RuDesktop

Документация

Сервер: администрирование и пользование

RuDesktop

Версия 3.1 • сформировано 21.11.2026

Оглавление

1 Руководство администратора **3**

1.1 Архитектура сервера 3
1.2 Системные требования 9
1.3 Установка\обновление сервера 13
1.4 Сетевые настройки 36
1.5 Настройки сервера 76
1.6 Команды сервера 95
1.7 Развертывание отказоустойчивого кластера 256
1.8 Резервное копирование 263
1.9 Логи сервера 266
1.10 Мониторинг и метрики 268
1.11 Публикация событий в Syslog 271
1.12 Настройка мостов 292
1.13 Настройка точек распространения 295
1.14 Интеграции 302
1.15 Настройка PXE 324
1.16 Настройка Redis 339
1.17 Настройка Kickstart 342
1.18 API 345

2 Руководство пользователя **384**

2.1 Страница регистрации 384
2.2 Страница авторизации 392
2.3 Панель управления 400
2.4 Импорт записей в списки выбора 403
2.5 Портал самообслуживания 406
2.6 Удаленный доступ 411
2.7 Управление (UEM) 503
2.8 Сканирование сети 774
2.9 Установка OS 784
2.10 Обновления ОС 814

2.11 Организация 822
2.12 Аудит 941
2.13 Инвентаризация 966
2.14 Отчеты 989
2.15 Хранилище 1045
2.16 Администрирование 1067

ГЛАВА 1

Руководство администратора

1.1 Архитектура сервера

Архитектура сервера — описание состава компонентов сервера **RuDesktop** и схемы взаимодействия между ними. Раздел полезен при первичном развёртывании, диагностике и проектировании отказоустойчивой инсталляции.

1.1.1 Описание сервера

Сервер обеспечивает удалённые подключения к рабочим столам, управление политиками, задачами и правами доступа. Управление выполняется через веб-интерфейс, доступный по адресу сервера.

Примечание

По умолчанию сервер слушает на локальном IP-адресе и порту 443. Адрес и порт можно изменить — см. *Смена и установка IP* и *Смена стандартного порта*

Подсказка

Управление сервером описано в *Руководстве пользователя*

1.1.2 Стек

Компоненты сервера

- PostgreSQL — основная СУБД сервера. Хранит пользователей, группы, устройства, политики, задачи и события аудита
- Redis — кеш и канал для WebSocket-соединений (см. *Настройка Redis*)
- NGINX — фронтальный веб-сервер: терминирует TLS, проксирует запросы к веб-интерфейсу, серверной части и серверу подключений через unix-сокеты
- rudesktop-server — сервер подключений, выполняет две роли: **рандеву** — координирует установление прямых соединений между клиентами (служит точкой первичного обращения, через которую клиенты находят друг друга); **ретранслятор** (relay) — передаёт трафик через сервер, когда прямое соединение между клиентами невозможно (например, из-за NAT). Подбор ближайшего ретранслятора (моста) для клиента выполняется по географическим координатам
- rudesktop-pxe — PXE-сервер для установки ОС по сети. Содержит встроенные **TFTP** и **DHCP** серверы (см. *Настройка PXE*)
- Ansible — выполнение политик и задач на удалённых устройствах. Запуск плейбуков выполняется в фоновом режиме
- Django — административная панель и серверная часть веб-API, включая обработку WebSocket-соединений с клиентами
- YAML — формат описания политик и инвентаря Ansible
- TLS — шифрование трафика между сервером, клиентами и веб-интерфейсом

Распределённая инфраструктура

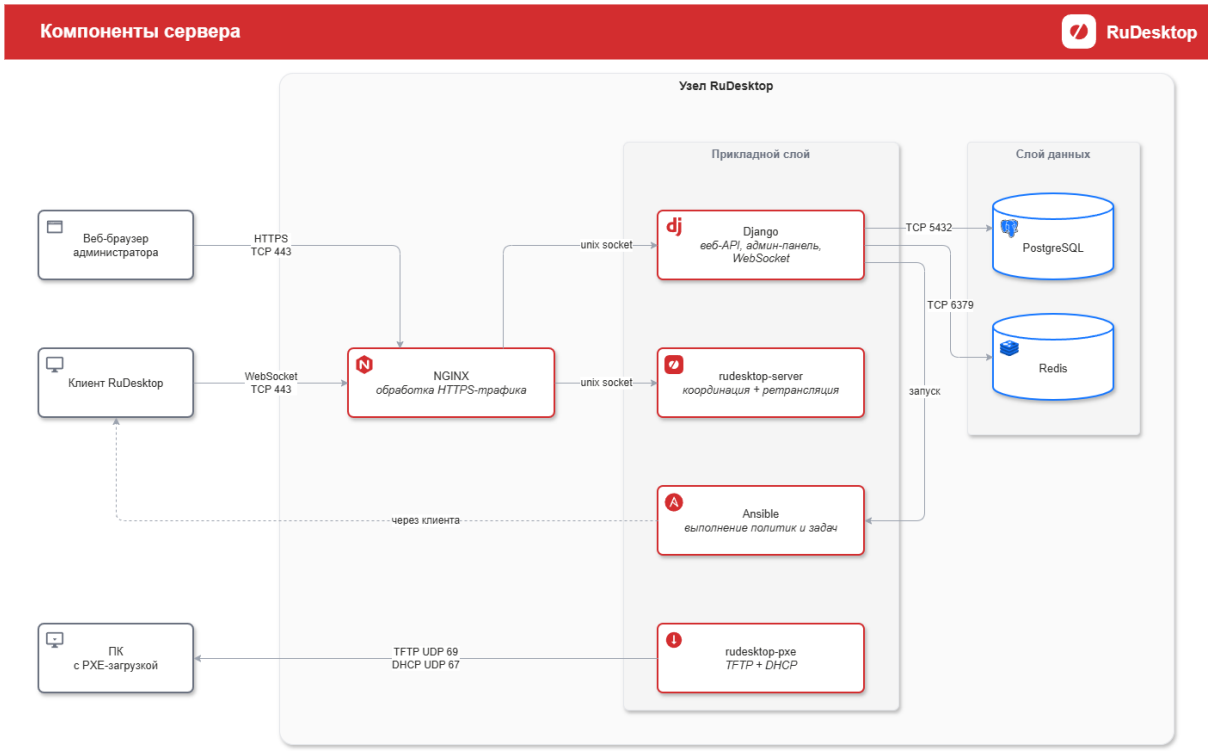
- Мост — отдельный сервер **RuDesktop**, развёрнутый в географически удалённой точке. Главный сервер по координатам подбирает ближайший к клиенту мост и направляет через него подключение, что сокращает сетевую задержку для удалённых филиалов. Подробнее: *Настройка мостов*
- Точка распространения — отдельный сервер **RuDesktop**, развёрнутый в режиме исполнителя. Забирает у главного сервера фоновые задачи (например, выполнение политик), выполняет их у себя и хранит локальный кэш файлов, чтобы не загружать их с главного сервера повторно. Позволяет вынести нагрузку с главного сервера и приблизить раздачу файлов к удалённым устройствам. Подробнее: *Настройка точек распространения*
- Клиент RuDesktop — кроссплатформенное приложение для конечного устройства (на схеме обозначен как «Агент»). Обеспечивает удалённое

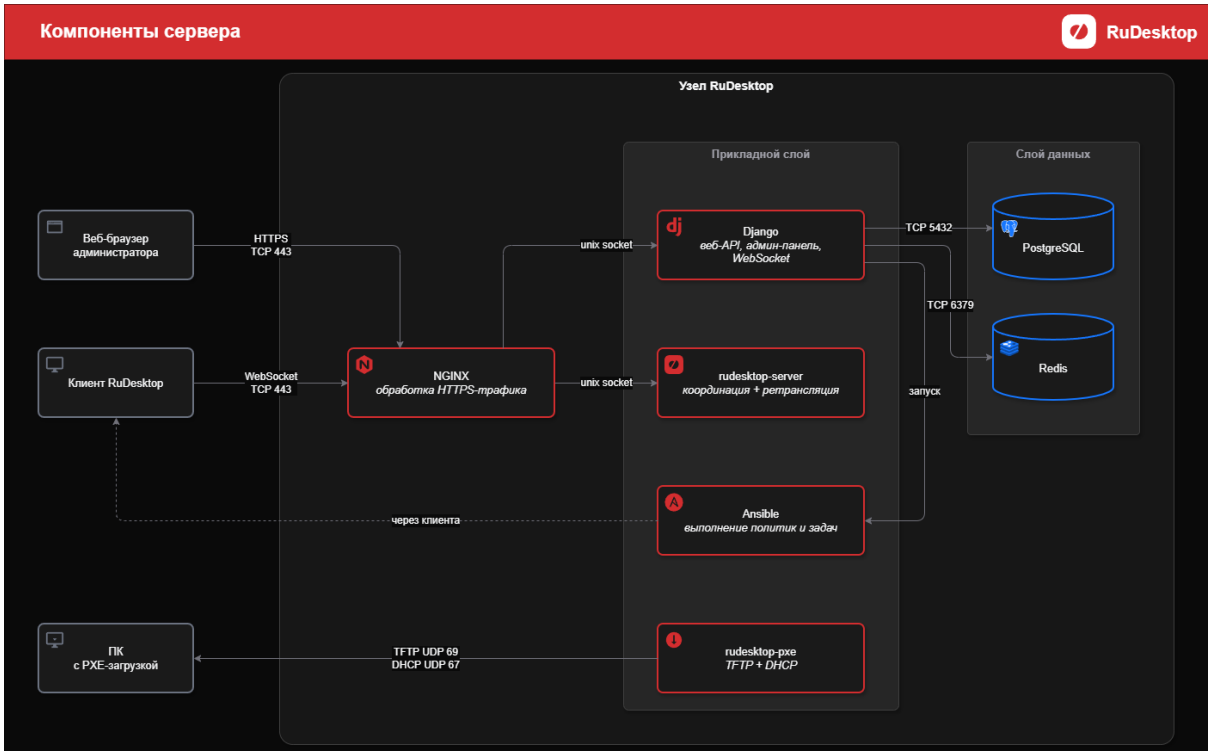
подключение к серверу, применение политик и инвентаризацию. Подробнее: Клиент RuDesktop

Внешние интегрируемые системы

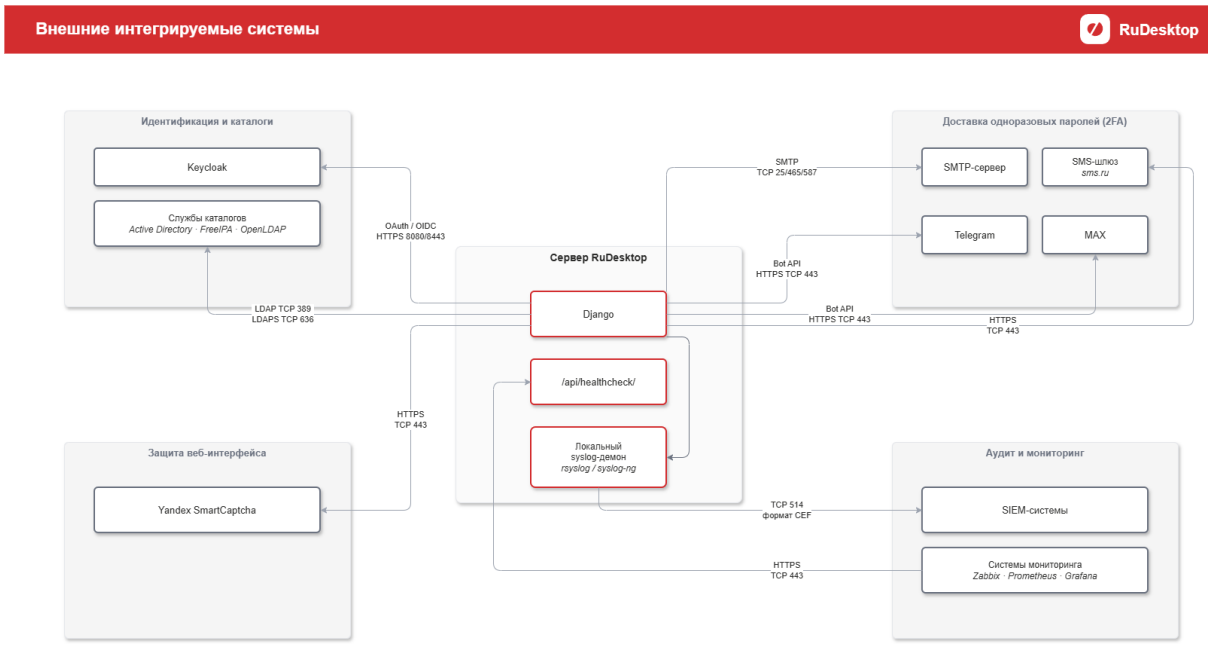
- Keycloak — внешний сервис проверки подлинности пользователей. Используется для единого входа и объединения учётных записей из разных источников. Подробнее: *Настройка Keycloak*
- Службы каталогов — интеграция с внешними каталогами пользователей по протоколу LDAP (в том числе по защищённой версии LDAPS): `Active Directory`, `FreeIPA`, `OpenLDAP`
- SMTP-сервер — внешний почтовый сервер для отправки уведомлений (приглашения, сброс паролей, события аудита) и одноразовых паролей для двухфакторной аутентификации по электронной почте. Подробнее: *Настройки SMTP*
- SMS-шлюз — внешний сервис для отправки одноразовых паролей по SMS при двухфакторной аутентификации. Поддерживается провайдер `sms.ru`. Подробнее: Двухфакторная аутентификация по SMS
- Telegram-бот — отправка одноразовых паролей через бот в мессенджере **Telegram** при двухфакторной аутентификации. Подробнее: Двухфакторная аутентификация через Telegram
- Мессенджер MAX — отправка одноразовых паролей через бот в мессенджере **MAX** при двухфакторной аутентификации. Подробнее: Двухфакторная аутентификация через MAX
- Yandex SmartCaptcha — внешний сервис проверки, защищающий веб-интерфейс от ботов при входе и регистрации. Подробнее: *Настройки авторизации*
- SIEM-системы — пересылка событий аудита во внешние системы управления событиями безопасности через локальный syslog-демон (`rsyslog` или `syslog-ng`) в формате CEF. Подробнее: *Отправка событий в SIEM*
- Системы мониторинга — внешние системы (`Zabbix`, `Prometheus`, `Grafana`) подключаются к серверу через эндпоинт `/api/healthcheck/`, команды `rude status` / `rude prof` и стандартные средства `systemd` и **PostgreSQL**. Подробнее: *Мониторинг и метрики*

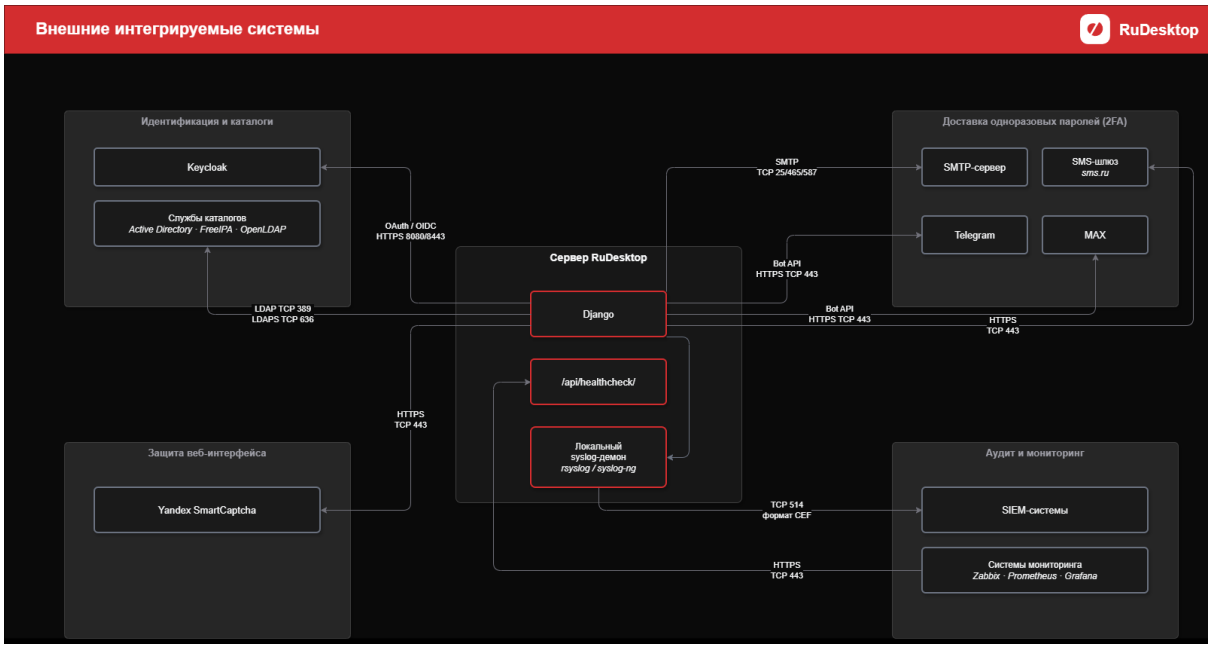
1.1.3 Схема компонентов сервера





1.1.4 Схема внешних интегрируемых систем





1.1.5 Передача файлов на устройства

При выполнении *политики*, использующей файлы из хранилища, данные проходят по цепочке **главный сервер → точка распространения → конечное устройство**:

1. **Главный сервер → точка распространения.** Точка распространения загружает файл из хранилища главного сервера в свой локальный кэш по протоколу **HTTPS**. Если файл уже кэширован и его контрольная сумма актуальна, повторная загрузка не выполняется. Подробнее: *Кэшированные файлы*

2. **Точка распространения → устройство.** Устройство загружает файл

напрямую с той точки распространения, которая выполняет задачу, также по **HTTPS**. Если нужного файла на точке не оказалось, она догружает его с главного сервера в момент выполнения

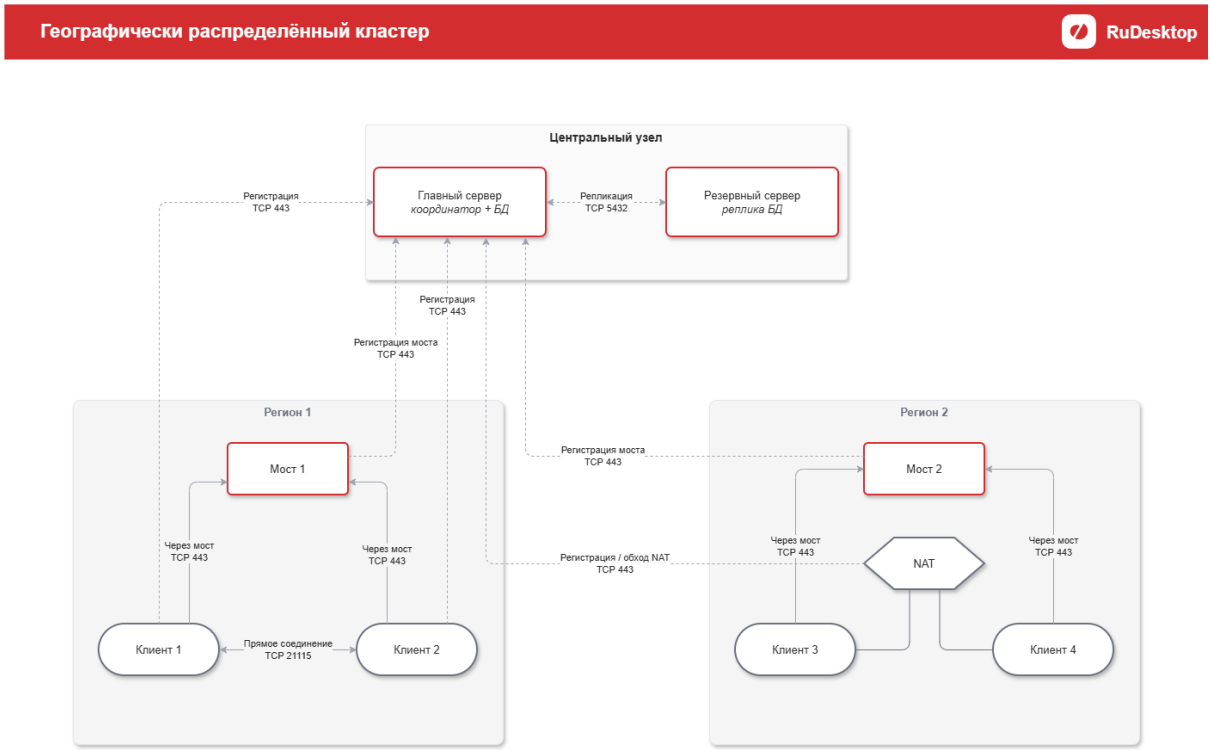
3. **Управляющий канал.** Команды на устройство (запуск задач и получение результата) передаются по протоколу **RuDesktop** через сервер подключений главного сервера — тем же WebSocket-каналом, что используется для сессий удалённого доступа, и отдельно от передачи самих файлов

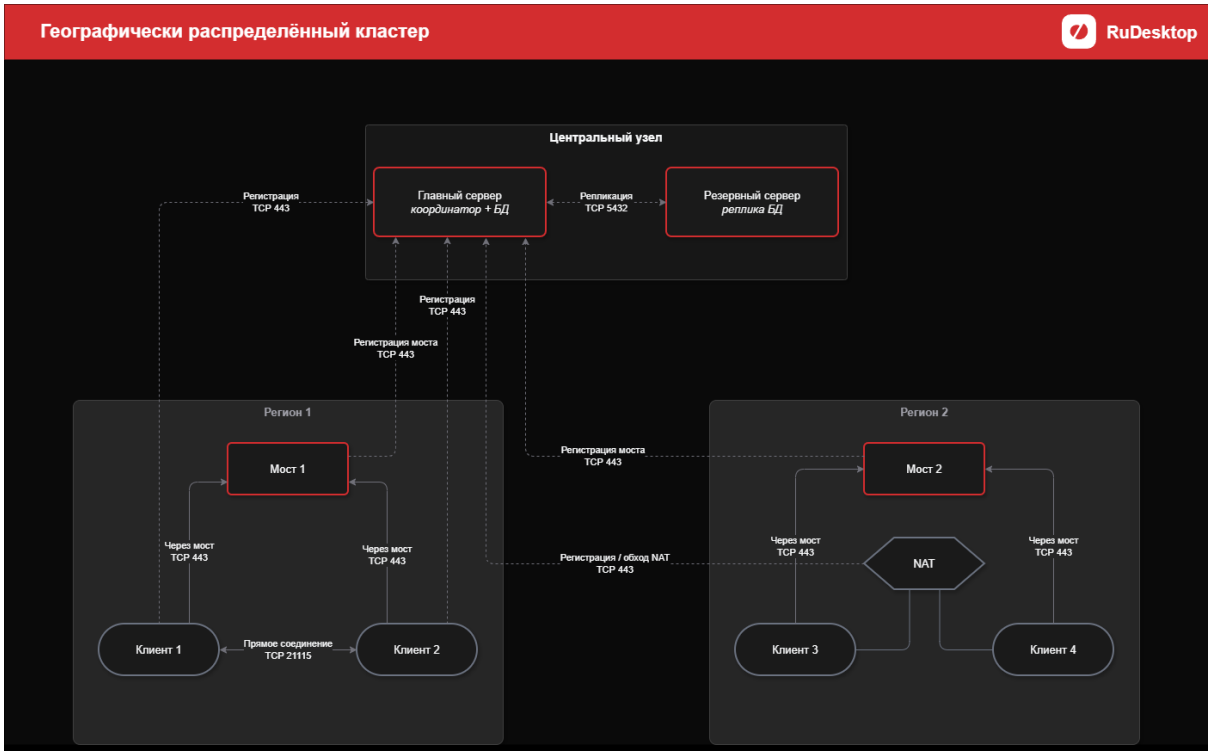
Примечание

Сетевые соединения и порты, которые требуется открыть на межсетевом экране, приведены в разделе *Настройка точек распространения*

1.1.6 Схема географически распределённого отказоустойчивого кластера

Для развёртывания нескольких узлов сервера с общими **PostgreSQL** и **Redis** см. *Развёртывание отказоустойчивого кластера*





1.2 Системные требования

Системные требования — поддерживаемые операционные системы и минимальные ресурсы (CPU, RAM, диск) для установки сервера **RuDesktop**. На разные сценарии (главный сервер, мост, точка распространения, отказоустойчивый кластер) ресурсы рассчитываются отдельно

1.2.1 Программные требования для сервера

Операционная система

Ubuntu

- 22
- 24

Debian

- 12
- 13

Astra

- 1.7
- 1.8

РЕД ОС

- 7.3
- 8

ALT Linux

- 10
- 10.1
- 10.2
- 10.3
- 10.3K
- 10.4
- 10.4K
- 11
- 11K

ОСнова

- 3.0

ROSA Linux

- 12.4

CentOS

- stream 9
- stream 10

Fedora

- 39
- 40
- 41
- 42

МСВСфера

- 10

AlmaLinux

- 9
- 10

SberOS

- 9.6

1.2.2 Системные требования для сервера с УД

Минимальные

- **Процессор (CPU):** 4 ядра
- **Оперативная память (RAM):** 8 ГБ
- **Место на жёстком диске:** 20 ГБ свободного места

- **Сетевое подключение:** 1 Мбит/с на одно подключение
- **PostgreSQL:** версия 14 или выше

1.2.3 Системные требования для сервера с УД и UEM (на 2000 АРМ)

- **Процессор (CPU):** 8 ядер или выше
- **Оперативная память (RAM):** 16 ГБ или выше

> **Подсказка**
>
> Чем больше объём оперативной памяти (RAM), тем быстрее выполняются политики на удалённых устройствах

- **Место на жёстком диске:** 100 ГБ свободного места плюс пространство для образов ОС и установочных пакетов
- **Сетевое подключение:** 1 Гбит/с
- **PostgreSQL:** версия 14 или выше

1.2.4 Требования к дисковой подсистеме

Для обеспечения стабильной работы сервера необходимо гарантировать надёжную работу дисковой подсистемы

Ниже приведены рекомендации по производительности дисковой подсистемы в зависимости от количества пользователей:

- Для поддержки 5000 пользователей дисковая подсистема должна обеспечивать не менее **1000 IOPS** (операций ввода-вывода в секунду)
- Для поддержки 10000 пользователей дисковая подсистема должна обеспечивать не менее **2000 IOPS**
- Задержка дисковой подсистемы не должна превышать **10–20 мс для HDD** и не более **10 мс для SSD**

Предупреждение

- Если дисковая подсистема работает нестабильно, это может привести к возникновению ошибок на сервере **RuDesktop**
- Такие ошибки могут проявляться в виде отказов в установлении удалённого соединения или проблем с работой веб-интерфейса и клиента **RuDesktop**

1.2.5 Сетевые требования и требования безопасности

Открытые порты

- **HTTPS (443)** — для работы клиентов **RuDesktop** и запуска политик на устройствах через веб-интерфейс

Безопасность

- Настроенный SSL/TLS-сертификат (по умолчанию используется самоподписанный, рекомендуется заменить на доверенный — см. *Добавление собственных SSL-сертификатов*)
- Настроенный межсетевой экран (Firewall) с ограничением доступа к административному веб-интерфейсу (см. *Ограничение доступа к веб-интерфейсу*)

Каналы до общих сервисов (для отказоустойчивого кластера)

При выносе **PostgreSQL** и **Redis** на отдельные серверы:

- Пропускная способность канала между узлами и общими сервисами — не менее **1 Гбит/с**
- Задержка должна быть минимально возможной (практический ориентир — менее **1 мс**); **Redis** критически чувствителен к задержкам

Подсказка

Подробнее — на странице *Развёртывание отказоустойчивого кластера*

1.2.6 Другие рекомендации

- Настроить ежедневное *резервное копирование* базы данных
- Использовать источник бесперебойного питания (UPS)
- Регулярно отслеживать свободное место на дисках, особенно в каталогах `/var/lib/rudesktop/` (медиа, kickstart, PXE) и `/var/log/rudesktop/` (логи)

1.3 Установка\обновление сервера

1.3.1 Установка из ISO-образа

Установка из ISO-образа — развёртывание сервера **RuDesktop** через готовый ISO-образ Ubuntu Server, в который уже включены сервер, СУБД и веб-сервер. Подходит для развёртывания «с нуля» как на физическом оборудовании, так и в виртуальной среде

Описание

Установка выполняется с предварительно подготовленного установочного образа ISO. Образ содержит:

- Пакет сервера **RuDesktop** 3.0
- Ubuntu Server 24.04
- PostgreSQL 16
- Nginx 1.24

Процесс полностью соответствует обычной инсталляции **Ubuntu** — будь то на реальное оборудование или в виртуальную среду

Подготовка

1. Загрузить образ системы: Ubuntu 24.04[1]
2. Изучить *системные требования*

Важно

При работе в виртуальной среде:

- Убедитесь, что ваш процессор поддерживает технологии аппаратной виртуализации
- Активируйте опцию виртуализации в настройках BIOS/UEFI вашего компьютера

Перед началом установки с ISO-образа в виртуальную машину необходимо предварительно установить платформу виртуализации: **VirtualBox**, **VMware** или аналогичную

Установка

1. Загрузиться с ISO-образа
2. В загрузочном меню выбрать один из вариантов установки:

[1] https://storage.rudesktop.ru/download/rudesktop_server_ub24.iso



- Install RuDesktop Server — предназначен для установки с доступом к интернету

Важно

В данном сценарии конфигурация **cloud-init** указывает загрузку пакетов из внешних источников

Примечание

Такой подход гарантирует получение самых последних версий всех компонентов, включая исправления ошибок и устранение уязвимостей безопасности

- Install RuDesktop Server without internet access — предназначен для установки в изолированной среде без доступа в интернет

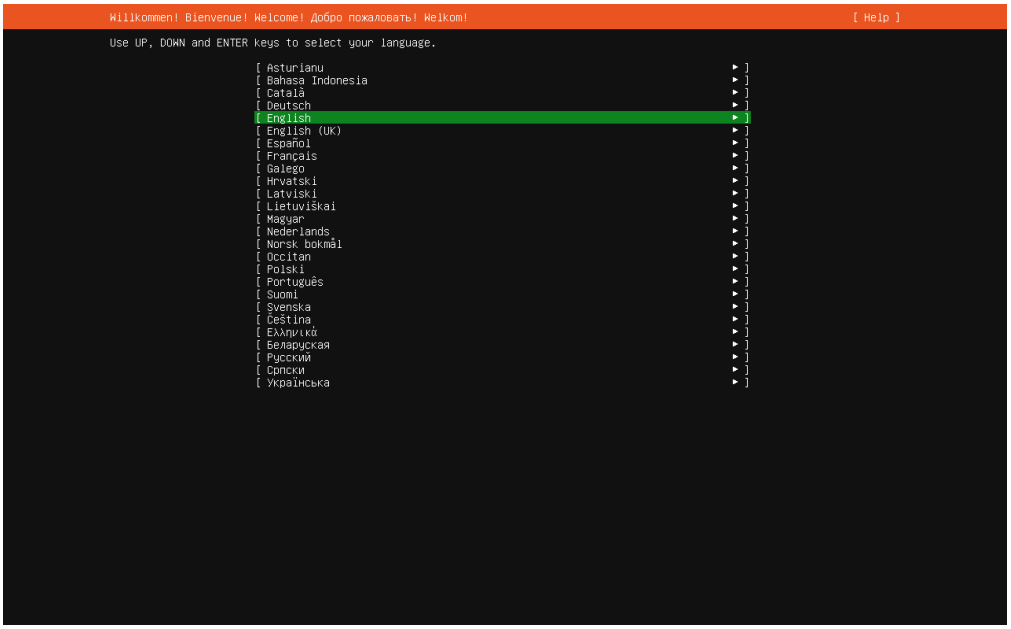
Важно

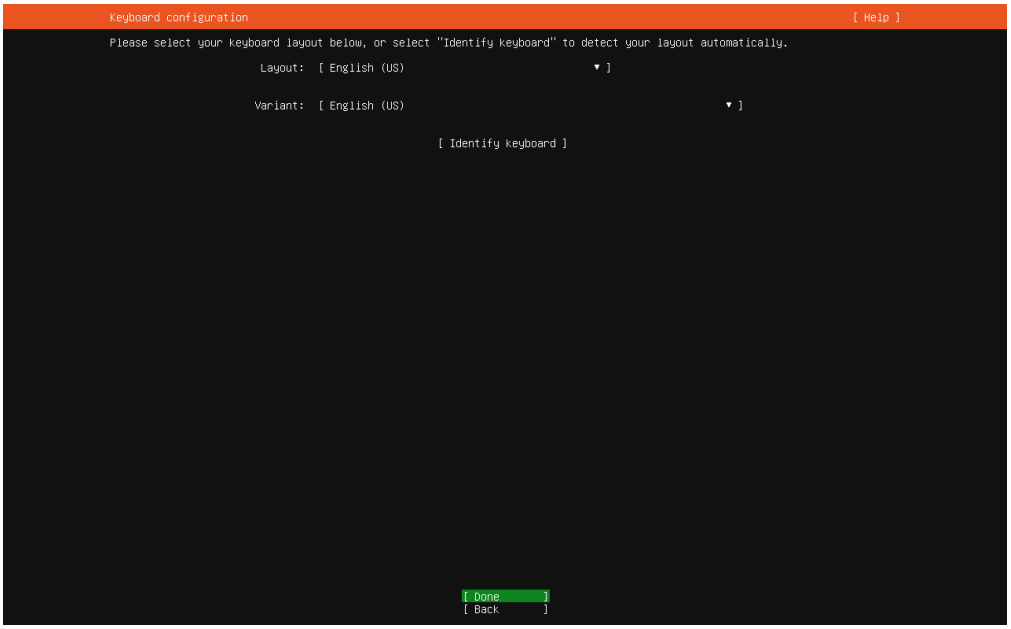
В данном сценарии конфигурация **cloud-init** указывает на установку пакетов из локального каталога `server/extras/`, расположенного внутри самого ISO-образа

Подсказка

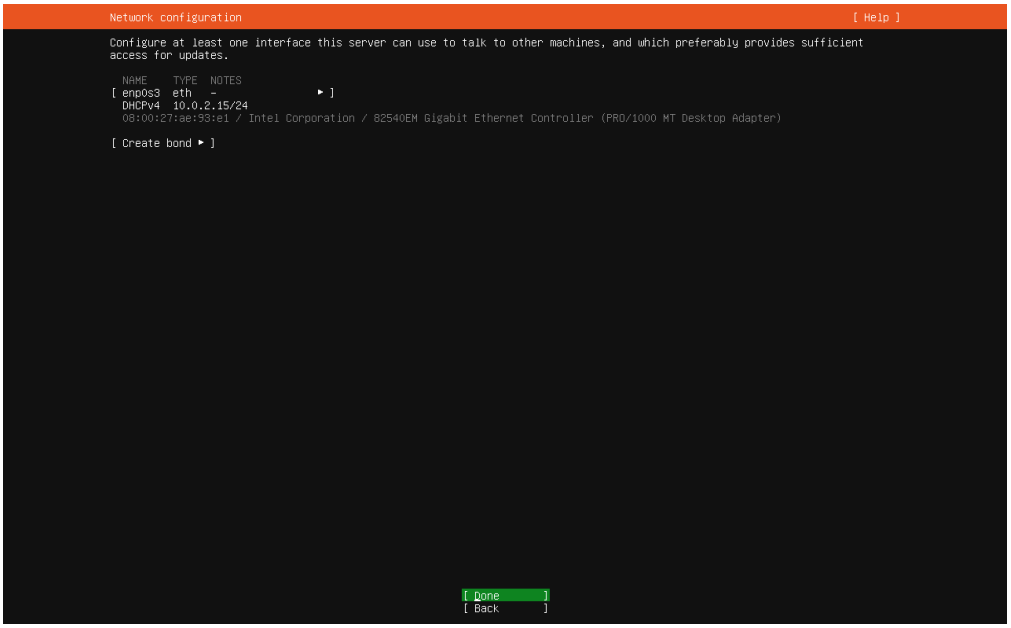
Если в течение 30 секунд не будет сделан выбор, система автоматически активирует таймаут и запустит вариант по умолчанию Install RuDesktop Server, после чего начнется процесс установки

3. Выбрать язык интерфейса и раскладку клавиатуры

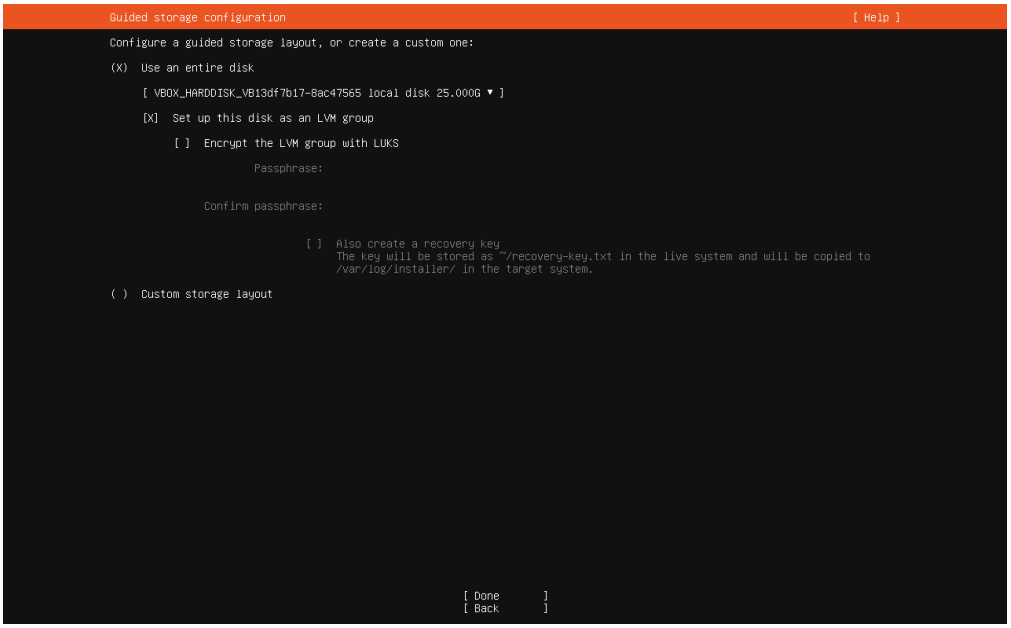


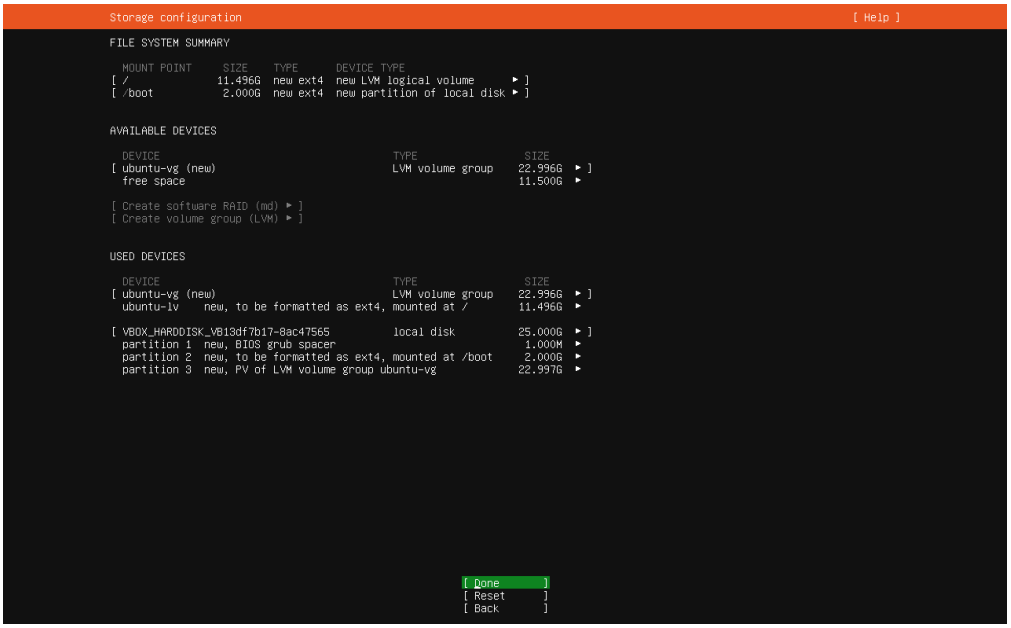


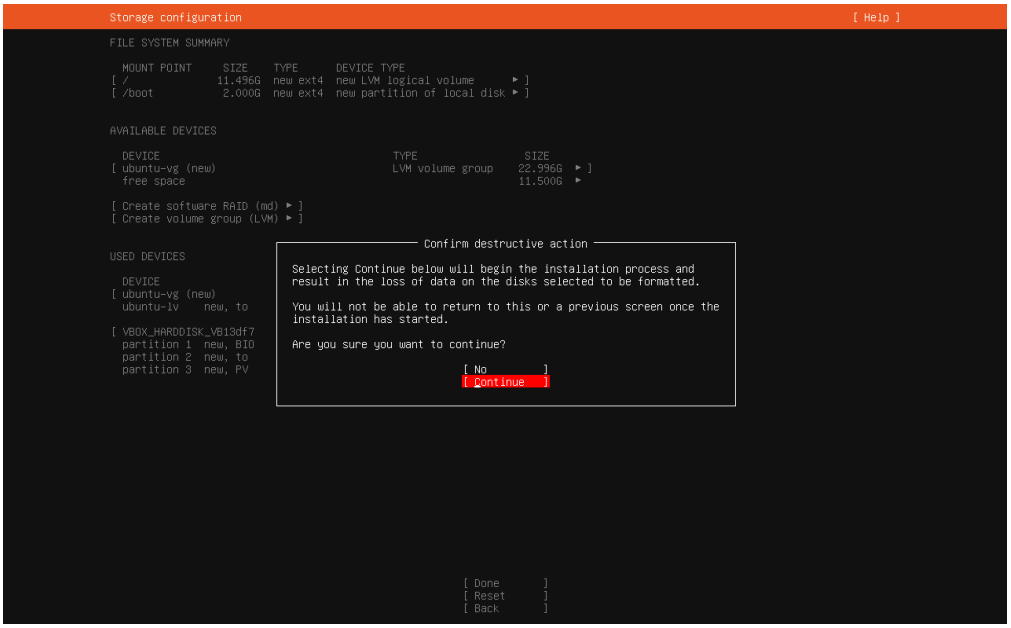
4. Настроить сеть



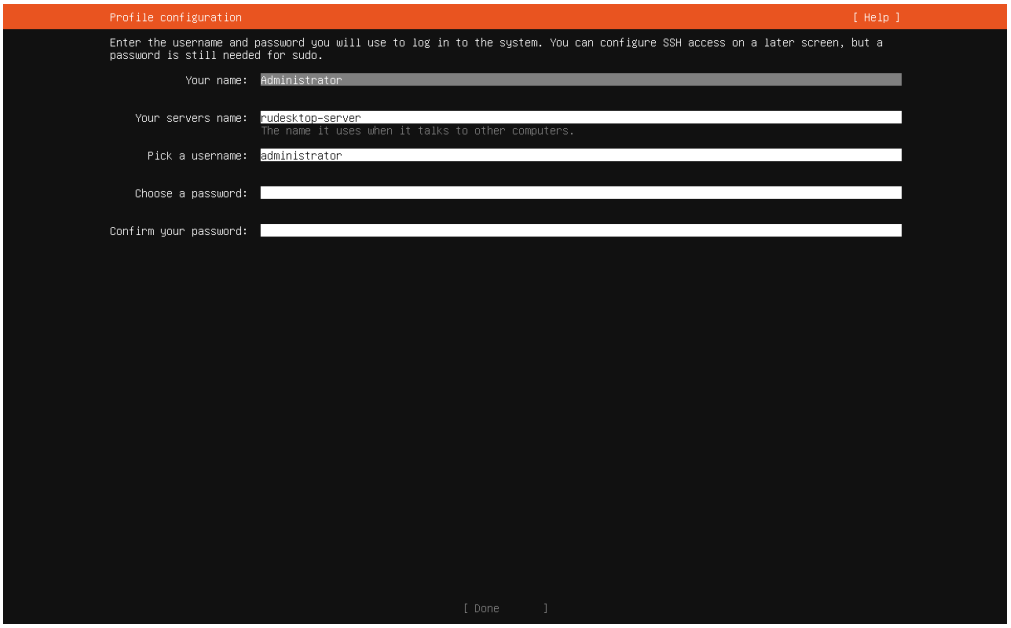
5. Настроить диск



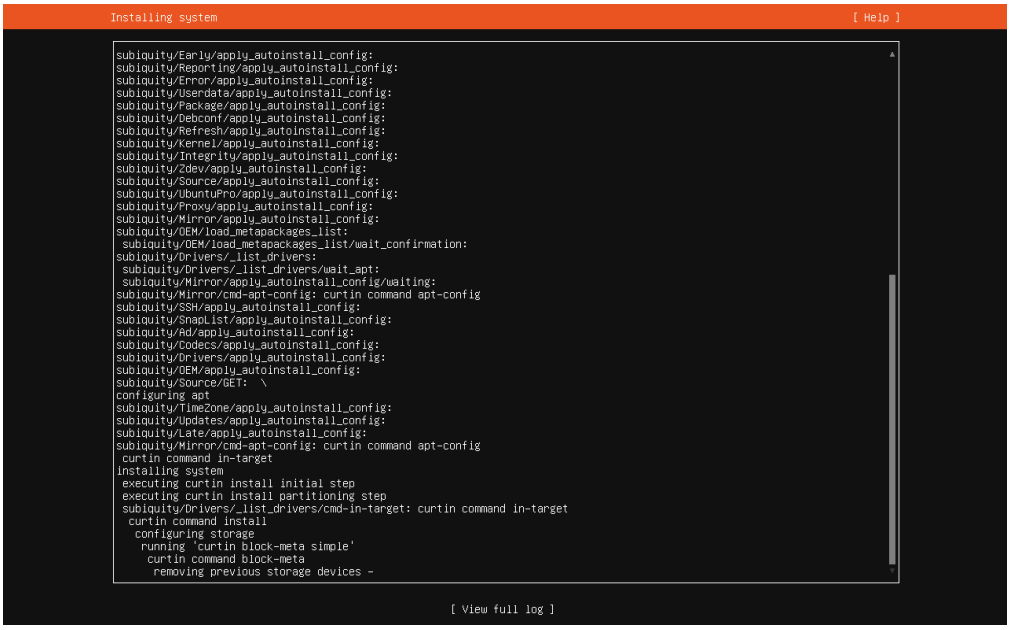




6. Задать имя сервера и создать пользователя



7. Дождаться завершения установки и автоматической перезагрузки операционной системы



Важно

При установке с использованием **VirtualBox** после завершения инсталляции и перезагрузки может появиться сообщение об ошибке размонтирования ISO-образа

Это сообщение не является ошибкой установки и не влияет на работоспособность системы

Действия для продолжения:

- Нажмите клавишу `Enter`

Виртуальная машина корректно завершит работу с установочным носителем

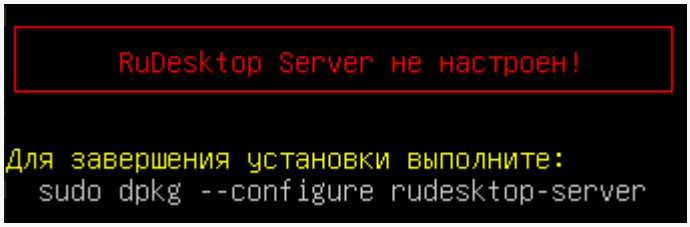
Система автоматически продолжит загрузку с только что установленной операционной системы

8. После перезагрузки ОС сервер **RuDesktop** будет установлен, но не настроен
9. Для настройки сервера **RuDesktop** выполните команду:

```
sudo dpkg --configure rudesktop-server
```

Важно

До момента выполнения указанной команды сервер **RuDesktop** останется в неподготовленном состоянии, а при каждом входе в систему будет появляться уведомление:



Завершение установки

Создание суперпользователя

После установки серверной части вам потребуется создать суперпользователя для доступа к веб-интерфейсу сервера **RuDesktop**

Для этого необходимо выполнить следующую команду:

```
rude createsuperuser
```

После выполнения команды необходимо ввести следующие данные:

```
Логин: [ввести_имя_пользователя]
Электронная почта: [ввести_email_пользователя]
Password: [ввести_пароль]
Password (again): [повторить_пароль]
Superuser created successfully
```

Активация лицензии

Выполнить активацию лицензии *по инструкции*

Смена адреса сервера

Если требуется, можно сменить адрес сервера *по инструкции*

Прочие настройки

- Сетевые настройки можно изучить в *Сетевые настройки*
- Команды сервера можно изучить в *Команды сервера*

Безопасность

Избегайте прямого доступа к серверу из внешней сети через SSH-протокол

При необходимости SSH-доступа строго соблюдайте меры защиты:

- Используйте аутентификацию по SSH-ключам вместо парольного входа
- Смените стандартный порт подключения (22) на произвольный нестандартный
- Настройте ограничение доступа по IP-адресам (firewall rules)
- Регулярно обновляйте SSH-сервер до актуальных версий

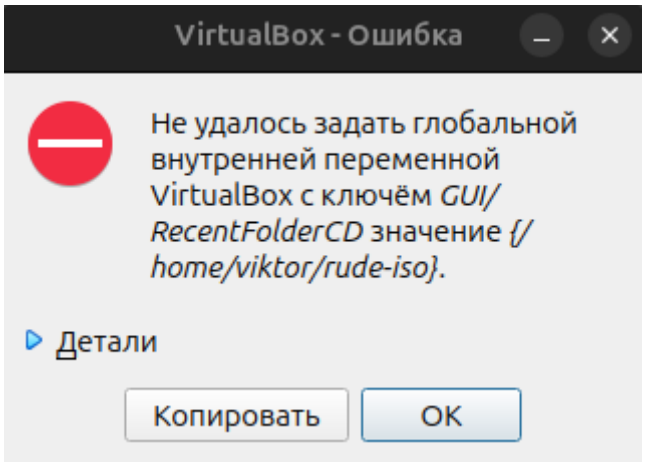
Важно

Эти меры существенно снижают риск несанкционированного доступа и автоматических атак на SSH-сервис

Возможные проблемы

VirtualBox

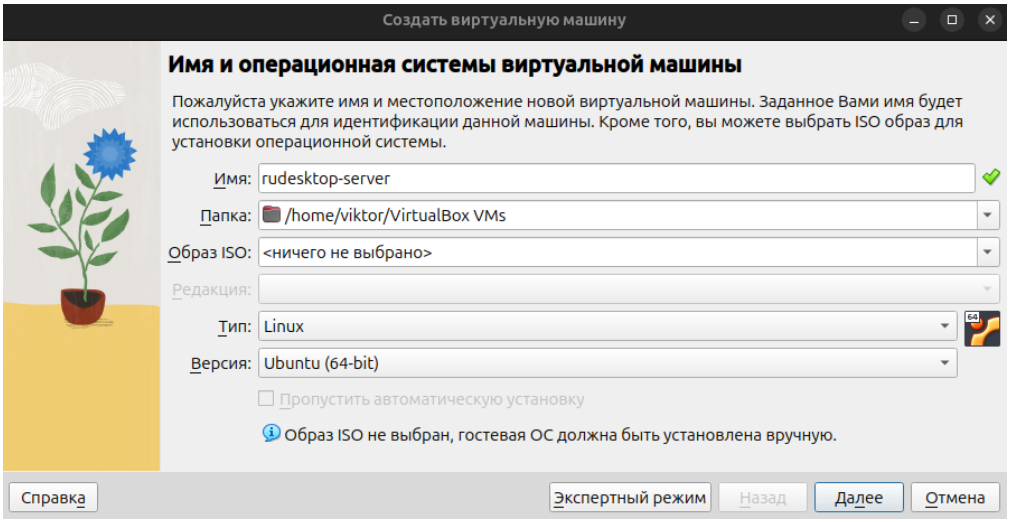
При выборе ISO в VirtualBox может появиться ошибка при выборе ISO файла при создании виртуальной машины



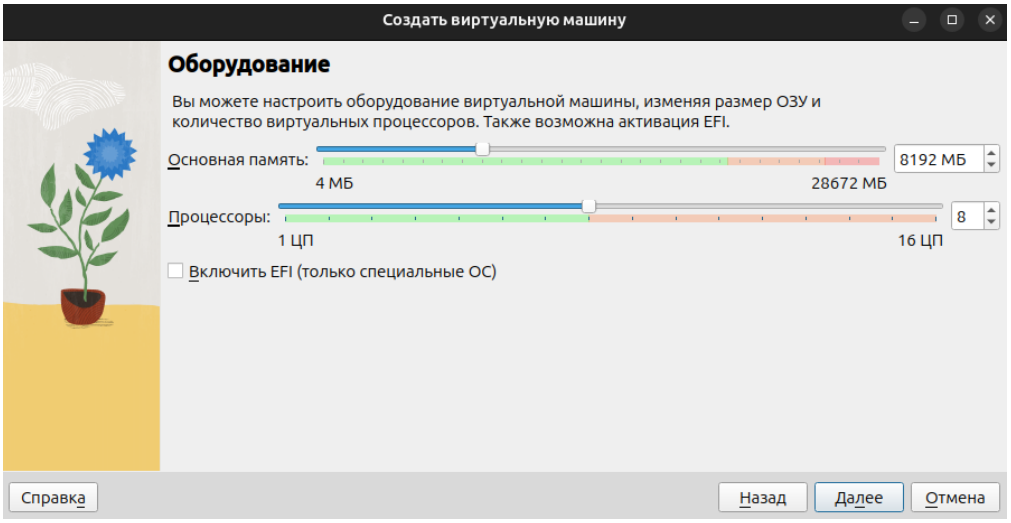
Решается тем, что создаем виртуальную машину без указания ISO файла и после создания выбираем ISO файл

1. Открыть **VirtualBox**

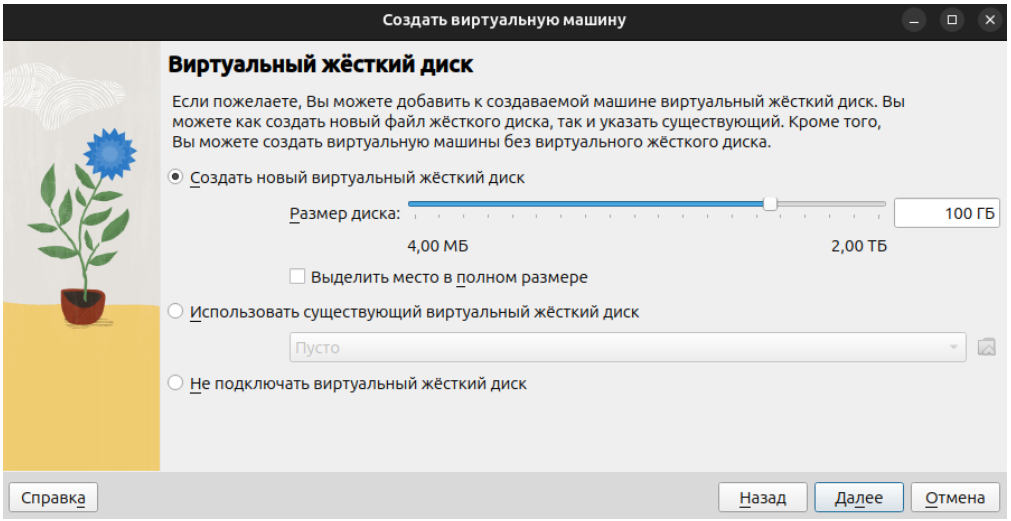
2. Нажать на кнопку **Создать**
3. В появившемся окне заполнить поля:
    - Имя: — Введите любое желаемое имя виртуальной машины, например **rudesktop-server**
    - Тип: — Выбираем **Linux**
    - Версия: — Выбираем **Ubuntu (64-bit)**



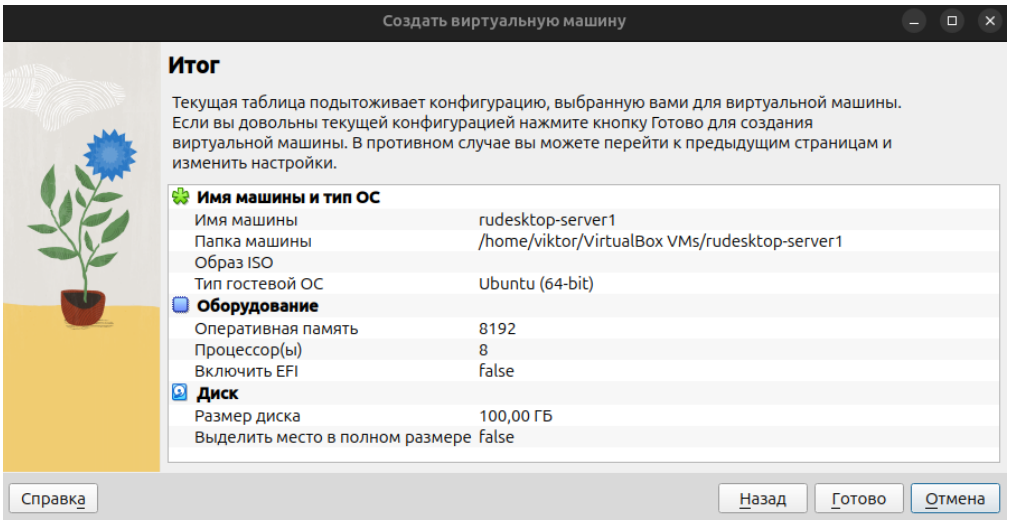
4. Нажимаем на кнопку Далее
5. Выбираем желаемое количество оперативной памяти и количество ядер процессора



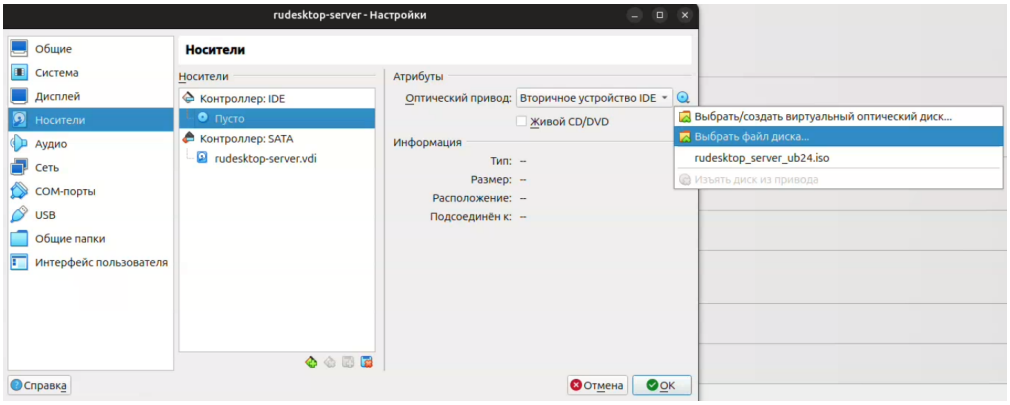
6. Нажимаем на кнопку Далее
7. Настраиваем жесткий диск, указываем размер диска



8. Нажимаем на кнопку Далее
9. Нажимаем на кнопку Готово



10. В списке появится новая созданная виртуальная машина, нажимаем на нее правой кнопкой и выбираем пункт Настроить
11. В появившемся окне выбираем категорию Носители
12. В колонке **Носители** находим Контроллер: IDE и нажимаем на **Пусто**
13. В колонке **Атрибуты** нажимаем на иконку диска и в появившемся меню выбираем пункт Выбрать файл диска... и выбираем загруженный ISO файл



14. Нажимаем на кнопку OK
15. Запускаем виртуальную машину и начинаем процесс установки ОС (см. раздел **Установка** выше на этой странице)

1.3.2 Установка в закрытый контур

Установка в закрытый контур — инструкция по развёртыванию сервера **RuDesktop** на изолированной площадке без доступа в интернет: установка из заранее скачанного архива и настройка локального репозитория для последующих обновлений

Установка

Важно

Если вы используете операционную систему Astra Linux (версии Воронеж или Смоленск), перед установкой сервера **RuDesktop** *отключите МКЦ* в соответствии с инструкцией

Для установки сервера **RuDesktop** в закрытом контуре без доступа к интернету выполните следующие шаги:

1. Скачайте архив

   Подсказка

   Архив можно запросить, обратившись в техническую поддержку компании **RuDesktop** по адресу support@rudesktop.ru

2. Распакуйте архив командой:

   ```
   tar -xvf /path/to/[ИМЯ_АРХИВА].tar.gz -C /
   ↪path/to/[ИМЯ_ПАПКИ]
   ```

3. Выполните команду установки сервера:

   Ubuntu/Debian/Astra/ОСнова

```
dpkg -i /path/to/folder/*.deb

или

apt install /path/to/folder/*.deb

или

apt-get install /path/to/folder/*.deb
```

РЕД ОС/Fedora/ROSA Linux

```
dnf install /path/to/folder/*.rpm
```

ALT Linux

```
apt-get install /path/to/folder/*.rpm

или

rpm -i /path/to/folder/*.rpm
```

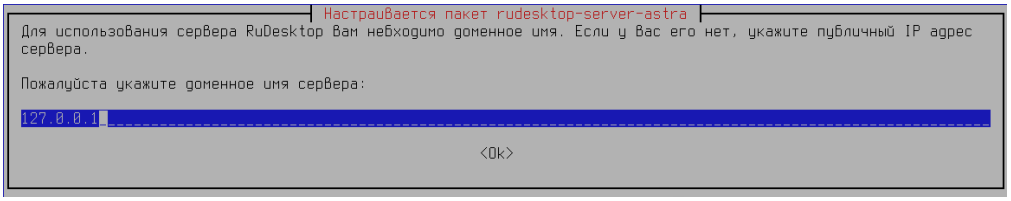
CentOS

```
dnf install /path/to/folder/*.rpm

или

yum install /path/to/folder/*.rpm
```

Примечание

Данная команда запустит установку всех пакетов из папки, которые необходимы для работы сервера

4. Во время установки сервера необходимо указать IP-адрес или доменное имя сервера



Важно

По умолчанию используется локальный IP-адрес

Для `.rpm` пакетов такой настройки нет, и после установки сервера следует обязательно выполнить команду *rude reinstall*

После выполнения команды в выводе отобразится следующая информация:

```
Stopping services
    Stopping nginx ...              OK
    Stopping web socket ...         OK
    Stopping web service ...        OK
    Stopping relay ...              OK
    Stopping ansible processes ... OK
    Stopping executor ...           OK
    Stopping pxe ...                OK
    Stopping smbd ...               OK
Starting services
    Start web socket ...            OK
    Start web service ...           OK
    Start relay ...                 OK
    Start executor ...              OK
    Start smbd ...                  OK
    Enable nginx ...                OK
    Start nginx ...                 OK
```

Создание суперпользователя

После установки серверной части вам потребуется создать суперпользователя для доступа к веб-интерфейсу сервера **RuDesktop**

Для этого необходимо выполнить следующую команду:

```
rude createsuperuser
```

После выполнения команды необходимо ввести следующие данные:

```
Логин: [ввести_имя_пользователя]
Электронная почта: [ввести_email_пользователя]
Password: [ввести_пароль]
Password (again): [повторить_пароль]
Superuser created successfully
```

1.3.3 Установка модуля аналитики

Доступно только в UEM версии

Установка модуля аналитики — установка отдельного пакета `rudesktop-superset` (встроенный **Apache Superset**), который служит для организации, обработки и визуализации данных из базы сервера **RuDesktop**

Важно

Если планируется установить сервер и активировать УД лицензию без UEM, то устанавливать модуль аналитики не нужно

Подсказка

После установки модуль управляется командами *rude superset start*, *stop*, *restart*, *status*, *backup* и *restore*

Установка DEB пакета

Используйте эту инструкцию для установки на следующие операционные системы:

Примечание

- Ubuntu
- Debian
- Astra
- ОСнова

Репозиторий используется тот же, что и для сервера **RuDesktop** — см. *Установку DEB пакета*

Установка модуля аналитики через пакетный менеджер

```
apt-get install rudesktop-superset -y
```

Обновление модуля аналитики через пакетный менеджер

```
apt-get install --only-upgrade rudesktop-superset -y
```

Установка RPM пакета

Используйте эту инструкцию для установки на следующие операционные системы:

Примечание

- ALT Linux
- AlterOS
- РЕД ОС
- РОСА
- МСВСфера
- CentOS
- Fedora

Важно

Репозиторий доступен для РЕД ОС, AlterOS и МСВСфера

Для установки на другие операционные системы скачайте .rpm пакет и установите его вручную через пакетный менеджер

Репозиторий используется тот же, что и для сервера **RuDesktop** — см. *Установку RPM пакета*

Установка модуля аналитики через пакетный менеджер

РЕД ОС/AlterOS/РОСА/МСВСфера/Fedora

```
dnf install rudesktop-superset -y
```

ALT Linux

```
apt-get install /path/to/folder/rudesktop-superset.rpm -y
```

Или

```
rpm -i /path/to/folder/rudesktop-superset.rpm
```

CentOS

```
dnf install /path/to/folder/rudesktop-superset.rpm -y
```

Или

```
yum install /path/to/folder/rudesktop-superset.rpm -y
```

Обновление модуля аналитики через пакетный менеджер

РЕД ОС/AlterOS/РОСА/МСВСфера/Fedora

```
dnf update rudesktop-superset -y
```

ALT Linux

```
apt-get install /path/to/folder/rudesktop-superset.rpm -y
```

Или

```
rpm -i /path/to/folder/rudesktop-superset.rpm
```

CentOS

```
dnf install /path/to/folder/rudesktop-superset.rpm -y
```

Или

```
yum install /path/to/folder/rudesktop-superset.rpm -y
```

Ссылки

Прямая ссылка на DEB-пакет[2]

[2] https://storage.rudesktop.ru/repos/stable3.1/pool/non-free/r/rudesktop-superset/rudesktop-superset-1.0.43.deb

Прямая ссылка на RPM-пакет[3]

[3] https://storage.rudesktop.ru/repos/stable3.1/rpms/rudesktop-superset-1.0.43.rpm

1.3.4 Установка сервера на Astra с МКЦ

Установка сервера на Astra с МКЦ — последовательность действий по подготовке Astra Linux Special Edition (1.7/1.8) к установке сервера **RuDesktop**: временное отключение **МКЦ** и **МРД** для создания управляющей учётной записи и обратное включение защитных механизмов

Описание

Для **ALSE 1.7/1.8** необходимо вкл/выкл МКЦ (Мандатный контроль целостности) и МРД (Мандатное управление доступом), чтобы создать управляющую учетную запись **RuDesktop**

Важно

Если не отключать МКЦ и МРД, то при создании пользователя возникнет ошибка `PAM account manager`

На установку сервера **RuDesktop** влияют два механизма безопасности **Astra Linux Special Edition**, которые необходимо временно отключить:

МКЦ — представляет собой механизм, который контролирует целостность информации и системных компонентов

Примечание

Его главная задача предотвратить модификацию данных и системных файлов неавторизованными или менее надежными процессами

МРД — представляет собой механизм, который контролирует конфиденциальность информации

Примечание

Его главная задача предотвратить утечку данных на основе их уровня допуска пользователя и уровня секретности информации

Подсказка

Третий механизм защиты **ALSE** — ЗПС (Замкнутая программная среда) — на установку сервера обычно не влияет и в инструкции не используется. Описание термина — в Глоссарии

Установка

Для установки сервера **RuDesktop** необходимо временно отключить встроенную защиту операционной системы:

1. Выключить МКЦ и МРД

   Есть два способа отключить МКЦ и МРД

   - Через команды:

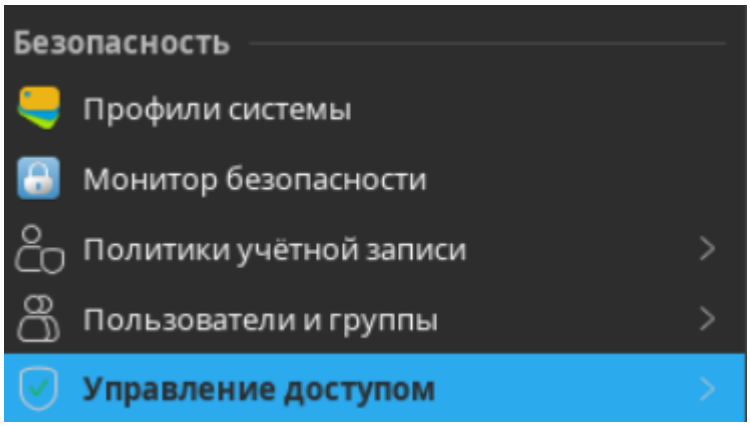
     ```
     sudo astra-mac-control disable
     ```

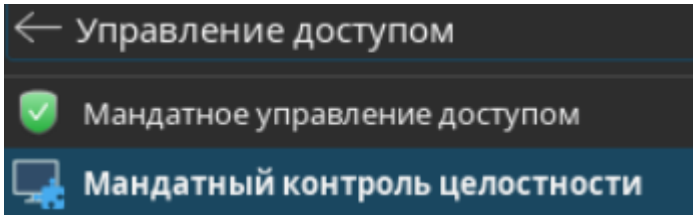
     И

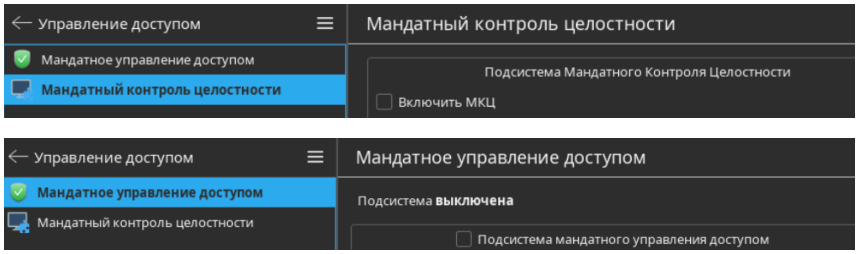
     ```
     sudo astra-mic-control disable
     ```

   - Через GUI:

     Параметры системы → Безопасность → Управление доступом → МКЦ / МРД







2. Перезагрузить систему
3. Осуществить установку сервера по инструкции *Установка\обновление сервера*
4. Включить МКЦ и МРД можно аналогично через GUI или через команды:

```
sudo astra-mac-control enable
```

И

```
sudo astra-mic-control enable
```

5. Перезагрузить систему

Сервер **RuDesktop** готов к работе

Установка/обновление сервера — инструкции по развёртыванию сервера **RuDesktop** в виде DEB- или RPM-пакета и его последующего обновления, а также созданию суперпользователя для входа в веб-интерфейс. Для отдельных сценариев есть выделенные страницы: *установка из ISO-образа*, *в закрытый контур*, *на Astra с МКЦ* и *установка модуля аналитики Apache Superset*

Предупреждение

При обновлении до версии 3.1 убедитесь, что у вас установлена версия **PostgreSQL** 14 или выше

Инструкции по миграции на новую версию PostgreSQL

Важно

Если у вас версия лицензии, например 2.9, и вы собираетесь обновить сервер, например до версии 3.1, при обновлении возникнет ошибка из-за несоответствия ключа лицензии, но после ошибки произойдет откат на предыдущую версию сервера

Чтобы избежать этой ошибки, выполните следующие шаги:

1. Запросите новый ключ, обратившись в отдел продаж компании **RuDesktop** по адресу sales@rudesktop.ru или к Вашему менеджеру
2. Обновите лицензионный ключ на странице *Лицензия*
3. Начните процедуру по обновлению сервера

1.3.5 Установка DEB пакета

Используйте эту инструкцию для установки на следующие операционные системы:

Примечание

- Ubuntu
- Debian
- Astra
- ОСнова

Важно

Если вы используете операционную систему Astra Linux (версии Воронеж или Смоленск), перед установкой сервера **RuDesktop** *отключите МКЦ* в соответствии с инструкцией

Установка или обновление одной командой

```
bash -c "$(wget -O - https://storage.rudesktop.ru/repos/stable3.1/
↪install-rudesktop-server-stable3.1-deb.sh)"
```

Репозиторий

```
deb https://storage.rudesktop.ru/repos/stable3.1 stable3.1 non-free
```

Добавление репозитория и публичного ключа

```
mkdir -p /usr/share/keyrings/
wget -qO - ␣
↪https://storage.rudesktop.ru/repos/stable3.1/rudesktop.gpg | sudo␣
↪gpg --dearmor -o /usr/share/keyrings/rudesktop.gpg
echo "deb [signed-by=/usr/share/keyrings/rudesktop.gpg]␣
↪https://storage.rudesktop.ru/repos/stable3.1 stable3.1 non-free"␣
↪| sudo tee /etc/apt/sources.list.d/rudesktop.list
apt-get update -y
```

Установка сервера через пакетный менеджер

```
apt-get install rudesktop-server -y
```

Обновление сервера через пакетный менеджер

```
apt-get install --only-upgrade rudesktop-server -y
```

Подсказка

При минорном обновлении база данных автоматически сохраняется в резервную копию — см. *Резервная копия при обновлении*

1.3.6 Установка RPM пакета

Используйте эту инструкцию для установки на следующие операционные системы:

Примечание

- ALT Linux
- AlterOS
- РЕД ОС
- РОСА
- МСВСфера
- CentOS
- Fedora

Установка или обновление одной командой

Важно

Установка или обновление сервера одной командой работает для `РЕД ОС`, `AlterOS` и `МСВСфера`

Для установки или обновления сервера на другие операционные системы скачайте `.rpm` пакет и установите его вручную через пакетный менеджер

```
bash -c "$(wget -O - https://storage.rudesktop.ru/repos/stable3.1/
↪install-rudesktop-server-stable3.1-rpm.sh)"
```

Добавление репозитория

Важно

Репозиторий доступен для `РЕД ОС`, `AlterOS` и `МСВСфера`

Для установки на другие операционные системы скачайте `.rpm` пакет и установите его вручную через пакетный менеджер

Добавить файл `/etc/yum.repos.d/rudesktop.repo` со следующим содержимым:

```
[rudesktop]
name=Rudesktop
baseurl=https://storage.rudesktop.ru/repos/stable3.1/rpms
gpgcheck=0
enabled=1
```

Установка сервера через пакетный менеджер

РЕД ОС/AlterOS/РОСА/МСВСфера/Fedora

```
dnf install rudesktop-server -y
```

ALT Linux

```
apt-get install /path/to/folder/rudesktop-server.rpm -y
```

Или

```
rpm -i /path/to/folder/rudesktop-server.rpm
```

CentOS

```
dnf install /path/to/folder/rudesktop-server.rpm -y
```

Или

```
yum install /path/to/folder/rudesktop-server.rpm -y
```

Важно

Для `.rpm` пакетов после установки сервера следует обязательно выполнить команду *rude reinstall*

Предупреждение

При выполнении данной команды на ALT Server необходимо указать порт отличный от 443

Обновление сервера через пакетный менеджер

РЕД ОС/AlterOS/РОСА/МСВСфера/Fedora

```
dnf update rudesktop-server -y
```

ALT Linux

```
apt-get install /path/to/folder/rudesktop-server.rpm -y
```

Или

```
rpm -i /path/to/folder/rudesktop-server.rpm
```

CentOS

```
dnf install /path/to/folder/rudesktop-server.rpm -y
```

Или

```
yum install /path/to/folder/rudesktop-server.rpm -y
```

Подсказка

При минорном обновлении база данных автоматически сохраняется в резервную копию — см. *Резервная копия при обновлении*

1.3.7 Резервная копия при обновлении

При обновлении на минорную версию (например, с версии 2.7 на 2.8) база данных автоматически сохраняется в виде резервной копии по пути:

```
/var/lib/rudesktop/
```

Поведением можно управлять через переменные окружения:

- `SKIP_BACKUP=true` — пропустить создание резервной копии
- `BACKUP_PATH="/path/to/file.gz"` — сохранить копию по указанному пути

Примеры:

DEB

Пропустить создание резервной копии:

```
SKIP_BACKUP=true apt-get install --only-upgrade rudesktop-server -y
```

Сохранить резервную копию по своему пути:

```
BACKUP_PATH="/home/rude/upgrade_backup.gz" apt-get install --
↪only-upgrade rudesktop-server -y
```

RPM

Пропустить создание резервной копии:

```
SKIP_BACKUP=true dnf update rudesktop-server -y
```

Сохранить резервную копию по своему пути:

```
BACKUP_PATH="/home/rude/upgrade_backup.gz" dnf update␣
↪rudesktop-server -y
```

1.3.8 Создание суперпользователя

После установки серверной части вам потребуется создать суперпользователя для доступа к веб-интерфейсу сервера **RuDesktop**

Для этого необходимо выполнить следующую команду:

```
rude createsuperuser
```

После выполнения команды необходимо ввести следующие данные:

```
Логин: [ввести_имя_пользователя]
Электронная почта: [ввести_email_пользователя]
Password: [ввести_пароль]
Password (again): [повторить_пароль]
Superuser created successfully
```

Подсказка

После создания суперпользователя вы можете войти в веб-интерфейс по адресу `https://[адрес_сервера]/` с указанными логином и паролем. Для смены пароля используйте *changepassword*

1.3.9 Ссылки

Скрипт установки DEB-пакета[4]
Скрипт установки RPM-пакета[5]

[4] https://storage.rudesktop.ru/repos/stable3.1/install-rudesktop-server-stable3.1-deb.sh
[5] https://storage.rudesktop.ru/repos/stable3.1/install-rudesktop-server-stable3.1-rpm.sh

Прямая ссылка на DEB-пакет[6]
Прямая ссылка на RPM-пакет[7]

[6] https://storage.rudesktop.ru/repos/stable3.1/pool/non-free/r/rudesktop-server/rudesktop-server-stable-3.1.576.deb
[7] https://storage.rudesktop.ru/repos/stable3.1/rpms/rudesktop-server-stable-3.1.576.rpm

1.4 Сетевые настройки

1.4.1 Добавление собственных SSL-сертификатов

Добавление собственных SSL-сертификатов — замена встроенных самоподписанных сертификатов на доверенные (например, выданные корпоративным центром сертификации или Let's Encrypt). Раздел описывает два сценария — прямую запись в `/var/lib/rudesktop/ca/` и переопределение через `nginx`

Важно

Перед заменой сертификатов рекомендуется сделать резервную копию каталога `/var/lib/rudesktop/ca/` — *rude reinstall* удаляет файлы CA, поэтому они не сохраняются автоматически

Примечание

Встроенный `nginx` отдаёт заголовок `Strict-Transport-Security: max-age=31536000; includeSubDomains`. Это означает, что браузер, один раз открывший веб-интерфейс по HTTPS, будет принудительно использовать HTTPS на этом домене ещё год — даже при последующих попытках обратиться по `http://`. Учитывайте это, если планируете временно откатываться на HTTP или менять схему публикации

Модулю аналитики требуется сертификат в формате **full-chain**: без промежуточных сертификатов вход в модуль завершается ошибкой «Отказано в доступе» — подробнее в разделе «Работа с корпоративным сертификатом» статьи *Смена адреса для модуля аналитики*

Добавление сертификата и ключа напрямую в /var/lib/rudesktop/ca/

Важно

Стандартные кейсы: необходимо защитить подключение с помощью корпоративного сертификата. В структуре отсутствует мост **RuDesktop** для балансировки нагрузки. Если требуется единый сертификат на несколько поддоменов — используйте wildcard

1. Скопируйте файлы сертификата `full-chain` и ключа в следующие директории:

```
/var/lib/rudesktop/ca/CA.pem
/var/lib/rudesktop/ca/CA.key
```

Важно

Содержимое должно быть в следующем формате:

```
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
...
-----END RSA PRIVATE KEY-----
```

Не удаляйте существующие сертификаты **RuDesktop**, добавляйте новые строки под уже имеющимися блоками

Примечание

Пути к этим файлам можно переопределить через переменные окружения `CA_CERT_PATH` и `CA_KEY_PATH` для нативного компонента `relay` / `rz`

2. Перезапустите сервер **RuDesktop**:

```
rude restart
```

После этого сервер будет работать с добавленным сертификатом

Добавление сертификата с изменением конфигурации nginx

Важно

Стандартные кейсы: в структуре используется мост **RuDesktop** для балансировки нагрузки или сертификат должен обслуживать только веб-интерфейс, а не нативный канал `relay` / `rz`. В этом случае сертификат подключается на уровне `nginx`, а не записывается в `CA.pem` / `CA.key`

1. Скопируйте файлы сертификата `full-chain` (например, `wc.pem` и `wc.key`) в указанную директорию:

```
/etc/ssl/private
```

2. Откройте конфигурацию nginx:

```
nano /etc/nginx/sites-enabled/rudesktop
```

3. Замените пути к сертификатам, например:

```
ssl_certificate     /etc/ssl/private/wc.pem;
ssl_certificate_key /etc/ssl/private/wc.key;
```

4. Проверьте конфигурацию nginx:

```
nginx -t
```

5. Укажите пути до сертификатов в `/etc/rudesktop-relay.toml` (для нативного компонента `relay` / `rz`):

```
ca_cert = "/path/to/cert"
ca_key = "/path/to/key"
```

> **Важно**
>
> Если файл `/etc/rudesktop-relay.toml` отсутствует, создайте его в указанной директории и убедитесь, что в `/etc/default/rudesktop` задан `RELAY_ARGS='-C /etc/rudesktop-relay.toml'`

6. Перезапустите сервер **RuDesktop**:

```
rude restart
```

После этого сервер будет работать с добавленным сертификатом

1.4.2 Смена и установка IP

Смена и установка IP — описание процедур изменения IP-адреса (или доменного имени) сервера **RuDesktop** через команды установки. Также описан режим использования двух адресов (например, для разных сетевых интерфейсов)

Смена IP-адреса сервера

Чтобы изменить IP-адрес сервера, в терминале на устройстве, где установлен сервер, выполните следующую команду:

```
rude install [СЕРВЕР]:[ПОРТ]
```

> **Подсказка**
>
> Указывать порт необязательно — по умолчанию используется 443. Подробно — на странице команды *install*

Смена IP-адреса сервера со сбросом данных

Чтобы изменить IP-адрес сервера с удалением локальной конфигурации и корневого CA, выполните:

```
rude reinstall [СЕРВЕР]:[ПОРТ]
```

Важно

Команда **деструктивная**: удаляет `/etc/default/rudesktop`, `/etc/rudesktop/`, конфиги nginx и корневой CA. После выполнения клиенты потеряют доверие к серверу. Подробно — на странице команды *reinstall*

Подсказка

Указывать порт необязательно — по умолчанию используется 443

Добавление двух IP-адресов на сервере

Чтобы сервер слушал на двух IP-адресах (например, на внутреннем и публичном интерфейсе одновременно), необходимо:

1. В терминале выполните установку с двумя адресами:

```
rude reinstall [СЕРВЕР_1]:[ПОРТ_1] [СЕРВЕР_2]:[ПОРТ_2]
```

Подсказка

Указывать порт необязательно — по умолчанию используется 443

Важно

`rude reinstall` удаляет `/etc/default/rudesktop` перед переустановкой, поэтому флаг `RELAY_ARGS` нужно добавлять **после** этого шага, а не до — иначе он будет затёрт

2. В файл `/etc/default/rudesktop` добавьте флаг для relay:

```
RELAY_ARGS='--usepublicip'
```

Примечание

Флаг `--usepublicip` (короткий вариант `-p`) включает в нативном компоненте `relay` / `rz` режим, при котором клиенту в качестве адреса ретранслятора возвращается тот же узел, по которому клиент сам подключился к серверу. Используется при нескольких сетевых интерфейсах, чтобы клиенты из внутренней и внешней сети получали свой адрес

3. Перезапустите сервер, чтобы новый `RELAY_ARGS` вступил в силу:

```
rude restart
```

1.4.3 Смена стандартного порта

Смена стандартного порта — изменение TCP-порта, на котором `nginx` принимает соединения с веб-интерфейсом сервера и клиентами **RuDesktop**

Для смены стандартного порта 443 сервера необходимо:

1. Отредактировать файл по пути `/etc/nginx/sites-enabled/rudesktop`:

   Найти блок `server { со строкой listen 443 ssl;` и заменить значение 443 на удобный порт:

```
server {

  server_name 192.168.10.10;

  listen 8443 ssl;
```

   Важно

   В файле есть второй `server { с listen 80;` — это HTTP-блок, который принудительно редиректит на HTTPS строкой `return 301 https://$host$request_uri;`. По умолчанию он отправляет клиента на `https://<host>` без явного порта (то есть на 443). Если вы перешли на нестандартный порт, замените редирект на `return 301 https://$host:<новый_порт>$request_uri;` — иначе HTTP-обращения по адресу сервера будут вести в никуда

2. Проверить корректность конфигурации nginx:

```
nginx -t
```

3. Перезагрузить сервер:

```
rude restart
```

Важно

Не забудьте открыть выбранный порт в межсетевом экране сервера и в правилах сетевого периметра. Клиенты **RuDesktop**, ранее подключённые к стандартному порту, потребуют переподключения с указанием нового адреса `host:port`

1.4.4 Смена адреса для модуля аналитики

Смена адреса для модуля аналитики — настройка публичного и локального адресов и портов встроенного **Apache Superset**, а также подключения к его базе данных через переменные окружения

Смена адреса и порта

Для смены адреса или порта модуля аналитики необходимо:

1. В файл по пути `/etc/default/rudesktop` добавить следующие строки:

```
SUPERSET_PUBLIC_HOST='PUBLIC_IP'
SUPERSET_PUBLIC_PORT='PUBLIC_PORT'
SUPERSET_LOCAL_HOST='LOCAL_IP'
SUPERSET_LOCAL_PORT='LOCAL_PORT'
```

Важно

Вы можете индивидуально переопределить параметры IP-адреса или порта модуля аналитики, используя соответствующие переменные окружения, а не все сразу

2. Перезагрузить модуль аналитики командой:

```
rude superset restart
```

Вынос базы данных модуля аналитики на отдельный сервер

По умолчанию модуль аналитики хранит свои данные в базе `superset` на том же сервере PostgreSQL, что и сервер **RuDesktop** (параметры подключения наследуются от `POSTGRES_*`). При необходимости базу данных модуля аналитики можно разместить на отдельном сервере PostgreSQL

Подсказка

О выносе на отдельный сервер основной базы данных сервера **RuDesktop** см. на странице *Настройка подключения и SSL для сторонней БД*

Важно

Параметры подключения нужно задать **до установки** модуля аналитики: при установке модуль создаёт структуру базы данных (миграции, дашборды, роли) в той базе, которая указана на этот момент

Базу данных и пользователя на внешнем сервере PostgreSQL необходимо **создать заранее вручную** — встроенное автосоздание базы работает только с локальным PostgreSQL

Чтобы разместить базу данных модуля аналитики на отдельном сервере:

1. На целевом сервере PostgreSQL создать пользователя и базу данных:

```
CREATE USER "superset" WITH PASSWORD 'PASSWORD';
CREATE DATABASE "superset"
    WITH OWNER = "superset"
    TEMPLATE = template0
    ENCODING = 'UTF8'
    LC_COLLATE = 'ru_RU.UTF-8'
    LC_CTYPE = 'ru_RU.UTF-8';
```

2. В файл по пути `/etc/default/rudesktop` добавить следующие строки:

```
POSTGRES_SUPERSET_HOST='IP_ADDRESS'    # Адрес базы␣
↪данных модуля аналитики
POSTGRES_SUPERSET_PORT='PORT'          # Порт базы данных
POSTGRES_SUPERSET_DB='superset'        # Имя базы данных
POSTGRES_SUPERSET_USER='superset'      # Имя пользователя
POSTGRES_SUPERSET_PASSWORD='PASSWORD' # Пароль
```

Примечание

Если переменные `POSTGRES_SUPERSET_*` не заданы, модуль аналитики использует те же параметры подключения, что и сервер **RuDesktop** (`POSTGRES_*`), с базой данных `superset`

Шифрование канала к базе данных модуля аналитики задаётся той же переменной `POSTGRES_SSL_MODE`, что и для основной базы сервера (см. *Настройка подключения и SSL для сторонней БД*)

3. Установить модуль аналитики — при установке его структура будет создана в указанной базе данных. См. *Установку модуля аналитики*

Подсказка

Если модуль аналитики уже установлен, задайте переменные `POSTGRES_SUPERSET_*` и выполните повторную инициализацию командой *rude superset install* — структура будет создана заново в новой базе данных

Работа с корпоративным сертификатом

Важно

При замене встроенного самоподписанного сертификата **RuDesktop** на корпоративный вход в модуль аналитики может завершаться ошибкой **«Отказано в доступе»** с записью в логах о неполной цепочке сертификатов

Причина: при авторизации модуль аналитики обменивается данными с сервером **RuDesktop** по HTTPS и проверяет сертификат строго, без дозагрузки промежуточных сертификатов, которую выполняют браузеры. Поэтому веб-интерфейс в браузере открывается, а вход в модуль аналитики — нет

Для работы модуля аналитики с корпоративным сертификатом:

1. Подключите сертификат в формате **full-chain** — файл сертификата должен содержать сертификат сервера и все промежуточные сертификаты корпоративного центра сертификации. Порядок замены — на странице *Добавление собственных SSL-сертификатов*
2. Если сертификат подключается на уровне **nginx** (второй сценарий статьи), завершите замену полностью: те же файлы укажите нативному компоненту **relay** в `/etc/rudesktop-relay.toml` — без этого шага relay продолжит использовать встроенный самоподписанный сертификат

```
ca_cert = "/etc/ssl/private/wc.pem"
ca_key = "/etc/ssl/private/wc.key"
```

Примечание

Если файла `/etc/rudesktop-relay.toml` ещё нет, создайте его и подключите через `RELAY_ARGS='-C /etc/rudesktop-relay.toml'` в `/etc/default/rudesktop` — см. *Конфигурационный файл rudesktop-relay.toml*

3. Перезапустите сервер:

```
rude restart
```

1.4.5 Ограничение доступа к веб-интерфейсу

Ограничение доступа к веб-интерфейсу — настройка `nginx` для разрешения доступа к административной панели только из определённых подсетей. Используется, когда веб-интерфейс должен быть недоступен извне организации, при этом клиентский трафик **RuDesktop** продолжает обслуживаться

Для ограничения внешнего доступа к веб-интерфейсу необходимо:

1. Отредактировать файл по пути `/etc/nginx/sites-enabled/rudesktop`:

   Найти блок `location / {` и заменить на следующее:

```
location / {
  include proxy_params;
  proxy_pass http://[СОКЕТ];
  allow [ПОДСЕТЬ];
  deny all;
}
```

Важно

- Вместо `[СОКЕТ]` укажите сокет. По умолчанию: `http://unix:/run/rudesktop-web.sock`
- Вместо `[ПОДСЕТЬ]` укажите локальную подсеть с маской

   Пример заполнения:

```
location / {
  include proxy_params;
  proxy_pass http://unix:/run/rudesktop-web.sock;
  allow 192.168.10.0/24;
  deny all;
}
```

Важно

Блок `location / {` обслуживает не только страницы веб-интерфейса, но и эндпоинты `/api/`, к которым обращаются клиенты **RuDesktop**: вход в клиент, адресная книга, настройки клиента, авторизация через браузер. Для клиентов из разрешённых подсетей всё продолжит работать, для остальных эти функции станут недоступны — само подключение к удалённым рабочим столам при этом не затрагивается, оно идёт через отдельный блок `location /v1/`

Если нужно закрыть веб-интерфейс, но сохранить эти функции для клиентов снаружи, применяйте ограничение вместе с *разделением портов*: там `/api/` и `/media/` вынесены в отдельный server-блок на клиентском порту и под ограничение не попадают

Важно

Пригласительные ссылки (`/connect/[TOKEH]/`) под это ограничение не попадают: их блок подключается через `include rudesktop_params;`, чтобы приглашённый пользователь мог открыть ссылку извне. Не зная токена ссылки, получить по этому адресу ничего нельзя. Если пригласительные ссылки тоже должны открываться только из разрешённых подсетей, добавьте в каждый server-блок, где есть `include rudesktop_params;` (при *разделении портов* — и в клиентский):

```
location ^~ /connect/ {
  include proxy_params;
  proxy_pass http://[COKET];
  allow [ПОДСЕТЬ];
  deny all;
}
```

2. Проверить корректность конфигурации nginx:

```
nginx -t
```

3. Перезагрузить сервер командой:

```
rude restart
```

Модуль аналитики

Модуль аналитики (встроенный **Apache Superset**) обращается к серверу **RuDesktop** не через сокет, а по его публичному адресу — `PUBLIC_HOST:PUBLIC_PORT` из файла `/etc/default/rudesktop` (или `SUPERSET_PUBLIC_HOST/SUPERSET_PUBLIC_PORT`, если они заданы, — см.

Смену адреса для модуля аналитики). Для `nginx` это обычные внешние запросы, приходящие с IP-адреса самого сервера, поэтому при включённом ограничении они попадают под `deny all`

Разрешение обращений сервера к самому себе

Вход в модуль аналитики выполняется через OAuth сервера **RuDesktop**, и два шага этого входа модуль выполняет сам, со стороны сервера:

- `POST /o/token/` — обмен кода авторизации на токен
- `GET /api/user/` — получение данных учётной записи по полученному токену

Если адрес сервера не разрешён, оба запроса получают `403` и вход в модуль аналитики не работает

Чтобы этого не происходило, в блок `location / {` нужно добавить разрешения для адреса самого сервера:

```
location / {
  include proxy_params;
  proxy_pass http://unix:/run/rudesktop-web.sock;
  allow [IP_СЕРВЕРА];
  allow 127.0.0.1;
  allow [ПОДСЕТЬ];
  deny all;
}
```

Важно

- Вместо `[IP_СЕРВЕРА]` укажите с маской `/32` тот IP-адрес, в который резолвится `PUBLIC_HOST` — по нему модуль аналитики обращается к серверу
- Одного `allow 127.0.0.1;` недостаточно. Когда сервер обращается сам к себе по своему же адресу, соединение идёт через петлевой интерфейс, но исходным адресом остаётся адрес сетевого интерфейса — `nginx` видит в `$remote_addr` именно `[IP_СЕРВЕРА]`. Строка с `127.0.0.1` нужна только для конфигураций, где `PUBLIC_HOST` резолвится в петлевой адрес
- Правила проверяются сверху вниз до первого совпадения, поэтому `deny all` всегда должен идти последним

Примечание

Ограничиться отдельным блоком `location = /o/token/` не получится: следующим шагом модуль запрашивает `/api/user/`, и без разрешения для этого эндпоинта вход всё равно завершится ошибкой. Заводить точечное правило и для `/api/user/` не следует — этот эндпоинт используют и клиенты **RuDesktop**

Ограничение доступа к самому модулю аналитики

Ограничение в блоке `location / {` на модуль аналитики **не распространяется**: он обслуживается отдельным блоком `location ^~ /analytics/ {`, а `nginx` применяет директивы только того `location`, который выбран для запроса. Поэтому после закрытия веб-интерфейса модуль аналитики остаётся доступен извне и его нужно ограничить отдельно

Чтобы закрыть доступ и к нему:

1. Отредактировать файл по пути `/etc/nginx/rudesktop_params`:

   Найти блок `location ^~ /analytics/ {` и добавить в него правила доступа:

```
location ^~ /analytics/ {
    proxy_pass␣
↪http://unix:/run/rudesktop-web-superset.sock;
    proxy_set_header   Accept-Encoding "";
    proxy_set_header   Host $host;
    proxy_set_header   X-Real-IP $remote_addr;
    proxy_set_header   X-Forwarded-For
↪$proxy_add_x_forwarded_for;
    proxy_set_header   X-Forwarded-Port
↪$server_port;
    proxy_set_header   X-Forwarded-Proto $scheme;
    allow [IP_СЕРВЕРА];
    allow 127.0.0.1;
    allow [ПОДСЕТЬ];
    deny all;
}
```

   Важно

   Разрешения для `[IP_СЕРВЕРА]` и `127.0.0.1` обязательны и здесь: при открытии пункта **Отчеты → Аналитика** сервер сам проверяет доступность модуля запросом на `/analytics/health` — по тому же адресу, по которому открыт веб-интерфейс. Если этот запрос заблокирован, вместо модуля откроется страница с предложением его установить

2. Проверить корректность конфигурации nginx:

```
nginx -t
```

3. Перезагрузить сервер командой:

```
rude restart
```

Важно

Файл `/etc/nginx/rudesktop_params` перезаписывается при каждом обновлении сервера — после обновления правила доступа к модулю аналитики нужно добавить заново

Примечание

Файл `/etc/nginx/rudesktop_params` подключается и в клиентском server-блоке (см. *Разделение портов*), поэтому правила действуют сразу на обоих портах — и на административном, и на клиентском

1.4.6 Разделение портов

Разделение портов — настройка `nginx` так, чтобы веб-интерфейс администратора и трафик клиентов **RuDesktop** обслуживались на разных TCP-портах. Это позволяет, например, оставить административный веб только во внутренней сети, а клиентский endpoint открыть наружу

Для разделения портов, используемых для подключения клиентов и веб-интерфейса, необходимо:

1. Создать копию основного конфига `nginx` под отдельный server-блок для клиентов:

```
cp /etc/nginx/sites-available/rudesktop /
↪etc/nginx/sites-available/rudesktop-client
```

2. Отредактировать скопированный файл по пути `/etc/nginx/sites-available/rudesktop-client`

Важно

В файле меняем только то, что описано ниже. Остальные `location`-блоки (в частности, `/v1/` — WebSocket к `relay` / `rz`, `/static/`, `/download/`, `/root.pem`, `/favicon.ico`), `include rudesktop_params;` и SSL-параметры — **оставляем как есть**: они нужны на клиентском порту для работы клиентов и проксирования встроенных эндпоинтов

Важно

Вместе с `include rudesktop_params;` на клиентский порт попадает и блок `location ^~ /analytics/ {` — *модуль аналитики* остаётся доступен и на клиентском порту, который обычно открыт наружу. Если это нежелательно, ограничьте доступ к нему отдельно — см. *Ограничение доступа к веб-интерфейсу*

1. Удалить из копии **первый** `server { listen 80; … }` блок (с редиректом `return 301 https://$host$request_uri;`):

   Этот блок уже обслуживается основным vhost-ом `/etc/nginx/sites-enabled/rudesktop` для того же `server_name`. Если оставить его в копии — при перезагрузке nginx выдаст предупреждение `conflicting server name … on 0.0.0.0:80, ignored`, и второй блок будет молча проигнорирован

2. Найти блок `server {` со строкой `listen 443 ssl;` и заменить значение 443 на удобный вам порт (этот порт будет использоваться для подключения клиентов **RuDesktop** к серверу):

```
server {

  server_name 192.168.10.10;

  listen 8443 ssl;
```

3. Найти блок `location / {` и заменить на следующее:

```
location /api/ {
  add_header 'Cache-Control' 'no-cache';
  include proxy_params;
  proxy_pass␣
↪http://unix:/run/rudesktop-web.sock;
}
```

4. Добавить новый блок `location /media/ {` после блока `location /api/ {`

```
location /media/ {
  add_header 'Cache-Control' 'no-cache';
  include proxy_params;
  proxy_pass␣
↪http://unix:/run/rudesktop-web.sock;
}
```

5. Добавить новый блок `location /portal/ {` после блока `location /media/ {`

```
location /portal/ {
  return 301 https://
↪$host:[АДМИН_ПОРТ]$request_uri;
}
```

Важно

Вместо [АДМИН_ПОРТ] здесь и во всех блоках ниже подставьте порт из /etc/nginx/sites-enabled/rudesktop (строка listen) — это порт админского веб-интерфейса. Если он не менялся, используйте 443

6. Добавить новые блоки location /login/ { и location /account/ { после блока location /portal/ { — они нужны для работы функции **Авторизация через браузер** в клиенте

```
location /login/ {
  return 301 https://
↪$host:[АДМИН_ПОРТ]$request_uri;
}

location /account/ {
  return 301 https://
↪$host:[АДМИН_ПОРТ]$request_uri;
}
```

Без них браузер при авторизации остаётся на клиентском порту, где страниц веб-интерфейса нет, и вместо формы входа пользователь получает 404

Важно

Вход при **Авторизации через браузер** выполняется на админском порту, поэтому он должен быть доступен с рабочего места пользователя. Если веб-интерфейс закрыт от пользователей (например, доступен только из внутренней сети), вход в клиент останется возможен только по логину и паролю

3. Активировать конфиг:

```
ln -s /etc/nginx/sites-available/rudesktop-client /
↪etc/nginx/sites-enabled/rudesktop-client
```

4. Проверить корректность конфигурации nginx:

```
nginx -t
```

5. Перезагрузить сервер командой:

```
rude restart
```

6. Указать клиентский порт в настройках сервера, чтобы установочные скрипты и пакеты (.sh, .msi, .apk) прописывали клиентам корректный

порт:

В административной панели откройте **Настройки → Настройки мостов** и задайте параметр **Порт подключения клиентов** равным порту из клиентского server-блока (в примере — 8443)

Важно

Без этого шага установщик берёт порт из адреса, по которому открыта веб-панель (443), и клиент подключается на 443 вместо клиентского порта. Пригласительные ссылки также формируются с этим портом. Блок `nginx` для них подключается через `include rudesktop_params;`, добавлять его вручную не нужно

1.4.7 Настройка подключения и SSL для сторонней БД

Настройка подключения и SSL для сторонней БД — подключение сервера **RuDesktop** к внешнему PostgreSQL-инстансу и опциональное шифрование канала. Используется при выносе БД на отдельный сервер или для отказоустойчивого кластера

Подсказка

Подробнее о развёртывании сервера с общим внешним PostgreSQL см. на странице *Развёртывание отказоустойчивого кластера*

О выносе на отдельный сервер базы данных модуля аналитики (**Apache Superset**) см. на странице *Смена адреса для модуля аналитики*

Настройка подключения к сторонней БД

Чтобы настроить подключение к сторонней базе данных PostgreSQL, необходимо:

1. В файл по пути `/etc/default/rudesktop` добавить следующие строки:

```
POSTGRES_HOST='IP_ADDRESS' # Адрес базы данных
POSTGRES_PORT='PORT' # Порт базы данных
POSTGRES_DB='DB_NAME' # Имя базы данных
POSTGRES_USER='USER' # Имя пользователя
POSTGRES_PASSWORD='PASSWORD' # Пароль
```

2. Перезагрузить сервер командой:

```
rude restart
```

Настройка SSL для подключения к БД

Чтобы настроить SSL для подключения к базе данных PostgreSQL, необходимо:

1. Загрузить сертификат `root.crt` на устройство, где установлен сервер RuDesktop
2. В файл по пути `/etc/default/rudesktop` добавить следующие строки:

```
POSTGRES_SSL_MODE='verify-ca'
POSTGRES_CA_FILE=/path/to/root.crt
```

Или без указания сертификата:

```
POSTGRES_SSL_MODE='require'
```

Важно

`POSTGRES_SSL_MODE` принимает значения из таблицы:

sslmode	Защита от прослушивания	Защита от MITM	Описание
disable	Нет	Нет	Безопасность не важна — соединение не шифруется
allow	Возможно	Нет	Безопасность не важна; шифрование используется только если сервер сам этого требует
prefer	Возможно	Нет	Шифрование используется при поддержке сервером; в остальном — открытое соединение
require	Да	Нет	Соединение всегда шифруется; идентичность сервера не проверяется

verify-ca	Да	В зависимости от политики CA	Соединение шифруется и проверяется по корневому сертификату CA

3. Перезагрузить сервер командой:

```
rude restart
```

4. Убедиться, что в логах сервера отсутствуют ошибки, командой:

```
cat /var/log/rudesktop/server.log
```

Пример логов после перезагрузки сервера:

```
2025-05-20 11:08:47  INFO rudesktop_server: Server␣
↪started with: Options { db_host: "", db_name: "",␣
↪db_user: "", db_pass: MASKED, db_port: 5432,␣
↪db_pool_size: 64, db_ssl_mode: VerifyCa, db_ca_cert:␣
↪Some("path/to/root.crt"), this_server: "",␣
↪redis_server: "redis://localhost:32459/", ca_key: "/
↪var/lib/rudesktop/ca/CA.key", ca_cert: "/
↪var/lib/rudesktop/ca/CA.pem", log_level: "info",␣
↪version: "", license_version: "", rendezvous_mode:␣
↪None, server: [], master: None, api_key: "", trace: 0,␣
↪max_session_duration: 7200, use_public_ip: false,␣
↪conflict: None, hostname_as_id: None, use_geo_relay:␣
↪false, flush_interval: 60, flush_batch: 1000,␣
↪cache_ttl: 300, cache_preload: false, keep_statuses:␣
↪false, geoip_db: "geolocation/SxGeoCity.dat" }
2025-05-20 11:08:47  INFO rudesktop_server: Start in␣
↪master mode with cached database
2025-05-20 11:08:47  INFO rudesktop_server: Start␣
↪listener on /run/rudesktop/rude.sock
```

1.4.8 Настройка unix-socket

Настройка unix-socket — переключение взаимодействия между `nginx` и нативным компонентом `relay` с TCP-сокета на unix-сокет в файловой системе. Снижает накладные расходы и убирает зависимость от свободного TCP-порта

Добавлено в версии 2.7: Эта настройка добавлена по умолчанию — на новых установках сервер уже работает через unix-socket. Раздел нужен для перехода со старых установок

Для переключения на unix socket вам необходимо:

1. Открыть для редактирования файл по пути `/etc/nginx/sites-enabled/rudesktop` командой:

```
nano /etc/nginx/sites-enabled/rudesktop
```

2. Найти блок `location /v1/` и изменить **proxy_pass**:

```
location /v1/ {
  proxy_pass http://unix:/run/rudesktop/rude.sock;
```

3. Открыть для редактирования файл по пути `/etc/default/rudesktop` командой:

```
nano /etc/default/rudesktop
```

4. Изменить значение в **RELAY_ARGS** на следующее:

```
RELAY_ARGS='-C /etc/rudesktop-relay.toml'
```

5. Открыть для редактирования файл по пути `/etc/rudesktop-relay.toml` командой:

```
nano /etc/rudesktop-relay.toml
```

6. Добавить следующие строки:

```
[[server]]
listen = "/run/rudesktop/rude.sock"
```

7. Проверить корректность конфигурации nginx:

```
nginx -t
```

8. Перезапустить сервер командой:

```
rude restart
```

1.4.9 Развёртывание за обратным прокси

Развёртывание за обратным прокси — установка сервера **RuDesktop** во внутренней сети с внешним **HAProxy** или **Nginx** перед ним, который принимает подключения снаружи и пересылает их на сервер. Раздел описывает, какой трафик можно проксировать и каким способом, готовые примеры конфигураций и список типовых проблем

Настройка балансировщика Nginx перед RuDesktop

Инструкция описывает настройку отдельного Nginx перед одним сервером **RuDesktop** с передачей настоящего IP-адреса клиента в веб-часть и управляющий канал `/v1/`

В этой схеме клиенты подключаются к балансировщику, а он пересылает HTTPS- и WebSocket-запросы на сервер

```
Клиент -> Nginx (192.0.2.20:443) -> RuDesktop (192.0.2.10:443)
```

Если сервер видит адрес балансировщика вместо адреса устройства, проверка IP в магазине приложений может завершиться ошибкой 403

Подготовка

В примерах используются условные IP-адреса из диапазонов, зарезервированных для документации. Перед выполнением команд замените их адресами вашей инфраструктуры:

Узел	Адрес
Сервер RuDesktop	`192.0.2.10`
Балансировщик Nginx	`192.0.2.20`
Клиент для проверки	`198.51.100.30`

Команды выполняются с правами root на указанной в разделе машине. Пример установки Nginx рассчитан на Debian/Ubuntu с каталогами `sites-available` и `sites-enabled`

Перед настройкой сохраните копии изменяемых конфигурационных файлов. Балансировщик должен иметь доступ к порту `443/TCP` сервера, а клиент - к порту `443/TCP` балансировщика

Примечание

Пример рассчитан на IPv4 и одну внешнюю точку входа без дополнительных прокси перед ней. В текущей проверке IP магазина приложений IPv6 не поддерживается

Настройка нескольких серверов с общими данными описана отдельно: *Развертывание отказоустойчивого кластера*

Настройка сервера RuDesktop

Сертификат для балансировщика

Балансировщику нужен сертификат для адреса, по которому к нему обращаются клиенты. Ниже приведен выпуск сертификата встроенным центром сертификации RuDesktop

На сервере RuDesktop подготовьте каталог и ключ:

```
cd /var/lib/rudesktop/ca
umask 077
mkdir -p front
chmod 700 front
openssl genrsa -out front/front.key 2048
```

Создайте файл `/var/lib/rudesktop/ca/front/front.cnf`:

```
[req]
distinguished_name = dn
req_extensions = v3
prompt = no

[dn]
C = RU
O = RuDesktop
CN = 192.0.2.20

[v3]
subjectAltName = IP:192.0.2.20
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
```

Если клиенты обращаются по имени, например `rudesktop.example.org`, укажите `CN = rudesktop.example.org` и `subjectAltName = DNS:rudesktop.example.org`

Выпустите и проверьте сертификат:

```
openssl req -new -key front/front.key -out front/front.csr -config␣
↪front/front.cnf
openssl x509 -req -in front/front.csr -CA CA.pem -CAkey CA.key -
↪CAcreateserial \
  -out front/front.crt -days 3650 -extensions v3 -extfile␣
↪front/front.cnf
openssl verify -CAfile CA.pem front/front.crt
```

При успешной проверке последняя команда выведет `front/front.crt: OK`. Срок действия сертификата в примере - 3650 дней; задайте срок по правилам вашей организации

Важно

На балансировщик передаются только `front.crt`, `front.key` и публичный `CA.pem`. Закрытый ключ центра сертификации `CA.key` должен оставаться на сервере

Браузер на клиентском устройстве должен доверять этому CA. Выпуск сертификата не добавляет CA в доверенные автоматически. Другой вариант - *Добавление собственных SSL-сертификатов*

Передача IP-адреса клиента

На сервере RuDesktop создайте файл `/etc/nginx/conf.d/00-realip-rudesktop.conf`:

```
set_real_ip_from 192.0.2.20;
real_ip_header X-Forwarded-For;
real_ip_recursive on;
```

Nginx будет принимать переданный IP только от указанного балансировщика и использовать его как адрес клиента

Предупреждение

В `set_real_ip_from` указывайте только адрес доверенного балансировщика. Не используйте `0.0.0.0/0`: это позволит постороннему отправителю подменить IP, используемый проверками доступа

Для этих директив нужен модуль `http_realip`. Если `nginx -t` сообщает `unknown directive`, проверьте наличие `--with-http_realip_module` в выводе `nginx -V` и состав установленного пакета Nginx

Адрес и порт в управляющем канале

Компонент RuDesktop, обслуживающий `/v1/`, ожидает `X-Real-Ip` в формате `IP:порт`. При восстановлении IP из заголовка без номера порта значение `$remote_port` может оказаться пустым; адрес с пустым портом приводит к ответу 400

На сервере RuDesktop создайте файл `/etc/nginx/conf.d/01-rport-fallback.conf`:

```
map $remote_port $rport {
    default $remote_port;
    ""      0;
}
```

В файле `/etc/nginx/sites-available/rudesktop`, внутри `location /v1/`, замените строку:

```
proxy_set_header X-Real-Ip $remote_addr:$remote_port;
```

на:

```
proxy_set_header X-Real-Ip $remote_addr:$rport;
```

Порт `0` здесь служит подстановкой для неизвестного порта клиента. Это не порт, к которому нужно подключаться

Для запросов к веб-части сохраните штатную настройку `/etc/nginx/proxy_params`:

```
proxy_set_header X-Forwarded-For $remote_addr;
```

После обработки Real IP эта строка передает веб-части восстановленный адрес клиента. Магазин сравнивает его с IP, записанным при подключении устройства через `/v1/`

Предупреждение

Команда `rude reinstall` удаляет конфигурацию RuDesktop, его Nginx-vhost и файлы CA сервера, затем запускает установку заново. После нее нужно повторно проверить публичный адрес, сертификаты и доверие клиентов, а также восстановить правку `X-Real-Ip`

Файлы из `/etc/nginx/conf.d/` эта команда непосредственно не удаляет, но наличие этих файлов не восстанавливает остальные настройки

Публичный адрес сервера

В `/etc/rudesktop/settings` измените существующие значения, сохранив остальные настройки и необходимые адреса в `ALLOWED_HOSTS`:

```
PUBLIC_HOST = '192.0.2.20'
ALLOWED_HOSTS = ['localhost', '192.0.2.10', '192.0.2.20']
```

В `/etc/default/rudesktop` измените `PUBLIC_HOST`:

```
PUBLIC_HOST='192.0.2.20'
```

При подключении по DNS-имени используйте его вместо адреса балансировщика. В `PUBLIC_HOST` не указывайте `https://`; пример использует стандартный публичный порт 443

Сервер формирует `CSRF_TRUSTED_ORIGINS` из `PUBLIC_HOST` и `PUBLIC_PORT`. Для этого примера доверенным адресом будет `https://192.0.2.20`

В обоих блоках `server` файла `/etc/nginx/sites-available/rudesktop` добавьте адрес балансировщика в существующий `server_name`, сохранив нужные имена сервера. Например:

```
server_name 192.0.2.10 192.0.2.20;
```

Примените изменения на сервере:

```
systemctl restart rudesktop-web
nginx -t && systemctl reload nginx
```

Перезагрузка Nginx выполняется только при успешной проверке конфигурации

Настройка балансировщика

Установка Nginx и сертификата

На машине балансировщика установите Nginx:

```
apt-get update && apt-get install -y nginx
```

Передайте по защищенному каналу `front.crt`, `front.key` и `CA.pem` с сервера в каталог, доступный только root на балансировщике. Перейдите в этот каталог

и выполните:

```
install -d -m 700 /etc/ssl/rudesktop
cat front.crt CA.pem > /etc/ssl/rudesktop/front-fullchain.crt
install -m 600 front.key /etc/ssl/rudesktop/front.key
install -m 644 CA.pem /etc/ssl/rudesktop/CA.pem
chmod 644 /etc/ssl/rudesktop/front-fullchain.crt
```

В файле цепочки первым идет сертификат балансировщика, затем сертификат CA

Параметры WebSocket

Создайте на балансировщике файл `/etc/nginx/conf.d/upgrade-map.conf`:

```
map $http_upgrade $connection_upgrade {
    default upgrade;
    ''      close;
}
```

Блок `map` должен подключаться внутри `http {}`. Если переменная `$connection_upgrade` уже объявлена в конфигурации балансировщика, используйте существующее объявление

Конфигурация сайта

Создайте файл `/etc/nginx/sites-available/rudesktop-front`:

```
upstream rudesktop_backend {
    server 192.0.2.10:443;
    keepalive 32;
}

server {
    listen 80;
    server_name 192.0.2.20;
    location /tftp/ { return 404; }
    location / { return 301 https://$host$request_uri; }
}

server {
    listen 443 ssl;
    server_name 192.0.2.20;

    ssl_certificate /etc/ssl/rudesktop/front-fullchain.crt;
    ssl_certificate_key /etc/ssl/rudesktop/front.key;
    client_max_body_size 1000G;

    location /v1/ {
        proxy_pass https://rudesktop_backend;
        proxy_ssl_verify off;
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
        proxy_http_version 1.1;
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $remote_addr;
        proxy_set_header X-Forwarded-Proto https;
        proxy_set_header X-Forwarded-Host $host;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $connection_upgrade;
        proxy_connect_timeout 120s;
        proxy_send_timeout 600s;
        proxy_read_timeout 600s;
    }

    location /ws/ {
        proxy_pass https://rudesktop_backend;
        proxy_ssl_verify off;
        proxy_http_version 1.1;
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $remote_addr;
        proxy_set_header X-Forwarded-Proto https;
        proxy_set_header X-Forwarded-Host $host;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $connection_upgrade;
        proxy_read_timeout 600s;
    }

    location / {
        proxy_pass https://rudesktop_backend;
        proxy_ssl_verify off;
        proxy_http_version 1.1;
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $remote_addr;
        proxy_set_header X-Forwarded-Proto https;
        proxy_set_header X-Forwarded-Host $host;
        add_header Cache-Control 'no-cache';
    }
}
```

В этом примере балансировщик формирует `X-Forwarded-For` из адреса соединения с клиентом. Заголовок, присланный самим клиентом, не используется как источник его IP

Важно

- Используйте показанную конфигурацию клиентского порта с HTTP/1.1 и WebSocket Upgrade, без включения HTTP/2

- Заголовки повторены в каждом `location`: при наличии собственных `proxy_set_header` этот блок не наследует набор заголовков с уровня `server`
- В примере `proxy_ssl_verify off` отключает проверку сертификата внутреннего сервера. Соединение шифруется, но подлинность сервера не проверяется; такой вариант требует доверенного внутреннего сетевого сегмента
- Для проверки сертификата внутреннего сервера настройте `proxy_ssl_verify on`, `proxy_ssl_trusted_certificate` и `proxy_ssl_name`, соответствующий сертификату сервера
- HTTP-путь `/tftp/` через балансировщик закрыт; PXE-устройства в этой схеме должны обращаться к узлу публикации напрямую. Для PXE через балансировщик нужна отдельная настройка

Включите сайт, если ссылка еще не создана:

```
ln -s /etc/nginx/sites-available/rudesktop-front /
↪etc/nginx/sites-enabled/rudesktop-front
```

На отдельной новой машине со штатным сайтом Nginx отключите его, удалив только символическую ссылку `/etc/nginx/sites-enabled/default`. Если Nginx уже обслуживает другие сайты, сохраните их и проверьте, что они не конфликтуют с новым `server_name`

Проверьте и примените конфигурацию балансировщика:

```
nginx -t && systemctl reload nginx
```

Укажите адрес балансировщика `192.0.2.20:443` в настройках подключения клиентов RuDesktop и переподключите их

Проверка подключения

Проверка IP на сервере

Временно добавьте на сервере RuDesktop в HTTPS-блок `server` файла `/etc/nginx/sites-available/rudesktop`:

```
location = /_debug_ip {
    default_type text/plain;
    return 200 "remote_addr=$remote_addr xff=
↪$http_x_forwarded_for\n";
}
```

Примените конфигурацию сервера:

```
nginx -t && systemctl reload nginx
```

С клиентской машины выполните запрос через балансировщик, указав путь к публичному CA, полученному от администратора:

```
curl --cacert /path/to/CA.pem https://192.0.2.20/_debug_ip
```

При прямом маршруте без NAT в ответе должны быть адреса клиента, например `remote_addr=198.51.100.30 xff=198.51.100.30`. При NAT будет виден адрес, с которого клиент пришел на балансировщик

После проверки удалите весь временный блок `location = /_debug_ip` и снова выполните `nginx -t && systemctl reload nginx` на сервере

Проверка адреса устройства

После переподключения клиента проверьте поле Сетевой адрес в его карточке. Также можно выполнить на сервере запрос только для чтения:

```
echo "SELECT server_id, hostname, addr FROM peers_server ORDER BY␣
↪updated DESC LIMIT 10;" | rude sql
```

В `addr` должен быть IP клиента, видимый балансировщику, а не адрес `192.0.2.20`. Суффикс `:0` допустим после настройки подстановки порта

Если сохраняется ошибка 400 при подключении клиента, проверьте правку `X-Real-Ip` в `location /v1/` сервера и передачу заголовков WebSocket на балансировщике

Если магазин приложений возвращает 403

После опознания устройства сервер проверяет право его группы, совпадение IP и авторизацию пользователя. Ошибка 403 сама по себе не определяет, какая из этих проверок не пройдена

Для диагностики откройте на сервере:

```
rude shell
```

И выполните, заменив <id> и <uuid> значениями из адреса магазина `/portal/app_store/?id=...&uuid=...`:

```
from automation.utils import get_server_permissions
from peers.models import Server
from django.contrib.auth.models import Group

device = Server.objects.get(server_id="<id>", uuid="<uuid>")
print("addr:", device.addr)
print("app_store:", "account.can_use_app_store" in␣
↪get_server_permissions(device.server_id))
print("groups:", list(Group.objects.filter(server__server_id=device.
↪server_id).values_list("name", flat=True)))
```

1. Если `app_store` равно `False`, выдайте право Может использовать магазин приложений группе, в которой состоит устройство. Авторизация под администратором не заменяет это право

2. Сравните IP в `addr` с адресом из проверки `/_debug_ip`. При несовпадении проверьте маршрут браузера и клиента, настройки Real IP и переподключите клиент
3. Если право есть и IP совпадает, авторизуйтесь в портале. Если по правилам организации нужен вход без авторизации, включите в *Настройки* настройку Неавторизованный пользователь может видеть магазин приложений (IP адрес должен совпадать)

Настройка `VIEW_APP_STORE_WITHOUT_AUTH` отменяет только требование авторизации пользователя; право группы устройства и совпадение IP продолжают проверяться

Подробная настройка прав и публикации приложений: Публикация приложения в магазине приложений

Связанные страницы

- *Развёртывание за обратным прокси*
- *Публикация через WAF и AntiDDoS*
- *Разделение портов*
- Модуль Real IP в Nginx[8]
- Передача заголовков proxy_set_header[9]
- Проксирование WebSocket в Nginx[10]

Для настройки Nginx на двух машинах используйте *Настройка балансировщика Nginx перед RuDesktop*

Важно

По умолчанию сервер **RuDesktop** уже разворачивает у себя локальный **Nginx**, который терминирует TLS на `443` и проксирует запросы к вебчасти и к нативному компоненту `relay / rz` через unix-сокеты `/run/rudesktop-web.sock` и `/run/rudesktop/rude.sock` (см. *Архитектура*). Эта страница описывает **внешний** обратный прокси, который ставится **перед** сервером **RuDesktop**

Зачем нужен обратный прокси перед RuDesktop

Типовые сценарии:

- **TLS-терминация на единой точке** — сертификаты обслуживаются одним фронтом, не на каждом узле
- **Единая точка входа** для нескольких внутренних сервисов организации
- **Балансировка** между несколькими узлами *отказоустойчивого кластера*

[8] https://nginx.org/en/docs/http/ngx_http_realip_module.html
[9] https://nginx.org/en/docs/http/ngx_http_proxy_module.html#proxy_set_header
[10] https://nginx.org/en/docs/http/websocket.html

- **Ограничение доступа** — фильтрация по IP, ACL, аутентификация заголовка
- **Публикация веб-части наружу**, при том что прямой TCP-доступ к `relay` / `rz` остаётся внутри периметра

Какой трафик принимает сервер RuDesktop

По умолчанию весь трафик клиентов и веб-интерфейса идёт **через единый порт ``443/TCP``** на встроенный **Nginx** сервера, который терминирует TLS и проксирует запросы к веб-части и компоненту `relay` / `rz` через unix-сокеты. Снаружи это выглядит как обычный HTTPS-сайт с дополнительным WebSocket-эндпоинтом

Эндпоинты на `443/TCP`:

- `/` — административная веб-панель и API (`/api/`, `/portal/`, `/media/`)
- `/v1/` — **WebSocket**-канал к нативному компоненту `relay` / `rz` через unix-сокет `/run/rudesktop/rude.sock`. Используется десктопным и мобильным клиентами для управляющего канала и сессионного трафика
- `/ws/` — **WebSocket**-канал к веб-части (`/run/rudesktop-web.sock`). Используется браузерным интерфейсом для live-обновлений и для обратной совместимости при разделении портов
- `/analytics/` — встроенный модуль аналитики (**Apache Superset**), проксируется на unix-сокет `/run/rudesktop-web-superset.sock`
- `/static/` — статика веб-интерфейса (alias `/usr/share/rudesktop/public/`)
- `/download/` — установочные пакеты клиентов (alias `/usr/share/rudesktop/public/download/`)
- `/tftp/` — файлы для PXE-установки (alias `/var/lib/rudesktop/pxe/tftp/`); единственный путь, доступный по HTTP на `80/TCP` без редиректа на HTTPS
- `/root.pem` — публичный CA-сертификат сервера, отдаваемый клиентам

Дополнительно при *Разделении портов* клиентский трафик можно вынести на отдельный HTTPS-порт (например, `8443`) с набором эндпоинтов `/api/`, `/media/`, `/portal/`, `/v1/`, `/ws/` — это всё тот же L7 HTTPS, не отдельный TCP-поток

Важно

Большая часть путей выше (`/analytics/`, `/ws/`, `/tftp/`, защищённые медиа и др.) объявлена в файле `/etc/nginx/rudesktop_params`, который подключается во встроенный vhost директивой `include rudesktop_params;`. При ручной правке `/etc/nginx/sites-enabled/rudesktop` не удаляйте этот `include` — иначе перечисленные эндпоинты перестанут работать

Подсказка

Весь трафик RuDesktop — это HTTP(S) с поддержкой WebSocket. Достаточно одного L7-прокси (HAProxy `mode http` или Nginx). Отдельный TCP-passthrough для какого-либо нестандартного порта **не требуется**

Что можно проксировать и каким способом

Что	Режим прокси	Особенности
`/` — веб и API	L7 HTTP(S)	Стандартное HTTPS-проксирование. Передавать `X-Forwarded-For`, `X-Forwarded-Proto`, `Host`
`/v1/` — WebSocket к `relay` / `rz`	L7 HTTP(S) с upgrade	Обязательны заголовки `Upgrade: websocket` / `Connection: upgrade`. Увеличить таймауты чтения/записи до `600s`
`/ws/` — WebSocket к веб-части	L7 HTTP(S) с upgrade	Те же требования, что и для `/v1/` : `Upgrade` / `Connection: upgrade`
`/analytics/` — модуль аналитики	L7 HTTP(S)	Проксируется как `/`. Особенности доступа описаны в *Смена адреса для модуля аналитики*
`/portal/`, `/api/`, `/media/`, `/static/`, `/download/`, `/root.pem`	L7 HTTP(S)	Ничего особенного, проксируется как `/`
`/tftp/`	L7 HTTP	Раздаётся также по HTTP без TLS (порт `80/TCP`) — для совместимости с PXE-загрузчиками. Если PXE используется, то проксирование `/tftp/` нужно делать **по HTTP, не редиректя на HTTPS**. PXE-загрузчики не умеют HTTPS, и редирект на 443 сломает им загрузку. При отсутствии PXE проще не публиковать этот путь через фронт вообще

Важно

Что нельзя: проксировать `/v1/` без upgrade-заголовков WebSocket. Если фронтальный прокси настроен только на HTTP без upgrade — управляющий канал клиента не установится, в десктопном клиенте будет вечный «Подключение...», в веб-интерфейсе пропадут live-обновления

Подсказка

Дефолты встроенного nginx (см. /etc/nginx/sites-enabled/rudesktop), которые имеет смысл воспроизвести и на внешнем фронте: proxy_connect_timeout 120s, proxy_send_timeout 600s, proxy_read_timeout 600s для /v1/ и client_max_body_size 1000G (загрузка пакетов и обновлений может превышать стандартные ограничения)

Подготовка сервера RuDesktop

Перед включением фронтального прокси:

1. Убедитесь, что встроенный сервер работает на 127.0.0.1 или unix-сокете и **не выставлен наружу** напрямую — см. *Смена и установка IP*, *Ограничение доступа к веб*
2. Если фронт будет терминировать TLS — на самом сервере **RuDesktop** можно оставить самоподписанный сертификат (он используется только во внутренней сети). Для прямого подключения клиентов к серверу без фронта см. *Добавление собственных SSL-сертификатов*
3. Зафиксируйте **публичный FQDN**, по которому клиенты будут обращаться к фронту. При новой установке задайте его командой:

   ```
   rude install rd.example.com
   ```

   При установке формируется /etc/default/rudesktop с переменными PUBLIC_HOST='rd.example.com' и PUBLIC_PORT='443'. Из них веб-часть формирует CSRF_TRUSTED_ORIGINS и публичные ссылки

   Для уже установленного сервера измените публичный адрес и допустимые имена по инструкции *Настройка балансировщика Nginx перед RuDesktop*. Учтите, что rude reinstall удаляет текущие конфигурационные файлы и CA сервера
4. Настройте встроенный Nginx принимать IP только от доверенного внешнего прокси и передавать адрес с корректным портом в /v1/. Настройки сервера приведены в *Адрес и порт в управляющем канале*; адрес доверенного узла должен соответствовать вашему Nginx или HAProxy

Подсказка

Подробнее о смене адреса сервера и о работе с двумя адресами одновременно — *Смена и установка IP*

Пример конфигурации HAProxy

Универсальный вариант — единый фронтенд на 443/TCP с TLS-терминацией, проксирование веба и WebSocket к одному backend-серверу **RuDesktop** на адресе 10.0.0.10:443

```
# /etc/haproxy/haproxy.cfg

global
    maxconn 50000
    log /dev/log local0
    ssl-default-bind-options no-sslv3 no-tlsv10 no-tlsv11
    tune.ssl.default-dh-param 2048

defaults
    log     global
    mode    http
    option  httplog
    option  dontlognull
    timeout connect 10s
    timeout client  600s
    timeout server  600s
    timeout tunnel  1h

frontend rudesktop_https
    bind *:443 ssl crt /etc/haproxy/certs/rudesktop.pem alpn␣
 ↪h2,http/1.1
    http-request set-header X-Forwarded-Proto https
    http-request set-header X-Forwarded-Port  %[dst_port]
    # FQDN, по которому ходят клиенты
    http-request set-header X-Forwarded-Host  %[req.hdr(host)]

    default_backend rudesktop_web

backend rudesktop_web
    balance roundrobin
    option forwardfor
    option http-server-close
    # Проброс WebSocket-апгрейда
    http-request set-header Connection upgrade if { hdr(Upgrade) -i␣
 ↪websocket }
    server rd1 10.0.0.10:443 ssl verify none check
```

Важно

- `timeout tunnel 1h` обязателен — иначе HAProxy будет рвать длинные WebSocket-соединения по таймауту
- `ssl verify none` подходит для встроенного самоподписанного сертификата сервера. Для строгой проверки замените на `verify required ca-file /etc/haproxy/ca/rudesktop_ca.pem`
- При наличии нескольких узлов кластера добавьте ещё `server rd2 ... ;`, но подключения должны быть **sticky** по cookie или source IP, чтобы один клиент попадал на один и тот же узел в рамках сессии

Если веб и клиентский трафик разнесены по разным портам

При использовании *Разделения портов* на стороне сервера клиентский трафик слушает на отдельном HTTPS-порту (например, 8443). На фронте это можно отразить вторым HTTPS-frontend'ом с тем же набором заголовков и таймаутов:

```
frontend rudesktop_client_https
    bind *:8443 ssl crt /etc/haproxy/certs/rudesktop.pem
    http-request set-header X-Forwarded-Proto https
    default_backend rudesktop_client_backend

backend rudesktop_client_backend
    option forwardfor
    http-request set-header Connection upgrade if { hdr(Upgrade) -i␣
↪websocket }
    server rd1 10.0.0.10:8443 ssl verify none check
```

Пример конфигурации Nginx

Пошаговая инструкция вынесена на страницу *Настройка балансировщика Nginx перед RuDesktop*

Она включает выпуск сертификата, настройку Nginx на обеих машинах, передачу IP клиента в веб-часть и `/v1/`, применение настроек и диагностику ошибок 400/403

Важно

Для сохранения адреса клиента недостаточно настроить только внешний прокси. На сервере RuDesktop также нужны доверие к адресу балансировщика и корректная передача `IP:порт` в управляющий канал

Решение проблем

Mixed content / CSRF Origin checking failed

- **Причина:** клиент обращается по IP или домену, который не был указан при `rude install`, из-за чего этот адрес отсутствует в `CSRF_TRUSTED_ORIGINS` и Django отклоняет запрос
- **Решение:** проверить передачу `X-Forwarded-Proto: https` и `X-Forwarded-Host: <FQDN>`. Значения `PUBLIC_HOST` и `PUBLIC_PORT` должны соответствовать адресу и порту фронта; порядок изменения на установленном сервере описан в *Настройка балансировщика Nginx перед RuDesktop*. Из них Django формирует `CSRF_TRUSTED_ORIGINS` вида `https://<PUBLIC_HOST>` или `https://<PUBLIC_HOST>:<PUBLIC_PORT>` при нестандартном порте

Ошибка 403 в магазине приложений

Проверьте передачу IP на обоих прокси, переподключите клиент и сравните адрес запроса с полем Сетевой адрес устройства. Затем проверьте права группы устройства и авторизацию пользователя по *инструкции диагностики*

Связанные страницы

- *Архитектура сервера*
- *Добавление собственных SSL-сертификатов*
- *Смена стандартного порта*
- *Разделение портов*
- *Ограничение доступа к веб*
- *Развёртывание отказоустойчивого кластера*

1.4.10 Публикация через WAF и AntiDDoS

Публикация через WAF и AntiDDoS — публикация клиентского порта сервера **RuDesktop** наружу через средства веб-защиты (**WAF**, **AntiDDoS** и подобные узлы очистки трафика). Раздел описывает рекомендуемые режимы работы защитного решения (**TCP passthrough** / **L7**), требования к публикуемым эндпоинтам, типичные ошибки разделения портов, пример конфигурации **Nginx** на бэкенде и приёмы диагностики

Важно

Раздел применим только при работе с **локальным сервером RuDesktop**, развёрнутым внутри периметра организации с внешним защитным узлом перед ним

Общий принцип

Клиент **RuDesktop** использует **один клиентский адрес и порт** не только для **WebSocket**, но и для служебных HTTPS API-запросов. Через клиентский порт должны проходить:

- `/v1/` — WebSocket/WSS, основной клиентский канал
- `/api/login/` — авторизация пользователя
- `/api/logout/` — выход из учётной записи
- `/api/ssolist/` — получение списка SSO-доменов
- `/api/user/` — информация об авторизованном пользователе
- `/api/client-settings/` — клиентские настройки
- `/api/banner/` — баннер в клиенте
- `/api/ab/load/` — загрузка адресной книги
- `/root.pem` — публичный CA-сертификат сервера **RuDesktop**
- `/download/` — загрузка дистрибутива клиента, если используется

Важно

Нельзя публиковать наружу **только** `/v1/` как отдельный WebSocket-порт, если остальные API остаются на другом порту. Клиент **RuDesktop** не разделяет автоматически «API-порт» и «WSS-порт»: если в клиенте указан `server.example.ru:8443`, то и `/v1/`, и `/api/...`, и `/root.pem` будут запрашиваться через `8443`

Рекомендуемый вариант — TCP passthrough

Если **WAF/AntiDDoS** некорректно обрабатывает **WebSocket** или смешанный трафик HTTP + WebSocket, рекомендуется публиковать весь клиентский порт **RuDesktop** в одном из режимов **TCP proxy** / **RAW** / **L4 passthrough** / **TLS passthrough**

Защитное решение в этом режиме **не должно**:

- разбирать **HTTP**- и **WebSocket**-протоколы;
- менять методы, заголовки или тело запроса;
- инспектировать трафик как обычный короткий HTTP-запрос.

Оно должно передавать **TCP**-трафик до backend как есть

Рабочая схема:

```
Клиент RuDesktop
        ↓
WAF, AntiDDoS  (TCP proxy / RAW / L4 passthrough)
        ↓
Reverse proxy (Nginx, UserGate, HAProxy)
        ↓
Сервер RuDesktop
```

Подсказка

В этом режиме **TLS** обычно завершается уже на backend-стороне — на встроенном **Nginx** сервера **RuDesktop** или на собственном *обратном прокси*

Когда можно использовать L7

L7-режим допустим только если **WAF/AntiDDoS** умеет на одном listener (порту) корректно пропускать одновременно:

- обычные HTTPS API-запросы (`/api/...`, `/root.pem` и другие);
- **WebSocket Upgrade** на `/v1/`.

Для `/v1/` клиент отправляет:

```
GET /v1/ HTTP/1.1
Upgrade: websocket
Connection: Upgrade
```

Успешный ответ сервера:

```
101 Switching Protocols
```

Примечание

HAProxy в штатной схеме умеет переводить HTTP-соединение в WebSocket-туннель после **upgrade**, но для таких соединений критичны корректные заголовки и таймауты. Готовый пример конфигурации — в разделе *Развёртывание за обратным прокси*

При работе через L7 защитное решение **обязательно** должно:

- **не менять HTTP-метод** для `/v1/` — серверный компонент `rude` принимает на этом пути только `GET` с `Upgrade: websocket`, прочие методы (`POST`, `HEAD`, `OPTIONS`) возвращают `404 Not Found`;
- **не делать healthcheck** на `/v1/` — обычный `GET` без WebSocket-заголовков возвращает `400 Bad Request`. Для health-проб используйте `GET /` на бэкенде `rude` (отдаёт `OK`) или `GET /root.pem` на nginx-vhost;

- **не инспектировать** `/v1/` как короткий HTTP-запрос — WebSocket-сессия может жить часами;
- **увеличить таймауты** для долгоживущих WebSocket-сессий (рекомендуемые значения — `proxy_send_timeout 600s`, `proxy_read_timeout 600s`);
- **передавать без модификации** заголовки `Upgrade` и `Connection`;
- **передавать** заголовки `Host`, `X-Real-Ip` (в формате `$remote_addr:$remote_port`), `X-Forwarded-For`, `X-Forwarded-Proto`.

Важно

Если L7-решение не умеет корректно пропускать **WebSocket** — его нужно переводить в режим **TCP/L4**. Это типовой подход: не все reverse proxy корректно поддерживают **WebSocket**, и в таких случаях TCP mode — рабочая альтернатива

Разделение портов RuDesktop

Разделение портов между админкой и клиентским трафиком — поддерживаемый сценарий (см. *Разделение портов*), но критически важно правильно распределить эндпоинты по портам

Правильно:

- 443 — веб-интерфейс администратора, доступен только внутри сети или через VPN;
- 8443 — клиентский порт **RuDesktop**, публикуется наружу через **WAF/AntiDDoS**.

На клиентском порту 8443 обязательно должны быть доступны:

- `/v1/`
- `/api/login/`
- `/api/logout/`
- `/api/ssolist/`
- `/api/user/`
- `/api/client-settings/`
- `/api/banner/`
- `/api/ab/load/`
- `/root.pem`
- `/download/` — если используется загрузка дистрибутивов через клиентский порт

Неправильно:

- 443 — API;
- 8443 — только `/v1/` WebSocket.

Такой вариант приведёт к ошибкам авторизации, получения настроек, адресной книги и SSO: клиент запросит `/api/login/` через 8443, не получит ответа и не сможет залогиниться

Пример backend Nginx для клиентского порта

Условный пример, который можно адаптировать под конкретную установку:

```
server {
    listen 8443 ssl;
    server_name rd.example.com;

    ssl_certificate     /path/to/fullchain.pem;
    ssl_certificate_key /path/to/private.key;

    client_max_body_size 1000G;

    location /v1/ {
        proxy_pass http://unix:/run/rudesktop/rude.sock;

        proxy_connect_timeout 120s;
        proxy_send_timeout    600s;
        proxy_read_timeout    600s;

        proxy_http_version 1.1;
        proxy_set_header Host              $http_host;
        proxy_set_header X-Real-Ip
↪$remote_addr:$remote_port;
        proxy_set_header X-Forwarded-For
↪$proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header Upgrade           $http_upgrade;
        proxy_set_header Connection        "upgrade";
    }

    location /api/ {
        include proxy_params;
        # Для сценария «двойной прокси» (WAF/AntiDDoS перед nginx)␣
↪переопределяем
        # X-Forwarded-For, чтобы сохранить цепочку IP, добавленную␣
↪защитным узлом
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_pass http://unix:/run/rudesktop-web.sock;
    }

    location /root.pem {
        expires -1;
        alias /var/lib/rudesktop/ca/CA.pem;
    }

    location /download/ {
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
        alias /usr/share/rudesktop/public/download/;
    }

    include rudesktop_params;
}
```

Важно

Для `/v1/` заголовок `X-Real-Ip` должен передаваться в формате `$remote_addr:$remote_port` — с указанием порта источника. Серверный компонент `rude` парсит это значение как `SocketAddr` и при отсутствии порта отбивает соединение с ошибкой `Failed to parse X-Real-IP`. Для остальных эндпоинтов (`/api/`, обслуживается Django через `proxy_params`) достаточно стандартного `$remote_addr`

Важно

Если **WAF/AntiDDoS** работает в режиме **TCP RAW** и не передаёт `X-Forwarded-For`, backend будет видеть IP защитного узла, а не реальный IP пользователя. Если нужен реальный IP клиента — отдельно согласовывайте поддержку **PROXY protocol** на стороне защитного решения. Включать `proxy_protocol` на принимающей стороне можно **только** если защитный узел действительно его передаёт, иначе все соединения будут разрываться

Диагностика

Проверка TLS-уровня

```
openssl s_client -connect rd.example.com:8443 -servername␣
↪rd.example.com -showcerts
```

Нормально — возвращается сертификат сервера

Плохо — ошибки вида:

```
wrong version number
packet length too long
no peer certificate available
```

Обычно это означает путаницу режимов (HTTP, HTTPS, TCP) на стороне защитного узла или включённый **PROXY protocol** без поддержки на backend

Проверка HTTP API

```
curl -vk https://rd.example.com:8443/root.pem
curl -vk -X POST https://rd.example.com:8443/api/ssolist/ \
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
    -H "Content-Type: application/json" \
    -d '{}'
```

Подсказка

Даже если сервер вернул `401`, `403` или `405` — **это лучше**, чем обрыв соединения: запрос дошёл до HTTP-приложения, и проблема не в публикации

Плохо — следующие симптомы означают, что трафик до приложения не доходит:

```
503 Service Unavailable
connection closed before message completed
empty reply from server
```

Связанные страницы

- *Развёртывание за обратным прокси* — общая схема и примеры конфигураций **HAProxy** и **Nginx**
- *Разделение портов* — разделение административного и клиентского трафика по разным портам
- *Ограничение доступа к веб* — как закрыть админ-панель от внешнего доступа
- *Добавление собственных SSL-сертификатов* — замена встроенных самоподписанных сертификатов на доверенные для клиентского порта

Сетевые настройки — раздел с инструкциями по конфигурации сетевых параметров сервера **RuDesktop**: установка собственных SSL-сертификатов, смена IP-адресов и портов, разделение служебного и публичного трафика, ограничение доступа к веб-интерфейсу, настройка подключения к внешней базе данных, работа через unix-socket, развёртывание за обратным прокси и публикация через WAF/AntiDDoS

Добавление собственных SSL-сертификатов

Замена встроенных самоподписанных сертификатов на доверенные

Смена и установка IP

Изменение IP-адреса сервера и его публикация для клиентов

Смена стандартного порта

Перенастройка сервера на нестандартный TCP-порт

Смена адреса для модуля аналитики

Настройка адреса встроенного **Apache Superset** и вынос его базы данных на отдельный сервер

Ограничение доступа к веб-интерфейсу

Закрытие веб-интерфейса и модуля аналитики от внешних подключений

Разделение портов

Вынесение веб-интерфейса и трафика клиентов на разные порты

Настройка подключения и SSL для сторонней БД

Подключение сервера к внешней PostgreSQL с защищённым каналом

Настройка unix-socket

Перевод сервера на работу через unix-socket вместо TCP

Развёртывание за обратным прокси

Установка сервера за HAProxy или Nginx, проксирование WebSocket, типовые проблемы
Настройка балансировщика Nginx перед RuDesktop - пошаговая настройка сертификата, передачи IP и проверка магазина приложений

Публикация через WAF и AntiDDoS

Публикация клиентского порта через средства веб-защиты: TCP passthrough, L7-режим, разделение портов, пример Nginx, диагностика

1.5 Настройки сервера

1.5.1 Настройка уровня логирования

Описание

Параметр **LOG_LEVEL** определяет уровень логирования и какие сообщения будут записываться в файл `/var/log/rudesktop/rudesktop.log`

Вы можете выбирать из следующих уровней логирования:

- **DEBUG** — записывает все сообщения, в том числе диагностическую информацию, полезную для отладки. **Значение по умолчанию**
- **INFO** — записывает общую информацию о работе системы, включая важные события
- **WARNING** — записывает предупреждения о потенциальных проблемах, которые не мешают выполнению

- **ERROR** — записывает ошибки, которые мешают выполнению одной или нескольких функций
- **CRITICAL** — записывает критические ошибки, которые могут привести к отказу системы

Важно

Когда вы задаёте **LOG_LEVEL**, будут записываться сообщения только этого уровня и уровней выше в порядке их серьёзности

Например, если установлен уровень **INFO**, то будут записываться **INFO**, **WARNING**, **ERROR** и **CRITICAL**, но не **DEBUG**

Это позволяет контролировать объём информации, поступающей в логи, что может быть полезно для улучшения производительности и упрощения анализа журнала

Настройка

Чтобы настроить уровень логирования, добавьте или измените параметр **LOG_LEVEL** в файле конфигурации `/etc/rudesktop/settings` (Python-файл)

Примечание

Параметр `LOG_LEVEL` влияет на основные логи сервера. Для отдельных служебных логгеров (`axes`, `django`, `redis`) уровни зафиксированы в коде и не переопределяются, чтобы не засорять журнал

Пример

Чтобы установить уровень логирования на **INFO**, добавьте или измените следующую строку:

```
LOG_LEVEL = 'INFO'
```

После изменения файла конфигурации выполните команду для перезапуска сервера и применения новых настроек:

```
rude restart
```

Подсказка

Подробнее о расположении файлов логов см. на странице *Логи сервера*

1.5.2 Настройка Gunicorn

Описание

Gunicorn управляет рабочими процессами (воркерами) веб-части сервера **RuDesktop** и позволяет эффективно обрабатывать несколько запросов одновременно. Запускается с воркер-классом `uvicorn.workers.UvicornWorker`, бьёт на unix-сокет `/run/rudesktop-web.sock` с таймаутом 600 секунд

Настройка **Gunicorn** позволяет:

- **Увеличить производительность** — настройка количества воркеров под профиль нагрузки сервера, чтобы улучшить скорость обработки запросов и общую отзывчивость
- **Эффективно использовать ресурсы** — слишком большое или малое количество воркеров приводит к простоям или нехватке памяти
- **Устойчивость к нагрузке** — правильная настройка позволяет справляться с большими объёмами трафика, обеспечивая стабильность даже под нагрузкой

Конфигурация воркеров

Чтобы настроить количество воркеров, откройте файл по пути `/etc/default/rudesktop` и добавьте параметр, например:

```
GUNICORN_WORKERS=4
```

Важно

Значение можно адаптировать в зависимости от ресурсов вашего сервера

После изменения параметра перезапустите веб-службу:

```
rude restart rudesktop-web.service
```

или сервер целиком:

```
rude restart
```

Автоматическое выставление

Если параметр `GUNICORN_WORKERS` не задан в файле `/etc/default/rudesktop`, количество воркеров рассчитывается автоматически по формуле:

```
workers = min(2 × CPU + 1, 12)
```

— то есть **в два раза больше количества ядер плюс один**, но не более 12

Пример

- 2 ядра CPU → 2 × 2 + 1 = 5 воркеров
- 4 ядра CPU → 2 × 4 + 1 = 9 воркеров
- 8 ядер CPU → 2 × 8 + 1 = 17 → ограничено максимумом 12 воркеров
- 16 ядер CPU → также 12 воркеров (упирается в потолок)

1.5.3 Настройка определения геолокации

Описание

Геолокация — определение города и координат устройства по его IP-адресу. Используется для:

- отображения устройств на *карте*
- подбора ближайшего *моста* при подключении к удалённому филиалу
- статистики по локациям подключений

Сервер **RuDesktop** определяет геолокацию **автоматически** для устройств с публичными IP-адресами по встроенной базе геолокации. Для устройств с приватными IP-адресами (например, во внутренней корпоративной сети) автоматическое определение не работает — для них настраиваются *Подсети*

Как это работает

Сервер при запуске загружает в память встроенную базу геолокации, которая входит в поставку. Дополнительно настраивать саму базу не требуется

Если для устройства геолокация определена, в данных устройства сохраняются город, регион, страна и координаты. Эти значения используются на странице **«Карта»** и при выборе ближайшего моста

Шаги настройки

Стандартный сценарий настройки состоит из трёх шагов:

1. **Загрузить справочник городов** в базу данных. Этот справочник используется в форме *подсети* и при сопоставлении IP→город:

   ```
   rude load_cities
   ```

   Подробности — на странице *load_cities*

2. **Проверить, что внешний IP резолвится корректно**:

   ```
   rude locate 8.8.8.8
   rude locate 81.19.72.32
   ```

   Команда выведет город, в который сервер сопоставил указанный IP. Подробности — на странице *locate*

3. **Проставить геолокацию устройствам, у которых её ещё нет**:

```
rude update_peers_geo
```

Команда вычислит геолокацию для всех устройств, у которых она ещё не сохранена в базе. Подробности — на странице *update_peers_geo*

Подсказка

Команду можно повесить на `cron`, чтобы геопозиции на карте оставались актуальными по мере подключения новых устройств

Перепроверка сохранённых геолокаций

Если внешний клиент попадает в неверный город (например, после обновления сервера или массового изменения подсетей), пересчитайте сохранённые геолокации:

```
rude locate --all
```

Команда пройдёт по всем сохранённым в базе геолокациям и обновит записи, у которых результат изменился. Подробности — на странице *locate*

Диагностика

Симптом	Что проверить
`rude locate <публичный IP>` возвращает неверный город	Выполните `rude locate --all` для пересчёта сохранённых записей после обновления сервера
Устройства с публичными IP не появляются на карте	Геолокация записывается при подключении устройства. Для давно неактивных устройств выполните `rude update_peers_geo`
Устройства с приватными IP не определяются автоматически	Это ожидаемо — для приватных адресов настраиваются *Подсети*

См. также

- *Подсети* — определение геолокации для устройств с приватными IP-адресами
- *Карта* — отображение устройств по геопозиции
- *load_cities*, *locate*, *update_peers_geo* — CLI-команды для работы с геолокацией

1.5.4 Обзор конфигурационных файлов

Файл конфигурации /etc/default/rudesktop

Файл конфигурации — переменные окружения, через которые задаются адреса, параметры базы данных и режим работы всех компонентов сервера **RuDesktop**

Описание

Все службы сервера — веб-интерфейс, relay, executor, PXE и Redis — запускаются через команду `rude`, и при каждом запуске файл `/etc/default/rudesktop` читается как источник переменных окружения. Файл создаётся автоматически при установке сервера командой *rude install*; владелец — `root`, группа — `rudesktop`

Файл переживает обновления пакета: установщик не перезаписывает уже существующие значения. Полностью файл удаляется деструктивной командой *rude reinstall* или при полном удалении пакета сервера

Подсказка

На этой странице описаны базовые параметры. Конфигурация relay — на странице *rudesktop-relay.toml*, дополнительные параметры для нестандартных сценариев и диагностики — на странице *Расширенные параметры*

Применение изменений

1. Отредактируйте файл, например:

   ```
   nano /etc/default/rudesktop
   ```

2. Перезапустите сервер целиком:

   ```
   rude restart
   ```

   или только нужную службу:

   ```
   rude restart rudesktop-web.service
   ```

Важно

Адрес сервера (`PUBLIC_HOST`, `PUBLIC_PORT`, `PUBLIC_IP`) и аргументы установки меняются командами установки, а не правкой файла. Порядок действий описан на странице *Смена и установка IP*; полная перегенерация конфигурации **nginx** и сертификатов выполняется деструктивной командой *rude reinstall*

Адреса и порты

Переменная	Назначение
`PUBLIC_HOST`	Публичный домен или IP-адрес, по которому клиенты и браузеры обращаются к серверу. Используется веб-интерфейсом, relay и при генерации **nginx**
`PUBLIC_PORT`	Публичный порт. Если при установке порт не указан, используется 443
`PUBLIC_IP`	Публичный IP-адрес сервера; заполняется установщиком при генерации конфигурации. Используется *PXE-сервером* и *публикацией образов ОС*; при пустом значении PXE-сервер определяет адрес из `PUBLIC_HOST`
`LOCAL_HOST` / `LOCAL_PORT`	Локальный адрес сервера для *режима двух IP*, когда из внутренней и внешней сети сервер доступен по разным адресам. Если при установке передан один адрес, совпадают с `PUBLIC_HOST` / `PUBLIC_PORT`

Режим установки

Переменная	Назначение
`INSTALL_MODE`	Роль узла при развёртывании. Задаётся при установке пакета и определяет состав включаемых служб: `standalone` — полный сервер (по умолчанию), `relay` — *мост*, `executor` — *исполнитель или точка распространения*
`INSTALL_ARGS`	Аргументы, переданные команде `rude install` (адреса сервера). Заполняется установщиком автоматически и используется при повторной установке без аргументов — вручную не редактируется

База данных

Переменная	Назначение
POSTGRES_HOST	Адрес PostgreSQL. По умолчанию localhost
POSTGRES_PORT	Порт PostgreSQL. По умолчанию 5432
POSTGRES_DB	Имя базы данных. По умолчанию rudesktop
POSTGRES_USER	Пользователь базы данных. По умолчанию rudesktop
POSTGRES_PASSWORD	Пароль базы данных; генерируется установщиком
POSTGRES_SSL_MODE	Режим SSL-соединения с PostgreSQL. По умолчанию disable
POSTGRES_CA_FILE	Путь к сертификату CA (root.crt) для режимов проверки verify-ca и verify-full

Подсказка

Подключение к внешнему PostgreSQL и полный список значений POSTGRES_SSL_MODE — на странице *Настройка подключения и SSL для сторонней БД*

Служебные параметры

Переменная	Назначение
SECRET_KEY	Секретный ключ веб-интерфейса: подпись сессий и токенов. Генерируется установщиком; смена значения прерывает активные сессии пользователей
SMB_PASSWORD	Пароль учётной записи rudesktop для доступа к файлам сервера по протоколу SMB — используется при установке ОС по сети и миграции Windows на Linux; генерируется установщиком
TFTP_BLOCK_SIZE_LIMI	Лимит размера блока данных TFTP-сервера PXE в байтах. По умолчанию 512; подробнее — *Настройка размера блока TFTP*
UPGRADE_BACKUP	Резервная копия базы данных перед мажорным обновлением пакета: always (по умолчанию), ask, never. Подробнее — *Резервное копирование*
GUNICORN_WORKERS	Число рабочих процессов веб-интерфейса. Без значения рассчитывается автоматически. Подробнее — *Настройка Gunicorn*
REDIS_URL	Адрес Redis, например redis://localhost:32459; для подключения с паролем — redis://:password@address:port. Подробнее — *Настройка Redis*

Важно

Значения SECRET_KEY, POSTGRES_PASSWORD и SMB_PASSWORD генерируются автоматически. Не публикуйте их и не меняйте без необходимости: смена SECRET_KEY прерывает активные сессии и подписанные токены, а рассинхронизация POSTGRES_PASSWORD с самим PostgreSQL приводит к недоступности сервера

Типовые сценарии

Подробные пошаговые инструкции по частым задачам вынесены в отдельные страницы:

- Вынести базу данных на отдельный PostgreSQL или включить SSL-соединение с БД — *Настройка подключения и SSL для сторонней БД*
- Подключить внешний Redis, в том числе с паролем — *Настройка Redis*
- Изменить число воркеров веб-интерфейса — *Настройка Gunicorn*
- Управлять резервной копией базы данных перед обновлением пакета — *Резервное копирование*
- Сменить адрес или порт сервера, настроить два IP-адреса — *Смена и установка IP*

Конфигурационный файл rudesktop-relay.toml

Файл rudesktop-relay.toml — дополнительная конфигурация **relay**, компонента сервера, через который устройства обмениваются трафиком при подключении не напрямую. Используется при развёртывании *мостов* и для параметров, которые нельзя задать в */etc/default/rudesktop*

Описание

Файл по пути /etc/rudesktop-relay.toml установщиком не создаётся. Чтобы relay читал его, добавьте в /etc/default/rudesktop строку:

```
RELAY_ARGS='-C /etc/rudesktop-relay.toml'
```

Без файла relay работает на значениях из /etc/default/rudesktop: адрес сервера берётся из PUBLIC_HOST:PUBLIC_PORT, подключение к базе данных — из POSTGRES_*, Redis — из REDIS_URL

Приоритет параметров (от меньшего к большему):

1. значения из /etc/default/rudesktop
2. ключи rudesktop-relay.toml
3. аргументы из RELAY_ARGS (перекрывают одноимённые ключи файла)

Режим моста

relay работает как мост, если в файле задан раздел `[master]` с адресом главного сервера. С таким разделом relay подключается к главному серверу по WebSocket и использует его базу данных вместо локальной, а ключ `api_key` на мосте и на главном сервере должен совпадать — по нему серверы аутентифицируют друг друга

Подсказка

Полный порядок развёртывания моста с примером файла — на странице *Настройка мостов*

Ключи

Мост

Ключ	Назначение
`api_key`	Общий секрет моста и главного сервера; значения на обеих сторонах должны совпадать
`master.url`	Адрес главного сервера для режима моста, например `wss://192.168.10.10/v1/`. Заданный ключ переводит relay в режим моста

Подключение к базе данных и Redis

Ключ	Назначение
`db_host` / `db_port` / `db_name` / `db_user` / `db_pass`	Подключение к PostgreSQL. По умолчанию — значения `POSTGRES_*` из `/etc/default/rudesktop`
`db_pool_size`	Размер пула соединений с базой данных. По умолчанию `64`
`db_ca_cert`	Путь к сертификату CA для SSL-соединения с БД
`redis_server`	Адрес Redis в формате URL. По умолчанию — значение `REDIS_URL` из `/etc/default/rudesktop`

Важно

Режим SSL к базе данных ключом `db_ssl_mode` задать нельзя: независимо от файла всегда используется переменная `POSTGRES_SSL_MODE` из `/etc/default/rudesktop`

Слушатели и сертификаты

Ключ	Назначение
`[[server]]`	Массив слушателей relay. В каждом элементе: `listen` — адрес (`host:port`) или путь unix-сокета (начинается с `/`), `key` и `cert` — пути к ключу и сертификату TLS (без них слушатель работает без шифрования), `webroot` — каталог, из которого HTTP-слушатель отдаёт файлы проверки домена при автоматическом выпуске сертификатов. Если слушатели не заданы, relay слушает unix-сокет `/run/rudesktop/rude.sock`
`ca_key` / `ca_cert`	Пути к ключу и сертификату корневого центра сертификации, которым сервер подписывает сертификаты устройств и мостов. По умолчанию `/var/lib/rudesktop/ca/CA.key` и `/var/lib/rudesktop/ca/CA.pem`

Поведение соединений

Примечание

Способ подключения (`auto` / прямое / через ретранслятор), выдача нового ID при смене hostname и использование hostname как ID настраиваются в веб-интерфейсе на странице **Настройки** — в файле они не задаются

Ключ	Назначение
`use_public_ip`	Возвращать клиенту адрес ретранслятора по тому узлу, к которому клиент подключился. Для сервера с несколькими сетевыми интерфейсами; аналог аргумента `-p`
`trace`	Включает запись в лог обмена сообщениями протокола между клиентами и сервером; уровень детализации 1–9. Аналог аргумента `-t`

Статусы устройств и кеш

Ключ	Назначение
`cache_ttl`	Время жизни в Redis кеша состояния подключенных устройств (адрес, версия, статус), секунды. По умолчанию `300`
`flush_interval`	Как часто изменения статусов устройств переносятся из очереди Redis в базу данных, секунды. По умолчанию `60`
`flush_batch`	Сколько изменений статусов записывается в базу за один раз. По умолчанию `1000`
`cache_preload`	Загрузить состояние всех устройств из базы данных в кеш Redis при старте relay, до первых подключений. По умолчанию выключено — кеш заполняется по мере обращений
`keep_statuses`	Не сбрасывать статусы устройств при перезапуске relay. По умолчанию выключено — при каждом старте службы все устройства отмечаются офлайн до следующего выхода на связь
`disable_updater`	Отключить фоновый перенос изменений статусов устройств из Redis в базу данных (задачу, управляемую `flush_interval` и `flush_batch`). Статусы в базе перестают обновляться. По умолчанию выключено — перенос выполняется

Логи и диагностика

Ключ	Назначение
`log_level`	Уровень логирования: `trace`, `debug`, `info`, `warn`, `error`. По умолчанию `info`
`log_path`	Путь к файлу лога relay. По умолчанию `/var/log/rudesktop/server.log`

Примеры

Диагностика соединений

Если подключения к серверу устанавливаются с ошибками, на время диагностики включите подробный лог и трассировку протокола:

```
log_level = "debug"
trace = 5
```

После диагностики верните `log_level = "info"` и удалите `trace`: с трассировкой файл лога быстро растёт

Не сбрасывать статусы при перезапусках

Если relay перезапускается несколько раз подряд (например, во время работ на сервере), чтобы устройства не отмечались офлайн при каждом старте, добавьте:

```
keep_statuses = true
```

Уберите ключ по окончании работ: при штатной работе статусы должны сбрасываться при старте, иначе устройства, отключившиеся во время простоя сервера, будут оставаться числиться онлайн

Применение изменений

После изменения файла перезапустите relay:

```
rude restart rudesktop-relay.service
```

Расширенные параметры сервера

Расширенные параметры — дополнительные переменные файла `/etc/default/rudesktop` для нестандартных сценариев: диагностика, отладка, вынесенные хранилища, тонкая настройка relay

Предупреждение

Базовая настройка сервера не требует этих параметров. Используйте их только для конкретной задачи: неверные значения могут нарушить работу сервера, а временные значения диагностики — например, подробное логирование — возвращайте обратно после проверки

Изменения применяются так же, как для *базовых параметров*: правка файла и перезапуск *rude restart*

Аргументы relay

`RELAY_ARGS` — аргументы, которые relay получает при каждом запуске. Переменная создаётся установщиком пустой

Основное применение — подключение TOML-конфигурации relay, подробнее — на странице *Конфигурационный файл rudesktop-relay.toml*:

```
RELAY_ARGS='-C /etc/rudesktop-relay.toml'
```

Аргумент	Назначение
`-C, --config <PATH>`	Путь к TOML-файлу конфигурации relay
`-l, --loglevel <LEVEL>`	Уровень логирования: `trace`, `debug`, `info`, `warn`, `error`
`-t, --trace <LEVEL>`	Запись в лог обмена сообщениями протокола между клиентами и сервером, уровень детализации 1–9
`-p, --usepublicip`	Возвращать клиенту адрес ретранслятора по тому узлу, к которому клиент подключился. Используется на сервере с несколькими сетевыми интерфейсами — подробнее в *Смене и установке IP*

Подсказка

Полный список аргументов relay выводит команда:

```
/usr/share/rudesktop/rudesktop-server --help
```

Настройка мостов с `-C` описана на странице *Настройка мостов*

Адрес главного сервера

`SETUP_SERVER` — адрес главного сервера для узлов, развёрнутых не в режиме `standalone` (например, `executor`). Определяет адрес сервера установки — источник клиентских пакетов и публикуемых образов ОС; задаётся на каждой точке распространения. Если переменная не задана, используется `PUBLIC_HOST:PUBLIC_PORT`

Применяется на точках распространения — см. *Настройка точек распространения*

Модуль аналитики

По умолчанию модуль аналитики (**Apache Superset**) использует адреса и базу данных основного сервера. Переменные ниже задают отдельные значения:

Переменная	Назначение
SUPERSET_PUBLIC_HOST / SUPERSET_PUBLIC_PORT	Публичный адрес модуля аналитики
SUPERSET_LOCAL_HOST / SUPERSET_LOCAL_PORT	Локальный адрес модуля аналитики
POSTGRES_SUPERSET_HO / POSTGRES_SUPERSET_PO / POSTGRES_SUPERSET_US / POSTGRES_SUPERSET_PA	Подключение к базе данных модуля аналитики; по умолчанию наследуют значения POSTGRES_*
POSTGRES_SUPERSET_DB	Имя базы данных модуля аналитики; фиксированное значение superset

Подсказка

Пример настройки — на странице *Смена адреса для модуля аналитики*

Каталоги и хранилища

Переменная	Назначение
DATA_DIR	Корневой каталог данных сервера: загруженные файлы и медиа, репозитории, сертификаты CA, kickstart-преднастройки. По умолчанию /var/lib/rudesktop
LOGS_DIR	Каталог логов сервера. По умолчанию /var/log/rudesktop
REPOSITORY_DISKS_DIR	Каталог *хранилища образов дисков* для установки ОС и миграции. По умолчанию <DATA_DIR>/disks
REPOSITORY_DISK_CACH	Максимальный размер локального кеша образов дисков. По умолчанию 10G

Важно

После смены DATA_DIR перенесите данные на новый путь и сохраните права пользователя rudesktop, иначе сервер не запустится

Пути relay

Переменная	Назначение
`CA_KEY_PATH`	Путь к ключу корневого CA, которым relay подписывает сертификаты устройств и мостов. По умолчанию `/var/lib/rudesktop/ca/CA.key`
`CA_CERT_PATH`	Путь к сертификату корневого CA. По умолчанию `/var/lib/rudesktop/ca/CA.pem`
`RZ_SERVER_LOG_PATH`	Путь к файлу лога relay; расположение логов описано на странице *Логи сервера*. По умолчанию `/var/log/rudesktop/server.log`

Системный пользователь

Примечание

Имя системного пользователя `SYS_USER` и группы `SYS_GROUP` (по умолчанию `rudesktop`) задаются до чтения файла конфигурации — указание их в `/etc/default/rudesktop` не действует

Обзор конфигурационных файлов — какие файлы настроек использует сервер **RuDesktop**, где они находятся, какие создаёт установщик и какие можно править вручную

Состав

Все файлы создаёт установщик при установке сервера

Файл	Назначение	Ручная правка
`/etc/default/rudesktop`	Переменные окружения всех компонентов: адреса, база данных, режим установки — *переменные и сценарии*	Да
`/etc/rudesktop-relay.toml`	Конфигурация relay: мосты, слушатели, статусы и кеш — *ключи TOML*	Да, создаётся вручную
`/etc/rudesktop/settings`	Настройки веб-интерфейса: `ALLOWED_HOSTS`, `DEBUG_TOOLS`	Да
`/etc/nginx/sites-available/rudesktop`	Виртуальный хост **nginx**: проксирование, SSL, сжатие	Да
`/etc/nginx/nginx.conf`	Основной конфиг **nginx**; создаётся при установке, лимиты воркеров обновляются установщиком	Да, с осторожностью
`/etc/nginx/rudesktop_params` и `/etc/nginx/rudesktop_pxe_params`	Вспомогательные файлы **nginx**, подключаемые к виртуальному хосту: правила загрузки пакетов, PXE, защищённые медиафайлы	Нет, перезаписываются
`/etc/rudesktop/ansible.cfg`	Конфигурация **Ansible** для политик и задач	Нет, перезаписывается
`/etc/rudesktop/redis.conf`	Конфигурация встроенного Redis; копируется при установке, если отсутствует — *настройка Redis*	Редко
`/var/lib/rudesktop/ca/`	Ключ и сертификат корневого CA, конфигурация выпуска сертификатов	Нет

Что перезаписывается при каждой установке

Повторный запуск *rude install* не трогает уже существующие файлы, кроме:

- `/etc/rudesktop/ansible.cfg`
- `/etc/nginx/rudesktop_params` и `/etc/nginx/rudesktop_pxe_params`
- `/var/lib/rudesktop/ca/config.cfg`

Деструктивная команда *rude reinstall* удаляет `/etc/default/rudesktop`, каталог `/etc/rudesktop` целиком, виртуальный хост **nginx** и корневой CA, после чего генерирует их заново — ручные правки этих файлов пропадут

Настройки веб-интерфейса /etc/rudesktop/settings

Файл дополнительных настроек веб-интерфейса. Генерируется при установке и содержит адреса сервера из установки:

```
PUBLIC_HOST='example.com'
PUBLIC_PORT='443'
LOCAL_HOST='example.com'
LOCAL_PORT='443'
DEBUG_TOOLS=False
ALLOWED_HOSTS = ['example.com',]
```

Типичные случаи ручной правки:

- **Добавить адреса в** `ALLOWED_HOSTS` — если сервер отвечает по доменам или IP, не указанным при установке (например, при публикации через балансировщик). Без этого веб-интерфейс по такому адресу вернёт `400 Bad Request`. Например, сервер дополнительно отвечает по `server2.example.com`:

  ```
  ALLOWED_HOSTS = ['example.com', 'server2.example.com',]
  ```

- `DEBUG_TOOLS=True` — включает отладочную панель. Только на время диагностики

Предупреждение

`PUBLIC_HOST` и `PUBLIC_PORT` в этом файле дублируют значения */etc/default/rudesktop* — синхронизируйте их вручную, если меняете адрес сервера

Конфигурация nginx

Виртуальный хост `/etc/nginx/sites-available/rudesktop` — основной файл для ручных правок сервера: ограничение доступа, собственные сертификаты, проксирование через WAF. Типовые изменения описаны в разделе *Сетевые настройки*:

- *Ограничение доступа к веб-интерфейсу*
- *Добавление SSL-сертификата*
- *Публикация через WAF / Anti-DDoS*
- *Настройка nginx как балансировщика*

Файлы `rudesktop_params` и `rudesktop_pxe_params` подключаются к виртуальному хосту автоматически и перезаписываются при каждой установке — свои location-блоки добавляйте в виртуальный хост, а не в эти файлы

Ansible и Redis

`/etc/rudesktop/ansible.cfg` перегенерируется установщиком; рабочие параметры **Ansible** — число параллельных потоков и таймауты — задаются в веб-интерфейсе на странице **Настройки** и применяются при запуске задач

Подключение сервера к Redis задаётся переменной `REDIS_URL` в `/etc/default/rudesktop`, сам `redis.conf` правится только для специфических сценариев — *Настройка Redis*

Дополнительные переменные для нестандартных сценариев собраны на странице *Расширенные параметры*

Настройки сервера — раздел с инструкциями по конфигурации компонентов сервера **RuDesktop**: уровень детализации логов, параметры запуска веб-приложения через **Gunicorn**, определение геолокации устройств, обзор конфигурационных файлов, файлы конфигурации `/etc/default/rudesktop` и `rudesktop-relay.toml`, расширенные параметры для технической поддержки

Настройка уровня логирования
Управление подробностью логов сервера и его компонентов

Настройка Gunicorn
Параметры рабочих процессов веб-сервера Gunicorn

Настройка определения геолокации
База геолокации и шаги для определения города по IP устройства

Обзор конфигурационных файлов
Все файлы настроек сервера: назначение, генерация, правила ручной правки

Файл конфигурации
Переменные `/etc/default/rudesktop`: адреса, база данных, режим установки

Конфигурация relay
Ключи `rudesktop-relay.toml`: мосты, слушатели, статусы и кеш

Расширенные параметры
Дополнительные переменные для технической поддержки и нестандартных сценариев

1.6 Команды сервера

1.6.1 Действия с адресной книгой

addressbook

Импорт и экспорт адресной книги пользователя

Зачем нужна

Команда переносит *личную адресную книгу* пользователя между серверами или восстанавливает её из бэкапа в формате JSON. Через веб-интерфейс адресная книга добавляется только вручную, и для массового переноса/восстановления нужна именно CLI-команда

Типичные случаи применения:

- миграция пользователя на другой сервер **RuDesktop** — выгрузка с одного, загрузка на другом
- восстановление адресной книги после случайного удаления адресов или сброса учётной записи
- массовая раздача типового набора адресов сотрудникам — подготовить эталонный JSON и импортировать всем нужным пользователям
- бэкап адресных книг ключевых сотрудников отдельно от резервной копии всего сервера

Синтаксис

```
rude addressbook --user [имя_пользователя] import [путь_до_файла]
rude addressbook --user [имя_пользователя] export [путь_до_файла]
```

Параметры

Параметр	Описание
–user	Имя пользователя (обязательный)
import	Подкоманда импорта адресной книги из файла
export	Подкоманда экспорта адресной книги в файл (формат JSON)
путь_до_файла	Путь до файла-источника (для `import`) или файла-приёмника (для `export`)

Важно

При импорте текущая личная адресная книга и теги указанного пользователя **полностью замещаются** содержимым файла. Общие книги команда не затрагивает

Пример

Импорт адресной книги

Чтобы импортировать пользователю адресную книгу из файла, введите следующее:

```
rude addressbook --user rude import /home/rude/addressbook.json
```

После успешного импорта у пользователя на странице **«Адреса»** появятся адреса из файла

Экспорт адресной книги

Чтобы выгрузить адресную книгу пользователя в файл (формат JSON), введите следующее:

```
rude addressbook --user rude export /home/rude/addressbook.json
```

В файл будут записаны адреса личной книги пользователя (с их alias и тегами) и список тегов, назначенных этим адресам

Примечание

В экспорт попадают только теги, назначенные хотя бы одному адресу. Теги без адресов в файл не выгружаются

Действия с адресной книгой — CLI-команды для импорта и обслуживания адресной книги пользователей сервера

Команда	Описание
addressbook	Импорт адресной книги

1.6.2 Действия с гео

load_cities

Загрузка справочника городов в базу данных для определения геолокации

Зачем нужна

Команда заполняет на сервере таблицу городов из встроенного датасета. Эти города используются для определения геолокации устройств по IP и при настройке *подсетей* в админ-панели — выпадающий список городов в форме подсети берётся именно из этой таблицы

Типичные случаи применения:

- первичная инициализация справочника после установки сервера, если города не подгрузились автоматически
- обновление встроенного списка городов после обновления версии сервера
- восстановление таблицы городов после очистки БД или нештатного отказа геолокационного модуля

Синтаксис

```
rude load_cities [--quiet]
```

Параметры

Параметр	Описание
--quiet	Загрузить города без вывода

Примечание

Служебная команда — используется, когда базу городов для определения геолокации подключений клиентов нужно обновить или загрузить впервые

Подсказка

Полный сценарий настройки определения геолокации описан на странице *Настройка определения геолокации*

Пример

```
rude load_cities
Loading cities dataset... OK (1134 cities loaded from file)
OK (1134 cities loaded to database)
```

Тихий режим (без вывода в консоль):

```
rude load_cities --quiet
```

locate

Определение геолокации по IP-адресу

Зачем нужна

Команда вручную проверяет, в какой город сервер сопоставит указанный IP-адрес: либо по правилам *подсетей*, либо по внешним базам геолокации. Также пересчитывает все сохранённые в базе геолокации устройств — режим `--all`

Типичные случаи применения:

- проверить корректность настройки правил подсетей перед массовым применением (что подсеть действительно сопоставляется нужному городу)
- диагностика неверной геопозиции на *карте*: на каком этапе IP получает не тот город
- пересчёт всех сохранённых геолокаций после массового изменения правил подсетей или обновления внешних баз
- разовая проверка IP, по которому подключился внешний клиент, без открытия админ-панели

Синтаксис

```
rude locate [ip_address ...]
rude locate --all
```

Параметры

Параметр	Описание
ip_address	Один или несколько IP-адресов через пробел, для которых нужно определить геолокацию
--all	Перепроверить все сохранённые в БД геолокации и вывести только те записи, у которых результат изменился

Примечание

В первой форме передаётся один или несколько IP-адресов через пробел — для каждого выводится определённая геолокация. Во второй форме команда проходит по всем сохранённым в базе геолокациям и сообщает о записях, у которых результат изменился, с подсчётом «битых» (без определённого города)

Подсказка

Полный сценарий настройки определения геолокации описан на странице *Настройка определения геолокации*

Примеры

Определение геолокации одного IP-адреса:

```
rude locate 8.8.8.8
США
```

```
rude locate 81.19.72.32
Москва, Россия
```

Определение геолокации нескольких IP-адресов одной командой:

```
rude locate 8.8.8.8 81.19.72.32
```

Перепроверка всех сохранённых геолокаций:

```
rude locate --all
```

update_peers_geo

Обновление геолокации устройств на основе их IP-адресов

Зачем нужна

Команда массово вычисляет геолокацию для устройств, у которых её ещё нет в базе. По результатам устройства появляются на *карте* и в фильтрах по городу. Без этой команды геолокация записывается только при подключении устройства к серверу — у давно неактивных устройств она может отсутствовать

Типичные случаи применения:

- разовое заполнение геолокации после первичного импорта большого парка устройств
- перерасчёт после массового изменения *подсетей*, чтобы устройства с приватными IP получили нужный город
- регулярный пересчёт по расписанию — добавление вызова в cron, чтобы данные на карте оставались актуальными

Синтаксис

```
rude update_peers_geo [--quiet]
```

Параметры

Параметр	Описание
--quiet	Не выводить служебные сообщения в консоль

Примечание

Команда выбирает IP-адреса устройств, по которым ещё нет записи в таблице геолокаций, определяет для них геолокацию и сохраняет результат в базу данных

Подсказка

Полный сценарий настройки определения геолокации описан на странице *Настройка определения геолокации*

Пример

Чтобы обновить геолокацию у устройств, введите следующее:

```
rude update_peers_geo
```

После выполнения команды отобразится количество обработанных адресов:

```
Updating geo locations... OK (0 peers updated)
```

Действия с гео — CLI-команды для загрузки списка городов, определения геопозиции устройств и обновления геоданных по подключённым клиентам

Команда	Описание
load_cities	Выполнение загрузки параметров городов из файла
locate	Обнаружение геолокации по IP-адресу
update_peers_geo	Обновление геолокации у устройств на основе IP-адресов

1.6.3 Действия с логами

clean_audit_logs

Удаление старых записей аудита из базы данных

Зачем нужна

Команда удаляет старые записи журнала аудита из таблицы `audit_logevent` за рамками указанного периода. Журнал аудита со временем заметно растёт и занимает место в базе — команда позволяет ограничить глубину хранения, не дожидаясь автоматической ротации

Типичные случаи применения:

- регулярная очистка по расписанию (запуск из cron) — поддерживать журнал в установленных по политике границах
- разовая чистка после длительной эксплуатации сервера, когда таблица аудита разрослась и замедляет запросы
- освобождение места под бэкапы базы или подготовка к миграции на другой сервер
- соблюдение требований политики хранения персональных данных — удалить данные старше срока хранения

Важно

Команда удаляет данные **необратимо**. Перед запуском сделайте *резервную копию* базы данных или экспортируйте нужные записи аудита

Синтаксис

```
rude clean_audit_logs [minutes/hours/days/weeks] [amount] [--
↪batch-size N] [--batch-pause SECONDS]
```

Параметры

Параметр	Описание
{minutes/hours/days/weeks}	Единица измерения периода: `minutes` (минуты), `hours` (часы), `days` (дни), `weeks` (недели)
amount	Количество единиц периода (целое число)
–batch-size	Количество записей в одном батче удаления. Значение по умолчанию: `10000`
–batch-pause	Пауза между полными батчами в секундах. Значение по умолчанию: `0.1`. Значение `0` отключает паузы

Регулировка нагрузки на базу данных

Записи удаляются батчами в отдельных транзакциях. По умолчанию один батч содержит **10 000 записей**, а между полными батчами команда делает паузу **0,1 секунды**. Такой режим ограничивает размер одной транзакции и даёт базе данных короткие интервалы для обработки других запросов.

Параметры `--batch-size` и `--batch-pause` позволяют регулировать нагрузку:

- меньший размер батча и более длинная пауза снижают пиковую нагрузку на базу данных, но увеличивают общее время очистки
- больший размер батча и короткая пауза ускоряют очистку, но создают более высокую нагрузку на диски, WAL и autovacuum
- значение `--batch-pause 0` отключает паузы между батчами

Важно

Команда удаляет **все** записи аудита (`audit_logevent`), которые старше указанного периода. Операция необратима — без предварительного резервного копирования восстановить данные будет невозможно

Пример

Чтобы удалить логи аудита, которым более пяти дней, введите следующее:

```
rude clean_audit_logs days 5
```

После выполнения команды логи аудита старше пяти дней будут удалены, и на странице **«Все логи»** они будут отсутствовать

Чтобы снизить нагрузку на базу данных при удалении большого объёма логов, можно использовать батчи по 5 000 записей с паузой 0,2 секунды:

```
rude clean_audit_logs days 5 --batch-size 5000 --batch-pause 0.2
```

clean_job_logs

Удаление старых логов выполнения задач из базы данных

Зачем нужна

Команда удаляет только записи о результатах выполнения UEM-задач (`audit_logevent` с `name = JOB_RESULT`), не трогая остальные записи аудита (входы, HTTP-запросы, CRUD-события). Логи задач — самая «тяжёлая» часть журнала на серверах с регулярной инвентаризацией и массовыми политиками: они быстрее остальных переполняют базу

Типичные случаи применения:

- регулярная очистка логов задач по расписанию, чтобы журнал не разрастался без контроля
- сократить размер журнала задач после массового запуска инвентаризации или большой партии политик
- освобождение места в базе перед бэкапом или миграцией без потери остального аудита (входов, доступов, изменений объектов)

Важно

Команда удаляет данные **необратимо**. Перед запуском сделайте *резервную копию* базы или сохраните нужные записи о выполнении задач отдельно

Синтаксис

```
rude clean_job_logs [minutes/hours/days/weeks] [amount] [--
↪batch-size N] [--batch-pause SECONDS]
```

Параметры

Параметр	Описание
{minutes/hours/days/weeks}	Единица измерения периода: `minutes` (минуты), `hours` (часы), `days` (дни), `weeks` (недели)
amount	Количество единиц периода (целое число)
–batch-size	Количество записей в одном батче удаления. Значение по умолчанию: `10000`
–batch-pause	Пауза между полными батчами в секундах. Значение по умолчанию: `0.1`. Значение `0` отключает паузы

Регулировка нагрузки на базу данных

Записи удаляются батчами в отдельных транзакциях. По умолчанию один батч содержит **10 000 записей**, а между полными батчами команда делает паузу **0,1 секунды**. Такой режим ограничивает размер одной транзакции и даёт базе данных короткие интервалы для обработки других запросов.

Параметры `--batch-size` и `--batch-pause` позволяют регулировать нагрузку:

- меньший размер батча и более длинная пауза снижают пиковую нагрузку на базу данных, но увеличивают общее время очистки
- больший размер батча и короткая пауза ускоряют очистку, но создают более высокую нагрузку на диски, WAL и autovacuum

- значение `--batch-pause 0` отключает паузы между батчами

Важно

В отличие от `clean_audit_logs`, команда удаляет только записи о результатах выполнения задач (записи аудита с `name = JOB_RESULT`). Остальные записи аудита (входы, HTTP-запросы, CRUD-события и т.д.) сохраняются. Операция необратима

Пример

Чтобы удалить логи задач, которым более пяти дней, введите следующее:

```
rude clean_job_logs days 5
```

После выполнения команды записи о выполнении задач старше пяти дней будут удалены

Чтобы снизить нагрузку на базу данных при удалении большого объёма логов, можно использовать батчи по 5 000 записей с паузой 0,2 секунды:

```
rude clean_job_logs days 5 --batch-size 5000 --batch-pause 0.2
```

Действия с логами — CLI-команды для очистки журналов аудита и логов выполнения задач за указанный период

Команда	Описание
clean_audit_logs	Удаление старых логов аудита
clean_job_logs	Удаление старых логов задач

1.6.4 Действия с сервером

backup

Создание резервной копии базы данных сервера

Зачем нужна

Команда сохраняет дамп БД сервера **RuDesktop** в один сжатый файл `.gz`. Это базовая операция резервного копирования: в дамп попадают учётные записи, права, политики, инвентаризация, журналы аудита, адресные книги — все данные сервера, кроме отдельной БД модуля аналитики (для неё есть *superset backup*)

Типичные случаи применения:

- регулярное резервное копирование по расписанию (cron) — основная страховка от потери данных
- бэкап перед обновлением сервера, миграцией БД или внесением рискованных изменений

- срочный бэкап перед деструктивными командами (*reinstall*, массовое удаление, чистка логов)
- подготовка к восстановлению на другом сервере или к миграции

Синтаксис

```
rude backup /path/to/file.gz
```

Параметры

- путь к файлу — обязательный параметр, должен иметь расширение `.gz`. Указывайте полный путь

Примечание

Дополнительные аргументы после имени файла передаются напрямую в `pg_dump`

Наиболее востребованные аргументы:

Аргумент	Описание
--no-security-labels	Не выгружать метки безопасности (`SECURITY LABEL`). Нужен, если дамп снимается на системе с мандатным управлением доступом, а восстанавливаться будет на обычной
--disable-mac	Не выгружать мандатные метки **Astra Linux SE**: `MAC LABEL`, `MAC CCR` и параметр таблиц `macs`
--schema-only	Выгрузить только структуру базы, без данных. Удобно для быстрой проверки состава дампа или сравнения схем двух серверов
--no-owner	Не выгружать команды смены владельца объектов. Полезно, если на целевом сервере другое имя роли — владельца БД
--no-privileges	Не выгружать команды выдачи прав (`GRANT/REVOKE`). Применяется вместе с `--no-owner` при переносе на сервер с другим набором ролей

Важно

Проброс дополнительных аргументов работает начиная с версии сервера **2.9.927**. На более ранних версиях файл `/usr/share/rudesktop/bin/backup` не передаёт их в `pg_dump`: аргументы молча игнорируются, а дамп снимается без них. Порядок ручной правки файла описан на странице *migrate_postgresql*

Важно

Два аргумента передавать нельзя:

- `--data-only` — команда всегда снимает дамп с `--clean`, а `pg_dump` отвергает такое сочетание с ошибкой `options -c/--clean and -a/--data-only cannot be used together`
- `--format` — команда сохраняет дамп в текстовом формате, а *restore* распаковывает файл через `zcat`. Архив в любом другом формате восстановить этой командой не получится

Резервная копия на Astra Linux SE

Если сервер работает на **Astra Linux Special Edition** и использует поставляемую в составе ОС сборку PostgreSQL с поддержкой МРД, `pg_dump` записывает в дамп мандатные метки объектов. На обычном PostgreSQL такой дамп развернуть не получится — он не понимает эти конструкции, и *restore* выдаст ошибки:

```
ОШИБКА: нераспознанный параметр "macs"
ОШИБКА: отношение "public.account_dynamicgroup" не существует
ОШИБКА: ошибка синтаксиса (примерное положение: "MAC")
СТРОКА 1: MAC LABEL ON TABLE public.account_dynamicgroup IS '{0,0}';
```

Важно

Восстановление при этом **не прерывается**: таблицы с мандатными метками не создаются, а зависимые от них команды выпадают в ошибку. База остаётся заполненной частично, поэтому ориентироваться на «команда завершилась» нельзя — нужно смотреть вывод

Чтобы дамп можно было развернуть на любом сервере, снимайте его с двумя аргументами:

```
rude backup /home/rude/backup.gz --no-security-labels --disable-mac
```

Важно

Аргумент `--disable-mac` поддерживает только сборка `pg_dump` с поддержкой МРД. На обычном PostgreSQL команда завершится с ошибкой `unrecognized option '--disable-mac'`, и файл дампа создан не будет. Проверить, что аргументы доступны в текущей сборке:

```
pg_dump --help | grep -E "disable-mac|no-security-labels"
```

Проверить, что аргументы отработали, можно поиском мандатных конструкций в готовом файле — пустой вывод означает, что дамп чистый:

```
zgrep -nE "^MAC (LABEL|CCR) |macs *=|^SECURITY LABEL " /
↪home/rude/backup.gz | head -20
```

Примечание

Искать нужно именно эти конструкции: простой поиск по слову `mac` даст ложные срабатывания на MAC-адресах устройств в данных инвентаризации

Важно

Аргументы указываются **только при создании** дампа. У команды *restore* аналогов нет — она передаёт SQL напрямую в `psql`. Если резервная копия уже снята без этих аргументов, её нужно создать заново

Подсказка

Если резервная копия предназначена для восстановления обратно на **ALSE** с МРД, снимайте её **без** этих аргументов — иначе мандатные метки объектов будут потеряны. Подробнее о механизмах защиты **ALSE** — на странице *Установка сервера на Astra с МКЦ*

Пример

Чтобы создать резервную копию базы данных сервера, введите следующее:

```
rude backup /home/rude/backup.gz
```

После выполнения команды по указанному пути появится файл со сжатым дампом базы данных, созданный с флагами `--clean --create --blobs --compress=9`

Подсказка

Подробнее об использовании, восстановлении и автоматизации см. на странице *Резервное копирование*

collectstatic

Сбор статических файлов веб-интерфейса в один каталог (стандартная команда Django)

Примечание

Используется при первичной установке и обновлении сервера. Если статика повреждена или были изменены файлы, можно запустить команду повторно

Зачем нужна

Команда собирает все CSS, JS, изображения и шрифты веб-интерфейса в один каталог `/usr/share/rudesktop/public`, откуда их раздаёт **nginx**. Без актуального содержимого этого каталога админ-панель отображается «без стилей» или с битыми скриптами. Обычно команда вызывается автоматически установщиком, ручной запуск нужен в нестандартных случаях

Типичные случаи применения:

- ручное восстановление после сбоя обновления сервера, когда статика не пересобралась
- разовая пересборка после ручного изменения шаблонов или CSS/JS
- диагностика: убедиться, что все файлы статики на месте после миграции на новый диск или каталог

Синтаксис

```
rude collectstatic
```

Пример

Чтобы собрать файлы в одном месте, введите следующее:

```
rude collectstatic
```

На запрос подтверждения введите следующее:

```
yes
```

После выполнения команды файлы будут скопированы по пути `/usr/share/rudesktop/public`

clean_video_records

Удаление устаревших видеозаписей сессий

Зачем нужна

Команда удаляет из каталога хранения видеозаписи сессий удалённого доступа старше указанного срока и убирает соответствующие записи из базы данных. Видеозаписи — самые объёмные файлы на сервере, и без регулярной очистки каталог быстро занимает весь диск

Типичные случаи применения:

- регулярная очистка по расписанию — запускается автоматически политикой *Обслуживание сервера*
- разовое освобождение места, когда диск сервера заполнен видеозаписями
- соблюдение требований к сроку хранения записей сессий, принятых в организации
- подготовка к бэкапу или миграции сервера — сократить объём переносимых данных

Важно

Команда удаляет файлы **необратимо**. Восстановить удалённые видеозаписи невозможно

Синтаксис

```
rude clean_video_records [--retention-days N]
```

Параметры

Параметр	Описание
--retention-days	Срок хранения видеозаписей в днях: записи старше указанного срока будут удалены. Значение `0` отключает очистку. Если параметр не указан, удаляются **все** видеозаписи

Опасно

Запуск команды **без параметра** `--retention-days` удаляет **все** видеозаписи независимо от их возраста. Чтобы удалить только устаревшие, всегда указывайте срок хранения

Что именно удаляется

Команда работает только внутри каталога, заданного параметром Путь для хранения видеозаписей в разделе **Администрирование** → *Настройки*. Файлы за пределами этого каталога не затрагиваются

Обрабатываются файлы с расширениями `.webm` и `.mp4`. Вместе с файлами из базы данных удаляются записи о видеозаписях, файлы которых отсутствуют на диске

Текущий объём каталога и количество записей отображаются в том же разделе настроек, в блоке **Видеозаписи**

Пример

1. Удалить видеозаписи старше 90 дней:

   ```
   rude clean_video_records --retention-days 90
   ```

   После выполнения команда выведет итог: количество удалённых файлов, количество удалённых записей в базе данных и объём освобождённого места

2. Проверить, что очистка отключена (команда ничего не удалит):

   ```
   rude clean_video_records --retention-days 0
   ```

   Значение `0` отключает очистку — команда сообщит об этом и завершится

3. Удалить все видеозаписи (например, перед выводом сервера из эксплуатации):

   ```
   rude clean_video_records
   ```

   Опасно

   Будут удалены все видеозаписи на сервере. Убедитесь, что нужные записи выгружены заранее

constance

Получение и установка параметров конфигурации сервера

Подсказка

Данные параметры находятся на странице **«Настройки»** в веб-интерфейсе

Зачем нужна

Команда работает с параметрами *Настройки* сервера из CLI: показать все ключи (`list`), прочитать конкретный (`get`), задать значение (`set`), удалить устаревшие ключи (`remove_stale_keys`). Полезна, когда веб-интерфейс недоступен или требуется автоматизировать настройку

Типичные случаи применения:

- настроить параметры сервера в скрипте развёртывания (`set` в составе Ansible/CI)
- быстро проверить значение нужного параметра в консоли без открытия админ-панели

- массовое восстановление настроек после ручной правки БД или после миграции
- `remove_stale_keys` — после обновления сервера, когда часть параметров была удалена из кода, но осталась в БД

Синтаксис

```
rude constance list
rude constance get [ключ]
rude constance set [ключ] [значение]
rude constance remove_stale_keys
```

Параметры

Параметр	Описание
list	Получение списка всех ключей и их значений
get [ключ]	Получение значения конкретного ключа
set [ключ] [значение]	Установка значения для конкретного ключа
remove_stale_keys	Удаление устаревших ключей

Пример

Получение списка всех ключей

Чтобы получить список со всеми ключами и их значениями, введите следующее:

```
rude constance list
```

После выполнения команды в выводе отобразятся ключи и их значения

```
REGISTRATIONN_ALLOWED FALSE
DEFAULT_PEER_GROP     2
DEFAULT_USER_GROUP    1
SMTP_HOST             localhost
SMTP_PORT             25
...
```

Получение значения ключа

Чтобы получить значение ключа, введите следующее:

```
rude constance get [ключ]
```

После выполнения команды в выводе отобразится значение ключа

Установка значения для ключа

Чтобы установить значение для ключа, введите следующее:

```
rude constance set [ключ] [значение]
```

После выполнения команды значение у ключа успешно изменится

Подсказка

Чтобы убедиться в том, что значение у ключа изменилось, можно выполнить команду `rude constance get [ключ]`

Удаление устаревших ключей

Чтобы удалить устаревшие ключи, введите следующее:

```
rude constance remove_stale_keys
```

После выполнения команды устаревшие ключи успешно удалятся

Подсказка

Ключ считается устаревшим, если он существует в базе данных, но отсутствует в конфигурации

delete

Удаление устройств из БД сервера по дате последней активности

Зачем нужна

Команда удаляет из таблицы *Устройства* устройства со статусом «Не в сети», последняя активность которых была не позднее указанного количества дней назад

Удаление устройств и связанной истории выполняется небольшими порциями, чтобы снизить расход памяти при большой очистке

Типичные случаи применения:

- регулярная плановая чистка через cron - удаление неактивных устройств
- разовая большая чистка после многолетней эксплуатации сервера
- удаление конкретного устройства по идентификатору
- очистка дублирующих записей с подключением по SSH

Важно

Перед удалением сделайте *резервную копию* сервера

При отборе по `--last_active` или `--server_id` без флага `--really` команда только показывает количество объектов под удаление

Опасно

Для режима `--ssh` предварительного подсчета нет: команда изменяет данные и удаляет дублирующие SSH-записи даже без `--really`

Синтаксис

```
rude delete [--last_active N] [--batch-size N] [--really]
rude delete --server_id ID [--batch-size N] [--really]
rude delete --ssh
```

Параметры

Параметр	Описание
--last_active N	Отобрать устройства не в сети с последней активностью не позднее `N` дней назад (по умолчанию `30`, диапазон `0..9998`)
--server_id ID	Отобрать устройство с указанным `server_id` без проверки срока неактивности и статуса, параметр `--last_active` при этом не используется
--batch-size N	Размер порции обработки, целое число больше нуля (по умолчанию `1000`), не больше `100` устройств или `1000` записей истории за этап
--really	Выполнить удаление выбранных устройств, без этого флага выполняется только подсчет (кроме отдельного режима `--ssh`)
--ssh	Выполнить отдельную очистку дублирующих SSH-записей, остальные параметры команды не используются, подтверждение `--really` не требуется

Важно

`--server_id` задает отбор по конкретному идентификатору вместо отбора по сроку неактивности и статусу

Не используйте этот параметр для проверки того, что устройство давно не подключалось: заданное устройство может быть удалено независимо от его активности

Примечание

По умолчанию `--last_active = 30` дней, допустимые значения - от `0` до `9998` включительно

Размер порции и остановка очистки

Параметр `--batch-size` задает размер порции обработки и должен быть больше нуля

По умолчанию используется значение `1000`, при этом за один этап обрабатывается не больше `100` устройств или `1000` записей связанной истории

Чтобы уменьшить размер порции, укажите меньшее значение, например `--batch-size 50`

При удалении по сроку неактивности сервер повторно проверяет состояние устройства между этапами очистки Если устройство снова подключилось или его дата последней активности обновилась и оно больше не подходит под условия, дальнейшая очистка этого устройства прекращается

Предупреждение

Очистка не является одной общей транзакцией: завершенные этапы сохраняются отдельно

При остановке часть устройств или связанной истории уже может быть удалена, даже если команда не завершилась успешно Повторное подключение устройства также не восстанавливает уже очищенную историю

Если запись занята другой операцией или превышено время выполнения SQL, команда останавливается с сообщением об ошибке После устранения причины можно повторить команду с теми же параметрами для обработки оставшихся данных

После успешного завершения команда выводит количество удаленных устройств

Очистка SSH-дубликатов

`--ssh` запускает отдельную очистку дублирующих записей с подключением по SSH и перенос настроек доступа на совпадающие по адресу записи устройств

В этом режиме параметры `--last_active`, `--server_id`, `--batch-size` и `--really` не используются Это не способ включить SSH-устройства в удаление по сроку неактивности

Примеры

1. Чтобы посчитать, сколько устройств попадает под критерии по умолчанию (без фактического удаления):

   ```
   rude delete
   ```

   Для выборки до 500 устройств включительно отчет содержит количество устройств и подсчитанных связанных объектов:

   ```
   Данные по заданным параметрам:
   Устройства: 1
   Связи server-group: 1
   ```

   Если найдено больше 500 устройств, выводится только количество устройств

2. Чтобы удалить устройства не в сети с последней активностью не позднее 60 дней назад:

   ```
   rude delete --last_active 60 --really
   ```

3. Чтобы уменьшить размер порции при очистке:

   ```
   rude delete --last_active 60 --batch-size 50 --really
   ```

4. Чтобы удалить конкретное устройство по идентификатору:

   ```
   rude delete --server_id 123456789 --really
   ```

5. Чтобы очистить дублирующие SSH-записи после создания резервной копии:

   ```
   rude delete --ssh
   ```

diag

Сбор диагностической информации о сервере в архив для передачи в техподдержку

Примечание

Команда собирает в один архив:

- Версию сервера `rude relay --version`
- Конфигурационные файлы (`/etc/default/rudesktop`, `/etc/relay.cfg`, `/etc/rudesktop-relay.toml`, `/etc/rudesktop/settings`, `/etc/hosts`) — пароли и секреты вырезаются
- Текущие значения `rude constance` (тоже без секретов)
- Список устройств по типу ОС из таблицы `peers_server`
- Конфиги `peers_relay`

- Информацию об ОС, hostname, аппаратном и сетевом обеспечении
- Список установленных пакетов
- Логи сервера (`/var/log/rudesktop/`), nginx (`/var/log/nginx/`), syslog, PostgreSQL и `/var/log/messages`

Зачем нужна

Команда собирает «диагностический пакет» сервера для технической поддержки **RuDesktop** — конфиги, логи, версии, состояние ОС и БД — в один архив. Перед упаковкой автоматически вырезает пароли и секреты из конфигов; при необходимости архив можно зашифровать GPG-паролем для безопасной передачи

Типичные случаи применения:

- обращение в техническую поддержку: одной командой собрать всё нужное, не выискивая логи и конфиги вручную
- разбор инцидента собственными силами — снимок состояния сервера на момент проблемы
- передача данных стороннему специалисту по защищённому каналу с шифрованием через `-P`
- архивирование снимков состояния сервера по расписанию для последующего разбора

Синтаксис

```
rude diag [-o out_dir] [-P password]
```

Параметры

Параметр	Описание
-o	Каталог, в который сохранится архив (по умолчанию `/tmp/`)
-P	Пароль для шифрования архива (используется GPG). При наличии флага архив сохраняется в формате `.tar.gz.gpg`

Важно

Без указания `-P` архив сохраняется в формате `.tar.gz`. С паролем — архив шифруется через GPG и сохраняется как `.tar.gz.gpg`. Чтобы распаковать зашифрованный архив:

```
gpg --decrypt rude_diag_<дата>.tar.gz.gpg | tar -xzvf -
```

Пример

1. Чтобы выполнить сбор диагностики без указания пути и пароля, введите следующее:

   ```
   rude diag
   ```

   Архив будет сохранён по пути `/tmp/rude_diag_[ДАТА]_[ВРЕМЯ].tar.gz`

2. Чтобы указать другой каталог для архива:

   ```
   rude diag -o /home/user
   ```

   Архив будет сохранён в `/home/user/rude_diag_[ДАТА]_[ВРЕМЯ].tar.gz`

3. Чтобы создать зашифрованный архив с паролем:

   ```
   rude diag -P 123456
   ```

   Архив будет сохранён по пути `/tmp/rude_diag_[ДАТА]_[ВРЕМЯ].tar.gz.gpg`

4. С указанием каталога и пароля:

   ```
   rude diag -o /home/user -P 123456
   ```

   Архив будет сохранён в `/home/user/rude_diag_[ДАТА]_[ВРЕМЯ].tar.gz.gpg`

gencert

Генерация сертификата для моста с использованием центра сертификации **RuDesktop**

Важно

Полезно, когда один сертификат **SSL/TLS** необходимо использовать для нескольких доменов или поддоменов. Через параметр `--certAltnames` можно указать дополнительные имена (Subject Alternative Names, SAN) — сертификат будет считаться действительным для всех них

Зачем нужна

Команда выпускает сертификат для нового *моста* собственным CA сервера **RuDesktop**. Без валидного сертификата мост не сможет участвовать в защищённом обмене с центральным сервером — этот сертификат и есть «удостоверение» моста в инфраструктуре

Типичные случаи применения:

- разворачивание нового моста в филиале — для него нужен индивидуальный сертификат от CA центрального сервера
- перевыпуск сертификата моста при истечении срока действия или при подозрении на компрометацию ключа
- выпуск сертификата с альтернативными именами (SAN), чтобы один мост обслуживал несколько доменов или подсетей

Синтаксис

```
rude gencert [IP|domain]
rude gencert [IP|domain] --certAltnames [name1,name2,...]
```

Примечание

Команда вызывает `rudesktop-server --genCert` и принимает любые поддерживаемые им флаги

Пример

Чтобы сгенерировать сертификат для моста, введите следующее:

```
rude gencert 192.168.10.10
```

С указанием альтернативных имён:

```
rude gencert 192.168.10.10 --certAltnames␣
↪example.com,api.example.com
```

После успешной генерации сертификат и приватный ключ будут доступны по путям `/tmp/CA.pem` и `/tmp/CA.key`

install

Первичная установка сервера

Зачем нужна

Команда — основной шаг установки сервера **RuDesktop** после распаковки пакета. Инициализирует БД, генерирует сертификаты, копирует unit-файлы systemd, включает и запускает все службы. Что именно устанавливается, определяется режимом `INSTALL_MODE`: полная установка, только мост или только executor

Типичные случаи применения:

- первичное развёртывание сервера на чистой системе сразу после установки пакета
- развёртывание дополнительного моста в филиале (`INSTALL_MODE=relay`)

- развёртывание точки распространения политик в подразделении (`INSTALL_MODE=executor`)
- повторный прогон установки в процессе восстановления, если служба не настроена корректно

Синтаксис

```
rude install [IP:Port]
rude install [доменное_имя:Port]
```

Примечание

Команда выполняет инициализацию сервера, копирует unit-файлы systemd, включает их и запускает службы. Состав устанавливаемых компонентов зависит от переменной `INSTALL_MODE` в `/etc/default/rudesktop`:

- **standalone** (по умолчанию) — Redis, web, relay, executor, PXE
- **relay** — только relay (мост)
- **executor** — executor и web (без relay) — для точек распространения политик

Указывать порт необязательно — по умолчанию используется 443

Пример

Чтобы установить сервер с указанием IP-адреса и портом по умолчанию, введите следующее:

```
rude install 192.168.10.10
```

Чтобы установить сервер с доменным именем и нестандартным портом:

```
rude install example.com:8443
```

Подсказка

Для самоподписных сертификатов рекомендуется указывать доменное имя — это обеспечит выпуск сертификата на имя, а не на адрес

license

Получение информации о текущей лицензии сервера

Подсказка

Та же информация отображается на странице **«Лицензия»** в веб-интерфейсе

Зачем нужна

Команда показывает квоты и срок действия лицензии в консоли — без открытия веб-интерфейса. Удобна для скриптовой проверки и мониторинга: достаточно ли осталось хостов/сессий/аккаунтов, не подходит ли срок к концу

Типичные случаи применения:

- быстрая проверка состояния лицензии перед развёртыванием новых устройств
- скриптовый мониторинг — алерт, если до истечения лицензии осталось мало дней
- сверка активной лицензии при разборе обращения «не удаётся добавить устройство — превышен лимит»
- регулярный отчёт о квотах для руководства без захода в админ-панель

Синтаксис

```
rude license
```

Пример

Чтобы получить информацию о лицензии, введите следующее:

```
rude license
```

После выполнения команды в выводе отобразятся ключевые квоты и срок действия лицензии:

```
License info
  Hosts    — квота по компьютерам и устройствам, и сколько␣
↪использовано
  Sessions — квота по активным подключениям, и сколько использовано
  Accounts — квота по учётным записям пользователей, и сколько␣
↪использовано
  UEM      — доступны ли функции UEM (управление конфигурациями)
  Expired  — дата и время окончания действия лицензии
```

maintain

Регламентное обслуживание сервера: ротация и сжатие логов, очистка устаревших файлов

Зачем нужна

Команда — точка входа в плановое обслуживание сервера: ротация и сжатие журналов в `/var/log/rudesktop/`, удаление архивов старше указанного срока. Запускается автоматически встроенной политикой «Обслуживание сервера»; вручную нужна, когда требуется внеплановая чистка или диагностика

Типичные случаи применения:

- внеплановая чистка после периода интенсивных подключений, когда логи разрослись быстрее обычного
- обслуживание серверов, где автоматическая политика ещё не настроена
- разовое сокращение срока хранения архивных логов перед бэкапом или миграцией
- диагностика: ручной запуск, чтобы убедиться, что обслуживание отрабатывает без ошибок

Синтаксис

```
rude maintain [--log-delete-after-days N]
```

Параметры

Параметр	Описание
--log-delete-after-days	Срок хранения архивных логов в днях (по умолчанию `30`). Файлы `rudesktop.log.*` и `server.log.*` старше указанного срока, а также архивы `archive_<timestamp>/` будут удалены. Допускается дробное значение, например `0.5` — полсуток

Примечание

Команда выполняет следующие операции в каталоге `/var/log/rudesktop/`:

1. Сжимает в gzip файлы `rudesktop.log.*` и `server.log.*` старше **1 дня** в подкаталог `archive_<timestamp>/`
2. Удаляет несжатые файлы и архивы старше срока, заданного в `--log-delete-after-days`

Команда запускается автоматически по расписанию через политику **«Обслуживание сервера»** (см. *Политики*). При необходимости её можно вызвать вручную

Важно

Срок хранения должен быть неотрицательным числом. Отрицательное значение или нечисловой текст команда отвергает: она завершится с ошибкой `Invalid log retention period` и кодом возврата 2, не выполнив никаких действий

Если значение параметра пустое, команда использует срок по умолчанию — `30` дней. Поэтому политика **«Обслуживание сервера»** с незаполненным полем История логов (дни) отрабатывает штатно

Примечание

Видеозаписи сессий команда не затрагивает — для них есть отдельная команда *clean_video_records*. Политика **«Обслуживание сервера»** запускает обе

Примеры

1. Запустить обслуживание со сроком хранения по умолчанию (30 дней):

```
rude maintain
```

2. Удалить архивные логи старше 60 дней:

```
rude maintain --log-delete-after-days 60
```

3. Запустить обслуживание со сроком хранения 7 дней (минимальное удержание):

```
rude maintain --log-delete-after-days 7
```

Подсказка

Расположение и состав логов описаны на странице *Логи сервера*

migrate_postgresql

Данная команда выполняет миграцию базы данных на новую версию **PostgreSQL**

Это означает, что существующие данные и схемы из текущей версии **PostgreSQL** будут перенесены в установленную новую версию

Зачем нужна

Команда переносит БД сервера **RuDesktop** с одной версии **PostgreSQL** на другую без потери данных. Это требуется при обновлении ОС, на которой версия PostgreSQL по умолчанию выше или ниже текущей, либо при плановом переходе на более свежую СУБД ради новых возможностей и поддержки

Типичные случаи применения:

- обновление операционной системы (например, Astra 1.7 / РЕД ОС / Ubuntu), при котором поднимается версия PostgreSQL — старый кластер нужно перенести в новый
- обновление сервера **RuDesktop** до новой мажорной версии, для которой минимальная версия PostgreSQL выше текущей
- миграция с устаревшей версии PostgreSQL на поддерживаемую — для безопасности и совместимости

Важно

Перед миграцией обязательно сделайте *резервную копию* базы. Процедура миграции зависит от ОС — пошаговые инструкции по типовым окружениям приведены ниже

Синтаксис

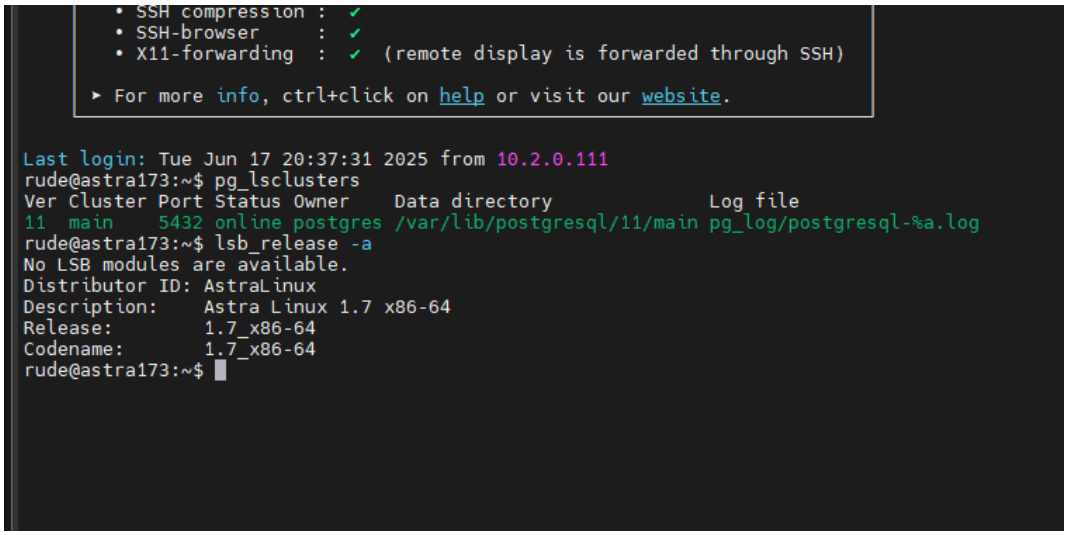
```
rude migrate_postgresql --to [ВЕРСИЯ_POSTGRESQL]
```

Пример

Astra 1.7.x

В данном руководстве описывается пошаговый процесс обновления **PostgreSQL** с версии 11 до версии 14 на Astra Linux 1.7.x для дальнейшего обновления сервера **RuDesktop** до версии 2.9

Окружение стенда:



Сервер **RuDesktop** 2.8.1705

Обновление **PostgreSQL** с 11 до 14 версии:

1. Заменить содержимое файла по пути `/usr/share/rudesktop/bin/backup`:

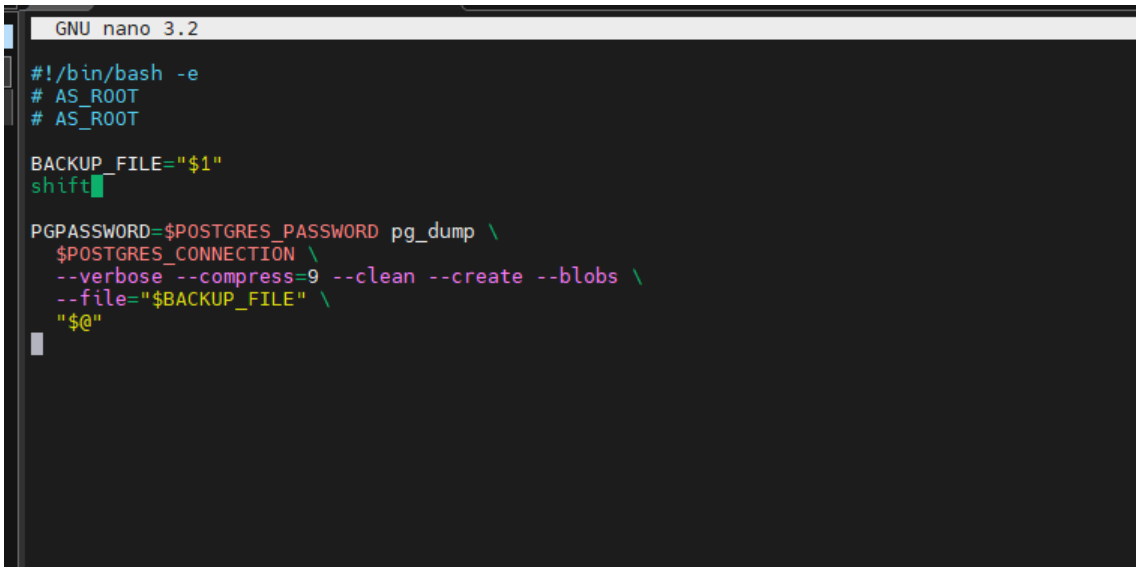
```
#!/bin/bash -e
# AS_ROOT

BACKUP_FILE="$1"
shift

PGPASSWORD=$POSTGRES_PASSWORD pg_dump \
  $POSTGRES_CONNECTION \
  --verbose --compress=9 --clean --create --blobs \
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  --file="$BACKUP_FILE" \
  "$@"
```

Пример:



2. Создать бэкап БД командой:

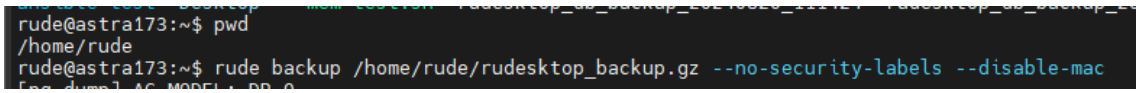
```
rude backup /path/to/file.gz --no-security-labels --disable-mac
```

Важно

Вместо `/path/to/file.gz` указать полный путь, куда будет сохранен файл бэкапа с указанием названия файла

Подробнее о команде *backup*

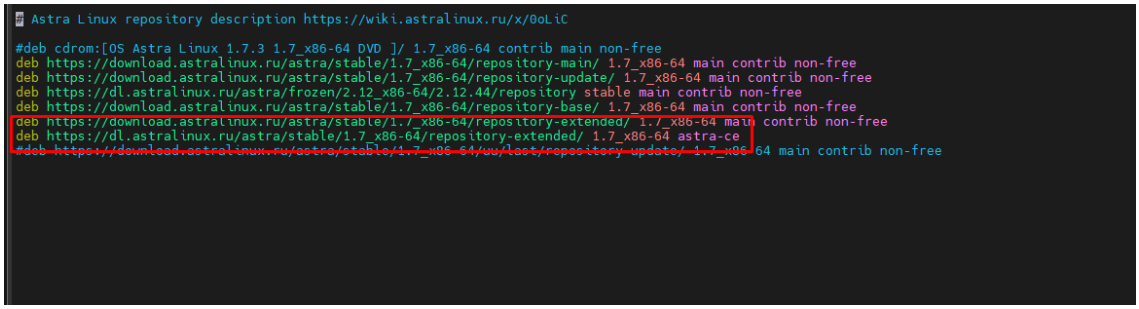
Пример:



3. Добавить расширенный репозиторий **astra-ce** в файл по пути `/etc/apt/source.list`:

```
deb https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-
↪extended/ 1.7_x86-64 astra-ce
```

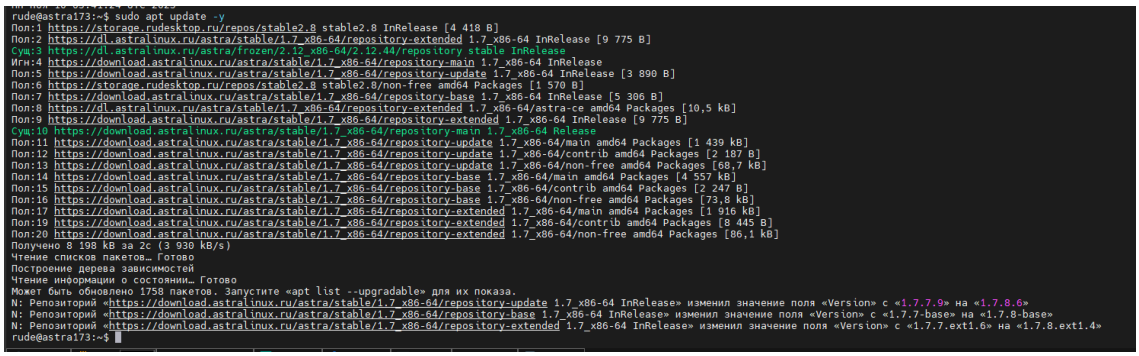
Пример:



