратно-независимый протокол, разработанный компанией Microsoft для подключения цифровых плееров к ЭВМ
Push-уведомления	Текстовые сообщения, предназначенные для оперативной (мгновенной) доставки на устройство пользователей
QR-код	Quick response code – код быстрого реагирования, матричный код (двумерный штрихкод)
SSID	Service Set Identifier – символьное название беспроводной точки доступа Wi-Fi, служащее для идентификации ее среди других точек пользователями или устройствами, подключающимися к сети
WLAN	Wireless Local Area Network – локальная сеть, построенная на основе беспроводных технологий

ПРИЛОЖЕНИЕ 1

Описание используемых значков

Значок	Описание
Модель устройства	
	– смартфон Аврора; – защищенный смартфон Аврора
	– планшет Аврора; – защищенный планшет Аврора
	– смартфон Android; – защищенный смартфон Android
	– планшет Android; – защищенный планшет Android
	Неизвестная модель устройства Android
	КПК Аврора
	КПК Android
	ПК Linux
	Неизвестная модель устройства Аврора
	Неизвестная модель устройства Android
	Неизвестная модель устройства Linux
Тип группы устройств	
	Динамическая группа. **ПРИМЕЧАНИЕ.** Группа, в которую устройства добавляются автоматически согласно выбранному алгоритму добавления
	Статическая группа
Тип пользователя	
	Пользователь. **ПРИМЕЧАНИЕ.** Добавляется в ПУ вручную или с помощью импорта CSV-файла
	Пользователь из орг.подразделения. **ПРИМЕЧАНИЕ.** Пользователь, полученный из LDAP
Тип группы пользователей	
	Группа пользователей. **ПРИМЕЧАНИЕ.** Создается вручную или с помощью импорта CSV-файла
	Группа безопасности
	Организационное подразделение. **ПРИМЕЧАНИЕ.** Группа пользователей, полученная из LDAP
	Динамическая группа. **ПРИМЕЧАНИЕ.** Группа пользователей, полученная по дополнительным атрибутам из LDAP

Значок	Описание
Статус жизненного цикла	
	Зарегистрировано. **ПРИМЕЧАНИЕ.** Устройство, добавленное в ПУ
	В процессе активации. **ПРИМЕЧАНИЕ.** Сгенерирован QR-код для устройств
	Активировано. **ПРИМЕЧАНИЕ.** Устройство активировано
	Очищено. **ПРИМЕЧАНИЕ.** Устройство очищено (сброшено к заводским настройкам)
	Архивное. **ПРИМЕЧАНИЕ.** Устройство архивировано (удалено)
	Давно не подключалось. **ПРИМЕЧАНИЕ.** Устройство не подключалось к ППО в течение времени, большего, чем задано в настройках
Соответствие назначенной политике	
	Соответствует политике. **ПРИМЕЧАНИЕ.** Устройство активировано и соответствует назначенным политикам
	Не соответствует политике. **ПРИМЕЧАНИЕ.** Устройство активировано и не соответствует хотя бы 1 назначенной политике
	Не управляется. **ПРИМЕЧАНИЕ.** Устройство не управляется ПУ
	Управление политиками доступно только для активированных устройств
Тип сообщения о событии	
	Информационное
	Предупреждение
	Критическое
	Отладочное

ПРИЛОЖЕНИЕ 2

Рекомендации по конвертации CSV-файла в книгу Excel

Для успешной конвертации экспортированного CSV-файла (п. 2.2.7) в книгу Excel необходимо выполнить следующие действия:

– открыть CSV-файл с помощью MS Excel;

– перейти во вкладку «Данные» (Рисунок 2.1);

– на панели инструментов выбрать «Получить данные»;

– в раскрывающемся списке выбрать «Из файла», далее «Из текстового/ CSV-файла»;

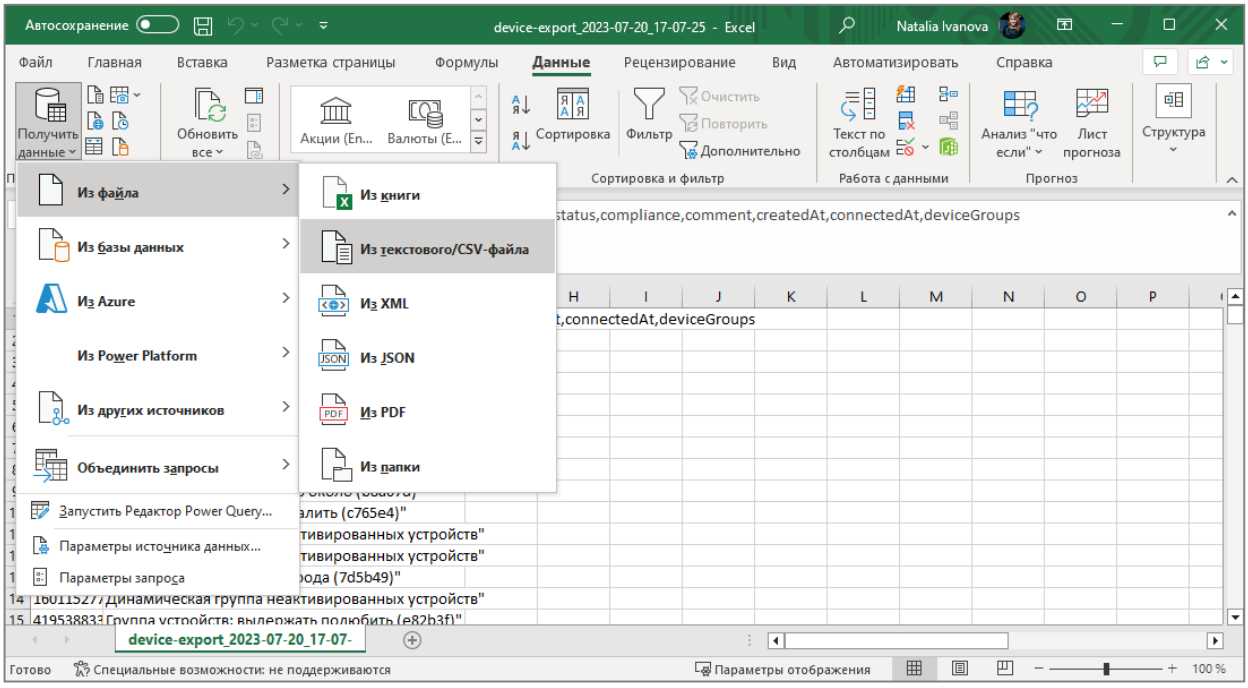


Рисунок 2.1

– выбрать файл экспорта и нажать кнопку «Импорт» (Рисунок 2.2);

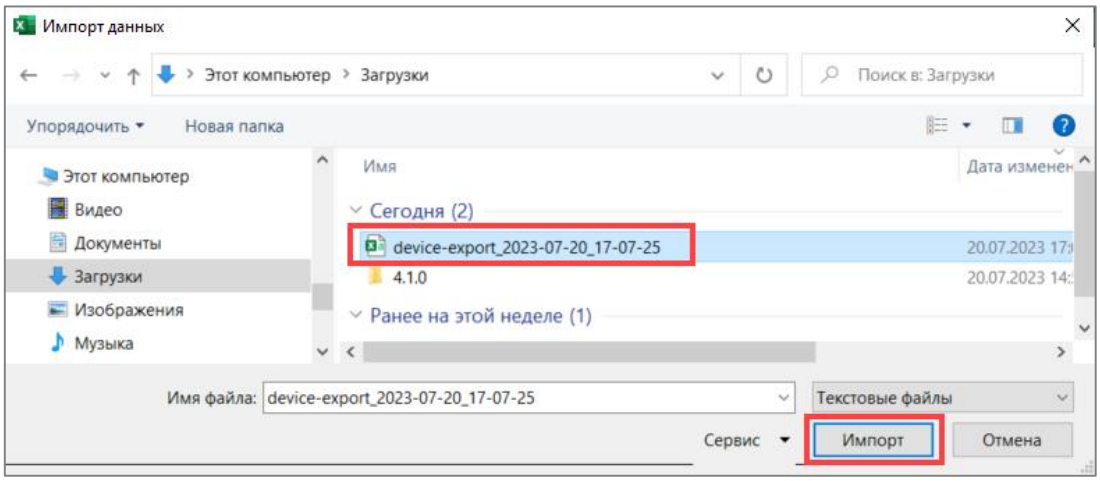


Рисунок 2.2

– убедиться, что в поле «Разделитель» выбрано значение «Запятая», и нажать на кнопку «Преобразовать данные» (Рисунок 2.3);

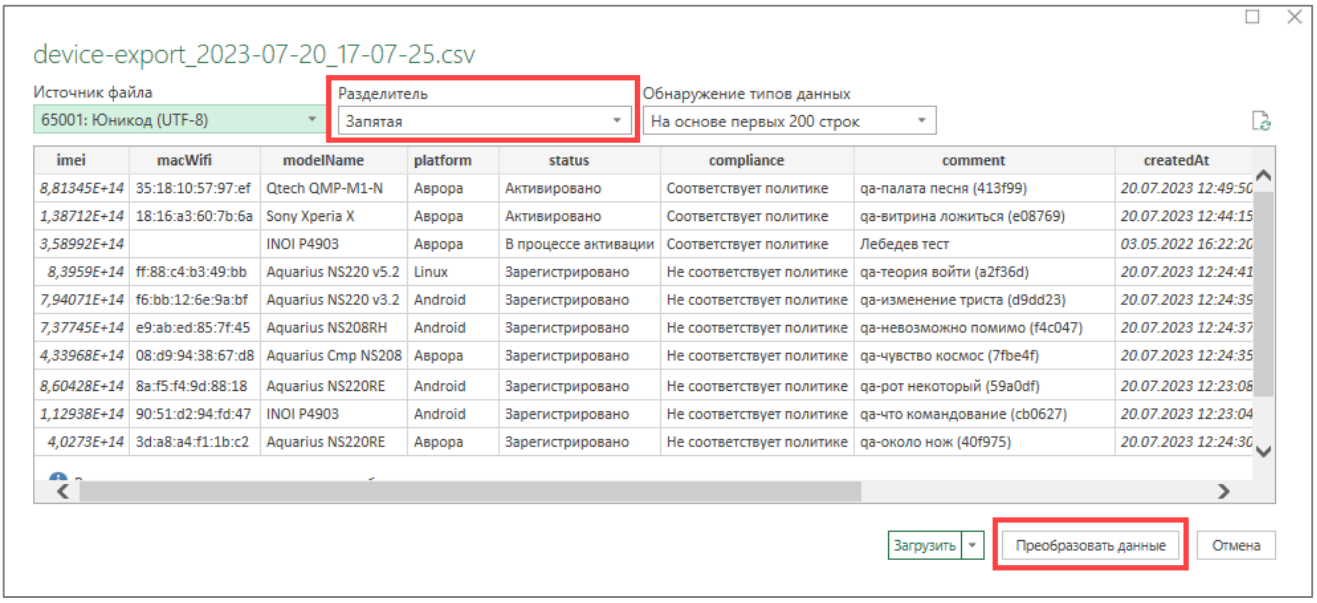


Рисунок 2.3

– убедиться, что в столбце «deviceGroups» отображаются связки групп (группы, перечисленные через точку с запятой) (Рисунок 2.4);

– нажать «Закрыть и загрузить».

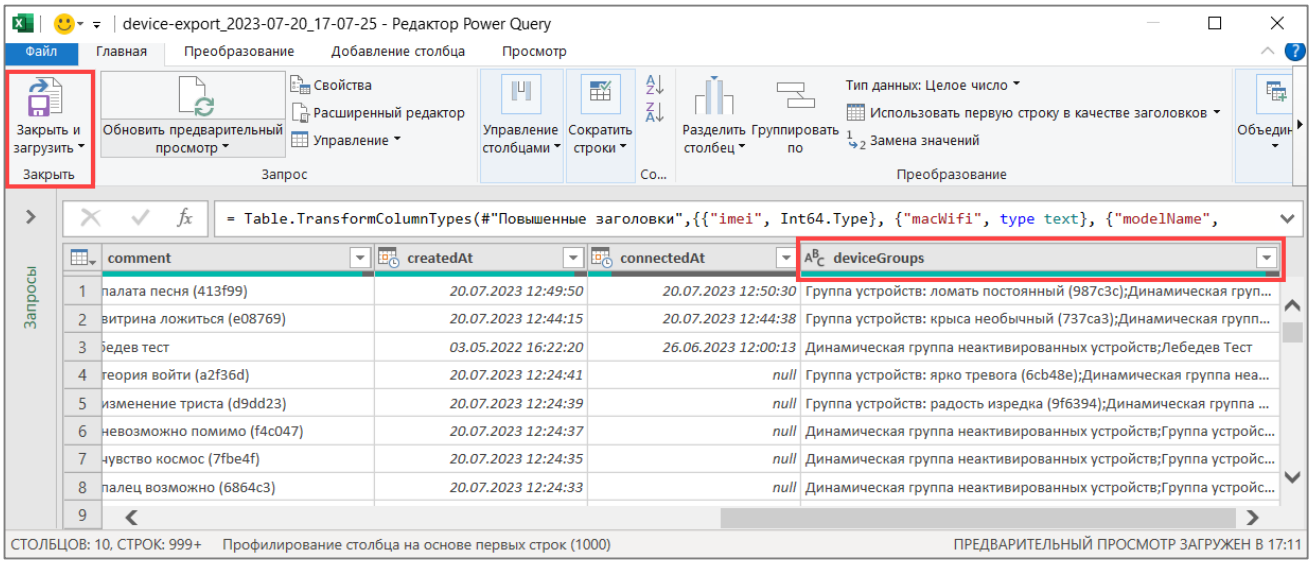


Рисунок 2.4

В результате отобразится книга Excel, сконвертированная из CSV-файла экспорта.