4. Выполнить команду по обновлению репозиториев:

```
apt update -y
```

Пример:



Важно

Если при выполнении команды по обновлению репозиториев возникают ошибки, проверьте время на сервере:

```
date -u
timedatectl status
```

Пример:

```
rude@astra173:~$ date -u
Чт июн 26 08:38:44 UTC 2025
rude@astra173:~$ timedatectl status
               Local time: Чт 2025-06-26 15:38:51 +07
           Universal time: Чт 2025-06-26 08:38:51 UTC
                 RTC time: Пн 2025-11-10 06:20:28
                Time zone: Asia/Krasnoyarsk (+07, +0700)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
rude@astra173:~$ sudo timedatectl set-ntp true
rude@astra173:~$ sudo systemctl enable --now systemd-timesyncd
rude@astra173:~$ timedatectl status
               Local time: Пн 2025-11-10 13:20:49 +07
           Universal time: Пн 2025-11-10 06:20:49 UTC
                 RTC time: Пн 2025-11-10 06:20:49
                Time zone: Asia/Krasnoyarsk (+07, +0700)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
rude@astra173:~$
```

5. Остановить cluster **PostgreSQL** 11 командой:

```
pg_dropcluster 11 main --stop
```

6. Проверить отсутствие cluster

```
pg_lsclusters
```

Если clusters отсутствуют, появится следующее сообщение

```
rude@astra173:~$ pg_lsclusters
Ver Cluster Port Status Owner Data directory Log file
rude@astra173:~$
```

7. Удалить **PostgreSQL** 11 командой:

```
apt remove postgresql-11
```

Пример:

```
rude@astra-1:~$ sudo apt remove postgresql-11
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
  libbasicusageenvironment1 libepubgen-0.1-1 libgroupsock8 liblivemedia77 libllvm15
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
  libjson-perl libpq5 postgresql postgresql-14 postgresql-client-14 postgresql-client-common postgresql-common
Предлагаемые пакеты:
  postgresql-doc postgresql-doc-14
Рекомендуемые пакеты:
  libjson-xs-perl
Следующие пакеты будут УДАЛЕНЫ:
  postgresql-11 postgresql-client-11
Следующие НОВЫЕ пакеты будут установлены:
  libjson-perl postgresql-14 postgresql-client-14
Следующие пакеты будут обновлены:
  libpq5 postgresql postgresql-client-common postgresql-common
Обновлено 4 пакетов, установлено 3 новых пакетов, для удаления отмечено 2 пакетов, и 1350 пакетов не обновлено.
Необходимо скачать 18,3 MB архивов.
После данной операции объём занятого дискового пространства возрастёт на 5 557 kB.
```

Важно

PostgreSQL 11 будет удалён, вместо него будет установлен **PostgreSQL** 14, а также будет создан новый кластер, который работает на порту 5432

В выводе терминала можно увидеть, что:

- Следующие пакеты будут УДАЛЕНЫ: postgresql-11 и postgresql-client-11
- Следующие НОВЫЕ пакеты будут установлены: postgresql-14 и postgresql-client-14

8. Проверить cluster для 14 версии **PostgreSQL**:

```
pg_lsclusters
```

Пример:

```
rude@astra173:~$ pg_lsclusters
Ver Cluster Port Status Owner    Data directory              Log file
14  main    5432 online postgres /var/lib/postgresql/14/main /var/log/postgresql/postgresql-14-main.log
rude@astra173:~$
```

Важно

Если в `Ver` значение **14**, в `Port` значение **5432** и в `Status` значение **online**, значит cluster работает и можно продолжать

9. Внести изменения в конфигурационный файл по пути `/etc/postgresql/14/main/pg_hba.conf`

Найти строку:

```
host    all             all             127.0.0.1/32            md5
```

И заменить на:

```
host    all             all             0.0.0.0/0            ␣
↪        md5
```

10. Внести изменения в конфигурационный файл по пути `/etc/postgresql/14/main/postgresql.conf`

    Найти строку:

    ```
    listen_addresses
    ```

    В начале строки удалить символ # и значение `localhost` изменить на *

    ```
    listen_addresses = '*'
    ```

    Найти строку:

    ```
    max_connections
    ```

    Изменить значение на 500

    ```
    max_connections = 500
    ```

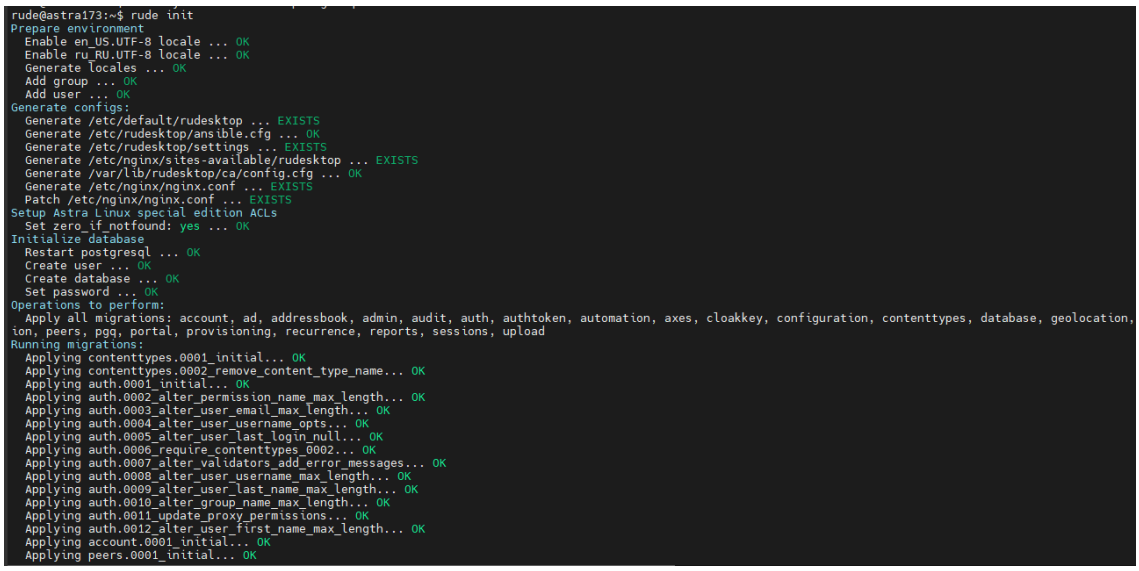
11. Перезапустить **PostgreSQL** командой:

    ```
    systemctl restart postgresql
    ```

12. Выполнить инициализацию сервера **RuDesktop** командой:

    ```
    rude init
    ```

    Пример:



13. Выполнить восстановление БД командой:

    ```
    rude restore /path/to/file.gz
    ```

    Пример:

```
rude@astra173:~$ sudo rude restore /home/rude/backup_rudesktop.gz
Stopping services
  Stopping nginx ... OK
  Stopping web socket ... OK
  Stopping web service ... OK
  Stopping relay ... OK
  Stopping redis service ... OK
  Stopping executor ... OK
  Stopping pxe ... OK
  Stopping smbd ... OK
SET
SET
SET
SET
SET
 set_config
------------

(1 строка)

SET
SET
SET
SET
SET
DROP DATABASE
CREATE DATABASE
```

Важно

Вместо `/path/to/file.gz` укажите путь до файла с бэкапом

14. Проверить версию **PostgreSQL** командой:

```
echo "select * from version()" | rude sql
```

Пример:

```
rude@astra173:~$ sudo echo "select * from version()" | rude sql
                                                 version
-------------------------------------------------------------------------------------------------------------
 PostgreSQL 14.19 (Debian 1:14.19-1) on x86_64-pc-linux-gnu, compiled by gcc (AstraLinux 8.3.0-6+b1) 8.3.0, 64-bit
(1 строка)

rude@astra173:~$
```

Важно

Если в выводе отображается версия 14, то сервер **RuDesktop** работает на новой версии PostgreSQL

15. Зайти в веб-интерфейс сервера **RuDesktop** в браузере и убедиться, что:
    - Веб-интерфейс открывается
    - Авторизация работает
    - Лицензия присутствует

- Прочие данные восстановились после restore

16. Обновить сервер **RuDesktop** до версии 2.9 любым удобным способом по инструкции *Установка\обновление сервера*

РЕД ОС 7.3.x

В данном руководстве описывается пошаговый процесс обновления **PostgreSQL** с версии 12 до версии 16 на РЕД ОС 7.3.x для дальнейшего обновления сервера **RuDesktop** до версии `2.9`

Окружение стенда:

```
[root@template-redos-736 rude]# lsb_release -a
LSB Version:    :core-4.1-amd64:core-4.1-noarch
Distributor ID: RED SOFT
Description:    RED OS release MUROM (7.3.6) DESKTOP Standard Edition
Release:        7.3
Edition:        Standard
Codename:       MUROM
```

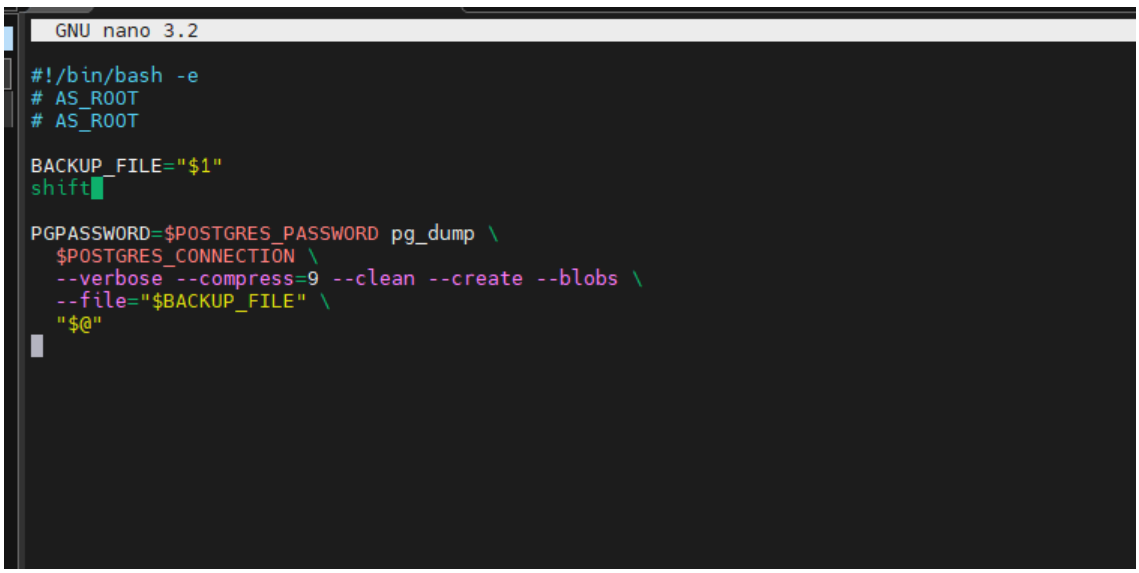
Сервер **RuDesktop** 2.8.1705

Обновление **PostgreSQL** с 12 до 16 версии:

1. Заменить содержимое файла по пути `/usr/share/rudesktop/bin/backup`:

```
#!/bin/bash -e
# AS_ROOT

BACKUP_FILE="$1"
shift

PGPASSWORD=$POSTGRES_PASSWORD pg_dump \
  $POSTGRES_CONNECTION \
  --verbose --compress=9 --clean --create --blobs \
  --file="$BACKUP_FILE" \
  "$@"
```

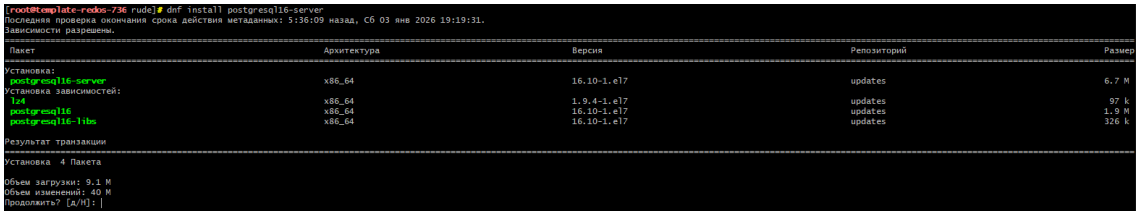
Пример:



2. Установить **PostgreSQL** 16 командой:

```
dnf install postgresql16-server
```

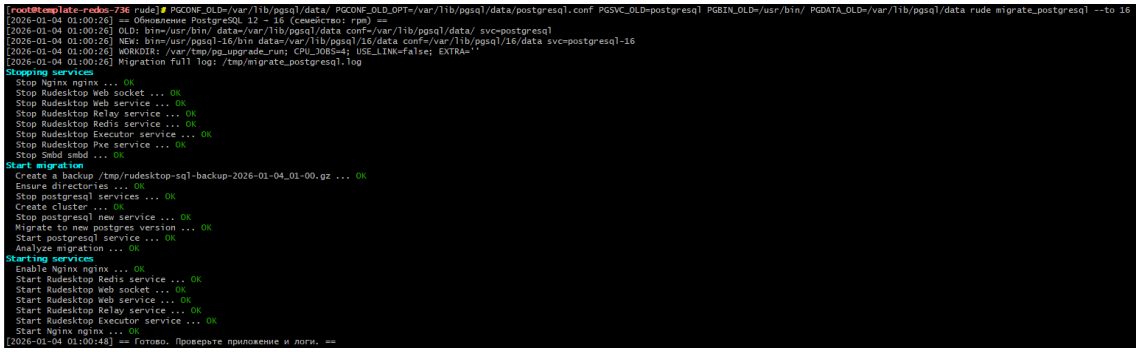
Пример:



3. Запустить процесс миграции с **PostgreSQL** 12 до 16 версии командой:

```
PGCONF_OLD=/var/lib/pgsql/data/ PGCONF_OLD_OPT=/
↪var/lib/pgsql/data/postgresql.conf PGSVC_OLD=postgresql␣
↪PGBIN_OLD=/usr/bin/ PGDATA_OLD=/var/lib/pgsql/data rude␣
↪migrate_postgresql --to 16
```

Пример:



4. Остановить службу **PostgreSQL** 12 версии командой:

```
systemctl stop postgresql.service
```

5. Отключить автоматический запуск службы **PostgreSQL** 12 версии командой:

```
systemctl disable postgresql.service
```

6. Добавить маску для службы **PostgreSQL** 12 версии командой:

```
systemctl mask postgresql.service
```

Важно

Необходимо для того, чтобы после перезапуска ПК, версия **PostgreSQL** 12 не запускалась автоматически

Данная команда делает следующее:

- Создаёт символическую ссылку от файла юнита `/etc/systemd/system/postgresql.service` на специальное устройство `/dev/null`. Это эффективно блокирует любой доступ к файлу юнита, предотвращая запуск службы
- Предотвращает автоматический и ручной запуск: служба не будет запускаться автоматически при загрузке системы, и попытки вручную запустить её с использованием `systemctl start` не будут успешными, пока она замаскирована
- Защищает от запуска через зависимости: другие службы или процессы, которые могли бы вызвать запуск `postgresql.service` через зависимости, также не смогут этого сделать

7. Внести изменения в конфигурационный файл по пути `/var/lib/pgsql/16/data/postgresql.conf` для **PostgreSQL** 16 версии:

   Найти строку:

   ```
   listen_addresses
   ```

   В начале строки удалить символ # и значение `localhost` изменить на *

   ```
   listen_addresses = '*'
   ```

   Найти строку:

   ```
   max_connections
   ```

   Заменить значение на 500

   ```
   max_connections = 500
   ```

8. Внести изменения в конфигурационный файл по пути `/var/lib/pgsql/16/data/pg_hba.conf` для **PostgreSQL** 16 версии:

   Найти строку:

   ```
   host    all             all             127.0.0.0/32    ␣
    ↪          md5
   ```

   Заменить на:

   ```
   host    all             all             0.0.0.0/0       ␣
    ↪          md5
   ```

9. Запустить службу **PostgreSQL** 16 версии и добавить ее в автозагрузку командой:

   ```
   systemctl enable postgresql-16.service --now
   ```

10. Проверить статус службы **PostgreSQL** 16 версии командой:

```
systemctl status postgresql-16.service
```

Подсказка

В статусе должно отображаться `active (running)`

11. Проверить версию **PostgreSQL** командой:

```
echo "select * from version()" | rude sql
```

Пример:



Важно

Если в выводе отображается версия 16, то сервер **RuDesktop** работает на новой версии **PostgreSQL**

12. Зайти в веб-интерфейс сервера **RuDesktop** в браузере и убедиться, что:
    - Веб-интерфейс открывается
    - Авторизация работает
    - Лицензия присутствует
    - И прочее
13. Обновить сервер **RuDesktop** до версии 2.9 любым удобным способом по инструкции *Установка\обновление сервера*

Ubuntu 20

В данном руководстве описывается пошаговый процесс обновления операционной системы Ubuntu с версии 20.04 до версии 22.04, а также обновление **PostgreSQL** с версии 12 до версии 14 для дальнейшего обновления сервера **RuDesktop** до версии `2.9`

Обновление с 20 до 22 Ubuntu

1. Обновить текущие пакеты в системе

   Откройте терминал и выполните команды для обновления всех пакетов в вашей текущей системе:

   ```
   sudo apt update
   sudo apt upgrade
   sudo apt dist-upgrade
   ```

2. Запустить обновление ОС

   Выполните следующую команду для запуска процесса обновления ОС:

```
sudo do-release-upgrade
```

Важно

После обновления Ubuntu с версии 20.04 до 22.04 по умолчанию будет установлена новая версия **PostgreSQL 14**. Поэтому необходимо выполнить миграцию на эту версию

3. Просмотр доступных кластеров

   Чтобы просмотреть доступные кластеры **PostgreSQL**, выполните следующую команду:

   ```
   pg_lsclusters
   ```

   Подсказка

   Если в списке присутствует кластер **PostgreSQL** версии 14, необходимо его остановить следующей командой:

   ```
   sudo pg_dropcluster 14 main --stop
   ```

   После этого необходимо запустить кластер версии 12 следующей командой:

   ```
   systemctl start postgresql@12-main
   ```

4. Запустить процесс миграции

   ```
   rude migrate_postgresql --to 14
   ```

5. Проверка работы сервера на новой версии PostgreSQL

   Чтобы убедиться, что сервер работает на новой версии **PostgreSQL**, выполните следующую команду:

   ```
   echo "select * from version()" | rude sql
   ```

   В ответ вы получите информацию о версии PostgreSQL, например:

   ```
   PostgreSQL 14.19 (Ubuntu 14.19-0ubuntu0.22.04.1) on␣
   ↪x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 11.
   ↪4.0-1ubuntu1~22.04.2) 11.4.0, 64-bit
   ```

6. Если вы видите, что **PostgreSQL** работает на версии 14, это означает, что миграция прошла успешно, и вы можете перейти к обновлению сервера до версии 2.9 любым удобным способом по инструкции *Установка\обновление сервера*

ping

Проверка доступности удалённого сервера **RuDesktop** или моста

Примечание

Команда использует встроенный в **RuDesktop** клиент `ping`, который проверяет именно протокол **RuDesktop** (а не ICMP). Полезно для диагностики связности с другим сервером или мостом

Зачем нужна

Команда отвечает на вопрос «работает ли узел RuDesktop по адресу X», а не «отвечает ли хост на сетевом уровне». В отличие от системного ICMP-ping, проверяет именно протокол **RuDesktop**: даже если хост отвечает на пакеты, его служба **RuDesktop** может быть недоступна или ответить ошибкой

Типичные случаи применения:

- диагностика подключения нового моста к центральному серверу — проверить, что протокольное рукопожатие проходит
- разбор инцидента «клиенты не подключаются к серверу» — отделить сетевые проблемы от проблем со службой
- проверка доступности альтернативного сервера, прописанного в настройках клиента
- мониторинг — добавить в скрипт регулярную проверку и алерт при недоступности

Синтаксис

```
rude ping [АДРЕС_СЕРВЕРА]
```

Пример

Чтобы проверить, доступен ли удалённый сервер или мост, введите следующее:

```
rude ping 192.168.10.1
```

После выполнения команды, если удалённый сервер доступен, будет отображено время отклика

prof

Отображение текущих SQL-запросов сервера к базе данных

Примечание

Команда выводит активные запросы PostgreSQL, выполняемые от пользователя `rudesktop`, с PID и временем работы. Полезна при поиске долгих запросов и анализе нагрузки

Зачем нужна

Команда — встроенный профилировщик, показывающий, что именно сервер делает с базой прямо сейчас: какие запросы выполняются, как давно, и при необходимости — план их выполнения. Это первый инструмент при подозрении на «медленный сервер»: позволяет увидеть тяжёлые/длинные SQL-запросы, не подключаясь напрямую к PostgreSQL

Типичные случаи применения:

- веб-интерфейс «тормозит» — посмотреть, какие запросы выполняются дольше остальных
- разбор инцидента «сервер упёрся в БД» — найти зависшие транзакции, чтобы прибить их по PID
- оптимизация: `--explain` показывает план запроса, по которому можно понять, нужен ли индекс
- регулярный снимок активности БД для анализа нагрузки в часы пик

Важно

Перед первым использованием выполните `rude prof init` — без этого длинные запросы будут обрезаться

Синтаксис

```
rude prof
rude prof --explain
rude prof init [BUFSIZE]
```

Параметры

Параметр	Описание
--explain	Дополнительно вывести план выполнения каждого запроса (EXPLAIN ANALYZE)

продолжается на следующей странице

Таблица 14 – продолжение с предыдущей страницы

Параметр	Описание
init [BUFSIZE]	Подкоманда: установить `track_activity_query_size` в конфиге PostgreSQL 13 и перезапустить службу. По умолчанию `BUFSIZE=65535`

Важно

Подкоманда `init` изменяет `track_activity_query_size` в `/etc/postgresql/13/main/postgresql.conf` и перезапускает PostgreSQL — без неё длинные запросы могут отображаться обрезанными. По умолчанию `BUFSIZE=65535`

Пример

1. Чтобы увидеть текущие запросы к базе данных, введите следующее:

```
rude prof
```

После выполнения команды, если в данный момент выполняются запросы, в выводе отобразятся PID, время и текст запроса:

```
PID: 2783750 TIME: 00:00:00.172882

UPDATE "peers_server" SET "facts" = '{"paths": [],
 ↪"monitors":
[{"week": 42, "year": 2014, "resolution": "1280x800",
 ↪"manufacturer": "RHT", ...}], ...
```

2. Чтобы получить план выполнения запросов (`EXPLAIN ANALYZE`), введите следующее:

```
rude prof --explain
```

После выполнения команды для каждого запроса дополнительно будет выведен план выполнения:

```
PID: 2796472 TIME: -00:00:00.001071

INSERT INTO inventory_assethistory (...)
...


 ↪                QUERY PLAN
-----------------------------------------------------------
 ↪-----------------------------------------------------------
 ↪-----------------------------------------
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
Insert on inventory_assethistory  (cost=19.24..19.26␣
↪rows=1 width=1080) (actual time=0.102..0.102 rows=0␣
↪loops=1)
...
Planning Time: 0.775 ms
Execution Time: 0.210 ms
```

3. Чтобы инициализировать буфер для отображения полных текстов запросов (выполняется один раз):

```
rude prof init
```

Чтобы задать другой размер буфера (например, 1 МБ):

```
rude prof init 1048576
```

reconnect

Сброс сертификата устройства в БД для повторного получения от клиента

Подсказка

Если при выполнении политик появляется ошибка `Wrong password`, это означает, что мастер-пароль на сервере и на устройстве не совпадают. Команда обнуляет поле `certificate` в БД — клиент при следующем пинге отправит актуальные сертификат и мастер-пароль на сервер

Зачем нужна

Команда устраняет рассинхронизацию между сервером и устройством по паре «сертификат + мастер-пароль». Если эти данные на сервере устарели или повреждены, политики падают с ошибкой `Wrong password`, а удалённые подключения могут не проходить. `reconnect` обнуляет данные на стороне сервера — клиент при следующем пинге пришлёт актуальные значения, и связь восстановится

Типичные случаи применения:

- политики массово завершаются с `Wrong password` после миграции или восстановления БД из старого бэкапа
- на устройстве переустановили клиент или запустили regenerate-master-key, но запись на сервере осталась со старым паролем
- разовая «синхронизация» сертификата у одного проблемного устройства без сброса состояния на самом устройстве

Синтаксис

```
rude reconnect
rude reconnect [server_id]
```

Параметры

Параметр	Описание
[server_id]	Идентификатор устройства. Если не указан — сертификат сбрасывается у **всех** устройств

Пример

1. Чтобы сбросить сертификат у всех устройств, введите следующее:

   ```
   rude reconnect
   ```

   После выполнения команды все устройства, подключённые к серверу, при следующем пинге отправят актуальные сертификат и мастер-пароль

2. Чтобы сбросить сертификат у конкретного устройства, введите следующее:

   ```
   rude reconnect 123456789
   ```

   После выполнения команды указанное устройство при следующем пинге отправит актуальные сертификат и мастер-пароль на сервер

reinstall

Переустановка сервера: сброс конфигурации и повторный запуск установки

Зачем нужна

Команда — фактически «*install* с нуля»: удаляет старые конфигурационные файлы и центр сертификации (CA), затем заново разворачивает сервер. После этого сервер получает свежий CA и новые сертификаты — все ранее зарегистрированные клиенты больше не доверяют новому серверу и должны подключиться заново

Типичные случаи применения:

- развёртывание нового сервера на месте старого (старая инсталляция остаётся, но «теряется» — нужно вручную перерегистрировать клиентов)
- восстановление сервера после повреждения конфигов и сертификатов, когда привычные команды не помогают

- смена IP/домена сервера с полной перевыпуском CA вместо точечной правки конфигов

Важно

Команда **деструктивна**: уничтожает текущую конфигурацию и CA. Перед запуском обязательно сделайте *резервную копию* базы и сохраните копию каталога `/var/lib/rudesktop/ca/` — иначе восстановление прежнего состояния станет невозможно

Синтаксис

```
rude reinstall [DOMAIN:PORT] [IP:PORT] ...
```

Важно

Команда выполняет следующие операции:

1. **Удаляет** `/etc/default/rudesktop`, `/etc/rudesktop/`, конфиги nginx (`sites-available/rudesktop`, `sites-enabled/rudesktop`)
2. **Удаляет** корневой сертификат CA (`/var/lib/rudesktop/ca/CA.*`, `*.cfg`)
3. Запускает `rude install` с переданными аргументами

После переустановки сервер использует новый CA — все ранее зарегистрированные клиенты потеряют доверие к серверу и потребуют переподключения

Подсказка

Если используются самоподписные сертификаты, указывайте **доменное имя**, а не IP-адрес — сертификат будет выпущен по имени

Пример

Чтобы переустановить сервер с IP-адресом, введите следующее:

```
rude reinstall 192.168.10.10
```

С доменным именем:

```
rude reinstall example.com
```

С доменным именем и резервным IP-адресом:

```
rude reinstall example.com 192.168.10.10
```

Подсказка

Указывать порт необязательно — по умолчанию используется 443

relay

Запуск нативного компонента сервера `rudesktop-server` с заданными аргументами

Примечание

Это служебная команда. В обычной работе компонент relay/rz запускается systemd-юнитом `rudesktop-relay.service`. Чаще всего администратор использует её только для получения версии сервера

Зачем нужна

Команда даёт прямой доступ к нативному бинарю `rudesktop-server` — основному компоненту, обслуживающему протокол **RuDesktop**. В повседневной работе он запускается systemd-юнитом `rudesktop-relay.service`; обращаться к нему через `rude relay` стоит для получения точной версии или передачи диагностических флагов

Типичные случаи применения:

- быстрое получение точной версии сервера для отчёта в техподдержку (`rude relay --version`)
- передача служебных флагов, которые поддерживает только нативный бинарь (с осторожностью)
- разовая диагностика поведения компонента вне контекста запуска через systemd

Синтаксис

```
rude relay --version
rude relay [другие_аргументы]
```

Параметры

Параметр	Описание
--version	Вывести версию сервера и завершить работу
[другие_аргументы]	Дополнительные флаги передаются напрямую в `rudesktop-server`. Полный список зависит от версии сервера

Пример

Чтобы получить версию сервера, введите следующее:

```
rude relay --version
```

После выполнения команды в выводе отобразится:

```
rudesktop-server 2.9.406-15824
```

restart

Перезапуск служб сервера

Зачем нужна

Команда последовательно останавливает и заново запускает службы сервера **RuDesktop** в правильном порядке (от nginx и веб-службы до relay/executor/pxe). Без параметров перезапускает весь набор; можно ограничиться одной службой по имени

Типичные случаи применения:

- применение изменений в конфигурации сервера, которые требуют перезапуска
- восстановление работы после сбоя одной из служб без перезагрузки ОС
- регламентный перезапуск после обновления **RuDesktop** или системных пакетов
- точечный перезапуск отдельной службы (например, только `rudesktop-relay.service`), не затрагивая остальные

Синтаксис

```
rude restart
rude restart [имя_службы.service|.socket]
rude restart executor
```

Примечание

Команда последовательно вызывает `rude stop` и `rude start` с теми же аргументами. Без параметров перезапускаются все службы согласно режиму установки

Пример

Чтобы перезапустить все службы сервера, введите следующее:

```
rude restart
```

После выполнения команды в выводе отобразится следующая информация:

```
Stopping services
  Stopping nginx ...              OK
  Stopping web socket ...         OK
  Stopping web service ...        OK
  Stopping relay ...              OK
  Stopping ansible processes ... OK
  Stopping executor ...           OK
  Stopping pxe ...                OK
  Stopping smbd ...               OK
Starting services
  Start web socket ...            OK
  Start web service ...           OK
  Start relay ...                 OK
  Start executor ...              OK
  Start smbd ...                  OK
  Enable nginx ...                OK
  Start nginx ...                 OK
```

Чтобы перезапустить только одну службу:

```
rude restart rudesktop-relay.service
```

restore

Восстановление базы данных сервера из резервной копии

Зачем нужна

Команда полностью замещает текущую БД сервера содержимым ранее сохранённого *backup*. После восстановления возвращаются все учётные записи, права, политики, журналы аудита и инвентаризация на момент создания дампа

Типичные случаи применения:

- восстановление после сбоя БД, ошибочного массового удаления или повреждения данных
- откат после неудачного обновления сервера или ошибочной массовой операции
- перенос сервера на другую машину при миграции
- развёртывание тестовой среды из дампа продакшена для расследования инцидента

Важно

Восстановление **деструктивно**: текущая база удаляется. Перед запуском обязательно сделайте *свежий backup* текущего состояния — на случай отката

Синтаксис

```
rude restore /path/to/file.gz
```

Параметры

- путь к файлу — обязательный параметр. Указывайте полный путь к файлу резервной копии в формате `.gz`, созданному командой `rude backup`

Важно

Восстановление — деструктивная операция:

- Сервер останавливается на время выполнения
- Существующая база данных удаляется и пересоздаётся
- После восстановления сервер автоматически запускается заново

Примечание

Если дамп снят на **Astra Linux Special Edition** сборкой PostgreSQL с поддержкой МРД, а восстанавливается на обычном PostgreSQL, в выводе появятся ошибки `нераспознанный параметр "macs"` и `ошибка синтаксиса (примерное положение: "MAC")`, а часть таблиц не будет создана. Команда `restore` мандатные метки не вырезает — дамп нужно создать заново с аргументами `--no-security-labels --disable-mac`, см. *backup*

Пример

Чтобы восстановить базу данных сервера из резервной копии, введите следующее:

```
rude restore /home/rude/backup.gz
```

После выполнения команды текущая база будет заменена на содержимое дампа, и сервер запустится заново

Подсказка

Подробнее о резервном копировании и восстановлении см. на странице *Резервное копирование*

setup_server

Установка сервера в качестве рандеву (rendezvous) для удалённого доступа

Важно

Служебная команда. Применяется автоматически при *установке сервера* и при настройке *точек распространения*. В большинстве случаев администратору не требуется запускать её вручную

Зачем нужна

Команда задаёт текущему серверу роль **rendezvous** в инфраструктуре **RuDesktop** — точки, через которую клиенты находят друг друга и устанавливают подключения. Запускается автоматически в составе *install* и при настройке точек распространения; вручную нужна, когда конфигурация рандеву рассинхронизировалась или была повреждена

Типичные случаи применения:

- ручная настройка rendezvous, если установщик не отработал эту часть до конца
- перенастройка домена/IP/порта rendezvous на действующем сервере без полной переустановки
- разделение ролей: задать рандеву без обновления списка моста (`--skip-relay`) при тонкой настройке инфраструктуры
- восстановление конфигурации после ручных правок или повреждений в БД

Синтаксис

```
rude setup_server [--verbose] [--skip-relay] [domain]
```

Параметры

Параметр	Описание
--verbose	Подробный вывод (включает уровень логирования `debug` для библиотеки соединения)
--skip-relay	Не записывать указанный хост как активный relay в БД (только настроить локальное подключение к рандеву)
domain	Адрес рандеву-сервера в формате `host` или `host:port` (обязательный)

Примечание

Аргумент `domain` принимает значение в формате `host` или `host:port`. По умолчанию (без `--skip-relay`) команда также записывает указанный хост как активный relay в БД

Пример

```
rude setup_server 127.0.0.1
Set relay to ... 127.0.0.1
```

С указанием порта:

```
rude setup_server example.com:8443
```

Без обновления списка relay:

```
rude setup_server --skip-relay 127.0.0.1
```

start

Запуск служб сервера

Зачем нужна

Команда запускает службы сервера **RuDesktop** в правильном порядке зависимостей. Без аргумента поднимается весь набор согласно режиму установки; с именем службы — только она. Используется после плановой остановки или при первоначальном включении сервера

Типичные случаи применения:

- запуск сервера после плановой остановки (обновление, обслуживание)
- старт служб после первичной установки или развёртывания из бэкапа
- точечный подъём отдельной службы (например, `rudesktop-relay.service`), которая остановлена при работающем остальном сервере
- восстановление работы сервера в скрипте автоматизации

Синтаксис

```
rude start
rude start [имя_службы.service|.socket]
rude start executor
```

Примечание

Без аргумента команда запускает полный набор служб. Конкретный набор зависит от режима установки (`INSTALL_MODE` в `/etc/default/rudesktop`):

- **full** (по умолчанию) — Redis, web, relay, executor, nginx, PXE и SMB (если включены)
- **relay** — только relay и nginx
- **executor** — executor, web, nginx (без relay)

Примечание

Службы `rudesktop-pxe.service` и `smbd` нужны только для *установки ОС по сети*, поэтому в режимах **full** и **executor** команда приводит их состояние в соответствие с наличием опубликованных образов:

- есть опубликованные образы — службы включаются в автозагрузку и запускаются
- опубликованных образов нет — включённые ранее службы отключаются из автозагрузки и останавливаются

Учитываются образы, опубликованные именно на этом сервере: в режиме **executor** — на самом раннере, в режиме **full** — на основном сервере. В режиме **relay** эти службы не используются, и команда их не трогает

Параметры

Параметр	Описание
[имя_службы.service|.socket]	Запустить только указанную системную службу — нужно передать имя с суффиксом `.service` или `.socket` (например, `rudesktop-relay.service`)
executor	Запустить только службу `rudesktop-executor.service`

Пример

Чтобы запустить все службы сервера, введите следующее:

```
rude start
```

После выполнения команды в выводе отобразится следующая информация:

```
Starting services
  Start web socket ...          OK
  Start web service ...         OK
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  Start relay ...                 OK
  Start executor ...              OK
  Start smbd ...                  OK
  Enable nginx ...                OK
  Start nginx ...                 OK
```

Чтобы запустить только одну службу, например, relay:

```
rude start rudesktop-relay.service
```

status

Получение информации о статусах служб сервера

Зачем нужна

Команда показывает состояние всех служб сервера **RuDesktop** в одной таблице: активны ли они сейчас, включён ли автозапуск и время последнего изменения. Состав служб зависит от режима установки. Альтернатива — запускать `systemctl status` для каждой службы отдельно

Типичные случаи применения:

- быстрая проверка после установки/обновления, что все нужные службы поднялись
- разбор инцидента «сервер не отвечает» — увидеть, какая именно служба упала
- скриптовый мониторинг — разобрать вывод и завести алерт при неактивных службах
- сверка после *restart* или *start*, что все службы вернулись в строй

Синтаксис

```
rude status
```

Примечание

Состав отображаемых служб зависит от режима установки (`INSTALL_MODE` в `/etc/default/rudesktop`):

- **full** (по умолчанию) — Redis, web, relay, executor, PXE, SMB, nginx и текущая служба PostgreSQL
- **relay** — relay и nginx
- **executor** — executor, web и nginx

Пример

Чтобы получить информацию о статусах служб сервера, введите следующее:

```
rude status
```

После выполнения команды в выводе отобразится следующая информация:

```
Service (Description)                                                  |␣
↪Active  | Enabled | Since
------------------------------------------------------------------------
↪---------------------------------------
rudesktop-relay.service (RuDesktop Relay)                              |␣
↪active  | enabled | Thu 2025-05-15 14:29:48 +07
rudesktop-executor.service (RuDesktop executor service)                |␣
↪active  | enabled | Thu 2025-05-15 14:29:36 +07
rudesktop-web.service (RuDesktop admin panel)                          |␣
↪active  | enabled | Thu 2025-05-15 14:29:35 +07
rudesktop-web.socket (RuDesktop admin socket)                          |␣
↪active  | enabled | Thu 2025-05-15 14:29:35 +07
```

Активные службы выводятся зелёным цветом, неактивные — красным

stop

Остановка служб сервера

Зачем нужна

Команда корректно останавливает службы сервера **RuDesktop** в правильном порядке: сначала nginx и веб-служба, затем relay/executor и фоновые процессы. После остановки сервер недоступен по сети и не выполняет UEM-задачи

Типичные случаи применения:

- плановое обслуживание сервера (миграция БД, переезд на другой хост, физическое перемещение)
- остановка перед *backup* или *restore*, чтобы избежать конкурентной нагрузки
- точечная остановка одной службы для отладки, не выключая остальной сервер
- аварийное завершение работы сервера

Синтаксис

```
rude stop
rude stop [имя_службы.service|.socket]
rude stop executor
```

Примечание

Без аргумента команда останавливает полный набор служб согласно режиму установки (`INSTALL_MODE` в `/etc/default/rudesktop`):

- **full** (по умолчанию) — Redis, web, relay, executor, nginx, PXE и SMB
- **relay** — relay и nginx
- **executor** — executor, web, nginx, PXE и SMB

Примечание

В режиме **executor** службы `rudesktop-pxe.service` и `smbd` останавливаются вместе с остальными: раннер может раздавать образы ОС по сети, и при остановке эта раздача тоже должна прекратиться

Параметры

Параметр	Описание
[имя_службы.service|.socket]	Остановить только указанную системную службу
executor	Остановить только службу `rudesktop-executor.service`

Пример

Чтобы остановить все службы сервера, введите следующее:

```
rude stop
```

После выполнения команды в выводе отобразится следующая информация:

```
Stopping services
  Stopping nginx ...              OK
  Stopping web socket ...         OK
  Stopping web service ...        OK
  Stopping relay ...              OK
  Stopping ansible processes ... OK
  Stopping executor ...           OK
  Stopping pxe ...                OK
  Stopping smbd ...               OK
```

Чтобы остановить только одну службу, например, executor:

```
rude stop rudesktop-executor.service
```

Действия с сервером — CLI-команды для управления самим сервером **RuDesktop**: установка/переустановка, запуск/остановка/перезапуск служб,

диагностика, миграция базы, управление лицензией, генерация сертификатов и обслуживание моста

Команда	Описание
backup	Создание резервной копии базы данных сервера
collectstatic	Сбор статических файлов в одном каталоге
clean_video_records	Удаление устаревших видеозаписей сессий
constance	Получение и установка параметров конфигурации сервера
delete	Очистка устройств по дате последней активности на сервере
diag	Сбор информации для диагностики сервера
gencert	Генерация сертификата для моста
install	Первичная установка сервера и его служб
license	Получение информации о лицензии
maintain	Регламентное обслуживание сервера: ротация логов и удаление устаревших архивов
migrate_postgresql	Миграция БД на другую версию PostgreSQL
ping	Проверка доступности удалённого сервера
prof	Отображение запросов к базе данных
reconnect	Получение сертификата и мастер-пароля с устройства
reinstall	Переустановка сервера со сбросом конфигурации и сертификатов CA (**деструктивно**)
relay	Получение информации о версии сервера
restart	Перезапуск сервера
restore	Восстановление базы данных сервера из резервной копии (**деструктивно**)
setup_server	Установка сервера в качестве рандеву для подключения удалённого доступа
start	Запуск сервера
status	Получение информации о статусах служб сервера
stop	Остановка сервера

1.6.5 Действия с учетными записями

axes_list_attempts

Список неуспешных попыток авторизации

Зачем нужна

Команда показывает текущие неуспешные попытки входа в веб-интерфейс **RuDesktop** (django-axes): IP-адрес, имя пользователя и счётчик неудач. По достижении порога IP/пользователь блокируется — список помогает понять, кто близок к блокировке или уже заблокирован

Типичные случаи применения:

- разбор обращения от пользователя «не могу войти, забыл пароль» — посмотреть, не заблокирован ли его IP
- мониторинг подозрительной активности (брутфорс) — частые попытки с одного IP с разными логинами
- быстрая проверка состояния перед ручным сбросом блокировки через *axes_reset_ip* или *axes_reset_username*

Синтаксис

```
rude axes_list_attempts
```

Пример

Чтобы вывести список текущих неуспешных попыток входа, введите следующее:

```
rude axes_list_attempts
```

Для каждой записи в выводе отобразятся IP-адрес, имя пользователя и количество неуспешных попыток с момента первого срабатывания:

```
192.168.0.10    admin    3
10.1.0.7        rude     5
```

axes_reset_failure_logs

Удаление старых записей о неуспешных попытках входа (`AccessAttempt`)

Зачем нужна

Команда чистит историю неуспешных попыток в таблице `AccessAttempt`. В отличие от *axes_reset*, который снимает все блокировки разом, эта команда удаляет именно **записи в журнале** — нужна для контроля размера таблицы и соблюдения политики хранения, не отзывая текущие блокировки

Типичные случаи применения:

- регулярная очистка через cron, чтобы таблица неуспешных попыток не разрасталась бесконечно
- соблюдение политики хранения данных безопасности (например, хранить попытки только за последние N дней)
- освобождение места перед бэкапом или миграцией БД

Синтаксис

```
rude axes_reset_failure_logs [--age days]
```

Параметры

Параметр	Описание
--age	Срок хранения записей в днях (по умолчанию 30). Удаляются записи старше указанного срока

Примечание

Команда чистит таблицу `AccessAttempt` (только записи о неуспешных попытках). Для удаления полного журнала доступа используйте *axes_reset_logs*

Пример

Чтобы удалить записи о неуспешных попытках старше 30 дней (значение по умолчанию):

```
rude axes_reset_failure_logs
```

Чтобы изменить срок, например, до 7 дней:

```
rude axes_reset_failure_logs --age 7
```

После выполнения команды отобразится количество удалённых записей:

```
24 logs removed.
```

axes_reset_ip_username

Сброс всех неуспешных попыток входа и блокировок для пары «IP-адрес + имя пользователя»

Зачем нужна

Команда снимает блокировку только для конкретной пары «IP + логин». В отличие от *axes_reset_ip* и *axes_reset_username*, не разблокирует ни весь IP, ни весь логин — только точное пересечение. Используется, когда блокировка применяется по комбинации (это управляется настройками django-axes)

Типичные случаи применения:

- пользователь работает с общего IP (терминальный сервер, общий выход NAT) и заблокирован только под своим логином — снять блокировку только для него, не трогая других пользователей с того же IP
- частая ситуация в виртуальных средах: несколько пользователей работают с одного RDP-сервера, нужно разблокировать одного, оставив историю остальных

Синтаксис

```
rude axes_reset_ip_username [ip] [username]
```

Параметры

Параметр	Описание
ip	IP-адрес для сброса
username	Имя пользователя для сброса неудачных попыток авторизации

Примечание

В отличие от `axes_reset_ip` и `axes_reset_username`, эта команда сбрасывает только записи, у которых **одновременно** совпадают IP-адрес и имя пользователя. Используется для точечной разблокировки

Пример

```
rude axes_reset_ip_username 10.1.0.7 admin
1 attempts removed.
```

После выполнения команды пользователь `admin` с IP-адреса `10.1.0.7` сможет снова авторизоваться в веб-интерфейсе **RuDesktop**

axes_reset_ip

Сброс блокировок и неуспешных попыток входа для одного или нескольких IP-адресов

Зачем нужна

Команда снимает блокировку конкретного IP-адреса (или нескольких сразу). После многократных неудачных попыток входа django-axes блокирует IP — пользователь с этого адреса не может авторизоваться даже с верными учётными данными. `axes_reset_ip` позволяет точечно разблокировать нужные адреса, не сбрасывая блокировки остальных

Типичные случаи применения:

- легитимный пользователь забыл пароль, перебирал варианты и заблокировал свой IP — нужно разблокировать его, не трогая остальные блокировки
- сотрудник сменил рабочее место или вернулся из командировки и его IP попал под блокировку из-за чужих попыток с того же адреса
- разблокировка адреса оператора после расследования и подтверждения, что попытки были ошибочными

Подсказка

Чтобы посмотреть текущие активные блокировки, используйте *axes_list_attempts*

Синтаксис

```
rude axes_reset_ip [IP1] [IP2] ...
```

Пример

Чтобы сбросить блокировку одного IP-адреса, введите следующее:

```
rude axes_reset_ip 192.168.0.1
```

Чтобы сбросить блокировки нескольких IP-адресов одной командой:

```
rude axes_reset_ip 192.168.0.1 10.1.0.7
```

После выполнения команды отобразится количество удалённых записей. Заблокированные пользователи смогут авторизоваться в веб-интерфейсе:

```
2 attempts removed.
```

axes_reset_logs

Удаление старых записей журнала доступа (`AccessLog`)

Зачем нужна

Команда чистит таблицу `AccessLog` — полный журнал событий входа (и успешных, и неуспешных). В отличие от *axes_reset_failure_logs*, удаляющей только неуспешные попытки, `axes_reset_logs` обрезает весь журнал входов

Типичные случаи применения:

- регулярная очистка журнала входов через cron, чтобы он не разрастался без контроля
- соблюдение политики хранения данных безопасности (например, хранить журнал входов только за нужный период)
- освобождение места перед бэкапом или миграцией БД

Синтаксис

```
rude axes_reset_logs [--age days]
```

Параметры

Параметр	Описание
--age	Срок хранения записей в днях (по умолчанию 30). Удаляются записи старше указанного срока

Примечание

Команда чистит таблицу `AccessLog` (полный журнал входов и попыток). Для удаления только записей с неуспешными попытками используйте *axes_reset_failure_logs*

Пример

Чтобы удалить записи журнала доступа старше 30 дней (значение по умолчанию):

```
rude axes_reset_logs
```

Чтобы изменить срок хранения, например, до 7 дней:

```
rude axes_reset_logs --age 7
```

После выполнения команды отобразится количество удалённых записей:

```
142 logs removed.
```

axes_reset_username

Сброс блокировок и неуспешных попыток входа для одного или нескольких пользователей

Зачем нужна

Команда снимает блокировку для конкретных пользователей — независимо от того, с каких IP-адресов были попытки. Удобно, когда блокировка применяется по логину (это управляется настройками django-axes), и требуется разблокировать конкретные учётные записи

Типичные случаи применения:

- пользователь забыл пароль и заблокировал свой аккаунт несколькими неверными попытками — нужно разблокировать
- массовая блокировка нескольких сотрудников из-за смены пароля — разблокировать всех одной командой со списком логинов
- помощь пользователю с мобильным IP, который меняется — *axes_reset_ip* не подходит, проще снять блокировку по логину

Синтаксис

```
rude axes_reset_username [username1] [username2] ...
```

Пример

Чтобы сбросить блокировку одного пользователя, введите следующее:

```
rude axes_reset_username rudesktop
```

Чтобы сбросить блокировки нескольких пользователей одной командой:

```
rude axes_reset_username admin rudesktop user1
```

После выполнения команды отобразится количество удалённых записей. Пользователи смогут авторизоваться в веб-интерфейсе:

```
3 attempts removed.
```

axes_reset

Сброс всех неуспешных попыток входа и блокировок

Зачем нужна

Команда снимает **все** активные блокировки django-axes за один шаг — пустеет вся таблица `AccessAttempt`, никто не остаётся заблокированным. Используется как «аварийная кнопка», когда нужно быстро вернуть всем пользователям доступ к веб-интерфейсу

Типичные случаи применения:

- массовая ошибка пользователей после смены политики паролей или внедрения новой системы аутентификации — все попадают под блокировку
- сбой почтового канала или 2FA, из-за которого пользователи не получали коды и упирались в блокировку
- сброс блокировок после тестовой проверки безопасности (нагрузочное тестирование, пентест)

Важно

Команда **снимает все блокировки одновременно**, в том числе те, что могли быть результатом реальной атаки. Перед запуском проверьте *axes_list_attempts* — нет ли среди заблокированных подозрительной активности

Синтаксис

```
rude axes_reset
```

Примечание

Команда удаляет все записи о неуспешных попытках входа без фильтрации — снимает блокировки со всех заблокированных IP-адресов и пользователей одновременно

Пример

Чтобы сбросить все блокировки и неуспешные попытки, введите следующее:

```
rude axes_reset
```

После выполнения команды отобразится количество удалённых записей:

```
5 attempts removed.
```

Если попыток нет — команда выведет `No attempts found.`

bad_auth_list

Список событий неуспешного входа и блокировок IP за указанный период

Зачем нужна

Команда выводит исторический срез событий безопасности из аудита (`LOGIN_ERROR` и `AUTH_BLOCK_IP`) за выбранное окно. В отличие от *axes_list_attempts*, который показывает только текущие активные попытки,

`bad_auth_list` берёт данные из журнала аудита — туда попадают все события за период

Типичные случаи применения:

- разбор инцидента: посмотреть, было ли давление на конкретные учётные записи в нужном временном окне
- регулярный аудит безопасности — выгрузить журнал неуспешных попыток за неделю/месяц для отчёта
- расследование жалобы пользователя «не мог войти позавчера» — найти соответствующее событие в журнале

Синтаксис

```
rude bad_auth_list [--days N]
```

Параметры

Параметр	Описание
--days	Период в днях для выборки событий (по умолчанию 7)

Примечание

Команда выводит события аудита с типами `LOGIN_ERROR` (неуспешный вход) и `AUTH_BLOCK_IP` (блокировка IP-адреса) за указанный период

Пример

Чтобы получить список за последние 7 дней (по умолчанию), введите следующее:

```
rude bad_auth_list
```

Чтобы изменить период, например, за последний день:

```
rude bad_auth_list --days 1
```

После выполнения команды в выводе отобразится:

```
time                username    IP          event_type
2025-10-14 12:08:31  rudesktop  127.0.0.1   LOGIN_ERROR
2025-10-14 13:35:01  test       127.0.0.1   AUTH_BLOCK_IP
```

Если за период событий нет — команда выведет `Logs not found.`

changepassword

Интерактивная смена пароля пользователя (стандартная команда Django)

Зачем нужна

Команда позволяет администратору сменить пароль любому пользователю с консоли — без отправки ссылок на email и без знания старого пароля. Стандартная команда Django, пароль вводится в скрытом режиме и в историю shell не попадает

Типичные случаи применения:

- пользователь забыл пароль и не настроил восстановление по email — администратор задаёт новый пароль вручную
- сброс пароля при служебной необходимости (увольнение, передача учётной записи)
- настройка тестовых или сервисных учётных записей при первичной установке

Подсказка

Для пользователя `admin` есть упрощённая команда *passwd*, не требующая ввода имени учётной записи

Синтаксис

```
rude changepassword [имя_пользователя]
```

Примечание

Пароль вводится в скрытом интерактивном режиме (не попадает в историю shell). Для смены пароля пользователя `admin` существует упрощённая команда *passwd*

Пример

Чтобы изменить пароль пользователя, введите следующее:

```
rude changepassword [имя_пользователя]

Changing password for user 'имя_пользователя'
Password: [ввести_новый_пароль]
Password (again): [повторить_новый_пароль]
Password changed successfully for user 'имя_пользователя'
```

После выполнения команды пароль будет успешно изменён на введённый

clean_otp

Удаление одноразовых паролей за указанный период

Зачем нужна

Команда удаляет устаревшие одноразовые пароли (OTP) из таблицы. У OTP очень короткий полезный срок жизни (минуты) — после использования или истечения времени они только занимают место в БД. Команда обычно вызывается из планового обслуживания *maintain*

Типичные случаи применения:

- регулярное обслуживание: команда уже включена в плановое выполнение *maintain*, отдельный запуск нужен только при ручном обслуживании
- разовая чистка таблицы OTP, если она существенно разрослась после периода интенсивной 2FA-нагрузки
- освобождение места перед бэкапом или миграцией БД

Синтаксис

```
rude clean_otp [minutes/hours/days/weeks] [amount]
```

Параметры

Параметр	Описание
{minutes/hours/days/weeks}	Единица измерения периода: `minutes` (минуты), `hours` (часы), `days` (дни), `weeks` (недели)
amount	Количество единиц периода (целое число)

Примечание

Команда удаляет записи OTP с `date_joined` в диапазоне «период назад → сейчас». Используется в составе планового обслуживания через `rude maintain` — у одноразовых паролей очень короткий полезный срок жизни (минуты), поэтому записи в этом диапазоне уже неактуальны и могут быть удалены без риска

Пример

Чтобы удалить одноразовые пароли за последние пять дней, введите следующее:

```
rude clean_otp days 5
```

После выполнения команды отобранные одноразовые пароли будут удалены из БД

createsuperuser

Создание пользователя с правами суперпользователя (стандартная команда Django)

Примечание

Суперпользователь имеет полные права на сервере **RuDesktop**. Для работы с REST API через токен достаточно обычной учётной записи с ограниченными правами — см. *Настройка доступа*

Зачем нужна

Команда создаёт *пользователя со статусом суперпользователя* напрямую через CLI. Это единственный способ завести первого администратора сразу после установки сервера, когда веб-интерфейс ещё недоступен. Также используется для аварийного восстановления, если все суперпользователи были удалены или заблокированы

Типичные случаи применения:

- первичная инициализация сервера сразу после установки — создать первую административную учётную запись
- восстановление доступа, если в результате ошибочных действий были удалены/деактивированы все суперпользователи
- создание дополнительной административной учётной записи для разделения ответственности между администраторами

Важно

Не выдавайте статус суперпользователя широкому кругу — для большинства задач достаточно *прав группы*

Синтаксис

```
rude createsuperuser
```

Пример

Чтобы создать пользователя с полными правами, введите следующее:

```
rude createsuperuser

Логин: [ввести_имя_пользователя]
Электронная почта: [ввести_email_пользователя]
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
Password: [ввести_пароль]
Password (again): [повторить_пароль]
Superuser created successfully
```

После выполнения команды пользователь с полными правами будет успешно создан

disable_mfa

Отключение методов 2FA для пользователя

Важно

Методы не удаляются, а лишь отключаются (поле `enabled` устанавливается в `False`). Их можно будет снова включить в профиле пользователя

Зачем нужна

Команда снимает у пользователя все настроенные методы двухфакторной аутентификации — доступ возвращается с обычным паролем без второго фактора. Используется в аварийных ситуациях: пользователь потерял доступ к 2FA-устройству и не может войти в веб-интерфейс самостоятельно

Типичные случаи применения:

- сотрудник потерял телефон с приложением-аутентификатором или больше не получает SMS — нужно вернуть ему доступ
- замена устройства 2FA: отключить старый метод, чтобы пользователь настроил новый
- разовый сброс 2FA при увольнении/смене ответственности — для дальнейшей передачи учётной записи
- скриптовая массовая операция с `-y` — без интерактивного подтверждения

Подсказка

Перед боевым запуском проверьте список ключей флагом `--dry-run` — он покажет, что будет отключено, без записи в БД

Синтаксис

```
rude disable_mfa [user] [--by username|id] [--dry-run] [-y|--yes]
```

Параметры

Параметр	Описание
user	Идентификатор пользователя — по умолчанию имя пользователя или числовой ID
--by	Явно указать тип идентификатора: `username` или `id`. Если не указан, числовое значение интерпретируется как ID, иначе — как имя пользователя
--dry-run	Показать список ключей и не вносить изменения в БД
-y / --yes	Не запрашивать подтверждение перед отключением

Пример

Чтобы отключить методы 2FA у пользователя `test`, введите следующее:

```
rude disable_mfa test
```

При выполнении команды потребуется подтвердить отключение метода(ов):

```
User: test (id=2)
Keys to disable: 1
- id=2, type=telegram, serial=None, enabled=True,␣
 ↪last_used=2025-10-31 09:01:47.611199+00:00
Proceed to set enabled=False for these keys? [y/N]: y
```

После подтверждения отобразится сообщение об успешном отключении:

```
Deactivated 1 key(s).
```

Чтобы пропустить запрос подтверждения (например, для скриптов), используйте флаг `-y`:

```
rude disable_mfa test -y
```

Чтобы только посмотреть, какие ключи будут отключены, без записи в БД, используйте `--dry-run`:

```
rude disable_mfa test --dry-run
```

Чтобы указать пользователя по числовому ID:

```
rude disable_mfa 42 --by id
```

После выполнения команды пользователь сможет авторизовываться в веб-интерфейсе сервера **RuDesktop** без необходимости использовать двухфакторную аутентификацию

normalize_phones

Приведение номеров телефонов всех пользователей к стандартному виду

Зачем нужна

Команда массово приводит номера телефонов учётных записей к каноничному виду `+7xxx...`. Без этого номера, введённые в разных форматах (`8xxx`, `+7 (xxx)`, `8-xxx` и т.п.), будут считаться разными — это мешает 2FA по SMS, поиску по номеру и подключению к мобильным устройствам по верифицированному номеру

Типичные случаи применения:

- после массового импорта пользователей из AD/LDAP, где номера хранятся в произвольном формате
- разовая чистка после нескольких лет работы сервера, когда форматы накопились
- подготовка к включению 2FA по SMS — нормализация снижает количество ошибок отправки
- настройка подключения к мобильным устройствам, когда сравнение идёт по номеру

Синтаксис

```
rude normalize_phones
```

Примечание

Команда проходит по всем пользователям с заполненным телефоном и приводит номер к каноничному виду (`+7xxx...`). Пользователи без телефона пропускаются. Ошибки нормализации логируются, но не прерывают выполнение

Пример

Чтобы привести номера телефонов у всех учётных записей к виду `+7xxx`, введите следующее:

```
rude normalize_phones
```

В стандартный вывод печатается строка для каждого обработанного пользователя с его именем и нормализованным номером

```
user1 +79161234567
user2 +79169876543
```

passwd

Смена пароля пользователя **«admin»**

Подсказка

Если пользователь **«admin»** не создан на сервере, после выполнения команды он будет создан, и ему будет присвоен введённый пароль

Зачем нужна

Упрощённая команда специально для пользователя `admin` — задаёт ему пароль одной командой без интерактивного диалога. Если `admin` ещё не существует, создаётся автоматически. Используется в скриптах развёртывания и аварийном восстановлении доступа

Типичные случаи применения:

- скрипт первичной настройки сервера: установить и сразу задать пароль `admin`
- автоматизация в Ansible/CI — нужно задать пароль строго неинтерактивно
- аварийное восстановление доступа, когда забыт пароль `admin`

Предупреждение

Пароль передаётся аргументом командной строки и попадает в историю shell и в список процессов. Для интерактивной смены, не оставляющей пароль в истории, используйте *changepassword*

Синтаксис

```
rude passwd [новый_пароль]
```

Пример

Чтобы заменить пароль у пользователя **«admin»**, введите следующее:

```
rude passwd 123456
```

После выполнения команды пароль пользователя **«admin»** будет успешно изменён на введённый и появится сообщение:

```
Password changed
```

Важно

Если не указать новый пароль, произойдёт ошибка с текстом `Specify password`

Предупреждение

Пароль в этой команде передаётся аргументом командной строки и попадает в историю shell и в список процессов. Для интерактивной смены пароля используйте *changepassword*

Действия с учетными записями — CLI-команды для управления локальными пользователями сервера: создание суперпользователя, смена пароля, сброс OTP/MFA, работа со списком неудачных попыток входа (Axes), нормализация номеров телефонов

Команда	Описание
axes_list_attempts	Формирование списка ошибочных попыток авторизации
axes_reset_failure_logs	Сброс неуспешных попыток доступа
axes_reset_ip_username	Сбросить все попытки доступа и блокировки для данного IP-адреса и имени пользователя
axes_reset_ip	Сброс блокировки IP-адреса
axes_reset_logs	Сброс неуспешных попыток входа для всех IP
axes_reset_username	Сброс блокировки пользователя
axes_reset	Сброс всех блокировок по IP-адресу
bad_auth_list	Получение списка заблокированных пользователей
changepassword	Смена пароля пользователя
clean_otp	Удаление старых одноразовых паролей
createsuperuser	Создание пользователя с полными правами
disable_mfa	Отключение методов 2FA для конкретного пользователя
normalize_phones	Приведение номера телефона к стандартному виду
passwd	Смена пароля пользователя **admin**

1.6.6 Действия с файлами

file

Управление файлами в репозиториях сервера

Подсказка

Файлы из репозиториев доступны на странице **«Файлы»** в веб-интерфейсе

Зачем нужна

Команда работает с файловыми *репозиториями* сервера из CLI: показывает список зарегистрированных файлов, регистрирует новые без копирования через веб-интерфейс и чистит «битые» записи и временные файлы. В отличие от загрузки через веб, форма `file add` принимает уже лежащий на диске файл и просто добавляет запись в базу — это удобно для крупных артефактов и серверной автоматизации

Типичные случаи применения:

- регистрация большого установочного пакета (несколько ГБ), который проще положить на сервер по SCP, чем загружать через браузер
- автоматизация: скрипт сборки артефактов копирует файл на сервер и одной командой регистрирует его в репозитории **RuDesktop**
- регулярная очистка `file cleanup` через cron — удаление записей о файлах, которые были вручную удалены с диска, и подчистка временного каталога
- инвентаризация содержимого репозитория `file list` — просмотр id и путей всех зарегистрированных файлов

Синтаксис

```
rude file list
rude file add [путь_до_файла]
rude file cleanup [--quiet]
```

Параметры

Параметр	Описание
list	Вывести список зарегистрированных файлов с их ID оригинальным именем и путём
add [путь_до_файла]	Зарегистрировать существующий файл сервера в репозитории (без перемещения файла)

продолжается на следующей странице

Таблица 21 – продолжение с предыдущей страницы

Параметр	Описание
cleanup	Удалить «битые» записи (файлов нет на диске) и очистить временный каталог от старых файлов
--quiet	Не выводить служебные сообщения в консоль (используется только с `cleanup`)

Пример

Получение списка всех файлов

Чтобы получить список всех файлов, введите следующее:

```
rude file list
```

После выполнения команды в выводе отобразится список файлов:

```
ID  Имя файла    Путь до файла
1   [имя_файла]  /var/lib/rudesktop/media/files/[Дата]/[имя_файла]
2   [имя_файла]  /var/lib/rudesktop/media/files/[Дата]/[имя_файла]
```

Добавление файла

Чтобы добавить файл из файловой системы сервера в репозиторий, введите следующее:

```
rude file add [путь_до_файла]
```

Команда регистрирует файл в БД (создаёт запись `upload.File`) — оригинальный файл при этом не перемещается. Если по указанному пути файла нет или он недоступен на чтение, команда завершится ошибкой `File ... is not readable`

Очистка неиспользуемых файлов

Чтобы удалить устаревшие файлы, введите следующее:

```
rude file cleanup
```

Команда выполняет две операции:

1. Проходит по всем записям в БД и удаляет те, для которых файла на диске больше не существует (запись считается «битой»)
2. Очищает временный каталог `MEDIA_TMP_DIR` от файлов старше `MAX_TEMP_FILE_AGE` секунд и удаляет опустевшие подкаталоги

Чтобы запустить очистку без вывода в консоль, добавьте флаг `--quiet`:

```
rude file cleanup --quiet
```

Действия с файлами — CLI-команды для работы с файлами, хранящимися в репозиториях сервера

Команда	Описание
file	Управление файлами

1.6.7 Действия с фактами и отчетами

report generate

Генерация отчёта по шаблону

Зачем нужна

Команда запускает генерацию *отчёта* по существующему *шаблону* из консоли — без открытия веб-интерфейса. Поддерживается выбор формата (PDF/XLSX), фильтрация по конкретным устройствам, указание момента «состояние на дату» и доставка готового файла на почту

Типичные случаи применения:

- автоматическая генерация регулярных отчётов из cron — например, еженедельной выгрузки на email руководителя
- массовая выгрузка отчётов по расписанию без участия оператора
- разовая генерация отчёта на конкретную дату прошлого периода (через `--start_timestamp`) — для аудита или согласования
- получение отчёта по ограниченному списку устройств без создания нового шаблона в веб-интерфейсе

Синтаксис

```
rude report generate [id_шаблона] [--type pdf|xlsx] [--user␣
↪id_пользователя] [--servers id1,id2,...] [--start_timestamp␣
↪datetime]
```

Параметры

Параметр	Описание
id_шаблона	ID шаблона отчёта в системе (обязательный)
--type	Формат отчёта: `pdf` или `xlsx` (по умолчанию `pdf`)

продолжается на следующей странице

Таблица 23 – продолжение с предыдущей страницы

Параметр	Описание
--user	ID пользователя, которому отправляется уведомление о готовности отчёта (необязательно)
--servers	Список ID устройств через запятую — отчёт будет ограничен только этими устройствами (необязательно)
--start_timestamp	Дата и время создания отчёта в формате ISO 8601 (необязательно; по умолчанию используется текущее время)

Примечание

Поддерживаются только форматы `pdf` (по умолчанию) и `xlsx`. Любой другой формат завершит команду ошибкой `Не распознан формат отчета`

Пример

Генерация PDF без отправки пользователю:

```
rude report generate [id_шаблона] --type pdf
```

Генерация XLSX без отправки пользователю:

```
rude report generate [id_шаблона] --type xlsx
```

Подсказка

После выполнения команды готовые отчёты будут доступны для загрузки на странице **«Готовые отчёты»** в веб-интерфейсе

Генерация PDF с отправкой пользователю:

```
rude report generate [id_шаблона] --user [id_пользователя] --type␣
↪pdf
```

Генерация XLSX с отправкой пользователю:

```
rude report generate [id_шаблона] --user [id_пользователя] --type␣
↪xlsx
```

Генерация отчёта только по выбранным устройствам и с указанием времени создания:

```
rude report generate [id_шаблона] --type pdf --servers 12,15,18 --
↪start_timestamp "2025-04-01 09:00:00"
```

Подсказка

После выполнения команды с параметром `--user` готовый отчёт будет доступен для загрузки в веб-интерфейсе и пользователю будет отправлено письмо

update_inventory

Обновление инвентарных данных всех устройств

Зачем нужна

Команда пересчитывает инвентарные поля (оборудование, ПО, пользователи, ОС) для всех устройств в базе из уже собранных Ansible-фактов. В отличие от запуска политики **Инвентаризация**, не обращается к самим устройствам — переразбирает уже сохранённые данные

Типичные случаи применения:

- после обновления сервера, в котором изменилась логика разбора фактов в *Инвентаризации*
- после массового импорта устройств с уже известными фактами
- восстановление сводной таблицы инвентаризации, если в ней появились пробелы или некорректные значения

Синтаксис

```
rude update_inventory
```

Примечание

Команда проходит по всем устройствам в БД и пересчитывает инвентарную информацию (оборудование, ПО, пользователи, ОС). Используется при обновлении логики обработки фактов или после массового импорта устройств

Пример

Чтобы обновить поля для раздела **«Инвентаризация»**, введите следующее:

```
rude update_inventory
```

Действия с фактами и отчетами — CLI-команды для построения отчётов из шаблонов и обновления данных инвентаризации устройств

Команда	Описание
report	Генерация отчетов

продолжается на следующей странице

Таблица 24 – продолжение с предыдущей страницы

Команда	Описание
update_inventory	Обновление полей для раздела «Инвентаризация»

1.6.8 Действия с API

token create

Создание токена доступа к API для пользователя

Зачем нужна

Команда выпускает токен для доступа к административному API сервера от имени конкретного пользователя. Только так токены и создаются — в веб-интерфейсе соответствующего пункта нет, выпуск ключей сознательно вынесен в CLI и доступен только тому, у кого есть SSH-доступ к серверу

Типичные случаи применения:

- интеграция с внешней системой (CMDB, мониторинг, ITSM), которой нужно вызывать API **RuDesktop** — токен прописывается в её конфигурации
- скрипты автоматизации администратора, использующие API без интерактивного входа
- выпуск технического токена для CI/CD-пайплайна, который выкатывает политики или собирает инвентаризацию

Важно

Значение токена выводится **один раз** при создании — посмотреть его повторно нельзя. При утере отзовите токен через *token revoke* и выпустите новый

Синтаксис

```
rude token create [имя_пользователя]
```

Параметры

Параметр	Описание
имя_пользователя	Имя существующего пользователя сервера (обязательный)

Важно

Для одного пользователя может существовать только один активный токен. Попытка создать второй вернёт ошибку `Token already exists for this user`. Чтобы перевыпустить токен, сначала отзовите существующий через *token revoke*

Пример

Чтобы создать токен пользователю, введите следующее:

```
rude token create rude
```

После выполнения команды в стандартный вывод напечатается значение токена. Сохраните его — повторно получить тот же токен будет нельзя

Подсказка

Подробнее об использовании токена см. на странице *Настройка доступа*

token list

Получение списка всех выпущенных токенов API

Зачем нужна

Команда показывает все живые API-токены — кому и когда были выданы. Список выпущенных токенов нигде в веб-интерфейсе не отображается, поэтому это единственный способ увидеть, какие интеграции и пользователи имеют действующий доступ к API

Типичные случаи применения:

- инвентаризация активных токенов и сверка их с подтверждённым перечнем интеграций
- поиск «бесхозных» токенов от уволившихся пользователей или закрытых интеграций — кандидатов на отзыв
- быстрая сверка значения токена, если интеграция перестала работать — есть ли токен в системе и принадлежит ли он нужному пользователю

Синтаксис

```
rude token list
```

Пример

Чтобы получить список созданных токенов, введите следующее:

```
rude token list
```

В выводе для каждого токена показаны: дата и время создания, имя пользователя и значение токена

```
2024-08-29 07:23:33.581116+00:00 rude
↪a1b2c3d4e5f67890abcdef1234567890
```

Подсказка

Подробнее об использовании токена см. на странице *Настройка доступа*

token revoke

Отзыв токена доступа к API

Зачем нужна

Команда удаляет API-токен из базы — после этого все запросы с этим токеном будут отклонены. Используется для немедленного блокирования скомпрометированного или устаревшего токена и для перевыпуска (на одного пользователя допускается только один активный токен)

Типичные случаи применения:

- утечка токена — нужно немедленно вывести его из обращения
- перевыпуск токена для пользователя: сначала отозвать старый, затем создать новый через *token create*
- закрытие интеграции с внешней системой, чтобы её токен больше не имел доступа
- регулярная ротация токенов по политике безопасности

Синтаксис

```
rude token revoke [значение_токена]
```

Параметры

Параметр	Описание
значение_токена	Значение существующего токена (получить можно командой *token list*)

Пример

Чтобы отозвать токен, введите следующее:

```
rude token revoke abcdef1234567890
```

После выполнения команды токен становится недействительным — все последующие запросы с этим токеном будут отклонены

Подсказка

Подробнее об использовании токенов см. на странице *Настройка доступа*

Действия с API — CLI-команды для выпуска и просмотра токенов доступа к REST API сервера

Команда	Описание
token create	Создание токена
token list	Получение списка с созданными токенами
token revoke	Отзыв токена

1.6.9 Действия с LDAP

keycloak

Взаимодействие с KeyCloak: импорт и удаление пользователей и групп

Зачем нужна

Команда вручную запускает обмен с подключённым *Keycloak*: `sync` втягивает пользователей и группы из realm в **RuDesktop**, `clean` удаляет всё, что было импортировано из этого источника. Без команды синхронизация выполняется только при настроенном расписании или при первичном подключении

Типичные случаи применения:

- немедленно подтянуть свежие изменения из Keycloak (новые пользователи, обновление состава групп) без ожидания планового запуска
- проверка корректности подключения к Keycloak после изменения настроек realm — синхронизировать и убедиться, что объекты появились
- `clean` — полная отвязка от Keycloak: удалить всех импортированных пользователей и группы, например, перед сменой источника аутентификации
- разовая ручная подгрузка после массового добавления учётных записей в Keycloak

Синтаксис

```
rude keycloak sync
rude keycloak clean
```

Параметры

Параметр	Описание
sync	Запустить синхронизацию с KeyCloak (импорт пользователей и групп)
clean	Удалить с сервера импортированных из KeyCloak пользователей и групп

Пример

1. Чтобы выполнить синхронизацию с KeyCloak, введите следующее:

   ```
   rude keycloak sync
   ```

   После выполнения команды пользователи и группы, существующие в подключённом realm KeyCloak, будут импортированы на сервер **RuDesktop**

2. Чтобы очистить данные, полученные при синхронизации с KeyCloak, введите следующее:

   ```
   rude keycloak clean
   ```

   После выполнения команды:

   - Будут удалены пользователи, чей логин содержит `@<realm_name>` (импортированные из KeyCloak)
   - Будут удалены группы, у которых заполнено поле `key_cloak_group` и id выше зарезервированных системных
   - Связи устройств с этими группами и группы пользователей также удаляются

ldap

Взаимодействие с доменом LDAP/Active Directory

Зачем нужна

Команда — это набор действий администратора по обмену с подключённым *доменом*: разовая синхронизация (`sync`), привязка устройств к пользователям домена по логину (`link`), перенос объектов между доменами (`migrate`) и полная очистка от доменных данных (`clean`)

Типичные случаи применения:

- `sync` — немедленная подгрузка свежих изменений из AD/LDAP без ожидания плановой синхронизации
- `link` — после массового импорта устройств: автоматически привязать каждое к доменному пользователю с тем же логином, чтобы не делать это вручную
- `migrate` — переезд между доменами (смена имени домена, объединение или разделение AD-леса) без ручного восстановления связей
- `clean` — отказ от доменной интеграции, миграция на Keycloak или локальные учётки: убрать все доменные объекты, оставив локальных пользователей нетронутыми

Синтаксис

```
rude ldap sync
rude ldap clean
rude ldap link
rude ldap migrate [source_domain] [dest_domain]
```

Параметры

Параметр	Описание
sync	Запустить синхронизацию с доменом (импорт пользователей и групп)
clean	Очистить данные предыдущей синхронизации (удаляются доменные пользователи и группы)
link	Привязать устройства к доменным пользователям по их логину
migrate [source] [dest]	Перенести пользователей и группы из домена `source` в домен `dest`

Пример

1. Чтобы выполнить синхронизацию с доменом, введите следующее:

   ```
   rude ldap sync
   ```

   После выполнения команды все данные, полученные при синхронизации с доменом, будут добавлены на сервер **RuDesktop**

   ```
   Synchronization started at 17.10.2024 17:24:43
   Synchronize win2012.local
       Group: group1 ... OK
       Host: WINDOWS-11 ... OK
           Add to group: Сотрудник поддержки ... OK
   ```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
Delete non existing objects
    Delete 0 groups
    Unlink 0 hosts
Synchronization finished at [ДАТА_ВРЕМЯ] and took 2.27␣
↪seconds
```

2. Чтобы привязать устройства к пользователям домена, введите следующее:

   ```
   rude ldap link
   ```

   После выполнения команды устройства будут связаны с соответствующими доменными пользователями (по их логину)

3. Чтобы перенести пользователей и группы из одного домена в другой, введите следующее:

   ```
   rude ldap migrate old.example.com new.example.com
   ```

   Команда меняет принадлежность объектов с исходного домена на целевой. Используется при смене имени домена или переезде

4. Чтобы очистить данные, полученные при синхронизации с доменом, введите следующее:

   ```
   rude ldap clean
   ```

   После выполнения команды все доменные пользователи и группы (кроме локальных, у которых `DN` содержит `dc=local`) будут удалены с сервера **RuDesktop**

Действия с LDAP — CLI-команды для запуска синхронизации со службами каталогов **LDAP** и **KeyCloak**

Команда	Описание
keycloak	Взаимодействие с KeyCloak
ldap	Взаимодействие с доменом

1.6.10 Действия с UEM

job

Управление задачами

Зачем нужна

Команда работает с UEM-*задачами* из CLI: показывает список задач с путями до их playbook'ов, запускает задачу немедленно (с подробным выводом Ansible при необходимости) и выводит сам playbook для просмотра. В веб-интерфейсе

доступен только запуск через расписание или ручной триггер — CLI добавляет возможность запустить задачу с подробным логом и заглянуть в сгенерированный playbook

Типичные случаи применения:

- срочный запуск задачи без открытия веб-интерфейса (например, во время инцидента)
- отладка проблемной задачи с флагом `--verbose` — Ansible выводит подробности по каждому шагу, что недоступно из веб-интерфейса
- проверка содержимого сгенерированного playbook'а перед запуском, чтобы убедиться в корректности параметров политики
- автоматизация — запуск задачи из скрипта по событию во внешней системе (cron, мониторинг, CI/CD)

Синтаксис

```
rude job list
rude job run [id_задачи] [--verbose]
rude job show [id_задачи ...]
```

Параметры

Параметр	Описание	
list	Вывести список всех задач с их ID	названием и путём к playbook
run [id_задачи]	Запустить задачу с указанным ID	
--verbose	Включить подробный вывод Ansible (флаг `-vvv`); используется только с `run`	
show [id_задачи ...]	Показать playbook одной или нескольких задач (можно перечислить несколько ID через пробел)	

Пример

1. Чтобы получить список всех задач, введите следующее:

   ```
   rude job list
   ```

   После выполнения команды в выводе отобразится следующая информация:

```
#ID           #Название задачи  #Путь до playbook
1001      Обслуживание сервера  /var/lib/rudesktop/
↪playbooks/job_1001_обслуживание-сервера.yaml
1002            Инвентаризация  /
↪var/lib/rudesktop/playbooks/job_1002_инвентаризация.yaml
10000  Автообновление клиентов  /var/lib/rudesktop/
↪playbooks/job_10000_автообновление-клиентов.yaml
10003            Обновление ОС  /
↪var/lib/rudesktop/playbooks/job_10003_обновление-oc.yaml
```

2. Чтобы запустить задачу, введите следующее:

```
rude job run 1002
```

После выполнения команды в выводе отобразится следующая информация:

```
Процесс запущен в 2024-10-16 16:30:44
astra21245orel             : ok=20   changed=11
↪unreachable=0    failed=0    skipped=11   rescued=0
↪ignored=0
alt10ws                    : ok=20   changed=11
↪unreachable=0    failed=0    skipped=11   rescued=0
↪ignored=0
host-29                    : ok=20   changed=11
↪unreachable=0    failed=0    skipped=11   rescued=0
↪ignored=0
...
Выполнено: 100.00%|████████████████████████| 12/12
↪[01:33<00:00, 7.76s/хост]
Процесс завершен в 2024-10-16 16:32:17
```

Чтобы запустить задачу с подробным выводом Ansible (флаг `-vvv`), добавьте `--verbose`:

```
rude job run 1002 --verbose
```

3. Чтобы посмотреть playbook одной или нескольких задач, введите следующее:

```
rude job show 1002
```

или для нескольких задач сразу:

```
rude job show 1002 1003 1004
```

После выполнения команды для каждой задачи будет выведен путь к её playbook и его содержимое

policy

Управление политиками

Зачем нужна

Команда — CLI-эквивалент работы с *политиками* из веб-интерфейса: список всех политик с путями до их playbook'ов, разовый запуск политики (опционально только на выбранных узлах) и просмотр сгенерированного playbook'а. В отличие от запуска через задачу, `policy run` работает напрямую с политикой и принимает список узлов через аргумент

Типичные случаи применения:

- разовый запуск политики на одном-двух конкретных устройствах без создания отдельной задачи
- отладка политики с флагом `--verbose` — увидеть подробный вывод Ansible по каждому шагу
- проверка содержимого сгенерированного playbook'а (`policy show`) перед запуском или для разбора некорректного поведения
- автоматизация: запустить политику из скрипта по триггеру внешней системы

Синтаксис

```
rude policy list
rude policy run [id_политики] [--hosts host1 host2 ...] [--verbose]
rude policy show [id_политики ...]
```

Параметры

Параметр	Описание	
list	Вывести список всех политик с их ID	названием и путём к playbook
run [id_политики]	Запустить политику с указанным ID	
--hosts	Список узлов через пробел для запуска политики (по умолчанию — все узлы); используется только с `run`	
--verbose	Включить подробный вывод Ansible (флаг `-vvv`); используется только с `run`	

продолжается на следующей странице

Таблица 30 – продолжение с предыдущей страницы

Параметр	Описание
show [id_политики ...]	Показать playbook одной или нескольких политик (можно перечислить несколько ID через пробел)

Пример

1. Чтобы получить список всех политик, введите следующее:

```
rude policy list
```

После выполнения команды в выводе отобразится следующая информация:

```
#ID         #Название политики  #Путь до playbook
1001      Обслуживание сервера  /var/lib/rudesktop/
↪playbooks/job_1001_обслуживание-сервера.yaml
1002            Инвентаризация  /
↪var/lib/rudesktop/playbooks/job_1002_инвентаризация.yaml
10000  Автообновление клиентов  /var/lib/rudesktop/
↪playbooks/job_10000_автообновление-клиентов.yaml
10003            Обновление ОС  /
↪var/lib/rudesktop/playbooks/job_10003_обновление-oc.yaml
```

2. Чтобы запустить политику, введите следующее:

```
rude policy run 1002
```

Чтобы запустить политику только на указанных узлах (по умолчанию — на всех):

```
rude policy run 1002 --hosts host1 host2
```

Чтобы запустить политику с подробным выводом Ansible (флаг `-vvv`):

```
rude policy run 1002 --verbose
```

После выполнения команды в выводе отобразится следующая информация:

```
PLAY [Обслуживание сервера RuDesktop \ Обслуживание␣
↪сервера] ************

TASK [Обслуживание сервера] ************
changed: [localhost]

PLAY RECAP ************
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
localhost                  : ok=1    changed=1    ␣
↪unreachable=0    failed=0    skipped=0    rescued=0    ␣
↪ignored=0
```

3. Чтобы посмотреть playbook одной или нескольких политик, введите следующее:

```
rude policy show 1002
```

или для нескольких политик сразу:

```
rude policy show 1002 1003
```

После выполнения команды в выводе для каждой политики отобразится её playbook

```
Playbook ID 1002 /var/lib/rudesktop/playbooks/policy_1002
↪_обслуживание-сервера.yaml
- connection: local
gather_facts: false
hosts:
- localhost
name: Обслуживание сервера RuDesktop \ Обслуживание␣
↪сервера
strategy: inproc
tasks:
- ansible.builtin.command: rude maintain --
↪log-delete-after-days '{{ log_delete_after_days
    }}'
    delegate_to: localhost
    name: Обслуживание сервера
    run_once: true
vars:
    ansible_interpreter_python_fallback:
    - python3.14
    - python3.13
    - python3.12
    - python3.11
    - python3.10
    - python3.9
    - python3.8
    - python3.7
    - python3.6
    - python2.6
    - /usr/bin/python2
    - /usr/bin/python3
    - /usr/bin/python
    - /usr/libexec/platform-python
    - python
    log_delete_after_days: null
```

remote

Выполнение команд и обмен файлами с удалёнными устройствами с сервера

Зачем нужна

Команда даёт администратору низкоуровневый CLI-канал к устройствам напрямую с сервера, не открывая графическую сессию: скачать логи (`logs`), скопировать файл на устройство (`put`) или с устройства (`get`), выполнить произвольную команду (`exec`). По сути это «sudo по сети» через инфраструктуру **RuDesktop** — без SSH и предварительной настройки

Типичные случаи применения:

- `logs` — массовый сбор клиентских логов с проблемного устройства для разбора инцидента, вместе с `info.txt` об оборудовании
- `put` — точечная доставка файла на устройство (патч, скрипт, конфиг), когда не хочется создавать отдельную политику
- `get` — забрать файл с устройства (конфиг, дамп, отчёт) для анализа на сервере
- `exec` — выполнить разовую команду на конкретном устройстве из скрипта администратора без создания политики «Выполнить команду»

Важно

Команда требует мастер-пароль устройства — он берётся из БД, либо передаётся через `--password`. Без мастер-пароля устройство не пустит сервер и команда завершится ошибкой

Синтаксис

```
rude remote --id [ID_устройства] [--password password] [--loglevel␣
↪level] logs [--source path] [--target path]
rude remote --id [ID_устройства] [--password password] [--loglevel␣
↪level] put [путь/на_сервере] [путь/на_устройстве]
rude remote --id [ID_устройства] [--password password] [--loglevel␣
↪level] get [путь/на_устройстве] [путь/на_сервере]
rude remote --id [ID_устройства] [--password password] [--loglevel␣
↪level] exec [команда]
```

Параметры

Параметр	Описание
--id	Идентификатор устройства (server_id) — обязательный

продолжается на следующей странице

Таблица 31 – продолжение с предыдущей страницы

Параметр	Описание
--password	Пароль для подключения. Если не указан, используется мастер-пароль устройства из БД
--loglevel	Уровень логирования библиотеки соединения: `error` (по умолчанию), `warning`, `info`, `debug`
logs	Сбор логов клиента **RuDesktop** с устройства (по умолчанию в `/tmp/<peer_id>/`)
--source	Путь на устройстве (для подкоманды `logs`); если задан, скачивается только указанный файл или папка
--target	Локальный путь для сохранения логов (для подкоманды `logs`); по умолчанию `/tmp/<peer_id>/`
put [src] [dst]	Копирование файла с сервера на удалённое устройство
get [src] [dst]	Копирование файла с удалённого устройства на сервер
exec [команда]	Выполнение команды на удалённом устройстве

Примечание

Если параметр `--password` не указан — команда использует мастер-пароль устройства, сохранённый в БД. Если у устройства нет мастер-пароля, команда завершится ошибкой `Please specify password`

Пример

1. Чтобы скачать логи с удалённого устройства на сервер, введите следующее:

```
rude remote --id 123456789 logs
```

После выполнения команды логи (root и пользовательские) будут загружены на сервер. Для каждой ОС используются разные пути:

- **Windows** — `C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\RuDesktop` и `C:\Users\<username>\AppData\Roaming\RuDesktop`
- **Linux** — `/root/.local/share/logs/RuDesktop` и `/home/<username>/.local/share/logs/RuDesktop`
- **macOS** — `/private/var/root/Library/Logs/RuDesktop`

По умолчанию логи сохраняются в `/tmp/<peer_id>/`. Рядом создаётся файл `info.txt` с основной информацией об устройстве и его ресурсах

Чтобы загрузить логи в конкретный каталог, используйте флаг `--target`:

```
rude remote --id 123456789 logs --target /
↪var/log/peer_logs
```

Чтобы скачать только указанный файл или папку с устройства, используйте флаг `--source`:

```
rude remote --id 123456789 logs --source
↪"C:\\Path\\To\\file.log" --target /tmp/peer.log
```

2. Чтобы скопировать файл с сервера на удалённое устройство, введите следующее:

```
rude remote --id 123456789 put /tmp/1.txt /
↪home/user/1.txt
```

После выполнения команды файл будет скопирован с сервера на удалённое устройство

3. Чтобы скопировать файл с удалённого устройства на сервер, введите следующее:

```
rude remote --id 123456789 get /home/user/1.txt /
↪tmp/1.txt
```

После выполнения команды файл будет скопирован с удалённого устройства на сервер

4. Чтобы выполнить команду на удалённом устройстве, введите следующее:

```
rude remote --id 123456798 exec mkdir /home/user/test
```

После выполнения команды папка будет создана на удалённом устройстве по указанному пути

Действия с UEM — CLI-команды модуля **Управление конфигурациями (UEM)**: запуск задач и политик, удалённое выполнение операций на устройствах

Команда	Описание
job	Управление задачами
policy	Управление политиками
remote	Выполнение команд с сервера на удалённых устройствах

1.6.11 Действия с модулем аналитики

superset install

Установка и инициализация службы модуля аналитики

Зачем нужна

Команда выполняет полную настройку модуля аналитики **Apache Superset**: инициализирует базу данных (*superset init*), устанавливает и включает systemd-службу и сокет `rudesktop-analytics`, после чего запускает модуль. Выполняется автоматически при установке пакета `rudesktop-superset`; вручную нужна для повторной инициализации модуля

Типичные случаи применения:

- повторная инициализация после изменения параметров подключения к БД (`POSTGRES_SUPERSET_*`), например при выносе базы данных на отдельный сервер
- восстановление службы после ручного удаления systemd-юнитов

Синтаксис

```
rude superset install
```

Пример

Чтобы установить и инициализировать модуль аналитики, введите следующее:

```
rude superset install
```

После выполнения команды в выводе отобразится следующая информация:

```
Initialize superset database
  Create database ... OK
Initialize analytics
  Running migrations ... OK
  Initialize ... OK
  Load database ... OK
  Create base user ... OK
  Load dashboard ... OK
  Load roles ... OK
Install server
  Enable analytics service ... OK
  Enable analytics socket  ... OK
Stop superset socket   ... OK
Stop superset service  ... OK
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
Start superset socket  ... OK
Start superset service ... OK
```

superset init

Инициализация базы данных модуля аналитики

Зачем нужна

Команда создаёт структуру базы данных модуля аналитики **Apache Superset** и наполняет её исходными данными: применяет миграции, регистрирует базу сервера **RuDesktop** как источник данных, создаёт встроенного администратора, импортирует базовые дашборды и роли. Выполняется автоматически при установке модуля; вручную нужна для инициализации новой базы данных или восстановления её структуры

Типичные случаи применения:

- инициализация структуры в новой базе данных модуля аналитики (например, вынесенной на отдельный сервер)
- восстановление структуры после ручного вмешательства в БД
- повторная загрузка базовых дашбордов и ролей

Важно

Если база данных не существует, команда пытается создать её на **локальном** PostgreSQL. Для базы данных на внешнем сервере её необходимо создать заранее вручную — см. *Смена адреса для модуля аналитики*

Синтаксис

```
rude superset init
```

Пример

Чтобы инициализировать базу данных модуля аналитики, введите следующее:

```
rude superset init
```

После выполнения команды в выводе отобразится следующая информация:

```
Initialize superset database
  Create database ... OK
Initialize analytics
  Running migrations ... OK
  Initialize ... OK
  Load database ... OK
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  Create base user ... OK
  Load dashboard ... OK
  Load roles ... OK
```

superset backup

Создание резервной копии базы данных модуля аналитики

Зачем нужна

Команда сохраняет дамп БД модуля аналитики **Apache Superset** (`rudesktop-analytics`) в один сжатый файл `.gz`. Дамп Superset делается **отдельно** от основной базы сервера: данные дашбордов, графиков и пользовательских настроек Superset живут в собственной БД, и обычное *rude backup* их не затрагивает

Типичные случаи применения:

- регулярное резервное копирование настроек Superset через cron вместе с бэкапом основной БД
- бэкап перед обновлением модуля аналитики или миграцией на другой сервер
- сохранение состояния Superset перед массовым изменением дашбордов — на случай отката

Синтаксис

```
rude superset backup /path/to/file.gz
```

Параметры

- путь к файлу — обязательный параметр, должен иметь расширение `.gz`. Указывайте полный путь

Пример

Чтобы создать резервную копию базы данных модуля аналитики, введите следующее:

```
rude superset backup /home/rude/superset_backup.gz
```

После выполнения команды по указанному пути появится файл со сжатым дампом базы данных модуля аналитики

Подсказка

Подробнее об использовании и автоматизации см. на странице *Резервное копирование*

superset restart

Перезапуск модуля аналитики

Зачем нужна

Команда останавливает и заново запускает службу и сокет `rudesktop-analytics`. Используется, когда нужно применить изменения в конфигурации модуля аналитики или восстановить его работу после сбоя — без полного перезапуска сервера **RuDesktop**

Типичные случаи применения:

- модуль аналитики «завис» или перестал отвечать
- применение изменений в конфигурационных файлах Superset
- восстановление работы после *superset restore* или ручного вмешательства в БД

Синтаксис

```
rude superset restart
```

Пример

Чтобы перезапустить модуль аналитики, введите следующее:

```
rude superset restart
```

После выполнения команды в выводе отобразится следующая информация:

```
Stop superset socket   ... OK
Stop superset service  ... OK
Start superset socket  ... OK
Start superset service ... OK
```

superset restore

Восстановление базы данных модуля аналитики из резервной копии

Зачем нужна

Команда полностью замещает текущую БД модуля аналитики содержимым файла, ранее созданного *superset backup*. После восстановления возвращаются все дашборды, графики, источники данных и пользовательские настройки Superset

Типичные случаи применения:

- восстановление после сбоя БД Superset или ошибочного массового удаления дашбордов
- перенос настроек Superset на новый сервер при миграции

- откат после неудачного обновления модуля аналитики или ручного изменения БД

Важно

Восстановление **деструктивно** для текущих данных Superset. Перед запуском убедитесь, что у вас есть актуальный дамп текущего состояния — на случай отката

Синтаксис

```
rude superset restore /path/to/file.gz
```

Параметры

- путь к файлу — обязательный параметр. Указывайте полный путь к файлу резервной копии в формате `.gz`, созданному командой `rude superset backup`

Важно

На время восстановления модуль аналитики временно недоступен — текущая база модуля будет заменена данными из дампа

Пример

Чтобы восстановить базу данных модуля аналитики из резервной копии, введите следующее:

```
rude superset restore /home/rude/superset_backup.gz
```

Подсказка

Подробнее о резервном копировании и восстановлении см. на странице *Резервное копирование*

superset status

Получение информации о статусах служб модуля аналитики

Зачем нужна

Команда показывает состояние службы и сокета модуля аналитики (`rudesktop-analytics.service` / `rudesktop-analytics.socket`): активна ли служба, включён ли автозапуск и время последнего изменения состояния. По сути аналог `systemctl status`, но в одной строке для каждого юнита и без лишнего вывода

Типичные случаи применения:

- быстрая проверка работоспособности модуля при недоступности дашбордов в веб-интерфейсе
- скриптовый мониторинг — разобрать вывод и завести алерт, если служба не `active`
- сверка после *superset restart* или *superset start*, что службы поднялись

Синтаксис

```
rude superset status
```

Пример

Чтобы получить информацию о статусах служб модуля аналитики, введите следующее:

```
rude superset status
```

После выполнения команды в выводе отобразится следующая информация:

```
Service (Description)                                                  |␣
↪Active  | Enabled | Since
------------------------------------------------------------------------
↪---------------------------------------
rudesktop-analytics.service (Apache Superset admin panel)    |␣
↪active  | enabled | Thu 2025-05-15 14:29:48 +07
rudesktop-analytics.socket (RuDesktop superset socket)       |␣
↪active  | enabled | Thu 2025-05-15 14:29:36 +07
```

superset start

Запуск модуля аналитики (Apache Superset)

Примечание

Команды `rude superset *` доступны только при установленном модуле аналитики (пакет `rudesktop-superset`)

Зачем нужна

Команда поднимает службу и сокет `rudesktop-analytics` после остановки. Без активной службы дашборды Superset недоступны в веб-интерфейсе и не отрабатывают расписания обновления

Типичные случаи применения:

- запуск модуля после плановой остановки на обслуживание или миграцию

- старт службы после ручной установки пакета `rudesktop-superset`
- восстановление работы после нештатной остановки

Синтаксис

```
rude superset start
```

Пример

Чтобы запустить модуль аналитики, введите следующее:

```
rude superset start
```

После выполнения команды в выводе отобразится следующая информация:

```
Start superset socket  ... OK
Start superset service ... OK
```

superset stop

Остановка модуля аналитики

Зачем нужна

Команда останавливает службу и сокет `rudesktop-analytics`. После остановки дашборды и API Superset недоступны до следующего *superset start*, при этом основная база сервера и веб-интерфейс **RuDesktop** продолжают работать

Типичные случаи применения:

- плановое обслуживание модуля аналитики (обновление, миграция БД)
- освобождение ресурсов сервера при пиковой нагрузке на основной модуль, если аналитика временно не нужна
- остановка перед *superset restore* или ручным вмешательством в БД Superset

Синтаксис

```
rude superset stop
```

Пример

Чтобы остановить модуль аналитики, введите следующее:

```
rude superset stop
```

После выполнения команды в выводе отобразится следующая информация:

```
Stop superset socket  ... OK
Stop superset service ... OK
```

superset drop

Пересоздание базы данных модуля аналитики

Зачем нужна

Команда полностью удаляет базу данных модуля аналитики **Apache Superset** и создаёт её заново с нуля. Все дашборды, графики, источники данных и пользовательские настройки Superset сбрасываются к исходному состоянию. Используется для сброса модуля аналитики, когда восстановление из резервной копии невозможно или нецелесообразно

Типичные случаи применения:

- сброс модуля аналитики к исходному состоянию
- устранение неустранимых проблем со структурой или данными БД Superset

Важно

Команда **деструктивна**: текущая база данных модуля аналитики удаляется безвозвратно вместе со всеми пользовательскими дашбордами и настройками. Перед запуском создайте резервную копию командой *superset backup*

Примечание

Команда работает с **локальным** PostgreSQL: удаление базы выполняется командой `dropdb` от пользователя `postgres`. Для базы данных на внешнем сервере используйте средства этого сервера

Синтаксис

```
rude superset drop
```

Пример

Чтобы пересоздать базу данных модуля аналитики, введите следующее:

```
rude superset drop
```

После выполнения команды текущая база данных модуля аналитики будет удалена и создана заново с базовыми дашбордами и ролями

superset token

Управление токенами доступа к REST API модуля аналитики

Зачем нужна

Команда выпускает, показывает и отзывает токены для машинного доступа к REST API модуля аналитики: внешняя система передаёт токен в заголовке `Authorization: Bearer [TOKEN]` и работает с API без входа через веб-интерфейс. Типичный сценарий — *передача внешних справочников в модуль аналитики*

Токены привязываются к учётной записи модуля аналитики и наследуют её роль. Пользователь должен уже существовать в модуле: учётные записи создаются автоматически при первом входе через **SSO** или вручную (см. ниже) — если пользователя нет, команда откажет. Роль берётся как у пользователя: суперпользователь **RuDesktop** имеет **Admin**, обычные пользователи — **Public** (токен такого пользователя не сможет загружать файлы; команда предупредит об этом)

Для технической учётной записи, которая нужна только под токен, пользователя можно создать прямо в модуле аналитики — без учётной записи на сервере **RuDesktop** и без входа по SSO. В интерфейсе: откройте `https://[SERVER_ADDR]/analytics/users/add` и создайте пользователя с ролью **Admin**

Или через CLI:

```
rude superset fab create-user --role Admin --username␣
↪analytics_uploader \
    --firstname analytics_uploader --lastname "" \
    --email analytics_uploader@local --password␣
↪[произвольный_пароль]
```

Пароль нужен только при создании: вход в веб-интерфейс модуля всегда идёт через **SSO**, пароль нигде не используется

Предупреждение

Под технической учётной записью не выполняйте вход по **SSO**: при входе роль пересинхронизируется с сервера **RuDesktop**, и если эта учётная запись там не суперпользователь — роль **Admin** сменится на **Public**

Важно

Значение токена выводится **один раз** при создании — посмотреть его повторно нельзя. При утере отзовите токен и выпустите новый

Типичные случаи применения:

- выпуск токена для внешней системы, загружающей справочники через REST API

- отзыв скомпрометированного или более не нужного токена
- проверка, какими токенами и когда пользовались (`list` показывает `uuid` и статус)

Синтаксис

```
rude superset token create [имя_пользователя] [--days N] [--name␣
↪ИМЯ]
rude superset token list [<имя_пользователя|id>]
rude superset token revoke [токен | uuid] [--purge]
rude superset token prune
```

Подкоманды

`create [имя_пользователя] [--days N] [--name ИМЯ]`
: Выпустить токен для существующего пользователя модуля аналитики (по имени или идентификатору). Без `--days` токен бессрочный — действует до отзыва; `--days N` ограничивает срок действия N днями с момента выпуска. `--name` задаёт отображаемое имя ключа — удобно при нескольких ключах, чтобы в `list` было видно, какой ключ какой интеграции принадлежит; без `--name` ключ создаётся без имени (в списке отображается прочерк). Печатает значение токена один раз

`list [<имя_пользователя|id>]`
: Показать токены всех пользователей или только указанного: дату создания, пользователя, имя ключа, `uuid`, статус (`активен` / `отозван/истёк`) и срок действия, если задан. Значение токена не показывается — оно хранится только в виде хэша

`revoke [токен | uuid] [--purge]`
: Отозвать токен по его значению либо по `uuid` из `list`. Отзыв применяется сразу. Без `--purge` отозванный токен остаётся в списке со статусом `отозван/истёк` (история); `--purge` дополнительно удаляет запись о нём из списка

`prune`
: Удалить из списка разом все отозванные и истёкшие токены; активные не затрагиваются

Пример

Выпуск токена для служебной учётной записи:

```
rude superset token create analytics_uploader
```

После выполнения команды в выводе отобразится следующее:

```
sst_1YdKk2mS9QpZ8xN3vL5rA7wTbGhJ4cE6fU2iO0dPqR
```

Токен на ограниченный срок (30 дней):

```
rude superset token create analytics_uploader --days 30
```

После выполнения команды в выводе отобразится следующее:

```
sst_1YdKk2mS9QpZ8xN3vL5rA7wTbGhJ4cE6fU2iO0dPqR
Действует до: 05.12.2026 14:10
```

Список токенов и отзыв:

```
rude superset token list
rude superset token revoke␣
↪sst_1YdKk2mS9QpZ8xN3vL5rA7wTbGhJ4cE6fU2iO0dPqR
```

Действия с модулем аналитики — CLI-команды для управления встроенным **Apache Superset**: установка и инициализация, запуск, остановка, перезапуск, проверка статуса, резервное копирование, пересоздание базы данных и управление токенами доступа к REST API

Команда	Описание
superset install	Установка и инициализация службы модуля аналитики
superset init	Инициализация базы данных модуля аналитики
superset backup	Создание резервной копии базы данных модуля аналитики
superset restart	Перезапуск модуля аналитики
superset restore	Восстановление базы данных модуля аналитики из резервной копии
superset start	Запуск модуля аналитики
superset status	Получение информации о статусах служб модуля аналитики
superset stop	Остановка модуля аналитики
superset drop	Пересоздание базы данных модуля аналитики
superset token	Управление токенами доступа к REST API модуля аналитики

1.6.12 Действия с дополнительными командами сервера

analyze

Анализ серверного лога или списка IP-адресов на наличие в БД устройств с этими адресами

Зачем нужна

Команда сопоставляет внешний список IP-адресов или серверный лог со списком устройств в БД сервера: показывает, какие из IP принадлежат зарегистрированным устройствам, и наоборот. Позволяет быстро ответить на вопрос «кто это был?» не разбираясь руками с таблицей устройств

Типичные случаи применения:

- разбор инцидента: на руках есть список IP из логов IDS/прокси/firewall — нужно понять, какие из них принадлежат корпоративным устройствам
- расследование подозрительной активности по серверному логу — какие устройства фигурировали в событиях за период
- инвентаризация: сверка реальных подключающихся IP-адресов с известными устройствами

Синтаксис

```
rude analyze ip-list [путь_до_файла]
rude analyze srv-log [путь_до_файла]
```

Параметры

Параметр	Описание
analyze	Анализ файла на наличие IP-адресов
ip-list	Список ip-адресов из файла
srv-log	Список ip-адресов из файла-лога сервера или
путь_до_файла	Полный путь до файла со списком ip-адресов или путь до файла-лога «чего-то» для поиска в нём ip-адресов

Примечание

Подкоманда `ip-list` принимает файл со списком IP-адресов (IP-адрес во втором столбце); `srv-log` — файл серверного лога, в котором ищутся события (Connected/Accept/Disconnected и пр.) и IP-адреса. По обоим вариантам команда сопоставляет адреса с устройствами в БД

Пример

Служебная команда сервера, обычно не применяется пользователем в Linux-консоли — нужна для разбора инцидентов и сопоставления событий лога с устройствами

```
rude analyze ip-list /path/to/ips.txt
rude analyze srv-log /var/log/rudesktop/server.log
```

check

Проверка всего проекта Django на наличие потенциальных проблем

Зачем нужна

Команда — стандартная Django-проверка приложений на типовые проблемы конфигурации (несовместимые миграции, ошибки в моделях, проблемы безопасности, неверные настройки развёртывания). Не меняет данные, только сообщает о найденных проблемах с уровнями серьёзности от `DEBUG` до `CRITICAL`

Типичные случаи применения:

- профилактическая проверка состояния сервера после обновления — все ли проверки прошли
- `--deploy` — диагностика настроек безопасности перед публикацией сервера во внешнюю сеть
- разбор инцидента, когда сервер «странно себя ведёт» — иногда первопричина видна именно здесь
- проверка после ручного изменения настроек `settings` или БД

Синтаксис

```
rude check [--tag TAGS] [--list-tags] [--deploy] [--fail-level
↪{CRITICAL,ERROR,WARNING,INFO,DEBUG}] [--database {default}]
```

Параметры

Параметр	Описание
--tag TAGS	Вы можете использовать эти теги чтобы ограничить выполняемые проверки только теми которые относятся к определенной категории. Например чтобы выполнять только проверки моделей и совместимости - выполните команду:
--list-tags	Показать все тэги.
--deploy	Активирует некоторые дополнительные проверки которые применимы только к параметрам развертывания.
--fail-level {CRITICAL ERROR WARNING INFO DEBUG}	Указывает уровень логгирования который приведет к завершению выполнения команды с ненулевым статусом. По умолчанию используется значение ERROR.

продолжается на следующей странице

Таблица 35 – продолжение с предыдущей страницы

Параметр	Описание
--database {default}	Указывает базу данных для выполнения проверок требующих доступа к базе данных

Пример

Команда не используется пользователем из Linux-консоли, а применяется только для проверки проекта после его создания или изменения

clearsessions

Очистка сессий с истекшим сроком годности

Зачем нужна

Команда удаляет из БД истёкшие записи сессий веб-интерфейса. По умолчанию Django хранит истёкшие сессии до явной очистки — со временем таблица `django_session` разрастается и замедляет работу. Команда обычно входит в плановое обслуживание

Типичные случаи применения:

- регулярная очистка через cron — поддерживать таблицу сессий в разумных пределах
- разовая чистка после длительной эксплуатации сервера или массового пика входов
- освобождение места перед бэкапом или миграцией БД

Синтаксис

```
rude clearsessions
```

Пример

Команда не используется пользователем из Linux-консоли, а применяется только для сброса просроченных сессий

cleartokens

Очистка просроченных токенов

Зачем нужна

Команда удаляет из БД истёкшие OAuth-токены и refresh-токены. Истёкшие токены недействительны, но без чистки продолжают занимать место в таблицах. Команда нужна для регулярного обслуживания при активной интеграции через OAuth

Типичные случаи применения:

- регулярная очистка через cron на серверах с активной OAuth-интеграцией
- разовая чистка после массового выпуска коротко-живущих токенов (например, после нагрузочного теста)
- освобождение места перед бэкапом или миграцией БД

Синтаксис

```
rude cleartokens
```

Пример

Команда не используется пользователем из Linux-консоли, а применяется только для сброса просроченных токенов

client

Установка клиента RuDesktop по ssh

Зачем нужна

Команда удалённо устанавливает клиент **RuDesktop** на машину по SSH — без необходимости заходить на каждое устройство и запускать инсталлятор. Поддерживает массовую установку на список хостов: сервер сам подключается, копирует пакет и выполняет установку

Типичные случаи применения:

- первичная массовая раскатка клиента на парк Linux/macOS машин при внедрении **RuDesktop**
- развёртывание на новых серверах из ansible-playbook'а или скрипта инвентаризации
- альтернатива политике установки, когда устройства ещё не зарегистрированы и не могут получать политики

Синтаксис

```
rude client install
```

Параметры

Команда	Описание
--port	Порт который будет проверен на открытость

продолжается на следующей странице

Таблица 36 – продолжение с предыдущей страницы

Команда	Описание
--username	Логин для авторизации
--password	Пароль для авторизации
--become	Использовать пользователя с повышенными правами
--headless	Установить headless версию клиента
--become_user	Пользователь с повышенными правами
--become_password	Пароль для пользователя с повышенными правами
--become_method	Метод повышения привилегий
--subnet_mask	Маска подсети
--connection	Тип соединения
--private_key_file	Путь к приватному ключу
--password_file	Путь к приватному ключу
--skip-packages-update	Не выполнять обновление пакетов на Linux-устройствах

Примеры

Служебная команда сервера не применяется пользователем в Linux-консоли

compilemessages

Компиляция po-файлов в mo-файлы для использования со встроенной поддержкой gettext

Предупреждение

Служебная Django-команда — применяется при сборке проекта **RuDesktop**. В рабочей инсталляции запуск, как правило, не требуется

Синтаксис

```
rude compilemessages [--locale LOCALE] [--exclude EXCLUDE] [--
↪use-fuzzy] [--ignore PATTERN]
```

Параметры

Параметр	Описание
--locale	Locale(s) to process (e.g. de_AT). Default is to process all. Can be used multiple times.

продолжается на следующей странице

Таблица 37 – продолжение с предыдущей страницы

Параметр	Описание
--exclude	Locales to exclude. Default is none. Can be used multiple times.
--use-fuzzy	Use fuzzy translations.
--ignore PATTERN	Ignore directories matching this glob-style pattern. Use multiple times to ignore more.

Пример

Команда не используется пользователем из Linux-консоли, а применяется только для компиляции локали сервера при сборке проекта

createapplication

Создание нового приложения программным способом

Зачем нужна

Команда регистрирует на сервере новое OAuth-приложение из CLI, минуя веб-интерфейс. Принимает все параметры приложения (тип, redirect URI, секрет, алгоритм подписи и т.д.) и создаёт запись в БД

Типичные случаи применения:

- автоматизация развёртывания: задать в скрипте установки уже готовые OAuth-клиенты для интеграций
- массовое создание OAuth-приложений в окружении (dev/test/prod) с фиксированными `client_id`
- безопасное задание секрета без отображения в браузере (`--client-secret` напрямую в CLI)

Синтаксис

```
rude createapplication [--client-id CLIENT_ID] [--user USER] [--
↪redirect-uris REDIRECT_URIS] [--post-logout-redirect-uris␣
↪POST_LOGOUT_REDIRECT_URIS] [--client-secret CLIENT_SECRET] [--
↪no-hash-client-secret] [--name NAME] [--skip-authorization] [--
↪algorithm ALGORITHM]
```

Параметры

Параметр	Описание
--client-id	Идентификатор нового приложения

продолжается на следующей странице

Таблица 38 – продолжение с предыдущей страницы

Параметр	Описание
--user	Пользователь которому принадлежит приложение
--redirect-uris	URI перенаправления это должна быть строка разделенная пробелами например: „URI1 URI2“
--post-logout-redirect-uris	URI перенаправления после выхода из системы это должна быть строка разделенная пробелами например: „URI1 URI2“
--client-secret	Секрет для этого приложения
--no-hash-client-secret	Не хешировать секрет клиента
--name	Имя этого приложения
--skip-authorization	Если задано полностью обойти форму авторизации даже при первом использовании приложения
--algorithm	Алгоритм подписи токена OIDC для этого приложения один из следующих: RS256HS256

Пример

Команда не используется пользователем из Linux-консоли, а применяется только для создания нового приложения сервера при сборке проекта

createcachetable

Создание таблицы необходимые для использования кэша SQL

Зачем нужна

Команда создаёт в БД таблицу под Django-кэш типа «database». Если в настройках сервера используется именно этот тип кэша, без таблицы кэширование не работает — запросы будут падать с ошибкой о несуществующей таблице

Типичные случаи применения:

- первичная инициализация сервера, если она не была выполнена автоматически
- восстановление таблицы кэша после ручной чистки БД
- `--dry-run` — посмотреть SQL-запросы создания таблицы, не выполняя их (для аудита)

Синтаксис

```
rude createcachetable [--database {default}] [--dry-run]
```

Параметры

Параметр	Описание
--database	Указывает базу данных в которой будут размещены таблицы кэша
--dry-run	Не создает таблицу а просто выводит SQL-запрос который будет выполнен

Пример

Команда не используется пользователем из Linux-консоли, а применяется только для создания кэша для приложения сервера при сборке проекта

dbshell

Запуск клиента командной строки для указанной базы данных или базу данных по умолчанию если она не указана

Предупреждение

Служебная Django-команда. Прямые SQL-операции в рабочей БД могут нарушить целостность данных — используйте только для диагностики и обращайтесь к ней с правами root

Синтаксис

```
rude dbshell [--database {default}]
```

Параметры

Параметр	Описание
--database	Указывает базу данных в которой следует открыть оболочку. По умолчанию используется база данных «по умолчанию»

Пример

Команда используется пользователем из Linux-консоли, если необходимо подключиться к локальной БД сервера Rudesktop, чтобы исполнить SQL-команды или провести другие манипуляции в контексте PSQL

```
rude dbshell
psql (14.20 (Ubuntu 14.20-0ubuntu0.22.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384,␣
↪bits: 256, compression: off)
Type "help" for help.

rudesktop=> help
You are using psql, the command-line interface to PostgreSQL.
Type:  \copyright for distribution terms
    \h for help with SQL commands
    \? for help with psql commands
    \g or terminate with semicolon to execute query
    \q to quit
rudesktop=> quit
```

diffsettings

Отображение различия между текущим файлом settings.py и настройками Django по умолчанию

Предупреждение

Служебная Django-команда — нужна для сравнения текущей конфигурации сервера с дефолтами Django. В рабочей инсталляции запуск, как правило, не требуется

Синтаксис

```
rude diffsettings [--all] [--default MODULE] [--output
↪{hash,unified}]
```

Параметры

Параметр	Описание
--all	Отображает все настройки независимо от их значений. В режиме «hash» значения по умолчанию предваряются символом «###»

продолжается на следующей странице

Таблица 41 – продолжение с предыдущей страницы

Параметр	Описание
--default	Модуль настроек с которым сравниваются текущие настройки. Оставьте пустым чтобы сравнивать с настройками Django по умолчанию
--output	Выбирает формат вывода. В режиме «hash» отображаются все измененные настройки при этом настройки не входящие в настройки по умолчанию префиксом является ###. В режиме «unified» префикс к настройке по умолчанию добавляется знак минус а к измененной настройке — знак плюс

Примеры

Команда не используется пользователями, нужна только для сравнения файлов конфигурации приложения Django

drf_create_token

Создание токена DRF для заданного пользователя

Зачем нужна

Команда — стандартный механизм Django REST Framework для выдачи токена аутентификации пользователю. Это альтернатива основной команде *token create*, использующая стандартный механизм DRF без дополнительной обвязки **RuDesktop**. Применяется в специфических интеграциях, рассчитанных на DRF Token Authentication

Типичные случаи применения:

- интеграция с внешним инструментом, который умеет работать только со стандартным DRF-токеном
- `-r` / `--reset` — перевыпуск токена пользователю с одновременным удалением старого
- автоматизация в скрипте, где требуется именно DRF-механизм

Подсказка

Для штатной работы с API используется *token create*

Синтаксис

```
rude drf_create_token [-r] username
```

Параметры

Параметр	Описание
--reset	Сбросить существующий токен пользователя и создать новый
username	Имя пользователя для создания DRF-токена

Примеры

Команда сбрасывает прошлый DRF-токен и генерирует новый для пользователя 1234

```
rude drf_create_token --reset 1234
```

dumpdata

Вывод содержимого базы данных в виде фикстуры заданного формата

Предупреждение

Служебная Django-команда. Для штатного резервного копирования базы используйте *backup* — она формирует совместимый с сервером дамп **PostgreSQL**

Синтаксис

```
rude dumpdata [--format FORMAT] [--indent INDENT] [--database
↪{default}] [--exclude EXCLUDE] [--natural-foreign] [--
↪natural-primary] [--all] [--pks PRIMARY_KEYS] [--output OUTPUT] [-
↪-version] app_label
```

Параметры

Параметр	Описание
--format	Задает формат сериализации выходных данных для фикстур
--indent	Задает уровень отступа используемый при форматированном выводе
--database	Указывает конкретную базу данных для вывода фикстур. По умолчанию используется база данных «default»
--exclude	app_label или app_label. ModelName для исключения (используйте несколько –exclude для исключения нескольких приложений/моделей)
--natural-foreign	Использовать естественные внешние ключи если они доступны
--natural-primary	Использовать естественные первичные ключи если они доступны
--all	Использовать базовый менеджер Django для вывода всех моделей хранящихся в базе данных включая те которые в противном случае были бы отфильтрованы или изменены пользовательским менеджером
--pks	Выводить только объекты с заданными первичными ключами. Принимает список ключей разделенных запятыми. Этот параметр работает только при указании одной модели
--output	Указывает файл в который будет записан вывод
app_label[.ModelName]	Ограничивает вывод данных указанным app_label или app_label.ModelName

Примеры

Команда выводит содержимое базы данных в виде фикстуры заданного формата в файл `/tmp/rude_dumpdata.txt`

Команда может использоваться для переноса данных между серверами см. *loaddata*

```
rude dumpdata --output /tmp/rude_dumpdata.txt
```

event

Помещает событие во внутреннюю очередь задач (PGQ — PostgreSQL-based queue)

Примечание

Команда вызывает `queue.push(event_name, args)`. Зарегистрированный воркер `executor` подхватывает событие из очереди и обрабатывает его. Используется как для штатных задач (синхронизация LDAP, чистка кэша), так и для отладки очереди

Зачем нужна

Команда позволяет администратору вручную поставить любое именованное событие в очередь задач сервера — то самое, что обычно ставится автоматически по расписанию или по триггерам в коде. Воркер *executor* подхватит событие и выполнит его

Типичные случаи применения:

- немедленный запуск штатных фоновых задач (синхронизация LDAP, очистка кэша, перерасчёт прав) без ожидания планового вызова
- разовое выполнение команды из скрипта без необходимости ждать расписания
- отладка работоспособности очереди — поставить событие `debug` и убедиться, что воркер его обработал
- обработка инцидентов: «сервер не успевает за нагрузкой» — посмотреть, как очередь отрабатывает добавляемые события

Синтаксис

```
rude event <имя_события> [аргументы в JSON]
```

Параметры

Параметр	Описание
debug	Тестовое событие
session_status	Обновить статус сессии
started	Сигнал о старте
geoadd	Добавить геоданные
sync	Синхронизация
run_report_generation	Запустить генерацию отчёта
run_command	Выполнить команду
run_playbook	Запустить Ansible playbook
run_job	Запустить задание
logevent	Записать событие в лог
notify	Отправить уведомление
sync_ldap_domains_task	Синхронизировать LDAP домен
delete_queryset	Удалить набор объектов
export_queryset	Экспортировать данные

продолжается на следующей странице

Таблица 44 – продолжение с предыдущей страницы

Параметр	Описание
run_inventory_report_collector	Собрать инвентарный отчёт
notify_reports_ready_collector	Уведомить о готовности отчётов
notify_about_ticket	Уведомить о тикете
notify_about_job_finish	Уведомить о завершении задания
flush_server_cache	Очистить кэш сервера
bulk_fetch_logs	Загрузить логи пачкой
run_peer_jobs_after_os_install	Запустить задания после установки ОС
session_record	Записать сессию
generate_manifest	Сгенерировать манифест

Примеры

1. Поместить событие some_task в очередь, где его подхватит воркер и выполнит

```
rude event some_task arg1 arg2
```

2. Очистить весь кэш серверов

```
rude event flush_server_cache
```

3. Синхронизировать LDAP домен

```
rude event sync_ldap_domains_task
```

4. Дебаг (просто проверить что очередь работает)

```
rude event debug
```

executor

Фоновый процесс-воркер — постоянно крутится на сервере и выполняет задачи из очереди

Зачем нужна

Команда запускает процесс-воркер, который и есть «исполнитель» сервера: он подхватывает задачи из очереди (UEM-задачи, синхронизация LDAP, фоновые операции) и исполняет их параллельно. Без работающего `executor` сервер не выполняет ни одну фоновую задачу — UEM перестаёт работать, плановые операции стоят на месте

В обычном режиме executor запущен под systemd как `rudesktop-executor.service`. Ручной запуск нужен для отладки, разовой обработки очереди или в специфичных сценариях

Типичные случаи применения:

- запуск дополнительной точки распространения (runner) на отдельной машине
- отладка обработки задач — запустить executor вручную в foreground, увидеть лог в реальном времени
- настройка интервала опроса (`--delay`) или режима LISTEN/NOTIFY (`--listen`) для оптимизации нагрузки на БД
- разовая обработка зависшей очереди после восстановления службы

Описание

Что происходит при старте

1. Находит себя в базе — ищет запись Runner по PUBLIC_HOST (hostname сервера). Если режим executor и записи нет — падает с ошибкой: «Точка распространения не найдена в админ-панели. Пожалуйста, создайте точку распространения...»
2. Записывает в Redis информацию о машине: ОС, количество CPU, RAM, версию rudesktop — это видно в интерфейсе администратора
3. Определяет количество воркеров (параллельных процессов):
    - Если в настройках Runner'а выставлено is_auto_forks = True — считает автоматически: (cpu_count - load_average) * 2.5
    - Если задано вручную (forks = 8) — использует это число

Основной цикл (бесконечный) каждую итерацию:

1. Запустить просроченные задачи по расписанию (Job.objects.due())
2. Взять задачи из очереди и выполнить их (пока есть)
3. Каждые ~8 минут — обновить метаинфо в Redis и пересчитать воркеры
4. Подождать –delay секунд (или событие NOTIFY от PostgreSQL)

Если Runner отключён в админке (enabled = False) — цикл пропускается, процесс спит 60 секунд и снова проверяет

Приоритеты задач

Задачи берутся из очереди по приоритету (сначала высокий), потом по времени создания:

- Критический - 10
- Высокий - 7
- Средний - 5
- Низкий (по умолчанию) - 0
- Принудительный запуск - 1000

Остановка

При Ctrl+C или SIGTERM — все задачи со статусом IN_PROGRESS текущего runner'а удаляются из очереди, затем процесс завершается

Синтаксис

```
rude executor [--delay DELAY] [--listen]
```

Параметры

Параметр	Описание
--delay	Количество секунд которое нужно подождать чтобы проверить наличие новых задач.
--listen	Используйте LISTEN/NOTIFY для ожидания событий.

Примеры

1. Просто запустить (проверяет очередь каждую секунду)

   ```
   rude executor
   ```

2. Проверять очередь каждые 5 секунд (меньше нагрузки на БД)

   ```
   rude executor --delay 5
   ```

3. Использовать PostgreSQL NOTIFY — реагировать мгновенно, без polling

   ```
   rude executor --listen
   ```

4. Комбинация: мгновенная реакция + резервный интервал 3 секунды

   ```
   rude executor --listen --delay 3
   ```

export

Экспорт сетевого графа

Зачем нужна

Команда выгружает граф связей объектов сервера (*Граф*) в один из машинно-читаемых форматов: `json`, `gexf` (Gephi) или `sif` (Cytoscape). Полученный файл можно открыть в специализированных инструментах визуализации и анализа графов — для расследования связей, поиска изолированных участков, построения отчётов

Типичные случаи применения:

- передача графа специалисту по безопасности или консультанту для анализа в стороннем инструменте
- построение визуализации в Gephi/Cytoscape для презентации или сложного отчёта
- регулярная выгрузка графа для последующего сравнения по версиям и поиска изменений
- интеграция с системами аналитики, понимающими графовые форматы

Синтаксис

```
rude export [--format {gexf,json,sif}] output
```

Параметры

Параметр	Описание
--format	Формат выгрузки варианты {gexfjsonsif}
output	Файл для экспорта сетевого графа

Примеры

Экспорт в файл `/tmp/django_graph.json` сетевого графа

```
rude export /tmp/django_graph.json
Exported to JSON file /tmp/django_graph.json
```

findstatic

Поиск абсолютных путей к заданным статическим файлам и вывод сообщения

Предупреждение

Служебная Django-команда. В рабочей инсталляции запуск, как правило, не требуется

Синтаксис

```
rude findstatic --first staticfile
```

Параметры

Параметр	Описание
--first	Возвращает только первое совпадение для каждого статического файла
staticfile	Имя файла для поиска пути

Примеры

Найти и вывести сообщение к абсолютным путям к файлу `/tmp/rude`

Служебная команда сервера не применяется пользователем в Linux-консоли

```
rude findstatic /tmp/rude
```

fix_groups

Исправление символов в названиях CN\DN путях для аккаунтов импортированных из LDAP-каталога

Зачем нужна

Команда нормализует пути CN/DN в учётных записях, импортированных из LDAP/AD: исправляет неэкранированные или некорректно сохранённые символы, из-за которых поиск, привязка к группам или повторная синхронизация могут отрабатывать неправильно

Типичные случаи применения:

- разовая чистка после первичного импорта из доменов с нестандартными символами (кириллица, скобки, запятые в OU)
- восстановление корректных DN после миграции с одной версии сервера на другую
- разбор обращения «после синхронизации часть пользователей не привязалась к группе» — fix_groups часто решает проблему

Синтаксис

```
rude fix_groups
```

Примеры

Служебная команда сервера не применяется пользователем в Linux-консоли

flush

Удаление всех данных из БД включая данные добавленные во время миграций

Предупреждение

Деструктивная команда. Удаляет все данные из базы сервера, операция необратима. Не запускайте на работающем сервере и обязательно создайте *резервную копию* перед использованием. Команда служебная (Django) — для повседневной работы не применяется

Синтаксис

```
rude flush
```

Параметры

Параметр	Описание
--noinput	Указывает Django НЕ запрашивать у пользователя ввод каких-либо данных
--database	Указывает базу данных для очистки. По умолчанию используется база данных «default»

Примеры

```
rude flush
You have requested a flush of the database.
This will IRREVERSIBLY DESTROY all data currently in the
 ↪"rudesktop" database,
and return each table to an empty state.
Are you sure you want to do this?

Type 'yes' to continue, or 'no' to cancel: no
Flush cancelled.
```

Команда нужна для очистки сервера от накопленных данных. В данном примере была выбрана опция - «no», т.е. не стирать все данные

Важно

Команда уничтожает все данные на сервере, не запускайте её никогда, если сервер находится в работе

generateschema

Генерация настроенной схемы API для проекта

Предупреждение

Служебная Django-команда. Для получения готовой OpenAPI-схемы сервера используйте встроенные эндпоинты — см. *API*

Синтаксис

```
rude generateschema [--title TITLE] [--url URL] [--description␣
↪DESCRIPTION] [--format {openapi,openapi-json}] [--urlconf␣
↪URLCONF] [--generator_class GENERATOR_CLASS] [--file FILE] [--
↪api_version API_VERSION]
```

Параметры

Параметр	Описание
--title	Название
--url	URL-адрес
--description	Описание
--format	Формат генерации схемы варианты {openapi\openapi-json}
--urlconf	Ссылка на конфигурацию
--generator_class	Класс для генератора схемы
--file	Вывод в файл по пути
--api_version	Версия API которую нужно

Примеры

Служебная команда сервера не применяется пользователем в Linux-консоли

genmodels

Генерация моделей и перечислений для модуля аудита

Предупреждение

Служебная команда — нужна только разработчикам **RuDesktop** при изменении схемы CEF-полей аудита. В рабочей инсталляции запуск не требуется

Синтаксис

```
rude genmodels
```

Примечание

Команда читает константы `SEVERITY`, `EVENTS`, `SIGNATURES` и `EXTENSIONS` из `audit/enums.py` и печатает в стандартный вывод исходный код Python с моделью `GeneratedLogEvent`, перечислениями и полями CEF. Используется при разработке для регенерации файла `audit/generated.py`

Примеры

Перенаправить вывод в файл:

```
rude genmodels > /tmp/generated.py
```

Служебная команда сервера, обычно не применяется пользователем в Linux-консоли — нужна только разработчикам при изменении схемы CEF-полей аудита

inspectdb

Проверка таблиц в указанной БД и вывод информации о модуле модели Django

Предупреждение

Служебная Django-команда — генерирует модели по структуре БД. В рабочей инсталляции запуск, как правило, не требуется

Синтаксис

```
rude inspectdb [--database {default}] [--include-partitions] [--
↪include-views]
```

Параметры

Параметр	Описание
--database	Указывает базу данных для проверки. По умолчанию используется база данных «default»
--include-partitions	Также выводит модели для таблиц разделов
--include-views	Также выводит модели для представлений базы данных
table	Выбирает какие таблицы или представления следует проверить

Примеры

Вывод информации о таблице «upload_file»

```
rude inspectdb upload_file
# This is an auto-generated Django model module.
# You'll have to do the following manually to clean this up:
#   * Rearrange models' order
#   * Make sure each model has one field with primary_key=True
#   * Make sure each ForeignKey and OneToOneField has `on_delete`␣
 ↪set to the desired behavior
#   * Remove `managed = False` lines if you wish to allow Django to␣
 ↪create, modify, and delete the table
# Feel free to rename the models, but don't rename db_table values␣
 ↪or field names.
from django.db import models

class UploadFile(models.Model):
    guid = models.CharField(unique=True, max_length=40)
    created = models.DateTimeField()
    uploaded_file = models.CharField(max_length=255)
    original_filename = models.CharField(max_length=1024)
    repository = models.ForeignKey('UploadRepository',␣
 ↪models.DO_NOTHING, blank=True, null=True)
    sha1_sum = models.CharField(max_length=40, blank=True,␣
 ↪null=True)

    class Meta:
        managed = False
        db_table = 'upload_file'
```

loaddata

Установка указанных фикстур в БД

Предупреждение

Служебная Django-команда. Для штатного восстановления базы используйте *restore* — она работает с дампами **PostgreSQL**, формируемыми командой *backup*

Синтаксис

```
rude loaddata [--database {default}] [--app APP_LABEL] [--
↪ignorenonexistent] [-e EXCLUDE] [--format FORMAT] [--keep_fields␣
↪KEEP_FIELDS [KEEP_FIELDS ...]]
```

Параметры

Параметр	Описание
--database	Указывает конкретную базу данных для загрузки фикстур. По умолчанию используется база данных «default»
--app	Искать фикстуры только в указанном приложении
--ignorenonexistent	Игнорирует записи в сериализованных данных для полей которые в данный момент отсутствуют в модели
--exclude	Метка приложения или app_label.ModelName для исключения. Может использоваться несколько раз
--format	Формат сериализованных данных при чтении из стандартного ввода
--keep_fields	Поля для пропуска при загрузке фикстур

Примеры

Служебная команда - используется для загрузки фикстур в БД сервера для приложения Django

makemessages

Извлечение строк для перевода в .po-файлы (обёртка над Django `makemessages` для русской локали)

Предупреждение

Служебная команда — нужна только разработчикам **RuDesktop** при добавлении новых строк для перевода. В рабочей инсталляции запуск не требуется

Синтаксис

```
rude makemessages
```

Параметры

Параметр	Описание
-l LOCALE	Локаль (например -l en)
-d DOMAIN	Домен (django или djangojs)
-a	Все локали
-e EXT	Расширения файлов для поиска
-i PATTERN	Игнорировать паттерн/директорию
--no-wrap	Не переносить строки в .po
--no-location	Не добавлять комментарии с путями
-s / --symlinks	Использовать симлинки
--keep-pot	Сохранять .pot файл

Примечание

Команда выполняет последовательность действий:

1. Создаёт временные симлинки на пакеты `constance` и `import_export`
2. Запускает `manage.py makemessages -l ru -i env -i gui -s` для извлечения строк Python/HTML
3. Запускает `manage.py makemessages -d djangojs -l ru -i env -i gui -s` для извлечения строк JavaScript
4. Копирует переводы из `constance` и `import_export` в `locale3party/`
5. Удаляет временные симлинки

Поддерживается **только русская локаль** (`-l ru`)

Примеры

Служебная команда сервера, не применяется пользователем в Linux-консоли — нужна разработчикам при добавлении новых строк для перевода

makemigrations

Создание новых миграций для приложений

Предупреждение

Служебная команда — нужна только разработчикам **RuDesktop** при изменении моделей данных. В рабочей инсталляции запуск не требуется и может привести к рассинхронизации схемы БД с кодом сервера

Синтаксис

```
rude makemigrations [--dry-run] [--merge] [--empty] [--noinput] [-n␣
↪NAME] [--no-header] [--check] [--scriptable] [--update] app_label
```

Параметры

Параметр	Описание
--dry-run	Показать какие миграции будут созданы; фактически не записывать их.
--merge	Включить исправление конфликтов миграций.
--empty	Создать пустую миграцию.
--noinput	Указывает Django НЕ запрашивать у пользователя ввод каких-либо данных.
--name	Использовать это имя для файла(ов) миграции.
--no-header	Не добавлять комментарии заголовка к новым файлам миграции.
--check	Выйти с ненулевым статусом если изменения модели не содержат миграций и фактически не записывают их. Подразумевает –dry-run.
--scriptable	Перенаправлять вывод логов и запросы ввода в stderr - записывая в stdout только пути к сгенерированным файлам миграций.
--update	Объединить изменения модели с последней миграцией и оптимизировать соответствующие операции.
app_label	Указывает метку(и) приложения(й) для которого(ых) нужно создать миграции.

Примеры

Служебная команда сервера не применяется пользователем в Linux-консоли

migrate

Применение миграций схемы БД (стандартная команда Django)

Зачем нужна

Команда применяет к БД ожидающие миграции — изменения структуры таблиц, индексы, добавление/удаление полей. Без свежих миграций сервер новой версии не работает корректно. Обычно команда вызывается автоматически инсталлятором; ручной запуск нужен при нестандартных сценариях

Типичные случаи применения:

- ручной запуск миграций после восстановления базы из старого *backup* при работающем новом сервере
- применение миграций отдельного приложения после ручного вмешательства в БД
- `--plan` — посмотреть, какие миграции будут применены, без записи (аудит перед обновлением)
- откат миграций приложения до конкретной (например, при откате версии сервера)

Важно

Перед запуском обязательно сделайте *резервную копию* базы. Откат миграций может быть невозможен или приведёт к потере данных, добавленных после применения новой схемы

Синтаксис

```
rude migrate [--noinput] [--database {default}] [--fake] [--
↪fake-initial] [--plan] [--run-syncdb] [--check] [--prune]␣
↪[app_label] [migration_name]
```

Примечание

Применяет ожидающие миграции к базе данных. Без параметров мигрирует все приложения. Используется при обновлении сервера и установке. Полную документацию см. в Django docs[11]

[11] https://docs.djangoproject.com/en/stable/ref/django-admin/#migrate

Примеры

Применить все миграции:

```
rude migrate
```

Применить миграции конкретного приложения:

```
rude migrate account
```

Откатить миграции приложения до определённой:

```
rude migrate account 0010_some_migration
```

Служебная команда сервера, обычно вызывается автоматически при установке/обновлении

oauth_app

Создание и получение OAuth-приложения

> **Важно**
>
> Команда требует активной лицензии **UEM**. При её отсутствии команда завершится с сообщением «Недостаточный уровень лицензии: для создания необходим UEM»

Зачем нужна

Команда — обёртка над стандартным *createapplication*, заточенная под идемпотентную работу: при `--if-not-exists` повторный запуск не создаёт дубликат, а только обновляет `redirect_uris` у существующего приложения. Подкоманда `get` возвращает данные приложения по имени

Типичные случаи применения:

- скрипты развёртывания, которые могут перезапускаться многократно — нужен предсказуемый «создать, если ещё нет»
- автоматизация на CI/CD, где регистрация OAuth-клиентов идёт в составе пайплайна
- `get` — получить `client_id` / `client_secret` существующего приложения, чтобы передать его внешней системе

Синтаксис

```
rude oauth_app create [--client-id CLIENT_ID] [--user USER] [--
↪redirect-uris REDIRECT_URIS]
                      [--post-logout-redirect-uris␣
↪POST_LOGOUT_REDIRECT_URIS]
                      [--client-secret CLIENT_SECRET] [--
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
↪no-hash-client-secret]
                      [--name NAME] [--skip-authorization] [--
↪algorithm ALGORITHM]
                      [--if-not-exists] client_type␣
↪authorization_grant_type
rude oauth_app get --name [name]
```

Параметры

Параметр	Описание
create	Создать новое приложение OAuth
client_type	Тип клиента один из: конфиденциальный или публичный
authorization_grant_type	Тип используемого предоставления авторизации один из: {authorization-code urn: ietf:params:oauth:grant-type:device_code implicit password client-credentials openid-hybrid}
--client-id CLIENT_ID	ID нового приложения
--user USER	Пользователь которому принадлежит приложение
--redirect-uris REDIRECT_URIS	URI перенаправления (должны быть строками разделенными пробелами например: „URI1 URI2“)
--post-logout-redirect-uris POST_LOGOUT_REDIRECT_URIS	URI перенаправления после выхода из системы (должны быть строками разделенными пробелами например: „URI1 URI2“)
--client-secret CLIENT_SECRET	Секрет для этого приложения
--no-hash-client-secret	Не хешировать секрет клиента
--name NAME	Имя этого приложения
--skip-authorization	Если установлено полностью пропускать форму авторизации даже при первом использовании приложения
--algorithm ALGORITHM	Алгоритм подписи токена OIDC для этого приложения (один из: RS256 HS256)
get	Получить существующее приложение OAuth
name	Имя приложения для получения

Примечание

Подкоманда `create` наследует флаги стандартной команды `createapplication` из `django-oauth-toolkit` и добавляет флаг

`--if-not-exists`: если приложение с таким `client_id` или `name` уже существует, новое не создаётся, а у существующего обновляется только `redirect_uris`

Подкоманда `get` возвращает данные приложения по его имени (через `--name`)

Примеры

Служебная команда сервера, обычно не применяется пользователем в Linux-консоли — используется в скриптах развёртывания

optimizemigration

Оптимизация операций для указанной миграции

Предупреждение

Служебная Django-команда — нужна разработчикам при оптимизации файлов миграций. В рабочей инсталляции запуск не требуется

Синтаксис

```
rude optimizemigration app_label migration_name
```

Параметры

Параметр	Описание
app_label	Метка приложения для которого оптимизируется миграция.
migration_name	Имя миграции для которой оптимизируются операции.

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

playbook

Запуск указанного playbook на исполнение

Зачем нужна

Команда напрямую запускает Ansible-playbook из каталога `/var/lib/rudesktop/playbooks/` — низкоуровневый аналог *policy run* и *job run*. По умолчанию выполняется на всех онлайн-устройствах, как «Тестовый запуск» в веб-интерфейсе

Типичные случаи применения:

- отладка проблемного playbook — запустить вручную, посмотреть подробный вывод Ansible
- разовый запуск политики в обход стандартного механизма задач
- проверка корректности генерации playbook'а после изменения шаблона политики
- воспроизведение проблемы для разбора с технической поддержкой

Синтаксис

```
rude playbook /
↪var/lib/rudesktop/playbooks/job_1002_инвентаризация.yaml
```

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

Важно

Если не передаются параметры команды, то команда запускается с множеством параметров по умолчанию на исполнение для всех АРМ в онлайне, аналогично запуску политики в тестовом режиме на все АРМ в веб-консоли сервера на странице «UEM - Политики - выбрать_политику - вкладка Тестовый запуск»

provise

Django-команда для генерации конфигурационных файлов для PXE-сервера

Важно

Подготавливает настройки для автоматической сетевой установки ОС (Windows/Linux) на компьютеры — создаёт конфиги с параметрами: домен, IP сервера, язык, логин/пароль администратора, тип ОС, часовой пояс

Зачем нужна

Команда генерирует полный набор конфигов, скриптов и файлов автоответов для PXE-инфраструктуры **RuDesktop** — автоматической сетевой установки ОС на чистое железо. На вход берутся параметры (домен сервера, тип ОС, локаль, учётка администратора, часовой пояс, ID образа), на выходе — готовые `smb.conf`, `answers_*.xml`, `preseed.cfg`, `ks.cfg`, скрипты iPXE и постустановки

Типичные случаи применения:

- первичная настройка PXE-сервера для массовой раскатки ОС в филиалах
- регенерация конфигов после смены домена, IP сервера или параметров образа ОС
- автоматизация: вызов из скрипта развёртывания, который потом заливает результат в каталог PXE
- разовая генерация конфигов под нестандартный образ ОС

Синтаксис

```
rude provise cfg
```

Параметры

Параметр	Описание
--root	Папка куда сохранять конфиги
--public_host	IP сервера (для подключения клиентов)
--domain	Домен и порт сервера
--os_type	Тип ОС
--admin_password	Пароль администратора
--lang	ru-RU
--timezone	Europe/Moscow
--admin_login	Администратор
--os_image_id	None

Пример

Пример вызова (как в publish):

```
rude provise cfg \
  --root /var/lib/rudesktop/pxe \
  --domain myserver.com:443 \
  --public_host 192.168.1.10 \
  --lang "RU-ru" \
  --admin_login "Администратор" \
  --admin_password "P@ssw0rd" \
  --os_type WINDOWS10 \
  --timezone Europe/Moscow \
  --os_image_id 42
```

Что генерирует:

- `smb.conf` — настройки Samba (Windows-шара с образом)
- `answers_uefi.xml`, `answers_mbr.xml` — файлы автоответов для установки Windows
- `autoexec.ipxe` — скрипт загрузки по сети (iPXE)
- `preseed.cfg`, `preseed-astra-1-8.yaml` — автоустановка Debian/Astra Linux
- `ks.cfg` — kickstart для RedHat/Alt Linux
- `bootstrap.sh`, `install.bat`, `setupComplete.ps1` — скрипты после установки

remove_stale_contenttypes

Удаление устаревших типов контента из БД

Зачем нужна

Команда удаляет из таблицы `django_content_type` записи, которые больше не соответствуют ни одной модели в текущей версии сервера. Со временем после обновлений и рефакторингов в этой таблице остаются «висячие» записи — они не вредят, но засоряют БД и могут мешать восстановлению из бэкапа на новой версии

Типичные случаи применения:

- разовая чистка после серии обновлений сервера, в ходе которых удалялись или переименовывались модели
- подготовка БД к миграции на новую версию или другой сервер
- разрешение конфликтов content_type после ручного вмешательства в БД

Синтаксис

```
rude remove_stale_contenttypes [--noinput] [--database {default}] [-
↪-include-stale-apps]
```

Параметры

Параметр	Описание
--noinput	Указывает Django НЕ запрашивать у пользователя ввод каких-либо данных
--database {default}	Указывает используемую базу данных. По умолчанию используется база данных «default»
--include-stale-apps	Удаляет устаревшие типы контента включая те что были удалены из INSTALLED_APPS ранее установленных приложений

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

run_job

Синхронный запуск конкретной задачи по её ID

Зачем нужна

Команда выполняет конкретную UEM-задачу **синхронно** в текущем процессе, дожидаясь её завершения. В отличие от *job run*, который ставит задачу в очередь и завершается, `run_job` блокируется до конца выполнения и возвращает результат сразу

Типичные случаи применения:

- скрипты автоматизации, которым нужно дождаться окончания задачи и продолжить работу с её результатом
- тестирование новой задачи в контролируемом окружении — увидеть полный вывод без переключения на логи executor'а
- разовый запуск нескольких задач строго последовательно (передача нескольких ID)

Синтаксис

```
rude run_job [--update_heartbeat 0|1] job_id [job_id ...]
```

Параметры

Параметр	Описание
--update_heartbeat UPDATE_HEARTBEAT	Если указан параметр запускает поток для асинхронного обновления статуса пульса задачи

Примечание

Команда работает синхронно — ожидает завершения задачи, в отличие от планового запуска через `executor`. Задача не запустится, если она уже выполняется в данный момент

Примеры

Запустить одну задачу:

```
rude run_job 1002
```

Запустить несколько задач последовательно:

```
rude run_job 1001 1002 1003
```

Отключить асинхронное обновление heartbeat:

```
rude run_job 1002 --update_heartbeat 0
```

Служебная команда сервера, обычно не применяется пользователем в Linux-консоли — для штатного запуска задач используйте *job run*

runserver

Запуск легковесного веб-сервера для разработки

Предупреждение

Служебная Django-команда для разработки. Не предназначена для production и не должна использоваться в рабочей инсталляции — запуск веб-части осуществляется службой `rudesktop-web.service` под управлением **Gunicorn**

Синтаксис

```
rude runserver [--nothreading] [--noreload] [--nostatic] [--
↪insecure] addrport
```

Параметры

Параметр	Описание
addrport	Необязательный номер порта или ipaddr:port
--nothreading	Указывает Django НЕ использовать многопоточность
--noreload	Указывает Django НЕ использовать автоматическую перезагрузку
--nostatic	Указывает Django НЕ обслуживать статические файлы по STATIC_URL
--insecure	Разрешает обслуживание статических файлов даже если DEBUG равно False

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли. Запускает сервер Django, для быстрой проверки работы изменённых файлов проекта.

```
rude runserver
Performing system checks...

System check identified no issues (0 silenced).
February 19, 2026 - 21:36:27
Django version 5.2.11, using settings 'rudesktop.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.

WARNING: This is a development server. Do not use it in a␣
↪production setting. Use a production WSGI or ASGI server instead.
For more information on production servers see:␣
↪https://docs.djangoproject.com/en/5.2/howto/deployment/
```

sendtestemail

Отправка тестового письма на указанные в качестве аргументов адреса электронной почты

Зачем нужна

Команда отправляет тестовое письмо через настроенный SMTP-сервер. Самый быстрый способ проверить, что параметры почты в *Настройках* корректны, до того как сервер начнёт рассылать настоящие уведомления, инвайты и пароли

Типичные случаи применения:

- проверка SMTP-настроек после первичной установки или их изменения
- диагностика обращения «не получаю письма от RuDesktop» — определить, кто виноват: сервер или почтовая инфраструктура
- `--admins` / `--managers` — отправить тест на адреса из соответствующих секций `settings.py` (проверка списков получателей)

Синтаксис

```
rude sendtestemail [--managers] [--admins] email
```

Параметры

Параметр	Описание
email	Один или несколько адресов электронной почты для отправки тестового письма
--managers	Отправляет тестовое письмо на адреса указанные в settings.MANAGERS
--admins	Отправляет тестовое письмо на адреса указанные в settings.ADMINS

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

set_option

Установка значения опции в нативной библиотеке `libpydesktop`

Зачем нужна

Команда настраивает параметры **нативного** компонента сервера `libpydesktop` — отдельной C++ библиотеки, обслуживающей протокол **RuDesktop**. У неё свой набор опций, недоступных через `rude constance` (тот работает с Django-настройками)

Типичные случаи применения:

- разовая настройка нативного компонента в нестандартной инсталляции — обычно вызывается автоматически в *install* и *setup_server*
- разрешить самоподписной сертификат на тестовом стенде (`danger-accept-invalid-cert Y`)
- ручная корректировка конфигурации после миграции, если установщик не отработал нужный шаг

Синтаксис

```
rude set_option [key] [value]
```

Параметры

Параметр	Описание
key	Параметр для установки
value	Значение параметра для установки

Примечание

Команда вызывает `libpydesktop.set_option(key, value)`. Используется при установке сервера и настройке точек распространения для применения параметров (например, `danger-accept-invalid-cert Y`)

Примеры

Служебная команда сервера, обычно не применяется пользователем в Linux-консоли. Применяется автоматически в скриптах `install` и `setup_server`

```
rude set_option danger-accept-invalid-cert Y
  Set option danger-accept-invalid-cert = Y
```

shell

Интерактивный Python REPL в окружении Django-проекта (стандартная команда Django)

Предупреждение

Служебная команда. Прямые ORM-операции в работающей БД могут нарушить целостность данных — используйте только для диагностики и под root, обязательно сделав *резервную копию* перед изменениями

Синтаксис

```
rude shell
```

Примечание

После запуска Python-окружение Django загружено: можно работать с моделями, выполнять ORM-запросы, отлаживать. Используется для разовых административных операций и диагностики

Примеры

Запустить Python-shell сервера:

```
rude shell
```

После запуска можно работать с моделями:

```
>>> from peers.models import Server
>>> Server.objects.count()
42
>>> from account.models import User
>>> User.objects.filter(is_active=False).count()
3
```

Служебная команда сервера, нужна разработчикам и для отладочных операций

showmigrations

Отображения всех доступных миграции для текущего проекта

Зачем нужна

Команда показывает список всех миграций приложений сервера и отметку «применена/не применена» ([X] / [ ]). Используется для аудита состояния схемы БД до и после *migrate*, особенно при разборе неудачных обновлений

Типичные случаи применения:

- проверка после обновления сервера, что все ожидаемые миграции применились
- разбор инцидента «после обновления что-то не работает» — найти миграцию, которая не применилась
- `--plan` — посмотреть план применения миграций перед запуском *migrate*
- сравнение состояния миграций между несколькими серверами при отладке

Синтаксис

```
rude showmigrations [--database {default}] [--list | --plan]␣
↪app_label
```

Параметры

Параметр	Описание
app_label	Метки приложений для которых следует ограничить вывод
--database {default}	Указывает базу данных для отображения миграций. По умолчанию используется база данных «default»
--list	-l - Отображает список всех миграций и примененных миграций. При уровне детализации 2 или выше будут включены примененные даты и время
--plan	-p Отображает все миграции в порядке их применения. При уровне детализации 2 или выше будут включены все прямые зависимости миграций и обратные зависимости (run_before)

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли.

```
rude showmigrations
account
 [X] 0001_initial
 [X] 0002_group_ad_group
 [X] 0003_auto_20221114_1921
 [X] 0004_auto_20221117_1223
 ...
```

spectacular

Создание схемы для API соответствующую стандарту OpenAPI3

Важно

- Предупреждения служат индикатором того, где ваш API не может быть корректно разрешен. @extend_schema и @extend_schema_field — ваши лучшие помощники
- Спецификация должна быть корректной в любом случае

- Не забудьте настроить метаданные ваших API, такие как серверы, версия, URL, документация и так далее, в вашем файле SPECTACULAR_SETTINGS.»

Зачем нужна

Команда генерирует машинно-читаемое описание HTTP-API сервера в формате **OpenAPI 3** (YAML или JSON). Полученную схему можно скормить генератору SDK, импортировать в Postman/Insomnia или использовать как контракт для интеграции

Типичные случаи применения:

- получение актуальной схемы API установленного сервера для интеграции внешней системы
- генерация клиентского SDK на нужном языке программирования
- импорт API в инструмент тестирования (Postman, Insomnia) для сценариев QA
- сверка контракта API между версиями сервера при обновлении

Синтаксис

```
rude spectacular [--format {openapi,openapi-json}] [--urlconf␣
↪URLCONF] [--generator-class GENERATOR_CLASS] [--file FILE] [--
↪fail-on-warn] [--validate] [--api-version API_VERSION] [--lang␣
↪LANG] [--color] [--custom-settings CUSTOM_SETTINGS]
```

Параметры

Параметр	Описание
--format	Вариант генерации (openapi или openapi-json)
--urlconf	Ссылка на ваш URL-сайта
--generator-class	GENERATOR_CLASS
--file	Файл для экспорта
--fail-on-warn	
--validate	
--api-version	Версия API
--lang	LANG
--color	
--custom-settings	CUSTOM_SETTINGS

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли используется разработчиками для генерации схем API в приложении

sqlflush

Получение списка SQL-запросов необходимых для восстановления всех таблиц в БД до состояния в котором они находились сразу после установки

Предупреждение

Служебная Django-команда. Команда только показывает SQL — но если выполнить полученные запросы вручную, **все данные сервера будут удалены безвозвратно**

Синтаксис

```
rude sqlflush
```

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

sqlmigrate

Вывод SQL-запросов для указанной миграции

Предупреждение

Служебная Django-команда — нужна разработчикам для просмотра SQL миграций. В рабочей инсталляции запуск, как правило, не требуется

Синтаксис

```
rude sqlmigrate [--database {default}] [--backwards] app_label␣
↪migration_name
```

Параметры

Параметр	Описание
app_label	метка приложения содержащего миграцию
migration_name	имя миграции для которой нужно вывести SQL-запросы
--database {default}	указывает базу данных для создания SQL-запросов. По умолчанию используется база данных «default»
--backwards	создает SQL-запросы для отмены миграции а не для ее применения

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

sqlsequencereset

Вывод SQL-запросов для сброса последовательностей для указанных имен приложения

Предупреждение

Служебная Django-команда. В рабочей инсталляции запуск, как правило, не требуется

Синтаксис

```
rude sqlsequencereset app_label
```

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

squashmigrations

Объединение существующих наборов миграций в одну новую

Предупреждение

Служебная команда — нужна разработчикам **RuDesktop** при оптимизации цепочки миграций. В рабочей инсталляции запуск не требуется и может привести к рассинхронизации схемы БД с кодом сервера

Синтаксис

```
rude squashmigrations [--no-optimize] [--noinput] [--squashed-name␣
↪SQUASHED_NAME] [--no-header] app_label start_migration_name␣
↪migration_name
```

Параметры

Параметр	Описание
app_label	Метка приложения для которого нужно объединить миграции
start_migration_name	Миграции будут объединены начиная с этой миграции и включая ее
migration_name	Миграции будут объединены до этой миграции включительно
--no-optimize	Не пытаться оптимизировать сжатые операции
--noinput (–no-input)	Указывает Django НЕ запрашивать у пользователя ввод каких-либо данных
--squashed-name SQUASHED_NAME	Задает имя новой сжатой миграции

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

startapp

Создание структуры каталогов приложения Django для заданного имени приложения в текущем каталоге или при необходимости в указанном каталоге

Предупреждение

Служебная Django-команда — нужна разработчикам при создании нового приложения внутри проекта **RuDesktop**. В рабочей инсталляции запуск не требуется

Синтаксис

```
rude startapp [--template TEMPLATE] [--extension EXTENSIONS] [--
↪name FILES] [--exclude [EXCLUDE]]
```

Параметры

Параметр	Описание
name	Имя приложения или проекта
directory	Необязательный целевой каталог
--template	Путь или URL-адрес для загрузки шаблона
--extension EXTENSIONS	Расширение(я) файла(ов) для рендеринга (по умолчанию: «py»). Разделяйте несколько расширений запятыми или используйте -e несколько раз
--name FILES	Имя(имена) файла(ов) для рендеринга. Разделяйте несколько имен файлов запятыми или используйте -n несколько раз
--exclude [ИСКЛЮЧИТЬ]	Имя(имена) каталога(ов) для исключения помимо .git и __pycache__. Может использоваться несколько раз

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

startproject

Создание структуры каталогов проекта Django для заданного имени проекта в текущем каталоге или при необходимости в указанном каталоге

Предупреждение

Служебная Django-команда — нужна разработчикам при инициализации нового Django-проекта. В рабочей инсталляции запуск не требуется

Синтаксис

```
rude startproject
```

Параметры

Параметр	Описание
name — имя приложения или проекта	

продолжается на следующей странице

Таблица 67 – продолжение с предыдущей страницы

Параметр	Описание
directory — необязательный целевой каталог	
--template TEMPLATE	Путь или URL-адрес для загрузки шаблона
--extension EXTENSIONS	Расширение(я) файла(ов) для рендеринга (по умолчанию: «py»). Разделяйте несколько расширений запятыми или используйте -e несколько раз
--name FILES	Имя(имена) файла(ов) для рендеринга. Разделяйте несколько имен файлов запятыми или используйте -n несколько раз
--exclude ИСКЛЮЧИТЬ	Имя(имена) каталога(ов) для исключения помимо .git и __pycache__. Может использоваться несколько раз

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

test

Обнаружение и запуск тестов в указанных модулях или текущем каталоге

Предупреждение

Служебная Django-команда — запускает unit-тесты в окружении сервера и создаёт временную тестовую БД. В рабочей инсталляции запуск не требуется

Синтаксис

```
rude test [--noinput] [--testrunner TESTRUNNER] [--failfast] [-t␣
↪TOP_LEVEL] [-p PATTERN] [--keepdb] [--shuffle [SEED]] [-r] [--
↪debug-mode] [-d] [--parallel [N]] [--tag TAGS] [--exclude-tag␣
↪EXCLUDE_TAGS] [--pdb] [-b] [--no-faulthandler] [--timing] [-k␣
↪TEST_NAME_PATTERNS] test_label
```

Параметры

Параметр	Описание
test_label	Пути к модулям для тестирования; может быть modulename (modulename.TestCase) или (modulename.TestCase.test_method)
--noinput	Указывает Django НЕ запрашивать у пользователя ввод каких-либо данных
--testrunner TESTRUNNER	Указывает Django использовать указанный класс запуска тестов вместо класса указанного в параметре TEST_RUNNER
--failfast	Останавливает набор тестов после первой ошибки
--top-level-directory TOP_LEVEL	Верхний уровень проекта для обнаружения модульных тестов
--pattern PATTERN	Шаблон соответствия тестов. По умолчанию test*.py
--keepdb	Сохраняет базу данных тестов между запусками
--shuffle [SEED]	Перемешивает порядок тестовых случаев
--reverse	Изменяет порядок тестовых случаев на обратный
-debug-mode	Устанавливает settings. DEBUG в значение True
--debug-sql	Выводит в лог SQL-запросы при сбое
-parallel [N]	Запускает тесты используя до N параллельных процессов. Используйте значение «auto» чтобы запустить один тестовый процесс для каждого ядра процессора
-tag TAGS	Запускает только тесты с указанным тегом. Может использоваться несколько раз
-exclude-tag EXCLUDE_TAGS	Не запускает тесты с указанным тегом. Может использоваться несколько раз
-pdb	Запускает отладчик (pdb или ipdb если установлен) при ошибке или сбое
--buffer	Отбрасывает вывод от прошедших тестов
--no-faulthandler	Отключает модуль обработки ошибок Python во время тестов
--timing	Выводит время выполнения включая время настройки базы данных и общее время выполнения

продолжается на следующей странице

Таблица 68 – продолжение с предыдущей страницы

Параметр	Описание
-k TEST_NAME_PATTERNS	Запускать только тестовые методы и классы соответствующие шаблону или подстроке. Можно использовать несколько раз. Аналогично опции unittest -k

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

testserver

Запуск сервера для разработки с данными из указанных фикстур

Предупреждение

Служебная Django-команда для разработки. Не предназначена для production — в рабочей инсталляции запуск не требуется

Синтаксис

```
rude testserver [--noinput] [--addrport ADDRPORT] [--ipv6] fixture
```

Параметры

Параметр	Описание
fixture	Путь(и) к фикстурам которые необходимо загрузить перед запуском сервера
--noinput	Указывает Django НЕ запрашивать у пользователя ввод каких-либо данных
--addrport ADDRPORT	Номер порта или IP-адрес:порт для запуска сервера
--ipv6	Указывает Django использовать IPv6-адрес

Примеры

Служебная команда сервера обычно не применяется пользователем в Linux-консоли

Действия с дополнительными командами сервера — расширенные **Django**-команды и обслуживающие команды: миграции, обслуживание базы данных и кэша, сброс токенов и сессий, диагностика, локализация, тестирование, генерация схемы API и другие низкоуровневые операции

Команда	Описание
analyze	Анализ списков на наличие в нём IP-адресов из файла или лога
check	Проверка всего проекта Django на наличие потенциальных проблем
clearsessions	Очистка сессий с истекшим сроком годности
cleartokens	Очистка просроченных токенов
client	Установка клиента RuDesktop по ssh
compilemessages	Компиляция po-файлов в mo-файлы для использования со встроенной поддержкой gettext
createapplication	Создание нового приложения программным способом
createcachetable	Создание таблицы необходимые для использования кэша SQL
dbshell	Запуск клиента командной строки для указанной базы данных или базу данных по умолчанию если она не указана
delete	Очистка устройств по дате последней активности на сервере
diffsettings	Отображение различия между текущим файлом settings.py и настройками Django по умолчанию
drf_create_token	Создание токена DRF для заданного пользователя
dumpdata	Вывод содержимого базы данных в виде фикстуры заданного формата
event	Django-команда которая кидает событие в очередь задач
executor	Фоновый процесс-воркер — постоянно крутится на сервере и выполняет задачи из очереди
export	Экспорт сетевого графа
findstatic	Поиск абсолютных путей к заданным статическим файлам и вывод сообщения
fix_groups	Исправление символов в названиях CN\DN путях для аккаунтов импортированных из LDAP-каталога
flush	Удаление всех данных из БД включая данные добавленные во время миграций

продолжается на следующей странице

Таблица 70 – продолжение с предыдущей страницы

Команда	Описание
generateschema	Генерация настроенной схемы API для проекта
genmodels	Создание моделей аудита и перечислений
inspectdb	Проверка таблиц в указанной БД и вывод информации о модуле модели Django
loaddata	Установка указанных фикстур в БД
makemessages	Утилита для генерации PO-файлов с переводом на национальный язык с эталонного образца для каждого элемента приложения
makemigrations	Создание новых миграций для приложений
migrate	Применение миграций для приложений
oauth_app	Создание нового приложения программным способом
optimizemigration	Оптимизация операций для указанной миграции
playbook	Запуск указанного playbook на исполнение
provise	Django-команда для генерации конфигурационных файлов для PXE-сервера
remove_stale_contenttypes	Удаление устаревших типов контента из БД
run_job	Запуск конкретной задачи по её ID в БД сервера
runserver	Запуск легковесного веб-сервера для разработки
sendtestemail	Отправка тестового письма на указанные в качестве аргументов адреса электронной почты
set_option	Установка значений для переменной
shell	Вход в терминал Python в окружении сервера
showmigrations	Отображения всех доступных миграции для текущего проекта
spectacular	Создание схемы для API соответствующую стандарту OpenAPI3
sqlflush	Получение списка SQL-запросов необходимых для восстановления всех таблиц в БД до состояния в котором они находились сразу после установки
sqlmigrate	Вывод SQL-запросов для указанной миграции

продолжается на следующей странице

Таблица 70 – продолжение с предыдущей страницы

Команда	Описание
sqlsequencereset	Вывод SQL-запросов для сброса последовательностей для указанных имен приложения
squashmigrations	Объединение существующих наборов миграций в одну новую
startapp	Создание структуры каталогов приложения Django для заданного имени приложения в текущем каталоге или при необходимости в указанном каталоге
startproject	Создание структуры каталогов проекта Django для заданного имени проекта в текущем каталоге или при необходимости в указанном каталоге
test	Обнаружение и запуск тестов в указанных модулях или текущем каталоге
testserver	Запуск сервера для разработки с данными из указанных фикстур

Команды сервера — справочник CLI-команд утилиты `rude`, через которую системный администратор управляет сервером **RuDesktop** из консоли. Команды сгруппированы по областям применения: учётные записи, серверные операции, работа с файлами и данными, API-токены, синхронизация с LDAP, UEM-задачи, аналитика **Apache Superset**, обслуживающие команды и расширенные **Django**-команды

Подсказка

Все команды выполняются на сервере под пользователем с правами **root** (`sudo rude <команда>`). Список доступных команд можно вывести в любой момент через `rude --help`

Предупреждение

В таблице ниже команды, помеченные как **деструктивно**, изменяют или удаляют данные без подтверждения — выполняйте их только после *резервного копирования*

Команды с пометкой **dev** предназначены для разработки и обслуживания исходного кода **RuDesktop**. В рабочей инсталляции их запуск, как правило, не требуется и может привести к непредсказуемому поведению

1.6.13 Группы команд

Действия с сервером
Установка, перезапуск, диагностика, сертификаты, лицензия

Действия с учётными записями
Создание суперпользователя, смена пароля, сброс блокировок и MFA

Действия с логами
Очистка логов аудита и логов задач

Действия с адресной книгой
Импорт адресной книги пользователя из файла

Действия с геолокацией
Загрузка городов и определение геолокации устройств по IP

Действия с файлами
Управление файлами сервера

Действия с фактами и отчётами
Генерация отчётов и обновление данных инвентаризации

Действия с API
Создание, просмотр и отзыв API-токенов

Действия с LDAP
Взаимодействие с доменом и Keycloak

Действия с UEM

Управление задачами, политиками и удалённым выполнением команд

Действия с модулем аналитики

Управление встроенным **Apache Superset**

Дополнительные команды

Расширенные Django-команды и обслуживающие операции

1.6.14 Полный список команд

Команда	Описание
Действия с адресной книгой	
addressbook	Импорт адресной книги для пользователя из файла
Действия с геолокацией	
load_cities	Загрузка параметров городов из файла
locate	Определение геолокации по IP-адресу
update_peers_geo	Обновление геолокации устройств на основе IP-адресов
Действия с логами	
clean_audit_logs	Удаление старых логов аудита
clean_job_logs	Удаление старых логов задач
Действия с сервером	
backup	Создание резервной копии базы данных сервера
collectstatic	Сбор статических файлов в одном каталоге
clean_video_records	Удаление устаревших видеозаписей сессий
constance	Получение и установка параметров конфигурации сервера
delete	Очистка устройств по дате последней активности на сервере

продолжается на следующей странице

Таблица 71 – продолжение с предыдущей страницы

Команда	Описание
diag	Сбор информации для диагностики сервера
gencert	Генерация сертификата для моста
install	Первичная установка сервера и его служб
license	Получение информации о лицензии
maintain	Регламентное обслуживание сервера: ротация логов и удаление устаревших архивов
migrate_postgresql	Миграция БД на другую версию PostgreSQL
ping	Проверка доступности удалённого сервера
prof	Отображение запросов к базе данных
reconnect	Получение сертификата и мастер-пароля с устройства
reinstall	Переустановка сервера со сбросом конфигурации и сертификатов CA (**деструктивно**)
relay	Получение информации о версии сервера
restart	Перезапуск сервера
restore	Восстановление базы данных сервера из резервной копии (**деструктивно**)
setup_server	Установка сервера в качестве рандеву для подключения удалённого доступа
start	Запуск сервера
status	Получение информации о статусах служб сервера
stop	Остановка сервера
Действия с учётными записями	
axes_list_attempts	Формирование списка ошибочных попыток авторизации

продолжается на следующей странице

Таблица 71 – продолжение с предыдущей страницы

Команда	Описание
axes_reset_failure_logs	Сброс журнала неуспешных попыток доступа
axes_reset_ip_username	Сброс попыток доступа и блокировок для пары IP-адрес/имя пользователя
axes_reset_ip	Сброс блокировки IP-адреса
axes_reset_logs	Сброс неуспешных попыток входа для всех IP
axes_reset_username	Сброс блокировки пользователя
axes_reset	Сброс всех блокировок
bad_auth_list	Получение списка заблокированных пользователей
changepassword	Смена пароля пользователя
clean_otp	Удаление устаревших одноразовых паролей
createsuperuser	Создание пользователя с полными правами
disable_mfa	Отключение методов 2FA для конкретного пользователя
normalize_phones	Приведение номеров телефонов к стандартному виду
passwd	Смена пароля пользователя **admin**
Действия с файлами	
file	Управление файлами
Действия с фактами и отчётами	
report generate	Генерация отчётов
update_inventory	Обновление полей для раздела «Инвентаризация»
Действия с API	
token create	Создание токена
token list	Получение списка созданных токенов
token revoke	Отзыв токена
Действия с LDAP	
keycloak	Взаимодействие с Keycloak

продолжается на следующей странице

Таблица 71 – продолжение с предыдущей страницы

Команда	Описание
ldap	Взаимодействие с доменом
Действия с UEM	
job	Управление задачами
policy	Управление политиками
remote	Выполнение команд с сервера на удалённых устройствах
Действия с модулем аналитики	
superset backup	Создание резервной копии базы данных модуля аналитики
superset drop	Пересоздание базы данных модуля аналитики (**деструктивно**)
superset init	Инициализация базы данных модуля аналитики
superset install	Установка и инициализация службы модуля аналитики
superset restart	Перезапуск модуля аналитики
superset restore	Восстановление базы данных модуля аналитики из резервной копии (**деструктивно**)
superset start	Запуск модуля аналитики
superset status	Получение информации о статусах служб модуля аналитики
superset stop	Остановка модуля аналитики
superset token	Управление токенами доступа к REST API модуля аналитики
Дополнительные команды (Django и обслуживающие)	
analyze	Анализ списков на наличие IP-адресов из файла или лога
check	Проверка проекта Django на наличие потенциальных проблем

продолжается на следующей странице

Таблица 71 – продолжение с предыдущей страницы

Команда	Описание
clearsessions	Очистка сессий с истекшим сроком действия
cleartokens	Очистка просроченных токенов
client	Установка клиента **RuDesktop** по SSH
compilemessages	Компиляция po-файлов в mo-файлы для встроенной поддержки gettext (**dev**)
createapplication	Создание нового OAuth-приложения программным способом
createcachetable	Создание таблиц для использования кэша SQL
dbshell	Запуск клиента командной строки для базы данных (**dev**)
diffsettings	Отображение различий между текущим settings.py и настройками Django по умолчанию (**dev**)
drf_create_token	Создание токена DRF для заданного пользователя
dumpdata	Вывод содержимого базы данных в виде фикстуры заданного формата (**dev**)
event	Постановка события в очередь задач
executor	Фоновый процесс-воркер — постоянно выполняет задачи из очереди
export	Экспорт сетевого графа
findstatic	Поиск абсолютных путей к статическим файлам (**dev**)
fix_groups	Исправление символов в путях CN/DN для аккаунтов из LDAP-каталога
flush	Удаление всех данных из БД (**деструктивно** **dev**)

продолжается на следующей странице

Таблица 71 – продолжение с предыдущей страницы

Команда	Описание
generateschema	Генерация схемы API для проекта (**dev**)
genmodels	Создание моделей аудита и перечислений (**dev**)
inspectdb	Вывод информации о моделях Django по таблицам БД (**dev**)
loaddata	Установка фикстур в БД (**dev**)
makemessages	Генерация po-файлов с переводами (**dev**)
makemigrations	Создание новых миграций для приложений (**dev**)
migrate	Применение миграций для приложений
oauth_app	Создание нового OAuth-приложения программным способом
optimizemigration	Оптимизация операций для указанной миграции (**dev**)
playbook	Запуск указанного playbook на исполнение
provise	Генерация конфигурационных файлов для PXE-сервера
remove_stale_contenttype	Удаление устаревших типов контента из БД
run_job	Запуск задачи по её ID в БД сервера
runserver	Запуск встроенного веб-сервера для разработки (**dev**)
sendtestemail	Отправка тестового письма на указанные адреса
set_option	Установка значения переменной конфигурации
shell	Вход в терминал Python в окружении сервера (**dev**)
showmigrations	Отображение всех доступных миграций для текущего проекта

продолжается на следующей странице

Таблица 71 – продолжение с предыдущей страницы

Команда	Описание
spectacular	Создание схемы API в соответствии со стандартом OpenAPI 3
sqlflush	Получение SQL-запросов для восстановления таблиц БД до начального состояния (**dev**)
sqlmigrate	Вывод SQL-запросов для указанной миграции (**dev**)
sqlsequencereset	Вывод SQL-запросов для сброса последовательностей по именам приложений (**dev**)
squashmigrations	Объединение существующих наборов миграций в одну новую (**dev**)
startapp	Создание структуры каталогов нового Django-приложения (**dev**)
startproject	Создание структуры каталогов нового Django-проекта (**dev**)
test	Обнаружение и запуск тестов в указанных модулях (**dev**)
testserver	Запуск сервера для разработки с данными из фикстур (**dev**)

1.7 Развертывание отказоустойчивого кластера

Развертывание отказоустойчивого кластера — инструкция по установке нескольких серверов **RuDesktop** в режиме высокой доступности (HA) с общими **PostgreSQL** и **Redis**, балансировкой нагрузки и автоматическим переключением при отказе узла или целой площадки

1.7.1 Цель

Обеспечение непрерывной работы сервера **RuDesktop** при отказе одного узла или целой площадки (ЦОД)

- Количество узлов **RuDesktop** может быть 2, 3 или более (N)
- Данные (состояние, конфигурация, сессии) должны быть **общими** для всех узлов

Под общими данными понимаются:

- PostgreSQL — основное хранилище постоянных данных (пользователи, группы, устройства, настройки)
- Redis — общий кэш, хранилище состояний и механизм внутренней синхронизации компонентов

1.7.2 Термины

- Failover — процесс автоматического или регламентного переключения нагрузки с отказавшего узла/площадки на работоспособный
- Active-Active — схема, при которой все узлы одновременно обрабатывают пользовательский трафик
- Active-Passive — схема, при которой один узел (активный) обрабатывает трафик, а другие (пассивные) находятся в режиме горячего или холодного резерва
- Требования к RPO/RTO — выбор архитектуры зависит от допустимого времени восстановления (RTO) и потери данных (RPO)

1.7.3 Референс-архитектура

Внешний вход (WAN)

Пользователи подключаются к единой точке входа по TLS 443 (HTTPS/WSS). Реализация может быть одной из двух:

- **Через интеллектуальный балансировщик** (гео-балансировщик), который на основе health-чеков направляет трафик только на доступные узлы (предпочтительно для схемы Active-Active)
- **Через регламентный failover** (Active-Passive) — переключение маршрута, DNS-записи или правил балансировщика вручную по инструкции

Важно

Стандартный DNS Round-Robin **не является** отказоустойчивым решением, так как не проверяет доступность узлов

Узлы RuDesktop

На каждой физической или виртуальной площадке развёртывается полный набор компонентов **RuDesktop**:

- **RuDesktop server** (web-интерфейс, административная панель, backend-логика)
- **Nginx** (обработка TLS/SSL, проксирование WebSocket-соединений)
- **relay/rz** (компоненты для установки и поддержания пользовательских соединений)

Примечание

В стандартной сборке RuDesktop Server уже включены встроенные инстансы **PostgreSQL**, **Redis** и **nginx**. Однако в отказоустойчивой схеме эти компоненты **выносятся** и становятся общими для всех узлов кластера

Общие данные (Shared Storage)

В отказоустойчивой конфигурации компоненты, которые обычно работают локально, становятся общими:

- **PostgreSQL** — единый кластер БД, доступный всем узлам **RuDesktop** (вместо встроенной локальной БД)
- **Redis** — единый кластер или инстанс Redis, доступный всем узлам **RuDesktop** (вместо встроенного локального Redis)

1.7.4 Сетевые требования

1. **Канал между узлами RuDesktop и общими сервисами (PostgreSQL/Redis):**
   - Пропускная способность: не менее **1 Gbit/s**
   - Задержка (latency): должна быть **минимально возможной** (практический ориентир — менее 1 мс). Redis критически чувствителен к задержкам
2. **Безопасность доступа:**
   - Доступ к портам PostgreSQL и Redis должен быть разрешён **только** с IP-адресов узлов **RuDesktop** (или их подсетей)
   - Использование межсетевых экранов (firewall) и механизмов контроля доступа (например, `pg_hba.conf` в PostgreSQL, `bind` и `requirepass` в Redis) **обязательно**

1.7.5 Подключение внешней PostgreSQL

Принцип работы с кластером БД

RuDesktop не управляет репликацией и отказоустойчивостью PostgreSQL. Администрирование кластера (Patroni, streaming replication, managed cloud database) — зона ответственности администраторов СУБД

RuDesktop подключается к **единой точке входа (endpoint)**, которая всегда указывает на текущий первичный узел (Primary) БД

Это может быть:

- Виртуальный IP-адрес (VIP)
- DNS-имя (FQDN), переключаемое при смене Primary
- Специализированный прокси (HAProxy, PgBouncer) перед кластером

Конфигурация подключения на узле RuDesktop

Подключение настраивается в файле `/etc/default/rudesktop` на **каждом** узле с помощью переменных окружения:

```
POSTGRES_HOST='hostname_or_ip'
POSTGRES_PORT='port'
POSTGRES_DB='database_name'
POSTGRES_USER='username'
POSTGRES_PASSWORD='password'
```

Важно

В шаблоне `/etc/default/rudesktop`, формируемом при установке сервера, переменная `POSTGRES_USER` отсутствует — её нужно добавить вручную при подключении к внешней БД. Для встроенного PostgreSQL по умолчанию используется пользователь `rudesktop`

Примечание

Если `POSTGRES_PORT` не указан — используется стандартный порт PostgreSQL 5432

После внесения изменений необходимо перезапустить сервер:

```
rude restart
```

Подключение с использованием SSL/TLS

Для безопасного подключения добавьте в `/etc/default/rudesktop` следующие параметры:

```
POSTGRES_SSL_MODE=verify-ca  # или require
POSTGRES_CA_FILE=/path/to/ca.crt
```

1. Разместите CA-сертификат по указанному пути на **каждом** узле
2. После внесения изменений необходимо перезапустить сервер:

   ```
   rude restart
   ```

Подсказка

Допустимые значения `POSTGRES_SSL_MODE`: `disable`, `allow`, `prefer`, `require`, `verify-ca`

1.7.6 Подключение внешнего Redis

Подключение настраивается так же, как для одиночного сервера — см. *Настройка Redis*. Параметры `redis_server` (в `/etc/rudesktop-relay.toml`) и `REDIS_URL` (в `/etc/default/rudesktop`) должны указывать на один и тот же общий инстанс **Redis** на **каждом** узле кластера

Важно

Специфика кластера:

- Параметры `redis_server`, `REDIS_URL` и `RELAY_ARGS` должны быть **идентичными** на всех узлах **RuDesktop** — иначе компоненты будут работать с разными хранилищами кеша и сессий
- Общий инстанс **Redis** становится единой точкой отказа: рекомендуется развернуть его в отказоустойчивой конфигурации (Sentinel/Cluster) или с горячим резервом
- Доступ к **Redis** должен быть закрыт правилами файрвола и защищён `requirepass` (см. раздел «Безопасность» на странице *Настройка Redis*)

1.7.7 Проверка связности и состояния

После настройки убедитесь в корректности работы:

1. **PostgreSQL:** Проверьте подключение с узла RuDesktop (например, с помощью `psql` или `nc`)

```
PGPASSWORD=<password> psql -h <host> -p <port> -U <user>␣
↪-d <db> -c "SELECT 1"
```

2. **Redis:** Убедитесь, что компоненты видят общий кэш. Проверить можно командой:

```
redis-cli -h <host> -p <port> -a <password> PING
```

   Ожидаемый ответ — `PONG`

3. **Внутренняя синхронизация:** Убедитесь, что сессии пользователей, созданные на одном узле, видны на другом (через общий Redis)

1.7.8 Единые параметры на всех узлах RuDesktop

Для работы в едином контуре **все узлы должны иметь идентичные ключевые параметры**:

- **В файле ``/etc/default/rudesktop``:**
  - SECRET_KEY — **должен быть одинаковым** на всех узлах
  - REDIS_URL — должен указывать на один и тот же инстанс Redis
  - RELAY_ARGS — должен быть идентичным
- **В файле ``/etc/rudesktop-relay.toml``:**
  - redis_server — должен указывать на один и тот же инстанс Redis

1.7.9 Назначение конфигурационных файлов

- `/etc/default/rudesktop` — переменные окружения и общие параметры запуска для web/backend компонентов (включая строки подключения к PostgreSQL и Redis, `RELAY_ARGS`)
- `/etc/rudesktop-relay.toml` (и другие `.toml` файлы в `/etc/rudesktop/`) — конфигурация низкоуровневых компонентов (relay, rz и др.)

1.7.10 Пошаговый план внедрения

Шаг 1. Определение архитектуры

- Выбор схемы: Active-Active или Active-Passive
- Определение места размещения и архитектуры кластеров PostgreSQL и Redis

Шаг 2. Подготовка сетевой инфраструктуры

Обеспечьте сетевое взаимодействие:

- **RuDesktop** узлы ↔ Кластер PostgreSQL
- **RuDesktop** узлы ↔ Кластер Redis
- Пользователи ↔ Точка входа (балансировщик) на 443/TLS порт

Шаг 3. Подключение внешней PostgreSQL

На **каждом** узле **RuDesktop**:

1. Создайте резервную копию текущей базы данных перед изменениями (см. *Резервное копирование*)
2. Отредактируйте `/etc/default/rudesktop`, задав параметры `POSTGRES_*` (включая `POSTGRES_USER`)
3. При необходимости настройте SSL
4. Выполните `rude restart`

Шаг 4. Подключение внешнего Redis

На **каждом** узле **RuDesktop**:

1. Отредактируйте `/etc/rudesktop-relay.toml`, задав `redis_server`
2. Отредактируйте `/etc/default/rudesktop`, задав `REDIS_URL` и `RELAY_ARGS`
3. Выполните `rude restart`

Шаг 5. Унификация секретов и параметров

Убедитесь, что на всех узлах идентичны:

- SECRET_KEY
- REDIS_URL
- redis_server
- RELAY_ARGS

Шаг 6. Настройка внешнего входа (WAN)

- Для Active-Active: Настройте балансировщик с health-чеками на доступность узлов
- Для Active-Passive: Подготовьте процедуру регламентного переключения (DNS, правила балансировщика)

Шаг 7. Защита сервисов данных

- Настройте правила файрвола для PostgreSQL и Redis, разрешающие доступ только с подсетей узлов **RuDesktop**
- Для Redis **обязательно** установите стойкий пароль

Шаг 8. Тестирование отказоустойчивости

Проведите плановые тесты:

1. **Отказ узла RuDesktop.** Остановите один узел и убедитесь, что устройства автоматически переподключаются к другим узлам, а пользовательские сессии не прерываются
2. **Переключение Primary в PostgreSQL.** Имитируйте отказ кластера БД (переключение Primary) и убедитесь, что **RuDesktop** возобновляет работу после кратковременного перерыва в соединении — без ручных действий
3. **Отказ Redis.** Имитируйте недоступность общего инстанса **Redis** и зафиксируйте время восстановления после возврата сервиса. **Redis** является единой точкой отказа кластера — на основании результатов теста спланируйте его развёртывание в отказоустойчивой конфигурации (Sentinel, Cluster) или с горячим резервом

1.8 Резервное копирование

Резервное копирование — описание команд `rude backup` и `rude restore` для создания и восстановления дампа базы данных сервера **RuDesktop** и аналогичных команд для модуля аналитики (**Apache Superset**)

Важно

Команда `rude backup` сохраняет **только базу данных PostgreSQL**. Для полного восстановления сервера на чистой инсталляции дополнительно потребуется сохранить:

- `/etc/default/rudesktop` — параметры запуска и переменные окружения
- `/etc/rudesktop/settings` — настройки веб/backend
- `/etc/rudesktop-relay.toml` — конфигурация relay (если используется)
- `/var/lib/rudesktop/media/` — загруженные файлы (репозитории, отчёты)
- `/var/lib/rudesktop/user/` — пользовательские override-конфиги (PXE, Ansible)
- `/var/lib/rudesktop/kickstart/` — kickstart-сценарии
- `/var/lib/rudesktop/ca/` — сертификаты CA сервера

1.8.1 Резервная копия перед обновлением пакета

При обновлении серверного пакета DEB или RPM поведение автоматического резервного копирования задаётся переменной `UPGRADE_BACKUP` в `/etc/default/rudesktop`:

- `always` — создавать копию автоматически; значение по умолчанию
- `ask` — спросить перед созданием копии. Пустой ответ означает согласие; без доступного терминала копия создаётся автоматически
- `never` — не создавать автоматическую копию

Например, для запроса при интерактивном обновлении:

```
UPGRADE_BACKUP='ask'
```

Этот выбор относится к обновлениям с увеличением первых двух компонентов версии, например с `3.0` до `3.1`. Обычное обновление сборки внутри той же версии само по себе копию не создаёт

По умолчанию дамп сохраняется в `/var/lib/rudesktop/upgrade_backup.gz`; переменная `BACKUP_PATH` позволяет задать другой путь. `FORCE_BACKUP=true` принудительно включает копирование и имеет приоритет над остальными условиями. Без него `SKIP_BACKUP=true` и режим установки `INSTALL_MODE=relay` исключают автоматическое копирование

Ручная команда `rude backup` от значения `UPGRADE_BACKUP` не зависит. Автоматический дамп также сохраняет только базу данных — дополнительные файлы для восстановления перечислены выше

1.8.2 База данных сервера

Создание резервной копии

Команда выполняет `pg_dump` базы **RuDesktop** в gzip-сжатый файл. Подробно — на странице команды *backup*

```
rude backup /path/to/file
```

Подсказка

Рекомендуется выполнять резервное копирование перед каждым обновлением сервера или системы

Важно

- Файл должен иметь расширение `.gz` — дамп сохраняется в сжатом формате
- Указывайте **полный путь** к файлу

Примечание

На **Astra Linux Special Edition** сборка PostgreSQL с поддержкой МРД записывает в дамп мандатные метки объектов, из-за которых восстановление на обычном PostgreSQL пройдёт с ошибками и создаст базу частично. Чтобы копия оставалась переносимой, снимайте её с дополнительными аргументами:

```
rude backup /path/to/file.gz --no-security-labels --disable-mac
```

Разбор аргументов и способ проверки готового дампа — на странице команды *backup*

Восстановление из резервной копии

Подробно — на странице команды *restore*

```
rude restore /path/to/file
```

Важно

Восстановление — **деструктивная операция**:

- Сервер **RuDesktop** останавливается на время выполнения

- Существующая база данных **удаляется и пересоздаётся** (`pg_dump` создан с флагами `--clean --create`) — все текущие данные будут заменены данными из дампа
- После восстановления сервер автоматически запускается заново

Перед запуском убедитесь, что:

- На диске достаточно свободного места для распакованного дампа
- Файл дампа создан этой же или совместимой версией сервера

Пример

Создание резервной копии:

```
rude backup /home/rude/backup.gz
```

Восстановление:

```
rude restore /home/rude/backup.gz
```

1.8.3 База данных модуля аналитики

Если на сервере установлен модуль аналитики (**Apache Superset**), его база данных копируется отдельно

Создание резервной копии

Подробно — на странице команды *superset backup*

```
rude superset backup /path/to/file
```

Восстановление из резервной копии

Подробно — на странице команды *superset restore*

```
rude superset restore /path/to/file
```

Важно

- Файл должен иметь расширение `.gz`
- Указывайте полный путь к файлу
- При восстановлении модуль аналитики временно недоступен

Пример

Создание резервной копии:

```
rude superset backup /home/rude/superset_backup.gz
```

Восстановление:

```
rude superset restore /home/rude/superset_backup.gz
```

1.8.4 Автоматизация

Для настройки через веб-интерфейс используйте системную политику *Резервное копирование базы данных*. Она позволяет выбрать локальный каталог сервера, настроить срок хранения и запускать создание копии по расписанию через стандартный механизм заданий.

Команду `rude backup` также можно запускать по расписанию через `cron`. Пример — ежедневное создание копии в 2:00 ночи с именем по дате:

```
0 2 * * * /usr/bin/rude backup /var/backups/rudesktop/rudesktop-
↪$(date +\%Y-\%m-\%d).gz
```

Подсказка

Не забывайте периодически удалять или переносить старые архивы — каталог с дампами быстро растёт. Например, удалить файлы старше 30 дней:

```
find /var/backups/rudesktop/ -name "*.gz" -mtime +30 -delete
```

1.9 Логи сервера

Логи сервера — расположение и описание логов компонентов сервера **RuDesktop** на файловой системе. Раздел полезен при диагностике сбоев и обращении в техническую поддержку

1.9.1 Расположение логов

Все файлы логов находятся в каталоге:

```
/var/log/rudesktop/
```

Важно

Каталог имеет права доступа `700` и принадлежит пользователю `rudesktop` — для просмотра содержимого требуются права `sudo`

1.9.2 Состав логов

Файл	Назначение
`rudesktop.log`	Логи Django-части сервера: веб-интерфейс, API, фоновые задачи, синхронизация с LDAP/AD
`execution.log`	Логи модуля выполнения политик и задач (executor)
`server.log`	Логи нативных компонентов `relay` / `rz` (Rust): подключения клиентов, маршрутизация трафика
`updater.log`	Логи службы обновления сервера
`redis.log`	Логи встроенного Redis
`superset.log`	Логи модуля аналитики (**Apache Superset**). Присутствует только при установленном модуле аналитики
`domains/job_<domain_id>.log`	Подробные логи последней синхронизации с конкретным доменом LDAP/AD
`hosts/<имя_файла>.log`	Архивные логи Ansible-задач, выполнявшихся в старой архитектуре (на устройство)
`client_logs/<server_id>/...`	Логи клиента **RuDesktop**, загруженные с устройства через веб-интерфейс
`archive_<timestamp>/*.gz`	Сжатые архивы старых файлов `rudesktop.log.*` и `server.log.*`

Примечание

В текущей архитектуре логи отдельных запусков политик (job logs) сохраняются не в файлы, а в базу данных (модель `LogEvent`). Каталог `hosts/` остаётся для совместимости со старыми задачами

1.9.3 Ротация и очистка

Серверные логи ротируются автоматически:

- `rudesktop.log` и `execution.log` ротируются Python-обработчиком `ConcurrentRotatingFileHandler` — при достижении размера **5 МБ** файл переименовывается в `*.log.1`, `*.log.2` и т.д., хранится **5 копий**
- Команда *maintain* (запускается по расписанию) сжимает в gzip файлы `rudesktop.log.*` и `server.log.*` старше **1 дня** в подкаталог `archive_<timestamp>/` и удаляет файлы и архивы старше **30 дней**
- `superset.log` ротируется самим модулем аналитики (по времени) и командой `maintain` не обрабатывается

Подсказка

Параметр срока хранения можно переопределить флагом `--log-delete-after-days`:

```
rude maintain --log-delete-after-days 60
```

1.9.4 Связанные команды

- *clean_audit_logs* — удаление старых записей аудита из базы данных
- *clean_job_logs* — удаление старых логов задач из базы данных
- *diag* — сбор всех логов и конфигов в один архив для передачи в техническую поддержку

1.10 Мониторинг и метрики

Мониторинг сервера RuDesktop — набор встроенных средств для проверки доступности служб, наблюдения за нагрузкой на базу данных и сбора диагностической информации. Раздел описывает, какие точки контроля доступны «из коробки» и как использовать их во внешних системах мониторинга

Подсказка

Встроенного экспортёра метрик в формате **Prometheus** в сервере **RuDesktop** нет. Для интеграции с системами мониторинга (**Zabbix**, **Prometheus**, **Grafana**) используются эндпоинт `/api/healthcheck/`, команды `rude status` / `rude prof` и стандартные средства `systemd` и **PostgreSQL**

1.10.1 Что контролировать

Минимальный набор точек, которые имеет смысл наблюдать в продуктивной среде:

Точка контроля	Чем проверять
Доступность веб-API	HTTP-запрос к `/api/healthcheck/`
Состояние служб сервера	`rude status` или `systemctl is-active rudesktop-*`
Нагрузка на базу данных	`rude prof` (активные SQL-запросы и их длительность)
Свободное место под логи и БД	`df -h /var/log /var/lib/postgresql`
Доступность Redis	`redis-cli -h <addr> -p <port> PING`
Доступность узла кластера	`rude ping <ip>` (по протоколу **RuDesktop**)

1.10.2 Healthcheck-эндпоинт

Сервер предоставляет открытый эндпоинт для внешних балансировщиков и систем мониторинга:

```
GET https://<адрес_сервера>/api/healthcheck/
```

Эндпоинт не требует аутентификации и возвращает JSON-ответ:

```
{"health_check": "passed successfully"}
```

Важно

Эндпоинт подтверждает, что веб-служба `rudesktop-web` принимает HTTP-запросы и Django успешно отрабатывает маршрут. Он **не проверяет** доступность базы данных, **Redis** и нативных компонентов `relay` / `executor` — для них используйте отдельные проверки (см. раздел ниже)

Пример проверки из скрипта мониторинга:

```
curl -fsS https://server.example.com/api/healthcheck/ \
    | grep -q '"passed successfully"' \
    && echo OK || echo FAIL
```

Пример блока для **HAProxy** перед сервером:

```
backend rudesktop_web
    option httpchk GET /api/healthcheck/
    http-check expect string passed successfully
    server web1 10.0.0.11:443 check ssl verify none
    server web2 10.0.0.12:443 check ssl verify none
```

1.10.3 Состояние служб

Команда *status* выводит статусы всех служб сервера в зависимости от режима установки (`INSTALL_MODE`):

```
rude status
```

Активные службы выводятся зелёным, неактивные — красным. Для интеграции со скриптом удобнее использовать `systemctl`:

```
systemctl is-active rudesktop-web rudesktop-relay rudesktop-executor
```

Подсказка

В режиме **full** контролируйте: `rudesktop-web`, `rudesktop-relay`, `rudesktop-executor`, `rudesktop-redis`, `nginx` и текущую службу **PostgreSQL**. В режимах **relay** и **executor** состав служб отличается — см. описание команды *status*

1.10.4 Нагрузка на базу данных

Команда *prof* показывает активные SQL-запросы пользователя `rudesktop` с PID и временем работы. Применяется для поиска долгих запросов и анализа нагрузки:

```
rude prof
rude prof --explain
```

Важно

Перед первым использованием выполните однократно `rude prof init` — команда увеличивает `track_activity_query_size` в **PostgreSQL** и перезапускает службу, иначе тексты длинных запросов будут обрезаны

Дополнительно используйте стандартные средства **PostgreSQL**:

- Системное представление `pg_stat_activity` — все активные сессии и их состояние
- Расширение `pg_stat_statements` — статистика по выполненным запросам (включается в `postgresql.conf`)

1.10.5 Логи и диагностика

Для локального анализа используются логи в `/var/log/rudesktop/` (см. *Логи сервера*). Для передачи в техническую поддержку используйте команду *diag* — она собирает логи, конфиги, версии и информацию об ОС в один архив:

```
rude diag
rude diag -P <пароль>     # с шифрованием GPG
```

Подсказка

Команда `diag` автоматически вырезает пароли и секреты из конфигов перед упаковкой архива

Дублирование событий аудита во внешний **Syslog**-приёмник настраивается отдельно — см. *Публикация событий в Syslog*. Этот канал удобно использовать для интеграции с **SIEM** (например, **RuSIEM**) и для долговременного хранения событий безопасности

1.10.6 Интеграция с внешними системами

Поскольку встроенного экспортёра метрик нет, типичные сценарии интеграции выглядят так:

Система	Способ интеграции
Zabbix	HTTP-агент на `/api/healthcheck/` для веб-службы; `UserParameter` со скриптами-обёртками над `rude status` и `systemctl is-active` для остальных служб; стандартные шаблоны для **PostgreSQL** и хост-метрик
Prometheus	`blackbox_exporter` для проверки `/api/healthcheck/`; `node_exporter` для CPU/RAM/-диска; `postgres_exporter` для базы данных; `redis_exporter` для **Redis**
Grafana	Дашборды на основе данных **Prometheus** или прямого подключения к **PostgreSQL**
SIEM (RuSIEM и др.)	Публикация событий аудита через **Syslog** — см. *Публикация событий в Syslog*

Важно

При размещении сервера за обратным прокси убедитесь, что эндпоинт `/api/healthcheck/` не закрыт авторизацией на уровне прокси, иначе проверки балансировщика будут возвращать 401/403

1.10.7 Связанные команды

- *status* — статусы служб сервера
- *prof* — активные SQL-запросы и план выполнения
- *diag* — сбор диагностического архива для техподдержки
- *ping* — проверка доступности удалённого сервера по протоколу **RuDesktop**
- *constance* — чтение и изменение параметров конфигурации сервера

1.11 Публикация событий в Syslog

1.11.1 Настройка отправки событий в SIEM-систему

Настройка отправки событий в SIEM-систему — пошаговая инструкция по интеграции **RuDesktop** с внешним SIEM через протокол Syslog в формате CEF (Common Event Format)

Описание

Сервер **RuDesktop** отправляет события аудита по сети в локальный syslog-демон (`rsyslog` или `syslog-ng`). Локальный демон, в свою очередь, либо записывает события в системный журнал, либо пересылает их в SIEM-систему

Важно

RuDesktop отправляет события в syslog-демон по протоколу **TCP** на порт, указанный в параметре `SYSLOG_PORT`. Это означает, что локальный демон должен принимать TCP-соединения

Настройка локального syslog-демона

Процесс настройки состоит из двух этапов: конфигурация системного логгера (`rsyslog` или `syslog-ng`) на приём событий от **RuDesktop**, и настройка самого **RuDesktop** для отправки логов

rsyslog

1. Раскомментируйте в файле `/etc/rsyslog.conf` строки для включения модуля приёма TCP-соединений:

```
module(load="imtcp")
input(type="imtcp" port="514")
```

2. При необходимости добавьте в конец файла правило для пересылки событий в SIEM. Например, чтобы отправлять все события, содержащие ключевое слово `ADT` (логи аудита **RuDesktop**), на сервер с IP-адресом `192.168.11.75` по протоколу UDP, используйте следующее правило:

```
if ($msg contains 'ADT') then @192.168.11.75
```

Примечание

Символ `@` означает отправку по протоколу UDP. Для отправки по TCP используйте `@@`

Важно

Перед внесением изменений в файл `/etc/rsyslog.conf` рекомендуется сделать его резервную копию. Ошибка при редактировании файла может привести к некорректной работе системы

3. Перезапустите сервис **rsyslog**:

```
systemctl restart rsyslog
```

syslog-ng

1. Создайте новый файл по пути `/etc/syslog-ng/conf.d/remote-514.conf` и добавьте в него следующее содержимое для приёма логов по TCP:

```
source s_remote_514 {
    tcp(ip("0.0.0.0") port(514));
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
};
log {
    source(s_remote_514);
    destination(d_syslog);
};
```

При необходимости добавьте пересылку на удалённый SIEM-сервер. Например, чтобы отправлять все события, содержащие ключевое слово ADT (логи аудита **RuDesktop**), на сервер с IP-адресом 192.168.11.75 по протоколу UDP, используйте следующую конфигурацию:

```
# Источник для приёма логов от RuDesktop
source s_remote_514 {
    tcp(ip("0.0.0.0") port(514));
};

# Назначение для локальной записи в системный журнал
destination d_local {
    file("/var/log/syslog");
};

# Назначение для отправки на удалённый SIEM-сервер
destination d_siem {
    udp("192.168.11.75" port(514));
};

# Фильтр для отбора событий с ключевым словом ADT
filter f_adt {
    message("ADT");
};

# Логика обработки: всё, что приходит от RuDesktop,␣
↪пишем локально
log {
    source(s_remote_514);
    destination(d_local);
};

# Отдельное правило: если в сообщении есть ADT,␣
↪отправляем ещё и в SIEM
log {
    source(s_remote_514);
    filter(f_adt);
    destination(d_siem);
};
```

Примечание

Для отправки по протоколу TCP используйте `tcp("192.168.11.75" port(514))` вместо `udp(...)`

2. Перезапустите сервис **syslog-ng**:

```
systemctl restart syslog-ng
```

Настройка RuDesktop

1. Внесите в файл `/etc/rudesktop/settings` параметры подключения к syslog-приёмнику. Файл написан на синтаксисе Python:

```
SYSLOG_HOST = 'localhost'
SYSLOG_PORT = 514
```

Примечание

Если syslog-демон работает на той же машине, что и **RuDesktop**, используйте `localhost`. Для подключения к внешнему серверу укажите его IP-адрес или DNS-имя

2. Перезапустите сервер **RuDesktop** для применения настроек:

```
rude restart
```

3. Включите отправку нужных групп событий в админ-панели

   Перейдите в блок **«Настройки логов»** на странице *Настройки* и активируйте тумблеры тех событий, которые требуются по политике аудита:

   - Записывать статус подключений в syslog — события удалённых сессий (группа SESSIONS)
   - Записывать результаты запуска политик в syslog — результаты выполнения задач и политик (группа POLICY)
   - Записывать события аутентификации админ панели в syslog — входы в веб-интерфейс (группа AUTH)
   - Записывать события HTTP запросов в syslog — все HTTP-запросы к веб-интерфейсу (группа HTTP)
   - Записывать события CRUD (изменения объектов) в syslog — создание, изменение и удаление объектов (группа CRUD)
   - Записывать события Экспорта в syslog — экспорт данных из любых страниц (группа COLLECTOR)

Важно

До включения хотя бы одного из тумблеров **RuDesktop** не отправляет в syslog ни одного события, даже если `SYSLOG_HOST` указан корректно

Дополнительная настройка

В примерах выше для `rsyslog` и `syslog-ng` была показана фильтрация по содержимому сообщения. Это особенно полезно, если вы хотите отправлять в SIEM только значимые события (например, только события аудита с тегом `ADT`), а не весь системный лог

Подсказка

Как работает фильтрация:

- **rsyslog:** Строка `if $msg contains 'ADT' then @192.168.11.75` означает, что если сообщение содержит подстроку `ADT`, оно будет отправлено на удалённый хост `192.168.11.75` по UDP
- **syslog-ng:** Создаётся фильтр `filter f_adt { message("ADT"); };`, который отбирает сообщения с ключевым словом `ADT`. Затем отдельное правило `log` отправляет отфильтрованные сообщения на назначение `d_siem`

Все события **RuDesktop**, содержащие ключевое слово `ADT` (которое добавляется в логи безопасности), будут автоматически дублироваться на ваш SIEM-сервер для централизованного сбора и корреляции, при этом продолжая записываться в локальные логи сервера

1.11.2 Свойства syslog-сообщений в формате CEF

Классы событий из группы AUTH

Описание

Группа AUTH — эта страница предоставляет информацию о классах событий, связанных с процессами аутентификации в системе

Группа AUTH охватывает все события, связанные с проверкой подлинности пользователей и управлением доступом. Подробное описание этих событий поможет вам лучше понимать, контролировать и управлять безопасностью аутентификации в вашей системе

Каждое событие сопровождается набором ключей и значений, которые дают детализированную информацию в зависимости от типа события. Эти события передаются в формате CEF через syslog-сообщения и могут содержать различную информацию в зависимости от контекста и установленных параметров безопасности

Важно

Чтобы события группы AUTH отправлялись в syslog, в *Настройках логов* должен быть включён тумблер Записывать события аутентификации админ панели в syslog

Допустимые значения

В CEF-сообщениях событий из группы AUTH можно использовать различные ключи, чтобы точно описать каждое событие в соответствии с его характеристиками

	Название поля	Описание	Пример значения
CEF [заголовок]	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	ADT
	Device Product	Тип продукта	RuDesktop
	Device Version	Версия продукт	2.7.924
	Source	Тип журнала	AUTH
	Origin	Тип события	LOGOUT/LOGIN/LOGIN_ERROR
	Severity	Важность события	Может принимать значения: 7 — информационные или 3 — ошибки
CEF [расширение]	cs1	Имя журнала событий	Аутентификация
	cs1Label	Описание для поля cs1	log_source
	cs2	Описание типа события	Вход/Выход/Ошибка входа
	cs2Label	Описание для поля cs2	log_event_type
	cs3	Результат проверки кода OTP (только для события «LOGIN_ERROR»)	True/False
	cs3Label	Описание для поля cs3 (только для события «LOGIN_ERROR»)	log_bad_otp
	src	IP-адрес с которого была попытка аутентификации	192.168.0.1

продолжается на следующей странице

Таблица 72 – продолжение с предыдущей страницы

	Название поля	Описание	Пример значения
	rt	Время регистрации события на сервере	Jan 16 2025 10:05:34
	suser	Пользователь который пытался пройти аутентификацию или пользователь который вышел из системы	user

Примеры

Вход локального пользователя:

```
Jan 17 10:32:21 rudesktop syslogcef[523983]␣
↪CEF:0|ADT|RuDesktop|2.7.924|AUTH|LOGIN|7|cs1=Аутентификация␣
↪cs1Label=log_source cs2=Вход cs2Label=log_event_type␣
↪rt=Jan 17 2025 17:32:21 src=10.3.0.150 suser=user
```

Вход доменного пользователя:

```
Jan 17 10:32:17 rudesktop syslogcef[523982]␣
↪CEF:0|ADT|RuDesktop|2.7.924|AUTH|LOGOUT|7|cs1=Аутентификация␣
↪cs1Label=log_source cs2=Выход cs2Label=log_event_type␣
↪rt=Jan 17 2025 17:32:17 src=10.3.0.150 suser=user@test.loc
```

Ошибка авторизации, неверный код для 2FA (OTP):

```
Jan 21 06:28:17 rudesktop syslogcef[2904663]
↪CEF:0|ADT|RuDesktop|2.7.928|AUTH|LOGIN_
↪ERROR|3|cs1=Аутентификация cs1Label=log_source cs2=Ошибка
↪входа cs2Label=log_event_type cs3=False cs3Label=log_bad_
↪otp rt=Jan 21 2025 13:28:17 src=10.3.0.150 suser=user
```

Выход пользователя:

```
Jan 17 10:32:24 rudesktop syslogcef[523980]␣
↪CEF:0|ADT|RuDesktop|2.7.924|AUTH|LOGOUT|7|cs1=Аутентификация␣
↪cs1Label=log_source cs2=Выход cs2Label=log_event_type␣
↪rt=Jan 17 2025 17:32:24 src=10.3.0.150 suser=user
```

Классы событий из группы COLLECTOR

Описание

Группа COLLECTOR — эта страница содержит описание классов событий, относящихся к группе COLLECTOR, которая отвечает за сбор и обработку логов в системе

События из группы COLLECTOR помогают в мониторинге работы системы сбора логов, позволяя своевременно выявлять и устранять возможные неполадки

Каждое событие сопровождается набором ключей и значений, которые дают детализированную информацию в зависимости от типа события. Эти события передаются в формате CEF через syslog-сообщения и могут содержать различную информацию в зависимости от контекста и установленных параметров безопасности

Важно

Чтобы события типа EXPORT из группы COLLECTOR отправлялись в syslog, в *Настройках логов* должен быть включён тумблер Записывать события Экспорта в syslog

Допустимые значения (для типа событий EXPORT)

В CEF-сообщениях событий из группы COLLECTOR можно использовать различные ключи, чтобы точно описать каждое событие в соответствии с его характеристиками

	Название поля	Описание	Пример значения
CEF [заголовок]	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	ADT
	Device Product	Тип продукта	RuDesktop
	Device Version	Версия продукт	2.7.924
	Source	Тип журнала	COLLECTOR
	Origin	Тип события	EXPORT
	Severity	Важность события	Может принимать значения: 7 — информационные
CEF [расширение]	cs1	Имя журнала событий	Сборщик логов
	cs1Label	Описание для поля cs1	log_source
	cs2	Описание типа события	Экспорт
	cs2Label	Описание для поля cs2	log_event_type
	cs3	Тип объектов	audit-HTTP запрос
	cs3Label	Описание для поля cs3	log_object_type

продолжается на следующей странице

Таблица 73 – продолжение с предыдущей страницы

	Название поля	Описание	Пример значения
	cs4	Количество строк в выгрузке	Целое положительное число от 1 до 2-х миллиардов
	cs4Label	Описание поля cs4	log_object_count
	rt	Время регистрации события на сервере	Jan 16 2025 10:05:34
	suser	Пользователь который был ассоциирован с запросом	user

Примеры

Экспорт 6 строк логов со страницы `Аудит -> HTTP запрос`:

```
Jan 15 08:50:52 rudesktop syslogcef[24972]␣
↪CEF:0|ADT|RuDesktop|2.7.924|COLLECTOR|EXPORT|7|cs1=Сборщик␣
↪логов cs1Label=log_source cs2=Экспорт␣
↪cs2Label=log_event_type cs3=audit-HTTP запрос␣
↪cs3Label=log_object_type cs4=6 cs4Label=log_object_count␣
↪rt=Jan 15 2025 08:50:52 suser=user
```

Классы событий из группы CRUD

Описание

Группа CRUD — эта страница содержит информацию о классах событий, относящихся к группе CRUD, которая включает операции создания, обновления и удаления объектов в системе. События данной группы фиксируют ключевые изменения в данных и управляют жизненным циклом объектов, таких как записи в базе данных или элементы интерфейса

События из группы CRUD помогают отслеживать взаимодействия с данными и обеспечивают прозрачность в управлении ими. Каждое событие содержит ключи и значения, которые подробно описывают его природу и контекст, включая информацию о том, какой объект был создан, обновлён или удалён, а также какие изменения были внесены

Каждое событие сопровождается набором ключей и значений, которые дают детализированную информацию в зависимости от типа события. Эти события передаются в формате CEF через syslog-сообщения и могут содержать различную информацию в зависимости от контекста и установленных параметров безопасности

Важно

Чтобы события группы CRUD отправлялись в syslog, в *Настройках логов* должен быть включён тумблер Записывать события CRUD (изменения объектов) в syslog

Допустимые значения

В CEF-сообщениях событий из группы CRUD можно использовать различные ключи, чтобы точно описать каждое событие в соответствии с его характеристиками

	Название поля	Описание	Пример значения
CEF [заголовок]	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	ADT
	Device Product	Тип продукта	RuDesktop
	Device Version	Версия продукт	2.7.924
	Source	Тип журнала	CRUD
	Origin	Тип события	CREATE/UPDATE/DELETE
	Severity	Важность события	Может принимать значения: 7 — информационные
CEF [расширение]	cs1	Имя журнала событий	Объект
	cs1Label	Описание для поля cs1	log_source
	cs2	Описание типа события	Создан/Обновлен/Удален
	cs2Label	Описание для поля cs2	log_event_type
	cs3	Тип объекта	pgq-Команда
	cs3Label	Описание для поля cs3	log_object_type
	cs4	Содержимое объекта	[execute] notify:None {}
	cs4Label	Описание для поля cs4	log_object
	rt	Время регистрации события на сервере	Jan 16 2025 10:05:34
	suser	Пользователь который был ассоциирован с запросом	user

	Название поля	Описание	Пример значения
CEF [заголовок]	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	ADT
	Device Product	Тип продукта	RuDesktop
	Device Version	Версия продукт	2.7.924
	Source	Тип журнала	CRUD
	Origin	Тип события	M2M_ADD, M2M_ADD_REV, M2M_CLEAR, M2M_REMOVE
	Severity	Важность события	Может принимать значения: 7 — информационные
CEF [расширение]	cs1	Имя журнала событий	Объект
	cs1Label	Описание для поля cs1	log_source
	cs2	Описание типа события	Добавлена связь-/Добавлена обратная связь-/Удалены все связи/Удалена связь
	cs2Label	Описание для поля cs2	log_event_type
	cs3	Тип первого объекта при СозданииИзмененииУдалении M2M связи	account-Пользователь
	cs3Label	Описание для поля cs3	log_object1_type
	cs4	Тип второго объекта при СозданииИзмененииУдалении M2M связи	auth-группа
	cs4Label	Описание для поля cs4	log_object2_type
	cs5	Список значений для «объекта 1» (log_object1_type)	test
	cs5Label	Описание для поля cs5	log_object1
	cs6	Список значений для «объекта 2» (log_object2_type)	[Гость/Руководитель подразделения/…]

продолжается на следующей странице

Таблица 75 – продолжение с предыдущей страницы

	Название поля	Описание	Пример значения
	cs6Label	Описание для поля cs6	log_object2
	rt	Время регистрации события на сервере	Jan 16 2025 10:05:34
	suser	Пользователь которого удалось или не удалось сопоставить с командой выполнения действий над объектами	None/user

Примеры

Удаление задачи из очереди:

```
Jan 17 10:16:55 rudesktop syslogcef[527645]␣
↪CEF:0|ADT|RuDesktop|2.7.924|CRUD|DELETE|7|cs1=Объект␣
↪cs1Label=log_source cs2=Удален cs2Label=log_event_type␣
↪cs3=pgq-Команда cs3Label=log_object_type cs4=[execute]␣
↪notify:None {'email': None, 'phone': None, 'context': {
↪'access_code': 996088, 'expired_time': 5}, 'user_id': 19,
↪'template_body': 'success_code_ready.txt',
↪'template_subject': 'success_code_subject.txt'}␣
↪cs4Label=log_object rt=Jan 17 2025 17:16:55 suser=user
```

Удаление связи для пользователя:

```
Jan 17 10:43:10 rudesktop syslogcef[523982]␣
↪CEF:0|ADT|RuDesktop|2.7.924|CRUD|M2M_REMOVE|7|cs1=Объект␣
↪cs1Label=log_source cs2=Удалена связь␣
↪cs2Label=log_event_type cs3=account-Пользователь␣
↪cs3Label=log_object1_type cs4=auth-группа␣
↪cs4Label=log_object2_type cs5=test cs5Label=log_object1␣
↪cs6=[Гость, Руководитель подразделения, Администратор]␣
↪cs6Label=log_object2 rt=Jan 17 2025 17:43:10 suser=None
```

Классы событий из группы HTTP

Описание

Группа HTTP — эта страница содержит информацию о классах событий, связанных с HTTP-активностью на веб-сервере. Группа событий HTTP охватывает логи работы веб-интерфейса, фиксируя действия пользователей на сайте, такие как какие страницы были открыты и какие ресурсы запрашивались

События из группы HTTP играют важную роль в мониторинге трафика и анализе поведения пользователей. Они помогают выявлять наиболее востребо-

ванные ресурсы, отслеживать активность пользователей, а также обнаруживать попытки несанкционированного доступа

Каждое событие сопровождается набором ключей и значений, которые дают детализированную информацию в зависимости от типа события. Эти события передаются в формате CEF через syslog-сообщения и могут содержать различную информацию в зависимости от контекста и установленных параметров безопасности

Важно

Чтобы события группы HTTP отправлялись в syslog, в *Настройках логов* должен быть включён тумблер Записывать события HTTP запросов в syslog

Допустимые значения

В CEF-сообщениях событий из группы HTTP можно использовать различные ключи, чтобы точно описать каждое событие в соответствии с его характеристиками

	Название поля	Описание	Пример значения
CEF [заголовок]	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	ADT
	Device Product	Тип продукта	RuDesktop
	Device Version	Версия продукт	2.7.924
	Source	Тип журнала	HTTP
	Origin	Тип события	HTTP_REQUEST
	Severity	Важность события	Может принимать значения: 7 — информационные
CEF [расширение]	cs1	Имя журнала событий	HTTP
	cs1Label	Описание для поля cs1	log_source
	cs2	Описание типа события	HTTP запрос
	cs2Label	Описание для поля cs2	log_event_type
	requestMethod	Метод запроса	GET/POST
	request	URL-адрес запроса клиента	https://192.168.0.1/check-updates/
	rt	Время регистрации события на сервере	Jan 16 2025 10:05:34
	shost	IP-адрес с которого выполнялись запросы	192.168.0.1

продолжается на следующей странице

Таблица 76 – продолжение с предыдущей страницы

	Название поля	Описание	Пример значения
	suser	Пользователь который был ассоциирован с запросом	user

Примеры

Открытие страницы авторизации **Rudesktop** неавторизированным пользователем:

```
Jan 17 11:06:16 rudesktop syslogcef[523981]␣
↪CEF:0|ADT|RuDesktop|2.7.924|HTTP|HTTP_REQUEST|7|cs1=HTTP␣
↪cs1Label=log_source cs2=HTTP запрос␣
↪cs2Label=log_event_type requestMethod=POST␣
↪request=https://192.168.0.1/login/?next\=/ rt=Jan 17 2025␣
↪18:06:16 shost=192.168.0.2 suser=None
```

Классы событий из группы POLICY

Описание

Группа POLICY — эта страница предоставляет информацию о классах событий, связанных с исполнением политик и задач в системе. Группа событий POLICY охватывает действия, связанные с применением и управлением различными политиками, которые устанавливают правила и процедуры для управления системой и её ресурсами

События из группы POLICY помогают отслеживать, когда и как политики применяются или изменяются, обеспечивая прозрачность и контроль над процессами в системе. Эти события могут включать информацию о запуске задач, изменении конфигураций, а также мониторинге соответствия установленным правилам

Каждое событие сопровождается набором ключей и значений, которые дают детализированную информацию в зависимости от типа события. Эти события передаются в формате CEF через syslog-сообщения и могут содержать различную информацию в зависимости от контекста и установленных параметров безопасности

Важно

Чтобы события группы POLICY отправлялись в syslog, в *Настройках логов* должен быть включён тумблер Записывать результаты запуска политик в syslog

Допустимые значения

В CEF-сообщениях событий из группы POLICY можно использовать различные ключи, чтобы точно описать каждое событие в соответствии с его характеристиками

	Название поля	Описание	Пример значения
CEF [заголовок]	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	ADT
	Device Product	Тип продукта	RuDesktop
	Device Version	Версия продукт	2.7.924
	Source	Тип журнала	POLICY
	Origin	Тип события	JOB_RESULT/JOB_START
	Severity	Важность события	Может принимать значения: 7 — информационные
CEF [расширение]	cs1	Имя журнала событий	Политика
	cs1Label	Описание для поля cs1	log_source
	cs2	Описание типа события	Результат задачи/Запуск задачи
	cs2Label	Описание для поля cs2	log_event_type
	cs3	Имя устройства над которым производилось исполнение политикизадачи	user@PC-1 (483669353)
	cs3Label	Описание для поля cs3	log_devicename
	cs4	Название политики	Обслуживание сервера/AD SYNC/Инвентаризация и т.п.
	cs4Label	Описание для поля cs4	log_policy_name

продолжается на следующей странице

Таблица 77 – продолжение с предыдущей страницы

	Название поля	Описание	Пример значения
	cs5	Название задачи	Обслуживание сервера/Инвентаризация/Любое название и т.п.
	cs5Label	Описание для поля cs5	log_job_name
	end	Время окончания задачи или политики	Jan 16 2025 10:05:34
	msg	Информационное сообщение в формате Ansible о результатах выполнения задачи или политики	{«ok»: 1/»failures»: 0/»unreachable»: 0/»changed»: 1/»skipped»: 0/»rescued»: 0/»ignored»: 0}
	rt	Время регистрации события на сервере	Jan 16 2025 10:05:34
	start	Время запуска задачи или политики	Jan 16 2025 10:05:31
	suser	Пользователь который инициировал исполнение задачи или политики	user

Примеры

Пример запуска задачи `Обслуживание сервера`:

```
Jan 16 10:05:34 rudesktop syslogcef[5228]␣
↪CEF:0|ADT|RuDesktop|2.7.924|POLICY|JOB_RESULT|7|cs1=Политика␣
↪cs1Label=log_source cs2=Результат задачи␣
↪cs2Label=log_event_type cs3=None cs3Label=log_devicename␣
↪cs4=Обслуживание сервера cs4Label=log_policy_name␣
↪cs5Label=log_job_name end=Jan 16 2025 10:05:34 msg={"ok":␣
↪1, "failures": 0, "unreachable": 0, "changed": 1,
↪"skipped": 0, "rescued": 0, "ignored": 0} rt=Jan 16 2025␣
↪10:05:34 start=Jan 16 2025 10:05:31 suser=user
```

Пример запуска политики `Инвентаризация`:

```
Jan 16 10:37:09 rudesktop syslogcef[16653]␣
↪CEF:0|ADT|RuDesktop|2.7.924|POLICY|JOB_RESULT|7|cs1=Политика␣
↪cs1Label=log_source cs2=Результат задачи␣
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
↪cs2Label=log_event_type cs3=f.vochmincev@DEV-08␣
↪(483669353) cs3Label=log_devicename cs4=Инвентаризация␣
↪устройств cs4Label=log_policy_name cs5Label=log_job_name␣
↪end=Jan 16 2025 10:37:09 msg={"ok": 14, "failures": 0,
↪"unreachable": 0, "changed": 5, "skipped": 17, "rescued":␣
↪0, "ignored": 0} rt=Jan 16 2025 10:37:09 start=Jan 16␣
↪2025 10:36:28 suser=user
```

Классы событий из группы SESSIONS

Описание

Группа SESSIONS — эта страница содержит информацию о классах событий, связанных с сессиями удаленных подключений. Группа событий SESSIONS охватывает процессы, связанные с установлением и завершением удаленных подключений

События из группы SESSIONS позволяют фиксировать детали подключения. Это может включать информацию о времени начала и завершения сессий, пользователях, IP-адресах и других параметрах, связанных с удаленным доступом

Каждое событие сопровождается набором ключей и значений, которые дают детализированную информацию в зависимости от типа события. Эти события передаются в формате CEF через syslog-сообщения и могут содержать различную информацию в зависимости от контекста и установленных параметров безопасности

Важно

Чтобы события группы SESSIONS отправлялись в syslog, в *Настройках логов* должен быть включён тумблер Записывать статус подключений в syslog

Допустимые значения

В CEF-сообщениях событий из группы SESSIONS можно использовать различные ключи, чтобы точно описать каждое событие в соответствии с его характеристиками

	Название поля	Описание	Пример значения
CEF [заголовок]	CEF:Version	Версия CEF	CEF:0
	Device Vendor	Производитель продукта	ADT
	Device Product	Тип продукта	RuDesktop
	Device Version	Версия продукт	2.7.924
	Source	Тип журнала	SESSIONS

продолжается на следующей странице

Таблица 78 – продолжение с предыдущей страницы

	Название поля	Описание	Пример значения
	Origin	Тип события	SESSION_WAIT, SESSION_STARTED, SESSION_FINISHED, SESSION_WARNING
	Severity	Важность события	Может принимать значения: 7 — информационные
CEF [расширение]	cs1	Имя журнала событий	Сессии подключений
	cs1Label	Описание для поля cs1	log_source
	cs2	Описание типа события	Ожидание подключения сессии/Начало сессии/Завершение сессии/Предупреждение сессии
	cs2Label	Описание для поля cs2	log_event_type
	cs3	Статус сессии	Строка
	cs3Label	Описание для поля cs3	session_status
	cs4	ID хоста оператора сессии	123456789
	cs4Label	Описание для поля cs4	source_host_id
	cs5	ID хоста клиента сессии	123456780
	cs5Label	Описание для поля cs5	destination_host_id
	cs6	UUID сессии	Строка
	cs6Label	Описание для поля cs6	session_uuid
	shost	Имя хоста оператора	pc-1
	dhost	Имя хоста клиента	pc-2
	src	IP-адрес хоста оператора	10.64.36.26
	dst	IP-адрес хоста клиента	192.168.49.166
	suser	Имя пользователя хоста оператора	user1
	duser	Имя пользователя хоста клиента	user2

продолжается на следующей странице

Таблица 78 – продолжение с предыдущей страницы

	Название поля	Описание	Пример значения
	flexString1	Логин пользователя RuDesktop — инициатора подключения	admin
	flexString1Label	Описание для поля flexString1	rudesktop_user
	flexString2	Полное имя пользователя RuDesktop — передаётся если заполнено в профиле	Тестовый Оператор
	flexString2Label	Описание для поля flexString2	rudesktop_user_full_name
	suid	ID пользователя RuDesktop — инициатора подключения	42
	msg	Тип подключения и способ соединения — punch_type не передаётся если способ не определён	connection_type:Рабочий стол punch_type:RELAY
	rt	Время регистрации события на сервере	Jan 16 2025 10:05:34

Примеры

Запись начала удалённого подключения оператора к клиенту:

```
Jan 15 08:57:36 rudesktop syslogcef[36365]
↪CEF:0|ADT|RuDesktop|3.0.1563|SESSIONS|SESSION_
↪STARTED|7|cs1=Сессии подключений cs1Label=log_source
↪cs2=Начало сессии cs2Label=log_event_type cs3=ACTIVE
↪cs3Label=session_status cs4=483669353 cs4Label=source_host
↪_id cs5=483669354 cs5Label=destination_host_id
↪cs6=72ec5477-f393-45e7-aa61-b424cf3c7dc9 cs6Label=session_
↪uuid dhost=PC-02 dst=192.168.49.166 duser=user2
↪flexString1=admin flexString1Label=rudesktop_user
↪flexString2=Тестовый Оператор flexString2Label=rudesktop_
↪user_full_name msg=connection_type:Рабочий стол punch_
↪type:RELAY rt=Jan 15 2025 08:57:36 shost=PC-01 src=10.64.
↪36.26 suid=42 suser=user1
```

Свойства syslog-сообщений в формате CEF — справочник по структу-

ре syslog-сообщений, отправляемых сервером **RuDesktop** в формате **CEF (Common Event Format)** в кодировке UTF-8. Раздел сгруппирован по типам событий: AUTH, COLLECTOR, CRUD, HTTP, POLICY, SESSIONS

Структура CEF-сообщения

Каждое syslog-сообщение от **RuDesktop** имеет следующую структуру:

```
CEF:0|Vendor|Product|Version|SignatureId|Name|Severity|Extension
```

Где:

- `CEF:0` — версия формата CEF (всегда `0`)
- `Vendor` — производитель (`ADT`)
- `Product` — продукт (`RuDesktop`)
- `Version` — версия сервера (например, `2.7.924`)
- `SignatureId` — идентификатор группы событий (`AUTH`, `HTTP`, `CRUD` и т.п.)
- `Name` — конкретный класс события внутри группы (`LOGIN`, `DELETE`, `JOB_RESULT` и т.п.)
- `Severity` — уровень критичности (от `0` до `10`)
- `Extension` — список ключей-значений с детализированной информацией о событии (например, `suser=user src=10.3.0.150 rt=...`)

Подсказка

Формат CEF поддерживается большинством SIEM-систем (ArcSight, Splunk, QRadar, RuSIEM и др.), что позволяет использовать стандартные парсеры без дополнительной настройки

Группы событий

Классы событий из группы AUTH

События авторизации в веб-интерфейсе

Классы событий из группы COLLECTOR

События экспорта и сбора данных

Классы событий из группы CRUD

События создания, изменения и удаления объектов

Классы событий из группы HTTP

События HTTP-запросов к API

Классы событий из группы POLICY
События выполнения политик и задач

Классы событий из группы SESSIONS
События удалённых сессий и передачи файлов

Публикация событий в Syslog — описание интеграции сервера **RuDesktop** с внешними SIEM-системами через протокол Syslog. Каждое событие безопасности отправляется отдельным syslog-сообщением в формате **CEF (Common Event Format)** в кодировке UTF-8

Подсказка

CEF (Common Event Format) — стандартный текстовый формат логов безопасности от компании Micro Focus, поддерживаемый большинством SIEM-систем (ArcSight, Splunk, QRadar, RuSIEM и др.). Сообщение состоит из заголовка (Vendor, Product, Version, SignatureId, Name, Severity) и набора ключей-значений в свободном формате

1.11.3 Как это работает

Включение интеграции состоит из трёх шагов:

1. На стороне ОС сервера — настроить локальный syslog-демон (`rsyslog` или `syslog-ng`) на приём сообщений по TCP и при необходимости — на пересылку в SIEM
2. В файле `/etc/rudesktop/settings` указать адрес syslog-приёмника через параметры `SYSLOG_HOST` и `SYSLOG_PORT`, после чего перезапустить сервер
3. В веб-интерфейсе администратора в блоке **«Настройки логов»** на странице *Настройки* включить тумблеры для тех групп событий, которые нужно отправлять в syslog

Важно

По умолчанию все тумблеры выключены — даже после настройки `SYSLOG_HOST` ни одного события в syslog **не уйдёт**, пока в веб-интерфейсе не будут активированы соответствующие переключатели

Настройка отправки событий в SIEM-систему
Активация Syslog-экспорта и подключение к внешнему SIEM-приёмнику

Свойства syslog-сообщений в формате CEF
Описание полей и групп событий в Syslog-сообщениях

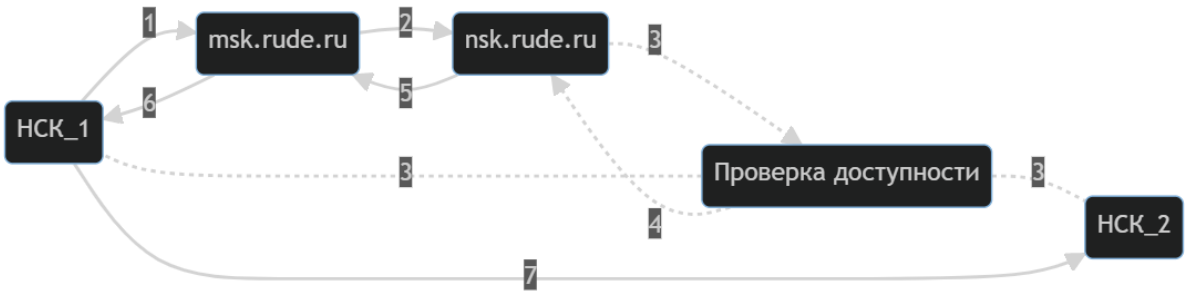
1.12 Настройка мостов

Мост — это отдельный сервер **RuDesktop**, развёрнутый в географически удалённой точке. Главный сервер по координатам подбирает ближайший к клиенту мост и направляет через него подключение, что сокращает сетевую задержку для удалённых филиалов

Примечание

Регистрация моста на главном сервере и описание его параметров — на странице *Мосты*. Этот раздел описывает развёртывание самого сервера-моста

1.12.1 Схема подключения



Примечание

1. Обращение к основному серверу `msk.rude.ru`
2. `msk.rude.ru` проверяет наличие ближайшего моста к клиенту
3. Мост `nsk.rude.ru` проверяет доступность НСК_1 и НСК_2
4. Оба клиента доступны
5. Мост `nsk.rude.ru` сообщает основному серверу, что оба клиента доступны
6. Основной сервер передает клиенту НСК_1, что подключение к НСК_2 будет производиться через мост `nsk.rude.ru`
7. Подключение к НСК_2 через мост `nsk.rude.ru`

1.12.2 Поддерживаемые операционные системы

DEB

- Ubuntu
- Debian
- Astra
- ОСнова

RPM

- ALT Linux
- AlterOS
- РЕД ОС
- РОСА
- МСВСфера
- CentOS
- Fedora

1.12.3 Установка моста

1. Запустите установку сервера с переменной `INSTALL_MODE=relay`:

   DEB

   ```
   INSTALL_MODE=relay apt install rudesktop-server
   ```

   RPM

   ```
   INSTALL_MODE=relay dnf install rudesktop-server
   ```

   Затем выполните команду переконфигурации, указав адрес моста:

   ```
   INSTALL_MODE=relay rude reinstall <IP_ИЛИ_ДОМЕН_МОСТА>
   ```

   Примечание

   Команда `rude reinstall` удаляет ранее созданные конфигурационные файлы и сертификаты, после чего повторно запускает установку с указанным адресом. Для DEB-сборки этот шаг не требуется — значения подставляются на этапе `apt install`

2. На сервере моста создайте файл конфигурации по пути `/etc/rudesktop-relay.toml` и добавьте следующие строки:

   ```
   api_key = "СЛУЧАЙНАЯ СТРОКА"

   [master]
   url = "wss://АДРЕС_ГЛАВНОГО_СЕРВЕРА/v1/"
   ```

3. В файл по пути `/etc/default/rudesktop` на мосте добавьте следующую строку:

   ```
   RELAY_ARGS='-C /etc/rudesktop-relay.toml'
   ```

4. На главном сервере создайте файл конфигурации по пути `/etc/rudesktop-relay.toml` и добавьте следующую строку:

```
api_key = "СЛУЧАЙНАЯ СТРОКА"
```

Важно

`api_key` на главном сервере и на мосте должны совпадать

5. В файл по пути `/etc/default/rudesktop` на главном сервере добавьте следующую строку:

```
RELAY_ARGS='-C /etc/rudesktop-relay.toml'
```

6. Создайте сертификат для моста

   Если вы используете центр сертификации **RuDesktop**, то:

   1. Сгенерируйте сертификаты для моста следующей командой, указав IP-адрес или домен моста:

      ```
      rude gencert <IP_ИЛИ_ДОМЕН_МОСТА>
      ```

      Подсказка

      Подробнее о команде *gencert*

   2. Передайте сгенерированные сертификаты с главного сервера на мост

      Подсказка

      Сгенерированные сертификаты доступны по пути `/tmp/CA.key` и `/tmp/CA.pem`

   3. На мосте полученные сертификаты переместите по пути `/var/lib/rudesktop/ca/` с заменой
   4. Перезагрузите мост командой:

      ```
      rude restart
      ```

   Если вы используете свой центр сертификации, то на странице *Сертификаты* в веб-интерфейсе главного сервера добавьте сертификат моста

Подсказка

Сертификат находится по пути: `/var/lib/rudesktop/ca/CA.pem`

7. На странице *Мосты* в веб-интерфейсе главного сервера добавьте адрес созданного моста
8. Перезагрузите главный сервер командой:

```
rude restart
```

1.13 Настройка точек распространения

Настройка точек распространения — развёртывание дополнительных узлов **RuDesktop** в режиме исполнителя (`INSTALL_MODE=executor`), которые подключаются к общим **Redis** и **PostgreSQL** главного сервера, забирают оттуда задачи (например, выполнение политик) и выполняют их у себя — это снимает нагрузку с главного сервера и позволяет распараллелить выполнение задач между несколькими узлами

Регистрация и параметры точки распространения настраиваются на странице *Точки распространения* в веб-интерфейсе

Предупреждение

Версии сервера **RuDesktop** на главном узле и на точке распространения должны совпадать. После обновления главного сервера на новую версию точку распространения необходимо обновить до той же версии — иначе часть функциональности может работать некорректно

1.13.1 Сетевые порты и потоки данных

Точка распространения участвует в передаче файлов на устройства по цепочке **главный сервер → точка распространения → конечное устройство**. Ниже приведены сетевые соединения, которые нужно разрешить на межсетевом экране.

Соединение	Инициатор	Протокол	Порт
Кэширование файла: точка распространения загружает файл из хранилища главного сервера	Точка распространения → главный сервер	HTTPS (TCP)	веб-порт главного сервера (по умолчанию 443)
Загрузка файла на устройство: устройство забирает файл с точки распространения	Конечное устройство → точка распространения	HTTPS (TCP)	веб-порт точки распространения (по умолчанию 443)
Управляющий канал: запуск задач и получение результата (протокол **RuDesktop**)	Конечное устройство и точка распространения → главный сервер (сервер подключений)	WSS (WebSocket поверх TLS)	443
Доступ к общим службам главного сервера	Точка распространения → главный сервер	Redis / PostgreSQL	32459 / порт **PostgreSQL**
Управление по SSH (если для устройства выбран тип подключения SSH)	Точка распространения → конечное устройство	SSH (TCP)	22
Обнаружение PXE и передача параметров загрузки	PXE-клиент → точка распространения	DHCP / ProxyDHCP (UDP)	67 / 4011
Получение начального PXE-загрузчика	PXE-клиент → точка распространения	TFTP (UDP)	69
Получение установочных файлов Windows и обмен данными миграции	Мигрируемое устройство ↔ точка распространения	SMB (TCP)	445

Примечание

Значение 443 приведено по умолчанию — фактически это веб-порт узла (параметр PUBLIC_PORT), заданный при установке. Если узел развёрнут на нестандартном порту (например, на ALT Server порт отличается от 443), укажите соответствующий порт

Важно

В штатном режиме (протокол **RuDesktop**) на управляемых устройствах **не требуется открывать входящие порты** — и управляющий канал, и загрузка файла выполняются исходящими соединениями от самого устройства. Входящий доступ по веб-порту нужен только на серверных узлах: главном сервере и точках распространения

1.13.2 Подключение точки распространения

Для подключения точки распространения к серверу **RuDesktop** выполните следующие шаги

Создание точки распространения в веб-интерфейсе

Создайте точку распространения на странице *Точки распространения* в веб-интерфейсе главного сервера. На этом этапе достаточно указать название и IPv4-адрес узла — параметры будут применены, когда узел выйдет на связь

Настройка главного сервера

Примечание

Этот раздел нужен, если **Redis** и **PostgreSQL** развёрнуты на самом главном сервере — для того, чтобы открыть к ним сетевой доступ с узла точки распространения. Если базы вынесены на отдельные серверы, настраивайте сетевой доступ на них и переходите сразу к разделу *Настройка точки распространения*

Чтобы подключить точку распространения к главному серверу, на котором развёрнуты **Redis** и **Postgres**, необходимо открыть к ним внешнее подключение

Для этого выполните следующие действия:

Redis

Чтобы открыть доступ к **Redis** и защитить его паролем, отредактируйте файл конфигурации, который находится по пути `/etc/rudesktop/redis.conf`

В файле найдите строку, начинающуюся с `bind`, и укажите IP-адрес сервера, например:

```
bind 127.0.0.1 192.168.10.10 -::1
```

И добавьте пароль

```
requirepass <ваш_пароль>
```

Подсказка

Не забудьте заменить `<ваш_пароль>` на актуальный и сложный пароль

Важно

Настройка `requirepass` потребует пароля для всех подключений, что усилит безопасность **Redis-сервера**

В файле `/etc/default/rudesktop` определите переменную, которая используется для указания адреса **Redis**:

```
REDIS_URL='redis://:<ваш_пароль>@127.0.0.1:32459'
```

Postgres

Чтобы открыть доступ к **Postgres** только для определенных узлов, отредактируйте файл конфигурации, который находится по пути `/etc/postgresql/<version>/main/postgresql.conf`

Важно

Возможные пути на разных ОС:

- postgresql.conf

```
/var/lib/pgsql/data/postgresql.conf
/var/lib/pgsql/<version>/data/postgresql.conf
/etc/postgresql/<version>/main/postgresql.conf
/usr/local/pgsql/data/postgresql.conf
```

- pg_hba.conf

```
/var/lib/pgsql/data/pg_hba.conf
/var/lib/pgsql/<version>/data/pg_hba.conf
/etc/postgresql/<version>/main/pg_hba.conf
/usr/local/pgsql/data/pg_hba.conf
```

В файле найдите строку, начинающуюся с `listen_addresses`, и укажите IP-адрес узла, которому вы хотите предоставить доступ, например:

```
listen_addresses = '*'
```

Откройте файл `pg_hba.conf` в той же директории и добавьте строку для разрешения доступа с нужного IP-адреса, например:

```
host    all             all             0.0.0.0/0               ␣
↪ md5
```

Перезапустите службу postgresql:

```
sudo systemctl restart postgresql
```

Перезапустите сервер командой:

```
rude restart
```

Также вы можете развернуть *Redis* и *Postgres* отдельно от главного сервера **RuDesktop** по инструкциям и подключить главный сервер и точку распространения к ним

Настройка точки распространения

1. Добавьте репозиторий

   DEB

   ```
   mkdir -p /usr/share/keyrings/
   wget -qO - https://storage.rudesktop.ru/repos/stable3.1/
    ↪rudesktop.gpg | sudo gpg --dearmor -o /usr/share/
    ↪keyrings/rudesktop.gpg
   echo "deb [signed-by=/usr/share/keyrings/rudesktop.gpg]␣
    ↪https://storage.rudesktop.ru/repos/stable3.1 stable3.1␣
    ↪non-free" | sudo tee /
    ↪etc/apt/sources.list.d/rudesktop.list
   apt-get update -y
   ```

   RPM

   Важно

   Репозиторий доступен для `РЕД ОС`, `AlterOS` и `МСВСфера`

   Для установки на другие операционные системы скачайте *.rpm* пакет и установите его вручную через пакетный менеджер

   Добавьте файл `/etc/yum.repos.d/rudesktop.repo` со следующим содержимым:

   ```
   [rudesktop]
   name=Rudesktop
   baseurl=https://storage.rudesktop.ru/repos/stable3.1/rpms
   gpgcheck=0
   enabled=1
   ```

2. Установите сервер **RuDesktop** с переменной `INSTALL_MODE=executor` на узле:

   DEB

   ```
   INSTALL_MODE=executor apt install rudesktop-server -y
   ```

RPM

```
INSTALL_MODE=executor dnf install rudesktop-server -y
```

Важно

Для `.rpm` пакетов после установки сервера следует обязательно выполнить команду *rude reinstall*

Предупреждение

При выполнении данной команды на ALT Server необходимо указать порт отличный от 443

3. Откройте файл по пути `/etc/default/rudesktop` и добавьте следующее:

```
SETUP_SERVER='Адрес главного сервера'

SECRET_KEY='SECRET_KEY главного сервера'

REDIS_URL='Адрес и порт Redis'

POSTGRES_HOST='Адрес БД'
POSTGRES_PORT='Порт БД'
POSTGRES_DB='Имя БД'
POSTGRES_USER='Пользователь БД'
POSTGRES_PASSWORD='Пароль БД'

PUBLIC_IP='IPv4 адрес точки распространения'
PUBLIC_HOST='Адрес точки распространения, доступный␣
↪PXE-клиентам'
PUBLIC_PORT='Веб-порт точки распространения'
```

Важно

- SETUP_SERVER — укажите адрес главного сервера, например `192.168.10.10`
- SECRET_KEY — скопируйте значение `SECRET_KEY` из файла `/etc/default/rudesktop` главного сервера. Значение должно быть одинаковым на главном сервере и точке распространения: оно используется для проверки подписанных ссылок при загрузке ISO и других файлов
- REDIS_URL — укажите адрес и порт **Redis**, если необходимо с паролем, например `redis://:password@192.168.10.10:32459`
- POSTGRES — укажите настройки **Postgres**

- PUBLIC_IP, PUBLIC_HOST и PUBLIC_PORT — укажите собственный адрес и веб-порт точки. Эти значения используются при генерации PXE-конфигурации и должны быть доступны устройствам в обслуживаемой сети

Предупреждение

Не публикуйте значение `SECRET_KEY` и не передавайте его в открытом виде. Если ключи главного сервера и точки различаются, загрузка ISO завершится ошибкой `403 Forbidden` с сообщением `Signature does not match`

Примечание

Если целевой PXE-образ опубликован на точке распространения, стадии миграции выполняются на этой точке, а собранные данные сохраняются в её SMB-каталоге `migrations`. Устройство получает PXE-файлы и данные миграции с точки распространения, но установленный клиент и запросы завершения установки подключаются к главному серверу, указанному в `SETUP_SERVER`

4. Выполните команду, указав адрес главного сервера:

```
rude setup_server --skip-relay <АДРЕС_ГЛАВНОГО_СЕРВЕРА>
```

5. Перезагрузите узел командой:

```
rude restart
```

6. Запустите задачу и убедитесь, что политики запустились на точке распространения. Перейдите на страницу *Очередь задач* — в колонке Точка распространения должно отображаться название настроенного узла

Проверка доступности Redis

Примечание

Раздел опциональный — нужен только для диагностики, если точка распространения не получает задачи

Чтобы убедиться, что узел может подключиться к **Redis** главного сервера:

1. Установите на узле пакет `redis-tools`
2. Подключитесь к **Redis** главного сервера:

```
redis-cli -h <АДРЕС_ГЛАВНОГО_СЕРВЕРА> -p 32459
```

3. Выполните авторизацию командой AUTH:

```
AUTH <ваш_пароль>
```

Если в ответ возвращается OK, авторизация успешна

Важно

Не передавайте пароль в командной строке через -a или --pass — он может попасть в историю shell или быть виден другим пользователям через список процессов. Используйте интерактивный AUTH после подключения

4. Выполните команду PING. Ответ PONG означает, что узел успешно установил соединение с **Redis**

1.13.3 Обновление точки распространения

После обновления главного сервера на новую версию обновите точку распространения до **той же версии** — иначе часть функциональности может работать некорректно.

Обновление выполняется на узле точки распространения:

1. Обновите пакет сервера **RuDesktop**:

DEB

```
apt-get update -y
apt-get install --only-upgrade rudesktop-server -y
```

RPM

```
dnf update rudesktop-server -y
```

2. Перезапустите узел:

```
rude restart
```

3. Убедитесь, что точка снова вышла на связь: на вкладке **«Информация об узле»** страницы *Точки распространения* отобразится актуальная версия сервера

1.14 Интеграции

1.14.1 Интеграция с модулем аналитики

Доступно только в UEM версии

Интеграция с модулем аналитики — передача справочных данных из внешней системы в отдельную таблицу базы данных сервера **RuDesktop** через REST API модуля аналитики, без предоставления внешней системе прямого доступа к PostgreSQL

Назначение

Во внешней системе часто хранится актуальный справочник, который нужен в отчётах: перечень ПО с признаками запрета, список разрешённых устройств и т.п. Если справочник меняется, каждый раз вручную переписывать SQL виртуального датасета неудобно

Интеграция работает так:

1. На сервере выпускается токен доступа к REST API модуля аналитики — командой `rude superset token create`
2. Внешняя система передаёт токен в заголовке `Authorization` запросов и загружает справочник в виде CSV-файла
3. По загрузке в базе данных сервера создаётся отдельная таблица со справочником
4. Виртуальный датасет читает справочник из этой таблицы вместо жёстко заданных значений
5. При изменении справочника внешняя система повторяет загрузку — таблица заменяется целиком, SQL датасета не меняется

Подсказка

Модуль аналитики — встроенный Apache Superset[12]. Порядок его установки — на странице *Установка модуля аналитики*, устройство раздела **Аналитика** — в *руководстве пользователя*

Требования

- Лицензия **UEM** и установленный запущенный модуль аналитики (`rude superset status`)
- У подключения **RuDesktopDB** включена настройка **«Загрузка из файла»**: **Отчёты** → **Аналитика** → **Базы данных** → наведите на **RuDesktopDB** → **Редактировать** → включите переключатель **«Загрузка из файла»** (подробнее — *Базы данных*)
- Токен доступа, выпущенный командой `rude superset token create`
- Сетевой доступ с узла внешней системы к веб-интерфейсу сервера (порт 443)

Загрузка файлов требует роли **Admin** модуля аналитики. Роль назначается автоматически при входе через **SSO**: суперпользователь **RuDesktop** получает **Admin**, остальные пользователи — **Public** без права загрузки. Пользователь,

[12] https://superset.apache.org/

на которого выпускается токен, должен уже существовать в модуле аналитики — два способа его завести:

- **техническая учётная запись под загрузку** (рекомендуется): создайте её прямо в модуле аналитики с ролью **Admin** — через интерфейс (`https://[SERVER_ADDR]/analytics/users/add`) или командой `rude superset fab create-user` (см. *superset token*). Учётная запись на сервере **RuDesktop** для неё не нужна, вход по SSO выполнять не требуется
- **существующий пользователь**: если пользователь уже входил в раздел **Аналитика**, его учётная запись создалась автоматически при первом входе

Шаг 1. Получение токена

Токен выпускается на сервере командой *superset token create* и печатается в стандартный вывод — сохраните его, повторно получить значение нельзя:

```
rude superset token create [имя_пользователя]
```

Дальше токен передаётся в заголовке `Authorization` каждого запроса к REST API модуля аналитики:

```
curl -k -H "Authorization: Bearer [TOKEN]" -H "Accept:␣
↪application/json" \
   "https://[SERVER_ADDR]/analytics/api/v1/database/"
```

Ответ `200` со списком подключённых баз подтверждает, что доступ работает. Поле `id` записи `RuDesktopDB` в `result` — идентификатор базы, в которую загружается справочник (для единственной базы обычно 1); далее в примерах используется `[DATABASE_ID]`

Примечание

Ответ `401` на запрос с корректным токеном означает, что установленный модуль аналитики ещё не поддерживает авторизацию по токенам — обновите пакет `rudesktop-superset`

Важно

Передавайте `Accept: application/json` во всех запросах. Без этого заголовка (например, в curl по умолчанию) сообщения об ошибках API могут приходить не в JSON, а HTML-страницей с кодом `500` — с заголовком тот же запрос возвращает корректный JSON-ответ со статусом 4xx и описанием ошибки

Шаг 2. Подготовка CSV-файла

Первая строка файла — имена колонок. Для справочника ПО с параметрами `software`, `pattern`, `exclude`, `kind`, `allowed`:

```
software,pattern,exclude,kind,allowed
Bittorrent,bittorrent,,forbidden,
Transmission,transmission,common|libtransmission,forbidden,
Wireshark,wireshark,,restricted,"RU78994,RM83190"
AnyDesk,anydesk,,restricted,RDU3478
```

Правила форматирования:

- Пустое поле загружается как `NULL`
- Значение с запятой заключается в двойные кавычки: `"RU78994,RM83190"`
- Регулярное выражение в колонке `exclude` передаётся как обычная строка, спецсимволы экранировать не нужно: `common|libtransmission`

Проверить, что модуль аналитики правильно читает файл, можно до загрузки — эндпоинт вернёт распознанные колонки:

```
curl -k -H "Authorization: Bearer [TOKEN]" -H "Accept:␣
↪application/json" -X POST \

↪"https://[SERVER_ADDR]/analytics/api/v1/database/upload_metadata/"␣
↪\
    -F "file=@perechen.csv" -F "type=csv"
```

Ответ: `{"result": {"items": [{"column_names": ["software", "pattern", "exclude", "kind", "allowed"], "sheet_name": null}]}}`

Шаг 3. Первая загрузка справочника

Загрузка создаёт в базе таблицу с указанным именем:

```
curl -k -H "Authorization: Bearer [TOKEN]" -H "Accept:␣
↪application/json" -X POST \
    "https://[SERVER_ADDR]/analytics/api/v1/database/[DATABASE_ID]/u
↪pload/" \
    -F "file=@perechen.csv" \
    -F "type=csv" \
    -F "schema=public" \
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
    -F "table_name=perechen" \
    -F "already_exists=fail" \
    -F 'column_data_types={"software": "string", "pattern":
↪"string", "exclude": "string", "kind": "string", "allowed":
↪"string"}'
```

Успешная загрузка возвращает `201` и `{"message": "OK"}`

Обязательные параметры:

- `table_name` — имя создаваемой таблицы, в примере `perechen`; таблица создаётся в схеме из параметра `schema` (`public`)
- `type` — формат файла, `csv`
- `already_exists` — поведение при существующей таблице: `fail` (ошибка), `replace` (заменить данные), `append` (добавить строки)
- `column_data_types` — JSON со строковыми типами колонок

Предупреждение

Явно указывайте типы колонок через `column_data_types`. При автоматическом определении полностью пустая колонка получает неверный тип — например, колонка `exclude`, в которой все значения пустые, создаётся как `double precision`. С явными типами все пять колонок создаются строковыми (`TEXT`)

Поддерживаются типы библиотеки pandas: `string`, `int`, `float`, `boolean` и другие

Шаг 4. Обновление справочника

Для повторной загрузки в существующую таблицу укажите `already_exists=replace` — предыдущее содержимое полностью заменяется новыми данными:

```
curl -k -H "Authorization: Bearer [TOKEN]" -H "Accept:␣
↪application/json" -X POST \
    "https://[SERVER_ADDR]/analytics/api/v1/database/[DATABASE_ID]/u
↪pload/" \
    -F "file=@perechen.csv" \
    -F "type=csv" \
    -F "schema=public" \
    -F "table_name=perechen" \
    -F "already_exists=replace" \
    -F 'column_data_types={"software": "string", "pattern":
↪"string", "exclude": "string", "kind": "string", "allowed":
↪"string"}'
```

Примечание

При `already_exists=fail` и уже существующей таблице данные не меняются, запрос возвращает 422 с сообщением «Таблица уже существует...». Для регулярного обновления используйте `replace`

Важно

Режим `replace` пересоздаёт таблицу целиком. Если во внешней системе изменился не только состав строк, но и состав колонок, обновите столбцы в датасете кнопкой **«Синхронизировать из источника»** — см. *Датасеты*

Использование в виртуальном датасете

Созданная таблица сразу доступна в **SQL Lab** и как источник для датасетов. В SQL виртуального датасета замените блок значений на выборку из таблицы

Было — справочник вписан в запрос:

```
WITH
perechen(software, pattern, exclude, kind, allowed) AS (
    VALUES
        ('Bittorrent', 'bittorrent', NULL, 'forbidden', NULL),
        ('Transmission', 'transmission', 'common|libtransmission',
↪'forbidden', NULL),
        ('Wireshark', 'wireshark', NULL, 'restricted',
↪'RU78994,RM83190'),
        ('AnyDesk', 'anydesk', NULL, 'restricted', 'RDU3478')
),
matched AS (
    ...
)
```

Стало — справочник читается из таблицы:

```
WITH
perechen(software, pattern, exclude, kind, allowed) AS (
    SELECT
        software,
        pattern,
        exclude,
        kind,
        allowed
    FROM public.perechen
),
matched AS (
    ...
)
```

Дальнейшая логика датасета не меняется. После обновления таблицы внеш-

ней системой при следующем выполнении запроса используется актуальное содержимое справочника

Полный пример скрипта загрузки

Скрипт проверяет файл и загружает его с полной заменой; подходит для запуска по расписанию из внешней системы:

```
#!/bin/bash
set -e

SERVER="https://[SERVER_ADDR]"
TOKEN="[TOKEN]"
DATABASE_ID="1"
TABLE="perechen"
FILE="perechen.csv"
TYPES='{"software": "string", "pattern": "string", "exclude":
 ↪"string", "kind": "string", "allowed": "string"}'
AUTH="Authorization: Bearer $TOKEN"
ACCEPT="Accept: application/json"

# 1. Проверка файла
curl -k -s -H "$AUTH" -H "$ACCEPT" -X POST "$SERVER/
 ↪analytics/api/v1/database/upload_metadata/" \
    -F "file=@$FILE" -F "type=csv"

# 2. Загрузка с полной заменой
curl -k -s -H "$AUTH" -H "$ACCEPT" -X POST "$SERVER/
 ↪analytics/api/v1/database/$DATABASE_ID/upload/" \
    -F "file=@$FILE" -F "type=csv" -F "schema=public" \
    -F "table_name=$TABLE" -F "already_exists=replace" \
    -F "column_data_types=$TYPES"
```

Хранение и отзыв токена

- Токен действует от имени учётной записи со всеми её правами — используйте учётную запись, созданную специально под интеграцию, и не используйте её для входа людей
- Храните токен как секрет — в хранилище секретов внешней системы, не в репозитории и не в открытом виде в задачах планировщика
- Срок действия можно ограничить при выпуске: `--days N` — по истечении токен перестаёт действовать сам, без отзыва
- Отзыв — командой `rude superset token revoke` (по значению токена или его `uuid` из списка *superset token list*); отзыв применяется сразу
- Между внешней системой и сервером должен использоваться HTTPS. Флаг `-k` в примерах отключает проверку встроенного самоподписанного сертификата; если на сервере установлен корпоративный сертификат, проверку лучше не отключать

1.14.2 Интеграция с Jatoba

Jatoba — ПО общего назначения, предназначенное для создания и управления реляционными базами данных

Примечание

Ядро СУБД Jatoba построено на основе одной из самых известных в мире СУБД с открытым исходным кодом `PostgreSQL`

Интеграция

Для интеграции вам необходимо:

- Подготовленный пакет сервера **RuDesktop**

  Важно

  Подготовленный пакет сервера можно получить, связавшись с нашим отделом продаж: sales@rudesktop.ru

- Пакет **Jatoba** с лицензионным ключом

Пример интеграции

1. Установить сервер **RuDesktop**
2. Установить и активировать **Jatoba**

   Примечание

   Руководство по установке Jatoba: https://www.gaz-is.ru/produkty/inform-sistemy/subd-jatoba#materialy

3. Проверить работоспособность сервиса **Jatoba**

   ```
   systemctl start jatoba-4
   systemctl enable jatoba-4
   ```

4. Выполнить предварительную сборку сервера

   ```
   rude install [СЕРВЕР:ПОРТ]
   ```

5. Перейти в `/etc/systemd/system` и заменить строку **postgresql.service** на **jatoba-4.service** в следующих файлах:
   - rudesktop-executor.service
   - rudesktop-pxe.service
   - rudesktop-relay.service
   - rudesktop-web.service

6. Отредактировать файл по пути `/var/lib/jatoba/4/data/pg_hba.conf` по шаблону:

```
# TYPE  DATABASE        USER            ADDRESS
 ↪       METHOD
# "local" is for Unix domain socket connections only
local   all             all
 ↪       peer
# IPv4 local connections:
host    all             all             127.0.0.1/32
 ↪       md5
# IPv6 local connections:
host    all             all             ::1/128
 ↪       md5
# Allow replication connections from localhost, by a␣
 ↪user with the
# replication privilege.
local   replication     all
 ↪       peer
host    replication     all             127.0.0.1/32
 ↪       md5
host    replication     all             ::1/128
 ↪       md5
```

7. Создать в СУБД пользователя **rudesktop** с паролем из файла `/var/default/rudesktop`

> **Важно**
>
> Пароль находится в поле **POSTGRES_PASSWORD**

8. Создать в СУБД базу данных с именем **rudesktop**

> **Важно**
>
> Выдать пользователю **rudesktop** все права на базу **rudesktop**

9. Запустить сервис **rudesktop-web**

```
systemctl start rudesktop-web.service
```

10. Запустить создание структуры базы данных сервера

```
rude migrate
```

11. Создать **суперпользователя** на сервере

```
rude createsuperuser
```

12. Теперь можно перейти в веб-интерфейс сервера, авторизоваться и начать пользоваться сервисом

1.14.3 Интеграция с KSC

KSC — Kaspersky Security Center, предназначенная для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации

Сведения о совместной работе приведены в разделе Совместимость с Kaspersky Endpoint Security

Если **Kaspersky Endpoint Security** сообщает об ошибке доверия к сертификату сервера **RuDesktop**, добавьте сертификат в доверенные через политику KES в KSC. Это настройка доверия со стороны KES; она не заменяет настройку сертификатов в других приложениях

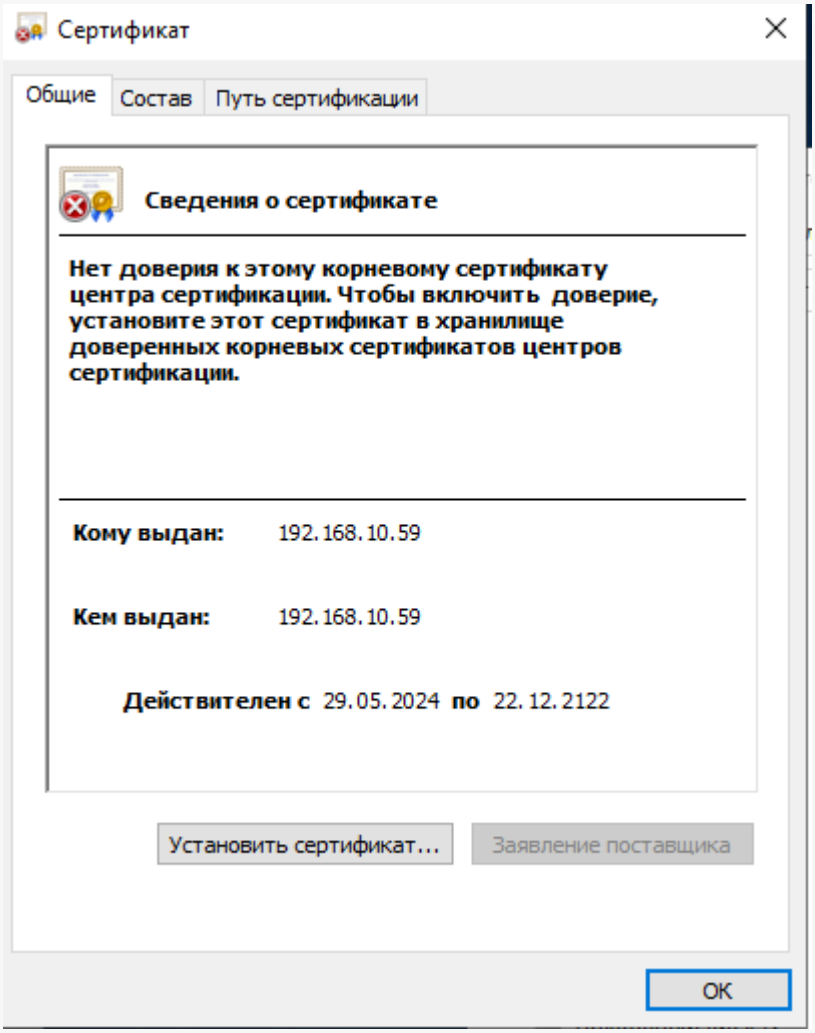
Действия на сервере RuDesktop

1. Перейти в веб-интерфейс сервера **RuDesktop**
2. Перейти на страницу **Администрирование** -> **Сертификаты**
3. Открыть свойства карточки сертификата
4. Скопировать текст сертификата
5. Создать текстовый файл и вставить в него скопированный текст
6. Сохранить файл с расширением `.cer`

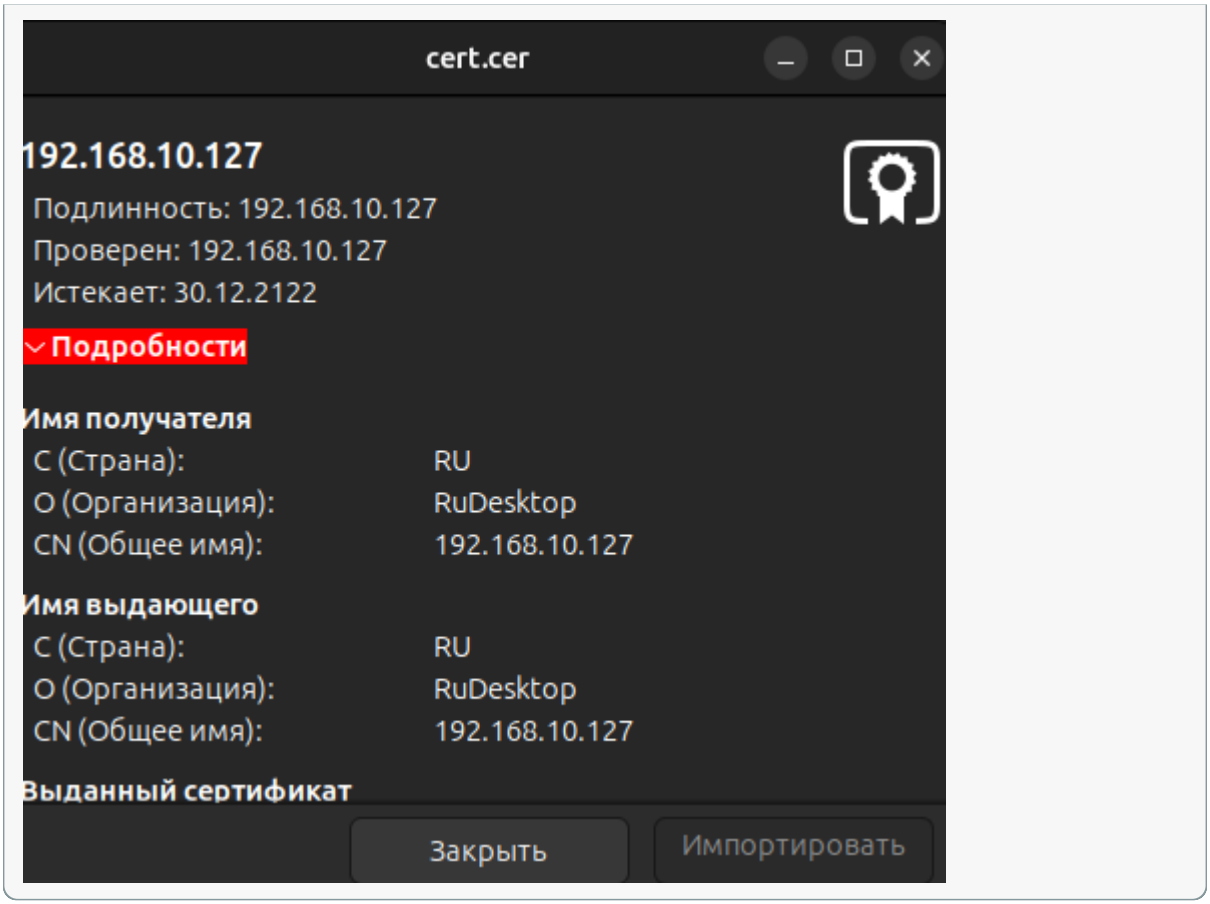
Примечание

Если действия выполнены верно, то при попытке открытия файла сертификата появится следующее окно:

На Windows

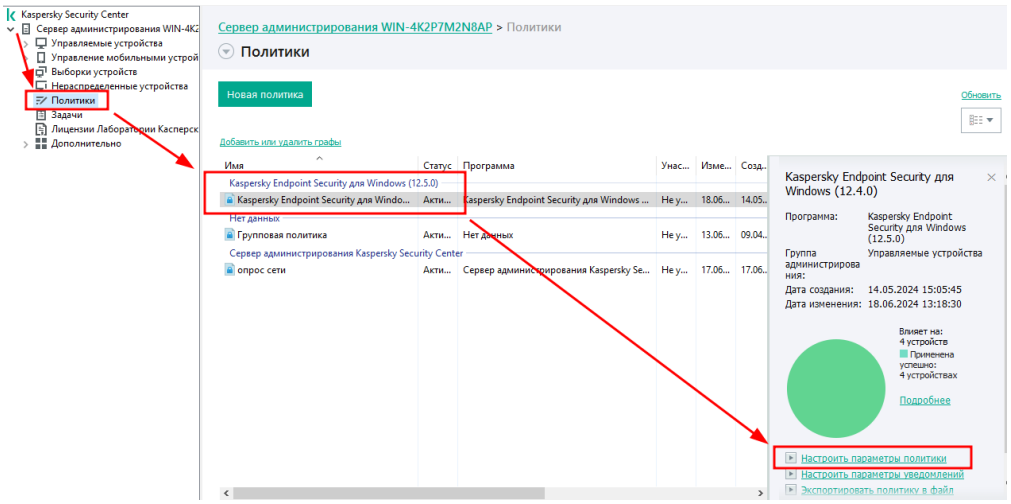

Сертификат
Общие
Состав
Путь сертификации
Сведения о сертификате
Нет доверия к этому корневому сертификату центра сертификации. Чтобы включить доверие, установите этот сертификат в хранилище доверенных корневых сертификатов центров сертификации.
Кому выдан: 192.168.10.59
Кем выдан: 192.168.10.59
Действителен с 29.05.2024 по 22.12.2122
Установить сертификат...
Заявление поставщика
OK

На Linux



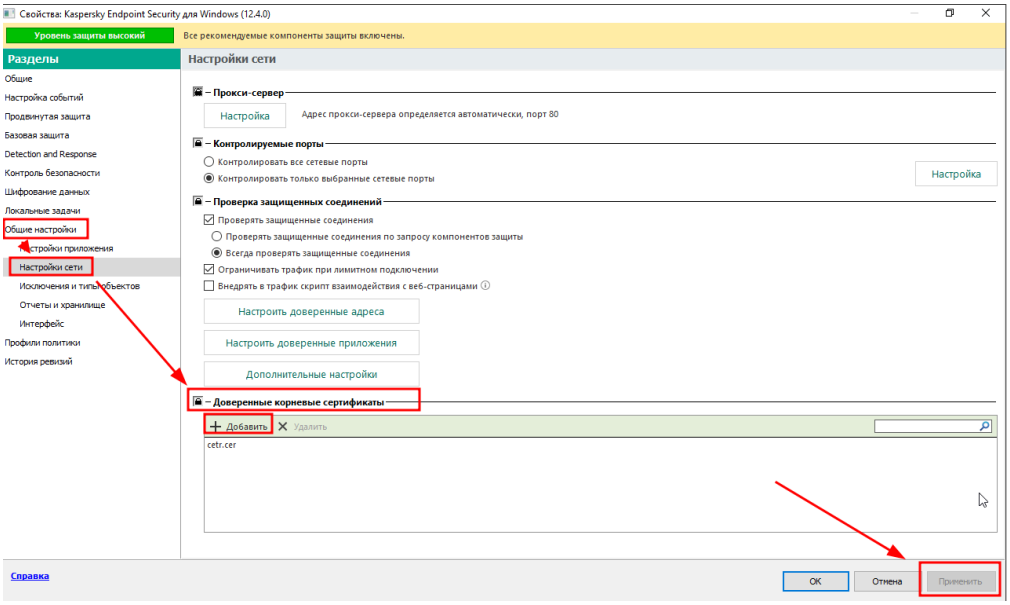
Действия в KSC

1. В панели администрирования перейти в **Политики**
2. Выбрать политику **Kaspersky Endpoint Security**
3. В блоке информации о политике выбрать пункт **Настроить параметры политики**



4. В открывшемся окне настроек политики перейти в группу настроек **Общие настройки -> Настройки сети**

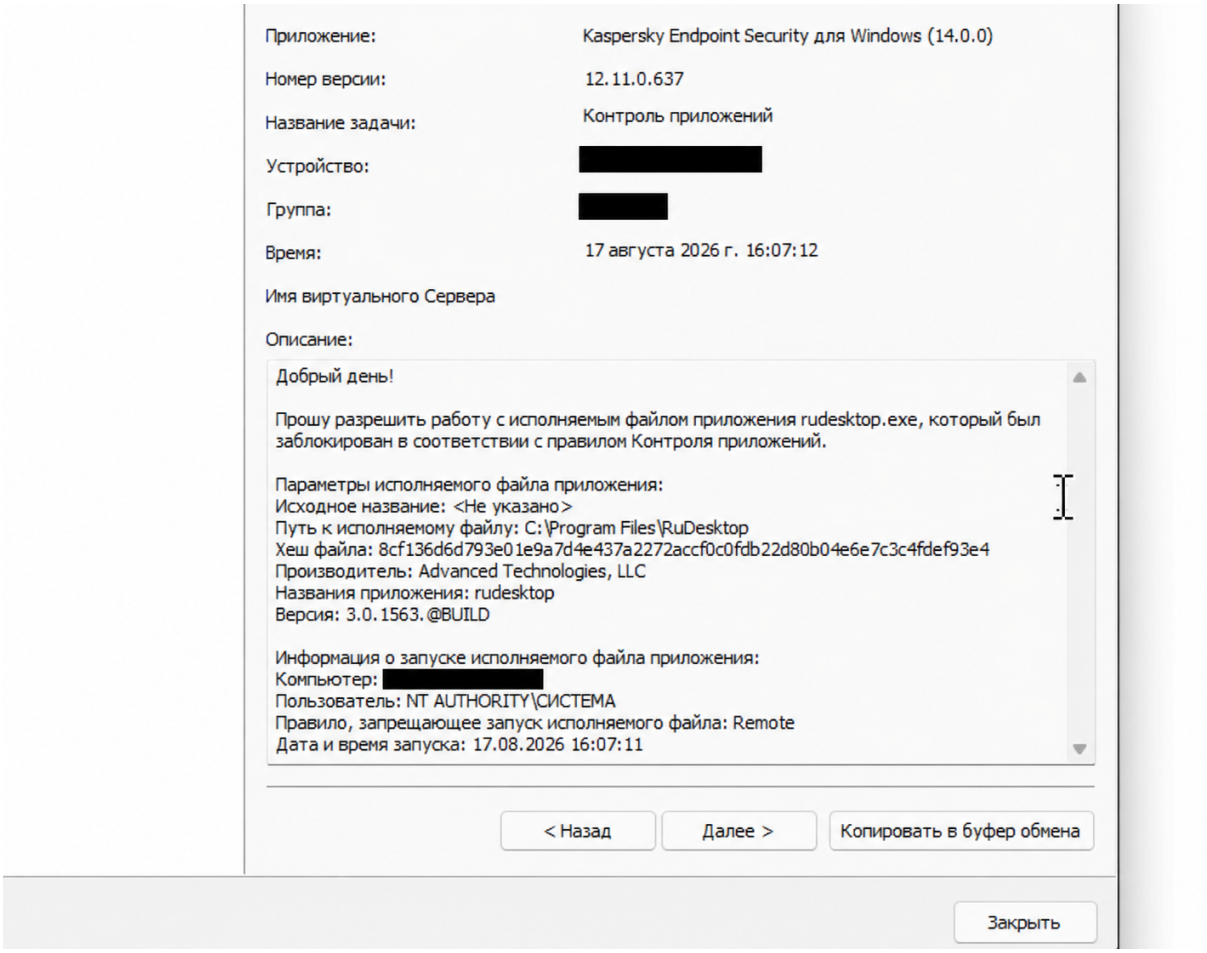
5. Нажать на кнопку **Добавить** в блоке **Доверенные корневые сертификаты**
6. Выбрать ранее созданный файл сертификата
7. Нажать кнопку **Применить**



8. Дождаться применения политики на рабочей станции и повторить подключение к серверу **RuDesktop**

Блокировка запуска Контролем приложений

Если запуск `rudesktop.exe` запрещён правилом **Контроля приложений** KES для Windows, настройте исключение для RuDesktop. Ниже приведён пример сообщения о блокировке



Настройка исключения

Если запрещающее правило использует пополняемую вручную категорию программ, примените рекомендацию технической поддержки RuDesktop:

1. По событию блокировки определить запрещающее правило и используемую им категорию программ
2. В KSC открыть используемую правилом пополняемую вручную категорию и настройку условий исключения программ из категории
3. Добавить условие **Сертификаты файлов из папки** и выбрать директорию с установочным MSI-пакетом **RuDesktop**
4. Проверить полученное условие: сертификат должен соответствовать подписи файла `rudesktop.exe`, запуск которого блокируется. Если сертификат не определился или отличается, обратиться в техническую поддержку RuDesktop
5. Сохранить изменения, дождаться их применения на устройстве и повторить запуск RuDesktop
6. Проверить удалённое подключение и выполнение используемых политик UEM при включённой защите, а также отсутствие повторной блокировки в событиях KES

Важно

Этот порядок предназначен для запрещающего правила. При использовании разрешающего списка настройте правило, разрешающее запуск RuDesktop. Названия и расположение элементов интерфейса зависят от версии и типа консоли KSC

Условие **Сертификаты файлов из папки** распространяется на файлы, подписанные выбранным сертификатом, а не только на MSI-пакет. Выберите каталог, содержащий только дистрибутив RuDesktop, чтобы не добавить сертификаты посторонних программ. Исключать весь каталог RuDesktop из антивирусной проверки для этой настройки не требуется

Описание условий включения и исключения программ — в документации Kaspersky[13]

1.14.4 Интеграция с Multifactor

Описание

Для добавления второго фактора аутентификации (например, подтверждения через приложение на телефоне) при авторизации в **RuDesktop** вы можете использовать популярное решение `Multifactor`

Настройка **RuDesktop** будет довольно простой — в качестве LDAP-сервера следует указать LDAP-прокси-сервер `Multifactor`

Подсказка

Подробную информацию о настройке можно найти здесь: LDAP proxy сервер для Linux[14]

Пример

1. Создать аккаунт на сайте Multifactor[15]

   Подсказка

   В качестве второго фактора авторизации будет использоваться мобильное приложение

2. Для использования `Multifactor` необходимо установить сервер внутри вашей сети для настройки LDAP-прокси

[13] https://support.kaspersky.com/KESWin/11.4.0/ru-RU/130537.htm
[14] https://multifactor.ru/docs/ldap-adapter/ldap-proxy-server-dlya-linux/
[15] https://multifactor.ru

Примечание

В приведенном примере использовалась виртуальная машина **Ubuntu 22.04**

3. В параметрах LDAP-прокси `Multifactor` необходимо указать данные для подключения к реальному LDAP-серверу

   Пример параметров:

```
<configSections>
        <section name="UserNameTransformRules" type="Mult
↪iFactor.Ldap.Adapter.Configuration.UserNameTransformRul
↪esSection, MultiFactor.Ldap.Adapter" />
</configSections>

<appSettings>
        <!--This service LDAP endpoint (0.0.0.0 - listen␣
↪all interfaces) -->
        <add key="adapter-ldap-endpoint" value=
↪"0.0.0.0:389"/>
        <!--This service LDAPS (TLS) endpoint (0.0.0.0␣
↪listen all interfaces) -->
        <add key="adapter-ldaps-endpoint" value=
↪"0.0.0.0:636"/>

        <!--Active Directory IP or domain -->
        <add key="ldap-server" value=
↪"ldap://win2012.local"/>

        <!-- Base DN for user binding. Example:␣
↪cn=users,cn=accounts,dc=domain,dc=local -->
        <!--<add key="ldap-base-dn" value=""/>-->

        <!--List of service accounts (Bind DN) delimited␣
↪by semicolon (option 1)-->
        <add key="ldap-service-accounts" value=
↪"cn=phil,cn=users,dc=win2012, dc=local"/>

        <!--Service accounts (Bind DN) organization unit␣
↪(OU) (option 2)-->
        <add key="ldap-service-accounts-ou" value=
↪"OU=Service Accounts"/>

        <!--ActiveDirectory access group (optional); -->
        <!--add key="active-directory-group"␣
↪value="MyApp Users"/-->

        <!--ActiveDirectory 2FA group (optional); -->
        <!--add key="active-directory-2fa-group"␣
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
↪value="MyApp 2FA Users"/-->

        <!--Multifactor API -->
        <add key="multifactor-api-url" value=
↪"https://api.multifactor.ru" />
        <!-- get it from multifactor management panel -->
        <add key="multifactor-nas-identifier" value=
↪"rs_ccf056cb5d94dd4880addaf4be36b" />
        <!-- get it from multifactor management panel -->
        <add key="multifactor-shared-secret" value="" />

        <!--HTTP proxy for API (optional) -->
        <!--add key="multifactor-api-proxy"␣
↪value="http://proxy:3128"/-->
        <!--add key="transform-ldap-identity"␣
↪value="upn"/-->

        <!-- minimal log level: 'Debug', 'Info', 'Warn',
↪'Error' -->
        <add key="logging-level" value="Debug"/>
        <!--<add_key="logging-format" value="json"/>-->
        <!--certificate password leave empty or null for␣
↪certificate without password-->
        <!--<add key="certificate-password"␣
↪value="XXXXXX" />-->
</appSettings>
```

4. В веб-интерфейсе **RuDesktop** необходимо *создать домен по инструкции*

> **Важно**
>
> Однако в качестве **IP-адреса** сервера домена следует указать **IP-адрес** LDAP-прокси-сервера `Multifactor`
>
> Проверка доступа должна пройти успешно

5. Войти в веб-интерфейс **RuDesktop** или авторизоваться в клиенте, используя доменную учётную запись

> **Важно**
>
> Если учётной записи ещё не существует в `Multifactor`, авторизация не будет успешной. Однако произойдёт важное событие: на сервер `Multifactor` будет отправлено уведомление о новой попытке входа с новым логином, и этот логин будет создан на стороне `Multifactor`

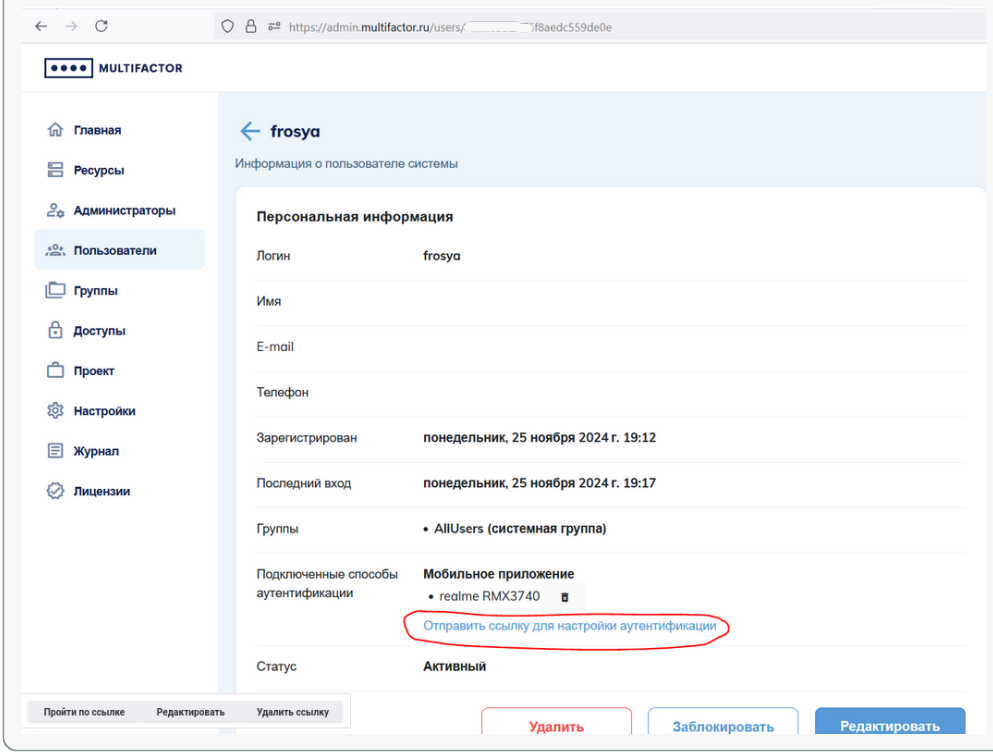
`Multifactor` работает только при наличии доступа к интернету по адресу: https://api.multifactor.ru. Необходимо обеспечить доступ к этому URL

6. Отправить клиенту инструкцию по настройке второго фактора аутентификации

Подсказка

Самый простой способ — использовать приложение

Для этого на портале `Multifactor` в разделе **Пользователи** найдите новый аккаунт и нажмите на кнопку Отправить ссылку для настройки аутентификации



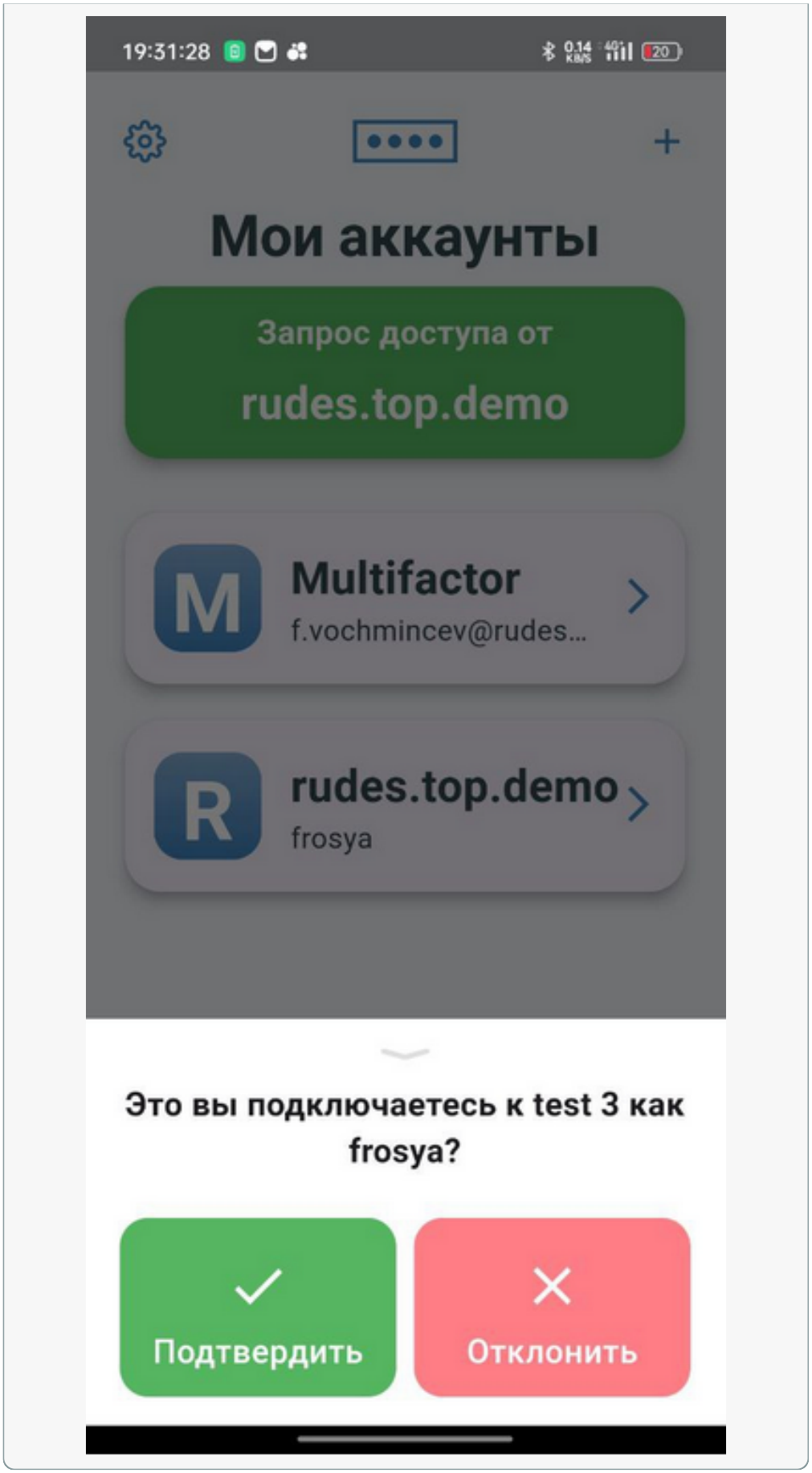
7. Пройти все шаги настройки второго фактора, используя письмо с инструкцией
8. Теперь при входе в веб-интерфейс **RuDesktop** или при авторизации в клиенте пользователь должен будет подтверждать свою авторизацию с помощью второго фактора

Важно

Только после этого он сможет войти в систему

Подсказка

Сообщение о получении второго фактора авторизации на телефоне в приложении `Multifactor` выглядит так:


19:31:28
Мои аккаунты
Запрос доступа от
rudes.top.demo
Multifactor
f.vochmincev@rudes...
rudes.top.demo
frosya
Это вы подключаетесь к test 3 как frosya?
Подтвердить
Отклонить

Важно

Перед подтверждением второго фактора авторизации сессия находится в ожидании

Это касается авторизации как в веб-интерфейсе **RuDesktop**, так и в клиенте

1.14.5 Интеграция с Rusiem

Описание

Интеграция с Rusiem позволяет получать события **RuDesktop** через Syslog, разбирать их в SIEM и настраивать корреляции для обнаружения инцидентов

Подсказка

Перед настройкой интеграции включите отправку событий из **RuDesktop** по инструкции: *Настройка Syslog*

Пример

1. Настроить отправку событий из **RuDesktop** в Syslog
2. Установить пакет парсера **RuDesktop** на сервере Rusiem

   ```
   dpkg -i <полный_путь_до_пакета>
   ```

3. Обновить базу знаний Rusiem для применения парсера

   ```
   /opt/rusiem/bin/update.sh --kb
   ```

   Подсказка

   Обычно парсер применяется через несколько минут

   Важно

   Если парсер не применился, перезапустите сервер с Rusiem

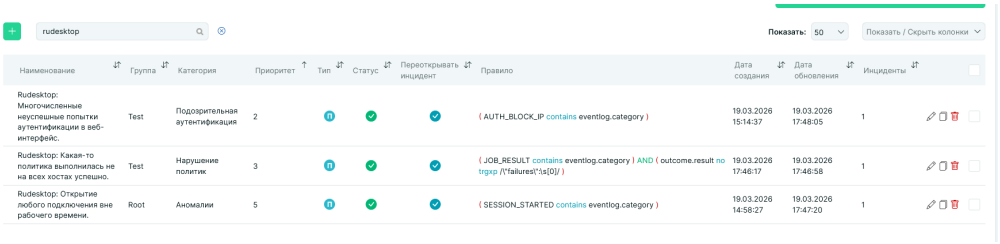
4. Создать или импортировать правила корреляции по событиям **RuDesktop**

   Скачайте файл с правилами корреляции

   Во вложенном файле содержатся три правила корреляции, настроенные в Rusiem

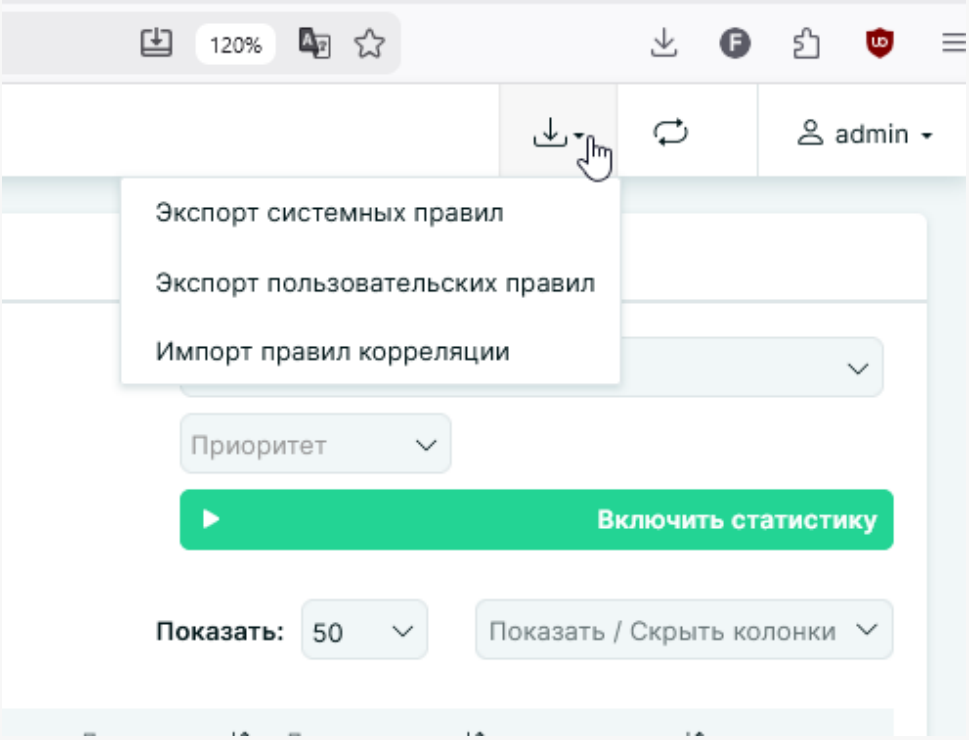
   Для каждого правила подготовлен отдельный кейс на основе событий **RuDesktop**:

- **RuDesktop: Многочисленные неуспешные попытки аутентификации в веб-интерфейс**
- **RuDesktop: Какая-то политика выполнилась не на всех хостах успешно**
- **RuDesktop: Открытие любого подключения вне рабочего времени**



Подсказка

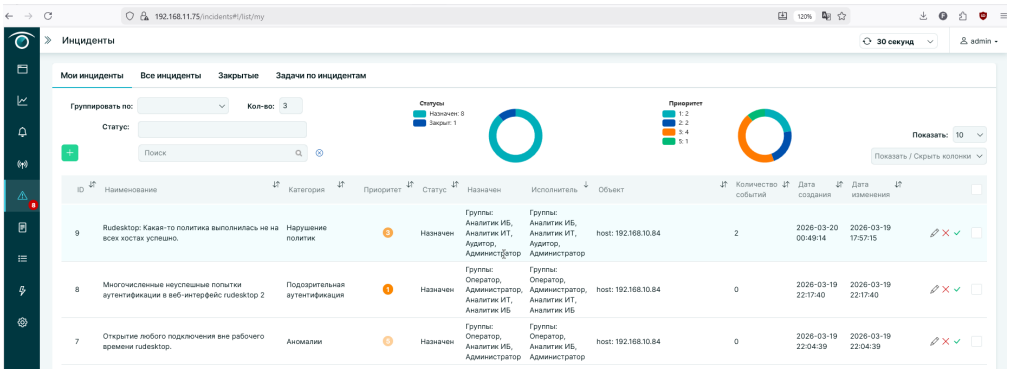
Чтобы загрузить правила корреляции, перейдите в раздел **Корреляции -> Правила корреляции**, нажмите кнопку со стрелкой вниз и выберите пункт **Импорт правил корреляции**



Затем выберите файл `rudesktop_correlation_rules.json`

После этого правила будут загружены в `Rusiem` для работы описанных политик

5. Проверить, что правила формируют инциденты в `Rusiem`



Интеграции — раздел с инструкциями по подключению сервера **RuDesktop** к внешним системам: использование российской СУБД **Jatoba** вместо PostgreSQL, синхронизация устройств с **Kaspersky Security Center**, многофакторная аутентификация через **Multifactor**, отправка аудита в **RuSIEM** и передача внешних справочников в модуль аналитики через REST API

Модуль аналитики

Передача внешних справочников через REST API

Jatoba

Использование российской СУБД Jatoba как замены PostgreSQL

Kaspersky Security Center

Двусторонняя интеграция с Kaspersky Security Center

Multifactor

Многофакторная аутентификация через сервис Multifactor

Rusiem

Отправка событий аудита в SIEM-систему RuSIEM

1.15 Настройка PXE

1.15.1 Описание PXE-сервера

Описание PXE-сервера — общий принцип работы встроенного PXE-сервера **RuDesktop** для удалённой установки ОС в локальной сети, состав компонентов сервиса, этапы загрузки клиента, схема DHCP-proxy, расположение загрузочных файлов и пользовательских override-конфигов

Определения

PXE (Preboot Execution Environment) — сетевой стандарт или протокол, созданный Intel, который определяет способ загрузки операционной системы через сеть, используя сетевую карту компьютера

> **Примечание**
>
> PXE-код, находящийся в ПЗУ сетевой карты или в прошивке BIOS/UEFI, получает от DHCP/BOOTP-сервера IP-адрес и параметры загрузки (адрес TFTP-сервера и имя загрузочного файла), после чего по протоколу TFTP загружает указанный файл и передаёт ему управление

BOOTP — протокол автоматической конфигурации IP-адреса (предшественник DHCP), работающий поверх UDP и позволяющий хосту получить сетевые параметры от сервера

TFTP — простой протокол передачи файлов, который позволяет клиенту получить файл с удалённого хоста или поместить файл на удалённый хост. Часто используется именно на этапе PXE-загрузки для получения первого загрузочного файла

Компоненты PXE-сервера RuDesktop

PXE-сервер реализован в виде systemd-сервиса `rudesktop-pxe.service` и включает:

- **DHCP-сервер на порту 67** — отвечает PXE-клиентам `DHCP Offer` (без выдачи IP-адреса). IP клиенту выдаёт обычный DHCP-сервер сети (например, MikroTik или DHCPD)
- **ProxyDHCP-сервер на порту 4011** — отвечает на `DHCP Request`, передавая адрес TFTP-сервера и имя загрузочного файла, выбранного с учётом архитектуры клиента
- **TFTP-сервер** — обслуживает каталог `/var/lib/rudesktop/pxe/tftp/`, отдаёт первичный загрузчик и iPXE-скрипты
- **SMB-сервер** (`smbd`) — используется для установки **Windows**: образ Windows PE/инсталлятор отдаётся клиенту по протоколу SMB после загрузки wimboot

Сервис автоматически запускается и останавливается при *публикации образа ОС*

Этапы работы PXE

1. Инициализация сети

   При включении компьютера выполняется процедура **POST** (Power-On Self Test), после чего инициализируется сетевой интерфейс и выполняется код **PXE** (через BIOS/UEFI или ПЗУ сетевой карты)

2. DHCP-запрос

   Компьютер, настроенный на загрузку через **PXE**, отправляет DHCP-запрос (DHCP Discover) в локальную сеть для получения IP-адреса и информации о загрузочном сервере

   Примечание

   Запрос может быть широковещательным

3. DHCP-ответ

   DHCP-сервер отвечает на запрос, предоставляя:

   - IP-адрес
   - Маску подсети
   - Шлюз
   - Дополнительные DHCP-опции

   Дополнительные DHCP Options (типичные):

   - **Option 66** — адрес TFTP-сервера (или next-server)
   - **Option 67** — имя начального загрузочного файла (например, ipxe.efi для UEFI или undionly.kpxe для BIOS). В ответе DHCP-сервер может также включать различные опции, которые помогают клиенту во время загрузки

   Важно

   Сервер **Rudesktop** использует собственный `DHCP PROXY`

4. Загрузка загрузчика

   После получения информации о TFTP-сервере и имени файла PXE-клиент загружает первичный сетевой загрузчик по протоколу TFTP

   Примечание

   Этот загрузчик может быть, например:

   - `iPXE` (файлы ipxe.efi, undionly.kpxe)
   - `PXELINUX` (pxelinux.0)
   - Другие сетевые загрузчики

   Именно этот файл, указанный в **Option 67**, является первым исполняемым кодом, который приходит по сети

5. Загрузка операционной системы

После загрузки первичного сетевого загрузчика (например, iPXE) он:

- Может предоставить меню для выбора операционной системы или сценария загрузки
- Может автоматически загрузить конфигурационный файл (например, autoexec.ipxe)
- Далее загружает ядро ОС, initrd или вспомогательные загрузчики

Для Windows на этом этапе обычно используется wimboot (как второй загрузчик), который:

- Загружается самим iPXE
- Затем загружает файлы Windows PE/установщика (WIM-образ и сопутствующие файлы) по протоколу **SMB** с сервера **RuDesktop** (служба `smbd` запускается автоматически при публикации образа Windows)

Для Linux через iPXE обычно загружаются:

- ядро (vmlinuz)
- initrd
- параметры командной строки ядра (часто описаны в autoexec.ipxe или аналогичном iPXE-скрипте)

6. Инициализация ОС

   После завершения загрузки образа операционной системы (Windows PE, инсталлятор Windows или Linux initrd+kernel), он передаётся в память, и компьютер начинает выполнение кода ОС

Как работает DHCP proxy

1. При загрузке PXE-клиента он отправляет в сеть широковещательное сообщение **DHCP Discover**, которое содержит список информации, которую клиент хотел бы получить от DHCP-сервера, а также сведения, идентифицирующие его как устройство с поддержкой PXE (через Option 60: PXEClient)
2. Обычный **DHCP-сервер** отвечает предложением (DHCP Offer), которое содержит возможные значения для сетевых настроек, запрашиваемых клиентом. Обычно это IP-адрес, маска подсети, адрес маршрутизатора (шлюза), адрес DNS-серверов и т.д.
3. Поскольку клиент идентифицировал себя как PXE-клиент, **ProxyDHCP-сервер** (в данном случае — RuDesktop) также отвечает предложением (DHCP Offer), но без информации об IP-адресе. Он оставляет выдачу IP-адреса обычному DHCP-серверу. ProxyDHCP-сервер предоставляет:
   - Адрес TFTP/загрузочного сервера (Option 66)
   - Имя загрузочного файла (Option 67), которые используются клиентом при последующей транзакции TFTP

4. Клиент PXE отвечает на выбранное предложение DHCP запросом (DHCP Request), в котором он официально запрашивает информацию о конфигурации IP-адреса у обычного DHCP-сервера
5. Обычный DHCP-сервер отвечает подтверждением (DHCP ACK), сообщая клиенту, что он может использовать выданные параметры конфигурации IP
6. Теперь клиент имеет:
    - Информацию о конфигурации IP-адреса
    - Имя сервера TFTP/загрузочного сервера
    - Имя начального загрузочного файла (например, undionly.kpxe или ipxe.efi), и инициирует транзакцию TFTP для загрузки этого загрузочного файла

Загрузочные файлы и конфигурация находятся по пути:

```
/var/lib/rudesktop/pxe/tftp/
```

Подсказка

В этом каталоге, как правило, расположены:

- `ipxe.efi / undionly.kpxe` — первичные PXE-загрузчики, которые указываются в DHCP Option 67
- `autoexec.ipxe` — основной iPXE-скрипт, который описывает, что и как загружать (ядра Linux, initrd, запуск wimboot и т.п.)

Пример установки ОС с PXE для Windows

После того как PXE-клиент:

1. Получил IP и параметры через обычный DHCP + DHCP-proxy
2. Загрузил по TFTP начальный загрузчик (например, ipxe.efi / undionly.kpxe)
3. iPXE выполнил скрипт (autoexec.ipxe) и через него загрузил wimboot, через wimboot на устройство загружается Windows PE/установочная среда

Далее ОС устанавливается по правилам, которые описаны в файлах `answers_mbr.xml` или `answers_uefi.xml` (в зависимости от режима загрузки — Legacy/MBR или UEFI)

Основные шаги установки:

- Форматирование дисков и разделов
- Создание системного раздела и раздела `C:\`
- Создание пользователя

Подсказка

Пользователь, создаваемый в системе, указывается при создании образа в веб-интерфейсе на странице *Образы OS*

Далее выполняется:

- Установка приложения RuDesktop
- Подключение приложения RuDesktop к серверу, с которого раздавался образ

Изменение конфигурации PXE

Переопределение конфигурации PXE возможно через добавление файла-конфигурации в пользовательскую директорию

- Основная директория (конфигурация по умолчанию):

```
/var/lib/rudesktop/pxe
```

- Пользовательская директория (override-конфиги):

```
/var/lib/rudesktop/user/pxe
```

Важно

- Приоритет выше у пользовательского конфига `/var/lib/rudesktop/user/`
- Директория `/var/lib/rudesktop/user/` используется для переопределения конфигов, таким образом можно изменить практически любой конфиг, не трогая системные файлы в `/var/lib/rudesktop/pxe`

Работа в разных подсетях

Для установки ОС на устройство с использованием PXE в разных подсетях требуется:

Настроить маршрутизацию между подсетями:

- **ProxyDHCP** сервер, находящийся в подсети 1, должен иметь доступ к подсети 2, где находится устройство
- Устройство из подсети 2 должно иметь доступ до **ProxyDHCP** сервера

Важно

Конфигурировать необходимо ту подсеть, где находится устройство, на которое устанавливается операционная система через PXE

DHCP-сервер должен быть настроен для этой клиентской подсети, чтобы устройство получало IP-адрес и параметры загрузки, даже если сам PXE-/ProxyDHCP-сервер находится в другой сети

Примеры конфигурации MikroTik или DHCPD:

- *Конфигурация для MikroTik*
- *Конфигурация для DHCPD*

Пример по изменению ответов для Windows

1. Создать конфиг-файл answers_uefi.xml
2. Добавить его в директорию по пути:

   ```
   /var/lib/rudesktop/user/pxe/overlay/answers_uefi.xml
   ```

3. Опубликовать образ повторно в веб-интерфейсе на странице *Образы OS*

Важно

Аналогичным способом можно осуществлять изменения любых файлов в `/var/lib/rudesktop/pxe`

1.15.2 Конфигурация для MikroTik

Конфигурация для MikroTik — пример стандартной настройки маршрутизатора **MikroTik** для PXE-загрузки: распределение портов по бриджам, настройка DHCP-серверов в каждой подсети и передача PXE-опций (адреса TFTP-сервера и имени загрузочного файла) клиентским устройствам

Примечание

Пример приведён для модели **MikroTik RouterBoard RB2011iL-IN**. На других моделях логика настройки идентична — отличаются только наборы интерфейсов

Подсказка

В примерах используются следующие адреса:

- **DHCP Server (mikrotik):** 192.168.1.1
- **Rudesktop server:** 192.168.2.1
- **Целевое устройство:** 192.168.3.1

В этой схеме MikroTik сам передаёт PXE-клиенту адрес TFTP-сервера (`Option 66`) и имя загрузочного файла (`Option 67`). Встроенный ProxyDHCP серве-

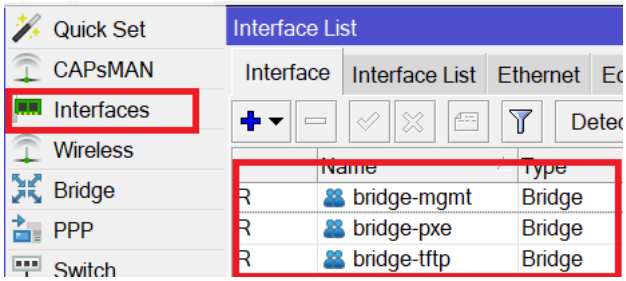
ра **RuDesktop** при этом не задействуется — использовать ProxyDHCP имеет смысл, когда DHCP-сервер не управляет PXE-опциями

Настройка MikroTik

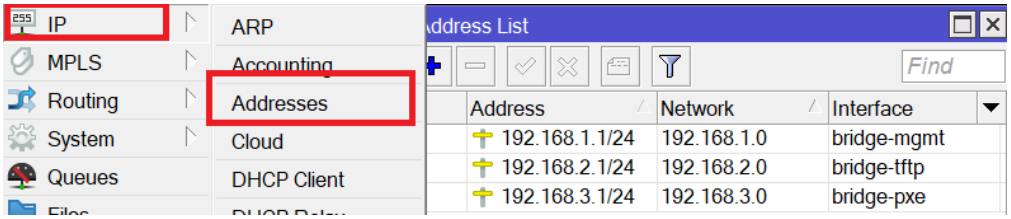
Конфигурация

Winbox

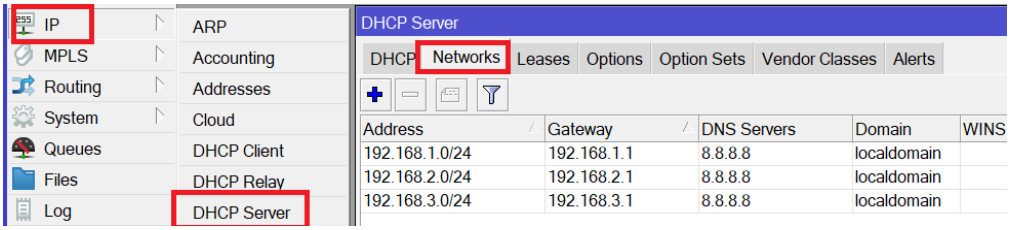
1. Раздел Interfaces — три bridge



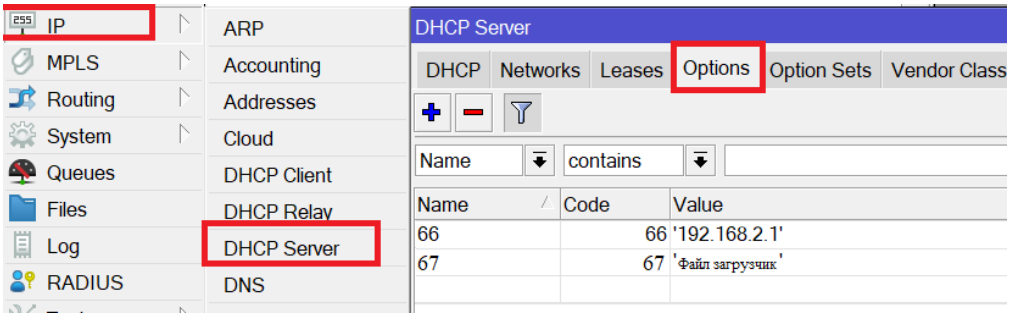
2. Раздел IP -> Addresses — три IP-адреса с интерфейсами



3. Раздел IP -> DHCP Server -> Networks — три сети с правильными интерфейсами



4. Раздел IP -> DHCP Server -> Options — набор `pxe-options` с тремя опциями



Терминал MikroTik

1. Подготовка и базовые настройки (как правило, уже есть в вашей сети):
    - Создание бриджей

```
/interface bridge add name=bridge-mgmt
/interface bridge add name=bridge-tftp
/interface bridge add name=bridge-pxe
```

- Распределение портов по бриджам

```
/interface bridge port add bridge=bridge-mgmt␣
↪interface=ether1
/interface bridge port add bridge=bridge-tftp␣
↪interface=ether2
/interface bridge port add bridge=bridge-pxe␣
↪interface=ether3
```

- Назначение IP-адресов

```
/ip address add address=192.168.1.1/24␣
↪interface=bridge-mgmt
/ip address add address=192.168.2.1/24␣
↪interface=bridge-tftp
/ip address add address=192.168.3.1/24␣
↪interface=bridge-pxe
```

2. Создание и настройка DHCP-серверов

- Создание пулов адресов

```
/ip pool add name=pool-mgmt␣
↪ranges=192.168.1.128-192.168.1.254
/ip pool add name=pool-tftp␣
↪ranges=192.168.2.128-192.168.2.254
/ip pool add name=pool-pxe␣
↪ranges=192.168.3.128-192.168.3.254
```

- Настройка DHCP-серверов

```
/ip dhcp-server add name=dhcp-mgmt interface=bridge-mgmt␣
↪address-pool=pool-mgmt lease-time=10m disabled=no
/ip dhcp-server add name=dhcp-tftp interface=bridge-tftp␣
↪address-pool=pool-tftp lease-time=10m disabled=no
/ip dhcp-server add name=dhcp-pxe interface=bridge-pxe␣
↪address-pool=pool-pxe lease-time=10m disabled=no
```

- Настройка сетей DHCP

```
/ip dhcp-server network add address=192.168.1.0/24␣
↪gateway=192.168.1.1 dns-server=8.8.8.8␣
↪domain=localdomain
/ip dhcp-server network add address=192.168.2.0/24␣
↪gateway=192.168.2.1 dns-server=8.8.8.8␣
↪domain=localdomain
/ip dhcp-server network add address=192.168.3.0/24␣
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
↪gateway=192.168.3.1 dns-server=8.8.8.8␣
↪domain=localdomain
```

3. Настройка PXE-загрузки

   - Создание DHCP-опций для PXE

```
/ip dhcp-server option add name=66 code=66 value="
↪'192.168.2.1'"
/ip dhcp-server option add name=67 code=67 value="
↪'ipxe.efi'"
```

Примечание

В примере выше `Option 67` всегда указывает на `ipxe.efi`, что подходит для UEFI x64. Если в сети присутствуют клиенты разных архитектур, MikroTik сам не умеет выбирать загрузочный файл по архитектуре — для арх-зависимого выбора используйте *конфигурацию для DHCPD* (где можно прописать условия по `option arch`) или встроенный ProxyDHCP сервера **RuDesktop** на порту 4011

Соответствие архитектур и файлов:

- UEFI x64 (код 00:07) загружает `ipxe.efi`
- UEFI ARM64 (код 00:0b) загружает `ipxe-arm64.efi`
- Остальные случаи (например, Legacy BIOS) загружают `undionly.kpxe`

   - Создание набора PXE-опций

```
/ip dhcp-server option sets add name=pxe-options␣
↪options=66,67
```

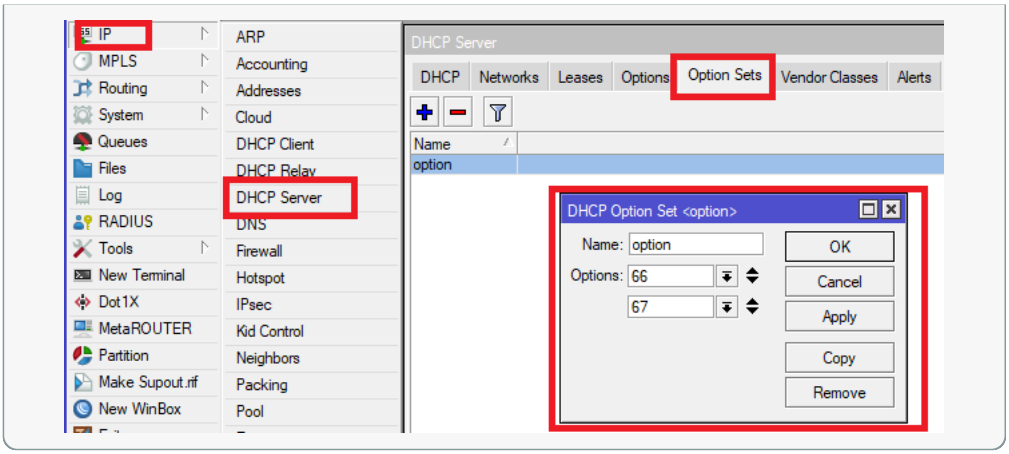
   - Применение PXE-опций к подсети клиентов

```
/ip dhcp-server network set [find where␣
↪address="192.168.3.0/24"] dhcp-option-set=pxe-options
```

Подсказка

Аналогично можно создать опции через winbox:

- Раздел IP -> DHCP Server -> Option Sets — набор `pxe-options` с тремя опциями



Проверка конфигурации

```
/interface bridge port print
/ip dhcp-server print
/ip dhcp-server network print
/ip dhcp-server option-sets print
```

Сохранение конфигурации

```
/system backup save name=pxe-final-config
```

Проверка работоспособности

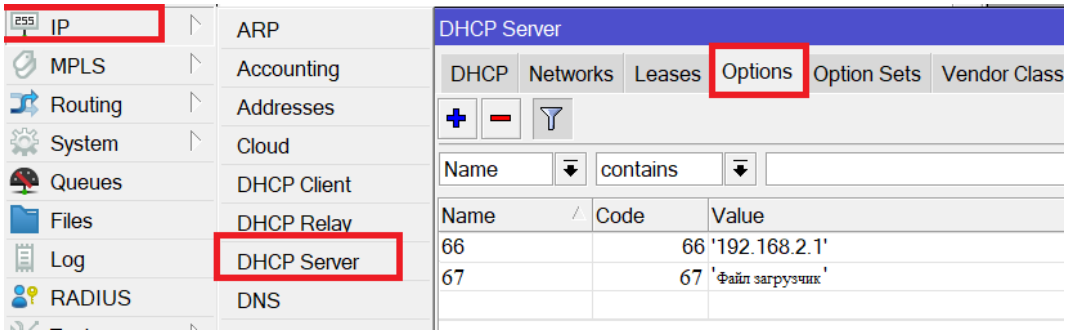
1. Подключить сервер **Rudesktop** к порту `ether2` — должен получить адрес **192.168.2.x**
2. На сервере **Rudesktop** опубликовать образ
3. Подключить устройство, где планируется установка ОС, к порту `ether3` — должен получить адрес **192.168.3.x** и PXE-опции
4. Проверить аренды: IP -> DHCP Server -> Leases
5. Проверить, что устройство получило адрес и началась загрузка ОС

Изменение конфигурации

Если требуется внести изменения, например, адрес сервера **Rudesktop** изменился, то это можно осуществить следующим образом:

Winbox

IP -> DHCP Server -> Options -> Редактировать options (66,67)



Терминал MikroTik

- Сменить адрес сервера **Rudesktop**

```
/ip dhcp-server option set [find name=option66] value="
↪'НОВЫЙ_IP_АДРЕС'"
```

- Сменить загрузочный файл

```
/ip dhcp-server option set [find name=option67] value="'ipxe.efi'"
```

Публикация образа и настройка устройства

1. На сервере **Rudesktop** осуществить *публикацию образа ОС*
2. На устройстве включить загрузку по сети и начать процедуру установки ОС по сети

1.15.3 Конфигурация для DHCPD

Конфигурация для DHCPD — пример настройки внешнего DHCP-сервера **ISC DHCPD** для работы с PXE-загрузкой через сервер **RuDesktop**: глобальные параметры, описание подсетей и арх-зависимый выбор загрузочного файла на основе `Option 60` / `Option 93`

Подсказка

В отличие от MikroTik, **DHCPD** позволяет указать разные загрузочные файлы для UEFI x64, UEFI ARM64 и Legacy BIOS прямо в конфигурации сервера

Настройка DHCPD

Настройте файл по пути `/etc/dhcp/dhcpd.conf` по примеру:

```
# Глобальные настройки
default-lease-time 600;
max-lease-time 7200;
authoritative;

option domain-name "localdomain";
option domain-name-servers 8.8.8.8;
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
# Настройки подсетей
option arch code 93 = unsigned integer 16;

# Subnet: vmnet1
subnet 192.168.193.0 netmask 255.255.255.0 {
  option routers 192.168.193.10;
  option broadcast-address 192.168.193.255;

  range 192.168.193.128 192.168.193.254;
}

# Subnet: vmnet2
subnet 192.168.152.0 netmask 255.255.255.0 {
  option routers 192.168.152.10;
  option broadcast-address 192.168.152.255;

  range 192.168.152.128 192.168.152.254;

  # Сервер ProxyDHCP
  next-server 192.168.193.128;

  # UEFI x64
  if option arch = 00:07 {
      filename "ipxe.efi";
  }
  # UEFI ARM64
  else if option arch = 00:0b {
      filename "ipxe-arm64.efi";
  }
  # Legacy BIOS
  else {
      filename "undionly.kpxe";
  }
  option root-path "tftp://192.168.193.128";
}
```

После сохранения файла перезапустите службу DHCPD:

```
systemctl restart isc-dhcp-server
```

Примечание

Имя сервиса может отличаться в зависимости от дистрибутива (`isc-dhcp-server`, `dhcpd`)

Сценарий работы

1. Клиент в сети vmnet2 запрашивает IP-адрес через DHCP
2. Сервер назначает ему адрес из диапазона `192.168.152.128-254`
3. Если клиент поддерживает PXE, он сообщает свою архитектуру через опцию arch
4. Сервер направляет клиента на TFTP-сервер (адрес сервера Rudesktop) и выдаёт соответствующий загрузочный файл
5. Клиент загружает образ и выполняет его

Логика выбора файла, исходя из архитектуры:

1. UEFI x64 (код 00:07) загружает `ipxe.efi`
2. UEFI ARM64 (код 00:0b) загружает `ipxe-arm64.efi`
3. Остальные случаи (например, Legacy BIOS) загружают `undionly.kpxe`

1.15.4 Настройка размера блока TFTP

Настройка размера блока TFTP — описание параметра `TFTP_BLOCK_SIZE_LIMIT`, который ограничивает максимальный размер полезной нагрузки одного TFTP-пакета. Используется для повышения надёжности PXE-загрузки в сетях со сложной топологией

Описание

Для повышения надёжности загрузки PXE в сложных сетевых окружениях (например, при использовании IPsec, строгих межсетевых экранах или проблемах с фрагментацией пакетов/MTU) установлен лимит размера блока данных TFTP-сервера

Важно

По умолчанию лимит размера полезной нагрузки (payload) составляет **512 байт** (значение задано в файле `/etc/default/rudesktop` после установки сервера)

Примечание

Параметр определяет именно **верхний предел**: TFTP-клиент и сервер согласовывают итоговый размер блока через расширение `blksize` (RFC 2348). Сервер не выдаёт больше байт за один пакет, чем разрешено лимитом, даже если клиент запросил большее значение

Изменение лимита

Для изменения значения по умолчанию необходимо отредактировать конфигурационный файл `/etc/default/rudesktop`

1. Откройте файл `/etc/default/rudesktop` в текстовом редакторе с правами root
2. Найдите или добавьте параметр `TFTP_BLOCK_SIZE_LIMIT`
3. Установите нужное значение. Например:

```
TFTP_BLOCK_SIZE_LIMIT=1024
```

Примечание

Если оставить параметр пустым (`TFTP_BLOCK_SIZE_LIMIT=`), лимит применяться **не будет**, и сервер сможет использовать большие размеры блоков, если это поддерживается клиентом

4. Сохраните изменения в файле
5. Перезапустите сервер **RuDesktop**

```
rude restart
```

Применение настроек

После изменения параметра необходимо заново *опубликовать образ операционной системы*, чтобы настройка вступила в силу

Подсказка

Типичные значения и сценарии:

- `512` — максимальная совместимость со всеми клиентами и любой сетевой инфраструктурой (значение по умолчанию)
- `1024` — компромисс между надёжностью и скоростью
- `1468` — максимальный размер для стандартного Ethernet (MTU 1500) без фрагментации IP-пакетов
- пустое значение — без ограничений, скорость передачи максимальная при условии стабильной сети

Настройка PXE — раздел с описанием встроенного PXE-сервера **RuDesktop**: принцип работы PXE и DHCP-proxy, конфигурация маршрутизатора **MikroTik** и службы **DHCPD** для PXE-загрузки в разных подсетях, настройка размера блока TFTP

Описание PXE-сервера

Принцип работы, компоненты `rudesktop-pxe`, этапы PXE-загрузки и схема DHCP-proxy

Конфигурация для MikroTik

Пример настройки маршрутизатора **MikroTik** для PXE-загрузки в нескольких подсетях

Конфигурация для DHCPD

Пример конфигурации внешнего ISC DHCPD с арх-зависимым выбором загрузочного файла

Настройка размера блока TFTP

Параметр `TFTP_BLOCK_SIZE_LIMIT` для повышения надёжности загрузки в сложных сетях

1.16 Настройка Redis

Настройка Redis — параметры встроенной службы **Redis**, которую сервер **RuDesktop** использует как кеш и брокер сообщений между компонентами. Раздел описывает расположение конфигурации, переключение на внешний экземпляр **Redis** и базовое обслуживание

Добавлено в версии 2.8:

- **Redis** устанавливается по умолчанию вместе с сервером и доступен по адресу `127.0.0.1:32459`
- Конфигурация Redis находится по пути `/etc/rudesktop/redis.conf`
- При необходимости можно использовать внешний **Redis**

1.16.1 Описание

Кеширование — это мощный метод, используемый для повышения производительности и эффективности приложения путём временного хранения часто используемых данных в памяти системы

Важно

Это значительно улучшает время отклика и снижает нагрузку на основные источники данных, такие как базы данных, за счёт минимизации повторяющихся операций извлечения данных

Сервер **RuDesktop** поддерживает кеширование с использованием **Redis**

1.16.2 Какие компоненты используют Redis

Redis используется одновременно несколькими компонентами **RuDesktop**:

- `relay` / `rz` — нативные компоненты сервера. Адрес **Redis** задаётся параметром `redis_server` в файле `/etc/rudesktop-relay.toml`
- `web` / `backend` — Django-часть сервера. Адрес **Redis** задаётся переменной окружения `REDIS_URL` в файле `/etc/default/rudesktop`

Важно

При подключении внешнего **Redis** обязательно задайте оба значения и убедитесь, что они указывают на один и тот же инстанс. Иначе компоненты будут работать с разными хранилищами кеша и состояний — это приведёт к рассинхронизации сессий и сбоям внутренней синхронизации

1.16.3 Настройка подключения к внешнему Redis

Для подключения сервера к внешнему **Redis** с аутентификацией по паролю или без выполните следующие шаги:

1. В файл по пути `/etc/rudesktop-relay.toml` добавьте параметр `redis_server`:

   Без аутентификации

   ```
   redis_server = "redis://address:port"
   ```

   С аутентификацией

   ```
   redis_server = "redis://:password@address:port"
   ```

   Подсказка

   - **password** — пароль
   - **address:port** — адрес и порт внешнего Redis

   Важно

   В том же файле `/etc/rudesktop-relay.toml` можно переопределить дополнительные параметры кеша relay/rz:

```
# Время жизни записей в кеше, в секундах (по␣
↪умолчанию 300)
cache_ttl = 300
# Загружать все устройства в кеш при старте сервера␣
↪(по умолчанию false)
cache_preload = false
# Период сохранения кеша устройств в базу, в секундах␣
↪(по умолчанию 60)
flush_interval = 60
# Количество записей для пакетного сброса в базу (по␣
↪умолчанию 1000)
flush_batch = 1000
```

2. В файл по пути `/etc/default/rudesktop` добавьте переменные:

```
REDIS_URL="redis://address:port"
# или с аутентификацией
REDIS_URL="redis://:password@address:port"

RELAY_ARGS='-C /etc/rudesktop-relay.toml'
```

Важно

`REDIS_URL` должен указывать на тот же инстанс **Redis**, что и `redis_server`

3. Перезапустите сервер:

```
rude restart
```

1.16.4 Проверка подключения

После перезапуска убедитесь, что сервер подключается к указанному **Redis**:

```
redis-cli -h <address> -p <port> -a <password> PING
```

Ответ `PONG` подтверждает доступность **Redis**

1.16.5 Безопасность

При сетевой доступности **Redis** обязательно примите меры безопасности:

- Настройте привязку (`bind`) только к необходимым интерфейсам
- **Обязательно** установите пароль (`requirepass` в конфигурации Redis)
- Ограничьте доступ правилами межсетевого экрана, разрешающими соединения только с IP-адресов узлов **RuDesktop**

Подсказка

Подробнее о вынесении **Redis** и **PostgreSQL** в общий контур для нескольких узлов **RuDesktop** см. на странице *Развертывание отказоустойчивого кластера*

1.17 Настройка Kickstart

Настройка Kickstart — описание серверных шаблонов **Kickstart**, которые сервер **RuDesktop** применяет к клиенту при первой установке или вручную через веб-интерфейс. Раздел описывает жизненный цикл применения Kickstart, расположение шаблонов на сервере, формат скриптов, добавление произвольных команд и итоговый конфиг на устройстве

Подсказка

Параметры **Kickstart** редактируются администратором через веб-интерфейс на странице *Kickstart*. Этот раздел описывает, как они хранятся и применяются на уровне файловой системы

1.17.1 Как работает Kickstart

1. Администратор задаёт параметры на странице **Kickstart** в веб-интерфейсе — отдельно для каждой платформы (Windows, Linux, macOS) и опционально добавляет произвольные команды
2. При сохранении формы сервер **RuDesktop** генерирует скрипт настройки клиента под каждую ОС и сохраняет его в файл `/var/lib/rudesktop/kickstart/<os>`, где `<os>` — `windows`, `linux` или `macos`
3. Скрипт автоматически запускается на устройстве при первой установке клиента **RuDesktop**, либо может быть применён вручную к уже установленному клиенту через кнопку Применить настройки Kickstart
4. Скрипт обновляет клиентский конфиг `RuDesktop2.toml` на устройстве и выполняет добавленные администратором произвольные команды

Примечание

Команда kickstart клиента позволяет вручную запросить и применить настройки Kickstart с сервера:

```
rudesktop --kickstart
```

1.17.2 Шаблоны на сервере

Сгенерированные скрипты находятся на сервере в следующих файлах:

```
/var/lib/rudesktop/kickstart/windows
/var/lib/rudesktop/kickstart/linux
/var/lib/rudesktop/kickstart/macos
```

Важно

Содержимое этих файлов формируется сервером автоматически при сохранении формы Kickstart в веб-интерфейсе. Не редактируйте сгенерированные скрипты напрямую — изменения будут перезаписаны при следующем сохранении

1.17.3 Произвольные команды

Помимо стандартных параметров, в Kickstart-скрипт можно добавить произвольные команды — например, очистку временных файлов или создание каталогов. Команды задаются на странице *Kickstart* во вкладке соответствующей платформы и записываются на стандартном языке оболочки этой ОС:

- **Windows** — PowerShell или CMD
- **Linux** — bash
- **macOS** — bash или zsh

Примеры:

Windows

Очистка временных файлов пользователя:

```
& "C:\Windows\system32\cmd.exe" /c del /q /s
 ↪"C:\Users\rude\AppData\Local\Temp\*"
```

Linux

Создание рабочего каталога:

```
mkdir -p /home/rude/Downloads/test
```

macOS

Установка прав на пользовательский каталог:

```
chown -R $(whoami) ~/Downloads
```

Важно

Команды выполняются с правами учётной записи, под которой работает клиент **RuDesktop** на устройстве. Если требуется повышение прав, используйте средства ОС (`sudo`, `runas` и т. п.)

Добавленные команды также отображаются в веб-интерфейсе на странице *Kickstart*

1.17.4 Конфиг клиента на устройстве

После применения Kickstart клиентский конфиг располагается на устройстве в следующих каталогах:

Windows

```
%windir%\ServiceProfiles\LocalService\AppData\Roaming\RuDesktop\
↪config\RuDesktop2.toml
```

Linux

```
/root/.config/RuDesktop/RuDesktop2.toml
```

macOS

```
/private/var/root/Library/Preferences/ru.desktop.RuDesktop/
↪RuDesktop2.toml
```

Файл написан в формате **TOML** и содержит параметры клиента (тёмная тема, разрешение буфера обмена, автоматическая запись сессий и т. д.) — состав параметров соответствует формам на странице *Kickstart* в веб-интерфейсе

Подсказка

Параллельно с `RuDesktop2.toml` в том же каталоге могут находиться вспомогательные файлы:

- `peers/<server_id>.toml` — сохранённые настройки для конкретного удалённого устройства
- `RuDesktop_logcollect.toml` — конфигурация сборщика логов

Расположение и состав конфигурации клиента описаны на странице Описание логов клиента

1.17.5 Применение Kickstart

- **Автоматически** при первой установке клиента **RuDesktop** — скрипт запускается сразу после развёртывания
- **Вручную** к уже установленным клиентам — через кнопку Применить настройки Kickstart на странице *Kickstart* с выбором конкретного устройства, группы или всех устройств
- **С устройства** — командой `rudesktop --kickstart` (см. kickstart) клиент запрашивает и применяет актуальные настройки с сервера

Важно

Kickstart переопределяет настройки клиента на устройстве. Снятая галочка задаёт выключенное значение параметра, а не возвращает его к значению по умолчанию. Например, снятая галочка **Включить темную тему** задаёт светлую тему

После изменения формы сохранить её и повторно применить настройки к нужным устройствам или группам

1.17.6 Запуск из командной строки сервера

Чтобы применить настройки к выбранным устройствам, укажите их имена из инвентаря Ansible:

```
rude kickstart --hosts host1 host2
```

Параметр `--verbose` включает подробный вывод. Применение настроек поддерживается на Windows, Linux и macOS

Важно

Без `--hosts` команда запускает задание для всех устройств инвентаря

Для запуска из внешней системы см. *Запуск Kickstart через API*

1.18 API

1.18.1 Настройка доступа

Настройка доступа — описание процедуры подготовки пользователя для работы с REST API сервера **RuDesktop**: создание учётной записи, выпуск токена через команду `rude token` и пример использования токена в HTTP-запросах

Создание пользователя

Создайте отдельного пользователя для API (например, `api_user`) с помощью команды:

```
rude createsuperuser
```

Предупреждение

Команда создаёт суперпользователя. После создания обязательно ограничьте права через панель администратора, оставив только те права, которые необходимы для решаемых задач (например, просмотр устройств, управление группами и задачами)

Управление токенами

Команда `rude token` поддерживает три операции — создание, просмотр и отзыв токенов

Создание токена

Подробно — на странице команды *token create*

```
rude token create [имя_пользователя]
```

В ответе в стандартный вывод печатается значение токена. Сохраните его — повторно получить тот же токен будет нельзя

Важно

Для одного пользователя может существовать только один активный токен. При попытке создать второй токен команда вернёт ошибку `Token already exists for this user`. Чтобы перевыпустить токен — сначала отзовите существующий

Просмотр списка токенов

Подробно — на странице команды *token list*

```
rude token list
```

В выводе для каждого токена показаны: дата создания, имя пользователя и значение токена

Отзыв токена

Подробно — на странице команды *token revoke*

```
rude token revoke [значение_токена]
```

После отзыва токен становится недействительным — все последующие запросы с этим токеном будут отклонены

Использование токена

Полученный токен передаётся в заголовке `Authorization` каждого запроса:

```
curl --header "Authorization: Token [TOKEN]" https://[SERVER_ADDR]/
↪api/peer/search/?hostname=XXXX
```

Примечание

Токен предоставляет API доступ от имени пользователя со всеми его правами. Храните токен как пароль — не передавайте его в открытом виде и не сохраняйте в публичных репозиториях

1.18.2 Функции API

Группы

Получение списка групп

Описание

Возвращает список групп устройств с входящими в них устройствами

Запрос

```
GET /account/api/group/
```

Права

Право *Группы → Просмотр*

Ответ


```
[
    {
        "name": "string",
        "server_set": [
            {
                "id": "int",
                "addr": "string",
                "status": "string",
                "username": "string",
                "hostname": "string",
                "server_id": "string",
                "connection": "string"
            }
        ],
        "dn": "string"
    }
]
```


Пример

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/account/api/group/'
```

Получение информации о группе

Описание

Возвращает информацию о конкретной группе по её идентификатору

Запрос

```
GET /account/api/group/{id}/
```

Параметры

- `id` — идентификатор группы

Права

Право *Группы → Просмотр*

Ответ


```
{
    "name": "string",
    "server_set": [
        {
            "id": "int",
            "addr": "string",
            "status": "string",
            "username": "string",
            "hostname": "string",
            "server_id": "string",
            "connection": "string"
        }
    ],
    "dn": "string"
}
```


Пример

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/account/api/group/1/'
```

Создание группы

Описание

Создаёт новую группу устройств. В `server_set` передаются имена хостов (`hostname`) устройств, которые должны входить в группу. Если `dn` не указан, он формируется автоматически на основе имени группы

Примечание

- В поле `name` можно передать имя со спецсимволами, например `Офис, склад`. Передавать имя нужно как обычную строку JSON, без дополнительного LDAP-экранирования

- Если dn не указан, сервер самостоятельно экранирует спецсимволы при его формировании
- Если dn задается явно, он должен быть корректной строкой DN с экранированием специальных символов в значениях компонентов

Запрос

```
POST /account/api/group/
```

Параметры

- name — имя группы (обязательно)
- server_set — список имён хостов устройств для добавления в группу (необязательно)
- dn — Distinguished Name группы (необязательно)

Права

Право *Группы → Создание*

Тело запроса

```
{
    "name": "string",
    "server_set": [
        "hostname"
    ],
    "dn": "string"
}
```

Ответ

```
{
    "name": "string",
    "server_set": [
        {
            "id": "int",
            "addr": "string",
            "status": "string",
            "username": "string",
            "hostname": "string",
            "server_id": "string",
            "connection": "string"
        }
    ],
```

```
    "dn": "string"
}
```

Пример

```
curl --location --request POST
↪'https://[SERVER_ADDR]/account/api/group/' \
--header 'Authorization: Token [TOKEN]' \
--header 'Content-Type: application/json' \
--data '{
    "name": "Бухгалтерия",
    "server_set": [ "host1", "host2" ]
}'
```

Обновление группы (PUT)

Описание

Полностью обновляет данные группы по её идентификатору. В теле запроса передаются все обновляемые параметры группы

Примечание

При запросе `PUT` поле `server_set` полностью перезаписывает текущий список устройств в группе

Запрос

```
PUT /account/api/group/{id}/
```

Параметры

- `id` — идентификатор группы

Права

Право *Группы → Изменение*

Тело запроса

```
{
    "name": "string",
    "server_set": [
        "hostname"
    ],
    "dn": "string"
}
```

Ответ


```
{
    "name": "string",
    "server_set": [
        {
            "id": "int",
            "addr": "string",
            "status": "string",
            "username": "string",
            "hostname": "string",
            "server_id": "string",
            "connection": "string"
        }
    ],
    "dn": "string"
}
```


Пример

```
curl --location --request PUT
↪'https://[SERVER_ADDR]/account/api/group/1/' \
--header 'Authorization: Token [TOKEN]' \
--header 'Content-Type: application/json' \
--data '{
    "name": "Бухгалтерия",
    "server_set": [ "host1", "host2" ]
}'
```

Обновление группы (PATCH)

Описание

Частично обновляет данные группы по её идентификатору. В теле запроса передаются только те параметры, которые требуется изменить

Запрос

```
PATCH /account/api/group/{id}/
```

Параметры

- `id` — идентификатор группы

Права

Право *Группы → Изменение*

Тело запроса

```
{
    "name": "string",
    "server_set": [
        "hostname"
    ],
    "dn": "string"
}
```

Ответ

```
{
    "name": "string",
    "server_set": [
        {
            "id": "int",
            "addr": "string",
            "status": "string",
            "username": "string",
            "hostname": "string",
            "server_id": "string",
            "connection": "string"
        }
    ],
    "dn": "string"
}
```

Пример

```
curl --location --request PATCH
↪'https://[SERVER_ADDR]/account/api/group/1/' \
--header 'Authorization: Token [TOKEN]' \
--header 'Content-Type: application/json' \
--data '{
    "name": "Новое имя группы"
}'
```

Удаление группы

Описание

Удаляет группу по её идентификатору

Запрос

```
DELETE /account/api/group/{id}/
```

Параметры

- `id` — идентификатор группы

Права

Право *Группы → Удаление*

Ответ

```
204 No Content
```

Пример

```
curl --location --request DELETE
↪'https://[SERVER_ADDR]/account/api/group/1/' \
--header 'Authorization: Token [TOKEN]'
```

Задачи

Запуск задачи или политики через API v2

Метод позволяет внешней системе запустить заранее созданную задачу или политику и получить журнал выполнения в ответе

Запрос

```
POST /api/v2/automation/runs/
Authorization: Token [TOKEN]
Content-Type: application/json
```

Права пользователя, которому выдан токен:

- **Может запускать политики** — для всех запросов к этому методу
- Право просмотра задач (`automation.view_job`) — дополнительно для запуска задачи

В JSON передать ровно одно из полей `job_id` или `policy_id`:

Таблица 79: Параметры запуска

Поле	Назначение
`job_id`	Числовой идентификатор задачи. Без списка целей используются устройства и группы из настроек задачи
`policy_id`	Числовой идентификатор политики. Обязательно указать устройства или группы
`device_ids`	Список строк с ID устройств RuDesktop, например `["130315737"]`. Это ID подключения, а не внутренние номера записей базы данных
`group_ids`	Список числовых идентификаторов групп, например `[3]`

Примечание

- Можно передать устройства и группы вместе
- Если для задачи явно переданы `device_ids` или `group_ids`, используются указанные цели вместо сохранённых в задаче
- Настройки самой задачи при этом не меняются

Примеры

Запустить политику на устройстве:

```
curl --no-buffer --request POST
↪'https://[SERVER_ADDR]/api/v2/automation/runs/' \
  --header 'Authorization: Token [TOKEN]' \
  --header 'Content-Type: application/json' \
  --data '{"policy_id": 12, "device_ids": ["130315737"]}'
```

Другие варианты тела запроса:

- Задача на её сохранённых целях: `{"job_id": 7}`
- Политика на группе: `{"policy_id": 12, "group_ids": [3]}`

Ответ и результат выполнения

Ответ содержит:

- Код `200` и тип содержимого `text/plain`
- Журнал, который поступает постепенно по мере выполнения
- Заголовок `X-Run-Id` — идентификатор запуска для сопоставления с аудитом
- Заголовок `X-Job-Id` — идентификатор задачи, только при запуске задачи

Важно

Код `200` означает принятие запуска. Итог выполнения нужно проверить по журналу и статусу задачи

Примечание

- Для получения полного журнала дождаться завершения ответа
- Закрытие соединения с API не отменяет задачу, уже поставленную в очередь

Таблица 80: Ошибки запроса

Код	Что проверить
400	Формат JSON, выбор только одной задачи или политики и наличие целей для политики
401	Наличие и корректность токена
403	Право запуска политик и, для задачи, право просмотра задач
404	Идентификаторы задачи, политики, устройств и групп
409	Задача уже выполняется или ожидает запуска; дождаться её завершения
422	Доступность шаблона, на основе которого создана политика

Получение списка задач

Описание

Возвращает список всех задач сервера **RuDesktop** одним ответом

Запрос

```
GET /automation/api/job/
```

Права

Право *Политики → Просмотр*

Ответ

```
[
    {
        "id": "int",
        "name": "string",
        "params": "string",
        "enabled": "boolean",
        "run_on_start": "boolean",
```

```
        "groups": [ "int" ],
        "peers": [
            {
                "id": "int",
                "addr": "string",
                "status": "string",
                "username": "string",
                "hostname": "string",
                "server_id": "string",
                "connection": "string"
            }
        ],
        "policies": [ "int" ],
        "dynamic_groups": [ "int" ],
        "reports": [ "int" ],
        "report_formats": [ "string" ]
    }
]
```

Пример

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/automation/api/job/'
```

Получение информации о задаче

Описание

Возвращает информацию о задаче по её идентификатору

Запрос

```
GET /automation/api/job/{id}/
```

Параметры

- `id` — идентификатор задачи

Права

Право *Политики → Просмотр*

Ответ

```
{
    "id": "int",
    "name": "string",
    "params": "string",
    "enabled": "boolean",
    "run_on_start": "boolean",
    "groups": [ "int" ],
    "peers": [
        {
            "id": "int",
            "addr": "string",
            "status": "string",
            "username": "string",
            "hostname": "string",
            "server_id": "string",
            "connection": "string"
        }
    ],
    "policies": [ "int" ],
    "dynamic_groups": [ "int" ],
    "reports": [ "int" ],
    "report_formats": [ "string" ]
}
```

Пример

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/automation/api/job/123/'
```

Получение статуса задачи

Описание

Возвращает текущее состояние выполнения задачи по её идентификатору. В поле `status` приходит готовая строка — та же, что отображается в столбце Статус на странице *Задачи*

Возможные значения:

- `Отключено` — задача выключена
- `Новая задача` — задача ещё ни разу не запускалась
- `Запускается` — задача поставлена в очередь
- `Выполняется` — задача выполняется в данный момент
- `Завершено` — последний запуск завершился успешно
- `Ошибка` — последний запуск завершился с ошибкой

Примечание

Если задачи с указанным идентификатором нет, сервер вернёт статус 404

Запрос

```
GET /automation/api/job/{id}/status/
```

Параметры

- id — идентификатор задачи

Права

Право *Политики → Просмотр*

Ответ

```
{
    "status": "string",
    "id": "int",
    "name": "string"
}
```

Пример

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/automation/api/job/123/status/'
```

Создание задачи

Описание

Создаёт новую задачу. В peers передаются имена хостов (hostname) или IP-адреса устройств. Должна быть указана хотя бы одна политика (policies) или хотя бы один отчёт (reports); при наличии отчётов обязательно нужно указать форматы отчётов (report_formats)

Запрос

```
POST /automation/api/job/
```

Параметры

- `name` — имя задачи (обязательно)
- `params` — расписание выполнения в формате RFC 5545 (RRULE)
- `enabled` — задача активна (`true`/`false`)
- `run_on_start` — запускать при включении устройства (`true`/`false`)
- `run_on_all_devices` — запускать на всех устройствах при пустых списках целей (`true`/`false`, по умолчанию `false`)
- `groups` — список идентификаторов статических групп
- `dynamic_groups` — список идентификаторов динамических групп
- `peers` — список имён хостов или IP-адресов устройств
- `policies` — список идентификаторов политик
- `reports` — список идентификаторов отчётов
- `report_formats` — список форматов отчётов (например, `pdf`, `xlsx`, `csv`, `html`)

Права

Право *Политики → Создание*

Примечание

В `peers` попадут только те устройства, которые доступны владельцу токена. Имена хостов и адреса, к которым у него нет доступа, будут молча отброшены

Тело запроса

```
{
    "name": "string",
    "params": "string",
    "enabled": "boolean",
    "run_on_start": "boolean",
    "groups": [ "int" ],
    "peers": [ "string" ],
    "policies": [ "int" ],
    "dynamic_groups": [ "int" ],
    "reports": [ "int" ],
    "report_formats": [ "string" ]
}
```

Ответ


```
{
    "id": "int",
    "name": "string",
    "params": "string",
    "enabled": "boolean",
    "run_on_start": "boolean",
    "groups": [ "int" ],
    "peers": [
        {
            "id": "int",
            "addr": "string",
            "status": "string",
            "username": "string",
            "hostname": "string",
            "server_id": "string",
            "connection": "string"
        }
    ],
    "policies": [ "int" ],
    "dynamic_groups": [ "int" ],
    "reports": [ "int" ],
    "report_formats": [ "string" ]
}
```


Пример

```
curl --location --request POST
↪'https://[SERVER_ADDR]/automation/api/job/' \
--header 'Authorization: Token [TOKEN]' \
--header 'Content-Type: application/json' \
--data '{
    "name": "Название задачи",
    "enabled": true,
    "run_on_start": true,
    "groups": [ 1 ],
    "peers": [ "host1", "host2" ],
    "policies": [ 1 ],
    "dynamic_groups": [],
    "reports": [],
    "report_formats": []
}'
```

Обновление задачи (PUT)

Описание

Полностью обновляет данные задачи с указанным идентификатором. В теле запроса передаются все параметры задачи

Примечание

Убедитесь, что вы указываете все поля корректно — неверный формат данных приведёт к ошибке

Запрос

```
PUT /automation/api/job/{id}/
```

Параметры

- `id` — идентификатор задачи

Права

Право *Политики → Изменение*

Тело запроса

```
{
    "name": "string",
    "params": "string",
    "enabled": "boolean",
    "run_on_start": "boolean",
    "groups": [ "int" ],
    "peers": [ "string" ],
    "policies": [ "int" ],
    "dynamic_groups": [ "int" ],
    "reports": [ "int" ],
    "report_formats": [ "string" ]
}
```

Ответ

```
{
    "id": "int",
    "name": "string",
    "params": "string",
    "enabled": "boolean",
    "run_on_start": "boolean",
```

```
    "groups": [ "int" ],
    "peers": [
        {
            "id": "int",
            "addr": "string",
            "status": "string",
            "username": "string",
            "hostname": "string",
            "server_id": "string",
            "connection": "string"
        }
    ],
    "policies": [ "int" ],
    "dynamic_groups": [ "int" ],
    "reports": [ "int" ],
    "report_formats": [ "string" ]
}
```

Пример

```
curl --location --request PUT
↪'https://[SERVER_ADDR]/automation/api/job/123/' \
--header 'Authorization: Token [TOKEN]' \
--header 'Content-Type: application/json' \
--data '{
    "name": "Название задачи",
    "enabled": true,
    "run_on_start": true,
    "groups": [ 1 ],
    "peers": [ "host1", "host2" ],
    "policies": [ 1 ],
    "dynamic_groups": [],
    "reports": [],
    "report_formats": []
}'
```

Обновление задачи (PATCH)

Описание

Частично обновляет данные задачи с указанным идентификатором. В теле запроса передаются только те параметры, которые требуется изменить

Запрос

```
PATCH /automation/api/job/{id}/
```

Параметры

- `id` — идентификатор задачи

Права

Право *Политики → Изменение*

Тело запроса

```
{
    "name": "string",
    "params": "string",
    "enabled": "boolean",
    "run_on_start": "boolean",
    "groups": [ "int" ],
    "peers": [ "string" ],
    "policies": [ "int" ],
    "dynamic_groups": [ "int" ],
    "reports": [ "int" ],
    "report_formats": [ "string" ]
}
```

Ответ

```
{
    "id": "int",
    "name": "string",
    "params": "string",
    "enabled": "boolean",
    "run_on_start": "boolean",
    "groups": [ "int" ],
    "peers": [
        {
            "id": "int",
            "addr": "string",
            "status": "string",
            "username": "string",
            "hostname": "string",
            "server_id": "string",
            "connection": "string"
        }
    ],
    "policies": [ "int" ],
    "dynamic_groups": [ "int" ],
    "reports": [ "int" ],
    "report_formats": [ "string" ]
}
```

Пример

```
curl --location --request PATCH
↪'https://[SERVER_ADDR]/automation/api/job/123/' \
--header 'Authorization: Token [TOKEN]' \
--header 'Content-Type: application/json' \
--data '{
    "enabled": false
}'
```

Остановка задач

Описание

Останавливает выполнение задач по списку их идентификаторов. Можно передать одну или несколько задач за один запрос

Примечание

Остановка применяется только к задачам, которые в данный момент выполняются. Задачи в очереди или уже завершённые не затрагиваются

Запрос

```
POST /automation/api/stop_job/
```

Параметры

- `obj_id` — список идентификаторов задач для остановки (обязательно, минимум одна задача)

Права

Право *Может запускать политики*

Тело запроса

```
{
    "obj_id": [ "int" ]
}
```

Ответ

```
{
    "message": "Задачи успешно остановлены"
}
```

Если ни одна из переданных задач не найдена, сервер вернёт статус `400` и сообщение `Задачи не найдены`

Пример

```
curl --location --request POST
↪'https://[SERVER_ADDR]/automation/api/stop_job/' \
--header 'Authorization: Token [TOKEN]' \
--header 'Content-Type: application/json' \
--data '{
    "obj_id": [ 123, 124 ]
}'
```

Удаление задачи

Описание

Удаляет задачу с указанным идентификатором

Запрос

```
DELETE /automation/api/job/{id}/
```

Параметры

- `id` — идентификатор задачи

Права

Право *Политики → Удаление*

Ответ

```
204 No Content
```

Пример

```
curl --location --request DELETE
↪'https://[SERVER_ADDR]/automation/api/job/123/' \
--header 'Authorization: Token [TOKEN]'
```

Запуск Kickstart через API

Чтобы применить сохранённые настройки Kickstart, отправьте запрос от имени пользователя с правом **Может управлять Kickstart**. В параметре `host` укажите имена устройств из инвентаря Ansible через запятую. Например, для двух устройств:

```
curl --no-buffer 'https://[SERVER_ADDR]/automation/api/executor/?kin
↪d=kickstart&host=host1,host2' \
  --header 'Authorization: Token [TOKEN]'
```

Важно

Без параметра `host` сервер запускает задание для всех устройств инвентаря

Сервер передаёт журнал по мере выполнения. В нём виден результат для каждого устройства. Для подробного вывода добавьте к запросу `&verbose=true`

При ответе `403` проверьте токен и право пользователя на управление Kickstart

Устройства

Получение списка устройств

Описание

Возвращает список устройств, зарегистрированных на сервере **RuDesktop**. Поддерживает фильтрацию по имени хоста и статусу, а также постраничную выборку через `offset` и `limit`

Возвращаются только устройства, доступные владельцу токена. Фильтры и постраничная выборка применяются к этому доступному списку

Поле `last_session` содержит дату и время последнего начала сеанса с участием устройства: учитываются как входящие, так и исходящие подключения. Если таких сеансов нет, возвращается `null`. Это не время последнего выхода устройства в онлайн и не время обновления инвентаризации

Важно

По умолчанию возвращается не более 50 устройств. Чтобы получить больше — укажите параметр `limit`, например `/api/peer/search/?limit=3000`

Запрос

```
GET /api/peer/search/
```

Параметры

- `hostname` — фильтр по имени хоста (поиск по подстроке)
- `status` — фильтр по статусу: `online` или `offline`
- `offset` — смещение в выборке (по умолчанию `0`)
- `limit` — максимальное число записей в ответе (по умолчанию `50`)

Права

Право *Устройства → Просмотр*

Ответ


```
{
    "items": [
        {
            "id": "int",
            "server_id": "string",
            "hostname": "string",
            "username": "string",
            "domain": "string",
            "platform": "string",
            "uname": "string",
            "version": "string",
            "addr": "string",
            "uuid": "string",
            "status": "string",
            "last_session": "2026-09-04T12:30:00Z"
        }
    ]
}
```


Пример

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/api/peer/search/?limit=3000'
```

Получение информации об устройстве

Описание

Возвращает информацию об устройствах, чьё имя хоста содержит указанную подстроку. Если совпадений несколько, в ответе вернутся все они

Запрос

```
GET /api/peer/search/?hostname=[HOSTNAME]
```

Параметры

- `hostname` — имя хоста (поиск по подстроке)

Права

Право *Устройства → Просмотр*

Ответ


```
{
    "items": [
        {
            "id": "int",
            "server_id": "string",
            "hostname": "string",
            "username": "string",
            "domain": "string",
            "platform": "string",
            "uname": "string",
            "version": "string",
            "addr": "string",
            "uuid": "string",
            "status": "string",
            "last_session": null
        }
    ]
}
```


Пример

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/api/peer/search/?hostname=[HOSTNAME]'
```

Получение информации о ресурсах устройства

Описание

Возвращает инвентарную информацию по ресурсам устройств, чьё имя хоста содержит указанную подстроку. Ресурсы сгруппированы по типу. Поддерживается исключение типов ресурсов через параметр `exclude`

Запрос

```
GET /api/assets/search/?hostname=[HOSTNAME]
```

Параметры

- `hostname` — имя хоста (поиск по подстроке). Если параметр не указан — возвращаются ресурсы всех устройств
- `exclude` — список типов ресурсов через запятую, которые нужно исключить из ответа. Доступные значения:
  - `hardware` — оборудование
  - `software` — программное обеспечение
  - `user` — пользователи
  - `group` — группы
  - `os` — операционная система

Права

Право *Инвентаризация → Просмотр*

Ответ


```
{
    "hardware": [
        "ACR Acer Technologies 59659"
    ],
    "software": [
        "code 1.99.2-1744250061",
        "perl 5.38.2-3.2ubuntu0.1"
    ],
    "user": [
        "rudesktop"
    ],
    "group": [
        "Группа с правами администратора: rudesktop"
    ],
    "os": [
        "Ubuntu 24.04"
    ]
}
```

Пример

Получение всех ресурсов устройства:

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/api/assets/search/?hostname=[HOSTNAME]'
```

Получение всех ресурсов устройства, кроме оборудования:

```
curl --header 'Authorization: Token [TOKEN]' --location 'https://[SE
↪RVER_ADDR]/api/assets/search/?hostname=[HOSTNAME]&exclude=hardware
↪'
```

Получение детальной информации о ресурсе

Описание

Возвращает подробную информацию о ресурсе по его идентификатору, включая историю появления и удаления ресурса на устройствах (`asset_history`)

Запрос

```
GET /api/assets/{id}/
```

Параметры

- `id` — идентификатор ресурса

Права

Право *Инвентаризация → Просмотр*

Ответ

```
{
    "id": "int",
    "name": "string",
    "asset_type": "string",
    "asset_sub_type": "string",
    "asset_history": [
        {
            "id": "int",
            "available_from": "datetime",
            "available_to": "datetime",
            "version": "string",
            "capacity": "int",
            "unit": "string"
        }
    ]
}
```

Пример

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/api/assets/42/'
```

Получение информации о ресурсах устройства (v2)

Описание

Расширенная версия запроса ресурсов: возвращает подробные сведения о каждом ресурсе (тип, подтип, версия, GUID, дополнительные факты, команда удаления, URL) сгруппированные по типу ресурса. Поддерживает фильтрацию по типу и подтипу

Запрос

```
GET /api/v2/assets/search/
```

Параметры

- `hostname` — фильтр по имени хоста (поиск по подстроке)
- `server_id` — фильтр по идентификатору устройства (поиск по подстроке). Применяется, если не указан `hostname`
- `asset_type` — список типов ресурсов через запятую для включения. Доступные значения: `software`, `os`, `hotfix`, `hardware`, `path`, `user`, `group`
- `asset_sub_type` — список подтипов ресурсов через запятую для включения. Доступные значения: `cpu`, `gpu`, `motherboard`, `ram`, `os`, `disk`, `pci`, `monitor`, `network`, `device`, `other`, `local_user`, `local_group`, `encryption`, `security`, `service`
- `exclude_asset_type` — список типов ресурсов через запятую для исключения
- `exclude_asset_sub_type` — список подтипов ресурсов через запятую для исключения

Права

Право *Инвентаризация → Просмотр*

Ответ

```
{
    "hardware": [
        {
            "name": "string",
            "asset_type": "string",
            "asset_sub_type": "string",
            "guid": "string",
            "version": "string",
            "facts": {},
            "uninstall": "string",
            "url": "string"
        }
    ],
    "software": [
        {
            "name": "string",
            "asset_type": "string",
            "asset_sub_type": "string",
            "guid": "string",
            "version": "string",
            "facts": {},
            "uninstall": "string",
            "url": "string"
        }
    ]
}
```


Пример

Получение всех ресурсов устройства:

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/api/v2/assets/search/?hostname=[HOSTNAME]'
```

Получение только оборудования (CPU и RAM) для устройства:

```
curl --header 'Authorization: Token [TOKEN]' --location 'https://[SE
↪RVER_ADDR]/api/v2/assets/search/?hostname=[HOSTNAME]&asset_type=ha
↪rdware&asset_sub_type=cpu,ram'
```

Получение всех ресурсов устройства, кроме программного обеспечения:

```
curl --header 'Authorization: Token [TOKEN]' --location 'https://[SE
↪RVER_ADDR]/api/v2/assets/search/?hostname=[HOSTNAME]&exclude_asset
↪_type=software'
```

Получение списка устройств (v2)

Описание

Возвращает список устройств вместе с их идентификаторами оборудования: `machine-id`, MAC-адресами и серийными номерами. Предназначен для сопоставления устройств **RuDesktop** с записями во внешних системах — CMDB, системах учёта и инвентаризации

В отличие от `/api/peer/search/`, ответ постраничный в формате `count/next/previous/results` и поддерживает поиск по идентификаторам оборудования

Запрос

```
GET /api/v2/devices/
```

Параметры

- `hostname` — фильтр по имени хоста (поиск по подстроке)
- `server_id` — фильтр по идентификатору устройства (поиск по подстроке)
- `status` — фильтр по статусу: `online` или `offline`
- `machine_id` — фильтр по `machine-id` устройства (точное совпадение)
- `serial` — фильтр по серийному номеру. Поиск идёт сразу по серийным номерам BIOS, системы и материнской платы, регистр не важен
- `mac` — фильтр по MAC-адресу. Формат записи и регистр не важны: подойдут `00:1A:2B:3C:4D:5E`, `00-1a-2b-3c-4d-5e` и `001a2b3c4d5e`
- `offset` — смещение в выборке (по умолчанию `0`)
- `limit` — максимальное число записей в ответе (по умолчанию `50`, максимум `500`)

Права

Одновременно два права: *Устройства → Просмотр* и *Инвентаризация → Просмотр*

Примечание

Возвращаются только устройства, доступные владельцу токена

Ответ

```
{
    "count": "int",
    "next": "string",
    "previous": "string",
    "results": [
        {
            "server_id": "string",
            "hostname": "string",
            "alias": "string",
            "domain": "string",
            "platform": "string",
            "status": "string",
            "identity": {
                "machine_id": "string",
                "mac_addresses": ["string"],
                "bios_serial": "string",
                "product_serial": "string",
                "board_serial": "string"
            },
            "facts_updated": "datetime"
        }
    ]
}
```

Примечание

Незаполненные и заведомо мусорные серийные номера (`0`, `unknown`, `To Be Filled By O.E.M.` и подобные) в ответе заменяются на `null` — их нельзя использовать для сопоставления устройств

Подсказка

Значения в `mac_addresses` приводятся к единому виду `00:1a:2b:3c:4d:5e`, собираются по всем актуальным сетевым адаптерам устройства и отсортированы

Пример

Получение первой страницы списка устройств:

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/api/v2/devices/?limit=200'
```

Поиск устройства по MAC-адресу:

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/api/v2/devices/?mac=00:1A:2B:3C:4D:5E'
```

Поиск устройства по серийному номеру:

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/api/v2/devices/?serial=[SERIAL]'
```

Получение карточки устройства (v2)

Описание

Возвращает полную карточку одного устройства по его идентификатору: те же поля, что и в списке, плюс инвентаризационные данные — оборудование, сгруппированное по видам, и программное обеспечение

Запрос

```
GET /api/v2/devices/{server_id}/
```

Параметры

- `server_id` — идентификатор устройства (точное совпадение)

Права

Одновременно два права: *Устройства → Просмотр* и *Инвентаризация → Просмотр*

Ответ


```
{
    "server_id": "string",
    "hostname": "string",
    "alias": "string",
    "domain": "string",
    "platform": "string",
    "status": "string",
    "identity": {
        "machine_id": "string",
        "mac_addresses": ["string"],
        "bios_serial": "string",
        "product_serial": "string",
        "board_serial": "string"
    },
    "facts_updated": "datetime",
    "hardware": {
        "cpu": [
            {
                "name": "string",
                "guid": "string",
                "version": "string",
```

```
                "facts": {},
                "capacity": "int",
                "unit": "string"
            }
        ],
        "gpu": [],
        "motherboard": [],
        "disks": [],
        "network": [],
        "monitors": [],
        "encryption": [],
        "security": [],
        "devices": [],
        "pci": [],
        "other": [],
        "ram": {
            "total": "float",
            "unit": "GB",
            "modules": []
        }
    },
    "software": {
        "os": {
            "name": "string",
            "guid": "string",
            "version": "string",
            "facts": {}
        },
        "applications": [
            {
                "name": "string",
                "guid": "string",
                "version": "string",
                "facts": {},
                "uninstall": "string",
                "url": "string"
            }
        ],
        "browser_extensions": [
            {
                "name": "string",
                "guid": "string",
                "version": "string",
                "facts": {}
            }
        ],
        "services": [],
        "updates": []
    }
}
```

Примечание

В `ram.total` возвращается суммарный объём всех модулей памяти, приведённый к гигабайтам

Оборудование, которое не удалось отнести ни к одной группе, попадает в `other`

Плагины браузеров возвращаются в `software.browser_extensions`, а не в `software.applications`. В `facts.browser` указано название браузера, `guid` имеет вид `<ключ браузера>:<идентификатор плагина>`, где ключ браузера: `chrome`, `edge`, `yandex`, `chromium`, `chromium-gost`, `opera` или `firefox`

Если инвентаризация устройства не выполнялась, группы возвращаются пустыми, а `software.os` — `null`

Пример

```
curl --header 'Authorization: Token [TOKEN]' --location
↪'https://[SERVER_ADDR]/api/v2/devices/[SERVER_ID]/'
```

Пригласительные ссылки

API v2 позволяет получать, создавать и удалять пригласительные ссылки для конкретного устройства. Авторизация по токену описана в *Настройке доступа*

В пути `server_id` — ID устройства RuDesktop, а не внутренний числовой идентификатор записи базы данных. Устройство должно быть доступно владельцу токена. Передавать UUID устройства для этих методов не требуется

Права

- Для получения списка — **Может видеть список пригласительных ссылок** либо **Может управлять пригласительными ссылками**
- Для создания и удаления — **Может управлять пригласительными ссылками**

Список ссылок также ограничен доступом пользователя к самим ссылкам. Наличие токена не даёт доступ ко всем устройствам и ссылкам сервера

По умолчанию пользователь видит свои ссылки. Право управления организацией добавляет ссылки её управляемых пользователей; право просмотра всех пригласительных ссылок расширяет список. Доступ к устройству всё равно требуется

Получение списка

```
GET /api/v2/devices/{server_id}/invite-links/
```

Параметры page и page_size управляют постраничной выборкой. По умолчанию на странице 10 ссылок, максимум — 100

```
curl --header 'Authorization: Token [TOKEN]' \
    'https://[SERVER_ADDR]/api/v2/devices/[DEVICE_ID]/invite-links/?
↪page=1&page_size=100'
```

Ответ содержит count, next, previous и список results. В записи ссылки возвращаются token, готовый адрес invite_url, server_id, отправитель, время действия, тип подключения, счётчики использований и ограничения доступа

Создание ссылки

```
POST /api/v2/devices/{server_id}/invite-links/
```

Пример ссылки для одного подключения к рабочему столу в течение часа:

```
curl --request POST \
    --header 'Authorization: Token [TOKEN]' \
    --header 'Content-Type: application/json' \
    --data '{
↪"expire_after_seconds":3600,"max_use_count":1,"invite_type":0}' \
    'https://[SERVER_ADDR]/api/v2/devices/[DEVICE_ID]/invite-links/'
```

Основные поля тела запроса:

- expire_after_seconds — время действия в секундах: 900, 3600, 7200, 18000, 86400, 604800 или 2592000; null — без ограничения по времени
- max_use_count — максимальное количество использований, не меньше 1; по умолчанию 1
- invite_type — разрешённый тип подключения: 0 — рабочий стол, 1 — передача файлов, 3 — RDP, 5 — терминал
- ask_for_connect — запрашивать пароль при подключении
- host_group_id — числовой ID группы, определяющей права подключения
- restrict_type — server, user или group; при выборе нужно также передать соответствующее поле restrict_to_server (ID устройства), restrict_to_user (ID пользователя) или restrict_to_group (ID группы)

Сервер назначает отправителем владельца токена и устанавливает начало действия при создании. Поля sender и date_create этим методом не задаются. При успехе возвращается код 201 и созданная ссылка с token и invite_url

Удаление ссылки

```
DELETE /api/v2/devices/{server_id}/invite-links/{token}/
```

В пути использовать token из ответа API, а не числовой id ссылки

```
curl --request DELETE --header 'Authorization: Token [TOKEN]' \
    'https://[SERVER_ADDR]/api/v2/devices/[DEVICE_ID]/invite-links/[
↪LINK_TOKEN]/'
```

При успехе возвращается 204 без тела ответа. После удаления ссылка не может использоваться для нового подключения

Сведения о параметрах и использовании ссылок доступны в *руководстве пользователя*

Регистрация пользователей

Оба метода доступны без токена. Перед показом формы регистрации клиент запрашивает настройки сервера

Проверить доступность регистрации

`GET /api/registration-allowed/` возвращает два поля:

- `allowed` — разрешена ли самостоятельная регистрация
- `requires_consent` — требуется ли согласие на обработку персональных данных

Зарегистрировать пользователя

Отправьте `POST /api/register/` с полями `username` (логин), `full_name` (полное имя), `email`, `password1` и `password2` (пароль и его подтверждение). Передайте номер в поле `phone`, если он обязателен на сервере. Название компании можно указать в поле `company`

Если `requires_consent` равно `true`, передайте `is_personal_data_processing_accepted` со значением `true` после того, как пользователь подтвердил согласие. Согласие на рассылку (`is_marketing_messages_accepted`) добровольное

- **201** — учётная запись создана, письмо отправлено на адрес из поля `email` ответа. Чтобы активировать запись, пользователю нужно перейти по ссылке в письме
- **400** — сервер вернул ошибки заполнения формы. Исправьте указанные поля и повторите запрос
- **403** — регистрация на сервере закрыта
- **503** — на сервере не настроена отправка почты или не удалось отправить письмо. Учётная запись не создана, запрос можно повторить после восстановления отправки

Функции API — описание методов REST API сервера **RuDesktop**, сгруппированных по сущностям: регистрация пользователей, операции с группами, задачами, устройствами и пригласительными ссылками

Группы

Методы для управления группами устройств

Задачи

Запуск политик и Kickstart, управление задачами

Устройства

Методы для работы со списком устройств и их ресурсами

Пригласительные ссылки

Получение списка, создание и удаление ссылок для устройства через API v2

Регистрация пользователей

Проверка доступности регистрации и создание учётной записи

API — раздел с описанием REST API сервера **RuDesktop**: получение токенов доступа и описание основных методов для интеграции с внешними системами и автоматизации рутинных операций

1.18.3 Авторизация

Для методов, требующих токен, передайте его в заголовке `Authorization`:

```
Authorization: Token [TOKEN]
```

Токен выпускается командой `rude token create [имя_пользователя]` (подробнее — в *Настройке доступа*)

Методы *регистрации пользователей* доступны без токена

1.18.4 Интерактивная схема API

Сервер предоставляет встроенную OpenAPI-схему и интерактивные интерфейсы для просмотра и тестирования эндпоинтов:

- `https://[SERVER_ADDR]/api/schema/` — OpenAPI-схема в формате YAML
- `https://[SERVER_ADDR]/api/schema/swagger-ui/` — интерактивный Swagger UI
- `https://[SERVER_ADDR]/api/schema/redoc/` — документация в формате ReDoc

Важно

Доступ к этим страницам разрешён только суперпользователю и осуществляется через сессионную авторизацию (вход в веб-интерфейс под суперпользователем)

Примечание

Схема включает все эндпоинты сервера, в том числе внутренние, используемые веб-интерфейсом и desktop-клиентом. Для интеграции с внешними системами через токен используйте методы, описанные в *Функциях API*

Примечание

REST API модуля аналитики (встроенный **Apache Superset**) устроен отдельно от API сервера: у него свои эндпоинты под префиксом `/analytics/api/` и свои токены доступа — они выпускаются командой `rude superset token create` и передаются в заголовке `Authorization`. Работа с ним — например, передача внешних справочников в таблицы базы сервера — описана на странице *Интеграция с модулем аналитики*

Настройка доступа

Получение и использование токена для доступа к API

Функции API

Описание методов REST API по группам

Руководство администратора — раздел для системных администраторов сервера **RuDesktop**: архитектура, системные требования, установка и обновление, сетевые настройки, настройки сервера и его компонентов, CLI-команды, развёртывание отказоустойчивого кластера, резервное копирование, логи и Syslog, настройка мостов и точек распространения, интеграции с внешними системами, PXE-сервер, Redis, Kickstart-преднастройки, REST API, диагностика и глоссарий

Подсказка

Все инструкции раздела предполагают наличие root-доступа на сервере и работают с локальным сервером **Удаленный доступ** или **Управление конфигурациями (UEM)**. Часть инструкций (например, отказоустойчивый кластер, PXE-сервер, Apache Superset) требует лицензии **UEM**

Сведения о совместной работе со средствами защиты на рабочих станциях приведены в разделе Совместимость со средствами защиты информации

Архитектура сервера

Состав компонентов и схема взаимодействия сервиса

Системные требования

Поддерживаемые ОС и минимальные ресурсы для развёртывания

Установка и обновление сервера
Способы развёртывания и порядок обновления

Сетевые настройки
Порты, SSL, IP-адреса и ограничения доступа

Настройки сервера
Параметры Gunicorn, уровни логирования и системные настройки

Команды сервера
CLI-команды `rude` для управления сервером и данными

Развертывание отказоустойчивого кластера
Установка нескольких серверов в режиме высокой доступности

Резервное копирование
Создание и восстановление резервных копий сервера

Логи сервера
Расположение логов сервера и его компонентов

Мониторинг и метрики
Healthcheck, контроль служб и интеграция с системами мониторинга

Публикация событий в Syslog
Дублирование событий аудита во внешний Syslog-приёмник

Настройка мостов
Развёртывание серверов-ретрансляторов для удалённых филиалов

Настройка точек распространения
Развёртывание серверов для распространения файлов и пакетов

Интеграции
Подключение к внешним системам — Jatoba, Kaspersky, Multifactor, RuSIEM и модуль аналитики

Настройка PXE
Конфигурация встроенного PXE-сервера для удалённой установки ОС

Настройка Redis
Параметры подключения и обслуживание Redis

API
REST API сервера, токены доступа и описание методов

Настройка Kickstart
Конфигурация автоматической преднастройки клиента **RuDesktop**

ГЛАВА 2

Руководство пользователя

2.1 Страница регистрации

Страница регистрации — форма создания учётной записи самим пользователем, без участия администратора

Подсказка

Страница регистрации доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)** при включённой *настройке сервера* **«Регистрация пользователей»**

2.1.1 Как это работает

Зарегистрироваться можно также в настольном клиенте

Если в настройках сервера включена самостоятельная регистрация, на *странице авторизации* появляется кнопка **«Создать учётную запись»**. По ней открывается форма регистрации; после её отправки сервер:

1. создаёт учётную запись со статусом **неактивна** (пользователь не может войти, пока не подтвердит email)
2. отправляет на указанный Email письмо со ссылкой для подтверждения

Важно

Если SMTP не настроен в *настройках сервера*, письмо не уйдёт и зарегистрированный пользователь не сможет авторизоваться

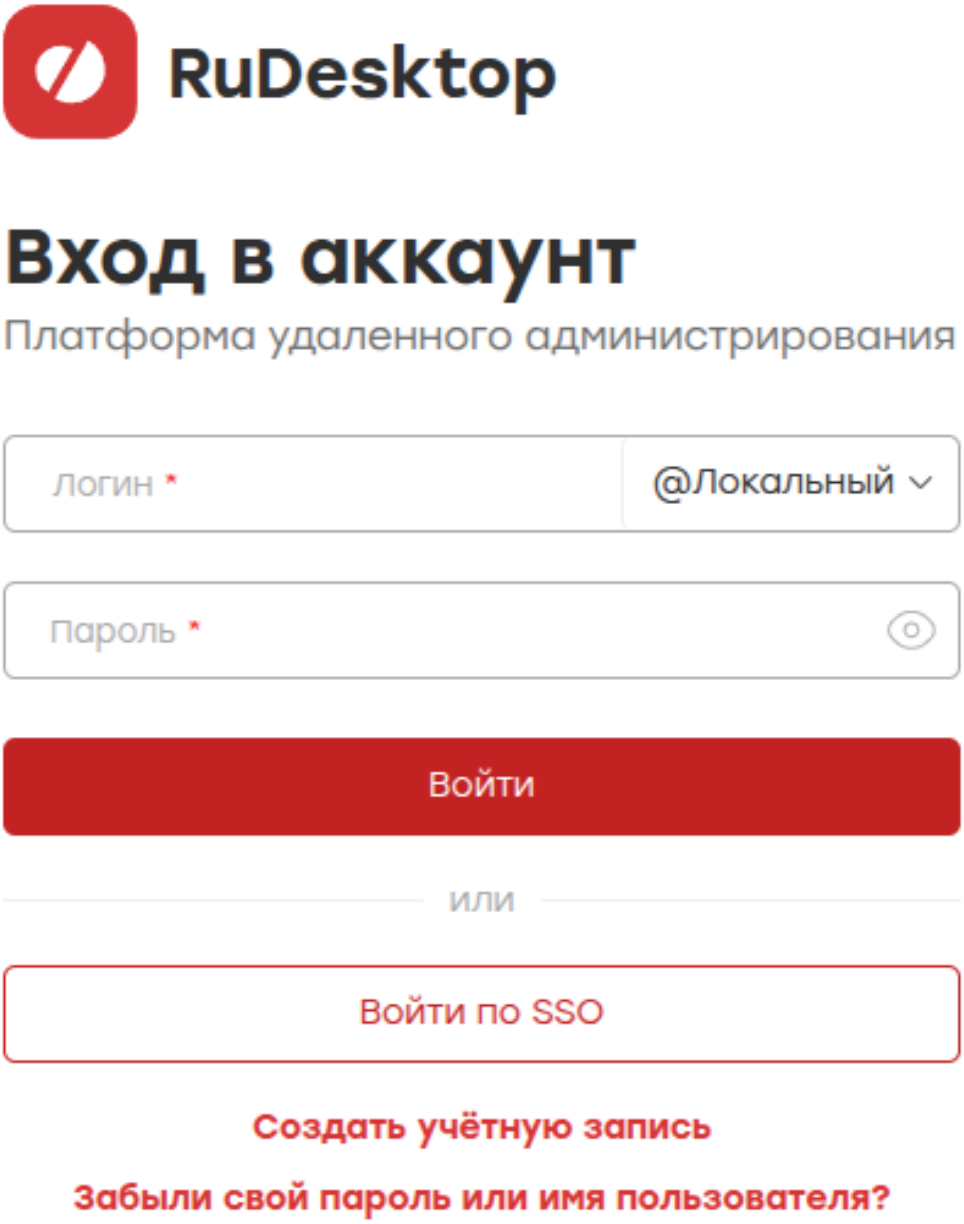
3. при переходе по ссылке учётная запись активируется и пользователь попадает на страницу с уведомлением о завершении регистрации

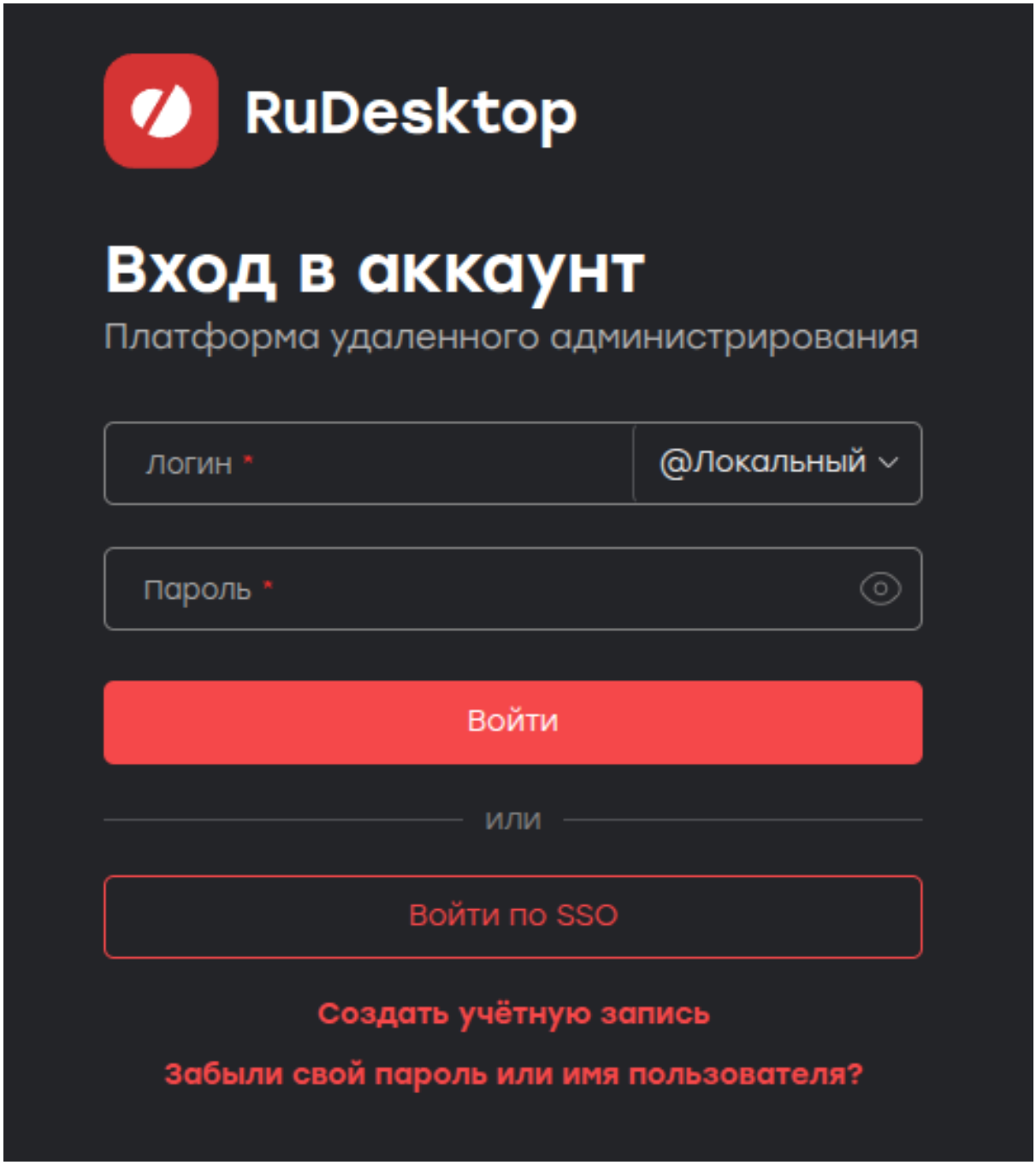
После завершения регистрации пользователь может войти в веб-интерфейс. Назначение прав, групп и подразделений выполняется администратором отдельно — самостоятельно зарегистрированный пользователь по умолчанию **не получает** доступа к управлению устройствами

Если авторизация не была выполнена ранее, при переходе в веб-интерфейс сервера откроется страница авторизации с возможностью регистрации нового пользователя

Важно

Эта функция доступна только при активации настройки *самостоятельной регистрации пользователей*

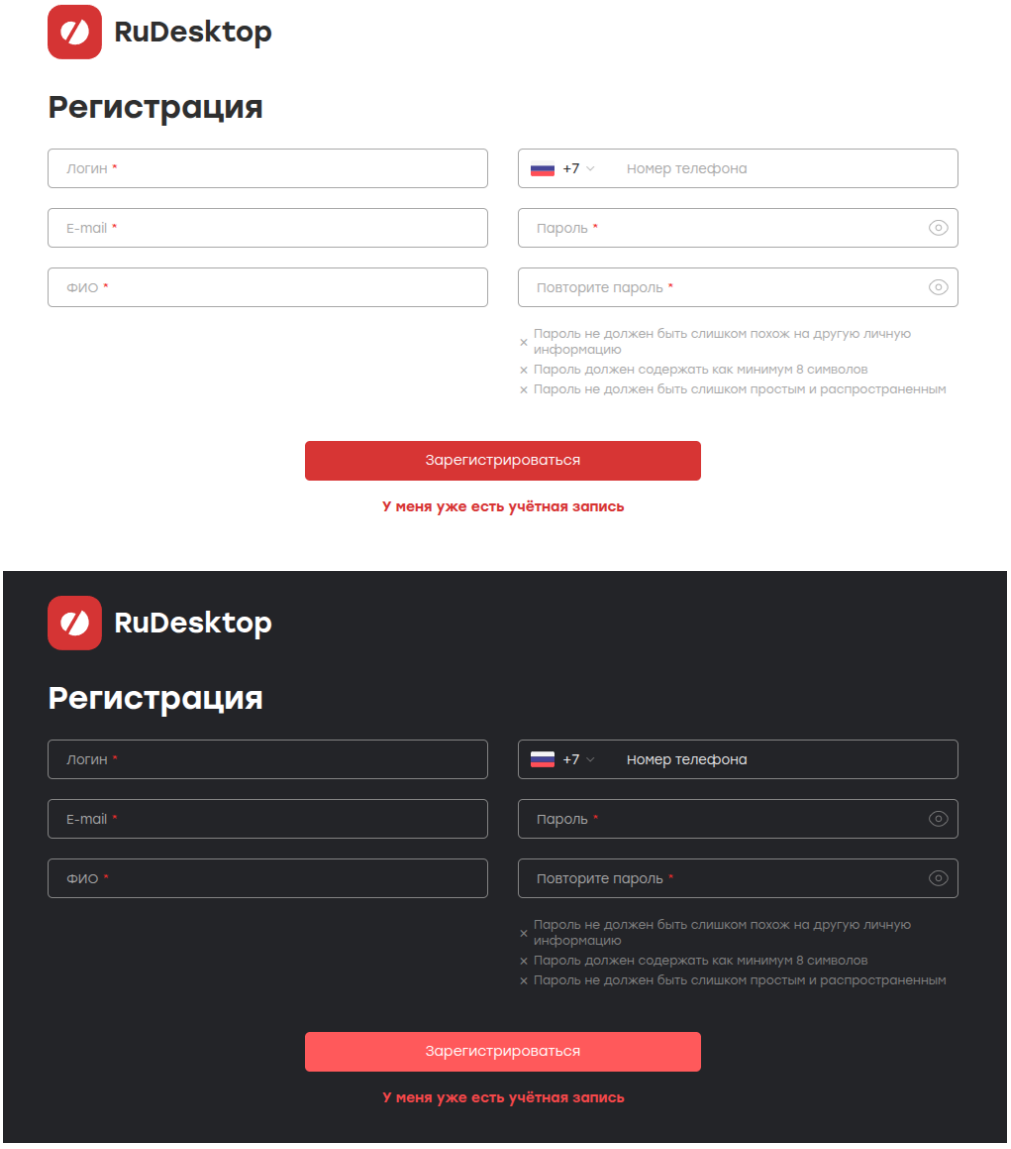

RuDesktop
Вход в аккаунт
Платформа удаленного администрирования
Логин *
@Локальный
Пароль *
Войти
или
Войти по SSO
Создать учётную запись
Забыли свой пароль или имя пользователя?



Для регистрации нового пользователя необходимо:

1. Нажать на кнопку `Создать учетную запись`

   После этого откроется страница регистрации



2. Заполнить поля формы:

   - Логин — обязательное поле
   - Номер телефона — поле с выбором страны и форматированием. Обязательность зависит от настройки сервера `Обязательный номер телефона`

     Подсказка

     Номер, уже указанный у другой учётной записи, использовать нельзя

   - E-mail — обязательное поле, на этот адрес приходит ссылка для подтверждения учётной записи
   - Пароль — обязательное поле; под полем выводятся подсказки к минимальным требованиям к паролю
   - ФИО — необязательное поле для отображаемого имени

- Повторите пароль — обязательное поле, должен совпадать с Пароль

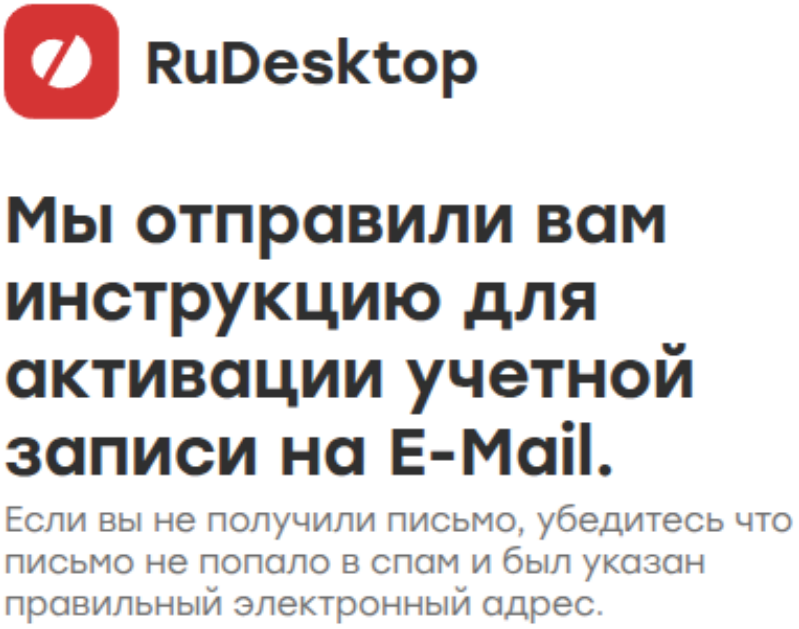
Примечание

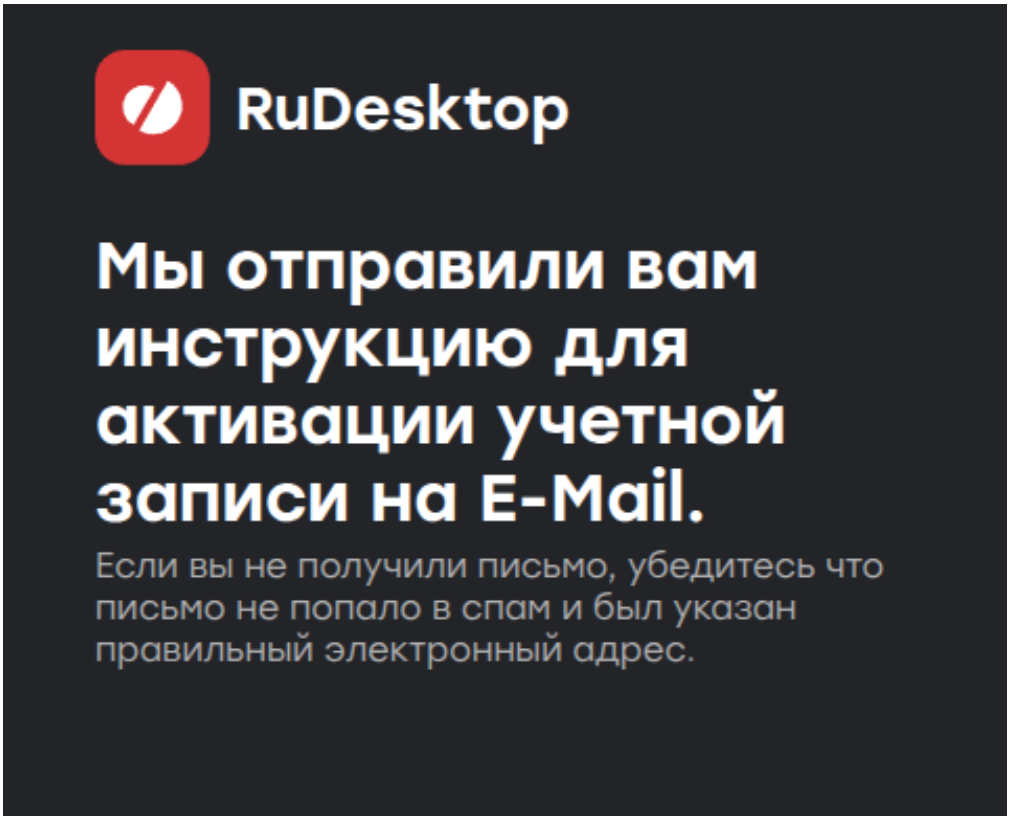
В облачной версии **RuDesktop** дополнительно отображаются обязательные чекбоксы согласия на обработку персональных данных и опциональный чекбокс согласия на получение информационных рассылок

Подсказка

Если в форме регистрации есть поле Капча, пройдите проверку перед отправкой

3. Нажать на кнопку Зарегистрироваться
4. Открыть почту и проверить входящее письмо

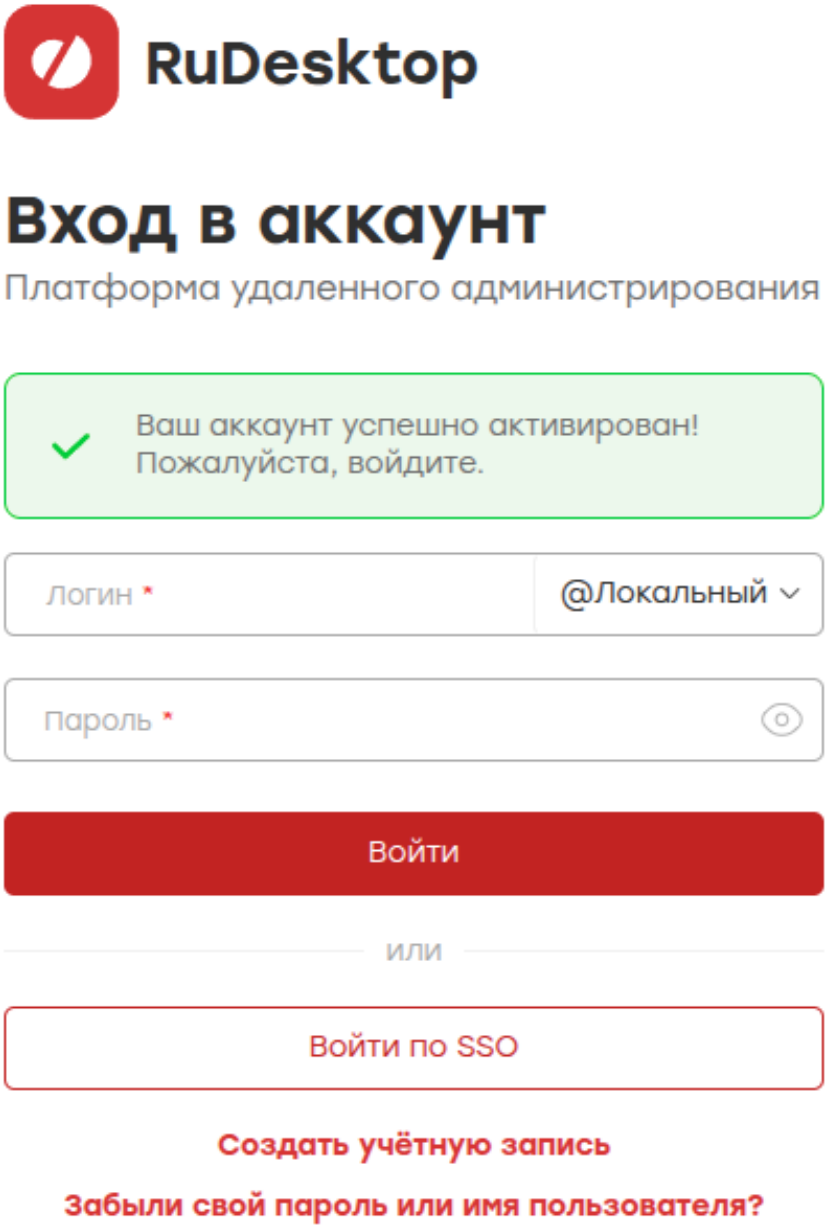


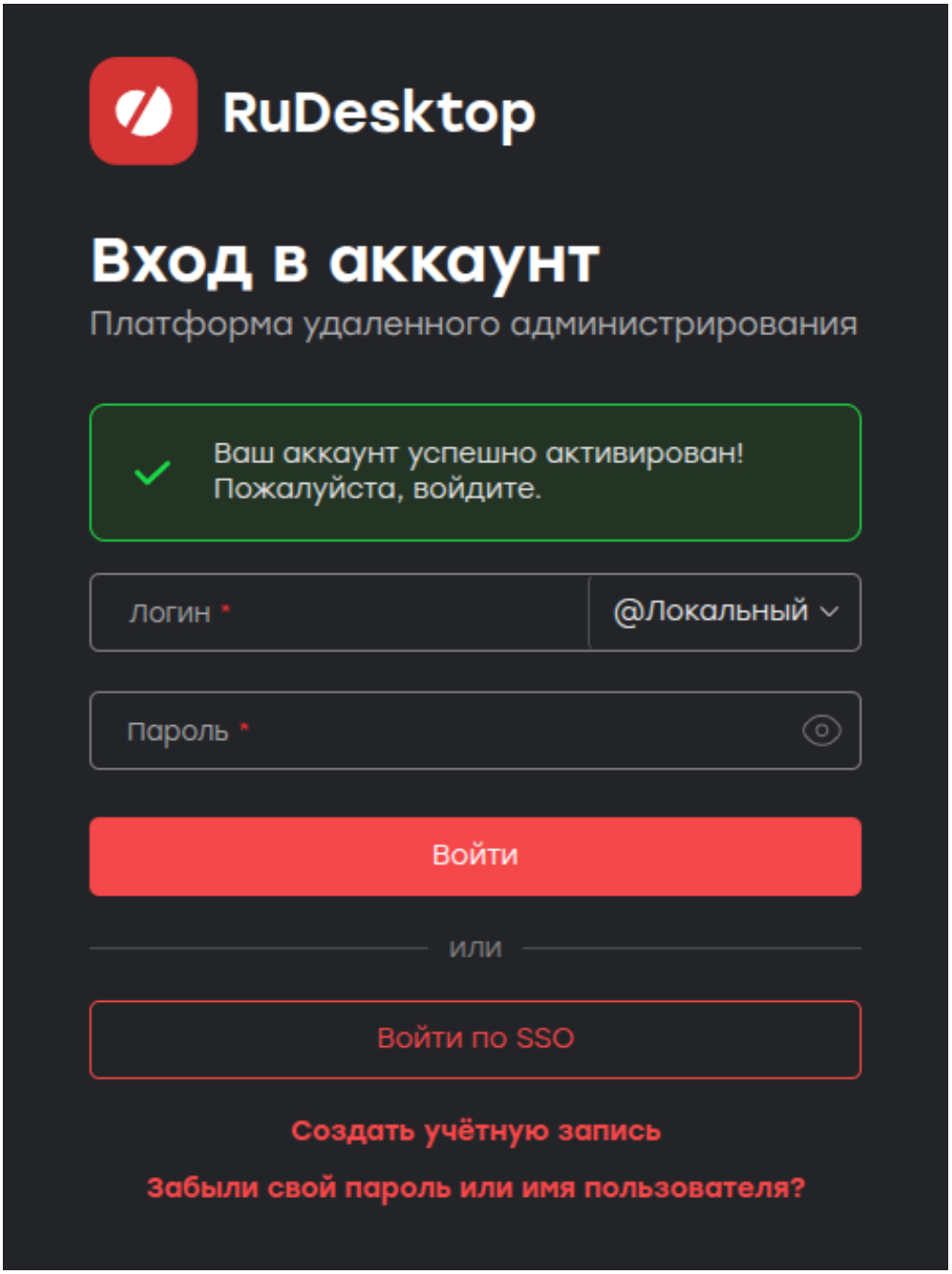


5. Перейти по ссылке из письма для подтверждения учетной записи

> **Важно**
>
> Переход по ссылке из письма обязателен для авторизации под учетной записью
>
> Без перехода по ссылке это вызовет ошибку о недостаточности прав, и авторизоваться не получится

6. После перехода по ссылке регистрация будет завершена


RuDesktop
Вход в аккаунт
Платформа удаленного администрирования
Ваш аккаунт успешно активирован!
Пожалуйста, войдите.
Логин *
@Локальный
Пароль *
Войти
или
Войти по SSO
Создать учётную запись
Забыли свой пароль или имя пользователя?



7. Нажать на кнопку Войти

Подробнее о *Страница авторизации*

2.2 Страница авторизации

Страница авторизации — точка входа в веб-интерфейс **RuDesktop**, доступная по корневому адресу сервера до выполнения входа

Подсказка

Страница авторизации доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

2.2.1 Как это работает

Сервер поддерживает несколько источников учётных записей и определяет, какие виджеты показывать на странице, в зависимости от конфигурации:

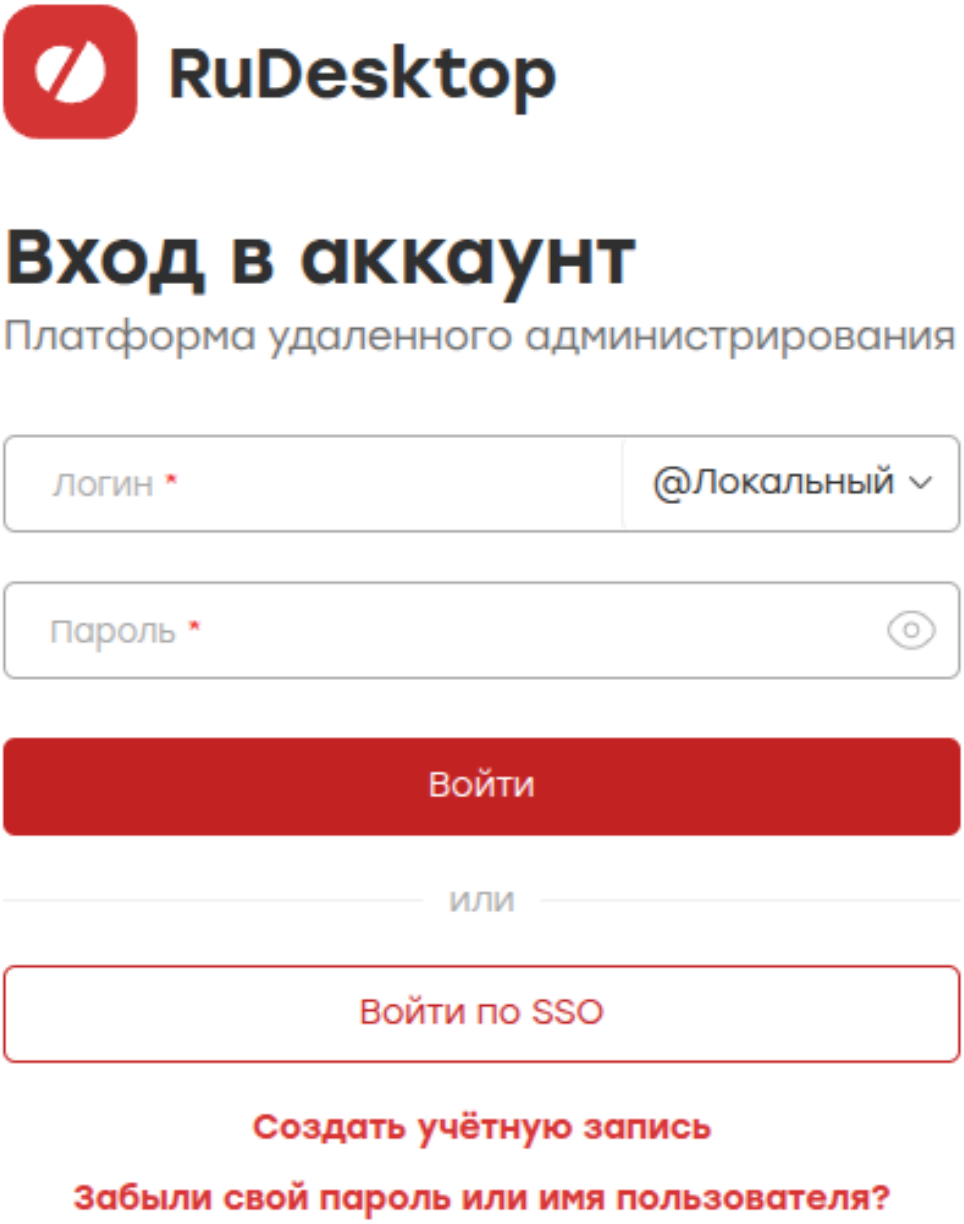
- **локальные учётные записи** — пользователь вводит логин (или Email) и пароль, проверка идёт по базе сервера
- **доменные учётные записи** — при наличии активных *доменов* справа от поля логина появляется выпадающий список; в нём отображаются как LDAP-домены, так и realms активных интеграций с **KeyCloak**, плюс пункт **Локальный**. Выбор домена переключает аутентификацию на LDAP-подключение к контроллеру или на соответствующий realm KeyCloak
- **внешний провайдер (KeyCloak)** — при наличии активной интеграции на странице появляется кнопка входа через *KeyCloak* (SSO)
- **самостоятельная регистрация** — кнопка «Создать учётную запись» отображается только при включённой соответствующей *настройке сервера*, см. *Страница регистрации*

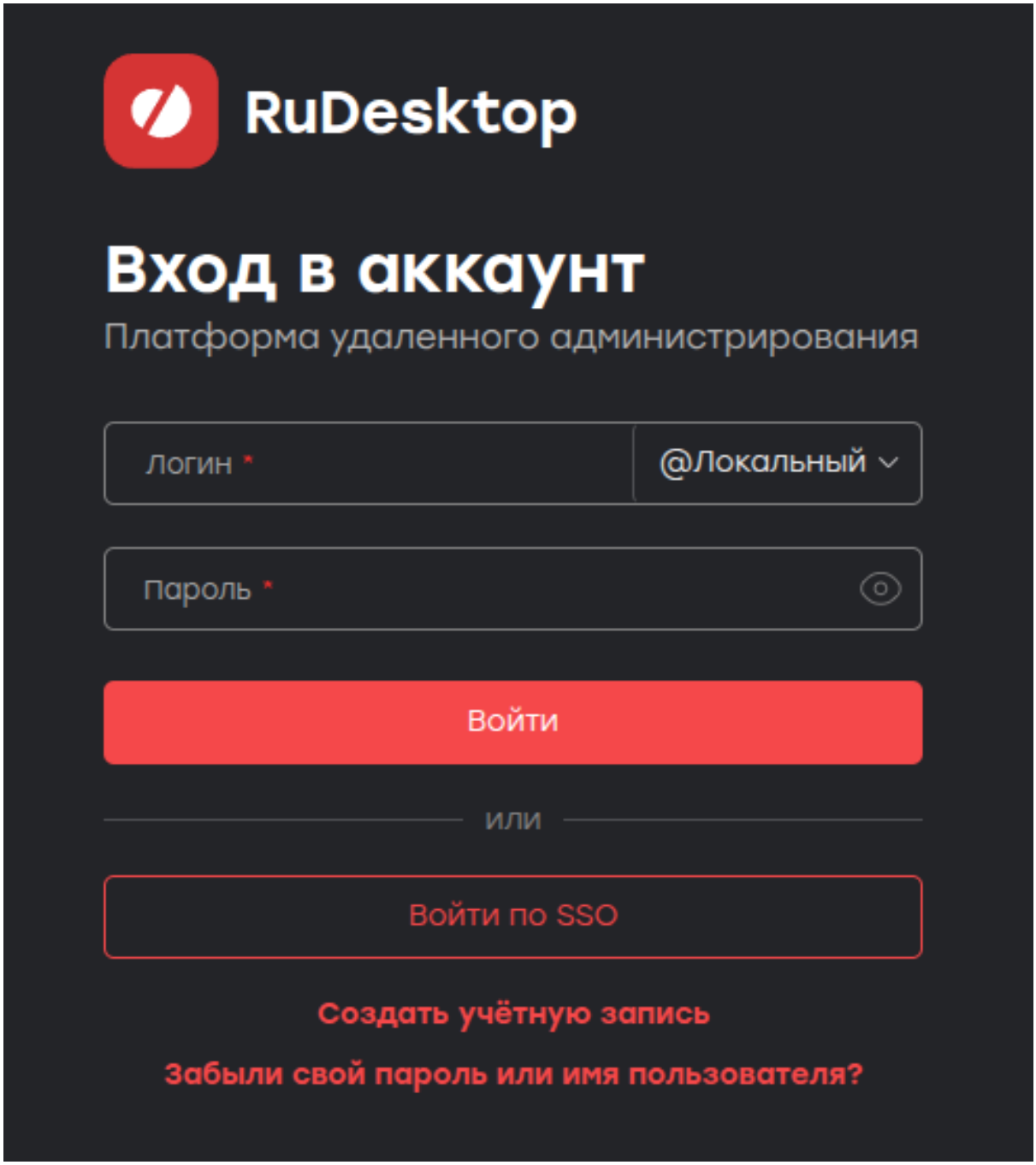
Если у пользователя включена *двухфакторная аутентификация*, после ввода логина и пароля сервер запрашивает одноразовый пароль (OTP) по выбранному каналу — SMS, Email, Telegram, MAX или через собственный сервер OTP

При успешной авторизации сервер открывает *Панель управления*

2.2.2 Авторизация

При переходе в веб-интерфейс сервера откроется страница авторизации, если авторизация не была выполнена ранее


RuDesktop
Вход в аккаунт
Платформа удаленного администрирования
Логин *
@Локальный
Пароль *
Войти
или
Войти по SSO
Создать учётную запись
Забыли свой пароль или имя пользователя?



Для входа необходимо ввести следующие данные в соответствующие поля:

- Логин или E-Mail — наименование поля меняется на Логин, если на сервере есть подключенные домены или **KeyCloak**
- Пароль — пароль учётной записи; рядом с полем доступна кнопка для временного отображения введённого пароля
- Капча — поле подтверждения, что вход выполняет человек

Подсказка

Капча появляется на форме входа только после нескольких подряд неудачных попыток авторизации. Поведение управляется параметрами в *настройках сервера*: общим флагом включения капчи и порогом числа неудачных попыток, после которого она показывается

Примечание

Также справа от поля Логин можно выбрать тип авторизации: локальная или доменная

Если вы хотите выполнить вход под доменным пользователем, необходимо кликнуть по полю и в выпадающем списке выбрать необходимый домен

Важно

Селектор домена отображается только при наличии подключенных доменов к серверу **RuDesktop** или активной интеграции с **KeyCloak**

После ввода логина и пароля необходимо нажать на кнопку Войти и авторизация будет выполнена

Подсказка

Если на сервере активирована интеграция с **KeyCloak** и в настройках включён вход по SSO, под кнопкой Войти отображается отдельная кнопка Войти по SSO для перехода в **KeyCloak**

Важно

При использовании двухфакторной авторизации (OTP) появятся ячейки для ввода одноразового пароля. Чтобы получить код, нажмите кнопку Запросить пароль

Одноразовый пароль придет в зависимости от выбранной настройки *двухфакторной авторизации*

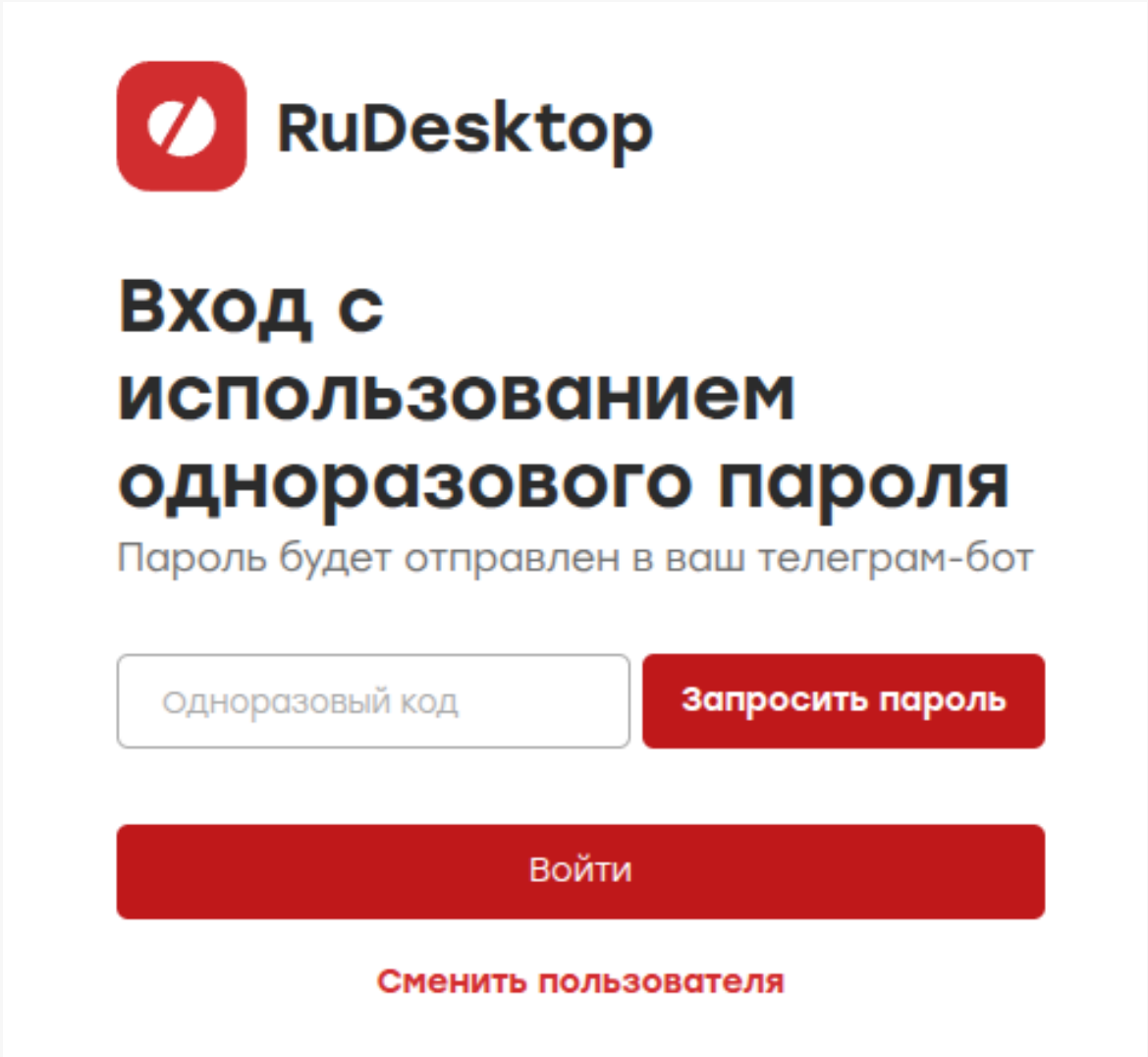
- СМС
- Email
- Телеграм

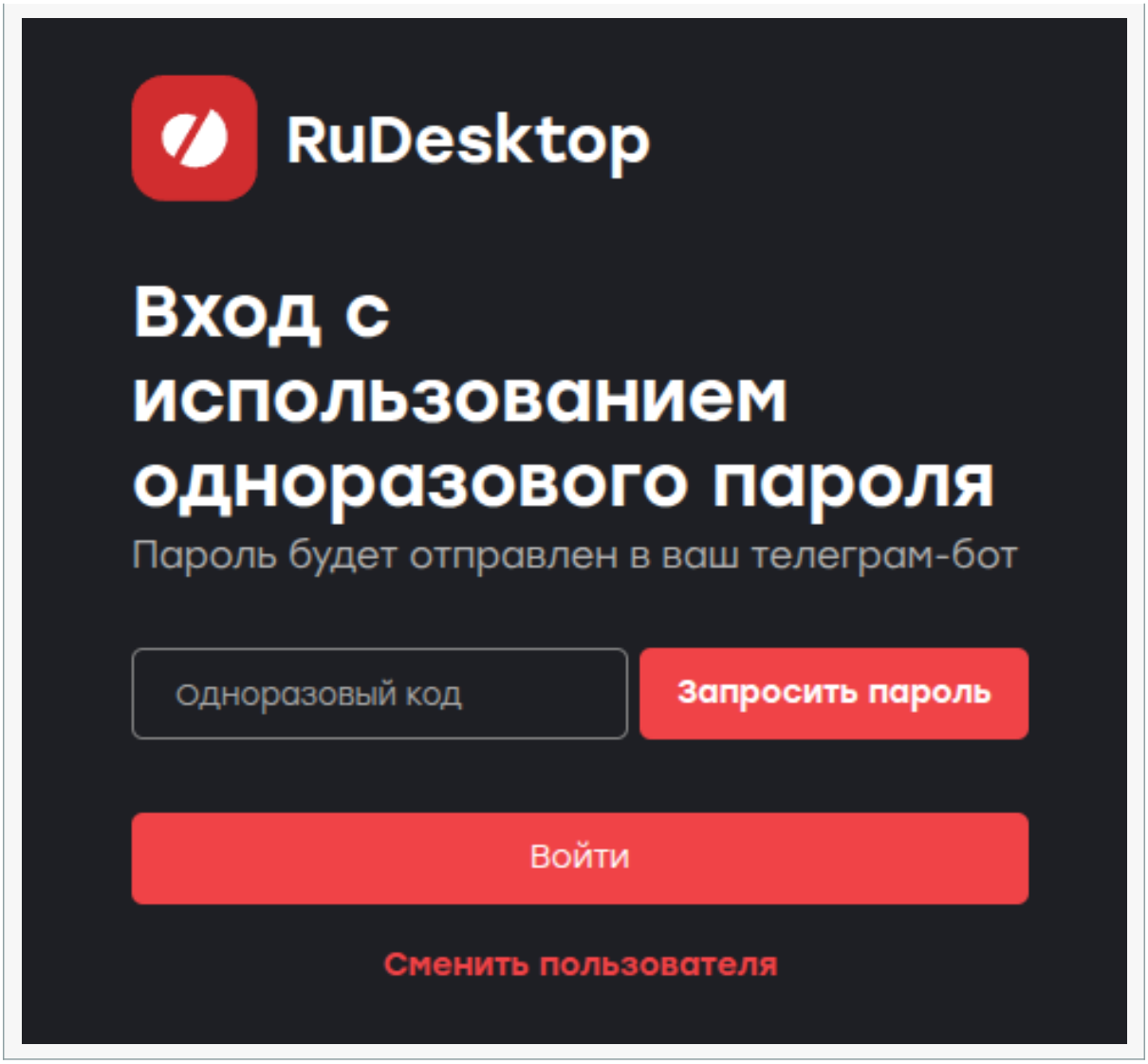
- MAX

- Собственный сервер OTP

Подсказка

При способе **Собственный сервер OTP** код генерирует и проверяет сторонний сервис, а канал доставки определяет он же. Подробнее — в кейсе Настройка двухфакторной авторизации через собственный сервер OTP





Дополнительные методы MFA

Помимо OTP по SMS/Email/Telegram/MAX и через собственный сервер OTP, **RuDesktop** поддерживает дополнительные методы многофакторной аутентификации (MFA). Если у пользователя настроено несколько методов, после ввода логина и пароля сервер откроет страницу выбора метода

Доступные методы:

- TOTP — одноразовый код из приложения-аутентификатора (Google Authenticator, Яндекс.Ключ и аналогичные), генерируемый по алгоритму Time-based One-Time Password
- FIDO2 (WebAuthn) — вход по аппаратному ключу безопасности или встроенной биометрии устройства
- PKI — вход по клиентскому сертификату X.509

Подключение и сброс методов MFA выполняются на вкладке Безопасность аккаунта в *свойствах пользователя*

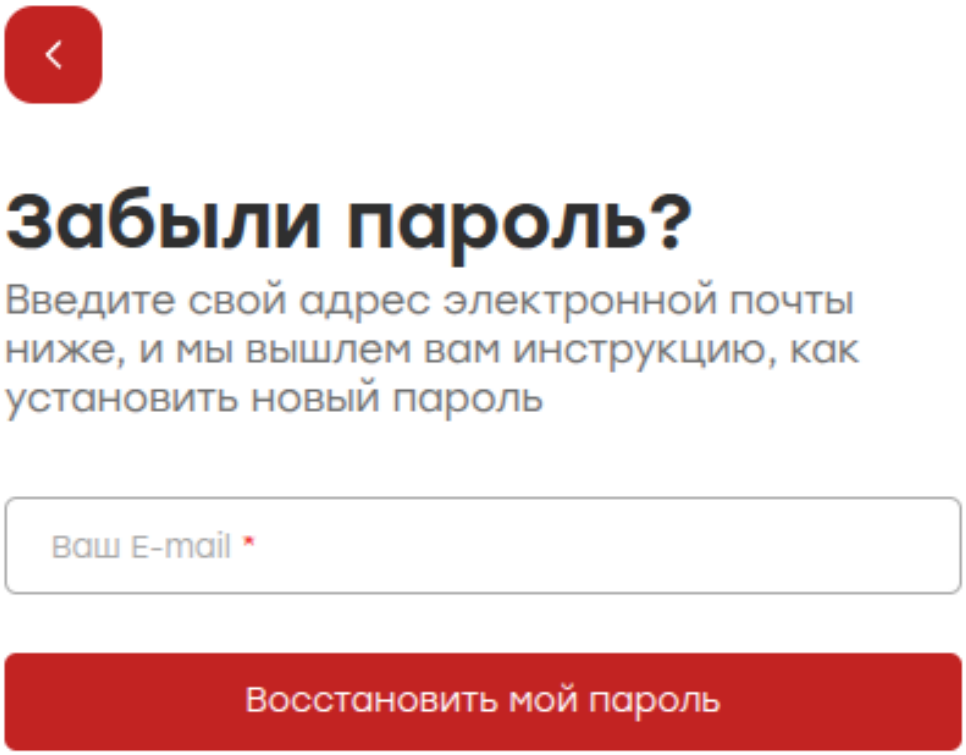
Примечание

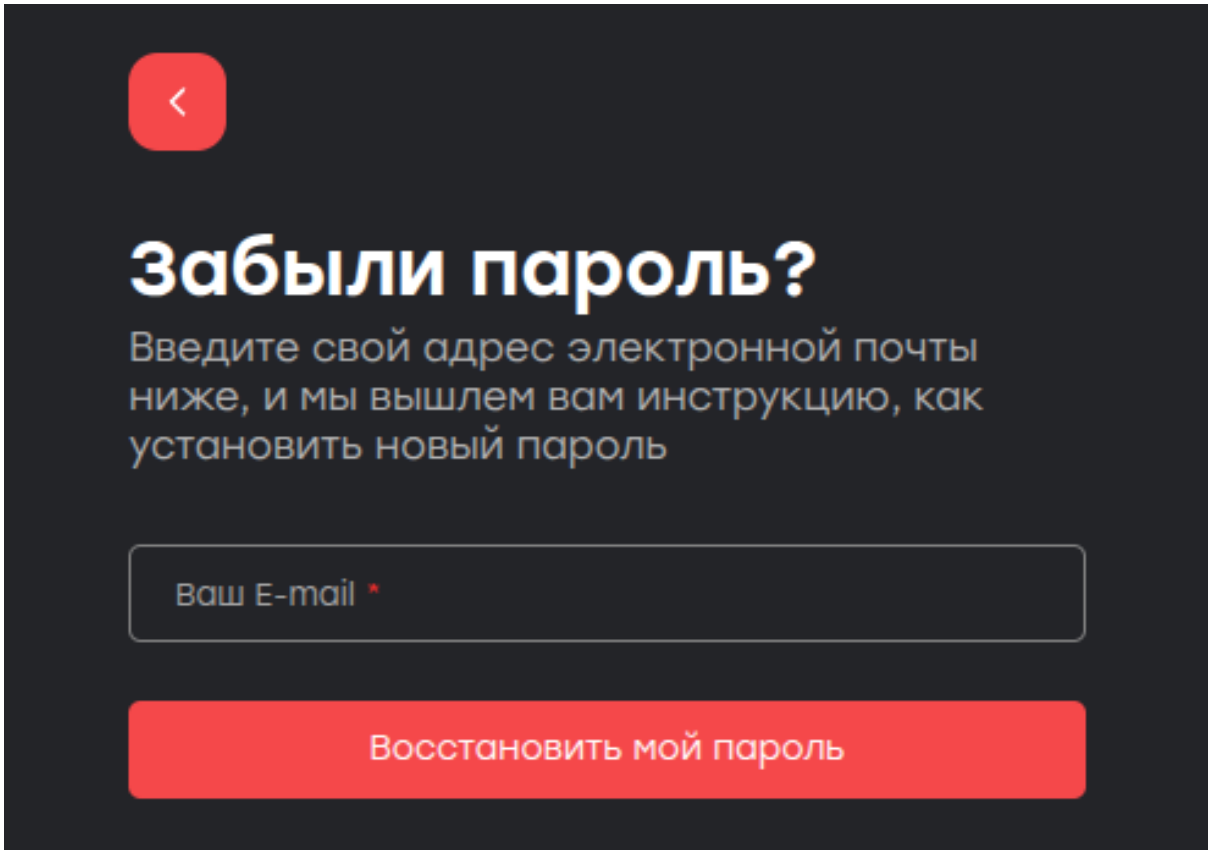
При входе с OTP или TOTP введите шестизначный код по одной цифре в каждую ячейку или вставьте его целиком из буфера обмена в любую ячейку. При вводе цифры курсор автоматически переходит к следующей ячейке. После заполнения всех шести ячеек код автоматически отправляется на проверку, нажимать кнопку Войти не требуется

После прохождения двухфакторной/многофакторной аутентификации вы попадете на страницу *Панель управления*

2.2.3 Восстановление пароля

Если вы забыли имя пользователя или пароль, нажмите на кнопку `Забыли свой пароль или имя пользователя?` и в следующем диалоговом окне в Ваш E-mail введите свой Email-адрес, который был указан при создании или регистрации вашей учетной записи





После этого нажмите на кнопку Восстановить мой пароль и ожидайте инструкцию на ваш Email-адрес

2.3 Панель управления

Панель управления — стартовая страница веб-интерфейса **RuDesktop**, открывающаяся после авторизации. Содержит сводные виджеты по серверу и блоки быстрого доступа к основным разделам

Подсказка

Панель управления доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

2.3.1 Как это работает

Страница состоит из нескольких независимых виджетов, каждый из которых формируется по данным соответствующего раздела системы:

- **«Устройства онлайн»**, **«Платформы»** — агрегаты по таблице *Устройства*
- **«Сессии»** — счётчики типов соединений (NAT/RELAY/LOCAL) из *Сессий*
- **«Активные сессии»** — диаграмма-полудонат с количеством активных подключений в текущий момент
- **«Состояние задач»** — таблица с прогрессом выполнения задач из *Задач*

- **«Последние действия»** — лента событий из журнала *Объектов*
- **«Установка клиентов»** — ссылки на установочные пакеты, видны только при наличии права **«Может устанавливать клиентов»**
- **«Блок быстрого доступа»** — автоматически формируемый список разделов системы со счётчиками и кнопками быстрых действий (Добавить-/Изменить/Перейти)

Часть виджетов скрывается, если у пользователя нет прав на соответствующий источник данных. Из шапки страницы доступны переходы в Справку[16], к новостям версии и в профиль пользователя

На круговых диаграммах **«Устройства онлайн»**, **«Платформы»** и **«Сессии»** можно перейти к записям:

- Нажмите на сектор, чтобы открыть список с фильтром по выбранному состоянию устройства, платформе или типу сессии
- Нажмите на число в центре, чтобы открыть список без фильтра диаграммы: для **«Устройства онлайн»** и **«Платформы»** откроются **«Устройства»**, для **«Сессии»** - **«Сессии»**

При переходе сохраняются ограничения доступа пользователя к записям



2.3.2 Навигационное меню

В левой части страницы расположено навигационное меню, позволяющее легко перемещаться между страницами

2.3.3 Шапка страницы

В шапке страницы расположены:

Слева:

- Кнопка `Справка` — при нажатии откроется страница с документацией

[16] https://help.rudesktop.ru/

- Кнопка `Поддержка` — при нажатии откроется страница для создания обращения в службу технической поддержки компании **RuDesktop**
- Ссылка `Версия X.X-build` — при нажатии откроется страница с историей версий, на которой отображены все улучшения и изменения по каждой версии

Справа:

- Индикатор `Доступна новая версия` — при нажатии откроется всплывающее окно, в котором отображается информация о доступной новой версии сервера

> **Важно**
>
> Индикатор отображается только суперпользователю

- Кнопка переключения темы (светлая/тёмная)
- Кнопка авторизованного пользователя — при нажатии на нее откроется контекстное меню, из которого можно перейти в профиль пользователя для изменения данных, сменить пароль или выйти из учетной записи на сервере
- Кнопка скрытия навигационного меню — при нажатии на которую произойдет скрытие или раскрытие навигационного меню

2.3.4 Установка клиентов

Ссылки для скачивания скриптов установки/установочных пакетов для клиентского приложения на все поддерживаемые ОС

> **Важно**
>
> Виджет отображается только пользователю с активным правом Может устанавливать клиентов

2.3.5 Устройства онлайн

Отображает данные по количеству устройств, которые находятся в сети

2.3.6 Платформы

Отображает данные по количеству устройств на конкретных платформах (Linux, Windows, Android, macOS)

2.3.7 Сессии

Отображает количество сессий по типу подключения: LOCAL (LOCAL — это подключение P2P внутри локальной сети), RELAY (RELAY — это узел, занимающийся получением/пересылкой (подключение через сервер)), NAT (NAT —

это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов) и **AUTO** (автоматический выбор типа сервером)

2.3.8 Активные сессии

Виджет в виде полудонат-диаграммы отображает количество подключений, находящихся в активном состоянии в текущий момент (со статусами LOCAL, NAT, RELAY)

Важно

Виджет отображается только пользователю с активным правом Может просматривать статистику

2.3.9 Состояние задач

Таблица отображает прогресс выполнения задач со столбцами: **Название**, **Статус**, **Прогресс**, **Успешно**, **Недоступно**, **Ошибка**

Важно

- Виджеты **«Устройства онлайн»**, **«Платформы»** и **«Сессии»** отображаются только пользователю с активным правом Может просматривать статистику
- Виджет **«Состояние задач»** отображается только пользователю с активным правом просмотра задач (Политики -> Просмотр)

2.3.10 Последние действия

В данном блоке отображается список последних действий с указанием имени пользователя, который произвел действие

2.3.11 Блок быстрого доступа

Автоматически формируемый список основных разделов системы. Для каждого раздела отображается количество записей и кнопки быстрых действий (Добавить/Изменить/Перейти). Состав блока зависит от прав пользователя — отображаются только те разделы, к которым у пользователя есть доступ

2.4 Импорт записей в списки выбора

Кнопка Импорт в правом столбце списка выбора позволяет добавить записи из файла. Она доступна в поддерживающих импорт полях, например при выборе устройств в свойствах задачи и доступа

Примечание

Импорт подбирает **существующие** записи сервера, доступные пользователю, а не создает новые устройства или задачи

Импорт также доступен для списков пользователей и устройств в свойствах группы и для списка групп в свойствах пользователя. Списки подразделений и динамических групп пользователя этим импортом не заполняются

Важно

Для импорта нужны права на изменение редактируемого объекта и доступ к соответствующим записям. Наличие права только на создание объекта недостаточно

2.4.1 Порядок действий

1. Откройте свойства задачи или доступа и нужный список выбора
2. Нажмите Импорт и выберите файл `.txt`, `.csv`, `.xls` или `.xlsx`
3. Проверьте добавленные записи в правом столбце и сообщения под списком
4. Нажмите Сохранить или Сохранить и продолжить в форме

Важно

Импорт только дополняет выбранное в форме: прежние записи не удаляются, повторения не добавляются

Пока форма не сохранена, изменения не вступают в силу

В отличие от массовых действий «Добавить и сохранить все», импорт можно использовать и при создании еще не сохраненной задачи или доступа

2.4.2 Формат файла

В простом списке укажите одну запись на строку или в первом столбце таблицы. Поиск выполняется без учета регистра:

- устройства - сначала по `server_id` (ID RuDesktop), затем по `hostname` (имя хоста);
- пользователи - сначала по `username` (логин), затем по `email`;
- группы и динамические группы - по `name` (название)

Пример списка устройств:

```
123456789
office-pc-01
```

Если одинаковое имя подходит нескольким устройствам, уточните запись с помощью двух столбцов и строки заголовка:

```
server_id;hostname
123456789;office-pc-01
```

В этом режиме должны совпасть все непустые значения в распознанных столбцах строки; столбцы с неизвестными заголовками не участвуют в поиске. Для пользователей можно использовать заголовок `username;email`. Режим нескольких столбцов включается, когда в заголовке распознаны как минимум два разных поля; иначе используется первый столбец, а первая строка считается данными, а не заголовком

Допустимы также названия полей интерфейса, перечисленные в подсказке кнопки импорта

2.4.3 Ограничения

- Размер файла - не более 5 МиБ, число непустых строк, включая заголовок, - не более 10 000
- Читаются первые 8 столбцов; в каждой ячейке учитываются только первые 255 символов
- В `.xlsx` читается активный лист, в `.xls` - первый лист
- Для `.xlsx` суммарный размер содержимого файла после распаковки не должен превышать 30 МиБ
- Для текстовых файлов поддерживаются UTF-8 и Windows-1251; разделитель CSV определяется среди запятой, точки с запятой и табуляции
- После 100 пустых строк подряд чтение прекращается

  Не разделяйте данные такими промежутками

Если запись не найдена или совпадение неоднозначно, она не добавляется и отображается в сообщении под списком. Проверьте ID, имя и права пользователя, уточните файл и повторите импорт. Импорт не расширяет права доступа к записям

2.4.4 Выбор записей с поиском

В списках с двумя столбцами можно последовательно найти и отметить несколько записей

1. В левом столбце найти первую запись и установить её флажок
2. Изменить поисковый запрос, найти и отметить следующую запись
3. Перенести отмеченные записи в правый столбец кнопкой со стрелкой
4. Проверить состав правого столбца и сохранить форму

Примечание

Изменение поискового запроса не снимает уже установленные флажки

При переносе учитываются и отмеченные записи, скрытые текущим поиском

После переноса поисковые строки очищаются

Подсказка

Флажок в левом столбце только отмечает запись для переноса. Чтобы включить запись в сохраняемый состав, перенести её вправо и сохранить форму

2.5 Портал самообслуживания

Доступен в УД и UEM версиях

Портал самообслуживания - отдельная веб-страница для конечных пользователей удалённых устройств: установка приложений по запросу и обращения в поддержку без участия администратора

Подсказка

Портал самообслуживания доступен при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Сам магазин приложений работает в обеих редакциях, но шаблоны установки стороннего ПО (*Установка пакета*, *Установка пакета из архива*, *Установка/удаление пакета из репозитория*) требуют **UEM**

В редакции **Удалённый доступ** в магазин можно опубликовать только встроенные RD-шаблоны - например, *Автоматическое обновление клиента RuDesktop*

Важно

Перейти на портал можно только из клиента **RuDesktop**, нажав Открыть в одном из разделов дополнительной области:

- **Поддержка и портал самообслуживания** - открывает портал с разделами **Магазин приложений** и **Обращение**
- **Магазин приложений** - открывает портал сразу на разделе **Магазин приложений**

2.5.1 Как это работает

Клиент **RuDesktop** открывает портал в браузере, передавая серверу идентификатор текущего устройства

Сервер по этому идентификатору определяет права устройства и пользователя и формирует две основные функции:

- **Магазин приложений** - список *политик*, у которых на вкладке **«Портал самообслуживания»** активирован чекбокс Показывать в магазине приложений

  Поведение кнопки в карточке приложения зависит от чекбокса Автоматический запуск в политике:

  - чекбокс активен - кнопка отображается как Установить, сервер сразу создаёт *задачу* на выполнение политики и запускает её на устройстве
  - чекбокс не активен - кнопка отображается как Запросить установку, сервер вместо запуска создаёт обращение типа **Запрос на выполнение политик**, которое ожидает обработки администратором

  История установок по каждому приложению видна по кнопке История установок рядом с карточкой

  Важно

  После входа в браузере права пользователя и группы устройства учитываются совместно.