Если необходимо отфильтровать устройства по группе, то необходимо:

– нажать на значок фильтра справа от названия столбца (Рисунок 2.5 [1]);

– ввести название группы;

– выбрать все результаты, содержащие название группы (Рисунок 2.5 [2]);

– нажать кнопку «ОК» (Рисунок 2.5 [3]).

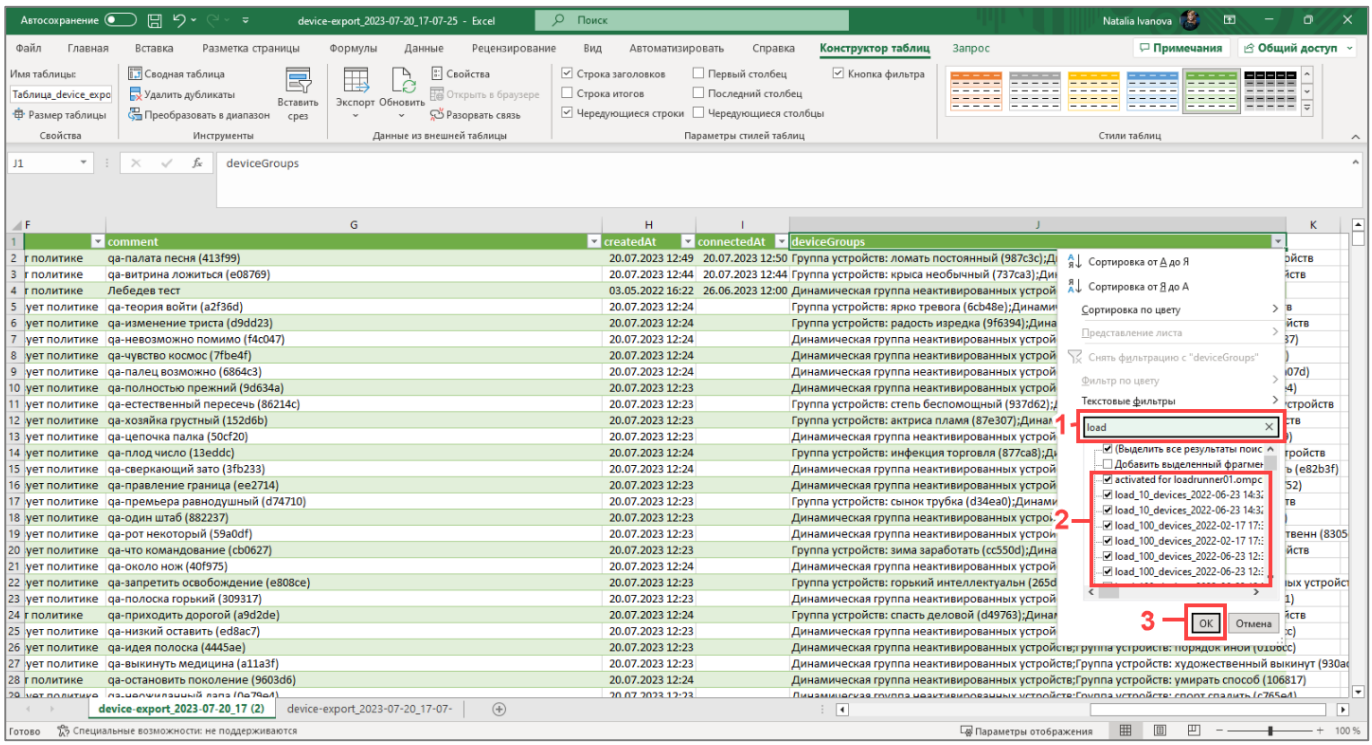

device-export_2023-07-20_17-07-25 - Excel
Natalia Ivanova
Конструктор таблиц
deviceGroups
comment
createdAt
connectedAt
deviceGroups
Сортировка от А до Я
Сортировка от Я до А
Сортировка по цвету
Представление листа
Снять фильтрацию с "deviceGroups"
Фильтр по цвету
Текстовые фильтры
load
1
2
3
OK
Отмена
device-export_2023-07-20_17 (2)
device-export_2023-07-20_17-07-

Рисунок 2.5

ПРИЛОЖЕНИЕ 3

Особенности выполнения скриптов на устройстве

Чтобы скрипт запустился, он должен обязательно иметь shebang и кодировку ASCII.

Для ОС семейства Linux скрипт запускается как исполняемый файл (равносильно вызову `./script.sh`).

Для ОС Android скрипт запускается через интерпретатор. Например, если в shebang указана строка `#!/usr/bin/env sh`, то полная команда запуска будет выглядеть:

```
/usr/bin/env sh script.sh
```

Для ОС семейства Linux скрипты запускаются с правами суперпользователя (root).

Для ОС Android скрипты запускаются с правами текущего (непривилегированного) пользователя.

Скрипты позволяют вернуть произвольный результат выполнения в виде строки, которая отобразится в состоянии карточки устройства. Этот результат можно использовать для формирования динамических групп.

Чтобы вернуть результат из скрипта, необходимо записать строку в файл, путь до которого передается в переменной окружения:

```
__OMP_SCRIPT_RESULT_FILE__.
```

ПРИМЕЧАНИЕ. Из файла считывается не более 64 ASCII-символов.

Пример скрипта на Bash для ОС семейства Linux:

```
#!/usr/bin/env sh
echo -n "Hello world!" > "${__OMP_SCRIPT_RESULT_FILE__}"
```

где:

– -n убирает \n в конце строки;

– кавычки и фигурные скобки вокруг имени переменной предотвращают ошибку `ambiguous redirect`.

Пример скрипта на Python:

```
#!/usr/bin/env python3
import os
resultFile = open(os.environ["__OMP_SCRIPT_RESULT_FILE__"], "w")
resultFile.write("Hello world!")
resultFile.close()
```

Пример скрипта на Bash для ОС Android:

```
#!/system/bin/env sh
echo -n "Hello world!" > "${__OMP_SCRIPT_RESULT_FILE__}"
```

где: "sh" или "bash" в конце строки по наличию в ОС Android.

Также допустимо использовать в shebang: `#!/usr/bin/env` вместо `#!/system/bin/env` (произойдет автоматическая замена).

ВНИМАНИЕ! ППО позволяет добавлять сторонние файлы или папки в управляемую папку. Если будет выбран исполняемый скрипт из папки в правиле «Скрипты/Выполнение на устройстве» рекомендуется писать скрипт так, чтобы он использовал в качестве зависимостей только те файлы, которые принадлежат управляемой папке, чтобы избежать ошибок.

ПРИЛОЖЕНИЕ 4

Подготовка устройства на базе ОС Android к удаленному подключению

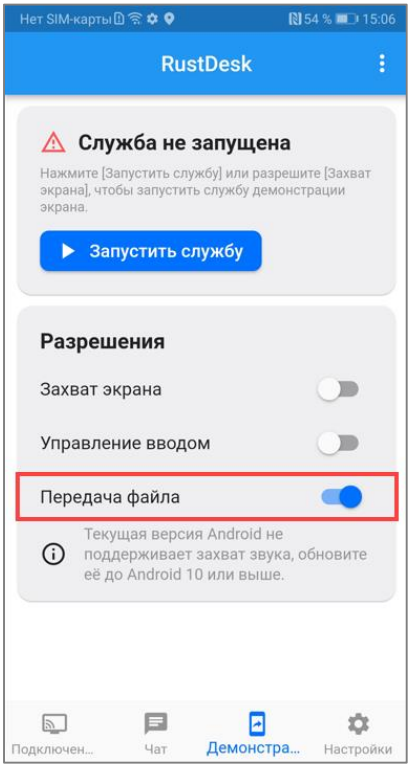


Рисунок 4.1

Для удаленного подключения к рабочему столу устройства необходимо вручную выдать требуемые разрешения приложению RustDesk на устройстве.

Для этого пользователю на устройстве необходимо выполнить следующие действия:

1) Открыть приложение RustDesk;

2) Убедиться, что разрешение на передачу файлов выдано (Рисунок 4.1). Это разрешение выдается автоматически при запуске удаленного подключения из ПУ.

ПРИМЕЧАНИЕ. Если по какой-либо причине (например, из-за особенности некоторых версий ОС Android) это разрешение не выдано, то необходимо:

– перевести переключатель «Передача файла» в положение «Включено»;

– коснуться кнопки «Разрешить», если ОС Android запросит подтверждение;

3) Выдать разрешение на управление вводом. Для этого необходимо:

– перевести переключатель «Управление вводом» в положение «Включено» (Рисунок 4.2);

– перейти в системные настройки (Рисунок 4.3);

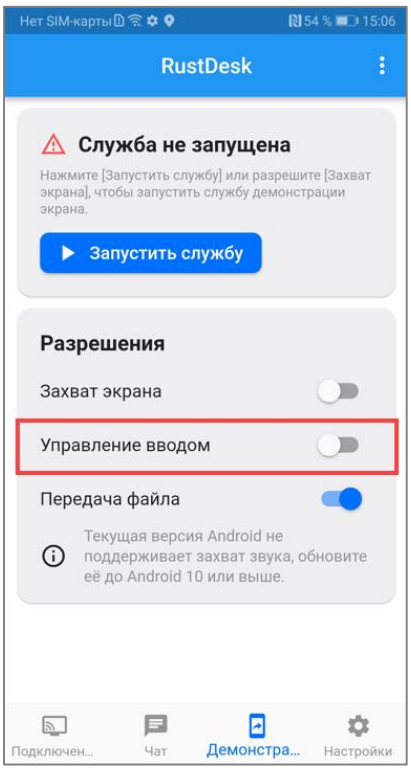


Рисунок 4.2

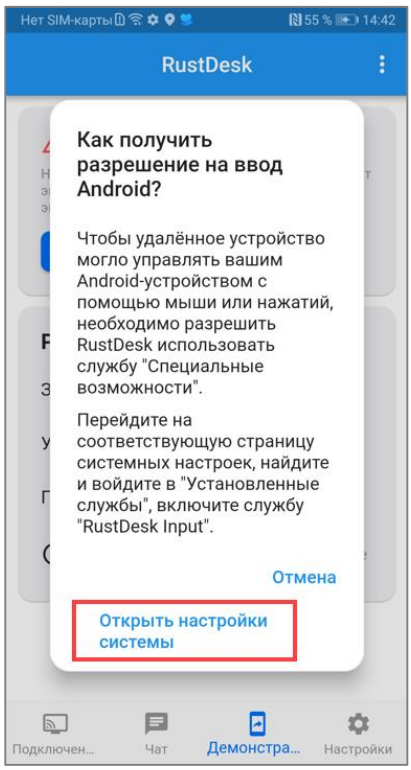


Рисунок 4.3

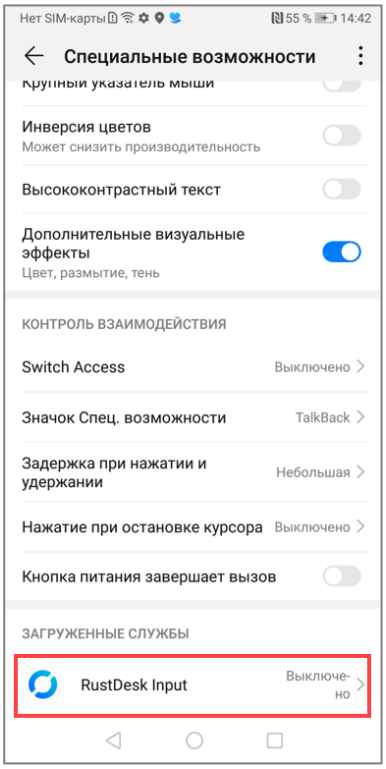


Рисунок 4.4

– коснуться RustDesk Input (Рисунок 4.4), перевести переключатель RustDesk Input в положение «Включено» (Рисунок 4.5) и подтвердить включение (Рисунок 4.6).