  - Может видеть магазин приложений в портале самообслуживания — просмотр каталога и запрос установки приложений без автоматического запуска
  - Может использовать магазин приложений — самостоятельная установка приложений с автоматическим запуском

  Подробная схема настройки и проверки прав описана в кейсе Публикация приложения в магазине приложений

- **Обращение** - форма создания *обращений* двух типов:

- **Обращение в поддержку** - текстовое сообщение, попадает в админ-панель со статусом «Открыт» для обработки администратором
- **Запрос на выполнение политик** - пользователь выбирает заранее опубликованные политики; политики с активированным чекбоксом Автоматический запуск запускаются на устройстве сразу, без подтверждения администратором, остальные ждут запуска на странице *Обращения*

> **Важно**
>
> Тип **«Запрос на выполнение политик»** отображается только на сервере с активной лицензией **UEM**

> **Примечание**
>
> В *настройках сервера* можно указать **«URL внешнего HelpDesk»** - тогда переход в раздел **«Обращение»** перенаправляет пользователя на внешний адрес (опционально с параметрами устройства), а встроенная форма не открывается

2.5.2 Навигационное меню

В левой части страницы расположено навигационное меню, позволяющее легко перемещаться между страницами

В навигационном меню расположены ссылки на следующие страницы:

1. Магазин приложений
2. Обращение

2.5.3 Магазин приложений

Магазин приложений - каталог доступных для установки приложений на удалённом устройстве

> **Важно**
>
> По умолчанию для доступа к магазину необходимо авторизоваться в веб-интерфейсе сервера **RuDesktop**
>
> На странице *Администрирование → Настройки* в блоке Безопасность можно активировать чекбокс Неавторизованный пользователь может видеть магазин приложений (IP адрес должен совпадать) - тогда магазин откроется без логина и пароля при условии, что IP запроса совпадает с полем Сетевой адрес в карточке устройства
>
> Подробнее - в кейсе Публикация приложения в магазине приложений

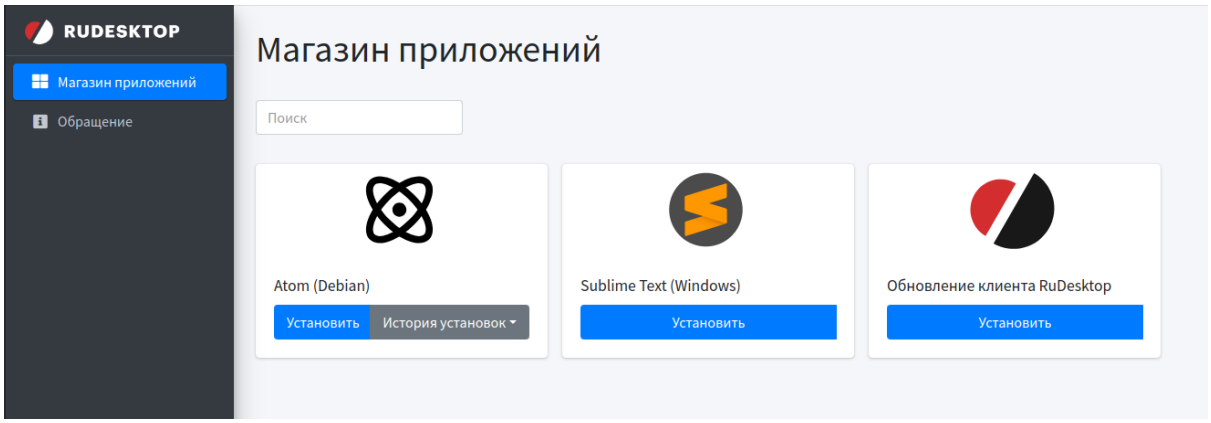
Внимание

Чтобы приложения отображались в магазине приложений, необходимо настроить параметры в политике на вкладке *«Портал самообслуживания»*

Если есть только право просмотра магазина:

- Каталог приложений доступен
- Можно отправить запрос для приложений, у которых отключён **Автоматический запуск**
- Автоматическая установка недоступна

На странице **«Магазин приложений»** отображено:



1. Поле поиска
2. Доступные для установки приложения, сгруппированные по категориям

Примечание

Категория задаётся в политике на вкладке *«Портал самообслуживания»* в поле Категория приложения (например, «Офисные пакеты», «Утилиты»)

Список категорий ведёт администратор сервера

Для установки приложения необходимо:

1. Нажать на кнопку Установить в карточке приложения

Примечание

Если в политике приложения не активирован чекбокс Автоматический запуск, кнопка отображается как Запросить установку - нажатие создаёт обращение типа **Запрос на выполнение политик**, которое ожидает обработки администратором на странице *Обращения*

2. Дождаться завершения установки на устройстве
3. После обновления страницы рядом с кнопкой Установить отобразится кнопка История установок

Примечание

При нажатии на кнопку История установок будут отображаться дата и статус каждой попытки установки приложения

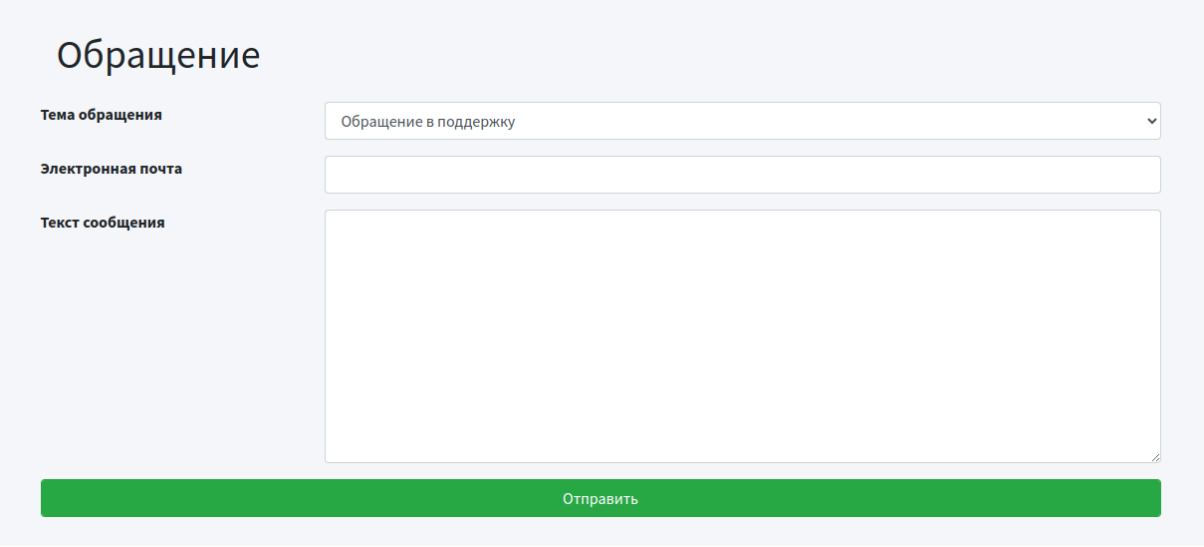
См. также

Пошаговая инструкция по публикации приложения в магазине: Публикация приложения в магазине приложений

2.5.4 Обращение

Обращение - это форма для создания запросов в техническую поддержку, либо создания запросов на выполнение политик

На странице **«Обращение»** отображено:



1. **Тема обращения** - выбор обращения
    1. Обращение в поддержку - для отправки текстового сообщения в службу поддержки
    2. Запрос на выполнение политик - запрос на выполнение политик на устройстве
2. **Электронная почта** - указание адреса электронной почты пользователя, который регистрирует обращение для обратной связи
3. **Политики** - выбор политик для выполнения запроса на устройстве

Важно

Данное поле доступно только при выборе обращения Запрос на выполнение политик

4. **Текст сообщения** - текст обращения в службу поддержки

2.5.5 Создание обращения и список обращений

Примечание

Пользователь создаёт обращение из клиента RuDesktop или через раздел **«Обращение»** портала самообслуживания. В административном списке обращений кнопка добавления не предусмотрена. Этот список предназначен для просмотра и обработки поступивших обращений

2.6 Удаленный доступ

2.6.1 Устройства

Свойства устройства

Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств

Примечание

Для просмотра страницы необходим доступ к устройству и право **«Устройства → Просмотр»**. Право **«Устройства → Изменение»** для просмотра данных не требуется. Оно нужно для сохранения изменений, в том числе групп и комментария

Если вкладка не отображается

Проверить права пользователя, в том числе полученные через группы, и наличие данных у выбранного устройства

- **«Дополнительная информация»** и **«Факты»** доступны с правом **«Инвентаризация → Просмотр»**, если у устройства уже есть собранные факты
- **«Группы»** требует права **«Группы → Просмотр»**
- Сведения LDAP доступны с правом просмотра доменов и при наличии связи устройства с объектом LDAP
- **«Логи»** требует права **«Может просматривать логи в свойствах устройства»**

- Управление логами требует отдельного права **«Может управлять логами устройства (загрузка и удаление)»**
- **«История входов»** доступна суперпользователю

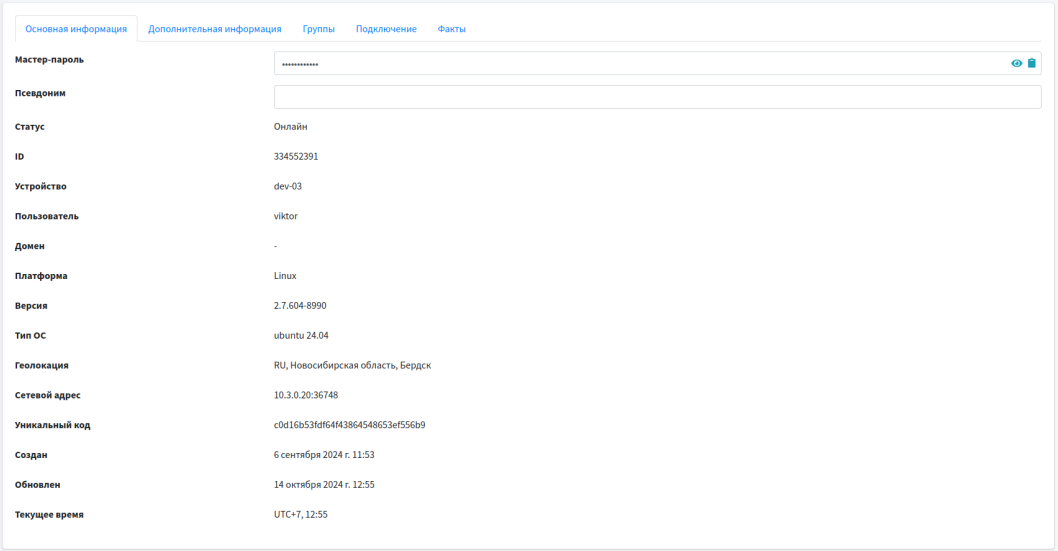
Подсказка

Например, чтобы дать сотруднику возможность просматривать инвентаризацию, предоставить доступ к нужным устройствам, просмотр устройств и просмотр инвентаризации. Право изменения устройств только ради чтения этих сведений выдавать не требуется. Если права выданы, но вкладок инвентаризации нет, выполнить сбор данных политикой инвентаризации и проверить результат на нужном устройстве

Описание вкладок

Основная информация

Доступные поля во вкладке Основная информация:



1. Мастер пароль - генерируется в момент подключения устройства к серверу

   Также его можно просмотреть

Важно

1. Просмотр мастер-пароля доступен только суперпользователю, а также пользователю, у которого активно право **«Может видеть мастер пароль»**
2. Мастер-пароль служит для подключения к устройству без ввода временного или постоянного пароля, но для этого нужно, чтобы было активно право подключения **«Доступ к устройствам по мастер паролю»** в *доступах*

3. Мастер-пароль служит для подключения сервера к устройству при выполнении политик

2. Псевдоним - имя, которое можно указать для удобства использования и поиска
3. Статус - офлайн/онлайн статус устройства в сети
4. ID - идентификатор устройства, который отображается в окне клиента **RuDesktop** и присваивается при подключении устройства к серверу
5. Устройство - имя хоста (hostname)
6. Пользователь - имя пользователя, выполнившего вход в учетную запись на устройстве

Примечание

Если устройство привязано к доменной учётной записи, в этом поле отображается ссылка на профиль владельца - с его ФИО, если оно заполнено, либо с логином

То же ФИО показывается в столбце Полное имя в таблице устройств

Подробнее о том, как устанавливается связь - *Как заполняется столбец «Полное имя»*

7. Домен - имя домена, к которому подключено устройство
8. Подразделение в домене - подразделения (OU) каталога, в которых находится устройство, от корня домена, например **Филиал №1/Отдел ИТ**. Заполняется при синхронизации с доменом; у устройств вне подразделений поле пустое
9. Путь до объекта в LDAP - информация о том, по какому пути в LDAP находится устройство
10. Платформа - операционная система, на которой запускается программа (например, Windows, Linux, macOS, Android)
11. Версия - версия клиентского приложения **RuDesktop**
12. Тип ОС - операционная система, установленная на устройстве
13. Геолокация - физическое расположение устройства относительно геопозиции или подсети
14. Сетевой адрес - IP-адрес устройства с указанием порта
15. Уникальный код - UUID устройства
16. Создан - дата и время первого подключения устройства к серверу
17. Обновлен - дата и время последнего ответа от устройства

18. Текущее время - текущее время на устройстве, в формате **«Часовой пояс, время»**

Дополнительная информация

Вкладка доступна с правом **Инвентаризация → Просмотр**, если у устройства есть собранные факты

Сводка

Данная вкладка разделена на две части и содержит информацию об оборудовании удалённого устройства:



Важно

Данные появляются после выполнения политики *Инвентаризация*

В левой части отображается следующая информация:

- Материнская плата
- Процессор
- Модули оперативной памяти
- Диск
- Видеокарта
- Подключенные мониторы
- Сетевая карта
- Данные о сетевых адресах
- MAC-адрес

Примечание

За исключением данных о сетевых и MAC-адресах, всю информацию можно рассмотреть более детально, нажав на название

В правой части отображается следующая информация:

- Занятое и свободное место на системном диске (Системный диск - это жёсткий диск или твердотельный накопитель (SSD), на котором установлена операционная система вашего компьютера)
- Статус S.M.A.R.T
- Наличие BitLocker
- Дата последней инвентаризации - время обновления инвентаризационных данных, отображаемое с учетом часового пояса веб-интерфейса

> **Подсказка**
>
> Вы можете открыть страницу с информацией о *наличии ресурсов* для данного устройства, нажав на дату
>
> Также доступна кнопка для копирования этой информации в буфер обмена или выгрузки в выбранный формат файла

Установленное ПО

Содержит программы, обнаруженные последней инвентаризацией: название и установленную версию. Столбцы **Издатель** и **Комментарий** появляются, если для программ есть соответствующие данные

Поле **Поиск по установленному ПО** отбирает строки этой таблицы. Нажатие на название открывает карточку ресурса в каталоге. Службы отображаются отдельно, на вкладке **Службы**

Если программа не отображается, выполнить инвентаризацию со сбором установленного ПО. История появления и удаления доступна в *Наличии ресурсов*, а сводка версий по устройствам — в *Аудите ПО*

Службы

Вкладка **Службы** внутри **Дополнительной информации** содержит информацию о службах удаленного устройства

Для устройств Android эта вкладка не отображается

Кнопка **Изменить статус выбранных служб** и флажки выбора служб доступны, если выполнены все условия:

- Используется версия **Управление конфигурациями (UEM)**
- У пользователя есть право **Может запускать политики**
- Устройство работает не под macOS

Примечание

Без UEM элементы управления скрыты. Собранные сведения о службах остаются доступны для просмотра с правом **Инвентаризация → Просмотр**

Важно

Данные появляются после выполнения политики *Инвентаризация*

Плагины браузера

Содержит включённые плагины браузеров, обнаруженные последней инвентаризацией: браузер, название плагина и его описание

Поле **Поиск по плагинам браузера** отбирает строки этой таблицы. Нажатие на название открывает карточку ресурса в каталоге

Читаются все профили браузеров всех пользователей устройства. Отключённые плагины, темы оформления и встроенные компоненты браузера не отображаются

Вкладка недоступна для устройств Android

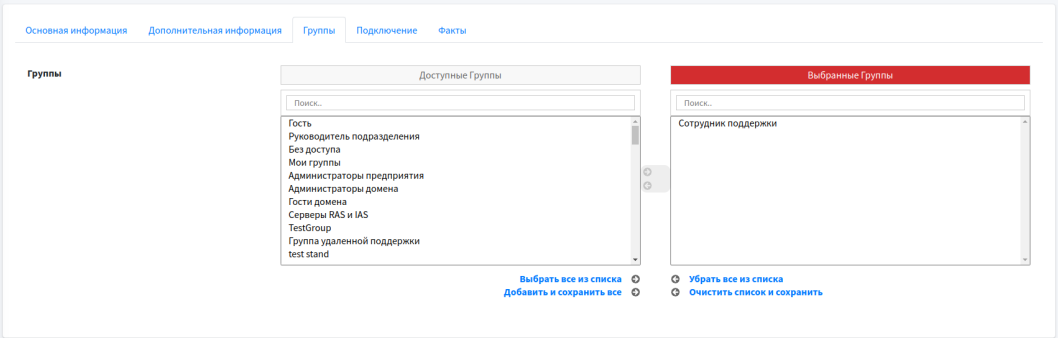
Важно

Данные появляются после выполнения политики *Инвентаризация* с выбранным типом данных **Пакет → Плагин браузера**

Группы

Вкладка доступна с правом **Группы → Просмотр**

Доступные поля во вкладке Группы:



На данной вкладке размещена таблица добавления устройства в группы

Таблица разделена на 2 блока:

1. Доступные группы
2. Выбранные группы

Для добавления устройства в группу необходимо кликнуть в блоке **«Доступные группы»** на необходимую группу и далее кликнуть на между блоков или двойным кликом по группе, после чего в меню действий нажать на кнопку Сохранить или Сохранить и продолжить

Примечание

- Устройство можно добавлять в неограниченное количество групп
- Группы необходимы для разграничения прав доступа к устройствам

  Подробнее о *группах*

Примечание

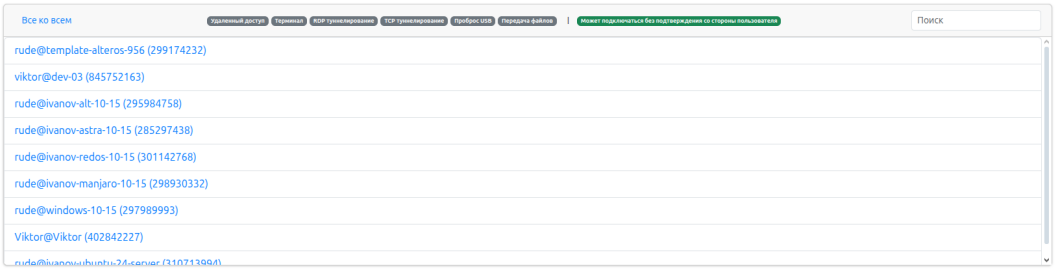
Помимо поштучного добавления доступны массовые действия над всем списком - кнопки Добавить и сохранить все и Очистить список и сохранить

Они доступны только после сохранения записи

При большом количестве элементов действие выполняется в фоновом режиме: отображается индикатор прогресса со счётчиком и кнопка Отменить задачу, а списки блокируются до завершения операции

Доступные устройства к подключению

На данной вкладке отображаются устройства, к которым возможно подключиться, а также указаны соответствующие разрешения и права



Для удобства предусмотрена функция поиска устройств, к которым существует возможность подключения

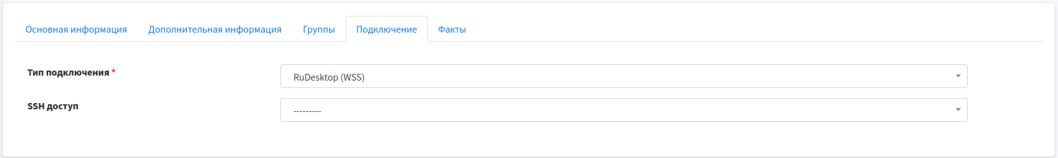
При нажатии на имя доступа открывается список доступных устройств

Подсказка

При нажатии на имя конкретного устройства произойдет переход на страницу его свойств

Подключение

Доступные поля во вкладке Подключение:



На данной вкладке можно настроить тип подключения

Для настройки подключения к устройству средствами клиентского приложения RuDesktop необходимо указать:

В поле Тип подключения выбрать пункт **«RuDesktop (WSS)»**

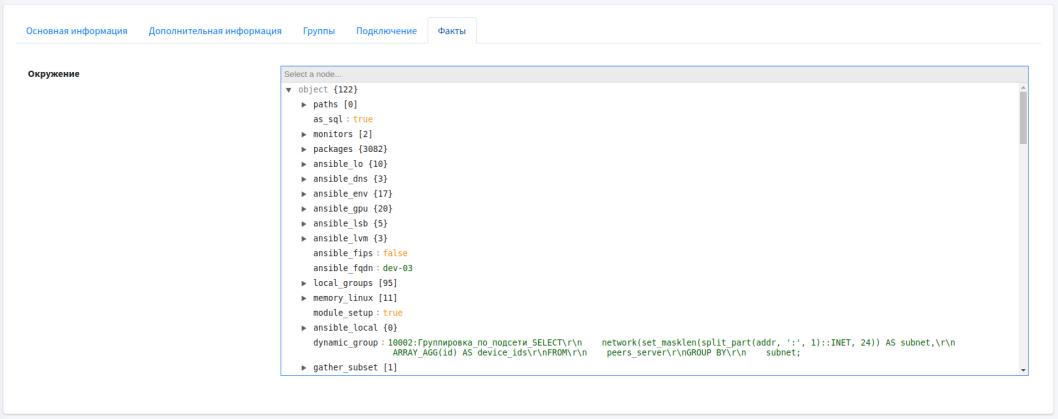
Факты

Важно

Вкладка доступна с правом **Инвентаризация → Просмотр**, если у устройства есть собранные факты

Данные отображаются через JSONEditor в режиме просмотра, в том числе без права изменения устройства

Доступные поля во вкладке Факты:



На данной вкладке отображаются факты об устройстве, собранные при выполнении политики *Инвентаризация*, которые в дальнейшем будут использоваться при формировании отчетов

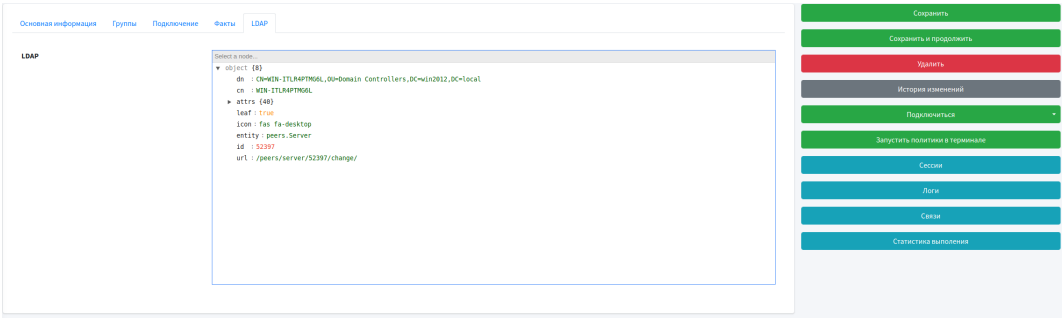
LDAP

Важно

Вкладка доступна с правом **Домены → Просмотр**, если у устройства заполнен DN - путь к объекту в каталоге

Данные отображаются через JSONEditor в режиме просмотра, в том числе без права изменения устройства

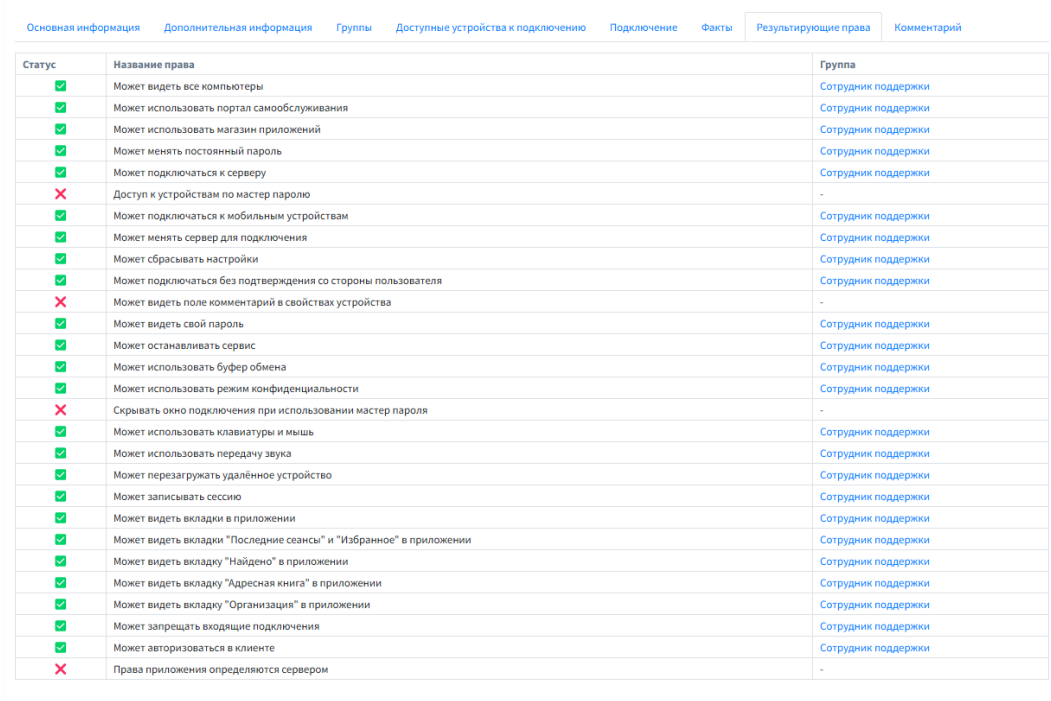
Доступные поля во вкладке LDAP:



На данной вкладке отображаются факты о домене, собранные после выполнения синхронизации с доменом

Результирующие права

На этой вкладке отображены доступные для данного устройства права



Статус	Название права	Группа
✓	Может видеть все компьютеры	Сотрудник поддержки
✓	Может использовать портал самообслуживания	Сотрудник поддержки
✓	Может использовать магазин приложений	Сотрудник поддержки
✓	Может менять постоянный пароль	Сотрудник поддержки
✓	Может подключаться к серверу	Сотрудник поддержки
✗	Доступ к устройствам по мастер паролю	-
✓	Может подключаться к мобильным устройствам	Сотрудник поддержки
✓	Может менять сервер для подключения	Сотрудник поддержки
✓	Может сбрасывать настройки	Сотрудник поддержки
✓	Может подключаться без подтверждения со стороны пользователя	Сотрудник поддержки
✗	Может видеть поле комментарий в свойствах устройства	-
✓	Может видеть свой пароль	Сотрудник поддержки
✓	Может останавливать сервис	Сотрудник поддержки
✓	Может использовать буфер обмена	Сотрудник поддержки
✓	Может использовать режим конфиденциальности	Сотрудник поддержки
✗	Скрывать окно подключения при использовании мастер пароля	-
✓	Может использовать клавиатуры и мышь	Сотрудник поддержки
✓	Может использовать передачу звука	Сотрудник поддержки
✓	Может перезагружать удалённое устройство	Сотрудник поддержки
✓	Может записывать сессию	Сотрудник поддержки
✓	Может видеть вкладки в приложении	Сотрудник поддержки
✓	Может видеть вкладки "Последние сеансы" и "Избранное" в приложении	Сотрудник поддержки
✓	Может видеть вкладку "Найдено" в приложении	Сотрудник поддержки
✓	Может видеть вкладку "Адресная книга" в приложении	Сотрудник поддержки
✓	Может видеть вкладку "Организация" в приложении	Сотрудник поддержки
✓	Может запрещать входящие подключения	Сотрудник поддержки
✓	Может авторизоваться в клиенте	Сотрудник поддержки
✗	Права приложения определяются сервером	-

В таблице отображаются статус права, название права и группа, из которой доступно это право

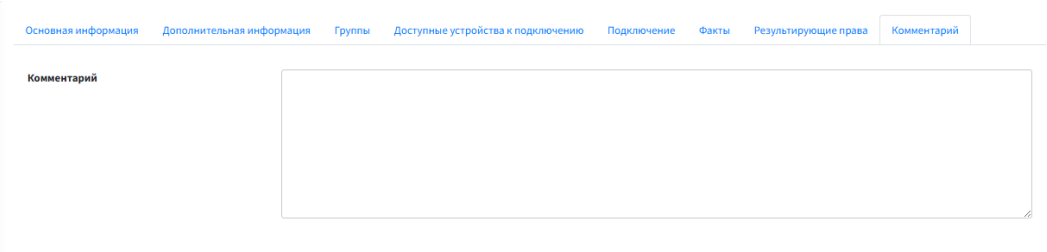
Важно

Права могут предоставляться несколькими группами, поэтому в колонке **«Группы»** могут отображаться две и более группы в зависимости от источников этого права

При нажатии на имя группы произойдет переход на страницу свойств данной группы

Комментарий

Доступные поля во вкладке Комментарий:



На данной вкладке можно указать комментарий к устройству

Важно

Чтобы вкладка была доступна, пользователю необходимо активировать право **«Может видеть поле комментарий в свойствах устройства»**

Логи

На этой вкладке отображены логи клиента **RuDesktop**, полученные с удаленного устройства

- **Может просматривать логи в свойствах устройства** - открывает вкладку и разрешает скачивание уже собранных логов
- **Может управлять логами устройства (загрузка и удаление)** - дополнительно разрешает загрузку логов с устройства, удаление выбранных файлов и удаление всех логов

  Без этого права кнопки управления и флажки выбора файлов скрыты

Операции доступны только для устройств, к которым у пользователя есть доступ

Сбор, скачивание и удаление логов недоступны в облачной версии

В таблице отображаются логи клиента **RuDesktop**, включая дату и время их получения

История входов

Вкладка доступна только суперпользователю

Показывает последние 100 событий смены имени пользователя устройства, начиная с самых новых

В таблице указаны дата и время записи события, новое и предыдущее имя пользователя

Новая строка может появиться с задержкой после получения сведений от клиента

Время строки отражает запись события на сервере, а не точное время входа в операционную систему

Если имя пустое, в соответствующем столбце отображается прочерк

Ограничение в 100 строк относится к отображению этой вкладки, а не к общему числу сохранённых событий

Событие создаётся, когда сервер получает от уже известного устройства имя пользователя, отличающееся от сохранённого

Поэтому повторный вход того же пользователя сам по себе не гарантирует новую строку, а первая регистрация устройства не является событием смены

Это история изменений сведений, полученных сервером, а не полный журнал успешных и неуспешных входов в операционную систему

Для проверки смены пользователя:

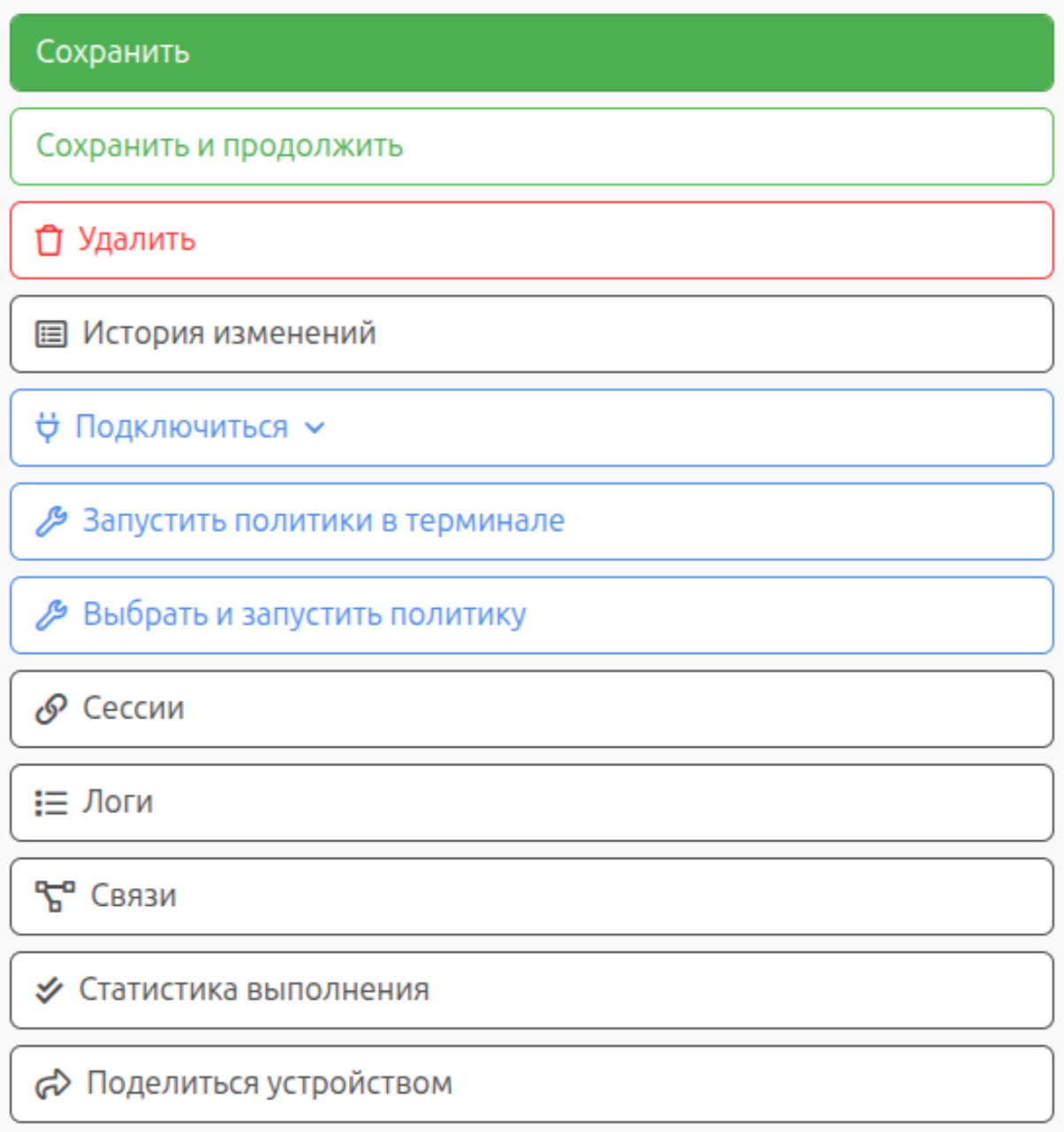
1. Открыть нужное устройство и вкладку **«История входов»**
2. Найти последнюю строку и сравнить новое и предыдущее имена
3. Сопоставить время с ожидаемой сменой пользователя
4. Если ожидаемой записи нет, проверить связь клиента с сервером и обновить страницу после передачи новых сведений

Сообщение **«История входов пуста»** означает отсутствие сохранённых событий этого типа для устройства

Оно не доказывает, что в ОС никто не входил

Меню действий

Меню действий расположено на всех вкладках страницы редактирования



Имеет следующие возможности:

1. Сохранить - производит сохранение внесенных изменений и перенаправляет на страницу *Устройства*
2. Сохранить и продолжить - производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить - производит удаление устройства и всех его связей, перенаправляя на страницу *Устройства*

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления устройства

2. После подтверждения удаления устройства произойдет переход на страницу *Устройства* и появится уведомление Устройство «НАЗВАНИЕ_УСТРОЙСТВА» был успешно удален

4. История изменений - отображает все изменения, выполненные для этого устройства
5. Подключиться - позволяет подключиться к рабочему столу, файловой системе, настроить TCP-туннелирование и выполнить подключение к терминалу удаленного устройства

Важно

Для успешного подключения клиент **RuDesktop** должен быть установлен как на устройстве, с которого выполняется подключение, так и на устройстве, к которому производится подключение

Внимание

При выборе типа подключения браузер запросит разрешение на запуск клиентского приложения, и эту возможность необходимо предоставить

6. Запустить политики в терминале - при выборе этого пункта произойдет запуск политик, предназначенных для данного устройства
7. Выбрать и запустить политику - при выборе этого пункта откроется окно с возможностью выбора политики, после чего её можно будет выполнить на данном устройстве
8. Сессии - отображает сессии, которые были запущены на этом устройстве
9. Логи - отображает логи выполнения задач и политик, запущенных для этого устройства
10. Связи - графически отображает входящие и исходящие соединения
11. Статистика выполнения - открывает страницу *Статистика выполнения* с отображением статистики выполнения задач на данном устройстве
12. Поделиться устройством - при выборе этого пункта произойдет переход на страницу *создания пригласительной ссылки* с автоматическим выбором этого устройства

Устройства - список подключенных к серверу устройств и подробная информация о каждом из них

Подсказка

Страница **«Устройства»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Важно

1. Пользователь видит только те устройства, к которым он успешно подключился в клиенте под своей учетной записью
2. Руководитель подразделения видит устройства других пользователей, входящие в его подразделение
3. Суперпользователь имеет доступ к просмотру всех устройств, а также пользователь, у которого активно право **«Может видеть все компьютеры»**

Как это работает

Запись об устройстве появляется на сервере **RuDesktop** одним из двух способов:

- **автоматически при подключении клиента** - при первом успешном подключении клиента **RuDesktop** к серверу устройство регистрируется и получает уникальный идентификатор (ID)
- **из домена** - при синхронизации с LDAP записи об устройствах сервер сопоставляет с уже зарегистрированными устройствами по имени хоста и привязывает их к доменным группам

Каждому устройству можно назначить псевдоним, привязать к одной или нескольким *группам* (через них наследуются права доступа), включить в *адресную книгу* для быстрых подключений и поделиться через *пригласительную ссылку*

Видимость устройств определяется правами текущего пользователя - без права **«Может видеть все компьютеры»** пользователь видит только устройства, к которым подключался лично, либо устройства своего подразделения (если активно право **«Руководитель подразделения»**)

Как заполняется столбец «Полное имя»

Столбец Полное имя показывает ФИО **владельца устройства**, а не сетевое имя самого устройства

Значение берётся из доменной учётной записи, к которой устройство привязано. Чтобы в столбце появилось ФИО, нужно выполнить следующие шаги

На стороне Active Directory / LDAP

1. Учётная запись пользователя должна существовать в домене

2. У учётной записи должен быть заполнен атрибут `displayName` (в свойствах AD-пользователя - поле **«Отображаемое имя»**) - именно его **RuDesktop** записывает в поле **«Полное имя»** при синхронизации

На стороне сервера RuDesktop

1. Подключить домен на странице *Домены* и включить его (флаг Включить)
2. Запустить синхронизацию пользователей домена - нажать кнопку Синхронизировать в свойствах домена

   Для регулярного обновления данных можно настроить периодический запуск через политику *Синхронизация со службой каталогов*

   После синхронизации в разделе *Пользователи* появятся учётные записи в формате `<username>@<domain>` с заполненным полем Полное имя

На стороне рабочей станции пользователя

1. Войти в операционную систему под доменной учётной записью (не под локальной)
2. Установить и запустить клиент **RuDesktop**, выполнить подключение к серверу

Что происходит автоматически

При подключении клиента сервер сравнивает имя пользователя ОС и домен с уже синхронизированными учётными записями (по логину `<username>@<domain>`) и автоматически связывает устройство с найденным пользователем

После этого в столбце Полное имя отображается ФИО владельца

Примечание

Если устройство впервые подключилось к серверу до того, как пользователь был синхронизирован из домена, связь может не установиться автоматически

В этом случае администратор может выполнить пакетную привязку командой *rude ldap link* - она пройдёт по всем устройствам и привяжет их к доменным пользователям с совпадающим логином

Важно

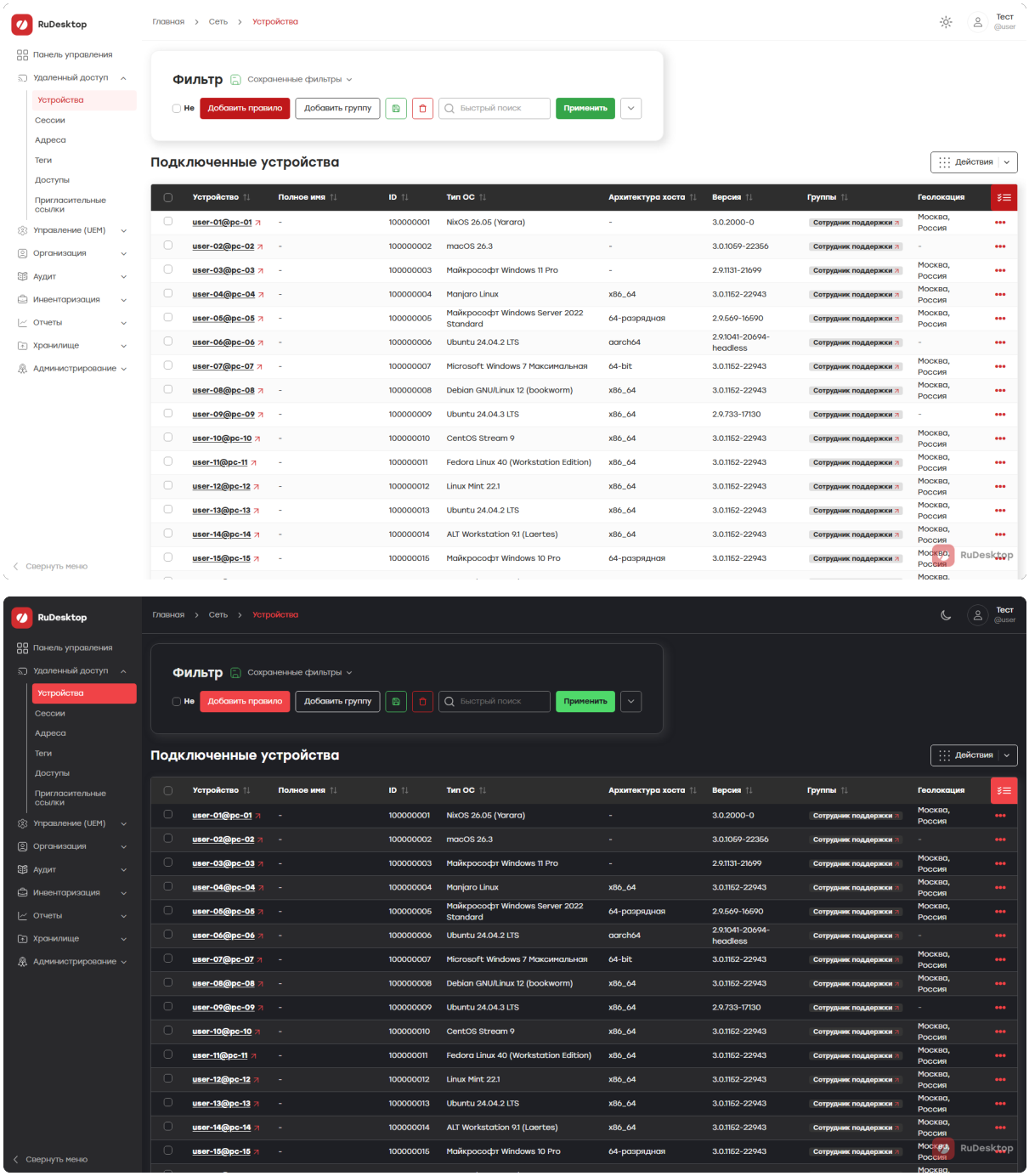
Столбец Полное имя останется пустым, если:

- на устройстве выполнен вход под **локальной** учётной записью ОС (нет доменной части)
- доменная часть, сообщённая клиентом, не совпадает с доменной частью логина пользователя в **RuDesktop**
- у пользователя в Active Directory не заполнен атрибут `displayName`

- домен не подключён к **RuDesktop** или не была выполнена синхронизация

Описание страницы

На странице **«Устройства»** отображено:



1. Меню Действия с операциями над страницей целиком: создание динамической группы из фильтра
2. Фильтр
3. Массовые действия

4. Таблица с возможностью настройки отображаемых столбцов

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. Версия - фильтрация устройств по версии клиента
2. Домен - фильтрация устройств по вхождениям в домены
3. Геолокация - фильтрация устройств по определённой геопозиции
4. Право - фильтрация устройств по назначенному праву доступа через группы
5. Название службы — отбор устройств, на которых обнаружена указанная служба
6. Статус службы — отбор устройств по состоянию обнаруженных служб, например **«Работает»** или **«Остановлена»**
7. Поле поиска - поиск по ключевому слову

> **Подсказка**
>
> Поиск по ключевому слову осуществляется по имени пользователя, имени хоста устройства (hostname), идентификатору (ID), типу операционной системы и её версии

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

> **Примечание**
>
> Фильтры служб доступны при наличии права **Инвентаризация → Просмотр**.
>
> Отбор использует сохранённые сведения инвентаризации. После изменения состояния службы выполнить инвентаризацию, чтобы обновить сведения

> **Подсказка**
>
> Чтобы найти устройства, где определённая служба остановлена, добавить в одну группу с объединением **И** два условия:
>
> - **Название службы** — выбрать точное имя службы из списка
> - **Статус службы** — выбрать **«Остановлена»**
>
> Оба условия проверяются для одной и той же службы, присутствующей на устройстве по сохранённым сведениям

При вводе списка чисел в фильтре подтверждайте каждое значение клавишей **Enter**. Для дробного числа можно использовать точку или запятую. Если появилось сообщение **«Некорректное значение»**, исправьте ввод — это число ещё не добавлено в список

Фильтр «В диапазоне». Если для поля выбран оператор В диапазоне, заполните обе границы диапазона

Важно

Если одна из границ не заполнена, это условие фильтра не применяется Пустая граница не означает отсутствие ограничения с одной стороны: в таблице может оказаться больше устройств, чем ожидалось

Перед массовыми действиями проверьте обе границы и получившийся список устройств

Создание динамической группы из фильтра

Настроенный на странице фильтр можно сохранить как *динамическую группу* типа **«Группа из фильтра»**, не переходя на страницу динамических групп и не описывая условия заново

Подсказка

Страница **«Динамические группы»**, на которой созданная группа доступна для просмотра и редактирования, открывается только при использовании локального сервера **Управление конфигурациями (UEM)**

Это удобно, когда выборка устройств нужна регулярно: например, «все устройства с определённой версией клиента» или «все устройства выбранного домена». Сам фильтр тоже можно сохранить - кнопкой Сохранить фильтр, но сохранённый фильтр остаётся личной настройкой пользователя и служит для повторного применения на этой странице и настройки *автоматического добавления устройств в адресную книгу*

Динамическая группа - это объект сервера: её состав хранится отдельно, она видна всем, у кого есть доступ к динамическим группам, и её можно указывать в области действия *задач* и в *доступах*. Для создания группы из фильтра пользователю нужно право **Динамические группы → Создание**. Чтобы создать группу:

1. Настроить фильтр так, чтобы в таблице остались нужные устройства
2. Открыть меню Действия в шапке страницы
3. Выбрать пункт Создать динамическую группу на основе фильтра
4. В открывшемся окне **«Создать динамическую группу»** ввести название группы
5. Нажать на кнопку Создать

   Можно отменить данную операцию, нажав на кнопку Отмена

6. Появится уведомление о создании группы со ссылкой Перейти к группе - по ней открываются свойства созданной динамической группы

Созданная группа получает тип **«Группа из фильтра»**, а условия текущего фильтра сохраняются в её выражении. Одновременно создаётся одноимённая **загруженная динамическая группа**, в которую сразу попадают устройства, подходящие под эти условия - именно загруженные группы указываются в области действия задач и в доступах

Важно

1. Действие доступно при наличии права **Группы → Изменение**
2. Название группы должно быть уникальным среди динамических групп (без учёта регистра) и не может быть пустым - иначе в окне появится сообщение об ошибке
3. В группу попадают **только условия фильтра**

   Значение, введённое в Поле поиска, в выражение группы не переносится - если выборка получена поиском по ключевому слову, её нужно повторить условиями фильтра
4. Если фильтр не задан, условия окажутся пустыми и в группу попадут **все устройства**
5. Состав группы формируется по всем устройствам сервера, а не только по видимым текущему пользователю - в неё могут попасть устройства, которых пользователь не видит на странице

Примечание

В дальнейшем состав группы пересчитывается по общим правилам динамических групп - во время инвентаризации устройств

Подробнее об этом и о работе с выражением см. на странице *Динамические группы*

Массовые действия

Массовые действия позволяют выполнить одну и ту же операцию сразу над несколькими устройствами, не открывая свойства каждого из них

Панель массовых действий появляется под таблицей, как только отмечено хотя бы одно устройство. Общий порядок работы одинаков для всех действий:

1. Отметить необходимые устройства в таблице
2. Выбрать действие в списке Действия с выбранными объектами
3. Заполнить дополнительные поля, если действие их запрашивает (тип подключения, формат файла) - пока обязательное поле не заполнено, кнопка Выполнить неактивна
4. Нажать на кнопку Выполнить

Часть действий выполняется сразу, часть - открывает промежуточную страницу с подтверждением или окно с выбором параметров

Важно

В панели есть кнопка Выбрать все

Она распространяет действие на **всю текущую выборку** - на все устройства, отобранные фильтром и поиском, а не только на отмеченные на текущей странице

Рядом с кнопкой отображается счётчик: Выбрано N из M или Выбраны все объекты

Сбросить выбор можно кнопкой Снять выделение

Примечание

Массовое действие всегда работает только с теми устройствами, которые видны текущему пользователю

Кнопка Выбрать все выбирает все устройства из его видимой выборки, а не все устройства сервера - правила видимости описаны в начале страницы

Что делает каждое действие:

Действие	Что делает
Удалить выбранные устройства	Удаляет записи об устройствах с сервера вместе со связанными записями (группы, адреса в адресных книгах, подключения, инвентарные данные) Перед удалением открывается страница подтверждения со списком связанных объектов
Изменить группы	Добавляет выбранные группы к текущим, заменяет ими текущий набор или убирает их у устройств - в зависимости от выбранного режима
Скопировать в адресную книгу выбранные компьютеры	Добавляет выбранные устройства в личную *адресную книгу* пользователя, авторизованного на сервере Устройства, которые уже есть в книге, повторно не добавляются
Выбрать и запустить политику	Запускает выбранную *политику* на всех отмеченных устройствах и показывает ход выполнения в окне с логами

продолжается на следующей странице

Таблица 1 – продолжение с предыдущей страницы

Действие	Что делает
Загрузить логи для выбранных устройств	Ставит в очередь фоновый сбор логов клиента **RuDesktop** с выбранных устройств
Экспортировать выбранные устройства	Выгружает данные выбранных устройств в файл В файл попадают столбцы, включённые в таблице на момент экспорта

Важно

1. Массовые действия доступны только при наличии права **Устройства → Изменение** - без него список действий пуст
2. Действие Удалить выбранные устройства дополнительно требует права **Устройства → Удаление**
3. Действие Выбрать и запустить политику дополнительно требует права *Может запускать политики*
4. Действие Экспортировать выбранные устройства дополнительно требует права *Может экспортировать данные*
5. Действие Загрузить логи для выбранных устройств требует права **Может управлять логами устройства (загрузка и удаление)** и отсутствует в облачной версии **RuDesktop**
6. В зависимости от прав отдельные действия могут отсутствовать

Удаление устройств

Действие удаляет записи об устройствах с сервера **RuDesktop** вместе со связанными записями: снимается членство в группах, удаляются *адреса* этих устройств во всех адресных книгах, записи о подключениях и *сессиях*, история геолокации и собранные инвентарные данные

Примечание

Записи на странице *Логи исполнения* при этом сохраняются - у них лишь снимается привязка к удалённому устройству

Для массового удаления устройств необходимо:

1. Отметить необходимые устройства в таблице
2. Выбрать действие Удалить выбранные устройства
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие устройства будут удалены, и их связи

5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору

6. Выбранные устройства будут удалены

Важно

Вид страницы подтверждения и способ удаления зависят от количества выбранных устройств:

- **до 100 устройств включительно** - на странице подтверждения перечисляются сами устройства и связанные с ними записи

  Удаление выполняется сразу, и после подтверждения устройства пропадают из таблицы

- **более 100 устройств** - на странице подтверждения отображается только количество удаляемых записей, без перечисления связей

  Само удаление ставится в очередь и выполняется в фоне: появляется сообщение вида **«Удаление N устройств в процессе...»**, а записи исчезают из таблицы не сразу

  Ход выполнения можно отследить на странице *Очередь задач* по задаче **«Удаление данных»**

Важно

Удаление записи не удаляет клиент **RuDesktop** с самого устройства

Если клиент продолжит работу, при следующем подключении к серверу устройство появится в списке снова - уже как новая запись, без прежних групп, псевдонима и других настроек

Новая запись попадёт в группу, указанную в настройке *Группа по умолчанию для новых компьютеров*

Изменение групп устройств

Действие **«Изменить группы»** меняет членство выбранных устройств в обычных группах RuDesktop. Группы используются при определении *прав доступа* и выборе устройств для задач

1. Открыть **«Удалённый доступ → Устройства»** и отфильтровать нужные устройства
2. Отметить устройства, выбрать массовое действие **«Изменить группы»** и нажать **«Выполнить»**
3. На открывшейся странице проверить список устройств и столбец **«Текущие группы»**
4. В блоке **«Выберите действие»** выбрать режим по таблице ниже

5. Найти и отметить хотя бы одну группу
6. Проверить режим и выбор, затем нажать **«Изменить группы»**
7. Вернуться к устройствам и проверить столбец **«Группы»** или вкладку **«Группы»** в карточке одного из устройств

Режим	Что произойдёт	Пример
Добавить	Сохранит текущие группы и добавит выбранные	Было «Офис», выбрано «Обновления» - останутся обе группы
Назначить	Полностью заменит текущие группы выбранным набором	Было «Офис», выбрано «Обновления» - останется только «Обновления»
Удалить	Уберёт выбранные группы у устройств, остальные сохранит	Было «Офис» и «Обновления», выбрано «Обновления» - останется «Офис»

По умолчанию выбран режим **«Добавить»**. При удалении доступны группы, в которых состоит хотя бы одно из выбранных устройств. Если конкретное устройство в выбранную группу не входит, остальные его группы сохранятся. Удаление членства не удаляет саму группу или устройство

Важно

Режим **«Назначить»** заменяет весь набор групп у каждого выбранного устройства

Для добавления одной группы с сохранением индивидуальных наборов использовать **«Добавить»**

Подсказка

Список групп подгружается при прокрутке. Кнопка **«Выбрать все в загруженном списке»** отмечает только загруженные группы. Для поиска конкретной группы использовать поиск по имени

Примечание

Пустой выбор групп не очищает членство - форма сообщает **«Не выбраны группы»**. Чтобы убрать все группы, выбрать **«Удалить»** и отметить нужные текущие группы

Для выхода без применения использовать **«Нет, вернуться обратно»**

Права и ограничения

- Для отображения списка групп нужно право **«Группы → Просмотр»**
- Изменение членства может изменить доступ пользователей к устройствам После операции проверить доступ для затронутых групп пользователей
- Состав динамических групп определяется их правилами и этим действием не меняется
- При последующей синхронизации устройства со службой каталогов членство может быть заново сформировано по данным домена

Например, чтобы включить компьютеры нескольких отделов в группу для обновления, отобрать эти компьютеры и применить **«Добавить»** с группой **«Обновления»**. Отделы у каждого компьютера сохранятся. После завершения работ применить **«Удалить»** только к группе **«Обновления»**

Пошаговый пример: Временная группа устройств без изменения групп отделов

Копирование устройств в адресные книги

Действие добавляет выбранные устройства в одну или несколько *адресных книг*. Можно выбрать свою личную книгу и другие книги, доступные на запись; суперпользователю также доступны личные книги других пользователей.

1. Отметить необходимые устройства в таблице.
2. Выбрать `Скопировать в адресную книгу выбранные компьютеры` и нажать `Выполнить`.
3. На открывшейся странице проверить список устройств и отметить книги-получатели. Для поиска книги можно использовать строку поиска.
4. Проверить выбор и сводку количества записей и пользователей перед подтверждением.
5. Нажать `Скопировать`.

Кнопки `Выбрать все` и `Отменить выбор` действуют на книги, которые видны с учётом поиска. Ранее отмеченные книги, скрытые поиском, сохраняют выбор — перед подтверждением очистить поиск и проверить полный список.

Результат выводится отдельно для каждой книги: сколько устройств добавлено и сколько уже было в ней.

Если нужно перенести также псевдонимы, комментарии и теги из существующей книги, использовать *копирование со страницы Адреса*. Копирование со страницы `Устройства` создаёт новые адреса без этих данных.

Примечание

Если устройство уже есть в книге, повторная запись не создаётся, а существующие данные адреса сохраняются. Новые записи создаются без псевдонима; заполнить его можно на странице *Адреса*.

Операция записывается в *журнал аудита* событием `Добавление в адресную книгу` для каждой выбранной книги.

Запуск политики

Действие однократно запускает выбранную *политику* на всех отмеченных устройствах - без создания *задачи* и расписания

Для массового запуска политики необходимо:

1. Отметить необходимые устройства в таблице
2. Выбрать действие Выбрать и запустить политику
3. Нажать на кнопку Выполнить
4. Откроется окно **«Выберите политику»** - выбрать необходимую политику из списка
5. Нажать на кнопку Запустить в терминале
6. Откроется окно с отображением логов, в котором виден ход выполнения политики

Примечание

Результат выполнения по каждому устройству также сохраняется на странице *Логи исполнения*

Загрузка логов с устройств

Действие запрашивает у клиентов **RuDesktop** их локальные логи и загружает их на сервер

Сбор выполняется в фоне: сервер по очереди обращается к каждому выбранному устройству, упаковывает полученные логи в архив и сохраняет его в свойствах устройства. Для массовой загрузки логов с устройств необходимо:

1. Отметить необходимые устройства в таблице
2. Выбрать действие Загрузить логи для выбранных устройств
3. Нажать на кнопку Выполнить

4. Будет запущен фоновый сбор логов с выбранных устройств - после завершения логи будут доступны в свойствах каждого устройства во вкладке *Логи*

Важно

1. Логи собираются только с устройств, доступных на момент выполнения

   Если устройство офлайн или не отвечает, логи с него не собираются: повторных попыток и отложенной передачи при следующем подключении не предусмотрено - действие нужно запустить заново

2. Сообщение о запуске появляется сразу и не отражает результат сбора

   Отчёт по каждому устройству в интерфейсе не выводится - проверить, откуда логи получены, можно во вкладке **«Логи»** свойств устройства

3. Действие требует права **Может управлять логами устройства (загрузка и удаление)** и отсутствует в облачной версии **RuDesktop**

Экспорт устройств

Действие выгружает данные выбранных устройств в файл - например, для инвентарного отчёта или передачи списка устройств в другую систему

Примечание

Выгружаются те столбцы, которые включены в таблице на момент экспорта

Чтобы получить в файле дополнительные данные (MAC-адрес, IPv4-адреса, мониторы и другие), нужно предварительно включить соответствующие столбцы в настройке отображения таблицы

Для массового экспорта устройств необходимо:

1. Отметить необходимые устройства в таблице
2. Выбрать действие Экспортировать выбранные устройства
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Примечание

Доступные форматы выгрузки: **CSV**, **XLS**, **XLSX**, **TSV**, **ODS**, **JSON**, **YAML**, **HTML**

Набор форматов зависит от компонентов, установленных на сервере, поэтому отдельные пункты могут отсутствовать

Важно

1. Если выбрано более 1000 устройств, экспорт выполняется в фоне: файл не скачивается сразу, а сохраняется на сервере в репозитории **Отчеты** и становится доступен на странице *Файлы*

   Ход выполнения виден на странице *Очередь задач* по задаче **«Экспорт»**

2. Формат **XLS** не поддерживает ячейки с текстом длиннее 32767 символов

   Если в выгрузке есть такие значения (например, длинный список фактов инвентаризации), экспорт завершится ошибкой с предложением выбрать другой формат - в этом случае подойдёт **XLSX** или **CSV**

Таблица

Таблица разбита по столбцам:

1. Устройство - имя устройства, отображается по маске **имя_пользователя@hostname**
2. Пользователь - имя пользователя операционной системы, под которым ведётся работа на устройстве (System Account)
3. Полное имя - полное имя (ФИО) владельца устройства

   Заполняется при привязке устройства к доменному пользователю - подробнее см. раздел *Как заполняется столбец «Полное имя»* выше
4. Имя хоста - имя хоста устройства (hostname)
5. Псевдоним - имя, заданное в свойствах устройства для удобного поиска и идентификации
6. ID - идентификатор устройства, который отображается в окне клиентского приложения и присваивается при подключении устройства к серверу
7. Тип соединения - тип соединения с устройством, **RuDesktop (WSS)**
8. Тип ОС - операционная система, установленная на устройстве
9. Архитектура хоста - архитектура процессора устройства (x86_64, arm64 и т.п.)
10. Версия - версия установленного клиента RuDesktop
11. Группы - группы, в которые входит устройство
12. Путь до объекта в LDAP - DN устройства в каталоге LDAP/Active Directory, заполняется при синхронизации с доменом
13. Подразделение в домене - подразделения (OU) каталога, в которых находится устройство, от корня домена, например **Филиал №1/Отдел ИТ**. Заполняется при синхронизации с доменом; у устройств вне подразделений поле пустое
14. Геолокация - геолокация устройства

15. Создан - дата и время первого подключения устройства к серверу
16. Обновлен - дата и время последнего ответа от устройства
17. Текущее время - текущее время на устройстве с учётом часового пояса
18. IPv4-адреса - список IPv4-адресов устройства
19. MAC-адрес - отображение MAC-адреса устройства
20. Мониторы - информация о подключённых мониторах
21. SN-устройства/UUID - первое доступное значение: серийный номер материнской платы, серийный номер устройства или UUID устройства. Пустые и служебные значения производителя игнорируются; при отсутствии данных отображается прочерк
22. Дата последней инвентаризации - дата последнего успешного выполнения политики инвентаризации на устройстве

Нажатие на заголовок сортируемого столбца меняет порядок записей

Примечание

- Выбранная сортировка восстанавливается при повторном открытии списка
- Настройки сохраняются отдельно для разных таблиц в текущем браузере
- В другом браузере сортировку нужно выбрать заново

Также в таблице можно удалять и добавлять столбцы

Важно

По умолчанию отключены столбцы **Пользователь**, **Имя хоста**, **Псевдоним**, **Тип соединения**, **Путь до объекта в LDAP**, **Подразделение в домене**, **Создан**, **Обновлен**, **Текущее время**, **IPv4-адреса**, **MAC-адрес**, **Мониторы**, **SN-устройства/UUID** и **Дата последней инвентаризации**

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

- Редактировать - при выборе этого пункта откроются свойства устройства
- Удалить - при выборе этого пункта устройство будет удалено и его связи
- История изменений - при выборе этого пункта будет отображена история устройства: создание/редактирование и пользователь, который выполнил данные операции

- Подключиться - при наведении курсора на данный пункт откроется контекстное меню с вариантами подключения:
  - Рабочий стол - выполнить подключение к рабочему столу удаленного устройства
  - Передача файлов - выполнить подключение к файловой системе удаленного устройства
  - TCP-туннелирование - настройка TCP-туннелирования
  - RDP - выполнить подключение через Remote Desktop Protocol (протокол удалённого рабочего стола)
  - Разбудить (Wake On LAN) - выполнить пробуждение устройства через WOL

    Важно

    1. Для того чтобы разбудить устройство, необходимо хотя бы один раз подключиться к удалённому устройству
    2. Устройство должно находиться в той же подсети, что и устройство, с которого производится попытка пробуждения

  - Подключиться к терминалу - выполнить подключение к терминалу удаленного устройства

    Важно

    Для того чтобы подключение прошло успешно, на устройстве, с которого происходит подключение, и на устройстве, на которое происходит подключение, должен быть установлен клиент RuDesktop

  - Проброс USB - выполнить проброс USB-устройств с локального компьютера на удалённое устройство
  - Системный монитор - открыть в клиенте список процессов удалённого компьютера
- Запустить политики в терминале - при выборе этого пункта произойдет запуск политик, предназначенных для данного устройства
- Выбрать и запустить политику - при выборе этого пункта откроется окно с возможностью выбора политики, после чего её можно будет выполнить на данном устройстве
- Сессии - при выборе этого пункта произойдет переход на страницу *Сессии* с активным фильтром по этому устройству
- Логи - при выборе этого пункта произойдет переход на страницу *Логи исполнения* с активным фильтром по этому устройству

- Связи - при выборе этого пункта произойдет переход на страницу *Граф*, где будет графически отображены входящие и исходящие соединения пользователя
- Статистика выполнения - при выборе этого пункта произойдет переход на страницу *Статистика выполнения* с отображением статистики выполнения задач на данном устройстве
- Поделиться устройством - при выборе этого пункта произойдет переход на страницу *создания пригласительной ссылки* с автоматическим выбором этого устройства
- История геолокации - при выборе этого пункта произойдет переход на страницу с историей геолокации устройства

  Пункт доступен при наличии права `Может видеть карту`
- Чёрный список - при выборе этого пункта произойдет переход на страницу *Чёрный список* с активным фильтром по этому устройству

  Пункт доступен при наличии права на просмотр чёрного списка

Свойства устройства

Подробнее о *свойствах устройства*

Массовые действия с фильтром

Чтобы выполнить действие для всех устройств, подходящих под условие:

1. Настроить фильтр и при необходимости строку поиска
2. Проверить состав результатов
3. Отметить устройство, чтобы открыть панель массовых действий
4. Нажать **«Выбрать все»**, если действие нужно для всей найденной выборки, включая другие страницы
5. Выбрать действие, заполнить его параметры и нажать **«Выполнить»**

Примечание

Выбор всех объектов учитывает текущие фильтр и поиск

Устройства, не подходящие под эти условия, в массовое действие не включаются

Если нужно обработать только несколько устройств, отметить их по отдельности без **«Выбрать все»**. После изменения условий фильтра проверить выбор заново перед выполнением действия

2.6.2 Сессии

Сессии — сеанс подключения. В таблице на данной странице отображаются как активные, так и неактивные сессии

Подсказка

Страница **«Сессии»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Важно

1. Пользователь видит только свои сессии
2. Владелец подразделения имеет доступ к просмотру всех сессий пользователей, входящих в его подразделение
3. Суперпользователь имеет доступ к просмотру всех сессий, а также пользователь, у которого активно право **«Может видеть все сессии»**

Как это работает

Запись о сессии создаётся сервером **RuDesktop** в момент установки подключения и обновляется в реальном времени до его завершения. На странице видны как активные сессии (статус **Онлайн**), так и завершённые (**Офлайн**) — они различаются по полю **«Окончание»**

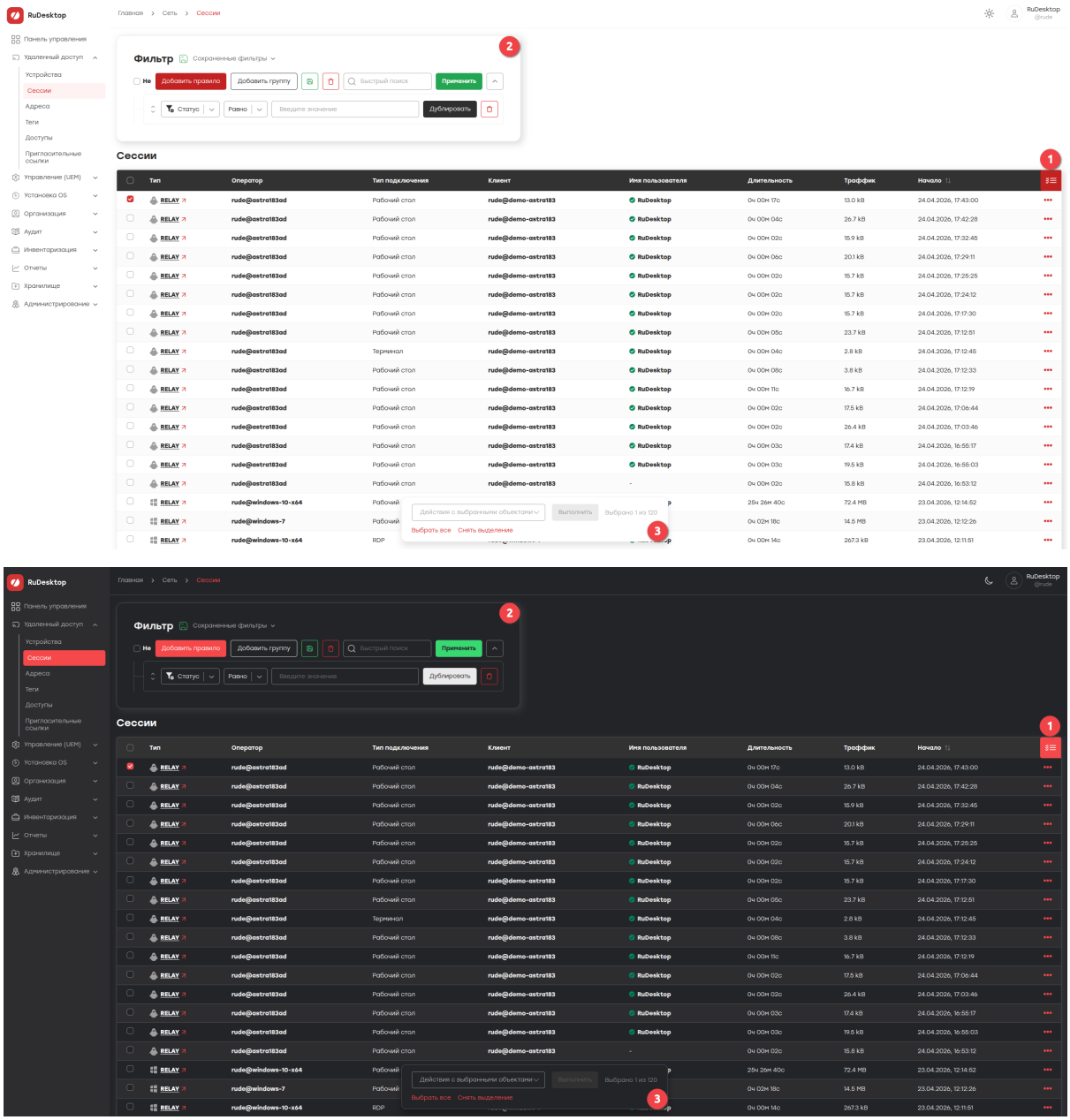
В сессии фиксируются:

- **тип соединения** — `LOCAL` (P2P в локальной сети), `NAT` (через преобразование адресов) или `RELAY` (через *мост*)
- **тип подключения** — Рабочий стол, Передача файлов, Терминал, RDP, TCP-туннелирование, Проброс USB
- **оператор и клиент** — устройство, инициировавшее подключение, и устройство, к которому подключались
- **трафик и длительность** — итоговый объём и время сессии
- **видеозаписи и записи передачи файлов** — при включённом мониторинге для группы устройств (см. *Группы*, вкладка **Мониторинг**)

Сессии, требующие принудительной записи, всегда проходят через `RELAY` (мост) — это нужно для перехвата трафика и формирования файлов записи. Активную сессию можно завершить вручную действием Прервать сессию (кроме типов **RDP** и **TCP**) — для этого пользователю нужно право **«Может прерывать сессии»**

Описание страницы

На странице **«Сессии»** отображено:



1. Фильтр
2. Массовые действия
3. Таблица с возможностью настройки отображаемых столбцов

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. `Статус` — фильтрация сессий по статусу: **Подключение**, **Активная**, **Завершена** или **Ошибка**

2. Тип подключения — фильтрация сессий по типу подключения: **Рабочий стол**, **Передача файлов**, **TCP-туннелирование**, **RDP**, **Терминал**, **Проброс USB**
3. Поле поиска — поиск по ключевому слову

> **Подсказка**
>
> Поиск осуществляется по идентификатору, hostname, имени пользователя и адресу как оператора, так и клиента, статусу сессии и связанному с ней пользователю **RuDesktop**

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные сессии — удаляет выбранные записи из таблицы
2. Экспортировать выбранные сессии — позволяет экспортировать в файл выбранные сессии

> **Примечание**
>
> После выбора данного действия нужно выбрать необходимый формат файла

> **Важно**
>
> В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление сессий

Для массового удаления сессий необходимо:

1. Отметить необходимые сессии в таблице
2. Выбрать действие Удалить выбранные сессии
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие сессии будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору

6. Выбранные сессии будут удалены

Экспорт сессий

Для массового экспорта сессий необходимо:

1. Отметить необходимые сессии в таблице
2. Выбрать действие Экспортировать выбранные сессии
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Тип` — тип соединения с устройством: LOCAL, NAT, RELAY
2. `Тип подключения` — тип подключения с устройством: Рабочий стол, Передача файлов, Терминал, RDP, TCP-туннелирование, Проброс USB
3. `Оператор` — имя устройства оператора, отображается по маске **имя_пользователя@hostname**
4. `Клиент` — имя устройства клиента, отображается по маске **имя_пользователя@hostname**
5. `Имя пользователя` — имя пользователя в системе RuDesktop, который инициировал подключение

> **Важно**
>
> Имя пользователя отображается только, когда выполнена авторизация в клиенте под пользователем

6. `Адрес оператора` — имя адреса оператора
7. `Адрес клиента` — имя адреса клиента
8. `Длительность` — длительность сессии (подключения)
9. `Трафик` — объем затраченного для сессии трафика
10. `Начало` — время начала сессии

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. Редактировать — при выборе этого пункта откроются свойства сессии
2. Удалить — при выборе этого пункта сессия будет удалена

3. История изменений — при выборе этого пункта будет отображена история сессии: создание/редактирование и пользователь, который выполнил данные операции
4. Подключиться — открывает клиент **RuDesktop** для подключения к устройству, указанному в поле **Клиент** выбранной сессии

> **Примечание**
>
> - Действие отображается только у незавершенных сессий типа **Рабочий стол**
> - На компьютере оператора должен быть установлен клиент **RuDesktop**, обрабатывающий ссылки `rudesktop://`
> - Для нового подключения требуется обычная авторизация на удаленном устройстве

> **Подсказка**
>
> Если рабочий стол этого устройства уже открыт в вашем клиенте, клиент переключится на его вкладку
>
> Иначе начнется подключение к устройству

5. Прервать сессию — при выборе этого пункта сессия будет прервана

> **Важно**
>
> - Прерывать сессии можно все, кроме **RDP** и **TCP**
> - Это действие доступно пользователям, имеющим право **Может прерывать сессии**

Свойства сессии

Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств сессии

Доступная информация:

Основная информация

1. Тип соединения — тип соединения с устройством: LOCAL, NAT, RELAY
2. Тип подключения — тип подключения с устройством: Рабочий стол, Передача файлов, Терминал, RDP, TCP-туннелирование, Проброс USB
3. Статус — статус сессии
4. Уникальный код — UUID сессии

5. Оператор — имя устройства оператора, отображается по маске **имя_пользователя@hostname**
6. Клиент — имя устройства клиента, отображается по маске **имя_пользователя@hostname**
7. Пользователь — имя пользователя в системе RuDesktop, который инициировал подключение. Поле отображается только при наличии права на просмотр пользователей
8. Начало — время начала сессии
9. Окончание — время завершения сессии
10. Трафик — объем затраченного для сессии трафика
11. Комментарий — поле для указания комментария

Записи сессии

На этой вкладке отображаются видеозаписи сессии, выполненные при удалённом подключении к устройству

Важно

Процесс обработки видеозаписи начинается сразу после открытия свойств конкретной сессии

Вы можете просматривать видеозаписи как в режиме реального времени (Live), так и после завершения сессии

Подсказка

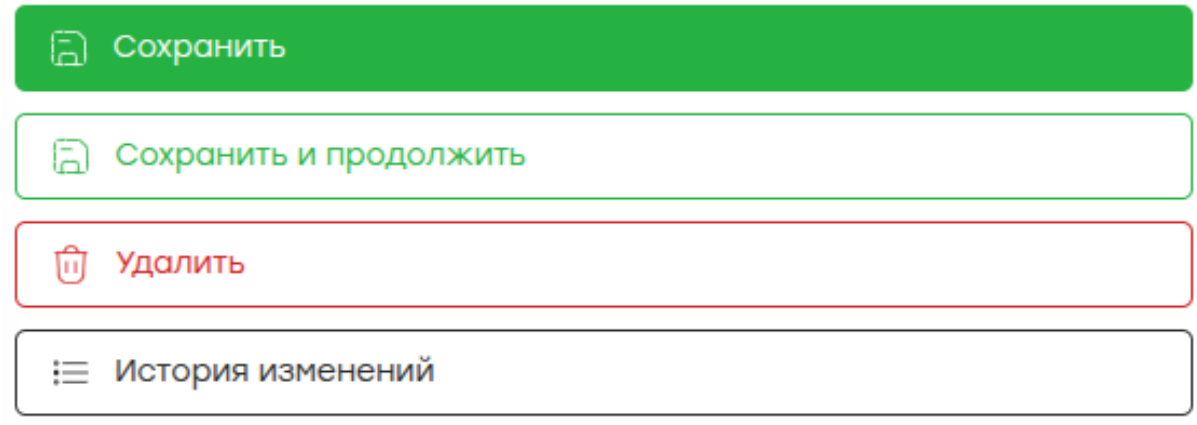
Если обработку видеозаписи остановили в очереди задач, снова откройте запись в свойствах сессии. Обработка начнётся заново, если исходная запись сохранилась

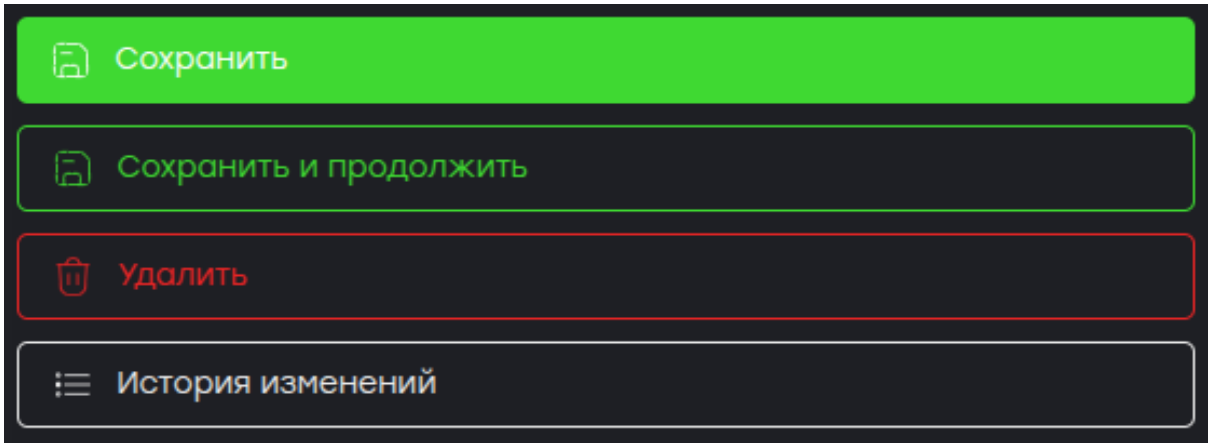
Записи передачи файлов

В этой вкладке отображаются записи действий при передаче файлов в табличном формате

Меню действий

Меню действий расположено на всех вкладках страницы редактирования





Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Сессии»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление сессии и перенаправляет на страницу **«Сессии»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления сессии
2. После подтверждения удаления сессии произойдет переход на страницу **«Сессии»** и появится уведомление Сессия «НАЗВАНИЕ_СЕССИИ» была успешно удалена

4. История изменений — отображает все изменения, выполненные для этой сессии
5. Прервать сессию — производит прерывание сессии

Важно

- Прерывать сессии можно все, кроме **RDP** и **TCP**
- Это действие доступно пользователям, имеющим право **«Может прерывать сессии»**

2.6.3 Адресные книги

Адресные книги — именованные наборы *адресов* и *тегов* с раздельным доступом. Одна и та же страница управляет как личной книгой пользователя, так и общими книгами, к которым выдан доступ отдельным пользователям или группам

Подсказка

Страница **«Адресные книги»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Важно

- Пользователь видит свою личную книгу, общие книги, к которым ему выдан доступ, а также книги, которыми он владеет
- *Руководитель подразделения* дополнительно видит общие книги своего подразделения
- Суперпользователь имеет доступ ко всем адресным книгам

Как это работает

Адресная книга — это контейнер, в котором хранятся записи об устройствах (*адреса*) и *теги* для их классификации. Теги принадлежат книге: один и тот же тег в разных книгах — это разные теги, а удаление или переименование тега затрагивает только его книгу. При удалении тега сами адреса не удаляются — снимается только его привязка к ним

Примечание

Одно устройство может присутствовать в книге только один раз, но одно и то же устройство можно добавить в несколько разных книг

Книги делятся на два типа:

Тип	Описание
Личная	Создаётся автоматически для каждого пользователя в единственном экземпляре при создании учётной записи. Её владельцем всегда является сам пользователь, и она никогда не привязывается к подразделению. Удалить личную книгу может только суперпользователь — остальным пользователям, включая её владельца, удаление недоступно В эту книгу клиент автоматически сохраняет устройства при включенной опции **Сохранять последний сеанс в адресную книгу** С ней также работает команда *rude addressbook*
Общая	Создаётся вручную на странице **«Адресные книги»** (при наличии права **Адресная книга → Создание**) или автоматически для каждого подразделения. Общую книгу можно привязать к подразделению, поделиться ею с пользователями и группами и удалить

Примечание

- В настольном клиенте **RuDesktop** можно переключаться между личной и доступными общими книгами, искать адреса, фильтровать их по тегам и подключаться к устройствам
- При уровне **Изменение** или **Управление** доступны добавление, переименование и удаление адресов и тегов
- Создание общих книг и выдача доступа выполняются в веб-интерфейсе сервера

Подробнее — Адресная книга в клиенте

Автоматическое создание книг

Часть книг создаётся сервером без участия пользователя:

- **личная книга** создаётся при создании учётной записи пользователя. Её название формируется в виде **Личная книга - имя_пользователя** и меняется вслед за именем пользователя. Если название было изменено вручную, оно больше не обновляется автоматически
- **общая книга подразделения** создаётся при создании *подразделения*. Такая книга создаётся с названием **Общая книга — название_подразделения** и без явного владельца; ею управляет *руководитель этого подразделения* (уровень доступа **Управление**)

Примечание

При обновлении сервера до версии с адресными книгами адреса и теги существующих пользователей переносятся в их личные книги, а для пользователей, у которых раньше было право видеть общую адресную книгу подразделения, содержимое собирается в общую книгу подразделения с уровнем доступа **Просмотр**

Доступ к книге

Доступ к общей книге выдаётся отдельным пользователям или группам на одном из трёх уровней:

Уровень	Возможности
Просмотр	Просматривать адреса и теги книги и подключаться к устройствам
Изменение	Всё, что доступно на уровне **Просмотр**, а также добавление, редактирование и удаление адресов и тегов в книге

продолжается на следующей странице

Таблица 3 – продолжение с предыдущей страницы

Уровень	Возможности
Управление	Всё, что доступно на уровне **Изменение**, а также редактирование самой книги, управление доступом, включение/выключение и удаление книги

Важно

- Владелец книги всегда имеет уровень **Управление**
- Руководитель подразделения имеет уровень **Управление** для общих книг своего подразделения
- Суперпользователь имеет уровень **Управление** для всех книг
- При выдаче доступа группе его получают все её участники, в том числе добавленные в группу позже

Состояние книги

Каждая книга может быть **включена** или **выключена**. Если книга выключена, её содержимое (адреса и теги) скрывается от пользователей, а сама книга остаётся видимой владельцу, чтобы её можно было включить обратно. Выключение используется для временной приостановки доступа без удаления данных

Что происходит при удалении

Важно

- При удалении **устройства** на странице *Устройства* связанные с ним адреса автоматически удаляются из всех книг
- При удалении **пользователя** удаляются все **общие** книги, которыми он владеет, вместе с их адресами, тегами и выданными доступами. Книги подразделений создаются без явного владельца и удаление пользователя переживают — поэтому, чтобы общая книга не зависела от одного человека, привязывайте её к подразделению
- При удалении **подразделения** его общая книга не удаляется, а теряет привязку к подразделению
- При удалении **книги** удаляются все входящие в неё адреса, теги и выданные доступы

Описание страницы

На странице **«Адресные книги»** отображено:

1. Кнопка Добавить адресную книгу
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление книги

При нажатии на кнопку Добавить адресную книгу откроется страница создания книги. Созданная таким образом книга является **общей**, и вы автоматически получаете к ней уровень доступа **Управление**

Важно

Кнопка Добавить адресную книгу доступна при наличии права **Адресная книга → Создание**

Содержит поля:

- Название* — необходимо ввести название книги
- Включена — состояние книги (по умолчанию включена)
- `Автоматическое добавление устройств` и `Условие` — настройка *пополнения книги по сохранённому фильтру*
- Описание — произвольное описание книги
- Подразделение — привязка книги к подразделению

Важно

1. Поле Подразделение доступно при наличии права *Подразделения → Просмотр* (суперпользователю доступно всегда)
2. Выбрать можно только подразделения, которыми управляет пользователь; суперпользователю доступны все подразделения

Для создания книги нужно нажать на кнопку Сохранить или Сохранить и продолжить

Подсказка

Общую книгу можно также создать сразу из готового набора адресов — массовым действием **«Создать новую книгу из выбранных адресов»** на странице *Адреса*

Автоматическое добавление устройств

Книгу можно пополнять устройствами по сохранённому фильтру со страницы *Устройства*. Например, добавлять устройства определённого подразделения или с нужной операционной системой.

1. На странице `Устройства` настроить условия отбора и нажать `Сохранить фильтр`.
2. Открыть создание или редактирование адресной книги, в которую нужно добавлять устройства.
3. Включить `Автоматическое добавление устройств`.
4. В поле `Условие` выбрать сохранённый фильтр. В списке доступны собственные сохранённые фильтры устройств.
5. Сохранить книгу.

При сохранении включённой книги в неё добавляются подходящие устройства, доступные пользователю, который выбрал условие. В дальнейшем условие проверяется при запуске клиента на устройстве. Для повторного заполнения книги уже имеющимися устройствами можно сохранить её ещё раз.

Устройства, которые уже есть в книге, повторно не добавляются. Новые адреса создаются без псевдонима.

Примечание

Это автоматическое добавление, а не синхронизация состава книги: если устройство перестало соответствовать условию, его адрес остаётся в книге. Выключение автодобавления также не удаляет ранее добавленные адреса.

В книге сохраняется выбранное условие. Если изменить исходный сохранённый фильтр, для применения новых правил нужно снова выбрать его в книге и сохранить изменения.

Автодобавление не работает для выключенной книги или при блокировке либо удалении автора условия. В последнем случае другой пользователь с правом управления книгой должен выбрать условие заново.

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

- Личная книга — фильтрация книг по типу (личная / общая)
- Включена — фильтрация книг по состоянию (включена / выключена)
- Подразделение — фильтрация книг по подразделению

> **Примечание**
>
> Фильтр Подразделение доступен только суперпользователю и руководителю подразделения

- Поле поиска — поиск по названию, описанию книги, а также по имени и e-mail владельца

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Массовые действия позволяют выполнить одну и ту же операцию сразу над несколькими книгами, не открывая свойства каждой из них

Панель массовых действий появляется под таблицей, как только отмечена хотя бы одна книга. Общий порядок работы одинаков для всех действий:

1. Отметить необходимые книги в таблице
2. Выбрать действие в списке Действия с выбранными объектами
3. Заполнить дополнительные поля, если действие их запрашивает (состояние) — пока обязательное поле не заполнено, кнопка Выполнить неактивна
4. Нажать на кнопку Выполнить

> **Важно**
>
> В панели есть кнопка Выбрать все. Она распространяет действие на **всю текущую выборку** — на все книги, отобранные фильтром и поиском, а не только на отмеченные на текущей странице. Рядом отображается счётчик Выбрано N из M или Выбраны все объекты, сбросить выбор можно кнопкой Снять выделение

Что делает каждое действие:

Действие	Что делает
Включить / выключить адресные книги	Переводит выбранные книги в состояние **Включена** или **Выключена**. Содержимое выключенной книги скрывается, но сохраняется, и книгу можно включить обратно
Удалить выбранные адресные книги	Удаляет книги вместе со всеми их *адресами* и *тегами*

Важно

1. Оба действия работают только с книгами, доступными с уровнем **Управление**
2. При включении и выключении книги без такого уровня пропускаются, а их количество показывается в предупреждении
3. Личные книги удалить нельзя — они пропускаются с предупреждением. Исключение составляет суперпользователь: для него ограничение не действует
4. В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Включение и выключение книг

Выключение — это способ временно убрать книгу из обращения, не удаляя её. Содержимое выключенной книги скрывается, но сохраняется на сервере, и книгу в любой момент можно включить обратно

Для массового изменения состояния книг необходимо:

1. Отметить необходимые книги в таблице
2. Выбрать действие Включить / выключить адресные книги
3. В поле Состояние выбрать значение **Включить** или **Выключить**
4. Нажать на кнопку Выполнить
5. Состояние выбранных книг будет изменено

Важно

Выключенная книга перестаёт открываться в клиентском приложении **RuDesktop** — она пропадает из переключателя книг вместе со своими адресами. Включить её обратно можно только в веб-интерфейсе

Примечание

1. Действие применяется только к книгам с уровнем доступа **Управление**; остальные пропускаются с предупреждением
2. Книги, уже находящиеся в нужном состоянии, не изменяются и в счётчик не попадают. Если ни одна книга не изменилась и ничего не пропущено, появится сообщение **«Выбранные книги уже в нужном состоянии»**

Удаление книг

Действие удаляет книги без возможности восстановления. Вместе с книгой удаляются все её *адреса* и *теги*, а также выданные на неё доступы. Сами устройства при этом не удаляются и остаются на странице *Устройства*

Подсказка

Если книгу нужно убрать из обращения временно, вместо удаления её можно выключить — содержимое сохранится

Для массового удаления книг необходимо:

1. Отметить необходимые книги в таблице
2. Выбрать действие Удалить выбранные адресные книги
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие книги будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные книги (кроме личных) будут удалены

Примечание

Личные книги отсеиваются до страницы подтверждения, поэтому в списке удаляемых их не будет, а о количестве пропущенных появится предупреждение. Если в выборке не осталось ни одной книги, доступной для удаления, страница подтверждения не откроется

Таблица

Таблица разбита по столбцам:

- `Название` — название книги
- `Включена` — состояние книги (включена / выключена)

- Тип — тип книги: **Личная** или **Общая**
- Подразделение — подразделение, к которому привязана книга
- Адреса — количество адресов в книге; ссылка открывает страницу *Адреса*, отфильтрованную по этой книге
- Доступы — количество выданных доступов; ссылка открывает вкладку Доступ к адресной книге в свойствах книги
- Владелец — владелец книги

Примечание

Столбцы Подразделение и Владелец отображаются только суперпользователю и руководителю подразделения

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

- Редактировать — при выборе этого пункта откроются свойства книги
- Удалить — при выборе этого пункта книга будет удалена

Примечание

Пункт Удалить недоступен для личной книги (удалить личную книгу может только суперпользователь)

- История изменений — при выборе этого пункта будет отображена история книги: создание/редактирование и пользователь, который выполнил данные операции

Важно

Операции Редактировать и Удалить доступны только при наличии уровня доступа **Управление**

Свойства книги

При нажатии на кнопку Редактировать откроется страница свойств книги, состоящая из нескольких вкладок

Основная информация

Содержит поля:

- Название — название книги
- Включена — состояние книги
- Описание — описание книги
- Подразделение — подразделение книги (поле доступно при наличии права *Подразделения → Просмотр*; для личной книги недоступно)

Адреса

Вкладка отображает адреса, входящие в книгу, и позволяет управлять ими, не переходя на страницу *Адреса*

На вкладке доступны:

- Поле поиска — поиск адресов внутри книги (по псевдониму, ID, имени устройства)
- Кнопка Добавить адрес — открывает страницу добавления адреса с уже выбранной текущей книгой
- Кнопка Очистить адресную книгу — удаляет все адреса из книги (после подтверждения)
- Таблица адресов со столбцами:
  - `Адрес` — псевдоним или имя устройства и его ID с кнопкой копирования; нажатие на название открывает страницу редактирования адреса
  - `Теги` — теги адреса; нажатие на тег открывает список адресов, отфильтрованный по этому тегу
  - `Удалить` — удаление адреса из книги (после подтверждения)
- Строка **Всего:** с количеством адресов в книге

Примечание

- Список адресов подгружается по мере прокрутки
- Управление адресами на вкладке Адреса доступно при уровне доступа **Управление**; пользователи с уровнем **Изменение** редактируют адреса на странице *Адреса*

Доступ к адресной книге

Вкладка служит для выдачи и отзыва доступа к книге. Доступна только для общих книг и только при наличии уровня доступа **Управление**

Для добавления доступа необходимо нажать на кнопку Добавить ещё доступ и заполнить строку:

- Пользователь — пользователь, которому выдаётся доступ
- Группа — группа, которой выдаётся доступ
- Право — уровень доступа: **Просмотр**, **Изменение** или **Управление**
- Выдал — пользователь, выдавший доступ (заполняется автоматически)
- Дата — дата выдачи доступа (заполняется автоматически)

Важно

- В строке необходимо заполнить либо поле Пользователь, либо поле Группа, но не оба сразу
- Нельзя выдать доступ одному и тому же пользователю или группе дважды в пределах одной книги
- Поле Группа недоступно в облачной версии

Для удаления доступа необходимо нажать на кнопку в строке доступа

Владелец

Вкладка позволяет изменить владельца общей книги и доступна только суперпользователю и только если у книги есть владелец. У автоматически созданных книг подразделений владельца нет, поэтому для них вкладка не отображается

Содержит поле:

- Владелец — владелец книги; при изменении значения владелец книги будет изменён

Меню действий

Меню действий расположено на всех вкладках страницы редактирования

Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Адресные книги»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление книги и перенаправляет на страницу **«Адресные книги»**

Примечание

Удаление недоступно для личной книги (удалить личную книгу может только суперпользователь)

4. История изменений — отображает все изменения, выполненные для этой книги

2.6.4 Адреса

Импорт адресов

Импорт адресов - данная страница служит для добавления адресов и тегов из файла в свою личную адресную книгу

Подсказка

Страница **«Импорт адресов»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Подсказка

Например, один пользователь может экспортировать свою адресную книгу в файл и передать его другому пользователю

Затем этот пользователь может импортировать файл, и адреса вместе с тегами добавятся в его адресную книгу



Важно

Кнопка Импортировать адреса доступна только при наличии права на добавление адресов (**Адресная книга → Создание**)

Как это работает

Импорт принимает файл в одном из табличных форматов (`CSV`, `XLS`, `XLSX`, `JSON`, `YAML`, `TSV`)

Каждая строка описывает один адрес, который будет добавлен в личную книгу пользователя, выполнившего импорт:

- `peer__server_id` - обязательное поле, ID существующего на сервере устройства (по нему адрес связывается с реальным устройством)
- `alias` - псевдоним, отображаемый в адресной книге
- `tags` - список *тегов* для классификации; теги, которых нет в личной книге, создаются автоматически
- `comment` - произвольный комментарий к адресу

При обработке файла **RuDesktop** валидирует строки по очереди:

- валидные записи добавляются в *Адреса* в личную книгу пользователя, выполнившего импорт

- невалидные строки (например, `peer__server_id` указывает на несуществующее устройство) пропускаются - после импорта по ним выводится сообщение об ошибке

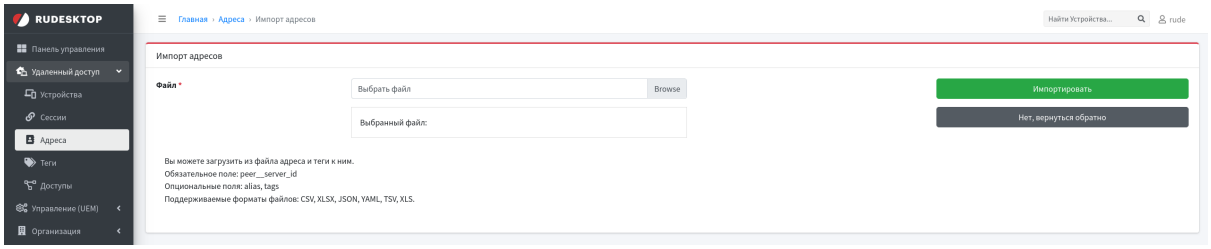
  Остальные адреса при этом импортируются успешно

Подсказка

Для удобного создания файла можно сначала экспортировать существующую адресную книгу с другого сервера или у другого пользователя через массовое действие **«Экспортировать выбранные адреса»** на странице *Адреса*, и затем импортировать его обратно

Описание страницы

На странице **«Импорт адресов»** отображено:



1. Файл адресов
2. Описание шаблона

Файл адресов

Поле для выбора заполненного файла с адресами и тегами

Важно

Файл может иметь расширения: `*.csv`, `*.xls`, `*.xlsx`, `*.json`, `*.yaml`, `*.tsv`

Описание шаблона

Можно импортировать адреса и теги к ним из файла

- Обязательное поле: `peer__server_id`
- Опциональные поля: `alias`, `tags`, `comment`

Важно

Если в файле импорта некоторые адреса не являются валидными, реализован механизм, позволяющий пропускать такие ошибки Это значит, что валидные записи будут успешно импортированы, а по невалидным записям будет выдано сообщение об ошибке

Пример импорта

1. Создать файл по шаблону
2. Нажать на кнопку Импортировать адреса
3. В поле Файл адресов выбрать созданный файл
4. Нажать на кнопку Импортировать
5. После импорта в таблице адресов появятся адреса, которые были указаны в файле

ID	Название	Теги	Пользователь
483670715	Peer 3	Rude 3	test
417273056	Peer 2	Rude 2	test
310713994	Peer 1	Rude 1	test

Выбор файла перетаскиванием

Подсказка

Файл импорта можно перетащить из файлового менеджера в поле выбора файла. После этого проверить имя в строке **«Выбранный файл»** и продолжить импорт

Примечание

Перетаскивание заменяет выбор файла кнопкой, но само по себе не запускает импорт

Переносить один файл за раз: если перетащить несколько, будет выбран первый

Перед повторным импортом проверить результат предыдущей операции, чтобы не повторять уже выполненные действия

Адреса — записи об устройствах, сохранённые в *адресные книги* для быстрого подключения

Подсказка

Страница **«Адреса»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Важно

- Пользователь видит адреса из своей личной книги, из общих книг, к которым ему выдан доступ, а также из книг, которыми он владеет
- *Руководитель подразделения* дополнительно видит адреса из общих книг своего подразделения
- Суперпользователь имеет доступ к просмотру адресов во всех книгах

Как это работает

Адрес — это запись в *адресной книге*, привязанная к ID устройства. По адресу можно быстро подключиться к рабочему столу, передать файлы, открыть терминал, RDP, настроить TCP-туннелирование или разбудить устройство по Wake-on-LAN — без поиска по общей таблице *Устройства*

Каждый адрес всегда находится в одной адресной книге. Если книга при создании адреса не выбрана, адрес добавляется в личную книгу пользователя. Возможность изменять адреса зависит от уровня доступа к их книге: для добавления, редактирования и удаления адреса нужен уровень **Изменение** или **Управление**. Адреса из книг, к которым выдан только уровень **Просмотр**, отображаются в таблице, но недоступны для изменения

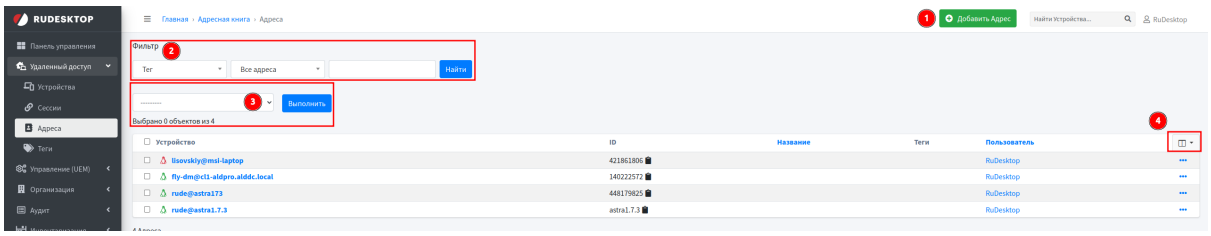
Запись об адресе появляется одним из способов:

- **создаётся вручную** через кнопку Добавить Адрес
- **импортируется из файла** (CSV/XLS/XLSX/JSON/YAML/TSV) — см. *Импорт адресов*
- **копируется из таблицы** *Устройства* массовым действием **«Скопировать в адресную книгу выбранные компьютеры»** — на странице подтверждения можно выбрать одну или несколько доступных книг; новые записи создаются без псевдонима
- **создаётся в клиенте RuDesktop** при сохранении устройства в адресную книгу

Каждому адресу можно назначить псевдоним и *теги* — теги используются для классификации и фильтрации адресов. Теги принадлежат книге адреса: назначить адресу можно только теги из его книги

Описание страницы

На странице **«Адреса»** отображено:

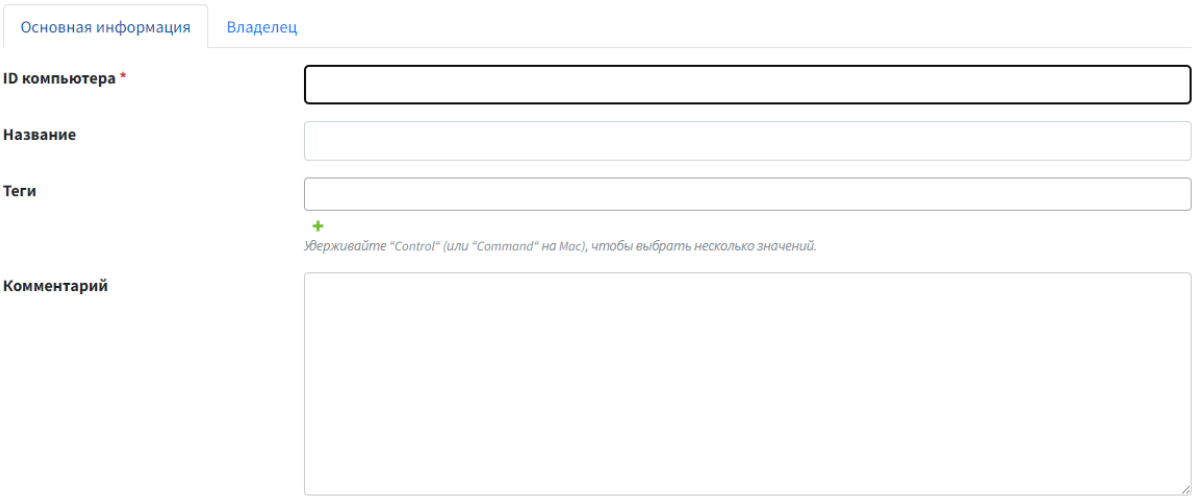


1. Кнопка Добавить Адрес

2. Кнопка Импортировать адреса
3. Фильтр
4. Массовые действия
5. Таблица с возможностью настройки отображаемых столбцов

Добавление адреса

При нажатии на кнопку Добавить Адрес откроется страница добавления адреса со следующими полями:



- Адресная книга — книга, в которую будет добавлен адрес

> **Важно**
>
> 1. Если книга не выбрана, адрес будет добавлен в личную книгу пользователя
> 2. В списке доступны только книги, в которые у вас есть право записи (уровень **Изменение** или **Управление**); суперпользователю доступны все книги

- ID компьютера* — необходимо ввести существующий ID удаленного компьютера
- Название — псевдоним для адреса
- Теги — назначение тегов для адреса; список тегов зависит от выбранной книги
- Комментарий — добавление заметок или дополнительных сведений

Для добавления адреса нужно нажать на кнопку Сохранить или Сохранить и продолжить

Импорт адресов из файла

Подробнее об *импорте адресов из файла*

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

- Адресная книга — выбор конкретной книги для отображения её адресов
- Адресная книга (Моя / Общая) — фильтрация по типу книги: **Моя** (адреса из ваших книг) или **Общая** (адреса из общих книг)

> **Примечание**
>
> Фильтр по типу доступен только суперпользователю и руководителю подразделения

- Теги — фильтрация адресов по тегу, назначенному на адрес
- Поле поиска — введите часть ID, имени или адреса устройства, имени пользователя либо псевдонима. Для поиска по тегу введите начало его названия

Введите запрос в поле **Быстрый поиск** и нажмите **Применить**

Массовые действия

Массовые действия позволяют выполнить одну и ту же операцию сразу над несколькими адресами, не открывая свойства каждого из них

Панель массовых действий появляется под таблицей, как только отмечен хотя бы один адрес. Общий порядок работы одинаков для всех действий:

1. Отметить необходимые адреса в таблице
2. Выбрать действие в списке Действия с выбранными объектами
3. Заполнить дополнительные поля, если действие их запрашивает (формат файла) — пока обязательное поле не заполнено, кнопка Выполнить неактивна
4. Нажать на кнопку Выполнить

Большинство действий открывает промежуточную страницу, на которой перечислены выбранные адреса и предлагается выбрать книгу, пользователей или теги

Важно

В панели есть кнопка Выбрать все. Она распространяет действие на **всю текущую выборку** — на все адреса, отобранные фильтром и поиском, а не только на отмеченные на текущей странице. Рядом отображается счётчик Выбрано N из M или Выбраны все объекты, сбросить выбор можно кнопкой Снять выделение

Примечание

1. Действие всегда работает только с теми адресами, которые видны текущему пользователю — правила видимости описаны в начале страницы
2. Назначить теги и Удалить выбранные адреса изменяют сами адреса, поэтому применяются лишь к тем из них, чьи книги доступны с уровнем **Изменение** или **Управление**. Остальные пропускаются, а их количество показывается в предупреждении
3. Действия копирования исходные адреса не изменяют, поэтому права записи на их книги не требуют — достаточно того, что адреса видны. Право записи нужно только на книгу-получатель

Что делает каждое действие:

Действие	Что делает
Скопировать в адресную книгу	Создаёт копии выбранных адресов в одной или нескольких выбранных книгах. Исходные адреса остаются на месте. Устройства, которые уже есть в книге-получателе, пропускаются
Скопировать в книги другим пользователям	Создаёт копии выбранных адресов в личных книгах выбранных пользователей. Если у пользователя уже есть адрес этого устройства, запись **перезаписывается** данными исходного адреса
Создать новую книгу из выбранных адресов	Создаёт новую общую книгу, копирует в неё выбранные адреса и назначает вас её владельцем
Назначить теги	**Добавляет** выбранные теги к адресам. Уже назначенные теги сохраняются
Экспортировать выбранные адреса	Выгружает данные выбранных адресов в файл фиксированного набора полей

продолжается на следующей странице

Таблица 5 – продолжение с предыдущей страницы

Действие	Что делает
Удалить выбранные адреса	Удаляет отмеченные записи из их книг. Само устройство и его адреса в других книгах не затрагиваются
Удалить адрес из всех адресных книг	Удаляет записи об устройствах выбранных адресов **из всех книг**, доступных вам на запись, а не только из книг отмеченных адресов

Важно

1. Действие Скопировать в книги другим пользователям доступно суперпользователю и пользователям с правом *Просмотр всех пользователей в административной панели* или *Руководитель подразделения*
2. Действие Создать новую книгу из выбранных адресов доступно суперпользователю и пользователям с правом **Руководитель подразделения**
3. Действие Экспортировать выбранные адреса требует права **Может экспортировать данные**
4. В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Копирование адресов в адресную книгу

Действие создаёт копии выбранных адресов в одной или нескольких выбранных книгах. Вместе с адресом переносятся его псевдоним, комментарий и теги — теги при этом создаются заново в книге-получателе, если тегов с такими названиями там ещё нет. Исходные адреса остаются в своих книгах

Для массового копирования адресов в другие книги необходимо:

1. Отметить необходимые адреса в таблице
2. Выбрать действие Скопировать в адресную книгу
3. Нажать на кнопку Выполнить
4. Откроется страница выбора книги-получателя

1. Отметить одну или несколько книг из списка. Доступны только книги, в которые у вас есть право записи; можно воспользоваться поиском
2. Проверить сводку количества записей и пользователей перед подтверждением
3. Нажать на кнопку Скопировать

   Можно отменить данную операцию, нажав на кнопку Нет, вернуться обратно

4. Выбранные адреса будут скопированы в каждую отмеченную книгу

> **Примечание**
>
> Адреса, устройства которых уже есть в книге-получателе, не копируются повторно

Кнопки `Выбрать все` и `Отменить выбор` действуют на книги, видимые с учётом поиска. Выбор скрытых поиском книг сохраняется. Чтобы проверить весь выбор, очистить поиск.

Для каждой книги выводится результат копирования и создаётся событие `Добавление в адресную книгу` в *журнале аудита*. Исходные адреса не удаляются.

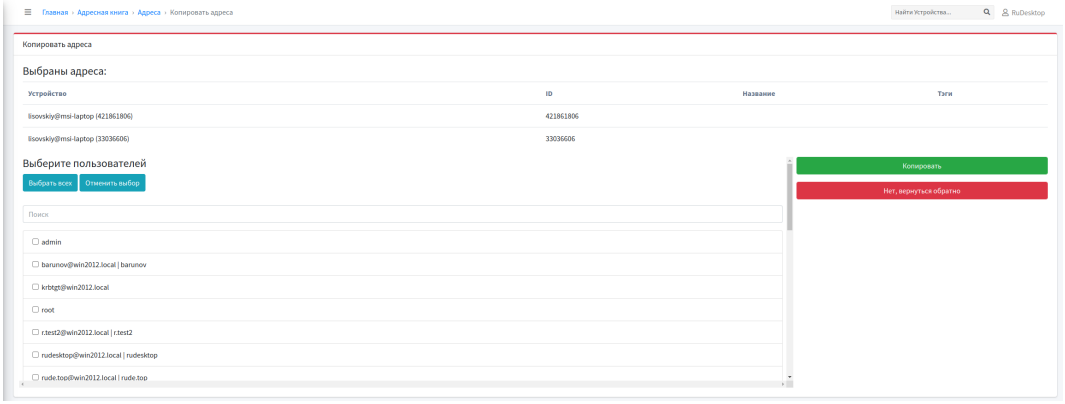
Копирование адресов другим пользователям

Действие создаёт копии выбранных адресов в личных книгах выбранных пользователей — вместе с псевдонимом, комментарием и тегами

> **Важно**
>
> В отличие от копирования в книгу, здесь совпадающие записи **не пропускаются**. Если у пользователя в личной книге уже есть адрес этого устройства, его псевдоним и комментарий будут заменены значениями из копируемого адреса, а теги — добавлены к уже назначенным

Для массового копирования адресов в личные книги других пользователей необходимо:

1. Отметить необходимые адреса в таблице
2. Выбрать действие Скопировать в книги другим пользователям
3. Нажать на кнопку Выполнить
4. Откроется страница выбора пользователей



1. Далее необходимо выбрать одного или нескольких пользователей (можно так же использовать поиск по имени, либо при необ-

ходимости воспользоваться кнопками Выбрать все и Отменить выбор)

2. При необходимости отобрать пользователей полем Группа. Оно доступно при наличии права на просмотр групп; фильтр ограничивает список получателей, но не выдаёт доступ к книге всей группе
3. Проверить выбранных пользователей и сводку перед подтверждением
4. После выбора необходимых пользователей нажать на кнопку Скопировать

   Можно отменить данную операцию, нажав на кнопку Нет, вернуться обратно
5. Выбранные адреса будут скопированы в личные книги выбранных пользователей

Важно

1. Действие Скопировать в книги другим пользователям доступно суперпользователю, а также пользователям с правом **«Просмотр всех пользователей в административной панели»** или **«Руководитель подразделения»**
2. В списке отображаются только пользователи, доступные текущему пользователю; себя в этом списке выбрать нельзя
3. Если доступных пользователей нет, действие не выполнится и появится предупреждение

Поиск и фильтр по группе не снимают ранее установленный выбор. Кнопки Выбрать все и Отменить выбор применяются к видимым пользователям. Перед копированием очистить поиск и выбрать Все группы, чтобы проверить получателей.

Копирование в личную книгу каждого получателя фиксируется отдельным событием Добавление в адресную книгу в журнале аудита.

Создание книги из выбранных адресов

Действие создаёт новую **общую** книгу и копирует в неё выбранные адреса вместе с псевдонимами, комментариями и тегами. Исходные адреса остаются в своих книгах

Для создания новой общей книги из выбранных адресов необходимо:

1. Отметить необходимые адреса в таблице
2. Выбрать действие Создать новую книгу из выбранных адресов
3. Нажать на кнопку Выполнить
4. В поле Название книги ввести название новой книги

5. Нажать на кнопку Создать книгу
6. Будет создана новая общая книга с выбранными адресами; её владельцем станете вы

Важно

1. Действие Создать новую книгу из выбранных адресов доступно только суперпользователю и пользователю с правом **«Руководитель подразделения»**
2. Вы получаете на новую книгу уровень доступа **Управление**. Чтобы книгой могли пользоваться другие, доступ к ней нужно выдать отдельно на странице *Адресные книги*
3. Книга создаётся без привязки к подразделению — при необходимости её можно указать в свойствах книги
4. Название книги обязательно: если поле пустое, книга не создастся и появится предупреждение

Назначение тегов адресам

Действие назначает выбранные *теги* сразу нескольким адресам

Важно

Действие **добавляет** теги к уже назначенным, а не заменяет их: ранее назначенные теги у адресов сохраняются. Чтобы снять тег, его нужно убрать в свойствах адреса

Для массового назначения тегов адресам необходимо:

1. Отметить необходимые адреса в таблице
2. Выбрать действие Назначить теги
3. Нажать на кнопку Выполнить
4. Откроется страница выбора тегов для назначения выбранным адресам
5. Далее необходимо выбрать один или несколько тегов (можно так же использовать поиск по имени, либо при необходимости воспользоваться кнопками Выбрать все и Отменить выбор)
6. После выбора необходимых тегов нажать на кнопку Назначить

   Можно отменить данную операцию, нажав на кнопку Нет, вернуться обратно
7. Выбранные теги будут назначены выбранным адресам

Примечание

1. Теги назначаются в пределах каждой книги: тег подбирается по названию в книге самого адреса, а если тега с таким названием там ещё нет — он создаётся с тем же цветом. Поэтому один и тот же тег можно назначить адресам из разных книг за одно действие
2. Адреса из книг, к которым нет права записи, пропускаются — их количество показывается в предупреждении
3. В списке доступны теги из всех книг, к которым у вас есть доступ, — в том числе из книг с уровнем **Просмотр**. Выбранный тег переносится в книгу адреса по названию, поэтому исходная книга тега значения не имеет. Если доступных тегов нет, действие не выполнится и появится предупреждение

Экспорт адресов

Действие выгружает данные выбранных адресов в файл — например, для передачи списка в другую систему или для последующего *импорта*

Примечание

В файл выгружается фиксированный набор полей: ID устройства, имя хоста, имя пользователя устройства, псевдоним адреса и теги. Настройка отображаемых столбцов таблицы на состав файла не влияет

Для массового экспорта адресов необходимо:

1. Отметить необходимые адреса в таблице
2. Выбрать действие Экспортировать выбранные адреса
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Важно

1. Доступные форматы выгрузки: **CSV**, **XLS**, **XLSX**, **TSV**, **ODS**, **JSON**, **YAML**, **HTML**. Набор форматов зависит от компонентов, установленных на сервере, поэтому отдельные пункты могут отсутствовать
2. Если выбрано более 1000 адресов, экспорт выполняется в фоне: файл не скачивается сразу, а сохраняется на сервере в репозитории **Отчеты** и становится доступен на странице *Файлы*. Ход выполнения виден на странице *Очередь задач* по задаче **«Экспорт»**
3. Формат **XLS** не поддерживает ячейки с текстом длиннее 32767 символов — при таких значениях экспорт завершится ошибкой с предложением выбрать другой формат

Удаление адресов

Действие удаляет отмеченные записи из их книг. Само устройство при этом не удаляется и остаётся на странице *Устройства*, а его адреса в других книгах не затрагиваются

Для массового удаления адресов необходимо:

1. Отметить необходимые адреса в таблице
2. Выбрать действие Удалить выбранные адреса
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие адреса будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору

   1. Выбранные адреса будут удалены

Примечание

Удаляются только адреса из книг, к которым у вас есть право записи; остальные пропускаются с уведомлением

Удаление адреса из всех адресных книг

Действие работает не с отмеченными записями, а с **устройствами**, на которые они ссылаются: для каждого такого устройства удаляются все его адреса во всех книгах, доступных вам на запись

Это удобно, когда устройство выведено из эксплуатации и его записи нужно убрать у всех сразу, не разыскивая их по книгам

Для удаления адресов устройств из всех книг необходимо:

1. Отметить в таблице любые адреса нужных устройств — достаточно одного адреса на устройство
2. Выбрать действие Удалить адрес из всех адресных книг
3. Нажать на кнопку Выполнить
4. Появится уведомление с количеством удалённых записей и устройств

Важно

1. Действие выполняется сразу, без страницы подтверждения — отменить его нельзя

2. Удаляются адреса не только из тех книг, которые видны в таблице, но из **всех** книг с уровнем доступа **Изменение** или **Управление**, включая чужие общие книги. Записи в книгах, на запись в которые прав нет, остаются нетронутыми
3. Сами устройства не удаляются и остаются на странице *Устройства*

Таблица

Таблица разбита по столбцам:

- `Адрес` — имя устройства с индикатором платформы и статуса (в сети / не в сети)
- `ID` — идентификатор устройства, который отображается в окне клиентского приложения и присваивается при подключении устройства к серверу
- `Псевдоним` — псевдоним адреса, можно задать в свойствах адреса для более удобной работы
- `Теги` — метки для классификации адресов и упрощения поиска
- `Адресная книга` — книга, в которой находится адрес; ссылка открывает свойства книги

Примечание

- Столбец `Псевдоним устройства` по умолчанию скрыт — его можно включить через настройку отображаемых столбцов
- Столбец `Адресная книга` отображается только при наличии доступа к просмотру адресных книг

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

- Редактировать — при выборе этого пункта откроются свойства адреса
- Удалить — при выборе этого пункта адрес будет удален
- История изменений — при выборе этого пункта будет отображена история адреса: создание/редактирование и пользователь, который выполнил данные операции
- Подключиться — при наведении курсора на данный пункт откроется контекстное меню с вариантами подключения:
  - Рабочий стол — выполнить подключение к рабочему столу удаленного устройства

- Передача файлов — выполнить подключение к файловой системе удаленного устройства
- TCP-туннелирование — настройка TCP туннелирования
- RDP — выполнить подключение через Remote Desktop Protocol (протокол удалённого рабочего стола)
- Разбудить (Wake On LAN) — выполнить пробуждение устройства через WOL

> **Важно**
>
> * Для того чтобы разбудить устройство, необходимо хотя бы один раз подключиться к удалённому устройству
> * Устройство должно находиться в той же подсети, что и устройство, с которого производится попытка пробуждения

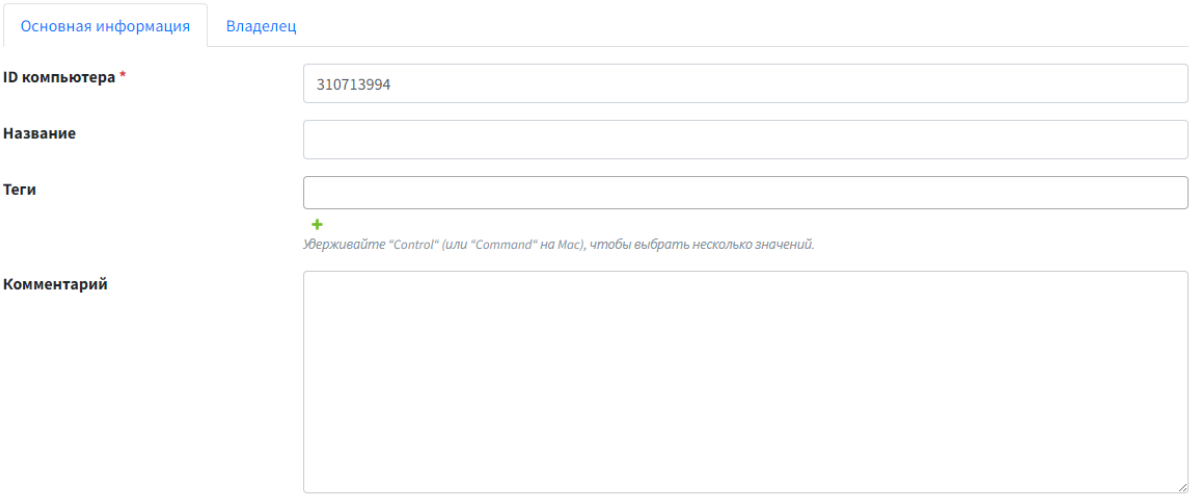
- Подключиться к терминалу — выполнить подключение к терминалу удаленного устройства
- Проброс USB — выполнить проброс USB-устройств с локального компьютера на удалённое устройство

> **Важно**
>
> Действия Редактировать и Удалить доступны только для адресов из книг, к которым у вас есть право записи

Свойства адреса

Редактирование

При нажатии на кнопку Редактировать откроется страница свойств



Доступные поля:

- Адресная книга — книга, в которой находится адрес

> **Важно**
>
> В зависимости от уровня доступа к книге адреса внесение изменений может быть недоступно. Подробнее об *адресных книгах* и *правах*

- ID компьютера — идентификатор устройства, который отображается в окне клиентского приложения и присваивается при подключении устройства к серверу
- Название — псевдоним адреса
- Теги — метки для классификации адресов и упрощения поиска
- Комментарий — заметки или дополнительные сведения

Меню действий

Меню действий расположено на всех вкладках страницы редактирования



Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Адреса»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление адреса и перенаправляет на страницу **«Адреса»**

> **Примечание**
>
> 1. После нажатия на кнопку Удалить откроется страница подтверждения удаления адреса

2. После подтверждения удаления адреса произойдет переход на страницу **«Адреса»** и появится уведомление Адрес «НАЗВАНИЕ_АДРЕСА» был успешно удален

4. История изменений — отображает все изменения, выполненные для этого адреса
5. Подключиться — позволяет подключится к рабочему столу, файловой системе, RDP, настроить TCP-туннелирование и выполнить подключение к терминалу удаленного устройства

Важно

Для того чтобы подключение прошло успешно, на устройстве, с которого происходит подключение, и на устройстве, на которое происходит подключение, должен быть установлен клиент RuDesktop

Внимание

При выборе типа подключения браузер запросит разрешение на запуск клиентского приложения, и необходимо предоставить данную возможность

2.6.5 Теги

Теги — метки для классификации адресов и упрощения поиска, добавленные пользователями

Подсказка

Страница **«Теги»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Важно

- Пользователь видит теги из своей личной книги, из общих книг, к которым ему выдан доступ, а также из книг, которыми он владеет
- *Руководитель подразделения* дополнительно видит теги из общих книг своего подразделения
- Суперпользователь имеет доступ к просмотру тегов во всех книгах

Как это работает

Тег — это пользовательская метка, которую можно повесить на один или несколько *адресов*. Тег принадлежит *адресной книге*: один и тот же тег в разных книгах — это разные теги. Назначить адресу можно только теги из его книги

Теги используются как универсальный механизм классификации:

- группировка адресов по проектам, заказчикам, локациям, ролям сервера
- быстрая фильтрация адресов на странице **«Адреса»** по выбранному тегу
- передача тега вместе с адресом при экспорте/импорте адресной книги

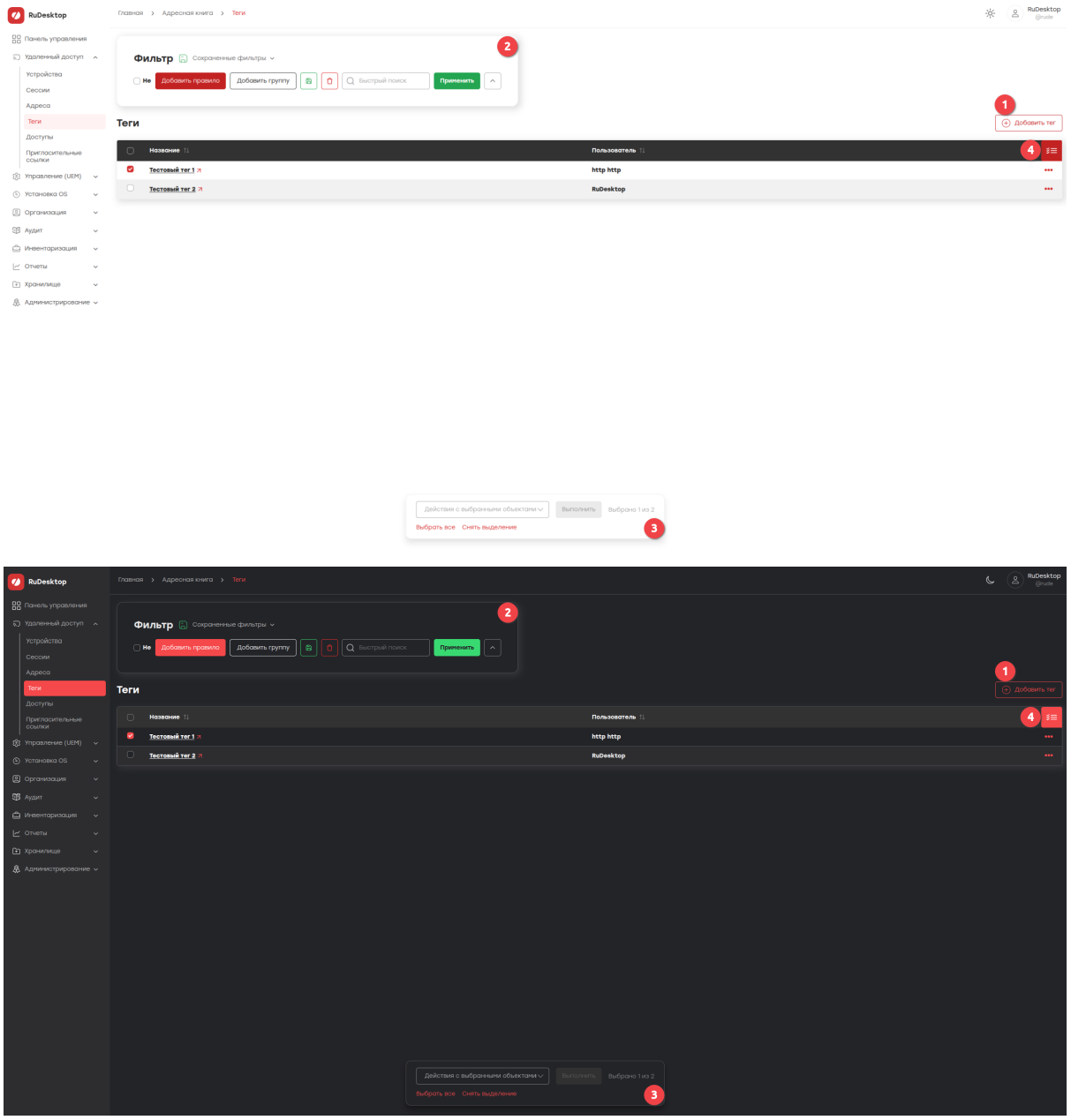
Возможность создавать, переименовывать и удалять теги зависит от уровня доступа к их книге: нужен уровень **Изменение** или **Управление**

Примечание

Удаление тега не удаляет связанные с ним адреса — снимается только привязка тега к адресам

Описание страницы

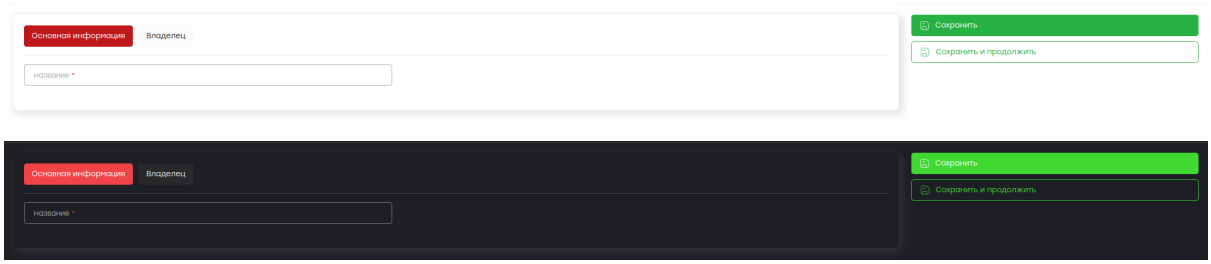
На странице **«Теги»** отображено:



1. Кнопка Добавить Тег
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление тега

При нажатии на кнопку Добавить Тег откроется страница добавления тега со следующими полями:



- Название* — необходимо заполнить название тега
- Адресная книга — книга, в которой будет создан тег

> **Важно**
>
> 1. Если книга не выбрана, тег будет создан в личной книге пользователя
> 2. В списке доступны только книги, в которые у вас есть право записи (уровень **Изменение** или **Управление**); суперпользователю доступны все книги
> 3. В пределах одной книги не может быть двух тегов с одинаковым названием

Для добавления тега нужно нажать на кнопку Сохранить или Сохранить и продолжить

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

- Теги (Мои / Общие) — фильтрация тегов по типу книги: **Мои** (теги из ваших книг) или **Общие** (теги из общих книг)

Примечание

Фильтр по типу доступен только суперпользователю и руководителю подразделения

- Адресная книга — фильтрация тегов по книге

Для выполнения фильтрации необходимо нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные теги — удалить выбранные записи из таблицы
2. Экспортировать выбранные теги — позволяет экспортировать в файл выбранные теги

Примечание

После выбора данного действия нужно выбрать необходимый формат файла

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление тегов

Для массового удаления тегов необходимо:

1. Отметить необходимые теги в таблице
2. Выбрать действие Удалить выбранные теги
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие теги будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные теги будут удалены

Экспорт тегов

Для массового экспорта тегов необходимо:

1. Отметить необходимые теги в таблице
2. Выбрать действие Экспортировать выбранные теги
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. Название — наименование тега
2. Адресная книга — книга, которой принадлежит тег; ссылка открывает свойства книги
3. Использований — количество адресов с этим тегом; ссылка открывает список адресов, отфильтрованный по тегу

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. Редактировать — при выборе этого пункта откроются свойства тега, где можно изменить его название или книгу
2. Удалить — при выборе этого пункта тег будет удален
3. История изменений — при выборе этого пункта будет отображена история тега: создание/редактирование и пользователь, который выполнил данные операции

Важно

Операции Редактировать и Удалить доступны только для тегов из книг, к которым у вас есть право записи

Свойства тега

Редактирование

При нажатии на кнопку Редактировать откроется страница свойств

Доступные поля:

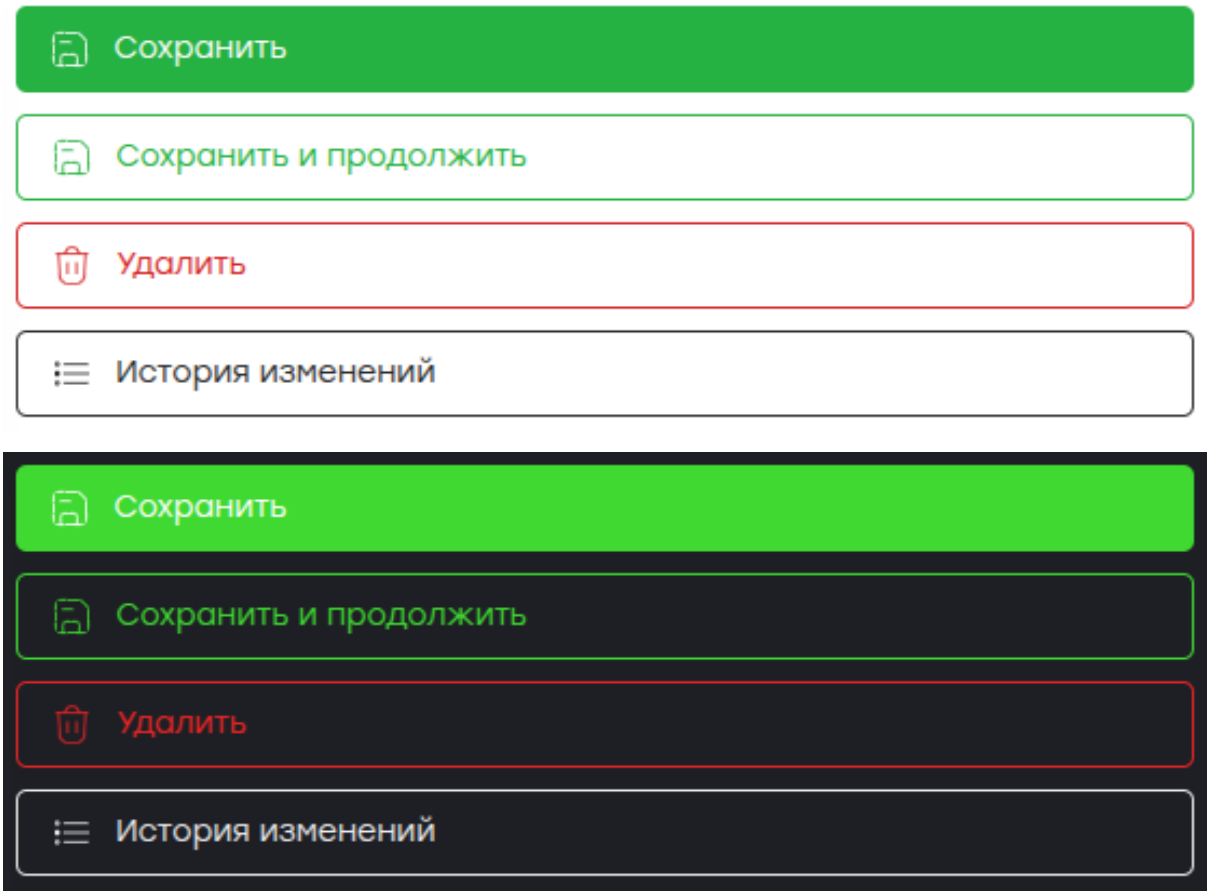
- Название — отображаемое название тега
- Адресная книга — книга, которой принадлежит тег

Важно

1. В зависимости от уровня доступа к книге внесение изменений может быть недоступно
2. Подробнее об *адресных книгах* и *правах*

Меню действий

Меню действий расположено справа на всех вкладках страницы редактирования



Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Теги»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление тега и перенаправляет на страницу **«Теги»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления тега
2. После подтверждения удаления тега произойдет переход на страницу **«Теги»** и появится уведомление Тег «НАЗВАНИЕ_ТЕГА» был успешно удален

4. История изменений — отображает все изменения, выполненные для этого тега

2.6.6 Доступы

Доступы — на этой странице вы можете настроить разрешения для подключения к удаленным устройствам

Подсказка

Страница **«Доступы»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Примечание

Вы можете определить, какие пользователи, устройства или группы устройств имеют разрешение подключаться к определённым удалённым устройствам или группам устройств

Как это работает

При заполнении списков устройств, пользователей, групп и динамических групп можно использовать кнопку Импорт в правом столбце. Она дополняет выбор существующими записями из файла; для применения изменений сохраните доступ. Подробности: *Импорт записей в списки выбора*

Доступ — это правило, которое отвечает на вопрос «**кто и как может подключаться к каким устройствам**». Каждое правило состоит из четырёх частей:

- **Подключаемые устройства** — кому разрешено инициировать подключение (пользователи, устройства, группы, динамические группы или «все»)
- **Устройства для подключения** — к чему разрешено подключаться (устройства, группы, динамические группы или «все»)
- **Права подключения** — что разрешено делать в рамках сессии (мастер-пароль, скрытое подключение, без подтверждения, удалённый терминал администратором и т.д.)

- **Разрешения** — типы подключений, по которым работает доступ (Удалённый рабочий стол, Передача файлов, Терминал, RDP, TCP-туннелирование, Проброс USB, Системный монитор)

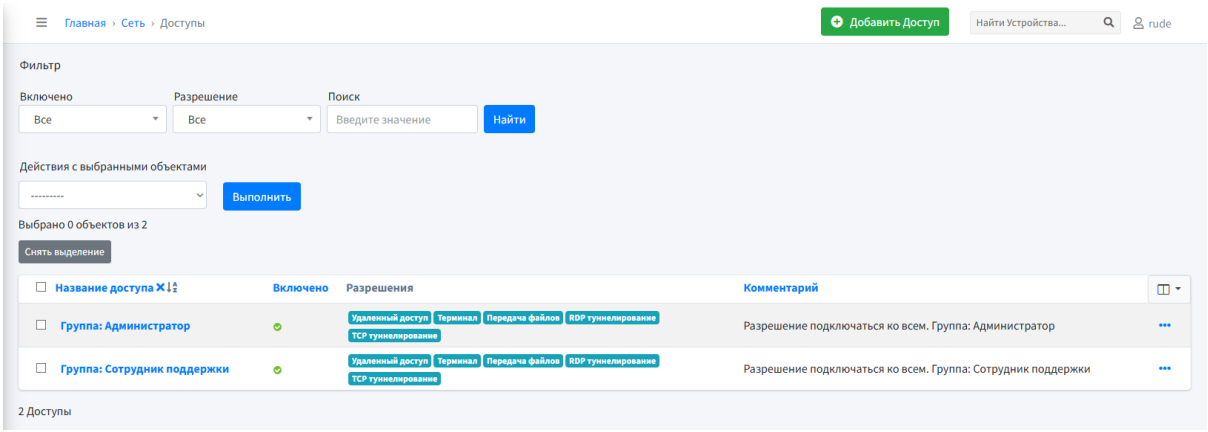
При подключении сервер проверяет совпадения по всем активным правилам и собирает итоговый набор прав и разрешений. Если для пары «оператор → клиент» нет ни одного активного правила, подключение запрещено

Важно

- Исключений для суперпользователя нет: для подключения к устройству ему, как и остальным операторам, нужен активный доступ, включающий пару «оператор → устройство» с нужным типом подключения. Без такого доступа подключение завершится ошибкой недостатка прав
- При авторизации в клиенте суперпользователь автоматически получает все разрешения — в том числе не назначенные ни одним доступом. Эти разрешения расширяют возможности уже разрешённого доступа, но сами по себе подключение не открывают
- Правило с выключенным флагом Включено не учитывается при подборе прав, но сохраняется и его можно включить обратно

Описание страницы

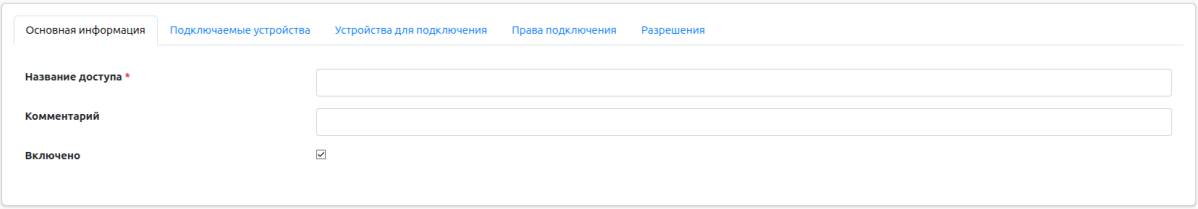
На странице **«Доступы»** отображено:



1. Кнопка Добавить Доступ
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление доступа

При нажатии на кнопку Добавить Доступ откроется страница добавления доступа со следующими вкладками:



Основная информация

- Название доступа — обязательное поле для указания соответствующего имени доступа
- Комментарий — необязательное поле, позволяет добавить дополнительную информацию или замечания
- Включено — используется для включения или отключения доступа

Подключаемые устройства

На этой вкладке вы можете задать, какие устройства могут инициализировать подключение

Подсказка

Вы можете разрешить доступ ко всем устройствам либо ограничить его конкретными группами, динамическими группами, отдельными устройствами или пользователями

- Все устройства — все устройства будут иметь разрешение на подключение
- Группы — выбор конкретных групп, которые будут иметь разрешение на подключение
- Пользователи — выбор конкретных пользователей, которые будут иметь разрешение на подключение
- Устройства — выбор конкретных устройств, которые будут иметь разрешение на подключение
- Дин.Группы — выбор конкретных динамических групп, которые будут иметь разрешение на подключение

Примечание

В полях Группы, Пользователи, Устройства и Дин.Группы (на обеих вкладках), помимо поштучного добавления, доступны массовые действия над всем списком — кнопки Добавить и сохранить все и Очистить список и сохранить. Они доступны только после сохранения записи. При большом количестве элементов действие выполняется в фоновом режиме: отображается индикатор прогресса со счётчиком и кнопка Отменить задачу, а списки блокируются до завершения операции

Устройства для подключения

На этой вкладке вы можете задать, к каким устройствам, группам или динамическим группам можно подключаться

Подсказка

Вы можете разрешить доступ ко всем устройствам либо ограничить его конкретными группами, динамическими группами или отдельными устройствами

- Все устройства — предоставляет возможность подключения ко всем устройствам
- Группы — выбор конкретных групп, к которым будет предоставлен доступ для подключения
- Устройства — выбор конкретных устройств, к которым будет предоставлен доступ для подключения
- Дин.Группы — выбор конкретных динамических групп, к которым будет предоставлен доступ для подключения

Права подключения

На этой вкладке вы можете выбрать права подключения, которые будут предоставлены при подключении

- Может подключаться без подтверждения со стороны пользователя — право предоставляет возможность инициировать удаленную сессию без подтверждения со стороны удаленного устройства

  Подсказка

  Если это право не активно, но активно право на подключение с использованием мастер-пароля, все равно потребуется подтвердить подключение на удаленном устройстве

- Доступ к устройствам по мастер паролю — право предоставляет возможность подключаться к устройствам с помощью мастер-пароля, вместо ввода временного или постоянного пароля

- Скрывать окно подключения при использовании мастер пароля — право предоставляет возможность не отображать окно подключения на удаленном устройстве, что позволяет подключиться в скрытом режиме

> **Подсказка**
>
> Данное право работает только если активно право **Доступ к устройствам по мастер паролю**

- Может управлять клиентом на удаленном устройстве — право разрешает использовать интерфейс клиента на удаленном устройстве во время подключения
- Может подключаться к удалённому терминалу в качестве администратора — право дает возможность открывать удаленный терминал с повышенными правами, если такой режим поддерживается удаленным устройством

> **Важно**
>
> Суперпользователю, как и остальным операторам, для подключения нужен активный доступ с нужным типом подключения для пары «оператор → устройство»: без него подключение завершится ошибкой недостатка прав
>
> Все разрешения — в том числе не назначенные ни одним доступом, например подключение без подтверждения, — суперпользователь получает автоматически при авторизации в клиенте. Эти разрешения расширяют возможности уже разрешённого доступа, но сами по себе подключение не открывают

Разрешения

На этой вкладке вы можете выбрать типы подключений, по которым будет предоставлен доступ на подключение

- Удаленный доступ — разрешение на подключение к удаленному рабочему столу
- Передача файлов — разрешение на подключение к файловой системе удаленного устройства
- Терминал — разрешение на подключение к терминалу удаленного устройства
- TCP туннелирование — разрешение на установку туннеля с удалённым устройством
- RDP туннелирование — разрешение на подключение по RDP с удаленным устройством
- Проброс USB — разрешение проброса USB на удаленное устройство
- Системный монитор — разрешение просмотра процессов и управления их завершением через системный монитор

Для добавления доступа нужно нажать на кнопку Сохранить или Сохранить и продолжить

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

- Включено — фильтрация доступов по статусу
- Разрешение — фильтрация доступов по активным разрешениям
- Права подключения — фильтрация доступов по выбранным правам подключения (мастер-пароль, скрытое подключение, без подтверждения и т.д.)
- Поле поиска — поиск по ключевому слову

> **Подсказка**
>
> Поиск по ключевому слову осуществляется по названию доступа и комментарию

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Массовые действия позволяют выполнить одну и ту же операцию сразу над несколькими доступами, не открывая свойства каждого из них

Панель массовых действий появляется под таблицей, как только отмечен хотя бы один доступ. Общий порядок работы одинаков для всех действий:

1. Отметить необходимые доступы в таблице
2. Выбрать действие в списке Действия с выбранными объектами
3. Нажать на кнопку Выполнить

> **Важно**
>
> В панели есть кнопка Выбрать все. Она распространяет действие на **всю текущую выборку** — на все доступы, отобранные фильтром и поиском, а не только на отмеченные на текущей странице. Рядом отображается счётчик Выбрано N из M или Выбраны все объекты, сбросить выбор можно кнопкой Снять выделение

Что делает каждое действие:

Действие	Что делает
Удалить выбранные доступы	Удаляет правила с сервера. Пользователи, группы и устройства, перечисленные в правилах, не затрагиваются
Включить разрешение	Включает у выбранных правил флаг Включено, после чего они снова учитываются при подборе прав
Выключить разрешение	Снимает этот флаг: правила сохраняются, но перестают учитываться при подключении
Изменить права	Открывает отдельную страницу, на которой можно разом задать всем выбранным правилам новый набор прав подключения и разрешённых типов подключения

Важно

1. Действия Включить разрешение, Выключить разрешение и Изменить права требуют права **Доступы → Изменение**
2. Действие Удалить выбранные доступы требует права **Доступы → Удаление**
3. В зависимости от прав действия могут отсутствовать

Примечание

Выключение доступа — обратимая операция: правило остаётся в таблице со снятым флагом Включено и в любой момент включается обратно. Если правило больше не нужно, его следует удалить

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление доступов

Для массового удаления доступов необходимо:

1. Отметить необходимые доступы в таблице
2. Выбрать действие Удалить выбранные доступы
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие доступы будут удалены
5. Нажать на кнопку Да, я уверен

Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору

6. Выбранные доступы будут удалены

Включение доступов

Для массового включения доступов необходимо:

1. Отметить необходимые доступы в таблице
2. Выбрать действие Включить разрешение
3. Нажать на кнопку Выполнить
4. Выбранные доступы будут успешно включены

Выключение доступов

Для массового выключения доступов необходимо:

1. Отметить необходимые доступы в таблице
2. Выбрать действие Выключить разрешение
3. Нажать на кнопку Выполнить
4. Выбранные доступы будут успешно выключены

Изменение прав

Действие задаёт всем выбранным правилам один и тот же набор прав подключения и разрешённых типов подключения. Остальные части правила — кто подключается, к чему подключается, название и комментарий — не меняются

Страница разделена на два независимых блока — **Права подключения** и **Разрешения**. У каждого блока есть собственный переключатель Переопределить, и блок применяется, только если этот переключатель включён:

Блок	Что произойдёт при включённом переключателе
Права подключения	Прежний набор прав у правила **заменяется** отмеченным
Разрешения	Отмеченные типы подключения становятся разрешёнными, а все **неотмеченные — явно запрещёнными**

Для массового изменения прав или разрешений необходимо:

1. Отметить необходимые доступы в таблице
2. Выбрать действие Изменить права
3. Нажать на кнопку Выполнить

4. Откроется страница **«Массовое действие»**: вверху — таблица Исходные доступы со списком выбранных правил, ниже — блоки **Права подключения** и **Разрешения**
5. Включить переключатель Переопределить у того блока, который нужно изменить, и отметить в нём нужные значения

> **Важно**
>
> Блок с выключенным переключателем не применяется вовсе — соответствующие настройки правил остаются прежними. Это позволяет менять, например, только разрешения, не трогая права подключения

> **Важно**
>
> Оба блока работают на **замену**, а не на дополнение. Набор отмеченных значений становится итоговым для всех выбранных правил, а прежние значения теряются — в том числе те, что отличались у разных правил. Если у части правил были права, которые нужно сохранить, отметьте их вместе с новыми
>
> При выполнении массового действия настройки прав и разрешений переопределяются. Это означает, что текущие настройки будут изменены на новые, которые вы выбрали в процессе выполнения массового действия

6. Нажать на кнопку Применить
7. Выбранные доступы будут изменены

Таблица

Таблица разбита по столбцам:

1. Название доступа — наименование доступа
2. Включено — статус доступа
3. Разрешения — отображение доступных типов подключений
4. Права подключения — отображение доступных прав подключения
5. Комментарий — отображение комментария

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. Редактировать — при выборе этого пункта откроются свойства доступа, где можно изменить его параметры

2. Удалить — при выборе этого пункта доступ будет удален
3. История изменений — при выборе этого пункта будет отображена история доступа: создание/редактирование и пользователь, который выполнил данные операции
4. Включить\Выключить — при выборе этого пункта доступ будет включен или выключен

Свойства доступа

Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств

Основная информация

- Название доступа — необходимо заполнить название доступа
- Комментарий — необязательное поле для указания комментария
- Включено — включение или выключение доступа

Подключаемые устройства

- Все устройства — все устройства будут иметь разрешение на подключение
- Группы — выбор конкретных групп, которые будут иметь разрешение на подключение
- Пользователи — выбор конкретных пользователей, которые будут иметь разрешение на подключение
- Устройства — выбор конкретных устройств, которые будут иметь разрешение на подключение
- Дин.Группы — выбор конкретных динамических групп, которые будут иметь разрешение на подключение

Примечание

В полях Группы, Пользователи, Устройства и Дин.Группы (на обеих вкладках), помимо поштучного добавления, доступны массовые действия над всем списком — кнопки Добавить и сохранить все и Очистить список и сохранить. Они доступны только после сохранения записи. При большом количестве элементов действие выполняется в фоновом режиме: отображается индикатор прогресса со счётчиком и кнопка Отменить задачу, а списки блокируются до завершения операции

Устройства для подключения

- Все устройства — предоставляет возможность подключения ко всем устройствам
- Группы — выбор конкретных групп, к которым будет предоставлен доступ для подключения

- Устройства — выбор конкретных устройств, к которым будет предоставлен доступ для подключения
- Дин.Группы — выбор конкретных динамических групп, к которым будет предоставлен доступ для подключения

Права подключения

- Может подключаться без подтверждения со стороны пользователя — право предоставляет возможность инициировать удаленную сессию без подтверждения со стороны удаленного устройства

> **Подсказка**
>
> Если это право не активно, но активно право на подключение с использованием мастер-пароля, все равно потребуется подтвердить подключение на удаленном устройстве

- Доступ к устройствам по мастер паролю — право предоставляет возможность подключаться к устройствам с помощью мастер-пароля, вместо ввода временного или постоянного пароля
- Скрывать окно подключения при использовании мастер пароля — право предоставляет возможность не отображать окно подключения на удаленном устройстве, что позволяет подключиться в скрытом режиме

> **Подсказка**
>
> Данное право работает только если активно право **Доступ к устройствам по мастер паролю**

- Может управлять клиентом на удаленном устройстве — право разрешает использовать интерфейс клиента на удаленном устройстве во время подключения
- Может подключаться к удалённому терминалу в качестве администратора — право дает возможность открывать удаленный терминал с повышенными правами, если такой режим поддерживается удаленным устройством

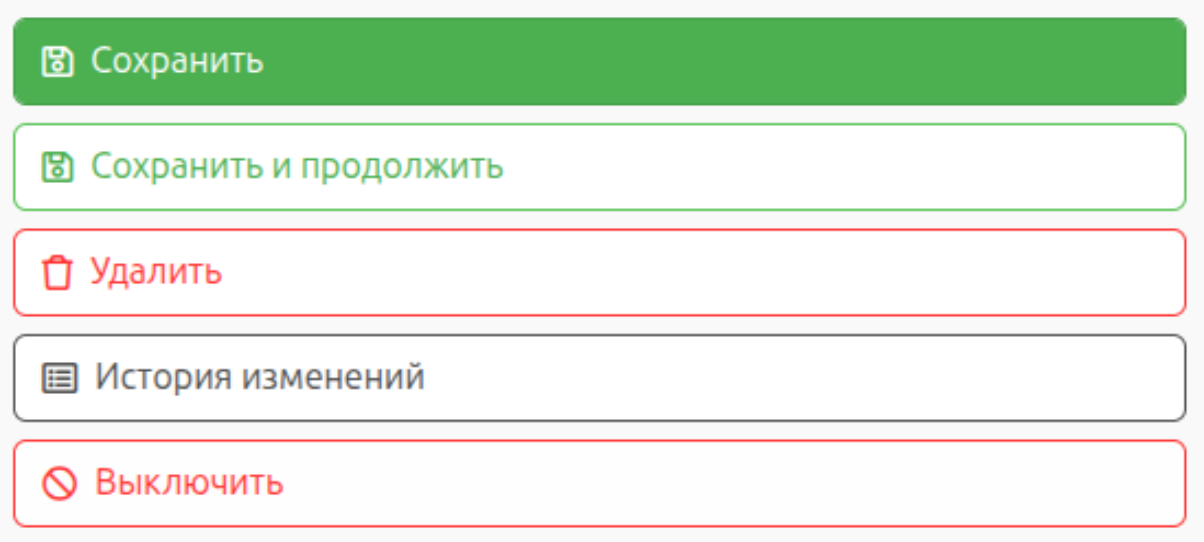
> **Важно**
>
> Суперпользователю, как и остальным операторам, для подключения нужен активный доступ с нужным типом подключения для пары «оператор → устройство»: без него подключение завершится ошибкой недостатка прав
>
> Все разрешения — в том числе не назначенные ни одним доступом, например подключение без подтверждения, — суперпользователь получает автоматически при авторизации в клиенте. Эти разрешения расширяют возможности уже разрешённого доступа, но сами по себе подключение не открывают

Разрешения

- Удаленный доступ — разрешение на подключение к удаленному рабочему столу
- Передача файлов — разрешение на подключение к файловой системе удаленного устройства
- Терминал — разрешение на подключение к терминалу удаленного устройства
- TCP туннелирование — разрешение на установку туннеля с удалённым устройством
- RDP туннелирование — разрешение на подключение по RDP с удаленным устройством
- Проброс USB — разрешение проброса USB на удаленное устройство
- Системный монитор — разрешение просмотра процессов и управления их завершением через системный монитор

Меню действий

Меню действий расположено справа на всех вкладках страницы редактирования



Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Доступы»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление доступа и перенаправляет на страницу **«Доступы»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления доступа
2. После подтверждения удаления доступа произойдет переход на страницу **«Доступы»** и появится уведомление Доступ «НАЗВАНИЕ_ДОСТУПА» был успешно удален

4. История изменений — отображает все изменения, выполненные для этого доступа
5. Включить\Выключить — производит включение или отключение доступа

2.6.7 Пригласительные ссылки

Пригласительные ссылки — на этой странице вы можете создавать и управлять пригласительными ссылками для удаленного подключения к устройству

Подсказка

Страница **«Пригласительные ссылки»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Важно

1. Пользователь видит только те пригласительные ссылки, которые он создал
2. Руководитель подразделения видит пригласительные ссылки других пользователей, входящих в его подразделение
3. Суперпользователь имеет доступ к просмотру всех пригласительных ссылок
4. Присутствует право «Может видеть все пригласительные ссылки», позволяющее видеть все созданные ссылки на сервере

Как это работает

Пригласительная ссылка — это ограниченная по времени и количеству использований ссылка для подключения к конкретному устройству. Используется как универсальный механизм выдачи временного доступа:

- передача доступа третьему лицу без явного назначения прав в *Доступах*
- ограничение окна действия по дате начала и сроку годности
- ограничение круга подключающихся: любое устройство, конкретное устройство, пользователь или группа

- переопределение прав подключения через выбранную группу прав

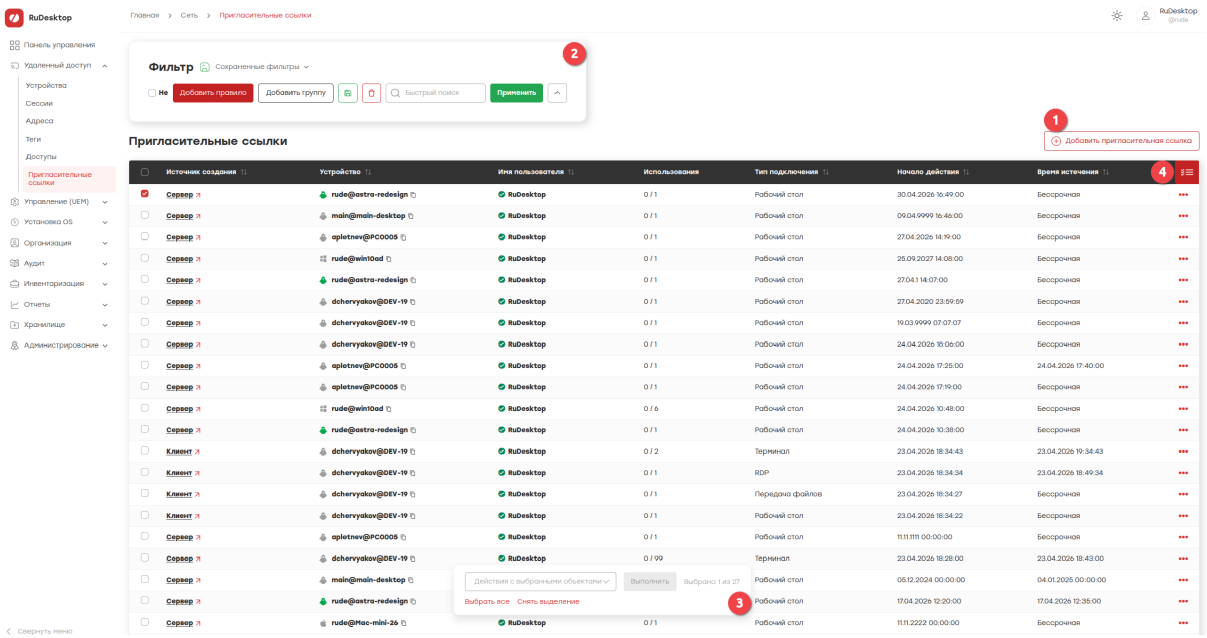
Ссылки можно создавать как в веб-интерфейсе, так и в клиенте **RuDesktop**. При создании в клиенте набор полей сокращён (нельзя задать дату начала, тип ограничения и группу прав), и ссылка автоматически привязывается к устройству-инициатору. Ссылки, созданные в веб-интерфейсе, не отображаются в клиенте, обратный путь — отображаются

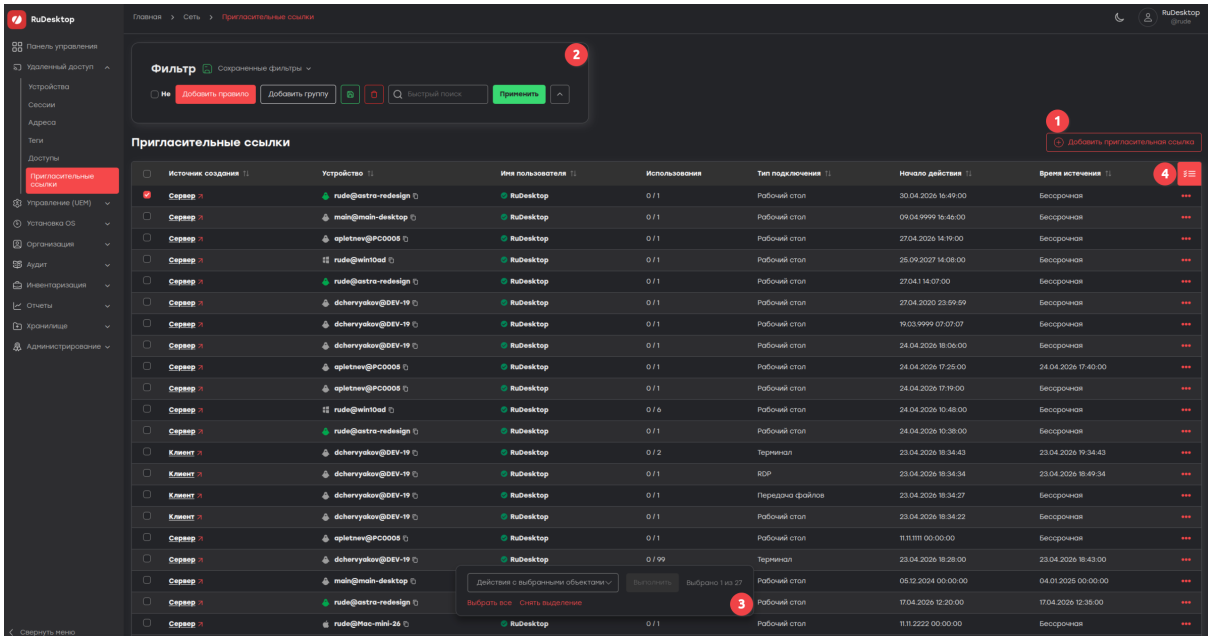
Важно

Для отображения кнопки создания ссылки в клиенте у пользователя или устройства должно быть активно право **«Может управлять приглашениями для устройств»**

Описание страницы

На странице **«Пригласительные ссылки»** отображено:





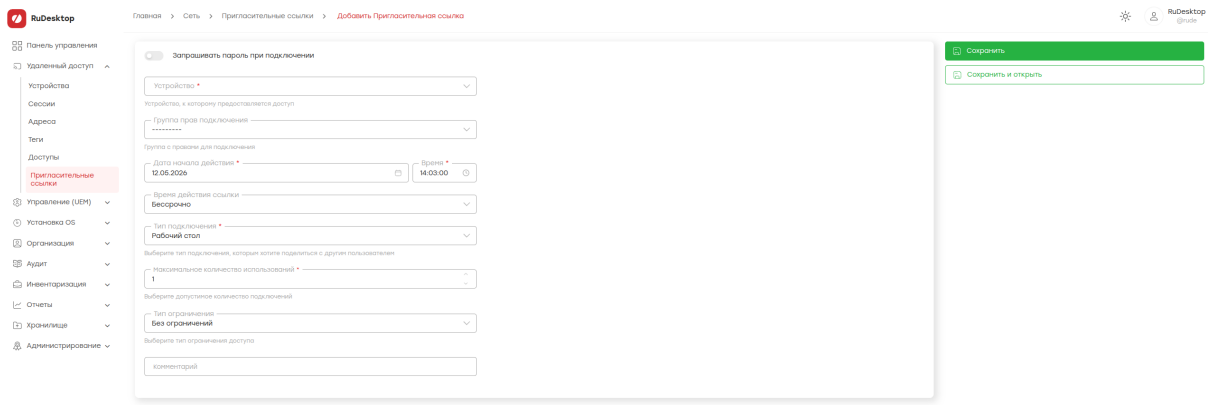
1. Кнопка Добавить пригласительная ссылка
2. Фильтр
3. Таблица с возможностью настройки отображаемых столбцов

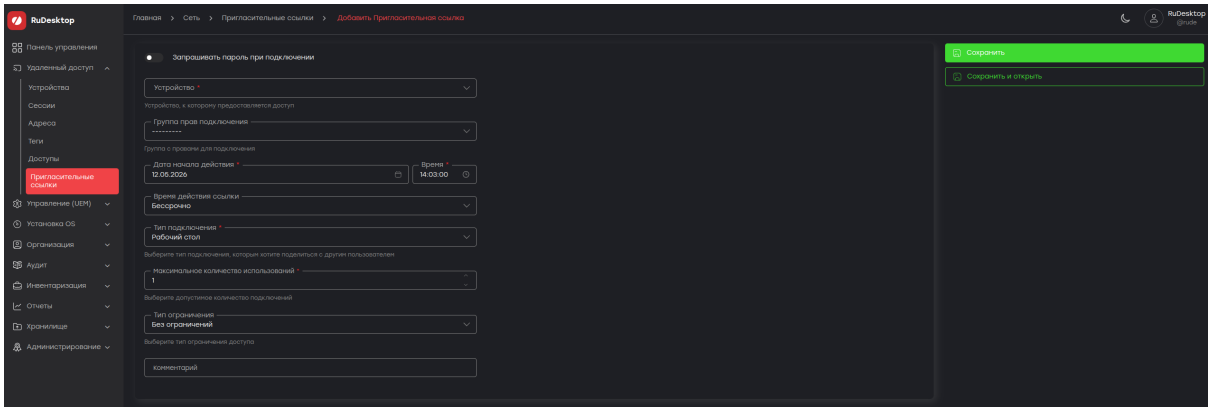
Примечание

1. Созданные ссылки можно увидеть в свойствах устройства на вкладке Приглашения. Для отображения вкладки необходимо выдать право **Может видеть пригласительные ссылки в свойствах устройства**
2. Есть возможность подключаться по пригласительной ссылке клиенту, который подключен к другому серверу. Для работы этой функции необходимо на сервере, к которому подключено устройство, с которого будет происходить подключение, предоставить право **Может подключаться к другому серверу по приглашению**. На сервере, где подключено устройство, к которому планируется подключиться, нужно выбрать группу для подключения, на которую будет создан доступ на странице **Доступы**
3. Если создать пригласительную ссылку в клиенте без выполнения входа под пользователем, то на сервере в колонке Имя пользователя будет отображаться «-»

Добавление ссылки

При нажатии на кнопку Добавить пригласительная ссылка откроется страница добавления ссылки со следующими параметрами:





1. Запрашивать пароль при подключении — параметр отвечает за то, будет ли подключение с вводом пароля или без ввода пароля

> **Важно**
>
> Если у устройства отсутствует право «Может подключаться без подтверждения со стороны пользователя», появится окно с запросом на подтверждение. После того как подключение будет подтверждено, устройство подключится без необходимости ввода пароля

> **Примечание**
>
> В облачной версии **RuDesktop** этот параметр скрыт: подключение по пригласительной ссылке всегда выполняется с запросом пароля

2. Устройство* — выбор устройства, для которого будет создана пригласительная ссылка
3. Группа прав подключения — выбор группы для переопределения прав подключения

Важно

Чтобы поле было доступно, необходимо иметь активное право **Может выбирать группу при создании ссылки для подключения**

4. Дата начала действия* — выбор даты и времени, с которой начнет действовать пригласительная ссылка
5. Время действия ссылки — выбор времени, сколько времени будет действовать пригласительная ссылка. Доступные значения: **15 минут**, **1 час**, **2 часа**, **5 часов**, **1 день**, **7 дней**, **1 месяц**
6. Тип подключения — выбор типа подключения, который будет использоваться для доступа по пригласительной ссылке. Доступные значения: **Рабочий стол**, **Передача файлов**, **RDP**, **Терминал**
7. Максимальное количество использований* — указание, сколько раз можно воспользоваться пригласительной ссылкой

Важно

Если установлено значение 1, то после одного подключения повторное подключение будет невозможно

8. Тип ограничения — выбор типа ограничения для подключения

Подсказка

- Без ограничений — возможно подключение с любого устройства, если это позволяют права доступа
- Устройство — выбор конкретного устройства, с которого можно подключиться
- Пользователь — выбор конкретного пользователя, который может подключиться
- Группа — выбор конкретной группы, которая может подключиться

Важно

Все устройства, добавленные в эту группу, смогут подключаться к устройству, указанному в пригласительной ссылке

9. Комментарий — добавление заметок или дополнительных сведений

Для добавления ссылки нужно нажать на кнопку Сохранить или Сохранить и продолжить

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. Активен — фильтрация по статусу активности ссылки
2. Отправитель — фильтрация по пользователю, создавшему ссылку
3. Начало действия — фильтрация по дате начала действия ссылки
4. Источник создания — фильтрация по источнику создания: **Клиент** или **Сервер**
5. Время истечения — фильтрация по сроку действия. Доступные значения: **Бессрочный**, **15 минут**, **1 час**, **2 часа**, **5 часов**, **1 день**, **7 дней**, **1 месяц**
6. Тип ограничения — фильтрация по типу ограничения: **Без ограничений**, **Устройство**, **Пользователь**, **Группа**

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Таблица

Таблица разбита по столбцам:

1. Источник создания — место создания ссылки: **Клиент** или **Сервер**
2. Устройство — устройство, для которого создана пригласительная ссылка
3. Имя пользователя — пользователь, создавший пригласительную ссылку
4. Использования — текущее и максимальное количество использований ссылки в формате `текущее / максимум`
5. Тип подключения — тип подключения, разрешённый для ссылки: **Рабочий стол**, **Передача файлов**, **RDP**, **Терминал**
6. Начало действия — дата и время, с которых ссылка валидна
7. Время истечения — дата и время окончания действия ссылки или значение **Бессрочная**

Операции

В строке таблицы доступны следующие действия:

1. Клик по значению в столбце Источник создания — открывает страницу свойств пригласительной ссылки для просмотра и редактирования
2. рядом с устройством в столбце Устройство — копирует URL пригласительной ссылки в буфер обмена для последующей передачи

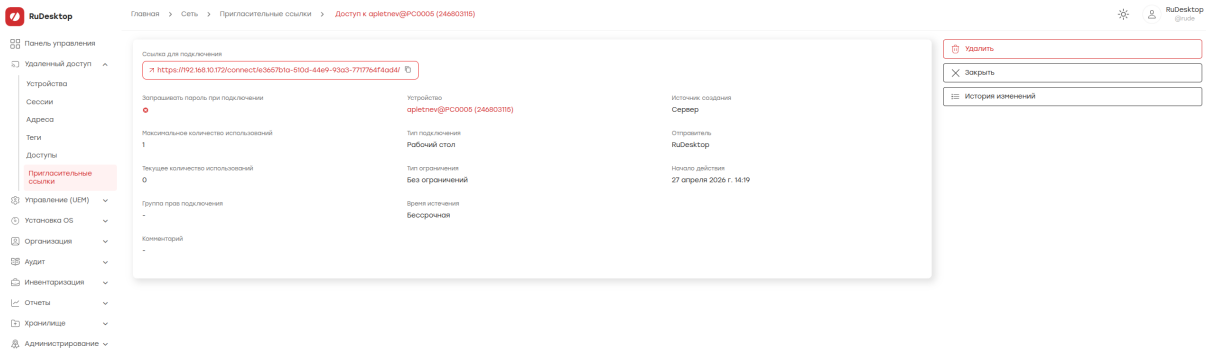
Примечание

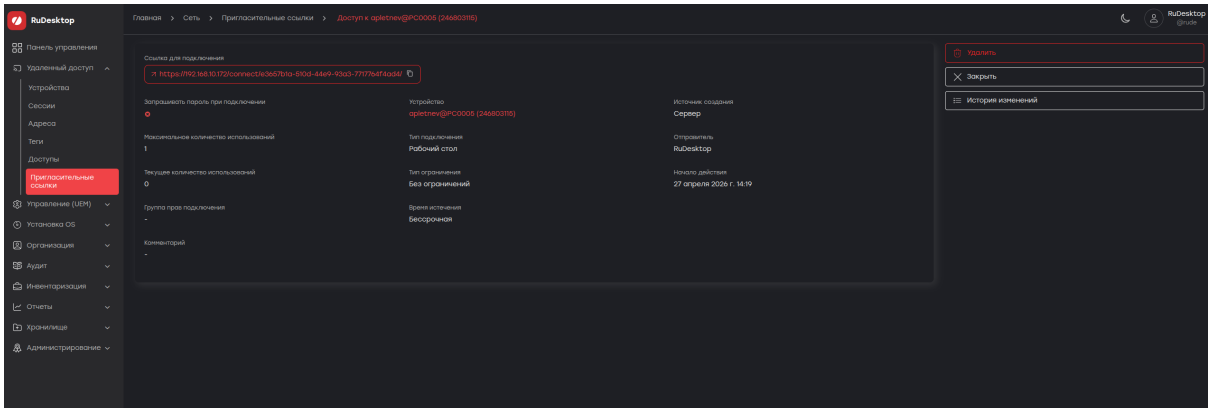
Удаление пригласительной ссылки и просмотр истории изменений выполняются со страницы свойств через *Меню действий*

Свойства пригласительной ссылки

Редактирование

При нажатии на кнопку Редактировать откроется страница свойств





На странице доступны следующие параметры:

1. Ссылка для подключения — отображение готового URL для копирования и передачи третьему лицу
2. Запрашивать пароль при подключении — параметр отвечает за то, будет ли подключение с вводом пароля или без ввода пароля
3. Отправитель — пользователь, создавший пригласительную ссылку
4. Устройство — устройство, для которого создана пригласительная ссылка
5. Группа прав подключения — группа для переопределения прав подключения
6. Дата начала действия — дата и время начала действия ссылки
7. Время действия ссылки — срок действия ссылки
8. Тип подключения — разрешённый тип подключения
9. Максимальное количество использований — лимит подключений по ссылке
10. Текущее количество использований — сколько раз ссылка уже была использована
11. Источник создания — место создания ссылки: **Клиент** или **Сервер**

12. Тип ограничения — тип ограничения для подключения
13. Комментарий — заметки или дополнительные сведения

Важно

В зависимости от прав, выданных вашему пользователю, внесение некоторых изменений может быть недоступно. Подробнее о *правах*

Меню действий

Меню действий расположено справа на странице редактирования

Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Пригласительные ссылки»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление пригласительной ссылки и перенаправляет на страницу **«Пригласительные ссылки»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления
2. После подтверждения удаления произойдет переход на страницу **«Пригласительные ссылки»** и появится уведомление об успешном удалении

4. История изменений — отображает все изменения, выполненные для этой пригласительной ссылки

Связанные кейсы

- *Управление ссылками через API v2*
- Управление пригласительными ссылками в веб-интерфейсе
- Создание пригласительной ссылки в десктопном клиенте
- Создание пригласительной ссылки в мобильном клиенте Android

Удаленный доступ — основной раздел для работы с подключенными устройствами: список устройств с их свойствами и подключениями, журнал сессий с видеозаписями, адресные книги с адресами и тегами для быстрого подключения, правила доступа (ACL) для разграничения, кто к кому может подключаться, и пригласительные ссылки для разовых подключений

Подсказка

Раздел **«Удаленный доступ»** доступен при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Устройства
Список подключенных устройств и их свойства

Сессии
Журнал удалённых сессий с видеозаписями

Адресные книги
Именованные наборы адресов и тегов с раздельным доступом

Адреса
Адреса устройств в адресных книгах для быстрого подключения

Теги
Метки для классификации адресов и упрощения поиска

Доступы
Правила, кто к каким устройствам может подключаться

Пригласительные ссылки
Одноразовые ссылки для подключения к устройству

2.7 Управление (UEM)

Доступно в УД и UEM версиях

2.7.1 Политики

Доступны в УД и UEM версиях

Шаблоны политик

Обслуживание и администрирование

Выполнить команду

Доступна только в UEM версии

Описание

Выполнить команду — политика для выполнения произвольных команд оболочки `Bash` и `PowerShell` на удалённых устройствах

Политика подходит для администрирования, устранения неполадок и автоматизации рутинных задач

Примечание

Поддерживаемые операционные системы:

- Linux
- macOS
- Windows

Важно

Данная политика предоставляет прямой доступ к командной строке устройств

Рекомендуется:

- Проводить `Тестовый запуск` на одном устройстве перед массовым применением
- Предварительно проверять команды на тестовом стенде
- Предоставлять доступ к созданию таких политик только доверенным администраторам

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Команда — команда или скрипт для выполнения на целевом устройстве

  Важно

  Поле обязательно для заполнения

  - Для Linux/macOS используйте синтаксис `Bash`

- Для Windows используйте синтаксис `PowerShell` или команды `CMD`
- Команда может быть многострочной

Остальные вкладки описаны на странице *Политики*

Пример

Для получения сводной информации о свободном месте на устройстве:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Выполнить команду»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Выполнить команду
4. Заполнить поле `Команда`

   Например: echo «Место на диске:»; df -h –output=source,size,used,avail
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
7. После применения политики:
   - В логе выполнения политики отобразится вывод команды

```
"Место на диске:",
    "Файл.система   Размер Использовано  Дост",
    "tmpfs            6,3G         2,8M  6,3G",
    "/dev/nvme0n1p6   192G         116G   67G",
    "tmpfs             32G          76M   32G",
    "tmpfs            5,0M         4,0K  5,0M",
    "efivarfs         256K         115K  137K",
    "tmpfs             32G            0   32G",
    "/dev/nvme0n1p1    96M          34M   63M",
    "tmpfs            6,3G         2,5M  6,3G"
```

Примечание

Если команда завершится с ненулевым кодом возврата, политика завершится ошибкой

В результатах выполнения будут показаны `stdout` и `stderr` команды

Добавление запланированного задания в cron

Доступна только в UEM версии

Описание

Добавление запланированного задания в cron — политика, которая позволяет создавать и настраивать периодически выполняемые задачи на Linux и macOS. На Linux используется cron, на macOS — LaunchAgent

Политика подходит для автоматизации рутинных операций: очистки временных файлов, резервного копирования, мониторинга системы и регулярного запуска скриптов

Примечание

Поддерживаемые операционные системы:

- Linux
- macOS

Важно

На Linux политика создаёт cron-задание, а на macOS — LaunchAgent выбранного пользователя. Задание выполняется с привилегиями указанного пользователя

Рекомендуется:

- Тщательно проверять команды перед добавлением в планировщик
- Указывать минимально необходимые права доступа для пользователя задания
- Тестировать задания вручную перед добавлением в cron

Примечание

Дополнительные особенности работы политики:

- Перед применением политики имя задания и значения расписания очищаются от пробелов по краям

- Если указанный пользователь не существует на устройстве, политика завершится понятной ошибкой
- На macOS создание LaunchAgent для пользователя `root` через эту политику не поддерживается
- При повторном запуске с теми же параметрами политика не создает дубликат задания, а обновляет или подтверждает существующее состояние

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

- Название задания — уникальный идентификатор задания

> **Важно**
>
> Используйте понятные названия для лёгкой идентификации задания
>
> Пробелы в начале и конце имени задания автоматически игнорируются
>
> Пример: `Check root free space`

- Команда задания — команда или скрипт для выполнения

> **Важно**
>
> Указывайте полный путь к исполняемым файлам или используйте абсолютные пути в скриптах
>
> Пример: `/usr/local/bin/backup.sh` или `bash -c "/scripts/cleanup.sh"`

- Имя пользователя — учетная запись, от имени которой будет выполняться задание

Важно

Если оставить поле пустым, по умолчанию будет использоваться пользователь `root` на Linux и активный пользователь консоли на macOS

Для повышения безопасности рекомендуется использовать непривилегированных пользователей

Если указать несуществующего пользователя, политика завершится ошибкой

На macOS нельзя использовать пользователя `root` для создания LaunchAgent через эту политику

- Минуты — минута выполнения задания (0-59)

Примечание

Оставьте пустым для выполнения каждую минуту (*)

Примеры: `0` (в начале часа), `30` (в половине), `*/15` (каждые 15 минут)

На macOS через LaunchAgent поддерживаются только * или одно числовое значение

- Часы — час выполнения задания (0-23)

Примечание

Оставьте пустым для выполнения каждый час (*)

Примеры: `0` (полночь), `12` (полдень), `2` (2 часа ночи)

На macOS через LaunchAgent поддерживаются только * или одно числовое значение

- День недели — день недели выполнения (0-6, где 0 - воскресенье)

Примечание

Оставьте пустым для выполнения каждый день (*)

Примеры: `1` (понедельник), `6` (суббота), `0` (воскресенье)

На macOS через LaunchAgent поддерживаются только * или одно числовое значение

- Месяц — месяц выполнения задания (1-12)

Примечание

Оставьте пустым для выполнения каждый месяц (*)

Примеры: 1 (январь), 12 (декабрь), */3 (каждые 3 месяца)

На macOS через LaunchAgent поддерживаются только * или одно числовое значение

Остальные вкладки описаны на странице *Политики*

Пример

Для настройки ежедневной очистки временных файлов в 2:30 ночи:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Добавление запланированного задания в cron»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Ежедневная очистка временных файлов
4. Заполнить поле `Название задания`

   Например: Cleaning temporary system files
5. Заполнить поле `Команда задания`

   Например: find /tmp -type f -mtime +7 -delete
6. Заполнить поле `Имя пользователя`

   Например: root на Linux или rude на macOS

   Примечание

   Для операций с системными файлами на Linux могут потребоваться права root

   На macOS указывайте обычного пользователя, для которого нужно создать LaunchAgent
7. Заполнить поле `Минуты`

   Например: 30
8. Заполнить поле `Часы`

   Например: 2
9. Поля `День недели` и `Месяц` оставить пустыми
10. Нажать на кнопку Сохранить
11. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики

12. После применения политики:
    - На Linux будет создано cron-задание, а на macOS — LaunchAgent с параметрами задания `Cleaning temporary system files`
    - Задание будет выполняться каждый день в 2:30 ночи
    - Будут удаляться файлы в директории `/tmp`, созданные более 7 дней назад
    - Для macOS в результате выполнения будут показаны статус и путь файла LaunchAgent и launcher-скрипта

Предупреждение

При настройке cron-заданий учитывайте:

- Cron не имеет доступа к переменным окружения пользователя (*PATH*, *HOME* и т.д.)
- Всегда указывайте полные пути к исполняемым файлам
- Для отладки полезно перенаправлять вывод команд в лог-файлы
- Регулярно проверяйте выполнение заданий через системные логи (`/var/log/cron` или `/var/log/syslog`)
- На macOS LaunchAgent создается только для конкретного пользователя, поэтому при смене пользователя задание нужно создать заново

Удаление запланированного задания из cron

Доступна только в UEM версии

Описание

Удаление запланированного задания из cron — политика, которая позволяет удалить ранее созданную периодическую задачу на устройствах под управлением Linux и macOS. На Linux удаляется запись из cron, на macOS — соответствующий LaunchAgent.

Эта политика удобна для отключения устаревших заданий, остановки временной автоматизации и очистки задач, которые больше не должны запускаться на устройстве.

Примечание

Поддерживаемые операционные системы:

- Linux
- macOS

Важно

На Linux политика удаляет cron-задание, а на macOS — LaunchAgent выбранного пользователя. Чтобы удалить именно ту задачу, которая была создана политикой добавления, укажите то же значение поля `Название задания` и того же пользователя, что использовались при создании

Рекомендуется:

- Перед удалением проверить имя задания в исходной политике или на устройстве
- Указывать того же пользователя, от имени которого создавалось задание
- Учитывать, что на macOS для неактивного пользователя удаление файлов будет выполнено сразу, а выгрузка из сессии может потребовать повторного входа

Примечание

Дополнительные особенности работы политики:

- Перед удалением имя задания очищается от пробелов по краям
- Если указанный пользователь не существует на устройстве, политика завершится понятной ошибкой
- На macOS удаление LaunchAgent для пользователя `root` через эту политику не поддерживается
- При повторном запуске для уже удаленного задания политика завершится успешно и сообщит, что изменения не потребовались

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Название задания — уникальный идентификатор задания в cron или LaunchAgent

> **Важно**
>
> Укажите то же имя, которое использовалось при создании задания
>
> Пробелы в начале и конце имени задания автоматически игнорируются
>
> Пример: `Cleaning temporary system files`

- Имя пользователя — учетная запись, у которой нужно удалить задание

> **Важно**
>
> Если оставить поле пустым, по умолчанию будет использоваться пользователь `root` на Linux и активный пользователь консоли на macOS
>
> На macOS рекомендуется указывать того же обычного пользователя, для которого ранее создавался LaunchAgent
>
> Если указать несуществующего пользователя, политика завершится понятной ошибкой
>
> На macOS нельзя использовать пользователя `root` для удаления LaunchAgent через эту политику

Остальные вкладки описаны на странице *Политики*

Пример

Для удаления задания ежедневной очистки временных файлов:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Удаление запланированного задания из cron»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Удаление ежедневной очистки временных файлов
4. Заполнить поле `Название задания`

   Например: Cleaning temporary system files
5. Заполнить поле `Имя пользователя`

   Например: root на Linux или rude на macOS
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
8. После применения политики:

- На Linux запись задания будет удалена из cron пользователя
- На macOS будут удалены файлы LaunchAgent и launcher-скрипта для задания `Cleaning temporary system files`
- Если LaunchAgent был загружен в активную сессию пользователя, он будет выгружен автоматически
- При повторном запуске для уже удаленного задания политика сообщит, что задание уже отсутствовало и изменения не потребовались

Предупреждение

При удалении запланированных заданий учитывайте:

- Политика удаляет задачу по имени, поэтому важно указать точное значение поля `Название задания`
- На macOS удаление относится только к LaunchAgent, созданному для конкретного пользователя
- Если на macOS задание было загружено в сессии неактивного пользователя, для полного прекращения работы может потребоваться повторный вход
- В результатах выполнения для macOS отображаются статус и путь файла LaunchAgent и launcher-скрипта, чтобы было проще проверить итоговое состояние

Изменение состояния службы

Доступна только в UEM версии

Описание

Изменение состояния службы - политика для управления системными службами на Windows и Linux. Политика подходит для запуска и остановки служб при обслуживании устройства и применении изменений конфигурации

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux с systemd

Важно

Управление системными службами может повлиять на работоспособность устройства

Рекомендуется:

- Останавливать только те службы, в назначении которых вы уверены
- Тестировать изменения на нерабочих устройствах перед применением на рабочих
- Иметь план отката на случай непредвиденных проблем

Свойства политики

После выбора шаблона политики откроется окно с её свойствами. Вкладка **«Политика»** содержит следующие поля:

- Название - имя политики в системе

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Имя службы - название одной или нескольких служб для управления

  Важно

  Можно выбрать одну или несколько служб из списка или ввести названия вручную

  Указывать системное имя службы, а не её отображаемое описание

  - Примеры для Windows: `Spooler`, `wuauserv`, `WSearch`
  - Примеры для Linux: `sshd`, `nginx`, `postgresql`

- Действие - операция для выполнения над службой
  - **Запустить** - запускает указанные службы
  - **Остановить** - останавливает указанные службы

Остальные вкладки описаны на странице *Политики*

Пример

Для запуска службы печати на Windows-устройстве:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Изменение состояния службы»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Запуск службы печати

4. Заполнить поле `Имя службы`

   Например: Spooler

   > **Примечание**
   >
   > Для поиска службы можно начать вводить ее название и выбрать из списка предложенных

5. В поле **«Действие»** выбрать нужную операцию

   Например: Запустить

6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики

Проверка результата

Политика применяет выбранное действие ко всем указанным службам и проверяет их состояние. Успешный результат означает, что проверка подтвердила требуемое состояние каждой службы. Если состояние хотя бы одной службы подтвердить не удалось, выполнение завершается с ошибкой. Открыть результат выполнения на нужном устройстве и проверить, какая служба не перешла в требуемое состояние

Проверить правильность имени службы и её наличие на устройстве, затем устранить причину ошибки и повторить запуск

> **Примечание**
>
> Политика также обновляет сведения о службах в инвентаризации
>
> Ошибка обновления инвентаризации сама по себе не отменяет выполненный запуск или остановку службы
>
> Если сведения в карточке не обновились, проверить состояние непосредственно на устройстве и повторить сбор инвентаризации

> **Предупреждение**
>
> Если изменить состояние одной из служб не удалось, другие уже могли изменить состояние
>
> Общая ошибка не означает, что все службы остались в исходном состоянии

> **Примечание**
>
> **Как найти имена служб:**

- **Windows:** Открыть **«Службы»** (`services.msc`) или выполнить `sc.exe query` в командной строке
- **Linux:** Выполнить `systemctl list-unit-files --type=service`

Предупреждение

Важные предупреждения:

- Остановка критических системных служб может привести к неработоспособности устройства
- Некоторые службы имеют зависимости, их остановка может повлиять на другие службы
- Запуск и остановка происходят во время выполнения политики

Инвентаризация

Доступна в УД и UEM версиях

Описание

Инвентаризация — политика для сбора данных с удалённого устройства

Состав собираемых данных зависит от выбранных типов и операционной системы устройства

Например, можно собирать сведения об установленном ПО, службах, плагинах браузеров, аппаратной части устройства и проверять наличие указанных файлов или директорий

Плагины собираются из браузеров Google Chrome, Microsoft Edge, Яндекс Браузер, Chromium, Chromium-Gost, Opera и Mozilla Firefox. Chromium-Gost из репозитория ALT хранит профили в `~/.config/chromium-gost`. Сборка Chromium-Gost с сайта разработчика хранит профили в каталоге Chromium, поэтому плагины из этого каталога относятся к Chromium-Gost, если на устройстве установлен он, а не Chromium. Читаются все профили браузеров всех пользователей устройства; отключённые плагины не собираются

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux
- macOS

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Выберите типы данных для сбора — набор категорий инвентаризации, которые нужно собрать с устройства

  Примечание

  Набор доступных данных зависит от операционной системы устройства

  Чем больше выбранных категорий, тем больше сведений будет обновлено в инвентаризации

- Наличие путей — в этом поле указываются пути к искомым директориям или файлам

  Примечание

  Пути разделяются переводом строки

  Проверка путей используется вместе с выбором соответствующего типа данных для сбора

Остальные вкладки описаны на странице *Политики*

Пример

Для сбора данных с устройств, подключенных к серверу, необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**

2. Выбрать шаблон политики **«Инвентаризация»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Инвентаризация
4. При необходимости выбрать значения в поле `Выберите типы данных для сбора`

   Например: Установленные приложения, Службы, Наличие путей
5. При необходимости заполнить поле `Наличие путей`

   Например:

   ```
   /opt/application
   /etc/application/config.yaml
   ```
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
8. После применения политики:
   - Будут собраны выбранные типы данных об устройстве
   - При заполнении поля `Наличие путей` будет проверено существование указанных файлов и директорий

Мониторинг запуска приложений

Доступна только в UEM версии

Описание

Мониторинг запуска приложений — политика для настройки аудита запуска исполняемых файлов на Linux-устройствах с помощью `auditd`

Политика подходит для отслеживания запуска программ пользователями в задачах безопасности и аудита

Примечание

Поддерживаемые операционные системы:

- Linux

Важно

Эта политика настраивает системный демон аудита

Рекомендуется:

- Настраивать мониторинг только на необходимых устройствах

- Проверять, что на устройстве достаточно места для логов аудита
- Регулярно архивировать и очищать логи аудита

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

- Идентифицирующий ключ — уникальный ключ для пометки записей в логах аудита

> **Важно**
>
> Ключ помогает фильтровать записи, относящиеся именно к этому правилу мониторинга

- Состояние auditd — выбор состояния демона аудита
  - **Включено** — демон `auditd` будет запущен и настроен на автозапуск
  - **Выключено** — политика попытается остановить демон `auditd`

> **Важно**
>
> На дистрибутивах семейства RPM (RedOS, RedHat, AlterOS, MSVSphere) и Alt Linux служба `auditd` никогда не останавливается — даже при выборе значения `Выключено` политика оставит демон запущенным и в автозапуске, и будет отключён только сборщик логов

- Состояние сборщика — выбор режима работы сборщика логов
  - **Включить слежение за логом** — начнется сбор и отправка логов аудита
  - **Отключить слежение за логом** — сбор логов аудита будет прекращен

Примечание

Если для поля `Состояние auditd` выбрано значение `Выключено`, политика принудительно отключит и сборщик логов

Остальные вкладки описаны на странице *Политики*

Пример

Для настройки мониторинга запуска приложений в каталоге `/usr/bin/`:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Мониторинг запуска приложений»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Мониторинг запуска приложений в каталоге /usr/bin/
4. Заполнить поле `Идентифицирующий ключ`

   Например: monitoring_app_launch

   Примечание

   Ключ появится в логах аудита рядом с записями о запуске программ
5. Выбрать состояние `Состояние auditd`

   Например: Включено
6. Выбрать состояние `Состояние сборщика`

   Например: Включить слежение за логом
7. Нажать на кнопку Сохранить
8. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
9. После применения политики:
   - На устройстве будет установлен и настроен `auditd`
   - Будут созданы правила аудита для отслеживания запуска программ из `/usr/bin/`
   - Демон `auditd` будет запущен
   - Начнется сбор логов

Примечание

Что отслеживается:

- Запуск любых программ из каталога `/usr/bin/`
- Только действия пользователей с UID >= 1000
- Системные вызовы `execve`

Предупреждение

После включения мониторинга проверьте, что на устройстве достаточно свободного места, так как логи аудита могут быстро расти при активном использовании системы

На части Linux-дистрибутивов остановка `auditd` может быть ограничена системной политикой, поэтому служба может остаться активной даже при выборе значения `Выключено`

Сборщик лога

Доступна только в UEM версии

Описание

Сборщик лога — политика для настройки сбора и отправки логов из указанных файлов на устройствах

Политика подходит для централизованного сбора логов приложений и системных событий при диагностике, аудите и разборе инцидентов

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

Эта политика настраивает сбор логов через клиент **RuDesktop**

Рекомендуется:

- Настраивать сбор только тех логов, которые действительно нужны
- Проверять корректность указанных путей к файлам
- Учитывать нагрузку на сеть при сборе объемных логов

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

- Путь — полный путь к файлу лога для сбора

> **Подсказка**
>
> Укажите абсолютный путь к файлу лога
>
> Примеры:
>
> - Windows: `C:\Program Files\Application\logs\app.log`
> - Linux: `/var/log/application/app.log`
> - macOS: `/Library/Logs/Application/app.log`

- Состояние — выбор режима работы сборщика логов
  - **Включить слежение за логом** — начнется сбор и отправка указанного лога на сервер **RuDesktop**

> **Примечание**
>
> После применения политики playbook проверяет, что путь к файлу появился в конфигурации сборщика логов

  - **Отключить слежение за логом** — сбор указанного лога будет прекращен

Остальные вкладки описаны на странице *Политики*

Пример

Для настройки сбора лога приложения из файла `/var/log/myapp/application.log` на Linux-устройстве:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Сборщик лога»** из списка предложенных шаблонов
3. Заполнить поле `Название`

Например: Сбор лога приложения MyApp

4. Заполнить поле `Путь`

   Например: /var/log/myapp/application.log

5. Выбрать состояние `Состояние`

   Например: Включить слежение за логом

6. Нажать на кнопку Сохранить

7. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики

8. После применения политики:

   - На удаленном устройстве будет создана или обновлена конфигурация сборщика логов

```
[[collectors]]
path = '/var/log/myapp/application.log'
initial_buffer_size = 8192

Где initial_buffer_size - размер внесенных изменений,␣
↪при которых данные будут отправляться на сервер
```

   Данный конфигурационный файл находится по пути:

   Windows

```
C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\
↪RuDesktop\config\RuDesktop_logcollect.toml
```

   Linux

```
/root/.config/RuDesktop/RuDesktop_logcollect.toml
```

   Также playbook может использовать один из пользовательских каталогов `/home/*/.config/RuDesktop` или `/home/*/.config/rudesktop`

   Если на устройстве осталась конфигурация старого формата, при проверке также учитывается файл `RuDesktop_logconnect.toml`

   macOS

```
/private/var/root/Library/Preferences/ru.desktop.
↪RuDesktop/RuDesktop_logcollect.toml
```

Для просмотра новых записей в логе:

1. Перейти на страницу *Все логи* в веб-интерфейсе сервера **RuDesktop**
2. В фильтре добавить правило Тип события и выбрать Строка лога
3. Нажать на кнопку Применить фильтр

После этого отобразятся новые строки, которые были добавлены в лог-файл с момента запуска политики

Управление SSH-ключами пользователя

Доступна только в UEM версии

Описание

Управление SSH-ключами пользователя — политика для добавления или удаления публичных SSH-ключей пользователей на Linux и macOS

Политика подходит для централизованного управления доступом по SSH без пароля

Примечание

Поддерживаемые операционные системы:

- Linux
- macOS

Важно

SSH-ключи предоставляют доступ к устройству без ввода пароля

Рекомендуется:

- Хранить приватные SSH-ключи в безопасном месте
- Регулярно обновлять и ротировать SSH-ключи
- Удалять неиспользуемые или скомпрометированные ключи
- По возможности использовать ключи с парольной фразой

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Имя пользователя — учётная запись пользователя, для которой управляются SSH-ключи

> **Важно**
>
> Пользователь должен существовать на целевом устройстве
>
> Пример: `deploy`, `admin`, `user`

- Действие — операция для SSH-ключа
  - **Добавить** — добавляет указанный публичный SSH-ключ пользователю
  - **Удалить** — удаляет указанный публичный SSH-ключ у пользователя
- Публичный SSH-ключ — содержимое публичного SSH-ключа

> **Важно**
>
> Для добавления укажите полное содержимое публичного ключа
>
> Для удаления укажите тот же ключ, который был добавлен ранее
>
> Пример: `ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC... user@host`

Остальные вкладки описаны на странице *Политики*

Пример

Для добавления SSH-ключа пользователю `deploy`:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Управление SSH-ключами пользователя»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Добавление SSH-ключа для пользователя deploy
4. Заполнить поле `Имя пользователя`

   Например: deploy
5. Выбрать действие `Действие`

   Например: Добавить
6. Заполнить поле `Публичный SSH-ключ`

   Пример формата: `ssh-rsa <данные ключа> user@deploy-host`

Примечание

Ключ должен быть в однострочном формате. Обычно это содержимое файла `id_rsa.pub` или `id_ed25519.pub`

7. Нажать на кнопку Сохранить
8. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
9. После применения политики:
    - На устройстве будет создана директория `~/.ssh` (если не существует) с правами 0700
    - Будет создан или обновлён файл `~/.ssh/authorized_keys` с правами 0600
    - Указанный SSH-ключ будет добавлен в файл `authorized_keys`
    - Владельцем файлов будет указанный пользователь
    - Пользователь сможет подключаться по SSH с соответствующего приватного ключа

Для удаления SSH-ключа у пользователя `deploy`:

1. Заполнить поле `Название`

    Например: Удаление SSH-ключа пользователя deploy
2. Заполнить поле `Имя пользователя`

    Например: deploy
3. Выбрать действие `Действие`

    Например: Удалить
4. Заполнить поле `Публичный SSH-ключ`

    Пример формата: `ssh-rsa <данные ключа> user@deploy-host`

Важно

Для удаления необходимо указать точно такой же ключ, который был добавлен ранее

5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики

Примечание

Расположение файлов SSH-ключей:

- **Linux:** `/home/<username>/.ssh/authorized_keys`

- **macOS:** `/Users/<username>/.ssh/authorized_keys`

Формат SSH-ключа: `<тип_ключа> <содержимое_ключа> <комментарий>`

Предупреждение

Важные предупреждения:

- Публичный SSH-ключ должен быть в корректном формате
- При добавлении дублирующихся ключей они будут проигнорированы
- Удаление ключа работает только при точном совпадении всего содержимого ключа
- При удалении несуществующего ключа операция завершится успешно
- Убедитесь, что пользователь существует на целевом устройстве
- На macOS домашняя директория всегда имеет путь `/Users/<username>`

Управление sudoers

Доступна только в UEM версии

Описание

Управление sudoers — политика для управления правами sudo пользователей и групп на Linux и macOS

Политика подходит для выдачи ограниченных привилегий root без полного доступа к учетной записи root

Примечание

Поддерживаемые операционные системы:

- Linux
- macOS

Важно

Настройка прав sudo предоставляет пользователям частичные привилегии root

Рекомендуется:

- Предоставлять минимально необходимые права для выполнения задач
- Использовать группы вместо отдельных пользователей
- Регулярно пересматривать и обновлять права sudo

- Для критических команд требовать ввод пароля

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

- Название права — уникальный идентификатор правила sudoers

> **Важно**
>
> Используйте понятные названия для лёгкой идентификации правила
>
> Пример: `Monitoring_access`, `Backup_privileges`, `Network_admin`

- Группа пользователей — группа Linux/macOS, которой предоставляются права

> **Примечание**
>
> Для действия `Добавить право` поле обязательно
>
> Для действия `Удалить право` поле можно оставить пустым
>
> Пример: `developers`, `admins`, `monitoring`

- Действие — операция для правила sudoers
  - **Добавить право** — создает новое правило sudoers с указанными параметрами
  - **Удалить право** — удаляет существующее правило sudoers по его названию
- Команды — список команд, которые можно выполнять с правами sudo

> **Важно**
>
> Для действия `Добавить право` нужно указать хотя бы одну команду

Указывайте полные пути к исполняемым файлам. Каждую команду указывайте с новой строки

Примеры:

- `/usr/bin/systemctl restart nginx`
- `/usr/bin/cat /var/log/syslog`
- `ALL` (полный доступ)

- Не требовать пароль для sudo — опция отключения запроса пароля

Примечание

Если опция активна, пользователи смогут выполнять sudo-команды без ввода пароля

Рекомендуется отключать для критических команд

Остальные вкладки описаны на странице *Политики*

Пример

Для предоставления группе `developers` прав на перезапуск веб-сервера:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Управление sudoers»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Права перезапуска nginx для разработчиков
4. Заполнить поле `Название права`

   Например: nginx_restart_access

   Примечание

   Пробелы в названии будут автоматически заменены на подчеркивания
5. Заполнить поле `Группа пользователей`

   Например: developers
6. Выбрать действие `Действие`

   Например: Добавить право
7. Заполнить поле `Команды`

   Например:

```
/usr/bin/systemctl restart nginx
/usr/bin/systemctl status nginx
```

Важно

Каждая команда должна быть на отдельной строке

8. Отключить опцию `Не требовать пароль для sudo` (оставить неактивной)
9. Нажать на кнопку Сохранить
10. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
11. После применения политики:
    - В файле `/etc/sudoers.d/nginx_restart_access` будет создано правило
    - Члены группы `developers` смогут выполнять `sudo systemctl restart nginx` и `sudo systemctl status nginx`
    - При выполнении команд будет запрашиваться пароль пользователя

Для удаления права:

1. Заполнить поле `Название`

   Например: Удаление прав nginx_restart_access
2. Заполнить поле `Название права`

   Например: nginx_restart_access

Важно

Указывайте точно такое же название, какое использовалось при создании

3. Поля `Группа пользователей`, `Команды` можно оставить пустыми
4. Выбрать действие `Действие`

   Например: Удалить право
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики

Примечание

Расположение правил sudoers:

- Правила создаются в директории `/etc/sudoers.d/`

- Имя файла соответствует `Названию права` с заменой пробелов на подчеркивания
- Формат правила для группы: `%группа ALL=(ALL) /путь/к/команде`
- Если включена опция `Не требовать пароль для sudo`, в правило добавляется `NOPASSWD:`

Пример созданного правила:

```
# nginx_restart_access
%developers ALL=(ALL) /usr/bin/systemctl restart nginx
%developers ALL=(ALL) /usr/bin/systemctl status nginx
```

Предупреждение

Важные предупреждения:

- Неправильная настройка sudoers может заблокировать доступ к системе
- Правила в `/etc/sudoers.d/` должны иметь права `0440`
- Использование `ALL` предоставляет полные привилегии root
- Опция `NOPASSWD` снижает безопасность, используйте её только когда это действительно нужно
- Всегда проверяйте синтаксис правил с помощью `visudo -c`
- Удаление права удаляет весь файл правила, а не отдельные команды

Инвентаризация Android

Доступна только в MDM версии

Описание

Инвентаризация Android — политика, которая собирает инвентаризационные данные с Android-устройства через MDM-механизм

Политика используется для обновления сведений об аппаратной части, установленном программном обеспечении и контроля состояния управляемых Android-устройств

При выполнении политики собираются:

- Сведения о процессоре, материнской плате и объёме оперативной памяти
- Версия операционной системы и идентификатор устройства
- Список установленных приложений с их версиями

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующее поле:

- Название — имя политики в системе

Примечание

Дополнительные параметры для этой политики не требуются

Остальные вкладки описаны на странице *Политики*

Пример

Для запуска инвентаризации Android-устройства:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Инвентаризация Android»**
3. Заполнить поле `Название`

   Например: Инвентаризация корпоративных смартфонов
4. Нажать на кнопку Сохранить
5. Выполнить `Тестовый запуск` на устройстве Android
6. После применения политики:
   - RuDesktop обновит инвентаризационные данные устройства
   - Сведения о процессоре, материнской плате, оперативной памяти, операционной системе и установленном ПО будут актуализированы

Где посмотреть результат

После успешного выполнения открыть *свойства устройства* и проверить обновлённые сведения об оборудовании и установленном ПО. Ресурсы устройства также доступны в разделе *Инвентаризация*.

Сведения о производителе и модели Android-устройства учитываются в данных материнской платы.

Предупреждение

Важные предупреждения:

- Если устройство недоступно или MDM-команды не отвечают, инвентаризация может не обновиться
- Состав собираемых данных зависит от возможностей Android-агента
- Рекомендуется выполнять инвентаризацию после изменений в составе приложений на устройстве

Выполнить команду
Запуск произвольной команды на устройстве

Добавление запланированного задания в cron
Создание задания cron на Linux/macOS-устройстве

Удаление запланированного задания из cron
Удаление задания cron с устройства

Изменение состояния службы
Запуск, остановка или перезапуск службы на устройстве

Инвентаризация
Сбор данных о ПО и оборудовании устройства

Мониторинг запуска приложений
Контроль запуска указанных приложений на устройстве

Сборщик лога
Сбор логов клиента RuDesktop с устройства

Управление SSH-ключами пользователя
Добавление и удаление SSH-ключей у локального пользователя

Управление sudoers
Настройка прав sudo для пользователей

Инвентаризация Android
Сбор данных с Android-устройства

Обслуживание сервера RuDesktop

Обслуживание сервера

Доступна в УД и UEM версиях

Описание

Обслуживание сервера — политика для очистки истории логов сервера и удаления устаревших видеозаписей сессий, если они старше заданного периода

Политика выполняется локально на сервере **RuDesktop** и запускает встроенные команды обслуживания сервера: *maintain* для логов и *clean_video_records* для видеозаписей

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

- История логов (дни) — количество дней от текущей даты, за которые логи удаляться не будут

> **Важно**
>
> Поле является необязательным
>
> Если не заполнить данное поле, то политика отработает со значением по умолчанию, равным 30 дням

- Видеозаписи (дни) — количество дней от текущей даты, за которые видеозаписи сессий удаляться не будут

> **Важно**
>
> Поле является необязательным
>
> Значение `0` или незаполненное поле отключают очистку видеозаписей: политика обработает только логи

Опасно

Видеозаписи удаляются с сервера безвозвратно. Перед первым запуском убедитесь, что указанный срок хранения соответствует принятым в организации требованиям

Оба поля принимают целые числа не меньше нуля. Текущий объём и количество видеозаписей можно посмотреть в разделе **Администрирование** → *Настройки*, блок **Видеозаписи**

Остальные вкладки описаны на странице *Политики*

Пример

Для очистки логов сервера и устаревших видеозаписей необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Обслуживание сервера»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Обслуживание сервера
4. При необходимости заполнить поле `История логов (дни)`

   Например: 30
5. При необходимости заполнить поле `Видеозаписи (дни)`

   Например: 90
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` для проверки работоспособности политики
8. После применения политики:
   - На сервере будет запущена команда обслуживания с указанным сроком хранения логов
   - Будут удалены видеозаписи сессий старше указанного срока, а в отчёте о выполнении отобразятся оба срока хранения

Резервное копирование базы данных

Доступна в УД и UEM версиях

Описание

Резервное копирование базы данных — политика для создания локальной резервной копии основной базы данных сервера **RuDesktop**. Политика выполняется на самом сервере, а расписание задаётся через стандартный механизм заданий политик.

В копию не входят файлы репозиториев, видеозаписи, конфигурация сервера, база аналитики и внешние хранилища.

Свойства политики

После выбора шаблона политики откроются её свойства.

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики
- Каталог резервных копий — абсолютный путь к локальному каталогу на сервере
- Удалять старые резервные копии — включает автоматическое удаление копий после успешного создания новой
- Срок хранения (дни) — возраст копий, после которого они будут удалены; при включённом удалении значение должно быть не меньше 1

По умолчанию копии сохраняются в `/var/backups/rudesktop`. Этот каталог не удаляется при удалении пакета RuDesktop. Файлы получают имя вида `rudesktop-2026-10-19_02-00-00.sql.gz`.

Важно

Указанный каталог должен быть доступен для записи сервисному пользователю **RuDesktop**. Автоматическая очистка затрагивает только обычные файлы с именами указанного выше формата в этом каталоге. Нельзя сохранять резервные копии в каталоги, содержимое которых раздаётся веб-сервером RuDesktop: `/var/lib/rudesktop/pxe`, `/var/lib/rudesktop/media` и `/usr/share/rudesktop/public`, включая их подкаталоги.

Настройка расписания

1. Создайте политику из шаблона **«Резервное копирование базы данных»**
2. Укажите локальный каталог и параметры хранения
3. Сохраните политику и выполните тестовый запуск
4. Создайте для политики задание и выберите требуемое расписание

Результат создания копии и ошибки выполнения доступны в журнале задания.

Очистка устройств

Доступна в УД и UEM версиях

Описание

Очистка устройств — политика для удаления из базы данных сервера **RuDesktop** устройств в одном из двух режимов:

- Удаление только обычных устройств, которые не были активны в течение заданного количества дней
- Удаление только SSH-устройств (заглушек, добавленных через импорт устройств), на которых не установлен клиент **RuDesktop**

> **Важно**
>
> Одновременное удаление обычных и SSH-устройств этой политикой не предусмотрено

> **Важно**
>
> Параметр задается в настройках политики

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

  > **Важно**
  >
  > Для выполнения или сохранения политики название обязательно для заполнения

- Последняя активность — последняя активность устройства, в днях от текущей даты

  > **Важно**
  >
  > Устройства, которые последний раз были активны более указанного значения, будут удалены

- Удаление SSH устройств — переключает режим работы политики
  - Если выбрано Не удалять, будут удаляться только обычные устройства по фильтру Последняя активность
  - Если выбрано Удалить, будут удаляться только SSH-устройства (заглушки, добавленные через импорт устройств), на которых не установлен клиент **RuDesktop**

Остальные вкладки описаны на странице *Политики*

Пример

Для удаления только обычных устройств необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Очистка устройств»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Очистка устройств
4. При необходимости заполнить поле `Последняя активность`
5. Выбрать в поле `Удаление SSH устройств` -> `Не удалять`
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` для проверки работоспособности политики
8. После применения политики:
   - С сервера будут удалены только обычные устройства, которые не были активны в течение последних 30 дней

Для удаления только SSH-устройств необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Очистка устройств»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Очистка SSH-устройств
4. При необходимости заполнить поле `Последняя активность`

   Например: 30
5. Выбрать в поле `Удаление SSH устройств` -> `Удалить`
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` для проверки работоспособности политики
8. После применения политики:
   - С сервера будут удалены только SSH-устройства (заглушки, добавленные через импорт устройств), на которых не установлен клиент **RuDesktop**

Синхронизация со службой каталогов

Доступна в УД и UEM версиях

Описание

Синхронизация со службой каталогов — политика для запуска синхронизации со всеми активными доменами, настроенными на сервере **RuDesktop**

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

Остальные вкладки описаны на странице *Политики*

Пример

Для синхронизации с добавленными доменами необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Синхронизация со службой каталогов»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Синхронизация со службой каталогов
4. Нажать на кнопку Сохранить
5. Выполнить `Тестовый запуск` для проверки работоспособности политики
6. После применения политики:
   - Произойдёт синхронизация со всеми подключенными *доменами* к серверу **RuDesktop**

Обслуживание сервера

Очистка истории логов сервера и устаревших видеозаписей сессий

Резервное копирование базы данных

Создание локальных резервных копий основной базы данных сервера по расписанию

Очистка устройств

Удаление неактивных устройств с сервера по периоду неактивности

Синхронизация со службой каталогов

Запуск синхронизации с активными доменами LDAP по расписанию

Управление безопасностью и доступом

Блокировка USB-накопителей

Доступна только в UEM версии

Описание

Блокировка USB-накопителей — политика для управления доступом к USB-устройствам хранения данных на устройствах под управлением Windows и Linux

Политика помогает предотвратить несанкционированное копирование данных, заражение устройств через USB-носители и утечку конфиденциальной информации через съёмные носители

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux

Важно

Политика влияет на доступ к USB-накопителям

Рекомендуется:

- Информировать пользователей о политике использования USB-носителей
- Обеспечить альтернативные способы передачи файлов (сетевые диски, облачные хранилища)

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

Важно

Для выполнения или сохранения политики название обязательно для заполнения

- Действие — операция для применения к USB-накопителям
  - **Заблокировать** — запрещает использование USB-флешек и внешних жестких дисков
  - **Разблокировать** — разрешает использование USB-флешек и внешних жестких дисков

Остальные вкладки описаны на странице *Политики*

Пример

Блокировка USB-накопителей:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Блокировка USB-накопителей»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Блокировка USB-накопителей на рабочих станциях
4. Выбрать действие `Действие`

   Например: Заблокировать
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
7. После применения политики:

   На Windows-устройстве:

   - В реестре будет установлено значение `Start = 4` для службы USBSTOR
   - Подключенные USB-накопители будут отключены
   - Служба Plug and Play будет перезапущена для применения изменений
   - Новые USB-накопители не будут определяться системой

   На Linux-устройстве:

   - Будет создано правило udev в `/etc/udev/rules.d/80-block-usb-storage.rules`
   - Правила udev будут перезагружены
   - Подключенные USB-накопители будут заблокированы
   - Новые USB-накопители будут автоматически блокироваться при подключении

Разблокировка USB-накопителей:

1. Заполнить поле `Название`

   Например: Разблокировка USB-накопителей

2. Выбрать действие `Действие`

   Например: Разблокировать

3. Нажать на кнопку Сохранить

4. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики

5. После применения политики:

   На Windows-устройстве:

   - В реестре будет установлено значение `Start = 3` для службы USBSTOR
   - Отключенные USB-накопители будут повторно активированы
   - Служба Plug and Play будет перезапущена

   На Linux-устройстве:

   - Правило udev будет удалено
   - Правила udev будут перезагружены
   - Заблокированные USB-накопители будут разблокированы

Примечание

Что блокируется:

- USB-флеш-накопители
- Внешние USB-жесткие диски
- Кард-ридеры с картами памяти
- Другие USB-устройства хранения данных

Что НЕ блокируется:

- USB-клавиатуры и мыши
- USB-принтеры и сканеры
- USB-камеры и микрофоны
- Внутренние SATA/NVMe диски
- Bluetooth-устройства

Предупреждение

Важные предупреждения:

- Уже подключенные устройства могут потребовать повторного подключения после разблокировки
- Некоторые специализированные USB-устройства могут быть ошибочно заблокированы
- Политика не препятствует использованию других типов съемных носителей (CD/DVD, сетевые диски)
- Опытные пользователи могут обойти блокировку при наличии физического доступа к устройству

Блокировка пользователей

Доступна только в UEM версии

Описание

Блокировка пользователей — политика для блокировки всех пользователей на устройстве, кроме тех, которые указаны в белом списке

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux
- macOS

Важно

При пустом белом списке на Linux и macOS политика может затронуть в том числе пользователя `root`

На Linux и macOS политика блокирует учетные записи через изменение shell и блокировку пароля, а также пытается завершить активные пользовательские сеансы

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

Важно

Для выполнения или сохранения политики название обязательно для заполнения

- Белый список — в это поле необходимо написать пользователей, не подлежащих блокировке, через запятую

  Например: `root,rude`

Остальные вкладки описаны на странице *Политики*

Пример

Для блокировки пользователей на устройствах необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Блокировка пользователей»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Блокировка пользователей
4. Заполнить поле `Белый список`, если необходимо

   Например: Пользователь1, Пользователь2
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
7. После применения политики:
   - Пользователи на удалённом устройстве будут заблокированы, за исключением тех, которые были указаны в белом списке

Разблокировка пользователей

Доступна только в UEM версии

Описание

Разблокировка пользователей — политика для разблокировки всех пользователей на устройстве, кроме тех, которые указаны в чёрном списке

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux

- macOS

Важно

При пустом черном списке на Linux и macOS политика может затронуть в том числе пользователя `root`

На Linux и macOS политика пытается восстановить shell и снять блокировку аутентификации пользователя

Для части Linux-пользователей может потребоваться задание нового пароля, если прежний хеш пароля не удается восстановить

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Черный список — в это поле необходимо написать пользователей, не подлежащих разблокировке, через запятую

  Например: `root,rude`

Остальные вкладки описаны на странице *Политики*

Пример

Для разблокировки пользователей на устройствах необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Разблокировка пользователей»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Разблокировка пользователей
4. Заполнить поле `Черный список`, если необходимо

   Например: Пользователь1, Пользователь2
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики

7. После применения политики:
    - Будет выполнена попытка разблокировки пользователей на удалённом устройстве, за исключением тех, которые были указаны в чёрном списке

Блокировка USB-накопителей
Запрет подключения USB-накопителей на устройстве

Блокировка пользователей
Блокировка локальных учётных записей на устройстве

Разблокировка пользователей
Разблокировка ранее заблокированных учётных записей

Управление директориями и файлами

Создание директории

Доступна только в UEM версии

Политика создаёт каталог и недостающие промежуточные каталоги на Windows, Linux и macOS

Параметры

Указать **«Название»** и **«Путь до директории»**. Путь должен быть абсолютным: например, `C:\data\app` или `\\server\share\app` для Windows, `/data/app` для Linux и macOS. Это путь на целевом устройстве, а не на сервере RuDesktop. Для сетевого пути устройство и учётная запись выполнения должны иметь доступ к ресурсу. Политика не запрашивает отдельный пароль сетевого ресурса

Пример запуска

1. Создать политику по шаблону **«Создание директории»**
2. Задать название **«Подготовка каталога приложения»**
3. Указать путь `/data/app/cache` для Linux-устройства
4. Сохранить и выполнить **«Тестовый запуск»** на одном устройстве
5. Проверить результат задания и наличие каталога на этом устройстве

Если `/data/app` ещё не существует, эти каталоги также будут созданы. Если каталог уже есть, он сохраняется вместе с содержимым, повторное создание не требуется

Проверка ошибок

Если по указанному пути находится обычный файл, создание каталога не сможет завершиться успешно. При ошибке проверить полный путь, права учётной записи выполнения, доступность диска и сетевого ресурса

Примечание

Политика проверяет наличие каталога после операции, но не настраивает отдельные права доступа для сотрудников. При необходимости права на созданный каталог настраивать отдельно

Общие вкладки и назначение описаны на странице *Политики*

Удаление директории

Доступна только в UEM версии

Политика удаляет каталог со всеми вложенными файлами и папками на Windows, Linux и macOS

Параметры

Указать **«Название»** и **«Путь до директории»**. Путь должен быть абсолютным: например, `C:\temp\old-data` или `/tmp/old-data`. Это путь на целевом устройстве, а не на сервере RuDesktop

Предупреждение

Удаление не переносит содержимое в корзину и не создаёт резервную копию

«Тестовый запуск» также выполняет настоящее удаление

Проверить путь и состав каталога, а нужные данные сохранить до запуска

Пример запуска

1. Создать на тестовом устройстве отдельный ненужный каталог, например `/tmp/policy-delete-example`
2. Создать политику по шаблону **«Удаление директории»**
3. Указать название и полный путь к этому каталогу
4. Сохранить и выполнить **«Тестовый запуск»** на выбранном устройстве
5. Проверить результат задания и отсутствие каталога
6. После проверки настроить рабочий путь и назначение политики

Если каталог уже отсутствует, повторное удаление не требуется

Предупреждение

Не указывать путь к обычному файлу: шаблон предназначен для каталогов, а обработка файла отличается между ОС. Не использовать корневые и системные каталоги и не рассчитывать на то, что политика сама определит назначение выбранной папки

Проверка ошибок

При ошибке проверить права на каталог и его содержимое, доступность диска и открытые файлы

Важно

Часть содержимого может быть уже удалена до возникновения ошибки. Повторный запуск продолжит удаление оставшихся данных, а не восстановит их. Для возврата данных потребуется заранее созданная резервная копия

Общие вкладки и назначение описаны на странице *Политики*

Удаление файлов

Доступна только в UEM версии

Описание

Удаление файлов — политика для удаления одного или нескольких файлов по указанному пути и шаблону поиска

Политика удобна для очистки временных файлов, старых журналов и других наборов файлов, которые можно описать маской

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Предупреждение

Важное предупреждение:

- Удаление файлов выполняется без возможности отмены
- При использовании шаблонов поиска проверьте, что маска не затрагивает лишние файлы

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Путь до директории с файлом — каталог, в котором будет выполняться поиск файлов

> **Примечание**
>
> Необходимо указывать абсолютный путь
>
> На Linux и macOS поиск выполняется только в пределах указанного каталога без рекурсивного обхода вложенных директорий

- Название файла/выражение для поиска файлов — имя файла или шаблон поиска

> **Примечание**
>
> Например: `*.log` или `temp-*.tmp`

Остальные вкладки описаны на странице *Политики*

Пример

Для удаления всех файлов `.log` в каталоге `/var/log`:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Удаление файлов»**
3. Заполнить поле `Название`

   Например: Очистка логов
4. Заполнить поле `Путь до директории с файлом`

   Например: /var/log/
5. Заполнить поле `Название файла/выражение для поиска файлов`

   Например: *.log
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве
8. После применения политики:
   - Все найденные по маске файлы будут удалены
   - Поиск выполняется в пределах указанного каталога

Примечание

Технические особенности:

- На Windows поиск файлов выполняется через `win_find`
- На Linux и macOS используется команда `find` с ограничением поиска текущим каталогом
- Удаление найденных файлов выполняется отдельно для каждого результата поиска

Предупреждение

Важные предупреждения:

- Ошибочно заданная маска может затронуть больше файлов, чем ожидалось
- Политика не спрашивает подтверждение перед удалением найденных файлов
- Перед массовым запуском рекомендуется проверить шаблон на тестовом устройстве

Перемещение файла

Доступна только в UEM версии

Описание

Перемещение файла — политика для перемещения файла из одного расположения в другое на том же устройстве

Политика подходит для архивирования и перераскладки рабочих данных

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

Если целевой файл уже существует, он будет перезаписан

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Путь до файла — полный путь к исходному файлу
- Путь назначения — полный путь, куда файл должен быть перемещен

Примечание

Можно указать как полный путь к целевому файлу, так и путь к директории

Если указан путь к директории, файл будет перемещен в нее под исходным именем

Остальные вкладки описаны на странице *Политики*

Пример

Для перемещения файла `/var/log/syslog` в архивную директорию:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Перемещение файла»**
3. Заполнить поле `Название`

   Например: Перенос системного лога в архив
4. Заполнить поле `Путь до файла`

   Например: /var/log/syslog
5. Заполнить поле `Путь назначения`

   Например: /tmp/archive/syslog.log
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве
8. После применения политики:
   - Файл будет перемещён в новое расположение
   - Исходный файл перестанет существовать по прежнему пути

Примечание

Технические особенности:

- На Windows перемещение выполняется через `Move-Item`
- На Linux и macOS используется команда `mv -f`
- Политика работает в пределах одного устройства

Предупреждение

Важные предупреждения:

- Если целевой файл уже существует, он будет перезаписан
- При недостатке прав на чтение, запись или удаление перемещение завершится ошибкой
- Перед запуском рекомендуется проверить корректность обоих путей

Загрузка файла

Доступна только в UEM версии

Описание

Загрузка файла — политика для загрузки файла на устройство по указанному абсолютному пути с проверкой контрольной суммы SHA1

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux
- macOS

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

Важно

Для выполнения или сохранения политики название обязательно для заполнения

- Файл — файл для загрузки на удалённое устройство

Подсказка

- Кнопка Browse открывает окно выбора файла на компьютере
- Кнопка Репозиторий открывает окно выбора файла из внутреннего репозитория сервера **RuDesktop**

Важно

Файлы отображаются из всех репозиториев, которые созданы на сервере **RuDesktop**

- Файл можно перетащить в поле Выберите файл или перетащите его сюда
- После загрузки на устройство для файла проверяется контрольная сумма SHA1

- Путь — абсолютный путь назначения на удалённом устройстве

Подсказка

- Нужно указать абсолютный путь к файлу или директории назначения
- Можно указать путь к директории; в этом случае файл будет загружен в эту директорию под исходным именем
- Если файл уже существует и его контрольная сумма совпадает с исходной, повторная загрузка не выполняется
- Если файл уже существует и его контрольная сумма отличается, политика попытается перезаписать его
- На Windows путь должен быть указан в Windows-формате, на Linux и macOS — в Unix-формате
- Для Windows в именах файлов и каталогов недопустимы символы `<>:"|?*`

Остальные вкладки описаны на странице *Политики*

Пример

Для загрузки файла на удалённое устройство необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **«Политики»**
2. Выбрать шаблон политики **«Загрузка файла»** из списка предложенных шаблонов

3. Заполнить поле `Название`

   Например: Загрузка файла

4. Выбрать файл
5. Заполнить поле `Путь`

   Например для Windows: C:UsersrudeDownloadsreport.txt

   Например для Linux: /home/rude/Downloads/report.txt

   Например для macOS: /Users/rude/Downloads/report.txt

6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
8. После применения политики:
   - если файл отсутствует, он будет загружен на устройство
   - если файл уже существует и совпадает по SHA1, повторная загрузка будет пропущена
   - если файл уже существует и отличается по SHA1, политика попытается перезаписать его

Загрузка файла на Android устройство

Доступна только в MDM версии

Описание

Политика загружает выбранный файл с сервера **RuDesktop** на Android-устройство в указанную папку общего хранилища. Файл сначала передаётся во временную папку клиента, затем сохраняется в целевую папку под заданным именем. Путь сохранённого файла выводится в итоговом сообщении задания

Подготовка

Требуется клиент RuDesktop с поддержкой этой политики. Устройство должно быть зарегистрировано в MDM. Для обычного сценария управления RuDesktop используется регистрация с правами владельца устройства (Device Owner), описанная в кейсе настройки MDM

Поведение при сохранении зависит от версии Android:

- **Android до 10** — файл сохраняется напрямую в файловую систему: доступна любая папка общего хранилища, недостающие вложенные папки создаются автоматически
- **Android 10 и новее** — файл сохраняется через MediaStore: доступны только системные корневые папки, а тип файла должен соответствовать папке (см. «Ограничения и подводные камни»)

Свойства политики

На вкладке **«Политика»** заполнить:

- Название — имя политики в системе, обязательно для заполнения
- Файл — обязательный файл для загрузки. Кнопка Browse открывает окно выбора файла на компьютере, кнопка Репозиторий — выбор из внутреннего репозитория сервера **RuDesktop**; файл также можно перетащить в поле выбора
- Куда сохранять — обязательный путь к целевой папке относительно корня внутреннего хранилища, например `Download/reports/v2`. Допускается и абсолютный путь хранилища — префиксы `/sdcard`, `/storage/emulated/0`, `/storage/self/primary`, `/mnt/sdcard` отбрасываются автоматически. Регистр корневой папки не важен: `download` будет приведён к `Download`
- Перезаписывать файл — заменить существующий файл с тем же именем. Работает только на Android до 10
- Название файла с которым сохраняем файл на устройстве — имя сохраняемого файла. Если оставить поле пустым, используется исходное имя выбранного файла. Указывается только имя: символ `/` в имени не допускается

Остальные вкладки описаны на странице *Политики*

Ограничения и подводные камни

Корневые папки на Android 10 и новее. MediaStore принимает только системные корневые папки, и для каждой разрешён свой тип содержимого:

- любые файлы — `Download`, `Documents`, `Podcasts`
- изображения и видео — `DCIM`, `Pictures`
- только видео — `Movies`
- только аудио — `Music`, `Ringtones`, `Alarms`, `Notifications`, `Audiobooks`

`Recordings` доступна начиная с Android 12.

Предупреждение

Тип файла определяется по расширению. Если расширение неизвестно системе, файл получает тип `application/octet-stream` и его не примет ни одна «медиа»-папка (`DCIM`, `Pictures`, `Movies`, `Music` и другие) — такой файл можно сохранить только в `Download`, `Documents` или `Podcasts`. Файл без расширения в «медиа»-папку загрузить не получится

Прочие ограничения:

- Путь не должен содержать элементы `.` и `..` — такие пути отклоняются

- На Android 10+ параметр **«Перезаписывать файл»** не действует: существующий файл не заменяется, при совпадении имени система сохраняет копию с номером, например `example (1).txt`
- На Android до 10 без включённой перезаписи к имени также добавляется номер копии: `example.txt` станет `example (1).txt`
- После сохранения проверяется размер файла: если на устройстве не хватило места или запись оборвалась, задание завершится ошибкой, а на Android 10+ частично записанный файл удаляется
- Файл передаётся в два этапа: во временную папку клиента (кэш приложения) и затем копируется в целевую папку. На время выполнения на устройстве требуется свободное место примерно вдвое больше размера файла; временная копия остаётся в кэше приложения и удаляется системой самостоятельно
- Во время записи на Android 10+ файл скрыт от других приложений и становится виден только после завершения сохранения

Ошибки загрузки и их причины — в разделе «Если загрузка не выполнена»

Пример и проверка

1. Нажать Добавить Политику на странице **«Политики»**
2. Выбрать шаблон **«Загрузка файла на Android устройство»** в категории **«Управление директориями и файлами»**
3. Заполнить **«Название»**, например `Выгрузка отчётов на терминал`
4. Выбрать файл в поле **«Файл»**
5. Указать **«Куда сохранять»**, например `Download/reports` — для Android 10+ корневая папка должна быть из разрешённого списка
6. При необходимости задать **«Название файла с которым сохраняем файл на устройстве»**
7. Нажать Сохранить. Само сохранение не загружает файл на устройство
8. На вкладке **«Тестовый запуск»** выбрать одно устройство и нажать **«Запустить»**
9. Проверить окно логирования: задание завершится успешно и выведет путь сохранённого файла на устройстве
10. Открыть файловый менеджер на устройстве и убедиться, что файл находится в целевой папке и открывается

Для загрузки на несколько устройств добавить политику в *задачу*. Каждый запуск загружает файл заново; при включённой перезаписи (Android до 10) файл заменяется, иначе рядом появляется копия с номером

Если загрузка не выполнена

- `Unknown MDM command` — установить клиент RuDesktop с поддержкой политики
- `Invalid `from path`: is null or blank` / `Invalid `target path`: is null or blank` — заполнить обязательные поля **«Файл»** и **«Куда сохранять»**
- `File not found: ...` — исходный файл не передан во временную папку; проверить состояние устройства и повторить запуск
- `Invalid file name: ...` — поле **«Название файла с которым сохраняем файл на устройстве»** содержит `/`; имя файла не должно быть путём
- `Empty folder path` / `Invalid folder path: ...` — поле **«Куда сохранять»** пустое или содержит `.` / `..`
- `Unsupported Folder: ... Acceptable: Download, Documents, ...` — на Android 10+ корневая папка не входит в разрешённый список
- `The folder Recordings is accessible via the API 31` — папка `Recordings` доступна только с Android 12
- `The file with type ... cannot be saved in ...` — тип файла (по расширению) не подходит для выбранной корневой папки
- `Write error: ...` — ошибка записи на устройстве, чаще всего нехватка места или недоступность хранилища
- `Saved file is missing or incomplete: ...` — сохранённый файл не прошёл проверку размера; проверить свободное место и повторить запуск

Копирование файла

Доступна только в UEM версии

Описание

Копирование файла — политика для копирования файлов между разными расположениями на одном устройстве под управлением Windows, Linux или macOS

Политика подходит для резервного копирования и распространения файлов в пределах одного устройства

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

Политика перезаписывает существующие файлы в целевом расположении

Рекомендуется:

- Проверять существование целевых файлов перед копированием
- Использовать уникальные имена для целевых файлов при копировании в общие директории
- Проверять права доступа к исходному и целевому расположению
- Убедиться, что на диске достаточно свободного места

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Путь до файла — абсолютный путь к исходному файлу для копирования

  Важно

  Указывайте полный путь к файлу, включая имя файла

  Примеры:

  - Windows: `C:\Windows\System32\drivers\etc\hosts`
  - Linux: `/var/log/syslog`
  - macOS: `/var/log/system.log`

- Путь назначения — абсолютный путь, куда будет скопирован файл

  Важно

  Можно указать полный путь, включая имя целевого файла, либо путь к директории

  Если указан путь к директории, файл будет скопирован в нее под исходным именем

  Примеры:

  - Windows: `C:\Temp\backup_hosts.txt`

- Linux: `/tmp/syslog_backup.log`
- macOS: `/Users/Shared/system_log_backup.log`

Остальные вкладки описаны на странице *Политики*

Пример

Для создания резервной копии файла hosts на Windows-устройстве:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Копирование файла»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Резервное копирование файла hosts
4. Заполнить поле `Путь до файла`

   Например: C:\Windows\System32\drivers\etc\hosts

   Примечание

   Файл должен существовать на устройстве и быть доступным для чтения
5. Заполнить поле `Путь назначения`

   Например: C:\Backup\hosts_backup.txt
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
8. После применения политики:
   - На Windows-устройстве файл будет скопирован через `Copy-Item`
   - На Linux/macOS-устройстве файл будет скопирован командой `cp -f`
   - Если целевой файл уже существует, он будет полностью перезаписан
   - Копирование происходит в пределах одного устройства

Для копирования системного лога на Linux для анализа:

1. Заполнить поле `Название`

   Например: Копирование syslog для анализа
2. Заполнить поле `Путь до файла`

   Например: /var/log/syslog
3. Заполнить поле `Путь назначения`

Например: /tmp/syslog_analysis.log

4. Нажать на кнопку Сохранить
5. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики

Примечание

Особенности копирования:

- **Windows:** Копирование выполняется через `Copy-Item`
- **Linux/macOS:** Копирование выполняется командой `cp -f`
- **Перезапись:** существующие файлы перезаписываются без предупреждения
- **Директории:** Если целевой путь является директорией, файл будет скопирован в нее с исходным именем

Предупреждение

Важные предупреждения:

- Файлы перезаписываются без возможности отмены
- Убедитесь, что целевая директория существует
- На Windows пути чувствительны к регистру только при определенных настройках файловой системы
- Символы *, ?, [,] в путях не поддерживаются
- Копирование больших файлов может занять значительное время

Копирование и перемещение директории

Доступна только в UEM версии

Описание

Копирование и перемещение директории - политика для копирования или перемещения директории со всем содержимым внутри устройства. Политика подходит для резервного копирования рабочих каталогов, переноса данных на другой диск и перераскладки структуры файлов

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux

- macOS

Важно

Исходная директория помещается внутрь целевой и сохраняет своё имя

Например, при копировании `/opt/data` в `/mnt/backup` результатом будет `/mnt/backup/data`

Свойства политики

После выбора шаблона политики откроется окно с её свойствами. Вкладка **«Политика»** содержит следующие поля:

- Название - имя политики в системе
- Путь до исходной директории - полный путь к директории, которую требуется скопировать или переместить

Примечание

Для Windows необходимо указывать абсолютный путь вида `C:\data\folder` или `\\server\share\dir`

Для Linux и macOS необходимо указывать абсолютный путь, начинающийся с `/`

- Путь до целевой директории - полный путь к директории, внутрь которой будет помещена исходная директория

Примечание

Недостающие каталоги на пути будут созданы автоматически

Если итоговая папка с именем исходной директории уже существует, её содержимое дополняется и обновляется

Файлы с совпадающими именами могут быть заменены исходными, а посторонние файлы автоматически не удаляются

- Операция - режим работы политики
  - **Копирование** - создаёт копию директории, исходная директория остаётся без изменений
  - **Перемещение** - переносит директорию, исходная директория удаляется после успешного переноса

Остальные вкладки описаны на странице *Политики*

Пример

Для копирования рабочего каталога `/opt/data` в резервное хранилище:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Копирование и перемещение директории»**
3. Заполнить поле `Название`

   Подсказка

   Например: Резервное копирование рабочего каталога

4. Заполнить поле `Путь до исходной директории`

   Подсказка

   Например: /opt/data

5. Заполнить поле `Путь до целевой директории`

   Подсказка

   Например: /mnt/backup

6. В поле `Операция` выбрать Копирование
7. Нажать на кнопку Сохранить
8. Выполнить `Тестовый запуск` на устройстве
9. После применения политики:
   - Директория будет доступна по пути `/mnt/backup/data` со всем содержимым
   - Вложенные каталоги, включая пустые, будут перенесены полностью
   - При выборе перемещения исходная директория будет удалена после успешного переноса

Примечание

Проверка результата:

- После операции сверяются наличие каталога, количество файлов и вложенных каталогов, а также суммарный объём данных
- При существующем месте назначения учитывается его прежнее содержимое
- Такая проверка не сравнивает содержимое каждого файла побайтово

- Свободное место проверяется перед копированием, если его удаётся определить
- При перемещении в пределах одной файловой системы без копирования дополнительное место под полную копию не требуется
- Пути относятся к одному целевому устройству, политика не переносит каталог с одного клиента на другой

Предупреждение

Важные предупреждения:

- При выборе перемещения исходная директория удаляется без возможности восстановления
- Исходная директория не может быть корнем файловой системы или корнем сетевого ресурса
- Целевой путь не может совпадать с исходной директорией или находиться внутри неё
- Символические ссылки и точки соединения в качестве исходного или целевого пути не поддерживаются
- Целевой путь не может указывать на существующий файл
- При ошибке часть файлов в месте назначения уже может быть скопирована или заменена
- Автоматический откат операции не выполняется
- Перед запуском рекомендуется проверить корректность обоих путей

Как проверить путь назначения

Если исходная папка - `C:\Work\Reports`, а место назначения - `D:\Archive`, результат находится в `D:\Archive\Reports`

Подсказка

Не указывать `D:\Archive\Reports` в качестве места назначения, если дополнительная вложенность не нужна: в таком случае результат окажется в `D:\Archive\Reports\Reports`. Для копирования выбрать пустое место назначения, если важно получить отдельную копию без смешивания с прежними файлами

Для резервного хранения использовать отдельную папку на каждую копию, поскольку повторный запуск в то же место может заменить файлы

Что делать при ошибке перемещения

Проверить итоговый путь и наличие исходного каталога

Предупреждение

Если копирование завершилось, но удаление исходника не удалось, данные могут находиться в обоих местах, а часть исходного каталога уже может быть удалена. Не удалять оставшиеся исходные данные до проверки копии. Если ошибка возникла на итоговой проверке, исходник уже мог быть перемещён или удалён на предыдущем этапе

После исправления прав, свободного места или блокировок выбирать дальнейшее действие по фактическому состоянию каталогов

Скачивание файла по URL

Доступна только в UEM версии

Описание

Скачивание файла по URL - политика для загрузки файла на устройство по указанному веб-адресу. Политика подходит для доставки дистрибутивов, документов и обновлений на устройства без использования репозитория сервера

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

Файл скачивается самим устройством, поэтому указанный адрес должен быть доступен с устройства, а не с сервера управления

Свойства политики

После выбора шаблона политики откроется окно с её свойствами. Вкладка **«Политика»** содержит следующие поля:

- Название - имя политики в системе
- URL файла - полный адрес файла

  Примечание

  Адрес должен начинаться с `http://` или `https://`

- Имя файла - имя, под которым файл будет сохранён на устройстве

  Примечание

  Необязательное поле

  Если оставить его пустым, имя берётся из адреса

  Для адресов вида `https://example.com/download?id=42` лучше задать понятное имя с расширением, например `instructions.pdf`

  Без явного имени используется последняя часть пути URL, в этом примере `download`

  Если подходящее имя определить не удалось, используется `downloaded_file`

  Имя не должно содержать разделители пути: папка задаётся отдельным полем

- Свой путь к папке - папка, в которую будет сохранён файл

  Примечание

  Необязательное поле

  Если оставить его пустым, используется стандартная папка, выбранная ниже

  Недостающие каталоги на пути будут созданы автоматически

  Для Windows необходимо указывать абсолютный путь вида `C:\data\folder` или `\\server\share\dir`, для Linux и macOS - путь, начинающийся с `/`

- Стандартная папка - папка, используемая, если свой путь не задан
  - **Рабочий стол** - рабочий стол пользователя, вошедшего в систему
  - **Загрузки** - папка загрузок пользователя, вошедшего в систему
  - **Временная папка** - системная временная папка устройства
- Имя пользователя для доступа к файлу - учётная запись для авторизации на сервере

> **Примечание**
>
> Необязательное поле
>
> Заполняется, если файл доступен только после авторизации

- Пароль для доступа к файлу - пароль учётной записи

> **Примечание**
>
> Пароль нельзя указывать без имени пользователя

- Контрольная сумма файла - сумма для проверки целостности скачанного файла

> **Примечание**
>
> Необязательное поле
>
> Указывается в формате `алгоритм:сумма`
>
> Для SHA-256 после `sha256:` указать полную сумму из 64 шестнадцатеричных символов
>
> Получить ожидаемую сумму у поставщика файла или из своего доверенного источника
>
> Поддерживаются алгоритмы `md5`, `sha1`, `sha256`, `sha384` и `sha512`

- Проверка сертификата сервера - режим проверки сертификата при работе по `https`
  - **Проверять** - обычный режим работы
  - **Не проверять** - для доверенных внутренних серверов с самоподписанным сертификатом

Остальные вкладки описаны на странице *Политики*

Пример

Для загрузки дистрибутива в папку загрузок пользователя:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Скачивание файла по URL»**
3. Заполнить поле `Название`

   Подсказка

   Например: Загрузка дистрибутива на устройства

4. Заполнить поле `URL файла`

   Подсказка

   Например: https://example.com/files/app-1.2.3.msi

5. Поле `Имя файла` оставить пустым - имя будет взято из адреса
6. Поле `Свой путь к папке` оставить пустым
7. В поле `Стандартная папка` выбрать Загрузки
8. В поле `Проверка сертификата сервера` выбрать Проверять
9. Нажать на кнопку Сохранить
10. Выполнить `Тестовый запуск` на устройстве
11. После применения политики:
    - Файл будет сохранён в папке загрузок пользователя, вошедшего в систему
    - В результате выполнения будут указаны полный путь к файлу и его размер

Выбор папки и пользователя

Свой путь к папке имеет приоритет над стандартной папкой. Поле **«Стандартная папка»** всё равно нужно заполнить, даже если задан свой путь

Примечание

При выборе **«Рабочий стол»** или **«Загрузки»** политика определяет одного вошедшего пользователя устройства. Это не доставка во все пользовательские профили. Если на устройстве одновременно работают несколько пользователей, для предсказуемого места сохранения указать свой путь

Если вошедшего пользователя определить не удалось, стандартные пользовательские папки использовать нельзя - указать свой путь или временную папку

На Windows учитываются настройки расположения пользовательских папок, включая перенаправление в OneDrive. На Linux учитываются локализованные названия папок. На Linux и macOS при выборе стандартного рабочего стола или загрузок владельцем сохранённого файла назначается определённый пользователь

Важно

Скачивание в сетевую папку Windows требует доступа к ней у учётной записи, под которой выполняется политика. Поля имени и пароля для URL не предоставляют доступ к папке назначения

Повторный запуск и проверка результата

При повторном запуске политика снова обращается к источнику. Существование файла с таким именем не является причиной пропустить скачивание. Файл по тому же пути может быть заменён - для хранения нескольких версий указывать разные имена. Перед скачиванием проверяется свободное место, если удалось определить размер удалённого файла и доступный объём на устройстве

Отсутствие ошибки этой проверки не гарантирует, что места хватит до конца загрузки. После выполнения проверить в журнале итоговый путь, размер и результат проверки контрольной суммы, если она задана. Нулевой размер считается ошибкой

Предупреждение

При несовпадении контрольной суммы файл удаляется с устройства, а политика завершается ошибкой. Если сумма не задана, успешное скачивание не подтверждает, что сервер вернул именно нужный документ или установщик - по ссылке может оказаться страница входа

Политика сохраняет файл, но не запускает его и не устанавливает приложение

Если скачивание не удалось

- **401 или 403** - проверить доступ к файлу и учётные данные для URL
- **404 или 410** - проверить адрес и наличие файла у источника
- **Ошибка сертификата** - проверить сертификат сервера и доверие к нему на целевом устройстве
- **Недостаточно места** - освободить место на устройстве в месте сохранения файла
- **Не определена папка пользователя** - указать свой путь или временную папку

- **Ошибка записи** - проверить права учётной записи выполнения на папку назначения
- **Не совпадает контрольная сумма** - проверить файл у источника и ожидаемую сумму перед повторным запуском

Для проверки использовать прямую ссылку на файл, доступную с целевого устройства. Ссылка на страницу просмотра документа или сайт с интерактивным входом может не подходить для автоматического скачивания. Проверить политику на одном устройстве, затем применять к остальным

Редактирование реестра

Доступна только в UEM версии

Описание

Редактирование реестра - политика для добавления, изменения или удаления параметров в реестре Windows

Примечание

Данная политика доступна для выполнения на ОС:

- Windows

Свойства политики

После выбора шаблона политики откроются её свойства. Вкладка **«Политика»** содержит следующие поля:

- Название - имя политики

Важно

Для выполнения или сохранения политики название обязательно для заполнения

- Действие - запись или удаление параметра реестра
- Ветка реестра - путь в реестре для создаваемого или удаляемого параметра

Важно

Поддерживаются только ветки `HKLM:\`, `HKCU:\`, `HKCR:\`, `HKU:\`, `HKCC:\`

- Имя параметра - имя создаваемого или удаляемого параметра
- Тип параметра - тип параметра

- Значение параметра - значение параметра

> **Примечание**
>
> Для действия **«Удалить параметр»** поля **«Тип параметра»** и **«Значение параметра»** игнорируются
>
> Для действия **«Записать параметр»**:
>
> - для `string` и `expandstring` указывается текстовое значение
> - для `multistring` строки указываются через `;`
> - для `dword` и `qword` указывается десятичное значение или число в формате `0x`
> - для `binary` используется hex-строка, например `0A FF 1B`
> - для `none` поле значения должно быть пустым

- Перезагрузка - настройка поведения после применения изменений:
  - `Не перезагружать` - устройство не перезагружается
  - `Перезагрузить` - устройство перезагружается сразу после подтвержденного изменения, без предупреждения пользователя
  - `Предупредить пользователя и перезагрузить` - на устройстве показывается нейтральное предупреждение о перезагрузке с точным временем, чтобы пользователь успел сохранить работу: уведомление в центре уведомлений Windows

> **Примечание**
>
> Путь реестра и параметры политики в предупреждении не раскрываются
>
> В предупреждении есть кнопки `Перезагрузка` и `Закрыть`, а если отсрочка разрешена - еще и кнопка `Отложить`
>
> Если за устройством никто не работает, оно перезагрузится сразу

> **Примечание**
>
> `Перезагрузка` перезагружает устройство немедленно
>
> `Закрыть` только убирает предупреждение - перезагрузка всё равно произойдет в назначенное время

`Отложить` переносит перезагрузку на время из поля Отсрочка пользователем, минут, после чего предупреждение показывается повторно: за столько минут до новой перезагрузки, сколько задано в поле Отсрочка перезагрузки, минут

Примечание

Перезагрузка запускается только после подтвержденного изменения параметра реестра

Если параметр уже находится в требуемом состоянии и изменения не потребовались, устройство не перезагружается - причина указывается в итоге выполнения политики

Примечание

Перезагрузку, отложенную предыдущим запуском этой политики, следующий запуск с изменением параметра снимает перед планированием новой

- Отсрочка перезагрузки, минут - через сколько минут перезагрузить устройство после применения изменений реестра

Примечание

Всё это время пользователю показывается предупреждение с точным временем перезагрузки

Учитывается только при выборе `Предупредить пользователя и перезагрузить`

Если поле пустое, перезагрузка произойдет через 15 минут

- Отсрочка пользователем, минут - на сколько минут пользователь может отложить перезагрузку кнопкой в предупреждении

Примечание

Кнопка отсрочки показывается, только если это значение больше отсрочки перезагрузки

Учитывается только при выборе `Предупредить пользователя и перезагрузить`

Если поле пустое, отсрочка составит 60 минут

- Сколько раз можно отложить - сколько раз пользователь может отложить перезагрузку кнопкой в предупреждении

Примечание

Когда отсрочки закончились, кнопка больше не показывается

Учитывается только при выборе `Предупредить пользователя и перезагрузить`

Если поле пустое, отложить можно 1 раз

Остальные вкладки описаны на странице *Политики*

Пример

Для добавления параметра в ветку реестра необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Редактирование реестра»** из списка предложенных шаблонов
3. Заполнить поле `Название`

Подсказка

Например: Редактирование реестра

4. В поле `Действие` выбрать Записать параметр
5. Заполнить поле `Ветка реестра`

Подсказка

Например: `HKLM:\Software\MyCompany`

6. Заполнить поле `Имя параметра`

Подсказка

Например: EnableFeature

7. В поле `Тип параметра` выбрать string
8. Заполнить поле `Значение параметра`

Подсказка

Например: 1

9. При необходимости выбрать значение в поле `Перезагрузка` и настроить отсрочки

10. Нажать на кнопку Сохранить
11. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
12. После применения политики:

    В реестре будет добавлен указанный параметр с заданным значением по указанному пути

Проверка результата и перезагрузки

Предупреждение

«Тестовый запуск» действительно изменяет реестр и при выбранной перезагрузке может перезагрузить устройство. Сначала использовать отдельное тестовое устройство и убедиться, что выбранный параметр соответствует требованиям настраиваемой программы

В результате задания проверить, потребовалось ли изменение, и сообщение о перезагрузке. Затем проверить значение и тип параметра в нужной ветке реестра на устройстве

Примечание

Для пользовательских веток учитывать учётную запись, от имени которой выполняется политика. `HKCU` относится к этому пользователю, а не автоматически к каждому сотруднику, работающему за устройством

Например, при предупреждении с отсрочкой 15 минут и пользовательской отсрочкой 60 минут пользователь может нажать **«Отложить»**, чтобы перенести перезагрузку. Закрытие уведомления не отменяет запланированную перезагрузку. Если значение уже правильное, повторный запуск не назначает новую перезагрузку. Поэтому для проверки предупреждения нужно добиться реального изменения тестового параметра

Важно

Удаление или отключение политики на сервере не возвращает прежнее значение реестра. Для возврата выполнить отдельное изменение с прежним значением либо удалить созданный параметр, если именно это требуется приложению

Редактирование файла

Доступна только в UEM версии

Редактирование файла — политика для замены строк в текстовых файлах

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux
- macOS

Описание политики

После выбора шаблона политики откроются её свойства

Важно

Политика заменяет только существующую строку, совпавшую с заданным регулярным выражением

Если файл не найден или совпадение по шаблону отсутствует, политика завершится ошибкой

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Путь к файлу — абсолютный путь к файлу на удалённом устройстве

  Важно

  Для Windows нужно указывать абсолютный путь, например `C:\temp\file.txt`

  Для Linux и macOS нужно указывать абсолютный путь, начинающийся с `/`

- Шаблон строки — регулярное выражение для поиска строки в файле
- Новая строка — строка для замены шаблона
- Перезагрузка — настройка поведения после замены строки:
  - `Не перезапускать` — устройство не перезагружается
  - `Перезапустить` — устройство перезагружается сразу после подтвержденного изменения, без предупреждения пользователя

- `Предупредить пользователя и перезагрузить` — на устройстве показывается нейтральное предупреждение о перезагрузке с точным временем, чтобы пользователь успел сохранить работу: на Windows — уведомление в центре уведомлений, на Linux и macOS — окно в графической сессии. Путь к файлу, шаблон строки и новая строка в предупреждении не раскрываются. В предупреждении есть кнопки `Перезагрузка` (на Linux и macOS — `Перезагрузить сейчас`) и `Закрыть`, а если отсрочка разрешена — еще и кнопка `Отложить`. Если за устройством никто не работает, оно перезагрузится сразу

Примечание

Кнопка перезагрузки перезагружает устройство немедленно. `Закрыть` только убирает предупреждение — перезагрузка всё равно произойдет в назначенное время. `Отложить` переносит перезагрузку на время из поля Отсрочка пользователем, минут, после чего предупреждение показывается повторно: за столько минут до новой перезагрузки, сколько задано в поле Отсрочка перезагрузки, минут

Примечание

Перезагрузка запускается только после подтвержденного изменения строки. Если строка уже находится в требуемом виде и изменения не потребовались, устройство не перезагружается — причина указывается в итоге выполнения политики

Примечание

Перезагрузку, отложенную предыдущим запуском этой политики, следующий запуск с изменением строки снимает перед планированием новой

- Отсрочка перезагрузки, минут — через сколько минут перезагрузить устройство после замены строки. Всё это время пользователю показывается предупреждение с точным временем перезагрузки. Учитывается только при выборе `Предупредить пользователя и перезагрузить`. Если поле пустое, перезагрузка произойдет через 15 минут
- Отсрочка пользователем, минут — на сколько минут пользователь может отложить перезагрузку кнопкой в предупреждении. Кнопка отсрочки показывается, только если это значение больше отсрочки перезагрузки. Учитывается только при выборе `Предупредить пользователя и перезагрузить`. Если поле пустое, отсрочка составит 60 минут
- Сколько раз можно отложить — сколько раз пользователь может отложить перезагрузку кнопкой в предупреждении. Когда отсрочки закончились, кнопка больше не показывается. Учитывается только при выборе

`Предупредить пользователя и перезагрузить`. Если поле пустое, отложить можно 1 раз

Остальные вкладки описаны на странице *Политики*

Пример

При наличии текстового файла `*.txt` со следующим содержимым:

```
<
ip
hostname
>
```

Для изменения `hostname` на произвольную строку необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **«Политики»**
2. Выбрать шаблон политики **«Редактирование файла»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Редактирование txt
4. Заполнить поле `Путь к файлу`

   Например: /home/user/Documents/имя_файла.txt
5. Заполнить поле `Шаблон строки`

   Например: hostname
6. Заполнить поле `Новая строка`

   Например: новая строка
7. При необходимости выбрать значение в поле `Перезагрузка` и настроить отсрочки
8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:

    Содержимое файла будет изменено на:

```
<
ip
новая строка
>
```

Дополнительная информация

В файлах Ansible часто используются YAML и Jinja2, поэтому регулярные выражения удобно применять для поиска нужных строк и шаблонов

Поиск по ключевому слову

Регулярное выражение для поиска строки, начинающейся с ключевого слова (например, hosts):

Шаблон строки: ^hosts

Поиск по переменной

Регулярное выражение для поиска строки, содержащей переменную, например в формате Jinja2 `{{ variable_name }}`:

Шаблон строки: {{s*w+s*}}

Поиск по ключу и значению

Регулярное выражение для поиска строки в формате `ключ: значение`, например для поиска ключа `name`:

Шаблон строки: ^name:s*(.*)$

Поиск по комментарию

Регулярное выражение для поиска строки с комментарием, которая начинается с #:

Шаблон строки: #.*

Примечание

Эти примеры можно адаптировать под поиск строк в ваших файлах

Создание директории

Создание директории на устройстве по указанному пути

Удаление директории

Удаление директории с устройства

Удаление файлов

Удаление файлов с устройства по указанному пути

Перемещение файла
Перемещение файла из одной директории в другую

Загрузка файла
Загрузка файла на устройство из репозитория сервера

Загрузка файла на Android устройство
Загрузка файла в папку общего хранилища Android-устройства

Копирование файла
Копирование файла внутри устройства

Редактирование реестра
Изменение значений в реестре Windows

Редактирование файла
Изменение содержимого текстового файла на устройстве

Копирование и перемещение директории
Копирование или перемещение директории со всем содержимым

Скачивание файла по URL
Загрузка файла на устройство по веб-адресу

Управление пользователями и устройствами

Управление добавлением и удалением аккаунтов Android устройства

Доступна только в MDM версии

Подготовка и запуск

Примечание

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном

2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

> **Важно**
>
> Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Политика управляет возможностью пользователя добавлять и удалять учётные записи в настройках Android, например аккаунт почты. Это учётные записи на самом устройстве, а не пользователи организации RuDesktop. В поле **«Выбор действия»** выбрать **«Запретить»**, чтобы закрыть пользователю добавление и удаление аккаунтов, или **«Разрешить»**, чтобы снять этот запрет

Существующие аккаунты политика не удаляет, новые не создаёт и их пароли не меняет. После применения открыть раздел учётных записей Android и проверить доступность добавления и удаления. Для возврата возможности изменять аккаунты выполнить политику с действием **«Разрешить»**

Управление USB, MTP, OTG Android устройства

Доступна только в MDM версии

Подготовка и запуск

> **Примечание**
>
> Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном
2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

Важно

Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Политика ограничивает передачу файлов по USB и подключение внешних накопителей. В поле **«Выбор действия»** выбрать **«Запретить»** или **«Разрешить»**. При запрете блокируются передача файлов по MTP/PTP и монтирование физических носителей, в том числе SD-карт и USB-OTG накопителей

Примечание

На Android 12 и новее дополнительно отключается обмен данными по USB, если устройство поддерживает такое управление. Зарядка по USB сохраняется. На более ранних версиях и устройствах без поддержки полного отключения USB действуют ограничения передачи файлов и монтирования носителей. Не следует считать такой результат блокировкой всех возможных USB-устройств

После применения проверить подключение к компьютеру в режиме передачи файлов и подключение внешнего накопителя. Политика не форматирует накопители и не удаляет с них данные. Действие **«Разрешить»** снимает установленные ограничения и, на поддерживаемых устройствах, снова включает обмен данными по USB

Управление использованием микрофона Android устройства

Доступна только в MDM версии

Подготовка и запуск

Примечание

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном
2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

Важно

Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Политика запрещает использование микрофона через системное ограничение на его включение. В поле **«Выбор действия»** выбрать **«Запретить»** для установки ограничения или **«Разрешить»** для его снятия. Проверять результат следует в приложении, которому уже предоставлено разрешение на запись звука

Примечание

Снятие запрета не выдаёт приложениям разрешение на микрофон и не отменяет другие настройки конфиденциальности Android. Если запись попрежнему недоступна, проверить разрешение приложения и системный переключатель доступа к микрофону. Отдельная политика *управления переключателем микрофона* определяет, может ли пользователь менять этот переключатель

Управление доступом к переключателю микрофона Android

Доступна только в MDM версии

Подготовка и запуск

Примечание

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном
2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

> **Важно**
>
> Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Шаблон **Управление доступом к переключателю «Разрешить приложениям использовать микрофон» Android устройства** управляет возможностью менять системный переключатель доступа к микрофону

> **Примечание**
>
> Требуется Android 12 или новее. На более ранней версии выполнение завершается ошибкой неподдерживаемой возможности

В поле **«Выбор действия»** выбрать **«Запретить»**, чтобы заблокировать изменение переключателя, или **«Разрешить»**, чтобы вернуть управление пользователю

> **Важно**
>
> Эта настройка не задаёт желаемое состояние микрофона и не выдаёт разрешения отдельным приложениям. Для запрета использования микрофона применить *соответствующую политику*

После применения открыть настройки конфиденциальности Android и проверить доступность переключателя. Для возврата управления пользователю выполнить действие **«Разрешить»**

Управление разрешением режима полёта Android

Доступна только в MDM версии

Подготовка и запуск

> **Примечание**
>
> Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном

2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

> **Важно**
>
> Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Шаблон **«Управление разрешением режима „в полете“ Android устройства»** управляет правом пользователя менять режим полёта

> **Примечание**
>
> Требуется Android 9 или новее. На более ранней версии выполнение завершается ошибкой неподдерживаемой возможности

В поле **«Выбор действия»** выбрать **«Запретить»** для установки ограничения или **«Разрешить»** для его снятия. Действие **«Разрешить»** возвращает пользователю управление режимом полёта, а не включает этот режим. После применения проверить доступность переключателя режима полёта в настройках Android

> **Важно**
>
> Перед массовым применением проверить связь с сервером на одном устройстве. Устройство без связи не сможет получить последующую политику для изменения ограничения

Управление разрешением менять состояние Wi-Fi Android устройства

Доступна только в MDM версии

Подготовка и запуск

> **Примечание**
>
> Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном
2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

> **Важно**
>
> Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Политика управляет правом пользователя включать и выключать Wi-Fi в настройках Android и панели быстрых настроек

> **Примечание**
>
> Требуется Android 13 или новее. На более ранней версии выполнение завершается ошибкой неподдерживаемой возможности

В поле **«Выбор действия»** выбрать **«Запретить»**, чтобы заблокировать переключение Wi-Fi пользователем, или **«Разрешить»**, чтобы снять ограничение. Текущее состояние Wi-Fi эта политика не меняет. Для включения или выключения Wi-Fi использовать *политику управления состоянием*

> **Важно**
>
> На Android 13 и новее политика управления состоянием сама устанавливает запрет на переключение пользователем. Поэтому, если пользователю нужно разрешить переключение, выполнить разрешающую политику после политики управления состоянием

После применения проверить доступность переключателя Wi-Fi на устройстве. Перезагрузка не снимает установленный запрет

Управление минимальным уровнем безопасности Wi-Fi Android устройства

Доступна только в MDM версии

Подготовка и запуск

Примечание

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном
2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

   Важно

   Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Политика задаёт минимальный уровень защиты сетей Wi-Fi, к которым может подключаться устройство

Примечание

Требуется Android 13 или новее. На более ранней версии выполнение завершается ошибкой неподдерживаемой возможности

В поле **«Выбор действия»** доступны следующие уровни:

- **«Открытые (без шифрования)»** - разрешены любые сети, включая открытые
- **«Персональные сети (WEP+)»** - открытые сети запрещены, допускаются персональные сети WEP, WPA/WPA2/WPA3 и более защищённые сети
- **«Корп. сети (EAP)»** - требуется корпоративная аутентификация EAP или более высокий уровень
- **«Усиленные корп. сети (WPA3-Enterprise 192-bit)»** - требуется WPA3-Enterprise с защитой 192 бит

Важно

Это нижняя граница защиты, а не выбор конкретной сети. Политика не создаёт профиль Wi-Fi и не передаёт пароль или сертификаты для подключения

Предупреждение

Если текущая сеть не соответствует выбранному уровню, устройство может отключиться от неё и потерять связь с сервером

До запуска подготовить подходящую сеть и проверить подключение к ней либо обеспечить резервный доступ через мобильную сеть

После применения проверить, что устройство подключается к подходящей сети и остаётся доступным серверу

Подсказка

Для снятия требования к уровню защиты выполнить политику со значением **«Открытые (без шифрования)»**. Если связь уже потеряна, сначала восстановить её через разрешённую сеть или мобильный канал, иначе новая политика не поступит

Управление разрешением на установку обоев Android устройства

Доступна только в MDM версии

Подготовка и запуск

Примечание

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном
2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

Важно

Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Политика управляет возможностью пользователя менять обои в системных настройках. Требуется Android 7 или новее. В поле **«Выбор действия»** выбрать **«Запретить»** для установки ограничения или **«Разрешить»** для его снятия. Уже установленные обои эта политика не заменяет. Для выбора корпоративного изображения использовать *установку обоев*

Подсказка

Сначала установить нужное изображение и проверить результат, затем запретить его изменение. Если при последующей замене изображения устройство сообщает, что установка обоев запрещена, сначала снять ограничение, установить новое изображение и снова применить запрет

После применения проверить доступность смены обоев в настройках Android

Установка обоев рабочего стола Android устройства

Доступна только в MDM версии

Подготовка и запуск

Примечание

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном
2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

Важно

Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Политика загружает выбранное изображение на устройство и устанавливает его в качестве обоев. В поле **«Изображение»** выбрать файл JPG, JPEG или PNG. В поле **«Куда установить обои»** выбрать **«Рабочий стол»**, **«Экран блокировки»** или **«Рабочий стол и экран блокировки»**

Примечание

На Android 7 и новее можно задавать обои для экранов раздельно. На более ранних версиях обои общие, приоритет имеет изображение рабочего стола. Не использовать такие устройства для сценария с разными изображениями на двух экранах

Изображение должно быть исправным файлом поддерживаемого формата, а не файлом другого типа с изменённым расширением. После выполнения проверить выбранные экраны на устройстве. Если установка недоступна, проверить поддержку обоев устройством и *запрет их изменения*. Для замены обоев выбрать другой файл и повторно выполнить политику

Примечание

Предыдущее изображение автоматически не восстанавливается при отключении политики

Управление экраном блокировки Android устройства

Доступна только в MDM версии

Подготовка и запуск

Примечание

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner). Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

1. Создать политику с нужным шаблоном

2. Задать **«Название»** и параметры ниже, затем сохранить политику
3. Выполнить **«Тестовый запуск»** на одном устройстве

> **Важно**
>
> Тестовый запуск применяет изменения к выбранному устройству

4. Проверить результат задания и поведение устройства до назначения политики группе

Общие настройки назначения и запуска описаны на странице *Политики*

Действие и параметры

Политика ограничивает функции защищённого экрана блокировки: камеру, уведомления, способы биометрического входа и другие возможности. Она не задаёт PIN-код или пароль и не выполняет немедленную блокировку устройства

> **Предупреждение**
>
> Перед запретом биометрии убедиться, что пользователь знает действующий PIN-код, пароль или графический ключ

Режим блокировки экрана

В поле **«Режим блокировки экрана»** выбрать:

- **«Запретить всё»** - запретить функции экрана блокировки, управляемые Android через эту политику
- **«Разрешить всё»** - снять эти ограничения, в том числе ранее заданные отдельными флажками
- **«Пользовательская настройка»** - задать отдельные ограничения

В первых двух режимах расположенные ниже индивидуальные настройки и выбор режима биометрии не учитываются. В пользовательском режиме доступны флажки:

- **«Отключать камеру»** - закрыть доступ к камере с защищённого экрана блокировки
- **«Отключать отображение уведомлений»** - скрыть уведомления на защищённом экране блокировки
- **«Отключать Trust Agents»** - запретить доверенные способы удержания устройства разблокированным, например Smart Lock
- **«Отключать ярлыки (shortcuts)»** - отключить ярлыки экрана блокировки на Android 14 и новее

Установленный флажок запрещает соответствующую функцию, снятый разрешает её в рамках этой политики. Поэтому повторный запуск с другим набором флажков меняет и ранее установленные ограничения

Биометрия

В пользовательском режиме экрана выбрать значение **«Биометрия на экране блокировки»**:

- **«Запретить всё»** - запретить доступные способы биометрической разблокировки
- **«Разрешить всё»** - снять ограничения биометрии
- **«Пользовательская настройка»** - отдельно задать запрет отпечатка пальца, лица и радужной оболочки глаза

Примечание

Отдельные флажки биометрии учитываются только при пользовательской настройке обоих режимов. Управление лицом и радужкой поддерживается с Android 9. На более ранних версиях общий запрет биометрии относится к отпечатку пальца. Настройки лица, радужки и ярлыков на неподдерживаемой версии пропускаются, поэтому успешный запуск не подтверждает применение этих конкретных ограничений

Проверка и снятие ограничений

Заблокировать экран и проверить именно выбранные функции. Запрет камеры на экране блокировки не заменяет общий запрет использования камеры в приложениях. Для снятия всех ограничений этой политики выполнить её с режимом **«Разрешить всё»**. После снятия ограничений продолжают действовать требования других политик безопасности

Создание локального пользователя

Доступна только в UEM версии

Описание

Создание локального пользователя — политика для создания новой локальной учётной записи на устройстве или обновления существующей

Политика подходит для подготовки рабочих станций, выдачи временных учётных записей и настройки локальных сервисных пользователей

Примечание

Поддерживаемые операционные системы:

- Windows

- Linux
- macOS

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Имя пользователя — имя локальной учётной записи
- Группы — одна или несколько локальных групп

> **Примечание**
>
> Если нужно указать несколько групп, перечислите их через запятую
>
> На Windows группа **«Пользователи»** добавляется по умолчанию

- Пароль — пароль локальной учётной записи
- Оболочка (Linux/MacOS) — путь к командной оболочке

> **Примечание**
>
> Если поле не заполнено, по умолчанию используется `/bin/bash`

Остальные вкладки описаны на странице *Политики*

Пример

Для создания локального пользователя `operator`:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Создание локального пользователя»**
3. Заполнить поле `Название`

   Например: Создание локального оператора
4. Заполнить поле `Имя пользователя`

   Например: operator
5. При необходимости заполнить поле `Группы`

   Например: users, docker
6. Заполнить поле `Пароль`

Например: TempPass123

7. При необходимости заполнить поле `Оболочка (Linux/MacOS)`

   Например: /bin/bash

8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве
10. После применения политики:
    - На устройстве будет создан или обновлён локальный пользователь
    - Если заполнено поле `Группы`, пользователь будет добавлен в указанные локальные группы
    - На Linux и macOS для пользователя будет использована указанная оболочка или `/bin/bash` по умолчанию

Примечание

Технические особенности:

- На Windows пользователь создаётся или обновляется через модуль `win_user`
- На Linux и macOS используется модуль `user` с созданием домашнего каталога
- Перед применением политики указанные локальные группы проверяются на существование
- Для Linux и macOS можно явно указать путь к пользовательской оболочке, а при пустом поле используется `/bin/bash`

Предупреждение

Важные предупреждения:

- На Windows встроенная группа `Пользователи` или `Users` добавляется по умолчанию
- Если указать несуществующую группу, политика может завершиться ошибкой
- Имя пользователя не должно содержать пробелы, двоеточие `:` и переводы строки
- Пароль пользователя передается как обязательный параметр и должен быть указан в одну строку

Добавление локального пользователя в группу

Доступна только в UEM версии

Описание

Добавление локального пользователя в группу — политика для добавления существующей локальной учётной записи в одну или несколько локальных групп

Политика подходит для выдачи пользователю дополнительных прав, включения в рабочие группы и обновления членства без ручного входа на устройство

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

При включении опции перезаписи текущих групп существующее членство пользователя будет заменено указанным списком

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

Важно

Для выполнения или сохранения политики название обязательно для заполнения

- Имя пользователя — имя локального пользователя, которого нужно добавить в группу
- Группы — одна или несколько локальных групп

Примечание

Поле обязательно для заполнения

Если нужно указать несколько групп, перечислите их через запятую

- Перезаписать текущие группы — заменяет текущее членство пользователя указанными группами
  - Если опция выключена, пользователь будет **добавлен** в указанные группы
  - Если опция включена, пользователь будет состоять **только** в указанных группах

Остальные вкладки описаны на странице *Политики*

Пример

Для добавления пользователя `operator` в группы `users` и `docker`:

1. Нажать на кнопку Добавить Политику на странице **Политики**
2. Выбрать шаблон политики «**Добавление локального пользователя в группу**»
3. Заполнить поле `Название`

   Например: Назначение групп оператору
4. Заполнить поле `Имя пользователя`

   Например: operator
5. Заполнить поле `Группы`

   Например: users, docker
6. Оставить опцию `Перезаписать текущие группы` выключенной
7. Нажать на кнопку Сохранить
8. Выполнить `Тестовый запуск` на устройстве
9. После применения политики:
   - Пользователь будет добавлен в указанные локальные группы

- При включенной опции перезаписи пользователь останется только в перечисленных группах

Примечание

Технические особенности:

- На Windows политика проверяет существование локального пользователя и указанных групп, а затем обновляет членство через `win_user`
- На Linux членство изменяется через системную команду `usermod`
- На macOS используется управление локальным пользователем через модуль `user`
- Поддерживается указание нескольких групп через запятую

Предупреждение

Важные предупреждения:

- При перезаписи групп пользователь может потерять существующие права доступа
- Названия локальных групп должны соответствовать системе целевого устройства
- Политика не создаёт отсутствующие группы и не создаёт отсутствующего пользователя автоматически

Удаление учетных записей из локальной группы

Доступна только в UEM версии

Описание

Удаление учетных записей из локальной группы — политика, которая позволяет исключить локального пользователя из указанной локальной группы

Политика используется для отзыва привилегий, очистки членства в административных группах и приведения локальных прав в соответствие с политиками доступа

Перед изменением членства политика проверяет существование пользователя и группы на Windows и Linux

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux

- macOS

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Пользователь — локальная учетная запись, которую необходимо удалить из группы
- Локальная группа — группа, из которой будет удален пользователь

Остальные вкладки описаны на странице *Политики*

Пример

Для удаления пользователя `operator` из группы `Administrators`:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Удаление учетных записей из локальной группы»**
3. Заполнить поле `Название`

   Например: Отзыв локальных привилегий
4. Заполнить поле `Пользователь`

   Например: operator
5. Заполнить поле `Локальная группа`

   Например: Administrators
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве
8. После применения политики:
   - Указанная учетная запись будет исключена из выбранной локальной группы
   - Если пользователя уже нет в системе или он уже исключен из группы, изменения могут не потребоваться

Примечание

Технические особенности:

- На Windows используется модуль `win_group_membership` с последующей проверкой состава группы
- На Linux удаление из группы выполняется через `gpasswd -d`
- На macOS используется штатная команда `dseditgroup`

Предупреждение

Важные предупреждения:

- Удаление пользователя из административной группы может лишить его доступа к нужным функциям
- Политика не удаляет самого пользователя, а только меняет его членство в группе
- Если локальная группа не существует, выполнение политики завершится ошибкой

Создание и удаление локальных групп

Доступна только в UEM версии

Описание

Создание и удаление локальных групп - политика для создания или удаления локальных групп на устройстве. За один запуск можно обработать несколько групп, а при создании сразу добавить в них существующих пользователей

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

Политика не создаёт пользователей: учётные записи, которых нет на устройстве, будут перечислены в результате выполнения и не будут добавлены в группы

Системные группы операционной системы удалить нельзя, такая попытка завершится ошибкой

Свойства политики

После выбора шаблона политики откроется окно с её свойствами. Вкладка **«Политика»** содержит следующие поля:

- Название - имя политики в системе
- Имена групп - одно или несколько имён локальных групп через запятую

Примечание

Для Windows имя может содержать латинские и русские буквы, цифры, пробел, подчёркивание, точку и дефис, но не может начинаться с цифры, точки или дефиса

Для Linux и macOS имя должно начинаться со строчной латинской буквы или подчёркивания и может содержать строчные латинские буквы, цифры, подчёркивание и дефис

Максимальная длина имени - 32 символа для Linux и macOS и 256 символов для Windows

Повторяющиеся имена в поле не допускаются

- Действие - режим работы политики
  - **Создать** - создаёт указанные группы; уже существующие группы остаются без изменений
  - **Удалить** - удаляет указанные группы; отсутствующие группы пропускаются
- Пользователи для добавления в группы - учётные записи, которые будут добавлены во все указанные группы

Примечание

Необязательное поле

Учитывается только при создании групп, при удалении заполненное поле пропускается

Пользователи добавляются в дополнение к их текущему членству, существующие группы пользователя сохраняются

Повторяющиеся имена в поле не допускаются

Имя пользователя не может содержать символы `" / \ [ ] : ; | = , + * ? < >`

Остальные вкладки описаны на странице *Политики*

Пример

Для создания групп разработчиков и тестировщиков с добавлением пользователей:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Создание и удаление локальных групп»**
3. Заполнить поле `Название`

Подсказка

Например: Рабочие группы отдела разработки

4. Заполнить поле `Имена групп`

Подсказка

Например: developers, testers

5. В поле `Действие` выбрать Создать
6. Заполнить поле `Пользователи для добавления в группы`

Подсказка

Например: ivanov, petrov

7. Нажать на кнопку Сохранить
8. Выполнить `Тестовый запуск` на устройстве
9. После применения политики:
   - На устройстве будут созданы группы `developers` и `testers`
   - Указанные пользователи будут добавлены в обе группы
   - В результате выполнения будет указано, какие группы созданы, а какие уже существовали

Примечание

Проверка результата:

- На Windows имена групп и пользователей сравниваются без учёта регистра, на Linux и macOS регистр учитывается
- После выполнения проверяется наличие групп и членство указанных пользователей

Предупреждение

Важные предупреждения:

- Удаление системных групп запрещено и завершается ошибкой; создание группы с именем существующей системной группы также запрещено
- Пользователи, которых нет на устройстве, пропускаются: группы при этом создаются, а список ненайденных учётных записей выводится в результате выполнения

- На Linux и macOS группа не будет удалена, если она является основной группой существующего пользователя
- Изменения состава групп применяются к пользовательской сессии после повторного входа пользователя в систему
- Поле с пользователями учитывается только при создании; при удалении групп заполненное поле не приводит к ошибке, указанные значения пропускаются

Как выбрать нужную операцию

Группы этой политики находятся в операционной системе устройства. Они не являются группами устройств в организации RuDesktop и не создают группы Active Directory

Подсказка

Чтобы добавить нового сотрудника в уже существующую локальную группу, выбрать **«Создать»**, указать имя группы и существующего пользователя. Группа останется на месте, а её состав будет дополнен. Если указаны `developers, testers` и `ivanov, petrov`, оба пользователя добавляются в обе группы. Для разного состава групп нужны отдельные политики

Действие **«Удалить»** удаляет сами группы, но не учётные записи их участников. Для исключения пользователя с сохранением группы использовать шаблон *Удаление учетных записей из локальной группы*. Если в результате перечислены ненайденные пользователи, проверить их локальные имена и наличие учётных записей на каждом целевом устройстве

После исправления выполнить политику снова

Важно

При ошибке часть групп уже может быть обработана, автоматический возврат всех изменений не выполняется. Перед повторным запуском проверить результат по каждой группе

Изменение пароля локального пользователя

Доступна только в UEM версии

Описание

Изменение пароля локального пользователя — политика для смены пароля существующей локальной учётной записи

Политика используется при плановой смене паролей, восстановлении доступа и приведении локальных учётных записей к внутренним требованиям безопасности

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

На macOS для смены пароля требуется текущий пароль пользователя

Если локальный пользователь не существует, политика завершится ошибкой

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Имя пользователя — имя существующего локального пользователя
- Новый пароль — новый пароль для учётной записи
- Старый пароль (MacOS) — текущий пароль пользователя

Важно

Поле используется только при выполнении политики на macOS

Остальные вкладки описаны на странице *Политики*

Пример

Для смены пароля локального пользователя `operator`:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Изменение пароля локального пользователя»**
3. Заполнить поле `Название`

   Например: Смена пароля оператора
4. Заполнить поле `Имя пользователя`

   Например: operator
5. Заполнить поле `Новый пароль`

Например: NewSecurePass123

6. Если политика применяется на macOS, обязательно заполнить поле `Старый пароль (MacOS)`
7. Нажать на кнопку Сохранить
8. Выполнить `Тестовый запуск` на устройстве
9. После применения политики:
    - Пароль указанной локальной учётной записи будет изменён
    - На macOS пароль будет изменён только при корректно указанном текущем пароле пользователя

Примечание

Технические особенности:

- На Windows пароль изменяется через модуль `win_user`
- На Linux смена пароля выполняется командой `chpasswd` после проверки существования пользователя
- На macOS смена пароля выполняется с использованием команды `dscl` и требует старый пароль

Предупреждение

Важные предупреждения:

- Если указать неправильный старый пароль для macOS, смена пароля не выполнится
- Политика не создаёт пользователя, а меняет пароль только существующей учётной записи
- После смены пароля могут потребоваться обновления сохраненных учетных данных в приложениях и службах

Изменение имени локального пользователя

Доступна только в UEM версии

Описание

Изменение имени локального пользователя — политика для переименования существующей локальной учётной записи на устройстве

Политика полезна при стандартизации имён учётных записей, исправлении ошибочно созданных имён и приведении локальных пользователей к корпоративному шаблону

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

Перед переименованием убедитесь, что учётная запись не используется в активной сессии и что связанные сценарии или пути будут обновлены при необходимости

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Старое имя пользователя — текущее имя локальной учётной записи
- Новое имя пользователя — новое имя учётной записи

Остальные вкладки описаны на странице *Политики*

Пример

Для переименования пользователя `v.ivanov` в `viktor.ivanov`:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Изменение имени локального пользователя»**
3. Заполнить поле `Название`

   Например: Переименование локальной учетной записи
4. Заполнить поле `Старое имя пользователя`

   Например: v.ivanov
5. Заполнить поле `Новое имя пользователя`

   Например: viktor.ivanov
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве
8. После применения политики:
   - Локальная учётная запись будет переименована

- На Linux будет также переименована основная группа пользователя и перенесен домашний каталог в `/home/<новое_имя>`
- На macOS домашний каталог будет перенесен только если используется стандартный путь `/Users/<старое_имя>`

Примечание

Технические особенности:

- На Windows переименование выполняется через системные средства управления учётными записями
- На Linux дополнительно изменяются имя домашнего каталога и имя основной группы пользователя
- На macOS политика изменяет `RecordName` пользователя и при стандартном домашнем каталоге обновляет путь `NFSHomeDirectory`
- Политика работает только с уже существующими локальными учётными записями

Предупреждение

Важные предупреждения:

- Переименование пользователя может повлиять на сценарии, пути и задания, где используется старое имя
- Перед запуском рекомендуется завершить активные сеансы пользователя
- Если новое имя уже существует в системе, политика завершится ошибкой

Удаление/Блокирование локального пользователя

Доступна только в UEM версии

Описание

Удаление/Блокирование локального пользователя — политика для удаления локальной учётной записи с устройства или её блокировки без удаления

Политика полезна для отключения доступа уволенным сотрудникам, временной блокировки учётных записей и удаления неиспользуемых локальных пользователей

При удалении политика дополнительно проверяет, не используется ли учётная запись в активной пользовательской сессии

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

Удаление пользователя является необратимым действием. Перед применением проверьте, что учётная запись действительно больше не нужна

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Имя пользователя — локальная учётная запись, к которой будет применено действие
- Действие — режим работы политики
  - **Удалить** — полностью удаляет локального пользователя с устройства
  - **Заблокировать** — запрещает вход под локальной учётной записью

Остальные вкладки описаны на странице *Политики*

Пример

Для временной блокировки локального пользователя `contractor`:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Удаление/Блокирование локального пользователя»**
3. Заполнить поле `Название`

   Например: Блокировка временного пользователя
4. Заполнить поле `Имя пользователя`

   Например: contractor
5. В поле `Действие` выбрать Заблокировать
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве
8. После применения политики:

- Вход под указанной локальной учётной записью будет запрещён
- При выборе действия удаления локальная учётная запись будет удалена с устройства

Примечание

Технические особенности:

- На Windows блокировка выполняется через отключение учётной записи
- На Linux блокировка выполняется через смену shell на блокирующий и блокировку пароля
- На macOS блокировка выполняется через `password_lock` и установку shell `/sbin/nologin`
- На Linux при удалении используется `remove: true`, поэтому вместе с учётной записью удаляется и домашний каталог пользователя

Предупреждение

Важные предупреждения:

- Удаление учётной записи может привести к потере доступа к локальным данным пользователя
- Если пользователь находится в активной сессии, удаление завершится ошибкой
- Блокировка не удаляет домашний каталог и связанные пользовательские файлы

Схема управления питанием

Доступна только в UEM версии

Описание

Схема управления питанием — политика для переключения активного плана электропитания на устройстве Windows

Политика подходит для централизованного перевода рабочих станций в режим энергосбережения или повышенной производительности

Примечание

Поддерживаемые операционные системы:

- Windows

Важно

Для варианта **«Максимальная производительность»** политика использует отдельный GUID только на Windows 11

На других версиях Windows будет применена схема **«Высокая производительность»**

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Схема управления питанием — целевой план электропитания

  Доступны следующие значения:

  - **Экономия энергии**
  - **Сбалансированная**
  - **Высокая производительность**
  - **Максимальная производительность (Windows 11 Pro)**

Остальные вкладки описаны на странице *Политики*

Пример

Для перевода рабочих станций в режим высокой производительности:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Схема управления питанием»**
3. Заполнить поле `Название`

   Например: Высокая производительность для инженерных ПК
4. В поле `Схема управления питанием` выбрать Высокая производительность
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Windows
7. После применения политики:
   - Активный план электропитания на устройстве будет изменён
   - Система перейдёт в выбранный режим энергопотребления

Примечание

Технические особенности:

- Политика применяется только на устройствах Windows

- Для переключения используется системная утилита `powercfg.exe`
- Конкретный GUID плана питания подставляется автоматически в зависимости от выбранного режима

Предупреждение

Важные предупреждения:

- Не все планы электропитания доступны на каждой редакции Windows
- При выборе варианта **«Максимальная производительность (Windows 11 Pro)»** на версиях Windows ниже 11 фактически будет использована схема **«Высокая производительность»**
- Переключение на режим высокой производительности может увеличить энергопотребление устройства
- На ноутбуках изменение плана может заметно повлиять на время автономной работы

Применение конфигурации Kickstart

Доступна в УД и UEM версиях

Описание

Применение конфигурации Kickstart — политика для запуска конфигурации Kickstart на удалённом устройстве

Политика полезна для быстрого применения заранее подготовленных стартовых настроек без ручного запуска команды на целевой системе

Шаблон не содержит дополнительных параметров и просто запускает на устройстве команду `rudesktop --kickstart`

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующее поле:

- Название — имя политики в системе

Примечание

Дополнительные параметры для этой политики не требуются

Остальные вкладки описаны на странице *Политики*

Пример

Для запуска применения конфигурации Kickstart:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Применение конфигурации Kickstart»**
3. Заполнить поле `Название`

   Например: Применение стартовой конфигурации
4. Нажать на кнопку Сохранить
5. Выполнить `Тестовый запуск` на устройстве
6. После применения политики:
   - На устройстве будет запущена команда `rudesktop --kickstart`
   - Если команда завершится успешно, будет применена доступная на устройстве конфигурация Kickstart

Примечание

Технические особенности:

- Политика не требует дополнительных полей кроме названия
- На целевом устройстве выполняется команда `rudesktop --kickstart`
- Поддерживается запуск на Windows, Linux и macOS
- Политика завершается ошибкой, если команда возвращает ненулевой код

Предупреждение

Важные предупреждения:

- Для выполнения на устройстве должен быть доступен клиент `rudesktop` и право запуска команды
- Рекомендуется предварительно проверить работу конфигурации на тестовом устройстве

Управление режимом «Киоск» на Windows, Linux и macOS

Доступна только в UEM версии

Описание

Управление режимом «Киоск» на Windows, Linux и macOS — политика для включения или выключения режима киоска на устройстве, выбора приложения для запуска и передачи ему аргументов

Политика подходит для терминалов самообслуживания, информационных стоек, демонстрационных стендов и других сценариев, где устройство должно работать только с одним приложением

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

Реализация режима киоска зависит от операционной системы:

- **Windows** — политика заменяет системный shell через Winlogon и может дополнительно настроить автоматический вход в учетную запись
- **Linux** — политика создает автозапуск приложения в графической сессии через `/etc/xdg/autostart`
- **macOS** — политика создает LaunchAgent для автоматического запуска приложения

Рекомендуется:

- Предварительно проверять, что путь к приложению указан полностью и приложение уже установлено на устройстве
- Тестировать политику на одном устройстве перед массовым применением

- Учитывать, что на Windows изменения вступают в силу после следующего входа пользователя в систему
- Учитывать, что на Linux и macOS для применения настроек может потребоваться повторный вход пользователя

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Действие — основное действие политики
  - **Включить** — активирует режим киоска и настраивает запуск выбранного приложения
  - **Выключить** — отключает режим киоска и удаляет ранее созданную конфигурацию
- Путь до приложения — полный путь к приложению, которое должно запускаться в режиме киоска

  Важно

  Поле обязательно при выборе действия **«Включить»**

  Примеры:

  - **Windows:** `C:\Program Files\App\app.exe`
  - **Linux:** `/usr/bin/firefox`
  - **macOS:** `/Applications/Safari.app`

- Аргументы запуска — необязательные параметры запуска приложения

  Например: `--kiosk https://example.org`

- Автологон Windows — включает или отключает автоматический вход в Windows

Примечание

Поле используется только для Windows

- **Да** — после перезагрузки или выхода из системы Windows автоматически войдет в указанную учетную запись
- **Нет** — автологон не настраивается

- Учетная запись автологина Windows — учетная запись для автоматического входа

Важно

Поле используется только для Windows и только если для параметра **«Автологон Windows»** выбрано значение **«Да»**

Можно указать:

- локальную учетную запись, например: `kiosk`
- локальную учетную запись в явном виде, например: `.\kiosk`
- доменную учетную запись, например: `DOMAIN\kiosk`

- Пароль автологина Windows — пароль указанной учетной записи для автоматического входа

Важно

Поле используется только для Windows и только если для параметра **«Автологон Windows»** выбрано значение **«Да»**

Остальные вкладки описаны на странице *Политики*

Пример

Для настройки браузера в режиме киоска на Windows-устройстве:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Управление режимом «Киоск» на Windows, Linux и macOS»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Киоск для стойки регистрации
4. В поле `Действие` выбрать значение Включить
5. В поле `Путь до приложения` указать путь к приложению

   Например: C:\Program Files\Google\Chrome\Application\chrome.exe

6. При необходимости заполнить поле `Аргументы запуска`

   Например: –kiosk https://portal.company.local

7. Если устройство должно автоматически входить в учетную запись после перезагрузки, включить `Автологон Windows` и указать учетные данные
8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:
    - Приложение будет запускаться в режиме киоска при следующем входе пользователя в систему

Включение режима «Киоск» на Android

Доступна только в MDM версии

Описание

Включение режима «Киоск» на Android — политика для перевода устройства Android в ограниченный режим с запуском только одного указанного приложения

Политика подходит для специализированных сценариев:

- Информационные киоски
- Терминалы для клиентов
- Устройства для демонстрации продукции
- Контролируемого доступа к определенному функционалу

Примечание

Поддерживаемые операционные системы:

- Android 9 и выше

Важно

Эта политика заметно ограничивает функциональность устройства

Рекомендуется:

- Тщательно тестировать режим киоска перед развертыванием на рабочих устройствах
- Сохранять пароль для выхода из режима киоска в надежном месте
- Убедиться, что выбранное приложение стабильно работает в полноэкранном режиме

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

- Выбор действия — основное действие для применения к устройству
  - **Включить** — активирует режим киоска с указанными параметрами
  - **Выключить** — отключает режим киоска и восстанавливает стандартную функциональность устройства

> **Примечание**
>
> При выборе действия **«Выключить»** параметры интерфейса, пакет и настройки выхода из режима киоска не применяются

- Имя пакета — идентификатор Android-приложения для запуска в режиме киоска

> **Важно**
>
> Указывается только при выборе действия **«Включить»**
>
> Пример: `com.companyname.appname`

- Функции системного пользовательского интерфейса — настройка доступных элементов интерфейса

  Доступны следующие опции только при включении режима киоска:

  - **Отключить все функции системного пользовательского интерфейса** — отключение всех функций системного пользовательского интерфейса
  - **Показать кнопку «Домой»** — отображает стандартную кнопку возврата на главный экран
  - **Показать кнопку «Обзор»** — отображает кнопку переключения между приложениями

Важно

При активации этой опции, также должна быть активна кнопка **«Домой»**

- **Включить диалоговое окно глобальных действий** — позволяет открывать меню питания при длительном нажатии

Примечание

Если отключить эту опцию, пользователь не сможет открыть меню питания

- **Включить уведомления для всех приложений** — активирует показ уведомлений для всех приложений

Важно

При этом отображаются значки уведомлений в строке состояния, всплывающие уведомления и расширяемая панель уведомлений

Если включить эту опцию, также необходимо включить кнопку **«Домой»**. Нажатие на действия уведомлений и кнопки, открывающие новые панели, в режиме киоска не работает

- **Включить область системной информации в строке состояния** — отображает индикаторы сети, батареи, звука
- **Включить экран блокировки** — активирует стандартный экран блокировки устройства

Важно

Не подходит для устройств с общедоступными пользователями, таких как информационные киоски или цифровые вывески

- Опции для выхода из режима киоск — настройка механизма выхода из ограниченного режима
  - **Активация установки пароля выхода из режима киоск** — включает выход из режима **«Киоск»** по паролю
  - **Пароль** — пароль для выхода из режима киоска

Важно

Чтобы пароль применился, необходимо включить чекбокс **Активация установки пароля выхода из режима киоск**

- **Таймаут** — время в минутах до автоматического возврата в режим киоска

Важно

* По умолчанию: 30 минут
* Режим **«Киоск»** автоматически активируется после перезагрузки устройства или по истечении указанного времени

- **Выбор положения области скрытой кнопки** — расположение невидимой области для активации окна ввода пароля

Важно

* Положение по умолчанию: Вверху слева
* Необходимо выполнить 5 нажатий за 2 секунды в выбранную область
* Также форму ввода пароля можно вызвать 10 нажатиями на клавишу уменьшения громкости

Примечание

Для работы скрытого меню выхода может потребоваться разрешение **«Отображать поверх других приложений»**

После изменения параметров выхода из режима киоска на части устройств может потребоваться перезапуск

Остальные вкладки описаны на странице *Политики*

Пример

Для настройки устройства Android в качестве информационного киоска с приложением `com.company.presentation`:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Включение режима «Киоск» на Android»** из списка предложенных шаблонов

3. Заполнить поле `Название`

   Например: Настройка инфокиоска для презентации

4. Выбрать действие `Выбор действия`

   Например: Включить

5. Заполнить поле `Имя пакета`

   Например: com.company.presentation

6. Настроить `Функции системного пользовательского интерфейса`

   Например:

   - Отключить все функции системного пользовательского интерфейса — включено
   - Остальные опции — отключены

7. Настроить `Опции для выхода из режима киоск`

   Например:

   - Активация установки пароля выхода из режима киоск — включено
   - Пароль — `AdminExit123`
   - Таймаут — `30`
   - Выбор положения области скрытой кнопки — `Вверху слева`

8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:

    - На устройстве будет активирован режим киоска
    - Будет запущено приложение `com.company.presentation` в полноэкранном режиме
    - Будут применены выбранные ограничения системного интерфейса
    - Для выхода из режима потребуется:

      1. Нажать 5 раз за 2 секунды в левом верхнем углу экрана
      2. Ввести пароль: `AdminExit123`
      3. После перезагрузки или 30 минут устройство вернется в режим киоска

    Форму ввода пароля также можно открыть 10 нажатиями на клавишу уменьшения громкости

Ввод устройства в домен

Доступна только в UEM версии

Описание

Ввод устройства в домен — политика для ввода устройства в домен Active Directory на Windows, Linux и macOS

Политика проверяет входные параметры, подготавливает настройки, выполняет ввод в домен средствами соответствующей ОС и затем подтверждает результат

Примечание

Поддерживаемые операционные системы:

- Windows
- macOS
- Linux

Важно

Для ввода устройства в домен требуется доменная учётная запись с правом присоединять устройства к Active Directory

Перед запуском политики рекомендуется:

- указывать корректное DNS-имя домена
- заранее проверить доступность контроллера домена и корректность DNS
- убедиться, что имя устройства соответствует требованиям доменной инфраструктуры
- выполнять тестовый запуск на одном устройстве перед массовым применением

Примечание

Ключевые особенности работы политики:

- Для Linux и macOS обязательно требуется указать адрес контроллера домена
- Для Windows поле адреса контроллера домена необязательно, но при его указании политика может дополнительно настроить DNS сетевых адаптеров

- Поле `Имя подразделения` поддерживается на Windows, Linux и macOS. Если оставить его пустым, учетная запись компьютера будет создана в контейнере или подразделении по умолчанию
- Если устройство уже состоит в другом домене, политика завершится ошибкой и не будет автоматически переключать устройство между доменами
- При повторном запуске с теми же параметрами политика не должна повторно вводить устройство в домен, если состояние уже корректно подтверждено
- На некоторых Linux-системах команда `realm list` может не показывать текущее подключение даже при успешном вводе в домен. В таких случаях политика опирается на `adcli testjoin` и наличие рабочих конфигурационных файлов
- На Linux-системах, где `adcli` не поддерживает команду `show-computer`, политика пропускает эту проверку и подтверждает ввод по `adcli testjoin` и обязательным файлам конфигурации
- Если на Linux обнаружено неполное предыдущее подключение к домену, политика может сначала очистить старое состояние и затем повторно выполнить ввод в домен

Особенности по операционным системам

Windows

На Windows политика:

- при необходимости настраивает DNS-серверы сетевых адаптеров
- поддерживает указание подразделения Active Directory для создаваемой учетной записи компьютера
- автоматически перезагружает устройство только в том случае, если это требуется для завершения ввода в домен

Если Windows-устройство уже состоит в другом домене, политика завершится ошибкой и предложит сначала вывести устройство из текущего домена

macOS

На macOS политика:

- проверяет доступность встроенного AD-коннектора macOS
- настраивает DNS search domain и DNS-сервер на доступных сетевых сервисах
- проверяет разрешение домена, а также наличие LDAP и Kerberos SRV-записей
- пытается настроить синхронизацию времени с контроллером домена
- поддерживает указание подразделения Active Directory

- при необходимости использует нормализованный `Computer ID`, если локальное имя устройства содержит неподходящие символы

После успешного ввода macOS-устройства автоматическая перезагрузка не выполняется, но пользователю рекомендуется выйти из текущей сессии и войти доменной учетной записью

Linux

На Linux политика выполняет больше подготовительных действий, чем на Windows и macOS

Она может:

- автоматически установить необходимые пакеты для работы с доменом
- проверить текущее состояние доменного подключения до начала изменений
- восстановить неполное предыдущее подключение к домену
- настроить синхронизацию времени с контроллером домена
- получить сведения о домене через `realm` и `adcli`
- настроить `/etc/krb5.conf` и `/etc/sssd/sssd.conf`
- при необходимости скорректировать `/etc/hosts`
- настроить PAM и `/etc/nsswitch.conf`
- перезапустить и проверить службы `sssd` и, на части систем, `oddjobd`
- после успешного ввода в домен автоматически перезагрузить устройство

Предупреждение

Что может изменить политика на Linux:

- `/etc/chrony.conf`
- `/etc/krb5.conf`
- `/etc/sssd/sssd.conf`
- `/etc/hosts`
- `/etc/nsswitch.conf`
- PAM-конфигурацию, включая `/etc/pam.d/common-*` или `/etc/pam.d/system-auth`

Если на устройстве уже есть собственная нестандартная доменная или PAM-конфигурация, перед применением политики рекомендуется проверить её совместимость

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

- Имя домена — DNS-имя домена Active Directory, в который нужно ввести устройство

> **Важно**
>
> Указывайте именно DNS-имя домена
>
> Пример: `corp.company.local`

- Адрес контроллера домена — IP-адрес или FQDN контроллера домена Active Directory

> **Примечание**
>
> Для Linux и macOS это поле обязательно
>
> Для Windows поле необязательно, но может использоваться для настройки DNS сетевых интерфейсов
>
> Примеры: `192.168.10.157` или `dc01.corp.company.local`

- Имя администратора домена — имя доменной учетной записи, имеющей право присоединять устройства к домену

> **Важно**
>
> Указывайте учетную запись с правом ввода устройств в домен
>
> Пример: `Administrator` или `Администратор`

- Пароль администратора домена — пароль доменной учетной записи администратора
- Имя подразделения — необязательный параметр, позволяющий указать LDAP DN подразделения Active Directory, в котором должна быть создана учетная запись компьютера

Примечание

Поле поддерживается на Windows, Linux и macOS

Примеры:

- `OU=Linux,OU=Servers`
- `OU=Linux,OU=Servers,DC=corp,DC=local`

Если поле оставить пустым, учетная запись компьютера будет создана в контейнере или подразделении по умолчанию, настроенном в домене

Важно

Поле должно быть указано в формате LDAP DN

Остальные вкладки описаны на странице *Политики*

Как работает политика

Общая логика

При выполнении политика:

1. проверяет входные параметры
2. определяет тип операционной системы
3. проверяет, поддерживается ли ввод устройства в домен для данной ОС
4. подготавливает параметры подключения
5. выполняет ввод устройства в домен средствами соответствующей ОС
6. проверяет, что доменное подключение действительно работает
7. формирует итоговый результат выполнения

Что дополнительно делает Linux-ветка

На Linux политика выполняет расширенный сценарий:

1. проверяет текущее состояние доменного подключения
2. проверяет корректность hostname устройства
3. при необходимости устанавливает доменные зависимости
4. настраивает время и DNS/Kerberos-параметры
5. получает сведения о контроллере домена
6. выполняет ввод через `realm join` или резервно через `adcli join`
7. настраивает `krb5.conf`, `sssd.conf`, PAM и NSS

8. перезапускает службы и проверяет готовность доменной аутентификации
9. подтверждает успешный ввод через `adcli testjoin` и наличие обязательных файлов, а при поддержке дополнительно через `adcli show-computer`
10. запускает отложенную перезагрузку устройства

Пример

Для ввода устройства в домен необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Ввод устройства в домен»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Ввод устройства в домен
4. Заполнить поле `Имя домена`

   Например: corp.company.local
5. Заполнить поле `Адрес контроллера домена`

   Например: 192.168.10.157
6. Заполнить поле `Имя администратора домена`

   Например: Администратор
7. Заполнить поле `Пароль администратора домена`

   Например: Пароль
8. При необходимости заполнить поле `Имя подразделения`

   Например: OU=Linux,OU=Servers,DC=corp,DC=local
9. Нажать на кнопку Сохранить
10. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
11. После применения политики:
    - Устройство будет введено в указанный домен
    - На Windows устройство может быть автоматически перезагружено, если это требуется для завершения ввода в домен
    - На Linux устройство будет автоматически перезагружено после успешного ввода в домен
    - На macOS рекомендуется выйти из текущей сессии и войти доменной учетной записью
    - На Linux будут изменены системные настройки, необходимые для работы доменной аутентификации

Нюансы и возможные причины ошибок

Общие причины проблем

При вводе устройства в домен учитывайте:

- Некорректные DNS-настройки — одна из самых частых причин ошибок ввода в домен
- Неверное имя домена, адрес контроллера домена, имя администратора или пароль приведут к ошибке подключения
- Если устройство уже состоит в другом домене, политика не будет переключать его автоматически
- Перед массовым применением политики рекомендуется выполнить тестовый запуск на одном устройстве

Нюансы Linux

- Для Linux обязательно указывать адрес контроллера домена
- Linux-ветка чувствительна к корректности времени. Если время устройства заметно отличается от времени контроллера домена, Kerberos-аутентификация может не работать
- Если hostname устройства некорректный, политика завершится ошибкой до попытки ввода в домен
- Если в домене уже существует конфликтующая учетная запись компьютера с тем же именем, политика завершится ошибкой
- Если `realm discover` не смог обнаружить домен, политика попытается продолжить работу через `adcli`
- Если `realm list` после ввода не показывает домен, но `adcli testjoin` проходит успешно, политика все равно может считать ввод успешным
- Если команда `adcli show-computer` недоступна в используемой версии `adcli`, политика пропустит эту проверку и продолжит подтверждение ввода по доступным проверкам
- Если доменная учетная запись после ввода не начинает резолвиться через SSSD/NSS, вход пользователя может не работать до устранения проблемы
- На Astra Linux политика дополнительно отключает `ad_gpo_access_control` в `sssd.conf`, чтобы доменный вход не блокировался на сервисе `fly-dm` после успешного ввода в домен
- После успешного ввода Linux-устройство перезагружается автоматически, поэтому это нужно учитывать при запуске политики на рабочих машинах

Нюансы macOS

- На macOS должен быть доступен `/usr/sbin/dsconfigad`
- Для успешного ввода macOS-устройства в домен особенно важны корректные SRV-записи DNS и синхронизация времени
- Если локальное имя компьютера содержит неподходящие символы, для привязки может использоваться измененный `Computer ID`
- При ошибке вида `Node name wasn't found. (2000)` следует дополнительно проверить синхронизацию времени и DNS

Нюансы Windows

- На Windows политика может изменить DNS-настройки сетевых интерфейсов, если указан адрес контроллера домена
- После успешного ввода в домен Windows-устройство перезагружается только при необходимости

Вывод устройства из домена

Доступна только в UEM версии

Описание

Вывод устройства из домена — политика для вывода устройства из домена Active Directory на Windows, Linux и macOS

При необходимости политика также может сбросить DNS-настройки сетевых интерфейсов после вывода из домена

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Важно

Для вывода устройства из домена требуется учётная запись с соответствующими правами

Рекомендуется:

- Указывать корректное имя текущего домена устройства
- Проверять учётную запись администратора домена перед запуском политики

- Использовать сброс DNS-настроек только если устройство больше не должно использовать доменные DNS-серверы

Примечание

Дополнительные особенности работы политики:

- При повторном запуске с теми же параметрами политика не выполняет вывод повторно, если устройство уже выведено из указанного домена
- На macOS вывод из домена выполняется через штатный инструмент `dsconfigad`
- На Linux для вывода из домена используется утилита `realm`
- На Linux политика может предварительно установить пакет `realmd`, если он отсутствует на устройстве
- На Alt Linux политика выполняет `realm leave --remove` и дополнительно удаляет объект компьютера из Active Directory
- После вывода Linux-устройства из домена политика очищает кеш SSSD и перезапускает службы `sssd` и `oddjobd`
- Если устройство состоит в другом домене, политика завершится ошибкой проверки состояния

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Домен — DNS-имя домена, из которого нужно вывести устройство

  Важно

  Указывайте именно текущий домен устройства

  Пример: `corp.company.local`

- Сбросить DNS-настройки — параметр, определяющий, нужно ли сбросить DNS-настройки устройства после вывода из домена

Примечание

Если выбрать значение `Да`, политика сбросит DNS-настройки сетевых интерфейсов после вывода устройства из домена

Это удобно, если устройство больше не должно использовать DNS-контроллер домена

Политика не восстанавливает прежние пользовательские DNS-настройки, а очищает или сбрасывает их к значениям, которые задает операционная система или сетевой профиль

- Имя администратора домена — учётная запись, имеющая право выводить устройства из домена

Важно

Указывайте учётную запись с правом вывода устройств из домена

Пример: `Administrator` или `Администратор`

- Пароль администратора — пароль учётной записи администратора домена

Остальные вкладки описаны на странице *Политики*

Пример

Для вывода устройства из домена с одновременным сбросом DNS-настроек необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Вывод устройства из домена»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Вывод устройства из домена
4. Заполнить поле `Домен`

   Например: win2012.local
5. Заполнить поле `Сбросить DNS-настройки`

   Например: Да
6. Заполнить поле `Имя администратора домена`

   Например: Администратор
7. Заполнить поле `Пароль администратора`

   Например: Пароль

8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:
    - Устройство будет выведено из указанного домена
    - При включенном параметре `Сбросить DNS-настройки` будут сброшены DNS-настройки сетевых интерфейсов
    - Для macOS и Linux после успешного вывода рекомендуется повторный вход пользователя в систему

Предупреждение

При выводе устройства из домена учитывайте:

- После вывода доменные учётные записи могут перестать работать на устройстве до повторной настройки доступа
- Если устройство продолжит использовать доменные DNS-серверы без необходимости, это может вызывать задержки или ошибки разрешения имен
- При включенном параметре `Сбросить DNS-настройки` будут изменены текущие настройки сетевых интерфейсов, поэтому при наличии ручной DNS-конфигурации её может потребоваться настроить заново
- На Windows после успешного вывода из домена может потребоваться перезагрузка устройства

Управление отслеживанием геолокации Android

Доступна только в MDM версии

Описание

Управление отслеживанием геолокации Android — политика для управления сбором и отправкой данных о местоположении Android-устройств на сервер **RuDesktop**

Политика подходит для мониторинга перемещения корпоративных устройств, поиска утерянных устройств и задач логистики

Примечание

Поддерживаемые операционные системы:

- Android

Важно

Отслеживание геолокации связано с конфиденциальностью пользователей

Рекомендуется:

- Использовать минимально необходимый интервал обновления
- Регулярно удалять устаревшие данные геолокации

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Выбор действия — основное действие для управления отслеживанием геолокации
  - **Включить** — активирует сбор и отправку данных о местоположении устройства
  - **Выключить** — отключает сбор и отправку данных о местоположении устройства

  Примечание

  При выборе действия **«Выключить»** значение интервала обновления не используется

- Интервал обновления геолокации — частота обновления данных о местоположении в минутах

  Важно

  Указывается только при выборе действия **«Включить»**
  - Минимальное значение: 1 минута
  - По умолчанию: 1 минута

  Примечание

  Более частые обновления дают более точное отслеживание, но увеличивают расход заряда батареи

Остальные вкладки описаны на странице *Политики*

Пример

Для включения отслеживания геолокации устройства курьера с обновлением каждые 5 минут:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Управление отслеживанием геолокации Android»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Отслеживание геолокации курьерских устройств
4. Выбрать действие `Выбор действия`

   Например: Включить
5. Заполнить поле `Интервал обновления геолокации`

   Например: 5

   > **Примечание**
   >
   > Интервал 5 минут обеспечивает баланс между точностью отслеживания и энергопотреблением
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
8. После применения политики:
   - На устройстве будет включена отправка геолокации
   - Данные о местоположении будут отправляться на сервер каждые 5 минут
   - Геолокация будет доступна для просмотра на странице *Карта*

Для отключения отслеживания геолокации:

1. Заполнить поле `Название`

   Например: Отключение отслеживания геолокации
2. Выбрать действие `Выбор действия`

   Например: Выключить
3. Нажать на кнопку Сохранить
4. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
5. После применения политики:

- Сбор и отправка данных о местоположении будут прекращены

Примечание

Технические особенности:

- Политика включает или отключает отправку геолокации отдельной MDM-командой
- Интервал обновления передается только при включении отслеживания
- Требует разрешений на доступ к местоположению
- Точность зависит от доступных источников: GPS, Wi-Fi и мобильных сетей

Предупреждение

Важные предупреждения:

- Отслеживание геолокации значительно увеличивает расход батареи
- Требует включенных служб геолокации на устройстве
- Может не работать в помещениях или при плохом сигнале GPS
- Точность в городской среде выше, чем в сельской
- Для работы необходим доступ в интернет для отправки данных на сервер **RuDesktop**

Блокировка Android устройства

Доступна только в MDM версии

Описание

Блокировка Android устройства — политика для удалённой установки PIN-кода и ограничения числа неверных попыток ввода перед очисткой

Политика полезна для экстренного ограничения доступа к устройству и усиления защиты корпоративных Android-устройств

Примечание

Поддерживаемые операционные системы:

- Android

Важно

Для выполнения политики нужно включить хотя бы один из переключателей: установку PIN-кода или ограничение числа попыток ввода

Поле `Пароль` используется именно для PIN-кода и должно содержать не менее 4 цифр

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Активация установки PIN-кода — включает установку PIN-кода на устройстве
- Пароль — PIN-код устройства

Важно

Поле используется только при включенной опции **«Активация установки PIN-кода»**

Минимальная длина PIN-кода: 4 цифры

- Активация ограничения на количество попыток ввода пароля — включает контроль числа неверных попыток
- Количество попыток ввода — допустимое число неверных попыток

Важно

Поле используется только при включенной опции ограничения попыток

Если значение не указано, политика завершится ошибкой

Остальные вкладки описаны на странице *Политики*

Пример

Для установки PIN-кода `2580` и ограничения до 10 неверных попыток:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Блокировка Android устройства»**
3. Заполнить поле `Название`

   Например: Экстренная блокировка устройства
4. Включить опцию `Активация установки PIN-кода`

5. Заполнить поле Пароль

   Например: 2580

6. Включить опцию Активация ограничения на количество попыток ввода пароля
7. Заполнить поле Количество попыток ввода

   Например: 10

8. Нажать на кнопку Сохранить
9. Выполнить Тестовый запуск на устройстве Android
10. После применения политики:
    - На устройстве будет установлен PIN-код, если включена соответствующая опция
    - При необходимости будет задано ограничение на количество неверных попыток ввода

Примечание

Технические особенности:

- Политика использует отдельные MDM-команды для установки PIN-кода и ограничения числа попыток
- PIN-код передается только при включении опции его установки
- Ограничение числа попыток задается отдельной командой и может применяться независимо

Предупреждение

Важные предупреждения:

- Если забыть установленный PIN-код, разблокировка устройства может потребовать дополнительных действий администратора
- Слишком малое число допустимых попыток может привести к нежелательной очистке устройства, если такая логика включена на стороне Android
- Политика не выполнится, если не выбран ни один из переключателей

Управление запретом использования камеры на Android

Доступна только в MDM версии

Описание

Управление запретом использования камеры на Android — политика для централизованного разрешения или запрета использования камеры на Android-устройстве

Политика подходит для устройств в зонах с ограничениями по фото- и видеосъемке, терминалов самообслуживания и корпоративных устройств с повышенными требованиями безопасности

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — разрешение или запрет использования камеры
  - **Запретить** — отключает использование камеры на устройстве
  - **Разрешить** — возвращает доступ к камере

Примечание

Политика управляет общей настройкой камеры на устройстве, а не доступом отдельного приложения к камере

Остальные вкладки описаны на странице *Политики*

Пример

Для запрета использования камеры на корпоративных терминалах:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление запретом использования камеры на Android»**
3. Заполнить поле `Название`

   Например: Запрет камеры на терминалах
4. В поле `Выбор действия` выбрать Запретить
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android

7. После применения политики:
    - Использование камеры на устройстве будет запрещено или разрешено в зависимости от выбранного действия

Примечание

Технические особенности:

- Для применения используются MDM-команды Android
- Политика меняет именно системное разрешение на использование камеры на устройстве
- Действие применяется без необходимости ручной настройки на самом устройстве

Предупреждение

Важные предупреждения:

- Запрет камеры может повлиять на работу приложений, которым требуется фото- или видеосъемка
- После включения запрета пользователь не сможет использовать встроенную камеру до обратного применения политики
- Перед массовым разворачиванием рекомендуется проверить совместимость с рабочими приложениями

Управление доступом к режиму разработчика на Android

Доступна только в MDM версии

Описание

Управление доступом к режиму разработчика на Android — политика для разрешения или запрета использования режима разработчика на Android-устройстве

Политика помогает снизить риск несанкционированной отладки, подключения через ADB и изменения системных настроек пользователем

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — настройка доступа к режиму разработчика
  - **Запретить** — запрещает использование режима разработчика
  - **Разрешить** — разрешает доступ к режиму разработчика

Примечание

Политика управляет общей доступностью режима разработчика на устройстве

Остальные вкладки описаны на странице *Политики*

Пример

Для запрета режима разработчика на корпоративных смартфонах:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление доступом к режиму разработчика на Android»**
3. Заполнить поле `Название`

   Например: Запрет режима разработчика
4. В поле `Выбор действия` выбрать Запретить
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - Доступ к режиму разработчика будет запрещен или разрешен в зависимости от выбранного действия

Примечание

Технические особенности:

- Политика использует MDM-команды для управления режимом разработчика
- Применение выполняется централизованно без физического доступа к устройству
- Сценарий рассчитан на управляемые Android-устройства

Предупреждение

Важные предупреждения:

- Запрет режима разработчика может ограничить диагностику и обслуживание устройства
- Разрешение режима разработчика увеличивает риск несанкционированной отладки
- Перед изменением настройки стоит учесть требования безопасности вашей организации

Управление запретом на удаление Android приложений пользователем

Доступна только в MDM версии

Описание

Управление запретом на удаление Android приложений пользователем — политика для запрета или разрешения пользователю вручную удалять приложения на устройстве Android

Политика особенно полезна для киосков, корпоративных планшетов и мобильных рабочих мест, где набор приложений должен оставаться неизменным

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — разрешение или запрет пользовательского удаления приложений

- **Разрешить** — пользователь сможет вручную удалять приложения
- **Запретить** — пользователь не сможет вручную удалять приложения

Примечание

Политика управляет именно ручным удалением приложений пользователем на устройстве

Остальные вкладки описаны на странице *Политики*

Пример

Для запрета удаления приложений на рабочих планшетах:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление запретом на удаление Android приложений пользователем»**
3. Заполнить поле `Название`

   Например: Запрет удаления приложений
4. В поле `Выбор действия` выбрать Запретить
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - Пользователь сможет или не сможет удалять приложения вручную в зависимости от выбранного действия

Примечание

Технические особенности:

- Политика управляет пользовательским удалением приложений через MDM-команды
- Ограничение применяется на уровне управляемого Android-устройства
- Настройка действует для ручных действий пользователя на устройстве
- Действие можно изменить повторным запуском политики с противоположным выбором

Предупреждение

Важные предупреждения:

- Запрет удаления приложений может затруднить самостоятельную очистку устройства пользователем
- Рекомендуется сочетать эту политику с контролем установки приложений
- Перед включением запрета убедитесь, что набор приложений на устройстве уже приведен к нужному состоянию

Управление запретом на установку Android приложений пользователем

Доступна только в MDM версии

Описание

Управление запретом на установку Android приложений пользователем — политика для запрета или разрешения пользователю самостоятельно устанавливать приложения на Android-устройство

Политика помогает ограничить установку непроверенного ПО и сохранить контролируемый состав приложений на устройстве

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — разрешение или запрет пользовательской установки приложений
  - **Разрешить** — пользователь сможет устанавливать приложения вручную
  - **Запретить** — пользователь не сможет устанавливать приложения вручную

Примечание

Политика управляет именно ручной установкой приложений пользователем на устройстве

Остальные вкладки описаны на странице *Политики*

Пример

Для запрета установки приложений на управляемых устройствах:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление запретом на установку Android приложений пользователем»**
3. Заполнить поле `Название`

   Например: Запрет установки приложений
4. В поле `Выбор действия` выбрать Запретить
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - Пользователь сможет или не сможет самостоятельно устанавливать приложения в зависимости от выбранного действия

Примечание

Технические особенности:

- Политика использует MDM-команды для управления пользовательской установкой приложений
- Ограничение применяется на уровне устройства, а не отдельного приложения
- Действие можно в любой момент изменить повторным запуском политики с противоположным выбором

Предупреждение

Важные предупреждения:

- Запрет установки приложений может ограничить работу пользователей вне заранее утвержденного набора ПО
- Если пользователю нужны дополнительные приложения, их придется устанавливать централизованно
- Перед включением запрета рекомендуется проверить, что все необходимые приложения уже установлены

Управление действиями на устройстве Android при изменении SIM-карты

Доступна только в MDM версии

Описание

Управление действиями на устройстве Android при изменении SIM-карты — политика для настройки реакции устройства на смену SIM-карты: блокировки, полного сброса, снятия защиты или просмотра текущей конфигурации

Политика используется для защиты устройств от несанкционированной замены SIM-карты и потери корпоративного контроля над устройством

Примечание

Поддерживаемые операционные системы:

- Android

Важно

Для действий **«Заблокировать устройство при изменении SIM-карты»** и **«Полный сброс устройства»** требуется PIN-код, состоящий только из цифр

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — реакция устройства на изменение SIM-карты
  - **Заблокировать устройство при изменении SIM-карты**
  - **Полный сброс устройства (wipe) при изменении SIM-карты**
  - **Удалить существующую привязку SIM-карты**
  - **Показать текущую конфигурацию защиты от смены SIM-карты**

Примечание

При выборе действия **«Удалить существующую привязку SIM-карты»** политика снимает ранее настроенную защиту и для сценария блокировки, и для сценария полного сброса

- Введите PIN-код — PIN-код для сценариев блокировки или сброса

Важно

Поле обязательно только для действий блокировки или полного сброса

Остальные вкладки описаны на странице *Политики*

Пример

Для блокировки устройства при смене SIM-карты с PIN-кодом 1234:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление действиями на устройстве Android при изменении SIM-карты»**
3. Заполнить поле `Название`

   Например: Защита от смены SIM
4. В поле `Выбор действия` выбрать Заблокировать устройство при изменении SIM-карты
5. Заполнить поле `Введите PIN-код`

   Например: 1234
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве Android
8. После применения политики:
   - На устройстве будет настроена выбранная реакция на смену SIM-карты
   - При выборе режима блокировки или сброса будет использоваться заданный PIN-код
   - При выборе действия просмотра политика вернёт текущую конфигурацию защиты без изменения настроек

Примечание

Технические особенности:

- Политика поддерживает четыре режима: блокировка, сброс, снятие защиты и запрос текущей конфигурации
- Для сценариев блокировки и сброса PIN-код проверяется на непустое значение и цифровой формат
- При снятии защиты выполняется очистка настроек и для режима блокировки, и для режима wipe
- Управление выполняется через специализированные MDM-команды

Предупреждение

Важные предупреждения:

- Выбор сценария полного сброса приведёт к потере данных при срабатывании защиты
- Неверно введенный PIN-код может сделать настройку защиты бесполезной
- Перед включением защиты от смены SIM рекомендуется протестировать поведение на одном устройстве

Сброс Android устройства до заводских настроек

Доступна только в MDM версии

Описание

Сброс Android устройства до заводских настроек — политика для удалённой отправки команды полного сброса Android-устройства до заводского состояния

Политика применяется при утере устройства, передаче устройства другому сотруднику и необходимости полной очистки корпоративных данных

Примечание

Поддерживаемые операционные системы:

- Android

Предупреждение

Важное предупреждение:

- После выполнения политики все данные пользователя и локальные настройки на устройстве будут удалены
- Действие является необратимым

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующее поле:

- Название — имя политики в системе

Остальные вкладки описаны на странице *Политики*

Пример

Для удаленного полного сброса Android-устройства:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Сброс Android устройства до заводских настроек»**
3. Заполнить поле `Название`

   Например: Полный сброс потерянного устройства
4. Нажать на кнопку Сохранить
5. Выполнить `Тестовый запуск` на устройстве Android
6. После применения политики:
   - На устройство будет отправлена команда полного сброса до заводских настроек
   - После выполнения сброса локальные данные и пользовательские настройки будут удалены

Примечание

Технические особенности:

- Политика использует MDM-команду полного сброса Android-устройства
- Для выполнения не требуются дополнительные параметры кроме названия политики
- Шаблон отправляет команду на устройство, а не настраивает дополнительные шаги подтверждения в самой политике

Предупреждение

Важные предупреждения:

- После выполнения политики восстановить локальные данные средствами этой операции невозможно
- На устройстве будут удалены пользовательские данные, приложения и настройки
- После сброса устройству потребуется повторная настройка
- Перед запуском рекомендуется убедиться, что выбран именно нужный целевой хост

Управление режимом вызова Android устройства

Доступна только в MDM версии

Описание

Управление режимом вызова Android устройства — политика для централизованной установки режима вызова и уведомлений на Android-устройстве: Обычный, Вибрация или Без звука

Политика подходит для устройств в зонах, где требуется тишина (учебные классы, конференц-залы, медицинские учреждения), а также для централизованной нормализации поведения корпоративных устройств

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — режим вызова и уведомлений
  - **Обычный** — стандартный режим со звуковыми сигналами
  - **Вибрация** — звуковые сигналы отключены, остаётся только вибрация
  - **Без звука** — отключены и звук, и вибрация

Остальные вкладки описаны на странице *Политики*

Пример

Для перевода устройств учебных аудиторий в беззвучный режим:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление режимом вызова Android устройства»**
3. Заполнить поле `Название`

   Например: Беззвучный режим для учебных аудиторий
4. В поле `Выбор действия` выбрать Без звука
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - Устройство переключится в выбранный режим вызова и уведомлений

Примечание

Технические особенности:

- Политика меняет системный режим звонка через MDM-команду
- Изменение применяется немедленно без перезагрузки устройства
- Пользователь может изменить режим вручную после применения политики, для возврата к нужному режиму требуется повторный запуск политики

Предупреждение

Важные предупреждения:

- В беззвучном режиме пользователь может пропустить входящие вызовы и уведомления
- Режим вибрации может быть незаметен в шумной обстановке

Управление состоянием Wi-Fi Android устройства

Доступна только в MDM версии

Описание

Управление состоянием Wi-Fi Android устройства - политика для централизованного включения или выключения Wi-Fi на Android-устройстве. Политика подходит для зон с запретом беспроводной связи, для экономии заряда батареи на устройствах, не использующих Wi-Fi, а также при централизованном переходе на другой способ подключения

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами. Вкладка **«Политика»** содержит следующие поля:

- Название - имя политики в системе
- Выбор действия - состояние Wi-Fi на устройстве
  - **Выключить** - отключает Wi-Fi на устройстве
  - **Включить** - включает Wi-Fi на устройстве

Остальные вкладки описаны на странице *Политики*

Пример

Для отключения Wi-Fi на устройствах в защищённой зоне:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление состоянием Wi-Fi Android устройства»**
3. Заполнить поле `Название`

Подсказка

Например: Отключение Wi-Fi в защищённой зоне

4. В поле `Выбор действия` выбрать Выключить
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - Wi-Fi на устройстве будет включён или выключен в зависимости от выбранного действия

Примечание

Применение настройки:

- Изменение применяется без перезагрузки устройства
- На Android 13 и новее после включения или выключения Wi-Fi пользователь также теряет возможность переключать его вручную

- На более ранних версиях эта дополнительная блокировка не устанавливается

Предупреждение

Важные предупреждения:

- При отключении Wi-Fi устройство теряет связь с сервером **RuDesktop** по беспроводному каналу, если иные каналы недоступны
- Для последующего удалённого включения Wi-Fi устройству нужен другой работающий канал связи с сервером

Как вернуть пользователю управление

На Android 13 и новее выполнить *политику разрешения менять состояние Wi-Fi* с действием **«Разрешить»**

Важно

Если нужно включить Wi-Fi и оставить пользователю возможность выключать его, сначала включить Wi-Fi этой политикой, затем отдельно разрешить изменение состояния. Повторное выполнение политики управления состоянием снова установит запрет на ручное переключение

Предупреждение

До отключения Wi-Fi проверить резервный канал связи с сервером, например мобильную сеть. Если Wi-Fi был единственным каналом, новая политика для его включения не поступит, пока связь не будет восстановлена

Управление режимом яркости экрана Android устройства

Доступна только в MDM версии

Описание

Управление режимом яркости экрана Android устройства — политика для централизованного включения или выключения адаптивной (автоматической) яркости экрана на Android-устройстве

Политика подходит для централизованной настройки удобства использования экрана и для совместного использования с политикой настройки конкретного уровня яркости

Примечание

Поддерживаемые операционные системы:

- Android (требуется Android 9 или новее)

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — режим яркости экрана
  - **Выключить** — отключает адаптивную яркость (ручной режим)
  - **Включить** — включает адаптивную (автоматическую) яркость

Остальные вкладки описаны на странице *Политики*

Пример

Для включения адаптивной яркости на корпоративных смартфонах:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление режимом яркости экрана Android устройства»**
3. Заполнить поле `Название`

   Например: Адаптивная яркость на смартфонах
4. В поле `Выбор действия` выбрать Включить
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - Режим яркости экрана на устройстве будет переключён в адаптивный или ручной в зависимости от выбранного действия

Примечание

Технические особенности:

- Управление режимом яркости выполняется через MDM-команду
- Для работы политики требуется Android 9 или новее
- При включённой адаптивной яркости устройство автоматически подстраивает яркость экрана под уровень освещения
- Политика настройки конкретного уровня яркости автоматически отключает адаптивный режим

Предупреждение

Важные предупреждения:

Управление запретом установки Android приложений из неизвестных источников

Доступна только в MDM версии

Описание

Управление запретом установки Android приложений из неизвестных источников — политика для централизованного разрешения или запрета установки приложений из неизвестных источников (sideload) на Android-устройстве

Политика подходит для повышения безопасности корпоративных устройств, исключения установки непроверенного ПО и защиты от попадания вредоносных приложений в обход магазинов приложений

Примечание

Поддерживаемые операционные системы:

- Android (требуется Android 10 или новее)

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — разрешение установки из неизвестных источников
  - **Запретить** — блокирует установку приложений из неизвестных источников на устройстве
  - **Разрешить** — снимает запрет на установку из неизвестных источников

Остальные вкладки описаны на странице *Политики*

Пример

Для запрета установки приложений из неизвестных источников на корпоративных устройствах:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление запретом установки Android приложений из неизвестных источников»**

3. Заполнить поле Название

   Например: Запрет sideload приложений

4. В поле Выбор действия выбрать Запретить
5. Нажать на кнопку Сохранить
6. Выполнить Тестовый запуск на устройстве Android
7. После применения политики:
   - На устройстве будет применён запрет или разрешение установки приложений из неизвестных источников

Примечание

Технические особенности:

- Для работы политики требуется Android 10 или новее
- Запрет распространяется на все приложения, выполняющие установку APK вне официальных магазинов

Предупреждение

Важные предупреждения:

- При запрете установки из неизвестных источников пользователь не сможет установить APK-файлы вручную, в том числе из браузера или мессенджеров
- Политика не отменяет установку приложений администратором через MDM-команды

Управление временем до выключения экрана Android устройства

Доступна только в MDM версии

Описание

Управление временем до выключения экрана Android устройства — политика для централизованной установки времени бездействия до автоматического выключения экрана Android-устройства

Политика подходит для устройств-витрин, информационных табло и сценариев, в которых экран должен оставаться активным долгое время, либо наоборот — выключаться быстро для экономии заряда

Примечание

Поддерживаемые операционные системы:

- Android (требуется Android 9 или новее)

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Время работы экрана (в секундах) — интервал бездействия до выключения экрана

> **Важно**
>
> Если оставить поле пустым, установится максимально возможное значение (приблизительно 24.86 дней)

Остальные вкладки описаны на странице *Политики*

Пример

Для информационного табло, экран которого должен оставаться включённым максимально долго:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление временем до выключения экрана Android устройства»**
3. Заполнить поле `Название`

   Например: Экран информационного табло — без выключения
4. Оставить поле `Время работы экрана (в секундах)` пустым
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - На устройстве будет установлено максимально возможное время до выключения экрана

Для установки конкретного значения (например, 60 секунд):

1. Заполнить поле `Название`

   Например: Экран выключается через минуту
2. Заполнить поле `Время работы экрана (в секундах)`

   Например: 60
3. Нажать на кнопку Сохранить
4. Выполнить `Тестовый запуск` на устройстве Android
5. После применения политики:
   - Экран устройства будет выключаться через указанное количество секунд бездействия

Примечание

Технические особенности:

- Значение в секундах автоматически конвертируется в миллисекунды при отправке на устройство
- Для работы политики требуется Android 9 или новее

Предупреждение

Важные предупреждения:

- Постоянно включённый экран увеличивает износ дисплея и расход батареи
- Пользователь может изменить время выключения экрана вручную; для возврата к заданному значению требуется повторный запуск политики

Управление уровнем громкости Android устройства

Доступна только в MDM версии

Описание

Управление уровнем громкости Android устройства — политика для централизованной установки уровня громкости (0-100%) для выбранного типа звукового потока на Android-устройстве

Политика подходит для нормализации громкости корпоративных устройств, ограничения уровня звука в общественных помещениях и автоматизации сценариев работы с разными типами звука (звонок, медиа, будильник и т.д.)

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор типа звука — звуковой поток, для которого задаётся громкость
  - **Голосовые вызовы** — громкость во время телефонного разговора
  - **Системные звуки** — звуки системных событий

  - **Звонок** — громкость входящего вызова
  - **Медиа** — громкость воспроизведения музыки и видео
  - **Будильник** — громкость сигнала будильника
  - **Уведомления** — громкость уведомлений приложений
  - **Тоновый набор** — громкость DTMF-сигналов набора номера
- Уровень громкости (0-100%) — значение громкости в процентах от 0 до 100

> **Важно**
>
> Значение 0 полностью отключает звук выбранного типа

Остальные вкладки описаны на странице *Политики*

Пример

Для установки максимальной громкости будильника на дежурных устройствах:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление уровнем громкости Android устройства»**
3. Заполнить поле `Название`

   Например: Максимальная громкость будильника
4. В поле `Выбор типа звука` выбрать Будильник
5. Заполнить поле `Уровень громкости (0-100%)`

   Например: 100
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве Android
8. После применения политики:
   - На устройстве будет установлен заданный уровень громкости для выбранного типа звука

> **Примечание**
>
> **Технические особенности:**
>
> - Уровень громкости задаётся в процентах и преобразуется в шаги штатного регулятора громкости Android для выбранного типа звукового потока
> - Политика управляет ровно одним типом звука за один запуск; для настройки нескольких типов требуется создать несколько политик

Предупреждение

Важные предупреждения:

- Значение 0 полностью отключает звук выбранного типа — это может привести к пропуску уведомлений или вызовов
- Пользователь может изменить громкость вручную; для возврата к заданному значению требуется повторный запуск политики

Управление автоматической настройкой часового пояса Android устройства по геоданным

Доступна только в MDM версии

Описание

Управление автоматической настройкой часового пояса Android устройства по геоданным — политика для централизованного включения или выключения автоматического определения часового пояса на Android-устройстве по данным геолокации

Политика подходит для устройств, перемещаемых между часовыми поясами (мобильных сотрудников, командировочных), а также для централизованной нормализации поведения корпоративных устройств

Примечание

Поддерживаемые операционные системы:

- Android (требуется Android 11 или новее)

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — состояние автоматической настройки часового пояса
  - **Включить** — устройство автоматически определяет часовой пояс по геоданным
  - **Выключить** — автоматическое определение часового пояса отключается, часовой пояс задаётся вручную пользователем

Остальные вкладки описаны на странице *Политики*

Пример

Для включения автоматического определения часового пояса на устройствах мобильных сотрудников:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление автоматической настройкой часового пояса Android устройства по геоданным»**
3. Заполнить поле `Название`

   Например: Автоматический часовой пояс — мобильные сотрудники
4. В поле `Выбор действия` выбрать Включить
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - Часовой пояс на устройстве будет определяться автоматически по геоданным или будет отключён в зависимости от выбранного действия

Примечание

Технические особенности:

- Для работы политики требуется Android 11 или новее
- Для определения часового пояса по геоданным на устройстве должны быть включены службы геолокации

Предупреждение

Важные предупреждения:

- Если на устройстве отключены службы геолокации, автоматическое определение часового пояса работать не будет

Управление роумингом данных Android устройства

Доступна только в MDM версии

Описание

Управление роумингом данных Android устройства — политика для централизованного разрешения или запрета использования роуминга данных на Android-устройстве

Политика подходит для контроля расходов на мобильную связь, исключения нежелательного трафика в роуминге и для централизованной нормализации

поведения корпоративных устройств

Примечание

Поддерживаемые операционные системы:

- Android (требуется Android 7 или новее)

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — разрешение на использование роуминга данных
  - **Разрешить** — снимает запрет, пользователь может включить роуминг данных
  - **Запретить** — запрещает роуминг данных, отключает его и блокирует включение пользователем

Остальные вкладки описаны на странице *Политики*

Пример

Для запрета роуминга данных на корпоративных устройствах с целью контроля расходов:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление роумингом данных Android устройства»**
3. Заполнить поле `Название`

   Например: Запрет роуминга данных
4. В поле `Выбор действия` выбрать Запретить
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - На устройстве будет применён запрет или разрешение использования данных в роуминге

Примечание

Технические особенности:

- Для работы политики требуется Android 7 или новее

- Ограничение действует на уровне ОС и распространяется на все приложения, использующие мобильный интернет

Предупреждение

Важные предупреждения:

- При запрете роуминга устройство теряет доступ к мобильному интернету за границей и в зонах действия других операторов; связь через Wi-Fi остаётся доступной

Получение количества включений устройства Android

Доступна только в MDM версии

Описание

Получение количества включений устройства Android — политика для получения текущего значения счётчика включений Android-устройства

Политика подходит для диагностики стабильности устройства, аудита подозрительных перезагрузок и контроля количества циклов включения корпоративных устройств

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

Политика не требует пользовательских параметров — после выполнения текущее значение счётчика выводится в журнал выполнения политики

Остальные вкладки описаны на странице *Политики*

Пример

Для получения количества включений устройств в рамках аудита:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Получение количества включений устройства Android»**

3. Заполнить поле `Название`

   Например: Аудит количества включений Android-устройств

4. Нажать на кнопку Сохранить
5. Выполнить `Тестовый запуск` на устройстве Android
6. После применения политики:
   - В журнале выполнения политики будет выведено текущее значение счётчика включений устройства

Примечание

Технические особенности:

- Политика не изменяет настройки устройства, только запрашивает значение
- Если устройство не поддерживает счётчик, политика вернёт значение `null`

Предупреждение

Важные предупреждения:

- На некоторых сторонних прошивках Android значение счётчика включений может быть недоступно или сбрасываться при обновлении ОС

Управление работой экрана Android устройства при подключении к зарядному устройству

Доступна только в MDM версии

Описание

Управление работой экрана Android устройства при подключении к зарядному устройству — политика для централизованного включения или выключения режима постоянной работы экрана Android-устройства при подключении к источнику питания (AC, USB или беспроводной зарядке)

Политика подходит для устройств-витрин, информационных табло, кассовых терминалов и любых сценариев, в которых экран должен оставаться активным всё время, пока устройство подключено к питанию

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — режим работы экрана при зарядке
  - **Включить** — экран остаётся включённым при подключении к зарядному устройству (AC, USB, беспроводная зарядка)
  - **Выключить** — стандартное поведение, экран выключается по обычному таймеру независимо от состояния зарядки

Остальные вкладки описаны на странице *Политики*

Пример

Для постоянной работы экрана информационного табло, подключённого к питанию:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление работой экрана Android устройства при подключении к зарядному устройству»**
3. Заполнить поле `Название`

   Например: Постоянная работа экрана при зарядке
4. В поле `Выбор действия` выбрать Включить
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - При подключении устройства к зарядному устройству экран будет оставаться активным или выключаться по таймеру в зависимости от выбранного действия

Примечание

Технические особенности:

- При включении режима активируются все три типа источников питания: AC, USB и беспроводная зарядка
- Изменение применяется без перезагрузки устройства

Предупреждение

Важные предупреждения:

- Постоянная работа экрана увеличивает износ дисплея, особенно на устройствах с OLED-экраном (риск выгорания изображения)
- При работе политики экран остаётся включённым только во время зарядки; после отключения от питания используется стандартный таймер выключения экрана

Управление яркостью экрана Android устройства

Доступна только в MDM версии

Описание

Управление яркостью экрана Android устройства — политика для централизованной установки конкретного уровня яркости экрана на Android-устройстве (значение задаётся в нитах)

Политика подходит для устройств с фиксированными требованиями к яркости: информационных табло, цифровых вывесок, киосков самообслуживания, корпоративных терминалов

Примечание

Поддерживаемые операционные системы:

- Android (требуется Android 9 или новее)

Важно

При применении политики адаптивная (автоматическая) яркость на устройстве автоматически отключается, и режим яркости переключается в ручной. Это необходимо, чтобы устройство не переопределило заданное значение

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Уровень яркости (в нитах) — значение яркости в нитах

Важно

- Максимальная яркость различается на разных устройствах

- Превышение максимального значения приведёт к установке максимально возможного значения для устройства
- Обычные значения: от 1 до 1000 нит в зависимости от модели устройства

Остальные вкладки описаны на странице *Политики*

Пример

Для установки фиксированной яркости 500 нит на информационных табло:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление яркостью экрана Android устройства»**
3. Заполнить поле `Название`

   Например: Фиксированная яркость табло — 500 нит
4. Заполнить поле `Уровень яркости (в нитах)`

   Например: 500
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - На устройстве будет установлен заданный уровень яркости экрана
   - Адаптивная яркость будет автоматически отключена

Примечание

Технические особенности:

- Перед установкой значения яркости политика автоматически переключает режим яркости в ручной
- Для работы политики требуется Android 9 или новее
- Если требуется вернуть адаптивную яркость, используйте политику **«Управление режимом яркости экрана Android устройства»**

Предупреждение

Важные предупреждения:

- Политика отключает адаптивную яркость как побочный эффект; для возврата к автоматическому режиму нужно запустить отдельную политику

- Пользователь может изменить яркость вручную; для возврата к заданному значению требуется повторный запуск политики

Управление состоянием Bluetooth Android устройства

Доступна только в MDM версии

Описание

Управление состоянием Bluetooth Android устройства — политика для централизованного включения или выключения Bluetooth на Android-устройстве

Политика подходит для зон с запретом беспроводной связи, для экономии заряда батареи на устройствах, не использующих Bluetooth-аксессуары, а также для централизованной нормализации поведения корпоративных устройств

Примечание

Поддерживаемые операционные системы:

- Android (требуется Android 10 или новее)

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — состояние Bluetooth на устройстве
  - **Выключить** — отключает Bluetooth на устройстве
  - **Включить** — включает Bluetooth на устройстве

Остальные вкладки описаны на странице *Политики*

Пример

Для отключения Bluetooth на устройствах в защищённой зоне:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление состоянием Bluetooth Android устройства»**
3. Заполнить поле `Название`

   Например: Отключение Bluetooth в защищённой зоне
4. В поле `Выбор действия` выбрать Выключить
5. Нажать на кнопку Сохранить

6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
    - Bluetooth на устройстве будет включён или выключен в зависимости от выбранного действия

Примечание

Технические особенности:

- Перед изменением состояния Bluetooth политика автоматически предоставляет необходимые системные разрешения приложению
- Для работы политики требуется Android 10 или новее
- Изменение применяется без перезагрузки устройства

Предупреждение

Важные предупреждения:

- При отключении Bluetooth перестают работать все Bluetooth-аксессуары (гарнитуры, клавиатуры, метки, медицинские датчики и т.д.)
- Пользователь может изменить состояние Bluetooth вручную; для возврата к заданному состоянию требуется повторный запуск политики

Управление автоопределением времени Android устройства

Доступна только в MDM версии

Описание

Управление автоопределением времени Android устройства — политика для централизованного включения или выключения автоматического определения времени на Android-устройстве, а также для разрешения или запрета пользователю изменять эту настройку вручную

Политика подходит для централизованной синхронизации времени корпоративных устройств, исключения ручной правки часов и автоматизации сценариев работы со временем

Примечание

Поддерживаемые операционные системы:

- Android (требуется Android 11 или новее)

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — состояние автоопределения времени
  - **Включить** — устройство автоматически определяет время по сети
  - **Выключить** — автоматическое определение времени отключается, время задаётся вручную пользователем
- Управление запретом изменения опции на устройстве — может ли пользователь изменять настройку автоопределения времени вручную
  - **Разрешить** — пользователь может включать и выключать автоопределение времени в настройках устройства
  - **Запретить** — настройка автоопределения времени блокируется от изменения пользователем

Примечание

Оба параметра обрабатываются независимо: политика всегда применяет и автоопределение, и ограничение пользователя

Остальные вкладки описаны на странице *Политики*

Пример

Для включения автоматического определения времени и запрета его изменения пользователем:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Управление автоопределением времени Android устройства»**
3. Заполнить поле `Название`

   Например: Автоматическое время — без правок пользователем
4. В поле `Выбор действия` выбрать Включить
5. В поле `Управление запретом изменения опции на устройстве` выбрать Запретить
6. Нажать на кнопку Сохранить

7. Выполнить `Тестовый запуск` на устройстве Android
8. После применения политики:
    - Время на устройстве будет автоматически определяться по сети
    - Пользователь не сможет изменить настройку автоопределения времени вручную

Примечание

Технические особенности:

- Для работы политики требуется Android 11 или новее

Предупреждение

Важные предупреждения:

- При запрете изменения опции пользователь не сможет вручную скорректировать время даже при необходимости; снимать запрет следует через повторный запуск политики

Отправка уведомления на Android устройство

Доступна только в MDM версии

Описание

Политика отправляет текстовое уведомление администратора на Android-устройство. Подходит для оповещения пользователей о технических работах или необходимости выполнить действие

Примечание

Устройство должно быть зарегистрировано в MDM с клиентом RuDesktop, поддерживающим отправку уведомлений администратора. Порядок регистрации описан в кейсе настройки MDM

На устройстве должны быть разрешены уведомления клиента RuDesktop, а канал **«Сообщения администратора»** должен быть включён. Если уведомления приложения отключены, отправка завершится ошибкой. Отключение отдельного канала может скрыть сообщение без ошибки в задании

Свойства политики

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Сообщение — обязательный текст уведомления. Сообщение из одних пробелов не допускается

- Может ли пользователь закрыть уведомление — разрешение пользователю закрывать уведомление. При снятом флажке уведомление отправляется как постоянное

Остальные вкладки описаны на странице *Политики*

Пример

1. Нажать на кнопку **«Добавить Политику»**
2. В категории **«Управление пользователями и устройствами»** выбрать шаблон **«Отправка уведомления на Android устройство»**
3. Заполнить поле **«Название»**, например `Уведомление о технических работах`
4. В поле **«Сообщение»** указать текст, например `Сохраните работу: в 18:00 начнутся технические работы`
5. Установить флажок **«Может ли пользователь закрыть уведомление»**, если пользователь может убрать сообщение
6. Сохранить политику и выполнить **«Тестовый запуск»** на одном Android-устройстве
7. Проверить результат задания и появление уведомления на устройстве перед назначением политики группе

Важно

Тестовый запуск отправляет уведомление на выбранное устройство

Результат выполнения

Уведомление содержит заданное сообщение; длинный текст можно прочитать, развернув уведомление. На одном устройстве отображается одно уведомление администратора: новое сообщение заменяет предыдущее, в том числе отправленное другой политикой на основе того же шаблона. Повторная отправка также обновляет возможность закрытия уведомления. Нажатие на уведомление не закрывает его автоматически

Для изменения текста повторно запустить политику с новым сообщением. Для разрешения закрытия постоянного уведомления повторно отправить сообщение с установленным флажком **«Может ли пользователь закрыть уведомление»**, после чего пользователь сможет убрать его. Отдельной команды удаления уведомления в шаблоне нет; пустое сообщение для удаления не поддерживается

Перезагрузка устройства и повторный вход не требуются. Успешное выполнение задания подтверждает передачу уведомления системе Android, но не гарантирует его видимость и не подтверждает прочтение сообщения пользователем

Особенности отображения

- Всплывающий показ, звук и вибрация зависят от настроек канала уведомлений и режима **«Не беспокоить»**. Политика не отменяет эти настройки
- Текст разрешён к показу на экране блокировки; фактическое отображение зависит от настроек Android
- Полный текст сообщения выводится в результат выполнения задания. Это следует учитывать при выборе содержания уведомления

Если задание успешно, но сообщение не видно, проверить настройки уведомлений RuDesktop и канал **«Сообщения администратора»** на устройстве. Если получена ошибка `Unknown MDM command`, проверить, поддерживает ли установленная версия MDM-клиента эту политику

Управление языковыми настройками Android устройства

Доступна только в MDM версии

Описание

Политика разрешает или запрещает пользователю менять языковые настройки Android-устройства. Текущий язык не изменяется: политика управляет доступом к настройкам, а не выбором языка

Подготовка и запуск

> **Примечание**
>
> Требуется Android 9 или новее. Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner) и поддерживать эту политику. Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

Свойства политики

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Выбор действия — обязательный параметр:
  - **«Запретить»** — устанавливает ограничение на изменение языковых настроек пользователем
  - **«Разрешить»** — снимает установленное клиентом ограничение

Остальные вкладки описаны на странице *Политики*

Пример

1. Нажать на кнопку **«Добавить Политику»**
2. В категории **«Управление пользователями и устройствами»** выбрать шаблон **«Управление языковыми настройками Android устройства»**
3. Заполнить поле **«Название»**, например `Запрет изменения языка`
4. В поле **«Выбор действия»** выбрать **«Запретить»**
5. Сохранить политику и выполнить **«Тестовый запуск»** на одном устройстве Android
6. Проверить результат задания и доступность изменения языка в настройках устройства перед назначением политики группе

Важно

Тестовый запуск применяет ограничение к выбранному устройству

Результат и снятие ограничения

После действия **«Запретить»** пользователь не может менять языковые настройки. Текущий язык системы и настройки языка отдельных приложений политика самостоятельно не меняет. Перезагрузка и повторный вход не требуются

Для снятия ограничения повторно выполнить политику с действием **«Разрешить»**. Это действие снимает ограничение RuDesktop, но не отменяет ограничения, установленные другими администраторами или системой

Политика ограничивает изменение языка устройства средствами Android. Она не гарантирует блокировку собственного выбора языка внутри стороннего приложения и не управляет раскладками клавиатуры

Удаление политики на сервере само по себе не выполняет команду снятия ограничения на устройстве. Перед прекращением использования политики выполнить её с действием **«Разрешить»** и проверить результат

Если получена ошибка `Unknown MDM command`, проверить поддержку политики установленной версией клиента. При ошибке о неподдерживаемой функции проверить версию Android, а при ошибке `Application is not a device owner` — права клиента и регистрацию устройства в MDM

Управление пользователями Android устройства

Доступна только в MDM версии

Описание

Политика управляет возможностью добавлять и удалять пользователей Android-устройства, а также переключаться между ними. Это пользователи устройства, а не пользователи организации RuDesktop и не аккаунты почты или других приложений

Политика самостоятельно не создаёт и не удаляет пользователей, не переключает текущего пользователя и не меняет пароли

Подготовка и запуск

Примечание

Для выполнения всего шаблона требуется Android 9 или новее: установка и снятие запрета переключения используют функцию, доступную с этой версии. На более старом Android первое действие по добавлению и удалению пользователей может примениться, после чего действие по переключению завершится ошибкой. Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner) и поддерживать эту политику. Порядок регистрации описан в кейсе настройки MDM

Свойства политики

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Разрешить пользователю добавлять/удалять пользователей — обязательный выбор:
  - **«Запретить»** — запрещает добавление и удаление пользователей
  - **«Разрешить»** — снимает оба ограничения, установленные клиентом
- Разрешить пользователю переключаться между пользователями — обязательный выбор:
  - **«Запретить»** — запрещает переключение пользователей
  - **«Разрешить»** — снимает установленное клиентом ограничение на переключение

Параметры независимы: можно, например, запретить добавление и удаление пользователей, но разрешить переключение между существующими. Оба параметра применяются при каждом запуске политики

Остальные вкладки описаны на странице *Политики*

Пример

1. Нажать на кнопку **«Добавить Политику»**
2. В категории **«Управление пользователями и устройствами»** выбрать шаблон **«Управление пользователями Android устройства»**
3. Заполнить поле **«Название»**, например `Запрет управления пользователями`
4. Для обоих параметров выбрать **«Запретить»**
5. Сохранить политику и выполнить **«Тестовый запуск»** на одном устройстве Android
6. Проверить результат задания и доступность добавления, удаления и переключения пользователей в настройках устройства перед назначением политики группе

Важно

Тестовый запуск применяет изменения к выбранному устройству. Настройки выполняются последовательно: если задание завершится ошибкой, уже применённые изменения автоматически не откатываются. Даже добавление и удаление пользователей изменяются отдельными операциями внутри одной команды. Проверить состояние устройства и повторить запуск с нужными параметрами

Результат и снятие ограничений

Существующие пользователи и их данные сохраняются. Перезагрузка и повторный вход не требуются

Для снятия всех ограничений повторно выполнить политику, выбрав **«Разрешить»** в обоих полях. Для изменения только одной группы ограничений изменить соответствующее поле, а для второго оставить нужное действие

Снятие ограничений не добавляет поддержку нескольких пользователей на устройствах, где её нет, и не отменяет ограничения других администраторов или системы. Управление аккаунтами приложений описано в отдельной политике *добавления и удаления аккаунтов*

Особенности Android

- Запрет удаления пользователей не запрещает удаление рабочего или приватного профиля. Для защиты таких профилей нужны отдельные ограничения, которых в этом шаблоне нет
- Запрет переключения применяется ко всем пользователям устройства. Он ограничивает действия пользователя, но не запрещает владельцу устройства (Device Owner) программно переключать пользователей
- На корпоративном устройстве Android может устанавливать базовый запрет добавления пользователей, который нельзя снять действием **«Раз-**

решить». Успешное выполнение задания не гарантирует, что добавление пользователей станет доступно

Эти особенности описаны в документации Android UserManager[17]

Удаление политики на сервере само по себе не снимает ограничения с устройства. Перед прекращением использования политики выполнить её с действием **«Разрешить»** в обоих полях и проверить результат

Если получена ошибка `Unknown MDM command`, проверить поддержку политики установленной версией клиента. При ошибке о неподдерживаемой функции проверить версию Android, а при ошибке `Application is not a device owner` — права клиента и регистрацию устройства в MDM

Управление звонками и SMS Android устройства

Доступна только в MDM версии

Описание

Политика разрешает или запрещает пользователю совершать исходящие телефонные звонки, а также отправлять и получать SMS. Эти возможности настраиваются независимо друг от друга

Подготовка и запуск

Примечание

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner) и поддерживать эту политику. Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

До применения убедиться, что на выбранном устройстве работают обычные исходящие звонки, отправка и получение SMS. Это позволит отличить действие политики от отсутствия связи или ограничений оператора

Свойства политики

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Разрешить пользователю совершать исходящие звонки — обязательный выбор:
  - **«Запретить»** — устанавливает запрет исходящих телефонных звонков, кроме экстренных
  - **«Разрешить»** — снимает установленное клиентом ограничение на исходящие звонки

[17] https://developer.android.com/reference/android/os/UserManager

- Разрешить пользователю получать и отправлять SMS — обязательный выбор:
  - **«Запретить»** — запрещает отправку и получение SMS
  - **«Разрешить»** — снимает установленное клиентом ограничение на SMS

Оба параметра применяются при каждом запуске. Например, можно запретить исходящие звонки, но разрешить отправку и получение SMS. Отдельного выбора для входящих и исходящих SMS нет

Таблица 8: Сочетания параметров

Исходящие звонки	SMS	Действие политики
Запретить	Запретить	Установить оба ограничения
Запретить	Разрешить	Запретить исходящие звонки и снять запрет SMS
Разрешить	Запретить	Снять запрет исходящих звонков и запретить SMS
Разрешить	Разрешить	Снять оба ограничения, установленные клиентом

Выбора отдельных номеров, контактов или SIM-карт в шаблоне нет. Политика не удаляет сохранённые сообщения и журнал звонков

Остальные вкладки описаны на странице *Политики*

Пример

1. Нажать на кнопку **«Добавить Политику»**
2. В категории **«Управление пользователями и устройствами»** выбрать шаблон **«Управление звонками и SMS Android устройства»**
3. Заполнить поле **«Название»**, например `Запрет исходящих звонков и SMS`
4. Для обоих параметров выбрать **«Запретить»**
5. Сохранить политику, открыть вкладку **«Тестовый запуск»**, выбрать одно устройство Android и нажать **«Запустить»**. Само сохранение политики не применяет настройки к устройству
6. Проверить результат в окне логирования этой вкладки
7. Попытаться совершить обычный исходящий звонок, отправить SMS с устройства и отправить на него тестовое SMS с другого телефона. Проверять результат на управляемом устройстве: обычный исходящий звонок, отправка и получение SMS должны быть недоступны его пользователю. Входящий телефонный звонок политика не блокирует
8. После проверки добавить политику в *задачу* для нужных устройств или группы и настроить запуск

Важно

Тестовый запуск изменяет настройки выбранного устройства. Сначала применяется настройка исходящих звонков, затем SMS. Если второе действие завершится ошибкой, первое автоматически не откатывается. Проверить состояние устройства и повторить запуск с нужными параметрами

В журнале задачи с противоположным действием будут пропущены: например, при выборе **«Запретить»** для SMS задача **«Разрешение SMS»** не выполняется. Это ожидаемое поведение. После выполнения выбранных действий шаблон выводит итог с именем устройства и применёнными настройками

Успешное завершение задания означает, что команды выполнены без ошибки. Сам шаблон не делает контрольный звонок и не проверяет доставку SMS, поэтому проверка на устройстве нужна отдельно

Результат и снятие ограничений

Перезагрузка и повторный вход не требуются. Для снятия обоих ограничений:

1. Выбрать **«Разрешить»** в обоих полях и сохранить политику
2. Повторно выполнить её на тех устройствах, где нужно снять запреты, и проверить результат задания
3. Проверить обычный исходящий звонок, отправку и получение нового тестового SMS
4. Проверить задачи, которые применяют эту или другие политики звонков и SMS: последующий запуск с действием **«Запретить»** снова установит соответствующее ограничение

Для изменения одной настройки во втором поле оставить нужное действие: варианта **«Не изменять»** в шаблоне нет

Действие **«Разрешить»** снимает ограничения RuDesktop, но не отменяет ограничения других администраторов или системы и не устраняет проблемы связи

Удаление политики на сервере само по себе не снимает ограничения с устройства. Перед прекращением использования политики выполнить её с действием **«Разрешить»** в обоих полях и проверить результат

Особенности Android

- Экстренные звонки остаются доступны даже при запрете исходящих звонков
- Входящие телефонные звонки эта политика не запрещает
- При установке владельцем устройства запрет исходящих звонков относится к основному пользователю, а запрет SMS действует на всё устройство
- Шаблон не содержит отдельных настроек для звонков и сообщений через интернет в мессенджерах

Область действия ограничений описана в документации Android: исходящие звонки[18] и SMS[19]

Если результат отличается от ожидаемого

- `Unknown MDM command` — проверить поддержку политики установленной версией клиента
- `Application is not a device owner` — проверить права клиента и регистрацию устройства в MDM
- Задание завершилось ошибкой — по журналу определить, какая настройка успела примениться, проверить устройство и повторить запуск с нужными значениями обоих параметров
- После **«Разрешить»** звонки или SMS по-прежнему недоступны — проверить результат повторного запуска, другие политики и задачи, ограничения системы и работу связи
- Задание завершилось успешно, но запрет не действует — сверить выбранное устройство и параметры запуска, проверить обычные телефонные звонки и SMS, а не функции мессенджера. При сохранении проблемы зафиксировать модель устройства, версию Android, версию клиента и журнал выполнения для обращения в поддержку

Удаление пользовательских данных приложения Android устройства

Доступна только в MDM версии

Описание

Политика очищает пользовательские данные одного указанного приложения на Android-устройстве. Само приложение остаётся установленным. Действие соответствует очистке данных приложения в настройках Android: удаляются его локальные настройки и данные, а не только кэш

Подготовка

Требуется Android 9 или новее и клиент RuDesktop с поддержкой этой политики. Устройство должно быть зарегистрировано в MDM. Для обычного сценария управления RuDesktop используется регистрация с правами владельца устройства (Device Owner), описанная в кейсе настройки MDM

Перед запуском проверить точное имя пакета и наличие приложения на целевом устройстве. Имя пакета можно уточнить у поставщика приложения или в адресе его страницы Google Play: это значение параметра `id`, например `com.example.app`

[18] https://developer.android.com/reference/android/os/UserManager#DISALLOW_OUTGOING_CALLS

[19] https://developer.android.com/reference/android/os/UserManager#DISALLOW_SMS

Предупреждение

Удаление данных необратимо средствами этой политики. До запуска сохранить нужные данные средствами приложения и убедиться, что известны данные для повторного входа. **Тестовый запуск** также удаляет данные — это не предварительный просмотр. Шаблон не содержит отдельного подтверждения удаления

Свойства политики

На вкладке **«Политика»** заполнить:

- Название — имя политики в системе
- Пакет приложения — обязательное точное имя одного пакета, например `com.example.app`. Указывать без кавычек и пробелов; название приложения на экране, путь к APK, список пакетов и шаблоны с * не подходят

Остальные вкладки описаны на странице *Политики*

Пример и проверка

1. Создать политику в категории **«Управление пользователями и устройствами»** из шаблона **«Удаление пользовательских данных приложения Android устройства»**
2. Указать название, например `Очистка данных корпоративного приложения`
3. В поле **«Пакет приложения»** ввести имя нужного установленного пакета. `com.example.app` — пример формата, его нужно заменить реальным именем
4. Сохранить политику. Само сохранение не запускает очистку
5. На вкладке **«Тестовый запуск»** выбрать одно подготовленное устройство и нажать **«Запустить»**
6. Проверить окно логирования: задание должно завершиться успешно и вывести имя очищенного пакета
7. Открыть приложение на устройстве и проверить сброс локальных данных и настроек. При необходимости заново войти в приложение, настроить его и предоставить разрешения

Для применения к нескольким устройствам можно добавить политику в *задачу*. Каждый запуск снова очищает данные, накопленные приложением к этому моменту. При однократной очистке не настраивать повторный запуск по расписанию или при подключении устройства

Результат и ограничения

Клиент ожидает подтверждения результата очистки от Android. Перезагрузка устройства не требуется, но приложению может понадобиться повторный вход и первоначальная настройка. Удаление политики на сервере не восстанавливает очищенные данные

- Данные во внутренних каталогах приложения и его собственном каталоге на внешнем накопителе очищаются. Файлы, сохранённые вне этих каталогов, например экспортированные документы в общей папке, не гарантируется удалить этой операцией. Данные на сервере приложения она не удаляет
- Android также отзывает выданные приложению разрешения времени выполнения. После запуска приложение может запросить их снова
- Android не разрешает очищать данные приложений — администраторов устройства и защищённых системных пакетов. MDM-клиент RuDesktop не следует выбирать целью очистки
- В шаблоне нет выбора пользователя или рабочего профиля; очистка не является сбросом всего устройства и не гарантирует удаления данных всех экземпляров приложения в других профилях

Область очистки описана в документации Android: очистка данных приложения[20] и управление очисткой через MDM[21]

Если очистка не выполнена

- `Unknown MDM command` — проверить поддержку политики установленной версией клиента
- Сообщение о неподдерживаемой функции — проверить, что на устройстве Android 9 или новее
- `Package name is required` — заполнить поле **«Пакет приложения»**
- `Failed to clear data of ...: package is not installed or is protected` — проверить имя пакета, наличие приложения и ограничения на очистку защищённых приложений
- Ошибка прав доступа — проверить регистрацию клиента в MDM и его права управления устройством
- `Timed out waiting for data clearing of ...` — Android не подтвердил завершение за 30 секунд. Это не отменяет отправленную команду. Перед повторным запуском проверить состояние приложения на устройстве: очистка могла завершиться позже

Управление сбросом настроек сети к заводским Android устройства

Доступна только в MDM версии

[20] https://developer.android.com/reference/android/app/ActivityManager#clearApplicationUserData()

[21] https://developer.android.com/reference/android/app/admin/DevicePolicyManager#clearApplicationUserData(android.content.ComponentName,java.lang.String,java.util.concurrent.Executor,android.app.admin.DevicePolicyManager.OnClearApplicationUserDataListener)

Описание

Политика запрещает или разрешает пользователю сбрасывать настройки Wi-Fi, мобильной сети и Bluetooth. Она не выполняет сброс и не отключает сеть

Подготовка

Требуется Android 6 или новее и клиент RuDesktop с правами владельца устройства (Device Owner). Порядок регистрации устройства описан в кейсе настройки MDM

Свойства политики

На вкладке **Политика** указать **Название** и обязательный параметр **Выбор действия**:

- **Запретить** — запретить пользователю сброс сетевых настроек
- **Разрешить** — снять установленный клиентом запрет

Остальные вкладки описаны на странице *Политики*

Пример и проверка

1. Создать политику из шаблона **Управление пользователями и устройствами → Управление сбросом настроек сети к заводским Android устройства**
2. Указать название, например `Запрет сброса сети`, и выбрать **Запретить**
3. Сохранить и выполнить **Тестовый запуск** на одном Android-устройстве
4. Проверить результат задания и доступность сброса сети в настройках Android
5. Для снятия ограничения повторно выполнить политику с действием **Разрешить**

Перезагрузка и повторный вход не требуются. Удаление политики на сервере не снимает ограничение с устройства. При ошибке `Unknown MDM command` проверить поддержку команды установленным клиентом; при ошибке о правах владельца устройства — регистрацию в MDM

Управление видимостью пакетов Android устройства

Доступна только в MDM версии

Описание

Политика скрывает выбранные приложения на Android-устройстве через системный механизм управления устройством. Приложения не удаляются. Список скрытых пакетов сохраняется и повторно применяется после перезагрузки

Подготовка

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner) и поддерживать эту политику. Порядок регистрации описан в кейсе настройки MDM

Свойства политики

На вкладке **Политика** заполнить **Название** и **Список пакетов для скрытия**. Указывать точные имена пакетов, например `com.example.app`, а не названия приложений на экране устройства

Остальные вкладки описаны на странице *Политики*

Важно

Каждый запуск задаёт полный список скрываемых приложений. Пакеты, которые были скрыты ранее, но отсутствуют в новом списке, снова становятся видимыми. Пустой список возвращает видимость всем пакетам, ранее скрытым этим механизмом RuDesktop. Список общий для устройства: запуск другой политики из того же шаблона заменяет предыдущий список

Пример и проверка

1. Создать политику из шаблона **Управление пользователями и устройствами → Управление видимостью пакетов Android устройства**
2. Указать название, например `Скрытие корпоративного приложения`
3. Добавить `com.example.app` в **Список пакетов для скрытия**
4. Сохранить и выполнить **Тестовый запуск** на одном Android-устройстве
5. Проверить результат задания и отсутствие приложения в интерфейсе устройства
6. Для возврата видимости удалить пакет из списка и повторно выполнить политику

Важно

Нельзя скрывать собственный пакет MDM-клиента. Шаблон также отклоняет перечисленные в нём системно-критичные пакеты: SystemUI, настройки, распространённые лаунчеры и клавиатуры, компоненты Google Play. Перед применением к группе проверить список на тестовом устройстве

Установленные приложения скрываются без обязательной перезагрузки. Если пакет ещё не установлен, он остаётся в сохранённом списке для последующего скрытия; после установки приложение может оставаться видимым до перезагрузки. Удаление политики на сервере не возвращает видимость — сначала выполнить политику с нужным обновлённым или пустым списком

Очистка папки Android устройства

Доступна только в MDM версии

Описание

Политика рекурсивно очищает содержимое указанной папки на Android-устройстве. При включённом параметре **«Удалять папку»** после очистки удаляется и сама папка. Символьные ссылки удаляются как файлы, их цели не затрагиваются

Подготовка

Требуется клиент RuDesktop с поддержкой этой политики. Устройство должно быть зарегистрировано в MDM. Для обычного сценария управления RuDesktop используется регистрация с правами владельца устройства (Device Owner), описанная в кейсе настройки MDM

Путь указывается относительно корня внешнего хранилища устройства (`/storage/emulated/0`), например `Download/reports/v2`, либо абсолютным путём. Корень файловой системы и всего внешнего хранилища защищены от очистки: `/`, `/system`, `/data`, `/vendor`, `/proc`, `/sys`, `/dev`, `/storage`, `/storage/emulated`, `/storage/emulated/0`, `/sdcard`

Предупреждение

Удаление необратимо средствами этой политики. До запуска убедиться, что папка не содержит нужных пользователю данных. **Тестовый запуск** также удаляет содержимое — это не предварительный просмотр

Свойства политики

На вкладке **«Политика»** заполнить:

- Название — имя политики в системе
- Путь к папке — обязательный путь к очищаемой папке, например `Download/reports/v2`. Указывать без кавычек
- Удалять папку — если включено, после очистки удаляется и сама папка

Остальные вкладки описаны на странице *Политики*

Пример и проверка

1. Создать политику в категории **«Управление пользователями и устройствами»** из шаблона **«Очистка папки Android устройства»**
2. Указать название, например `Очистка отчётов на складском терминале`
3. В поле **«Путь к папке»** ввести путь к папке. `Download/reports/v2` — пример формата, его нужно заменить реальным путём
4. При необходимости удалить саму папку включить **«Удалять папку»**

5. Сохранить политику. Само сохранение не запускает очистку
6. На вкладке **«Тестовый запуск»** выбрать одно подготовленное устройство и нажать **«Запустить»**
7. Проверить окно логирования: задание должно завершиться успешно и вывести количество удалённых элементов и список неудалённых путей
8. Открыть файловый менеджер на устройстве и проверить, что папка пуста (или удалена при включённом параметре)

Для применения к нескольким устройствам можно добавить политику в *задачу*. Каждый запуск снова очищает содержимое, накопленное к этому моменту. При однократной очистке не настраивать повторный запуск по расписанию или при подключении устройства

Результат и ограничения

Перезагрузка устройства и повторный вход не требуются. Удаление политики на сервере не восстанавливает удалённые файлы

- Сама папка при включённом параметре **«Удалять папку»** удаляется, только если всё её содержимое удалено без ошибок; иначе папка остаётся с неудалёнными элементами
- Ошибка удаления отдельного элемента не прерывает очистку: путь попадает в список неудалённых в итоговом сообщении задания
- Защищённые системные каталоги очистить нельзя: задание завершится ошибкой `Path is forbidden`
- Очистка не является сбросом устройства и не затрагивает данные вне выбранной папки

Если очистка не выполнена

- `Unknown MDM command` — проверить поддержку политики установленной версией клиента
- `Invalid `path`: is null or blank` — заполнить поле **«Путь к папке»**
- `Path is forbidden: ...` — выбрать вложенную папку, а не корень хранилища или системный каталог
- `Folder not found: ...` — проверить существование папки на устройстве
- `No directory: ...` — путь указывает на файл, а не на папку
- `Access denied: ...` — проверить регистрацию клиента в MDM и права доступа к папке на устройстве

Управление NFC и Android Beam Android устройства

Доступна только в MDM версии

Описание

Политика запрещает или разрешает передачу файлов через Android Beam и использование NFC на Android-устройстве. Эти возможности настраиваются независимо друг от друга и работают на разных версиях Android: управление Android Beam — на Android 5.1–9, управление NFC — на Android 15 или новее

Подготовка и запуск

Примечание

Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner) и поддерживать эту политику. Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

Версия Android определяется автоматически при выполнении политики. Если она вне поддерживаемого диапазона, соответствующее действие пропускается, а задание завершается успешно с пояснением в итоговом сообщении: например, на Android 10 и новее передача через Android Beam не изменяется, так как Beam удалён из системы

До применения убедиться, что на выбранном устройстве работает передача файлов через Android Beam и NFC. Это позволит отличить действие политики от отключённого NFC-модуля или особенностей устройства

Свойства политики

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Android Beam: выбор действия — действие для передачи файлов через Android Beam:
  - **«Запретить»** — запрещает исходящую передачу файлов через Android Beam. Приём данных по NFC и чтение меток продолжают работать
  - **«Разрешить»** — снимает установленный клиентом запрет на передачу через Android Beam
- NFC: выбор действия — действие для использования NFC:
  - **«Запретить»** — выключает NFC-модуль устройства и запрещает пользователю включать его
  - **«Разрешить»** — снимает установленный запрет. NFC при этом не включается автоматически: пользователь включает его сам в настройках устройства

Оба параметра применяются при каждом запуске. Например, можно запретить передачу через Android Beam и одновременно разрешить использование

NFC. Отдельных настроек для чтения меток и приёма данных по NFC в шаблоне нет, как и варианта **«Не изменять»**

Таблица 9: Сочетания параметров

Android Beam	NFC	Действие политики
Запретить	Запретить	Установить оба ограничения
Запретить	Разрешить	Запретить передачу через Android Beam и снять запрет NFC
Разрешить	Запретить	Снять запрет Android Beam и запретить использование NFC
Разрешить	Разрешить	Снять оба ограничения, установленные клиентом

Действие для неподдерживаемой версии Android не выполняется: в итоговом сообщении задания оно отмечается как неизменённое. Второе действие при этом применяется обычно

Остальные вкладки описаны на странице *Политики*

Пример

1. Нажать на кнопку **«Добавить Политику»**
2. В категории **«Управление пользователями и устройствами»** выбрать шаблон **«Управление NFC и Android Beam Android устройства»**
3. Заполнить поле **«Название»**, например `Запрет Beam и NFC на кассовом терминале`
4. Для обоих параметров выбрать **«Запретить»**
5. Сохранить политику, открыть вкладку **«Тестовый запуск»**, выбрать одно устройство Android и нажать **«Запустить»**. Само сохранение политики не применяет настройки к устройству
6. Проверить результат в окне логирования этой вкладки
7. Проверить результат на управляемом устройстве. На Android 5.1–9 передача файла через Android Beam должна быть недоступна, на Android 15 и новее — выключено NFC и запрещено его включение в настройках устройства
8. После проверки добавить политику в *задачу* для нужных устройств или группы и настроить запуск

Важно

Тестовый запуск изменяет настройки выбранного устройства. Сначала применяется действие для Android Beam, затем для NFC. Если второе действие завершится ошибкой, первое автоматически не откатывается. Проверить состояние устройства и повторить запуск с нужными параметрами

В журнале задачи с противоположным действием будут пропущены: например, при выборе **«Запретить»** для NFC задача **«Применение разрешения на использование NFC»** не выполняется. Это ожидаемое поведение. После выполнения выбранных действий шаблон выводит итог с именем устройства, версией Android и состоянием обеих возможностей

Успешное завершение задания означает, что команды выполнены без ошибки. Сам шаблон не передаёт тестовый файл и не проверяет состояние NFC, поэтому проверка на устройстве нужна отдельно

Результат и снятие ограничений

Перезагрузка и повторный вход не требуются. Для снятия обоих ограничений:

1. Выбрать **«Разрешить»** в обоих полях и сохранить политику
2. Повторно выполнить её на тех устройствах, где нужно снять запреты, и проверить результат задания
3. На устройстве проверить доступность передачи через Android Beam. NFC после снятия запрета останется выключенным — включить его в настройках устройства
4. Проверить задачи, которые применяют эту или другие политики NFC и Android Beam: последующий запуск с действием **«Запретить»** снова установит соответствующее ограничение

Для изменения одной настройки во втором поле оставить нужное действие: варианта **«Не изменять»** в шаблоне нет

Действие **«Разрешить»** снимает ограничения RuDesktop, но не отменяет ограничения других администраторов или системы, не включает NFC и не восстанавливает Android Beam на устройствах, где он удалён системой

Удаление политики на сервере само по себе не снимает ограничения с устройства. Перед прекращением использования политики выполнить её с действием **«Разрешить»** в обоих полях и проверить результат

Особенности Android

- Android Beam существует только в Android 5.1–9: начиная с Android 10 передача файлов через Beam удалена из системы, и поле на таких устройствах не действует
- Запрет Android Beam ограничивает только исходящую передачу файлов: приём данных по NFC и чтение меток продолжают работать
- Запрет NFC требует Android 15 или новее и действует на всё устройство: NFC выключается, включение его в настройках становится недоступно пользователю
- Запрет передачи через Android Beam устанавливается для основного пользователя устройства, запрет NFC применяется глобально и действует для всех пользователей устройства

- Отдельного запрета чтения NFC-меток или данных на них в шаблоне нет: чтение меток ограничивается только вместе с использованием NFC целиком

Область действия ограничений описана в документации Android: Android Beam[22] и NFC[23]

Если результат отличается от ожидаемого

- `Unknown MDM command` — проверить поддержку политики установленной версией клиента
- `Application is not a device owner` — проверить права клиента и регистрацию устройства в MDM
- Задание завершилось успешно, но в итоговом сообщении передача через Android Beam или использование NFC отмечены как неизменённые — версия Android вне поддерживаемого диапазона. Это ожидаемое поведение, а не ошибка
- После **«Разрешить»** NFC не работает — запрет снят, но NFC-модуль остался выключенным. Включить NFC в настройках устройства и проверить его работу
- Передача через Android Beam не запрещается на Android 10 и новее — ожидаемо: Beam удалён из системы, ограничение на такие устройства не действует
- Запрет не действует — сверить выбранное устройство и параметры запуска, проверить, что передача выполняется именно через Android Beam или NFC, а не через Bluetooth или Wi-Fi Direct. При сохранении проблемы зафиксировать модель устройства, версию Android, версию клиента и журнал выполнения для обращения в поддержку

Управление конфигурацией приложения Android устройства

Доступна только в MDM версии

Описание

Политика применяет управляемую конфигурацию (managed configuration) к выбранному приложению на Android-устройстве. Конфигурация — JSON-файл с парами `"Название настройки": значение`, который готовится под конкретное приложение: набор настроек и их типы приложение объявляет само в своей схеме. Например, так настраивается корпоративный Google Chrome (`com.android.chrome`)

Перед применением конфигурация проверяется на устройстве по схеме приложения: совпадение названий и типов настроек. При любой ошибке провер-

[22] https://developer.android.com/reference/android/os/UserManager#DISALLOW_OUTGOING_BEAM

[23] https://developer.android.com/reference/android/os/UserManager#DISALLOW_NEAR_FIELD_COMMUNICATION_RADIO

ки конфигурация не применяется совсем. Набор настроек заменяется целиком: пустой объект `{}` сбрасывает все применённые значения

Подготовка и запуск

> **Примечание**
>
> Устройство должно быть зарегистрировано в MDM, а клиент RuDesktop должен иметь права владельца устройства (Device Owner) и поддерживать эту политику. Обычной установки Android-клиента недостаточно. Порядок регистрации описан в кейсе настройки MDM

Требования к конфигурации:

- Приложение должно быть установлено на устройстве и объявлять поддержку управляемой конфигурации. Если приложение не объявляет схему, задание завершится ошибкой
- Конфигурация готовится под установленную версию приложения: набор настроек и их типы различаются между версиями. Проверять конфигурацию на устройстве с той же версией приложения, на которую рассчитан файл
- Файл — корректный JSON-объект с расширением `.json`, например `{"Название настройки": "значение"}`. Допустимые названия и типы значений задаёт схема приложения; для корпоративных приложений их описывает документация приложения
- Поддерживаемые типы значений: логическое значение, число, строка, выбор одного варианта, выбор нескольких вариантов, вложенные объекты и массивы объектов (последние — на Android 6 или новее)

Свойства политики

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Пакет приложения — обязательное имя пакета целевого приложения, например `com.android.chrome`. Указывается без кавычек
- Файл конфигурации — обязательный JSON-файл. Кнопка Browse открывает окно выбора файла на компьютере, кнопка Репозиторий — выбор из внутреннего репозитория сервера **RuDesktop**; файл также можно перетащить в поле выбора

Остальные вкладки описаны на странице *Политики*

Пример и проверка

1. Нажать Добавить Политику на странице **«Политики»**

2. В категории **«Управление пользователями и устройствами»** выбрать шаблон **«Управление конфигурацией приложения Android устройства»**
3. Заполнить поле **«Название»**, например `Корпоративные настройки Chrome`
4. Указать **«Пакет приложения»**, например `com.android.chrome`
5. Выбрать JSON-файл конфигурации в поле **«Файл конфигурации»**
6. Сохранить политику. Само сохранение не применяет конфигурацию к устройству
7. На вкладке **«Тестовый запуск»** выбрать одно устройство и нажать **«Запустить»**
8. Проверить окно логирования: задание завершится успешно и выведет имя пакета, имя файла, путь к нему на устройстве и количество настроек в конфигурации
9. Проверить результат в самом приложении на устройстве. Часть настроек приложение применяет сразу, часть — после перезапуска приложения

Для применения к нескольким устройствам добавить политику в *задачу*. Каждый запуск заменяет конфигурацию целиком

Результат и изменение конфигурации

Перезагрузка устройства и повторный вход не требуются. Приложение может применить часть настроек только после собственного перезапуска

- Чтобы изменить отдельные настройки, подготовить новый JSON-файл со всем нужным набором и повторно запустить политику: предыдущая конфигурация заменяется целиком, а не дополняется
- Чтобы сбросить все применённые настройки, запустить политику с файлом, содержащим пустой объект `{}`
- Удаление политики на сервере не сбрасывает конфигурацию на устройстве: для сброса выполнить политику с `{}` до прекращения использования
- Конфигурация действует, пока приложение установлено. После удаления приложения пользователем его конфигурация сбрасывается системой; при повторной установке применить политику заново

Особенности Android

- Схема настроек определяется приложением, а не RuDesktop: одни приложения её объявляют, другие — нет. У приложения без схемы политика завершится ошибкой
- Проверка выполняется по всем настройкам сразу: при ошибке хотя бы в одной (неизвестное название, несовпадение типа, недопустимое значение варианта) конфигурация не применяется совсем
- Значение `null` не допускается ни для одной настройки

- Вложенные объекты и массивы объектов требуют Android 6 или новее
- Применённая конфигурация видна приложению через штатный механизм Android managed configuration; как именно приложение реагирует на настройки, определяет само приложение

Если конфигурация не применилась

- `Unknown MDM command` — установить клиент RuDesktop с поддержкой политики
- `Application is not a device owner` — проверить права клиента и регистрацию устройства в MDM
- `Application with package `...` is not installed` — приложения нет на устройстве; проверить имя пакета и установку приложения
- `... has no managed configuration` — приложение установлено, но не объявляет управляемую конфигурацию; политика к нему неприменима
- `invalid JSON: ...` — файл не является корректным JSON; проверить содержимое файла
- `...: unknown restriction` — названия настроек не совпадают со схемой приложения; проверить названия и версию приложения на устройстве
- `...: expected bool, got string` (и аналогичные) — тип значения не совпадает с объявленным в схеме; привести значения к нужным типам
- `...: '...' not in [...]` / `...: [...] not in [...]` — значение вне списка допустимых вариантов; выбрать значение из схемы
- `...: nested restrictions require SDK 23+` — вложенные настройки заданы для устройства с Android до 6
- Укажите корректное имя пакета Android... — поле **«Пакет приложения»** пустое, заполнено не именем пакета или не выбран JSON-файл

Создание локального пользователя

Создание локальной учётной записи на устройстве

Добавление локального пользователя в группу

Включение учётной записи в локальную группу

Удаление учетных записей из локальной группы

Исключение учётных записей из локальной группы

Создание и удаление локальных групп

Создание или удаление локальных групп на устройстве

Изменение пароля локального пользователя
Смена пароля локальной учётной записи

Изменение имени локального пользователя
Переименование локальной учётной записи

Удаление/Блокирование локального пользователя
Удаление или временная блокировка локальной учётной записи

Схема управления питанием
Настройка схемы электропитания на устройстве

Применение конфигурации Kickstart
Применение профиля Kickstart на клиенте RuDesktop

Управление режимом «Киоск» на Windows, Linux и macOS
Включение режима «Киоск» на десктопных ОС

Включение режима «Киоск» на Android
Включение режима «Киоск» на Android-устройстве

Ввод устройства в домен
Присоединение устройства к домену Active Directory

Вывод устройства из домена
Отключение устройства от домена Active Directory

Управление отслеживанием геолокации Android
Включение и отключение сбора координат с Android-устройства

Блокировка Android устройства
Удалённая блокировка экрана Android-устройства

Управление запретом использования камеры на Android
Запрет или разрешение использования камеры на Android

Управление доступом к режиму разработчика на Android
Запрет или разрешение режима разработчика на Android

Управление запретом на удаление Android приложений пользователем
Запрет пользователю удалять приложения на Android

Управление запретом на установку Android приложений пользователем
Запрет пользователю устанавливать приложения на Android

Управление действиями на устройстве Android при изменении SIM-карты
Реакция устройства на смену SIM-карты

Сброс Android устройства до заводских настроек
Полный сброс Android-устройства с потерей данных

Управление состоянием Wi-Fi Android устройства
Включение или выключение Wi-Fi на Android-устройстве

Управление состоянием Bluetooth Android устройства
Включение или выключение Bluetooth на Android-устройстве

Управление роумингом данных Android устройства
Разрешение или запрет передачи данных в роуминге

Управление яркостью экрана Android устройства
Установка конкретного уровня яркости экрана в нитах

Управление режимом яркости экрана Android устройства
Включение или выключение адаптивной яркости экрана

Управление временем до выключения экрана Android устройства
Установка тайм-аута выключения экрана при бездействии

Управление режимом вызова Android устройства

Установка режима вызова и уведомлений: обычный, вибрация, без звука

Управление уровнем громкости Android устройства

Установка уровня громкости для выбранного типа звукового потока

Управление автоопределением времени Android устройства

Управление автоматическим определением времени и доступом к настройке

Управление автоматической настройкой часового пояса Android устройства по геоданным

Автоматическое определение часового пояса по местоположению устройства

Управление работой экрана при подключении к зарядному устройству

Постоянная работа экрана при подключении к источнику питания

Управление запретом установки приложений из неизвестных источников

Разрешение или запрет установки APK вне официальных магазинов

Получение количества включений устройства Android

Запрос текущего значения счётчика включений Android-устройства

Управление добавлением и удалением аккаунтов Android устройства

Настройка, проверка результата и снятие ограничения

Управление USB, MTP, OTG Android устройства

Настройка, проверка результата и снятие ограничения

Управление использованием микрофона Android устройства

Настройка, проверка результата и снятие ограничения

Управление доступом к переключателю микрофона Android

Настройка, проверка результата и снятие ограничения

Управление разрешением режима полёта Android
Настройка, проверка результата и снятие ограничения

Управление разрешением менять состояние Wi-Fi Android устройства
Настройка, проверка результата и снятие ограничения

Управление минимальным уровнем безопасности Wi-Fi Android устройства
Настройка, проверка результата и снятие ограничения

Управление разрешением на установку обоев Android устройства
Настройка, проверка результата и снятие ограничения

Установка обоев рабочего стола Android устройства
Настройка, проверка результата и снятие ограничения

Управление экраном блокировки Android устройства
Настройка, проверка результата и снятие ограничения

Отправка уведомления на Android устройство
Отправка сообщения администратора с настройкой возможности закрытия уведомления

Управление языковыми настройками Android устройства
Запрет или разрешение пользователю менять языковые настройки

Управление пользователями Android устройства
Управление добавлением, удалением и переключением пользователей устройства

Управление сбросом настроек сети к заводским Android устройства
Запрет или разрешение пользователю сбрасывать настройки Wi-Fi, мобильной сети и Bluetooth

Управление видимостью пакетов Android устройства
Скрытие приложений по списку пакетов и возврат их видимости

Управление звонками и SMS Android устройства

Запрет или разрешение исходящих телефонных звонков, отправки и получения SMS

Удаление пользовательских данных приложения Android устройства

Очистка локальных данных и настроек выбранного приложения без его удаления

Очистка папки Android устройства

Рекурсивная очистка содержимого выбранной папки и удаление самой папки

Управление NFC и Android Beam Android устройства

Запрет или разрешение передачи файлов через Android Beam и использования NFC

Управление конфигурацией приложения Android устройства

Применение управляемой конфигурации к установленному приложению из JSON-файла

Установка и обновление ПО

Автоматическое обновление PowerShell

Доступна в УД и UEM версиях

Описание

Автоматическое обновление PowerShell — политика для обновления PowerShell до версии 5.1, что обеспечивает возможность выполнения политик на устройстве

Примечание

Данная политика доступна для выполнения только на ОС Windows

Важно

Политика обязательна для выполнения на устройствах с ОС Windows 7 SP1

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

Важно

Для выполнения или сохранения политики название обязательно для заполнения

Остальные вкладки описаны на странице *Политики*

Важно

- Если версия PowerShell на удалённом устройстве ниже версии 5.1, то PowerShell успешно обновится до версии 5.1
- Если версия PowerShell на удалённом устройстве равна версии 5.1, то политика пропустит это устройство и не будет выполняться
- Во время обновления политика может автоматически выполнить одну или несколько перезагрузок устройства

Пример

Для обновления **PowerShell** на устройствах необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **«Политики»**
2. Выбрать шаблон политики **«Автоматическое обновление PowerShell»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Обновление PowerShell
4. Нажать на кнопку Сохранить
5. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
6. После применения политики:
   - PowerShell будет обновлён до версии 5.1

Примечание

Во время выполнения политики может потребоваться дополнительная загрузка пакетов

Если Центр обновления Windows отключен, политика может временно включить его для установки компонентов

Автоматическое обновление клиента RuDesktop

Доступна в УД и UEM версиях

Описание

Автоматическое обновление — политика для обновления клиентского приложения **RuDesktop** на устройствах, подключённых к серверу

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux
- macOS

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

  Linux

  - Не выполнять обновление пакетов на Linux-устройствах — при включении этой опции системные пакеты Linux не будут обновляться перед обновлением клиента

  Windows

  - Не создавать ярлык на рабочем столе — при включении этой опции ярлык на рабочем столе не создаётся
  - Не создавать папку в меню «Пуск» — при включении этой опции папка в меню «Пуск» не создаётся

- Удалять установочный файл после успешного обновления — при включении этой опции установочный файл удаляется после успешного обновления

Остальные вкладки описаны на странице *Политики*

Важно

- Если версия клиента **RuDesktop** на устройстве ниже версии сервера, клиент будет обновлён до актуальной версии
- Если версия клиента **RuDesktop** на устройстве совпадает с версией сервера, политика пропустит это устройство
- На Windows обновление подготавливается через `Scheduled Task`, на Linux — через одноразовую задачу `cron`

Пример

Для обновления клиентов **RuDesktop** на устройствах, подключенных к серверу, необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **«Политики»**
2. Выбрать шаблон политики **«Автоматическое обновление»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Обновление клиентов RuDesktop
4. При необходимости настроить дополнительные параметры для нужной ОС
   - Для Linux: `Не выполнять обновление пакетов на Linux-устройствах`
   - Для Windows: `Не создавать ярлык на рабочем столе`, `Не создавать папку в меню "Пуск"`, `Удалять установочный файл после успешного обновления`
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
7. После применения политики:
   - Если на устройстве уже установлена актуальная версия клиента, обновление не будет выполняться
   - На Windows будет создана задача обновления для запуска MSI-установщика
   - На Linux будет создана одноразовая задача `cron` для запуска скрипта обновления
   - На macOS будет запущен сценарий обновления клиента

Автоматическое обновление Android клиента RuDesktop

Доступна только в MDM версии

Описание

Автоматическое обновление Android клиента RuDesktop — политика для отправки на Android-устройство команды обновления клиента RuDesktop до актуальной версии, доступной на сервере

Политика удобна для централизованного обновления управляемых Android-устройств без ручной переустановки клиента на каждом устройстве

Примечание

Поддерживаемые операционные системы:

- Android

Важно

Для успешного обновления устройство должно быть доступно и управляться через MDM

Рекомендуется:

- Выполнять пробный запуск на одном устройстве перед массовым обновлением
- Убедиться, что устройство имеет доступ к серверу RuDesktop и может получить пакет обновления
- Планировать обновление на время, когда кратковременное прерывание работы клиента допустимо

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующее поле:

- Название — имя политики в системе

Примечание

Дополнительные параметры для этой политики не требуются

Остальные вкладки описаны на странице *Политики*

Пример

Для обновления Android клиента RuDesktop на управляемых устройствах:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Автоматическое обновление Android клиента RuDesktop»**
3. Заполнить поле `Название`

   Например: Обновление Android клиентов
4. Нажать на кнопку Сохранить
5. Выполнить `Тестовый запуск` на одном устройстве
6. После применения политики:
   - На устройстве будет запущено обновление Android клиента **RuDesktop**
7. После успешной проверки запустить политику на остальных Android-устройствах

Обновление ОС

Доступна только в UEM версии

Описание

Обновление ОС - политика для поиска и установки обновлений через настроенные на устройстве источники ОС

См. также

Для установки обновлений Windows из локального каталога и подготовленных пакетов используется отдельный раздел *Обновления ОС* В нём сканирование и установка настраиваются отдельными задачами

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux

- macOS

Свойства политики

После выбора шаблона политики откроются её свойства. Вкладка **«Политика»** содержит следующие поля:

- Название - имя политики

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

- Категории обновлений для ОС Windows - список категорий обновлений для установки, можно указать:
  1. `CriticalUpdates` - критические обновления
  2. `SecurityUpdates` - обновления безопасности
  3. `UpdateRollups` - наборы исправлений и улучшений, объединённые в один пакет
  4. `Connectors` - обновления для отдельных типов программного обеспечения
  5. `DefinitionUpdates` - обновления определений, например для Windows Defender
  6. `FeaturePacks` - обновления функционала
  7. `FeatureUpdates` - крупные обновления Windows с новыми версиями или заметными изменениями функций
  8. `ServicePacks` - крупные наборы обновлений
  9. `Tools` - обновления инструментов и приложений
  10. `Updates` - стандартные обновления Windows
  11. `Drivers` - обновления для драйверов устройств
  12. `All` - поиск и установка всех актуальных обновлений
- Режим обновления для ОС Linux на основе DEB - доступны 2 режима:
  1. `safe` - более осторожный режим обновления пакетов
  2. `full` - полное обновление пакетов
- Обновлять ядро в ОС Linux на основе RPM - при включении этой опции будут обновлены пакеты ядра для RPM-систем, например RedOS, Red Hat, CentOS и Alt Linux
- Перезагрузка - выбор автоматической перезагрузки после изменений на Windows и поддерживаемых Linux-системах

Важно

Если поле `Категории обновлений для ОС Windows` оставить пустым, по умолчанию будут использованы `CriticalUpdates`, `SecurityUpdates` и `UpdateRollups`

Для Linux и macOS категории Windows Update не используются

Остальные вкладки описаны на странице *Политики*

Пример

Для обновления ОС Windows необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Обновление ОС»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Обновление Windows
4. Указать необходимые категории обновлений

   Например: `CriticalUpdates`, `SecurityUpdates`, `UpdateRollups`
5. В поле Перезагрузка выбрать опцию `Перезапустить`
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве под управлением Windows для проверки работоспособности политики
8. После применения политики:
   - На устройстве будут установлены доступные обновления из выбранных категорий
   - На Windows при выбранной опции перезагрузки и наличии изменений система будет перезапущена

Источники обновлений и ограничения

Политика использует Windows Update, пакетный менеджер Linux или `softwareupdate` на macOS. Настройки источников обновлений на устройстве она не заменяет. Перед запуском проверить доступность настроенных источников и свободное место. На Linux отдельные шаги предусмотрены для семейств Debian и Astra Linux, RED / RedHat / CentOS, Altlinux / Simply

Перед массовым запуском проверить политику на устройстве с используемым дистрибутивом Linux. Для DEB обновляется кэш APT и выполняется выбранный режим обновления

Перезагрузка и проверка результата

Предупреждение

На Windows и поддерживаемых Linux-системах вариант **«Перезапустить»** запускает перезагрузку, если при обновлении были выполнены изменения. Перезагрузка возможна и тогда, когда обновления не требуют обязательного перезапуска. Перед перезагрузкой предусмотрены сообщение пользователю и задержка 5 минут. Выбирать этот вариант на время, когда допустим перезапуск устройства

Примечание

На macOS используется встроенное средство обновления системы. На macOS эта политика автоматически не перезагружает устройство. После обновления проверить, нужна ли перезагрузка, и выполнить её отдельно

В журнале проверить выполнение шага обновления, ошибки и итоговое сообщение. Для macOS успешный итог подтверждает завершение команды без ошибки, а не отсутствие всех возможных обновлений. Если возникла ошибка, проверить источник обновлений и состояние пакетного менеджера или службы обновления на устройстве, затем повторить тестовый запуск

Удаление пакета

Доступна только в UEM версии

Описание

Удаление пакета — политика для удаления установленного ПО на удалённом устройстве по имени пакета, установочному файлу или команде удаления

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux
- macOS

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

Важно

Для выполнения или сохранения политики название обязательно для заполнения

- Пакет для удаления — поле для имени или идентификатора пакета в зависимости от типа установщика:
  - При выборе .deb или .rpm пакета поле будет содержать наименование пакета

    Подсказка

    Данное поле заполняется автоматически при выборе файла

  - При выборе .msi пакета поле будет содержать идентификатор пакета

    Подсказка

    Данное поле заполняется автоматически при выборе файла

  - При выборе `.exe` пакета поле можно оставить пустым

Подсказка

Поле поддерживает поиск по уже установленным пакетам. Начните вводить имя пакета — сервер по результатам *инвентаризации* предложит подходящие варианты, из которых можно выбрать нужный. Это позволяет заполнить поле без выбора установочного файла, если пакет уже известен серверу

Важно

Подсказки появляются только после выполнения политики **Инвентаризация** на устройствах — иначе серверу не из чего формировать список установленных пакетов

- Файл инсталлятора — выбор файла для определения пакета

Подсказка

- При нажатии на кнопку Browse откроется окно выбора файла на компьютере

- При нажатии на кнопку Репозиторий откроется всплывающее окно выбора файла из внутреннего репозитория сервера **RuDesktop**

  Важно

  Файлы отображаются из всех репозиториев, какие созданы на сервере **RuDesktop**

- Можно просто перетащить файл в поле Выберите файл или перетащите его сюда

- Команда удаления — команда и опции для удаления пакета

Важно

- Для удаления `.exe` пакетов нужно указать путь до uninstall-файла

  Важно

  После выполнения политики `Инвентаризация` в этом поле можно выбрать найденную команду удаления

- На Windows поле также можно использовать для запуска готовой команды удаления

Примечание

На macOS удаление может выполняться через `Homebrew`, по `.dmg` файлу или удалением `.app` из стандартных каталогов приложений

Примечание

На Windows политика поддерживает удаление приложений, установленных через **Microsoft Store** (UWP/APPX-пакеты). Имя пакета (`PackageFullName` или `Name`) появляется в подсказках поля Пакет для удаления после выполнения политики *Инвентаризация* — выберите его из списка, поле Файл инсталлятора при этом оставьте пустым

- Перезагрузка — настройка поведения после удаления, если требуется перезапуск

Остальные вкладки описаны на странице *Политики*

Пример

Удаление .exe пакета

Для удаления `.exe` пакета необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Удаление пакета»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Удаление пакета
4. Поле `Пакет для удаления` оставить пустым
5. Поле `Файл инсталлятора` оставить пустым
6. Заполнить поле `Команда удаления`

   Например, для удаления в «тихом» режиме: C:\Program Files\ProgramName\uninstall.exe и /s
7. Заполнить поле `Перезагрузка`

   Например: Не перезапускать
8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:
    - Выбранный пакет будет удалён с удалённого устройства

Удаление .msi пакета

Для удаления `.msi` пакета необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Удаление пакета»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Удаление пакета
4. Поле `Пакет для удаления` заполнится автоматически после выбора файла
5. Выбрать файл
6. При необходимости заполнить поле `Команда удаления`

   Например, для удаления в «тихом» режиме: /qn
7. Заполнить поле `Перезагрузка`

   Например: Не перезапускать

8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:
    - Выбранный пакет будет удалён с удалённого устройства

Удаление .deb или .rpm пакета

Для удаления `.deb` или `.rpm` пакета необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Удаление пакета»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Удаление пакета
4. Поле `Пакет для удаления` заполнится автоматически после выбора файла
5. Выбрать файл
6. Поле `Команда удаления` оставить пустым
7. Заполнить поле `Перезагрузка`

   Например: Не перезапускать
8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:
    - Выбранный пакет будет удалён с удалённого устройства

Удаление пакета Android

Доступна только в MDM версии

Описание

Удаление пакета Android — политика для удаления установленного Android-приложения по его package name

Политика полезна для централизованного удаления устаревших, тестовых и запрещённых приложений с корпоративных Android-устройств

Примечание

Поддерживаемые операционные системы:

- Android

Важно

Для корректного выполнения указывайте package name в нижнем регистре, например `com.company.appname`

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Пакет для удаления — package name Android-приложения

Примечание

Поле поддерживает поиск пакета по названию или ввод значения вручную

Остальные вкладки описаны на странице *Политики*

Пример

Для удаления приложения `com.company.appname`:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Удаление пакета Android»**
3. Заполнить поле `Название`

   Например: Удаление тестового приложения
4. Заполнить поле `Пакет для удаления`

   Например: com.company.appname
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android
7. После применения политики:
   - Указанное приложение будет удалено с устройства
   - Package name приложения больше не будет присутствовать в списке установленных пакетов

Примечание

Технические особенности:

- Политика поддерживает выбор пакета из поиска или ручной ввод package name

- Перед удалением выполняется базовая проверка формата имени пакета
- Удаление выполняется через MDM-команду удаления Android-приложения

Предупреждение

Важные предупреждения:

- Неверно указанный package name приведёт к ошибке выполнения или к отсутствию результата
- Удаление приложения может повлиять на рабочие процессы пользователя
- Перед запуском рекомендуется убедиться, что приложение действительно должно быть удалено с целевых устройств

Установка LibreOffice

Доступна только в UEM версии

Описание

Установка LibreOffice — политика для установки LibreOffice

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux
- macOS

Примечание

Политика использует подготовленные официальные установочные файлы LibreOffice и дополнительно устанавливает русскоязычный языковой пакет

Важно

Политика рассчитана на архитектуру `x86-64`

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

Остальные вкладки описаны на странице *Политики*

Пример

Для установки LibreOffice необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Установка LibreOffice»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Установка LibreOffice
4. Нажать на кнопку Сохранить
5. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
6. После применения политики:
   - LibreOffice и русскоязычный языковой пакет будут установлены на устройство

Установка пакета

Доступна только в UEM версии

Описание

Установка пакета — политика для установки приложения из загруженного установочного файла на Windows, Linux и macOS

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux
- macOS

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Файл — выбор файла для загрузки на удалённое устройство

  Подсказка

  - При нажатии на кнопку Browse откроется окно выбора файла на компьютере
  - При нажатии на кнопку Репозиторий откроется всплывающее окно выбора файла из внутреннего репозитория сервера **RuDesktop**

    Важно

    Файлы отображаются из всех репозиториев, созданных на сервере **RuDesktop**

  - Можно просто перетащить файл в поле Выберите файл или перетащите его сюда

- Параметры установки — ключи тихой установки, которые будут переданы установщику. Нажмите на поле, чтобы выбрать готовый набор, или введите свой. Нужный набор зависит от того, чем собран установщик:
  - `msiexec` и `.msi` — `/qn /norestart`
  - Inno Setup — `/VERYSILENT /SUPPRESSMSGBOXES /NORESTART`
  - NSIS — `/S`
  - WiX и загрузчики обновлений — `/quiet /norestart`

- InstallShield — `/s /v"/qn"` или `-s`

Важно

Чаще всего поле используется для `.msi` и `.exe` установщиков

- Пакет — поле для имени или идентификатора пакета в зависимости от типа установщика:
  - При выборе `.deb` или `.rpm` пакета поле будет содержать наименование пакета

    Подсказка

    Данное поле заполняется автоматически при выборе файла

  - При выборе `.msi` пакета поле будет содержать идентификатор пакета

    Подсказка

    Данное поле заполняется автоматически при выборе файла

  - При выборе `.exe` поле можно оставить пустым

Примечание

На Linux и macOS политика также поддерживает установщики, подходящие для текущей ОС, например `.dmg` и `.pkg` на macOS

- Версия пакета — необязательная версия для сравнения с уже установленной. Для `.msi`, `.deb` и `.rpm` определяется автоматически при выборе файла. Для `.exe` укажите вручную: **«Приложения и возможности»** → `Версия`, либо реестр `Uninstall` → `DisplayVersion`. Требует заполненного поля Пакет

Примечание

Для `.rpm` выпуск указывать не обязательно: значение `1.3.2` совпадет с установленным `1.3.2-1.el9`. Если нужно попасть в конкретный выпуск, укажите версию целиком вместе с ним

Примечание

Если версия не указана, политика при каждом запуске будет переустанавливать уже установленную программу и повторно перезагружать устройство

- Режим сравнения версии — как сравнивать значение поля Версия пакета с версией, установленной на устройстве:
  - `Точное совпадение` — значения должны совпасть полностью
  - `По префиксу` — достаточно совпадения начала: указанная `5.2` подойдет для установленной `5.2.00.0000`, но не для `5.20.1`
- Установка от имени пользователя — установка пакета через **«Планировщик задач»** Windows

Подсказка

Для установки пакетов, которые размещаются в профиле пользователя, например: `Yandex Telemost` или `eXpress`, необходимо использовать эту опцию

Важно

- Если список пользователей не указан, политика создаст задачи для всех локальных и доменных пользователей, которые хотя бы один раз входили в систему
- Эти задачи будут храниться в **«Планировщик задач»** или по пути

```
C:\Windows\System32\Tasks\RuDesktopServices
↪"
```

- Имя задачи начинается с `install_package_`. Далее через подчёркивание идут хеш имени пользователя и первые семь символов хеша имени файла пакета
- Для каждого пользователя создаются две задачи: установка и последующее удаление задачи установки
- Если пользователь уже вошёл в систему, пакет установится сразу после применения политики в тихом режиме
- Если одновременно открыто несколько сессий, установка будет запущена для всех этих пользователей
- Для пользователей без активной сессии задача будет ожидать входа в систему

- Пользователи для установки — список пользователей, для которых будет создана задача в планировщике

Подсказка

- Поле можно оставить пустым. В этом случае пакет будет установлен для всех пользователей, которые входили в систему на этом устройстве
- Для разделения пользователей используйте новую строку

Важно

Для доменных пользователей указывайте имя пользователя вместе с доменом, например: `exampleDomain\username`

- Удалить существующие задачи перед созданием новых — предварительно удаляет ранее созданные задачи установки для этого файла
- Удалить файл установщика после успешной установки — удаляет файл установщика из кэша после подтвержденной установки

Примечание

Для отложенной установки через задачи пользователя файл сохраняется до выполнения установки

- Перезагрузка — настройка поведения после установки:
  - `Не перезапускать` — устройство не перезагружается
  - `Перезапустить` — устройство перезагружается сразу после подтвержденной установки, без предупреждения пользователя
  - `Предупредить пользователя и перезапустить` — на устройстве показывается предупреждение с названием пакета и временем перезагрузки, чтобы пользователь успел сохранить работу: на Windows — уведомление в центре уведомлений с кнопками `Перезагрузка`, `Отложить` (если отсрочка разрешена) и `Закрыть`, на Linux и macOS — окно в графической сессии с теми же действиями. Если за устройством никто не работает, оно перезагрузится сразу

Примечание

Кнопка немедленной перезагрузки (`Перезагрузка` на Windows, `Перезагрузить сейчас` на Linux и macOS) перезагружает устройство немедленно. `Закрыть` только убирает предупреждение — перезагрузка всё равно произойдет в назначенное время. После отсрочки предупреждение показывается повторно: за столько минут до новой перезагрузки, сколько задано в поле Отсрочка перезагрузки, минут

Примечание

Перезагрузка запускается только после подтвержденной установки пакета. Если нужная версия уже была установлена и установка пропущена, устройство не перезагружается — причина указывается в итоге выполнения политики

Примечание

Перезагрузку, отложенную предыдущим запуском этой политики, следующий запуск снимает до начала установки, чтобы устройство не ушло в перезапуск посреди установки

Примечание

На Linux запланированная перезагрузка за 5 минут до срока перестает пускать в систему новых пользователей — это штатное поведение `shutdown`, одинаковое для всех дистрибутивов. Уже открытые сессии продолжают работать, вход под `root` разрешен. Если перезагрузку отменить, вход снова разрешается

Примечание

При включенной опции `Установка от имени пользователя` перезагрузка не выполняется ни при одном из вариантов: установка откладывается до входа пользователя и на момент запуска политики еще не выполнена, поэтому подтверждать и перезагружать нечего. В итоге выполнения политики это указывается отдельно

- Отсрочка перезагрузки, минут — через сколько минут перезагрузить устройство после установки. Всё это время пользователю показывается предупреждение с точным временем перезагрузки. Учитывается только при выборе `Предупредить пользователя и перезапустить`. Если поле пустое, перезагрузка произойдет через 15 минут
- Отсрочка пользователем, минут — на сколько минут пользователь может отложить перезагрузку кнопкой в предупреждении. Кнопка отсрочки показывается, только если это значение больше отсрочки перезагрузки. Учитывается только при выборе `Предупредить пользователя и перезапустить`. Если поле пустое, отсрочка составит 60 минут
- Сколько раз можно отложить — сколько раз пользователь может отложить перезагрузку кнопкой в предупреждении. Когда отсрочки закончились, кнопка больше не показывается. Учитывается только при выборе `Предупредить пользователя и перезапустить`. Если поле пустое, отложить можно 1 раз

Важно

Политика поддерживает установку как новой, так и более старой версии пакета, если это допускает установщик текущей ОС

Остальные вкладки описаны на странице *Политики*

Пример

Установка .exe пакета

Для установки `.exe` пакета необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Установка пакета»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Установка пакета
4. Выбрать файл
5. Заполнить поле `Параметры установки`

   Например, для установки в тихом режиме: /s
6. Заполнить поле `Пакет`

   Например: C:\Program Files\ProgramName\run.exe
7. Выбрать значение в поле `Перезагрузка`

   Например: Не перезапускать
8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:
    - Выбранный пакет будет установлен на удалённое устройство

Установка .msi пакета

Для установки `.msi` пакета необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Установка пакета»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Установка пакета

4. Выбрать файл
5. Заполнить поле Параметры установки

   Например, для установки в тихом режиме: /qn
6. Поле Пакет заполнится автоматически после выбора файла
7. Выбрать значение в поле Перезагрузка

   Например: Не перезапускать
8. Нажать на кнопку Сохранить
9. Выполнить Тестовый запуск на устройстве для проверки работоспособности политики
10. После применения политики:
    - Выбранный пакет будет установлен на удалённое устройство

Установка .deb или .rpm пакета

Для установки .deb или .rpm пакета необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Установка пакета»** из списка предложенных шаблонов
3. Заполнить поле Название

   Например: Установка пакета
4. Выбрать файл
5. Поле Параметры установки оставить пустым
6. Поле Пакет заполнится автоматически после выбора файла
7. Выбрать значение в поле Перезагрузка

   Например: Не перезапускать
8. Нажать на кнопку Сохранить
9. Выполнить Тестовый запуск на устройстве для проверки работоспособности политики
10. После применения политики:
    - Выбранный пакет будет установлен на удалённое устройство

См. также

Примеры установки конкретного ПО см. в разделе Кейсы → Установка ПО:

- Yandex Telemost
- eXpress
- PIX Task

Установка пакета Android

Доступна только в MDM версии

Описание

Установка пакета Android — политика для установки Android-приложения на управляемое устройство из одного APK-файла или из архива с несколькими APK

Политика используется для централизованной доставки корпоративных приложений, тестовых сборок и внутренних Android-пакетов

Примечание

Поддерживаемые операционные системы:

- Android

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе
- Файл — пакет приложения для загрузки и установки на устройство

Важно

Для обычного приложения выберите файл `.apk`. Если приложение состоит из базового APK и дополнительных частей (Split APK), выберите архив целиком, например `.apks` или `.xapk`. Распаковывать его вручную не нужно

Остальные вкладки описаны на странице *Политики*

Пример

Для установки корпоративного Android-приложения:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Установка пакета Android»**
3. Заполнить поле `Название`

   Например: Установка мобильного клиента
4. В поле `Файл` выбрать файл приложения или архив с его частями
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве Android

7. После запуска клиент загрузит файл и передаст его установщику Android. Проверьте на устройстве, что приложение установлено

Примечание

Технические особенности:

- Для загрузки файла на устройство используется механизм передачи файла агента
- Установка выполняется через MDM-команду установки APK
- Для составного пакета клиент устанавливает базовый APK вместе с подходящими частями за одну операцию. Для установки клиенту нужны права владельца устройства (Device Owner)

Предупреждение

Важные предупреждения:

- Устанавливаемый APK должен быть совместим с версией Android и архитектурой устройства
- Если на устройстве запрещена установка такого пакета, операция может завершиться ошибкой
- Перед массовой установкой рекомендуется протестировать приложение на одном устройстве

Установка пакета из архива

Доступна только в UEM версии

Описание

Установка пакета из архива — политика для установки приложения из загруженного архива на Windows-устройстве

Примечание

Данная политика доступна для выполнения на ОС:

- Windows

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

Важно

Для выполнения или сохранения политики название обязательно для заполнения

- Файл — выбор архива для загрузки на удалённое устройство

Важно

Обычно используется архив `.zip`

Подсказка

- При нажатии на кнопку Browse откроется окно выбора файла на компьютере
- При нажатии на кнопку Репозиторий откроется всплывающее окно выбора файла из внутреннего репозитория сервера **RuDesktop**

  Важно

  Файлы отображаются из всех репозиториев, которые созданы на сервере **RuDesktop**

- Можно просто перетащить файл в поле Выберите файл или перетащите его сюда

- Установщик в архиве — имя установочного файла внутри архива

Подсказка

Пример: setup.exe

- Пакет — необязательный идентификатор приложения для проверки в реестре Windows
- Имя программы — необязательное отображаемое имя приложения в Windows
- Версия пакета — необязательная версия для сравнения с уже установленной

Примечание

Если заполнить версию и одно из полей `Пакет` или `Имя программы`, политика сможет пропустить загрузку архива, если нужная версия уже установлена

- Режим сравнения версии — способ сравнения версии при предварительной проверке
  - `Точное совпадение`
  - `По префиксу (5.5.9 = 5.5.9.0)`
- Файл конфигурации установки (в архиве) — необязательный файл трансформации `.mst` для MSI-установщика
- Параметры установки — ключи тихой установки, которые будут переданы установщику. Нажмите на поле, чтобы выбрать готовый набор, или введите свой. Нужный набор зависит от того, чем собран установщик:
  - `msiexec` и `.msi` — `/qn /norestart`
  - Inno Setup — `/VERYSILENT /SUPPRESSMSGBOXES /NORESTART`
  - NSIS — `/S`
  - WiX и загрузчики обновлений — `/quiet /norestart`
  - InstallShield — `/s /v"/qn"` или `-s`
- Установка от имени пользователя — установка через планировщик задач Windows от имени выбранных пользователей
- Пользователи для установки — список пользователей для установки через планировщик задач
- Удалить архив и распакованные файлы после успешной установки — очищает кэш после подтвержденной установки
- Перезагрузка — настройка поведения после установки, если требуется перезапуск. Вариант `Предупредить пользователя и перезапустить` показывает на устройстве уведомление с названием пакета и временем перезагрузки, чтобы пользователь успел сохранить работу. В уведомлении есть кнопки `Перезагрузка`, `Отложить` (если отсрочка разрешена) и `Закрыть`. Если за устройством никто не работает, оно перезагрузится сразу

Примечание

`Перезагрузка` перезагружает устройство немедленно. `Закрыть` только убирает предупреждение — перезагрузка всё равно произойдет в назначенное время. `Отложить` переносит перезагрузку на время из поля Отсрочка пользователем, минут, после чего предупреждение показывается повторно: за столько минут до новой перезагрузки, сколько задано в поле Отсрочка перезагрузки, минут

Примечание

Перезагрузка запускается только после подтвержденной установки пакета. Если нужная версия уже была установлена и загрузка архива пропущена, устройство не перезагружается

Примечание

Перезагрузку, отложенную предыдущим запуском этой политики, следующий запуск снимает до начала установки, чтобы устройство не ушло в перезапуск посреди установки

Примечание

При включенной опции `Установка от имени пользователя` перезагрузка не выполняется ни при одном из вариантов: установка откладывается до входа пользователя и на момент запуска политики еще не выполнена, поэтому подтверждать и перезагружать нечего. В итоге выполнения политики это указывается отдельно

- Отсрочка перезагрузки, минут — через сколько минут перезагрузить устройство. Всё это время пользователю показывается предупреждение. Учитывается только при выборе `Предупредить пользователя и перезапустить`. Если поле пустое, перезагрузка произойдет через 15 минут
- Отсрочка пользователем, минут — на сколько минут пользователь может отложить перезагрузку кнопкой в предупреждении. Кнопка отсрочки показывается, только если это значение больше отсрочки перезагрузки. Учитывается только при выборе `Предупредить пользователя и перезапустить`. Если поле пустое, отсрочка составит 60 минут
- Сколько раз можно отложить — сколько раз пользователь может отложить перезагрузку кнопкой в предупреждении. Когда отсрочки закончились, кнопка больше не показывается. Учитывается только при выборе `Предупредить пользователя и перезапустить`. Если поле пустое, отложить можно 1 раз

Остальные вкладки описаны на странице *Политики*

Пример

Установка пакета из .zip архива

Для установки пакета из `.zip` архива на Windows необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики Установка пакета из архива из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Установка пакета из архива
4. Выбрать архив
5. Заполнить поле `Параметры установки`

Например, для установки в тихом режиме: /s

6. Заполнить поле `Установщик в архиве`

   Например: setup.exe

7. Заполнить поле `Перезагрузка`

   Например: Не перезапускать

8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:
    - Выбранный пакет будет установлен из архива на удалённое устройство

См. также

Примеры установки конкретного ПО см. в разделе Кейсы → Установка ПО:

- Kaspersky Endpoint Security
- 1C

Установка Python на Linux/macOS

Доступна в УД и UEM версиях

Описание

Установка Python на Linux/macOS — политика, которая разворачивает подготовленное Python-окружение из архива на устройства Linux или macOS

Политика подходит для поставки одинакового окружения на множество устройств, когда требуется фиксированная версия Python и набор зависимостей

Примечание

Поддерживаемые операционные системы:

- Linux
- macOS

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

- Архив окружения Python — пользовательский архив с подготовленным окружением

> **Примечание**
>
> Поддерживаются архивы `tar.gz` и `tar.xz`
>
> Если архив не указан, будет использован встроенный вариант, автоматически подобранный по ОС и архитектуре устройства

Остальные вкладки описаны на странице *Политики*

Пример

Для установки подготовленного Python-окружения на Linux-устройство:

1. Нажать на кнопку Добавить Политику
2. Выбрать шаблон политики **«Установка Python на Linux/macOS»**
3. Заполнить поле `Название`

   Например: Развертывание Python-окружения
4. При необходимости заполнить поле `Архив окружения Python`

   Например: python3.13.12-x86_64.tar.gz
5. Нажать на кнопку Сохранить
6. Выполнить `Тестовый запуск` на устройстве
7. После применения политики:
   - Python-окружение будет развернуто на устройстве
   - Будет использован пользовательский или встроенный архив, подходящий под платформу

> **Примечание**
>
> **Технические особенности:**
>
> - Политика определяет ОС и архитектуру устройства автоматически
> - Если архив не задан вручную, выбирается встроенный архив окружения
> - На macOS после распаковки выполняется переподпись бинарных файлов окружения
> - После установки интерпретатор сохраняется в кэше фактов как `discovered_interpreter_python`

Предупреждение

Важные предупреждения:

- Политика не предназначена для Windows
- Пользовательский архив должен быть корректным `tar`-архивом с ожидаемой структурой окружения
- Недостаток свободного места на диске может привести к сбою развертывания

Установка сертификата

Доступна только в UEM версии

Описание

Установка сертификата — политика для установки или удаления сертификата на удалённом устройстве

На macOS сертификат добавляется в выбранный keychain без явной настройки доверия, то есть в состоянии `unspecified` и не становится `trust` автоматически

Примечание

Данная политика доступна для выполнения на ОС:

- Windows
- Linux
- macOS

Свойства политики

После выбора шаблона политики откроются её свойства

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Сертификат — выбор файла сертификата для загрузки на удалённое устройство

Подсказка

- При нажатии на кнопку Browse откроется окно выбора файла на компьютере
- При нажатии на кнопку Репозиторий откроется всплывающее окно выбора файла из внутреннего репозитория сервера **RuDesktop**

  Важно

  Файлы отображаются из всех репозиториев, созданных на сервере **RuDesktop**

- Можно просто перетащить файл в поле Выберите файл или перетащите его сюда

- Режим выполнения — определяет, нужно установить или удалить сертификат
  - `установить сертификат`
  - `удалить сертификат`
- Имя хранилища сертификатов (Для Windows) — имя хранилища, которое будет использоваться при импорте сертификата или при поиске сертификата
- Тип хранилища для управления (Для Windows) — тип хранилища, который определяет место хранения сертификатов и уровень доступа к ним

Важно

- Используйте `system` для управления расположениями в системном хранилище LocalMachine и CurrentUser (по умолчанию)
- Используйте `service` для управления хранилищем учётной записи службы

- Пароль (Для Windows) — пароль к сертификату, если он требуется
- Хранилище сертификатов (Для macOS) — выбор системного или пользовательского keychain на macOS
- Пользовательский путь к keychain (Для macOS, опционально) — позволяет явно указать путь к keychain вместо стандартного хранилища

Остальные вкладки описаны на странице *Политики*

Пример

Установка сертификата на Windows

Для установки сертификата на Windows необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Установка сертификата»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Установка сертификата
4. Выбрать файл сертификата
5. В поле `Имя хранилища сертификатов (Для Windows)` выбрать имя хранилища

   Например: хранилище сертификатов для личных сертификатов
6. Заполнить поле `Тип хранилища для управления (Для Windows)`

   Например: system
7. Поле `Пароль (Для Windows)` оставить пустым
8. Нажать на кнопку Сохранить
9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:
    - Выбранный сертификат будет установлен на удалённое устройство

Установка сертификата на Linux

Для установки сертификата на Linux необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Установка сертификата»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Установка сертификата
4. Выбрать файл сертификата
5. Поле `Имя хранилища сертификатов (Для Windows)` оставить без изменений
6. Поле `Тип хранилища для управления (Для Windows)` оставить пустым
7. Поле `Пароль (Для Windows)` оставить пустым
8. Нажать на кнопку Сохранить

9. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
10. После применения политики:
    - Выбранный сертификат будет установлен на удалённое устройство

Установка сертификата на macOS

Для установки сертификата на macOS необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Установка сертификата»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Установка сертификата
4. Выбрать файл сертификата
5. В поле `Хранилище сертификатов (Для macOS)` выбрать нужное хранилище

   Например: системное хранилище
6. При необходимости заполнить поле `Пользовательский путь к keychain (Для macOS, опционально)`
7. Нажать на кнопку Сохранить
8. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
9. После применения политики:
    - Выбранный сертификат будет добавлен в выбранный keychain macOS

Установка и удаление пакета из репозитория

Доступна только в UEM версии

Описание

Установка/удаление пакета из репозитория — политика для установки, удаления и обновления пакетов из системных репозиториев на Windows, Linux и macOS

Примечание

Поддерживаемые операционные системы:

- Windows
- Linux
- macOS

Примечание

Как выполняется установка в зависимости от ОС:

- **Windows:** через `Chocolatey`
- **macOS:** через `Homebrew` (формулы)
- **Linux:** через системный пакетный менеджер

Важно

Важно учитывать:

- На Windows 7 / Windows Server 2008 R2 политика не поддерживается для Chocolatey-сценария
- На macOS для работы политики требуется установленный `Homebrew`
- Для Linux в поле пакетов нужно указывать точные имена пакетов

Свойства политики

После выбора шаблона политики откроется окно с её свойствами

Вкладка **«Политика»** содержит следующие поля:

- Название — имя политики в системе

  Важно

  Для выполнения или сохранения политики название обязательно для заполнения

- Действие — требуемое состояние пакета
  - `Установить пакет` — установка пакета, если он отсутствует
  - `Удалить пакет` — удаление пакета, если он установлен
  - `Обновить пакет до последней версии` — обновление установленного пакета до актуальной версии (или установка, если пакет отсутствует)
- Windows | Пакеты для установки (Chocolatey) — список пакетов Chocolatey для Windows-устройств

  Подсказка

  Можно выбрать один или несколько пакетов из справочника или указать точные имена вручную

- macOS | Пакеты для установки (Homebrew) — список формул Homebrew для macOS-устройств

Подсказка

Поддерживаются формулы Homebrew

Можно указать один или несколько пакетов

- Linux | Пакеты для установки — список Linux-пакетов для Linux-устройств

Подсказка

Указывайте точные имена пакетов

Можно перечислить несколько значений

Важно

Для текущей ОС используется только соответствующее ей поле со списком пакетов

На Windows 7 и Windows Server 2008 R2 эта политика не поддерживается

Остальные вкладки описаны на странице *Политики*

Пример

Для запуска политики необходимо:

1. Нажать на кнопку Добавить Политику в верхнем правом углу экрана на странице **Политики**
2. Выбрать шаблон политики **«Установка/удаление пакета из репозитория»** из списка предложенных шаблонов
3. Заполнить поле `Название`

   Например: Установка htop из репозитория
4. Выбрать значение в поле `Действие`

   Например: Установить пакет
5. Заполнить поле пакетов для нужной ОС
   - `Windows | Пакеты для установки (Chocolatey)`
   - `macOS | Пакеты для установки (Homebrew)`
   - `Linux | Пакеты для установки`

   Например: htop
6. Нажать на кнопку Сохранить
7. Выполнить `Тестовый запуск` на устройстве для проверки работоспособности политики
8. После применения политики:

- При `Установить пакет` пакет будет установлен, если его не было
- При `Удалить пакет` пакет будет удалён, если он был установлен
- При `Обновить пакет до последней версии` пакет будет обновлён до актуального состояния

Предупреждение

При работе с политикой учитывайте:

- Если указано некорректное имя пакета, установка или проверка завершится ошибкой
- На macOS при проблемах с правами на каталоги Homebrew политика может пытаться восстановить права на критичных каталогах
- На Windows при отсутствии Chocolatey сценарий удаления может завершиться без изменений, если пакет не обнаружен
- Перед массовым применением рекомендуется выполнить тестовый запуск на одном устройстве

Автоматическое обновление PowerShell

Обновление PowerShell на устройстве с Windows

Автоматическое обновление клиента RuDesktop

Обновление клиента RuDesktop на десктопных ОС

Автоматическое обновление Android клиента RuDesktop

Обновление клиента RuDesktop на Android-устройствах

Обновление ОС

Установка обновлений операционной системы устройства

Удаление пакета

Удаление установленного пакета с устройства

Удаление пакета Android

Удаление приложения с Android-устройства

Установка LibreOffice

Установка офисного пакета LibreOffice

Установка пакета Android
Установка APK-приложения на Android-устройство

Установка пакета
Установка пакета через системный пакетный менеджер

Установка пакета из архива
Установка ПО из архивного файла на устройстве

Установка Python на Linux/macOS
Установка Python на устройство Linux или macOS

Установка сертификата
Добавление корневого сертификата в хранилище устройства

Установка и удаление пакета из репозитория
Управление пакетами на устройстве через подключённый репозиторий

Шаблоны политик — каталог готовых Ansible-плейбуков, на основе которых создаются *политики*. Шаблоны сгруппированы по категориям

Подсказка

Каталог шаблонов и большинство шаблонов внутри доступны при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**. Шаблоны для управления Android-устройствами доступны только при наличии лицензии **MDM**

Обслуживание и администрирование
Шаблоны для инвентаризации, выполнения команд и управления службами

Обслуживание сервера RuDesktop
Шаблоны для обслуживания самого сервера RuDesktop

Управление безопасностью и доступом
Шаблоны для блокировки пользователей и USB-устройств

Управление директориями и файлами

Шаблоны для работы с файлами, директориями и реестром

Управление пользователями и устройствами

Шаблоны для управления локальными пользователями и параметрами устройств

Установка и обновление ПО

Шаблоны для установки, удаления и обновления пакетов и клиента

Политика — это операция, которую Ansible[24] выполняет на управляемом устройстве

Подсказка

Страница **«Политики»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Примечание

По умолчанию имеются предустановленные политики:

- Инвентаризация устройств — собирает факты с устройств и пересчитывает *динамические группы*
- Обновление устройств — обновляет клиент **RuDesktop** на устройствах до актуальной версии
- Обслуживание сервера — фоновое обслуживание самого сервера (очистка временных данных, переиндексация и т.п.)

Предустановленные политики можно удалить и редактировать

Как это работает

Политика создаётся не с нуля, а на основе **шаблона** — готового Ansible-плейбука. **RuDesktop** поставляется с библиотекой шаблонов (см. *Шаблоны политик*), сгруппированных по категориям: обслуживание и администрирование, обслуживание сервера, безопасность и доступ, файлы и директории, пользователи и устройства, установка и обновление ПО

Каждая политика хранит:

- **выбранный шаблон** — определяет, какой плейбук будет выполнен;
- **параметры** — введённые администратором значения полей шаблона (имена, пути, флаги, пароли);

[24] https://docs.ansible.com/

- **прикреплённые файлы** — установочные пакеты, сертификаты, скрипты и иконку для магазина приложений (загружаются на сервер при сохранении политики);
- **признаки публикации** — будет ли политика отображаться в *Портале самообслуживания* и в магазине приложений, нужно ли запускать её автоматически по обращению;
- **категорию приложения** — категория для отображения в магазине приложений (только для политик с публикацией в магазине).

При создании политики вы:

1. выбираете шаблон, описывающий **что** делать (установить пакет, изменить пароль, выполнить команду и т.д.);
2. задаёте параметры шаблона на вкладке Политика (имена, пути, флаги — набор полей зависит от шаблона);
3. при необходимости прикрепляете установочный файл или иконку (через Browse или из внутреннего *репозитория*);
4. при необходимости публикуете политику в Портал самообслуживания или Магазин приложений, чтобы пользователь мог запросить её через портал;
5. сохраняете — политика попадает в общий список и может быть запущена тестово, вручную или добавлена в *задачу*.

Сама политика **не запускается автоматически** при создании. Запустить её можно одним из способов:

- **Тестовый запуск** — кнопка Запустить на вкладке Тестовый запуск в свойствах политики; используется для проверки на конкретных устройствах перед массовым применением;
- **из контекстного меню устройства** — на странице *Устройства* через действие Политики → выбор нужной политики;
- **в составе задачи** — добавить политику в *задачу* и запускать по расписанию, при подключении устройства или вручную;
- **через обращение** — пользователь оформляет обращение через *Портал самообслуживания* и выбирает политику из списка опубликованных. При активном флаге Автоматический запуск политика выполнится сразу, без подтверждения администратора;
- **через магазин приложений** — пользователь нажимает Установить на карточке приложения в портале самообслуживания, и сервер сразу запускает соответствующую политику.

Результаты каждого запуска попадают в *Логи исполнения*, а агрегированная статистика по устройствам — на страницу *Статистика выполнения*

Системные и пользовательские шаблоны

Шаблоны делятся на две категории по происхождению:

- **системные** — поставляются вместе с сервером **RuDesktop**, их YAML-файлы лежат в каталоге системных плейбуков и **не редактируются** напрямую. На вкладке Шаблон они открываются только для просмотра;
- **пользовательские** — копии системных шаблонов или собственные плейбуки, созданные администратором. Хранятся в каталоге пользовательских плейбуков и доступны для редактирования.

Важно

Чтобы изменить логику системного плейбука, на вкладке Шаблон нажмите Создать новый шаблон на его основе, задайте уникальный ID и название — будет создана пользовательская копия, которую можно править. ID должен быть уникальным; иначе сервер не позволит сохранить копию

Доступность шаблонов и лицензия

Список шаблонов, отображаемых при добавлении политики, зависит от лицензии сервера:

- шаблоны базового удалённого доступа (например, инвентаризация и обслуживание клиента) доступны **в любой версии**;
- шаблоны управления мобильными устройствами доступны только при наличии лицензии **MDM**;
- остальные шаблоны (обслуживание, безопасность, файлы, пользователи, установка ПО) доступны только при наличии лицензии **UEM**.