ПРИМЕЧАНИЕ. Разрешение на управление вводом выдается единожды, положение переключателя будет сохранено для последующих запусков приложения RustDesk;

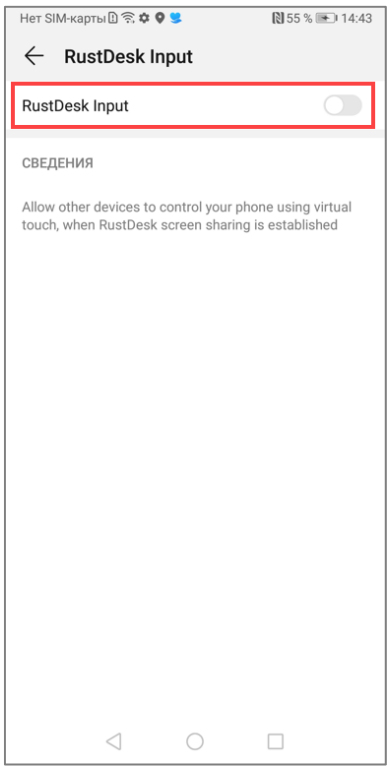


Рисунок 4.5

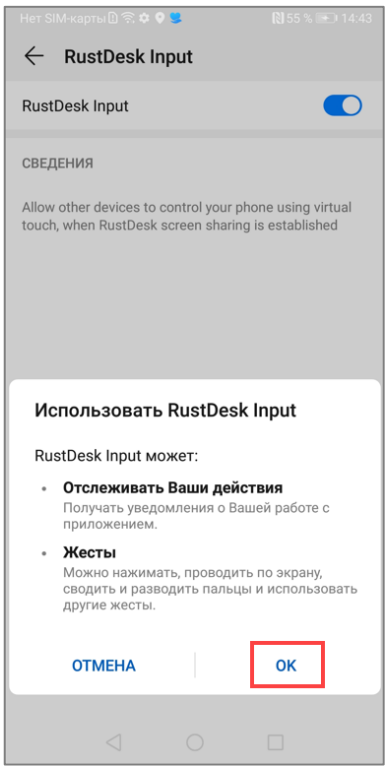


Рисунок 4.6

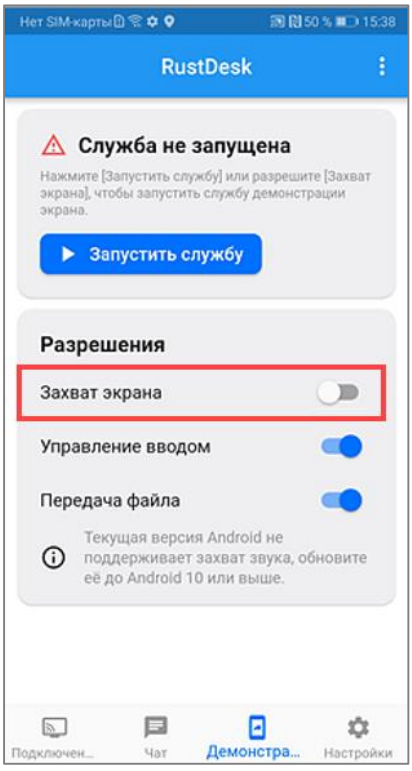


Рисунок 4.7

4) Выдать разрешение на захват экрана (применимо для ОС Android версий 7-9). Для этого необходимо:

– перевести переключатель «Захват экрана» в положение «Включено» (Рисунок 4.7);

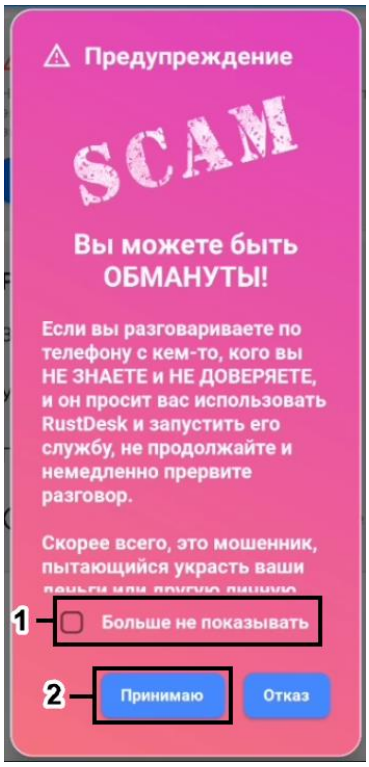


Рисунок 4.8

– ознакомиться с предупреждением о возможном мошенничестве (Рисунок 4.8);

– установить галочку в чекбоксе «Больше не показывать» (Рисунок 4.8 [1]) и выбрать «Принимаю» (Рисунок 4.8 [2]);

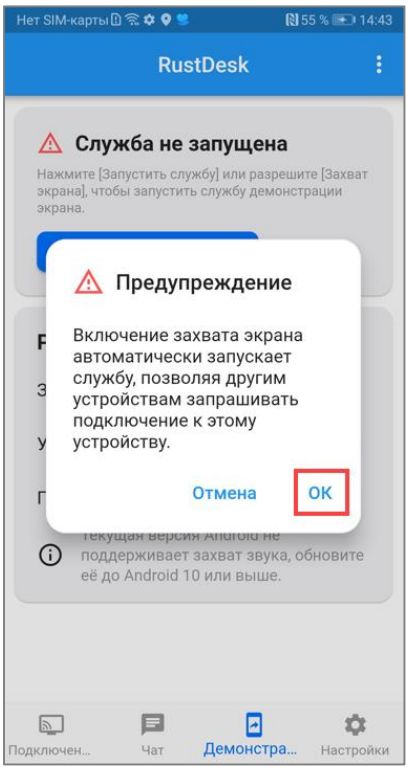


Рисунок 4.9

– ознакомиться с предупреждением, что включение захвата экрана автоматически запускает приложение RustDesk, и коснуться «OK» (Рисунок 4.9);

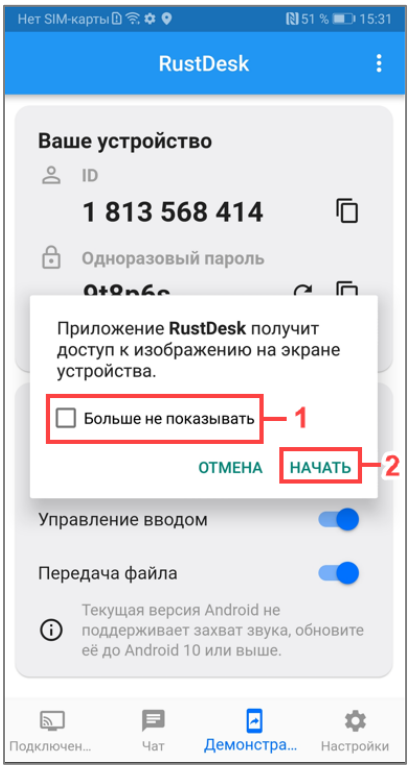


Рисунок 4.10

– установить галочку в чекбоксе «Больше не показывать» (Рисунок 4.10 [1]) и коснуться «Начать» (Рисунок 4.10 [2]).

В результате устройство будет готово к удаленному подключению.

ПРИМЕЧАНИЯ:

✓ Включение захвата экрана и службы RustDesk выполняется при удаленном подключении к устройству из ПУ;

✓ На устройствах с ОС Android версии 10 и выше при каждом удаленном подключении к устройству из ПУ необходимо подтверждать включение захвата экрана и службы RustDesk (Рисунок 4.11).

Исключение: подключение без подтверждения пользователя будет происходить, если на устройстве установлена сборка, подписанная подписью производителя (подробнее в пп. 2.1.1.7).



Рисунок 4.11

ВНИМАНИЕ! На устройствах с ОС Android версии 15 и выше при активном удаленном подключении (демонстрации экрана) окно ввода пароля (например, для выхода из режима киоска) не отображается - отображается черный экран. Начиная с ОС Android версии 15, Google усилил защиту конфиденциальных полей ввода: при определенных условиях (в том числе при удаленном подключении/трансляции экрана) система автоматически скрывает содержимое таких полей, зачерняя экран. Данное поведение является штатной мерой безопасности ОС Android.

Если необходимо при удаленном подключении выйти из режима киоска на устройстве с ОС Android версии 15 и выше, то используйте команду оперативного управления «Временно выключить режим киоска» (подробнее в п. 2.2.11.)

ПРИЛОЖЕНИЕ 5

Проверки на root-права на устройствах с ОС Android

На устройствах с ОС Android с периодичностью 1 раз в 1 час проводится ряд проверок на наличие root-прав (Таблица 5.1). Если хотя бы одна срабатывает, то Аврора Центр считает, что устройство имеет root-права.

Таблица 5.1

Имя метода	Описание	Ограничения
`checkRootManagementApps`	Проверяет, установлены ли какие-либо приложения для управления root-доступом (например, SuperSU или Magisk)	Может не обнаружить недавно разработанные или менее популярные приложения для управления root-доступом
`checkPotentiallyDangerousApps`	Проверяет, установлены ли какие-либо приложения, облегчающие получение root-доступа	– Ограничено предопределенным списком приложений; – Не может обнаружить пользовательские или менее известные опасные приложения
`checkRootCloakingApps`	Обнаруживает приложения, которые могут скрывать или маскировать root-доступ от инструментов обнаружения	Приложения для сокрытия root-доступа быстро развиваются, потенциально обходя механизмы обнаружения
`checkTestKeys`	Проверяет, подписана ли прошивка устройства тестовыми ключами Android, что происходит на AOSP или некоторых эмуляторах	Определяет только использование тестовых ключей и может пропустить рутированные устройства, использующие производственные ключи
`checkForSuBinary`	Проверяет наличие `su`-двоичного файла, обычно используемого для повышения привилегий	Дополнительные двоичные файлы могут быть переименованы или скрыты с помощью инструментов маскировки `root`, что позволяет обойти обнаружение

Имя метода	Описание	Ограничения
`checkSuExists`	Еще одна проверка существования `su`-двоичного файла с помощью «which su»	То же, что и `checkForSuBinary`, можно обойти, переименовав или скрыв двоичный файл
`checkForRWPath`	Проверяет по списку разделов, смонтирован ли раздел как доступный для чтения и записи, что является признаком получения прав-root	Некоторые новые методы root-доступа не требуют RW-доступа к `/system` разделу (например, системный root)
`checkForDangerousProps`	Проверяет наличие опасных свойств (`ro.debuggable`и `ro.secure`), которые указывают на то, что это может быть ненастоящее устройство Android	Можно обойти, если свойства сброшены или скрыты с помощью расширенных методов маскировки корня
`checkForRootNative`	Проверка наличия бинарного файла `su` на нативном уровне Android. Такого рода проверки тяжелее обойти	
`checkForMagiskBinary`	Проверяет общие места расположения бинарного файла Magisk	

ПРИЛОЖЕНИЕ 6

Использование регулярных выражений в INI и Key-value конфигурациях

Регулярное выражение — это специальный шаблон или последовательность символов, используемая для описания структуры текста и поиска совпадений в строках. Регулярные выражения созданы для решения таких задач, как проверка формата ввода, фильтрация данных, замена текста и многое другое.

Основные элементы регулярных выражений:

1) Метасимволы

Метасимволы позволяют обозначать специальные условия поиска:

– . — соответствует любому одному символу, кроме перевода строки (\n);

– * — ноль или больше повторений предыдущего элемента;

– + — одно или больше повторений предыдущего элемента;

– ? — ноль или одно повторение предыдущего элемента;

– {m,n} — диапазон повторений от m до n включительно;

– [abc] — класс символов, соответствует любому из указанных внутри квадратных скобок символов;

– [^abc] — класс символов с отрицанием соответствует любым символам, кроме указанных внутри квадратныхскобок;

– (abc) — группировка элементов, позволяет объединять части регулярного выражения в одну группу.

2) Якоря

Якоря помогают привязывать поиск к началу или концу строки:

– ^ — начало строки;

– $ — конец строки.

3) Экранированные символы

Некоторые символы имеют специальное значение в регулярных выражениях и требуют экранирования обратным слешем (\) перед использованием их буквально: ., *, +, ?, [], (), {}, |.