При смене лицензии часть шаблонов может перестать отображаться — уже созданные политики, созданные на этих шаблонах, останутся в базе, но запустить их без подходящей лицензии будет невозможно

Шифрование чувствительных данных

Поля типа Пароль в свойствах политики сохраняются в базе **зашифрованными** через механизм Ansible Vault — в открытом виде введённое значение в базе не лежит. При экспорте политики в файл такие поля попадают в выгрузку в том же зашифрованном виде

Подсказка

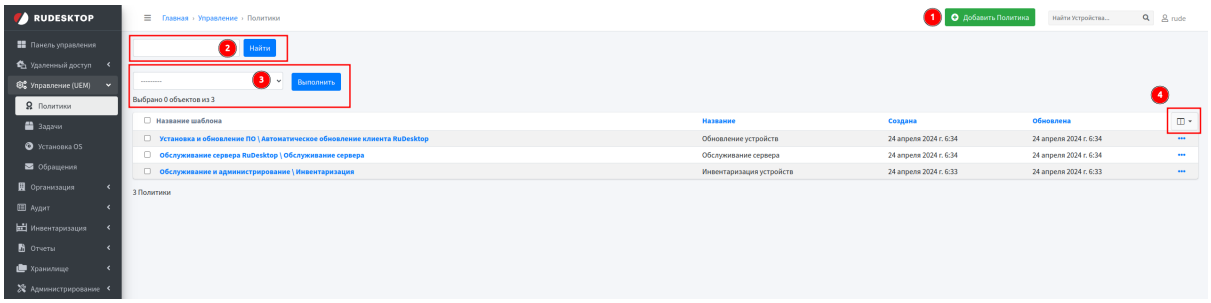
После сохранения политики ввести значение «снова посмотреть» в веб-интерфейсе нельзя — поле отображается как поле пароля и не показывает оригинал. Чтобы изменить пароль, нужно ввести его заново; старое зашифрованное значение будет перезаписано

Примечание

На время **выполнения** политики сервер расшифровывает пароли и подставляет их в плейбук, который передаётся **Ansible** — иначе агент не сможет ими воспользоваться. Этот промежуточный YAML существует только в процессе запуска и пользователю не показывается. На вкладке Шаблон отображается **тело шаблона** без значений параметров, поэтому пароли там никогда не появляются

Описание страницы

На странице **Политики** отображено:



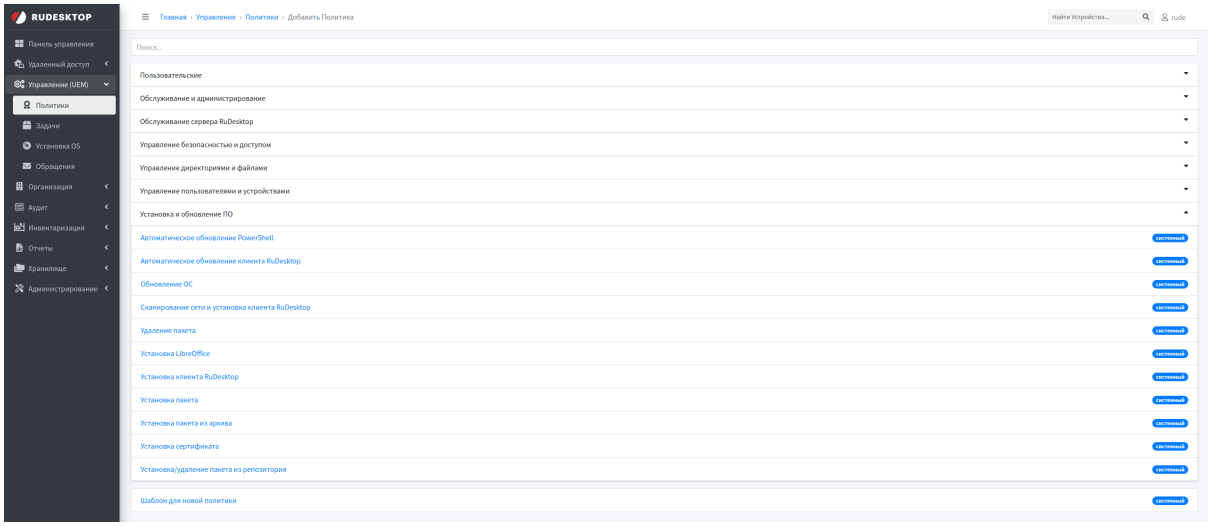
1. Кнопка Добавить Политику
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление политики

При нажатии на кнопку Добавить Политику откроется страница с выбором шаблона политики, в котором необходимо выбрать шаблон, а также указать параметры для выполнения политики

Чтобы выбрать шаблон, нужно нажать на нужную категорию, после чего она откроется и будут отображены шаблоны политик для выбора

Нажатие по другой категории закроет ранее открытую категорию



После выбора шаблона политики откроются ее свойства, которые поделены на 5 вкладок:

Политика

- Название — наименование политики

> **Важно**
>
> Для выполнения или сохранения политики название обязательно для заполнения

- Остальные поля отличаются в зависимости от шаблона политики. Подробнее о полях можно узнать в описании шаблонов политик

> **Подсказка**
>
> Поля типа Файл поддерживают как загрузку с компьютера через кнопку Browse (drag-and-drop тоже работает), так и выбор уже загруженного файла из внутреннего *репозитория* через кнопку Репозиторий. Поля типа Пароль сохраняются в зашифрованном виде через Ansible Vault — в дальнейшем посмотреть введённое значение нельзя, можно только перезаписать новым

Портал самообслуживания

Общие настройки

- **Показывать в разделе: «Портал самообслуживания»** — при создании обращения через портал самообслуживания будет возможность выбрать данную политику
- **Автоматический запуск** — после создания обращения политика выполнится автоматически, без подтверждения со стороны администратора

Магазин приложений

- **Показывать в магазине приложений** — при выборе этого чекбокса политика будет отображаться в магазине приложений

Важно

Если в Общие настройки не активирован чекбокс **Показывать в разделе: «Портал самообслуживания»**, то при активации чекбокса **Показывать в магазине приложений** чекбокс **Показывать в разделе: «Портал самообслуживания»** активируется автоматически

- **Категория приложения** — категория для группировки политики в магазине приложений (например, «Офисные пакеты», «Утилиты»). Список категорий ведётся отдельно — добавлять новые категории может администратор
- **Название приложения** — название будет отображено в магазине приложений
- **Описание приложения** — описание будет отображено в магазине приложений
- **Иконка приложения** — иконка будет отображена в магазине приложений

Важно

Рекомендуется использовать формат иконки `.svg`

Подсказка

Подробный сценарий публикации политики в магазине, включая выдачу прав пользователям и проверку отображения карточки приложения, описан в кейсе Публикация приложения в магазине приложений

Данные

Вкладка Данные содержит опции, которые были выбраны во вкладках Политика и Портал самообслуживания

Важно

Они необходимы для плейбука ansible. В ходе выполнения политики будут использоваться значения `vars`

Шаблон

Вкладка Шаблон содержит шаблон плейбука для выполнения

Подсказка

В пользовательском шаблоне выбранный файл доступен по имени параметра из `vars_prompt`. Например, если у поля `type: file` указано `name: installer`, путь к файлу в плейбуке — `{{ installer.path }}`

Редактор подсвечивает YAML и предлагает названия модулей Ansible, ключевые слова и параметры выбранного модуля. При наведении на модуль или параметр отображается справка, если она доступна на сервере. Результаты проверки синтаксиса показываются в редакторе: если сервер смог определить место ошибки, соответствующий участок выделяется

Примечание

Подсказки и проверка синтаксиса не заменяют Тестовый запуск. Они не подтверждают, что политика успешно выполнится на выбранной ОС с заданными параметрами и правами

Важно

- В этой вкладке можно просмотреть, как устроен шаблон
- Системный шаблон политики не предназначен для редактирования

Для создания политики на основе уже готового шаблона необходимо:

1. Выбрать предустановленную политику Шаблон для новой политики
2. Перейти во вкладку Шаблон и нажать на Создать новый шаблон на его основе
3. Ввести в поле ID шаблона уникальный ID шаблона и в поле Название шаблона

Примечание

Если ID не уникальный, система не позволит создать копию шаблона для редактирования

После чего внести необходимые правки в шаблоне и нажать на кнопку Сохранить шаблон

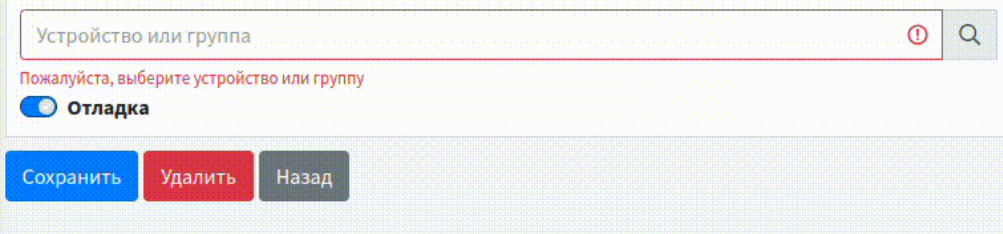
Тестовый запуск

- **Окно логирования** — в нем отображается лог выполнения политики в реальном времени; вывод стримится с сервера по мере поступления событий от Ansible
- **Выбор целей выполнения** — поле выбора устройств и групп, на которых будет выполнена политика. Поддерживается выбор сразу несколь-

ких целей: выбранные элементы отображаются в виде «чипов». Поиск по списку выполняется по мере ввода. Доступны вкладки-фильтры:

- Все — устройства, группы и динамические группы вместе
- Устройства — отдельные устройства (с иконкой ОС и статусом онлайн/офлайн)
- Группы — статические группы устройств
- Дин.группы — динамические группы

Также можно выбрать специальные цели Все устройства, Все группы и Все дин.группы



Примечание

Для выбора целей выполнения требуется право **Может запускать политики**, а также права на просмотр устройств и групп

- Кнопка Запустить запускает выполнение политики
- Кнопка Остановить останавливает выполнение политики
- Кнопка Сохранить лог позволяет загрузить файл с логом выполнения политики

Важно

Тестовый запуск выполняет политику **по-настоящему**: пакеты ставятся, файлы создаются, пароли меняются. Это полноценное применение политики к выбранным устройствам, а не симуляция. Используйте его для проверки на ограниченном круге устройств перед массовым применением через *задачу*

Подсказка

Перед запуском политика автоматически сохраняется. Если вкладка Политика не прошла валидацию (например, не заполнено обязательное поле), запуск не стартует — нужно сначала исправить ошибки в полях

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. `Название категории` — фильтрация политик по категории шаблона
2. `Название шаблона` — фильтрация политик по конкретному шаблону
3. `Поле поиска` — поиск по ключевому слову

Важно

Поиск работает как по названию шаблона, так и по названию политики

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные политики — удаляет выбранные записи из таблицы
2. Экспортировать выбранные политики — позволяет экспортировать в файл выбранные политики

Примечание

После выбора данного действия нужно выбрать необходимый формат файла

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление политик

Для массового удаления политик необходимо:

1. Отметить необходимые политики в таблице
2. Выбрать действие Удалить выбранные политики
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие политики будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные политики будут удалены

Экспорт политик

Для массового экспорта политик необходимо:

1. Отметить необходимые политики в таблице
2. Выбрать действие Экспортировать выбранные политики
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Название шаблона` — системное имя шаблона политики и категория, к которой принадлежит данная политика. Если шаблон политики был удалён (например, после смены лицензии), к имени добавляется пометка `[шаблон удален]`
2. `Название` — пользовательское название политики
3. `Создана` — дата и время создания политики
4. `Обновлена` — дата и время последнего изменения политики

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства политики
2. `Удалить` — при выборе этого пункта политика будет удалена
3. `История изменений` — при выборе этого пункта будет отображена история политики: создание/редактирование и пользователь, который выполнил данные операции

Важно

Удаление политики не удаляет уже накопленные *Логи исполнения* и *Статистику выполнения* — они продолжают храниться по идентификатору политики, и переход к ним остаётся возможен из соответствующих страниц

Шаблоны политик

Обслуживание и администрирование
Обслуживание сервера RuDesktop

Управление безопасностью и доступом
Управление директориями и файлами

Управление пользователями и устройствами
Установка и обновление ПО

2.7.2 Задачи

Доступны в УД и UEM версиях

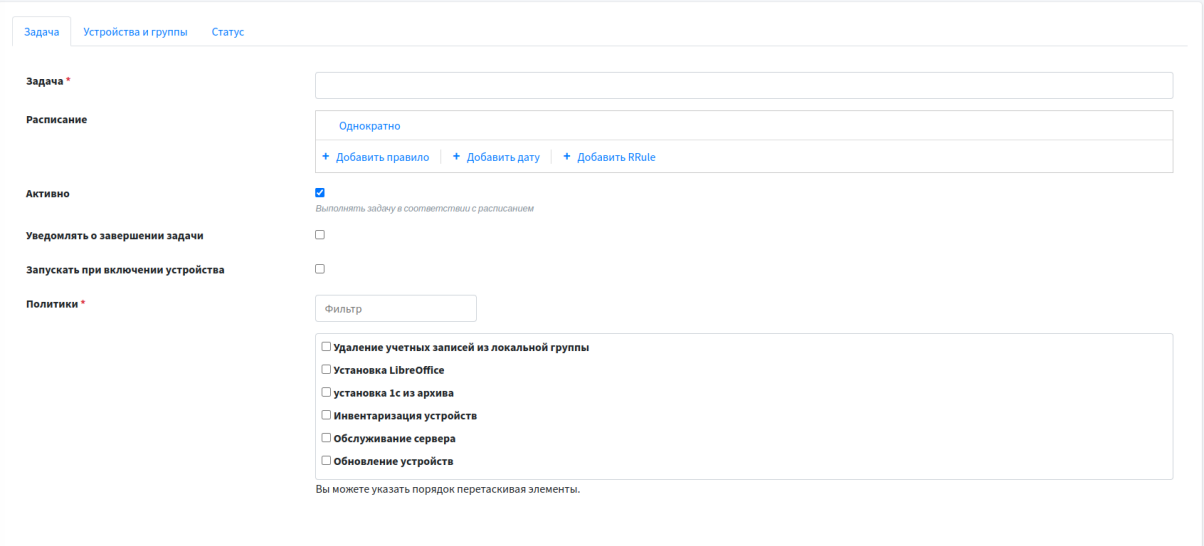
Создание задачи

Доступно в УД и UEM версиях

Вкладки

Задача

Вкладка Задача предоставляет возможность задать основные параметры задачи и включает следующие элементы:



- Задача — наименование задачи

> **Важно**
>
> Для сохранения задачи название обязательно для заполнения

- Расписание — данное поле служит для управления расписанием выполнения задачи

  По умолчанию установлен параметр **«Однократно»**, который подразумевает разовое выполнение

  Опции расписания:

  1. `Добавить правило` — при использовании этой опции можно настроить:
     1. Исключение
     2. Частоту выполнения политики (каждый год, месяц, неделю, день или час) начиная с определенной даты и времени
     3. Выбор дней выполнения политики
     4. Повторение выполнения политики до определенной даты
  2. `Добавить дату` — выбрать определенную дату и время для выполнения политики или сделать исключение
  3. `Добавить RRule` — можно сгенерировать формулу даты/интервала и прописать для выполнения

Подсказка

Формулу можно сгенерировать тут: https://icalendar.org/rrule-tool.html

- Активно — если этот чекбокс активирован, политика будет выполняться в соответствии с настроенным расписанием

Примечание

Если чек-бокс не активирован, задача не будет выполняться даже при наличии настроенного расписания

- Запускать при включении устройства — если этот чекбокс активирован, задача выполнится на устройстве, когда оно появится в онлайне
- Приоритет — в зависимости от выбранного приоритета задача будет выполнена в первую очередь или в последнюю

  Доступные уровни приоритета:

  - `Низкий приоритет` — задачи с низким приоритетом выполняются после всех задач со средним, высоким и критическим приоритетом
  - `Средний приоритет` — задачи со средним приоритетом выполняются после всех задач с высоким и критическим приоритетом, но до задач с низким приоритетом
  - `Высокий приоритет` — задачи с высоким приоритетом выполняются после задач с критическим приоритетом, но до задач со средним и низким приоритетами
  - `Критический приоритет` — задачи с критическим приоритетом выполняются в первую очередь, опережая все остальные задачи
- Политики — в рамках создаваемой задачи можно выбрать политики для выполнения, а также воспользоваться полем для поиска по политикам

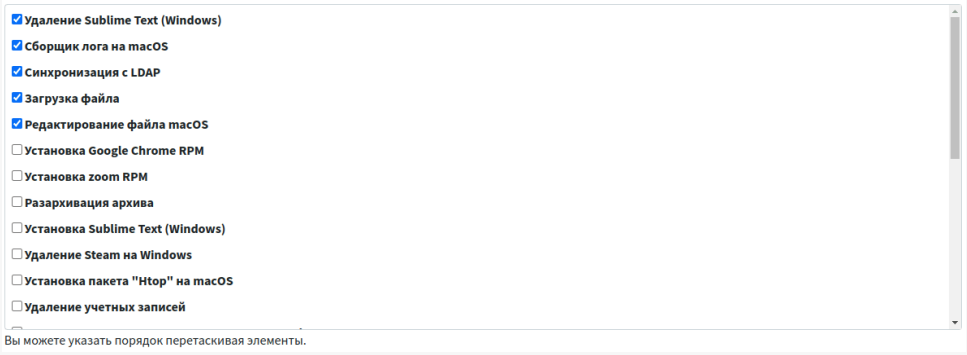
  Чтобы открыть страницу политики, нажмите на стрелку рядом с ее названием в списке Страница откроется в новой вкладке, поэтому можно посмотреть настройки политики, не закрывая форму задачи

Примечание

Стрелка отображается только при наличии права **«Политики» - «Просмотр»**

Важно

Очередность выполнения политик можно задать, перетаскивая элементы



Подсказка

Количество политик в одной задаче можно выбрать без ограничений

- Отчеты — выбор *шаблонов отчётов*, по которым после завершения задачи будут автоматически сформированы готовые отчёты. Поле представляет собой два блока: `Доступные Отчеты` (все доступные шаблоны) и `Выбранные Отчеты` (шаблоны, которые будут построены)

Подсказка

Чтобы добавить шаблон, дважды кликните по нему в блоке `Доступные Отчеты` или выделите и нажмите . В одной задаче можно выбрать несколько шаблонов — для каждого будет сформирован отдельный файл

- Форматы отчета — формат, в котором будут сформированы отчёты по выбранным шаблонам. Доступны два чекбокса:
  - **PDF**
  - **XLSX**

  Можно активировать оба — тогда для каждого шаблона будет построен отдельный файл в каждом из выбранных форматов

Важно

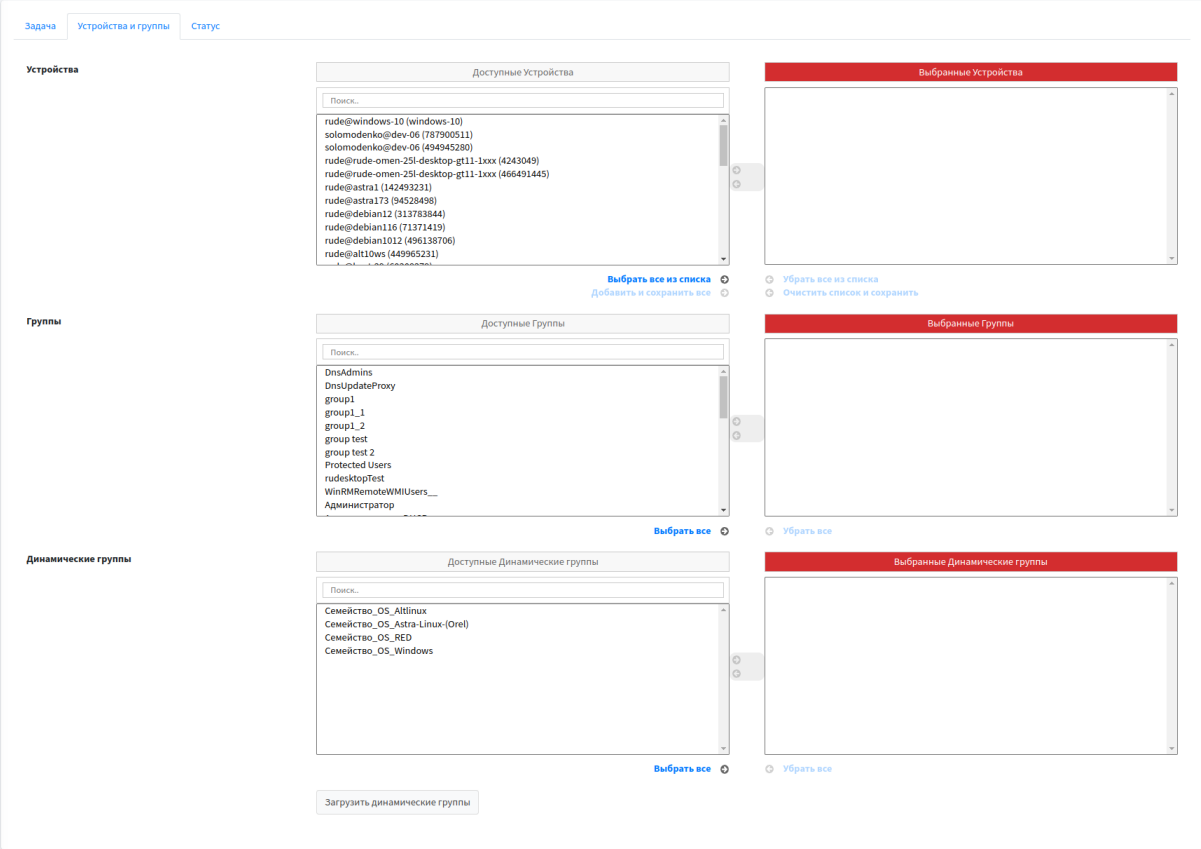
Поля Отчеты и Форматы отчета доступны только при использовании локального сервера **Управление конфигурациями (UEM)**. Готовые файлы появляются в разделе *Готовые отчеты*

Подсказка

После завершения задачи сервер автоматически отправляет уведомление со статусом выполнения и ссылкой на сформированные отчёты. Каналы доставки (Email, Telegram), получатели и шаблоны сообщений настраиваются на странице *Организация → Уведомления*

Устройства и группы

Вкладка Устройства и группы предоставляет возможность задать выполнение политики для определённых групп и/или устройств и включает следующие элементы:



- `Устройства` — позволяет выбрать устройства для выполнения задачи
- `Группы` — позволяет выбрать группы для выполнения задачи
- `Динамические группы` — позволяет выбрать динамические группы для выполнения задачи, доступна загрузка динамических групп. Подробнее о *динамических группах*
- `Запускать на всех устройствах` — разрешает выполнение на всех устройствах, только если списки устройств, групп и динамических групп пусты

Важно

- У новой задачи флажок `Запускать на всех устройствах` выключен

- Для выполнения на части устройств заполнить списки устройств или групп
- Для выполнения на всех устройствах оставить три списка пустыми и включить флажок
- Если в списках уже есть выбранные объекты, флажок не расширяет область выполнения до всех устройств

Подсказка

Чтобы добавить записи из левого столбца в правый, можно дважды щелкнуть по записи или выделить её и нажать на кнопку

Кнопка Импорт в правом столбце позволяет дополнить выбор устройств, групп или динамических групп из файла. Форматы, правила сопоставления и порядок сохранения описаны в *Импорт записей в списки выбора*. Это импорт списка целей выполнения, а не импорт определений задач

Кроме поштучного выбора доступны массовые действия над всем списком:

- Добавить и сохранить все — добавляет в задачу сразу все доступные записи
- Очистить список и сохранить — убирает из задачи все выбранные записи

Важно

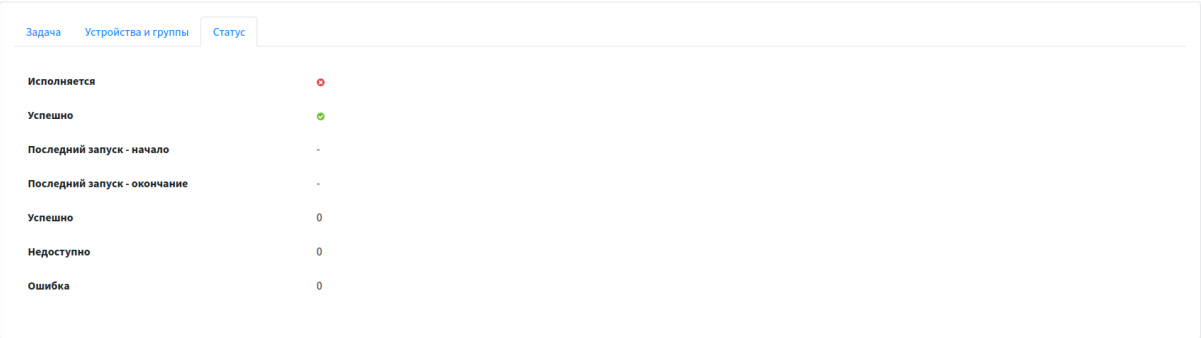
Массовые действия доступны только после сохранения задачи. Сохраните запись, чтобы добавить или удалить все элементы

Примечание

При большом количестве записей массовое действие выполняется **в фоновом режиме**: отображается индикатор прогресса («**Добавление записей**» / «**Удаление записей**») со счётчиком обработанных записей и процентом выполнения, а также кнопка Отменить задачу для прерывания операции. Пока фоновая задача выполняется, списки блокируются — перетаскивание, перемещение и прокрутка недоступны до её завершения

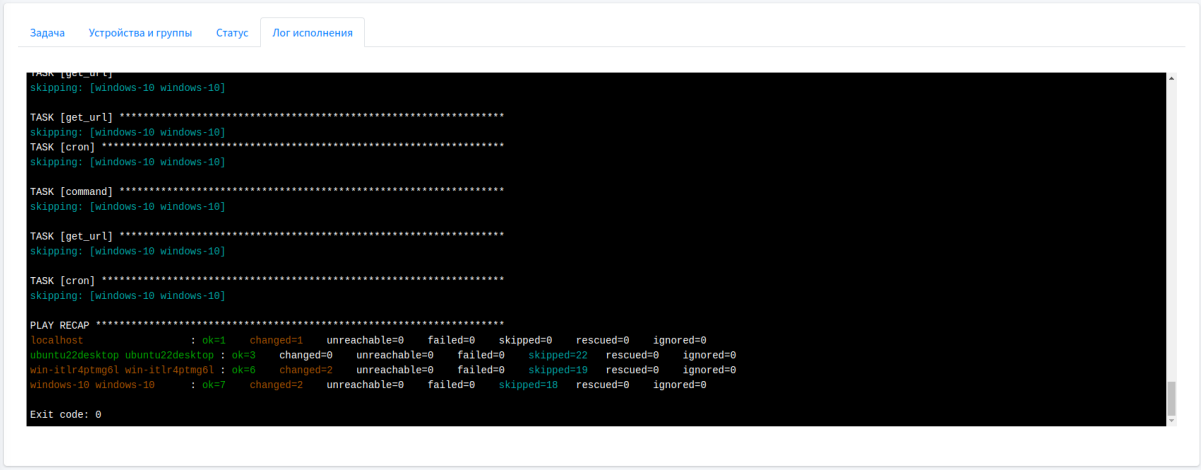
Статус

Вкладка Статус является информационной и отображает данные об успешности/неуспешности и времени выполнения задачи



Лог исполнения

Вкладка Лог исполнения является информационной и отображает лог выполнения задачи



Важно

Эта вкладка отобразится только после сохранения задачи

Примечание

- Если задача еще ни разу не была запущена, во вкладке **«Лог исполнения»** будет отображено сообщение: `Задача еще не запускалась`
- Логи Debug не отображаются во вкладке **«Лог исполнения»**

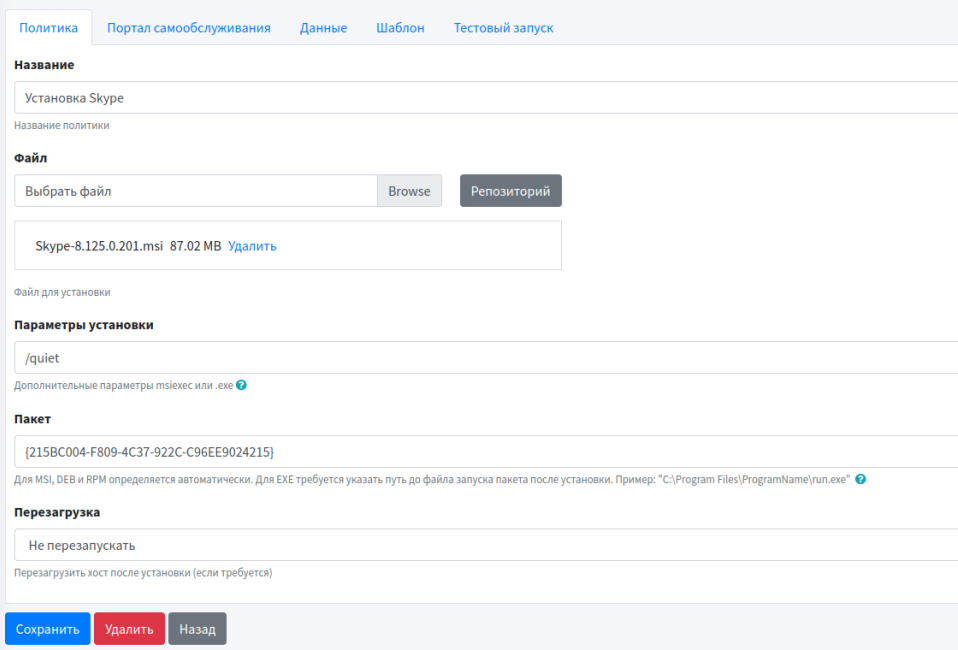
Пример

В качестве примера создадим задачу для автоматической подготовки рабочего места для сотрудника

Для этого нам понадобятся:

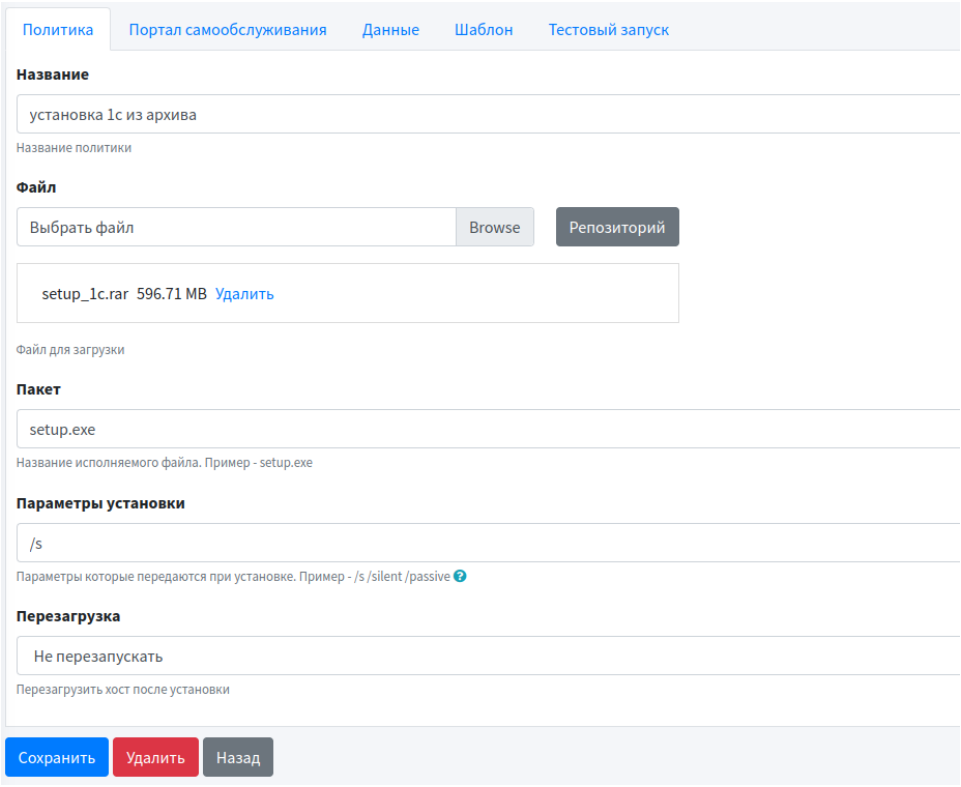
1. Созданные политики:
    1. Установка пакета — Установка Skype

        Пример настройки политики



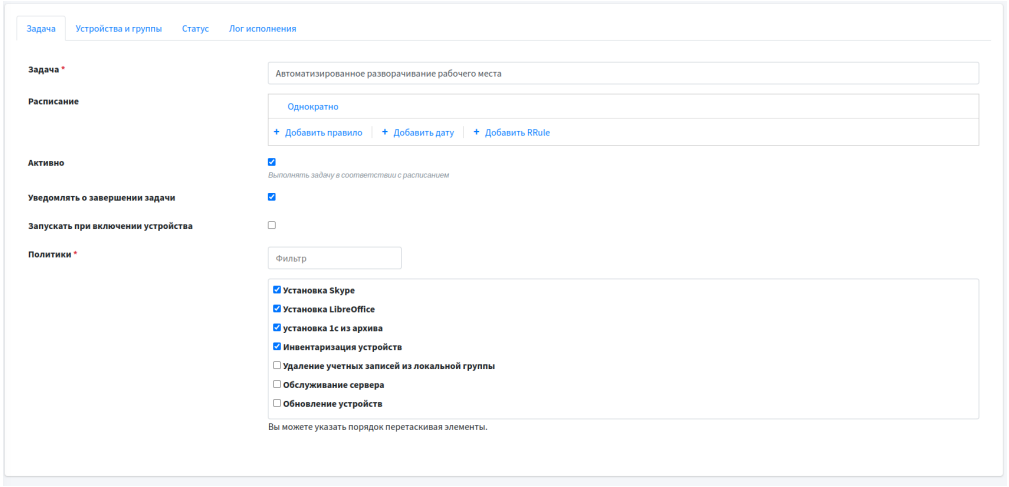
    2. Установка LibreOffice — настройка политики по умолчанию
    3. Установка Пакета из архива — Установка 1С

        Пример настройки политики



4. Инвентаризация — настройка политики по умолчанию

2. Создать задачу:



1. Задача — Автоматизированное разворачивание рабочего места
2. Расписание — Однократно
3. Активно — чекбокс активен
4. Запускать при включении устройства — чекбокс не активен
5. Политики — выбрать ранее созданные политики и выставить очередность

Подсказка

Политику **«Инвентаризация»** следует поставить последней, чтобы получить актуальную информацию по ресурсам после выполнения всех предыдущих политик

3. Во вкладке **«Устройства и группы»** в блоке `Устройства` выбрать необходимые устройства
4. Нажать на кнопку Сохранить или Сохранить и продолжить
5. Запустить выполнение задачи, нажав на кнопку Запустить в фоне или Запустить в терминале

Задачи — это набор политик с расширенными настройками для выполнения

Подсказка

Страница **«Задачи»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Как это работает

Задача объединяет одну или несколько *политик* в единый исполняемый блок и добавляет к ним:

- **расписание** — однократный запуск, по cron-выражению или периодически
- **область действия** — выбранные устройства, *группы* или *динамические группы*
- **приоритет** — порядок обработки в очереди, если запускается несколько задач параллельно
- **отчёты** — шаблоны *Отчётов*, которые автоматически формируются после завершения задачи (доступно только при UEM)
- **уведомления** — рассылка пользователю/администратору при завершении задачи со ссылкой на отчёт

Важно

На вкладке Устройства и группы выбрать область выполнения:

- **Отдельные устройства** — заполнить списки устройств, групп или динамических групп
- **Все устройства** — оставить эти списки пустыми и включить Запускать на всех устройствах

Подробности — в разделе *Создание задачи*

Примечание

В исходном порядке таблицы:

- Сначала показываются активные задачи, которые выполняются или ожидают запуска в очереди
- Затем — остальные задачи с учётом времени последнего запуска

При сортировке по заголовку столбца используется выбранный вами порядок

Жизненный цикл задачи:

1. **создаётся** вручную через Добавить Задачу или из обращения через *Портал самообслуживания*
2. **активируется** флагом Активно — без него задача не запускается по расписанию, даже если расписание задано
3. **ставится в очередь** — задача попадает в *очередь задач* и ждёт, когда освободится свободный поток для исполнения. В этот момент в столбце статуса отображается значение Запускается
4. **запускается** автоматически по расписанию, по событию выхода устройства на связь, вручную из контекстного меню или массовым действием Запустить выбранные задачи
5. **выполняется** на стороне сервера в фоновом режиме — статус и прогресс видны в таблице и на странице задачи
6. **завершается** со статусом Завершено или Ошибка. Логи и статистика доступны через действия Логи, График выполнения и Статистика выполнения, а уведомление о завершении уходит в выбранные каналы

Важно

Задача с активным расписанием продолжит запускаться, пока её не отключат флагом Активно или не удалят. Системные задачи (созданные из обращений в техподдержку) помечаются признаком Системная задача

Порядок выполнения политик

Если в задачу добавлено несколько политик, они выполняются **строго в том порядке, в котором добавлены**. Список политик внутри задачи можно сортировать — на странице создания или редактирования задачи политики перетаскиваются вверх и вниз, и сервер запустит их именно в этом порядке

Подсказка

Порядок важен для составных сценариев. Например, в паре Установка пакета → Перезагрузка установка должна идти первой, иначе устройство перезагрузится до установки. Аналогично для пары Обновление пакета → Инвентаризация — чтобы инвентаризация собрала уже обновлённый список ПО

Важно

Этот порядок относится только к политикам **внутри одной задачи**. Между разными задачами очерёдность определяется полем Приоритет и временем постановки задачи в очередь

Запуск при включении устройства

Помимо запуска по расписанию, задачу можно запускать в момент, когда устройство выходит на связь с сервером. Для этого в свойствах задачи активируется флаг Запускать при включении устройства

Когда устройство появляется онлайн, сервер автоматически подбирает все активные задачи с этим флагом, в область действия которых попадает данное устройство (через Устройства, Группы, Динамические группы или с пустой областью — на «всех»), и ставит их в очередь на выполнение

Примечание

Это основной способ применить политики к устройствам, которые были выключены в момент срабатывания расписания: как только устройство появится онлайн, нужные задачи отработают на нём автоматически

Подсказка

Запускать при включении устройства и расписание работают независимо и могут использоваться вместе. Если у задачи нет расписания, но активирован этот флаг, задача будет запускаться **только** при подключении устройства. Если нет ни флага, ни расписания, задача автоматически запускаться не будет — её придётся запускать вручную (см. *Запуск без расписания*)

Таймаут выполнения

Максимальное время выполнения задачи задаётся **глобально для всего сервера**, а не у каждой задачи. Значение настраивается в разделе *Администрирование → Настройки*, блок Настройки Ansible, поле Таймаут выполнения задачи. Значение по умолчанию — `300` секунд (5 минут)

Если задача выполняется дольше указанного времени, сервер принудительно

прерывает её и помечает запуск как неудачный — итоговый статус становится Ошибка

Важно

Таймаут общий для всех задач: его нельзя переопределить под конкретную задачу. Если в системе есть длительные операции (установка крупных пакетов, обслуживание сервера, копирование больших файлов), убедитесь, что глобальное значение достаточно большое — иначе они будут стабильно прерываться по таймауту

Приоритет задачи

Поле Приоритет определяет, в каком порядке сервер берёт задачи из очереди на выполнение, если одновременно ждут несколько задач. Чем выше приоритет, тем раньше задача будет запущена

Доступные значения:

- Критический приоритет — выполняется раньше прочих
- Высокий приоритет
- Средний приоритет
- Низкий приоритет — значение по умолчанию

Отдельно используется служебное значение Вне очереди, недоступное в свойствах задачи. Оно автоматически проставляется при ручном запуске задачи — через Запустить в фоне, Запустить в терминале или массовое действие Запустить выбранные задачи. Такие запуски проходят впереди любых задач из очереди — поэтому ручной запуск стартует немедленно, независимо от настроенного приоритета

Примечание

Приоритет влияет только на **порядок** запуска задач из очереди, а не на то, сколько задач может выполняться одновременно. Параллельность определяется числом потоков, заданных на странице *Точки распространения* в поле Потоки

Статус «Завершено» и «Ошибка»

В конце выполнения сервер выставляет итоговый статус по результатам каждого устройства из области действия. Для текущего запуска ведётся три счётчика:

- Успешно — число устройств, на которых задача выполнилась без ошибок
- Ошибка — число устройств, на которых выполнение завершилось ошибкой
- Недоступно — число устройств, до которых сервер не смог достучаться

Задача переводится в статус Ошибка, если выполняется хотя бы одно из условий:

- сам процесс выполнения был прерван (например, по таймауту, остановкой вручную или внутренней ошибкой);
- ни на одном устройстве задача не отработала успешно (Успешно равно нулю);
- хотя бы на одном устройстве выполнение завершилось ошибкой (Ошибка больше нуля);
- хотя бы одно устройство в области действия было недоступно (Недоступно больше нуля).

В остальных случаях задача получает статус Завершено. Это означает, что один недоступный или упавший хост в области действия приводит к итоговому статусу Ошибка у всей задачи — даже если часть устройств отработала корректно

Подсказка

Чтобы посмотреть, какие именно устройства попали в Ошибка или Недоступно, перейдите по действию Статистика выполнения — там видно результат по каждому устройству. Полные логи каждого исполнения доступны на странице *Логи исполнения*

Счётчики выполнения

В карточке задачи хранятся текущие значения трёх счётчиков — Успешно, Ошибка, Недоступно. Их поведение:

- при каждом новом запуске счётчики **сбрасываются в ноль** и накапливаются по мере того, как устройства возвращают результат;
- значения относятся к **последнему** запуску задачи и перезаписываются при следующем;
- по этим счётчикам формируется столбец Прогресс выполнения, итоговый статус задачи и тело уведомления о завершении

Уведомления о завершении

После завершения задачи сервер отправляет уведомление пользователю или администратору. В уведомление подставляются:

- название задачи;
- финальный прогресс выполнения (та же строка `XX.XX% (N/M)`, что отображается в столбце Прогресс выполнения);
- ссылка на сформированный отчёт, если в задаче настроены шаблоны *Отчётов*.

Какие события рассылаются, по каким каналам (электронная почта, Telegram и т.д.) и кому именно — настраивается на странице *Организация → Уведомления*. Там же указываются получатели и используемые шаблоны

Запуск без расписания

Если у задачи не задано расписание и **не активирован** флаг Запускать при включении устройства, она никогда не запустится сама. Столбец Следующий запуск для такой задачи остаётся пустым

Запустить её можно только вручную:

- из контекстного меню задачи действиями Запустить в фоне или Запустить в терминале;
- массовым действием Запустить выбранные задачи;
- автоматически — как часть обработки обращения через *Портал самообслуживания*.

Подсказка

Это нормальный сценарий для одноразовых задач — например, разовой установки ПО на конкретное устройство или ручного перезапуска службы. Для ручного запуска флаг Активно тоже не обязателен: задачу можно запустить из контекстного меню или массового действия, даже если она отключена

Прогресс выполнения

В столбце Прогресс выполнения для каждой задачи отображается строка вида `XX.XX% (N/M)`:

- **M** — общее число устройств, на которых задача должна отработать в текущем запуске (определяется областью действия — выбранными устройствами, группами и динамическими группами)
- **N** — число устройств, на которых задача уже **успешно завершилась** в текущем запуске (без ошибок и без недоступных хостов)
- **XX.XX%** — соотношение `N / M`, округлённое до двух знаков после запятой

Важно

В числителе учитываются **только успешные** результаты. Если устройство недоступно или выполнение завершилось ошибкой, такой результат **не попадает** в N — поэтому прогресс может не дойти до `100.00%`, даже когда задача уже завершилась. Итоговое распределение по статусам (успешно, ошибка, недоступно) удобно смотреть на страницах *Логи исполнения* и *Статистика выполнения*

Примечание

Прогресс считается относительно **последнего** запуска задачи и сбрасывается при каждом новом запуске. Пока задача ни разу не запускалась — в столбце отображается прочерк -. Значение обновляется автоматически по мере того, как устройства возвращают результат — отдельно перезагружать страницу не нужно

Примечание

По умолчанию имеются предустановленные задачи:

- Инвентаризация
- Обслуживание сервера

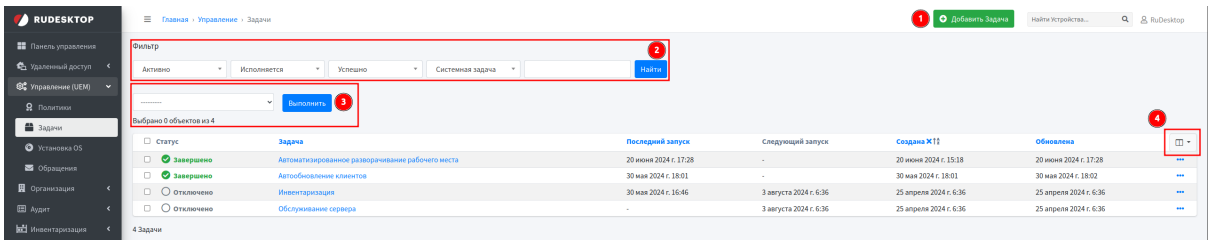
Подсказка

Данная задача включает следующие политики:
- Обслуживание сервера
- Обновление устройств

1. Предустановленные задачи можно удалить и редактировать
2. Предустановленные задачи по умолчанию отключены, но их можно активировать и настроить расписание

Описание страницы

На странице **Задачи** отображается:



1. Кнопка Добавить Задачу
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление задачи

При нажатии на кнопку Добавить Задачу откроется страница создания задачи, подробнее о *создании задачи*

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. `Активно` — фильтрация задач по статусу активности
2. `Исполняется` — фильтрация задач по статусу исполнения
3. `Успешно` — фильтрация задач по статусу успеха
4. `Системная задача` — фильтрация пользовательских и системных задач (Системные задачи создаются через обращение в техподдержку на выполнение политик)
5. `Поле поиска` — поиск по ключевому слову

Примечание

Системные задачи попадают на страницу только при включённой настройке Показывать системные задачи в блоке *Настройки Ansible*

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Массовые действия позволяют выполнить одну и ту же операцию сразу над несколькими задачами, не открывая свойства каждой из них

Панель массовых действий появляется под таблицей, как только отмечена хотя бы одна задача. Общий порядок работы одинаков для всех действий:

1. Отметить необходимые задачи в таблице
2. Выбрать действие в списке Действия с выбранными объектами
3. Заполнить дополнительные поля, если действие их запрашивает (формат файла) — пока обязательное поле не заполнено, кнопка Выполнить неактивна
4. Нажать на кнопку Выполнить

Важно

В панели есть кнопка Выбрать все. Она распространяет действие на **всю текущую выборку** — на все задачи, отобранные фильтром и поиском, а не только на отмеченные на текущей странице. Рядом отображается счётчик Выбрано N из M или Выбраны все объекты, сбросить выбор можно кнопкой Снять выделение

Что делает каждое действие:

Действие	Что делает
Удалить выбранные задачи	Удаляет записи о задачах с сервера. Политики, входившие в задачу, не удаляются
Включить выбранные задачи	Включает у задач параметр Выполнять задачу в соответствии с расписанием, после чего они снова запускаются по расписанию
Отключить выбранные задачи	Выключает этот параметр: задачи перестают запускаться по расписанию. Уже выполняющаяся задача при этом не прерывается
Запустить выбранные задачи	Ставит задачи в очередь на немедленное выполнение с наивысшим приоритетом Вне очереди, независимо от расписания
Остановить выбранные задачи	Прерывает выполнение задач и убирает их из очереди. Расписание при этом сохраняется, и по нему задача запустится снова
Экспортировать выбранные задачи	Выгружает в файл список названий выбранных задач

Важно

1. Действия Включить, Отключить и Запустить требуют права *Может запускать политики* — одного права **Политики → Изменение** для них недостаточно
2. Действие Остановить выбранные задачи требует права **Политики → Изменение**
3. Действие Удалить выбранные задачи требует права **Политики → Удаление**
4. Действие Экспортировать выбранные задачи требует права **Может экспортировать данные**
5. В зависимости от прав действия могут отсутствовать

Примечание

Пары действий легко перепутать: Отключить влияет только на будущие запуски по расписанию и не трогает текущее выполнение, а Остановить прерывает текущее выполнение, но не отменяет расписание. Чтобы задача и остановилась сейчас, и не запустилась снова, нужно применить оба действия

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление задач

Для массового удаления задач необходимо:

1. Отметить необходимые задачи в таблице
2. Выбрать действие Удалить выбранные задачи
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие задачи будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные задачи будут удалены

Важно

Вид страницы подтверждения и способ удаления зависят от количества выбранных задач:

- **до 100 задач включительно** — на странице подтверждения перечисляются сами задачи и связанные с ними записи, удаление выполняется сразу
- **более 100 задач** — на странице подтверждения отображается только количество удаляемых записей. Удаление ставится в очередь и выполняется в фоне: появляется сообщение вида **«Удаление N задач в процессе...»**, а записи исчезают из таблицы не сразу. Ход выполнения виден на странице *Очередь задач* по задаче **«Удаление данных»**

Примечание

Политики, входившие в удалённые задачи, остаются на странице *Политики*. Записи о прошлых запусках на странице *Логи исполнения* также сохраняются — у них лишь снимается привязка к удалённой задаче

Включение задач

Для массового включения задач необходимо:

1. Отметить необходимые задачи в таблице
2. Выбрать действие Включить выбранные задачи
3. Нажать на кнопку Выполнить
4. Выбранные задачи будут включены

Примечание

После выполнения данного действия появится уведомление о том, что задача включена, и статус в таблице изменится на

Отключение задач

Для массового отключения задач необходимо:

1. Отметить необходимые задачи в таблице
2. Выбрать действие Отключить выбранные задачи
3. Нажать на кнопку Выполнить
4. Выбранные задачи будут отключены

Примечание

После выполнения данного действия появится уведомление о том, что задача отключена, и статус в таблице изменится на

Важно

1. Задача с установленным расписанием не будет выполняться, пока ее не активировать
2. Отключение не прерывает выполнение: если задача уже запущена, она доработает до конца. Чтобы прервать её, используйте действие Остановить выбранные задачи
3. Отключение не мешает ручному запуску — действие Запустить выбранные задачи выполнит и отключённую задачу

Запуск задач

Для массового запуска задач необходимо:

1. Отметить необходимые задачи в таблице
2. Выбрать действие Запустить выбранные задачи
3. Нажать на кнопку Выполнить
4. Выбранные задачи будут запущены в фоне

Примечание

После выполнения данного действия статус в таблице изменится на . Запуск через это действие проходит Вне очереди — задачи стартуют немедленно, независимо от настроенного приоритета

Важно

Запуск через это действие принудительный, поэтому обычные ограничения на него не распространяются:

1. Задача запускается независимо от расписания и от параметра Выполнять задачу в соответствии с расписанием — **отключённые задачи тоже будут выполнены**
2. Задача запускается, даже если её предыдущее выполнение ещё не завершилось, — в результате один и тот же набор политик может выполняться на устройствах повторно
3. Дата в столбце Следующий запуск не сдвигается: ручной запуск не заменяет собой очередной запуск по расписанию

Остановка задач

Остановка учитывает и запуск, ещё ожидающий в очереди: такой запуск не должен начать выполнять политики после остановки. Новый ручной запуск или очередной запуск по расписанию снова разрешает выполнение задачи

Для массовой остановки задач необходимо:

1. Отметить необходимые задачи в таблице
2. Выбрать действие Остановить выбранные задачи
3. Нажать на кнопку Выполнить
4. Выбранные задачи будут остановлены

Важно

При остановке сервер прерывает все фоновые процессы этой задачи и снимает с неё признаки Исполняется и Ожидает исполнения. Если задача была активно запущена, она переводится в статус Ошибка, даже если часть устройств уже успела отработать; если задача только стояла в очереди и ещё не успела начать выполнение, её итоговый статус не меняется. Счётчики Успешно / Ошибка / Недоступно сохраняют значения на момент остановки и обнулятся только при следующем запуске

Примечание

При остановке задачи также удаляются ожидающие подзадачи этого запуска, чтобы они не продолжали занимать очередь. Уже выполненные изменения на устройствах не откатываются. Остановка текущего запуска не отключает расписание: чтобы запретить следующие автоматические запуски, снимите флаг Активно

Экспорт задач

Действие выгружает в файл перечень выбранных задач

Примечание

В файл попадает только **название** задачи — по одной строке на задачу. Расписание, приоритет, состав политик, область действия и статистика выполнения не выгружаются, а настройка отображаемых столбцов таблицы на состав файла не влияет

Для массового экспорта задач необходимо:

1. Отметить необходимые задачи в таблице
2. Выбрать действие Экспортировать выбранные задачи
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Важно

1. Доступные форматы выгрузки: **CSV**, **XLS**, **XLSX**, **TSV**, **ODS**, **JSON**, **YAML**, **HTML**. Набор форматов зависит от компонентов, установленных на сервере, поэтому отдельные пункты могут отсутствовать
2. Если выбрано более 1000 задач, экспорт выполняется в фоне: файл не скачивается сразу, а сохраняется на сервере в репозитории **Отчеты** и становится доступен на странице *Файлы*. Ход выполнения виден на странице *Очередь задач* по задаче **«Экспорт»**
3. Формат **XLS** не поддерживает ячейки с текстом длиннее 32767 символов — при таких значениях экспорт завершится ошибкой с предложением выбрать другой формат

Таблица

Таблица разбита по столбцам:

1. `Статус` — статус активности задачи
   - Новая задача — данный статус устанавливается у созданной задачи
   - Запускается — подготовка к выполнению задачи
   - Выполняется — задача находится в процессе выполнения
   - Завершено — успешное выполнение задачи
   - Ошибка — при выполнении задачи произошла ошибка
   - Отключено — у задачи отключена опция Активно (Выполнять задачу в соответствии с расписанием)

2. Задача — пользовательское название задачи
3. Приоритет — приоритет задачи в *очереди задач*: Критический, Высокий, Средний, Низкий или Вне очереди (выставляется автоматически для задач, запущенных вручную)
4. Прогресс выполнения — индикатор прогресса при выполнении задачи
5. Последний запуск — дата и время последнего запуска задачи
6. Следующий запуск — дата и время следующего запуска задачи по расписанию
7. Создана — дата и время создания задачи
8. Обновлена — дата и время последнего изменения задачи

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. Редактировать — при выборе этого пункта откроются свойства задачи
2. Удалить — при выборе этого пункта задача будет удалена
3. История изменений — при выборе этого пункта будет отображена история задачи: создание/редактирование и пользователь, который выполнил данные операции
4. Запустить в фоне — задача ставится в очередь со служебным приоритетом Вне очереди и выполняется на сервере без участия пользователя. Веб-интерфейс при этом не блокируется — за прогрессом и итогом нужно следить через столбцы Статус и Прогресс выполнения либо через действия Логи и Статистика выполнения. Подходит для регулярных и массовых запусков
5. Запустить в терминале — задача запускается так же, Вне очереди, но дополнительно открывается всплывающее окно терминала, в которое в реальном времени выводятся логи выполнения. В окне доступны кнопки Прервать (останавливает задачу так же, как действие Остановить) и Закрыть. Подходит для отладки одиночных запусков, когда нужен живой вывод
6. Логи — при выборе этого пункта произойдет переход на страницу *Логи исполнения* с активным фильтром по этой задаче
7. График выполнения — при выборе этого пункта произойдет переход на страницу *График выполнения* с визуализацией длительности и количества выполнений задачи
8. Статистика выполнения — при выборе этого пункта произойдет переход на страницу *Статистика выполнения* с отображением статусов выполнения задачи по каждому устройству

2.7.3 Обращения

Доступны в УД и UEM версиях

Обращения — это задачи, поступающие с удалённых устройств через портал самообслуживания. Обращения могут также включать запросы на выполнение политик

Подсказка

Страница **«Обращения»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Важно

При запросе на выполнение политик на основе уже готовых политик создаётся задача для выполнения на устройстве. Подробнее *о задачах* и *портале самообслуживания*

Подсказка

Задачи, созданные на основе запрошенных для выполнения политик, на странице **«Задачи»** получают статус Системная задача

Как это работает

Обращение создаётся пользователем удалённого устройства через клиентское приложение **RuDesktop** (раздел *Портал самообслуживания*). У обращения два возможных типа:

- **Обращение в поддержку** — текстовая заявка для сотрудника поддержки или администратора
- **Запрос на выполнение политик** — пользователь выбирает одну или несколько *политик*, отмеченных флагом Показывать в разделе: «Портал самообслуживания»

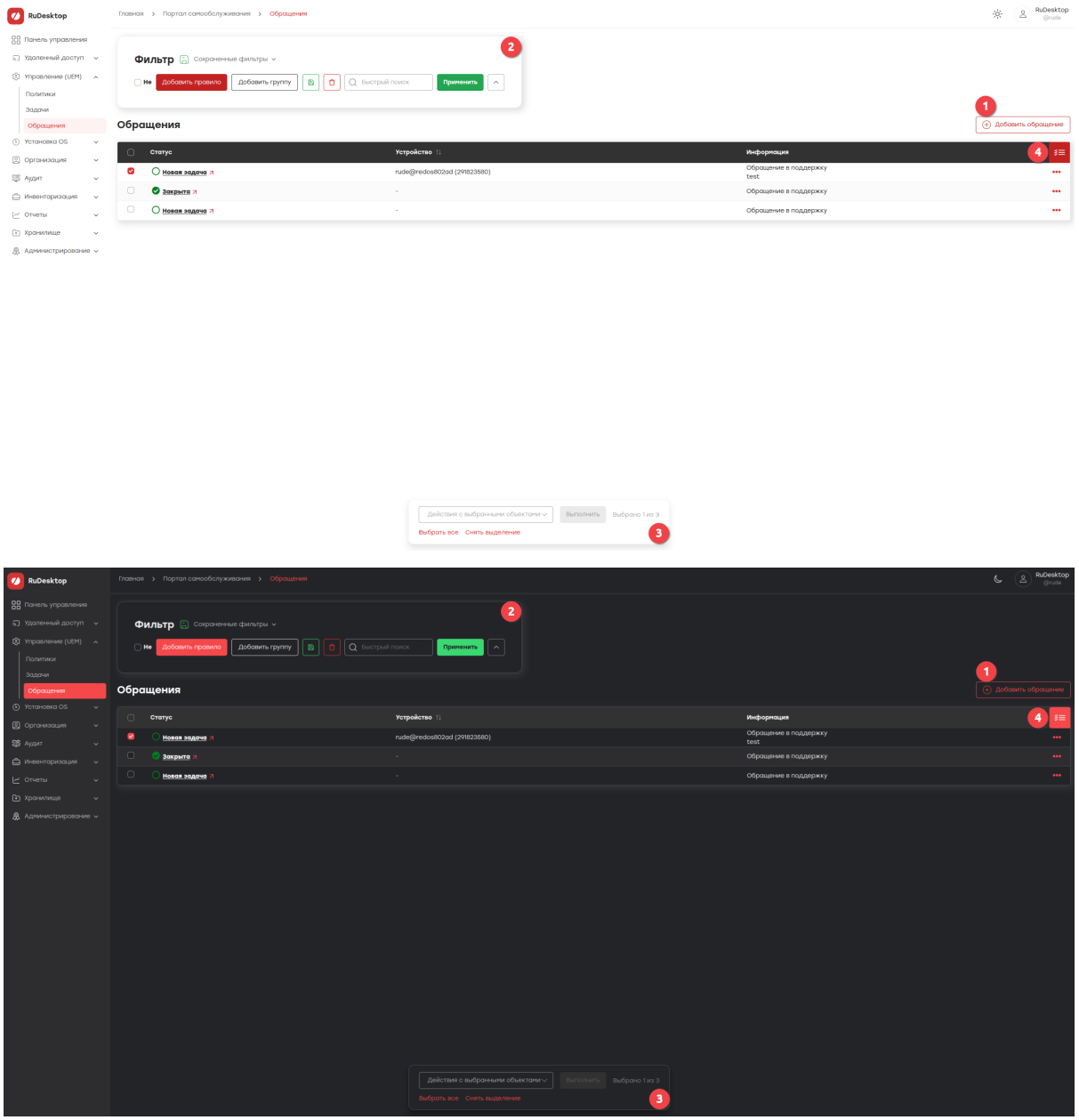
В зависимости от настроек политики и роли пользователя:

- если у политики включён флаг Автоматический запуск — задача создаётся и стартует сразу без участия администратора
- иначе обращение получает статус Открыт и ждёт, пока администратор не запустит задачу через действие Запустить задачи

Все задачи, созданные через обращения, отображаются на странице *Задачи* со специальным флагом Системная задача. Они проходят тот же цикл выполнения, что и обычные задачи. Цикл обращения: Открыт → Частично выполнены политики → Закрыт

Описание страницы

На странице **Обращения** отображено:



1. Кнопка Добавить обращение
2. Массовые действия
3. Таблица с возможностью настройки отображаемых столбцов

Добавление обращения

При нажатии на кнопку Добавить обращение откроется страница создания обращения

Массовые действия

Доступные действия:

1. Удалить выбранные обращения — удаление выбранных обращений

> **Важно**
>
> В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление обращений

Для массового удаления обращений необходимо:

1. Отметить необходимые обращения в таблице
2. Выбрать действие Удалить выбранные обращения
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие обращения будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные обращения будут удалены

Таблица

Таблица разбита по столбцам:

1. `Статус` — текущий статус обращения, есть 3 вида статусов:
   1. Новая задача — обращение, которое ещё не было взято в работу сотрудником поддержки или системным администратором, имеет статус Открыт
   2. Выполняется — обращение было принято в работу сотрудником поддержки или системным администратором, и такой запрос имеет статус Частично выполнены политики
   3. Закрыта — обращение было выполнено сотрудником поддержки или системным администратором; при таком обращении статус запроса в задаче изменяется на Закрыт
2. `Устройство` — имя устройства, с которого было отправлено обращение, отображается по маске **«имя_пользователя@имя_устройства»**
3. `Информация` — содержит информацию об обращении, такую как:
   1. Текстовое обращение в поддержку или запрос на выполнение политик

2. Текст обращения
3. Политика, запрошенная для выполнения

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

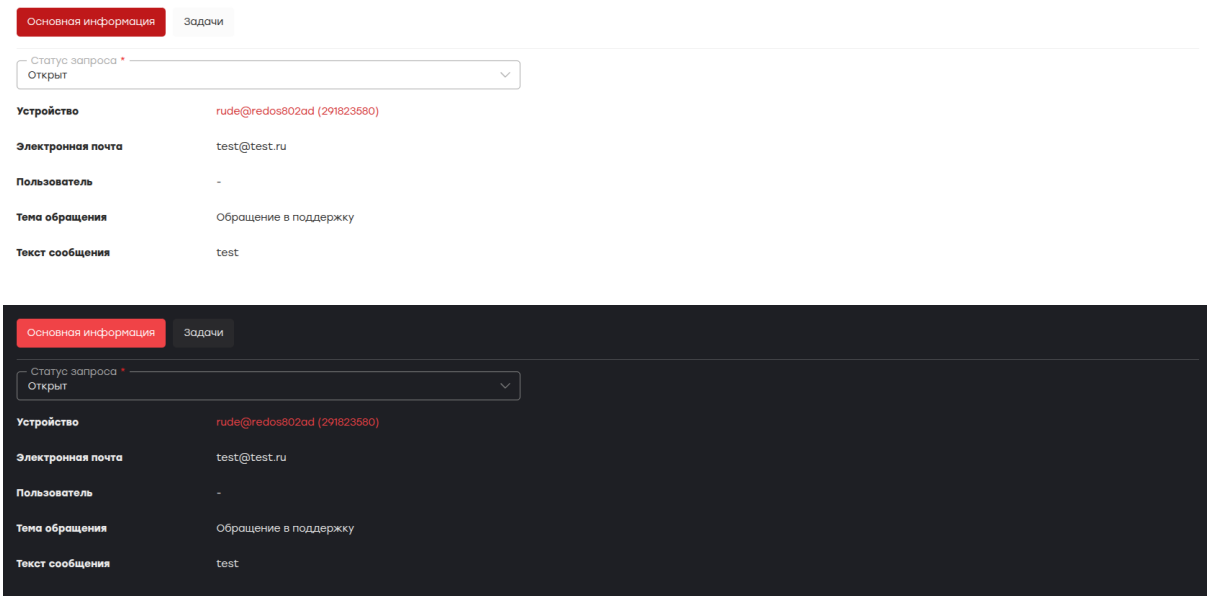
1. `Редактировать` — при выборе этого пункта откроются свойства обращения
2. `Удалить` — при выборе этого пункта обращение будет удалено
3. `История изменений` — при выборе этого пункта будет отображена история обращения: создание/редактирование и пользователь, который выполнил данные операции
4. `Запустить задачи` — при выборе этого пункта произойдёт запуск задачи на основе запрошенных для выполнения политик для удалённого устройства

Свойства обращения

Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств

Основная информация



1. Статус запроса — при открытии обращения отображается текущий статус обращения, после выполнения статус необходимо изменить

   Типы статусов:

   1. Открыт — обращение, которое ещё не было взято в работу

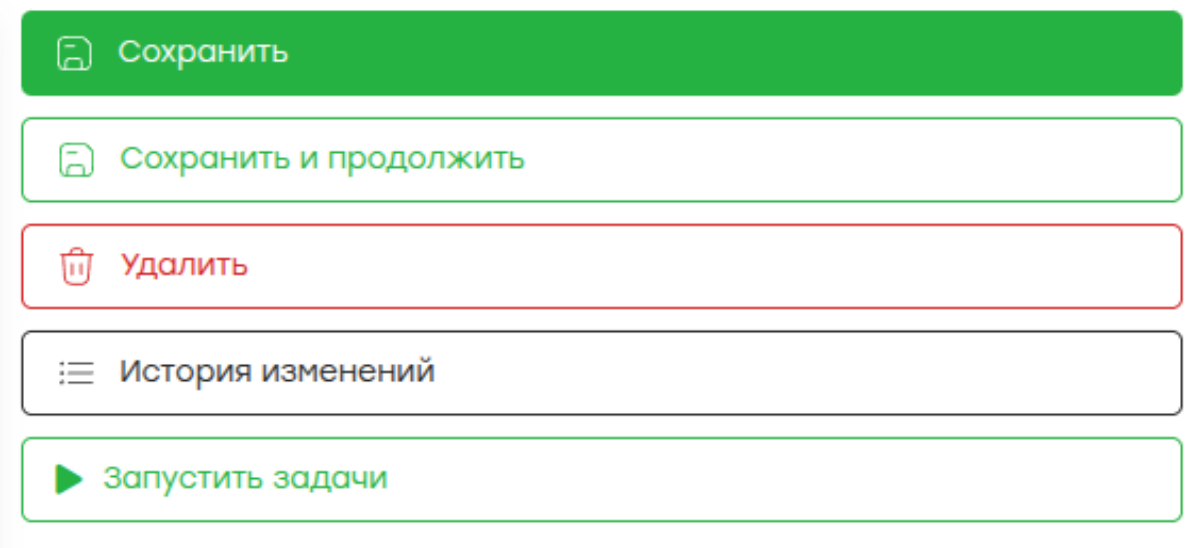
    2. Частично выполнены политики — обращение было принято в работу
    3. Закрыт — обращение было выполнено и закрыто
2. Устройство — имя устройства, с которого было отправлено обращение; отображается по маске **«имя_пользователя@имя_устройства»**
3. Электронная почта — электронная почта пользователя, сформировавшего обращение
4. Пользователь — имя пользователя, который сформировал обращение
5. Тема обращения — тип обращения: Обращение в поддержку или Запрос на выполнение политик
6. Текст сообщения — дополнительная информация, которая указывается при создании обращения

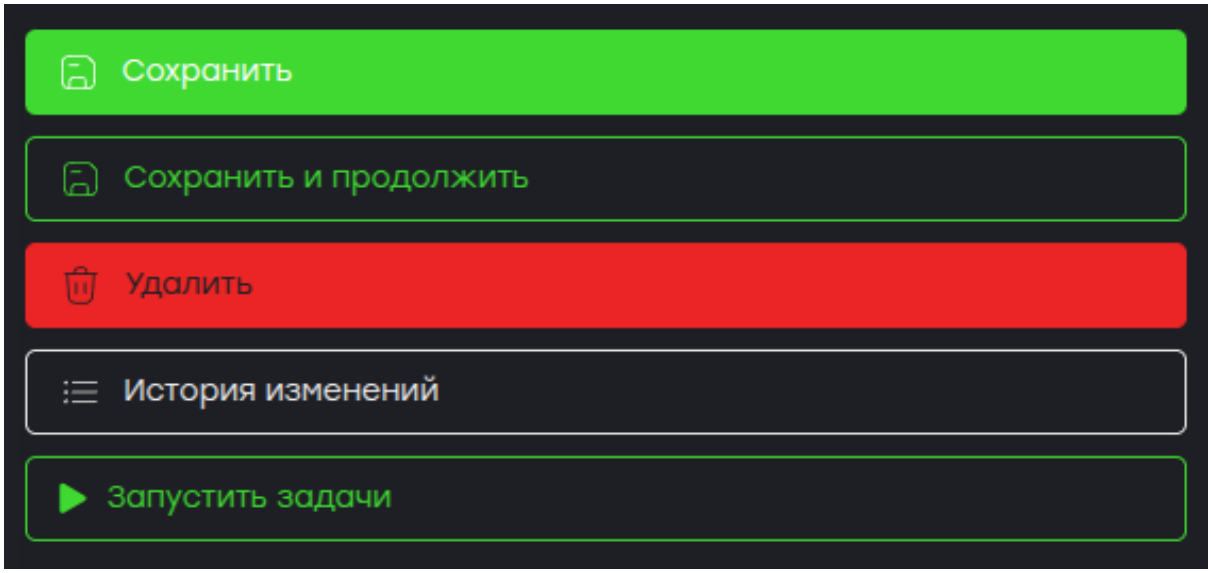
Задачи

Вкладка Задачи содержит ссылку на задачу, созданную на основе запрошенных для выполнения политик для удалённого устройства

Меню действий

Меню действий расположено на всех вкладках страницы редактирования





Имеет следующие возможности:

1. Сохранить — производит сохранение внесённых изменений и перенаправляет на страницу **«Обращения»**
2. Сохранить и продолжить — производит сохранение внесённых изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление обращения и перенаправляет на страницу **«Обращения»**

> **Примечание**
>
> 1. После нажатия на кнопку Удалить откроется страница подтверждения удаления обращения
> 2. После подтверждения удаления обращения произойдёт переход на страницу **«Обращения»** и появится уведомление Обращение «НАЗВАНИЕ_ОБРАЩЕНИЯ» было успешно удалено

4. История изменений — отображает все изменения, выполненные для этого обращения

2.7.4 Статистика выполнения

Доступна только в UEM версии

Статистика выполнения — это сводная таблица результатов выполнения задач: сколько устройств отработали успешно, у скольких задача внесла изменения и сколько устройств завершили задачу с ошибкой

Подсказка

Страница **«Статистика выполнения»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Важно

Страница не отображается в основном навигационном меню — открыть её можно только через действие Статистика выполнения в контекстном меню *Устройства*, *Задачи*, в дереве *Структура* или в свойствах устройства

Как это работает

В зависимости от того, откуда открыта страница, отображаются разные срезы данных:

- **Из контекстного меню задачи** (*Задачи*) — статистика этой задачи **по всем устройствам**, на которых она выполнялась. Каждая строка — одно устройство
- **Из контекстного меню устройства** (*Устройства*, *Структура*, свойства устройства) — статистика **всех задач**, которые выполнялись на этом устройстве. Каждая строка — одна задача

Числа в таблице — это количество шагов плейбука с соответствующим результатом. Каждое число кликабельно — переход открывает страницу *Логи исполнения* с активным фильтром по конкретной задаче, устройству, типу события и моменту запуска

Описание страницы

На странице **«Статистика выполнения»** отображено:

1. Поле поиска
2. Таблица с возможностью настройки отображаемых столбцов

Поиск

`Поле поиска` — поиск по ключевому слову

Подсказка

Поиск осуществляется по названию задачи

Для выполнения поиска необходимо заполнить поле и нажать на кнопку Найти

Таблица

Таблица разбита по столбцам:

В режиме **«статистика задачи по устройствам»** (открыта из контекстного меню задачи):

1. `Устройство` — устройство, на котором выполнялась задача (отображается по маске **«имя_пользователя@hostname»**). Цветовая отметка показывает итоговый статус: успех, изменения или ошибка
2. `Успешно` — количество шагов плейбука, завершившихся успешно. При нажатии открывает соответствующие записи в *Логах исполнения*
3. `Обновлено` — количество шагов плейбука, изменивших состояние устройства
4. `Ошибка` — количество шагов плейбука, завершившихся с ошибкой

В режиме **«статистика устройства по задачам»** (открыта из контекстного меню устройства):

1. `Название задачи` — задача, которая выполнялась на устройстве. Цветовая отметка показывает итоговый статус
2. `Успешно` — количество шагов плейбука, завершившихся успешно
3. `Обновлено` — количество шагов плейбука, изменивших состояние устройства
4. `Ошибка` — количество шагов плейбука, завершившихся с ошибкой

Примечание

Создавать или редактировать записи статистики вручную нельзя — таблица формируется автоматически по результатам выполнения задач

2.7.5 График выполнения

Доступен в УД и UEM версиях

График выполнения — это визуализация длительности и количества выполнений конкретной задачи по устройствам за последние **7 дней**

Подсказка

Страница **«График выполнения»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**. Доступ регулируется правом Может просматривать статистику

Важно

Страница не отображается в основном навигационном меню — открыть её можно через действие График выполнения в контекстном меню *Задачи*

Как это работает

Сервер **RuDesktop** анализирует журнал *Логов исполнения* за последние **7 дней**.

Для расчета используются записи, в которых заполнены время начала и время окончания выполнения

Описание страницы

На странице **«График выполнения»** отображено:

1. **Время выполнения задачи устройствами** — график средней длительности выполнения по минутным интервалам
   - Каждая линия соответствует устройству
   - На графике отображается не более десяти устройств
   - Обозначения линий расположены над графиком
2. **Количество запусков задачи и общее время выполнения по дням** — график с двумя осями:
   - Слева — показатель времени выполнения в секундах
   - Справа — количество запусков за день

   Дневные показатели учитывают все устройства

   Примечание

   Показатель времени основан на усредненных данных и может отличаться от суммы длительностей отдельных запусков

3. **Статус последнего выполнения задачи устройствами** — круговая диаграмма:
   - **Успешно** — количество устройств, у которых последний результат выполнения содержит успешные операции
   - **Ошибка** — количество устройств, у которых последний результат выполнения содержит ошибки

   Примечание

   Если последний результат содержит и успешные операции, и ошибки, устройство учитывается в обеих категориях

Примечание

- Если за последние 7 дней нет записей с заполненными временем начала и окончания, графики будут пустыми

- На круговой диаграмме учитывается только **последний** результат по каждому устройству; в графиках — все результаты за период
- Старые записи без времени окончания в расчет не попадают

Управление (UEM) — раздел для централизованного управления конфигурациями устройств: политики на основе **Ansible**, расписание их выполнения и обращения пользователей через портал самообслуживания

Подсказка

Раздел **«Управление (UEM)»** доступен при использовании локального сервера **Удаленный доступ** (с ограничениями) или **Управление конфигурациями (UEM)**

Примечание

Часть функциональности раздела доступна только при активной лицензии **UEM** — поля «Отчёты» и «Форматы отчётов» в *Задачах*, статистика и расширенные логи. Базовое создание политик и задач работает в обеих редакциях

Примечание

Удалённая установка ОС и миграция вынесены в отдельный раздел *Установка OS*

Политики

Операции на основе Ansible-плейбуков для выполнения на устройствах

Задачи

Расписание и группировка политик для выполнения

Обращения

Запросы пользователей через портал самообслуживания

Статистика выполнения

Сводка результатов выполнения задач по устройствам

График выполнения

График длительности и количества выполнений задачи

2.8 Сканирование сети

Сканирование сети - раздел веб-интерфейса для обнаружения устройств и установки на них клиента RuDesktop. Сканирование можно выполнять с сервера или через уже подключённое устройство - агент-исполнитель

2.8.1 Профили обнаружения

Профиль обнаружения определяет, где и каким способом искать устройства. В списке доступны поиск по названию и фильтры по типу профиля, признаку **«Включено»** и агенту-исполнителю

Создание профиля

1. Открыть **«Сканирование сети → Профили обнаружения»** и добавить профиль
2. Задать **«Название»** и выбрать **«Тип профиля»**
3. Заполнить **«Конфигурацию»** выбранного типа по описанию ниже
4. При необходимости выбрать **«Агент-исполнитель»** - подключённое устройство, из сети которого будет выполняться поиск

   Без него поиск выполняется с сервера

   Для Active Directory / LDAP используется только сервер
5. Для периодического поиска включить профиль и настроить вкладку **«Расписание»**
6. Сохранить профиль и выполнить **«Запустить сканирование»**
7. Проверить вкладку **«Лог сканирования»** и список *обнаруженных устройств*

Во время ручного запуска действие меняется на **«Остановить сканирование»**

Подсказка

Поле **«Включено»** управляет запуском по расписанию. Если нужен только разовый поиск, оставить профиль выключенным и запустить его вручную. Выключение профиля не удаляет ранее найденные устройства

Примечание

Остановка прерывает текущий запуск, но не отменяет уже сохранённые результаты и не выключает расписание. Чтобы прекратить последующие автоматические запуски, отдельно снять **«Включено»** и сохранить профиль

IP-диапазон

Указать одну или несколько подсетей в формате CIDR, например `192.168.10.0/24`. Для IPv6 можно указать `fd00:100::/120`; размер IPv6-подсети ограничен префиксом /112 или более длинным

- **«Порты для проверки»** - по умолчанию 22, 80, 443 и 445

  Добавить порты служб, которые требуется обнаруживать, например 5985 и 5986 для WinRM

  Подсказка

  Каждый порт — целое число от 1 до 65535. Для нескольких портов добавить строки кнопкой **«Добавить»**

  Пустые строки не добавляют порт в список проверяемых

- **«Таймаут, мс»** - время ожидания ответа; по умолчанию 1500 мс
- **«Параллельных подключений»** - по умолчанию 64, допустимо от 1 до 1024
- **«ICMP-опрос (ping)»** - дополнительная проверка доступности

  Если у исполнителя нет прав на ICMP-опрос, этот шаг пропускается

- **«Учитывать ARP/NDP-соседей»** - учитывать устройства с MAC-адресом в таблице соседей после опроса

  Это действует только в подсети исполнителя

Устройство попадает в результаты, если найден открытый проверяемый порт, получен ответ ICMP или обнаружен MAC-адрес в таблице соседей при включённом учёте ARP/NDP. Поэтому запись может появиться с пустым списком открытых портов. Это ещё не означает, что на неё можно установить клиент: для установки потребуется доступный транспорт и подходящие учётные данные

Active Directory / LDAP

Выбрать **«AD-домен»**, ранее настроенный в разделе *Домены*, и отметить **«Контейнеры / OU для сканирования»**. Поиск проходит по выбранным контейнерам вместе с их вложенными объектами. Если контейнеры не выбраны, используются области поиска, заданные в настройках домена. Для проверки доступности по умолчанию используются порты 445, 5985, 5986 и 22

Настроить **«Таймаут проверки порта, мс»**, если сеть требует большего времени ожидания

Важно

Этот способ выполняется на сервере

Поле **«Агент-исполнитель»** должно оставаться пустым

Серверу нужны доступ к настроенному домену и разрешение имён его компьютеров

NetBIOS / SMB broadcast

Указать **«Подсети для broadcast»** в формате IPv4 CIDR, **«Рабочая группа / домен»** и **«Таймаут, мс»**. Начальные значения - `WORKGROUP` и 2000 мс. Выбрать исполнителя в сети, в которой требуется обнаруживать устройства этим способом. Поле **«Рабочая группа / домен»** фильтрует результаты по имени группы без учёта регистра. Если нужны устройства всех групп, очистить поле

Начальное значение `WORKGROUP` может исключить компьютеры другого домена

Zeroconf / mDNS

- **«Типы сервисов»** - например `_workstation._tcp.local.`
- **«Сетевой интерфейс»** - имя интерфейса или IP-адрес; пустое значение означает прослушивание всех интерфейсов
- **«Время прослушивания, сек»** - по умолчанию 30 секунд, от 1 до 600

Профиль обнаруживает устройства по объявлениям выбранных сервисов

Если устройство не найдено

Проверить область поиска и доступность нужной сети именно с выбранного исполнителя. Для IP-профиля проверить порты и время ожидания; для AD - настройки домена, выбранные OU и разрешение имён; для mDNS - интерфейс и типы сервисов. Подробности выполнения доступны в **«Логе сканирования»**

Примечание

Журнал профиля показывает последний запуск и заменяется при новом сканировании. Нужные подробности ошибки следует сохранить до повторного запуска

2.8.2 Обнаруженные устройства

Обнаруженные устройства - результаты поиска из профилей сканирования. В списке отображаются IP-адрес, имя хоста, MAC-адрес, состояние, ссылка на управляемое устройство и время последнего обнаружения. Доступны поиск по IP, MAC, имени хоста и домену, а также фильтры по состоянию и ОС

Как это работает

Повторное обнаружение обновляет сведения об устройстве. В его карточке можно посмотреть домен, определённую ОС, открытые порты и время первого и последнего обнаружения. Полнота этих сведений зависит от способа поиска и ответов устройства

При редактировании карточки указывать:

- **IP-адрес** — адрес одного устройства, например `192.168.10.25` или `fd00:100::25`, без префикса подсети
- **MAC-адрес** — шесть пар цифр или букв от `a` до `f`, например `aa:bb:cc:dd:ee:ff`

> **Подсказка**
>
> Буквы приводятся к нижнему регистру, дефисы заменяются двоеточиями. Если адрес неизвестен, поле можно оставить пустым

- **Открытые порты** — целые числа от 1 до 65535 через запятую, например `22, 80, 443`

> **Подсказка**
>
> Если сведений о портах нет, поле можно оставить пустым

Состояния

- **«Новое»** - обнаруженная запись, ещё не переведённая в другое состояние
- **«Игнорируется»** - устройство исключено из автоматического отбора на установку
- **«Недоступно»** - отметка недоступного устройства; актуальный результат подключения следует проверить в журнале установки
- **«Управляемое»** - запись связана с устройством RuDesktop

Ссылка **«Управляемое устройство»** открывает его карточку

> **Примечание**
>
> Наличие записи в результатах сканирования само по себе не подтверждает доступность клиента для подключения прямо сейчас; проверяйте также время последнего обнаружения

Установка клиента на одно устройство

1. Подготовить *учётные данные* для подключения к устройству
2. В строке устройства выбрать **«Запустить установку»**
3. В окне **«Установка агента»** выбрать тип клиента и учётные данные

   Настройки можно подставить из существующего правила
4. Выбрать способ выполнения: автоматический выбор исполнителя, прямое подключение с сервера или конкретный агент-исполнитель

5. Запустить установку и открыть **«Лог установки»** в карточке устройства
6. Проверить результат в разделе **«Попытки установки»** и наличие связи с управляемым устройством

При автоматическом выборе используется агент, через которого устройство было обнаружено в последний раз среди наблюдений с агентом. Если таких наблюдений нет, выполняется прямое подключение с сервера

Важно

Этот выбор не проверяет текущую доступность агента: если он отключён, выбрать другого исполнителя или **«Напрямую с сервера»**, если серверу доступно устройство

Во время ручного запуска доступно действие **«Остановить установку»**

Примечание

Ручная установка из карточки использует выбранные в окне параметры

Условия отбора, расписание и признак **«Применять однократно»** правила на неё не распространяются

Подстановка из правила переносит тип клиента и учётные данные

Чтобы исключить устройство из правил авто-установки, открыть его карточку, выбрать состояние **«Игнорируется»** и сохранить. Ручной запуск установки из строки устройства остаётся отдельным действием и не использует этот автоматический отбор

Проверка результата

В **«Попытках установки»** доступны состояние, устройство, правило, учётные данные, агент-исполнитель и время выполнения. Возможные состояния: **«В очереди»**, **«Выполняется»**, **«Успех»**, **«Ошибка»**, **«Недоступно»**. Для ручной установки без правила соответствующее поле может быть пустым

Примечание

«Успех» означает завершение установки без зафиксированной ошибки и получение ID клиента. Привязка к **«Управляемому устройству»** требует, чтобы клиент зарегистрировался на сервере. Если попытка успешна, но ссылки нет, проверить адрес сервера в клиенте, связь с сервером и появление устройства в разделе **«Удалённый доступ → Устройства»**. Успешная попытка сама по себе не подтверждает, что устройство сейчас онлайн

При ошибке проверить журнал, выбранный транспорт, права учётной записи и доступность устройства с исполнителя. Затем повторить запуск. Для установки на несколько устройств использовать *правила авто-установки*

2.8.3 Учётные данные обнаружения

Учётные данные обнаружения задают способ подключения к найденному устройству для установки клиента. Для поиска через Active Directory используются настройки выбранного домена; наборы на этой странице нужны для последующей установки

Создание набора

1. Открыть **«Сканирование сети → Учётные данные обнаружения»** и добавить запись
2. Указать **«Название»**, **«Транспорт»**, **«Аутентификация»** и **«Пользователь»**
3. Заполнить поля выбранного метода

   Список методов зависит от транспорта
4. При необходимости указать **«Порт»** вместо стандартного порта транспорта
5. Сохранить запись и выбрать её при ручной установке или в правиле автоустановки

Транспорты и методы

Транспорт	Доступные методы аутентификации
SSH	Пароль, SSH-ключ, Kerberos, сертификат
WinRM / PSRP	Пароль, Kerberos, NTLM pass-the-hash, CredSSP, сертификат
SMBExec	Пароль, Kerberos, NTLM pass-the-hash

- **SSH** — при необходимости включить **«Повышение прав»** и заполнить метод, пользователя и пароль повышения прав. Учётная запись должна позволять установить клиент на целевой ОС
- **WinRM / PSRP** — выбрать **«Протокол»**: HTTP или HTTPS. Параметр **«Не проверять TLS»** управляет проверкой сертификата целевого устройства

Если поле **«Порт»** пустое, используются SSH - 22, SMBExec - 445, WinRM / PSRP - 5985 для HTTP или 5986 для HTTPS

Подсказка

Если порт указан вручную, допустимо целое число от 1 до 65535

В этом поле задаётся один порт подключения

Примечание

Порты профиля сканирования и порт учётных данных задаются независимо: первый список нужен для поиска, второй - для подключения при установке

Поля аутентификации

- **Пароль / CredSSP** - пароль выбранной учётной записи
- **SSH-ключ** - файл приватного ключа PEM и пароль ключа, если он зашифрован
- **Kerberos** - домен / realm и пароль либо keytab-файл

  Можно задать **«KDC / контроллер домена»**; при пустом поле KDC ищется через DNS
- **NTLM pass-the-hash** - NT-хеш либо значение в формате LM:NT
- **Сертификат** - сертификат для выбранного транспорта и файл его приватного ключа; при необходимости - пароль ключа

  Для SSH используется SSH-сертификат, для WinRM / PSRP - клиентский сертификат PEM и HTTPS

Файлы ключей и сертификатов выбираются через файловый виджет. Требуемые поля показываются после выбора транспорта и метода аутентификации

Примечание

При редактировании сохранённого набора секретные значения не отображаются

Чтобы сохранить прежний пароль или другой секрет при неизменном методе, оставить соответствующее поле пустым

2.8.4 Правила авто-установки

Правило авто-установки отбирает обнаруженные устройства по условиям и устанавливает на них выбранный тип клиента RuDesktop

Создание правила

1. Открыть **«Сканирование сети → Правила авто-установки»** и добавить правило
2. На время проверки снять **«Включено»**, чтобы правило не запускалось по расписанию

   Ручной запуск остаётся доступен
3. Указать **«Название»** и **«Профили обнаружения»**, к результатам которых оно применяется

Пустой список профилей означает все профили

4. Задать **«Условия»**: например, IP-адрес в нужной подсети и выбранная ОС

   Доступны также имя хоста, домен, MAC, открытые порты, состояние и вид профиля

5. Выбрать **«Тип клиента»**: **«Полный клиент»** или **«Без интерфейса (headless)»**
6. Добавить *учётные данные* и задать порядок их перебора
7. Настроить параметры исполнения и ограничить условия одним тестовым устройством
8. Сохранить правило, выполнить **«Запустить установку»** и проверить **«Лог установки»**

   После успешной проверки расширить условия отбора

9. Для повторных запусков включить правило и настроить **«Расписание»**

Важно

Пустые условия соответствуют всем обнаруженным устройствам в выбранных профилях

Перед запуском проверить область отбора

В текущей beta3.1 параметр **«Только сопоставление (dry-run)»** не гарантирует запуск без установки клиента

Пробную установку выполнять только на специально выбранном тестовом устройстве

Параметры исполнения

- **«Приоритет»** - порядок отображения правил: меньшие значения идут раньше

  Каждое правило запускается отдельно; поле не задаёт последовательную цепочку выполнения нескольких правил

- **«Не обновлять пакеты (Linux)»** - отключить обновление пакетов Linux при установке клиента
- **«Агент-исполнитель (явно)»** - устройство, через которое выполняется установка

  Если поле пустое, исполнитель выбирается по истории обнаружения; при отсутствии такого агента используется сервер

- **«Применять однократно»** - пропускать устройства, уже связанные с управляемым устройством, и устройства, у которых последняя попытка установки этого правила успешна
- **«Параллельных установок»** - ограничение одновременных установок; по умолчанию 10

В строках учётных данных поле **«Порядок»** определяет последовательность попыток подключения: меньшие значения проверяются раньше. Указать хотя бы один набор, подходящий целевым устройствам

Примечание

Режим **«Без интерфейса (headless)»** применяется только при установке на Linux. На Windows и macOS выбор этого режима не меняет тип устанавливаемого клиента

Проверка условий без запуска установки

При изменении условий и списка профилей форма показывает количество совпавших устройств. Значение с ≥ означает, что найдено как минимум указанное число устройств. Это нижняя граница количества совпадений, а не окончательное число

Примечание

Этот счётчик учитывает условия и профили. Фактических установок может быть меньше: при запуске отдельно исключаются игнорируемые устройства, активные попытки этого правила и уже установленные клиенты при включённом **«Применять однократно»**. Счётчик также не проверяет пароль и сетевую доступность

Повторные запуски и результаты

Автоматический отбор пропускает устройства в состоянии **«Игнорируется»** и устройства с ожидающей или выполняющейся попыткой этого правила. Неудачная установка может быть повторена при следующем запуске. Во время ручного запуска доступно **«Остановить установку»**. Проверять ход работы можно в **«Логе установки»** правила, а результаты по устройствам - в **«Попытках установки»**

Для разбора отдельной ошибки открыть также *карточку обнаруженного устройства*

Важно

Остановка прерывает выполнение, но не удаляет уже установленный клиент и не откатывает выполненные действия. Чтобы не было новых запусков по расписанию, снять **«Включено»** и сохранить правило

Журналы правила и устройства показывают последний запуск; записи **«Попыток установки»** позволяют отдельно посмотреть результаты предыдущих попыток. Снятие **«Применять однократно»** разрешает повторно отбирать устройство, но не гарантирует переустановку: на Linux и macOS перед установкой проверяется наличие клиента, и уже установленный клиент не устанавливается заново

Для обновления использовать политику *Автоматическое обновление клиента RuDesktop*

2.8.5 Как это работает

Профиль задаёт способ обнаружения, область поиска и расписание. Результаты попадают в список **«Обнаруженные устройства»**. После этого можно установить клиент на отдельное устройство или настроить правило авто-установки для устройств, соответствующих выбранным условиям. Сканирование и установка запускаются отдельно. У профиля обнаружения и правила авто-установки собственные расписания и журналы

Объекты раздела выполняют разные роли:

- **Профиль** — где искать устройства
- **Учётные данные** — как подключиться для установки
- **Правило** — на какие из найденных устройств установить клиент
- **Агент-исполнитель** — уже подключённое к серверу устройство для доступа к нужной сети

Примечание

Найденное устройство может ещё не иметь клиента RuDesktop

Важно

Перед началом выбрать исполнителя, которому доступна целевая сеть. Для установки на найденных устройствах должна быть доступна служба выбранного транспорта - SSH, WinRM / PSRP или SMBExec - и учётная запись с правами установки. Само обнаружение устройства не проверяет эти права

2.8.6 Начало работы

1. Создать *профиль обнаружения* для нужной сети
2. Запустить сканирование и проверить *обнаруженные устройства*
3. Подготовить *учётные данные* для установки клиента
4. Выполнить установку на одном устройстве и проверить её результат
5. Настроить *правило авто-установки* и его расписание для выбранной группы устройств

Для просмотра и изменения объектов раздела нужны соответствующие права пользователя или его группы. Запуск сканирования требует права изменения профиля, запуск установки - права изменения устройства или правила

Пошаговый пример: Развёртывание клиента в подсети

2.9 Установка OS

Доступна только в UEM версии

2.9.1 Образы OS

Доступны только в UEM версии

Образы OS - справочник образов операционных систем для удалённой установки в пределах одной локальной сети с помощью PXE-сервера, встроенного в сервер **RuDesktop**

Подсказка

Страница **«Образы OS»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Примечание

Инструкция по *настройке PXE-сервера*

Как это работает

Сервер **RuDesktop** содержит встроенный PXE-сервер, который раздаёт устройствам в локальной сети загрузочные файлы и параметры автоматической установки. Чтобы установить ОС:

1. на странице **«Образы OS»** добавляется **образ ОС** (ISO-файл, тип ОС, язык, часовой пояс, учётка локального администратора и набор задач для пост-установки)
2. для образа выбирается узел публикации: основной сервер или *точка распространения*
3. образ публикуется на выбранном узле действием Опубликовать - операция выполняется в фоне, а после её завершения устройства, загружающиеся в режиме PXE, будут предлагать выбрать этот образ в PXE-меню

Важно

Может быть опубликовано **несколько образов одновременно** - все они попадают в PXE-меню мультизагрузки

Один из опубликованных образов назначается образом по умолчанию и загружается автоматически по истечении таймаута

Подробнее - раздел *Мультизагрузка по PXE* ниже

Важно

Пока выполняется задача миграции, публикация, снятие с публикации и изменение образа по умолчанию ограничены на узле публикации ее образа ОС - основном сервере или выбранной точке распространения

Ограничение распространяется на все образы этого узла до завершения задачи

Подробнее о миграции - *Миграции* и *Задачи миграции*

4. устройство в BIOS переключается в режим **PXE-загрузки** и при включении автоматически забирает образ с сервера и проходит автоматическую установку
5. сразу после установки на устройстве выполняются **«Задачи после установки»** из настроек образа (по умолчанию это *Инвентаризация*, можно добавить любые *задачи*)

Примечание

PXE-клиент должен иметь сетевой доступ к выбранному узлу публикации

Для удалённой сети можно использовать точку распространения, расположенную в этой сети, и настроить локальный DHCP или DHCP relay

Предупреждение

При автоматической установке Windows штатный PXE-скрипт перед запуском установщика очищает **диск 0** командой `diskpart clean`

Разделы и данные на этом диске будут потеряны, даже если дальнейшая установка завершится ошибкой

До запуска сохраните нужные данные вне устройства и проверьте, какой физический диск Windows PE определяет как диск 0

Выбор другого диска в файле ответов не отменяет эту предварительную очистку

Мультизагрузка по PXE

PXE-сервер **RuDesktop** поддерживает **мультизагрузку**: одновременно может быть опубликовано несколько образов ОС. Все опубликованные образы попадают в единое **PXE-меню**, которое отображается на устройстве при загрузке по сети

Примечание

Если образы распределены между несколькими точками распространения, каждый узел формирует собственное PXE-меню только из назначенных ему образов. Образ по умолчанию также выбирается отдельно для каждого узла

Примечание

Ранее на PXE-сервере мог быть опубликован только один образ - публикация нового образа автоматически снимала с публикации предыдущий

Теперь образы накапливаются в меню и не вытесняют друг друга

PXE-меню

При PXE-загрузке устройства отображается меню **RuDesktop PXE Installation** со списком опубликованных образов и служебными пунктами:

1. **Список образов** - по одному пункту на каждый опубликованный образ ОС
2. **Local boot (boot from disk)** - загрузка с локального диска устройства
3. **iPXE shell** - переход в командную оболочку iPXE

Управление в меню:

- ↑ / ↓ - выбор пункта
- `Enter` - подтверждение выбора
- `S` - переход в оболочку iPXE

Примечание

Если ни один образ не опубликован, в меню отображается сообщение **«No published OS images»** с подсказкой опубликовать образ в веб-интерфейсе

Образ по умолчанию и таймаут

Один из опубликованных образов может быть назначен **образом по умолчанию**. Он предварительно выделен в меню и **загружается автоматически** по истечении таймаута, если пользователь не сделал выбор вручную. Назначить образ по умолчанию можно одним из способов:

- включить флаг PXE образ по умолчанию на странице редактирования образа (поле доступно только для **опубликованного** образа)
- выбрать действие Сделать PXE-образом по умолчанию в контекстном меню образа в таблице

Важно

Образом по умолчанию может быть назначен только **опубликованный** образ

При публикации первого образа он автоматически становится образом по умолчанию

Примечание

Признак образа по умолчанию отображается в таблице образов в столбце PXE образ по умолчанию

Таймаут автозагрузки задаётся параметром Таймаут меню PXE, секунд в *настройках сервера* (по умолчанию - **30** секунд). По истечении этого времени автоматически загружается образ по умолчанию

Важно

Чтобы новое значение таймаута вступило в силу, необходимо опубликовать или переопубликовать любой образ ОС, либо сменить образ по умолчанию - только после этого PXE-меню перегенерируется с обновлённым таймаутом

Важно

Пока выполняется задача миграции, на узле публикации ее образа ОС нельзя вручную изменить образ по умолчанию, опубликовать или снять с публикации другие образы

Подробнее - *Миграции*

Снятие с публикации и удаление

- Снять с публикации можно **отдельный образ** - остальные образы остаются в меню

  Примечание

  Если снимаемый образ был образом по умолчанию, образом по умолчанию автоматически становится другой опубликованный образ

- **Опубликованный образ нельзя удалить** - сначала снимите его с публикации, затем удалите

Важно

ISO-файл нельзя удалить из хранилища, пока на него ссылается запись образа ОС

Сначала снимите образ с публикации и удалите запись образа либо выберите в ней другой ISO-файл

Затем удаляйте прежний файл из хранилища

Примечание

При снятии образа Windows с публикации сервер пытается закрыть SMB-сеансы, использующие этот образ

Не снимайте образ с публикации во время установки Windows на устройствах: доступ к установочным файлам может прерваться

Если Windows PE не подключается к установочным файлам

После загрузки драйверов штатный скрипт инициализирует сеть и пытается подключить сетевую папку `install` как диск `Y:`. Выполняется до 30 попыток с интервалом около 10 секунд; перед запуском установки проверяется наличие `setup.exe`. Если сеть не инициализировалась или папка не подключилась, выводятся параметры сети и открывается командная строка

Проверьте сетевой адаптер, получение адреса по DHCP и доступность SMB на узле публикации образа. После устранения причины введите `exit`: скрипт повторит неудавшийся этап

Предупреждение

Это повтор сетевого этапа, а не отмена последующей очистки диска перед установкой

Выбор типа образа

Значение **«Тип OS»** должно соответствовать версии и установщику внутри загруженного ISO. Выбор похожего названия не преобразует один установщик в другой. В форме предусмотрены следующие варианты Linux:

Тип OS	Какой образ выбирать
Ubuntu 24/26	Образ с установщиком Subiquity и поддержкой Autoinstall
Debian 13	Установочный DVD для amd64 с пакетами для установки из локального источника
Astra Linux 1.7.x/2.12.x или ниже	Образ соответствующей версии Astra Linux
Astra Linux 1.8.x (astra-installer / live image)	Live-образ с astra-installer
Astra Linux 1.8.x (debian-installer image)	Образ с debian-installer
Alt Linux 10.2/10.3	Образ ALT соответствующей версии
Alt Linux 10.4	Образ ALT 10.4
Alt Linux 11.x	Образ ALT 11.x
RedOS 7 Linux	Образ РЕД ОС 7
RedOS 8 Linux	Образ РЕД ОС 8

Для Windows выбрать вариант, соответствующий редакции в ISO. Точный список вариантов Windows отображается в поле **«Тип OS»**

Важно

Для Debian 13 установочные пакеты берутся с опубликованного DVD через локальный сервер. Образ netinst с небольшим набором пакетов не заменяет полный DVD для такого сценария. Доступ в интернет для этого этапа установки Debian не требуется, но устройство должно иметь доступ к узлу публикации. Выбранный язык применяется к установленной системе, при этом текстовый установщик Debian работает на английском

Предупреждение

Штатная автоматическая установка переразмечает диск и удаляет находящиеся на нём данные

Для Debian выбирается первый диск, обнаруженный установщиком

При нескольких дисках заранее проверить выбор на тестовом устройстве и сохранить нужные данные

Выбор образа и его публикация сами по себе не создают резервную копию

Сначала опубликовать образ и проверить полный цикл установки на отдельном устройстве, включая появление клиента на сервере и задачи после установки. После замены ISO или параметров установки повторно опубликовать образ, чтобы устройство получило обновлённые установочные файлы

Медленная сеть и повторные попытки

При временной недоступности загрузочных файлов PXE повторяет загрузку выбранного образа. Для этого этапа предусмотрено до 30 попыток с паузой 10 секунд после неудачной попытки. Время самой загрузки добавляется к этим паузам, поэтому весь этап может занимать дольше пяти минут. Повторяется этап загрузки, а не весь процесс установки ОС. Если предел попыток исчерпан, загрузка останавливается с сообщением **«Boot failed»**

Проверить получение адреса по DHCP, сетевой адаптер, доступность узла публикации и наличие опубликованного образа. Повторные попытки помогают при временной задержке сети, но не исправляют отсутствующий драйвер или неверный адрес сервера

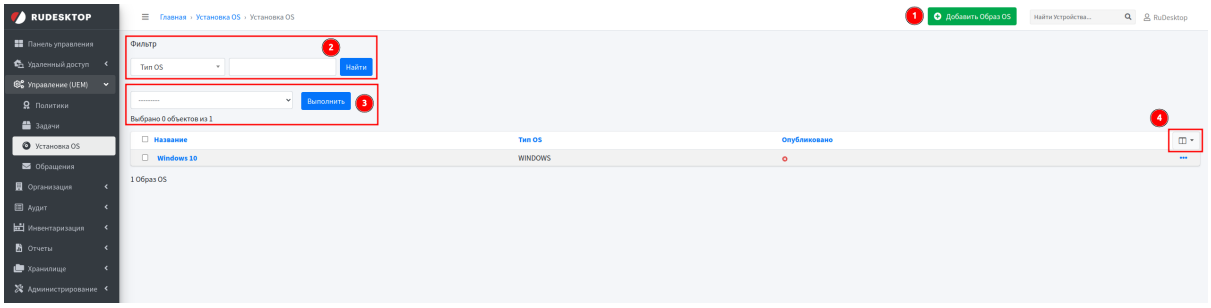
Подсказка

После установки ОС клиент также может появиться на сервере не сразу: загрузка клиента и отправка результата выполняются с повторными попытками при сетевых ошибках. Не запускать установку заново только из-за задержки появления клиента. Сначала проверить связь установленной ОС с сервером и результат установки клиента

Для Windows доступны журналы `C:\Windows\Temp\setupcomplete.log` и `C:\Windows\Temp\rudesktop-install.log`. Первый помогает проверить загрузку клиента и обращение к серверу, второй - установку MSI

Описание страницы

На странице **Образы OS** отображено:



1. Кнопка Добавить Образ OS
2. Фильтр

3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление образа OS

При нажатии на кнопку Добавить Образ OS откроется страница добавления образа со следующими полями:

1. Название - пользовательское название образа
2. Тип OS - выбор типа образа ОС (Windows/Ubuntu/Debian/Astra Linux/Alt Linux/RedOS Linux)
3. ISO образ - можно выбрать файл из репозитория сервера **RuDesktop**, либо выбрать на своём компьютере

Подсказка

- При нажатии на кнопку Browse откроется окно выбора файла на компьютере
- При нажатии на кнопку Репозиторий откроется всплывающее окно выбора файла из внутреннего репозитория сервера **RuDesktop**

  Важно

  Файлы отображаются из всех репозиториев, созданных на сервере **RuDesktop**

- Можно просто перетащить файл в поле Выберите файл или перетащите его сюда

4. Язык - язык ОС для установки на удалённое устройство
5. Часовой пояс - часовой пояс ОС для установки на удалённое устройство
6. Локальный администратор - имя пользователя локального администратора (будет создан при установке ОС на удалённое устройство)
7. Пароль локального администратора - пароль для учётной записи локального администратора, которая будет создана в ходе установки
8. Задачи после установки - выбор задач для выполнения на устройстве после установки ОС
9. Точка распространения - узел, на котором будет опубликован образ

Примечание

Пустое значение означает основной сервер

Фильтр

Можно формировать таблицу для получения определённых данных, используя фильтр:

1. `Тип ОС` - фильтрация образов по типу ОС
2. `Поле поиска` - поиск по ключевому слову

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные образы - удаление выбранных образов
2. Экспортировать выбранные образы - экспорт выбранных образов

> **Примечание**
>
> После выбора данного действия нужно выбрать необходимый формат файла

> **Важно**
>
> В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление образов

Для массового удаления образов необходимо:

1. Отметить необходимые образы в таблице
2. Выбрать действие Удалить выбранные образы
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие образы будут удалены
5. Нажать на кнопку Да, я уверен

> **Подсказка**
>
> Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору

6. Выбранные образы будут удалены

Экспорт образов

Для массового экспорта образов необходимо:

1. Отметить необходимые образы в таблице
2. Выбрать действие Экспортировать выбранные образы
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Название` - пользовательское название образа ОС
2. `Тип OS` - тип операционной системы образа ОС
3. `Опубликовано` - статус публикации образа на PXE-сервере
4. `Статус публикации` - текущее состояние фоновой операции: в очереди, публикация, опубликован, снятие с публикации или ошибка
5. `Точка распространения` - узел, который раздаёт образ по PXE
6. `PXE образ по умолчанию` - признак образа, выбранного для автоматической загрузки в PXE-меню по истечении таймаута

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню. Доступные действия:

1. `Редактировать` - при выборе этого пункта откроются свойства образа
2. `Удалить` - при выборе этого пункта образ будет удалён

> **Важно**
>
> Опубликованный образ удалить нельзя
>
> Сначала снимите его с публикации, затем удалите

3. `История изменений` - при выборе этого пункта будет отображена история образов: создание/редактирование и пользователь, который выполнил данные операции
4. `Опубликовать` - поставить в очередь публикацию образа на выбранном узле и добавление в его PXE-меню мультизагрузки
5. `Сделать PXE-образом по умолчанию` - при выборе этого пункта опубликованный образ назначается образом по умолчанию, который автоматически загружается в PXE-меню по истечении таймаута

Подсказка

Образом по умолчанию может быть назначен только опубликованный образ

Подробнее - раздел *Мультизагрузка по PXE*

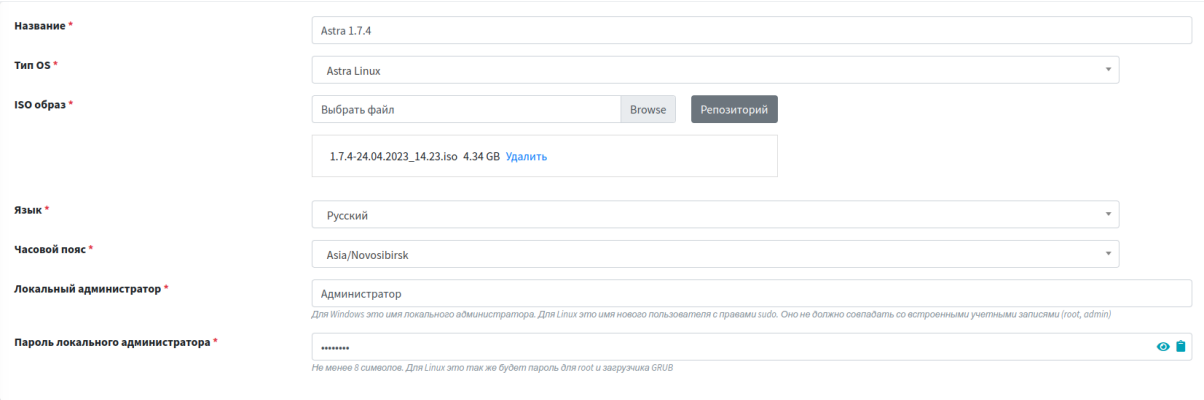
Важно

Пока выполняется задача миграции, действия публикации, снятия с публикации и назначения образа по умолчанию недоступны для всех образов на том же узле публикации - основном сервере или выбранной точке распространения

Свойства образа

Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств. Доступные поля:



1. Название - пользовательское название образа
2. Точка распространения - основной сервер или точка распространения, обслуживающая PXE-клиентов

   Примечание

   Для опубликованного образа поле нельзя изменить: сначала снимите образ с публикации

3. Тип OS - выбор типа образа ОС (Windows/Ubuntu/Debian/Astra Linux/Alt Linux/RedOS Linux)
4. ISO образ - можно выбрать файл из репозитория сервера **RuDesktop**, либо выбрать на своём компьютере
5. Язык - язык ОС для установки на удалённое устройство
6. Часовой пояс - часовой пояс ОС для установки на удалённое устройство

7. Локальный администратор - имя пользователя локального администратора (будет создан при установке ОС на удалённое устройство)
8. Пароль локального администратора - пароль для учётной записи локального администратора, которая будет создана в ходе установки
9. Задачи после установки - выбор задач для выполнения на устройстве после установки ОС
10. PXE образ по умолчанию - назначить этот образ образом по умолчанию в PXE-меню мультизагрузки

> **Примечание**
>
> Образ загрузится автоматически по истечении таймаута, если в меню не сделан выбор вручную
>
> Поле отображается только для **опубликованного** образа
>
> Подробнее - раздел *Мультизагрузка по PXE*

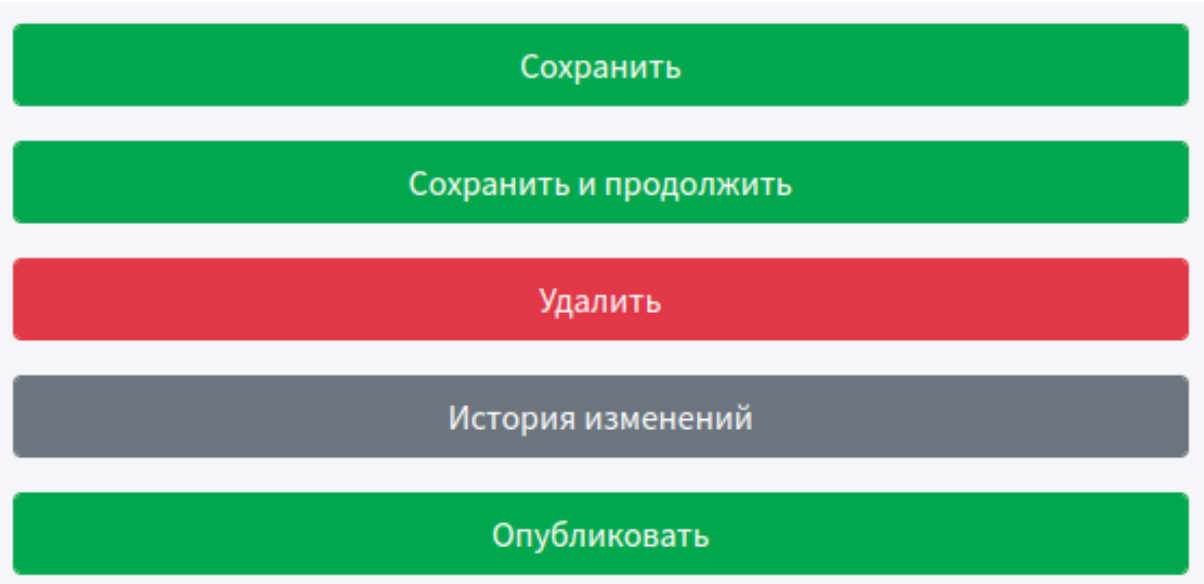
Проверка публикации

На вкладке Статус публикации отображаются состояние операции, время запуска и завершения, а также последняя ошибка

Вкладка Лог публикации содержит потоковый терминал с выводом скачивания ISO, генерации конфигурации, монтирования образа и запуска PXE/SMB

Меню действий

Меню действий расположено на всех вкладках страницы редактирования



Имеет следующие возможности:

1. Сохранить - производит сохранение внесённых изменений и перенаправляет на страницу **«Образы OS»**

2. Сохранить и продолжить - производит сохранение внесённых изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить - производит удаление образа и перенаправляет на страницу **«Образы OS»**

> **Примечание**
>
> 1. После нажатия на кнопку Удалить откроется страница подтверждения удаления образа
> 2. После подтверждения удаления образа произойдёт переход на страницу **«Образы OS»** и появится уведомление Образ OS «НАЗВАНИЕ_ОБРАЗА» был успешно удален

4. История изменений - отображает все изменения, выполненные для этого образа
5. Опубликовать - опубликовать образ ОС на PXE-сервере

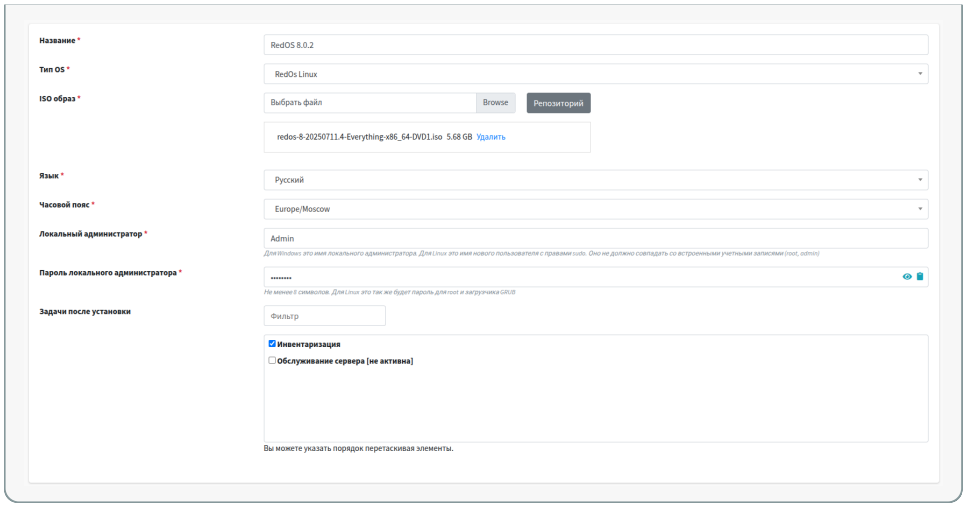
Пример

Добавление и публикация ISO образа ОС RedOS

Для публикации образа ОС и последующей установки на удалённое устройство необходимо:

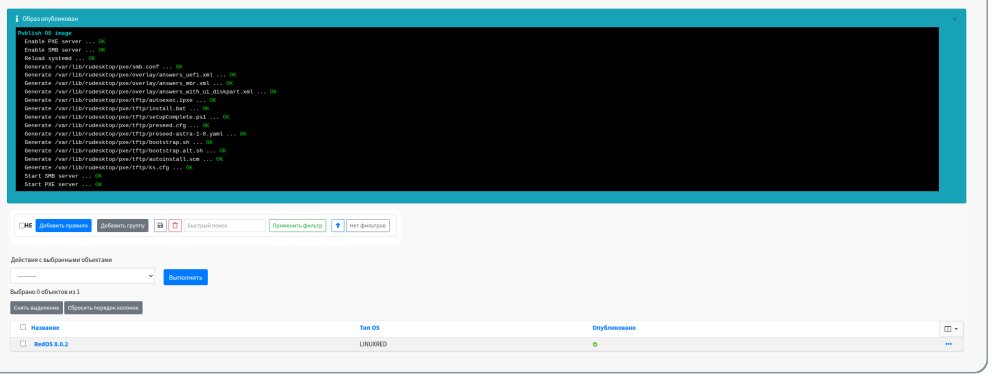
1. На странице **«Образы OS»** нажать на кнопку Добавить Образ OS
2. Заполнить следующие поля:
    1. Название - RedOS 8.0.2
    2. Тип OS - из выпадающего списка выбрать **RedOs Linux**
    3. ISO образ - загрузить файл образа с компьютера, либо выбрать его из внутреннего репозитория сервера **RuDesktop**
    4. Язык - Русский
    5. Часовой пояс - Europe/Moscow
    6. Локальный администратор - Admin
    7. Пароль локального администратора - Qwerty123
    8. Задачи после установки - отметить **Инвентаризация**

> **Примечание**
>
> Можно выбрать несколько задач и при необходимости указать порядок их выполнения перетаскиванием
>
> Пример:



3. Нажать на кнопку Сохранить и продолжить для сохранения образа
4. Нажать на кнопку Опубликовать

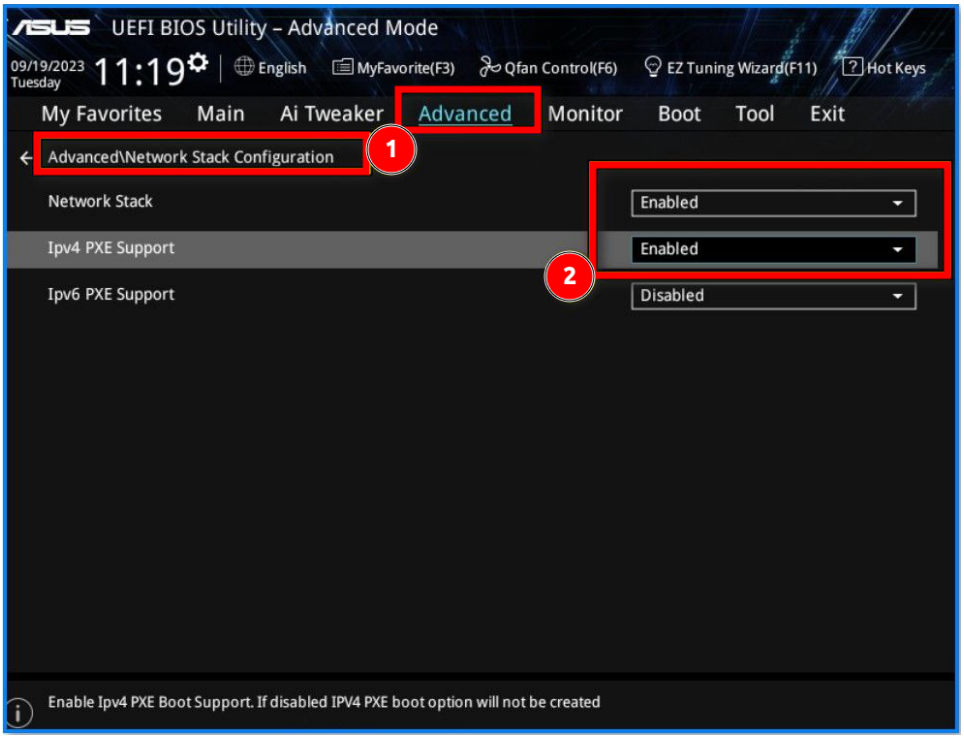
> **Примечание**
>
> После отобразится сообщение о постановке публикации в очередь
>
> Ход и результат операции можно посмотреть в свойствах образа на вкладках Статус публикации и Лог публикации



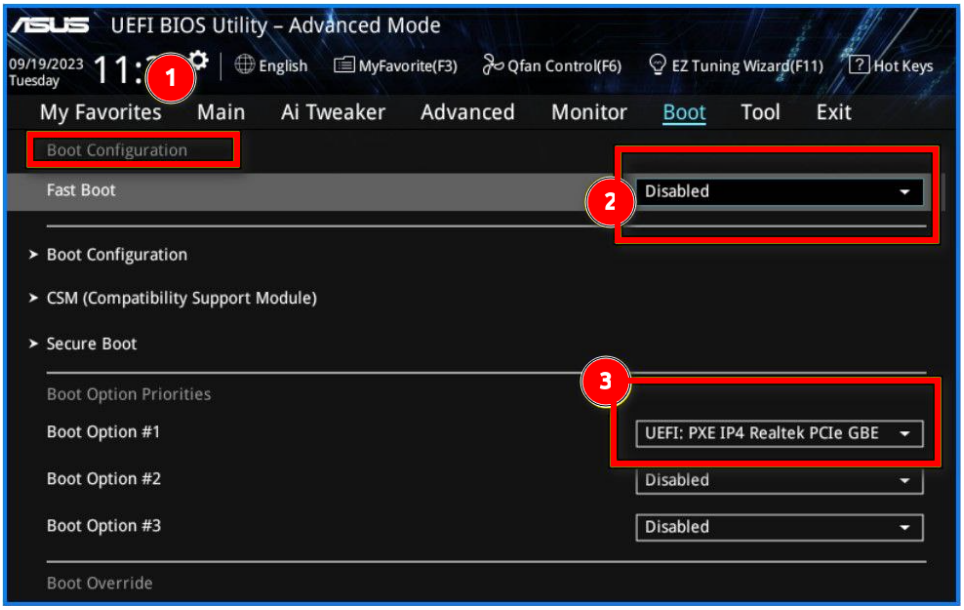
Предварительные настройки устройства

> **Важно**
>
> Расположение в BIOS данных настроек может отличаться в зависимости от версии/производителя BIOS

1. При запуске устройства перейти в BIOS
2. Переключиться в режим Advanced mode
3. Перейти во вкладку Network Stack Configuration
    1. Включить пункты Network Stack и Ipv4 PXE Support



4. Перейти во вкладку Boot
    1. Отключить Fast boot
    2. Установить UEFI: PXE Ipv4 Realtek PCIe GBE в пункте Boot Option



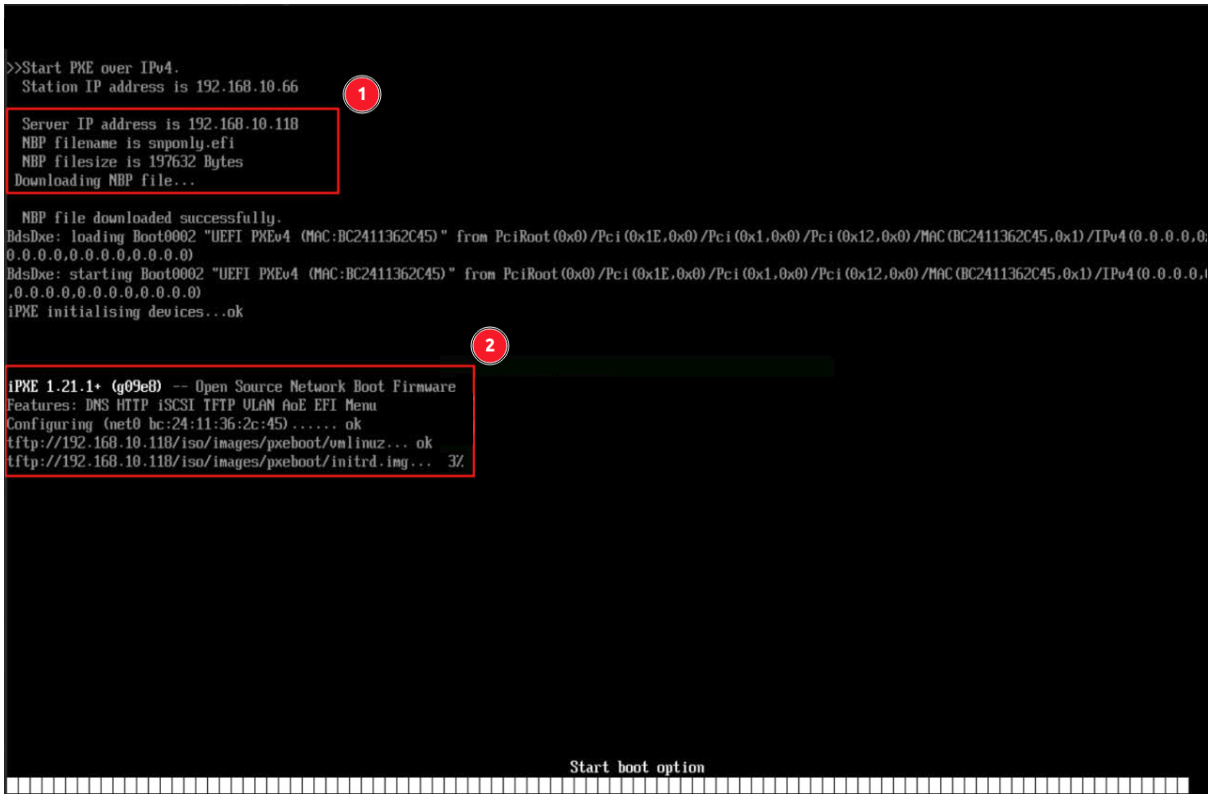
5. Перезапустить ПК с сохранением всех внесённых в BIOS изменений

Установка ОС

При правильном выполнении всех настроек при включении ПК отобразится:

1. Сообщение об успешном соединении с сервером
2. Процесс загрузки установочных файлов на устройство

3. После начнётся автоматическая установка ОС



2.9.2 Миграции

Доступны только в UEM версии

Миграции — справочник сценариев перехода устройств с **Windows** на **Linux**. Запись миграции описывает, какой образ ОС установить, кого из пользователей перенести, какие данные забрать с исходного устройства и какие задачи **UEM** выполнить после переустановки

Подсказка

Страница **«Миграции»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Примечание

Сама миграция запускается не на этой странице, а на странице *Задачи миграции*, где выбираются миграция, устройства и группы

Как это работает

Миграция — это многоэтапный сценарий перехода с **Windows** на **Linux**, который запускается из задачи миграции. На одну запись миграции могут ссылаться несколько задач миграции

1. На странице **«Образы OS»** добавляется и при необходимости публикуется целевой *образ Linux*
2. На странице **«Миграции»** создаётся запись миграции и заполняются вкладки:
   - Основная информация — название, целевой образ ОС, временный пароль локальных пользователей, учётные данные администратора домена и задачи UEM после миграции
   - Пользователи — какие пользователи переносятся
   - Выбор данных — какие директории, разделы и браузеры собираются с **Windows**
3. На странице *Задачи миграции* создаётся задача, выбирается данная миграция, устройства и/или группы, после чего запускается выполнение

Этапы миграции на устройстве

Каждое устройство в задаче миграции последовательно проходит этапы:

1. `Сбор данных` — на **Windows** запускается плейбук сбора. Собираются стандартные пользовательские директории, данные с несистемных разделов, дополнительные пути и **AppData** выбранных браузеров. Данные упаковываются в **TAR**-архивы и сохраняются в SMB-каталог узла, на котором опубликован целевой PXE-образ: точки распространения либо главного сервера. Рядом сохраняется `manifest.json` с описанием профилей пользователей и доменной информацией. После завершения сбора каждый архив автоматически проверяется по размеру и контрольной сумме **SHA256** из манифеста — при несовпадении этап завершается с ошибкой
2. `Сброс загрузчика` — устройство переводится в режим PXE-загрузки и перезапускается. Если целевой образ не опубликован к этому моменту, выполнение задачи останавливается с ошибкой
3. `Установка ОС` — устройство забирает опубликованный образ Linux с PXE-сервера и проходит автоматическую установку
4. `Восстановление` — на установленном **Linux** запускается плейбук восстановления. Создаются локальные пользователи, при необходимости устройство вводится в домен, восстанавливаются собранные ранее данные. После восстановления выполняются задачи UEM, выбранные в миграции
5. `Готово` — устройство считается мигрированным

Важно

Установка **Linux** через PXE затирает диск, выбранный установщиком. При нескольких физических дисках установщик может выбрать любой подходящий — содержимое диска будет потеряно. Перед запуском миграции необходимо убедиться, что нужные данные включены в сценарий миграции либо сохранены отдельно

Описание страницы

На странице **Миграции** отображено:

1. Кнопка Добавить Миграцию
2. Поле поиска
3. Таблица с возможностью настройки отображаемых столбцов

Добавление миграции

При нажатии на кнопку Добавить Миграцию откроется страница добавления миграции с тремя вкладками: **Основная информация**, **Пользователи** и **Выбор данных**

Основная информация

Доступные поля:

1. Название — пользовательское название миграции (должно быть уникальным)
2. Целевой образ ОС — образ Linux из справочника *Образы OS*, который будет установлен на устройство в ходе миграции

> **Важно**
>
> Образ должен быть опубликован к началу этапа `Сброс загрузчика`. При запуске задачи миграции сервер автоматически обеспечивает публикацию образа и назначает его образом по умолчанию для PXE на узле, указанном в свойствах образа. Публикация выполняется в фоне, ее завершения нужно дождаться. Другие опубликованные образы сохраняются в меню PXE

3. Временный пароль локальных пользователей — пароль, который будет установлен всем перенесённым локальным пользователям после миграции

> **Примечание**
>
> Локальные пароли **Windows** не переносятся. После миграции локальный пользователь входит с временным паролем и должен сменить его при первом логине. Если поле оставить пустым, пароль локальным пользователям задаваться не будет

4. Логин администратора домена — логин учётной записи с правом ввода устройств в домен. Заполняется только при миграции доменных пользователей
5. Пароль администратора домена — пароль соответствующей учётной записи

Важно

Если в собранных данных обнаружен факт включения исходного устройства в домен, но учётные данные администратора домена не заполнены, этап `Восстановление` завершается с ошибкой. После заполнения учётных данных миграцию можно продолжить действием Запустить/продолжить миграцию в задаче миграции — повторяется только этап с ошибкой, успешно завершённые этапы не перезапускаются

6. Задачи после миграции — выбор задач **UEM**, которые будут выполнены на устройстве после восстановления

Примечание

- Выбираются *задачи*, не политики
- Порядок выполнения задаётся перетаскиванием
- Расписание выбранных задач игнорируется: задачи выполняются однократно сразу после восстановления, только на мигрируемом устройстве
- Задачи, заданные в *образе ОС* (поле «Задачи после установки»), при миграции не выполняются — для миграции используются только задачи, указанные здесь
- Отчёты и уведомления по выбранным задачам формируются согласно их собственным настройкам, как и при обычном запуске задач **UEM**

Пользователи

Доступные поля:

1. Перенос всех пользователей — флаг переноса всех учётных записей, найденных на устройстве (локальных и доменных). По умолчанию включён. В зависимости от значения флага в форме отображается одно из двух полей-списков:
   - флаг включён — отображается Исключить пользователей
   - флаг снят — отображается Перенести пользователей
2. Перенести пользователей — список логинов, которые нужно перенести. Отображается, если флаг Перенос всех пользователей снят. Будут перенесены только указанные пользователи
3. Исключить пользователей — список логинов, которые не нужно переносить. Отображается, если флаг Перенос всех пользователей включён. Будут перенесены все найденные пользователи, кроме указанных

Примечание

В списках Перенести пользователей и Исключить пользователей имя пользователя сопоставляется по любому из вариантов:

- полное имя учётной записи в виде `DOMAIN\username`;
- короткое имя пользователя без домена (`username`);
- имя профильной папки в `C:\Users\`.

Сравнение регистронезависимое. Системные учётные записи Windows (`Administrator`, `Guest`, `DefaultAccount`, `WDAGUtilityAccount` и встроенные сервисные SID) исключаются из переноса автоматически

Примечание

Восстанавливаются как локальные, так и доменные пользователи

- Локальный пользователь восстанавливается с временным паролем из основной информации миграции
- Доменный пользователь восстанавливается с использованием доменных учётных данных и продолжает входить со своим доменным паролем; устройство при этом вводится в домен

Важно

Для **ALT Linux** и **RED OS** имена локальных пользователей с кириллическими символами автоматически транслитерируются в латиницу (например, `Иванов` → `ivanov`). Недопустимые в **Linux** символы заменяются на `_`. Логин пользователя в новой ОС будет отличаться от исходного — пользователю нужно входить под транслитерированным именем. Доменные пользователи переносятся без изменения имени

Примечание

Для отдельных дистрибутивов **Linux** возможны особенности дисплейного менеджера при первом входе доменного пользователя — например, имя пользователя может потребоваться ввести вручную. Это не зависит от **RuDesktop** и определяется поведением выбранного дистрибутива

Выбор данных

Доступные поля:

1. Перенос стандартных директорий пользователя — собирать стандартные пользовательские папки **Windows**: `Desktop` / `Documents` / `Downloads` / `Pictures` / `Videos` / `Music` и т.п.

Примечание

Стандартные директории восстанавливаются в домашние каталоги соответствующих пользователей **Linux** (`/home/<user>/...`) с автоматическим сопоставлением русских и английских имён папок

2. Перенос данных из не системных разделов — собирать содержимое других дисков (`D:\`, `E:\` и т.д.)

Примечание

Данные с несистемных разделов восстанавливаются в каталог `/opt/from_migration/` на устройстве **Linux**

3. Дополнительные директории/файлы — список дополнительных путей для переноса

Примечание

- Принимаются абсолютные пути и пути относительно домашних директорий пользователей
- Глобальные пути восстанавливаются в `/opt/from_migration/`. К имени каталога добавляется короткий хеш, чтобы одноимённые исходные пути не смешивались
- Запрещены сегмент `..`, двойной слеш (кроме UNC-префикса), символы перевода строки и нулевой байт; при попытке сохранить такой путь форма выдаст ошибку

4. Сбор данных браузеров — флажки браузеров для переноса: `Chrome`, `Yandex Browser`, `Firefox`, `Edge`

Важно

Перед сбором данных браузер принудительно закрывается на исходном устройстве. Несохранённые вкладки и текущая работа в браузере будут потеряны — пользователь должен сохранить их до запуска задачи миграции

Важно

Собирается только содержимое **AppData** выбранных браузеров. Собранные данные копируются как обычные пользовательские файлы и попадают в каталог `~/from_migration/` мигрируемого пользователя на **Linux** — они не подставляются

автоматически в профиль установленного на **Linux** браузера. Перенос «рабочего» профиля не гарантируется и зависит от версии браузера и совместимости форматов

Важно

На вкладке Выбор данных указываются только пользовательские данные/-файлы. Из исходной **Windows**-системы **не** переносятся:

- установленные программы и приложения;
- реестр **Windows**;
- системные настройки;
- драйверы устройств.

Необходимое программное обеспечение должно быть установлено на **Linux** отдельно — например, через *задачи UEM*, выбранные в поле Задачи после миграции

Меню действий

Меню действий расположено на всех вкладках страницы редактирования и имеет следующие возможности:

1. Сохранить — производит сохранение внесённых изменений и перенаправляет на страницу **«Миграции»**
2. Сохранить и продолжить — производит сохранение внесённых изменений и оставляет на странице редактирования
3. Удалить — производит удаление миграции

Важно

Миграцию нельзя удалить, если на неё ссылаются задачи миграции — сначала нужно удалить задачи миграции

4. История изменений — отображает все изменения, выполненные для этой миграции

Поиск

В верхней части страницы доступно поле поиска. Поиск выполняется по названию миграции и названию целевого образа ОС

Для выполнения поиска необходимо ввести значение в поле и нажать на кнопку Найти

Таблица

Таблица разбита по столбцам:

1. `Название` — пользовательское название миграции
2. `Целевой образ ОС` — образ Linux, который установится на устройство
3. `Обновлено` — дата последнего изменения миграции

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — откроет страницу свойств миграции
2. `Удалить` — удалит миграцию
3. `История изменений` — покажет историю изменений записи миграции

2.9.3 Задачи миграции

Доступны только в UEM версии

Задачи миграции — конкретный запуск сценария миграции на выбранных устройствах и/или группах. Задача миграции хранит ссылку на сценарий *Миграции*, набор устройств и групп для миграции, статус, лог исполнения и состояние миграции по каждому устройству

Подсказка

Страница **«Задачи миграции»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

Задача миграции — это «инстанс» сценария миграции, привязанный к конкретному набору устройств. На один сценарий миграции может ссылаться несколько задач миграции

Жизненный цикл задачи миграции

1. Задача создаётся в статусе `Новая`
2. По действию Запустить/продолжить миграцию сервер:
    - публикует целевой образ ОС, если он ещё не опубликован, и снимает с публикации остальные образы
    - запоминает, какой образ был фактически опубликован для этой задачи (поле Опубликованный образ)
    - определяет устройства по настройкам вкладки **Устройства и группы** и для каждого создаёт запись о ходе миграции

- переводит задачу в статус Запущена и ставит в очередь этапы миграции на каждом устройстве

Важно

Устройство не может одновременно участвовать в двух выполняющихся задачах миграции. Если устройство уже задействовано в другой задаче в статусе Запущена, оно будет автоматически пропущено и в текущую задачу не включится. Чтобы запустить миграцию повторно, нужно дождаться завершения предыдущей задачи на этом устройстве

Примечание

Несколько задач миграции могут выполняться параллельно — ограничение действует только на уровне отдельного устройства, не на уровне задач

3. По мере прохождения устройством этапов (Сбор данных → Сброс загрузчика → Установка ОС → Восстановление → Готово) обновляется его Состояние миграции устройства
4. Когда все устройства завершают миграцию, задача переходит в статус:
   - Выполнено — все устройства успешно завершили этап Готово
   - Ошибка — хотя бы одно устройство завершилось с ошибкой

Важно

Готовность мигрированного устройства к работе определяется только по статусу Готово соответствующего состояния миграции. До этого момента не рекомендуется использовать устройство — на нём ещё могут выполняться этапы восстановления и задачи **UEM** после миграции

Продолжение миграции после ошибки

Если на одном из устройств этап миграции завершился с ошибкой (статус Ошибка на вкладке *Состояния миграции устройств*), задачу не нужно создавать заново — миграцию можно продолжить с того этапа, на котором она прервалась

1. Устранить причину ошибки (см. Лог исполнения и Открыть лог устройства для конкретного устройства). Например — заполнить учётные данные администратора домена в *миграции*, восстановить сетевой доступ к устройству, исправить параметры PXE/DHCP
2. Нажать Запустить/продолжить миграцию. Сервер заново выполнит **только** тот этап, на котором возникла ошибка, на устройствах со статусом Ошибка. Этапы, успешно завершённые ранее (Успешно), повторно не запускаются. Устройства в статусе Готово пропускаются

Примечание

Полная перезагрузка сценария с этапа `Сбор данных` для конкретного устройства выполняется только через Сбросить миграцию — см. *Запустить/продолжить миграцию vs Сбросить миграцию*

Примечание

После миграции запись устройства на странице *Устройства* не дублируется — сохраняется та же запись, у которой меняется платформа с **Windows** на **Linux**

Запустить/продолжить миграцию vs Сбросить миграцию

- Запустить/продолжить миграцию — основное действие. Запускает миграцию, а после ошибки — повторяет именно тот этап, на котором возникла ошибка. Устройства и этапы, уже завершённые с результатом `Успешно`, повторно не запускаются. Используется для штатного восстановления после ошибок (например, после заполнения учётных данных администратора домена)
- Сбросить миграцию — вспомогательное действие. Удаляет состояния всех устройств, которые на момент сброса находятся в статусе `Ошибка` или `Выполняется`, и переводит задачу в статус `Ошибка`. После сброса последующий Запустить/продолжить миграцию начнёт миграцию для этих устройств заново с этапа `Сбор данных`. Действие предназначено для повторного прохождения сценария с начала, а не для штатного восстановления после ошибки

Примечание

Состояния устройств в статусе `Успешно` действие Сбросить миграцию не удаляет — повторно мигрировать уже мигрированное устройство в той же задаче не нужно

Важно

После сброса задачи и последующего запуска повторный сбор данных удаляет ранее собранные **TAR**-архивы и манифест устройства. Если эти данные нужны вне задачи миграции, их необходимо сохранить отдельно до выполнения сброса

Поведение при недоступности устройства

Если устройство временно недоступно (Offline), оркестратор повторяет запуск плейбука миграции до **10 раз** с интервалом **30 секунд**. Если за это время устройство не появилось в сети, состояние миграции переходит в `Ошибка`. После того как устройство станет доступно, миграцию можно продолжить действием Запустить/продолжить миграцию

Описание страницы

На странице **Задачи миграции** отображено:

1. Кнопка Добавить Задачу миграции
2. Поле поиска
3. Таблица с возможностью настройки отображаемых столбцов

Добавление задачи миграции

При нажатии на кнопку Добавить Задачу миграции открывается страница задачи миграции. Поля сгруппированы по вкладкам

Основная информация

Доступные поля:

1. Название — пользовательское название задачи миграции
2. Миграция — выбор сценария из справочника *Миграции*

Устройства и группы

Доступные поля:

1. Запускать на всех устройствах — если списки устройств и групп пусты, сервер включит в миграцию все Windows-устройства. Устройства с другими ОС будут пропущены. Если выбрать устройства или группы вручную, задача использует этот выбор
2. Устройства — конкретные устройства, на которые распространяется миграция
3. Группы — группы устройств, все участники которых будут включены в задачу
4. Динамические группы — динамические группы; принадлежность к ним вычисляется во время исполнения

Примечание

Кнопка Загрузить динамические группы обновляет состав динамических групп с учётом текущего окружения

Примечание

Помимо поштучного добавления доступны массовые действия над всем списком — кнопки Добавить и сохранить все и Очистить список и сохранить. Они доступны только после сохранения записи. При большом количестве элементов действие выполняется в фоновом режиме: отображается индикатор прогресса со счётчиком и кнопка Отменить задачу, а списки блокируются до завершения операции

Важно

Перед запуском задачи миграции рекомендуется проверить:

- выбраны устройства или группы либо включён флажок Запускать на всех устройствах
- в **BIOS** устройств включены **Network Stack** и **PXE** (см. *Предварительные настройки устройства*)
- сетевые сервисы PXE/DHCP в локальной сети доступны и работают
- в *миграции* заполнены учётные данные администратора домена — если на устройствах есть доменные пользователи. При отсутствии этих данных этап `Восстановление` завершится с ошибкой; в этом случае нужно дозаполнить миграцию и продолжить задачу действием Запустить/продолжить миграцию

Статус

Поля вкладки заполняются автоматически и доступны только для чтения

1. Статус — текущий статус задачи: `Новая` / `Запущена` / `Выполнено` / `Ошибка`
2. Запущено — дата и время старта задачи
3. Завершено — дата и время завершения задачи
4. Опубликованный образ — образ ОС, который был фактически опубликован при запуске данной задачи
5. Ошибка — текст последней ошибки задачи

Лог исполнения

Вкладка содержит онлайн-лог задачи миграции с группировкой сообщений по устройствам и этапам

В шапке лога устройства размещена ссылка Открыть лог устройства, переводящая на детальный журнал плейбуков для конкретного устройства. Сообщения с пометкой WARNING означают, что на этапе Сбор данных встретились предупреждения и миграция приостановлена — после анализа логов её можно продолжить или сбросить

Состояния миграции устройств

Вкладка отображает таблицу с одним рядом на каждое устройство задачи

Столбцы:

1. Устройство — исходная запись устройства до миграции
2. Стадия — этап, на котором сейчас находится устройство:
    - Сбор данных
    - Сброс загрузчика
    - Установка ОС
    - Восстановление
    - Готово
3. Статус — статус выполнения текущего этапа: Ожидает / Выполняется / Успешно / Ошибка
4. Запущено / Завершено — временные метки этапа
5. Устройство после миграции — запись устройства, на которой выполняется этап Восстановление. В штатном сценарии указывает на ту же запись, что и Устройство. Заполняется автоматически после успешной установки Linux
6. UUID устройства — аппаратный UUID, считанный на стадии Сбор данных. Используется для сопоставления исходного устройства и устройства, которое отчиталось об окончании установки ОС
7. Местоположение данных — каталог на узле публикации целевого PXE-образа, где хранятся собранные **TAR**-архивы и manifest.json для устройства. Для образа с выбранной точкой распространения каталог находится на этой точке, иначе — на главном сервере
8. Ошибка — текст последней ошибки этапа

Меню действий

Меню действий расположено на всех вкладках страницы задачи миграции

Имеет следующие возможности:

1. Сохранить — сохраняет внесённые изменения и перенаправляет на страницу **«Задачи миграции»**

2. Сохранить и продолжить — сохраняет изменения и оставляет на странице редактирования
3. Удалить — удаляет задачу миграции
4. История изменений — показывает историю изменений задачи
5. Запустить/продолжить миграцию — запускает или возобновляет миграцию (см. *Запустить/продолжить миграцию vs Сбросить миграцию*)
6. Сбросить миграцию — сбрасывает состояния устройств в статусах `Ошибка` и `Выполняется` (см. *Запустить/продолжить миграцию vs Сбросить миграцию*). Доступно только когда задача в статусе `Запущена` или `Ошибка`

Поиск

В верхней части страницы доступно поле поиска. Поиск выполняется по названию задачи, названию миграции и названию целевого образа ОС

Для выполнения поиска необходимо ввести значение в поле и нажать на кнопку Найти

Таблица

Таблица разбита по столбцам:

1. `Название` — пользовательское название задачи миграции
2. `Миграция` — выбранный сценарий миграции
3. `Статус` — текущий статус: `Новая` / `Запущена` / `Выполнено` / `Ошибка`

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — откроет страницу задачи миграции
2. `Удалить` — удалит задачу миграции
3. `История изменений` — покажет историю изменений задачи
4. `Запустить/продолжить миграцию` — запустит или продолжит миграцию по выбранной задаче
5. `Сбросить миграцию` — сбросит состояния устройств в статусах `Ошибка` и `Выполняется`. Доступно только когда задача в статусе `Запущена` или `Ошибка`

Уведомления

Если для задачи миграции включены *уведомления*, сервер **RuDesktop** отправляет:

- уведомление о завершении задачи миграции с указанием итогового статуса и прогресса (количество успешно мигрированных устройств от общего числа);
- уведомление о завершении миграции на каждом устройстве с указанием стадии и статуса. Включается отдельным флагом

Уведомления отправляются по тем же каналам, что и остальные уведомления **RuDesktop** — `Email`, `Telegram` и т.п. Подробнее о настройке каналов и правил — на странице *Уведомления*

Установка OS — раздел для удалённой установки операционных систем по сети и переноса устройств с **Windows** на **Linux** (миграция). Раздел включает справочник образов ОС, описание сценариев миграции и контроль выполнения миграции на устройствах

Подсказка

Раздел **«Установка OS»** доступен только при использовании локального сервера **Управление конфигурациями (UEM)**

Важно

Миграция поддерживается **только в направлении Windows → Linux**. Обратный сценарий (с Linux на Windows) и миграция между разными версиями одной и той же ОС не поддерживаются

Примечание

Установка ОС и миграция используют встроенный PXE-сервер **RuDesktop**. Инструкция по *настройке PXE-сервера*

Образы OS

Добавление и публикация образов ОС на PXE-сервере

Миграции

Описание сценария миграции **Windows → Linux**: целевой образ, пользователи, данные и задачи после миграции

Задачи миграции

Запуск миграции **Windows → Linux** на устройствах и группах, контроль выполнения по этапам

2.10 Обновления ОС

Доступны только в UEM версии

Обновления ОС - раздел для поиска и установки обновлений Windows с использованием локального каталога и заранее подготовленных пакетов. Обновляемым устройствам не требуется обращаться к внешнему источнику обновлений: каталог и пакеты передаются из инфраструктуры RuDesktop

2.10.1 Каталог и сканирование обновлений

Доступно только в UEM версии

Как это работает

Задача передаёт выбранный каталог на Windows-устройство и выполняет локальную проверку необходимых обновлений. Сканирование только определяет потребность в обновлениях; установка запускается отдельно

Добавление каталога

1. Подготовить файл каталога `Wsusscn2.cab`
2. Открыть **«Обновления ОС → Каталоги обновлений Windows»** и добавить запись
3. Заполнить **«Название»**, позволяющее отличить этот каталог от предыдущих
4. В поле **«Wsusscn2.cab»** загрузить файл или выбрать его из хранилища
5. Сохранить каталог

Результат поиска зависит от выбранного каталога. После получения нового каталога добавить его в RuDesktop, выбрать в задаче и повторить сканирование

Создание задачи сканирования

1. Открыть **«Задачи сканирования обновлений»** и добавить задачу
2. На вкладке **«Основное»** указать **«Название»** и **«Каталог»**
3. Выбрать **«Точку распространения»**:
   - **«Автоматически»** - задачу исполняет первый доступный узел;
   - **«Основной сервер»** - выполнять на основном сервере;
   - конкретная точка распространения - закрепить задачу за ней
4. На вкладке **«Устройства»** выбрать устройства, группы или динамические группы
5. Сохранить задачу и выполнить **«Запустить задачу»**

   Для нескольких задач в списке доступно действие **«Запустить выбранные задачи»**
6. Проверить вкладки **«Состояние»**, **«Лог исполнения»** и результаты по устройствам

Для периодической проверки включить **«Запускать по расписанию»**, настроить периодичность и проверить **«Следующий запуск»**. **«Приоритет»** задаёт приоритет обработки задачи в очереди: низкий, средний, высокий или критический. Он не связывает сканирование с установкой и не заменяет настройку их расписаний

Выбранные устройства, группы и динамические группы объединяются; повторно попавшее в выборку устройство обрабатывается один раз. Состав определяется при запуске, и в него включаются только устройства с ОС Windows по данным сервера. Пустой выбор не означает «все устройства»

Результаты сканирования

В карточке задачи отображаются статус, время последнего запуска и завершения, число успешных, пропущенных и ошибочных результатов. В результатах устройств показаны состояние, количество найденных обновлений и текст ошибки. В **«Пакетах обновлений»** появляются сведения об обнаруженных обновлениях

В **«Обновлениях устройств»** - пары «устройство - обновление» с признаком **«Требуется установка»** и ссылкой на последнее сканирование

Примечание

Повторная успешная проверка обновляет потребность устройства в рамках выбранного каталога. Записи других каталогов при этом не сбрасываются. Если хранятся результаты нескольких каталогов, использовать фильтр по каталогу перед выборочной установкой

Следующий шаг - *подготовить пакеты*

Если сканирование не выполнено

- **Нет подходящих Windows-устройств** - проверить выбранные устройства, состав групп и данные об ОС
- **Выбранная точка распространения отключена** - включить её либо изменить узел выполнения задачи
- **Устройство недоступно или завершилось с ошибкой** - открыть результат устройства и **«Лог исполнения»**, проверить подключение клиента и доступность файла каталога
- **Обновления не найдены** - проверить выбранный каталог и результат устройства

  Успешное сканирование с нулевым результатом означает, что по этому каталогу требуемые обновления не найдены

2.10.2 Пакеты обновлений

Доступны только в UEM версии

Пакеты обновлений - общий список обновлений Windows, найденных при сканировании устройств. Записи создаются по результатам сканирования

Как это работает

В списке доступны название, статьи KB, критичность, количество устройств, размер, статус пакета и связанный файл. Можно искать по названию или Update ID, фильтровать по каталогу, критичности, эксклюзивности и статусу. Карточка содержит описание, категории, ревизию, заменяемые обновления, ссылки загрузки и сведения о требовании перезагрузки

На вкладке **«Пакет»** задаётся файл для установки и отображается ошибка скачивания

Автоматическое скачивание

1. Выбрать **«Скачать пакет»** у нужного обновления или отметить несколько строк и выполнить **«Скачать пакеты обновлений»**
2. Дождаться перехода статуса из **«В очереди»** / **«Скачивается»** в **«Готов»**
3. Убедиться, что в поле **«Пакет обновления»** появился файл

Скачивание использует ссылки, полученные вместе со сведениями об обновлении. Если ссылок нет или загрузка завершилась ошибкой, открыть поле **«Ошибка скачивания»** и подготовить пакет вручную

Пакет из одного файла сохраняется как есть (**MSU**, **CAB** или **EXE**). Пакет из нескольких файлов собирается в ZIP-архив с исходными именами файлов

Файл сохраняется в репозиторий из настройки Репозиторий для пакетов обновлений того же блока. Свободное место в нём проверяется до скачивания: при нехватке в поле **«Ошибка скачивания»** указываются требуемый и доступный объём

Размер пакета ограничен настройкой Максимальный размер пакета обновления, ГБ в блоке **«Обновления ОС»** *настроек сервера* (по умолчанию 5 ГБ). Пакет крупнее предела отклоняется сразу, без скачивания: в поле **«Ошибка скачивания»** указываются размер пакета и действующий предел. Для таких пакетов увеличить предел или задать `0`, чтобы снять ограничение

Ручная загрузка

1. Подготовить файл, соответствующий выбранному обновлению и целевой системе
2. Открыть карточку обновления, вкладку **«Пакет»**
3. В поле **«Пакет обновления»** загрузить файл или выбрать его из хранилища
4. Сохранить карточку

Поддерживаются файлы **MSU**, **CAB**, **EXE** и **ZIP** с файлами обновления

Примечание

После привязки файла пакет получает статус **«Готов»**. Этот статус означает готовность файла к передаче; результат установки проверяется отдельно на каждом устройстве

Важно

Если обновление состоит из нескольких файлов, в пакете должны присутствовать все требуемые файлы с исходными именами. В ZIP-архиве они должны находиться в корне. Сообщение **«В пакете отсутствует файл»** означает, что установщик не нашёл ожидаемый файл: проверить состав пакета и имена файлов

Подсказка

После повторного сканирования статус может вернуться в **«Не скачан»** с сообщением **«Состав пакета изменился; скачайте обновление повторно»**. В этом случае подготовить пакет заново перед установкой

Важно

При работе в закрытой сети заранее подготовить все необходимые пакеты

Задача установки пытается скачать отсутствующие пакеты автоматически

Если подготовить хотя бы один необходимый пакет не удалось, задача завершается ошибкой до запуска установки на устройствах

После подготовки перейти к *установке обновлений*

Как читать статус пакета

- **«Не скачан»** - файл не подготовлен; скачать пакет или привязать его вручную
- **«В очереди»** - запрос на скачивание принят и ожидает обработки
- **«Скачивается»** - загрузка выполняется; дождаться завершения
- **«Готов»** - файл привязан к обновлению и может использоваться задачей установки
- **«Ошибка»** - открыть **«Ошибка скачивания»**, устранить причину и повторить скачивание либо загрузить файл вручную

У обновления с привязанным файлом действие **«Скачать пакет»** недоступно. Для замены вручную загруженного файла выбрать другой в поле **«Пакет обновления»** и сохранить карточку

2.10.3 Установка обновлений

Доступна только в UEM версии

Как это работает

Установка использует потребности, полученные при сканировании устройств. Перед запуском RuDesktop проверяет готовность пакетов и пытается скачать отсутствующие файлы. Затем выполняет установку и сохраняет результаты по каждому устройству

Выборочная установка

1. Открыть **«Обновления ОС → Обновления устройств»**
2. Отфильтровать записи по **«Требуется установка»** и при необходимости по каталогу
3. Выбрать нужные пары «устройство - обновление» и выполнить **«Установить»**
4. Открыть созданную задачу в **«Задачах установки обновлений»**
5. Проверить ход выполнения и результаты устройств

Действие создаёт задачу только для выбранных требуемых обновлений и сразу ставит её в очередь. Помимо права изменения обновлений устройств, пользователю нужно право добавления задач установки обновлений

Установка на выбранные устройства и группы

1. Открыть **«Задачи установки обновлений»** и добавить задачу
2. Указать **«Название»** и **«Точку распространения»**: автоматически, основной сервер или конкретную точку
3. На вкладке **«Устройства»** выбрать устройства, группы или динамические группы
4. Сохранить и выполнить **«Запустить задачу»**

Такая задача устанавливает все обновления, которые сейчас отмечены как требуемые для выбранных Windows-устройств. Для установки конкретных обновлений использовать выборочное действие из предыдущего раздела. Устройства без требуемых обновлений пропускаются

Важно

У общей задачи нет фильтра по каталогу: она использует все сохранённые требуемые обновления выбранных устройств. Если нужно ограничиться одним каталогом, отфильтровать **«Обновления устройств»** и выполнить выборочную установку

Для автоматического запуска включить **«Запускать по расписанию»** и задать периодичность. Задачи сканирования и установки имеют отдельные расписания: сначала должно завершиться сканирование, затем можно выполнять установку по обновлённым результатам

Проверка результата и перезагрузка

На вкладке **«Состояние»** доступны общий статус, время выполнения, счётчики и последняя ошибка. Статус **«Выполнено с ошибками»** требует проверки отдельных устройств, даже если часть обновлений установлена успешно. В результатах устройств отображаются количество установленных обновлений, признак **«Требуется перезагрузка»** и ошибка. Подробности доступны в **«Логе исполнения»**

Важно

Офлайн-установка фиксирует требование перезагрузки, но не выполняет её автоматически. Если перезагрузка требуется, выполнить её отдельно в согласованное время, затем повторить сканирование для проверки оставшихся обновлений

- Счётчики **«Успешно»**, **«Пропущено»** и **«Ошибки»** в задаче относятся к устройствам

- Количество установленных обновлений показано отдельно в результате каждого устройства
- **«Прогресс»** в списке задач показывает число завершённых результатов устройств из общего числа. Завершённый результат может быть успешным, пропущенным или ошибочным

Подсказка

Одно устройство с пятью установленными обновлениями даёт один успешный результат задачи

Статусы задачи

Статус	Что означает
Новая	Задача создана, запуск ещё не поставлен в очередь
В очереди	Запуск ожидает обработки Повторно запускать эту же задачу не требуется
Выполняется	Идёт подготовка или обработка устройств; окончательного результата ещё нет
Выполнено	Обработка завершена без ошибок Пропущенные устройства тоже допустимы, поэтому статус не означает, что на каждом устройстве установлены обновления
Выполнено с ошибками	Есть ошибки или недоступные устройства, а также успешные либо пропущенные результаты Проверить строки устройств и журнал
Ошибка	Не удалось подготовить запуск либо все результаты устройств завершились ошибкой или недоступностью Причина указана в состоянии и журнале

Эти общие статусы используются и для задач сканирования

Повторный запуск и расписание

Пока задача в очереди или выполняется, повторный ручной запуск не создаёт ещё одно выполнение той же задачи. После завершения её можно запустить снова

Примечание

Результаты устройств в карточке задачи заменяются результатами нового запуска; перед повторением сохранить нужные сведения о предыдущих ошибках. Снятие **«Запускать по расписанию»** отключает будущие плановые запуски, но не отменяет уже поставленное в очередь или выполняющееся задание. В карточке задачи обновления действие остановки не предусмотрено

Если установка не выполнена

- **Не удалось подготовить пакеты** - проверить статусы и ошибки в *Пакетах обновлений*; при необходимости загрузить файлы вручную
- **Пропущено** - проверить, есть ли у устройства требуемые обновления по последнему сканированию и входят ли они в выборочную задачу

  Этот статус также возможен, если при повторной проверке перед установкой все выбранные обновления оказались уже установленными или неприменимыми
- **Недоступно** - проверить подключение устройства и выбранный узел выполнения
- **Ошибка установки** - открыть результат устройства и журнал, проверить сообщение Windows и соответствие загруженного пакета обновлению

Для ошибки `0x80240016` журнал сообщает о другой выполняющейся установке или необходимости перезагрузки. Дождаться завершения установки либо перезагрузить устройство, затем повторить попытку. После устранения причины повторить сканирование и запустить установку оставшихся требуемых обновлений

2.10.4 Как это работает

1. Администратор добавляет файл `Wsusscn2.cab` в **«Каталоги обновлений Windows»**
2. **«Задача сканирования обновлений»** проверяет выбранные Windows-устройства по этому каталогу
3. Результаты появляются в **«Пакетах обновлений»** и **«Обновлениях устройств»**
4. Администратор подготавливает файлы нужных пакетов: скачивает их через сервер либо загружает вручную
5. **«Задача установки обновлений»** устанавливает подготовленные обновления на выбранные устройства

Примечание

Каталог содержит сведения для поиска обновлений. Для установки нужны отдельные файлы пакетов; загрузка одного CAB-каталога их не заменяет

2.10.5 Подготовка

Нужны лицензия UEM, права на соответствующие объекты раздела и Windows-устройства с подключённым клиентом RuDesktop. Устройства должны получать файлы из инфраструктуры сервера, а выбранная точка распространения должна быть включена и доступна для выполнения задач

Для автоматического скачивания пакетов исполняющему узлу нужен доступ к источникам загрузки. В закрытой сети заранее перенести каталог и пакеты в хранилище RuDesktop и выбрать их в соответствующих карточках

2.10.6 Страницы раздела

- *Каталог и сканирование* - подготовка каталога, выбор устройств, запуск и просмотр результата поиска
- *Пакеты обновлений* - скачивание и ручная загрузка пакетов
- *Установка обновлений* - выборочная установка, задачи для групп устройств, расписание и проверка результатов

Пошаговый пример: Обновление Windows в закрытой сети

См. также

Политика *Обновление ОС* выполняет обновление Windows, Linux и macOS через источники обновлений соответствующей ОС. Этот раздел описывает отдельный сценарий офлайн-обновления Windows

2.11 Организация

2.11.1 Структура

Структура — это страница, предназначенная для отображения групп, устройств и доменов сервера **RuDesktop** в виде единого дерева

Подсказка

Страница **«Структура»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Как это работает

Страница отображает все группы и устройства сервера **RuDesktop** в виде дерева. Дерево строится из двух источников:

- **локальных групп** сервера — это те же группы, что отображаются на странице *Группы*;
- **доменных групп**, импортированных через *интеграцию с LDAP* или Keycloak

Локальные группы собраны под единым служебным корнем Локальные объекты. Внутри него на свежеустановленном сервере уже создано две вложенные папки-контейнера:

- Права доступа — контейнер с **предустановленными группами-ролями**, которые поставляются вместе с сервером и нужны, чтобы быстро выдать пользователю стандартный набор прав. По умолчанию внутри этого узла находятся:
  - Администратор
  - Руководитель подразделения

  - Сотрудник поддержки
  - Гость
  - Без доступа

  Каждая из этих папок — обычная локальная группа, права которой настраиваются на вкладке Права в её *свойствах*. Название контейнера историческое: он сгруппировал ролевые группы, заранее настроенные «под права». При создании собственных групп их можно как помещать сюда, так и хранить вне него

- Мои группы — пустой контейнер для **собственных групп**, которые администратор создаёт сам (например, по подразделениям, локациям или назначению устройств)

Важно

«Право» в **RuDesktop** не является самостоятельным объектом — права всегда задаются у группы (на её вкладке Права) и наследуются её участниками. Узел Права доступа в дереве — это **не отдельная сущность прав**, а служебная папка с группами-ролями, которые поставляются в комплекте

Доменные группы располагаются под отдельным корневым узлом с именем домена и появляются в дереве только после настройки *интеграции с LDAP* или Keycloak

При выборе узла в иерархии в правой части отображаются устройства и подгруппы, входящие в выбранную группу. Из контекстного меню устройства можно перейти к его свойствам, истории, сессиям, логам, графу связей или подключиться к нему — без перехода на другие страницы

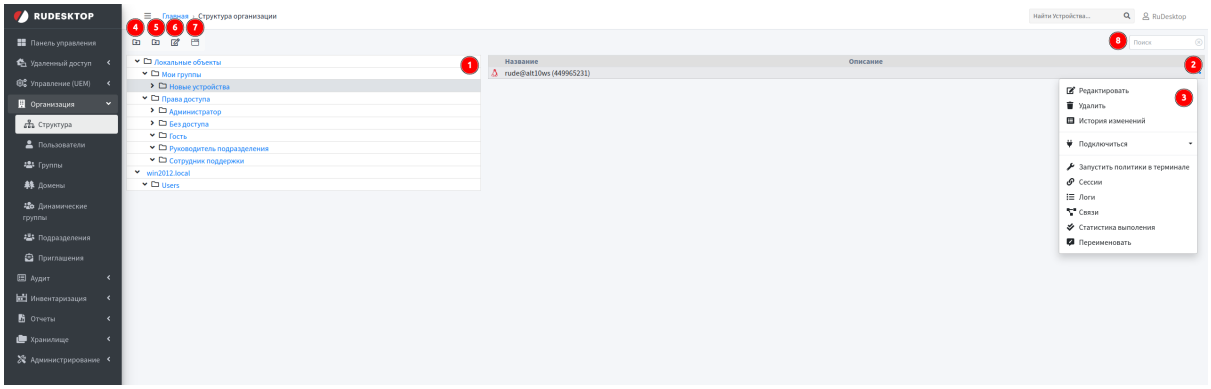
Прикладное значение

Страница используется для:

- **просмотра реальной структуры организации** — все локальные группы (включая ролевые из Права доступа и пользовательские в Мои группы) и доменные группы в одном дереве;
- **проверки того, что увидит конечный пользователь в клиенте RuDesktop** — клиент строит дерево доступных устройств по той же иерархии локальных групп, поэтому изменения здесь напрямую отражаются в окне клиента;
- **быстрой навигации по устройству** через контекстное меню — переход к свойствам, истории, сессиям, логам, графу связей или подключение к устройству без перехода на отдельные страницы

Описание страницы

На странице **Структура** отображено:



1. Иерархия
2. Устройства
3. Меню действий
4. Кнопка **«Создать группу»**
5. Кнопка **«Удалить группу»**
6. Кнопка **«Редактировать группу»**
7. Кнопка **«Свойства объекта»**
8. Поиск

Подсказка

В зависимости от прав некоторые кнопки могут отсутствовать

Иерархия

Дерево групп и устройств. Корневые узлы:

- Локальные объекты — все локальные группы сервера **RuDesktop**. На свежей инсталляции внутри уже есть служебные подузлы:
  - Права доступа — папка с предустановленными группами-ролями (Администратор, Руководитель подразделения, Сотрудник поддержки, Гость, Без доступа). Это обычные группы с заранее настроенными правами, не отдельный тип объектов
  - Мои группы — пустой контейнер для собственных групп администратора
- доменные узлы — корневые папки доменов из *интеграции с LDAP* или Keycloak; отображаются только при наличии настроенной интеграции

Устройства

Устройства и подгруппы, принадлежащие выбранной группе

Важно

При выборе домена отображаются группы домена, пользователи и устройства. Столбец **«Описание»** заполняется только у доменных записей

Меню действий

Важно

Данное меню отсутствует у доменных записей

Доступные действия:

1. Редактировать — при выборе этого пункта откроются свойства устройства. Подробнее о *свойствах устройства*
2. Удалить — при выборе этого пункта устройство будет удалено из группы
3. История изменений — при выборе этого пункта будет отображена история устройства: создание/редактирование и пользователь, который выполнил данные операции
4. Подключиться — подключение к рабочему столу устройства, передача файлов, доступ к терминалу, настройка TCP-туннелирования, RDP-подключение, проброс USB или удалённое включение по Wake-on-LAN
5. Политики — групповое действие, открывающее подменю с возможностью запустить все политики устройства или выбрать конкретную политику для запуска
6. Сессии — при выборе этого пункта произойдет переход на страницу **«Сессии»** с активным фильтром по этому устройству
7. Логи — при выборе этого пункта произойдет переход на страницу **«Логи исполнения»** с активным фильтром по этому устройству
8. Связи — при выборе этого пункта произойдет переход на страницу **«Граф»** с графическим отображением входящих и исходящих соединений на данном устройстве
9. Статистика выполнения — при выборе этого пункта произойдет переход на страницу *Статистика выполнения* с отображением статистики выполнения задач на данном устройстве
10. Поделиться устройством — формирование ссылки на устройство для совместного доступа
11. Переименовать — при выборе этого пункта появится всплывающее окно с возможностью задать псевдоним устройству

Подсказка

Если переименовать устройство, его псевдоним отобразится также на странице **«Устройства»**

Важно

В зависимости от прав пользователя, типа устройства и его текущего состояния отдельные действия могут быть недоступны или скрыты

Создание новой группы

Для создания новой группы необходимо:

1. Выбрать группу из существующих, в которой хотите создать новую группу
2. Нажать на кнопку `Создать группу`
3. Ввести уникальное имя группы
4. Нажать на кнопку Подтвердить

Новая группа будет успешно создана

Важно

Группе, созданной таким способом, по умолчанию не выдаются права

Для назначения прав необходимо перейти на страницу **«Группы»**, выбрать созданную группу и назначить ей права вручную

Удаление группы

Для удаления группы необходимо:

1. Выбрать группу, которую хотите удалить
2. Нажать на кнопку `Удалить группу`
3. В появившемся окне нажать на кнопку Подтвердить

Группа будет успешно удалена

Подсказка

Если в группу были добавлены устройства, то после её удаления у устройств также удалится привязка к этой группе

Редактирование группы

Для переименования группы необходимо:

1. Выбрать группу, которую хотите переименовать
2. Нажать на кнопку `Редактировать группу`
3. В появившемся окне ввести новое название группы
4. Нажать на кнопку Подтвердить

Группа будет успешно переименована

Свойства объекта

Для открытия свойств группы необходимо:

1. Выбрать группу
2. Нажать на кнопку `Свойства объекта`

Откроется страница со свойствами группы. Подробнее о *свойствах группы*

Поиск

Для поиска устройства в группах необходимо:

1. Выбрать группу, в которой хотите выполнить поиск
2. В поле `Поиск` ввести имя пользователя или имя устройства

После ввода значения в блоке **«Устройства»** отобразятся найденные устройства

Подсказка

Поиск осуществляется только в рамках выбранной группы или подгруппы

2.11.2 Пользователи

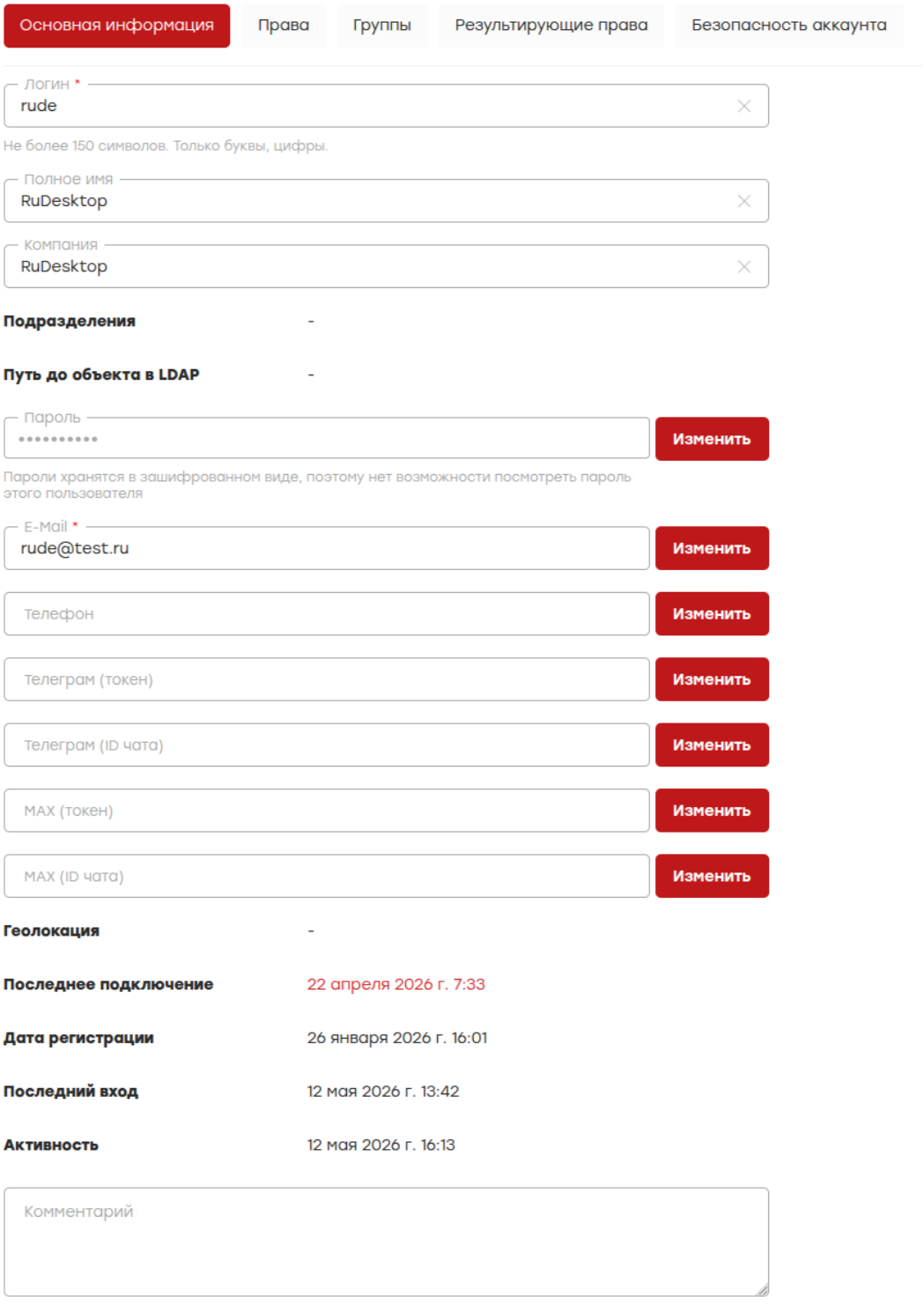
Свойства пользователя

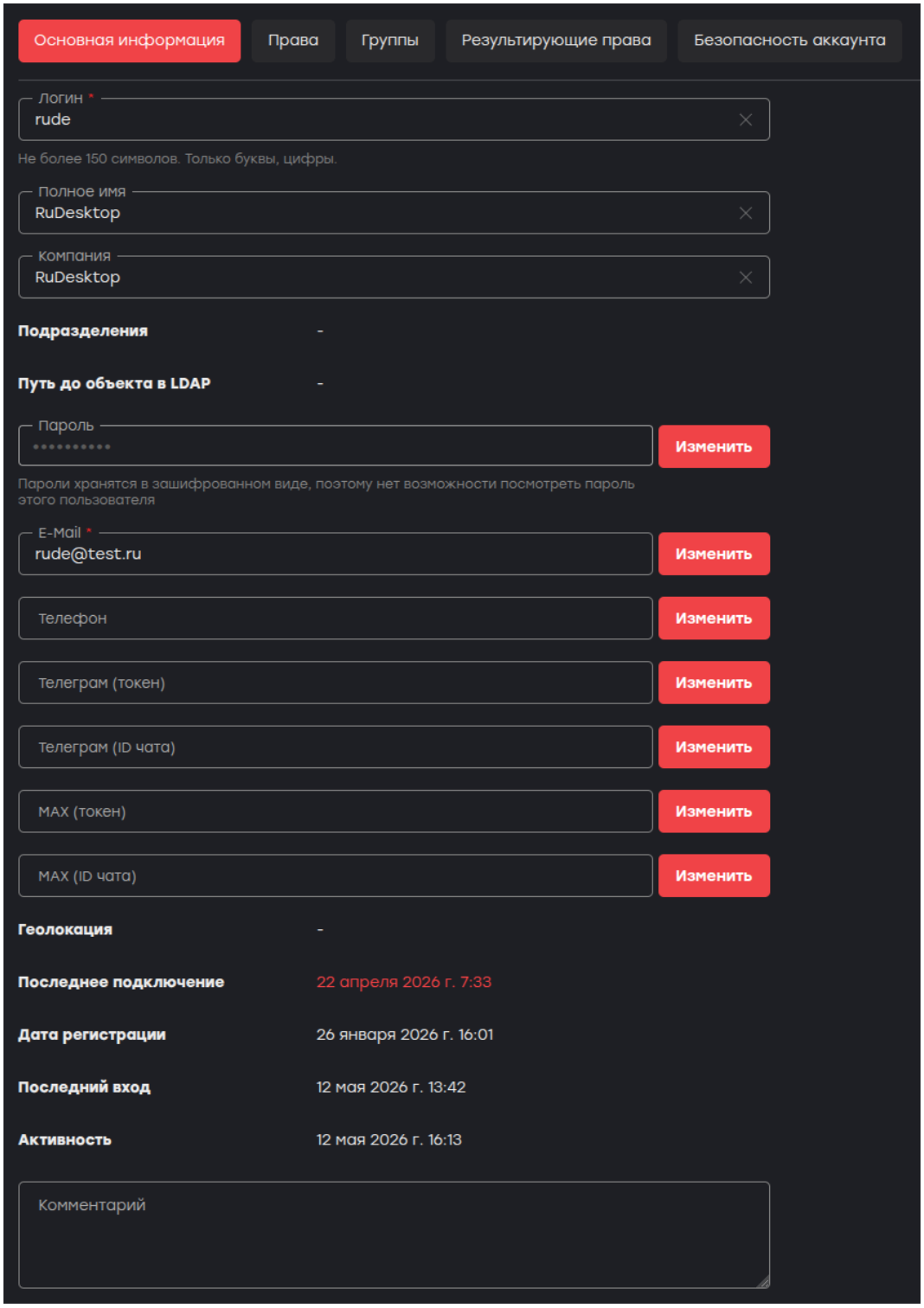
Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств

Основная информация

Доступные поля во вкладке Основная информация:


Основная информация
Права
Группы
Результирующие права
Безопасность аккаунта
Логин *
rude
Не более 150 символов. Только буквы, цифры.
Полное имя
RuDesktop
Компания
RuDesktop
Подразделения
-
Путь до объекта в LDAP
-
Пароль
••••••••••
Изменить
Пароли хранятся в зашифрованном виде, поэтому нет возможности посмотреть пароль этого пользователя
E-Mail *
rude@test.ru
Изменить
Телефон
Изменить
Телеграм (токен)
Изменить
Телеграм (ID чата)
Изменить
MAX (токен)
Изменить
MAX (ID чата)
Изменить
Геолокация
-
Последнее подключение
22 апреля 2026 г. 7:33
Дата регистрации
26 января 2026 г. 16:01
Последний вход
12 мая 2026 г. 13:42
Активность
12 мая 2026 г. 16:13
Комментарий



1. Логин — уникальный идентификатор пользователя, используемый для аутентификации при входе в систему или приложение
2. Полное имя — полное указание имени пользователя, включающее его имя, фамилию и, при необходимости, отчество
3. Компания — информация о том, к какой компании принадлежит пользователь
4. Подразделения — информация о том, к каким подразделениям

принадлежит пользователь

Важно

Поле отображается только при наличии права *Подразделения → Просмотр*

5. Путь до объекта в LDAP — информация о том, по какому пути в LDAP находится пользователь

Важно

Поле отображается только суперпользователю

6. Пароль — пароль пользователя

Подсказка

- Пароль не должен быть слишком похож на другую вашу личную информацию
- Пароль должен содержать как минимум 8 символов
- Пароль не должен быть слишком простым и распространенным

7. E-Mail — адрес электронной почты пользователя

Подсказка

E-Mail можно использовать в качестве логина для авторизации

8. Телефон — номер телефона пользователя

Подсказка

Один номер телефона можно привязать только к одной учётной записи

9. Телеграм (токен) — токен пользователя в Телеграм
10. Телеграм (ID чата) — ID чата в Телеграм для отправки уведомлений
11. MAX (токен) — токен пользователя в мессенджере **MAX**
12. MAX (ID чата) — ID чата в мессенджере **MAX** для отправки уведомлений

Подсказка

E-Mail, телефон, Telegram и MAX предназначены:

- Для двухфакторной аутентификации
- Для получения уведомлений

13. Геолокация — местоположение пользователя
14. Последнее подключение — дата последнего подключения к удаленному устройству

Подсказка

Данная информация отобразится только в том случае, если был выполнен вход под пользователем в клиенте **RuDesktop** и после этого было выполнено подключение к удаленному устройству

15. Дата регистрации — дата регистрации или создания пользователя на сервере **RuDesktop**
16. Последний вход — дата, когда пользователь в последний раз авторизовался на сервере **RuDesktop**
17. Активность — дата и время последней активности пользователя в веб-интерфейсе сервера **RuDesktop**
18. Комментарий — поле предназначено для оставления заметок
19. Согласие на обработку персональных данных — отметка, указывающая, что пользователь дал согласие на обработку персональных данных
20. Согласие на получение информационных рассылок — отметка, указывающая, что пользователь дал согласие на получение информационных рассылок

Права

Доступные поля во вкладке Права:

1. Активный — отметьте, чтобы пользователь мог войти в систему. Снятие отметки запрещает авторизацию без удаления учётной записи
2. Статус персонала — даёт пользователю доступ к административной панели **RuDesktop**
3. Статус суперпользователя — даёт пользователю все права без явного назначения

> **Важно**
>
> Изменять флаги Статус персонала и Статус суперпользователя может только суперпользователь

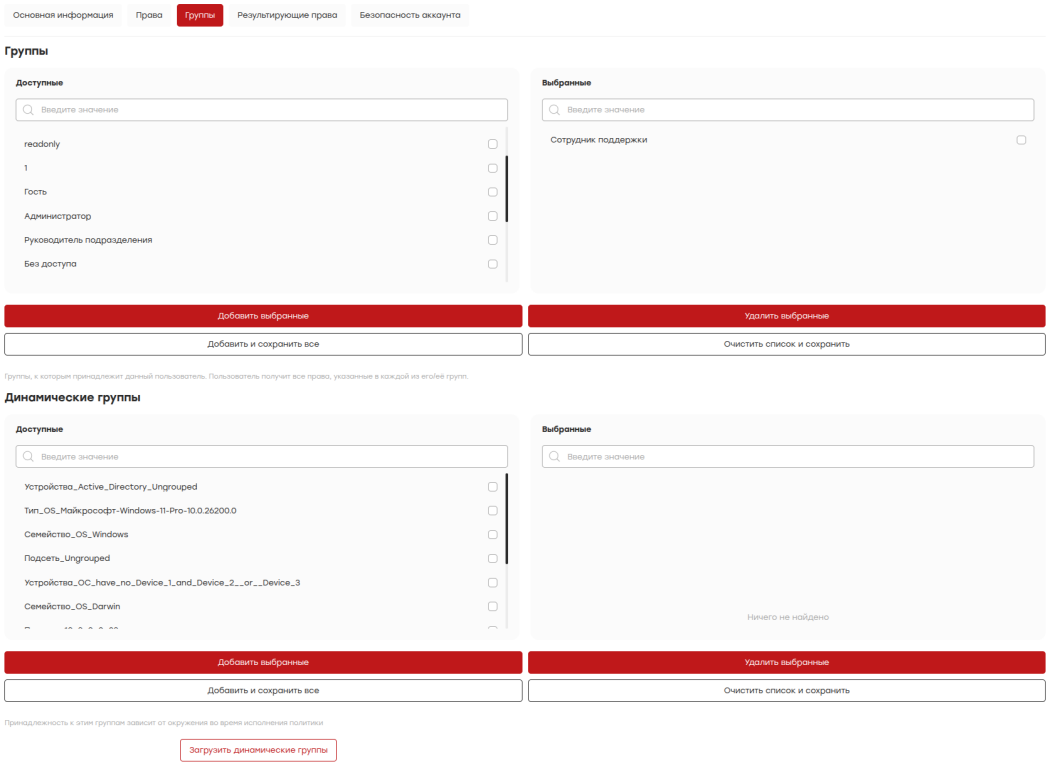
4. Права пользователя — индивидуальные права, выдаваемые конкретному пользователю в дополнение к правам, унаследованным от групп

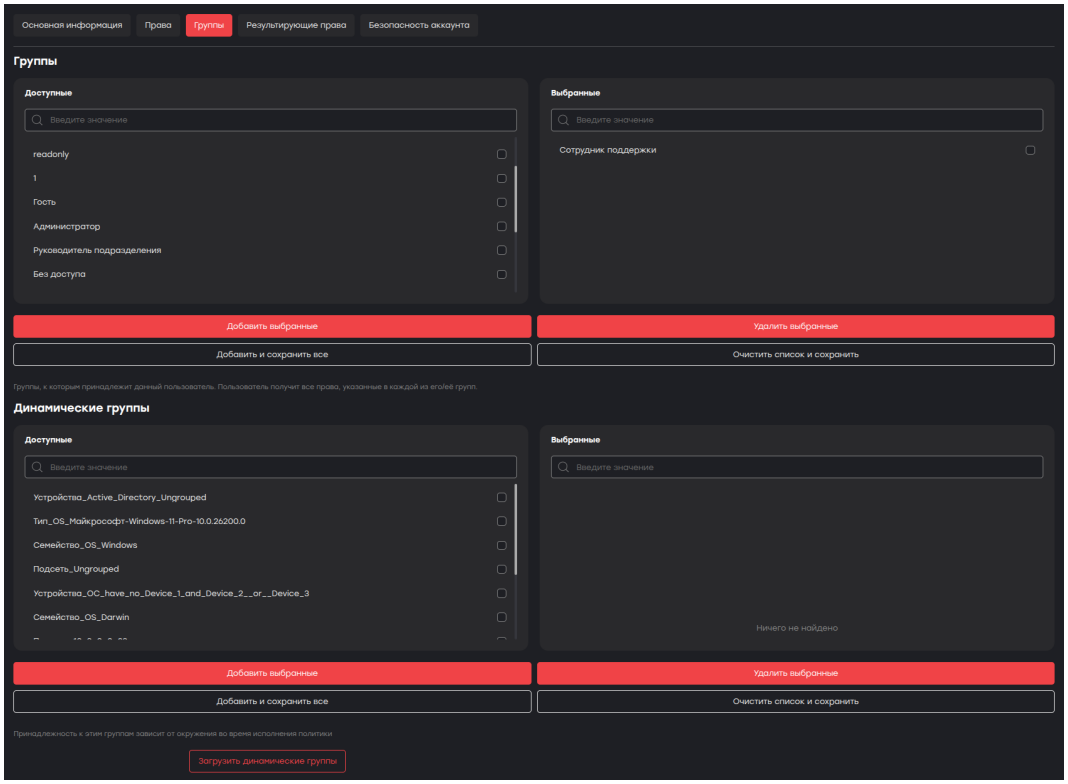
Подробнее о правах см. *Права пользователя*

Группы

Кнопка Импорт в списке групп позволяет добавить группы из файла по их названиям. Существующий выбор сохраняется, изменения применяются при сохранении пользователя. Подробнее: *Импорт записей в списки выбора*

Доступные поля во вкладке Группы:





На данной вкладке размещена таблица добавления пользователя в группы

Таблица разделена на 2 блока:

1. Доступные группы
2. Выбранные группы

Для добавления пользователя в группу необходимо кликнуть в блоке **«Доступные группы»** на необходимую группу и далее кликнуть на между блоков или двойным кликом по названию группы, после чего в меню действий нажать на кнопку Сохранить или Сохранить и продолжить

Примечание

Пользователя можно добавлять в неограниченное количество групп

Примечание

Помимо поштучного добавления доступны массовые действия над всем списком — кнопки Добавить и сохранить все и Очистить список и сохранить. Они доступны только

после сохранения записи. При большом количестве элементов действие выполняется в фоновом режиме: отображается индикатор прогресса со счётчиком и кнопка Отменить задачу, а списки блокируются до завершения операции

На вкладке также отображается поле Динамические группы — список загруженных динамических групп, в которые входит пользователь. Принадлежность к этим группам определяется автоматически и зависит от окружения во время исполнения политики

LDAP

Доступные поля во вкладке LDAP:

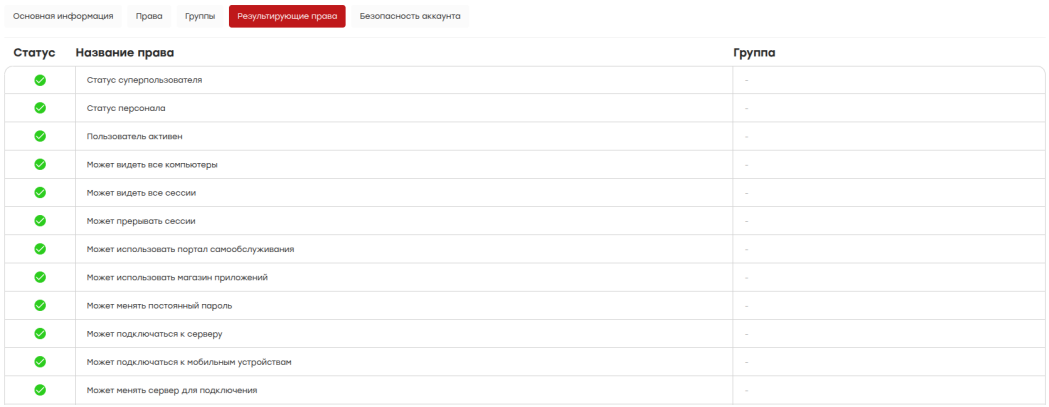
1. LDAP объект — атрибуты пользователя, полученные из домена при последней синхронизации

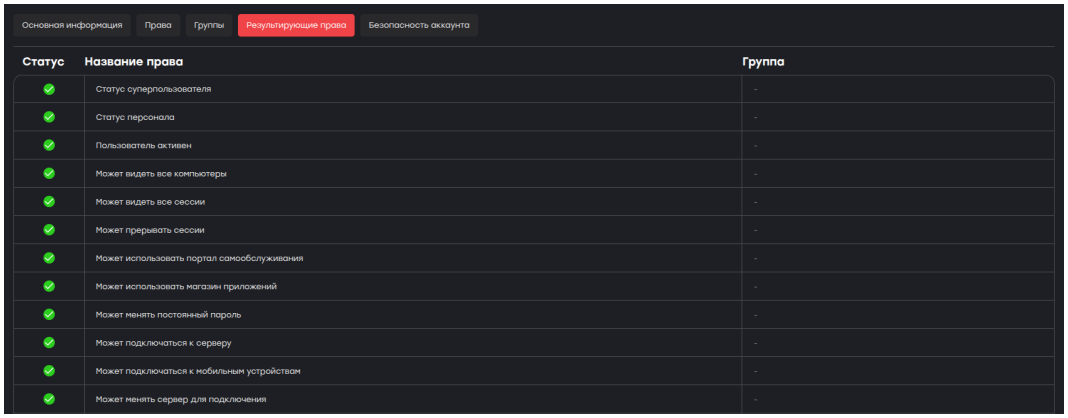
Примечание

Вкладка содержит данные только у пользователей, импортированных из домена. Для локальных пользователей блок остаётся пустым

Результирующие права

Вкладка отображает итоговый список прав, которыми обладает пользователь, с учётом унаследованных от групп прав, индивидуальных прав и статуса суперпользователя



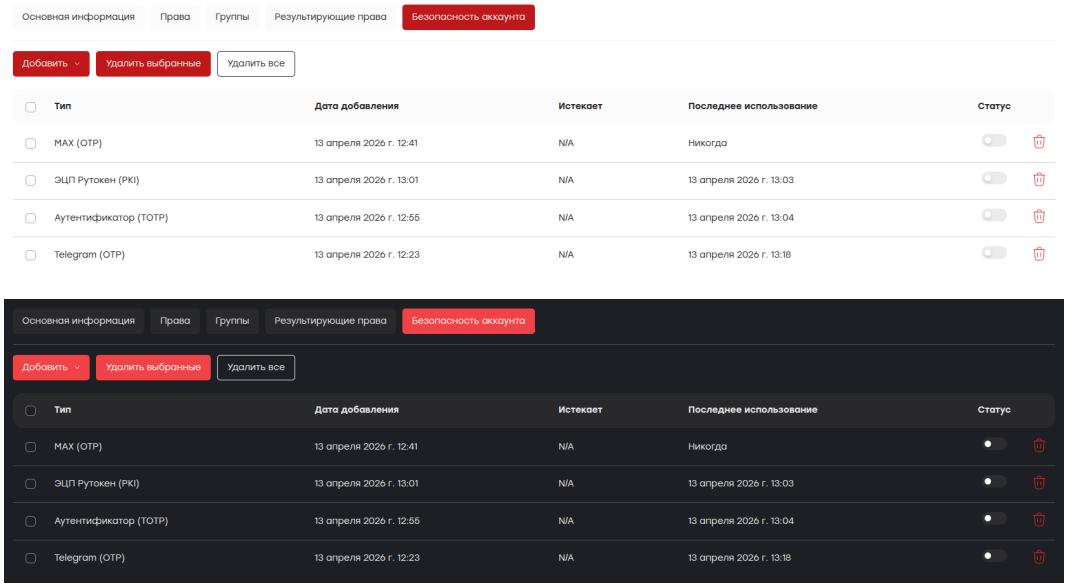


Примечание

Вкладка доступна только для просмотра — изменить права можно во вкладке Права или через *Группы*

Безопасность аккаунта

На вкладке отображается состояние двухфакторной аутентификации пользователя и доступные действия по её настройке или сбросу

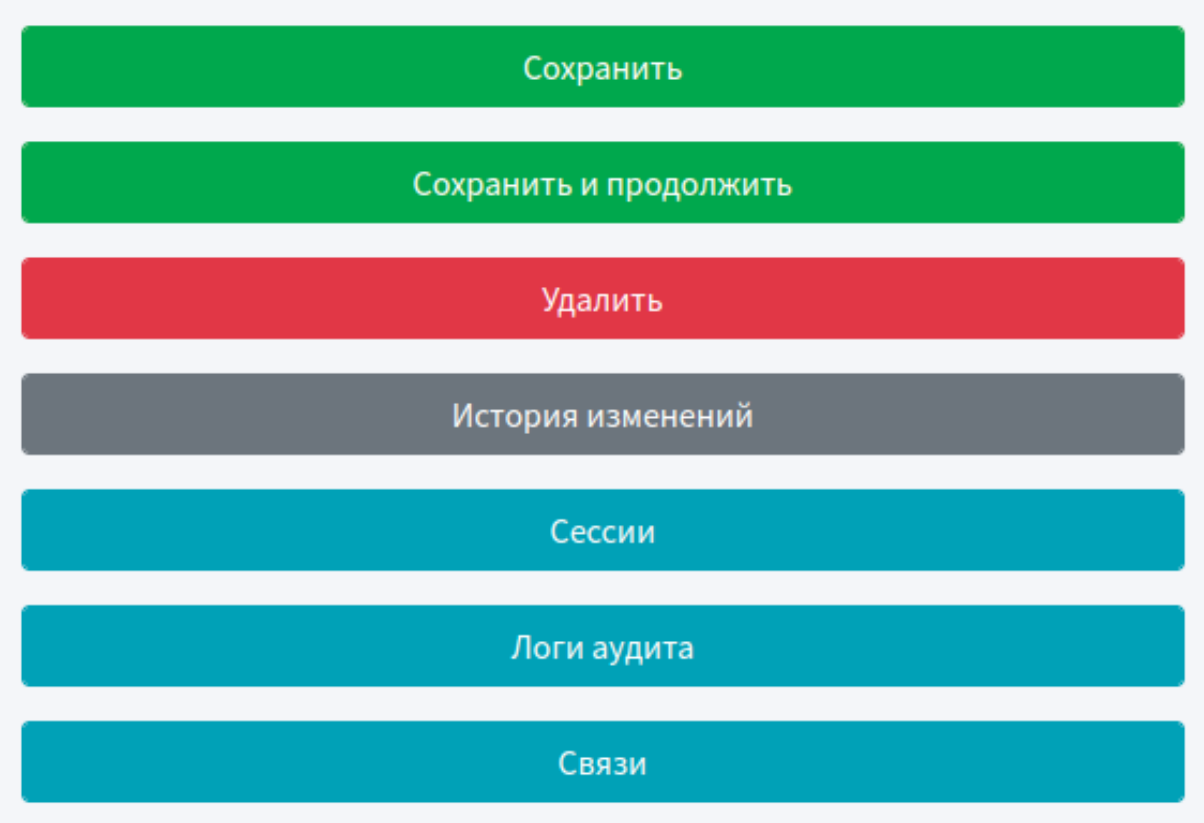


Важно

Вкладка отображается только пользователям, у которых есть права на изменение настроек безопасности

Меню действий

Меню действий расположено на всех вкладках страницы свойств



Имеет следующие возможности:

1. Сохранить - производит сохранение внесенных изменений и перенаправляет на страницу **«Пользователи»**
2. Сохранить и продолжить - производит сохранение внесенных изменений и позволяет остаться на странице свойств для выполнения дальнейших операций
3. Удалить - производит удаление пользователя и перенаправляет на страницу **«Пользователи»**

> **Примечание**
>
> 1. После нажатия на кнопку Удалить откроется страница подтверждения удаления пользователя
> 2. После подтверждения удаления пользователя произойдет переход на страницу **«Пользователи»** и появится уведомление Пользователь был успешно удален

4. История изменений - отображает все изменения, выполненные для этого пользователя
5. Сессии - отображает сессии, которые были запущены на этом пользователе
6. Логи аудита - отображает логи, связанные с этим пользователем
7. Связи - графически отображает входящие и исходящие соединения

8. Безопасность аккаунта - открывает страницу управления многофакторной аутентификацией пользователя

> **Важно**
>
> Кнопка отображается только пользователям, у которых есть права на изменение настроек безопасности

Права пользователя

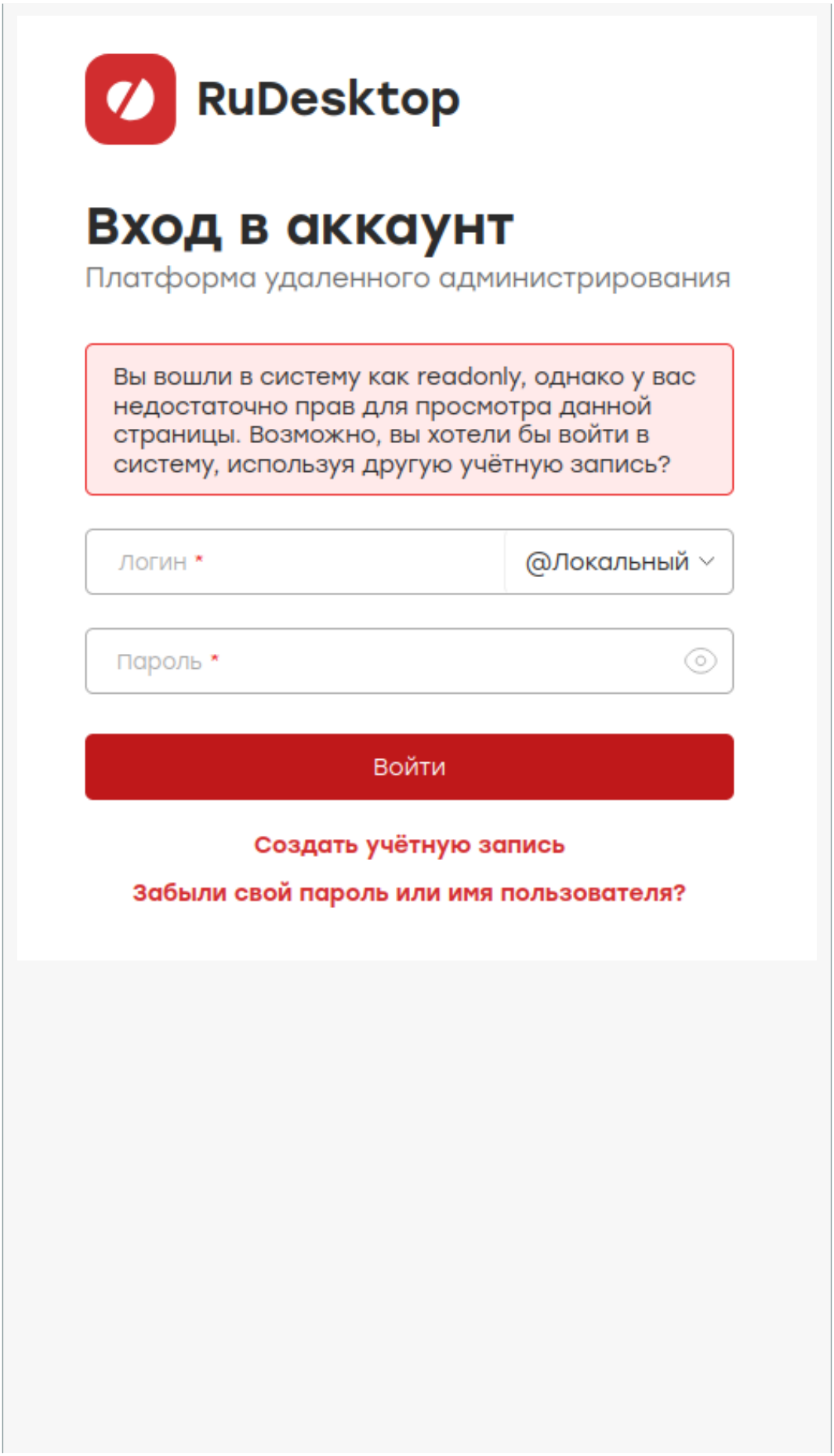
Порядок поиска и массового выбора прав описан на странице *Права группы*

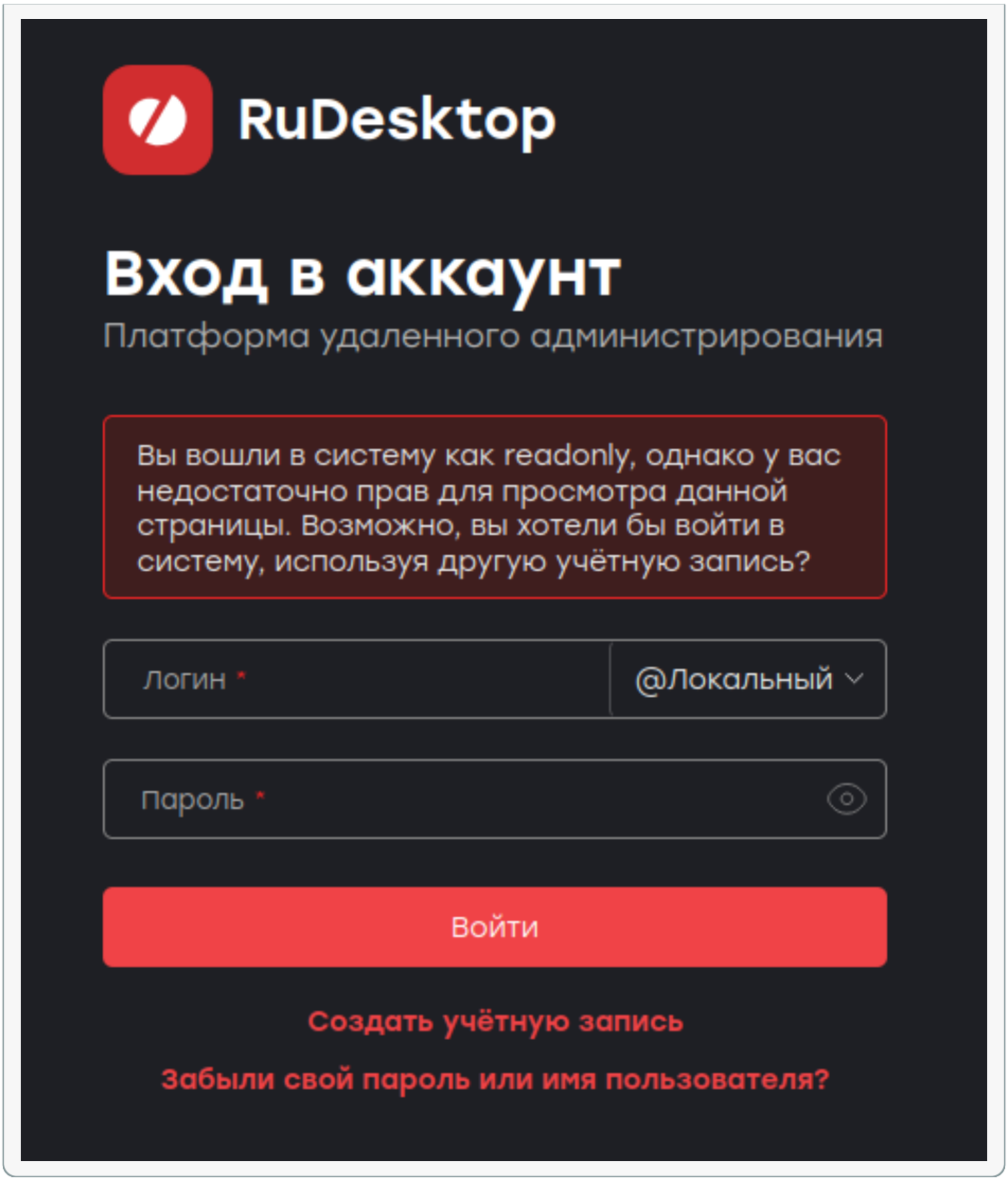
> **Примечание**
>
> Индивидуальные права дополняют права групп пользователя. Снятие индивидуального флажка не отменяет право, полученное через группу

Активный — флаг в этом поле активирует или деактивирует пользователя

Статус персонала — флаг в этом поле дает возможность пользователю авторизовываться в веб-интерфейсе сервера

> **Подсказка**
>
> Если флаг Статус персонала отсутствует, при попытке авторизоваться в веб-интерфейсе сервера появится ошибка


RuDesktop
Вход в аккаунт
Платформа удаленного администрирования
Вы вошли в систему как readonly, однако у вас недостаточно прав для просмотра данной страницы. Возможно, вы хотели бы войти в систему, используя другую учётную запись?
Логин *
@Локальный
Пароль *
Войти
Создать учётную запись
Забыли свой пароль или имя пользователя?



Статус суперпользователя — флаг в этом поле дает пользователю все права без явного их назначения и снимает фильтры видимости объектов

Что получает пользователь со статусом суперпользователя

Помимо всех CRUD-прав суперпользователь обходит фильтры видимости и получает доступ к разделам и действиям, недоступным обычным пользователям ни через какие комбинации прав

Полная видимость объектов на сервере

- все учётные записи на странице *Пользователи* (без ограничения подразделением и группами)
- все устройства на странице *Устройства*
- все сессии на странице *Сессии*

- все пригласительные ссылки на странице *Пригласительные ссылки*
- вся адресная книга — адреса всех пользователей сервера

Страницы, доступные только суперпользователю

- *QR-коды MDM* — отдельных прав на этот раздел не предусмотрено, страница доступна только при активном статусе суперпользователя
- вкладки **Доступные устройства к подключению** (список ACL устройства) и **Подключение** (служебные параметры подключения) в *свойствах устройства*

Действия, доступные только суперпользователю

- **Назначить статусы пользователям** — массовое назначение флагов Активный, Статус персонала, Статус суперпользователя через действие в списке пользователей
- редактирование флагов Активный, Статус персонала, Статус суперпользователя в карточке другого пользователя
- редактирование пароля других пользователей (для собственного пароля право не нужно)
- редактирование поля Доступ в свойствах сессии (для остальных пользователей оно read-only)
- изменение настроек **Удалённый мониторинг** и **Передача файлов** в группах

Дополнительные поля и фильтры

- в карточке пользователя — поля Комментарий, Путь до объекта в LDAP, Геолокация, Статус телефона, вкладка LDAP
- в карточке устройства — поля UUID, Путь до объекта в LDAP
- фильтры по флагам Активный, Статус персонала, Статус суперпользователя, Двухфакторная авторизация, Последний вход, Последняя активность, Телефон, E-Mail, Имя пользователя, Путь до объекта в LDAP, Компания в списке пользователей
- фильтры по правам, группам, UUID, пути до объекта в LDAP, фактам в списке устройств

Прочее

- предупреждение о ненастроенных *Доступах* при пустом списке ACL — показывается только суперпользователю

Важно

Статус суперпользователя следует выдавать только узкому кругу администраторов сервера. Для разграничения доступа в большинстве случаев достаточно комбинации *групповых прав* и доступов

Права доступа

Устройства

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Устройства* и видеть список устройств без возможности редактирования
- **Создание** — флаг в этом поле дает возможность пользователю добавлять записи устройств
- **Изменение** — флаг в этом поле дает возможность пользователю изменять псевдоним в *свойствах устройства*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять устройства

Сессии

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Сессии* и видеть список сессий без возможности редактирования
- **Изменение** — флаг в этом поле дает возможность пользователю изменять параметры сессий
- **Удаление** — флаг в этом поле дает возможность пользователю удалять сессии

Доступы

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Доступы* и видеть список доступов без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые доступы*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные доступы*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять доступы

Адресная книга

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Адресные книги*, *Адреса* и *Теги* и видеть список адресных книг, адресов и тегов без возможности создания и редактирования
- **Создание** — флаг в этом поле дает доступ пользователю к добавлению *адресов* и *тегов*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные адреса* и *теги*

- **Удаление** — флаг в этом поле дает возможность пользователю удалять добавленные адреса и теги

Приглашения

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Пригласительные ссылки* и видеть список созданных ссылок без возможности создания и удаления
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *пригласительные ссылки*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять пригласительные ссылки

Подсказка

Изменение существующих пригласительных ссылок в веб-интерфейсе не предусмотрено — для изменения параметров ссылку нужно удалить и создать заново. Объём видимых ссылок дополнительно регулируется правами **Руководитель подразделения** и **Может видеть все пригласительные ссылки**

Пользователи

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Пользователи* и видеть список пользователей без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новых пользователей*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленных пользователей*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять пользователей

Группы

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Группы* и видеть список групп без возможности создания и редактирования. Также открывает вкладку **Группы** в свойствах устройства
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые группы*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные группы*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять группы

Домены

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Домены* и видеть список доменов без возможности создания и редактирования. Также открывает вкладку **LDAP** в свойствах устройства, если у устройства заполнен DN
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые домены*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные домены*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять домены

Подразделения

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Подразделения* и видеть список подразделений без возможности создания и редактирования

> **Подсказка**
>
> Это право также управляет отображением поля Подразделения в *свойствах пользователя* и поля Подразделение в свойствах *адресной книги*

- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые подразделения*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные подразделения*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять подразделения

Политики

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Политики* и *Задачи* и видеть список политик и задач без возможности создания, редактирования и запуска
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *политики* и *задачи*
- **Изменение** — флаг в этом поле дает возможность пользователю изменять добавленные *политики* и *задачи*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять политики и задачи

Динамические группы

Права на просмотр, создание, изменение и удаление динамических групп назначаются отдельно. Право **Создание** также позволяет создать группу из текущего фильтра на странице **Устройства**

Портал

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Обращения* и видеть список обращений без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые обращения*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные обращения*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять обращения

Инвентаризация

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Наличие ресурсов* и *Каталог ресурсов* и видеть список собранных ресурсов с устройств без возможности редактирования и удаления. Также открывает вкладки **Дополнительная информация** и **Факты** в свойствах устройства при наличии собранных фактов
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые ресурсы*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные ресурсы*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять ресурсы

Уведомления

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Уведомления* и видеть список уведомлений без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые уведомления*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные уведомления*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять уведомления

Образы OS

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Образы OS* и видеть список образов ОС без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые образы OS*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные образы OS*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять образы OS

Отчеты

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Шаблоны* и *Готовые отчеты* и видеть список шаблонов и готовых отчетов без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые шаблоны*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные шаблоны*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять шаблоны и готовые отчеты

Файлы

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Репозитории* и *Файлы* и видеть список репозиториев и загруженных файлов без возможности создания, редактирования и загрузки файлов
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *репозитории* и *файлы*
- **Изменение** — флаг в этом поле дает возможность пользователю изменять добавленные *репозитории* и *файлы*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять репозитории и загруженные файлы

Аудит

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Логи исполнения*, *Объекты*, *Входы в систему*, *HTTP запросы*, *Логи сессий* и *Все логи* и видеть список логов

Черный список

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Черный список* и видеть список черных списков без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые черные списки*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные черные списки*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять черные списки

Белый список

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Белый список* и видеть список белых списков без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые белые списки*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные белые списки*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять белые списки

Подсети

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Подсети* и видеть список подсетей без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *подсети* для определения геопозиции устройств по IP-адресу
- **Изменение** — флаг в этом поле дает возможность пользователю изменять параметры существующих подсетей
- **Удаление** — флаг в этом поле дает возможность пользователю удалять подсети

Настройки

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Настройки*, *KeyCloak*, *Мосты* и *Очередь задач* и видеть настройки сервера, список keycloak, мостов и очередь задач без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *keycloak* и *мосты*
- **Изменение** — флаг в этом поле дает возможность пользователю изменять добавленные *keycloak*, *мосты* и *настройки*

- **Удаление** — флаг в этом поле дает возможность пользователю удалять Keycloak, мосты

Дополнительные права доступа

Организация

- Руководитель подразделения — флаг в этом поле расширяет область видимости объектов до всего подразделения пользователя. Без права пользователь видит только свои объекты (плюс объекты, доступные через группы); с правом — объекты любого пользователя своего подразделения

> **Подсказка**
>
> Конкретно при активном праве пользователь дополнительно получает:
>
> - на странице *Пользователи* — все учётные записи своего подразделения
> - на странице *Устройства* — устройства, к которым подключались пользователи подразделения
> - на странице *Сессии* — сессии всех пользователей подразделения
> - на страницах *Адресные книги* и *Адреса* — общие книги своего подразделения (в том числе автоматически созданную общую книгу подразделения) с уровнем доступа **Управление** и их адреса
> - на странице *Пригласительные ссылки* — ссылки, созданные пользователями подразделения
> - действие **Удалить из подразделения** в контекстном меню пользователя
>
> Без права пользователь видит только собственные объекты (личную адресную книгу, сессии, пригласительные ссылки) и объекты, явно доступные ему через группы или доступы

- Просмотр истории изменений объектов — флаг в этом поле дает возможность видеть в *панели управления* виджет последних изменений с записями всех пользователей сервера

> **Подсказка**
>
> Без этого права в виджете последних изменений пользователь видит только собственные действия, а действия других пользователей скрыты

- Просмотр всех пользователей в административной панели — флаг в этом

поле дает возможность видеть всех пользователей, созданных на сервере, на странице *Пользователи*. Без этого права пользователь видит только доступных ему пользователей

- Может настраивать безопасность своего аккаунта — флаг в этом поле дает возможность изменять собственные настройки безопасности, включая параметры двухфакторной авторизации
- Может настраивать безопасность других аккаунтов — флаг в этом поле дает возможность изменять настройки безопасности других пользователей, включая параметры двухфакторной авторизации

Устройства

- Может видеть все компьютеры — флаг в этом поле дает возможность видеть все устройства, подключенные к серверу, на странице *Устройства*
- Может видеть все сессии — флаг в этом поле дает возможность видеть все сессии, зарегистрированные на сервере, на странице *Сессии*
- Может прерывать сессии — флаг в этом поле дает возможность завершать активные удаленные сессии на странице *Сессии*
- Может использовать портал самообслуживания — флаг в этом поле дает возможность открывать портал самообслуживания из клиента
- Может использовать магазин приложений — флаг в этом поле дает возможность открывать магазин приложений из клиента
- Может менять постоянный пароль — флаг в этом поле дает возможность изменять постоянный пароль в клиенте

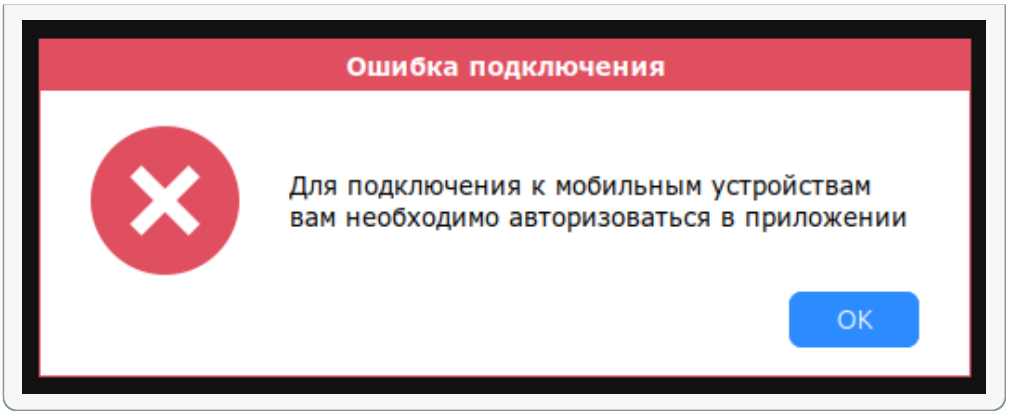
> **Подсказка**
>
> Если право не активно, то пункт **Установить постоянный пароль** будет недоступен для нажатия

- Может подключаться к серверу — флаг в этом поле дает возможность клиенту подключаться к серверу

> **Подсказка**
>
> Если право не активно, то устройства будут в статусе **Оффлайн** на странице *Устройства*

- Может подключаться к мобильным устройствам — флаг в этом поле дает возможность подключаться к мобильным устройствам

> **Подсказка**
>
> При попытке подключиться к мобильному устройству без наличия активного права появится ошибка подключения



- Может менять сервер для подключения — флаг в этом поле дает возможность изменять адрес сервера в клиенте
- Может сбрасывать настройки — флаг в этом поле дает возможность сбрасывать настройки в клиенте
- Может запоминать пароль при авторизации — флаг в этом поле дает возможность включать сохранение пароля при авторизации в клиенте
- Может видеть поле комментарий в свойствах устройства — флаг в этом поле дает возможность видеть вкладку *Комментарий* в свойствах устройства. Для изменения комментария также требуется право **Устройства → Изменение**
- Может просматривать логи в свойствах устройства — открывает вкладку **Логи** в свойствах доступного пользователю устройства и позволяет скачивать уже собранные логи
- Может управлять логами устройства (загрузка и удаление) — разрешает сбор логов с доступных устройств, включая действие **Загрузить логи для выбранных устройств**, и удаление собранных логов. Для работы через вкладку **Логи** также требуется право **Может просматривать логи в свойствах устройства**
- Может видеть сетевой адрес в свойствах устройства — флаг в этом поле дает возможность видеть сетевой адрес в *свойствах устройства*
- Может видеть результирующие права в свойствах устройства и пользователя — флаг в этом поле дает возможность видеть вкладку *Результирующие права* в свойствах устройства и пользователя
- Может просматривать карту — флаг в этом поле дает возможность открывать карту и просматривать геопозицию Android-устройств, для которых собраны геоданные

Подсказка

Без этого права страница *Карта* и переходы к ней недоступны. Право не включает сбор геоданных само по себе: геопозиция собирается только для Android-устройств через политику *Управление гео-трекингом Android*

- Может управлять Kickstart — флаг в этом поле дает возможность управлять настройками клиента **RuDesktop**, которые применяются при первой установке клиента или при запуске применения настроек Kickstart

> **Подсказка**
>
> Право открывает доступ к странице *Kickstart* и действиям применения настроек Kickstart к устройствам. Без права пользователь не сможет открыть страницу управления Kickstart и применить настройки клиента **RuDesktop** из веб-интерфейса

- Может просматривать граф — флаг в этом поле дает возможность открывать граф связей и просматривать связи объектов сервера

> **Подсказка**
>
> Право открывает страницу *Граф* и действия **Связи** в контекстных меню пользователей и устройств. Без права переход к графическому отображению связей недоступен

- Может выбирать группу при создании ссылки для подключения — флаг в этом поле дает возможность выбирать группу прав подключения при создании *пригласительной ссылки*

> **Подсказка**
>
> Без этого права поле Группа прав подключения при создании пригласительной ссылки недоступно. В этом случае ссылка создается с группой прав, определенной настройками доступа

- Может видеть пригласительные ссылки в свойствах устройства — флаг в этом поле дает возможность видеть вкладку Приглашения в свойствах устройства и просматривать пригласительные ссылки, доступные пользователю
- Может просматривать логи сессий — флаг в этом поле дает возможность просматривать журналы удаленных сессий, если они доступны для выбранного подключения

> **Подсказка**
>
> Право дает доступ именно к логам сессий. Для просмотра списка сессий дополнительно нужно право Сессии -> **Просмотр** или другое право, которое открывает пользователю нужные сессии

- Может видеть все пригласительные ссылки — флаг в этом поле дает возможность видеть все пригласительные ссылки на сервере, а не только

собственные ссылки или ссылки пользователей своего подразделения

- Может подключаться к другому серверу по приглашению — флаг в этом поле дает возможность использовать пригласительные ссылки для подключения к устройствам, которые находятся на другом сервере **RuDesktop**

Политики

- Может запускать политики — флаг в этом поле дает возможность выполнять политики и задачи на устройствах, в том числе изменять статус выбранных служб на вкладке **Службы** внутри **Дополнительной информации** в свойствах устройства. Изменение статуса служб недоступно для macOS

> **Важно**
>
> Если право не активно, то при выполнении политики произойдет ошибка о том, что не разрешено выполнять политики на устройстве

- Может просматривать статистику — флаг в этом поле дает возможность просматривать статистику выполнения политик и задач
- Может менять шаблон политики — флаг в этом поле дает возможность редактировать шаблоны политик

Права приложения

- Может управлять приглашениями для устройств — флаг в этом поле дает возможность создавать пригласительные ссылки из клиента и управлять ими для устройства

> **Подсказка**
>
> Без этого права в клиенте не отображается кнопка создания пригласительной ссылки для устройства. Для просмотра уже созданных ссылок в веб-интерфейсе используется право **Может видеть пригласительные ссылки в свойствах устройства**

- Может видеть свой пароль — флаг в этом поле дает возможность отображать пароль устройства в клиенте
- Может останавливать сервис — флаг в этом поле дает возможность остановить службу **RuDesktop** в настройках клиента
- Может использовать буфер обмена — флаг в этом поле дает возможность обмениваться текстом через общий буфер обмена во время удаленной сессии

- Может использовать режим конфиденциальности — флаг в этом поле дает возможность включать режим конфиденциальности во время удаленной сессии
- Может использовать клавиатуры и мышь — флаг в этом поле дает возможность управлять удаленным устройством с помощью клавиатуры и мыши во время сеанса подключения
- Может использовать передачу звука — флаг в этом поле дает возможность передавать звук удаленного устройства во время сеанса подключения
- Может перезагружать удалённое устройство — флаг в этом поле дает возможность перезагружать удаленное устройство во время сеанса подключения
- Может записывать сессию — флаг в этом поле дает возможность выполнять запись экрана во время сеанса подключения
- Может видеть вкладки в приложении — флаг в этом поле дает возможность видеть вкладки в клиенте
- Может видеть вкладки «Последние сеансы» и «Избранное» в приложении — флаг в этом поле дает возможность видеть вкладки Последние сеансы и Избранное в клиенте
- Может видеть вкладку «Найдено» в приложении — флаг в этом поле дает возможность видеть вкладку Найдено в клиенте

  Это право также разрешает использовать найденные в локальной сети устройства в подсказках при вводе удалённого ID. Без него эти устройства не подставляются из списка «Найдено»; то же устройство может быть предложено из другого доступного списка, например адресной книги.
- Может видеть вкладку «Адресная книга» в приложении — флаг в этом поле дает возможность видеть вкладку Адресная книга в клиенте
- Может видеть вкладку «Организация» в приложении — флаг в этом поле дает возможность видеть вкладку Организация в клиенте
- Может запрещать входящие подключения — флаг в этом поле дает возможность управлять опцией Разрешить входящие подключения в клиенте
- Может завершать входящие подключения в окне подключения — флаг в этом поле дает возможность видеть кнопку завершения подключения в окне менеджера подключений на устройстве, к которому подключаются

Подсказка

Без этого права кнопка завершения входящего подключения в окне подключения не отображается, и пользователь устройства не может вручную разорвать активную сессию из этого окна

- Может авторизоваться в клиенте — флаг в этом поле дает возможность авторизоваться в клиенте

> **Важно**
>
> Если право **Может авторизоваться в клиенте** не активно, даже при наличии прав **Может видеть вкладку «Адресная книга» в приложении** и **Может видеть вкладку «Организация» в приложении**, вкладки **Адресная книга** и **Организация** не будут отображаться

- Может использовать копирование и вставку файлов — флаг в этом поле дает возможность копировать и вставлять файлы между локальным и удаленным устройством во время удаленной сессии

> **Подсказка**
>
> Право управляет копированием файлов через буфер обмена и перетаскиванием файлов в окно удалённого рабочего стола во время сессии
>
> Для полноценного подключения к файловой системе удаленного устройства используется разрешение **Передача файлов** в *доступах*

- Может настраивать доступ к USB устройствам — флаг в этом поле дает возможность изменять настройки проброса USB-устройств в клиенте

> **Подсказка**
>
> Без этого права элементы настройки проброса USB в клиенте становятся недоступны для изменения. Для самой сессии проброса USB также должно быть разрешение **Проброс USB** в *доступах*

- Может настраивать доступ к удаленной печати — флаг в этом поле дает возможность включать и настраивать удаленную печать в клиенте

> **Подсказка**
>
> Без этого права пользователь может видеть состояние удаленной печати, но не может включать ее, выбирать принтер и менять параметры автоматической печати

- Может видеть поле ввода ID — флаг в этом поле дает возможность видеть в клиенте карточку с полем ввода ID для подключения к удалённому устройству

Подсказка

Без этого права карточка с полем ввода ID в клиенте не отображается, и пользователь не может ввести ID удалённого устройства для подключения. При этом баннер в клиенте продолжает отображаться, если он включен

Остальное

- Может устанавливать клиентов — флаг в этом поле дает возможность видеть виджет *Установка клиентов* и загружать установочные пакеты на главной странице
- Может экспортировать данные — флаг в этом поле дает возможность выбирать действие **«Экспортировать выбранные ...»** на всех доступных страницах, например *Экспорт устройств*
- Телефонный номер подтвержден — флаг в этом поле означает, что номер телефона подтвержден и можно подключаться к мобильным устройствам
- E-Mail подтвержден — флаг в этом поле дает возможность верифицировать E-Mail пользователя
- Права приложения определяются сервером — флаг в этом поле означает, что права приложения во время удаленной сессии определяются сервером. Если право активно, пользователь не может запросить изменение этих прав из окна подключения

Подсказка

Список прав, на которые применяется это право:

- Может использовать буфер обмена
- Может использовать клавиатуры и мышь
- Может использовать передачу звука
- Может перезагружать удалённое устройство
- Может записывать сессию

- Может видеть магазин приложений в портале самообслуживания — позволяет открывать каталог в *портале самообслуживания* и запрашивать установку приложений без автоматического запуска

Примечание

Для самостоятельной установки требуется право **Может использовать магазин приложений** у пользователя или группы устройства

- Может видеть мастер пароль — флаг в этом поле дает возможность просматривать мастер-пароль в *свойствах устройства*

Пользователи - это учетные записи, созданные на сервере, или пользователи, полученные после синхронизации с доменом

Подсказка

Страница **«Пользователи»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Как это работает

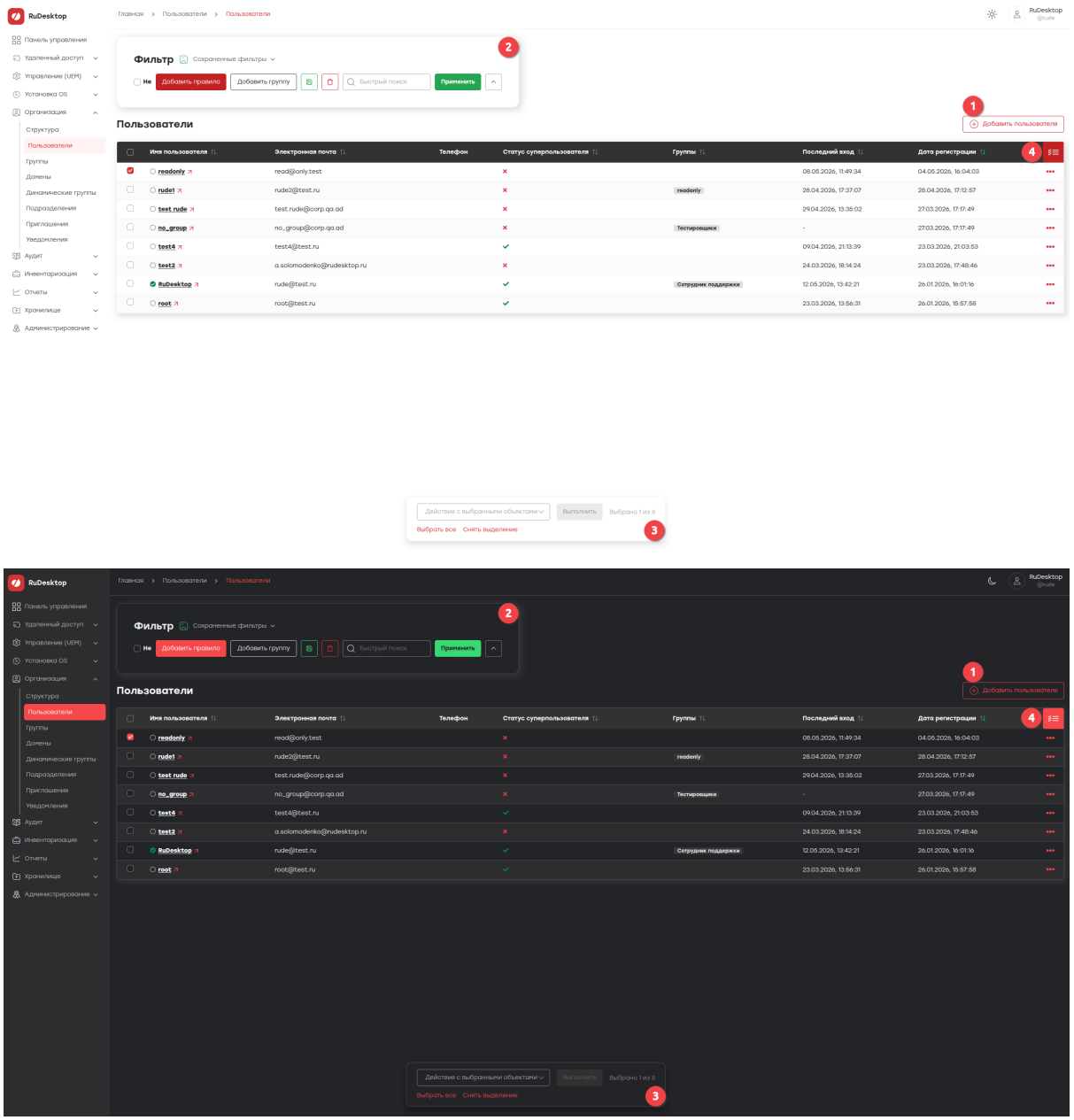
Учётная запись пользователя в **RuDesktop** появляется одним из пяти способов:

- **создаётся вручную** администратором на странице **«Пользователи»**
- **регистрируется самостоятельно** на странице регистрации сервера, если в *настройках сервера* включена опция самостоятельной регистрации
- **регистрируется по приглашению** - при принятии приглашения пользователь автоматически добавляется в подразделение отправителя (см. *Приглашения*)
- **импортируется из домена** при синхронизации или первой авторизации (см. *Домены*)
- **создаётся через консольную команду** *rude createsuperuser* на сервере - учётная запись с правами суперпользователя сразу появляется на странице **«Пользователи»**

Каждый пользователь связан с одной или несколькими *группами*, через которые наследует права доступа, и может входить в одно или несколько *подразделений*. Дополнительно пользователю можно назначить индивидуальные права, не входящие в группы. Контактные данные (E-Mail, телефон, Telegram, MAX) используются для двухфакторной аутентификации и получения *уведомлений*

Описание страницы

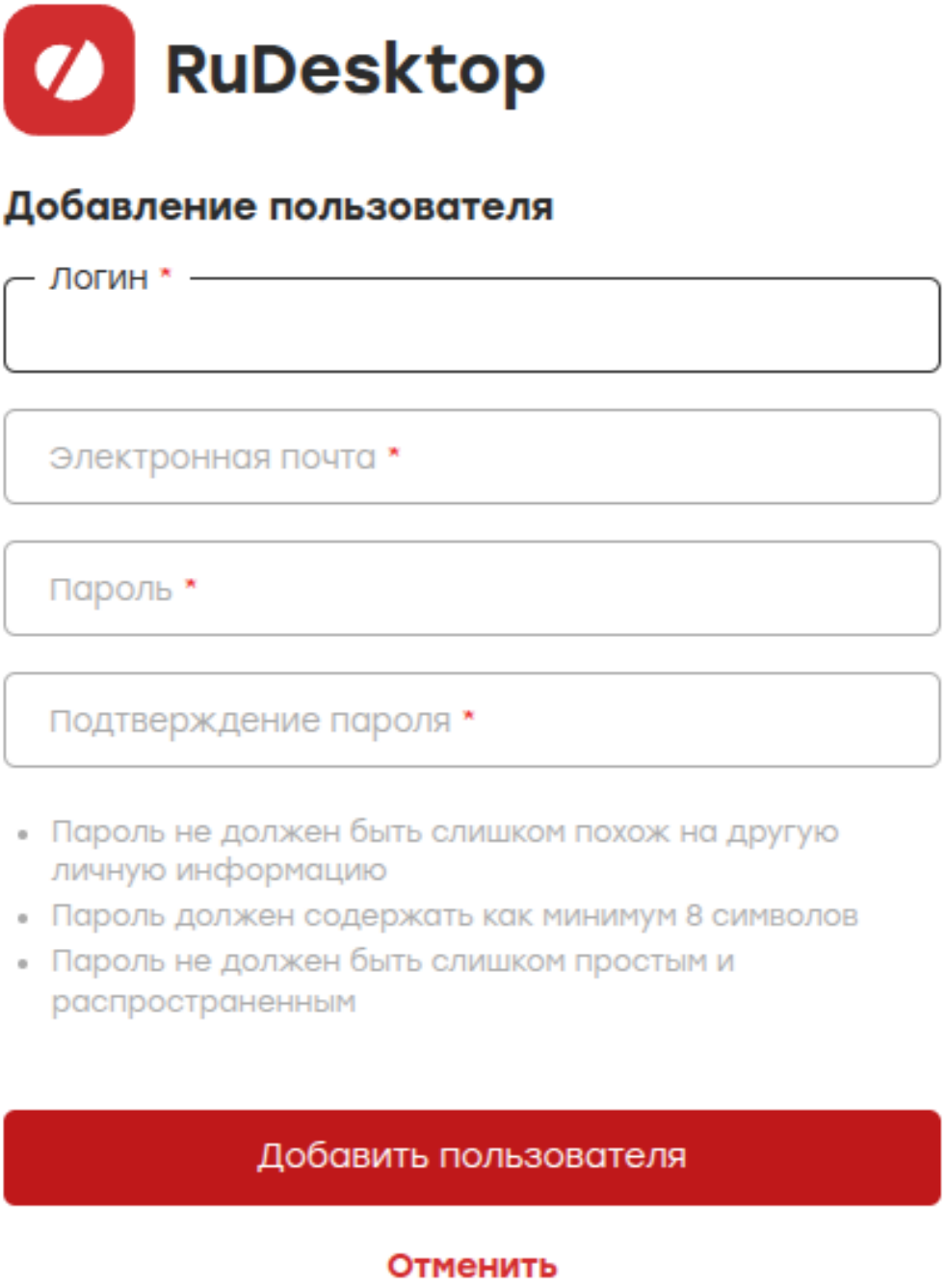
На странице **«Пользователи»** отображается:

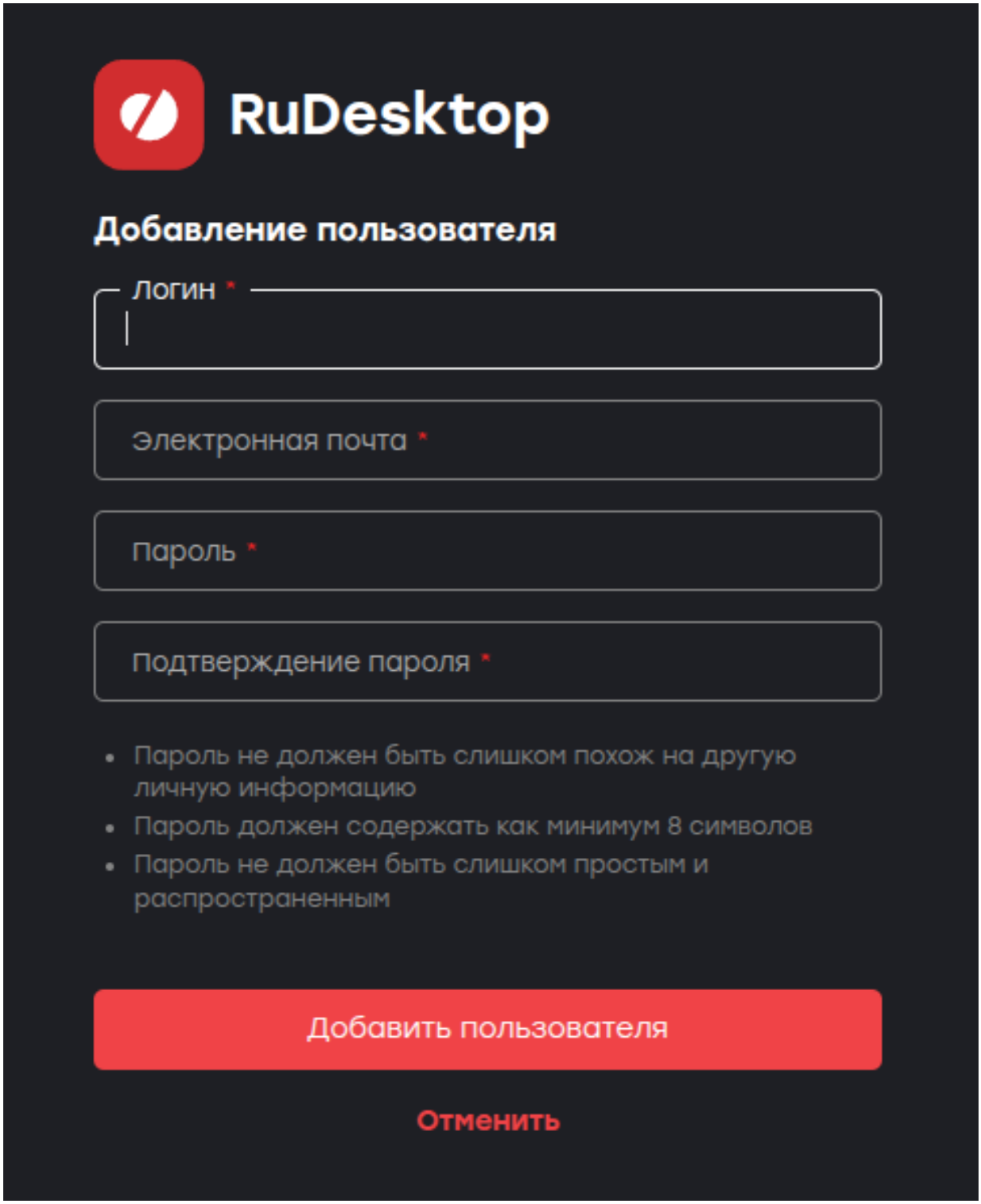


1. Кнопка Добавить Пользователя
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление пользователя

При нажатии на кнопку Добавить Пользователя откроется страница добавления пользователя со следующими полями:





1. Логин - имя пользователя
2. Электронная почта - электронная почта пользователя
3. Пароль - пароль пользователя

Подсказка

- Пароль не должен быть слишком похож на другую вашу личную информацию

- Ваш пароль должен содержать как минимум 8 символов
- Пароль не должен быть слишком простым и распространенным

4. Подтверждение пароля - подтверждение пароля пользователя

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. `Права` - фильтрация пользователей по назначенному праву доступа
2. `Домен` - фильтрация пользователей по принадлежности к домену
3. `Подразделение` - фильтрация пользователей по принадлежности к подразделению
4. `Поле поиска` - поиск по ключевому слову

Подсказка

Поиск осуществляется по логину, email, полному имени, компании, телефону, имени группы, названию подразделения и пути в LDAP

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Массовые действия позволяют выполнить одну и ту же операцию сразу над несколькими учётными записями, не открывая свойства каждой из них

Панель массовых действий появляется под таблицей, как только отмечен хотя бы один пользователь. Общий порядок работы одинаков для всех действий:

1. Отметить необходимых пользователей в таблице
2. Выбрать действие в списке Действия с выбранными объектами
3. Заполнить дополнительные поля, если действие их запрашивает (подразделение, значения статусов, формат файла) - пока обязательные поля не заполнены, кнопка Выполнить неактивна
4. Нажать на кнопку Выполнить

Важно

В панели есть кнопка Выбрать все

Она распространяет действие на **всю текущую выборку** - на всех пользователей, отобранных фильтром и поиском, а не только на отмеченных на текущей странице

Рядом отображается счётчик Выбрано N из M или Выбраны все объекты, сбросить выбор можно кнопкой Снять выделение

Что делает каждое действие:

Действие	Что делает
Удалить выбранных пользователей	Удаляет учётные записи с сервера вместе со всеми адресными книгами, которыми они владеют
Добавить пользователей в Подразделение	Добавляет выбранных пользователей в одно указанное *подразделение* Прежние подразделения сохраняются
Назначить статусы пользователям	Устанавливает выбранным пользователям значения сразу трёх флагов: **Суперпользователь**, **Персонал** и **Активный**
Экспортировать выбранных пользователей	Выгружает в файл имя пользователя, электронную почту, полное имя и компанию

Важно

1. Действие Добавить пользователей в Подразделение требует права **Подразделения → Изменение**
2. Действие Назначить статусы пользователям доступно только суперпользователю
3. Действие Удалить выбранных пользователей требует права **Пользователи → Удаление**
4. Действие Экспортировать выбранных пользователей требует права **Может экспортировать данные**
5. В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление пользователей

Для массового удаления пользователей необходимо:

1. Отметить необходимых пользователей в таблице
2. Выбрать действие Удалить выбранных пользователей

3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие пользователи будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные пользователи будут удалены

Важно

Вместе с учётной записью удаляются все *адресные книги*, владельцем которых она является, - не только личная книга пользователя, но и созданные им общие книги вместе со всеми их адресами

Если общая книга нужна другим сотрудникам, перед удалением пользователя смените у неё владельца

Примечание

1. Записи о действиях пользователя на страницах *Логи исполнения* сохраняются - у них лишь снимается привязка к удалённой учётной записи
2. При выборе более 100 пользователей удаление ставится в очередь и выполняется в фоне: записи исчезают из таблицы не сразу, а ход выполнения виден на странице *Очередь задач* по задаче **«Удаление данных»**

Добавление в подразделение

Для массового добавления пользователей в подразделение необходимо:

1. Отметить необходимых пользователей в таблице
2. Выбрать действие Добавить пользователей в Подразделение
3. Выбрать необходимое подразделение
4. Нажать на кнопку Выполнить
5. Выбранные пользователи будут добавлены в выбранное подразделение

Примечание

Действие **добавляет** подразделение, а не заменяет его: пользователь может состоять сразу в нескольких подразделениях, и прежние за ним сохраняются

Чтобы убрать пользователя из подразделения, это делается в свойствах самого *подразделения*

Назначение статусов пользователям

Действие задаёт выбранным пользователям значения трёх флагов учётной записи

Важно

Все три значения обязательны и применяются одновременно ко всем выбранным пользователям

Оставить какой-то из флагов «как был» нельзя - заданные значения перезапишут текущие, даже если у разных пользователей они различались

Поэтому перед выполнением убедитесь, что верно указаны все три поля, а не только то, которое требовалось изменить

Для массового изменения статусов пользователей необходимо:

1. Отметить необходимых пользователей в таблице
2. Выбрать действие Назначить статусы пользователям
3. Указать значения параметров:
   - `Суперпользователь` - выдача прав суперпользователя
   - `Персонал` - доступ к административной панели **RuDesktop**
   - `Активный` - активность учётной записи

     При значении `Нет` пользователь не сможет авторизоваться
4. Нажать на кнопку Выполнить
5. Указанные значения будут установлены всем выбранным пользователям

Важно

Действием можно снять статус суперпользователя и с самого себя, а значением `Активный` = `Нет` - заблокировать собственную учётную запись

Проверяйте состав выборки перед выполнением

Экспорт пользователей

Действие выгружает в файл перечень выбранных учётных записей

Примечание

В файл попадают только четыре поля: имя пользователя, электронная почта, полное имя и компания

Группы, подразделения, права и статусы не выгружаются, а настройка отображаемых столбцов таблицы на состав файла не влияет

Для массового экспорта пользователей необходимо:

1. Отметить необходимых пользователей в таблице
2. Выбрать действие Экспортировать выбранных пользователей
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Важно

1. Доступные форматы выгрузки: **CSV**, **XLS**, **XLSX**, **TSV**, **ODS**, **JSON**, **YAML**, **HTML**

   Набор форматов зависит от компонентов, установленных на сервере, поэтому отдельные пункты могут отсутствовать
2. Если выбрано более 1000 пользователей, экспорт выполняется в фоне: файл сохраняется на сервере в репозитории **Отчеты** и становится доступен на странице *Файлы*
3. Формат **XLS** не поддерживает ячейки с текстом длиннее 32767 символов - при таких значениях экспорт завершится ошибкой с предложением выбрать другой формат

Таблица

Логин и полное имя показываются в отдельных столбцах

Например, для учётной записи с логином `ivanov` и полным именем `Иван Иванов` в таблице будут видны оба значения

Примечание

Полное имя не подменяет логин в списке и само по себе не меняет данные для входа. Если полное имя не заполнено, отдельного значения в этом столбце не будет

Для поиска можно использовать как логин, так и полное имя. Таблица разбита по столбцам:

1. `Логин пользователя` - логин учётной записи, а при пустом логине её email
2. `Полное имя пользователя` - отдельное поле с полным именем
3. `Электронная почта` - электронная почта, указанная при регистрации или создании пользователя
4. `Телефон` - телефон пользователя

Подсказка

Чтобы отобразить номер телефона в таблице, необходимо ввести его в свойствах пользователя

5. Суперпользователь - отметка о наличии у пользователя статуса суперпользователя
6. Группы - группы, к которым принадлежит пользователь
7. Подразделения - подразделения, к которым принадлежит пользователь
8. Путь до объекта в LDAP - DN пользователя в LDAP
9. Последнее подключение - отображение даты и времени, когда пользователь в последний раз совершал подключение к удаленному устройству
10. Последний вход - отображает дату и время, когда пользователь в последний раз авторизовывался в веб-интерфейсе сервера **RuDesktop**
11. Дата регистрации - дата регистрации или создания пользователя на сервере **RuDesktop**

Примечание

Столбцы Подразделения, Путь до объекта в LDAP и Последнее подключение по умолчанию скрыты - их можно включить через настройку отображаемых столбцов

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. Редактировать - при выборе этого пункта откроются свойства пользователя
2. Удалить - при выборе этого пункта пользователь будет удален
3. Удалить из подразделения - при выборе этого пункта пользователь будет удалён из подразделения, не затрагивая саму учётную запись

Важно

Действие отображается только пользователю, не являющемуся суперпользователем, и недоступно для самого себя

4. История изменений - при выборе этого пункта будет отображена история пользователя: создание/редактирование и пользователь, который выполнил данные операции

5. `Сессии` - при выборе этого пункта произойдет переход на страницу *Сессии* с активным фильтром по этому пользователю
6. `Логи аудита` - при выборе этого пункта будут отображены логи, связанные с этим пользователем
7. `Связи` - при выборе этого пункта произойдет переход на страницу *Граф*, где будет графически отображены входящие и исходящие соединения пользователя
8. `Безопасность аккаунта` - при выборе этого пункта откроется страница управления многофакторной аутентификацией пользователя

Свойства пользователя

Подробнее о *свойствах пользователя*

2.11.3 Группы

Права группы

Как выбрать и проверить права

В форме есть таблица прав на объекты и блок специальных прав, сгруппированных по разделам и карточкам. Права на объекты определяют доступные операции: просмотр, создание, изменение и удаление. Специальные права управляют отдельными возможностями продукта

1. Открыть нужную группу и перейти к её правам
2. В таблице отметить только необходимые операции для нужных объектов
3. В блоке специальных прав ввести часть названия в поле **«Поиск права»**
4. Проверить название найденного права и пояснение рядом с ним, если для этого права предусмотрена подсказка
5. Отметить нужные права, очистить поиск и проверить весь выбранный набор
6. Сохранить группу и проверить действия под обычной учётной записью пользователя этой группы

Поиск специальных прав

- Поиск учитывает название права, а не текст его подсказки
- Регистр букв не важен; допускается неполное написание названия
- Перед выбором проверить полное название найденного права

Примечание

Поиск скрывает неподходящие строки, но не снимает уже выбранные флажки

Массовый выбор

- Кнопка **«Выбрать все»** внутри карточки действует на доступные строки этой карточки, которые не скрыты поиском
- Общая кнопка **«Выбрать все»** действует на такие строки всего блока специальных прав
- Если весь доступный набор уже выбран, повторное нажатие снимает выбор
- Сворачивание карточки само по себе не исключает её права из массового выбора
- В таблице прав на объекты флажок в заголовке столбца выбирает соответствующую операцию для строк, а флажок строки — операции этой строки. Эти элементы не ограничены поиском специальных прав

Важно

При выборе **«Создание»** автоматически включается **«Изменение»** той же строки, и его флажок блокируется, пока создание включено

Чтобы убрать изменение, сначала снять создание, затем проверить и при необходимости снять изменение

Недоступные флажки не меняются при массовом выборе. Набор отображаемых прав также зависит от редакции продукта. Для суперпользователя форма показывает права включёнными и недоступными для отдельного изменения

После выбора флажков сохранить форму

Если пользователь всё ещё имеет снятое право

Примечание

Права пользователя складываются из индивидуальных назначений и прав всех его групп. Снятие права в одной группе не является запретом, если оно осталось в другой группе или назначено пользователю напрямую. Статус суперпользователя также даёт права без отдельных назначений

1. Проверить все группы пользователя и его индивидуальные права
2. Посмотреть **«Результирующие права»** в карточке пользователя

   Для неё требуется право **«Просмотр результирующих прав»**
3. Для нужного специального права проверить, какие группы показаны источниками
4. Убрать ненужное назначение во всех соответствующих источниках и сохранить
5. Повторить проверку под учётной записью пользователя

В **«Результирующих правах»** показаны статус, название права и группы-источники. Если группа не указана, проверить индивидуальное назначение и статус суперпользователя - прочерк в столбце **«Группа»** не означает отсутствие права

Важно

Таблица содержит предусмотренные для неё специальные права и статусы пользователя. Она не является полным перечнем всех прав на создание, просмотр, изменение и удаление объектов. Таблица результирующих прав не заменяет проверку правил доступа к конкретному устройству и не перечисляет все условия выполнения действия

Например, право просмотра устройств само по себе не означает возможность подключаться к любому устройству сервера

Пошаговая настройка типовых ролей приведена в кейсе Настройка ролей

Права доступа

Устройства

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Устройства* и видеть список устройств без возможности редактирования
- **Создание** — флаг в этом поле дает возможность пользователю добавлять записи устройств
- **Изменение** — флаг в этом поле дает возможность пользователю изменять псевдоним в *свойствах устройства*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять устройства

Сессии

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Сессии* и видеть список сессий без возможности редактирования
- **Изменение** — флаг в этом поле дает возможность пользователю изменять параметры сессий
- **Удаление** — флаг в этом поле дает возможность пользователю удалять сессии

Доступы

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Доступы* и видеть список доступов без возможности создания и редактирования

- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые доступы*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные доступы*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять доступы

Адресная книга

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Адресные книги*, *Адреса* и *Теги* и видеть список адресных книг, адресов и тегов без возможности создания и редактирования
- **Создание** — флаг в этом поле дает доступ пользователю к добавлению *адресов* и *тегов*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные адреса* и *теги*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять добавленные адреса и теги

Приглашения

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Пригласительные ссылки* и видеть список созданных ссылок без возможности создания и удаления
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *пригласительные ссылки*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять пригласительные ссылки

Подсказка

Изменение существующих пригласительных ссылок в веб-интерфейсе не предусмотрено — для изменения параметров ссылку нужно удалить и создать заново. Объём видимых ссылок дополнительно регулируется правами **Руководитель подразделения** и **Может видеть все пригласительные ссылки**

Пользователи

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Пользователи* и видеть список пользователей без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новых пользователей*

- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленных пользователей*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять пользователей

Группы

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Группы* и видеть список групп без возможности создания и редактирования. Также открывает вкладку **Группы** в свойствах устройства
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые группы*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные группы*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять группы

Домены

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Домены* и видеть список доменов без возможности создания и редактирования. Также открывает вкладку **LDAP** в свойствах устройства, если у устройства заполнен DN
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые домены*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные домены*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять домены

Подразделения

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Подразделения* и видеть список подразделений без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые подразделения*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные подразделения*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять подразделения

Политики

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Политики* и *Задачи* и видеть список политик и задач без возможности создания, редактирования и запуска
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *политики* и *задачи*
- **Изменение** — флаг в этом поле дает возможность пользователю изменять добавленные *политики* и *задачи*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять политики и задачи

Динамические группы

Права на просмотр, создание, изменение и удаление динамических групп назначаются отдельно. Право **Создание** также позволяет создать группу из текущего фильтра на странице **Устройства**

Портал

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Обращения* и видеть список обращений без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые обращения*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные обращения*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять обращения

Инвентаризация

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Наличие ресурсов* и *Каталог ресурсов* и видеть список собранных ресурсов с устройств без возможности редактирования и удаления. Также открывает вкладки **Дополнительная информация** и **Факты** в свойствах устройства при наличии собранных фактов
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые ресурсы*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные ресурсы*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять ресурсы

Уведомления

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Уведомления* и видеть список уведомлений без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые уведомления*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные уведомления*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять уведомления

Образы OS

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Образы OS* и видеть список образов ОС без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые образы OS*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные образы OS*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять образы OS

Отчеты

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Шаблоны* и *Готовые отчеты* и видеть список шаблонов и готовых отчетов без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые шаблоны*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные шаблоны*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять шаблоны и готовые отчеты

Файлы

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Репозитории* и *Файлы* и видеть список репозиториев и загруженных файлов без возможности создания, редактирования и загрузки файлов
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *репозитории* и *файлы*
- **Изменение** — флаг в этом поле дает возможность пользователю изменять добавленные *репозитории* и *файлы*

- **Удаление** — флаг в этом поле дает возможность пользователю удалять репозитории и загруженные файлы

Аудит

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Логи исполнения*, *Объекты*, *Входы в систему*, *HTTP запросы*, *Логи сессий* и *Все логи* и видеть список логов

Черный список

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Черный список* и видеть список черных списков без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые черные списки*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные черные списки*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять черные списки

Белый список

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Белый список* и видеть список белых списков без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю *добавлять новые белые списки*
- **Изменение** — флаг в этом поле дает возможность пользователю *изменять добавленные белые списки*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять белые списки

Подсети

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к странице *Подсети* и видеть список подсетей без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *подсети* для определения геопозиции устройств по IP-адресу
- **Изменение** — флаг в этом поле дает возможность пользователю изменять параметры существующих подсетей
- **Удаление** — флаг в этом поле дает возможность пользователю удалять подсети

Настройки

- **Просмотр** — флаг в этом поле дает возможность пользователю получить доступ к страницам *Настройки*, *KeyCloak*, *Мосты* и *Очередь задач* и видеть настройки сервера, список keycloak, мостов и очередь задач без возможности создания и редактирования
- **Создание** — флаг в этом поле дает возможность пользователю добавлять новые *keycloak* и *мосты*
- **Изменение** — флаг в этом поле дает возможность пользователю изменять добавленные *keycloak*, *мосты* и *настройки*
- **Удаление** — флаг в этом поле дает возможность пользователю удалять Keycloak, мосты

Дополнительные права доступа

Организация

- Руководитель подразделения — флаг в этом поле расширяет область видимости объектов до всего подразделения пользователя. Без права пользователь видит только свои объекты (плюс объекты, доступные через группы); с правом — объекты любого пользователя своего подразделения

> **Подсказка**
>
> Конкретно при активном праве пользователь дополнительно получает:
>
> - на странице *Пользователи* — все учётные записи своего подразделения
> - на странице *Устройства* — устройства, к которым подключались пользователи подразделения
> - на странице *Сессии* — сессии всех пользователей подразделения
> - на страницах *Адресные книги* и *Адреса* — общие книги своего подразделения (в том числе автоматически созданную общую книгу подразделения) с уровнем доступа **Управление** и их адреса
> - на странице *Пригласительные ссылки* — ссылки, созданные пользователями подразделения
> - действие **Удалить из подразделения** в контекстном меню пользователя
>
> Без права пользователь видит только собственные объекты (личную адресную книгу, сессии, пригласительные ссылки) и объекты, явно доступные ему через группы или доступы

- Просмотр истории изменений объектов — флаг в этом поле дает возмож-

ность видеть в *панели управления* виджет последних изменений с записями всех пользователей сервера

> **Подсказка**
>
> Без этого права в виджете последних изменений пользователь видит только собственные действия, а действия других пользователей скрыты

- Просмотр всех пользователей в административной панели — флаг в этом поле дает возможность видеть всех пользователей, созданных на сервере, на странице *Пользователи*. Без этого права пользователь видит только доступных ему пользователей
- Может настраивать безопасность своего аккаунта — флаг в этом поле дает возможность изменять собственные настройки безопасности, включая параметры двухфакторной авторизации
- Может настраивать безопасность других аккаунтов — флаг в этом поле дает возможность изменять настройки безопасности других пользователей, включая параметры двухфакторной авторизации

Устройства

- Может видеть все компьютеры — флаг в этом поле дает возможность видеть все устройства, подключенные к серверу, на странице *Устройства*
- Может видеть все сессии — флаг в этом поле дает возможность видеть все сессии, зарегистрированные на сервере, на странице *Сессии*
- Может прерывать сессии — флаг в этом поле дает возможность завершать активные удаленные сессии на странице *Сессии*
- Может использовать портал самообслуживания — флаг в этом поле дает возможность открывать портал самообслуживания из клиента
- Может использовать магазин приложений — флаг в этом поле дает возможность открывать магазин приложений из клиента
- Может менять постоянный пароль — флаг в этом поле дает возможность изменять постоянный пароль в клиенте

> **Подсказка**
>
> Если право не активно, то пункт **Установить постоянный пароль** будет недоступен для нажатия

- Может подключаться к серверу — флаг в этом поле дает возможность клиенту подключаться к серверу

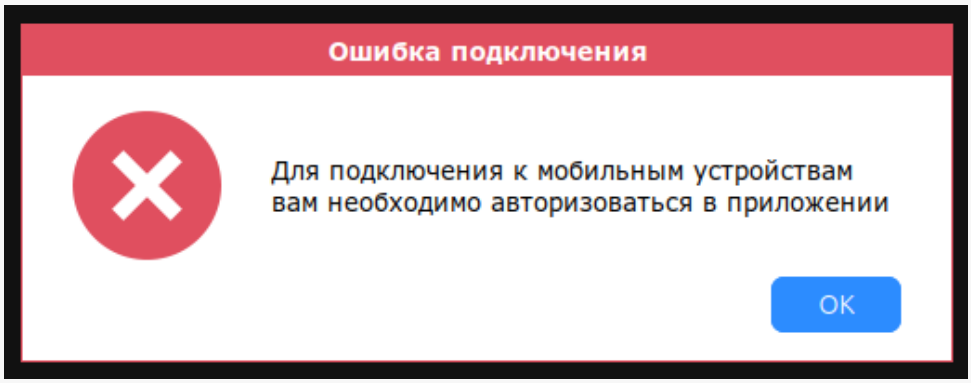
Подсказка

Если право не активно, то устройства будут в статусе **Оффлайн** на странице *Устройства*

- Может подключаться к мобильным устройствам — флаг в этом поле дает возможность подключаться к мобильным устройствам

Подсказка

При попытке подключиться к мобильному устройству без наличия активного права появится ошибка подключения



- Может менять сервер для подключения — флаг в этом поле дает возможность изменять адрес сервера в клиенте
- Может сбрасывать настройки — флаг в этом поле дает возможность сбрасывать настройки в клиенте
- Может запоминать пароль при авторизации — флаг в этом поле дает возможность включать сохранение пароля при авторизации в клиенте
- Может видеть поле комментарий в свойствах устройства — флаг в этом поле дает возможность видеть вкладку *Комментарий* в свойствах устройства. Для изменения комментария также требуется право **Устройства → Изменение**
- Может просматривать логи в свойствах устройства — открывает вкладку **Логи** в свойствах доступного пользователю устройства и позволяет скачивать уже собранные логи
- Может управлять логами устройства (загрузка и удаление) — разрешает сбор логов с доступных устройств, включая действие **Загрузить логи для выбранных устройств**, и удаление собранных логов. Для работы через вкладку **Логи** также требуется право **Может просматривать логи в свойствах устройства**
- Может видеть сетевой адрес в свойствах устройства — флаг в этом поле дает возможность видеть сетевой адрес в *свойствах устройства*
- Может видеть результирующие права в свойствах устройства и пользователя — флаг в этом поле дает возможность видеть вкладку *Результиру-*

ющие права в свойствах устройства и пользователя

- Может просматривать карту — флаг в этом поле дает возможность открывать карту и просматривать геопозицию Android-устройств, для которых собраны геоданные

> **Подсказка**
>
> Без этого права страница *Карта* и переходы к ней недоступны. Право не включает сбор геоданных само по себе: геопозиция собирается только для Android-устройств через политику *Управление гео-трекингом Android*

- Может управлять Kickstart — флаг в этом поле дает возможность управлять настройками клиента **RuDesktop**, которые применяются при первой установке клиента или при запуске применения настроек Kickstart

> **Подсказка**
>
> Право открывает доступ к странице *Kickstart* и действиям применения настроек Kickstart к устройствам. Без права пользователь не сможет открыть страницу управления Kickstart и применить настройки клиента **RuDesktop** из веб-интерфейса

- Может просматривать граф — флаг в этом поле дает возможность открывать граф связей и просматривать связи объектов сервера

> **Подсказка**
>
> Право открывает страницу *Граф* и действия **Связи** в контекстных меню пользователей и устройств. Без права переход к графическому отображению связей недоступен

- Может выбирать группу при создании ссылки для подключения — флаг в этом поле дает возможность выбирать группу прав подключения при создании *пригласительной ссылки*

> **Подсказка**
>
> Без этого права поле Группа прав подключения при создании пригласительной ссылки недоступно. В этом случае ссылка создается с группой прав, определенной настройками доступа

- Может видеть пригласительные ссылки в свойствах устройства — флаг в этом поле дает возможность видеть вкладку Приглашения в свойствах устройства и просматривать пригласительные ссылки, доступные пользователю

- Может просматривать логи сессий — флаг в этом поле дает возможность просматривать журналы удаленных сессий, если они доступны для выбранного подключения

> **Подсказка**
>
> Право дает доступ именно к логам сессий. Для просмотра списка сессий дополнительно нужно право Сессии -> **Просмотр** или другое право, которое открывает пользователю нужные сессии

- Может видеть все пригласительные ссылки — флаг в этом поле дает возможность видеть все пригласительные ссылки на сервере, а не только собственные ссылки или ссылки пользователей своего подразделения
- Может подключаться к другому серверу по приглашению — флаг в этом поле дает возможность использовать пригласительные ссылки для подключения к устройствам, которые находятся на другом сервере **RuDesktop**

Политики

- Может запускать политики — флаг в этом поле дает возможность выполнять политики и задачи на устройствах, в том числе изменять статус выбранных служб на вкладке **Службы** внутри **Дополнительной информации** в свойствах устройства. Изменение статуса служб недоступно для macOS

> **Важно**
>
> Если право не активно, то при выполнении политики произойдет ошибка о том, что не разрешено выполнять политики на устройстве

- Может просматривать статистику — флаг в этом поле дает возможность просматривать статистику выполнения политик и задач
- Может менять шаблон политики — флаг в этом поле дает возможность редактировать шаблоны политик

Права приложения

- Может управлять приглашениями для устройств — флаг в этом поле дает возможность создавать пригласительные ссылки из клиента и управлять ими для устройства

Подсказка

Без этого права в клиенте не отображается кнопка создания пригласительной ссылки для устройства. Для просмотра уже созданных ссылок в веб-интерфейсе используется право **Может видеть пригласительные ссылки в свойствах устройства**

- Может видеть свой пароль — флаг в этом поле дает возможность отображать пароль устройства в клиенте
- Может завершать входящие подключения в окне подключения — флаг в этом поле дает возможность завершать активное входящее подключение из окна подключения на управляемом устройстве. При наличии права в окне отображается кнопка **Отключить**; без права кнопка скрыта, и пользователь управляемого устройства не может прервать сеанс со своей стороны
- Может останавливать сервис — флаг в этом поле дает возможность остановить службу **RuDesktop** в настройках клиента
- Может использовать буфер обмена — флаг в этом поле дает возможность обмениваться текстом через общий буфер обмена во время удаленной сессии
- Может использовать режим конфиденциальности — флаг в этом поле дает возможность включать режим конфиденциальности во время удаленной сессии
- Может использовать клавиатуры и мышь — флаг в этом поле дает возможность управлять удаленным устройством с помощью клавиатуры и мыши во время сеанса подключения
- Может использовать передачу звука — флаг в этом поле дает возможность передавать звук удаленного устройства во время сеанса подключения
- Может перезагружать удалённое устройство — флаг в этом поле дает возможность перезагружать удаленное устройство во время сеанса подключения
- Может записывать сессию — флаг в этом поле дает возможность выполнять запись экрана во время сеанса подключения
- Может видеть вкладки в приложении — флаг в этом поле дает возможность видеть вкладки в клиенте
- Может видеть вкладки «Последние сеансы» и «Избранное» в приложении — флаг в этом поле дает возможность видеть вкладки Последние сеансы и Избранное в клиенте

Подсказка

Эти права также управляют подменю Избранное в контекстном меню значка **RuDesktop** в системном трее, из которого можно быстро подключиться к устройствам из списка избранного. Подменю отображается только при наличии обоих прав — **Может видеть вкладки в приложении** и **Может видеть вкладки «Последние сеансы» и «Избранное» в приложении** — и хотя бы одного избранного устройства. Без этих прав подменю в трее скрыто, и подключиться к устройствам через значок в трее нельзя

- Может видеть вкладку «Найдено» в приложении — флаг в этом поле дает возможность видеть вкладку Найдено в клиенте
- Может видеть вкладку «Адресная книга» в приложении — флаг в этом поле дает возможность видеть вкладку Адресная книга в клиенте
- Может видеть вкладку «Организация» в приложении — флаг в этом поле дает возможность видеть вкладку Организация в клиенте
- Может запрещать входящие подключения — флаг в этом поле дает возможность управлять опцией Разрешить входящие подключения в клиенте
- Может авторизоваться в клиенте — флаг в этом поле дает возможность авторизоваться в клиенте

Важно

Если право **Может авторизоваться в клиенте** не активно, даже при наличии прав **Может видеть вкладку «Адресная книга» в приложении** и **Может видеть вкладку «Организация» в приложении**, вкладки **Адресная книга** и **Организация** не будут отображаться

- Может использовать копирование и вставку файлов — флаг в этом поле дает возможность копировать и вставлять файлы между локальным и удаленным устройством во время удаленной сессии

Подсказка

Право управляет копированием файлов через буфер обмена и перетаскиванием файлов в окно удалённого рабочего стола во время сессии

Для полноценного подключения к файловой системе удаленного устройства используется разрешение **Передача файлов** в *доступах*

- Может настраивать доступ к USB устройствам — флаг в этом поле дает

возможность изменять настройки проброса USB-устройств в клиенте

> **Подсказка**
>
> Без этого права элементы настройки проброса USB в клиенте становятся недоступны для изменения. Для самой сессии проброса USB также должно быть разрешение **Проброс USB** в *доступах*

- Может настраивать доступ к удаленной печати — флаг в этом поле дает возможность включать и настраивать удаленную печать в клиенте

> **Подсказка**
>
> Без этого права пользователь может видеть состояние удаленной печати, но не может включать ее, выбирать принтер и менять параметры автоматической печати

- Может видеть поле ввода ID — флаг в этом поле дает возможность видеть в клиенте карточку с полем ввода ID для подключения к удалённому устройству

> **Подсказка**
>
> Без этого права карточка с полем ввода ID в клиенте не отображается, и пользователь не может ввести ID удалённого устройства для подключения. При этом баннер в клиенте продолжает отображаться, если он включен

Остальное

- Может устанавливать клиентов — флаг в этом поле дает возможность видеть виджет *Установка клиентов* и загружать установочные пакеты на главной странице
- Может экспортировать данные — флаг в этом поле дает возможность выбирать действие **«Экспортировать выбранные ...»** на всех доступных страницах, например *Экспорт устройств*
- Телефонный номер подтвержден — флаг в этом поле означает, что номер телефона подтвержден и можно подключаться к мобильным устройствам
- E-Mail подтвержден — флаг в этом поле дает возможность верифицировать E-Mail пользователя
- Права приложения определяются сервером — флаг в этом поле означает, что права приложения во время удаленной сессии определяются сервером. Если право активно, пользователь не может запросить изменение этих прав из окна подключения

Подсказка

Список прав, на которые применяется это право:

- Может использовать буфер обмена
- Может использовать клавиатуры и мышь
- Может использовать передачу звука
- Может перезагружать удалённое устройство
- Может записывать сессию

- Может видеть магазин приложений в портале самообслуживания — позволяет открывать каталог в *портале самообслуживания* и запрашивать установку приложений без автоматического запуска

Примечание

Для самостоятельной установки требуется право **Может использовать магазин приложений** у пользователя или группы устройства

- Может видеть мастер пароль — флаг в этом поле дает возможность просматривать мастер-пароль в *свойствах устройства*

Группы — это совокупность пользователей или (и) устройств, объединённых для получения одинакового уровня доступа и прав в системе

Подсказка

Страница **«Группы»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Примечание

По умолчанию имеются предустановленные группы:

- Администратор
- Без доступа
- Гость
- Мои группы
- Права доступа
- Руководитель подразделения
- Сотрудник поддержки

Предустановленные группы нельзя удалить, но их можно редактировать

Как это работает

Группа объединяет пользователей и устройства и определяет, что эти пользователи могут делать с устройствами. На группу назначается набор *прав доступа* — пользователи, состоящие в группе, наследуют эти права через **ИЛИ** (право считается выданным, если оно есть у пользователя напрямую или хотя бы в одной из его групп), а устройства, добавленные в группу, попадают в область действия этих прав

Группы используются для:

- разграничения прав доступа к устройствам между разными командами и ролями
- объединения устройств для применения политик и *уведомлений*
- включения принудительной записи удалённых сессий и передач файлов на стороне сервера
- связывания со внешними источниками — *доменными группами LDAP* и группами **KeyCloak**, чтобы членство пользователей в группе бралось из домена

Описание страницы

На странице **«Группы»** отображается:



1. Кнопка Импортировать группу
2. Кнопка Добавить Группу
3. Фильтр
4. Массовые действия
5. Таблица

Импорт в группу

При нажатии на кнопку Импортировать группу откроется страница импорта устройств в группу

Страница содержит поля:

1. Выбрать существующую группу — выпадающий список с группами, которые уже созданы на сервере **RuDesktop**. Поле и Название новой группы взаимоисключающие — нужно заполнить только одно из них

2. Название новой группы — название группы, которая будет создана при импорте. Поле и Выбрать существующую группу взаимоисключающие
3. Устройства из списка — выбор уже зарегистрированных на сервере устройств (множественный выбор)
4. Устройства — текстовое поле для ввода hostname устройств вручную

Важно

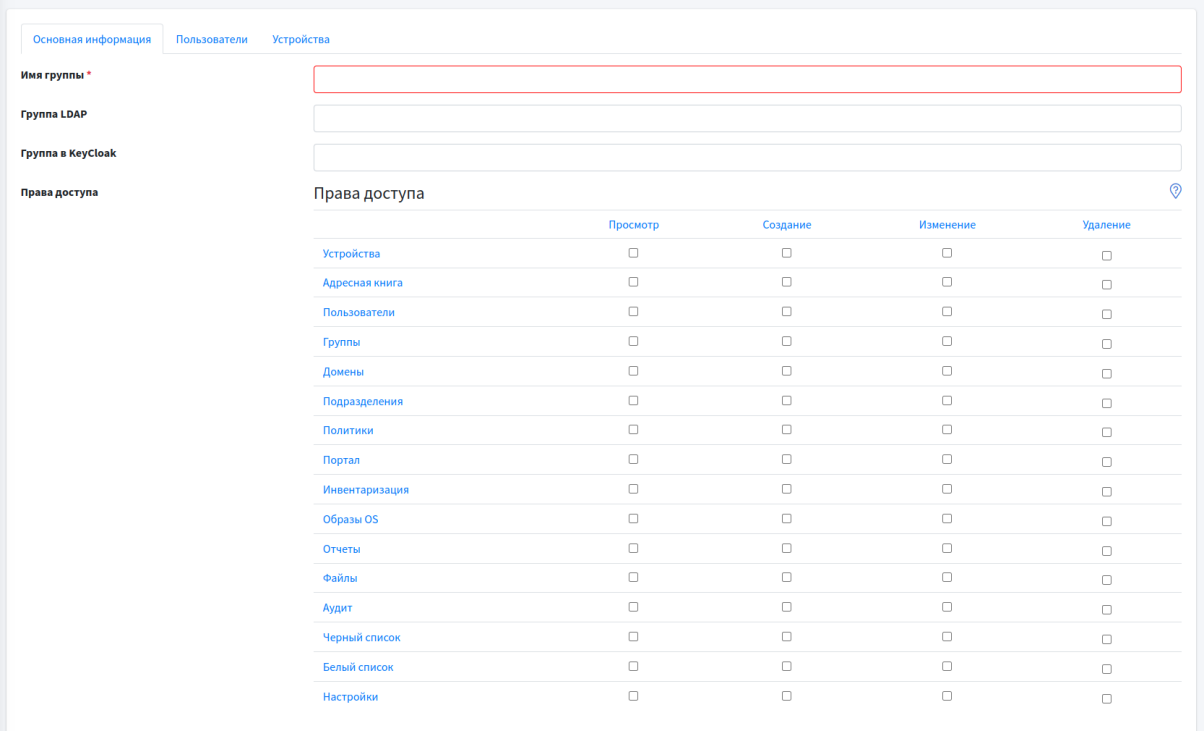
Для успешного импорта необходимо ввести hostname устройств:

- Устройство должно быть подключено к серверу **RuDesktop** и отображаться на странице **«Устройства»**
- Каждый hostname необходимо вводить с новой строки

Добавление группы

На вкладках пользователей и устройств кнопку Импорт можно использовать для дополнения состава группы из файла. После проверки найденных записей сохраните группу. Подробнее: *Импорт записей в списки выбора*

При нажатии на кнопку Добавить Группу откроется страница добавления группы со следующими вкладками:



Основная информация

Содержит поля:

1. Имя группы — наименование группы

Примечание

- В имени можно использовать запятые и другие печатные спецсимволы, например `Офис, склад` или `Отдел [1]`
- Вводить символы нужно без ручного экранирования: сервер обрабатывает их при создании и переименовании группы, отображении в дереве организации и выборе группы для выполнения задач
- Управляющие символы, включая перенос строки и табуляцию, недопустимы

2. Группа LDAP — наименование группы в LDAP
3. Группа в KeyCloak — наименование группы в KeyCloak

Подсказка

Указание названия группы в LDAP или KeyCloak производит связывание с локальной группой на сервере **RuDesktop** для получения прав

4. Права доступа — права доступа, устанавливаемые для создаваемой группы. Подробнее о *правах*

Пользователи

На данной вкладке размещена таблица добавления пользователей в группу

Таблица разделена на 2 блока:

1. Доступные пользователи
2. Выбранные пользователи

Для добавления пользователя в группу необходимо кликнуть в блоке **«Доступные пользователи»** на необходимого пользователя и далее кликнуть на между блоков или двойным кликом по имени пользователя, после чего в меню действий нажать на кнопку Сохранить или Сохранить и продолжить

Примечание

В группу можно добавлять неограниченное количество пользователей

Примечание

Помимо поштучного добавления доступны массовые действия над всем списком — кнопки Добавить и сохранить все и Очистить список и сохранить. Они доступны только после сохранения записи. При большом количестве элементов действие выполняется в фоновом режиме: отображается индикатор прогресса со счётчиком и кнопка Отменить задачу, а списки блокируются до завершения операции

Устройства

На данной вкладке размещена таблица добавления устройств в группу

Таблица разделена на 2 блока:

1. Доступные устройства
2. Выбранные устройства

Для добавления устройства в группу необходимо кликнуть в блоке **«Доступные устройства»** на необходимое устройство и далее кликнуть на между блоков или двойным кликом по имени устройства, после чего в меню действий нажать на кнопку Сохранить или Сохранить и продолжить

Примечание

В группу можно добавлять неограниченное количество устройств

Примечание

Помимо поштучного добавления доступны массовые действия над всем списком — кнопки Добавить и сохранить все и Очистить список и сохранить. Они доступны только после сохранения записи. При большом количестве элементов действие выполняется в фоновом режиме: отображается индикатор прогресса со счётчиком и кнопка Отменить задачу, а списки блокируются до завершения операции

LDAP

Содержит поле LDAP объект — атрибуты группы из LDAP, заполняется автоматически при синхронизации с доменом

Важно

Вкладка отображается только суперпользователю и только для групп, импортированных из домена

Мониторинг

Содержит поля:

1. Мониторинг удалённого подключения (запись видео) — включение принудительной записи удалённой сессии с сохранением видеофайлов на стороне сервера

> **Важно**
>
> - Обратите внимание, что процесс создания видео потребляет значительные ресурсы сервера. Проверьте, что у вашего сервера достаточно **CPU** и **RAM** для обработки записей без ущерба для производительности. При необходимости увеличьте доступные ресурсы
> - Качество записанного видео можно изменить в *настройках сервера*

2. Мониторинг передачи файлов — включение принудительной записи удалённой передачи файлов с сохранением записей на стороне сервера

> **Важно**
>
> - Если функции активированы, все подключения будут осуществляться через RELAY (мост)
> - Записи видео и действий в передаче файлов можно найти во вкладках *Записи сессии* или *Записи передачи файлов*. Используйте эти вкладки для просмотра видео или действий
> - Опция **Мониторинг** будет записывать видео и действия на всех устройствах, входящих в группу

Фильтр

Можно формировать таблицу для получения определённых данных, используя фильтр:

1. Домен — фильтрация групп по принадлежности к домену

> **Подсказка**
>
> - При выборе определённого домена в таблице отобразятся группы, принадлежащие этому домену
> - При выборе **«Локальные объекты»** отобразятся группы, созданные на сервере **RuDesktop**

2. Право — фильтрация групп по назначенному праву доступа
3. Поле поиска — поиск по ключевому слову

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Массовые действия позволяют выполнить одну и ту же операцию сразу над несколькими группами, не открывая свойства каждой из них

Панель массовых действий появляется под таблицей, как только отмечена хотя бы одна группа. Общий порядок работы одинаков для всех действий:

1. Отметить необходимые группы в таблице
2. Выбрать действие в списке Действия с выбранными объектами
3. Заполнить дополнительные поля, если действие их запрашивает (формат файла) — пока обязательное поле не заполнено, кнопка Выполнить неактивна
4. Нажать на кнопку Выполнить

Важно

В панели есть кнопка Выбрать все. Она распространяет действие на **всю текущую выборку** — на все группы, отобранные фильтром и поиском, а не только на отмеченные на текущей странице. Рядом отображается счётчик Выбрано N из M или Выбраны все объекты, сбросить выбор можно кнопкой Снять выделение

Что делает каждое действие:

Действие	Что делает
Удалить выбранные группы	Удаляет группы с сервера. Пользователи и устройства, входившие в них, не удаляются — с них лишь снимается членство
Копировать выбранные Группы	Переносит содержимое отмеченных групп — права, пользователей и устройства — в **другие, уже существующие** группы. Новые группы при этом не создаются
Экспортировать выбранные группы	Выгружает в файл название группы, её группу в домене и список назначенных прав

Важно

1. Действие Копировать выбранные Группы требует права **Группы → Изменение**

2. Действие Удалить выбранные группы требует права **Группы → Удаление**
3. Действие Экспортировать выбранные группы требует права **Может экспортировать данные**
4. В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление групп

Для массового удаления групп необходимо:

1. Отметить необходимые группы в таблице
2. Выбрать действие Удалить выбранные группы
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие группы будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные группы будут удалены

Важно

Предустановленные группы сервера удалить нельзя. Если такие группы попали в выборку, они исключаются из операции, а остальные удаляются — о пропущенных группах появится сообщение вида **«... защищен от изменения»**

Примечание

При удалении группы входившие в неё пользователи и устройства не удаляются — с них снимается только членство в этой группе. Вместе с группой перестают действовать *доступы* и права, которые выдавались через неё

Копирование групп

Несмотря на название, действие **не создаёт новых групп**. Оно берёт содержимое отмеченных (исходных) групп и добавляет его в другие, уже существующие группы, которые выбираются на открывшейся странице

Копировать можно три вида содержимого, каждый включается отдельным флагом:

Параметр копирования	Что переносится	По умолчанию
Скопировать права	Права, назначенные исходным группам	Включён
Скопировать пользователей	Пользователи, состоящие в исходных группах	Выключен
Скопировать устройства	Устройства, входящие в исходные группы	Выключен

Для массового копирования содержимого групп необходимо:

1. Отметить исходные группы в таблице
2. Выбрать действие Копировать выбранные Группы
3. Нажать на кнопку Выполнить
4. Откроется страница **«Копирование групп»**: в блоке Исходные группы перечислены отмеченные группы, в блоке Параметры копирования — флаги, а в блоке Группы выбираются группы-получатели
5. Отметить нужные параметры копирования
6. Отметить одну или несколько групп-получателей (доступны поиск по названию и кнопки Выбрать все в загруженном списке и Отменить выбор)
7. Нажать на кнопку Копировать группы

   Можно отменить данную операцию, нажав на кнопку Нет, вернуться назад
8. Содержимое исходных групп будет добавлено в выбранные группы

Важно

1. Содержимое **добавляется**, а не заменяет существующее: права, пользователи и устройства групп-получателей сохраняются, а совпадающие записи повторно не добавляются
2. Если отмечено несколько исходных групп, в каждую группу-получатель попадает объединённое содержимое всех исходных
3. Исходные группы не изменяются и в списке получателей не отображаются — скопировать группу саму в себя нельзя

Примечание

Список групп-получателей подгружается по мере прокрутки, поэтому кнопка Выбрать все в загруженном списке отмечает только уже загруженные группы. Чтобы найти группу, которой нет в видимой части списка, воспользуйтесь поиском

Экспорт групп

Для массового экспорта групп необходимо:

1. Отметить необходимые группы в таблице
2. Выбрать действие Экспортировать выбранные группы
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Имя группы` — наименование группы
2. `DN` — путь до группы в LDAP

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства группы
2. `Удалить` — при выборе этого пункта группа будет удалена

Важно

Предустановленные группы удалить нельзя

3. `Копировать группу` — при выборе этого пункта будет создана копия группы с тем же набором прав, пользователей и устройств
4. `История изменений` — при выборе этого пункта будет отображена история группы: создание/редактирование и пользователь, который выполнил данные операции

Свойства групп

Редактирование

Подробнее о *вкладках и полях группы*

Меню действий

Меню действий расположено на всех вкладках страницы свойств



Имеет следующие возможности:

1. Сохранить - производит сохранение внесённых изменений и перенаправляет на страницу **«Группы»**
2. Сохранить и продолжить - производит сохранение внесённых изменений и позволяет остаться на странице свойств для выполнения дальнейших операций
3. Удалить - производит удаление группы и перенаправляет на страницу **«Группы»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления группы
2. После подтверждения удаления группы произойдёт переход на страницу **«Группы»** и появится уведомление Группа была успешно удалена

Важно

Предустановленные группы удалить нельзя — кнопка для них недоступна

4. История изменений - отображает все изменения, выполненные для этой группы
5. Копировать группу - создаёт копию текущей группы с тем же набором прав, пользователей и устройств

2.11.4 Домены

Домены - это страница для добавления домена и его параметров для дальнейшей синхронизации

Подсказка

Интеграция с LDAP доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

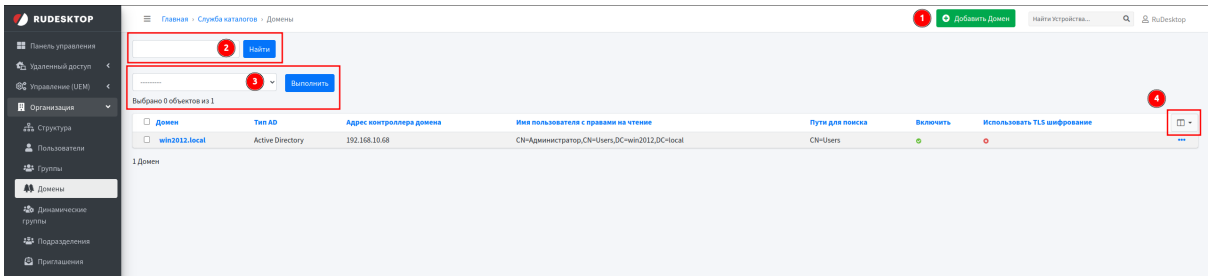
Примечание

Интеграция позволяет:

- Авторизовать доменных пользователей в **RuDesktop** по их учётным данным из LDAP
- Создавать группы RuDesktop на основе LDAP-групп
- Распределять устройства и пользователей на основании LDAP-групп

Описание страницы

На странице «**Домены**» отображаются:



1. Кнопка Добавить Домен
2. Поиск
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Сценарии использования

RuDesktop поддерживает два режима интеграции с доменом

Перед сохранением настроек стоит определиться, какой режим нужен - это влияет на необходимость периодической синхронизации

Только авторизация

Доменные пользователи входят в **RuDesktop** по своему обычному логину и паролю - сервер проверяет их через LDAP-подключение к контроллеру домена

Учётная запись в **RuDesktop** создаётся автоматически при первом входе; при входе также обновляются её данные и членство в группах. Полный список объектов домена заранее не загружается. **Когда подходит:**

- Не нужно заранее видеть в **RuDesktop** всех пользователей домена и назначать им права до входа
- Нет требования автоматически удалять учётные записи при отключении пользователя в домене

Что настроить: заполнить вкладку Основная информация, активировать Включить и сохранить настройки. Кнопка Синхронизировать не требуется

Авторизация и периодическая синхронизация

Пользователи и группы загружаются из домена в **RuDesktop**, а у уже зарегистрированных устройств обновляются данные LDAP и членство в группах. Параллельно работает доменная авторизация

Когда подходит:

- Нужно заранее видеть всех пользователей домена и назначать им права до их первого входа
- Требуется автоматически удалять учётные записи отключённых или удалённых в домене пользователей
- Нужно привязать уже зарегистрированные устройства к доменным группам

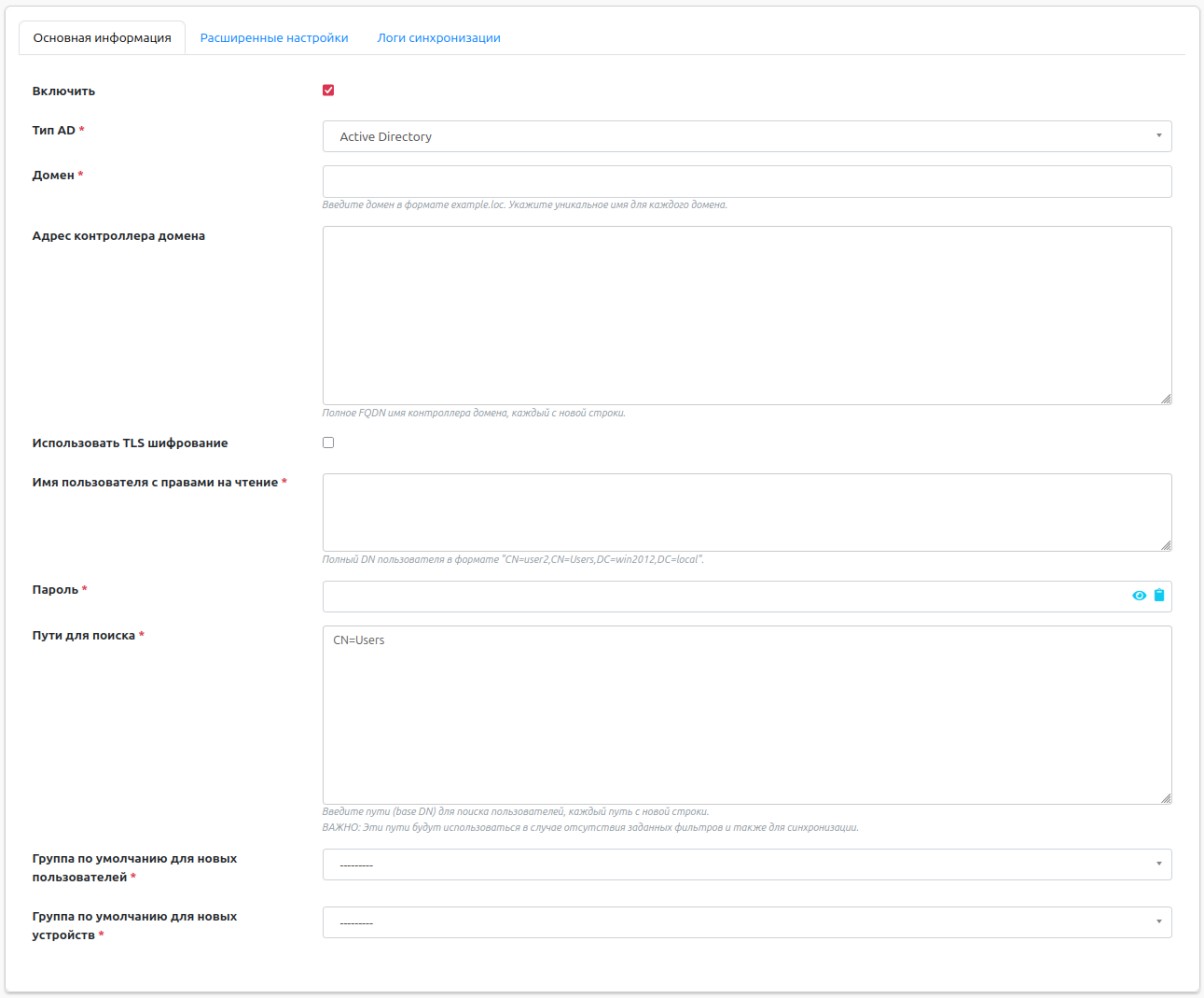
Что настроить: дополнительно к настройкам предыдущего режима - запустить синхронизацию вручную или настроить её по расписанию через политику *Синхронизация со службой каталогов*

Важно

На сервере одновременно может быть подключено несколько доменов с активным флагом Включить - пользователи разных доменов не пересекаются благодаря суффиксу `@<domain>` в логине

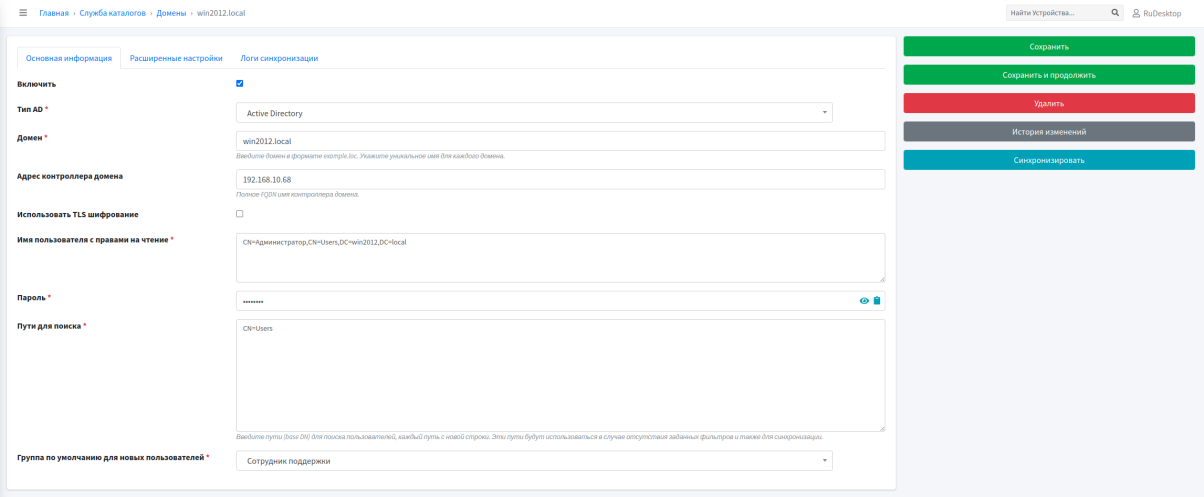
Добавление домена

Перед настройкой проверьте, что сервер RuDesktop разрешает FQDN контроллера через DNS и имеет доступ к его LDAP-службе: обычно **389/TCP** для LDAP или **636/TCP** для LDAPS. Подготовьте учётную запись с правами чтения нужных пользователей, групп, устройств и их атрибутов



При нажатии на кнопку Добавить Домен откроется страница добавления домена со следующими вкладками:

Основная информация



1. Поле Включить - активация связи с доменом

   Если настройка выключена, синхронизация и авторизация доменных пользователей не выполняются

2. Поле Тип AD - тип службы каталогов: `Active Directory`, `FreeIPA` или `OpenLDAP`

   От выбранного типа зависят стартовые LDAP-фильтры и атрибуты, по которым ищутся пользователи и группы

3. Поле Домен - уникальное имя домена в формате `example.loc`

> **Важно**
>
> Указывайте именно корневое имя домена, а не FQDN контроллера
>
> Это значение автоматически преобразуется в базовый DN (`example.loc` → `DC=example,DC=loc`) и используется как корень поиска при расширенных фильтрах, а также при автоматическом дописывании DN к Пути для поиска
>
> Если в поле ошибочно указать FQDN с префиксом узла (например, `dc01.example.loc`), базовый DN получит лишний компонент (`DC=dc01,DC=example,DC=loc`) - он не совпадёт с реальным корнем дерева LDAP, и поиск не найдёт объекты
>
> Для адреса контроллера используйте отдельное поле Адрес контроллера домена

4. Поле Адрес контроллера домена - FQDN-имя контроллера домена

> **Подсказка**
>
> Если контроллеров несколько, укажите каждый адрес с новой строки. **RuDesktop** будет последовательно пробовать контроллеры при ошибках связи. Ошибки учётных данных или прав нужно исправить отдельно — переключение на другой контроллер их не устраняет

5. Поле Использовать TLS шифрование - включение защищённого подключения по протоколу LDAPS

> **Важно**
>
> При включении этой настройки появляется поле Файл сертификата - в него необходимо загрузить корневой сертификат домена
>
> Без сертификата подключение не будет установлено

6. Поле Игнорировать ошибку сертификата - отображается при включении TLS

   Отключает строгую проверку цепочки доверия сертификата контроллера домена

Обычно оставляйте флаг выключенным: загрузите сертификат доверенного центра, выдавшего сертификат контроллера. Самоподписанный корневой сертификат не требует отключения проверки, если доверие настроено правильно

7. Поле Файл сертификата - сертификат доверенного центра сертификации в формате **PEM**

   Расширение может быть `.pem` или `.crt`, но содержимое должно быть в PEM. Файл необходим для подключения по TLS, в том числе при включённом флаге игнорирования ошибки сертификата

8. Поле Имя пользователя с правами на чтение - учётная запись для подключения к LDAP

   Подсказка

   Рекомендуется указывать **полный DN** пользователя, например `CN=user2,CN=Users,DC=win2012,DC=local`

   Если указано только имя (`user2`), значение поля Пути для поиска должно содержать путь до контейнера с этим пользователем - иначе **RuDesktop** не сможет найти учётную запись для привязки

9. Поле Пароль - пароль учётной записи с правами на чтение

10. Поле Пути для поиска - список base DN, в которых выполняется поиск пользователей, групп и устройств

    Подсказка

    Каждый путь указывается с новой строки

    Пути используются для поиска тех типов объектов, для которых не задан дополнительный фильтр на вкладке Расширенные настройки. Если соответствующий фильтр заполнен, поиск выполняется от корня домена, а указанные здесь пути не применяются

    Если путь не содержит `DC=...`, к нему автоматически добавляется DN домена

11. Поле Добавлять Primary Group - включить, если первичную группу пользователя из **Active Directory** (например, `Domain Users`) нужно учитывать при синхронизации членства

    По умолчанию AD не указывает primary group в атрибуте `memberOf`, и без этой настройки она не будет привязана к пользователю в **RuDesktop**

12. Поле Группа по умолчанию для новых пользователей - группа, назначаемая пользователю, если по результатам обработки LDAP ему не назначена ни одна доменная группа

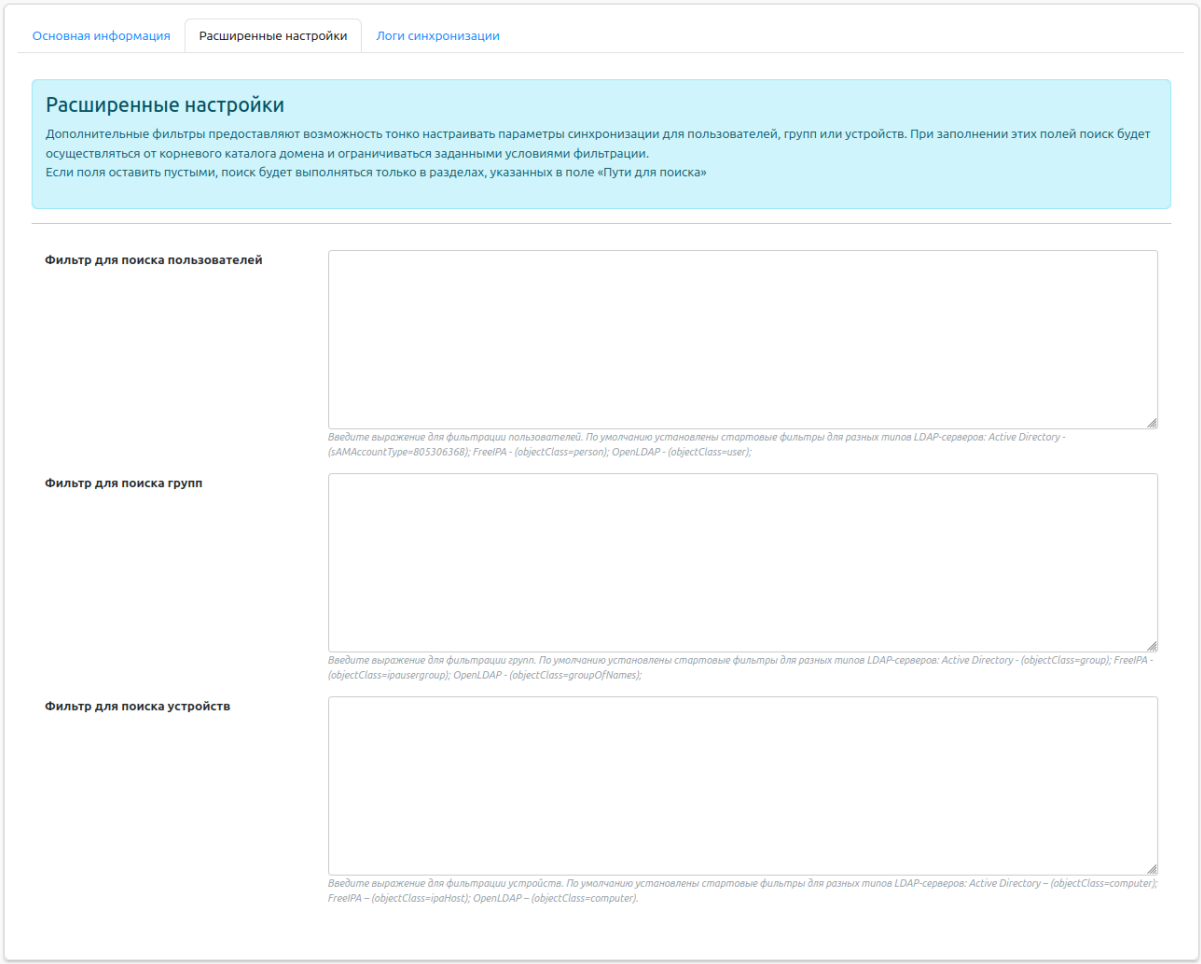
13. Поле Группа по умолчанию для новых устройств - группа для зарегистрированного устройства, которому при синхронизации не назначена ни одна доменная группа

> **Подсказка**
>
> Можно оставить значение ----------. Группы по умолчанию учитываются и при обновлении существующих записей; отсутствие группы по умолчанию не мешает синхронизации

14. Поле Назначить статус персонала новым пользователям - выдаёт новым пользователям из домена статус сотрудника и доступ в административную панель **RuDesktop**

    Снимайте флаг, если доменные пользователи должны попадать только в портал, без доступа к админке. Доступные разделы и действия определяются правами пользователя и его групп. Изменение флага не меняет статус уже созданных пользователей

Расширенные настройки



Расширенные фильтры позволяют тонко ограничить, какие пользователи, группы и устройства попадают в синхронизацию

Важно

Если поля оставить пустыми, основной поиск выполняется в разделах, указанных в поле Пути для поиска, с базовым фильтром по типу объекта. При синхронизации дополнительно могут учитываться участники найденных групп вне этих разделов

Если поле фильтра заполнено, поиск выполняется **от корневого каталога домена** - базовый DN формируется из поля Домен на вкладке Основная информация

Поле «Пути для поиска» в этом случае игнорируется для соответствующего типа объектов.

Например, если задан фильтр пользователей, подходящие пользователи ищутся по всему домену, даже за пределами указанных путей. Если фильтры групп и устройств при этом пусты, для их поиска продолжают использоваться Пути для поиска

Введённое условие добавляется к базовому фильтру через логическое **И**, поэтому в поле нужно указывать только дополнительные условия, без повторения базового фильтра по типу объекта

Если в поле Домен указано не корневое имя, а FQDN с префиксом узла (например, `dc01.example.loc`), корень поиска получит лишний компонент (`DC=dc01,DC=example,DC=loc`) и расширенные фильтры не найдут объекты в LDAP

1. Фильтр для поиска пользователей - дополнительные условия для отбора пользователей

Подсказка

Базовый фильтр (применяется автоматически):

- Active Directory: `(sAMAccountType=805306368)`
- FreeIPA: `(objectClass=person)`
- OpenLDAP: `(objectClass=user)`

Примеры дополнительных условий для Active Directory:

- Только пользователи указанной группы:

```
(memberOf=CN=rudesktop_users,OU=RuDesktop,
↪DC=rudesktop,DC=ad)
```

- Пользователи, состоящие в одной из нескольких групп:

```
(|(memberOf=CN=group1,OU=RuDesktop,DC=
↪rudesktop,DC=ad)(memberOf=CN=group2,OU=
↪RuDesktop,DC=rudesktop,DC=ad))
```

- Пользователи, состоящие одновременно в двух группах:

```
(&(memberOf=CN=group1,OU=RuDesktop,DC=
↪rudesktop,DC=ad)(memberOf=CN=group2,OU=
↪RuDesktop,DC=rudesktop,DC=ad))
```

2. Фильтр для поиска групп - дополнительные условия для отбора групп

Подсказка

Базовый фильтр (применяется автоматически):

- Active Directory: `(objectClass=group)`
- FreeIPA: `(objectClass=ipausergroup)`
- OpenLDAP: `(objectClass=groupOfNames)`

Пример дополнительного условия:

- Группы, имя которых начинается на `group`:

```
(cn=group*)
```

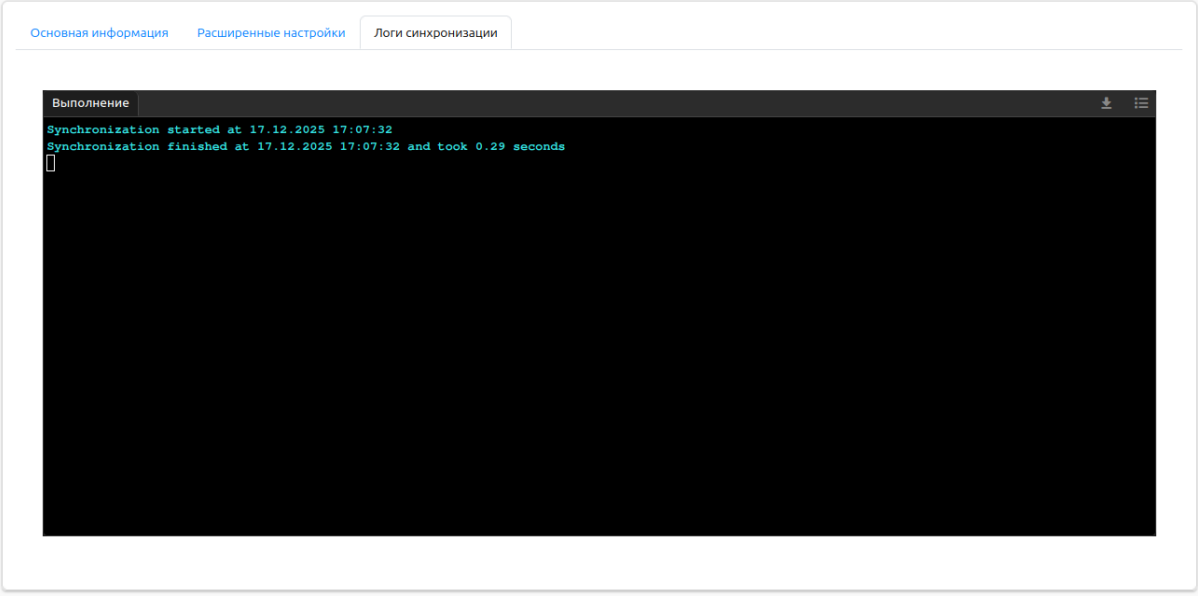
3. Фильтр для поиска устройств - дополнительные условия для отбора устройств

Подсказка

Базовый фильтр (применяется автоматически):

- Active Directory: `(objectClass=computer)`
- FreeIPA: `(objectClass=ipaHost)`
- OpenLDAP: `(objectClass=computer)`

Логи синхронизации



На этой вкладке отображаются логи выполнения синхронизации с доменом.

Ручной запуск выполняется в фоне: дождитесь сообщения о завершении и проверьте ошибки и предупреждения

Проверка настройки

1. Сохраните домен с включённым флагом Включить. При сохранении RuDesktop проверяет подключение к LDAP под указанной учётной записью; при ошибке активные настройки не сохраняются
2. Проверьте вход одного доменного пользователя, выбрав нужный домен на странице авторизации
3. Если нужна синхронизация, запустите её вручную и дождитесь завершения во вкладке Логи синхронизации
4. Проверьте пользователей, группы и несколько уже зарегистрированных устройств, а также назначенные права
5. После проверки настройте расписание синхронизации, если оно требуется

Сохранение домена само по себе не запускает периодическую синхронизацию. Успешное подключение при сохранении также не подтверждает правильность фильтров и полноту прав чтения всех объектов

Поиск

`Поле поиска` - поиск по имени домена, адресу контроллера или типу службы каталогов

Для выполнения поиска заполните поле и нажмите кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные домены - удаляет выбранные домены из таблицы
2. Экспортировать выбранные домены - позволяет экспортировать в файл выбранные домены

> **Примечание**
>
> После выбора этого действия необходимо выбрать формат файла

> **Важно**
>
> В зависимости от прав доступа некоторые действия могут отсутствовать

Для выполнения действия нажмите кнопку Выполнить

Удаление доменов

Для массового удаления доменов необходимо:

1. Отметить необходимые домены в таблице
2. Выбрать действие Удалить выбранные домены
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие домены будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные домены будут удалены

Экспорт доменов

Для массового экспорта доменов необходимо:

1. Отметить необходимые домены в таблице
2. Выбрать действие Экспортировать выбранные домены
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. Домен - показывает уникальное имя домена
2. Тип AD - показывает тип службы каталога: Active Directory, FreeIPA или OpenLDAP
3. Адрес контроллера домена - показывает IP-адрес или FQDN-имя контроллера домена
4. Имя пользователя с правами на чтение - отображение имени доменного пользователя, имеющего права на чтение
5. Пути для поиска - отображение путей для поиска пользователей или устройств
6. Включить - отображение активации подключения к домену
7. Использовать TLS шифрование - отображение использования TLS-шифрования

Операции

При нажатии на кнопку в правой части таблицы открывается контекстное меню

Доступные действия:

1. Редактировать - при выборе этого пункта откроются свойства домена
2. Удалить - при выборе этого пункта домен будет удален
3. История изменений - при выборе этого пункта будет отображена история домена: создание/редактирование и пользователь, который выполнил данные операции
4. Синхронизировать - при выборе этого пункта будет выполнена синхронизация с доменом

> **Важно**
>
> Синхронизацию с доменом выполнять необязательно, чтобы работала авторизация доменного пользователя
>
> Для этого достаточно добавить домен и сохранить настройки - учётная запись будет создана автоматически при первом входе

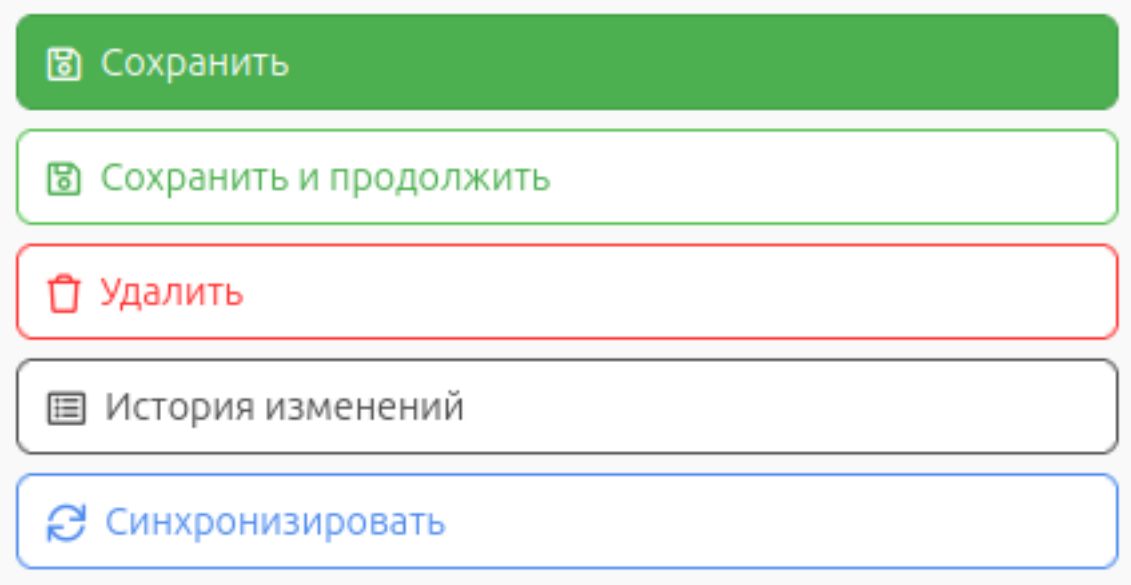
Свойства домена

Редактирование

При нажатии на кнопку Редактировать откроется страница свойств

Подробнее о вкладках и полях см. в разделе *Добавление домена*

Меню действий



Доступные действия:

1. Сохранить - производит сохранение внесенных изменений и перенаправляет на страницу **«Домены»**
2. Сохранить и продолжить - производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить - производит удаление домена и перенаправляет на страницу **«Домены»**

> **Примечание**
>
> 1. После нажатия на кнопку Удалить откроется страница подтверждения удаления домена
> 2. После подтверждения удаления домена произойдет переход на страницу **«Домены»** и появится уведомление Домен «НАЗВАНИЕ_ДОМЕНА» был успешно удален

4. История изменений - отображает все изменения, выполненные для этого домена
5. Синхронизировать - производит синхронизацию с доменом

Описание работы синхронизации с доменом

Синхронизация запускается кнопкой Синхронизировать или политикой *Синхронизация со службой каталогов*, которая периодически запускает синхронизацию со всеми активными доменами на сервере. **RuDesktop** обращается к контроллеру домена под учётной записью с правами на чтение и переносит данные в локальную базу в фиксированном порядке: сначала группы, затем устройства, затем пользователи и членство, в конце - очистка устаревших записей

Большие группы Active Directory

Контроллер домена может возвращать состав большой группы несколькими частями. RuDesktop дочитывает эти части автоматически - отдельную настройку размера группы в интерфейсе задавать не требуется. При синхронизации могут учитываться и участники найденных групп, расположенные вне заданных путей поиска. Само попадание в состав группы не отменяет остальные условия отбора пользователей и устройств при синхронизации

> **Важно**
>
> Если дочитать состав группы не удалось, например контроллер не вернул запрошенную часть, синхронизация этого домена сообщает об ошибке. После ошибки нельзя считать состав групп полностью обновлённым. Часть изменений уже могла сохраниться - устранить причину и повторить синхронизацию

Для проверки результата:

1. Выполнить синхронизацию домена и дождаться завершения
2. Проверить журнал на ошибки чтения участников группы
3. Проверить несколько ожидаемых пользователей и их группы в RuDesktop, включая участников вне основных путей поиска, если такие есть
4. При ошибке проверить доступность контроллера и права учётной записи на чтение объектов, затем повторить синхронизацию

Синхронизация групп

RuDesktop ищет группы в Пути для поиска, а при заполненном Фильтр для поиска групп — от корня домена. Для найденных групп создаются соответствующие группы RuDesktop или используются уже существующие записи

Что переносится:

- **Имя группы** (`cn`) - записывается в поле Название и одновременно в поле LDAP-группа локальной группы
- **Полный DN группы** - сохраняется и используется для однозначной привязки пользователя к группе при последующих синхронизациях

Важно

Права доступа локальных групп **RuDesktop** при синхронизации не изменяются

Назначение прав остаётся за администратором - это сделано для того, чтобы изменения в LDAP не могли случайно переписать набор разрешений на сервере

Синхронизация устройств

RuDesktop ищет в домене объекты по фильтру устройств (по умолчанию `computer` для AD, `ipaHost` для FreeIPA) и сопоставляет их с уже зарегистрированными в **RuDesktop** устройствами: сначала по имени хоста, затем, если совпадение не найдено, по имени вида `<имя хоста>.<домен>`. Регистр не учитывается. При нескольких совпадениях устройство не выбирается автоматически — в журнале отмечается конфликт

Что обновляется у найденного устройства:

- **DN** устройства в LDAP
- **Атрибуты LDAP** - записываются в поле `facts.ldap` устройства для дальнейшего использования в политиках и фильтрах
- **Членство в группах** - устройство привязывается к локальным группам, которые соответствуют его LDAP-группам (атрибут `memberOf`)

Примечание

Если устройство есть в домене, но ещё не зарегистрировано в **RuDesktop**, оно не появится в списке - синхронизация только дополняет данные у уже зарегистрированных устройств

Синхронизация пользователей

RuDesktop ищет пользователей по фильтру пользователей (по умолчанию `(sAMAccountType=805306368)` для AD, `(objectClass=person)` для FreeIPA). Без дополнительного фильтра используются Пути для поиска и участники найденных групп; с дополнительным фильтром — корень домена

Что переносится:

- **Логин** - сохраняется в формате `<username>@<domain>` (см. *Формат имени пользователя в RuDesktop*)
- **Полное имя**, **email**, **телефон**, **компания**
- **Членство в группах** - пользователь привязывается к локальным группам, соответствующим его LDAP-группам по DN

  Если включён параметр Добавлять Primary Group, дополнительно учитывается первичная группа

Важно

Вложенные группы Active Directory. При синхронизации и при входе по доменной учётной записи RuDesktop назначает пользователю группы из его атрибута `memberOf` с учётом путей поиска и фильтров домена. Родительские группы по цепочке членства не добавляются. Область группы (Global, Universal или Domain Local) этого правила не меняет. Настройки глубины вложенности нет. Параметр **Добавлять Primary Group** добавляет только основную группу пользователя

Например, Анна входит в группу **ИТ-филиал**, а та входит в группу **Операторы RuDesktop**. Если права назначены только операторам, Анна не получит их через **ИТ-филиал**. Чтобы предоставить ей доступ, добавьте Анну непосредственно в группу операторов или назначьте необходимые права локальной группе RuDesktop, связанной с **ИТ-филиал**

Если по результатам синхронизации пользователю не назначена ни одна доменная группа, используется Группа по умолчанию для новых пользователей, если она задана

Примечание

Найденные пользователи с признаком *Disabled* в **Active Directory** при синхронизации удаляются из **RuDesktop**. Это удаление учётной записи, а не только снятие флага её активности

Привязка устройств к пользователям

После синхронизации пользователей домена устройства автоматически связываются с соответствующими доменными учётными записями - по совпадению имени пользователя ОС и домена, который сообщает клиент **RuDesktop** при подключении

Синхронизация также обновляет привязку уже зарегистрированных устройств этого домена

Подсказка

Если связь отсутствует, проверьте имя пользователя ОС и домен в данных устройства и повторите синхронизацию. Для отдельной пакетной привязки администратор может воспользоваться командой *rude ldap link*

Подробнее о появлении ФИО владельца в таблице устройств - *Как заполняется столбец «Полное имя»*

Что происходит с удалёнными или отключёнными объектами

Синхронизация сверяет записи с полученным результатом поиска, а не со всем содержимым LDAP:

- **Пользователи** с сохранённым DN и логином `<username>@<domain>`, отсутствующие в полученном списке активных пользователей, удаляются. Общая очистка этого списка выполняется, если при синхронизации найден хотя бы один активный пользователь
- **Группы**, импортированные из этого домена и не найденные при поиске - удаляются

  Группа по умолчанию для новых пользователей при этом не трогается, даже если её DN отсутствует в LDAP
- **Устройства**, не попавшие в результат поиска, не удаляются — у них очищается поле DN, то есть привязка к объекту каталога

Важно

Изменение путей или фильтров может исключить ранее импортированные записи из результата поиска и привести к их удалению или отвязке. Перед запуском проверьте новую область поиска

Примечание

При синхронизации **список групп пользователя или устройства заменяется** результатом LDAP-сопоставления, связанными локальными группами и, при необходимости, группой по умолчанию. Ручные назначения

других групп не сохраняются. При обычном входе пользователя обновляются группы со связью LDAP; локальные группы без такой связи сохраняются

Формат имени пользователя в RuDesktop

Все пользователи, импортированные из домена, сохраняются в **RuDesktop** под именем по шаблону `<username>@<domain>` - это исключает конфликты с локальными пользователями и с пользователями из других доменов

Например: пользователь `user` из домена `example.loc` будет сохранён в **RuDesktop** как `user@example.loc`

Примечание

На странице авторизации выберите нужный домен в списке справа от логина и введите обычный доменный логин без суффикса. Суффикс `@<domain>` добавляется сервером автоматически. Подробнее — *Страница авторизации*

Имя со суффиксом отображается в списке пользователей в административной панели **RuDesktop**

Связь группы домена с локальной группой RuDesktop

Локальная группа **RuDesktop** используется для назначения прав, а группа домена - как внешний источник членства пользователя в этой группе

Связь устанавливается через поле Группа LDAP на локальной группе. При синхронизации **RuDesktop** автоматически создаёт локальные группы для всех найденных в домене групп и заполняет у них поле Группа LDAP

Для уже существующих локальных групп администратор может вручную указать связь - это удобно, когда права в **RuDesktop** настроены на стороне локальной группы, а членство нужно брать из домена. Чтобы вручную связать группу домена с локальной группой **RuDesktop**:

1. Открыть административную панель **RuDesktop**
2. Перейти в раздел **Организация** → *Группы*
3. Создать новую локальную группу или открыть существующую группу
4. На вкладке **Основная информация** в поле Группа LDAP указать имя группы домена так, как оно передаётся из LDAP (атрибут `cn`)

Подсказка

Указывайте только имя группы (например, `support`), без полного пути DN

> По полному DN группа привязывается к пользователю автоматически при синхронизации - поле Группа LDAP нужно для случаев, когда локальная группа создаётся в **RuDesktop** вручную

5. Настроить права доступа локальной группы **RuDesktop**
6. Нажать на кнопку Сохранить

После этого при синхронизации или авторизации пользователь, состоящий в указанной группе домена, будет автоматически добавлен в локальную группу и получит её права

Важно

Если у пользователя в LDAP отсутствует соответствующая группа, локальная группа из его членства убирается - как при синхронизации, так и при авторизации. **RuDesktop** при каждом входе доменного пользователя сверяет его группы с актуальным состоянием LDAP и сбрасывает все локальные группы со связкой в LDAP, которые не подтверждены доменом

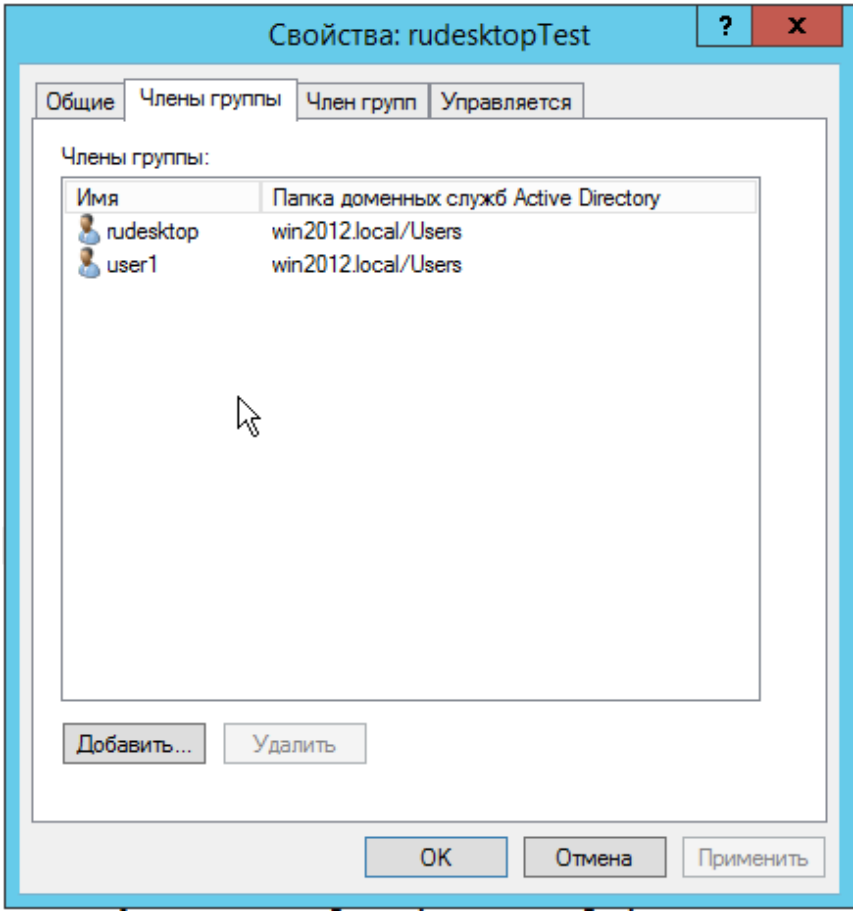
Поэтому ручное добавление пользователя в такую группу не сохраняется - чтобы право работало постоянно, добавляйте пользователя в нужную группу на стороне домена

Примеры

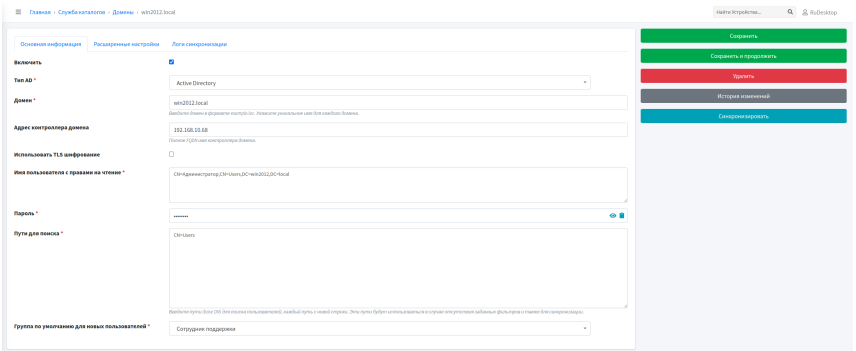
Active Directory

В качестве примера настройки интеграции с LDAP используются:

- Active Directory
- Windows Server 2012 R2
    1. Перейти на сервер Active Directory
    2. Открыть окно **«Выполнить»**, нажав клавиши Win + R
    3. Ввести `dsa.msc` и нажать Enter
    4. Перейти в `Users`
    5. Создать группу и поместить в нее пользователей



6. Открыть веб-интерфейс **RuDesktop**
7. Перейти на страницу **«Домены»**
8. Нажать на кнопку Добавить Домен
9. Заполнить поля



Важно

- В поле Имя пользователя с правами на чтение возможно указать полный DN пользователя в формате `CN=user2,CN=Users,DC=win2012,DC=local`

- Если в поле Имя пользователя с правами на чтение указали CN пользователя, то в Пути для поиска необходимо указать полный путь до его расположения
  - Например, в Имя пользователя с правами на чтение указали user2, то в Пути для поиска необходимо указать `CN=Users, DC=win2012,DC=local`

10. Выполнить синхронизацию

    После синхронизации будут созданы пользователи и группы, соответствующие условиям поиска. Для устройств обновятся данные уже зарегистрированных клиентов RuDesktop

    После выполненных действий можно авторизовываться под доменным пользователем

Альт Домен

Для подключения к **Альт Домен на базе Samba AD** используйте тип **Active Directory**

1. Убедитесь, что на контроллере настроен LDAPS и его адрес доступен с сервера RuDesktop
2. Получите у администратора домена сертификат центра, выдавшего сертификат контроллера, в формате PEM
3. На странице **Домены** добавьте домен и заполните:
   - Домен — корневое имя, например `test.alt`
   - Адрес контроллера домена — например `lnx-dc11.test.alt`
   - Тип AD — **Active Directory**
   - Использовать TLS шифрование — включено
   - Файл сертификата — сертификат доверенного центра
   - Учётную запись с правами чтения, пароль и пути поиска
4. Оставьте Игнорировать ошибку сертификата выключенным при корректно настроенном доверии
5. Сохраните активный домен и проверьте вход пользователя. При необходимости запустите синхронизацию и проверьте её журнал

Создавать новый центр сертификации специально для RuDesktop не требуется, если LDAPS уже настроен. Порядок настройки сертификатов на контроллере приведён в разделе «Настройка LDAP через SSL (LDAPS)» руководства Альт Домен[25]

[25] https://docs.altlinux.org/ru-RU/alt-domain/11.1/html/alt-domain/ldaps.html

2.11.5 Динамические группы

Доступны только в UEM версии

Динамические группы — это инструмент, позволяющий объединять устройства по заданным параметрам. Группировку можно выполнять на основе фактов Ansible, с использованием SQL-запросов или по результатам фильтра устройств

Подсказка

Страница **«Динамические группы»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Подсказка

По умолчанию на сервере уже есть пять предустановленных динамических групп, которые покрывают типовые сценарии:

- Семейство OS — группировка по семейству ОС (Windows, Linux, macOS и т.д.) на основе факта `ansible_os_family`
- Тип OS — группировка по дистрибутиву и его версии (например, «Ubuntu 22.04», «Windows 10») на основе фактов `ansible_distribution` и `ansible_distribution_version`
- Подсеть — группировка устройств по принадлежности к одной подсети (`/24`)
- Устройства Active Directory — группировка устройств, импортированных из Active Directory, по их месту в дереве AD
- Устройства ОС — группировка устройств по парам факт-значений из инвентаризации (например, по марке, модели, версии установленного ПО)

Как это работает

В отличие от обычных *групп*, состав которых задаётся вручную, **динамические группы** формируются автоматически на основе данных самих устройств. Это позволяет получать актуальные группировки без ручного сопровождения

Группа описывается **выражением**, которое выполняется на сервере и возвращает список устройств. Поддерживаются три типа выражений:

- `Маска` — Ansible-выражение, использующее факты устройств (ОС, подсеть, версия, пользовательские факты и т.д.)
- `SQL запрос` — SQL-запрос к базе данных сервера, возвращающий идентификаторы устройств и значение для группировки
- `Группа из фильтра` — фиксированный набор условий, заданный фильтром на странице *Устройства*

Результат выполнения выражения может быть **сгруппирован** по значению — тогда из одной записи **«Динамической группы»** автоматически создаётся набор **«Загруженных динамических групп»** (например, по одной на каждую найденную подсеть или версию ОС). Загруженные группы используются для запуска политик, фильтрации устройств, в области действия *задач* и в формах учётных записей пользователей

Важно

Состав загруженных динамических групп пересчитывается во время **инвентаризации устройств**:

- при ручном нажатии на кнопку Проверить и загрузить динамические группы в свойствах группы — сервер запускает инвентаризацию на устройствах и по её результатам обновляет группировки;
- при выполнении политики *Инвентаризация устройств* — после сбора фактов с устройства сервер пересчитывает его принадлежность к динамическим группам всех трёх типов.

Запуск других политик (установка ПО, выполнение команд и т.д.) **не** пересчитывает динамические группы — пока на устройстве не отработала инвентаризация, новые устройства в загруженные группы не попадают, а удалённые продолжают в них числиться

Чувствительность к регистру

Имена загруженных динамических групп сравниваются **с учётом регистра**. Если выражение возвращает значения, отличающиеся только регистром символов, сервер создаёт **разные** загруженные группы для каждого варианта написания

Важно

Например, если в одной из подсетей одно устройство называется `office-pc01`, второе — `Office-PC01`, а третье — `OFFICE-PC01`, и выражение группирует устройства по hostname, на вкладке Загруженные динамические группы появятся **три отдельные группы** с этими именами — по одному устройству в каждой. Политика, привязанная к одной из них, на остальные применяться не будет

Подсказка

Чтобы избежать расхождения, приводите значения к единому регистру прямо в выражении:

- в `Маска` — Ansible-фильтром `| lower`, например `{{ ansible_hostname | lower }}`
- в `SQL запрос` — функцией `LOWER()`, например `LOWER(hostname) AS hostname_key`

- в `Группа из фильтра` — приводя само поле фильтра к нужному виду в карточке устройства

После изменения выражения нажмите Проверить и загрузить динамические группы и при необходимости удалите устаревшие загруженные группы вручную

Описание страницы

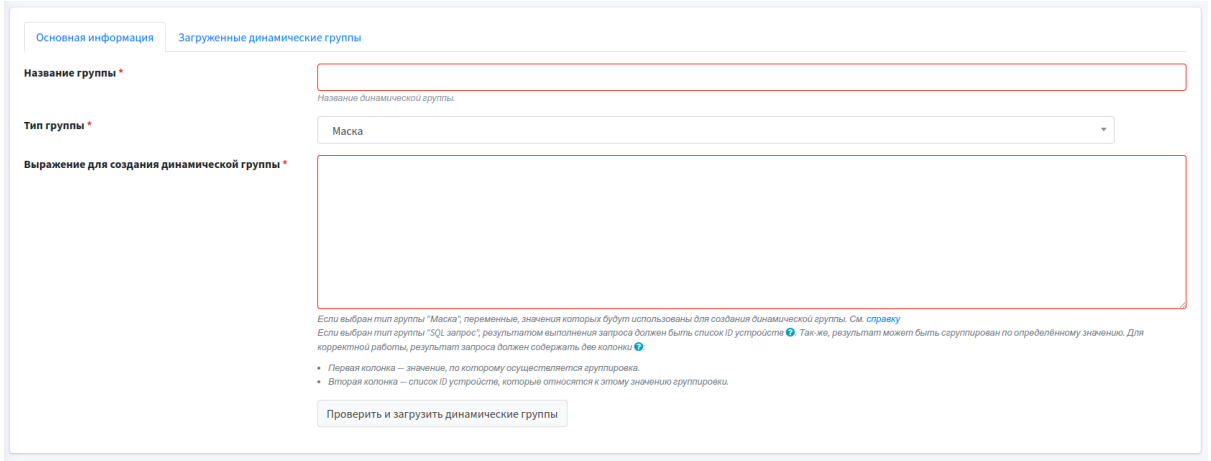
На странице **«Динамические группы»** отображено:



1. Кнопка Добавить Динамическую группу
2. Массовые действия
3. Таблица с возможностью настройки отображаемых столбцов

Добавление динамической группы

При нажатии на кнопку Добавить Динамическую группу откроется страница добавления динамической группы со следующими вкладками:



1. `Основная информация`
    1. Поле Название группы — наименование динамической группы
    2. Поле Тип группы — способ формирования группы:
        - `Маска` — на основе переменных и фактов Ansible
        - `SQL запрос` — на основе SQL-запроса к базе данных сервера
        - `Группа из фильтра` — на основе условий фильтра, заданного на странице **«Устройства»**

Подсказка

Тип `Группа из фильтра` устанавливается автоматически при создании динамической группы из применённого фильтра на странице *Устройства* — вручную выбрать его в выпадающем списке нельзя

Чтобы создать такую группу: примените на странице **«Устройства»** нужные фильтры, затем нажмите кнопку Создать динамическую группу — откроется окно ввода названия. После сохранения текущий набор условий фильтра запишется в выражение группы, а её тип автоматически станет Группа из фильтра

3. Поле Выражение для создания динамической группы — выражение для создания динамической группы может быть представлено в виде набора переменных Ansible или SQL-запроса
4. Кнопка Проверить и загрузить динамические группы — кнопка служит для выполнения Ansible-выражений или SQL-запросов для группировки устройств

2. `Загруженные динамические группы`

   Эта вкладка содержит таблицу с результатами загрузки группы:

   - `Название группы` — имя загруженной (дочерней) динамической группы
   - `Количество компьютеров` — количество устройств, входящих в загруженную группу

Подсказка

При нажатии на количество устройств произойдёт переход на страницу *Устройства* с активным фильтром по выбранной загруженной группе

Массовые действия

Доступные действия:

1. Удалить выбранные динамические группы — удаляет выбранные динамические группы из таблицы
2. Экспортировать выбранные динамические группы — позволяет экспортировать в файл выбранные динамические группы

Примечание

После выбора данного действия нужно выбрать необходимый формат файла

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление динамических групп

Для массового удаления динамических групп необходимо:

1. Отметить необходимые динамические группы в таблице
2. Выбрать действие Удалить выбранные динамические группы
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие динамические группы будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные динамические группы будут удалены

Экспорт динамических групп

Для массового экспорта динамических групп необходимо:

1. Отметить необходимые динамические группы в таблице
2. Выбрать действие Экспортировать выбранные динамические группы
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Название группы` — показывает имя динамической группы
2. `Тип группы` — показывает тип группы: Маска, SQL запрос или Группа из фильтра
3. `Выражение для создания динамической группы` — Ansible-выражение, тело SQL-запроса или сохранённый набор правил фильтра в зависимости от типа группы

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства динамической группы
2. `Удалить` — при выборе этого пункта динамическая группа будет удалена
3. `История изменений` — при выборе этого пункта будет отображена история динамической группы: создание/редактирование и пользователь, который выполнил данные операции

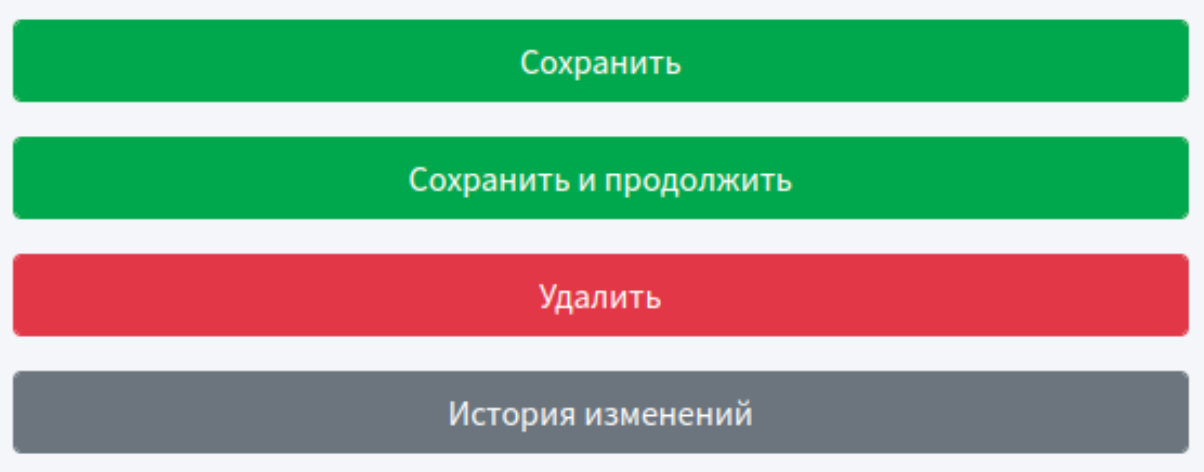
Свойства динамических групп

Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств

После чего откроется страница со свойствами динамической группы для изменения. Подробнее о *вкладках и полях*

Меню действий



Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Динамические группы»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление динамической группы и перенаправляет на страницу **«Динамические группы»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления динамической группы
2. После подтверждения удаления динамической группы произойдет переход на страницу **«Динамические группы»** и появится уведомление Динамическая группа «НАЗВАНИЕ_ГРУППЫ» была успешно удалена

4. История изменений — отображает все изменения, выполненные для этой динамической группы

Пример

Маска

Пример создания динамической группы для разделения устройств по подсетям на основе Ansible-фактов

Для создания динамической группы необходимо:

1. Нажать на кнопку Добавить Динамическую группу
2. Заполнить поля:
    1. Поле Название группы — Группировка по подсетям
    2. Поле Тип группы — Маска
    3. Поле Выражение для создания динамической группы:

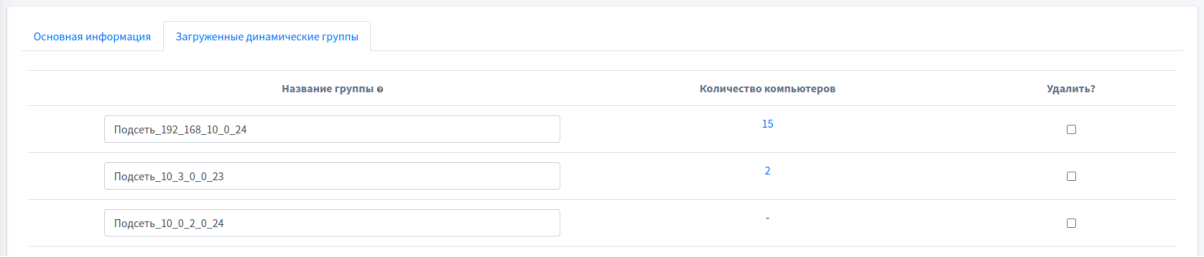
```
{{ ansible_facts | ip_subnet_filter | regex_replace('[/\.
↪]', '_') }}
```

3. Нажать на кнопку Проверить и загрузить динамические группы

    После этого откроется окно загрузки динамических групп, и начнется процесс их создания

4. После завершения загрузки динамических групп необходимо нажать на кнопку Закрыть

    Автоматически откроется вкладка **«Загруженные динамические группы»**, где будут отображены динамические группы и количество устройств в них



SQL запрос

Пример создания динамической группы для разделения устройств по подсетям на основе SQL-запроса

Для создания динамической группы необходимо:

1. Нажать на кнопку Добавить Динамическую группу
2. Заполнить поля:
    1. Поле Название группы — Группировка по подсетям
    2. Поле Тип группы — SQL-запрос
    3. Поле Выражение для создания динамической группы:

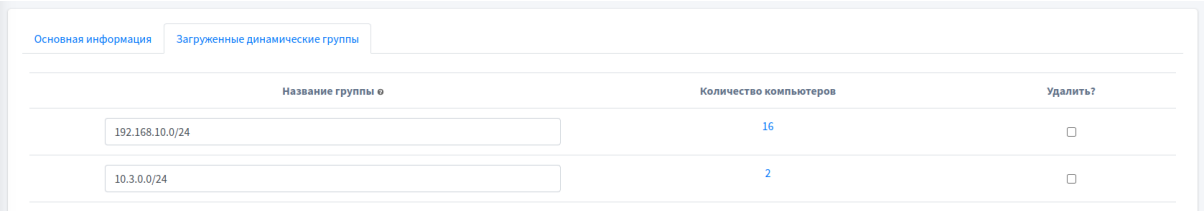
```
SELECT
    network(set_masklen(split_part(addr, ':', 1)::INET,␣
↪24)) AS subnet,
    ARRAY_AGG(id) AS device_ids
FROM
    peers_server
GROUP BY
    subnet;
```

3. Нажать на кнопку Проверить и загрузить динамические группы

    После этого откроется окно загрузки динамических групп, и начнется процесс их создания

4. После завершения загрузки динамических групп необходимо нажать на кнопку Закрыть

    Автоматически откроется вкладка **«Загруженные динамические группы»**, где будут отображены динамические группы и количество устройств в них



Пример создания динамической группы для разделения устройств по версии клиента **RuDesktop** на основе SQL-запроса

Для создания динамической группы необходимо:

1. Нажать на кнопку Добавить Динамическую группу
2. Заполнить поля:
    1. Поле Название группы — Группировка по версии клиента
    2. Поле Тип группы — SQL-запрос
    3. Поле Выражение для создания динамической группы:

```
SELECT
    version AS value,
    array_agg(id) AS servers
FROM
    peers_server
GROUP BY
    version;
```

3. Нажать на кнопку Проверить и загрузить динамические группы

   После этого откроется окно загрузки динамических групп, и начнется процесс их создания

4. После завершения загрузки динамических групп необходимо нажать на кнопку Закрыть

   Автоматически откроется вкладка **«Загруженные динамические группы»**, где будут отображены динамические группы и количество устройств в них

2.11.6 Подразделения

Подразделения — это группа пользователей и устройств, управление устройствами которых доступно только администратору подразделения

Подсказка

Страница **«Подразделения»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Подсказка

Для управления устройствами пользователей, входящих в подразделение, пользователям необходимо авторизоваться в клиентском приложении **RuDesktop**, чтобы администратор подразделения мог увидеть эти устройства на странице **«Устройства»**

Как это работает

Подразделение — это организационная единица, ограничивающая видимость пользователей и их устройств для конкретного администратора. У каждого подразделения один **руководитель** (администратор) и список **участников**

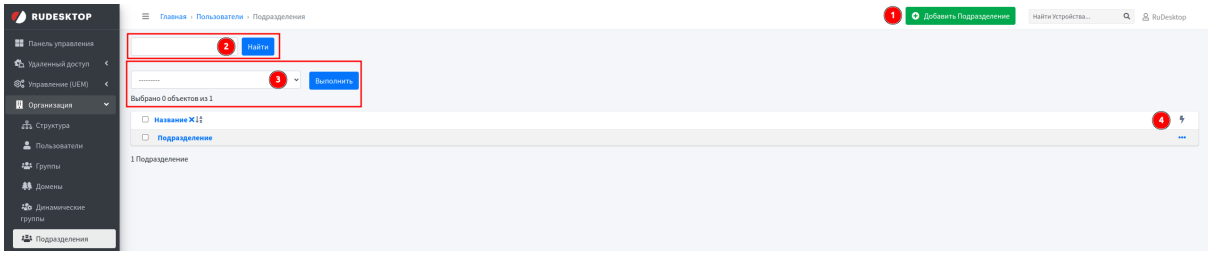
Руководитель видит на странице **«Пользователи»** только участников своего подразделения, а на странице **«Устройства»** — только те устройства, к которым подключались эти участники из клиента **RuDesktop**. Это позволяет разграничить зоны ответственности между администраторами без выдачи прав суперпользователя

Включить пользователя в подразделение можно тремя способами:

- вручную выбрать его в свойствах подразделения
- массово через действие Добавить пользователей в Подразделение на странице *Пользователи*
- отправить пользователю *приглашение* — при принятии он автоматически попадает в подразделение отправителя

Описание страницы

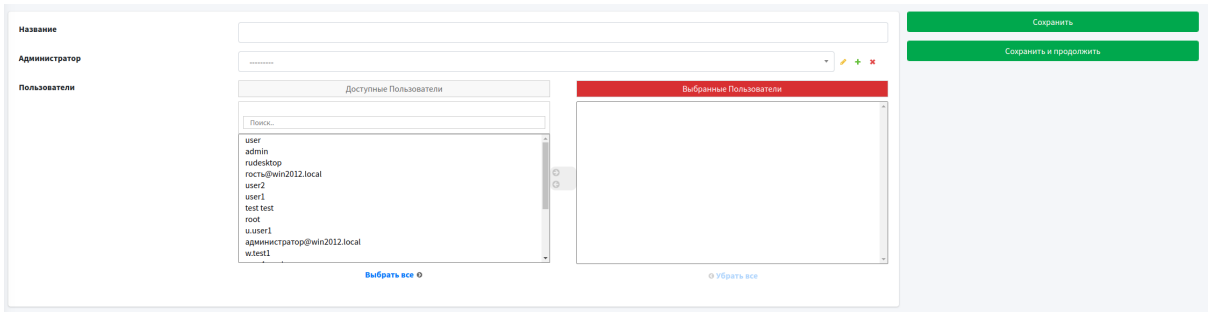
На странице **Подразделения** отображено:



1. Кнопка Добавить подразделение
2. Поиск
3. Массовые действия
4. Таблица

Добавление подразделения

При нажатии на кнопку Добавить подразделение откроется страница создания подразделения



- Название — наименование подразделения
- Администратор — выбор пользователя, который будет являться руководителем подразделения
- Пользователи — выбор пользователей, которые войдут в данное подразделение

Поиск

Поле поиска — поиск по ключевому слову

Подсказка

Поиск осуществляется по названию подразделения, а также по полному имени, электронной почте, телефону и компании руководителя подразделения

Для выполнения поиска необходимо заполнить поле поиска и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные подразделения — удаляет выбранные записи из таблицы
2. Экспортировать выбранные подразделения — позволяет экспортировать в файл выбранные подразделения

Примечание

После выбора данного действия нужно выбрать необходимый формат файла

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление подразделений

Для массового удаления подразделений необходимо:

1. Отметить необходимые подразделения в таблице
2. Выбрать действие Удалить выбранные подразделения
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие подразделения будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные подразделения будут удалены

Экспорт подразделений

Для массового экспорта подразделений необходимо:

1. Отметить необходимые подразделения в таблице
2. Выбрать действие Экспортировать выбранные подразделения
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Название` — наименование подразделения

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

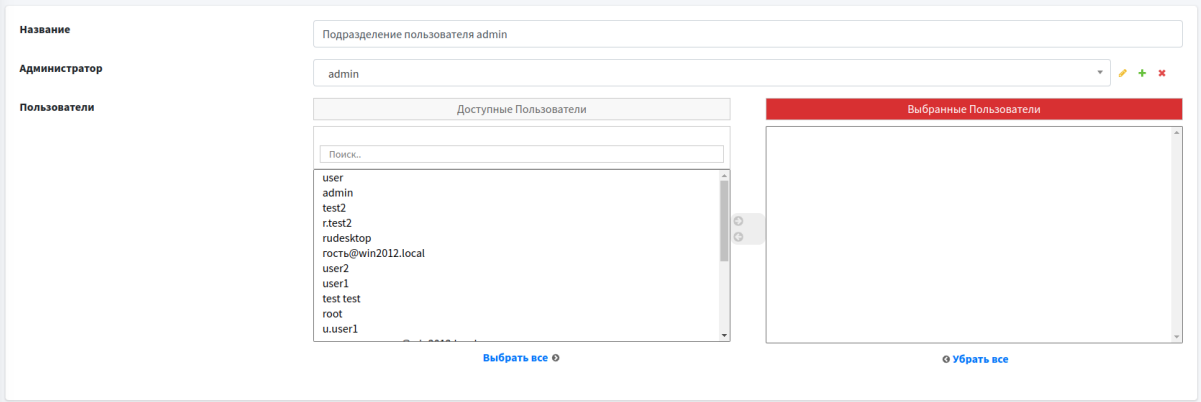
Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства подразделения
2. `Удалить` — при выборе этого пункта подразделение будет удалено
3. `История изменений` — при выборе этого пункта будет отображена история подразделения: создание/редактирование и пользователь, который выполнил данные операции

Свойства подразделения

Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств



1. `Название` — наименование подразделения
2. `Администратор` — выбор пользователя, который будет являться руководителем подразделения

3. `Пользователи` — выбор пользователей, которые войдут в данное подразделение

Меню действий



Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Подразделения»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление подразделения и перенаправляет на страницу **«Подразделения»**

> **Примечание**
>
> 1. После нажатия на кнопку Удалить откроется страница подтверждения удаления подразделения
> 2. После подтверждения удаления подразделения произойдет переход на страницу **«Подразделения»** и появится уведомление Подразделение «НАЗВАНИЕ_ПОДРАЗДЕЛЕНИЯ» было успешно удалено

4. История изменений — отображает все изменения, выполненные для этого подразделения

Пример

Рассмотрим пример: есть администратор и 5 пользователей с установленным клиентом **«RuDesktop»**, которыми должен управлять администратор

Администратор должен видеть пользователей и устройства только своего подразделения

Для того чтобы создать такое подразделение, необходимо:

1. Нажать на кнопку Добавить подразделение
2. Ввести название подразделения

   Например: Подразделение RuDesktop
3. Выбрать администратора подразделения

   Например: user
4. Добавить в правую колонку пользователей, которых хотим видеть в подразделении
5. Нажать на кнопку Сохранить

После выполнения этих действий пользователь будет видеть на странице **«Пользователи»** добавленных пользователей, а на странице **«Устройства»** — устройства, к которым подключались эти пользователи

Подсказка

Чтобы удалить пользователя из подразделения, нужно открыть страницу **«Пользователи»**, перейти в свойства пользователя и нажать на кнопку Удалить из подразделения

2.11.7 Приглашения

Приглашения — это страница для отправки приглашений на электронную почту новым или уже зарегистрированным пользователям с целью их добавления в подразделение

Подсказка

Страница **«Приглашения»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Как это работает

Отправка приглашения создаёт запись с уникальным ключом и отправляет на указанный E-Mail письмо со ссылкой вида `https://[АДРЕС_СЕРВЕРА]/account/invite/?key=[key]`. По этой ссылке адресат:

- регистрирует **новую** учётную запись, если у него ещё нет аккаунта в **RuDesktop**, либо
- авторизуется под **существующей** учётной записью, если уже зарегистрирован в системе

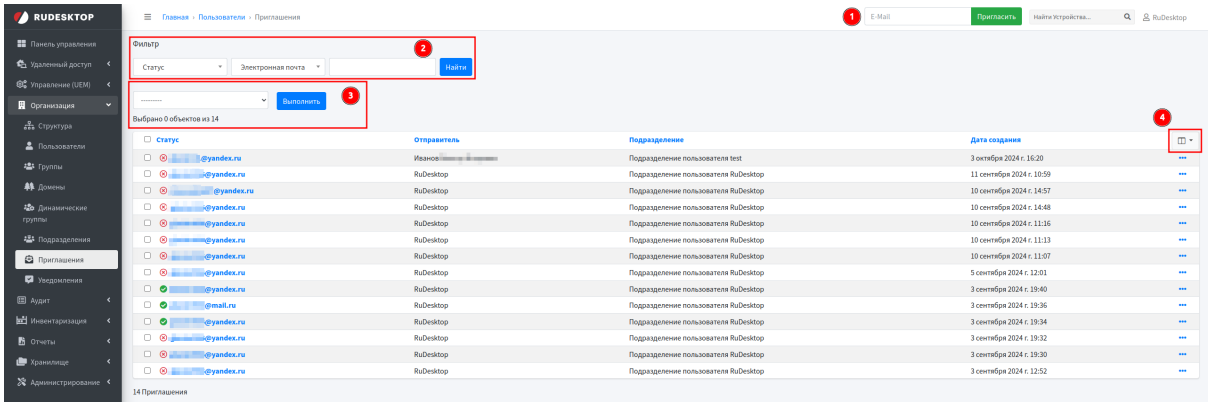
После принятия приглашения пользователь автоматически добавляется в *подразделение* отправителя. Срок действия приглашения — **7 дней**, после чего его необходимо переотправить или отменить

Важно

Перед использованием приглашений у сервера **RuDesktop** должна быть настроена SMTP-отправка писем — см. *Настройки сервера*, раздел **«Email»**

Описание страницы

На странице **Приглашения** отображено:



1. Поле E-Mail и кнопка Пригласить
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление приглашения

При вводе адреса электронной почты и нажатии на кнопку Пригласить будет отправлено приглашение на введённый адрес, и в таблице добавится новая запись

На электронную почту придёт письмо со следующей информацией:

```
Пользователь RuDesktop приглашает вас присоединиться к его␣
↪подразделению

Если вы согласны, перейдите по ссылке ниже и создайте себе учетную␣
↪запись или войдите в личный кабинет

https://[АДРЕС_СЕРВЕРА]/account/invite/?key=[key]
```

Важно

Срок действия приглашения составляет 7 дней. После этого вам потребуется отправить приглашение повторно

После создания новой учетной записи или успешной авторизации под существующей пользователь присоединится к подразделению того, кто отправил приглашение

Примечание

Если письмо с приглашением отправить не удалось, под формой появляется понятное сообщение об ошибке, а созданное приглашение автоматически деактивируется. Наиболее частые причины:

- **Ошибка аутентификации на SMTP сервере** — неверные логин или пароль. Для ряда почтовых сервисов (Яндекс, Mail.ru, Gmail и др.) требуется отдельный «пароль приложения»
- **Адрес отправителя не совпадает с учётной записью** — значение поля **Отправитель по умолчанию** (`From`) должно совпадать с полем **SMTP имя пользователя**
- **SMTP сервер отклонил адрес получателя** — проверьте корректность введённого адреса электронной почты
- **Превышено время ожидания ответа / не удалось подключиться к SMTP серверу** — проверьте адрес, порт и доступность SMTP-сервера (сеть, файрвол)

Параметры отправки настраиваются в разделе *Настройки сервера* → **Настройки SMTP**

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. `Статус` — фильтрация приглашений по их статусу

   Возможные значения:

   - `Приглашение просрочено` — приглашения, у которых истёк срок действия
   - `Приглашение принято` — приглашения, которые были приняты пользователем
   - `Ожидает регистрации пользователя` — приглашения, отправленные и не просроченные, по которым пользователь ещё не зарегистрировался
   - `Приглашение не активно` — приглашения, отменённые отправителем

2. `Отправитель` — фильтрация приглашений по пользователю, отправившему приглашение

> **Важно**
>
> Фильтр доступен только суперпользователю

3. `Поле поиска` — поиск по адресу электронной почты получателя или отправителя

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные приглашения — удаляет выбранные записи из таблицы

> **Важно**
>
> В зависимости от прав действия могут отсутствовать
>
> Только суперпользователь или пользователь с правом **«Пользователи» -> «Удаление»** может удалять приглашения

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление приглашений

Для массового удаления приглашений необходимо:

1. Отметить необходимые приглашения в таблице
2. Выбрать действие Удалить выбранные приглашения
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие приглашения будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные приглашения будут удалены

Таблица

Таблица разбита по столбцам:

1. `Статус` — статус и электронная почта, на который было отправлено приглашение

- - приглашение отправлено, но пользователь еще не зарегистрировался или не авторизовался
- - приглашение отменено или просрочено
- - приглашение принято

2. `Отправитель` — пользователь, который отправил приглашение
3. `Подразделение` — подразделение, в которое вступит пользователь после принятия приглашения
4. `Дата создания` — дата и время создания приглашения

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

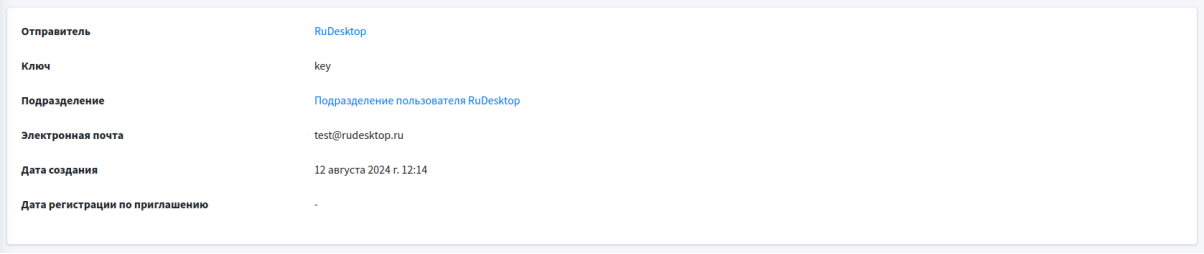
Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства приглашения
2. `Удалить` — при выборе этого пункта приглашение будет удалено
3. `История изменений` — при выборе этого пункта будет отображена история приглашения: создание/редактирование и пользователь, который выполнил данные операции
4. `Переотправить приглашение` — при выборе этого пункта приглашение будет отправлено повторно на указанную электронную почту
5. `Отменить приглашение` — при выборе этого пункта приглашение будет отменено и станет недоступным

Свойства приглашения

Просмотр

При нажатии на кнопку `Редактировать` откроется страница свойств в режиме **просмотра** — все поля доступны только для чтения



1. Отправитель — пользователь, который отправил приглашение
2. Ключ — уникальный ключ приглашения
3. Подразделение — подразделение, в которое вступит пользователь после принятия приглашения

4. Электронная почта — адрес электронной почты, на которую было отправлено приглашение
5. Дата создания — дата и время создания приглашения
6. Дата регистрации по приглашению — дата и время регистрации пользователя, который принял приглашение

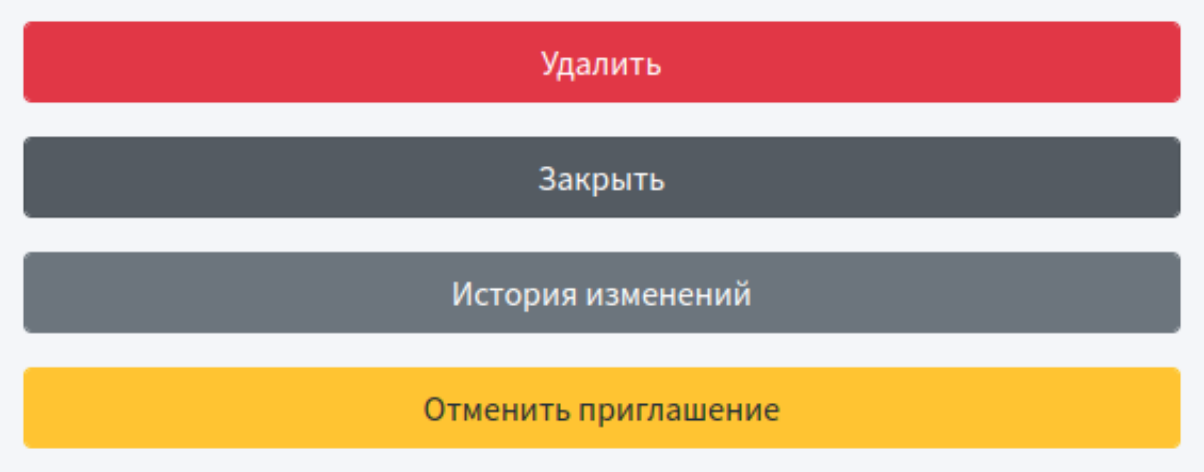
Важно

Поля Отправитель, Ключ и Подразделение отображаются только суперпользователю

Примечание

Изменять параметры существующего приглашения нельзя — для повторной отправки используйте действие Переотправить приглашение, для отмены — Отменить приглашение

Меню действий



Имеет следующие возможности:

1. Удалить — производит удаление приглашения и перенаправляет на страницу **«Приглашения»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления приглашения
2. После подтверждения удаления приглашения произойдет переход на страницу **«Приглашения»** и появится уведомление Приглашение «EMAIL» было успешно удалено

2. Закрыть — производит закрытие страницы и переход на страницу **«Приглашения»**
3. История изменений — отображает все изменения, выполненные для этого приглашения
4. Переотправить приглашение — производит повторную отправку приглашения на указанную электронную почту
5. Отменить приглашение — производит отмену приглашения

2.11.8 Уведомления

Доступны только в UEM версии

Уведомления — это страница для создания уведомлений о выполнении задач, получения готовых отчетов и изменения ресурсов

Подсказка

Страница **«Уведомления»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

Уведомление — это правило, которое описывает, **кому**, **по какому каналу** и **по какому событию** сервер должен отправлять оповещения. Одно правило может покрывать сразу несколько событий

Поддерживаемые **каналы доставки**:

- `Телефон` — отправка SMS на номер пользователя
- `Email` — на адрес электронной почты пользователя или общий адрес из настроек сервера
- `Telegram` — личный чат пользователя и/или общий чат из настроек сервера
- `MAX` — личный чат пользователя в мессенджере **MAX** и/или общий чат из настроек сервера
- `Webhook` — POST-запрос в формате JSON на указанный URL для событий SMART дисков

Поддерживаемые **события**:

- завершение выбранной задачи (политики, отчёта, синхронизации и т.д.)
- завершение выбранной *задачи миграции* и/или завершение миграции на каждом её устройстве
- готовность отчёта по выбранному шаблону
- изменение конфигурации устройств после выполнения политики **«Инвентаризация»** (с фильтром по классам ресурсов)
- поступление новых обращений в **Поддержку**

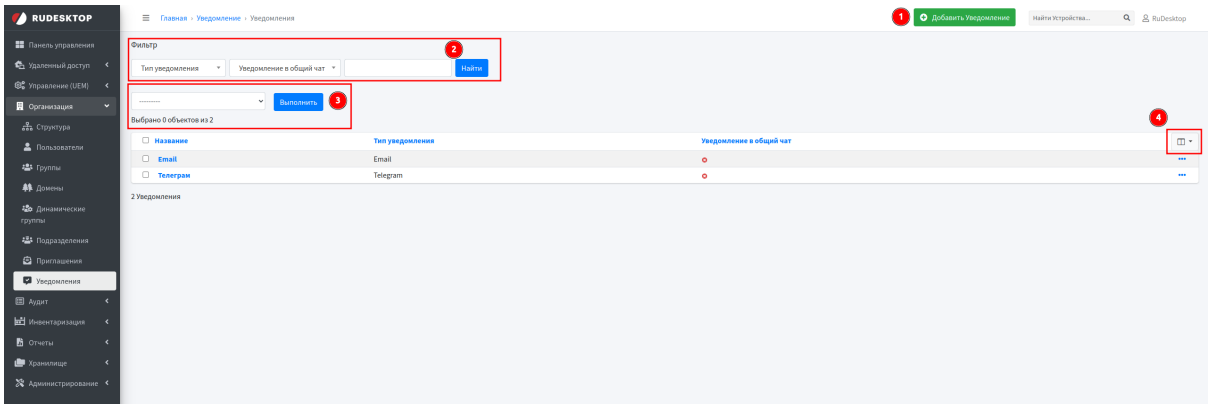
- блокировка IP-адреса при входе после превышения лимита неудачных попыток
- изменение версий отслеживаемого ПО после инвентаризации
- превышение количества мест лицензий ПО и новые установки без назначения лицензии
- изменение статуса SMART диска после инвентаризации — только через webhook

Важно

- Чтобы пользователь получал уведомления, в его *профиле* должны быть заполнены контактные данные (телефон, Email, Telegram, MAX) для выбранного канала
- Для отправки в общий чат соответствующие поля должны быть заполнены в *настройках сервера*

Описание страницы

На странице **Уведомления** отображено:

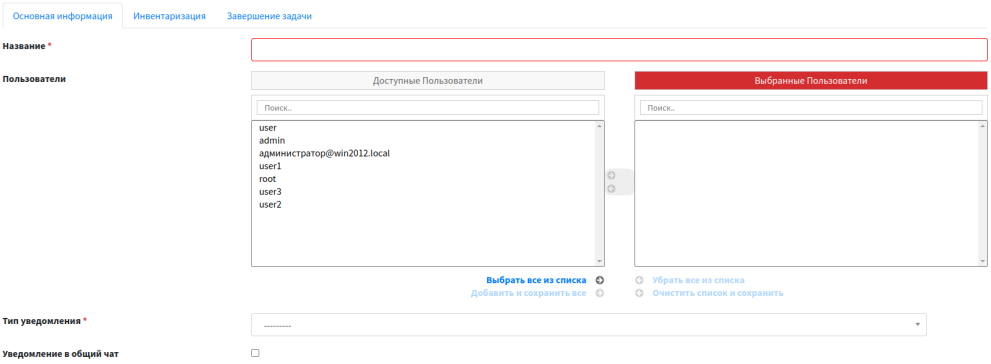


1. Кнопка Добавить Уведомление
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление уведомления

При нажатии на кнопку Добавить Уведомление откроется страница добавления уведомления со следующими вкладками:

1. `Основная информация`



Содержит поля:

1. Название — наименование уведомления
2. Пользователи — выбор получателей уведомлений

> **Важно**
>
> У выбранного пользователя в *профиле* должны быть указаны номер телефона, Email, Telegram или MAX, чтобы он мог получать уведомления в соответствии с выбранным типом

3. Тип уведомления — выбор способа получения уведомлений

> **Примечание**
>
> Уведомления могут быть отправлены на телефон, в Telegram, MAX или на Email. Для статусов SMART выбрать **Webhook** и заполнить **URL webhook**; получатели из поля **Пользователи** для этого канала не используются

4. Уведомление в общий чат — отправка уведомления в общий чат Telegram, MAX или на Email

> **Подсказка**
>
> Общий чат Telegram/MAX или адрес Email для общих уведомлений берётся из *настроек сервера*

> **Важно**
>
> Уведомления общего чата по Телефону не предусмотрены — при выборе этого типа поле должно быть выключено

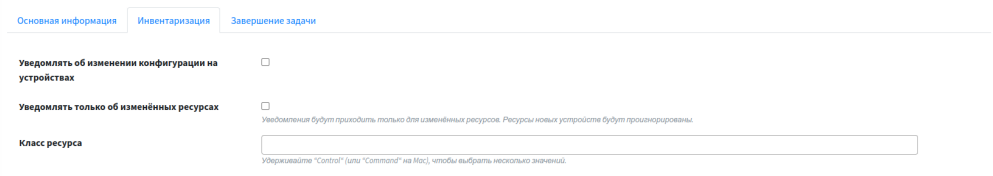
5. Уведомление о новых обращениях — отправка уведомлений о поступлении новых обращений в **Поддержку**

> **Подсказка**
>
> Получатели уведомлений берутся из списка пользователей, указанных в поле Пользователи

6. Уведомлять о блокировке IP при входе — отправка уведомлений при блокировке входа с IP-адреса после превышения лимита неудачных попыток

> **Подсказка**
>
> Порядок настройки и доступные каналы описаны в разделе *Уведомления о блокировке входа*

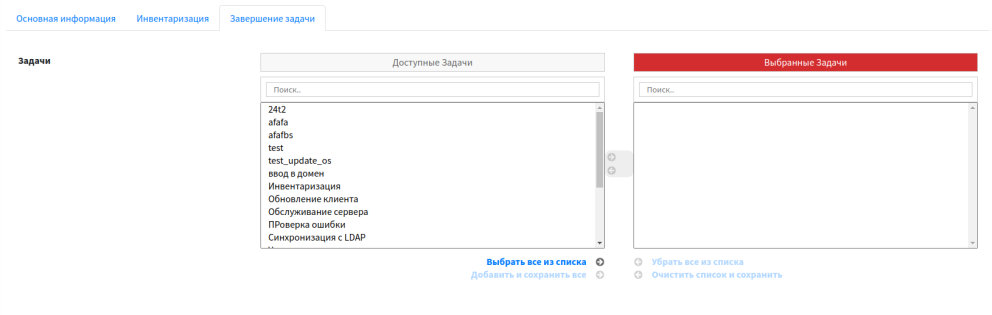
2. Инвентаризация



Содержит поля:

1. Уведомлять об изменении конфигурации на устройствах — активация этой опции позволит отправлять уведомления при изменении конфигурации устройств после выполнения политики **«Инвентаризация»**
2. Уведомлять только об изменённых ресурсах — при активации этого чекбокса уведомления будут приходить только для изменённых ресурсов. Ресурсы новых устройств будут игнорироваться
3. Класс ресурса — выбор классов ресурсов, по изменениям в которых следует присылать уведомления
4. Уведомлять об изменении версий отслеживаемого ПО — уведомления о смене версий программ, для которых в *Аудите ПО* включено отслеживание
5. Уведомлять о превышении количества лицензий на ПО — оповещения по данным инвентаризации; условия подсчёта и отправки описаны в разделе *Лицензии ПО*
6. Уведомлять об изменении статуса S.M.A.R.T дисков через webhook — отправка события об изменении ранее собранного статуса диска; требует тип **Webhook**

3. Завершение задачи



Содержит поля:

Задачи — выбор задач для уведомлений

Примечание

Можно выбрать как одну задачу для уведомлений, так и несколько

4. `Завершение задачи миграции`

   Содержит поля:

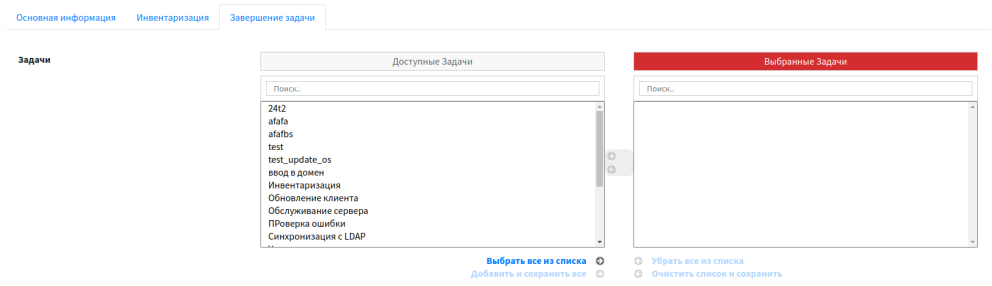
   1. Задачи миграции — выбор *задач миграции*, по которым отправлять уведомления

      Примечание

      Можно выбрать одну или несколько задач миграции

   2. Уведомлять о завершении миграции на каждом устройстве — флаг отправки уведомлений по каждому устройству задачи. Уведомление содержит название задачи миграции, устройство, текущую стадию и статус. По умолчанию включён
   3. Уведомлять в конце задачи миграции — флаг отправки итогового уведомления по задаче целиком. Уведомление содержит название, итоговый статус и прогресс (количество успешно мигрированных устройств от общего числа). По умолчанию выключен

5. `Отчеты`



Содержит поля:

Уведомить о новом отчете — выбор шаблонов отчетов для уведомлений

Примечание

Можно выбрать как один шаблон отчета для уведомлений, так и несколько

Уведомления о блокировке входа

1. Добавить уведомление и указать название, например **«Блокировка входа»**
2. На вкладке **Основная информация** выбрать получателей в поле **Пользователи** и **Тип уведомления**: Email, Telegram, MAX или Телефон
3. Включить **Уведомлять о блокировке IP при входе**
4. При необходимости включить **Уведомление в общий чат** для Email, Telegram или MAX
5. Сохранить уведомление

Примечание

В профилях получателей должны быть заполнены контактные данные для выбранного канала

Параметры общего чата или общего адреса Email задаются в настройках сервера

При следующей блокировке сервер отправит уведомление по настроенным правилам

- **Email, Telegram и MAX** — сообщение содержит имя пользователя, IP-адрес, время начала и окончания блокировки, количество неудачных попыток и длительность блокировки
- **Телефон** — SMS с коротким сообщением **«Блокировка IP при входе»**

Важно

Канал **Webhook** для этого события не поддерживается

Лимит попыток и время блокировки задаются в *настройках безопасности сервера*

Примечание

Уведомление сообщает о начале блокировки. Сообщение об окончании срока не отправляется

Уведомления о версиях ПО

На вкладке **Инвентаризация** включить **Уведомлять об изменении версий отслеживаемого ПО**. В *Аудите ПО* включить отслеживание нужных программ. Получатели и обычные каналы доставки задаются на вкладке **Основная информация**

Если для программы задана рекомендованная версия, сообщение формируется только при изменении на версию, не удовлетворяющую условию. Первая установка и полное удаление программы не являются событием смены версии

Флаг уведомлений о версиях работает независимо от **Уведомлять об изменении конфигурации на устройствах** и его фильтра **Класс ресурса**. Для уведомлений о конфигурации и о версиях лучше создать отдельные правила, если им нужны разные получатели или каналы

Webhook для статусов SMART

1. Добавить уведомление и выбрать тип **Webhook**
2. Указать **URL webhook** с протоколом `http` или `https` — адрес обработчика событий
3. При необходимости заполнить **Секрет webhook** для проверки подписи
4. На вкладке **Инвентаризация** включить **Уведомлять об изменении статуса S.M.A.R.T дисков через webhook**
5. Сохранить уведомление и выполнить инвентаризацию устройств со сбором данных дисков

Событие возникает при изменении статуса уже известного диска по сравнению с предыдущей инвентаризацией. Первая инвентаризация диска событие не создаёт. Сообщение содержит идентификатор и ссылку на устройство, сведения о диске, предыдущий и новый статусы. Изменение на неизвестный статус или восстановление нормального статуса также отправляется

Обработчик получает POST-запрос с `Content-Type: application/json` и заголовком `X-RuDesktop-Event: smart_status_changed`. В теле есть поля `event_type`, `timestamp`, `device`, `disk` и `smart_status`. Последнее содержит `old`, `new`, `old_state` и `new_state`; нормализованные состояния — `ok`, `bad` и `unknown`

Если задан секрет, заголовок `X-RuDesktop-Signature` содержит `sha256=<hex>` — HMAC-SHA256 от исходных байтов тела запроса с этим секретом. Для проверки подписи использовать исходное тело, а не JSON после повторной сериализации

Обработчик должен ответить кодом `2xx` в течение 10 секунд. Перенаправления не выполняются. При ошибке предусмотрены три повторные попытки с задержками 60, 300 и 900 секунд. Обработчик должен учитывать возможность повторного получения одного события

Примечание

Webhook предназначен для событий SMART. Для него нельзя включать уведомления в общий чат, о новых обращениях, об изменении конфигурации, выбирать задачи, задачи миграции или отчёты. Для уведомлений о версиях ПО использовать отдельное правило с обычным каналом доставки

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. `Поле поиска` — поиск по ключевому слову

Подсказка

Поиск по ключевому слову осуществляется по названию уведомления и типу уведомления

Для выполнения поиска необходимо заполнить поле и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные уведомления — удаляет выбранные уведомления из таблицы

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление уведомлений

Для массового удаления уведомлений необходимо:

1. Отметить необходимые уведомления в таблице
2. Выбрать действие Удалить выбранные уведомления
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие уведомления будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору

6. Выбранные уведомления будут удалены

Таблица

Таблица разбита по столбцам:

1. `Название` — отображает пользовательское название уведомления
2. `Тип уведомления` — отображает способ получения уведомлений
3. `Уведомление в общий чат` — отображает активность функции отправки уведомления в общий чат Telegram, MAX или Email

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства уведомления
2. `Удалить` — при выборе этого пункта уведомление будет удалено
3. `История изменений` — при выборе этого пункта будет отображена история уведомления: создание/редактирование и пользователь, который выполнил данные операции

Свойства уведомления

Меню действий

Меню действий расположено на всех вкладках страницы редактирования



Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Уведомления»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций

3. Удалить — производит удаление уведомления и перенаправляет на страницу **«Уведомления»**

> **Примечание**
>
> 1. После нажатия на кнопку Удалить откроется страница подтверждения удаления уведомления
> 2. После подтверждения удаления уведомления произойдет переход на страницу **«Уведомления»** и появится уведомление Уведомление «НАЗВАНИЕ_ОБРАЗА» было успешно удалено

4. История изменений — отображает все изменения, выполненные для этого уведомления

Пример

Чтобы добавить уведомление об изменениях в ресурсах устройства, завершении задачи и получении отчета с отправкой в Telegram конкретному пользователю, необходимо:

1. На странице **«Уведомления»** нажать на кнопку Добавить Уведомление
2. Заполнить следующие поля:

   `Основная информация`

   1. Название — Telegram
   2. Пользователи — выбрать пользователя, которому должны приходить уведомления и у которого заполнены настройки Telegram
   3. Тип уведомления — выбрать тип уведомления: Telegram
   4. Уведомление в общий чат — снять галочку

   `Инвентаризация`

   1. Уведомлять об изменении конфигурации на устройствах — установить галочку
   2. Уведомлять только об изменённых ресурсах — установить галочку
   3. Класс ресурса — выбрать необходимые классы

   `Завершение задачи`

   1. Задачи — выбрать задачу, например **«Инвентаризация»**

   `Отчеты`

   1. Уведомить о новом отчете — выбрать шаблон отчета, например **«Инвентаризация: Ресурсы в наличии»**

3. Нажать кнопку Сохранить для сохранения уведомления

4. Запустить задачу **«Инвентаризация»**
5. После выполнения задачи придет уведомление о её завершении в Telegram, а если были изменения в ресурсах устройств, также придут соответствующие уведомления и ссылка на готовый отчет

Организация — раздел для управления учётными записями и связями между ними: пользователи, группы (через них наследуются права), домены **LDAP** для синхронизации, динамические группы устройств, подразделения для разграничения зон ответственности администраторов, приглашения новых пользователей и правила уведомлений

Подсказка

Раздел **«Организация»** доступен при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**. Страницы *Динамические группы* и *Уведомления* доступны только при лицензии **UEM**

Структура
Иерархическое дерево групп, прав и доменов с устройствами

Пользователи
Учётные записи пользователей сервера

Группы
Группы пользователей и устройств с общими правами

Домены
Подключение к LDAP и синхронизация пользователей и устройств

Динамические группы
Автоматическая группировка устройств по фактам и SQL-запросам

Подразделения
Группы пользователей и устройств с отдельным администратором

Приглашения
Приглашения новых пользователей по электронной почте

Уведомления
Правила оповещений по событиям задач, отчётов и обращений

2.12 Аудит

Доступен только в UEM версии

2.12.1 Логи исполнения

Доступны только в UEM версии

Логи исполнения — на данной странице отображаются события выполнения задач и политик на устройствах

Подсказка

Страница **«Логи исполнения»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

Сервер фиксирует событие при каждом запуске и завершении задач и политик на устройствах. Каждая запись описывает один шаг выполнения и привязана к конкретной задаче, политике, устройству и пользователю, инициировавшему выполнение

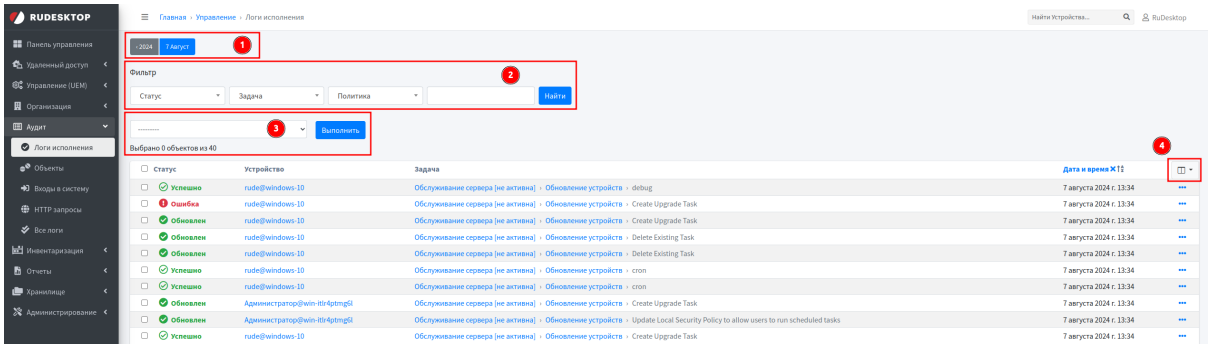
Записи на странице сгруппированы по событиям. На уровне отдельной записи фиксируется:

- статус выполнения (успех, ошибка, отмена и т.д.)
- задача и политика, в рамках которых выполнялся шаг
- устройство, на котором запускалось выполнение
- системные факты события и параметры подзадачи

В отличие от страницы *Объекты*, где регистрируются изменения сущностей сервера, **«Логи исполнения»** показывают только события, связанные с выполнением задач и политик. Из контекстного меню устройства или задачи можно перейти на эту страницу с предустановленным фильтром

Описание страницы

На странице **«Логи исполнения»** отображено:



1. Фильтр даты

2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Фильтр даты

Позволяет выбрать год, месяц и число с возможностью отображения событий за определённую дату

Фильтр

Можно формировать таблицу для получения определённых данных, используя фильтр:

1. `Статус` — статус выполнения задачи (Успешно, Обновлен, Недоступен, Пропущен, Игнорирован, Ошибка)
2. `Задача` — пользовательское наименование выполненной задачи
3. `Политика` — пользовательское наименование выполненной политики
4. `Инициатор` — фильтрация по пользователю, инициировавшему запуск, или по системе (запуск по расписанию)
5. `Поле поиска` — поиск по ключевому слову

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Экспортировать выбранные логи исполнения — экспорт выбранных событий

> **Примечание**
>
> После выбора данного действия нужно выбрать необходимый формат файла

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Экспорт событий

Для массового экспорта событий необходимо:

1. Отметить необходимые события в таблице
2. Выбрать действие Экспортировать выбранные логи исполнения
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Дата и время` — дата и время выполнения задачи
2. `Устройство` — устройство, на котором выполнялась задача
3. `Политики` — наименование политики, к которой относится задача
4. `Инициатор` — пользователь или система, инициировавшие запуск задачи
5. `Задача` — пользовательское наименование выполненной задачи

Примечание

`Статус` доступен как фильтр (значения: Успешно, Обновлен, Недоступен, Пропущен, Игнорирован, Ошибка), но в виде столбца таблицы не выводится

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства события

Свойства события

Редактирование

Страница содержит вкладки:

1. `Основная информация`:

1. **Дата и время** — дата и время создания события
2. **Уровень** — уровень логирования
3. **Источник** — источник события
4. **Тип события** — тип, которое произошло с событием
5. **Тип объекта** — тип, с которым выполнялись действия
6. **Пользователь** — пользователь, выполнивший действия
7. **Устройство** — устройство, на котором выполнялась задача/политика
8. **Задача** — наименование задачи
9. **Политика** — наименование политики
10. **Подзадача** — системное имя подзадачи

2. Дополнительно
    1. **Производитель** — имя вендора
    2. **Продукт** — название продукта
    3. **Версия** — версия ПО
    4. **Начало** — дата и время начала выполнения политики/задачи
3. Объект

    На данной вкладке отображаются системные факты события

2.12.2 Объекты

Доступны только в UEM версии

Объекты — на данной странице отображены события по добавлению, изменению или удалению объектов на различных страницах

Подсказка

Страница **«Объекты»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

RuDesktop автоматически фиксирует CRUD-события (создание, изменение, удаление) для объектов сервера: устройств, пользователей, групп, доступов, политик, шаблонов отчётов, настроек и т.д. Каждое событие сохраняет:

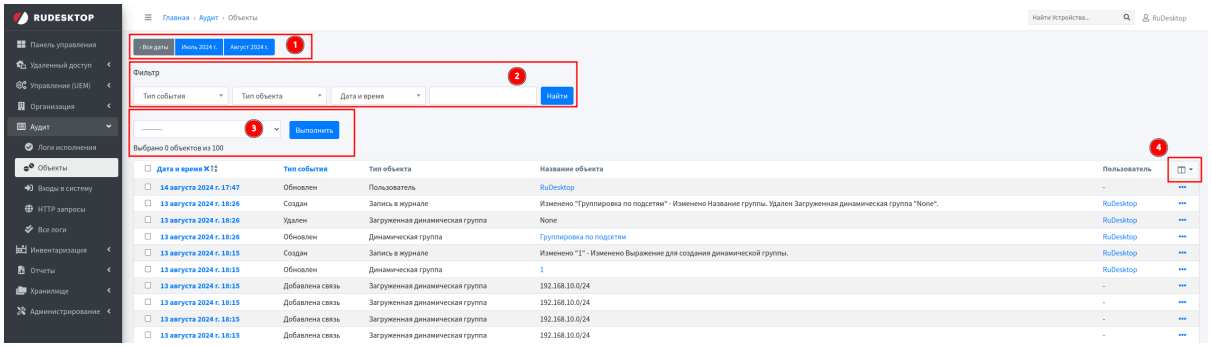
- тип события (добавлено / изменено / удалено)
- тип и название изменённого объекта
- пользователя, выполнившего операцию (или системное действие, если выполнено сервером)

- момент времени и контекст (задача, политика, устройство — если применимо)

В отличие от страницы *Логи исполнения*, где фиксируется выполнение задач и политик, страница **«Объекты»** отвечает на вопрос «**кто и когда менял конкретный объект**». Эти же события доступны через действие **«История изменений»** в контекстных меню объектов — там показывается срез логов, отфильтрованный по выбранному объекту

Описание страницы

На странице **«Объекты»** отображено:



1. Фильтр даты
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Фильтр даты

Позволяет выбрать год, месяц и число с возможностью отображения событий за определённую дату

Фильтр

Можно формировать таблицу для получения определённых данных, используя фильтр:

1. `Тип события` — тип, который произошёл с событием
2. `Тип объекта` — тип, с которым выполнялись действия
3. `Дата и время` — позволяет выбрать период
4. `Поле поиска` — поиск по ключевому слову

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Экспортировать выбранные объекты — экспорт выбранных событий

> **Примечание**
>
> После выбора данного действия нужно выбрать необходимый формат файла

> **Важно**
>
> В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Экспорт событий

Для массового экспорта событий необходимо:

1. Отметить необходимые события в таблице
2. Выбрать действие Экспортировать выбранные объекты
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Дата и время` — дата и время события
2. `Тип события` — тип, который произошёл с событием
3. `Тип объекта` — тип, с которым выполнялись действия
4. `Название объекта` — название объекта, с которым выполнялись действия
5. `Пользователь` — имя пользователя

> **Подсказка**
>
> При отображении в данном столбце — означает, что действие выполнялось от имени системы

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства события

Свойства события

Редактирование

Страница содержит вкладки:

1. `Основная информация`:
    1. **Дата и время** — дата и время создания события
    2. **Уровень** — уровень логирования
    3. **Источник** — источник события
    4. **Тип события** — тип, который произошёл с событием
    5. **Тип объекта** — тип, с которым выполнялись действия
    6. **Пользователь** — пользователь, выполнивший действия
    7. **Устройство** — устройство, на котором выполнялась задача/политика
    8. **Задача** — наименование задачи
    9. **Политика** — наименование политики
    10. **Подзадача** — системное имя подзадачи
2. `Дополнительно`
    1. **Производитель** — имя вендора
    2. **Продукт** — название продукта
    3. **Версия** — версия ПО
    4. **Message** — произвольное сообщение, содержащее более подробную информацию о событии

    Подсказка

    Многострочные записи могут быть получены с использованием в качестве разделителя новой строки

3. `Объект`

    На данной вкладке отображаются системные факты события

2.12.3 Входы в систему

Доступны только в UEM версии

Входы в систему — на данной странице отображены события о входах в веб-интерфейс сервера **RuDesktop**

Подсказка

Страница **«Входы в систему»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

Сервер фиксирует событие при каждой попытке входа в административную панель **RuDesktop** — как успешной, так и неудачной. Каждая запись содержит:

- момент времени и тип события (вход / неуспешная попытка / выход)
- учётную запись, под которой выполнялась попытка (включая случаи, когда учётная запись не существует или неактивна)
- хост и IP-адрес источника
- системные факты сессии

Страница используется для:

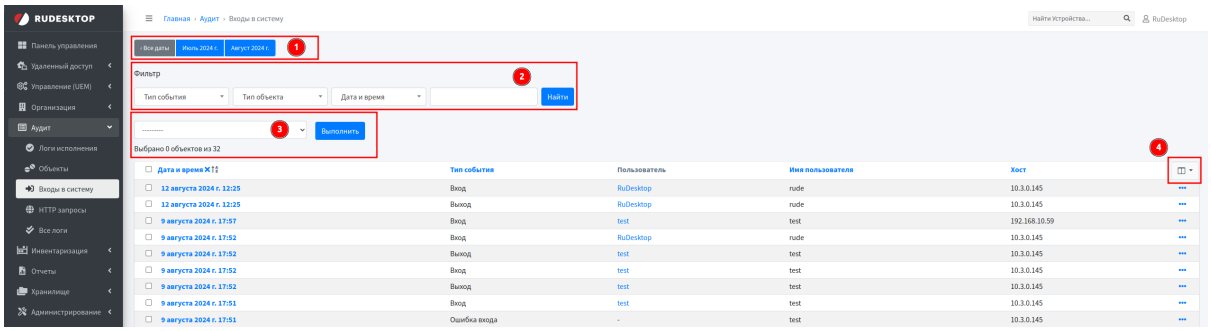
- расследования инцидентов с подозрительной активностью (множественные неудачные попытки, входы из необычных мест)
- сверки реальных входов с ожидаемыми (особенно для технических и доменных учёток)
- доказательной базы при разборе обращений в *Поддержку*

Примечание

Здесь регистрируются именно входы в **веб-интерфейс**. События входа в клиентское приложение **RuDesktop** на устройствах фиксируются отдельно — см. *Объекты* и *Логи исполнения*

Описание страницы

На странице **«Входы в систему»** отображено:



1. Фильтр даты
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Фильтр даты

Позволяет выбрать год, месяц и число с возможностью отображения событий за определённую дату

Фильтр

Можно формировать таблицу для получения определённых данных, используя фильтр:

1. `Тип события` — тип события (Вход, Выход, Ошибка входа)
2. `Дата и время` — позволяет выбрать период
3. `Поле поиска` — поиск по ключевому слову

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Экспортировать выбранные входы в систему — экспорт выбранных событий

Примечание

После выбора данного действия нужно выбрать необходимый формат файла

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Экспорт событий

Для массового экспорта событий необходимо:

1. Отметить необходимые события в таблице
2. Выбрать действие Экспортировать выбранные входы в систему
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Дата и время` — дата и время события
2. `Тип события` — тип события (Вход, Выход, Ошибка входа)
3. `Пользователь` — имя пользователя

Подсказка

При отображении в данном столбце — означает, что действие выполнялось от имени системы

4. `Имя пользователя источника` — идентификация пользователя по имени, под которым выполнялась попытка входа (заполняется в том числе для несуществующих или неактивных учётных записей)
5. `Адрес источника` — IP-адрес источника, с которого выполнялась попытка входа

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. Редактировать — при выборе этого пункта откроются свойства события

Свойства события

Редактирование

Страница содержит вкладки:

1. Основная информация:
    1. **Дата и время** — дата и время создания события
    2. **Уровень** — уровень логирования
    3. **Источник** — источник события
    4. **Тип события** — тип события, которое произошло
    5. **Тип объекта** — тип объекта, с которым выполнялись действия
    6. **Пользователь** — пользователь, выполнивший действия
    7. **Устройство** — устройство, на котором выполнялась задача/политика
    8. **Задача** — наименование задачи
    9. **Политика** — наименование политики
    10. **Подзадача** — системное имя подзадачи
2. Дополнительно
    1. **Производитель** — имя вендора
    2. **Продукт** — название продукта
    3. **Версия** — версия ПО
    4. **Хост** — определение источника, на который ссылается событие в IP-сети

> **Подсказка**
>
> Формат должен представлять собой полное доменное имя, связанное с исходным узлом, когда узел доступен
>
> Примеры: **«host.domain.com»** или **«хост»**

    5. **Имя пользователя** — идентификация исходного пользователя по имени

> **Подсказка**
>
> - Адреса электронной почты также сопоставляются с полями UserName
> - Отправитель является кандидатом для помещения в sourceUserName

3. `Объект`

   На данной вкладке отображаются системные факты события

2.12.4 HTTP запросы

Доступны только в UEM версии

HTTP запросы — на данной странице отображены события HTTP запросов

Подсказка

Страница **«HTTP запросы»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

Сервер фиксирует HTTP-запросы, поступающие к административной панели и API сервера **RuDesktop**. Запись содержит:

- метод запроса (`GET`, `POST`, `PUT`, `DELETE` и т.д.) и URL-адрес
- хост источника (FQDN или IP-адрес)
- учётную запись пользователя, от имени которого выполнен запрос (или системное действие)
- момент времени и системные факты события

Страница используется для:

- разбора инцидентов и нештатных обращений к API
- сверки автоматических интеграций (внешние скрипты, мониторинг, импорт/экспорт)
- проверки активности конкретного пользователя или хоста

Примечание

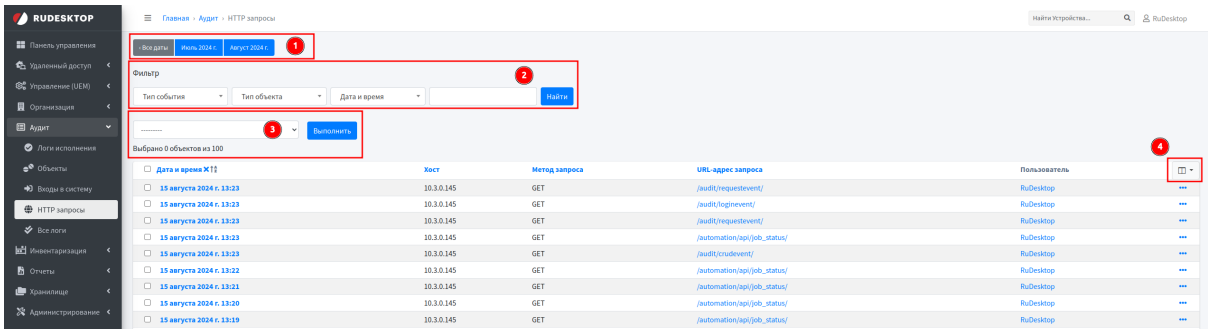
HTTP-запросы из клиентского приложения **RuDesktop** на устройствах в этот журнал не попадают — здесь фиксируются только обращения к серверу

Подсказка

Часть запросов можно исключать из журнала ещё до их регистрации. Для этого в *настройках сервера* заполните поле Исключения из логирования — указанные URL-адреса (через запятую, например: `/peers/get_peer_statuses/, /audit/requestevent/`) не будут попадать в **«HTTP запросы»** и в **«Все логи»**. Удобно для отсева частых служебных запросов, чтобы они не засоряли журналы

Описание страницы

На странице **«HTTP запросы»** отображено:



1. Фильтр даты
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Фильтр даты

Позволяет выбрать год, месяц и число с возможностью отображения событий за определённую дату

Фильтр

Можно формировать таблицу для получения определённых данных, используя фильтр:

1. `Дата и время` — позволяет выбрать период
2. `Поле поиска` — поиск по ключевому слову

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Экспортировать выбранные HTTP запросы — экспорт выбранных событий

> **Примечание**
>
> После выбора данного действия нужно выбрать необходимый формат файла

> **Важно**
>
> В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Экспорт событий

Для массового экспорта событий необходимо:

1. Отметить необходимые события в таблице
2. Выбрать действие Экспортировать выбранные HTTP запросы
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Дата и время` — дата и время события
2. `Хост` — источник, на который ссылается событие в IP-сети
3. `Метод запроса` — метод, используемый для доступа к адресу
4. `URL-адрес запроса` — адрес, к которому осуществляется доступ
5. `Пользователь` — имя пользователя

> **Подсказка**
>
> При отображении в данном столбце — означает, что действие выполнялось от имени системы

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства события

Свойства события

Редактирование

Страница содержит вкладки:

1. `Основная информация`:
    1. **Дата и время** — дата и время создания события

2. **Уровень** — уровень логирования
3. **Источник** — источник события
4. **Тип события** — тип, который произошёл с событием
5. **Тип объекта** — тип, с которым выполнялись действия
6. **Пользователь** — пользователь, выполнивший действия
7. **Устройство** — устройство, на котором выполнялась задача/политика
8. **Задача** — наименование задачи
9. **Политика** — наименование политики
10. **Подзадача** — системное имя подзадачи

2. Дополнительно
   1. **Производитель** — имя вендора
   2. **Продукт** — название продукта
   3. **Версия** — версия ПО
   4. **Метод запроса** — метод, используемый для доступа к адресу

      Подсказка

      Возможные значения: **«POST»**, **«GET»** ...

   5. **URL-адрес запроса** — содержит адрес, к которому осуществляется доступ

      Подсказка

      URL-адрес также должен содержать протокол, например, http://www.security.com

   6. **Хост** — определение источника, на который ссылается событие в IP-сети

      Подсказка

      Формат должен представлять собой полное доменное имя, связанное с исходным узлом, когда узел доступен

      Примеры: **«host.domain.com»** или **«хост»**

3. Объект

   На данной вкладке отображаются системные факты события

2.12.5 Логи сессий

Доступны только в UEM версии

Логи сессий — на данной странице отображены события удалённых сессий, связанные с записью видео и фиксацией действий при передаче файлов

Подсказка

Страница **«Логи сессий»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

Сервер фиксирует событие в журнале сессий в двух случаях, и оба связаны с включённым **Мониторингом** в свойствах *группы устройств*:

- **Видео запись сессии** — событие создаётся при записи удалённого подключения (рабочий стол) на стороне сервера. В одной сессии может быть несколько таких событий, если запись разбита на сегменты
- **Запись передачи файлов** — событие создаётся при каждом действии с файлом во время сессии передачи файлов: загрузка на устройство, скачивание с устройства, удаление, переименование и т.д. Каждое действие — отдельная запись с локальным и удалённым путями

Каждая запись логически привязана к конкретной *сессии* через её UUID — из логов можно перейти к самой сессии, и наоборот

Важно

- События в этот журнал попадают **только** при включённой принудительной записи в *группе устройств* (флаги Мониторинг удалённого подключения (запись видео) и Мониторинг передачи файлов)
- Для просмотра записей у пользователя должно быть активно право Может просматривать логи сессий
- Записи с принудительным мониторингом всегда проходят через RELAY (мост)

Описание страницы

На странице **«Логи сессий»** отображено:

1. Фильтр даты
2. Поиск
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Фильтр даты

Позволяет выбрать год, месяц и число с возможностью отображения событий за определённую дату

Поиск

`Поле поиска` — поиск по ключевому слову

Подсказка

Поиск осуществляется по уникальному идентификатору (UUID) сессии, локальному и удалённому пути файла

Для выполнения поиска необходимо заполнить поле и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Экспортировать выбранные логи сессий — экспорт выбранных событий

Примечание

После выбора данного действия нужно выбрать необходимый формат файла

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Экспорт событий

Для массового экспорта событий необходимо:

1. Отметить необходимые события в таблице
2. Выбрать действие Экспортировать выбранные логи сессий
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Дата и время` — момент регистрации события на сервере
2. `Тип события` — тип записи: **«Видео запись сессии»** или **«Запись передачи файлов»**
3. `Подключение` — ссылка на связанную сессию (UUID); при нажатии открывает страницу *Сессии* с активным фильтром по этой сессии
4. `Действие с файлом` — выполненное действие в передаче файлов (загрузка, скачивание, удаление и т.д.)

> **Подсказка**
>
> Поле заполнено только у событий типа **«Запись передачи файлов»**. Для видеозаписей сессий отображается –

5. `Локальный путь` — путь к файлу на устройстве оператора
6. `Удалённый путь` — путь к файлу на устройстве клиента
7. `Начало` — момент начала записи или действия
8. `Конец` — момент завершения записи или действия
9. `Длительность` — продолжительность события (рассчитывается автоматически как разница между началом и концом)

> **Примечание**
>
> Создавать события вручную нельзя — записи появляются только в результате удалённых сессий с включённым мониторингом

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства события

Свойства события

Редактирование

Все поля свойств события доступны только для просмотра

Страница содержит вкладки:

1. `Основное`
    1. **Дата и время** — момент регистрации события на сервере

2. **Тип события** — **«Видео запись сессии»** или **«Запись передачи файлов»**
3. **Источник** — внутренний источник события (`SESSIONS`)
4. **Подключение** — ссылка на связанную сессию

2. `Файловые атрибуты`
    1. **Действие с файлом** — выполненное действие (только для записей передачи файлов)
    2. **Локальный путь** — путь на устройстве оператора
    3. **Удалённый путь** — путь на устройстве клиента
3. `Время`
    1. **Начало** — момент начала события
    2. **Конец** — момент завершения события
    3. **Длительность** — рассчитанная продолжительность
4. `Служебное`

    Развёртываемая вкладка с сырым содержимым поля `ext` события в формате JSON. Используется для диагностики

> **Примечание**
>
> Сами файлы видеозаписей и записи действий передачи файлов смотрите в свойствах сессии на вкладках *Записи сессии* и *Записи передачи файлов*

2.12.6 Сроки хранения журналов

Доступны только в UEM версии

Старые записи аудита можно удалять автоматически, чтобы ограничить объём сохраняемой истории. Сроки задаются в разделе **«Администрирование»** на странице **«Настройки»**, в блоке **«Настройки логов»**

Какие сроки действуют

Для разных видов записей используются отдельные настройки:

Поле	По умолчанию	Что ограничивает
Хранить логи выполнения задач, дней	7	Подробные журналы выполнения задач, работы с отдельными устройствами и миграций
Хранить логи, собранные с устройств, дней	7	События, полученные при сборе журналов с устройств
Хранить HTTP-запросы и выдачу файлов, дней	14	Историю веб-запросов и выдачи файлов
Хранить результаты задач, дней	30	События с результатами выполнения задач
Хранить остальные события аудита, дней	0	Остальные виды событий аудита

Примечание

Значение **0** отключает автоматическое удаление для соответствующей категории

Поле остальных событий не заменяет отдельные сроки: например, значение 0 в последней строке не сохраняет бессрочно логи выполнения задач

Как изменить срок

1. Открыть настройки сервера и найти **«Настройки логов»**
2. Проверить текущие значения, поскольку они могут отличаться от значений по умолчанию
3. Указать число дней для нужных категорий
4. Нажать **«Сохранить»** внизу страницы

Очистка планируется автоматически раз в час и удаляет записи старше заданного срока. После сохранения уменьшенного срока записи не обязаны исчезнуть сразу

Предупреждение

Уменьшение срока может привести к удалению уже накопленной истории при следующей очистке

До изменения сохранить записи, которые ещё нужны для расследования или отчётности

Последующее увеличение срока не восстанавливает уже удалённые записи

Почему результат задачи есть, а подробного лога нет

Подробный журнал и событие результата имеют разные сроки хранения. Например, при значениях по умолчанию подробный журнал старше 7 дней уже может быть удалён, а результат задачи ещё доступен в пределах своего 30-дневного срока

Примечание

Сроки на этой странице относятся к записям аудита. Они не задают срок хранения видеозаписей сессий и не удаляют файлы из репозиториев

2.12.7 Все логи

Доступны только в UEM версии

Все логи — на данной странице отображены события всех действий, выполненных на сервере **RuDesktop**

Подсказка

Страница **«Все логи»** доступна только при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

Страница объединяет в одну таблицу все события, попадающие в журналы сервера, — независимо от их источника:

- выполнения задач и политик (как на *Логи исполнения*)
- изменения объектов сервера (как на *Объекты*)
- входов в веб-интерфейс (как на *Входы в систему*)
- HTTP-запросов к серверу (как на *HTTP запросы*)

В отличие от специализированных страниц, здесь видно всё подряд — это удобно для общего разбора инцидента, когда заранее неизвестно, в каком журнале искать. Каждая запись помимо общих полей содержит **контент** — структурированную информацию, специфичную для типа события

Подсказка

Сюда же попадает учёт трафика, отданного сервером по HTTP:

- **Выдача файла** — одна запись на каждую загрузку файла с сервера или с *точки распространения* с указанием пути, имени файла, объёма и того, была ли загрузка завершена. Если файл используется в политике, событие связывается с ней

- **Раздача при установке ОС** — одна запись на сеанс сетевой *установки ОС*: объём накапливается по мере скачивания образа, отдельно учитывается идентификатор образа

По этим событиям строятся графики **«Трафик выдачи файлов»** на странице *Тренды*

Важно

Кнопка Очистить все логи доступна только суперпользователю и удаляет события сразу из всех журналов аудита. Удалённые записи восстановить нельзя

Подсказка

Часть HTTP-запросов можно исключать из журналов ещё до их регистрации. Для этого в *настройках сервера* заполните поле Исключения из логирования — указанные префиксы путей или регулярные выражения (через запятую, например: `/peers/get_peer_statuses/, /audit/requestevent/`) не попадут ни в **«HTTP запросы»**, ни в **«Все логи»**. Удобно для отсева частых служебных запросов, чтобы они не засоряли журналы

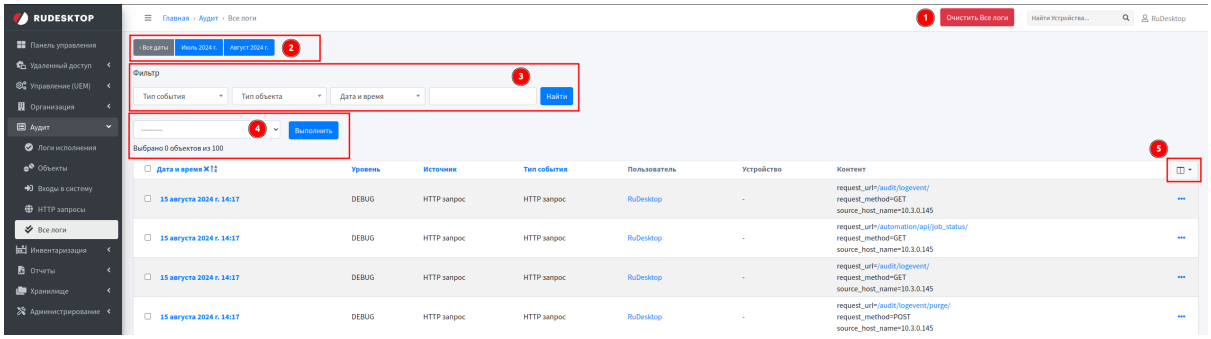
Добавление в адресную книгу

При массовом копировании устройств или адресов в книги, а также в личные книги выбранных пользователей создаётся событие `Добавление в адресную книгу`. Оно фиксирует инициатора операции и книгу-получатель. Для каждой выбранной книги создаётся отдельная запись, в том числе если все адреса уже присутствовали в ней.

В подробностях события можно проверить количество добавленных записей и пропусков. При копировании в личные книги других пользователей количество обработанных записей включает обновлённые адреса.

Описание страницы

На странице **«Все логи»** отображено:



1. Кнопка Очистить все логи

2. Фильтр даты
3. Фильтр
4. Массовые действия
5. Таблица с возможностью настройки отображаемых столбцов

Очистка всех логов

При нажатии на кнопку Очистить все логи произойдет удаление всех событий

> **Важно**
>
> Кнопка доступна только суперпользователю

Фильтр даты

Позволяет выбрать год, месяц и число с возможностью отображения событий за определённую дату

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. `Тип события` — тип, который произошел с событием
2. `Тип объекта` — тип, с которым выполнялись действия
3. `Дата и время` — позволяет выбрать период
4. `Поле поиска` — поиск по ключевому слову

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Экспортировать выбранные все логи — экспорт выбранных событий

> **Примечание**
>
> После выбора данного действия нужно выбрать необходимый формат файла

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Экспорт событий

Для массового экспорта событий необходимо:

1. Отметить необходимые события в таблице
2. Выбрать действие Экспортировать выбранные все логи
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Дата и время` — дата и время события
2. `Уровень` — уровень логирования
3. `Источник` — источник события
4. `Тип события` — тип, который произошел с событием
5. `Пользователь` — имя пользователя

Подсказка

При отображении в данном столбце — означает, что действие выполнялось от имени системы

6. `Устройство` — устройство, на котором выполнялось действие
7. `Контент` — информация о событии, на основании выполнения которого был выполнен лог

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства события

Свойства события

Редактирование

Страница содержит вкладки:

1. Основная информация:
    1. **Дата и время** — дата и время создания события
    2. **Уровень** — уровень логирования
    3. **Источник** — источник события
    4. **Тип события** — тип, который произошел с событием
    5. **Тип объекта** — тип, с которым выполнялись действия
    6. **Пользователь** — пользователь, выполнивший действия
    7. **Устройство** — устройство, на котором выполнялась задача/политика
    8. **Задача** — наименование задачи
    9. **Политика** — наименование политики
    10. **Подзадача** — системное имя подзадачи
2. Дополнительно
    1. **Производитель** — имя вендора
    2. **Продукт** — название продукта
    3. **Версия** — версия ПО

    Примечание

    Остальные поля отличаются от типа события

3. Объект

    На данной вкладке отображаются системные факты события

4. Лог

    На данной вкладке отображается полный текст лога события (поле заполняется при наличии расширенной информации)

Аудит - раздел для просмотра журналов событий сервера **RuDesktop**: выполнение задач и политик, изменения объектов (CRUD), входы в веб-интерфейс, HTTP-запросы к API, события удалённых сессий с записью видео и передачи файлов, а также сводный журнал по всем источникам

Подсказка

Раздел **«Аудит»** доступен только при использовании локального сервера **Управление конфигурациями (UEM)**

Часть запросов (например, к `/peers/get_peer_statuses/`) можно исключить из журналов через настройку **«Исключения из логирования»** в *настройках сервера*

Логи исполнения
События выполнения задач и политик на устройствах

Объекты
Журнал создания, изменения и удаления объектов сервера

Входы в систему
События авторизации в веб-интерфейсе сервера

HTTP запросы
Журнал HTTP-запросов к API сервера

Логи сессий
События записи видео и передачи файлов в удалённых сессиях

Все логи
Сводный журнал событий из всех источников

Сроки хранения журналов
Автоматическое удаление старых записей, значения по умолчанию и изменение сроков

2.13 Инвентаризация

2.13.1 Наличие ресурсов

Наличие ресурсов - программные и аппаратные компоненты удаленного устройства. Для установленного ПО доступны категории, типы, правообладатели и значимость для безопасности из *Классификатора ПО*. Использовать фильтр **«Классифицирован»** для поиска записей с назначенной классификацией или без неё

Классификацию отдельной записи можно выбрать в поле **«Классификатор ПО»** при наличии права изменения наличия ресурсов

Подсказка

Страница **«Наличие ресурсов»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Примечание

В таблице на странице представлены имеющиеся и отсутствующие ресурсы, включая удалённое программное обеспечение и изменения в аппаратной конфигурации устройства

Как это работает

Страница показывает **состояние ресурсов на конкретных устройствах** на момент последней инвентаризации

Каждая запись - это связка **ресурс + устройство** с двумя датами:

- **Присутствует с** - момент, когда ресурс впервые обнаружен на устройстве
- **Отсутствует с** - момент, когда ресурс перестал обнаруживаться (после деинсталляции пакета, замены оборудования и т.д.)

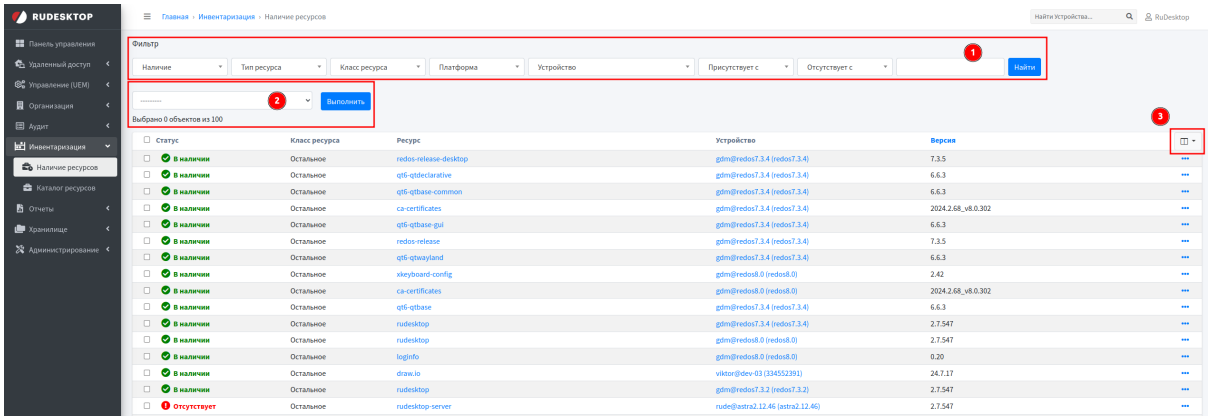
Записи появляются и обновляются автоматически после выполнения политики *Инвентаризация*. Сами **ресурсы** (карточки) хранятся отдельно - на странице *Каталог ресурсов*, а здесь отображается только их история наличия по устройствам

Подсказка

Для отслеживания файлов и директорий в политике **«Инвентаризация»** дополнительно нужно заполнить поле Наличие путей - без этого ресурсы типа `Файл/Директория` не появятся

Описание страницы

На странице **Наличие ресурсов** отображено:



1. Фильтр
2. Массовые действия
3. Таблица с возможностью настройки отображаемых столбцов

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. Наличие - фильтрация ресурсов в зависимости от их присутствия или отсутствия
2. Тип ресурса - фильтрация ресурсов по типу:
    1. `Пакет` - для отображения пакетов
    2. `Операционная система` - для отображения операционных систем
    3. `Патч` - для отображения патчей обновлений ОС
    4. `Устройство` - для отображения определенных устройств
    5. `Файл/Директория` - для отображения файлов и директорий

    > **Важно**
    >
    > Для отображения этих данных, в редактировании политики *Инвентаризация* необходимо заполнить поле Наличие путей

    6. `Пользователь` - для отображения учетных записей на устройствах
    7. `Группа` - для отображения групп пользователей
3. Класс ресурса - фильтрация ресурсов по классам:
    1. `Процессор` - для отображения процессоров устройств
    2. `Видеокарта` - для отображения видеокарт устройств
    3. `Материнская плата` - для отображения материнских плат устройств
    4. `Оперативная память` - для отображения оперативной памяти устройств
    5. `Система` - для отображения ОС устройств
    6. `Диск` - для отображения дисков устройств
    7. `PCI устройство` - PCI устройства расширений
    8. `Монитор` - для отображения мониторов устройств
    9. `Сеть` - для отображения сетевых устройств
    10. `Устройства` - для отображения аппаратной части устройств
    11. `Остальное` - для отображения пакетов или устройств, не попадающих в существующие классы

12. `Локальный пользователь` - для отображения локальных учетных записей на устройствах
13. `Локальная группа` - для отображения локальных групп пользователей на устройствах
14. `Шифрование` - отображение ПО для шифрования на устройствах (например BitLocker)
15. `Безопасность` - для отображения средств защиты и параметров безопасности устройств
16. `Служба` - для отображения системных служб устройств
17. `Плагин браузера` - для отображения плагинов, установленных в браузерах устройств

4. Платформа - фильтрация по типу платформы:
    1. `Android`
    2. `Linux`
    3. `Mac OS`
    4. `Windows`
5. Группа - фильтрация по группе устройств
6. Версия ОС - фильтрация по версии операционной системы устройства
7. Устройство - фильтрация по конкретному устройству
8. Присутствует с - для фильтрации присутствующих в определенном интервале ресурсов
9. Отсутствует с - для фильтрации отсутствующих в определенном интервале ресурсов
10. Поле поиска - поиск по ключевому слову

> **Подсказка**
>
> Поиск осуществляется по типу ресурса, имени и GUID ресурса, а также по идентификатору, hostname и имени пользователя устройства, и по версии ресурса

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные ресурсы - удаление выбранных ресурсов
2. Экспортировать выбранные ресурсы - экспорт выбранных ресурсов

Примечание

После выбора данного действия нужно выбрать необходимый формат файла

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление ресурсов

Для массового удаления ресурсов необходимо:

1. Отметить необходимые ресурсы в таблице
2. Выбрать действие Удалить выбранные ресурсы
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие ресурсы будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные ресурсы будут удалены

Экспорт ресурсов

Для массового экспорта ресурсов необходимо:

1. Отметить необходимые ресурсы в таблице
2. Выбрать действие Экспортировать выбранные ресурсы
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Статус` - наличие или отсутствие ресурса
2. `Класс ресурса` - класс, к которому принадлежит ресурс
3. `Ресурс` - наименование ресурса
4. `Пользователь` - имя пользователя устройства, на котором обнаружен ресурс

5. Устройство - устройство, к которому принадлежит ресурс
6. Дата установки - дата, когда ресурс был впервые обнаружен на устройстве
7. Версия - версия ресурса
8. Присутствует с - дата и время, когда ресурс стал доступен
9. Отсутствует с - дата и время, когда ресурс стал отсутствовать

Примечание

При нажатии на наименование устройства откроются *свойства устройства*

При нажатии на ресурс откроется карточка ресурса, подробнее на странице *Каталог ресурсов*

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. Редактировать - при выборе этого пункта откроются свойства ресурса
2. Удалить - при выборе этого пункта ресурс будет удален
3. История изменений - при выборе этого пункта будет отображена история ресурса: создание/редактирование и пользователь, который выполнил данные операции

Свойства ресурса

Редактирование

При нажатии на кнопку Редактировать откроется страница свойств

Доступные поля:

1. Единица измерения - является системной переменной

Подсказка

Отображается при открытии свойств дисков или оперативной памяти

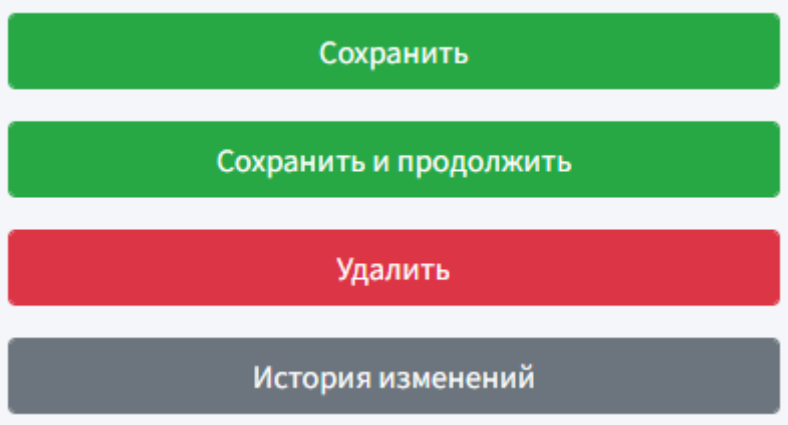
2. Ресурс - наименование ресурса
3. Устройство - устройство, к которому ресурс относится
4. Присутствует с - дата первого обнаружения ресурса
5. Отсутствует с - дата, с которой ресурс отсутствует

6. `Версия` - версия ресурса
7. `Классификатор ПО` - связь с пакетом в справочнике классификации
8. `Объем` - объем ресурса

> **Подсказка**
>
> Отображается при открытии свойств дисков или оперативной памяти

> **Примечание**
>
> Сведения о ресурсе, устройстве, версии, объёме и времени присутствия доступны только для чтения
>
> Записи появляются при инвентаризации, добавлять их вручную нельзя
>
> Поле **«Классификатор ПО»** можно изменить при наличии соответствующего права

Меню действий



Имеет следующие возможности:

1. Сохранить - производит сохранение внесенных изменений и перенаправляет на страницу **«Наличие ресурсов»**
2. Сохранить и продолжить - производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить - производит удаление ресурса и перенаправляет на страницу **«Наличие ресурсов»**

> **Примечание**
>
> 1. После нажатия на кнопку Удалить откроется страница подтверждения удаления ресурса

2. После подтверждения удаления ресурса произойдет переход на страницу **«Наличие ресурсов»** и появится уведомление Успешно удален ресурс

4. История изменений - отображает все изменения, выполненные для этого ресурса

2.13.2 Каталог ресурсов

Каталог ресурсов — программные и аппаратные компоненты удаленного устройства

Подсказка

Страница **«Каталог ресурсов»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Примечание

В таблице на данной странице показаны все ресурсы устройств, такие как удалённое программное обеспечение или изменения в аппаратной конфигурации устройства

Как это работает

Если на странице *Наличие ресурсов* отображается **связка ресурс + устройство**, то на странице **«Каталог ресурсов»** хранятся **карточки самих ресурсов** — без привязки к конкретному устройству

Каждая карточка описывает ресурс одной записью с уникальным идентификатором (GUID), типом и классом, набором фактов и при необходимости — командой для удаления и URL до источника. Карточки используются для:

- группировки одинаковых ресурсов с разных устройств в одну запись
- хранения «эталонных» данных (имя, версия, GUID, оригинальный URL)
- ссылок из таблицы наличия — кликом по ресурсу открывается его карточка
- ручного добавления ресурсов, которые не приходят с устройств автоматически

Большинство карточек создаётся автоматически при выполнении политики *Инвентаризация*, но при необходимости карточку можно создать вручную через кнопку Добавить ресурс

Подсказка

Столбец **«История»** показывает количество устройств, у которых этот ресурс зафиксирован — клик по числу открывает страницу *Наличие ресурсов* с активным фильтром по выбранной карточке

Уникальный идентификатор ресурса

У каждой карточки каталога есть уникальный идентификатор (GUID). Он нужен для того, чтобы система могла однозначно отличать одну запись от другой и не создавать дубликатов при повторных инвентаризациях устройств

Для ресурсов, добавленных вручную, идентификатор задаёт пользователь в поле Уникальный идентификатор. Для ресурсов, поступающих с устройств в ходе политики *Инвентаризация*, идентификатор рассчитывается сервером автоматически — одним из двух способов

Заводской или системный идентификатор

Используется тогда, когда у ресурса уже есть собственный надёжный идентификатор — он берётся напрямую из данных, присланных устройством:

1. `Операционная система` — ключ продукта Windows; если он недоступен — аппаратный UUID устройства
2. `Материнская плата` — серийный номер платы
3. `Диск` — собственный идентификатор тома (macOS), идентификатор таблицы разделов (Linux) или физический идентификатор устройства (Windows)
4. `Монитор` — серийный номер монитора
5. `Сеть` — MAC-адрес сетевого адаптера
6. `Устройства` (PCI и USB) — связка идентификатора производителя и идентификатора устройства (`VID:PID` или `VEN:DEV`)
7. `Шифрование` — Recovery ID BitLocker
8. `Локальный пользователь`, `Локальная группа` — SID учётной записи или группы
9. `Патч` — номер обновления (например, `KB5005565`)
10. `Пакет` для Windows — GUID установщика MSI, извлечённый из команды удаления
11. `Пакет` для Android — идентификатор приложения (например, `com.example.app`)
12. `Пакет` для Linux и macOS — имя пакета

Производный идентификатор, рассчитанный системой

Применяется для ресурсов, у которых нет собственного устойчивого идентификатора. В этом случае сервер берёт характеристики самого ресурса и идентификатор устройства, на котором он обнаружен, и преобразует их в короткий устойчивый код:

1. `Процессор` — идентификатор устройства + название процессора
2. `Видеокарта` — идентификатор устройства + производитель + модель
3. `Оперативная память` — название модуля + слот + производитель + объём
4. `Безопасность` (модуль TPM) — идентификатор устройства + производитель + версия спецификации
5. `Служба` — идентификатор устройства + имя службы
6. `Плагин браузера` — название браузера + идентификатор плагина

В качестве идентификатора устройства используется его аппаратный UUID, заданный на уровне материнской платы. Если получить его не удалось — используется сетевое имя (hostname)

Подсказка

Этот же способ работает как резервный для ресурсов из первого списка — если их собственный идентификатор отсутствует или недостоверен (например, серийный номер платы помечен как `Unknown`)

Примечание

Производный идентификатор всегда одинаковый для одного и того же ресурса на одном и том же устройстве — поэтому при повторной инвентаризации существующая карточка обновляется, а не создаётся заново

Важно

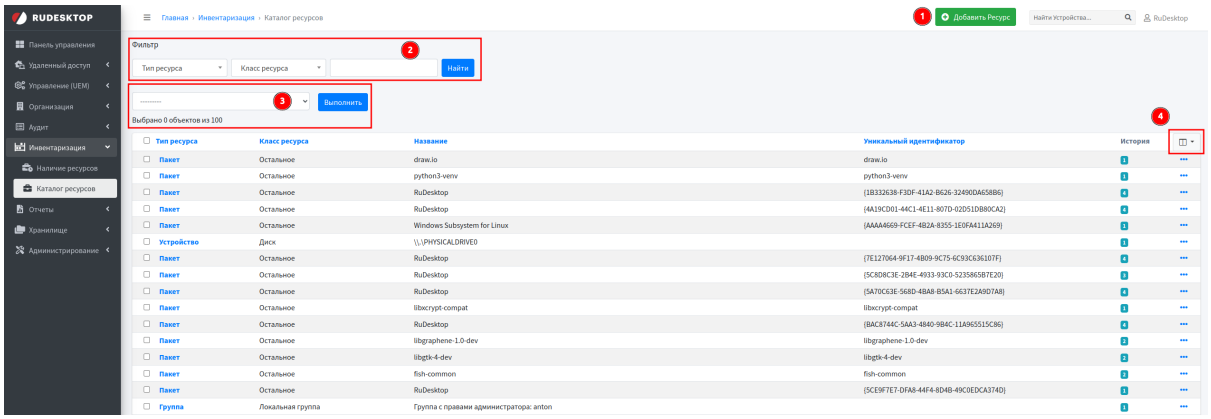
Если у устройства меняется аппаратный UUID (например, при пересоздании виртуальной машины без сохранения характеристик «железа»), производные идентификаторы всех его ресурсов изменятся — система воспримет их как новые карточки

Примечание

Для классов `Файл/Директория` и в редких случаях, когда устройство не передало необходимых данных, идентификатор может оставаться пустым — уникальность карточки в этом случае обеспечивается комбинацией типа, класса и названия

Описание страницы

На странице **«Каталог ресурсов»** отображено:



1. Кнопка Добавить ресурс
2. Фильтр
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление ресурса

При нажатии на кнопку Добавить ресурс откроется страница добавления ресурса со следующими полями:

1. Тип ресурса — тип, к которому принадлежит ресурс
2. Класс ресурса — класс, к которому принадлежит ресурс
3. Название — название ресурса
4. Уникальный идентификатор — уникальный идентификатор ресурса
5. Команда для удаления — команда для удаления установленного пакета
6. URL — URL до ресурса
7. Дополнительная информация — факты устройства, собранные при инвентаризации

Фильтр

Можно формировать таблицу для получения определенных данных, используя фильтр:

1. Тип ресурса — фильтрация ресурсов по типу:
    1. `Пакет` — для отображения пакетов
    2. `Операционная система` — для отображения операционных систем
    3. `Патч` — для отображения патчей обновлений ОС
    4. `Устройство` — для отображения определенных устройств
    5. `Файл/Директория` — для отображения файлов и директорий

Важно

Для отображения этих данных в редактировании политики *Инвентаризация* необходимо заполнить поле Наличие путей

6. `Пользователь` — для отображения учетных записей на устройствах
7. `Группа` — для отображения групп пользователей

2. Класс ресурса — фильтрация ресурсов по классам:
   1. `Процессор` — для отображения процессоров устройств
   2. `Видеокарта` — для отображения видеокарт устройств
   3. `Материнская плата` — для отображения материнских плат устройств
   4. `Оперативная память` — для отображения оперативной памяти устройств
   5. `Система` — для отображения ОС устройств
   6. `Диск` — для отображения дисков устройств
   7. `PCI устройство` — PCI устройства расширений
   8. `Монитор` — для отображения мониторов устройств
   9. `Сеть` — для отображения сетевых устройств
   10. `Устройства` — для отображения аппаратной части устройств
   11. `Остальное` — для отображения пакетов или устройств, не попадающих в существующие классы
   12. `Локальный пользователь` — для отображения локальных учетных записей на устройствах
   13. `Локальная группа` — для отображения локальных групп пользователей на устройствах
   14. `Шифрование` — отображение ПО для шифрования на устройствах (например BitLocker)
   15. `Безопасность` — для отображения средств защиты и параметров безопасности устройств
   16. `Служба` — для отображения системных служб устройств
   17. `Плагин браузера` — для отображения плагинов, установленных в браузерах устройств
3. Поле поиска — поиск по ключевому слову

Подсказка

Поиск осуществляется по типу ресурса, его наименованию и уникальному идентификатору (GUID)

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Массовые действия

Доступные действия:

1. Удалить выбранные ресурсы — удаление выбранных ресурсов
2. Экспортировать выбранные ресурсы — экспорт выбранных ресурсов

> **Примечание**
>
> После выбора данного действия нужно выбрать необходимый формат файла

> **Важно**
>
> В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление ресурсов

Для массового удаления ресурсов необходимо:

1. Отметить необходимые ресурсы в таблице
2. Выбрать действие Удалить выбранные ресурсы
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация, какие ресурсы будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные ресурсы будут удалены

Экспорт ресурсов

Для массового экспорта ресурсов необходимо:

1. Отметить необходимые ресурсы в таблице
2. Выбрать действие Экспортировать выбранные ресурсы
3. Выбрать необходимый формат файла
4. Нажать на кнопку Выполнить
5. Файл будет загружен на устройство

Таблица

Таблица разбита по столбцам:

1. `Тип ресурса` — тип, к которому принадлежит ресурс
2. `Класс ресурса` — класс, к которому принадлежит ресурс
3. `Название` — наименование ресурса
4. `Уникальный идентификатор` — уникальный идентификатор ресурса
5. `История` — иконка с цифрой, отображающая количество устройств, на которых присутствует или отсутствует этот ресурс

> **Подсказка**
>
> При нажатии на иконку произойдет переход на страницу *Наличие ресурсов* с активным фильтром по выбранному ресурсу

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе этого пункта откроются свойства ресурса
2. `Удалить` — при выборе этого пункта ресурс будет удален
3. `История изменений` — при выборе этого пункта будет отображена история ресурса: создание/редактирование и пользователь, который выполнил данные операции

Свойства ресурса

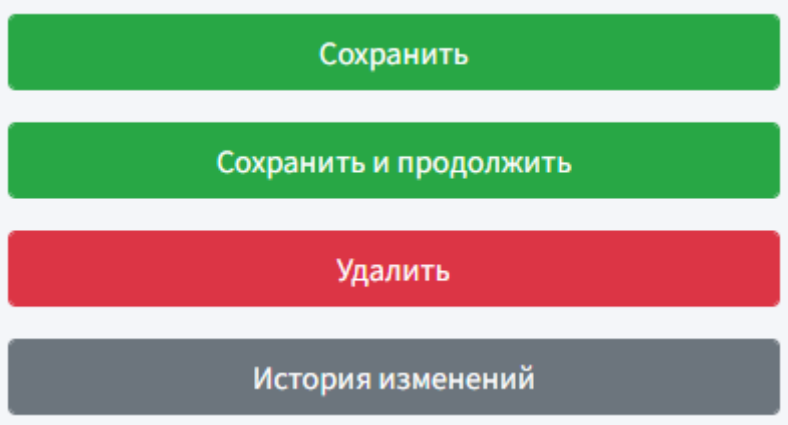
Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств

Доступные поля:

1. Тип ресурса — тип, к которому принадлежит ресурс
2. Класс ресурса — класс, к которому принадлежит ресурс
3. Название — название ресурса
4. Уникальный идентификатор — уникальный идентификатор ресурса
5. Команда для удаления — команда для удаления установленного пакета
6. URL — URL до ресурса
7. История — иконка с цифрой, отображающая количество устройств, на которых присутствует или отсутствует этот ресурс
8. Дополнительная информация — факты устройства, собранные при инвентаризации

Меню действий



Имеет следующие возможности:

1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Каталог ресурсов»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление ресурса и перенаправляет на страницу **«Каталог ресурсов»**

> **Примечание**
>
> 1. После нажатия на кнопку Удалить откроется страница подтверждения удаления ресурса
> 2. После подтверждения удаления ресурса произойдет переход на страницу **«Каталог ресурсов»** и появится уведомление Успешно удален ресурс

4. История изменений — отображает все изменения, выполненные для этого ресурса

2.13.3 Классификатор ПО

Классификатор ПО связывает обнаруженные пакеты с продуктами, категориями, типами ПО, значимостью для безопасности и правообладателями. Он помогает отбирать установленное ПО в разделе **«Наличие ресурсов»**

Как это работает

После обработки инвентаризации сервер сопоставляет присутствующие программные ресурсы без классификации со справочником. Для автоматической классификации в справочнике должна быть подходящая запись

При сопоставлении учитываются:

- **Семейство ОС** — одна программа может иметь разные записи для разных ОС
- **Имя пакета** — для Linux сохраняется различие точных имён, например `python3.11` и `python3.12` не считаются одним пакетом
- **Идентификатор продукта**, если он есть — для Windows и Android используется идентификатор, полученный при инвентаризации. Запись с заполненным ProductCode подбирается по идентификатору, а не только по похожему имени

При проверке совпадения учитывать ОС устройства и идентификатор программы. Отображаемое название установленной программы может отличаться от названия в классификаторе, например содержать номер версии или разрядность

Примечание

Службы и плагины браузеров исключены из автоматического сопоставления

Классификация назначается записи о наличии ресурса на конкретном устройстве. Она не заменяет сведения об установленной версии и не устанавливает, не удаляет и не блокирует программу

Продукт позволяет объединить пакеты одной программы, в том числе для разных ОС. Категория, тип ПО и значимость для безопасности относятся к продукту и общие для связанных с ним пакетов. Описание и правообладатель задаются в записи классификатора пакета

Просмотр и отбор установленного ПО

1. Выполнить инвентаризацию устройств со сбором установленного ПО
2. Открыть **«Инвентаризация → Наличие ресурсов»**
3. В фильтре **«Наличие»** выбрать присутствующие ресурсы, если нужен текущий состав
4. Использовать фильтры **«Категория ПО»**, **«Тип ПО»**, **«Значимость для безопасности»**, правообладателя и **«Классифицирован»**
5. Проверить устройство, ресурс и версию в найденных строках

В таблице доступны столбцы **«Категория ПО»** и **«Значимость для безопасности»**

Примечание

Если классификация отсутствует, в этих столбцах отображается прочерк. Это не означает отсутствие программы или установленную оценку её безопасности

Справочник пакетов

В **«Классификаторе ПО»** доступны поиск по пакету, ProductCode, продукту и правообладателю, а также фильтры по семейству ОС, категории, типу ПО и значимости для безопасности. Карточка содержит:

- **«Семейство ОС»** и **«Пакет»** - система и имя пакета для сопоставления
- **«ProductCode»** - идентификатор продукта, если он используется
- **«Продукт»** - общая классификация программы
- **«Описание»** и **«Правообладатель»** - дополнительные сведения о пакете

Для просмотра и изменения справочника нужны соответствующие права

Важно

При редактировании общего продукта учитывать, что его категория, тип и значимость изменятся для всех связанных записей классификатора

Если программа не классифицирована

1. Проверить, что инвентаризация завершилась и программа есть в **«Наличии ресурсов»** как присутствующая
2. Найти её в справочнике по имени пакета или идентификатору

   Учитывать семейство ОС - похожее название не гарантирует соответствие
3. При наличии подходящей записи открыть нужную строку **«Наличия ресурсов»**, выбрать **«Классификатор ПО»** и сохранить

Поиск в поле **«Классификатор ПО»** работает по имени пакета, ProductCode, названию продукта и категории ПО

Подсказка

Запись в списке содержит категорию, имя пакета и семейство ОС. Например:

```
Браузеры: firefox-esr (debian)
```

Результаты упорядочены по категории и имени пакета. Перед выбором сверить пакет и ОС с данными устройства

Для ручного назначения нужно право изменения наличия ресурсов. Открывать нужно действие **«Редактировать»** в строке наличия ресурса. Нажатие на название самого ресурса открывает его карточку в каталоге

Примечание

Ручное назначение действует на выбранную запись - другие устройства с такой же программой автоматически эту связь не получают. Автоматическое сопоставление заполняет только пустые связи. Уже выбранную классификацию оно не заменяет при следующей инвентаризации

Если подходящего пакета в справочнике нет, администратор с правами добавления пакетов и продуктов может создать нужные записи, выбрать существующие категорию, тип ПО и значимость для безопасности. Эти три справочника в интерфейсе доступны только для просмотра. Категории этого справочника описывают установленное ПО

Порядок категорий магазина приложений настраивается отдельно. После добавления пакета в справочник повторить инвентаризацию нужных устройств и проверить ранее неклассифицированные строки. Сохранение пакета само по себе не подтверждает, что существующие строки уже получили классификацию. Значимость для безопасности - характеристика продукта в справочнике

Она не является результатом проверки конкретного устройства на уязвимости. Наличие и версия программы отражают собранные данные - для проверки изменений на устройстве нужна новая инвентаризация

Пошаговый разбор поиска и ручного назначения приведён в кейсе Поиск установленного ПО по категориям

Для сводки установленных версий и проверки соответствия рекомендованной версии использовать *Аудит ПО*. Классификация пакетов отображается и в этом разделе

2.13.4 Аудит ПО

Аудит ПО показывает установленное ПО на доступных пользователю устройствах, диапазон обнаруженных версий и отклонения от рекомендованной версии. Данные обновляются после *инвентаризации* со сбором установленного ПО

Подготовка

1. Выполнить инвентаризацию устройств со сбором установленного ПО
2. Открыть **Инвентаризация → Аудит ПО**
3. Если инвентаризация выполнялась до появления этого раздела, администратору с правами суперпользователя нажать **Заполнить по данным инвентаризации**
4. Дождаться завершения фонового заполнения и обновить таблицу

Новая инвентаризация пополняет список автоматически. Ручное добавление и удаление записей в этом разделе недоступны

Примечание

Нужны права просмотра устройств и аудита ПО. Таблица и счётчики учитывают только устройства, доступные пользователю. Изменение настроек требует права изменения аудита ПО; рекомендации и флаг отслеживания сохраняются для общей записи ПО, а не отдельно для каждого пользователя

Просмотр списка

В таблице доступны название ПО, ОС, дистрибутив, сведения из *классификатора ПО*, количество устройств, диапазон версий, признак отслеживания, рекомендованная версия и количество устройств с несоответствующей версией

- Поиск выполняется по названию ПО и издателю
- Фильтры позволяют выбрать ОС, дистрибутив, отслеживаемое ПО, категорию, тип ПО и значимость для безопасности
- Нажатие на количество устройств открывает отфильтрованный *список устройств*
- Карточка ПО показывает распределение установленных версий и связанные ресурсы со ссылками на *историю наличия ресурсов*

Для Linux пакет учитывается отдельно по семействам дистрибутивов: версии одноимённого пакета в разных дистрибутивах могут иметь разный порядок сравнения. Службы и плагины браузеров не включаются в список установленного ПО

Для учёта приобретённых ключей и проверки количества установок использовать раздел *Лицензии ПО*

Рекомендованная версия

1. Открыть карточку нужного ПО
2. Выбрать **Оператор сравнения**: =, ≠, >, ≥, < или ≤
3. Заполнить **Рекомендованную версию**, например `2.0` с оператором ≥
4. Сохранить и проверить столбец **Устройств с несоответствующей версией**
5. Нажать на счётчик, чтобы перейти к устройствам с версиями, не удовлетворяющими условию

Для удаления условия очистить рекомендованную версию и сохранить карточку. Это поле служит для проверки собранных данных и само по себе не обновляет ПО

Примечание

Версии Debian и RPM сравниваются по правилам соответствующего формата, остальные — по числовым компонентам. Если версию нельзя упорядочить, использовать = или ≠ для точного сравнения. Вместо диапазона для таких версий может отображаться перечень значений; отсутствие версии показывается как **Неизвестная версия**

Версия, которую нельзя сравнить с рекомендацией, не включается в счётчик несоответствий. Поэтому нулевой счётчик сам по себе не подтверждает соответствие программ с неизвестными или несравнимыми версиями

Отслеживание изменений

1. В карточке включить **Отслеживать версию**, либо применить действие **Включить отслеживание версии** к одной или нескольким строкам
2. Создать *уведомление* и включить **Уведомлять об изменении версий отслеживаемого ПО**
3. Настроить канал и получателей, затем сохранить уведомление
4. Повторять инвентаризацию устройств, чтобы сервер обнаруживал изменения

Если рекомендованная версия не задана, уведомление сообщает об изменениях версий отслеживаемого ПО. Если задана — только об изменениях, после которых версия не соответствует условию. Первая установка, полное удаление программы и возврат к исходному набору версий в пределах периода сбора уведомления не считаются изменением версии для этого уведомления

Для прекращения отслеживания снять флаг в карточке или применить **Отключить отслеживание версии**. Проверка рекомендованной версии в таблице при этом остаётся доступна

2.13.5 Лицензии ПО

Раздел **Инвентаризация → Лицензии ПО** хранит сведения о приобретённых лицензиях на программы и сопоставляет количество мест с установленным ПО по данным *инвентаризации*. Добавление ключа в этот раздел не активирует программу на устройстве

Практический пример — Контроль количества лицензий на ПО

Подсказка

Для работы с разделом нужны права на лицензии ПО. Выбор ПО требует права просмотра аудита ПО, а назначение устройств — права просмотра устройств

Добавление лицензии

1. Выполнить инвентаризацию со сбором установленного ПО и проверить записи в *Аудите ПО*
2. Открыть **Инвентаризация → Лицензии ПО** и добавить лицензию
3. В поле **ПО** выбрать соответствующие записи из аудита. Для лицензии, распространяющейся на несколько ОС или дистрибутивов, можно выбрать несколько записей
4. Заполнить **Название лицензии**, **Ключ лицензии** и **Количество мест** — не меньше одного
5. При необходимости указать **Назначенные устройства** — компьютеры, за которыми закреплена лицензия
6. Сохранить запись и проверить счётчики в списке

Подсказка

Кнопка **Добавить устройства с выбранным ПО** подбирает устройства по результатам инвентаризации. Перед сохранением проверить список назначений и количество мест. Если добавлена только часть устройств, под списком появится сообщение об этом

Название и ключ вместе должны быть уникальны. Назначить одной лицензии больше устройств, чем указано мест, нельзя. Назначение устройства не устанавливает на него ПО

Важно

Запись без выбранного **ПО** можно сохранить, но она не участвует в подсчёте установок и проверке превышения. Связь с ПО задаётся вручную

Как считаются места и устройства

Если несколько лицензий связаны с одним и тем же ПО, их места суммируются. Связь может проходить через несколько записей ПО: например, лицензия на Windows и Linux объединяет их учёт с другими лицензиями, содержащими эти же записи. Поэтому объединяйте только те программы, для которых действительно действует общий лимит

При проверке превышения одно устройство учитывается один раз, даже если на нём установлены несколько программ из такого объединения

В таблице доступны:

- **Установлено** — количество доступных вам устройств с ПО, выбранным в данной лицензии. Красный цвет означает превышение общего числа мест у связанных лицензий
- **Назначено** — количество доступных вам устройств, закреплённых за этой лицензией
- **Установлено без назначения** — устройства с выбранным ПО, не назначенные ни одной из связанных лицензий. Если у связанных лицензий вообще нет назначенных устройств, этот контроль не применяется и отображается прочерк

Нажатие на счётчик открывает соответствующий список устройств

Поиск в списке лицензий работает по названию, ключу, связанному ПО, а также по имени, псевдониму или ID назначенного устройства. Доступен фильтр по ОС

Примечание

Записи лицензий общие для сервера. Счётчики и списки устройств ограничены вашими правами доступа, а превышение числа мест проверяется по всем устройствам сервера. Поэтому красный индикатор возможен и при небольшом числе видимых вам установок

Импорт из файла

В списке лицензий нажать **Импорт лицензий**, выбрать файл и нажать **Импортировать**. Поддерживаются CSV, XLSX, JSON, YAML, TSV и XLS

Подсказка

Размер файла — не больше 5 МБ, количество строк данных — не больше 10 000. Для CSV и TSV использовать кодировку UTF-8

Столбцы файла:

- **Название лицензии** (`name`) и **Ключ лицензии** (`key`) — обязательные
- **Количество мест** (`seats`) — необязательный
- **Назначенные устройства** (`peers`) — необязательный; в ячейке указывается один ID устройства RuDesktop