Например, чтобы искать точку именно как символ точки, нужно написать ее как \..

4) Пример регулярных выражений

Слово «Москва».

Регулярное выражение: ^\s*([^\n]+)$

Объяснение регулярного выражения:

– ^: начало строки;

– \s*: ноль или больше пробельных символов;

– ([^\n]+): захват группы, содержащей любые символы кроме символа новой строки (\n)).

– $: конец строки.

Номер паспорта в формате XXXX-XXXXXX.

Регулярное выражение: \d{4}-\d{6}.

Объяснение регулярного выражения:

– \d{4}: ровно четыре цифры;
– -: дефис;
– \d{6}: ровно шесть цифр.

ПРИЛОЖЕНИЕ 7

Проверка на смену SIM-карты

Предусловие:

SIM-A — доверенная (санкционированная) SIM-карта.

SIM-N — недоверенная SIM-карта.

Санкционированное состояние SIM-карты

При назначении сценария состояние SIM-карты на устройстве считается санкционированным:

– если в момент назначения установлена SIM-A (при пустом втором слоте) — событие не срабатывает;

– если оба слота пустые и после назначения сценария впервые вставлена SIM-A, то SIM-A считается санкционированной, событие не срабатывает, в журнале отображается запись «В устройстве зарегистрирована SIM-карта как доверенная».

Событие «Смена SIM-карты» срабатывает, когда:

– на устройство назначен офлайн-сценарий и зарегистрирована доверенная SIM-A;

– из устройства изъята SIM-A;

– в устройство вставлена другая SIM-N в любой слот.

Событие «Смена SIM-карты» не срабатывает, если:

– SIM-A вынули и вставили обратно в тот же слот;

– SIM-A вставили в другой слот;

– слот остался пустым;

– при двух SIM-картах переставили SIM местами;

– SIM-карта вставлена после добавления офлайн-сценария на устройстве — SIM-карта регистрируется как доверенная.

Отображение состояния

Когда сценарий назначен, в ПУ во вкладке «Управление» отображаются назначенная реакция и текущее состояние.

При применении реакции информация обновляется, и в журнале устройства фиксируется информация о примененной реакции.

Возврат доверенной SIM-карты

Если сценарий сработал при замене SIM-A на SIM-N, а затем SIM-A возвращена обратно, устройство считается вернувшимся в санкционированное состояние — офлайн-сценарий перестает действовать.

Одновременное использование двух SIM-карт

Варианты сценариев и логика функционирования системы:

1) Слоты пустые, назначается офлайн-сценарий, вставляются одновременно две SIM-карты - обе SIM-карты становятся санкционированными. Офлайн-сценарий не срабатывает.

2) Слоты пустые, назначается офлайн-сценарий, вставляется одна SIM-карта - она становится санкционированной, затем вставляется вторая SIM-карта во второй слот - эта SIM-карта уже будет считаться несанкционированной и офлайн-сценарий сработает.

3) В телефоне вставлены две SIM-карты, назначается офлайн-сценарий - обе SIM-карты становятся санкционированными. Офлайн-сценарий не срабатывает.

ПРИЛОЖЕНИЕ 8

Особенности удаленного пробуждения устройств

Особенности удаленного пробуждения устройств:

– пробуждение реализовано по технологии WoL - Wake-on-LAN;

– политика назначается на группу устройств. Устройство, которое находится в той же локальной подсети, пробуждает устройства, на которые назначена политика, и политика применяется на данных устройствах. Хотя бы одно устройство в каждой подсети должно быть включено;

– пробуждение доступно как для моментальной, так и для интервальной установки;

– механизм пробуждения совершает одну попытку пробуждения в заданном интервале времени. Однако, если на группу устройств назначено несколько политик, требующих пробуждения в заданные интервалы времени, отправка команды на пробуждение будет происходить не чаще одного раза в час. Когда требуется неоднократное применение политики и включено удаленное пробуждение, команда на пробуждение будет отправляться при каждом наступлении интервала до тех пор, пока устройство не будет соответствовать политике;

– не все устройства (а именно, их материнские платы) поддерживают WoL только из выключенного состояния. Пробуждение возможно из режима ожидания;

– пробуждение работает только внутри одной подсети, которая определяется по IP-адресу и маске подсети. Если IP-адреса и маски разных сетей пересекаются (например, при подключении через домашний роутер), удаленное пробуждение работать не будет.

Технические требования для удаленного пробуждения устройств:

– хотя бы одно устройство в каждой подсети, где необходимо пробуждать устройства, должно быть включено;

– на пробуждающем устройстве должен быть настроен соответствующий часовой пояс, равный часовому поясу устройств, которые необходимо пробуждать;

– устройства, предназначенные для удаленного пробуждения, должны:

- иметь сетевую карту, аппаратно поддерживающую функцию Wake-on-LAN (WoL);
- быть корректно настроены для удаленного пробуждения и иметь функцию WoL, включенной в BIOS/ UEFI и в ОС;
- оставаться подключенными к источнику питания;

– сетевая инфраструктура не должна отфильтровывать UDP пакеты на порту 9.

Доступные версии ОС

Удаленное пробуждение доступно для устройств с любой версией ОС семейства Linux, поддерживаемой ППО. При этом в роли пробуждающего устройства может быть устройство с любой ОС, поддерживаемой ППО.

ПРИЛОЖЕНИЕ 9

Работа с отчетами в ППО

ПРИМЕЧАНИЯ:

✓ Для работы с отчетами ППО рекомендуется использовать Grafana (тестирование проводилось на базе версии 11.6.2);

✓ Для формирования отчетов необходимо выполнить импорт отчетов в Grafana (подробнее в документе «Руководство администратора»).

ППО позволяет формировать следующие отчеты:

1) Аппаратное обеспечение по устройствам Linux;

2) Контроль последней активности устройств ППО. Особенность: для фильтрации необходимо использовать только временной период, оканчивающийся текущей датой. Например, «Last month» или «Last 2 days»;

3) Приложения, установленные из приложения «Аврора Маркет». Особенности:

– отчет разделен на два раздела по смыслу:

- «Количество успешных установок приложений» - показывает количество успешных установок приложений за все время работы с приложениями «Аврора Маркет» (начиная с релиза 5.6.0). Не привязан к фильтрам, не очищается;
- «Данные за период (не превышающий последние 90 дней)» - показывает статистику установок приложений за последние 90 дней (если во временном фильтре отчета не выбрал меньший период). Это максимальный срок, в течение которого хранятся расширенные данные по установкам. Этот раздел также позволяет анализировать активность за конкретный день, неделю или месяц;

– если релиз приложения был установлен в момент, когда на устройстве не было установлено или активировано приложение «Аврора Центр», то в отчете для такого тенанта будет отображен прочерк;

– если приложение «Аврора Центр» активировано на одном стенде (например, feat-1), а витрина и приложение заведены на другом стенде (например, feat-2), то в отчете в столбцах «ID устройства (EMM)» и «Код тенанта (EMM)» отобразятся данные с feat-1, а во всех остальных столбцах - данные с feat-2;

4) Производительность ППО;

5) События аудита ППО;

6) Статус обновления машин с ОС Linux;

7) Статус распространения приложений «Аврора Центр». При фильтрации по временному интервалу рекомендуется устанавливать значение границы фильтра «до» = «текущий момент» («To» = «now») в связи с тем, что в ППО не хранится историчность подключений устройств и в результат фильтрации попадут только те устройства, у которых дата последнего подключения находится в выбранном временном интервале;

8) Статус распространения скриптов ППО. При фильтрации по временному интервалу рекомендуем устанавливать значение границы фильтра «до» = «текущий момент» («To» = «now») в связи с тем, что в ППО не хранится историчность подключений устройств и в результат фильтрации попадут только те устройства, у которых дата последнего подключения находится в выбранном временном интервале;

9) Управление версиями пакетов;

10) Управление приложениями «Аврора Центра». Отчет разделен на три раздела по смыслу:

– «Приложения» - содержит информацию о целевом и текущем состоянии приложений, запрещающих списках, приложениях не под управлением и ожидаемых пакетах;

– «Файлы» - содержит информацию о целевом и текущем состоянии рабочих файлов, передаваемых на устройства;

– «Скрипты» - содержит информацию о назначении и результатах выполнения скриптов на устройствах;

11) Управление устройствами ППО;

12) Учетные записи ППО.

При необходимости вы можете настроить автоматическую рассылку отчетов Grafana на почту (подробнее в приложении (Приложение 10).

ПРИЛОЖЕНИЕ 10

Настройка автоматической рассылки отчетов Grafana на почту

ВНИМАНИЕ!

✓ Для управления и осуществления рассылки отчетов из Grafana на почтовые адреса, необходимо установить дополнительные плагины для Grafana. Подробная информация приведена в документе «Руководство администратора»;

✓ Название столбцов в сформированном файле для рассылки могут обрезаться из-за большого количества символов.

Предварительная настройка

При предварительной настройке необходимо указать URL до серверной части плагина OMP Grafana Email Backend.

ПРИМЕЧАНИЕ. Инструкция по настройке серверной части плагина OMP Grafana Email Backend приведена в документе «Руководство администратора».

Для предварительной настройки необходимо выполнить следующие действия:

1) Перейти в раздел «Dashboards» (Рисунок 9.1);

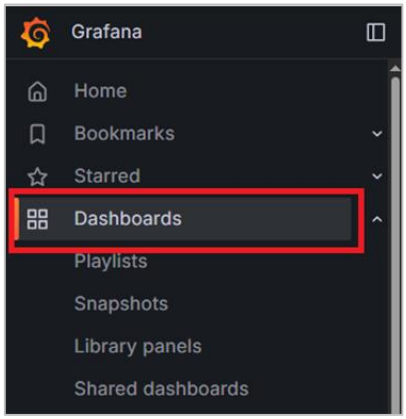


Рисунок 9.1

2) Найти дашборд «Управление почтовой рассылкой отчетов» (Рисунок 9.2);



Рисунок 9.2

3) Перейти в дашборд, нажав на его название;

4) Дождаться открытия страницы с дашбордом (Рисунок 9.3);

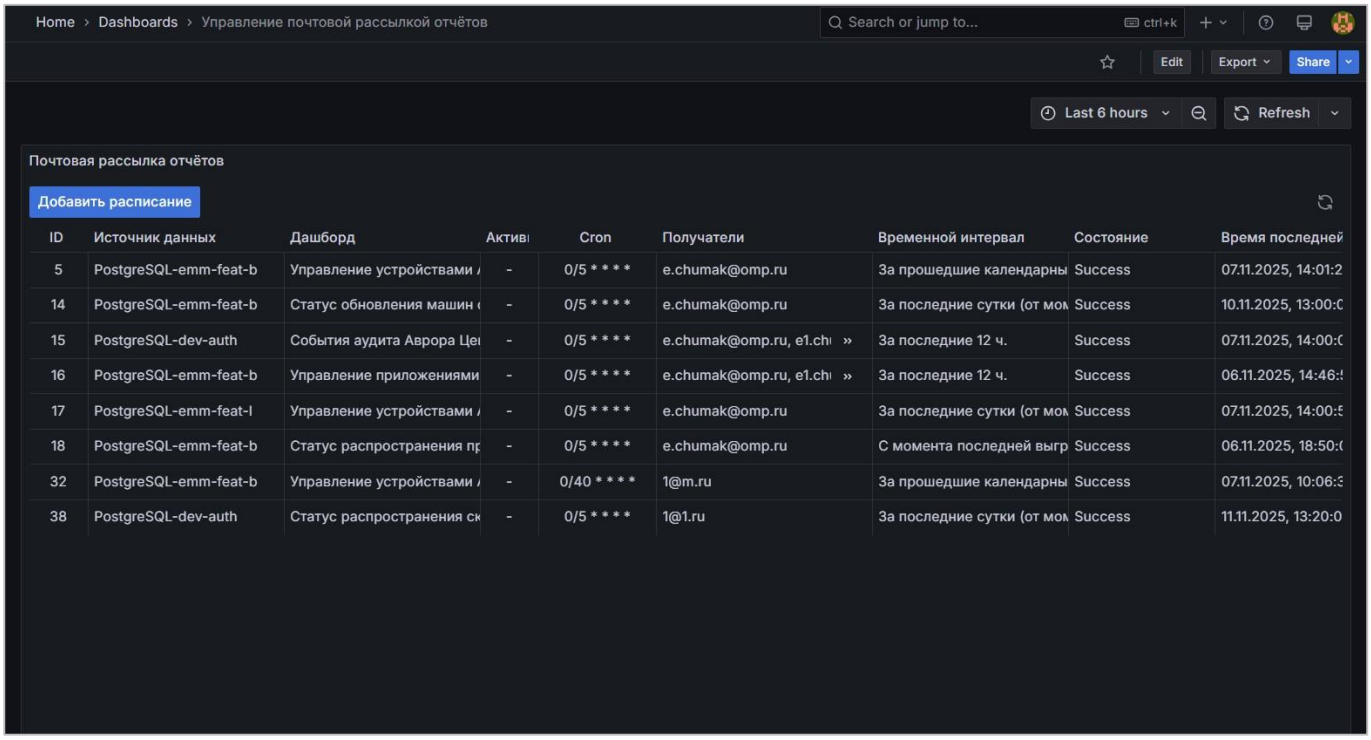


Рисунок 9.3

5) Нажать на значок ⋮ на панели дашборда (Рисунок 9.4);

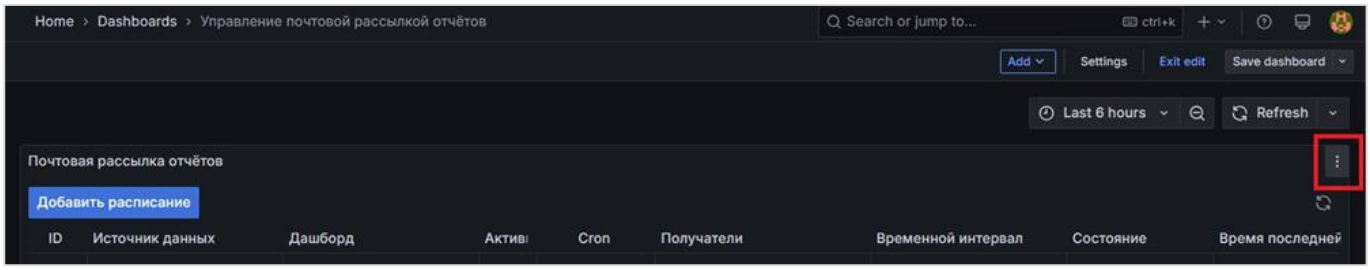


Рисунок 9.4

6) В раскрывающемся списке выбрать кнопку «Edit» (Рисунок 9.5);

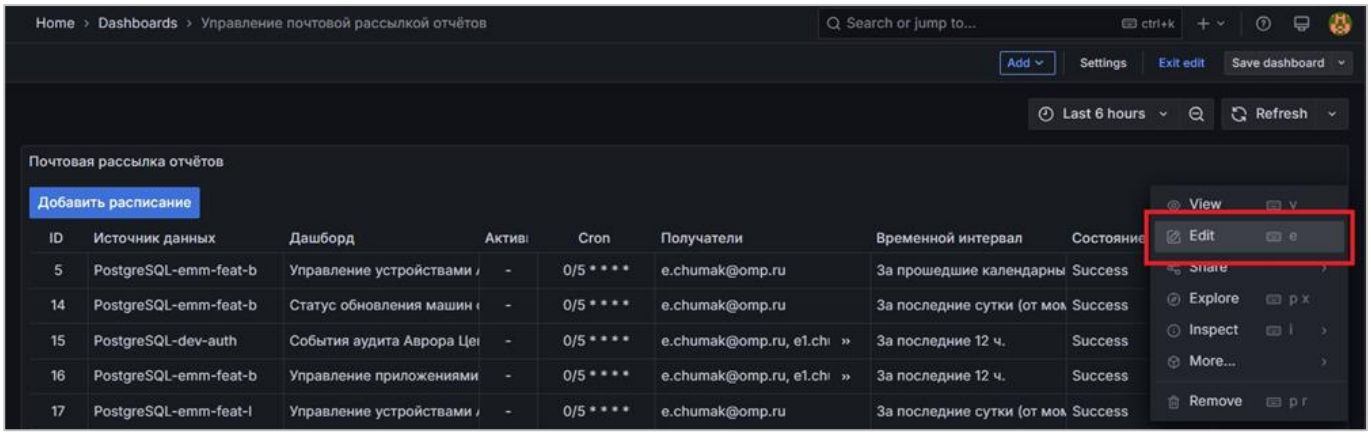


Рисунок 9.5

7) В правой панели настроек пролистать вниз до раздела «Grafana Email» (Рисунок 9.6);

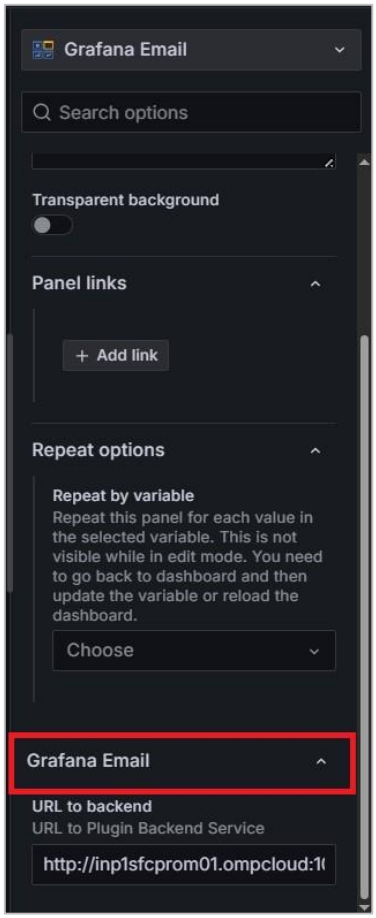


Рисунок 9.6

8) В поле «URL to backend» ввести адрес и номер порта до сервера, на котором развернута серверная часть плагина OMP Grafana Email Backend;

9) Сохранить изменения, нажав кнопку «Save dashboard» (Рисунок 9.7).

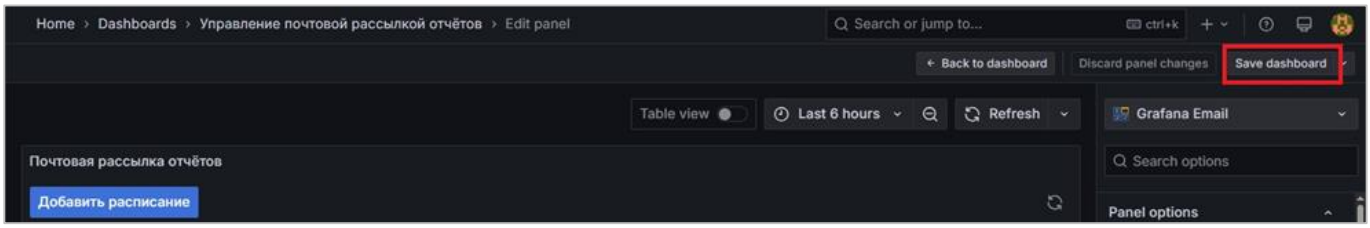


Рисунок 9.7

Создание рассылки

Для создания рассылки необходимо выполнить следующие действия:

1) Перейти в дашборд «Управление почтовой рассылкой отчетов», выполнив шаги 1-4 из пункта «Предварительная настройка» (см. Рисунок 9.3);

2) Нажать кнопку «Добавить расписание»;

3) Дождаться открытия модального окна «Добавление расписания» (Рисунок 9.8);

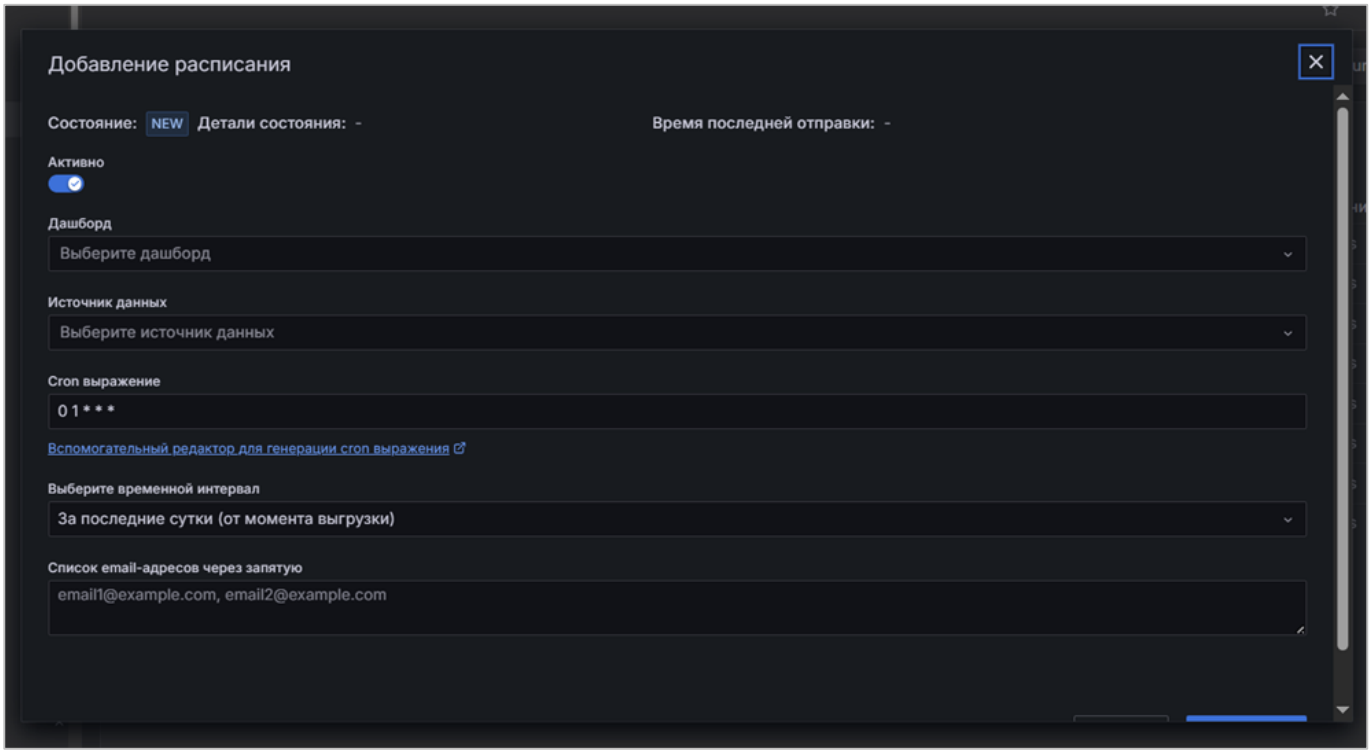


Рисунок 9.8

4) Выбрать из раскрывающегося списка «Дашборд» отчет, который необходимо рассылать (Рисунок 9.9);

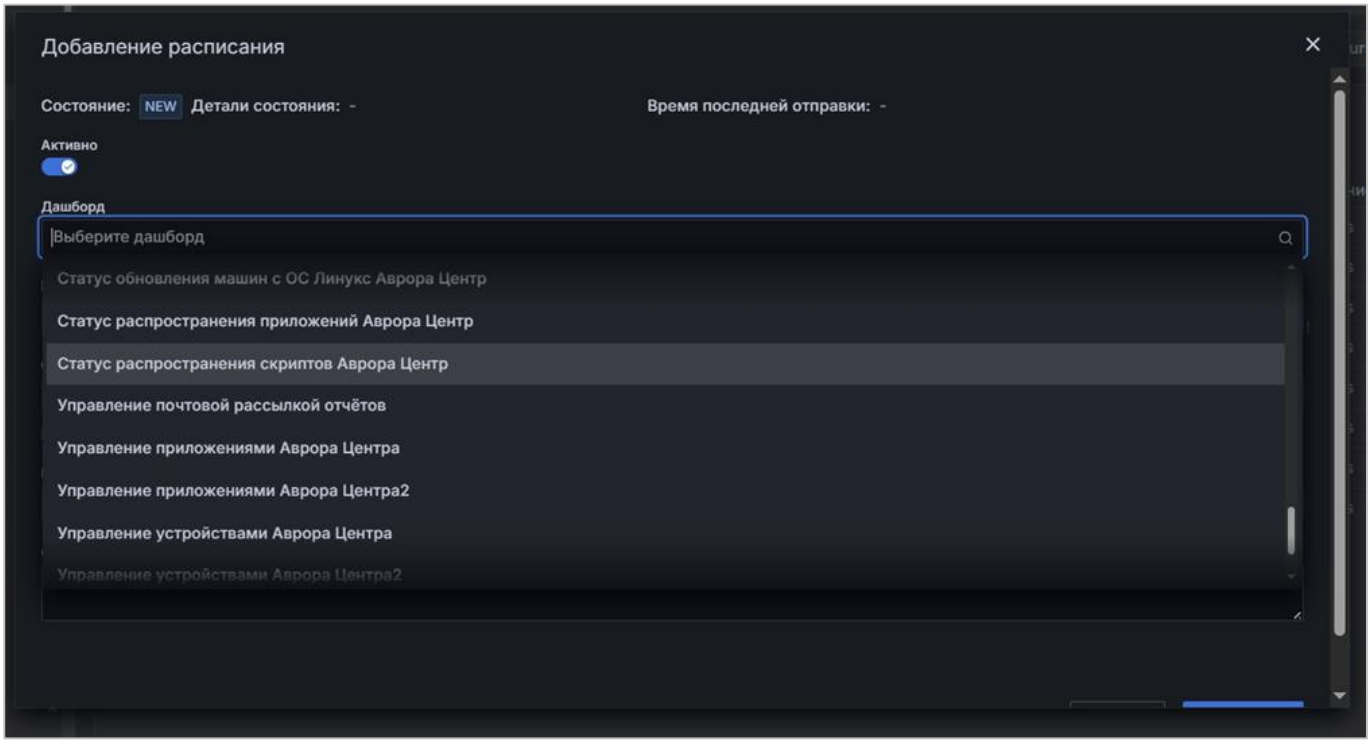


Рисунок 9.9

5) Выбрать из раскрывающегося списка «Источник данных» нужную базу данных, которая подключена (Рисунок 9.10);

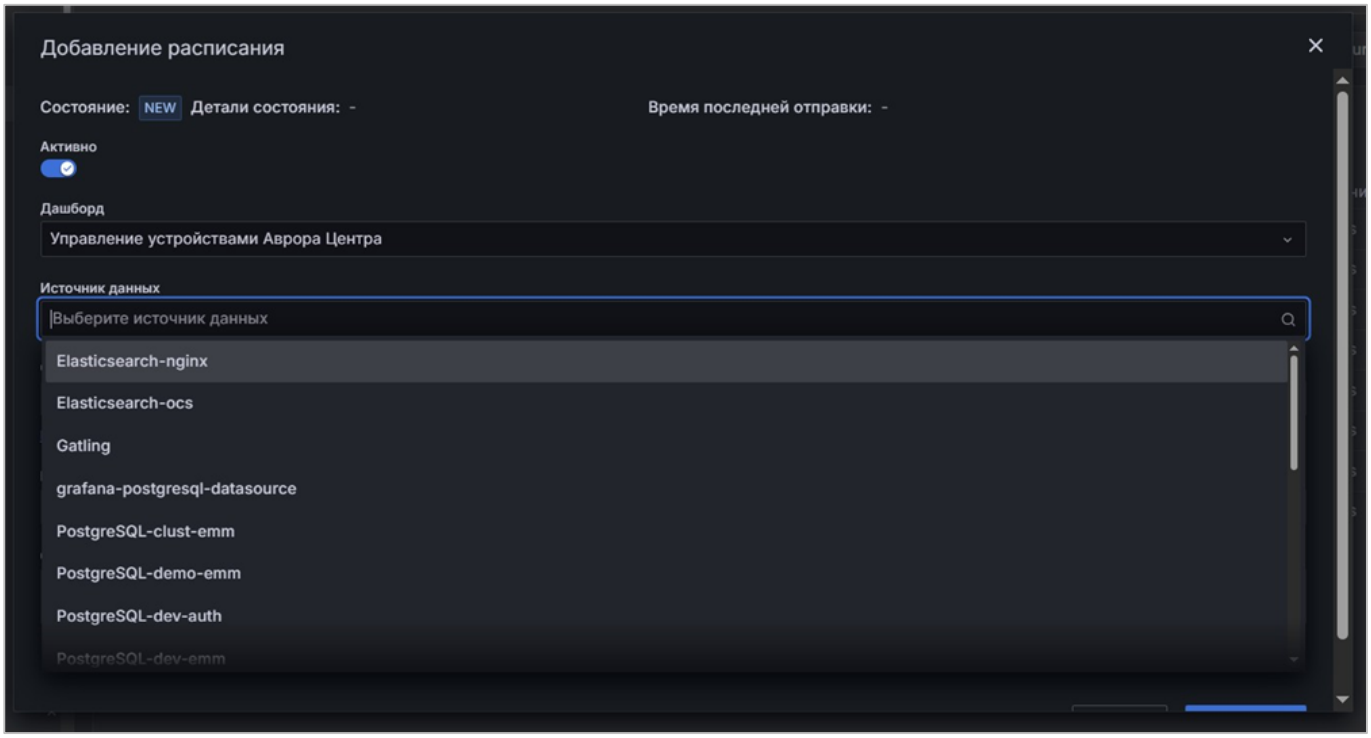


Рисунок 9.10

6) Задать в поле «Cron выражение» расписание, которое будет повторяться для рассылки (Рисунок 9.11).

ПРИМЕЧАНИЕ. Также возможно воспользоваться генератором cron выражений https://crontab.guru/;

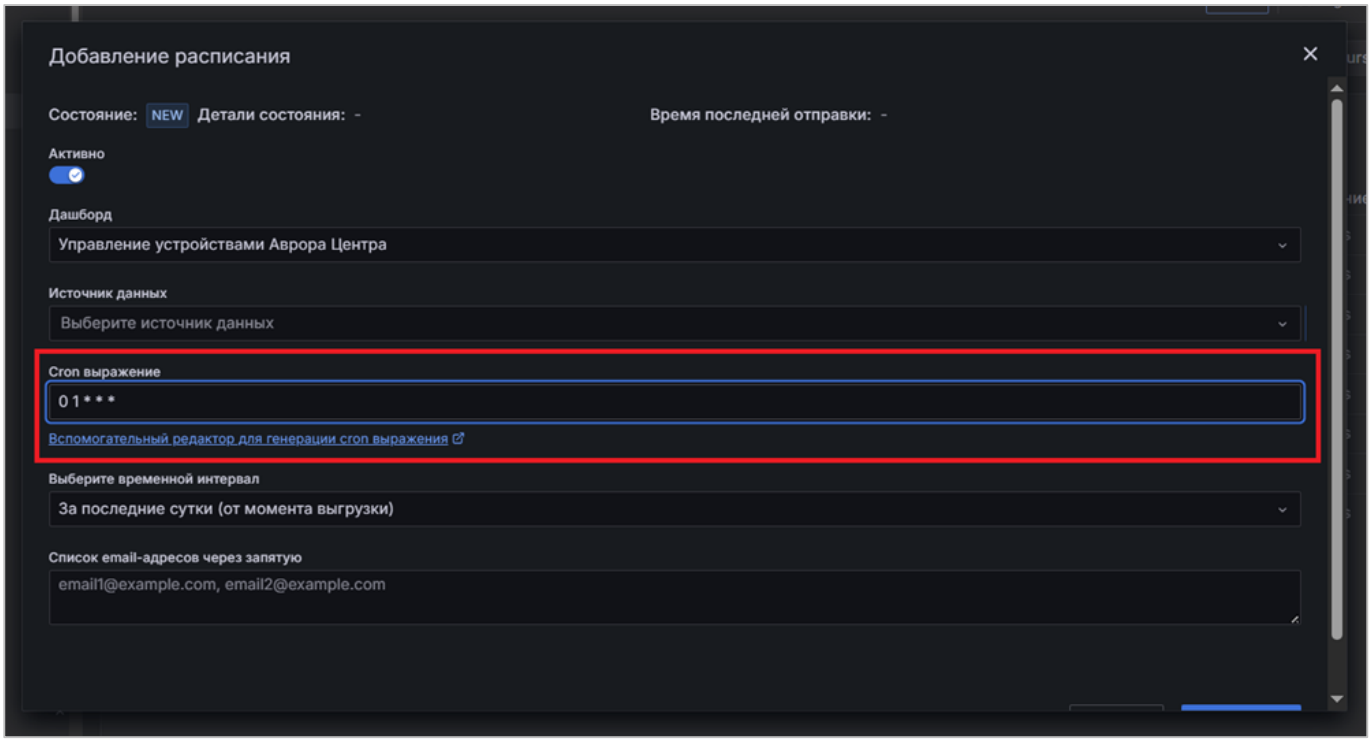


Рисунок 9.11

7) Выбрать из раскрывающегося списка значение временного интервала данных отчета (Рисунок 9.12):

– с момента последней запланированной выгрузки - формируются данные отчета между последней запланированной и ожидаемой в будущем рассылки;

– с момента последней выгрузки по факту - формируются данные отчета с момента последней успешной рассылки. В случае, если одна из итераций рассылки была неуспешной, то данные за этот период попадут в следующую итерацию рассылки;

– за последние сутки (от момента выгрузки) - формируются данные отчета именно за последние сутки, начиная с текущего времени;

– за прошедшие календарные сутки - формируются данные отчета за сегодняшний день, начиная с 00:00;

– задать время вручную - задается вручную интервал в секундах, за которые формируются данные отчета, начиная с текущего и прошлого времени;

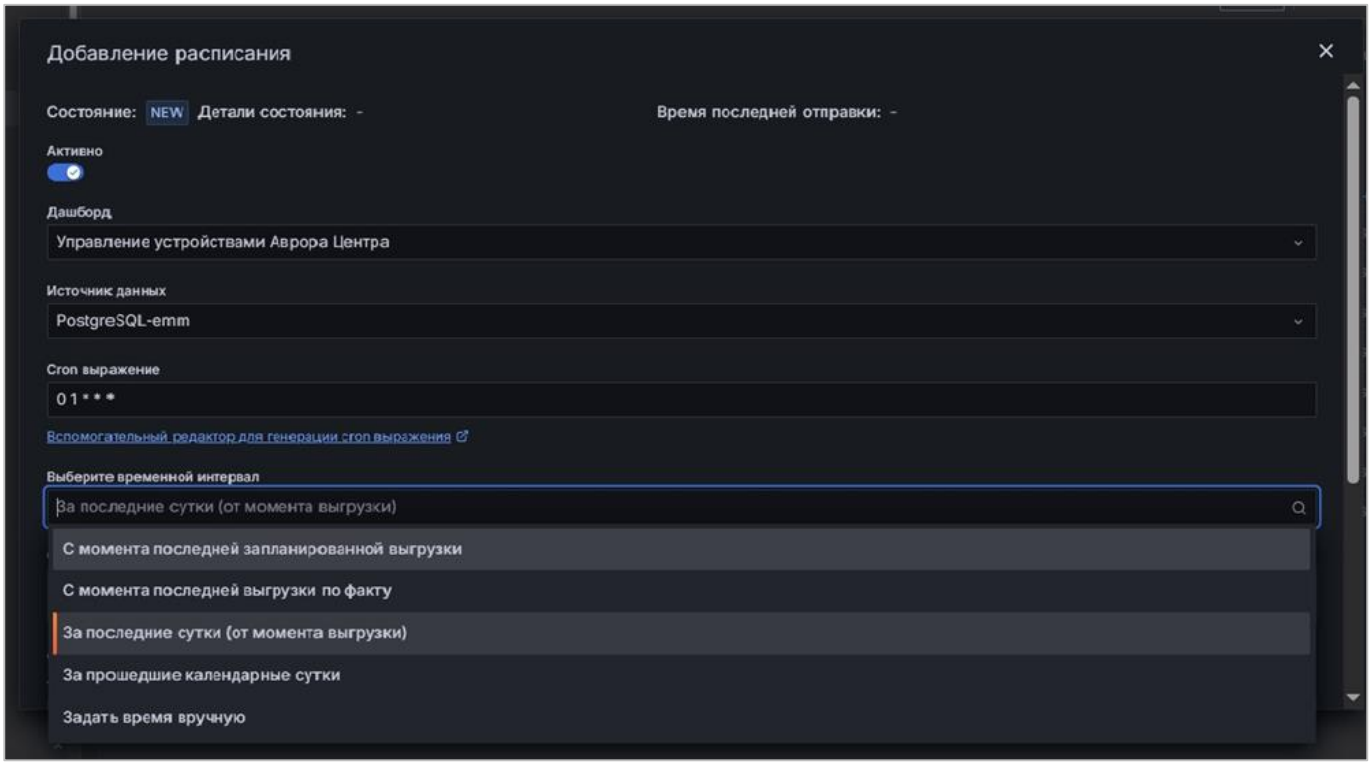


Рисунок 9.12

8) В поле «Список email-адресов через запятую» ввести нужные адреса электронной почты через запятую, для которых будет осуществляться рассылка выбранного отчета из Grafana (Рисунок 9.13);



Рисунок 9.13

9) При необходимости возможно отфильтровать данные отчета для рассылки (Рисунок 9.14).

ВНИМАНИЕ! Фильтры у каждого отчета могут быть разные. Фильтры, приведенные на рисунке (Рисунок 9.14), являются примером из отчета «Управление устройствами Аврора Центра»;



Рисунок 9.14

10) Нажать кнопку «Сохранить» (Рисунок 9.15).

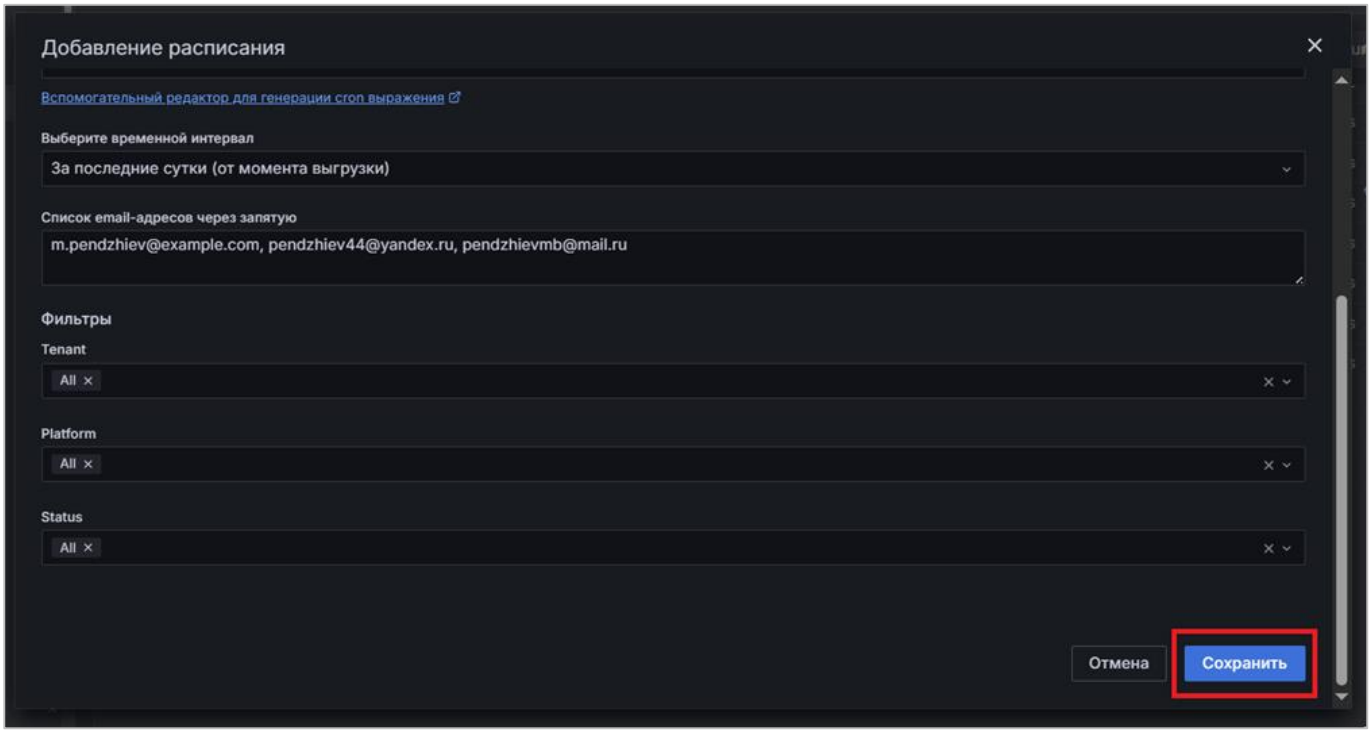


Рисунок 9.15

В результате успешного создания в списке с рассылками появится новое созданное расписание и отобразится соответствующее уведомление (Рисунок 9.16).

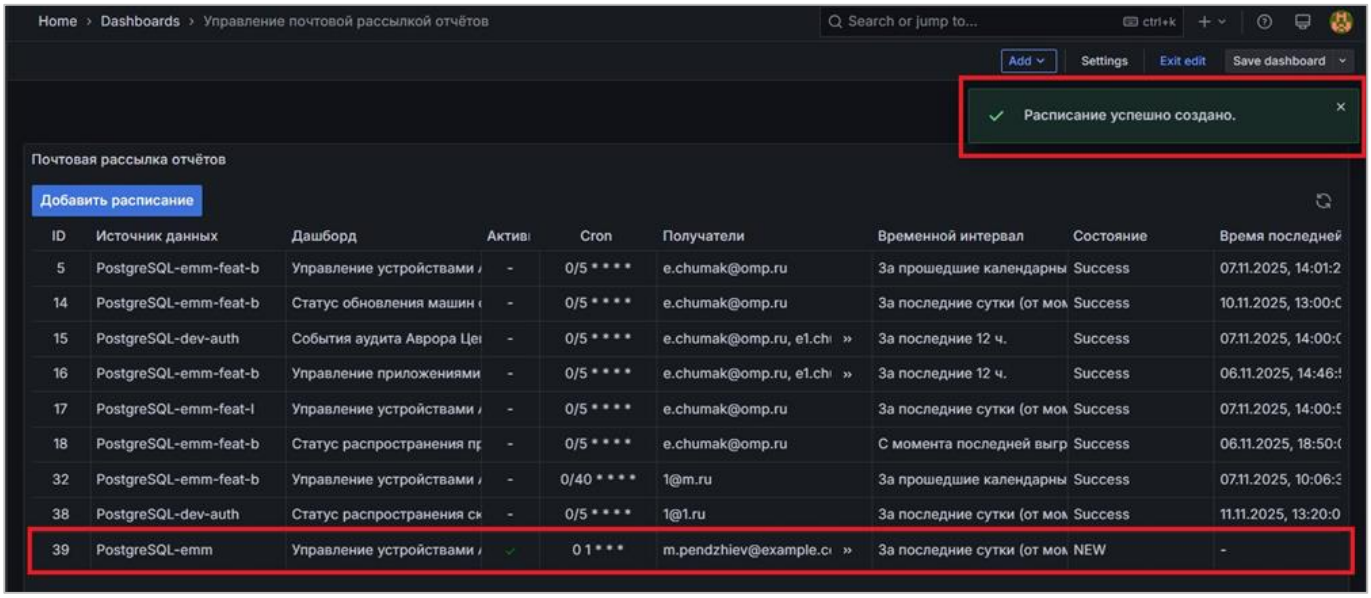


Рисунок 9.16

Редактирование рассылки

Для редактирования рассылки необходимо выполнить следующие действия:

1) Перейти в дашборд «Управление почтовой рассылкой отчетов», выполнив шаги 1-4 из пункта «Предварительная настройка» (см. Рисунок 9.3);

2) Пролистать вниз до конца дашборда, а затем прокрутить вправо до конца с помощью ползунка (Рисунок 9.17);

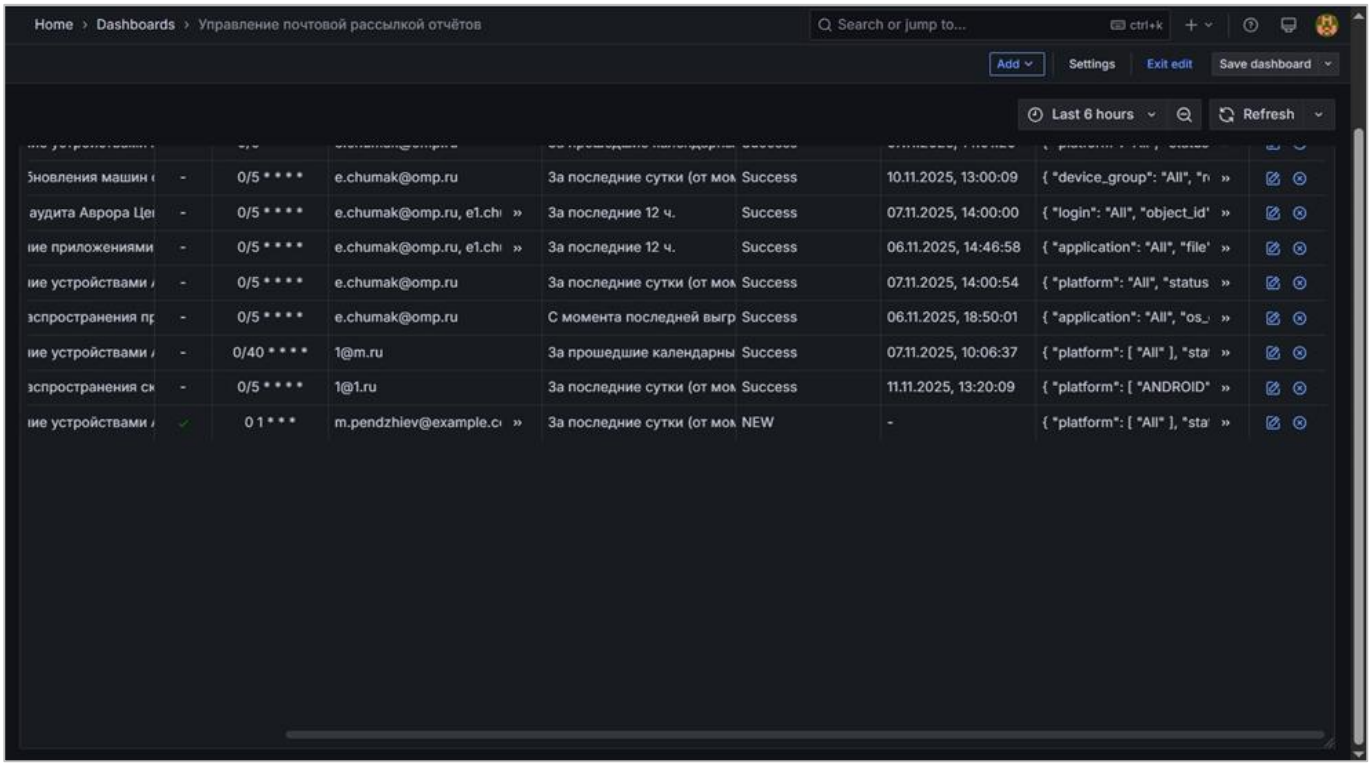


Рисунок 9.17

3) Выбрать из списка нужное расписание рассылки и нажать кнопку «Редактировать» (Рисунок 9.18);

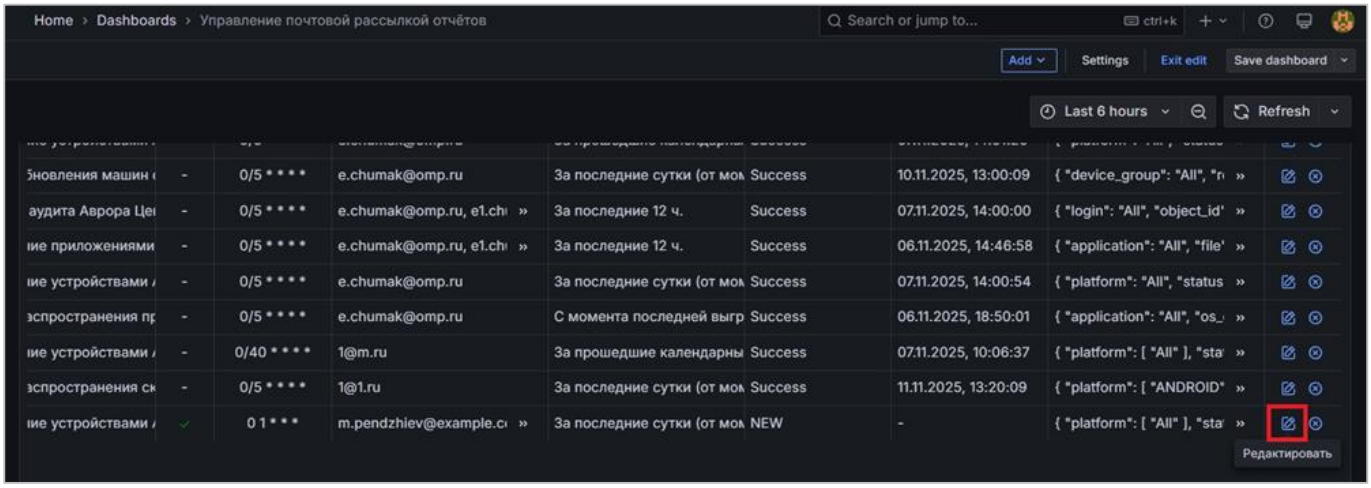


Рисунок 9.18

4) Дождаться открытия модального окна «Редактирование расписания» (Рисунок 9.19);

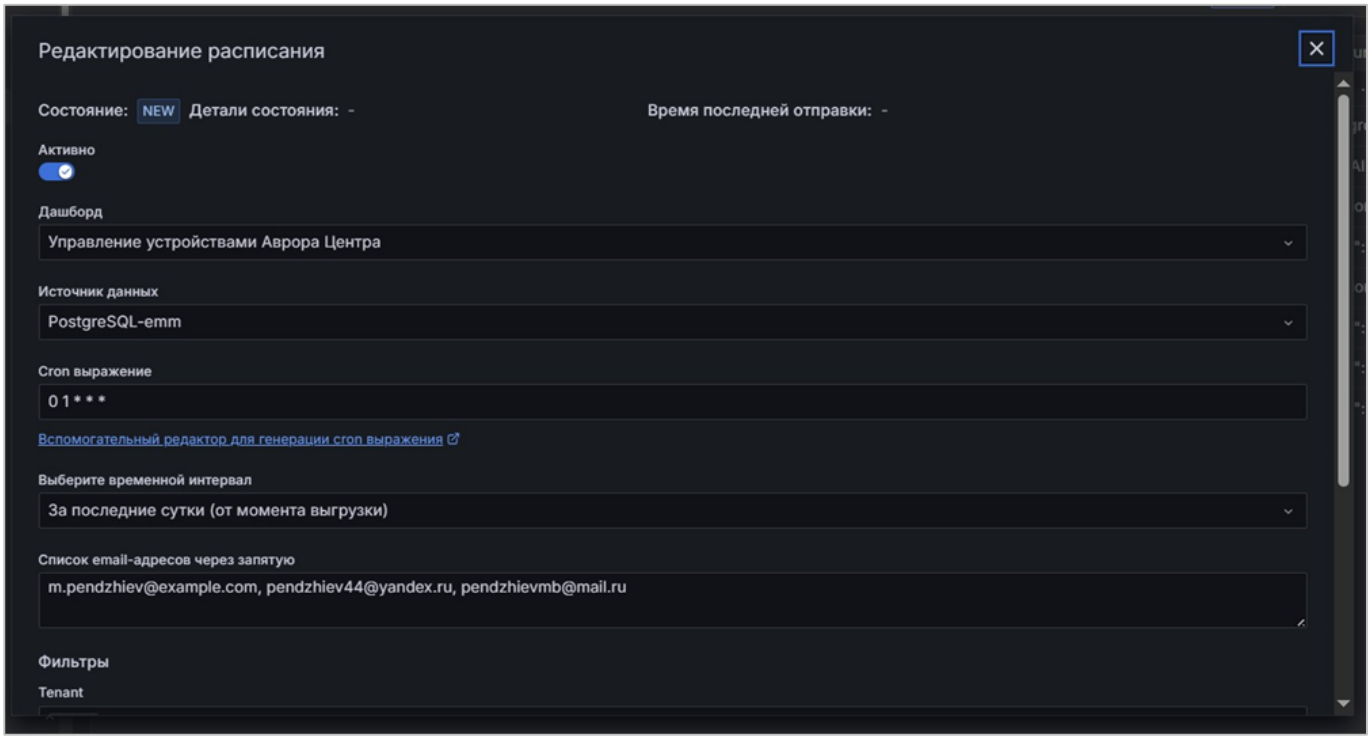


Рисунок 9.19

5) Отредактировать необходимые поля и сохранить изменения, нажав кнопку «Сохранить» (Рисунок 9.20).

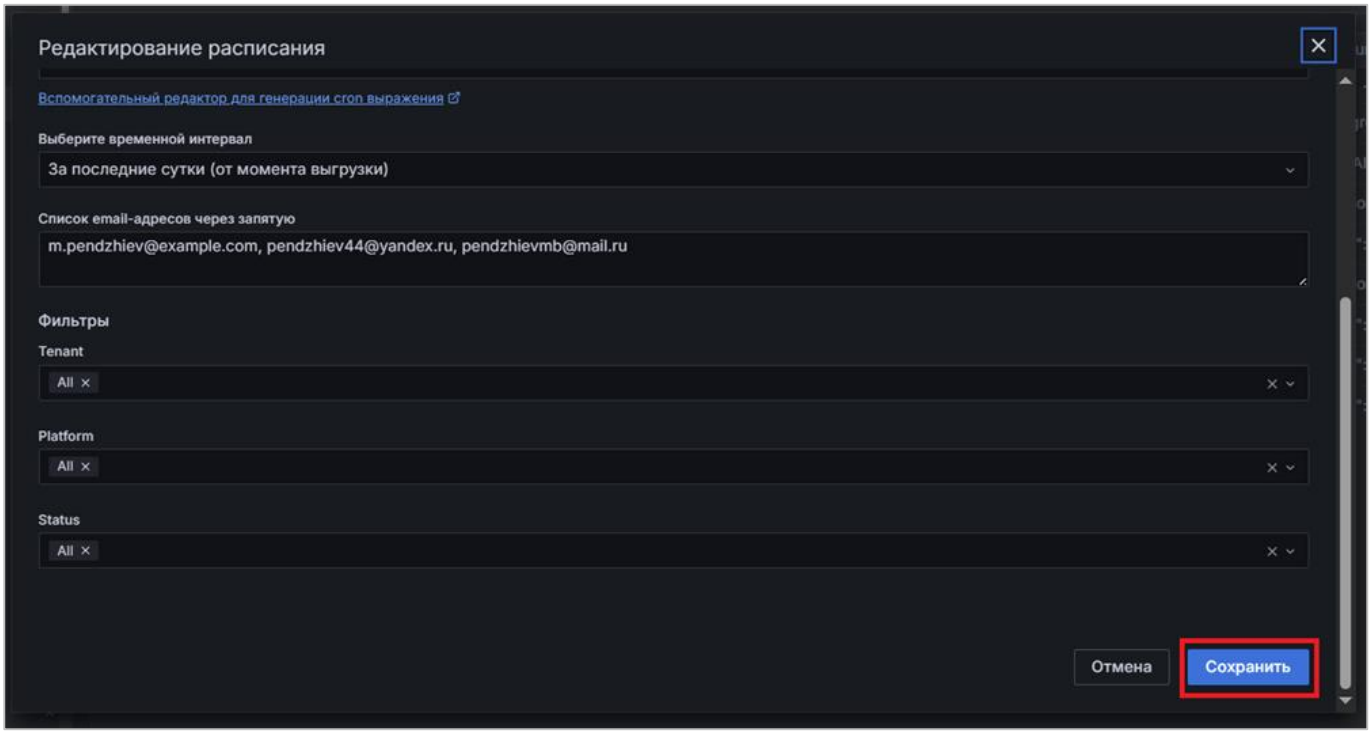


Рисунок 9.20

В результате успешного сохранения информация в списке с рассылками обновится и отобразится соответствующее уведомление (Рисунок 9.21).

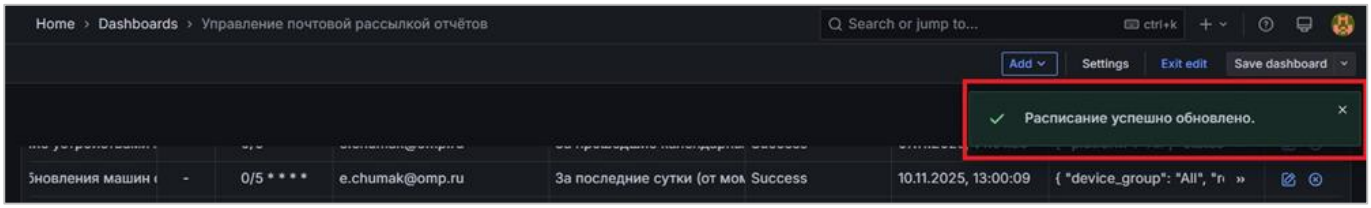


Рисунок 9.21

Удаление рассылки

Для удаления рассылки необходимо выполнить следующие действия:

1) Перейти в дашборд «Управление почтовой рассылкой отчетов», выполнив шаги 1-4 из пункта «Предварительная настройка» (см. Рисунок 9.3);

2) Пролистать вниз до конца дашборда, а затем прокрутить вправо до конца с помощью ползунка (см. Рисунок 9.17);

3) Выбрать из списка нужное расписание рассылки и нажать кнопку «⊗ Удалить» (Рисунок 9.22);

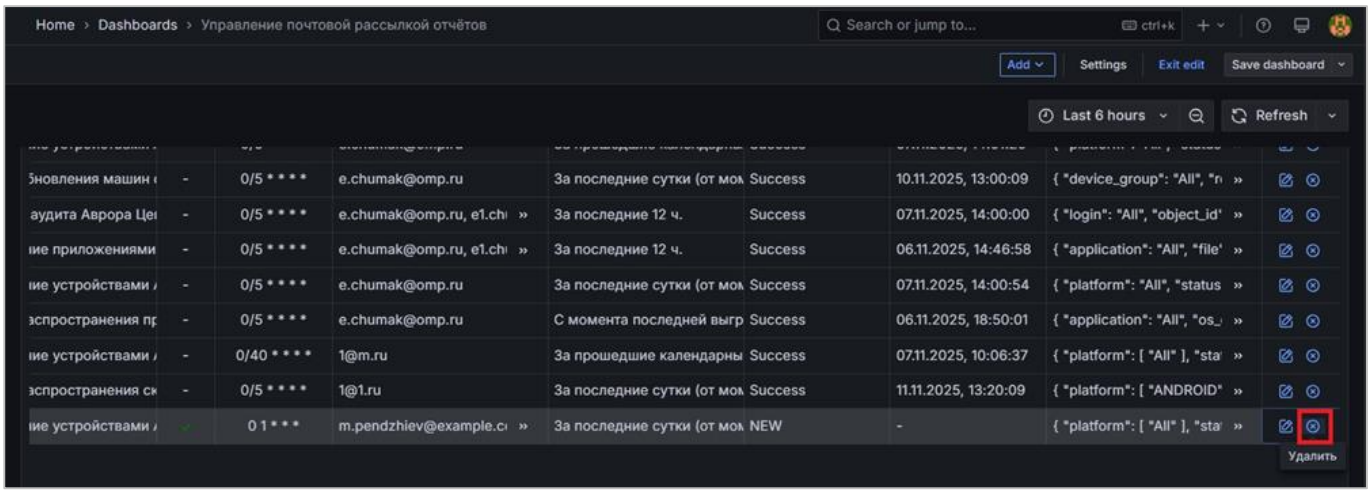


Рисунок 9.22

4) Подтвердить удаление в диалоговом окне, нажав кнопку «Подтвердить» (Рисунок 9.23).

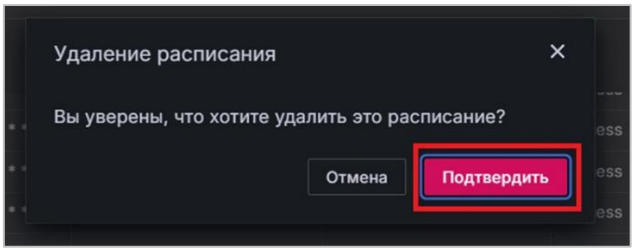


Рисунок 9.23

В результате успешного удаления отобразится соответствующее уведомление (Рисунок 9.24).

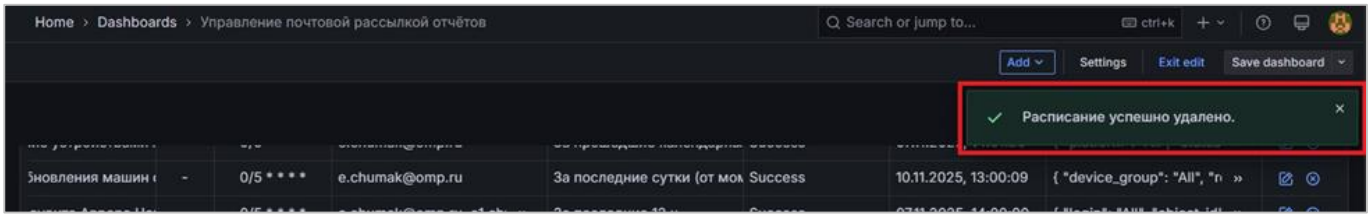

Home › Dashboards › Управление почтовой рассылкой отчётов
Search or jump to...
ctrl+k
Add
Settings
Exit edit
Save dashboard
Расписание успешно удалено.
0/5 * * * *
e.chumak@omp.ru
За последние сутки (от мок
Success
10.11.2025, 13:00:09

Рисунок 9.24

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ версии документа	Содержание изменения	ФИО	Дата
1.0	Начальная версия	Лебедев А. Пенджиев М. Иванова Н.	11.09.2026 г.
1.1	Внесены изменения	Пенджиев М. Иванова Н.	16.09.2026 г.
1.2	Внесены изменения	Пенджиев М.	01.10.2026 г.