Можно использовать русские заголовки или указанные в скобках имена полей. Чтобы назначить несколько устройств, повторить название и ключ в нескольких строках, указав разные ID. Такие строки создают одну лицензию; явно заданное количество мест в них должно совпадать. Если количество мест не заполнено, оно определяется по числу указанных устройств, но составляет не меньше одного

Устройства должны быть зарегистрированы на сервере и доступны пользователю, выполняющему импорт. Для импорта назначений нужны права просмотра устройств

При ошибках в строках новые лицензии не сохраняются: исправить файл и повторить импорт. Уже существующие пары «название — ключ» пропускаются с сообщением о конфликте, их данные не перезаписываются

После импорта открыть записи и выбрать **ПО**: импорт не создаёт эту связь автоматически

Уведомления

В UEM можно получать сообщения о превышении количества мест и установках без назначения:

1. Создать *уведомление*
2. На вкладке **Инвентаризация** включить **Уведомлять о превышении количества лицензий на ПО**
3. Настроить получателей и канал доставки — Email, телефон, Telegram или MAX — затем сохранить уведомление
4. Продолжать выполнять инвентаризацию со сбором установленного ПО

Сообщение о превышении отправляется при первом обнаружении, затем — при увеличении числа установок по сравнению с последним отправленным оповещением. Неизменившееся превышение не повторяется после каждой инвентаризации. После возврата в пределы лимита новое превышение снова вызывает оповещение

Сообщение об установке без назначения появляется при обнаружении новой установки на устройстве, не закреплённом ни за одной из связанных лицензий. Этот контроль работает только при наличии назначенных устройств у связанных лицензий

Инвентаризация - раздел для централизованного просмотра программных и аппаратных ресурсов, собранных с управляемых устройств. Содержит каталог карточек ресурсов и журнал их наличия по конкретным устройствам с историей появления и удаления

Подсказка

Раздел **«Инвентаризация»** доступен при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Данные в нём появляются после выполнения политики *Инвентаризация* на устройствах

Примечание

Сбор данных выполняется командами, которые запускает клиент на устройстве. На **32-битном** клиенте (установленном или portable), работающем в 64-битной **Windows**, сбор выполняется в 32-битной среде (WOW64): системный реестр и файловая система видны в 32-битном отображении, поэтому данные о 64-битных программах и компонентах могут не попасть в инвентаризацию. На 64-битных операционных системах используйте 64-битный клиент

Наличие ресурсов

Журнал наличия ресурсов на конкретных устройствах с историей

Каталог ресурсов

Карточки программных и аппаратных ресурсов с GUID

Классификатор ПО

Категории установленного ПО, типы, значимость для безопасности и правообладатели

Аудит ПО

Установленные версии ПО, рекомендации и отслеживание изменений

Лицензии ПО

Учёт ключей, количества мест и назначенных устройств, контроль превышения

2.14 Отчеты

Доступны в УД и UEM версиях

2.14.1 Аналитика

Доступна только в UEM версии

Главная

Доступна только в UEM версии

Примечание

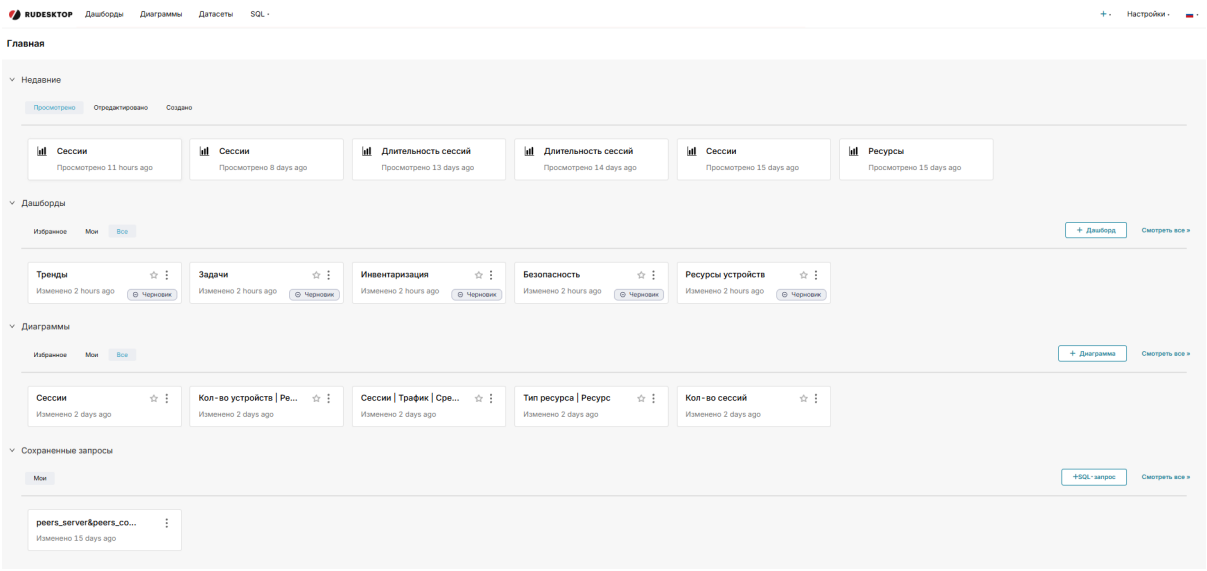
Страница является частью встроенного Apache Superset[26] и описывается здесь только в объёме, нужном для работы внутри **RuDesktop**. Полное описание см. в официальной документации Superset

Как это работает

Страница служит точкой входа в Superset из интерфейса **RuDesktop** и группирует ссылки на объекты, к которым у пользователя уже есть доступ. На вкладках Недавние и Сохраненные запросы выбор переключает источник по типу взаимодействия (что просматривал, редактировал, создавал, выполнял), а на вкладках Дашборды и Диаграммы — по типу владения (избранное, мои, все доступные)

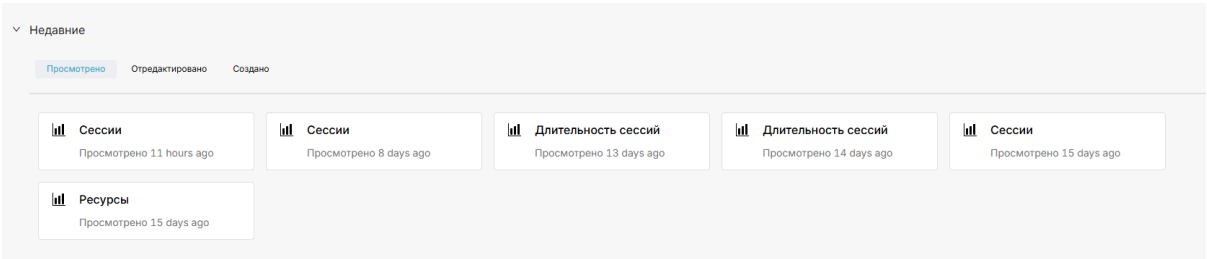
Описание

На странице представлены дашборды и диаграммы, доступные пользователю



Недавние

На вкладке Недавние представлена информация о дашбордах и диаграммах, которые пользователь недавно просматривал, редактировал или создавал



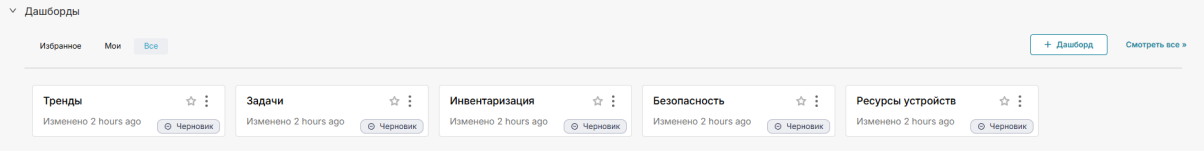
[26] https://superset.apache.org/

Можно выбрать один из следующих режимов отображения:

- Просмотрено — показывает дашборды и диаграммы, которые пользователь просматривал
- Отредактировано — содержит дашборды и диаграммы, которые редактировал пользователь
- Создано — включает дашборды и диаграммы, которые создал пользователь

Дашборды

На вкладке Дашборды представлена информация о дашбордах, которые доступны пользователю

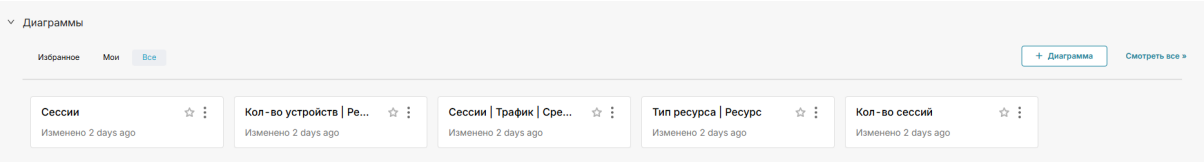


Можно выбрать один из следующих режимов отображения:

- Избранное — показывает дашборды, которые пользователь отметил как избранные
- Мои — содержит дашборды, владельцем которых является пользователь
- Все — включает дашборды, к которым пользователь имеет доступ

Диаграммы

На вкладке Диаграммы представлена информация о диаграммах, которые доступны пользователю

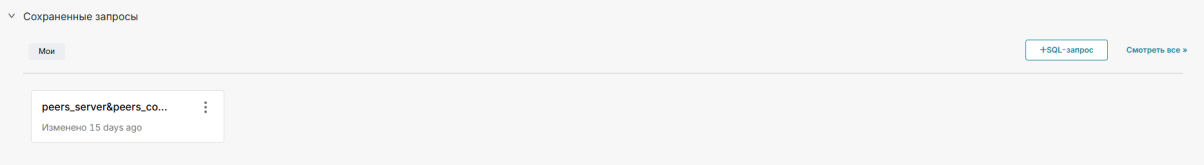


Можно выбрать один из следующих режимов отображения:

- Избранное — показывает диаграммы, которые пользователь отметил как избранные
- Мои — содержит диаграммы, владельцем которых является пользователь
- Все — включает диаграммы, к которым пользователь имеет доступ

Сохраненные запросы

На вкладке Сохраненные запросы представлена информация о пользовательских запросах, которые были сохранены



Можно выбрать один из следующих режимов отображения:

- Мои — показывает запросы, которые пользователь выполнял

Доступ и аутентификация

Доступно только в UEM версии

Примечание

Страница описывает интеграцию встроенного Apache Superset[27] с сервером **RuDesktop** в объёме, нужном для работы внутри **RuDesktop**. Полное описание системы ролей Superset см. в официальной документации

Как это работает

Вход в модуль аналитики выполняется через единый вход (**SSO**) сервера **RuDesktop** — отдельная учётная запись и пароль для Superset не требуются. Пользователь авторизуется своей учётной записью **RuDesktop**, а сервер передаёт в Superset его данные, статус и группы

Регистрация пользователей

При первом входе пользователь **автоматически регистрируется** в Superset — заводить его вручную не нужно

Важно

Войти в модуль аналитики могут только **активные** пользователи **RuDesktop**. Для заблокированных (неактивных) учётных записей вход не выполняется

Роли и права

Роль в Superset назначается на основании учётной записи **RuDesktop** и **пересчитывается при каждом входе** — изменение статуса пользователя на сервере применяется при его следующем входе в модуль аналитики

- **Суперпользователь RuDesktop** получает роль **Admin** — полный доступ к возможностям Superset
- Остальные пользователи получают роль по умолчанию (**Public**), права которой определяются настройками Superset

[27] https://superset.apache.org/

Подсказка

Доступ к конкретным объектам (дашбордам, диаграммам, датасетам, базам данных) определяет сам Superset на основании ролей. Подробнее о ролях и правах — в официальной документации Superset

Группы

Группы, в которых состоит пользователь в **RuDesktop**, при входе **автоматически создаются** в Superset, и пользователь добавляется в них. Это позволяет переиспользовать структуру групп **RuDesktop** для разграничения доступа в модуле аналитики

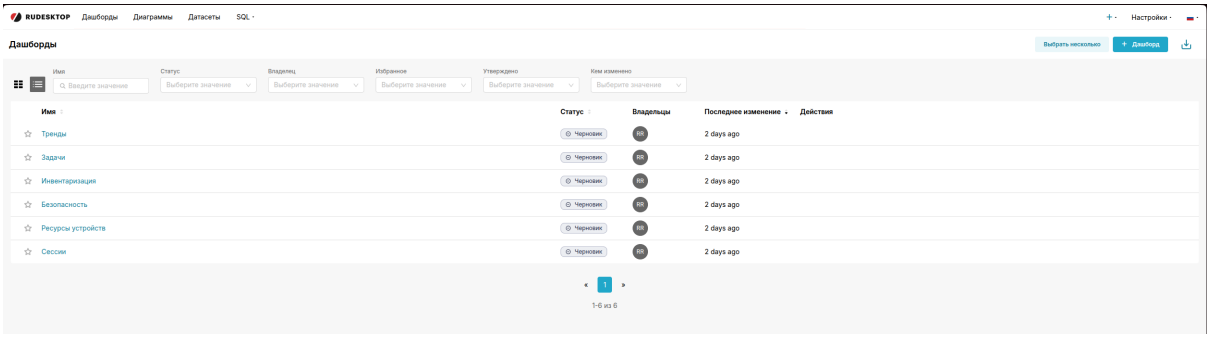
Дашборды

Доступны только в UEM версии

Дашборды — это объекты Apache Superset[28], объединяющие несколько диаграмм с общими фильтрами и разделителями

Примечание

Дашборды реализованы средствами встроенного **Apache Superset**. Полное описание возможностей см. в документации Superset[29]



Как это работает

Дашборд собирается из готовых *диаграмм* Superset и сохраняется как самостоятельный объект. На дашборде можно:

- размещать диаграммы в произвольном порядке через drag-and-drop, добавлять разделители и текстовые блоки
- настраивать **глобальные фильтры** — одно изменение фильтра применяется ко всем диаграммам дашборда сразу
- ограничивать доступ средствами ролевой модели Superset и выбором владельцев

[28] https://superset.apache.org/
[29] https://superset.apache.org/docs/using-superset/creating-your-first-dashboard

- публиковать дашборд (статус Опубликовано) или держать его как черновик до готовности
- экспортировать и импортировать дашборды между экземплярами Superset

Дашборд можно отметить как **избранный** — он попадёт в одноимённую вкладку на странице *Главная*

Описание

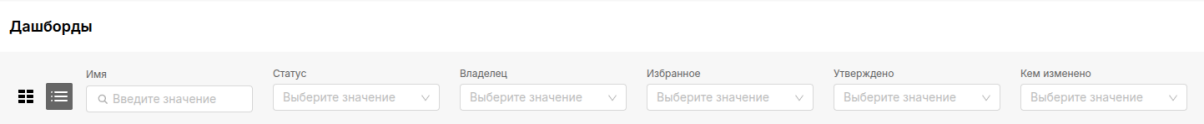
Эта страница предоставляет подробную информацию о дашбордах, включая фильтрацию и сортировку, а также функции экспорта и импорта

Примечание

Также доступны функции для создания, просмотра, редактирования и удаления дашбордов

При нажатии на имя дашборда из списка с подробной информацией о дашборде или из плитки с детальной информацией дашборд откроется в режиме просмотра

Фильтры



Дашборды можно отфильтровать по следующим критериям:

- Имя — название дашборда
- Статус — статус дашборда, доступные варианты: Опубликовано или Черновик
- Владелец — автор дашборда, доступные варианты основываются на списке пользователей
- Избранное — состояние дашборда, добавленного пользователем в избранное, доступные варианты: Да или Нет
- Утверждено — наличие информации об утверждении дашборда пользователем или ролью; доступные варианты: Да или Нет
- Кем изменено — пользователь, который последним редактировал дашборд, доступные варианты определяются списком пользователей

Сортировка

Сортировка в списочном режиме

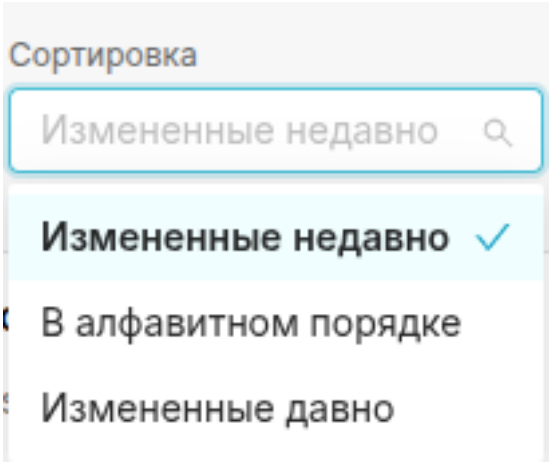
В списочном режиме дашборды можно отсортировать по следующим критериям:

- Имя — название дашборда
- Статус — текущее состояние дашборда, доступные варианты: `Опубликовано` и `Черновик`
- Последнее изменение — дата, когда дашборд был изменён в последний раз

Подсказка

По умолчанию дашборды сортируются по дате `Последнего изменения`

Сортировка в плиточном режиме



В плиточном режиме дашборды можно отсортировать по следующим критериям:

- Измененные недавно — по дате последнего изменения в порядке убывания
- В алфавитном порядке — по названию дашборда в порядке возрастания
- Измененные давно — по дате последнего изменения в порядке возрастания

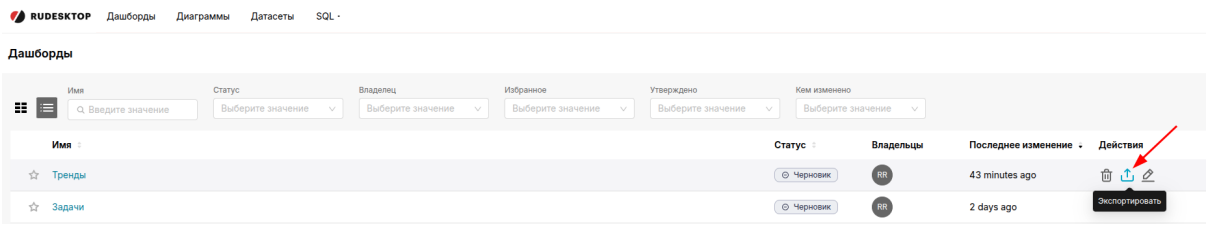
Подсказка

По умолчанию дашборды сортируются по критерию `Измененные недавно`

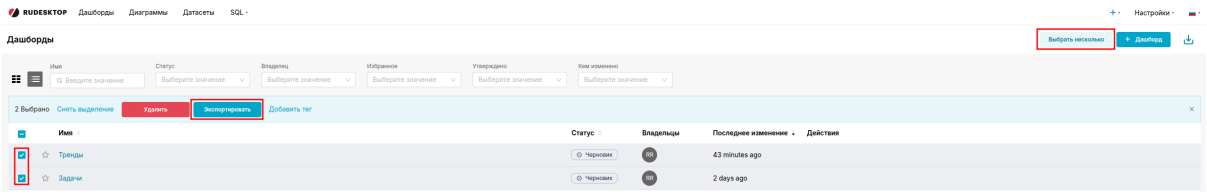
Экспорт

Экспорт в списочном режиме

Чтобы экспортировать один дашборд, наведите курсор на соответствующий элемент списка и выберите действие Экспортировать

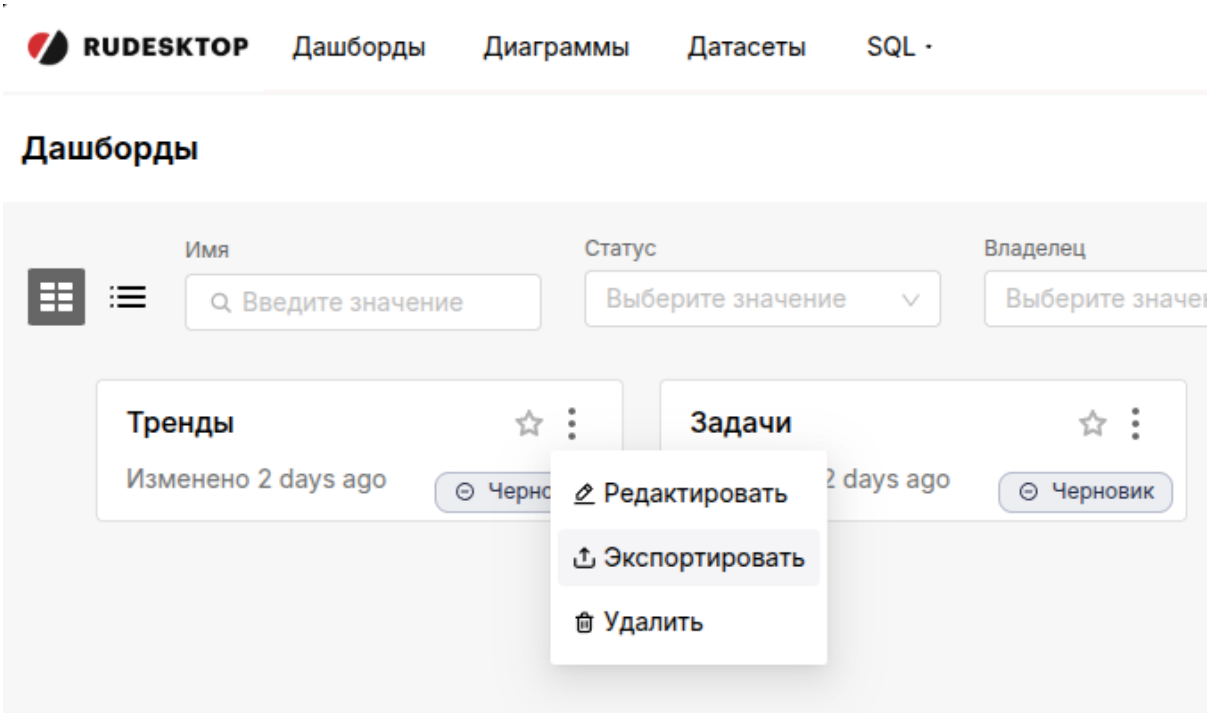


Для экспорта нескольких дашбордов нажмите на кнопку Выбрать несколько, отметьте нужные дашборды и затем нажмите на кнопку Экспортировать

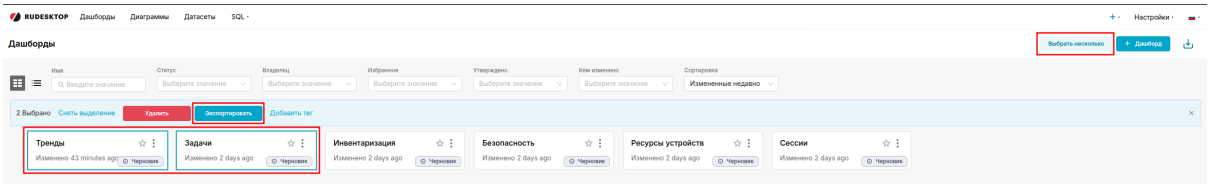


Экспорт в плиточном режиме

Чтобы экспортировать один дашборд, нажмите на кнопку , затем выберите действие Экспортировать



Для экспорта нескольких дашбордов нажмите на кнопку Выбрать несколько, выберите одну или несколько плиток, а затем нажмите на кнопку Экспортировать



Важно

В случае успешного выполнения экспорта дашбордов в папке `Загрузки` на устройстве пользователя появится архив с экспортированными дашбордами, где наименование архива будет отражать информацию о типе экспорта и дате выполнения операции

Импорт

Чтобы импортировать один или несколько дашбордов, выполните следующие действия:

1. Нажать на кнопку в правом верхнем углу
2. В появившемся окне нажать на кнопку Выбрать файл
3. В появившемся окне найти и выбрать нужный архив с экспортированными дашбордами
4. Нажать на кнопку Открыть

Важно

- Когда вы выбираете архив, информация о нем передается в интерфейс импорта дашбордов, и кнопка Импорт становится доступной
- Чтобы удалить информацию, наведите курсор на элемент списка и выберите `Удалить файл`
- Если вы выберете другой архив, текущая информация будет заменена новой

5. Нажать на кнопку Импорт

Важно

- При импорте дашбордов система сравнивает содержимое архива с данными в базе данных. Если найдены совпадения, пользователю отображается предупреждение
- Чтобы продолжить процесс, введите слово OVERWRITE в соответствующее поле и нажмите кнопку Перезаписать

Если импорт дашбордов прошел успешно, содержимое архива будет записано в базу данных. Затем все объекты из архива будут импортированы, и пользователь будет назначен владельцем этих импортированных объектов

Создание дашборда

Для создания дашборда необходимо нажать на кнопку + Дашборд в правом верхнем углу

Дашборд откроется в режиме, который позволяет редактировать его представление. Здесь вы можете задать название дашборда и добавить на него уже существующие диаграммы и элементы дизайна

Чтобы создать новую диаграмму в отдельной вкладке, нажмите на кнопку + Создать новую диаграмму

Подсказка

При сохранении диаграммы система предложит добавить ее в редактируемый дашборд

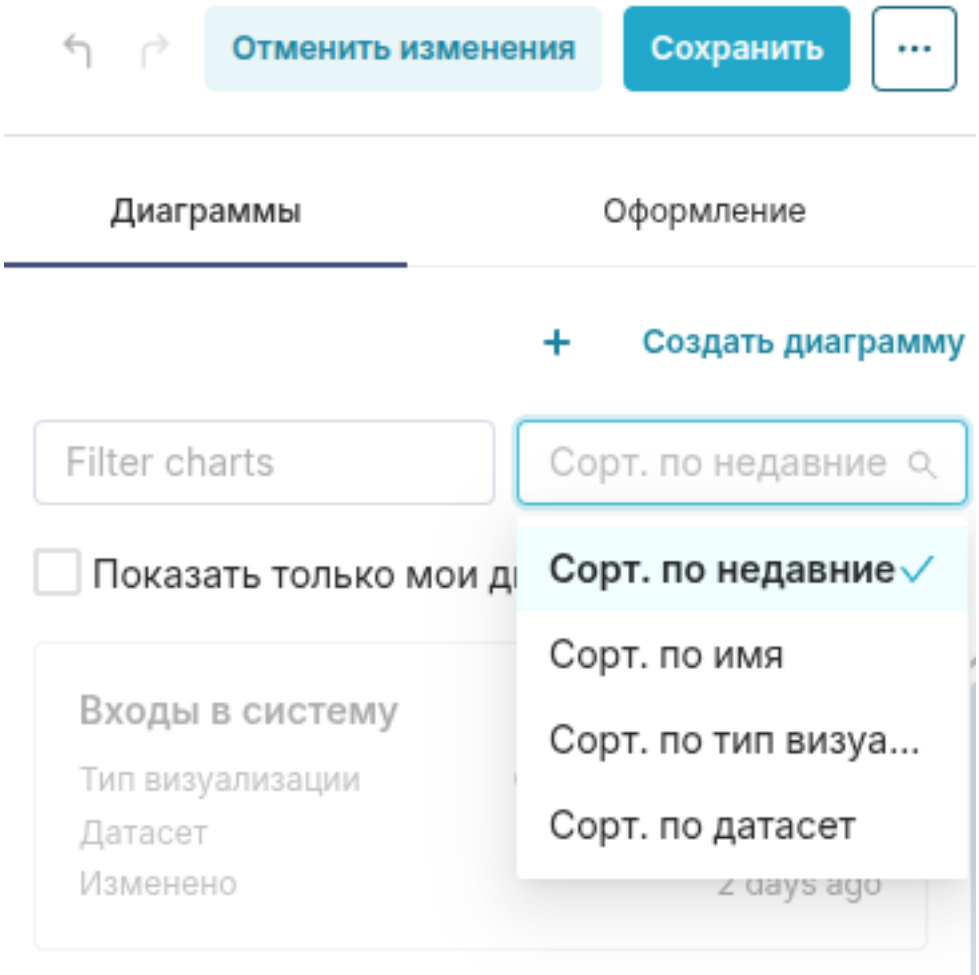
Примечание

По умолчанию будут показаны диаграммы, которые вы создали

Если хотите видеть все диаграммы, снимите отметку Показывать только мои диаграммы

Для завершения процесса необходимо нажать кнопку Сохранить

В режиме редактирования дашборда диаграммы можно сортировать по следующим критериям:



1. Недавние — по дате, когда диаграмма была изменена в последний раз
2. Имя — по названию диаграммы
3. Тип визуализации — по виду диаграммы, который определяется доступными типами в текущей версии программы
4. Датасет — по набору данных, связанному с одной или несколькими диаграммами, формируемому из доступных наборов данных

Подсказка

По умолчанию диаграммы сортируются по критерию Недавние

Просмотр дашборда

Просмотр в списочном режиме

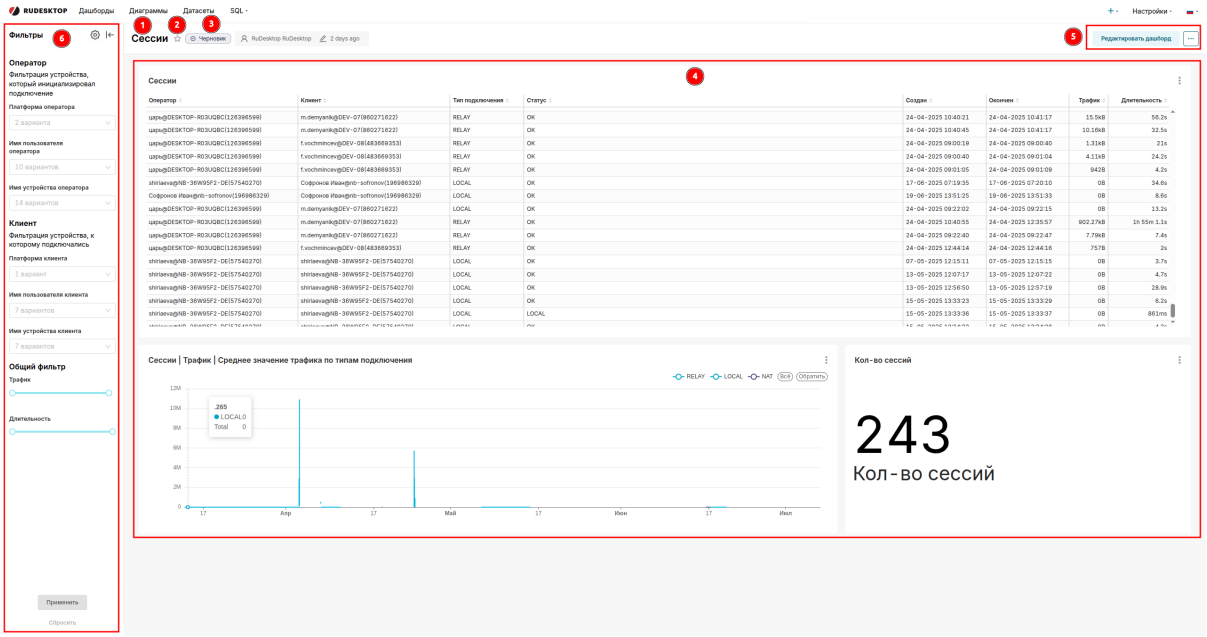
Чтобы просмотреть дашборд, нужно выбрать его название из списка, содержащего подробную информацию о дашборде

Просмотр в плиточном режиме

Чтобы просмотреть дашборд, нужно выбрать плитку, содержащую подробную информацию об этом дашборде

Структура интерфейса просмотра

Когда дашборд открывается в режиме просмотра, панель глобальных фильтров автоматически разворачивается, если такие фильтры имеются



Дашборд включает в себя следующие элементы:

1. Название дашборда
2. Информация о том, добавлен ли дашборд в список избранного
3. Статус дашборда
4. Подборка диаграмм
5. Комплект элементов оформления
6. Глобальные фильтры дашборда

Чтобы управлять панелью глобальных фильтров, используйте соответствующие иконки на панели

Для фильтрации данных, основываясь на выбранных значениях фильтров, нажмите на Применить в левом нижнем углу

Чтобы сбросить фильтры к значениям по умолчанию, воспользуйтесь кнопкой Сбросить в левом нижнем углу

Для того чтобы добавить дашборд в избранное, нажмите на кнопку

Чтобы изменить видимость дашборда, выберите текущий статус

Для доступа к интерфейсу управления глобальными фильтрами нажмите на кнопку -> Add or edit filters

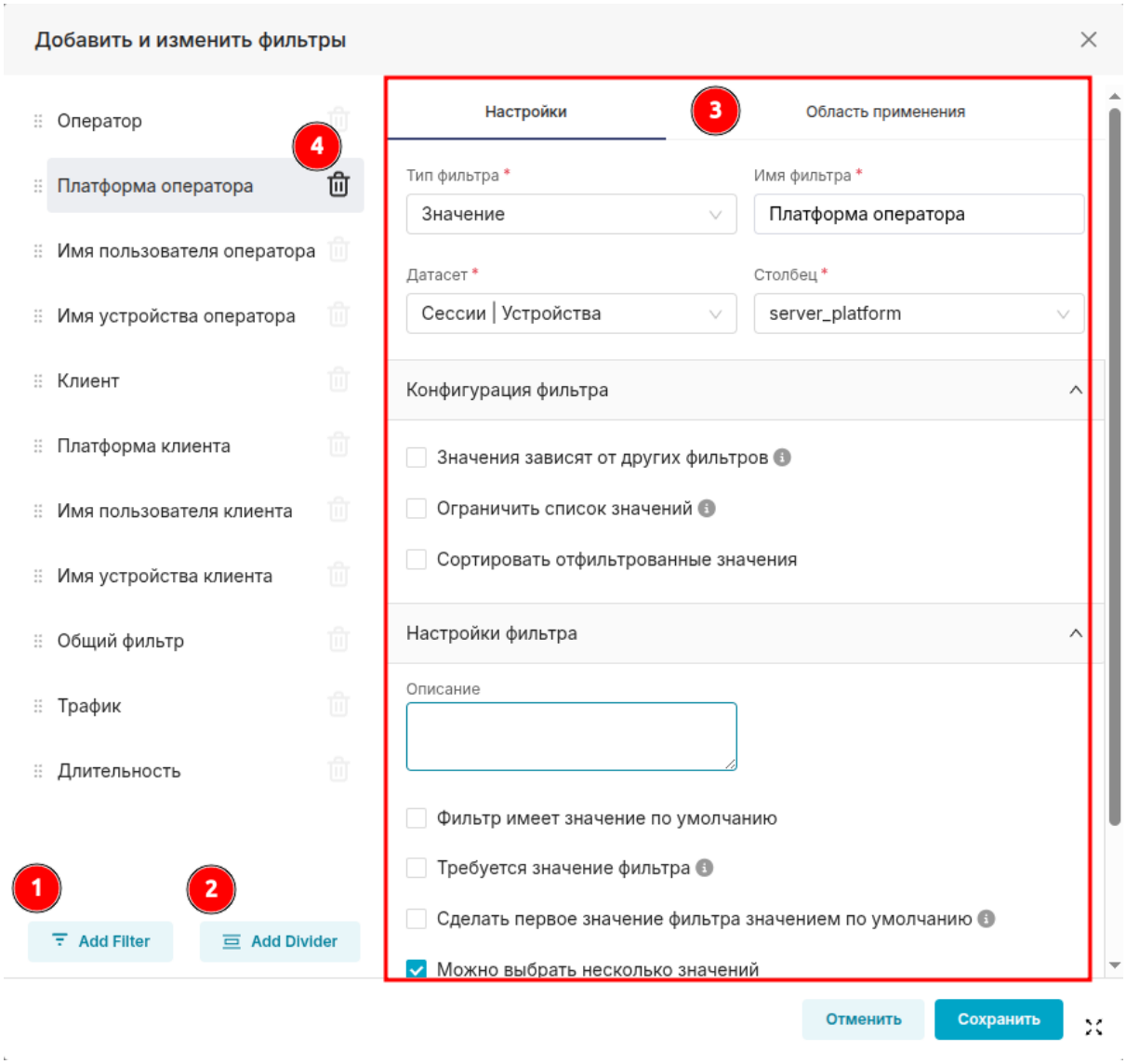
Чтобы переключиться в режим редактирования дашборда, нажмите на кнопку Редактировать дашборд

Интерфейс управления глобальными фильтрами

Глобальные фильтры позволяют осуществлять как индивидуальную фильтрацию данных, так и добавлять дополнительный уровень фильтрации

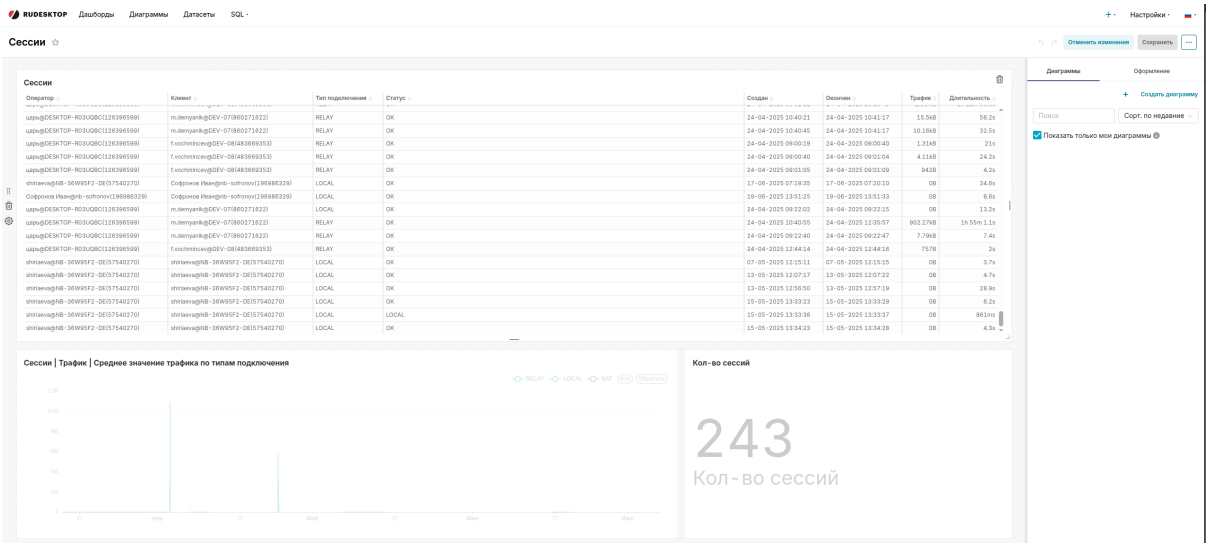
Эти фильтры можно применять ко всем диаграммам дашборда, к определённым или не использовать вовсе

Для удобства визуального восприятия фильтры можно группировать, используя разделители



1. Чтобы создать глобальный фильтр, нажмите на кнопку Add Filter
2. Для создания разделителя нажмите на кнопку Add Divider
3. Для изменения настроек объекта выберите его из списка и внесите нужные изменения
4. Чтобы удалить объект, воспользуйтесь кнопкой удаления рядом с элементом списка

Редактирование дашборда



Чтобы открыть дашборд в режиме редактирования, нужно выбрать его название из списка с подробной информацией о дашборде или из плитки, а затем нажать на кнопку Редактировать дашборд



Редактирование в списочном режиме

Чтобы изменить параметры дашборда, наведите курсор на элемент списка, содержащий подробную информацию о дашборде, и выберите действие Редактировать

Редактирование в плиточном режиме

Чтобы изменить параметры дашборда, наведите курсор на меню действий плитки, содержащей подробную информацию о дашборде, и выберите Редактировать

Структура интерфейса редактирования

Появится интерфейс настройки параметров для выбранного дашборда

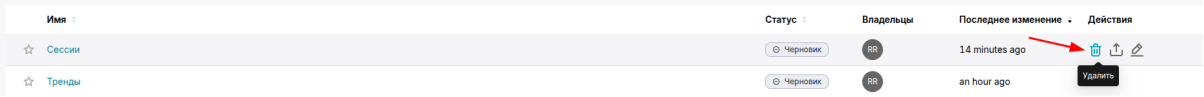
Подсказка

Чтобы сохранить изменения параметров, нажмите кнопку Сохранить в правом верхнем углу

Удаление дашборда

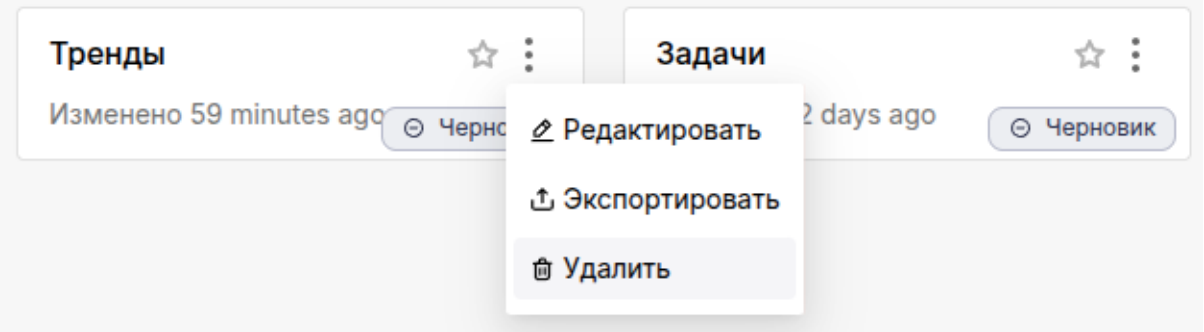
Удаление в списочном режиме

Чтобы удалить дашборд, наведите курсор на элемент списка, содержащий подробную информацию о дашборде, и выберите действие Удалить



Удаление в плиточном режиме

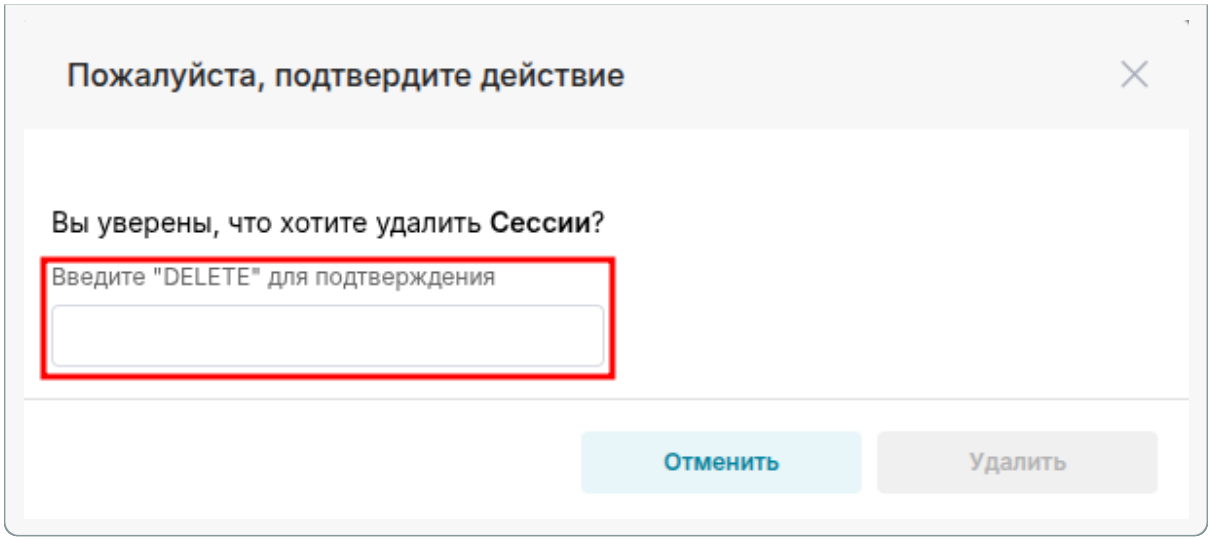
Чтобы удалить дашборд, наведите курсор на меню действий плитки с подробной информацией о дашборде и выберите опцию Удалить



Перед удалением дашборда появится предупреждающее сообщение

Подсказка

Чтобы подтвердить удаление, пользователю нужно ввести слово DELETE в соответствующее поле и затем нажать кнопку Удалить



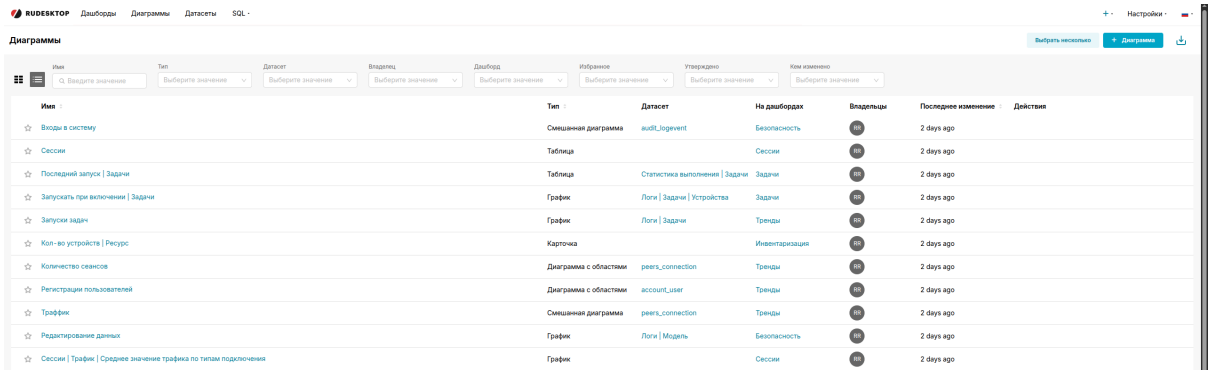
Диаграммы

Доступны только в UEM версии

Диаграммы — это отдельные визуализации (графики, таблицы, числовые показатели) Apache Superset[30], построенные на основе данных из датасетов

Примечание

Диаграммы реализованы средствами встроенного **Apache Superset**. Полное описание типов визуализаций и редактора см. в документации Superset[31]



Как это работает

Каждая диаграмма строится поверх одного *датасета* — данные диаграммы автоматически обновляются вслед за источником, и одна и та же диаграмма может включаться в разные дашборды

Поток создания диаграммы в Superset:

1. Выбрать датасет, на котором будет построена визуализация

[30] https://superset.apache.org/
[31] https://superset.apache.org/docs/using-superset/exploring-data

2. Выбрать тип диаграммы из набора, поддерживаемого Superset (линейный график, столбчатая диаграмма, таблица, число и т.д.)
3. Сконфигурировать измерения, метрики, фильтры и оформление
4. Сохранить диаграмму — она появится в общей таблице и сможет быть добавлена в *дашборды*

Диаграммы можно фильтровать, сортировать, добавлять в избранное, экспортировать и импортировать. Доступ ограничивается ролями Superset и правами на исходный датасет

Описание

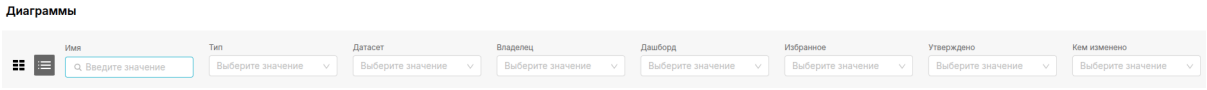
Эта страница предоставляет подробную информацию о диаграммах, включая фильтрацию и сортировку, а также функции экспорта и импорта

Примечание

Также доступны функции для создания, просмотра, редактирования и удаления диаграмм

При нажатии на имя диаграммы из списка с подробной информацией о диаграмме или из плитки с детальной информацией диаграмма откроется в режиме редактирования представления

Фильтры



Диаграммы можно отфильтровать по следующим критериям:

- Имя — идентификатор диаграммы
- Тип — тип диаграммы, варианты которого зависят от доступных в текущей версии типов
- Датасет — данные, связанные с диаграммой или несколькими диаграммами; список значений формируется из доступных наборов данных
- Владелец — автор диаграммы, список формируется из существующих пользователей
- Дашборд — дашборд, в который включены одна или несколько диаграмм; возможные варианты берутся из списка дашбордов
- Избранное — статус добавления диаграммы в избранное пользователем; варианты — `Да` или `Нет`
- Утверждено — наличие информации о пользователе или роли, утвердившей диаграмму; возможные ответы — `Да` или `Нет`
- Кем изменено — пользователь, который внес последние изменения; список значений берется из пользователей

Сортировка

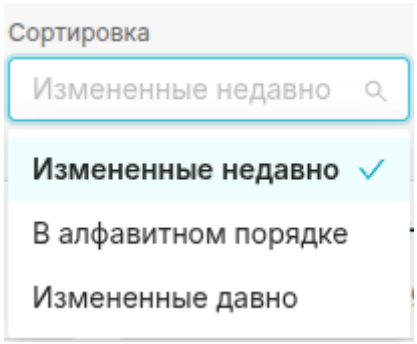
Сортировка в списочном режиме

В списочном режиме диаграммы можно отсортировать по следующим критериям:

- Имя — имя диаграммы
- Тип — вид диаграммы, варианты выбираются из доступных типов текущей версии
- Последнее изменение — дата, когда диаграмма была изменена в последний раз

> **Подсказка**
>
> По умолчанию дашборды сортируются по дате `Последнего изменения`

Сортировка в плиточном режиме



В плиточном режиме диаграммы можно отсортировать по следующим критериям:

- Измененные недавно — начиная с самых последних изменений
- В алфавитном порядке — в порядке возрастания названия диаграммы
- Измененные давно — начиная с наиболее старых изменений

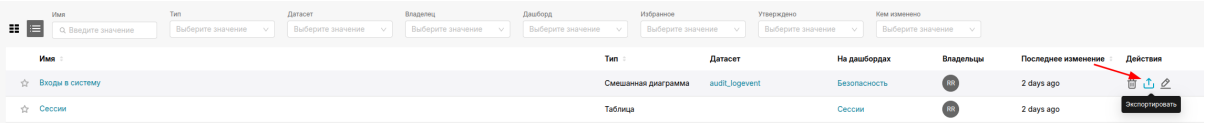
Подсказка

По умолчанию диаграммы сортируются по критерию Недавние изменения

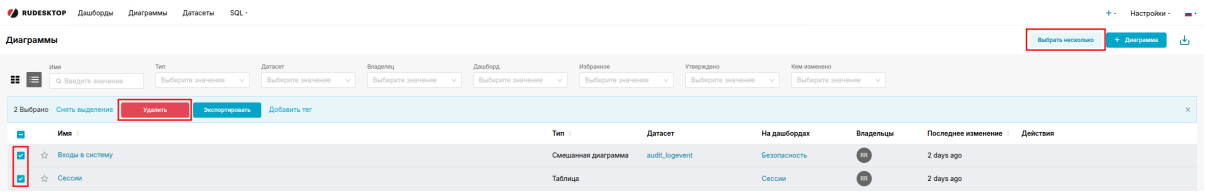
Экспорт

Экспорт в списочном режиме

Чтобы экспортировать одну диаграмму, наведите курсор на соответствующий элемент списка и выберите действие Экспортировать

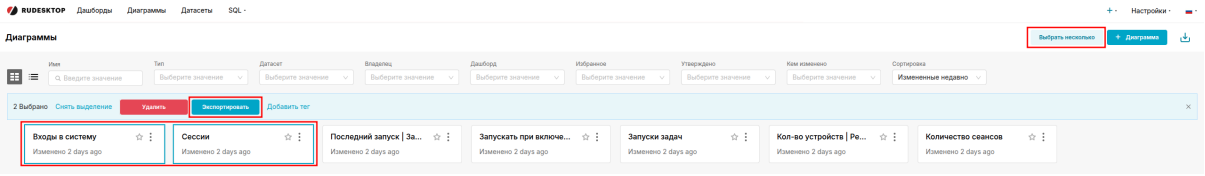


Для экспорта нескольких диаграмм нажмите на кнопку Выбрать несколько, отметьте нужные диаграммы и затем нажмите на кнопку Экспортировать

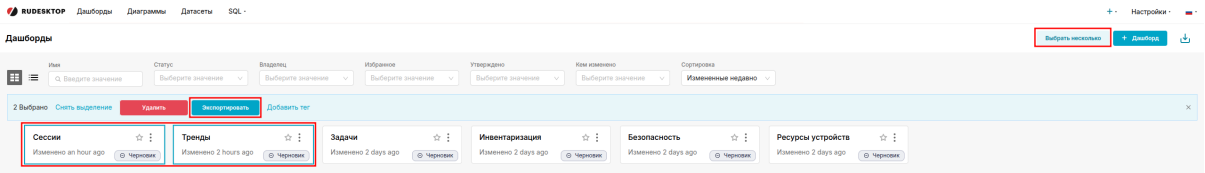


Экспорт в плиточном режиме

Чтобы экспортировать одну диаграмму, наведите курсор на , затем выберите действие Экспортировать



Для экспорта нескольких диаграмм нажмите на кнопку Выбрать несколько, выберите одну или несколько плиток, а затем нажмите на кнопку Экспортировать



Важно

В случае успешного выполнения экспорта диаграмм в папке `Загрузки` на устройстве пользователя появится архив с экспортированными диаграммами, где наименование архива будет отражать информацию о типе экспорта и дате выполнения операции

Импорт

Чтобы импортировать одну или несколько диаграмм, выполните следующие действия:

1. Нажать на кнопку в правом верхнем углу
2. В появившемся окне нажать на кнопку Выбрать файл
3. В появившемся окне найти и выбрать нужный архив с экспортированными диаграммами
4. Нажать на кнопку Открыть

Важно

- Когда вы выбираете архив, информация о нем передается в интерфейс импорта диаграмм, и кнопка Импорт становится доступной
- Чтобы удалить информацию, наведите курсор на элемент списка и выберите `Удалить файл`
- Если вы выберете другой архив, текущая информация будет заменена новой

5. Нажать на кнопку Импорт

Важно

- При импорте диаграмм система сравнивает содержимое архива с данными в базе данных. Если найдены совпадения, пользователю отображается предупреждение
- Чтобы продолжить процесс, введите слово OVERWRITE в соответствующее поле и нажмите кнопку Перезаписать

Если импорт диаграмм прошел успешно, содержимое архива будет записано в базу данных. Затем все объекты из архива будут импортированы, и пользователь будет назначен владельцем этих импортированных объектов

Создание диаграммы

Для создания диаграммы необходимо нажать на кнопку + Диаграмма в правом верхнем углу

Затем выберите датасет и тип диаграммы, после чего нажмите Создать диаграмму в правом нижнем углу

Подсказка

Для доступа к интерфейсу создания датасета выберите действие Создать датасет

Диаграмма откроется в режиме редактирования просмотра, где вы можете задать название диаграммы и указать нужные параметры для выбранного типа

Для сохранения изменений нажмите Сохранить

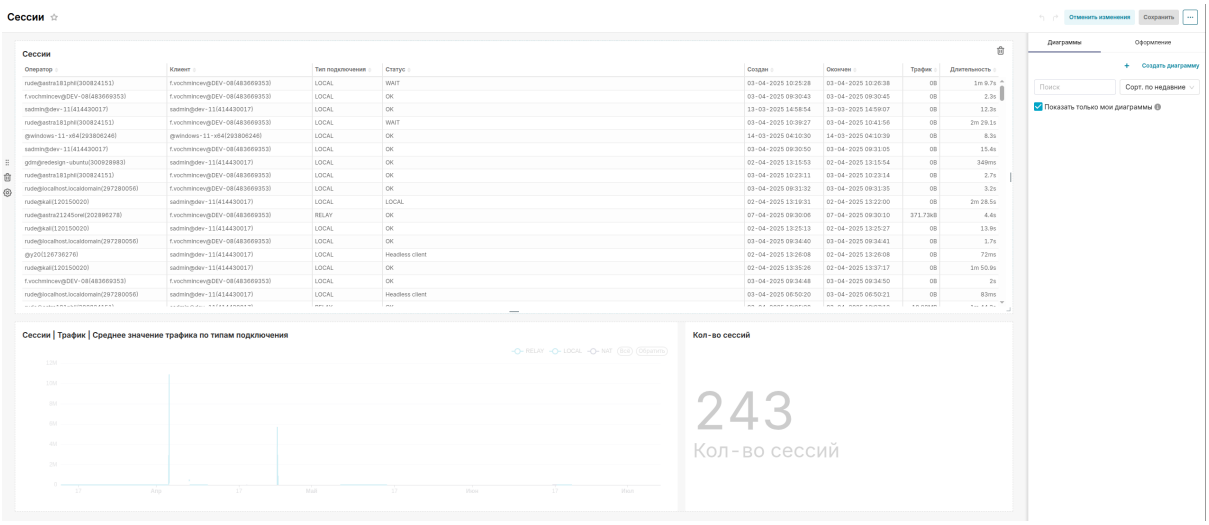
Информация о названии диаграммы передаётся в интерфейс сохранения

Важно

Если в поле Задайте имя диаграммы есть данные, кнопка Сохранить становится доступной

Чтобы разместить диаграмму в дашборде, выберите существующий дашборд

Редактирование диаграммы



Чтобы открыть диаграмму в режиме редактирования, нужно выбрать название диаграммы из списка с подробной информацией о ней или кликнуть на плитку с этой информацией

Редактирование в списочном режиме

Чтобы изменить параметры диаграммы, наведите курсор на элемент списка, содержащий подробную информацию о диаграмме, и выберите действие Редактировать

Редактирование в плиточном режиме

Чтобы изменить параметры диаграммы, наведите курсор на меню действий плитки, содержащей подробную информацию о диаграмме, и выберите Редактировать

Структура интерфейса редактирования

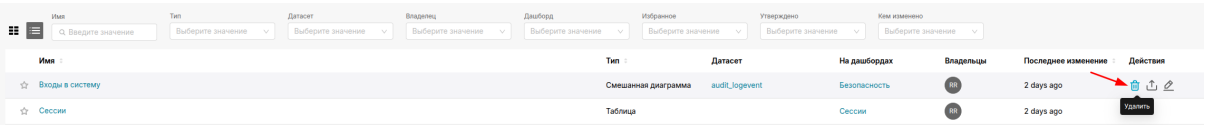
Появится интерфейс редактирования параметров для выбранной диаграммы

Чтобы сохранить значения параметров для этой диаграммы, нужно нажать кнопку Сохранить

Удаление диаграммы

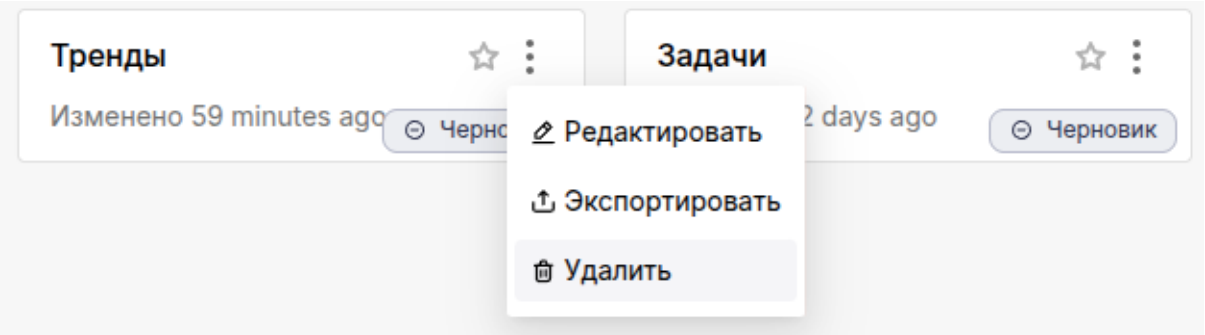
Удаление в списочном режиме

Чтобы удалить диаграмму, наведите курсор на элемент списка, содержащий подробную информацию о диаграмме, и выберите действие Удалить



Удаление в плиточном режиме

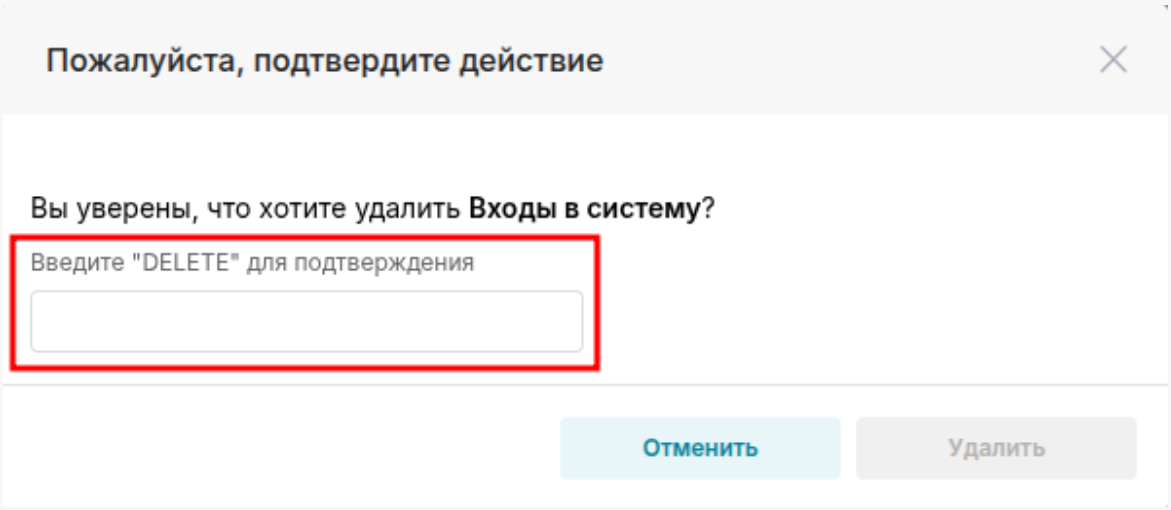
Чтобы удалить диаграмму, наведите курсор на меню действий плитки с подробной информацией о диаграмме и выберите опцию Удалить



Перед удалением диаграммы появится предупреждающее сообщение

Подсказка

Чтобы подтвердить удаление, пользователю нужно ввести слово DELETE в соответствующее поле и затем нажать кнопку Удалить



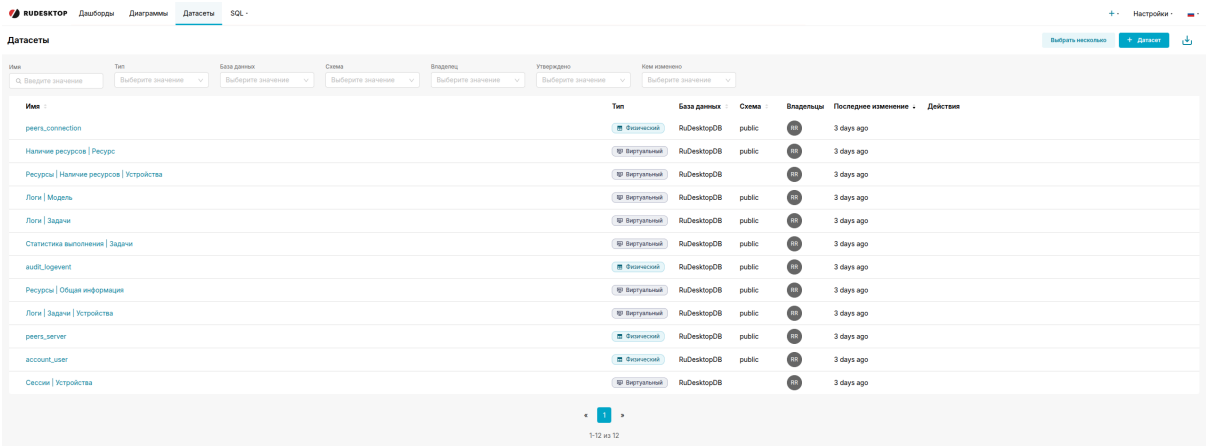
Датасеты

Доступны только в UEM версии

Датасеты — это объекты Apache Superset[32], на основе которых в **«Аналитике»** строятся диаграммы и дашборды

Примечание

Датасеты реализованы средствами встроенного **Apache Superset**. Полное описание см. в документации Superset[33]



[32] https://superset.apache.org/

[33] https://superset.apache.org/docs/using-superset/creating-your-first-dashboard#registering-a-new-table

Как это работает

Датасет — это слой Superset между подключённой *базой данных* и визуализациями. Поддерживаются два типа:

- **Физический** — соответствует таблице или представлению в исходной базе. Создаётся по существующему объекту, без модификации данных
- **Виртуальный** — задаётся произвольным SQL-запросом. Подходит, когда нужны вычисляемые столбцы, объединения нескольких таблиц или фильтрация данных до построения диаграмм

Подсказка

Если справочные данные, зашитые в SQL виртуального датасета, приходится регулярно обновлять, вынесите их в отдельную таблицу базы — внешняя система сможет обновлять её через REST API модуля аналитики без правки SQL. См. *Интеграцию с модулем аналитики*

Например, на дашборде **«Ресурсы устройств»** можно посмотреть, сколько места занято на дисках и сколько видеопамяти у устройств. Эти сведения собраны в датасете **«Ресурсы | Общая информация»**

Поверх любого датасета в Superset можно описать **рассчитываемые столбцы** и **метрики** — они становятся доступны во всех *диаграммах*, использующих датасет

Доступ к датасету определяется владельцем и ролями Superset. Поскольку диаграммы и дашборды строятся над датасетами, ограничение доступа на уровне датасета автоматически распространяется на связанные визуализации

Описание

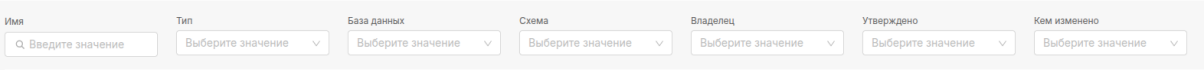
Эта страница предоставляет подробную информацию о датасетах, включая фильтрацию и сортировку, а также функции экспорта и импорта

Примечание

Также доступны функции для создания, просмотра, редактирования и удаления датасетов

При нажатии на имя датасета из списка с подробной информацией о датасете или из плитки с детальной информацией датасет откроется в режиме просмотра

Фильтры



Датасеты можно отфильтровать по следующим критериям:

- Имя — название датасета
- Тип — вид датасета, может быть `Виртуальный` или `Физический`
- База данных — система, связанная с одним или несколькими датасетами, варианты определяются существующими базами данных
- Схема — структура базы данных, связанная с датасетами, варианты зависят от доступных схем баз данных
- Владелец — автор датасета, варианты формируются из списка пользователей
- Утверждено — отображает наличие одобрения пользователем или группой, варианты — `Да` или `Нет`
- Кем изменено — пользователь, который вносил последние изменения, варианты выбираются из списка пользователей

Сортировка

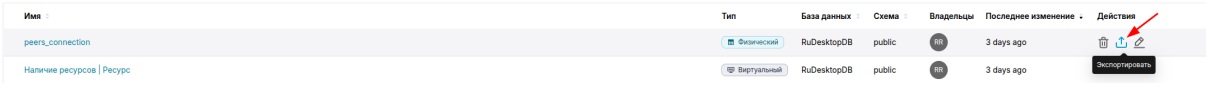
Датасеты можно отсортировать по следующим критериям:

- Имя — название датасета
- База данных — система, к которой привязаны один или несколько датасетов, варианты определяются существующими базами данных
- Схема — структура базы данных, связанная с одним или несколькими датасетами, возможные значения определяются доступными схемами
- Последнее изменение — дата, когда датасет редактировался в последний раз

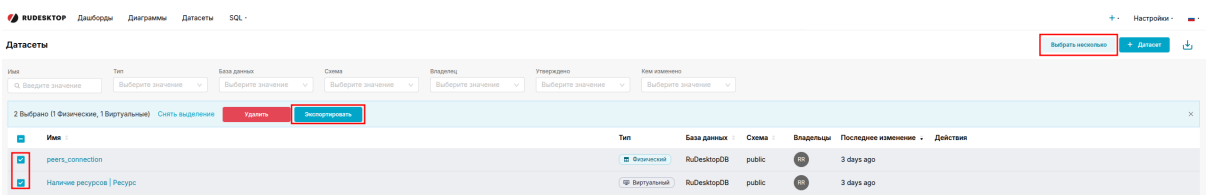
> **Подсказка**
>
> По умолчанию датасеты сортируются по дате `Последнего изменения`

Экспорт

Чтобы экспортировать один датасет, наведите курсор на соответствующий элемент списка и выберите действие Экспортировать



Для экспорта нескольких датасетов нажмите на кнопку Выбрать несколько, отметьте нужные датасеты и затем нажмите на кнопку Экспортировать



Важно

В случае успешного выполнения экспорта датасетов в папке `Загрузки` на устройстве пользователя появится архив с экспортированными датасетами, где наименование архива будет отражать информацию о типе экспорта и дате выполнения операции

Импорт

Чтобы импортировать один или несколько датасетов, выполните следующие действия:

1. Нажать на кнопку в правом верхнем углу
2. В появившемся окне нажать на кнопку Выбрать файл
3. В появившемся окне найти и выбрать нужный архив с экспортированными датасетами
4. Нажать на кнопку Открыть

Важно

- Когда вы выбираете архив, информация о нем передается в интерфейс импорта датасетов, и кнопка Импорт становится доступной
- Чтобы удалить информацию, наведите курсор на элемент списка и выберите `Удалить файл`
- Если вы выберете другой архив, текущая информация будет заменена новой

5. Нажать на кнопку Импорт

Важно

- При импорте датасетов система сравнивает содержимое архива с данными в базе данных. Если найдены совпадения, пользователю отображается предупреждение
- Чтобы продолжить процесс, введите слово OVERWRITE в соответствующее поле и нажмите кнопку Перезаписать

Если импорт датасетов прошел успешно, содержимое архива будет записано в базу данных. Затем все объекты из архива будут импортированы, и пользователь будет назначен владельцем этих импортированных объектов

Создание датасета

Для создания датасета необходимо нажать на кнопку + Датасет в правом верхнем углу

Затем выбрать базу данных, схему и таблицу

После этого следует нажать на кнопку Создать датасет и диаграмму

По завершении этой операции откроется интерфейс для создания диаграммы с выбранным датасетом

Редактирование датасета

Чтобы изменить параметры датасета, наведите курсор на элемент списка, содержащий подробную информацию о датасете, и выберите действие Редактировать

Откроется интерфейс для редактирования параметров выбранного датасета

Структура датасета включает в себя следующие элементы:

- Наименование набора данных
- Источник данных — это может быть физическая таблица или представление в базе данных или пользовательский SQL-запрос
- Набор мер
- Набор столбцов
- Набор вычисляемых столбцов
- Настройки датасета

Чтобы создать меру, перейдите на вкладку Меры и нажмите кнопку Добавить запись

Для редактирования меры выберите вкладку Меры, раскройте панель параметров для нужной меры и измените необходимые параметры

Чтобы удалить меру, перейдите на вкладку Меры и нажмите на значок удаления у соответствующей меры

Для синхронизации набора столбцов с полями источника данных перейдите на вкладку Столбцы и нажмите кнопку Синхронизировать из источника

Чтобы изменить столбец, выберите вкладку Столбцы, раскройте панель параметров для нужного столбца и измените необходимые параметры

Чтобы удалить столбец, выберите вкладку Столбцы и нажмите на значок удаления у соответствующего столбца

Чтобы создать вычисляемый столбец, выберите вкладку Вычисляемые столбцы и нажмите кнопку Добавить запись

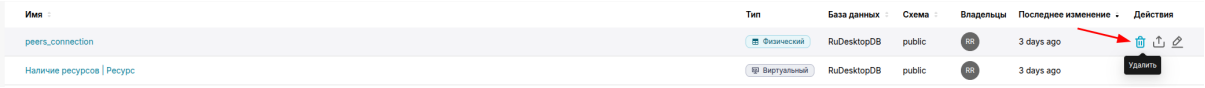
Для изменения вычисляемого столбца перейдите на вкладку Вычисляемые столбцы, раскройте панель параметров для нужного столбца и измените необходимые параметры

Чтобы удалить вычисляемый столбец, выберите вкладку Вычисляемые столбцы и нажмите на значок удаления у соответствующего столбца

Для сохранения изменений в параметрах датасета нажмите кнопку Сохранить

Удаление датасета

Чтобы удалить датасет, наведите курсор на элемент списка, содержащий подробную информацию о датасете, и выберите действие Удалить



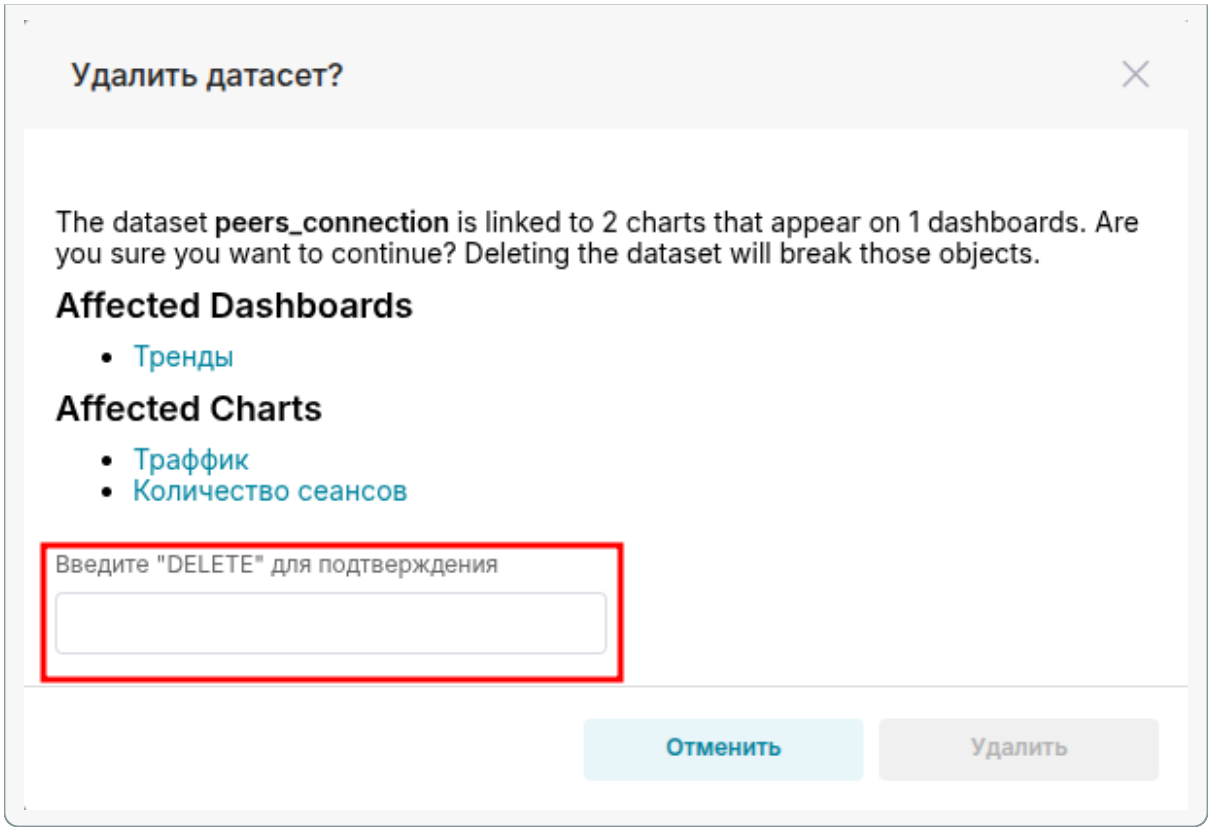
Важно

Перед удалением датасета выполняется проверка на наличие связанных объектов

Перед удалением датасета появится предупреждающее сообщение

Подсказка

Чтобы подтвердить удаление, пользователю нужно ввести слово DELETE в соответствующее поле и затем нажать кнопку Удалить



Базы данных

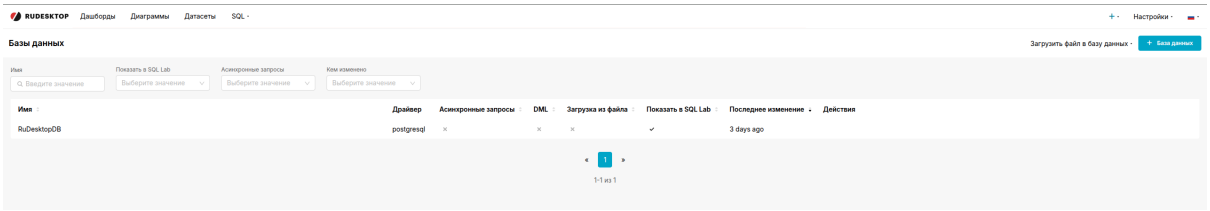
Доступны только в UEM версии

Базы данных — это подключения Apache Superset[34] к источникам данных, к которым обращаются датасеты, диаграммы и дашборды в **«Аналитике»**

[34] https://superset.apache.org/

Примечание

Подключения настраиваются и хранятся в встроенном **Apache Superset**. Полный список поддерживаемых источников и параметров см. в документации Superset[35]



Как это работает

По умолчанию в Superset уже подключена база данных самого сервера **RuDesktop** — это позволяет строить аналитические отчёты по уже накопленным в системе данным (устройствам, сессиям, пользователям, инвентаризации и т.д.) без дополнительной настройки

При необходимости можно подключить дополнительные базы средствами Superset. Параметры подключения определяют, какие возможности будут доступны при работе с этой базой:

- **Показать в SQL Lab** — позволяет выполнять произвольные запросы к базе через редактор SQL Lab Superset
- **Асинхронные запросы** — длительные запросы выполняются в фоне без блокировки интерфейса
- **DML** — разрешает выполнение модифицирующих запросов (INSERT/UPDATE/DELETE), а не только чтение
- **Загрузка из файла** — позволяет импортировать данные из файла напрямую в базу

После подключения база становится источником для *датасетов*, на которых строятся *диаграммы* и *дашборды*

Важно

Изменения параметров подключения и удаление базы влияют на все зависящие от неё датасеты, диаграммы и дашборды

Описание

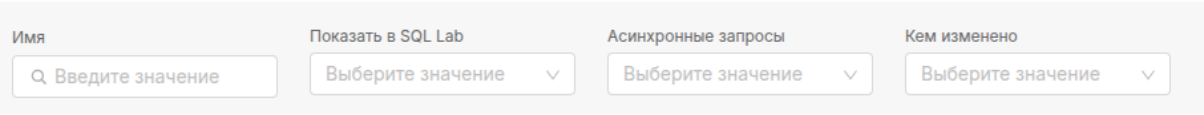
Эта страница предоставляет подробную информацию о базах данных, включая фильтрацию и сортировку

[35] https://superset.apache.org/docs/configuration/databases

Примечание

Также доступны функции для создания, просмотра, редактирования и удаления баз данных

Фильтры



Базы данных можно отфильтровать по следующим критериям:

- Имя — наименование, отображаемое для базы данных
- Показать в SQL Lab — указывает на то, доступна ли база данных в функции `Редактор SQL`, варианты — `Да` или `Нет`
- Асинхронные запросы — показывает, поддерживает ли база данных возможность «Асинхронное выполнение запросов», варианты — `Да` или `Нет`
- Кем изменено — имя пользователя, который в последний раз вносил изменения в базу данных. Возможные значения формируются из списка пользователей

Сортировка

Базы данных можно отсортировать по следующим критериям:

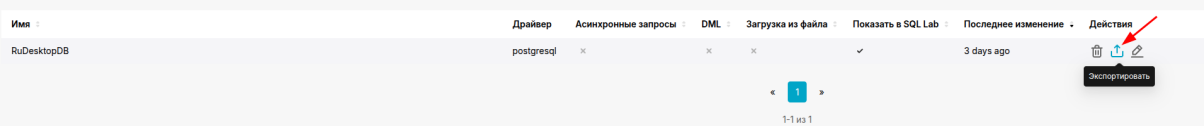
- Имя — наименование, отображаемое для базы данных
- Асинхронные запросы — показывает, поддерживается ли возможность «Асинхронное выполнение запросов», варианты — `Да` или `Нет`
- DML — указывает, разрешена ли функция `Разрешить DML`, варианты — `Да` или `Нет`
- Загрузка из файла — отражает, доступна ли функция `Разрешить загрузку файлов в базу данных`, варианты — `Да` или `Нет`
- Показать в SQL Lab — обозначает, присутствует ли база данных в функции `Редактор SQL`, варианты — `Да` или `Нет`
- Последнее изменение — дата, когда база данных была изменена в последний раз

Подсказка

По умолчанию базы данных сортируются по дате Последнего изменения

Экспорт

Чтобы экспортировать одну базу данных, наведите курсор на соответствующий элемент списка и выберите действие Экспортировать



Важно

В случае успешного выполнения экспорта баз данных в папке Загрузки на устройстве пользователя появится архив с экспортированными базами данных, где наименование архива будет отражать информацию о типе экспорта и дате выполнения операции

Импорт

Чтобы импортировать базу данных, нажмите на кнопку + База данных, затем выберите опцию Импортировать базу данных из файла

После этого выберите архив с экспортированной базой данных и нажмите Открыть

Данные о выбранном архиве будут переданы в интерфейс импорта базы данных

Важно

- При импорте базы данных система сравнивает содержимое архива с данными в базе данных. Если найдены совпадения, пользователю отображается предупреждение
- Чтобы продолжить операцию, необходимо ввести слово OVERWRITE в соответствующее поле и нажать кнопку Подключить

Если импорт базы данных прошел успешно, содержимое архива будет записано в базу данных. Затем все объекты из архива будут импортированы, и пользователь будет назначен владельцем этих импортированных объектов

Создание баз данных

Чтобы создать базу данных, нажмите кнопку + База данных, затем выберите плитку или элемент списка с названием базы данных

После этого задайте отображаемое имя базы данных и укажите необходимые параметры для выбранной базы данных

Для начала операции нажмите кнопку Подключить

После завершения операции будет открыт интерфейс для настройки дополнительных параметров выбранной базы данных

Интерфейс содержит такие разделы:

- Лаборатория SQL — позволяет управлять доступом к функции «Редактор SQL» и задавать разрешения, связанные с её использованием
- Производительность — позволяет настроить время жизни кэша компонентов и управлять доступом к функциям «Асинхронное выполнение запросов» и «Отмена запроса при закрытии вкладки»
- Безопасность — позволяет задать строку подключения с дополнительными параметрами, корневой сертификат, а также управлять доступностью функции «Имперсонировать пользователя»
- Прочее — включает настройки метаданных, параметры драйвера и версию базы данных

Чтобы сохранить изменения дополнительных параметров для выбранной базы данных, необходимо нажать кнопку Завершить

Чтобы создать базу данных с помощью функции `SQLAlchemy`, нужно на втором шаге выбрать действие Подключиться к этой базе через SQLAlchemy URI

Затем следует ввести отображаемое имя базы данных и указать строку подключения для функции `SQLAlchemy`, после чего нажать кнопку Подключить

В разделе Продвинутая настройка можно задать дополнительные параметры для выбранной базы данных

Интерфейс для создания базы данных может варьироваться в зависимости от типа выбранной базы данных

Редактирование баз данных

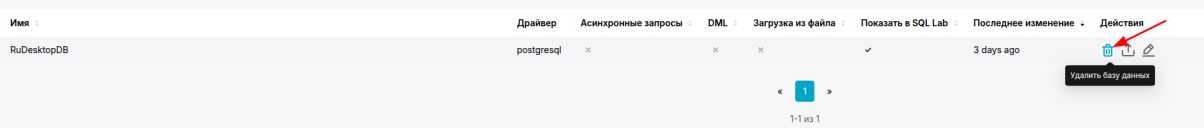
Чтобы изменить параметры базы данных, наведите курсор на элемент списка, содержащий подробную информацию о базе данных, и выберите действие Редактировать

Откроется интерфейс для редактирования параметров выбранной базы данных

Чтобы сохранить изменения параметров, необходимо нажать кнопку Завершить

Удаление баз данных

Чтобы удалить базу данных, наведите курсор на элемент списка, содержащий подробную информацию о базе данных, и выберите действие Удалить базу данных



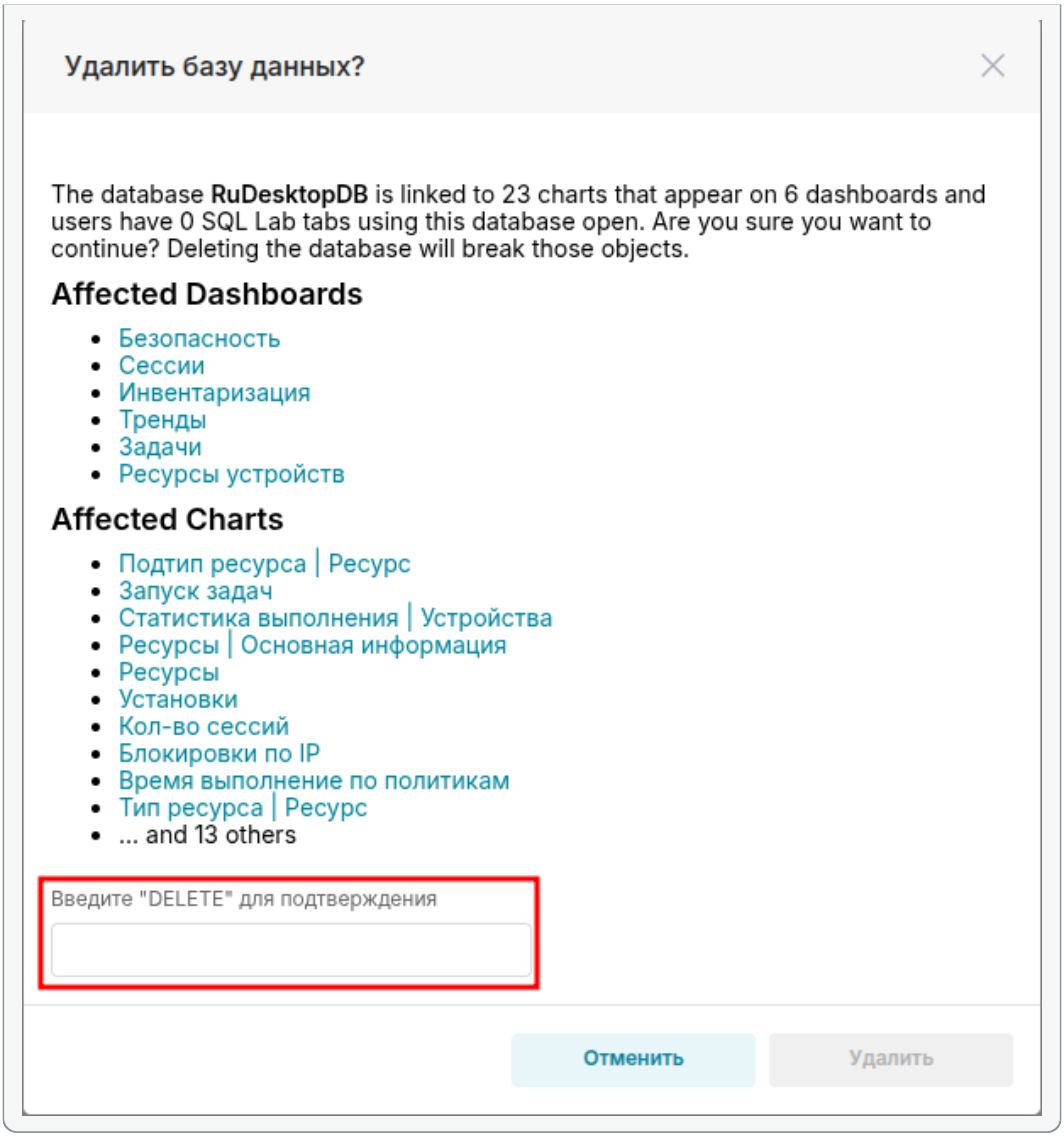
Важно

Перед удалением базы данных выполняется проверка на наличие связанных объектов

Перед удалением базы данных появится предупреждающее сообщение

Подсказка

Чтобы подтвердить удаление, пользователю нужно ввести слово DELETE в соответствующее поле и затем нажать кнопку Удалить



Аналитика — это раздел, в который встроен сторонний BI-сервис Apache Superset[36] для визуализации данных сервера **RuDesktop**

Подсказка

Раздел **«Аналитика»** доступен только при использовании локального сервера **Управление конфигурациями (UEM)**

Важно

Раздел работает на отдельном внешнем сервисе **Apache Superset**, который разворачивается рядом с сервером **RuDesktop**. Внутри **RuDesktop** интерфейс Superset открывается через единый вход (SSO) и оформлен в стиле системы, но все данные, объекты и операции хранятся и выполняются на стороне Superset, а не на сервере **RuDesktop**

[36] https://superset.apache.org/

Как это работает

Под единым интерфейсом раздела **«Аналитика»** работает интегрированный экземпляр **Apache Superset**. **RuDesktop** прокидывает в него учётную запись пользователя, его роль и адрес сервера, а сам Superset:

- хранит подключения к источникам данных (**Базы данных**)
- описывает наборы данных поверх таблиц и SQL-запросов (**Датасеты**)
- строит на них визуализации (**Диаграммы**) и собирает их в **Дашборды**

По умолчанию в Superset уже подключена база данных сервера **RuDesktop** — это позволяет сразу анализировать накопленные данные (устройства, сессии, пользователи, инвентаризация и т.д.) без дополнительной настройки

Доступ к объектам определяет сам Superset на основании ролей — права влияют как на видимость элементов интерфейса, так и на доступные действия с дашбордами, диаграммами, датасетами и базами данных. Дополнительно ограничения можно задавать **на уровне отдельных датасетов** — это автоматически ограничивает доступ к диаграммам и дашбордам, построенным на этих датасетах

Подсказка

Полное описание возможностей и интерфейса Superset смотрите в его официальной документации: https://superset.apache.org/docs/intro

Главная

Стартовая страница аналитики со ссылками на доступные объекты

Доступ и аутентификация

Вход через SSO RuDesktop, автоматическая регистрация, роли и группы

Дашборды

Рабочие пространства из набора диаграмм с общими фильтрами

Диаграммы

Визуализации данных из датасетов

Датасеты

Наборы данных для построения диаграмм и дашбордов

Базы данных

Подключения к источникам данных

2.14.2 Шаблоны

Доступны только в UEM версии

Шаблоны — на данной странице отображаются шаблоны отчетов для формирования отчетов

Подсказка

Страница **«Шаблоны»** доступна при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

Шаблон описывает структуру и оформление отчёта: какие поля выводить, в каком порядке, с какой группировкой и форматированием. Сам по себе шаблон не содержит данных — данные подставляются при построении отчёта по конкретным устройствам или группам

В **RuDesktop** используется встроенный визуальный редактор ReportBro[37], в котором шаблон можно собрать без программирования

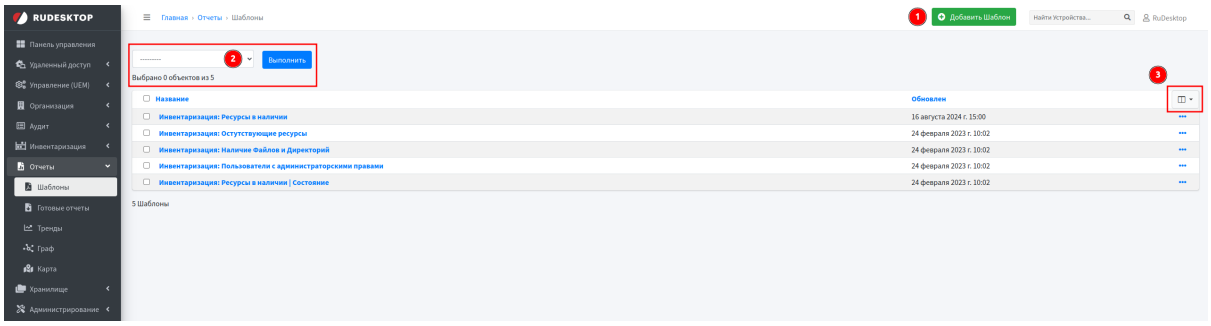
Готовые шаблоны можно использовать в трёх сценариях:

- **построение по запросу** — выбрать в таблице действие `Построить отчет в PDF` или `Построить отчет в XLSX` и указать набор устройств или групп
- **по расписанию** — через *задачу*, в которой выбран шаблон и периодичность запуска
- **с уведомлением** — связать шаблон с правилом *Уведомления*, чтобы готовый отчёт автоматически рассылался выбранным пользователям

Сформированные файлы появляются в разделе *Готовые отчеты*

Описание страницы

На странице **«Шаблоны»** отображено:



1. Кнопка Добавить шаблон
2. Массовые действия
3. Таблица с возможностью настройки отображаемых столбцов

[37] https://www.reportbro.com/doc/userguide

Добавление шаблона

При нажатии на кнопку Добавить шаблон откроется страница добавления шаблона

Встроенным редактором отчетов является ReportBro[38]

Массовые действия

Доступные действия:

1. Удалить выбранные шаблоны — удаляет выбранные шаблоны из таблицы

> **Важно**
>
> В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление шаблонов

Для массового удаления шаблонов необходимо:

1. Отметить необходимые шаблоны в таблице
2. Выбрать действие Удалить выбранные шаблоны
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие шаблоны будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные шаблоны будут удалены

Таблица

Таблица разбита по столбцам:

1. `Название` — название шаблона
2. `Обновлен` — дата и время последнего изменения шаблона

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

[38] https://www.reportbro.com/doc/userguide

1. Редактировать — при выборе этого пункта откроется редактор отчетов для редактирования выбранного шаблона
2. Удалить — при выборе данного пункта шаблон будет удален
3. История изменений — при выборе этого пункта будет отображена история изменений шаблона
4. Построить отчет в PDF — при выборе этого пункта будет открыт мастер построения отчета
5. Построить отчет в XLSX — при выборе этого пункта будет открыт мастер построения отчета

Предустановленные шаблоны

По умолчанию в системе присутствуют предустановленные шаблоны для построения отчетов:

1. **«Инвентаризация: Ресурсы в наличии»** — отображает все существующие на данный момент ресурсы устройств
2. **«Инвентаризация: Отсутствующие ресурсы»** — отображает ресурсы, которые не были обнаружены при очередной инвентаризации
3. **«Инвентаризация: Наличие Файлов и Директорий»** — отображает наличие файлов и директорий на устройствах при соответствующей настройке политики «Инвентаризация»
4. **«Инвентаризация: Пользователи с администраторскими правами»** — отображает имена пользователей с правами администратора на устройствах
5. **«Инвентаризация: Ресурсы в наличии | Состояние»** — отображает все существующие на данный момент ресурсы устройств и их состояние
6. **«Инвентаризация: ПО | Количество устройств»** — отображает список установленного ПО с количеством устройств, на которых оно обнаружено
7. **«Инвентаризация: Оборудование | Количество устройств»** — отображает список единиц оборудования с количеством устройств, на которых оно обнаружено
8. **«Удаленный доступ: Устройства»** — отображает информацию по SN, ФИО, мониторам, SN мониторов и дате последней активности устройств
9. **«Инвентаризация: История устройств»** — отображает историю устройств за все время по наличию и отсутствию
10. **«Удаленный доступ: Устройства - Оборудование»** — отображает информацию по SN, процессору, мат.плате, ОЗУ, объему ОЗУ, дискам, видеоадаптерам, сетевым адаптерам, мониторам и IP адресам

Построение отчетов

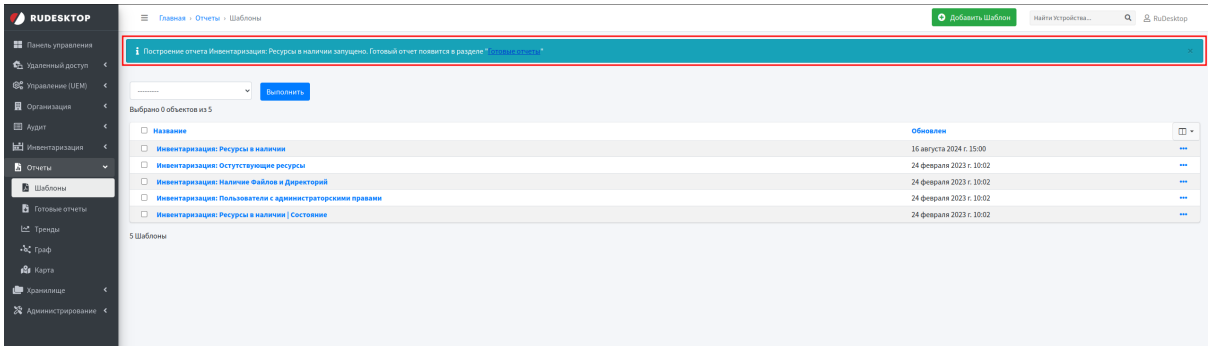
Для формирования отчета в нужном формате необходимо:

1. Нажать на кнопку с правого края таблицы и выбрать пункт `Построить отчет в PDF` или `Построить отчет в XLSX`

> **Подсказка**
>
> Содержание отчетов остается неизменным, независимо от того, выбран ли формат PDF или XLSX

2. На открывшейся странице в колонках `Устройства для которых создается отчет` или `Группы` выбрать устройства или группы, для которых будет сформирован отчет
3. После выбора устройств или группы необходимо нажать кнопку Построить отчет в PDF или Построить отчет в XLSX в зависимости от вашего выбора

После запуска формирования отчета произойдет автоматический переход на страницу **«Шаблоны»**, где вверху будет отображаться уведомление о начале построения отчета



После построения отчета его можно будет загрузить на странице *Готовые отчеты*

2.14.3 Готовые отчеты

Доступны только в UEM версии

Готовые отчеты — на данной странице отображаются сформированные отчеты после их построения на странице **«Шаблоны»**

Подсказка

Страница **«Готовые отчеты»** доступна при использовании локального сервера **Управление конфигурациями (UEM)**

Как это работает

Запись на странице **«Готовые отчеты»** появляется автоматически после запуска построения отчёта со страницы *Шаблоны*. Сервер выполняет построение в фоновом режиме, и до завершения генерации отчёт виден в списке со статусом «формируется»

Когда файл готов, его можно скачать прямо из таблицы — сам файл хранится в специальном системном репозитории отчётов и не доступен для редактирования. На странице свойств можно изменить только пользовательское имя файла

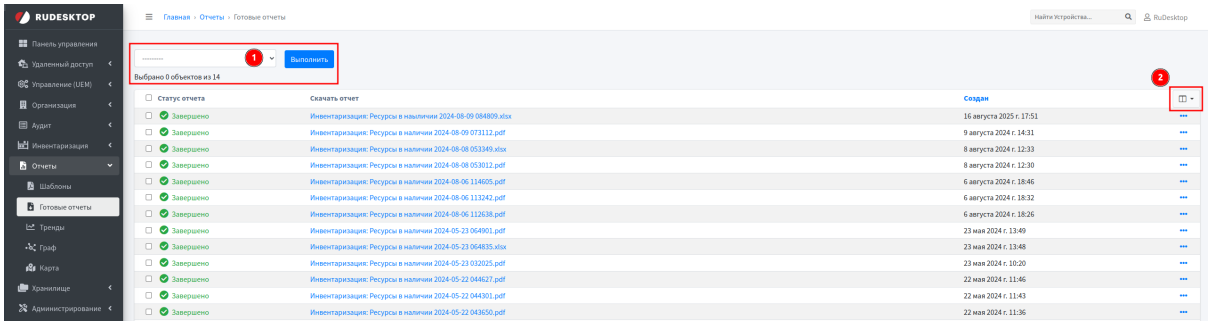
Из этого же раздела отчёт можно отправить заинтересованным пользователям через *Уведомления* — при настройке уведомления типа **«Отчеты»** ссылка на готовый отчёт автоматически попадёт в канал доставки (Email, Telegram, MAX)

Важно

Загружать или создавать готовые отчёты вручную нельзя — они формируются только сервером по шаблонам

Описание страницы

На странице **«Готовые отчеты»** отображено:



1. Массовые действия
2. Таблица с возможностью настройки отображаемых столбцов

Массовые действия

Доступные действия:

1. Удалить выбранные отчеты — удаляет выбранные отчеты из таблицы

Важно

В зависимости от прав действия могут отсутствовать

Для выполнения действия необходимо нажать на кнопку Выполнить

Удаление отчетов

Для массового удаления отчетов необходимо:

1. Отметить необходимые отчеты в таблице
2. Выбрать действие Удалить выбранные отчеты
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие отчеты будут удалены
5. Нажать на кнопку Да, я уверен

   Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору
6. Выбранные отчеты будут удалены

Таблица

Таблица разбита по столбцам:

1. `Статус отчета` — статус выполнения формирования отчета
2. `Скачать отчет` — ссылка для скачивания отчета

   Подсказка

   Для скачивания отчета нужно нажать на имя отчета
3. `Создан` — дата и время создания отчета

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — при выборе данного пункта откроются свойства отчета
2. `Удалить` — при выборе данного пункта отчет будет удален
3. `История изменений` — при выборе этого пункта будет отображена история изменений отчета

Свойства отчетов

Редактирование

При нажатии на кнопку `Редактировать` откроется страница свойств

1. Поле Репозиторий — репозиторий, в котором находится файл отчета
2. Поле GUID — уникальный идентификатор отчета
3. Поле Создан — дата и время создания отчета
4. Поле Файл — полный путь до директории отчета на машине с сервером RuDesktop
5. Поле Оригинальное имя файла — имя файла отчета
6. Поле Контрольная сумма SHA1 — контрольная сумма файла отчета

Примечание

Разрешено редактировать только поле Оригинальное имя файла

Меню действий

Меню действий расположено на всех вкладках страницы свойств



Имеет следующие возможности:

1. Сохранить - производит сохранение внесенных изменений и перенаправляет на страницу **«Готовые отчеты»**
2. Сохранить и продолжить - производит сохранение внесенных изменений и позволяет остаться на странице свойств для выполнения дальнейших операций
3. Удалить - производит удаление отчета и перенаправляет на страницу **«Готовые отчеты»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления отчета
2. После подтверждения удаления отчета произойдет переход на страницу **«Готовые отчеты»** и появится уведомление Отчет был успешно удален

4. История изменений - отображает все изменения, выполненные для этого отчета

2.14.4 Тренды

Доступны в УД и UEM версиях

Тренды — это страница, на которой отображается статистика по определённым показателям

Подсказка

Страница **«Тренды»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Как это работает

Страница строит сводные графики по данным сервера за выбранный период. Все графики обновляются автоматически при изменении периода или уровня детализации; кнопка Применить нужна только для применения фильтров сессий

Источники данных по графикам:

- **Установки** — информация о подключениях клиентов из таблицы *Устройства*
- **Регистрации** — учётные записи из таблицы *Пользователи*
- **Количество сеансов**, **Максимум одновременных сессий**, **Длительность сеансов**, **Трафик моста**, **Трафик моста (по типам подключений)** — данные из таблицы *Сессии*
- **Трафик выдачи файлов (по серверам)**, **Трафик выдачи файлов (по типам)** — события **«Выдача файла»** и **«Раздача при установке ОС»** из журнала *Все логи*

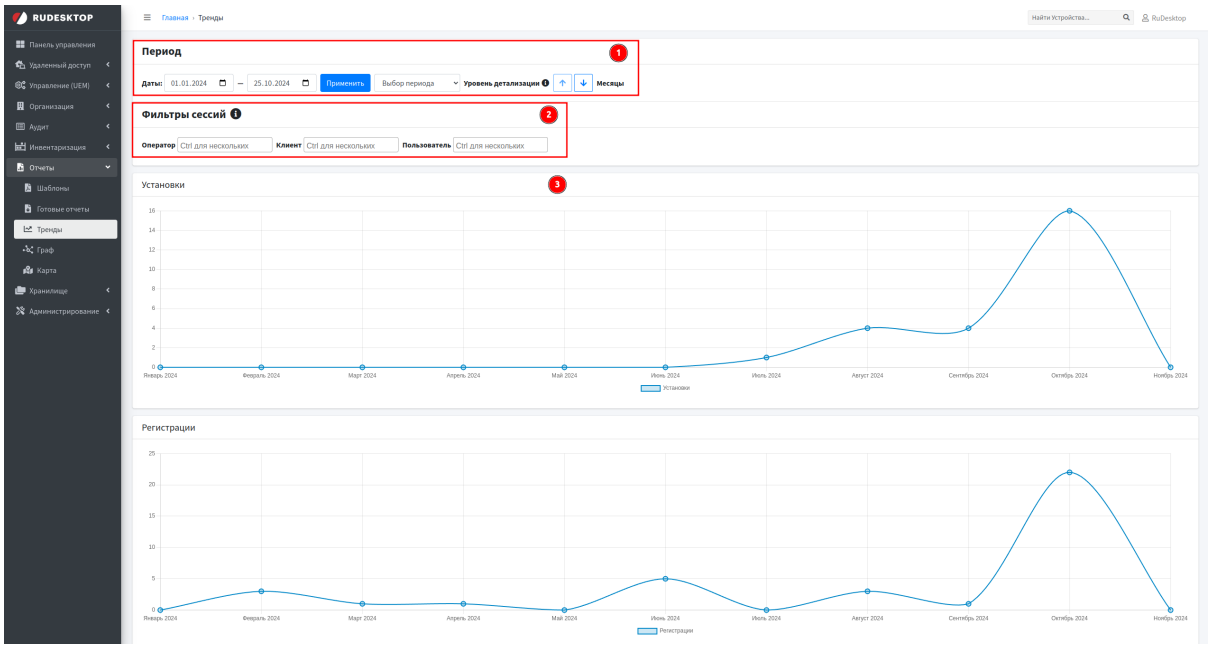
На графиках кликабельные маркеры — переход по маркеру открывает соответствующую страницу с предустановленным фильтром по выбранному периоду и значениям

Важно

Доступ к странице регулируется правом Может просматривать статистику. Без права страница недоступна

Описание страницы

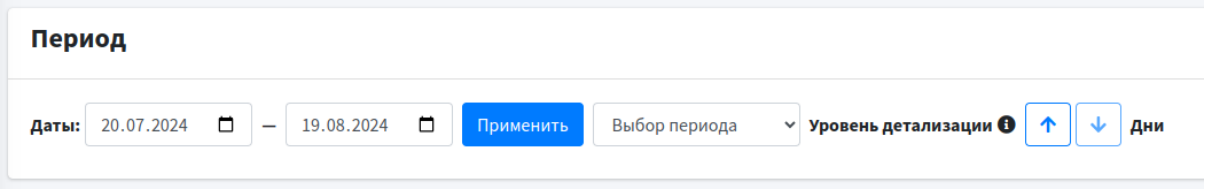
На странице **«Тренды»** отображено:



1. Настройка периода
2. Фильтры сессий
3. Графики
    - Установки
    - Регистрации
    - Количество сеансов
    - Максимум одновременных сессий
    - Длительность сеансов
    - Трафик моста
    - Трафик моста (по типам подключений)
    - Трафик выдачи файлов (по серверам)
    - Трафик выдачи файлов (по типам)

Настройка периода

В настройках периода присутствуют следующие опции:



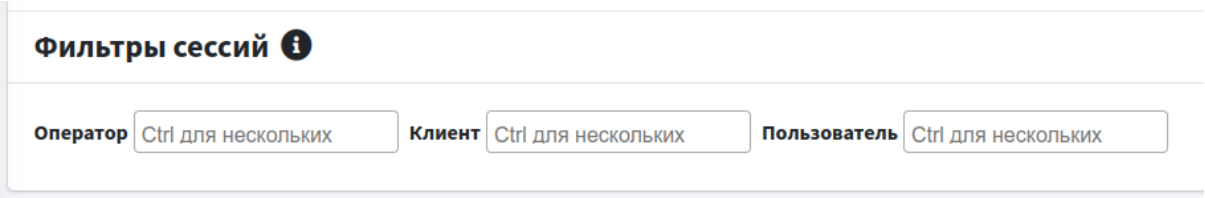
1. Даты — выбор диапазона, начиная с какой даты и по какую дату будет построен график для отображения статистики
2. Применить — эта кнопка предназначена для применения фильтров
3. Выбор периода — выбор, за какой период построить графики
4. Уровень детализации — выбор группировки данных по времени
    - **Месяцы**
    - **Недели**
    - **Дни**

Подсказка

Графики обновляются автоматически при выборе периода или смене уровня детализации, без нажатия на кнопку Применить

Фильтры сессий

В фильтре сессий присутствуют следующие опции:



1. Оператор — выбор устройства, которое выполняло подключение к удалённому устройству
2. Клиент — выбор устройства, к которому осуществлялось удалённое подключение
3. Пользователь — выбор пользователя, который осуществлял удалённое подключение

Примечание

Присутствует поиск по устройствам или пользователям
Возможен множественный выбор устройств или пользователей

Важно

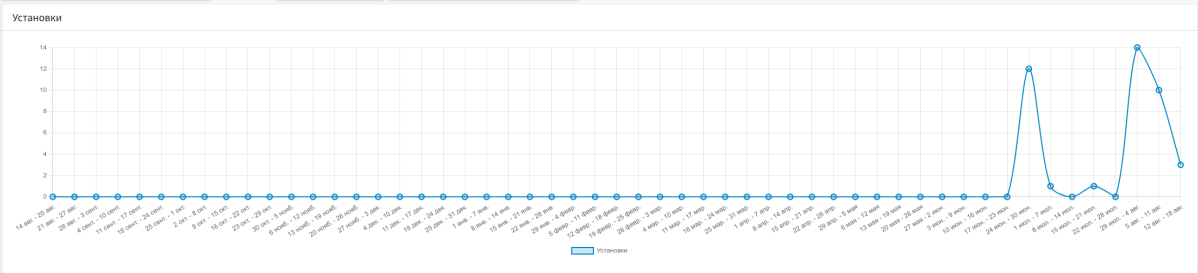
Данный фильтр предназначен только для графиков:

- Количество сеансов
- Максимум одновременных сессий
- Длительность сеансов
- Трафик моста
- Трафик моста (по типам подключений)

К графикам **«Трафик выдачи файлов»** фильтр не применяется — они строятся не по сессиям, а по журналу выдачи файлов

Графики

На графиках отображается статистика по показателям



На графиках присутствуют кликабельные маркеры значений. При клике произойдет переход на определенную страницу с установленным фильтром, которая зависит от графика

1. График **«Установки»** — отображает статистику по установкам клиента

   Подсказка

   Данные берутся со страницы *Устройства* из информации о подключении устройства к серверу **RuDesktop**

2. График **«Регистрации»** — отображает статистику по созданным или зарегистрированным пользователям

   Подсказка

   Данные берутся со страницы *Пользователи*

3. График **«Количество сеансов»** — отображает статистику по сессиям
4. График **«Максимум одновременных сессий»** — отображает максимальное количество одновременных активных сессий за выбранный период

5. График **«Длительность сеансов»** — отображает статистику по длительности сессий
6. График **«Трафик моста»** — отображает статистику по затраченному трафику сессий удалённого доступа

> **Подсказка**
>
> Данные берутся со страницы *Сессии*

> **Важно**
>
> В график не входят подключения типов **«Передача файлов»** и **«Политика»** — их трафик виден на графике **«Трафик моста (по типам подключений)»** отдельными линиями. Подключения, у которых тип не определён, в график попадают

7. График **«Трафик моста (по типам подключений)»** — тот же трафик моста, но разложенный на отдельные линии по типу подключения

   Отдельная линия строится для каждого типа подключения: **Рабочий стол**, **Передача файлов**, **TCP-туннелирование**, **RDP**, **Политика**, **Терминал**, **Проброс USB**

> **Примечание**
>
> Линии всех типов присутствуют в легенде всегда, даже если по типу за выбранный период не было трафика. Подключения, у которых тип не определён, выводятся отдельной линией **«Тип не определён»**

> **Подсказка**
>
> Данные берутся со страницы *Сессии*

8. График **«Трафик выдачи файлов (по серверам)»** — отображает объём данных, отданных устройствам по сети, в разрезе узлов, которые их отдавали

   Линии графика:

   - **Всего** — суммарный трафик по всем узлам, выделен более толстой линией
   - **Основной сервер** — трафик, отданный главным сервером
   - **Название точки распространения** — отдельная линия на каждую *точку распространения*, отдававшую файлы

- **Прочие TP (N)** — суммарная линия для остальных точек распространения, если их больше восьми

> **Примечание**
>
> Линия подписывается полем Название со страницы *Точки распространения*. Если узел не удалось сопоставить ни с одной зарегистрированной точкой, вместо названия в легенде выводится его адрес — в этом случае проверьте поле IPv4 адрес в свойствах точки распространения

9. График **«Трафик выдачи файлов (по типам)»** — тот же трафик выдачи, но разложенный на линии по назначению выдачи

   Линии графика:

   - **Всего** — суммарный трафик, выделен более толстой линией
   - **Политики** — загрузки файлов, которые используются хотя бы в одной *политике*
   - **Установки ОС** — данные, отданные устройствам при *установке ОС* по сети
   - **Загрузка файлов** — остальные загрузки файлов, не связанные ни с одной политикой

> **Подсказка**
>
> Данные обоих графиков выдачи берутся из журнала *Все логи* — из событий **«Выдача файла»** и **«Раздача при установке ОС»**. Клик по маркеру открывает журнал с фильтром по этим событиям и выбранному периоду

> **Примечание**
>
> В трафик установки ОС попадает и то, что устройство скачало по HTTP, и то, что было отдано по TFTP на этапе сетевой загрузки

2.14.5 Граф

Доступен в УД и UEM версиях

Граф — это страница, на которой отображаются ассоциации и подключения между устройствами

Подсказка

Страница **«Граф»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Как это работает

Страница строит графическое отображение связей между устройствами и поддерживает два режима:

- **Ассоциации** — связи устройств с одинаковыми UUID, IP-адресом или пользователем, но разными ID. Помогает находить дубликаты учётных записей одного устройства, переустановки и подмены
- **Подключения** — связи между устройствами по фактическим удалённым сессиям. Показывает, кто к кому подключался

Граф можно открыть с предварительно заданным фильтром:

- из списка *Устройства*, выбрав действие **Связи** в контекстном меню устройства
- из списка *Пользователи*, выбрав действие **Связи** в контекстном меню пользователя

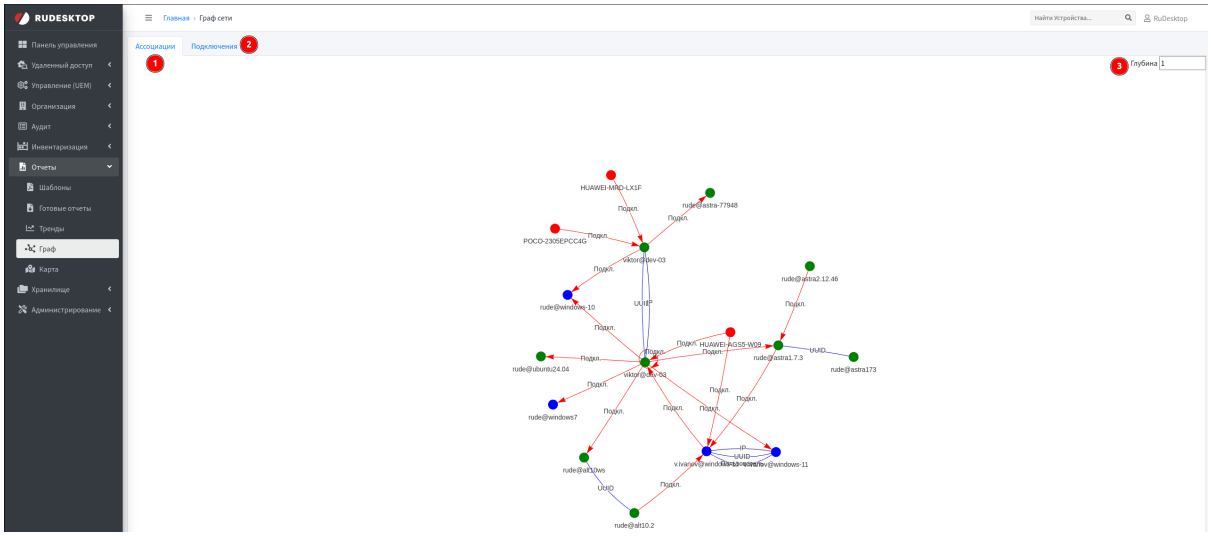
Без фильтра по умолчанию отображается граф последних 100 устройств, фигурировавших в подключениях

Важно

Доступ к странице регулируется правом Может просматривать граф. Без права страница и переходы к ней недоступны

Описание страницы

На странице **«Граф»** отображены:



1. Вкладка Ассоциации
2. Вкладка Подключения
3. Выбор глубины
4. Показать легенду

Вкладка ассоциаций

На этой вкладке отображаются ассоциации устройств с одинаковыми UUID, IP или пользователем, но разными ID

Вкладка подключений

На этой вкладке отображаются подключения между устройствами

Выбор глубины

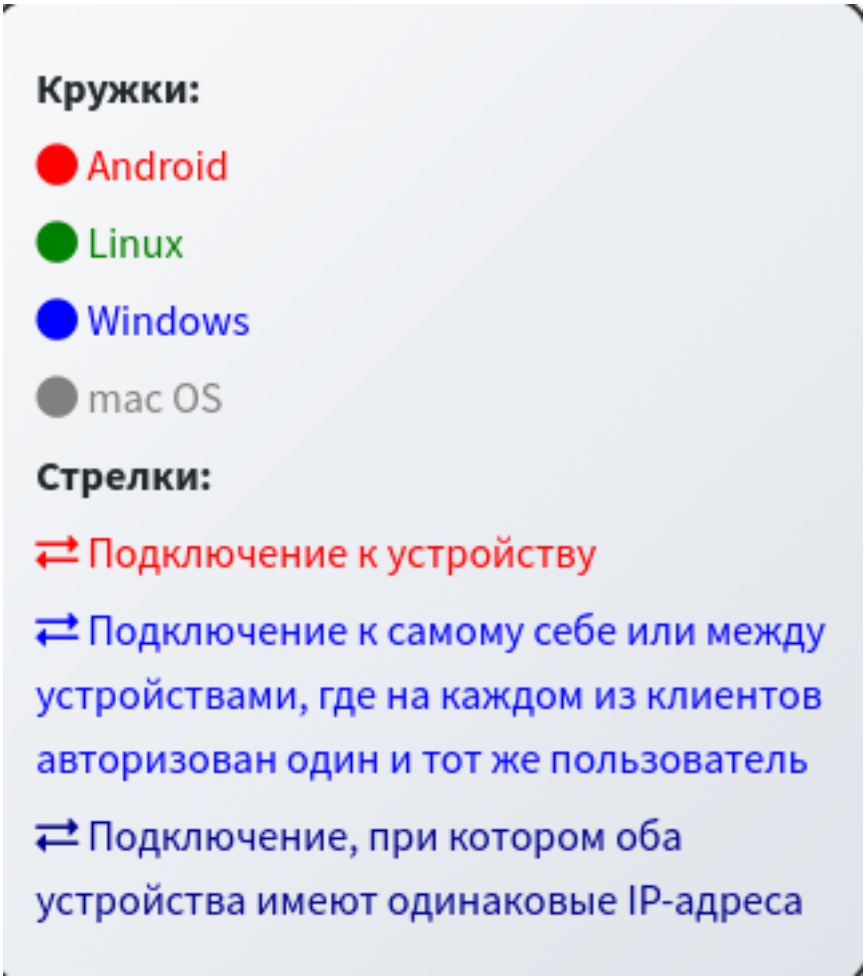
Данная опция отвечает за глубину отображения

Подсказка

Допустимы только положительные целые значения. Большая глубина увеличивает количество связей в графе и время его построения

Показать легенду

При установке флажка появляется окно с легендой, объясняющее назначение элементов



Примечание

Эта легенда предоставляет пояснения к различным элементам и настройкам, отображаемым на странице, чтобы пользователь чётко понимал, какую функцию выполняет каждый элемент и как они связаны друг с другом

Подсказка

При двойном нажатии на маркер устройства откроется страница свойств устройства

2.14.6 Карта

Доступна в УД и UEM версиях

Карта — это страница, на которой устройства отображаются по их геопозиции

Подсказка

Страница **«Карта»** доступна при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Важно

Карта работает на базе Яндекс.Карт

Подробнее о настройке *Яндекс Карт*

Как это работает

RuDesktop определяет геопозицию устройства одним из двух способов:

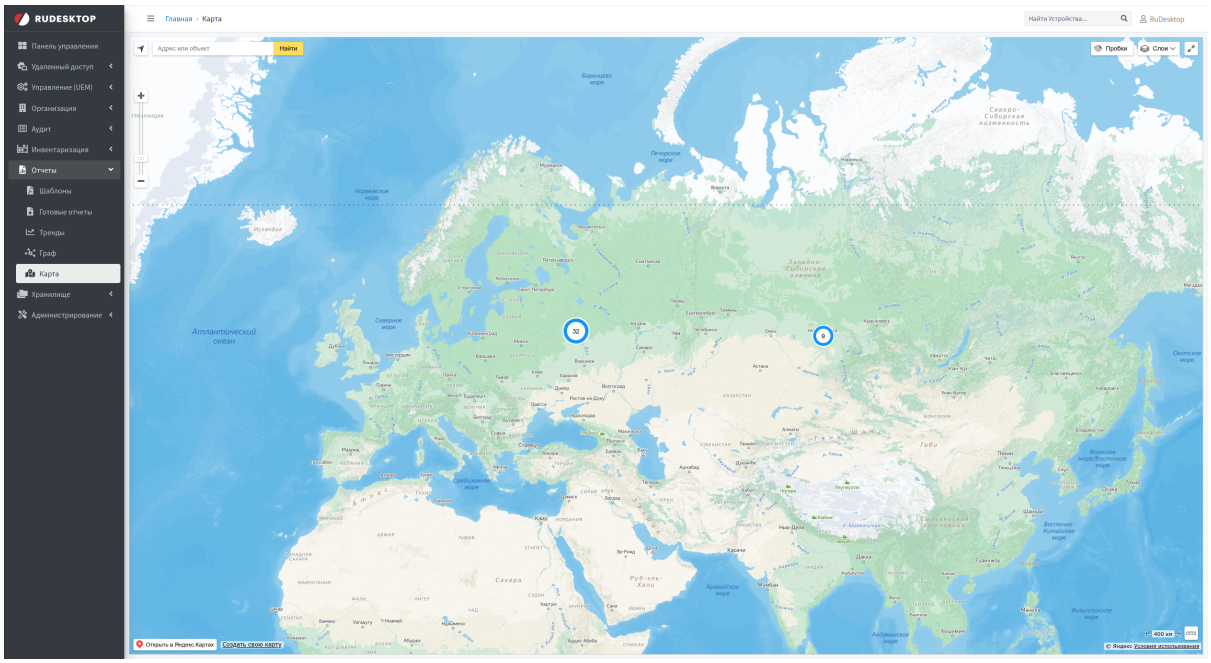
- **по внешнему IP-адресу** — для устройств, имеющих публичный адрес, координаты подбираются по внешним базам геолокации
- **по правилам подсетей** — для устройств с приватными IP-адресами координаты берутся из соответствующего правила (см. *Подсети*)

Дополнительно для Android-устройств можно собирать координаты непосредственно с устройства через политику *Управление гео-трекингом Android*

После того как координаты определены, устройство появляется на карте маркером. Несколько устройств в одной точке группируются в кластер — при нажатии на кластер открывается список устройств этой точки

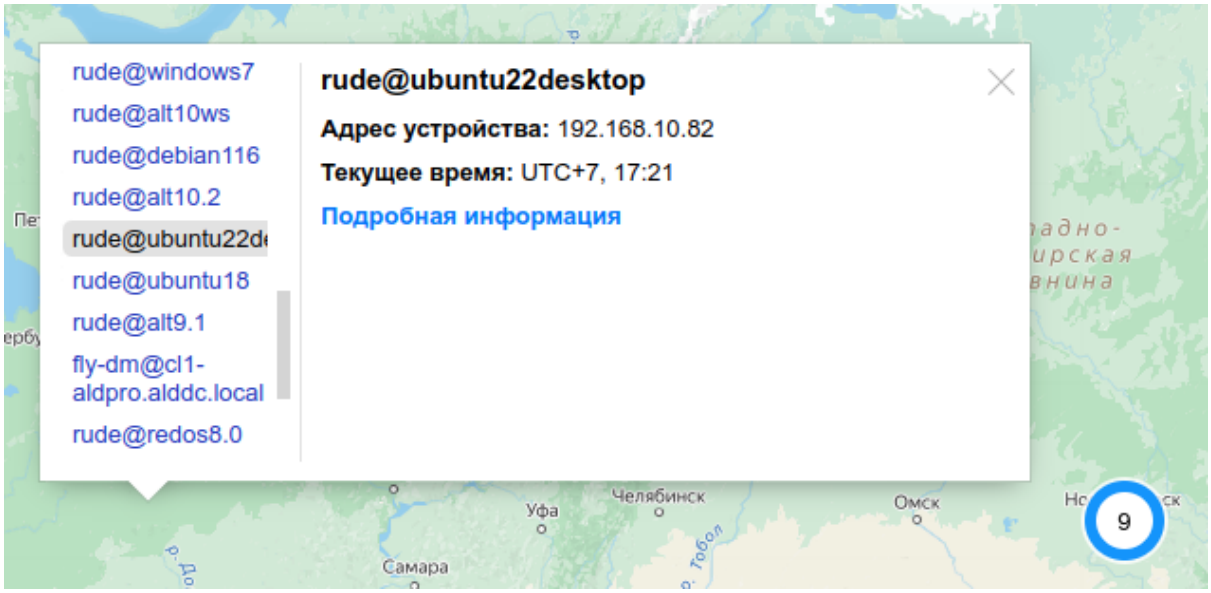
Важно

Доступ к странице регулируется правом Может просматривать карту. Без права страница и переходы к ней недоступны. Право не включает сбор геоданных само по себе



При нажатии на маркер устройства откроется окно с описанием устройств, находящихся в данной геопозиции

При нажатии на устройство отобразится следующая информация:



- Адрес устройства
- Текущее время в формате UTC + Время
- Ссылка на страницу свойств устройства

Отчеты — раздел для аналитики и визуализации данных сервера **RuDesktop**: встроенный BI-сервис **Apache Superset** с дашбордами и диаграммами, шаблоны и готовые отчёты на базе **ReportBro** в форматах PDF/XLSX, тренды по подключениям и сессиям, а также граф связей между устройствами и карта геопозиций

Подсказка

Раздел **«Отчеты»** доступен при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**. Страницы *Шаблоны*, *Готовые отчеты* и *Аналитика* доступны только при лицензии **UEM**

Аналитика

BI-сервис Apache Superset с дашбордами и диаграммами

Шаблоны

Шаблоны отчётов на базе ReportBro

Готовые отчеты

Сформированные отчёты в форматах PDF и XLSX

Тренды

Сводные графики по установкам, регистрациям и сессиям

Граф

Граф ассоциаций и подключений между устройствами

Карта

Карта устройств по их геопозиции

2.15 Хранилище

Доступно в УД и UEM версиях

2.15.1 Репозитории

Репозитории - на данной странице отображаются системные и пользовательские репозитории, созданные на сервере **RuDesktop**

Важно

При выборе файла из репозитория в *политиках* или *установке ОС* отображаются файлы только из системного репозитория **«Файловое хранилище»**

Для чего используется

Репозитории используются для логического разделения файлов в хранилище сервера **RuDesktop**

В репозиториях хранятся файлы, которые затем используются в *политиках*, установке ОС, отчётах и других сценариях работы сервера. Пользовательские репозитории удобно использовать для разделения файлов по назначению, подразделению или типу данных. Например, можно создать отдельный репозиторий для установочных пакетов, сертификатов или архивов

Как это работает

Каждый репозиторий соответствует отдельному каталогу на сервере **RuDesktop**

Путь до папки с репозиториями на сервере:

```
/var/lib/rudesktop/media/[КОРОТКОЕ_ИМЯ_РЕПОЗИТОРИЯ]
```

Примечание

Поле `Короткое имя` используется как имя каталога репозитория на сервере. После создания репозитория короткое имя недоступно для редактирования

При загрузке файла на странице *Файлы* пользователь выбирает репозиторий, в который будет сохранён файл. Если позже изменить репозиторий у файла, файл будет перемещён в каталог выбранного репозитория

Важно

Системные репозитории являются служебными

Их нельзя удалить, а часть полей недоступна для редактирования

Права доступа к репозиторию

Доступ к странице **«Репозитории»** и списку репозиториев определяется общими правами пользователя на раздел **«Хранилище»**

Эти права назначаются пользователю или группе на страницах *Права пользователя* и *Права группы*. Поле Права доступа в свойствах репозитория работает отдельно от доступа к самой странице

В этом поле выбираются системные права, которые должны быть у пользователя, чтобы он мог **скачать (загрузить) содержимое файлов** выбранного репозитория

Если права не отмечены, файлы репозитория доступны по подписанной ссылке без входа. Так устроен служебный репозиторий `files`, и так должен быть настроен репозиторий, из которого устройства скачивают пакеты (например, *пакеты обновлений Windows*)

Важно

Поле Права доступа влияет только на **скачивание содержимого файлов** и не управляет видимостью

Если у пользователя есть общие права на просмотр раздела **«Хранилище»**, он увидит и сам репозиторий в таблице, и список файлов в нём (названия, размеры и другие сведения) - независимо от прав, выбранных в этом поле

Ограничение применяется только в момент, когда пользователь пытается скачать содержимое файла

Примечание

Ограничение из поля Права доступа действует независимо от того, откуда пользователь открыл файл - со страницы *Файлы*, из сервисного портала или по ссылке в отчёте

Во всех случаях проверяется, есть ли у пользователя все выбранные права

Чтобы пользователь смог работать с файлами репозитория, необходимо:

1. Выдать пользователю или группе общие права на просмотр нужных страниц раздела **«Хранилище»**
2. Открыть свойства репозитория и выбрать в поле Права доступа права, которые будут разрешать доступ к файлам этого репозитория
3. Убедиться, что у пользователя есть все права, выбранные в поле Права доступа, напрямую или через группу

Например, если в поле Права доступа выбрано право **«Изменение файлов»**, пользователь сможет скачивать файлы репозитория только при наличии этого права. Право может быть назначено пользователю напрямую или через группу

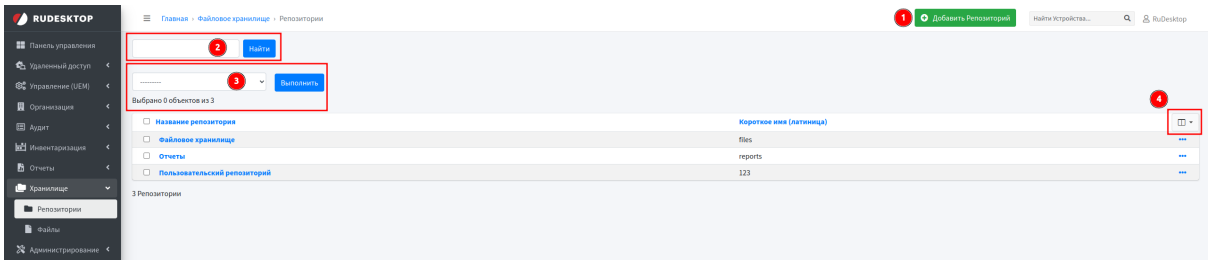
Примечание

Если в поле Права доступа выбрано несколько прав, пользователю нужны все выбранные права

Если поле оставлено пустым, для файлов репозитория не применяется дополнительное ограничение на уровне репозитория, но общие права на раздел и другие проверки доступа продолжают действовать

Описание страницы

На странице **«Репозитории»** отображено:



1. Кнопка Добавить репозиторий
2. Поиск
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Добавление репозитория

Для подключения сетевой папки сначала создать пустой пользовательский репозиторий, затем добавить *диск репозитория*

Примечание

Файлы такого репозитория поступают с сетевого ресурса только для чтения. Обычную загрузку через браузер выполнять в репозиторий без диска

При нажатии на кнопку Добавить репозиторий откроется страница добавления репозитория со следующими полями:

1. Поле Название репозитория - пользовательское название репозитория
2. Поле Короткое имя - название директории репозитория на сервере

Примечание

Поле может содержать только латинские буквы, цифры, символы: тире и подчёркивание

Чувствительно к регистру

3. Поле Адрес репозитория - адрес репозитория

Примечание

Адрес репозитория по умолчанию совпадает с адресом главного моста или текущего сервера

4. Поле Права доступа - системные права, необходимые для доступа к файлам репозитория

Поиск и фильтрация

Для поиска репозиториев можно использовать:

1. `Поле поиска` - поиск по названию репозитория или короткому имени

Для выполнения поиска необходимо заполнить поле и нажать на кнопку Найти

Таблица

Таблица разбита по столбцам:

1. `Название репозитория` - пользовательское название репозитория
2. `Короткое имя` - название директории репозитория на сервере

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` - открыть свойства репозитория
2. `Удалить` - удалить репозиторий
3. `История изменений` - открыть историю изменений репозитория
4. `Показать файлы` - открыть страницу *Файлы*, на которой будут отображены файлы, загруженные в данный репозиторий

Важно

Удалить можно только пользовательский репозиторий, в котором нет файлов

Массовые действия

Для выбранных репозиториев доступно действие:

1. Удалить выбранные репозитории - удаляет выбранные репозитории из таблицы

Важно

- В зависимости от прав пользователя действие может быть недоступно
- Если в репозиторий добавлены файлы, удалить его нельзя
- Системные репозитории удалить нельзя

Для выполнения действия необходимо отметить репозитории в таблице, выбрать действие Удалить выбранные репозитории и нажать на кнопку Выполнить

Удаление репозиториев

Для массового удаления репозиториев необходимо:

1. Отметить необходимые репозитории в таблице
2. Выбрать действие Удалить выбранные репозитории
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие репозитории будут удалены
5. Нажать на кнопку Да, я уверен

Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору

Свойства репозитория

При нажатии на кнопку `Редактировать` откроется страница свойств репозитория

Доступные поля:

1. Поле Название репозитория - пользовательское название репозитория
2. Поле Адрес репозитория - адрес репозитория
3. Поле Короткое имя - название директории репозитория на сервере
4. Поле Расположение - путь к каталогу репозитория на сервере
5. Поле Права доступа - системные права, необходимые для доступа к файлам репозитория

Примечание

Поля `Короткое имя` и `Расположение` доступны только для просмотра

Важно

Для системных репозиториев также недоступно редактирование полей `Адрес репозитория` и `Права доступа`

На странице свойств доступны следующие действия:

1. Сохранить - сохранить изменения и вернуться на страницу **«Репозитории»**
2. Сохранить и продолжить - сохранить изменения и остаться на странице редактирования
3. Удалить - удалить репозиторий
4. История изменений - просмотреть историю изменений

2.15.2 Диски репозиториев

Диск репозитория подключает сетевую папку к хранилищу RuDesktop. Файлы остаются на сетевом ресурсе и становятся доступны через выбранный репозиторий после подключения и синхронизации списка

Как это работает

Диск подключается на сервере только для чтения. RuDesktop получает список файлов и создаёт для них записи в разделе **«Файлы»**, которые можно выбирать в политиках и других сценариях

Примечание

Синхронизация обновляет эти записи, а не отправляет изменения обратно на сетевой ресурс

Для загрузки, изменения или удаления исходных файлов использовать сам сетевой ресурс, затем синхронизировать диск в RuDesktop

Для обычной загрузки файлов через браузер использовать отдельный репозиторий без подключённого диска

Подготовка

- Создать пустой пользовательский *репозиторий*

  Служебные репозитории и репозитории с файлами для подключения не подходят

- Обеспечить серверу доступ к сетевому ресурсу и подготовить учётные данные
- Выдать пользователю права на просмотр и изменение дисков репозиториев, а также необходимые права на репозиторий и файлы

Важно

К одному репозиторию подключается один диск. После создания диска выбрать для него другой репозиторий нельзя

Добавление и подключение

1. Открыть **«Хранилище → Диски репозиториев»** и добавить запись
2. Задать уникальное **«Название»** и выбрать пустой **«Репозиторий»**
3. Выбрать **«Тип»** и заполнить **«Сетевой путь»** по таблице ниже
4. Указать **«Имя пользователя»** и **«Пароль»**, если ресурс требует авторизации

   Для Samba и SFTP эти поля обязательны

5. На вкладке **«Синхронизация»** проверить **«Синхронизировать по расписанию»** и **«Расписание синхронизации»** - по умолчанию каждые 30 минут
6. Сохранить запись и выполнить **«Подключить»**
7. Дождаться результата на вкладке **«Состояние»**, затем открыть **«Файлы»** и отфильтровать их по выбранному репозиторию

Тип	Пример сетевого пути	Учётные данные
Samba	`//files.example.org/software/installers`	Пользователь и пароль, при необходимости `DOMAIN\user`
SFTP	`files.example.org:22/software`	Пользователь и пароль
WebDAV	`https://files.example.org/software`	Пользователь и пароль, если требуется авторизация

В пути можно указать порт сервера. Для Samba без явно заданного порта используется 445, для SFTP - 22. Учётные данные вводятся отдельными полями, их нельзя включать в сетевой путь

Подсказка

Сохранение записи ещё не подключает диск. После успешного подключения первая синхронизация запускается автоматически. Для обновления списка без ожидания расписания выполнить **«Синхронизировать»**

Действия доступны в меню строки диска и в его карточке при наличии прав. Они ставятся в очередь - уведомление о запуске ещё не означает завершение. Обновить страницу и проверить состояние, время и результат синхронизации. Если расписание отключено, первая синхронизация при подключении всё равно выполняется, а последующие обновления можно запускать вручную

Состояние и результаты

- **«Состояние»** описывает подключение: **«Отключён»**, **«Подключён»** или **«Ошибка»**
- **«Статус синхронизации»** описывает последний обход файлов: **«Ещё не запускалась»**, **«Синхронизация»**, **«Успешно»** или **«Ошибка»**

Проверять оба поля — подключение диска не гарантирует успешного чтения всего списка

В **«Результате синхронизации»** показано количество добавленных, обновлённых и удалённых записей, а также пропущенные файлы и сохранённые используемые записи

- Новые файлы добавляются в список
- Изменения определяются по размеру и времени изменения файла

- Исчезнувшие файлы удаляются из списка только после получения полного списка

  Если запись защищена ссылками из других объектов, она сохраняется

- При неполном списке удаление отсутствующих записей пропускается

  Причину неполной синхронизации смотреть в **«Последней ошибке»**

Обход включает вложенные папки выбранного сетевого пути. Папки не становятся отдельными записями файлов

Важно

Переименование или перенос файла в другую подпапку рассматривается как исчезновение прежнего пути и появление нового. Ссылки политик на старую запись автоматически на новую не переключаются. Если содержимое заменили, сохранив прежние размер и время изменения, синхронизация не обнаружит замену по этим признакам. Для новой версии установщика удобнее использовать новое имя файла, затем явно выбрать его в нужной политике

Пропускаются пути с символами ?, #, %, обратной косой чертой и управляющими символами, а также слишком длинные пути. Если файл пропущен, изменить его имя или сократить вложенность папок на сетевом ресурсе и повторить синхронизацию. Статус **«Успешно»** не исключает пропущенных файлов - проверять счётчики

Если в результате указано **«Не удалось обновить содержимое точки монтирования»**, список записей уже мог обновиться, но доступ к новым файлам требует проверки. Повторить синхронизацию, затем проверить скачивание нужного файла. Если сообщение сохраняется, передать его администратору сервера. Сохранённая запись отсутствующего файла не восстанавливает сам файл

Если он нужен политике или другому объекту, восстановить его на сетевом ресурсе либо выбрать другой файл

Изменение подключения и ключ SFTP

Чтобы изменить путь, тип, пользователя или пароль, сначала выполнить **«Отключить»** и дождаться состояния **«Отключён»**. После изменения сохранить запись и подключить диск снова

Подсказка

Пустое поле пароля при редактировании сохраняет прежний пароль

При первом подключении SFTP сервер сохраняет ключ хоста. Если ключ сервера изменился, подключение может завершиться ошибкой. После проверки нового ключа у администратора SFTP отключить диск, выполнить **«Сбросить ключ хоста SFTP»** и подключить снова

Отключение и удаление

- **«Отключить»** прекращает доступ через подключённый диск и его плановую синхронизацию, но сохраняет запись диска и список файлов. После повторного подключения расписание возобновляется, если включён параметр **«Синхронизировать по расписанию»**
- **Удаление диска** убирает его запись, связанные записи файлов и расписание. Исходные файлы сетевого ресурса не удаляются, репозиторий остаётся

Если файлы защищены ссылками из других объектов, удаление отклоняется. Проверить **«Последнюю ошибку»** и сначала заменить или убрать эти ссылки

Если файлы не появились

1. Проверить, выполнено ли **«Подключить»**, а не только сохранена запись
2. Проверить путь, учётные данные и доступ к ресурсу именно с сервера RuDesktop
3. Открыть **«Последнюю ошибку»** и **«Результат синхронизации»**
4. Если подключение работает, выполнить **«Синхронизировать»** и дождаться результата
5. В **«Файлах»** проверить фильтр репозитория

Если сообщение об ошибке указывает на невозможность запуска службы подключения, передать его администратору сервера

Пошаговый пример с общей папкой установщиков приведён в кейсе Подключение сетевой папки с установщиками

2.15.3 Файлы

Доступны в УД и UEM версиях

Файлы - на данной странице отображаются файлы, загруженные в *репозитории* на сервер **RuDesktop**, и файлы подключённых *сетевых дисков*

Примечание

По умолчанию отображаются файлы всех репозиториев

Для чего используется

Файлы используются в *политиках*, *установке ОС* и других сценариях, где серверу **RuDesktop** нужно передать на устройство установщик, архив, сертификат, скрипт или другой вложенный файл

Для установочных пакетов сервер может автоматически определить информацию о пакете: формат, имя, версию, идентификатор MSI и другие метаданные

Эти данные используются в политиках *Установка пакета* и *Удаление пакета*, например для автоматического заполнения имени пакета, версии или идентификатора MSI

Как это работает

Файл загружается в выбранный репозиторий и сохраняется на сервере **RuDesktop**

После загрузки сервер сохраняет оригинальное имя файла и рассчитывает контрольную сумму SHA1. Тип файла определяется при отображении файла на странице, а информация о пакете - при открытии свойств файла или использовании файла в политиках

Если файл используется в политиках и на сервере настроены *точки распространения*, файл можно заранее закэшировать на активных точках распространения

Подробнее о кэшировании см. на странице *Кэшированные файлы*

Важно

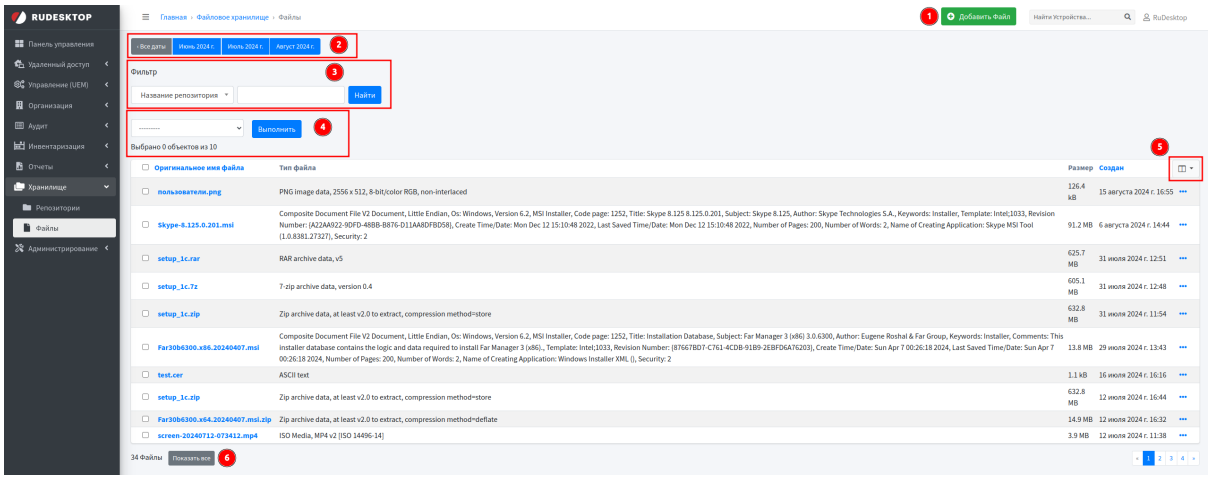
При удалении обычного загруженного файла удаляется исходный файл из хранилища сервера **RuDesktop**

Если файл был закэширован на точках распространения, связанные записи кэша также удаляются, а для точек распространения создаются задачи удаления локальных копий

Файлы сетевых дисков доступны только для чтения - изменять и удалять исходники нужно на самом сетевом ресурсе

Описание страницы

На странице **«Файлы»** отображается:



1. Кнопка Добавить файл
2. Фильтр даты
3. Фильтр

4. Массовые действия
5. Таблица с возможностью настройки отображаемых столбцов
6. Кнопка Показать все

Добавление файла

При нажатии на кнопку Добавить файл откроется страница добавления файла на сервер со следующими полями:

1. Поле Репозиторий - выбор *репозитория*, в который будет загружен файл
2. Поле Файл - выбор файла на своём устройстве

Недостаточно места при загрузке

Перед началом загрузки сервер проверяет свободное место для временного файла. Из доступного объёма вычитаются ещё не записанные части других активных загрузок и резерв сервера - по умолчанию 1 ГиБ. Поэтому показанный доступный объём может быть меньше свободного места на диске. Если файл не помещается, загрузка отклоняется с сообщением о размере файла и доступном месте

Дождаться завершения других загрузок либо освободить место на сервере, после чего повторить загрузку

Примечание

Свободное место на компьютере пользователя или на отдельном сетевом ресурсе не заменяет место во временном хранилище сервера

Если место заканчивается уже во время передачи, сервер сообщает об этом. После освобождения места загрузку потребуется повторить

Файлы сетевого диска

Такие записи появляются после синхронизации подключённого диска. Их нельзя заменить или удалить через карточку файла. Внести изменения на сетевом ресурсе и выполнить **«Синхронизировать»** в карточке *диска репозитория*

Поиск и фильтрация

Для фильтрации файлов можно использовать:

1. `Фильтр даты` - отображение файлов за выбранные год, месяц или день
2. `Название репозитория` - отображение файлов, находящихся в конкретном репозитории
3. `Поле поиска` - поиск по оригинальному имени файла, GUID или пути к файлу

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Таблица

Таблица разбита по столбцам:

1. `Оригинальное имя файла` - полное название файла
2. `Политики` - названия *политик*, в которых выбран файл
3. `Тип файла` - тип файла, определяется по содержимому файла
4. `Размер` - размер файла
5. `Создан` - дата загрузки файла на сервер
6. `Информация о пакете` - метаданные установочного пакета, если их удалось определить
7. `Кешировано` - *точки распространения*, на которых есть локальная копия файла

Примечание

Действие `Кэшировать` и столбец `Кешировано` доступны при наличии лицензии с функциями UEM

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` - открыть свойства файла
2. `Удалить` - удалить файл
3. `История изменений` - открыть историю изменений файла
4. `Скачать` - загрузить файл на устройство
5. `Кэшировать` - поставить файл в очередь на кэширование на активных точках распространения

Массовые действия

Доступные действия:

1. Удалить выбранные файлы - удаляет выбранные файлы из таблицы
2. Кэшировать выбранные файлы - ставит выбранные файлы в очередь на кэширование на активных *точках распространения*

Примечание

Действие Кэшировать выбранные файлы доступно при наличии лицензии с функциями UEM

Важно

В зависимости от прав пользователя отдельные действия могут быть недоступны

Для выполнения действия необходимо отметить файлы в таблице, выбрать нужное действие и нажать на кнопку Выполнить

Удаление файлов

Для массового удаления файлов необходимо:

1. Отметить необходимые файлы в таблице
2. Выбрать действие Удалить выбранные файлы
3. Нажать на кнопку Выполнить
4. На открывшейся странице будет отображаться информация о том, какие файлы будут удалены
5. Нажать на кнопку Да, я уверен

Можно отменить данную операцию, нажав на кнопку Нет, отменить и вернуться к выбору

Кэширование файлов

Для массового кэширования файлов необходимо:

1. Отметить необходимые файлы в таблице
2. Выбрать действие Кэшировать выбранные файлы
3. Нажать на кнопку Выполнить
4. Для каждой активной *точки распространения* будут созданы задачи **«Кэширование файла»**

Подробнее о кэшировании файлов см. на странице *Кэшированные файлы*

Кнопка «Показать все»

По умолчанию на странице отображается 10 файлов

При нажатии на кнопку Показать все будут показаны все файлы

Свойства файла

При нажатии на кнопку `Редактировать` откроется страница свойств файла

Основная информация

Доступные поля во вкладке **«Основная информация»**:

1. Поле Репозиторий - отображается *репозиторий*, в котором находится файл

> **Примечание**
>
> В выпадающем списке можно выбрать другой репозиторий для хранения файла

> **Важно**
>
> При смене репозитория файл будет перемещён в каталог выбранного репозитория на сервере, а путь к файлу обновится автоматически

2. Поле Оригинальное имя файла - отображается имя файла

> **Примечание**
>
> В данном поле можно изменить название файла

3. Поле Файл - отображается путь до файла на сервере

> **Примечание**
>
> Данное поле недоступно для редактирования

4. Поле Контрольная сумма SHA1 - отображается значение контрольной суммы загруженного файла

Информация о пакете

Для установочных пакетов во вкладке **«Информация о пакете»** отображаются данные, полученные из файла

Сервер пытается определить метаданные для следующих типов установочных пакетов:

1. `.msi` - Windows Installer: идентификатор продукта, название, версия и другие данные установщика
2. `.exe` - исполняемый установщик Windows: название, версия и другие доступные данные файла
3. `.deb` - Debian-пакет: имя пакета, версия, зависимости и другие данные пакета

4. `.rpm` - RPM-пакет: имя пакета, версия, зависимости и другие данные пакета
5. `.pkg.tar.zst` - пакет Arch Linux с Zstandard-сжатием: имя пакета, версия, зависимости и другие данные пакета
6. `.pkg.tar.xz` - пакет Arch Linux с XZ-сжатием: имя пакета, версия, зависимости и другие данные пакета
7. `.apk` - Android-приложение: имя пакета, версия и другие данные приложения
8. `.pkg` - установочный пакет macOS: идентификатор пакета, версия и другие данные установщика
9. `.dmg` - образ macOS: данные установочного образа, если их удалось определить

Примечание

Набор отображаемых полей зависит от типа пакета и данных, которые удалось получить из файла

Примечание

Информация о пакете определяется по содержимому файла

Если файл заменить и его контрольная сумма изменится, информация о пакете будет определена заново

Примечание

Вкладка **«Информация о пакете»** доступна только для просмотра

Данные формируются автоматически и не редактируются вручную

Полученная информация используется в политиках *Установка пакета* и *Удаление пакета*:

1. Для `.msi` в поле пакета может автоматически подставляться идентификатор продукта
2. Для `.deb` и `.rpm` в поле пакета может автоматически подставляться имя пакета
3. Версия пакета может использоваться политиками для проверки установленной версии приложения

Важно

Если информацию о пакете получить не удалось, вкладка **«Информация о пакете»** не отображается

В этом случае значения в настройках политики нужно указать вручную

На странице свойств доступны следующие действия:

1. Сохранить - сохранить изменения и вернуться на страницу **«Файлы»**
2. Сохранить и продолжить - сохранить изменения и остаться на странице редактирования
3. Удалить - удалить файл
4. История изменений - просмотреть историю изменений

2.15.4 Кэшированные файлы

Доступны только в UEM версии

Кэшированные файлы — на данной странице отображаются *файлы*, которые были загружены из хранилища сервера **RuDesktop** в локальный кэш *точек распространения*

Кэшированный файл всегда связан с конкретной *точкой распространения*: одна запись показывает, что выбранный файл доступен локально на указанной точке распространения

Один файл может быть кэширован на нескольких точках распространения. В этом случае на странице **«Кэшированные файлы»** для него будет несколько записей: по одной записи для каждой точки распространения

Важно

Страница доступна при наличии лицензии с функциями UEM

Для чего используется

Кэшированные файлы нужны для выполнения *политик*, в которых используются файлы из хранилища сервера **RuDesktop**

Если политика запускается на точке распространения, этой точке нужен доступ к выбранным в политике файлам: установочным пакетам, архивам, сертификатам, скриптам и другим вложениям. Кэширование заранее сохраняет такие файлы локально на точке распространения, чтобы при выполнении политики она могла использовать локальную копию файла

Это полезно, когда один и тот же файл используется в нескольких политиках или применяется к большому количеству устройств: точке распространения не нужно заново загружать файл с главного сервера при каждом запуске политики

Кэширование также снижает нагрузку на канал связи главного сервера. Файл загружается на точку распространения один раз, после чего дальнейшая работа с ним выполняется через локальную копию на этой точке. За счёт этого

передача файлов распределяется между точками распространения, а главный сервер не отдаёт один и тот же файл повторно для каждого запуска политики

Как это работает

Файлы кэшируются на *точках распространения*, чтобы фоновые задачи могли использовать локальную копию файла при выполнении *политик*

Кэширование запускается со страницы *Файлы*:

1. Для отдельного файла — через действие `Кэшировать` в меню записи
2. Для нескольких файлов — через массовое действие Кэшировать выбранные файлы

После запуска кэширования сервер создаёт задачу **«Кэширование файла»** для каждой активной точки распространения. Точка распространения загружает файл с основного сервера в свой локальный каталог `MEDIA_ROOT` и сохраняет запись на странице **«Кэшированные файлы»**

Важно

Если точка распространения не активна, задача кэширования для неё не создаётся. Например, если подключены две точки распространения, но активна только одна, файл будет кэширован только на активной точке распространения

Например, если файл кэшируется на трёх активных точках распространения и задачи успешно выполнены на каждой из них, на странице **«Кэшированные файлы»** будет по одной записи для каждой точки распространения. Если запись для пары `файл` + `точка распространения` уже существует, она обновится, а не будет создана повторно

Примечание

Если файл используется в *политике*, точка распространения также может загрузить его в кэш перед выполнением политики

Важно

Ручное добавление кэшированных файлов на этой странице не предусмотрено

Обновление кэшированной копии

Если файл на главном сервере был изменён или загружен повторно, кэшированная копия на точке распространения может стать неактуальной

При следующем кэшировании файла или перед выполнением политики точка распространения проверяет локальную копию по контрольной сумме SHA1.

Если контрольная сумма отличается от актуальной контрольной суммы файла на главном сервере, локальная копия удаляется и загружается заново

Передача файла на устройство

Когда *политика* с файлом выполняется на точке распространения, устройство загружает файл **напрямую с этой точки распространения** по протоколу **HTTPS**, а не с главного сервера. Точка распространения, выполняющая задачу, автоматически подставляет в задание ссылку на свою локальную копию файла

Если на точке распространения нужного файла не оказалось (например, кэширование не выполнялось), точка догружает файл с главного сервера в момент выполнения политики и затем отдаёт его устройству. За счёт этого выполнение политики не прерывается, а предварительное кэширование лишь ускоряет процесс и снижает нагрузку на канал главного сервера

Примечание

Сетевые соединения и порты, которые требуется открыть для передачи файлов и для управляющего канала, приведены в разделе *Настройка точек распространения*

Где проверить результат

Результат кэширования можно проверить:

1. На странице **«Кэшированные файлы»** — здесь отображаются записи по файлам и точкам распространения
2. На странице *Файлы* — в столбце Кешировано отображаются точки распространения, на которых есть локальная копия файла
3. На странице *Очередь задач* — здесь можно проверить выполнение задач **«Кэширование файла»** и **«Удаление кэшированного файла»**

Типовой сценарий

Для использования кэшированных файлов в политиках:

1. Загрузить файл на странице *Файлы*
2. Запустить кэширование файла
3. Проверить, что на странице **«Кэшированные файлы»** появилась запись для нужной точки распространения
4. Выбрать файл в настройках *политики*
5. Запустить политику на устройствах

Описание страницы

На странице **«Кэшированные файлы»** отображаются:

1. Фильтр по точке распространения
2. Поле поиска
3. Массовые действия
4. Таблица с возможностью настройки отображаемых столбцов

Поиск и фильтрация

Для фильтрации записей можно использовать:

1. `Точка распространения` — отображает файлы, кэшированные на выбранной точке распространения
2. `Поле поиска` — поиск по названию файла или названию точки распространения

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Таблица

Таблица разбита по столбцам:

1. `Файл` — файл из хранилища сервера **RuDesktop**
2. `Точка распространения` — точка распространения, на которой находится локальная копия файла
3. `Путь` — путь к файлу на сервере
4. `Контрольная сумма SHA1` — контрольная сумма кэшированной копии файла
5. `Дата кэширования` — дата и время создания записи о кэшировании
6. `Дата обновления` — дата и время последнего обновления записи

Примечание

На странице *Файлы* в столбце `Кешировано` отображаются точки распространения, на которых уже есть локальная копия файла

Операции

При нажатии на кнопку с правого края таблицы открывается контекстное меню

Доступные действия:

1. `Редактировать` — открыть свойства кэшированного файла
2. `Удалить` — удалить запись о кэшированном файле

3. История изменений — открыть историю изменений записи

Важно

При удалении записи сервер отправляет на связанную точку распространения задачу **«Удаление кэшированного файла»**. После выполнения задачи локальная копия файла удаляется с этой точки распространения

Удаление файла с главного сервера

Если удалить файл на странице *Файлы*, сервер удалит исходный файл из хранилища и связанные с ним записи на странице **«Кэшированные файлы»**

Для каждой удалённой записи кэшированного файла будет создана задача **«Удаление кэшированного файла»** на соответствующей точке распространения. После выполнения задачи точка распространения удалит локальную копию файла из своего кэша

Примечание

Если точка распространения недоступна, задача удаления будет ожидать выполнения в *очереди задач*

Важно

После удаления файла с главного сервера *политики* и другие операции, в которых был выбран этот файл, не смогут использовать его повторно. При необходимости файл нужно загрузить в хранилище заново и снова выбрать его в настройках политики

Массовые действия

Для выбранных записей доступно действие:

1. Удалить выбранные кэшированные файлы — удаление записей и постановка задач на удаление локальных копий файлов с соответствующих точек распространения

Важно

В зависимости от прав пользователя действие может быть недоступно

Для выполнения действия необходимо отметить записи в таблице, выбрать действие Удалить выбранные кэшированные файлы и нажать на кнопку Выполнить

Свойства кэшированного файла

При открытии записи отображаются следующие поля:

1. `Файл` — файл из хранилища сервера **RuDesktop**
2. `Точка распространения` — точка распространения, на которой находится локальная копия файла
3. `Контрольная сумма SHA1` — контрольная сумма кэшированной копии файла
4. `Дата кэширования` — дата и время создания записи о кэшировании
5. `Дата обновления` — дата и время последнего обновления записи
6. `Путь` — путь к файлу на сервере

Примечание

Поля на странице свойств доступны только для просмотра

На странице свойств доступны следующие действия:

1. Удалить — удалить запись о кэшированном файле и поставить задачу на удаление локальной копии с точки распространения
2. История изменений — просмотреть историю изменений

Хранилище - раздел для управления файловыми ресурсами сервера **RuDesktop**: репозитории как контейнеры для файлов, сами файлы (например, ISO-образы, дистрибутивы, скрипты, сертификаты, видеозаписи сессий и готовые отчёты) и кэшированные копии часто запрашиваемых файлов на устройствах для ускорения загрузки

Подсказка

Раздел **«Хранилище»** доступен при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**

Репозитории

Контейнеры для хранения файлов на сервере

Файлы

Загруженные на сервер файлы - ISO, дистрибутивы, скрипты, отчёты

Кэшированные файлы

Кэш часто запрашиваемых файлов на устройствах

Диски репозиториев

Подключение сетевых ресурсов Samba, SFTP и WebDAV для чтения файлов

2.16 Администрирование

2.16.1 Настройки

Описание страницы

Настройки - эта страница предназначена для конфигурации ключевых компонентов и интеграций с сервером **RuDesktop**

Как это работает

На странице собраны системные параметры сервера **RuDesktop**, которые влияют на безопасность, аутентификацию, интеграции и поведение клиента

Изменения применяются в соответствующих компонентах системы в зависимости от типа настройки

Доступные блоки настройки

На странице доступны следующие блоки:

1. Безопасность - настройка позволяет выбрать группы по умолчанию, длительность сессий, разрешение самостоятельной регистрации пользователей и доступ к пакетам клиента
2. Аутентификация - настройка позволяет конфигурировать двухфакторную авторизацию, тип авторизации, captcha и параметры входа
3. Настройки SMTP - настройка позволяет конфигурировать SMTP-сервер для отправки уведомлений на электронную почту
4. Настройки телеграм бота - настройка позволяет конфигурировать Telegram-бота для отправки уведомлений и одноразовых кодов
5. Настройки MAX бота - настройка позволяет конфигурировать бота мессенджера MAX для отправки уведомлений и одноразовых кодов
6. Настройки собственного сервера OTP - настройка позволяет указать адрес стороннего сервиса, который выдаёт и проверяет одноразовые коды
7. SMS шлюз - настройка позволяет конфигурировать SMS-шлюз для отправки уведомлений и одноразовых кодов
8. Настройки мостов - настройка позволяет конфигурировать адрес основного моста и тип подключения
9. Карты - настройка позволяет подключить Яндекс Карты
10. Обновления - настройка позволяет получать уведомления о новой версии сервера **RuDesktop**

11. Настройки HelpDesk - настройка позволяет перенаправлять обращения в техподдержку и передавать информацию о клиенте
12. Настройки Ansible - настройка позволяет конфигурировать количество потоков и таймаут выполнения задач
13. Настройки логов - настройка позволяет управлять логированием событий и исключениями из логирования
14. Настройки баннера (Клиент) - настройка позволяет отображать баннер в клиенте **RuDesktop**
15. Настройки баннера (Сайт) - настройка позволяет отображать баннер на странице *Панель управления*
16. Настройки клиента - настройка позволяет задать ограничения и исключения для длительности пользовательских сессий, а также правила формирования ID устройств
17. Видеозаписи - настройка позволяет изменить расположение хранения видеозаписей, настроить качество записанного видео и посмотреть занимаемый ими объём
18. PXE - настройка позволяет задать таймаут автозагрузки образа по умолчанию в PXE-меню мультизагрузки при *установке ОС*
19. Обновления ОС - настройки задают предел размера и репозиторий для пакетов, которые сервер скачивает с серверов Microsoft при *подготовке обновлений*

Безопасность

Блок управляет правилами автоматического распределения новых пользователей и устройств по группам, а также политиками сессий и публичного доступа

- Группа по умолчанию для новых компьютеров - локальная группа, в которую попадают новые устройства при первом подключении к серверу **RuDesktop**
- Группа по умолчанию для новых пользователей - локальная группа, в которую попадают новые пользователи при первой регистрации или добавлении

> **Подсказка**
>
> Список групп загружается со страницы *Группы*
>
> Та же группа подставляется при импорте пользователей и устройств из домена и **Keycloak**, если в их конфигурации не указана отдельная группа по умолчанию

- Разрешить самостоятельную регистрацию пользователей - активация формы самостоятельной регистрации пользователей

  Подробнее о *регистрации пользователей*

Важно

При включении этой настройки убедитесь, что у группы по умолчанию заданы минимально необходимые права - иначе зарегистрировавшийся пользователь не сможет работать в системе

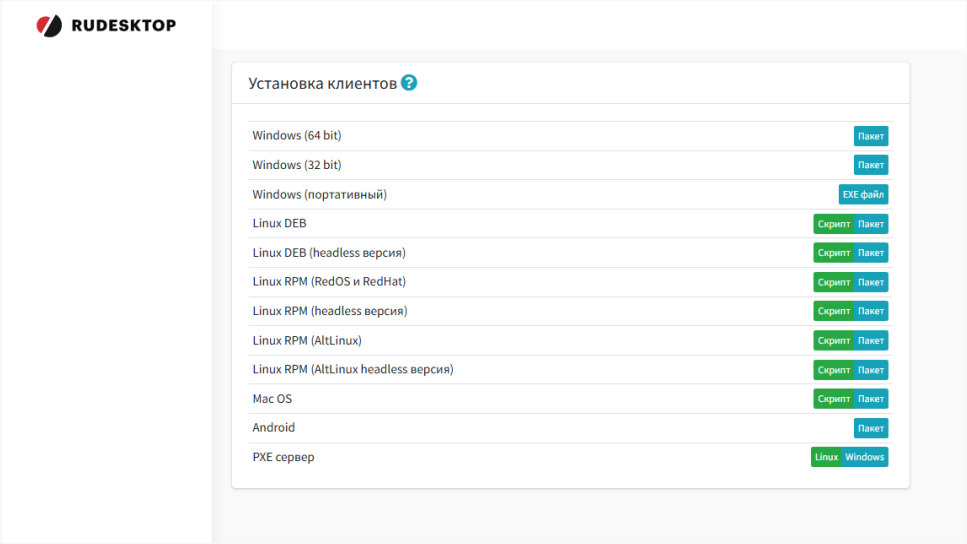
- Максимальная длительность сессии (в минутах) - время, через которое произойдёт автоматический выход из учётной записи в веб-интерфейсе

  Значение по умолчанию - `20160` минут (336 часов / 14 дней)

- Доступ к пакетам клиента неавторизованными пользователями - открывает доступ к странице загрузки пакетов клиента **RuDesktop** без авторизации

Примечание

Страница доступна по адресу `https://АДРЕС_СЕРВЕРА/dashboard/distr/`



Важно

Если опция не активирована, попытка перехода на страницу загрузки пакетов приведёт к ошибке `403`

- Неавторизованный пользователь может видеть магазин приложений (IP адрес должен совпадать) - разрешает открыть магазин приложений без авторизации, если IP-адрес запроса совпадает с IP-адресом зарегистрированного устройства

Важно

При включении этой настройки право **«Может использовать магазин приложений»** необходимо выдавать **устройству**, а не пользователю - иначе магазин не откроется

Аутентификация

Эта настройка необходима, если требуется двухфакторная аутентификация для получения одноразовых паролей при авторизации

- Двухфакторная авторизация - выбор второго фактора аутентификации при входе в веб-интерфейс и в клиент **RuDesktop**

  Доступные варианты:

  - **Отключена** - двухфакторная авторизация выключена
  - **Телефон (OTP)** - одноразовый код приходит по SMS на номер пользователя из его профиля

    Требует настроенного *SMS шлюз*
  - **Email (OTP)** - одноразовый код приходит на адрес электронной почты пользователя

    Требует настроенного *Настройки SMTP*
  - **Telegram (OTP)** - одноразовый код приходит в Telegram

    Требует настроенного *Настройки телеграм бота* и Telegram-токена пользователя в его профиле (либо включённой опции «Использовать токен бота Telegram из настроек при отправке OTP для всех пользователей»)
  - **MAX (OTP)** - одноразовый код приходит в мессенджер MAX

    Требует настроенного *Настройки MAX бота* и MAX-токена пользователя в его профиле (либо включённой опции «Использовать токен бота MAX из настроек при отправке OTP для всех пользователей»)
  - **Собственный сервер OTP** - одноразовый код выдаёт и проверяет сторонний сервис, к которому сервер обращается по HTTP

    Требует указанного URL сервиса - в профиле пользователя либо в блоке *Настройки собственного сервера OTP*

    Подробнее - в кейсе Настройка двухфакторной авторизации через собственный сервер OTP

Важно

Вариант доступен только на локальном сервере **RuDesktop**, в облачной версии он отсутствует

- **Аутентификатор (TOTP)** - одноразовый код генерируется приложением-аутентификатором на устройстве пользователя (Google Authenticator, Яндекс Ключ и аналоги)

  Не требует SMTP/SMS/мессенджеров

- **Электронный ключ (FIDO2)** - вход подтверждается аппаратным токеном FIDO2 (USB-ключ безопасности)
- **ЭЦП Рутокен (PKI)** - вход подтверждается электронной подписью на устройстве **Рутокен**

Важно

Для способов **Телефон**, **Email**, **Telegram** и **MAX**: если в профиле пользователя не указаны соответствующие контактные данные (номер телефона, e-mail, Telegram-токен, MAX-токен), одноразовый пароль не будет отправлен и пользователь не сможет войти

- Всегда запрашивать учётные данные при входе клиента через браузер, даже при наличии активной сессии - при активации клиента через браузер уже открытая сессия веб-интерфейса не засчитывается: пользователь должен ввести логин и пароль заново

Подсказка

Засчитывается только вход, выполненный **после** того, как клиент запросил активацию

Поэтому подтверждать вход повторно за одну активацию не потребуется

Подсказка

По умолчанию опция выключена: если пользователь уже авторизован в браузере, активация клиента подтверждается имеющейся сессией без повторного ввода логина и пароля

Включайте опцию на устройствах общего пользования, где браузером пользуются несколько человек

- Использовать токен бота Telegram из настроек при отправке OTP для всех пользователей - использовать общий токен Telegram-бота из системных настроек для отправки одноразовых кодов
- Использовать токен бота MAX из настроек при отправке OTP для всех пользователей - использовать общий токен MAX-бота из системных настроек для отправки одноразовых кодов
- Использовать URL собственного сервера OTP из настроек при отправке OTP для всех пользователей - использовать общий адрес стороннего сервиса OTP из блока *Настройки собственного сервера OTP* вместо адреса, заданного у каждого пользователя

> **Важно**
>
> Опция отображается только на локальном сервере **RuDesktop**

- Срок действия ключей для входа - срок действия ключей входа TOTP/FIDO2/PKI в днях

  По истечении пользователь будет вынужден перерегистрировать ключ

> **Подсказка**
>
> Значение `0` (по умолчанию) - срок действия не ограничен

- Напоминание об истекающем ключе входа - за сколько дней до истечения ключа пользователь получит уведомление о необходимости перерегистрации

  Значение по умолчанию - 14 дней

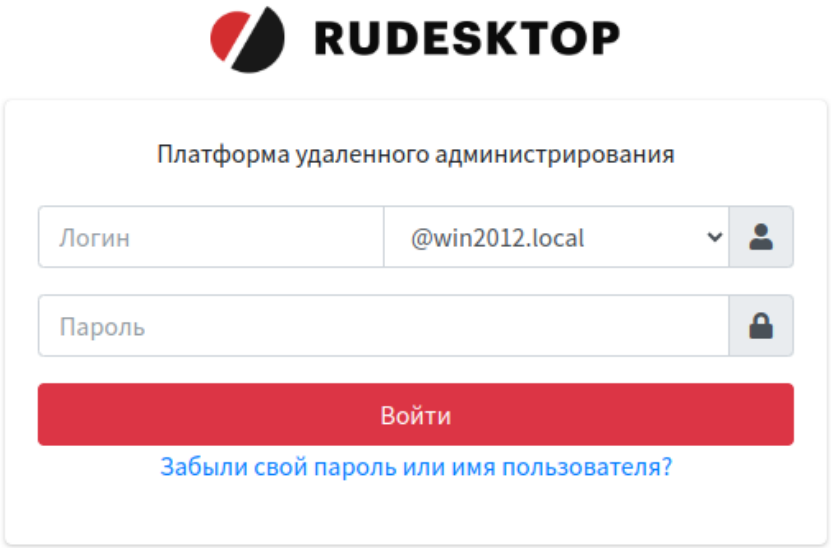
> **Подсказка**
>
> Значение `0` отключает напоминание

- Авторизация по умолчанию - выбор домена авторизации, который будет подставлен по умолчанию на странице входа в веб-интерфейс и в клиент

  Список вариантов формируется автоматически из подключённых источников аутентификации:

  - **Локальный** - встроенная база пользователей **RuDesktop**
  - **Имя домена** - каждый из доменов LDAP, добавленных на странице *Домены* с активным флагом `Включить`

- **Имя Realm** - каждый из подключённых **Keycloak** Realm со страницы *Keycloak*



Важно

Выбор домена/Realm доступен только при наличии настроенных и включённых *доменов* или конфигураций *Keycloak*

- Включить Captcha при входе в админ панель - данная настройка активирует использование `Captcha` для дополнительной защиты при авторизации в веб-интерфейсе

Важно

При отсутствии доступа к сервису https://smartcaptcha.yandexcloud.net/validate, капча не будет отображаться и проверяться

- Включить Captcha при регистрации в админ панели - данная настройка активирует использование `Captcha` на странице регистрации в веб-интерфейсе
- Клиентский ключ Yandex SmartCaptcha - это уникальный ключ, предоставляемый сервисом Yandex для интеграции технологии SmartCaptcha, необходимый для проверки и обработки Captcha при входе в веб-интерфейс

Важно

Убедитесь, что этот ключ правильно настроен для корректной работы Captcha

- Серверный ключ Yandex SmartCaptcha - это уникальный ключ, который используется для серверной проверки ответов от Yandex SmartCaptcha

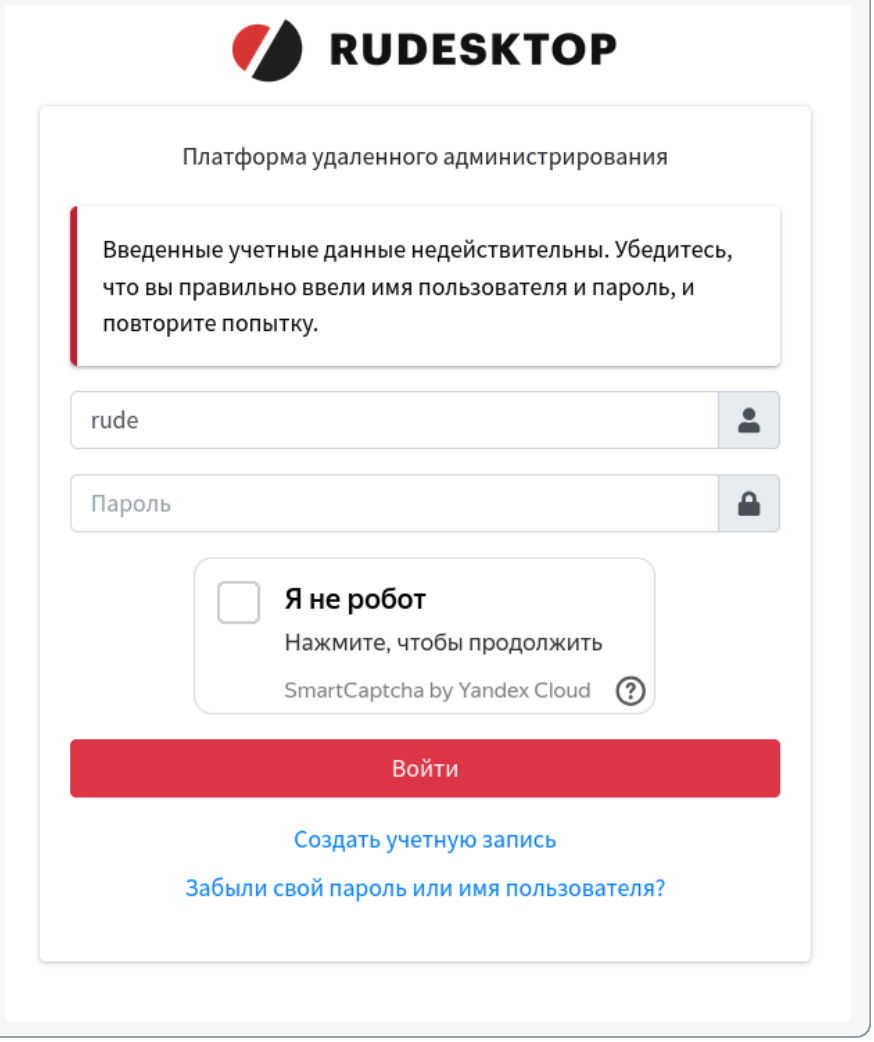
Важно

Он необходим для безопасной обработки и валидации Captcha на стороне сервера, обеспечивая дополнительную защиту от злоупотреблений

- Попытки входа до появления капчи - количество последовательных неудачных попыток входа, после которых пользователь должен пройти проверку через Captcha

Примечание

После нескольких неудачных попыток авторизации появится Captcha, которую необходимо пройти для успешной авторизации в веб-интерфейсе



Важно

Настройка данного значения помогает защитить административную панель от автоматических атак методом подбора паролей

- Попытки входа до блокировки IP - количество неудачных попыток аутентификации, после которого IP-адрес пользователя будет заблокирован

Подсказка

Значение `0` отключает блокировку IP

Значение по умолчанию - `10` попыток

Подсказка

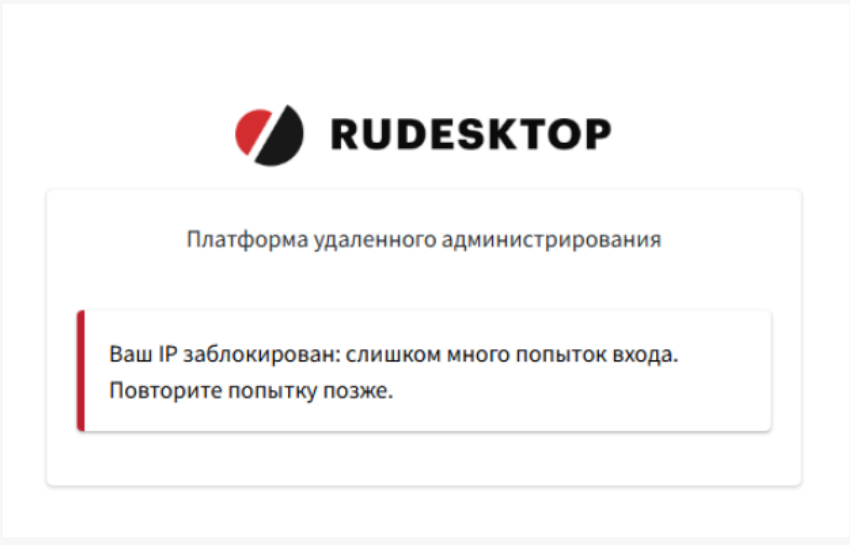
Для оповещения ответственных сотрудников включить **Уведомлять о блокировке IP при входе** в правиле *уведомлений*

Раздел уведомлений доступен в версии **Управление конфигурациями (UEM)**

Примечание

После блокировки IP-адреса будет отображено соответствующее сообщение

Возможность авторизации будет приостановлена



Подсказка

Чтобы сбросить блокировку IP-адреса, необходимо выполнить команду *rude axes_reset_ip*

- Время блокировки IP (в часах) - длительность блокировки IP-адреса в часах

  Допускаются дробные значения, например `0.5` (30 минут)

  Значение по умолчанию - `0.5`

Настройки SMTP

Эта настройка необходима для работы двухфакторной аутентификации, если выбран способ через `Email (OTP)`, а также для отправки различных уведомлений на почту (приглашения, сброс паролей, сообщения о событиях аудита)

- SMTP сервер - адрес SMTP-сервера, например `smtp.yandex.ru`
- SMTP порт - порт SMTP-сервера

  Стандартные значения: `25` (без шифрования), `465` (SSL), `587` (STARTTLS)
- SMTP имя пользователя - имя пользователя для авторизации на SMTP-сервере
- SMTP пароль - пароль или пароль приложения для авторизации на SMTP-сервере
- SMTP использовать TLS - включение шифрования (TLS/STARTTLS) при подключении к SMTP-серверу
- Отправитель по умолчанию - адрес, который будет указан в поле `From` отправляемых писем

  По умолчанию `no-reply@localhost`
- Получатель по умолчанию - адрес, на который отправляется тестовое сообщение и системные уведомления, не привязанные к конкретному пользователю
- Отправка тестового сообщения - кнопка отправки тестового письма на адрес из поля Получатель по умолчанию для проверки настроек

Если тестовое письмо не отправлено, рядом с кнопкой появится сообщение об ошибке. Например, если SMTP-сервер отклонил вход, проверьте имя пользователя и пароль

Настройки телеграм бота

Эта настройка необходима для работы двухфакторной аутентификации, если выбран способ через `Telegram (OTP)`, а также для отправки различных уведомлений в Telegram

- Токен для телеграм бота - токен используемого Telegram-бота, полученный у `@BotFather`

- ID чата телеграм бота - идентификатор чата для отправки общих уведомлений (системные сообщения, не относящиеся к конкретному пользователю)
- Отправка тестового сообщения - отправка тестового сообщения в указанный чат для проверки настроек

Настройки MAX бота

Эта настройка необходима для работы двухфакторной аутентификации, если выбран способ через `MAX (OTP)`, а также для отправки различных уведомлений в мессенджер MAX

- Токен для MAX бота - токен используемого MAX-бота
- ID чата MAX бота - идентификатор чата для отправки общих уведомлений
- Отправка тестового сообщения - отправка тестового сообщения в указанный чат для проверки настроек

Настройки собственного сервера OTP

Эта настройка необходима для работы двухфакторной аутентификации, если выбран способ через `Собственный сервер OTP`

- URL собственного сервера OTP - адрес стороннего сервиса, который отправляет и проверяет одноразовые пароли

  Допускаются только схемы `http` и `https`

Подсказка

Адрес применяется, когда в блоке *Аутентификация* включена опция Использовать URL собственного сервера OTP из настроек при отправке OTP для всех пользователей

Иначе используется адрес, заданный при регистрации ключа у конкретного пользователя

Важно

Блок отображается только на локальном сервере **RuDesktop**

Требования к стороннему сервису - формат запроса, формат ответа и таймаут - описаны в кейсе Настройка двухфакторной авторизации через собственный сервер OTP

SMS шлюз

Эта настройка необходима для работы двухфакторной аутентификации, если выбран способ через `Телефон (OTP)`, а также для отправки различных уведомлений по SMS

- SMS шлюз - выбор используемого SMS-шлюза

  Поддерживается провайдер `sms.ru`

  Значение `Нет` отключает отправку SMS

- Отправитель - имя или номер отправителя, зарегистрированный у провайдера
- Ключ API - ключ API для подключения к SMS-шлюзу

Настройки мостов

Блок управляет правилами выбора *моста* при подключении клиентов

- Адрес основного моста - адрес моста, через который подключаются клиенты по умолчанию

  По умолчанию указывается адрес самого главного сервера

  При наличии географически распределённых мостов адрес может уточняться автоматически на стороне сервера

- Порт подключения клиентов - порт, который прописывается клиентам в установочных скриптах и пакетах (`.sh`, `.msi`, `.apk`)

  По умолчанию совпадает с портом сервера (443)

  Значение нужно менять при *Разделении портов*, когда клиентский трафик вынесен на отдельный порт (например, 33443) - иначе клиенты будут подключаться на порт веб-интерфейса

- Тип подключения - способ подключения клиентов **RuDesktop**:
  - **Авто** - способ подключения определяется настройками самого клиента **RuDesktop**
  - **Мост** - клиент всегда подключается через мост, независимо от настроек на клиенте
  - **NAT** - клиент всегда устанавливает прямое подключение через NAT, независимо от настроек на клиенте

Карты

Блок настраивает интеграцию с **Яндекс.Картами** для отображения устройств на странице *Карты*

- Яндекс Карты API-ключ - ключ доступа к API **Яндекс.Карт**, выданный в кабинете разработчика Яндекс

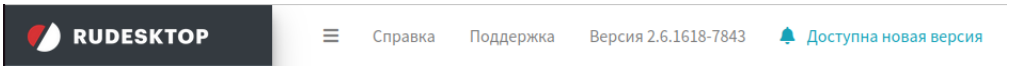
  Без ключа карта не загрузится

Обновления

Блок управляет уведомлениями о выпусках новых версий сервера **RuDesktop**

- Автоматически проверять обновления - если настройка активна, **RuDesktop** периодически проверяет наличие новой версии

При обнаружении на главной странице в шапке появляется подсказка с предложением обновиться



Настройки HelpDesk

Блок настраивает перенаправление пользователей из клиента **RuDesktop** на внешнюю страницу техподдержки (например, корпоративный портал заявок)

- Получать информацию о клиенте (query-параметры) - при включении к URL перенаправления добавляются query-параметры с данными об устройстве - это позволяет внешней системе автоматически предзаполнить форму заявки

  Включено по умолчанию

  Передаются три параметра:

  - `id` - ID устройства **RuDesktop**, например `385472910`
  - `hostname` - имя компьютера, например `support-105`
  - `address` - сетевой адрес устройства, например `192.168.1.45:21118`

  Пример адреса, на который попадёт пользователь: `https://helpdesk.corp.ru/ticket?id=385472910&hostname=support-105&address=192.168.1.45%3A21118`

  Примечание

  Устройство определяется по IP-адресу, с которого выполнен запрос. Если однозначно сопоставить адрес с устройством не удалось, перенаправление срабатывает без параметров

  URL перенаправления указывается без собственной строки параметров: query-параметры дописываются к адресу целиком, поэтому символ ? в самом адресе исказит результат

- Ссылка для перенаправления в тех.поддержку - URL внешней страницы техподдержки, на который будет перенаправлен пользователь

Подсказка

При нажатии на кнопку Открыть в клиенте **RuDesktop** произойдёт перенаправление на указанный адрес

Если поле пустое, кнопка не отображается

Настройки Ansible

Блок задаёт параметры выполнения задач Ansible (политики, проигрывание плейбуков на устройствах)

- Автоматическое определение потоков - при включении количество одновременно выполняемых задач рассчитывается автоматически по характеристикам сервера

  При выключении используется значение из поля Количество потоков

  Включено по умолчанию

- Количество потоков - количество одновременно выполняемых задач Ansible

  Используется только при выключенном автоопределении

  Значение по умолчанию - `10`

- Таймаут выполнения задачи - максимальное время выполнения одной задачи Ansible в секундах

  По истечении задача прерывается и помечается как неудачная

  Значение по умолчанию - `300` секунд (5 минут)

- Показывать системные задачи - при включении на странице *Задачи* отображаются также системные задачи (Системные задачи создаются через обращение в техподдержку на выполнение политик)

  Выключено по умолчанию - в списке видны только пользовательские задачи

Настройки логов

Блок управляет подробностью внутренних логов и дублированием событий аудита во внешний *syslog*

- Подробные логи синхронизации AD - при включении синхронизация с Active Directory дополнительно фиксирует в логе каждый объект (пользователя, группу, устройство) с результатом обработки

  Логи доступны во вкладке **«Логи синхронизации»** на странице *Домены*

  Используйте для диагностики, в обычном режиме оставляйте выключенным - иначе лог быстро растёт

- Записывать статус подключений в syslog - дублирует события подключений со страницы *Сессии* в системный syslog
- Записывать результаты запуска политик в syslog - дублирует результаты выполнения политик со страницы *Политики* в syslog
- Записывать события аутентификации админ панели в syslog - дублирует события входа в веб-интерфейс со страницы *Входы в систему* в syslog

- Записывать события HTTP запросов в syslog - дублирует все HTTP-запросы к веб-интерфейсу со страницы *HTTP запросы* в syslog
- Записывать события CRUD (изменения объектов) в syslog - дублирует все изменения объектов со страницы *Объекты* в syslog
- Записывать события Экспорта в syslog - дублирует действия экспорта данных в файлы из любых страниц веб-интерфейса в syslog
- Исключения из логирования — пути запросов, которые не нужно записывать в журнал аудита. Можно указать префикс пути или регулярное выражение; проверка начинается с начала пути

  Значения разделяются запятой. Например, `/peers/get_peer_statuses/, /audit/requestevent/` исключает запросы к этим путям и их продолжениям.

  Для пути с числовым идентификатором использовать выражение `/api/v2/addressbook/books/[0-9]+/tags/`. Оно подходит, например, для `/api/v2/addressbook/books/12/tags/`.

  Если нужно точное совпадение пути без продолжения, добавить `$` в конце выражения. Указывать путь, начинающийся с `/`, без доменного имени.

Подсказка

По умолчанию все настройки логов в syslog выключены - включайте только те события, которые требуются по политике аудита вашей организации

Настройки баннера (Клиент)

Эта настройка позволяет отобразить баннер в клиенте **RuDesktop**

- Включить - активация или деактивация настройки
- Ссылка на изображение баннера - указание URL-адреса самого изображения баннера

Подсказка

Поддерживаемые форматы изображения: jpg, png и webp
Рекомендуемые размеры изображения: 362 x 178 пикселей
Пример ссылки: https://rudesktop.ru/banner.jpg

- Ссылка, на которую ведёт баннер при клике - указание полного URL-адреса, на который перенаправляет баннер при нажатии на него

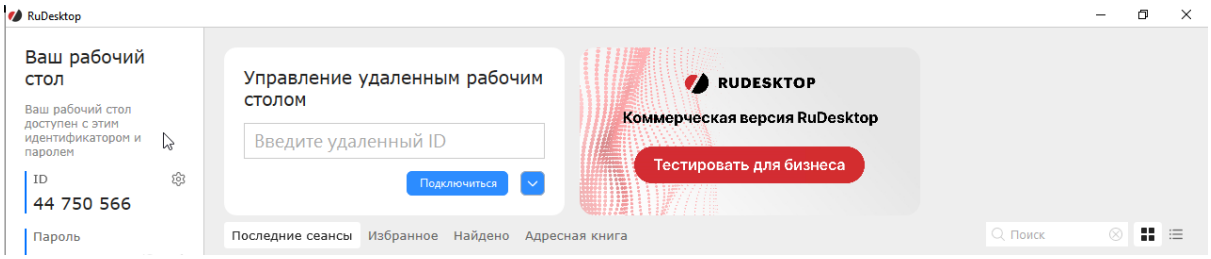
Подсказка

Пример ссылки: https://rudesktop.ru/

Важно

Баннер будет отображаться только на клиентах под управлением операционной системы Windows

Пример отображения баннера в клиенте:



При клике на баннер указанная ссылка откроется в браузере

Настройки баннера (Сайт)

Эта настройка позволяет отобразить баннер на странице *Панель управления*

- Включить - активация или деактивация настройки
- Ссылка на изображение баннера - указание URL-адреса самого изображения баннера

Подсказка

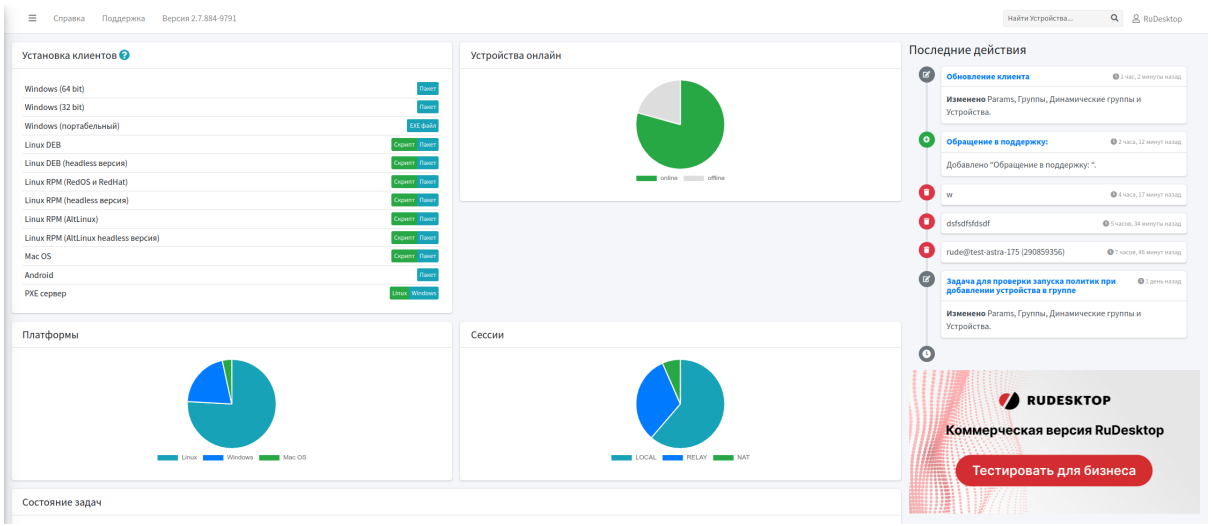
Поддерживаемые форматы изображения: jpg, png и webp
Рекомендуемые размеры изображения: 1300 × 232 пикселя
Пример ссылки: https://rudesktop.ru/banner.jpg

- Ссылка, на которую ведёт баннер при клике - указание полного URL-адреса, на который перенаправляет баннер при нажатии на него

Подсказка

Пример ссылки: https://rudesktop.ru/

Пример отображения баннера в веб-интерфейсе:



При клике на баннер указанная ссылка откроется в браузере

Настройки клиента

Этот блок задаёт ограничения на длительность сессий удалённого доступа в клиенте **RuDesktop**, чтобы автоматически прерывать неактивные подключения и ограничивать максимальное время сессии, а также определяет правила формирования идентификаторов устройств

- Не учитывать таймаут сессии в режиме просмотра - при включении бездействие в режиме просмотра экрана не учитывается, сессия не будет прерываться по таймауту
- Не учитывать таймаут сессии при голосовом чате - при включении бездействие во время голосового чата не учитывается
- Таймаут сессии при неактивности оператора - время прерывания сессии при бездействии оператора, в минутах

Подсказка

Значение `0` отключает таймаут - сессия не прерывается при простое

- Максимальная длительность сессии - максимальная длительность одной сессии удалённого доступа, в минутах

Подсказка

Значение `0` снимает ограничение - сессия может длиться неограниченное время

- Выдавать новый ID устройства при смене имени его хоста - при изменении hostname устройство регистрируется как новое и получает новый идентификатор

  Полезно, если имена хостов используются как уникальные идентификаторы парка устройств

Примечание

На устройствах **macOS** выдача нового ID при изменении только имени хоста не выполняется

Важно

Настройки **«Выдавать новый ID устройства при смене имени его хоста»** и **«Использовать hostname в качестве ID устройства»** взаимоисключающие

При включении одной переключатель второй становится недоступным

Для смены режима сначала выключить текущую настройку, затем включить нужную и сохранить изменения

- Использовать hostname в качестве ID устройства - вместо числового ID устройству присваивается его hostname

Важно

- Имя хоста должно быть уникальным в инфраструктуре - иначе при подключении устройств с одинаковым hostname возникнет конфликт идентификаторов
- Для устройств **Android** опция не применяется, у них всегда остаётся числовой ID
- При деактивации опции устройствам, у которых ID равен имени хоста, выдаётся новый числовой ID (прежние числовые ID не восстанавливаются)

Важно

Любая смена ID устройства (включение или выключение настроек выше, переименование хоста) сбрасывает на устройстве мастер-пароль, а прежняя запись устройства остаётся на сервере со старым ID

Подробнее о сценариях применения и подводных камнях - в кейсе Использование hostname в качестве ID устройства

Видеозаписи

Этот блок задаёт параметры хранения видеозаписей сессий удалённого доступа, создаваемых функцией *мониторинга*

- Путь для хранения видеозаписей - путь к каталогу на сервере, в котором сохраняются видеозаписи

  По умолчанию используется `/var/lib/rudesktop/video-records`

  Важно

  При изменении пути убедитесь, что у пользователя `rudesktop` есть права на запись в указанный каталог, иначе видеозаписи не будут сохраняться

- Размер папки, указанной в параметре «Путь для хранения видеозаписей» - суммарный объём **всех** файлов в каталоге хранения, а не только видеозаписей

  Примечание

  Поле информационное и недоступно для редактирования

  Значение вычисляется при открытии страницы

  Если каталог получить не удалось, вместо размера отображается причина: **Путь для хранения видеозаписей не задан**, **Каталог не существует** или **Указанный путь не является каталогом**

  При непредвиденной ошибке в обоих полях отображается **Не удалось получить данные**

- Количество записей - количество файлов `.webm` и `.mp4` в каталоге хранения

  Примечание

  Поле информационное и недоступно для редактирования

Если каталог получить не удалось, поле показывает `0`

Подсказка

Оба поля помогают оценить, сколько места занимают видеозаписи, и решить, нужна ли очистка

Удалить устаревшие записи можно политикой *Обслуживание сервера* или командой *clean_video_records*

- Качество видео - качество сохраняемых видеозаписей

  Доступные варианты:

  - **Низкое** - минимальный размер файла, рекомендуется для длительного хранения
  - **Среднее** - компромисс между размером и детализацией
  - **Высокое** - максимальная детализация, наибольший размер файла

Подсказка

Чем ниже качество, тем меньше размер видеозаписи на диске

PXE

Блок задаёт параметры PXE-меню мультизагрузки, которое отображается на устройстве при *установке ОС по сети*

- Таймаут меню PXE, секунд - время в секундах, по истечении которого в PXE-меню автоматически загружается образ по умолчанию, если пользователь не сделал выбор вручную

  Значение по умолчанию - `30`

Примечание

Образ по умолчанию назначается на странице *Образы OS*

Подробнее о работе меню - раздел «Мультизагрузка по PXE»

Важно

Чтобы новое значение таймаута вступило в силу, необходимо опубликовать или переопубликовать любой образ ОС, либо сменить образ по умолчанию - только после этого PXE-меню перегенерируется с обновлённым таймаутом

Обновления ОС

Блок задаёт предел размера и место хранения для автоматического скачивания пакетов при *подготовке обновлений Windows*

- Максимальный размер пакета обновления, ГБ - пакеты крупнее этого размера не скачиваются с серверов Microsoft. Размер пакета известен заранее по данным сканирования, поэтому превышение обнаруживается до начала загрузки, а текст ошибки в поле **«Ошибка скачивания»** указывает фактический размер и предел

  Значение по умолчанию - `5`. Значение `0` снимает ограничение

  Примечание

  Накопительные обновления Windows могут занимать более 10 ГБ. Перед увеличением предела убедиться, что на сервере достаточно свободного места

- Репозиторий для пакетов обновлений - *репозиторий*, в который сохраняются скачанные пакеты. Перед скачиванием проверяется свободное место в каталоге репозитория с учётом резерва в 1 ГБ; при нехватке в поле **«Ошибка скачивания»** указываются требуемый и доступный объём

  Значение по умолчанию - служебный репозиторий `files`

  Подсказка

  Чтобы хранить пакеты на отдельном диске, создать репозиторий, не отмечая в нём прав доступа, смонтировать диск в его каталог внутри хранилища файлов сервера (`/var/lib/rudesktop/media/<короткое имя>`) и выбрать этот репозиторий в настройке. Скачивание и сборка пакета выполняются внутри каталога репозитория, поэтому дополнительного места на системном диске не требуется

  Примечание

  В списке только репозитории, файлы которых устройства могут скачать по подписанной ссылке без входа: без прав доступа, не скрытые и не служебные (кроме `files`). Репозитории с подключённым сетевым диском (Samba, SFTP, WebDAV) также отсутствуют: такие диски подключаются только для чтения, а их файлами управляет синхронизация диска

- Каталог репозитория пакетов — точка монтирования - включить, если в каталог репозитория смонтирован отдельный диск. Пока диск не примонтирован (например, после перезагрузки), скачивание отклоняется с ошибкой **«Каталог репозитория не примонтирован»** вместо записи на системный диск под точкой монтирования

Значение по умолчанию - выключено

Сохранение настроек

После внесения изменений в любом из блоков необходимо нажать на кнопку Сохранить внизу страницы - без сохранения настройки не применятся

Примечание

Часть настроек применяется сразу после сохранения, часть - при следующем подключении клиентов или запуске соответствующих компонентов системы

Сроки хранения журналов

В блоке **«Настройки логов»** задаются отдельные сроки хранения подробных логов задач, собранных событий, HTTP-запросов, результатов задач и остальных событий аудита

Примечание

Значение **0** отключает автоматическое удаление только для соответствующей категории

Порядок настройки и значения по умолчанию описаны на странице *Сроки хранения журналов*

2.16.2 Keycloak

Описание страницы

Keycloak — это сервер аутентификации и авторизации с открытым исходным кодом, который обеспечивает безопасность и управление доступом для веб-приложений и сервисов

Как это работает

На странице создаётся конфигурация подключения к серверу **Keycloak** для авторизации пользователей и синхронизации данных

После настройки **Keycloak** может использоваться как поставщик единого входа (SSO), при этом пользователь проходит проверку учетных данных в **Keycloak**, а сервер **RuDesktop** получает результат авторизации и данные пользователя, включая группы, из токена или при синхронизации

Группы из **Keycloak** можно связать с локальными группами **RuDesktop**, чтобы назначать пользователям права **RuDesktop** на основании членства в группах **Keycloak**

Сценарии использования

RuDesktop поддерживает три режима интеграции с **Keycloak**. Перед созданием конфигурации стоит определиться, какой режим нужен — это влияет на набор включаемых чек-боксов и на то, какие шаги настройки **Keycloak** обязательны

Только SSO авторизация

Пользователи входят через единую форму **Keycloak**, но списки пользователей и групп в **RuDesktop** заранее не наполняются — учётная запись создаётся при первом входе

Что включать в RuDesktop:

- Включить — да
- Использовать для SSO авторизации — **да**
- Использовать для синхронизации — нет

Что настроить в Keycloak: клиент типа OpenID Connect (см. *Создание Clients*) и маппер **Group Membership** (см. *Настройка передачи групп для SSO*). Сервисный аккаунт не нужен

Только синхронизация

Пользователи и группы переносятся в **RuDesktop** по расписанию, вход выполняется по локальным учётным данным без перенаправления на **Keycloak**

Что включать в RuDesktop:

- Включить — да
- Использовать для SSO авторизации — нет
- Использовать для синхронизации — **да**

Что настроить в Keycloak: клиент OpenID Connect и сервисный аккаунт с ролями `realm-management` (см. *Настройка сервисного аккаунта*). Маппер групп не нужен — данные забираются через **API Keycloak**

SSO авторизация и синхронизация одновременно

Пользователи входят через **Keycloak**, а списки пользователей и групп параллельно синхронизируются в локальную базу

Что включать в RuDesktop:

- Включить — да
- Использовать для SSO авторизации — **да**
- Использовать для синхронизации — **да**

Что настроить в Keycloak: все шаги из обоих предыдущих режимов — клиент OpenID Connect, маппер **Group Membership** и сервисный аккаунт

Важно

На сервере **RuDesktop** одновременно может быть только одна конфигурация **Keycloak** с включённым параметром Использовать для SSO авторизации. Число конфигураций с включённой синхронизацией не ограничено — можно одновременно синхронизировать пользователей из нескольких Realms

Подготовка Keycloak

Для интеграции необходимо:

- Установить и настроить сервер **Keycloak**

Примечание

Руководство по установке Keycloak: https://www.keycloak.org/guides#server

- Создать клиентское приложение в Keycloak, чтобы получить конфигурационные данные для аутентификации и авторизации
- Настроить приложение для использования конфигурационных данных Keycloak

Настройка Keycloak

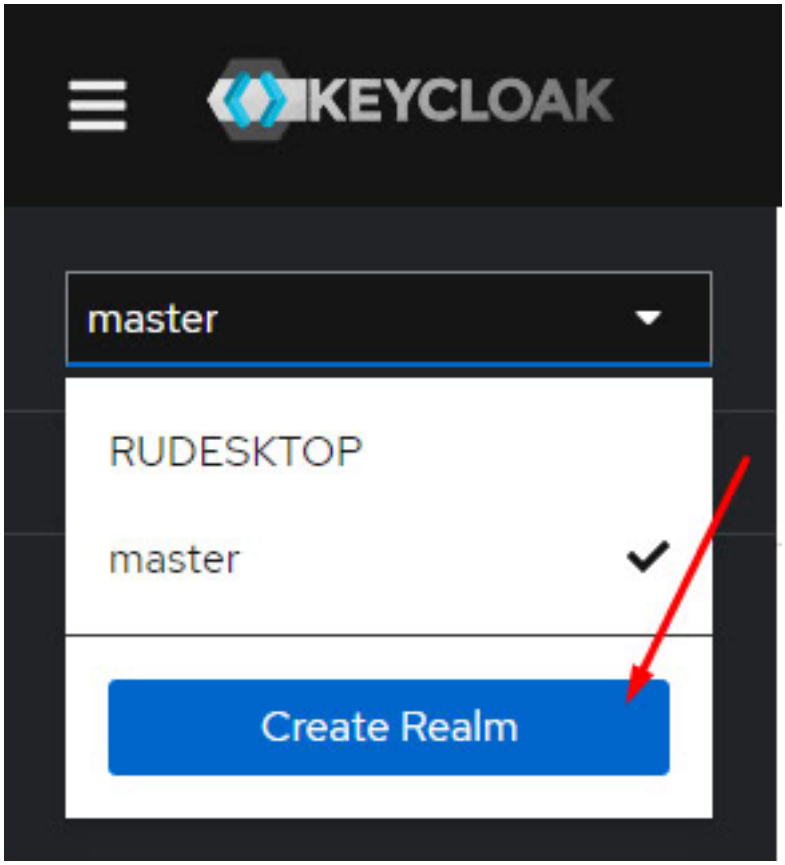
Примечание

Инструкция актуальна для **Keycloak версии 19** и выше с новой административной панелью. В более ранних версиях названия вкладок и расположение элементов могут отличаться, но смысл настроек остаётся прежним

Создание Realm

Realm (Изолированная область Keycloak, в которой управляются пользователи, роли, группы и клиенты) создаётся отдельно для интеграции с **RuDesktop**

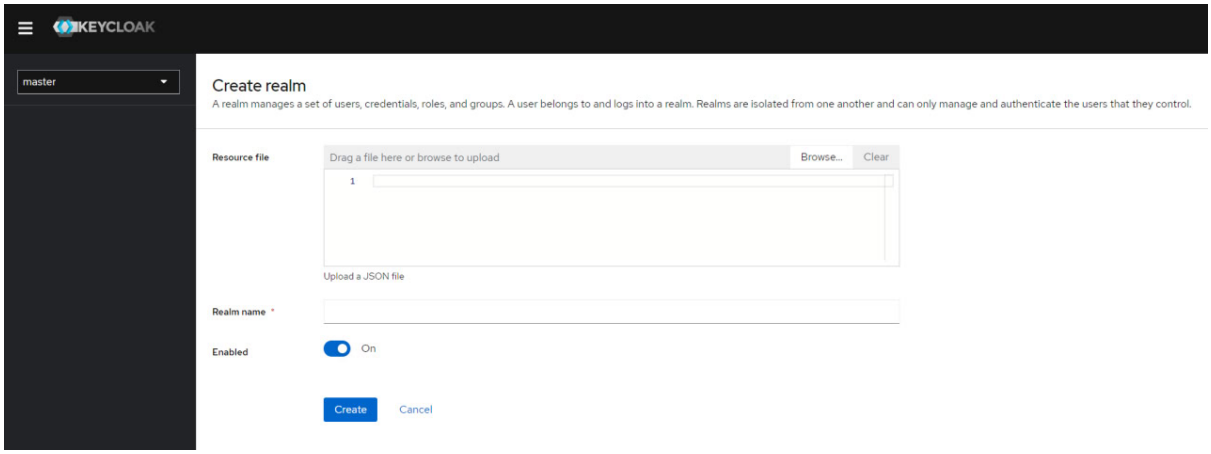
1. Войти в административную панель **Keycloak** под учётной записью администратора
2. Открыть выпадающий список Realm в левом верхнем углу панели
3. Нажать на кнопку Create Realm



4. В поле **Realm name** ввести название нового Realm

> **Примечание**
>
> Это же значение позже потребуется указать в поле Название Realm при создании конфигурации в **RuDesktop**

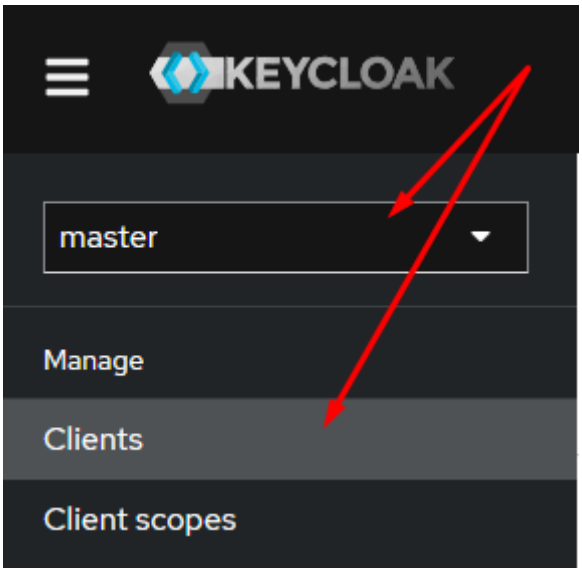
5. Убедиться, что переключатель **Enabled** включён
6. Нажать на кнопку Create



Создание Clients

Client (Запись о приложении, которому Keycloak разрешает запрашивать токены и авторизовать пользователей) создаётся для **RuDesktop** как клиент типа OpenID Connect

1. Войти в административную панель **Keycloak**
2. Убедиться, что в выпадающем списке слева выбран нужный Realm
3. Открыть раздел Clients в левом меню



4. Нажать на кнопку Create client
5. Во вкладке General Settings заполнить поля:

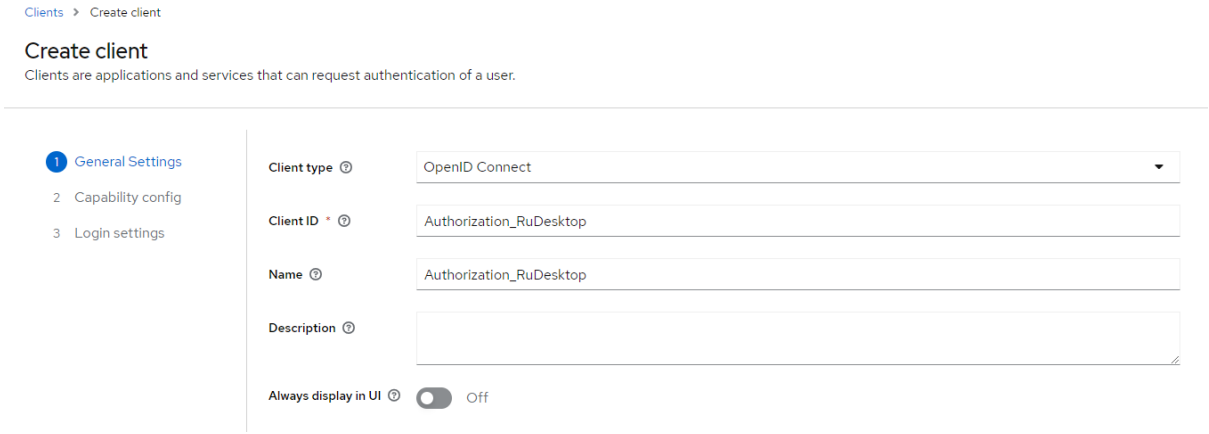
    5.1. **Client type** — выбрать значение `OpenID Connect`

    5.2. **Client ID** — ввести уникальный идентификатор клиента, например `rudesktop`

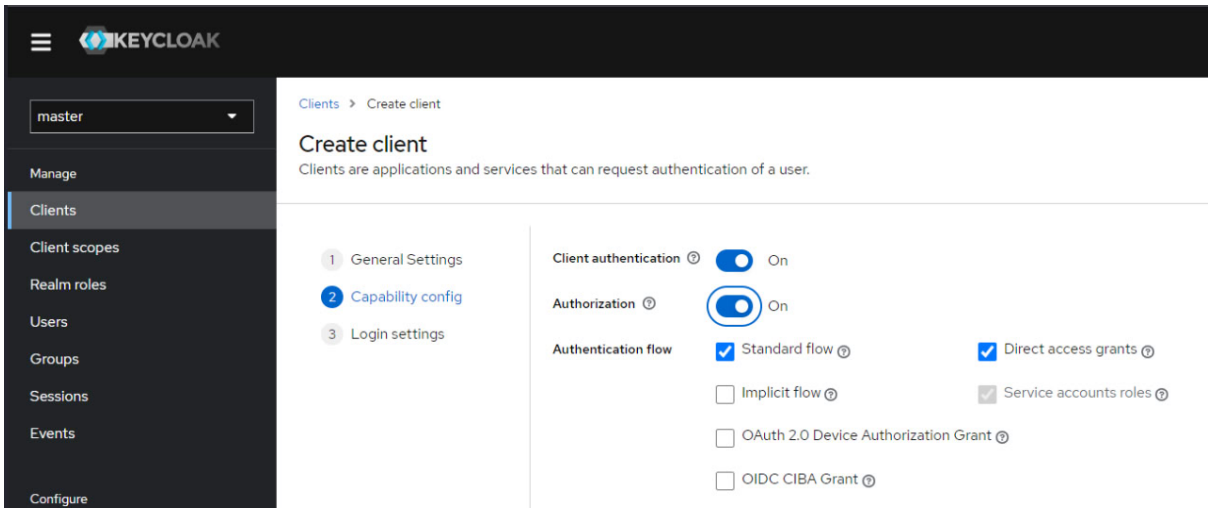
Примечание

Это же значение позже потребуется указать в поле ID клиента с правами на чтение при создании конфигурации в **RuDesktop**

5.3. **Name** — указать понятное название клиента



6. Нажать на кнопку Next и перейти во вкладку Capability config
7. Во вкладке Capability config настроить переключатели:
   - **Client authentication** — включить (нужно для генерации **Client Secret**, по которому **RuDesktop** подтверждает подлинность перед **Keycloak**)
   - **Standard flow** — включить (по этому потоку работает SSO **RuDesktop**)
   - **Service accounts roles** — включить, если планируется использовать синхронизацию пользователей и групп через **API Keycloak** (параметр **Использовать для синхронизации** в **RuDesktop**)
   - Остальные переключатели оставить со значениями по умолчанию



8. Нажать на кнопку Next и перейти во вкладку Login settings

9. Во вкладке Login settings заполнить поля:

   9.1. **Root URL** — указать базовый адрес сервера **RuDesktop**, например `https://rudesktop.example.com`

   9.2. **Home URL** — указать адрес страницы, на которую возвращается пользователь после авторизации, например `https://rudesktop.example.com/admin/`

   9.3. **Valid redirect URIs** — указать точный адрес обработчика обратного вызова **RuDesktop**:

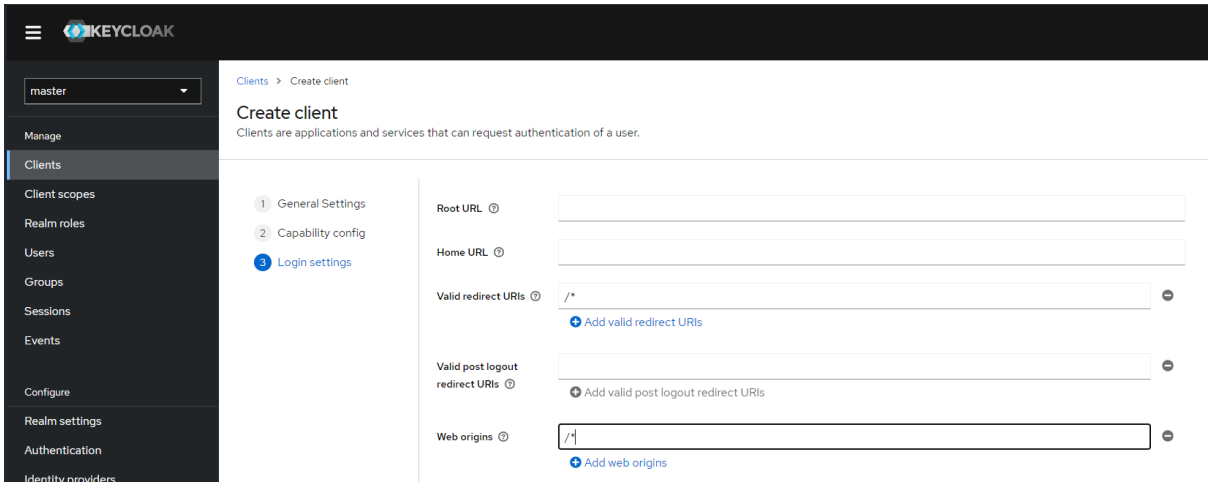
   ```
   https://rudesktop.example.com/keycloak/callback/
   ```

   Важно

   Не используйте маску `/*` или `*` в качестве значения **Valid redirect URIs** — это уязвимость класса *Open Redirect*. **RuDesktop** принимает callback только по адресу `/keycloak/callback/`, его и нужно указать целиком. Замените `rudesktop.example.com` на фактический домен вашего сервера **RuDesktop**; если адресов несколько, добавьте каждый отдельной строкой

   9.4. **Valid post logout redirect URIs** — указать страницу, на которую **Keycloak** возвращает пользователя после выхода, например `https://rudesktop.example.com/admin/login/`

   9.5. **Web origins** — указать домен **RuDesktop** для CORS, например `https://rudesktop.example.com` или значение `+` (использовать список из **Valid redirect URIs**)



10. Нажать на кнопку Save для завершения создания клиента

11. После сохранения **Keycloak** откроет страницу клиента. Перейти во вкладку Credentials и скопировать значение **Client Secret** — оно потребуется при создании конфигурации в **RuDesktop** (поле Ключ доступа к клиенту)

Важно

Client Secret отображается только в панели **Keycloak**. Если значение утеряно, его можно перегенерировать кнопкой **Regenerate**, но после этого потребуется обновить настройки и в **RuDesktop**

Настройка сервисного аккаунта

Примечание

Раздел нужен только при использовании синхронизации (параметр **Использовать для синхронизации** в **RuDesktop**). Если планируется только SSO авторизация — раздел можно пропустить

В режиме синхронизации **RuDesktop** обращается к **API Keycloak** от имени клиента, поэтому сервисному аккаунту нужно выдать права на чтение пользователей и групп

1. Открыть созданного клиента в разделе Clients
2. Перейти во вкладку Service accounts roles
3. Нажать на кнопку Assign role
4. В фильтре выбрать **Filter by clients** и назначить сервисному аккаунту следующие роли клиента `realm-management`:
   - `view-users` — для чтения списка пользователей и их атрибутов
   - `view-realm` — для чтения настроек Realm
   - `query-groups` — для чтения списка групп
   - `query-users` — для поиска пользователей по фильтрам

Важно

Без перечисленных ролей синхронизация завершится ошибкой `403 Forbidden`

Настройка передачи групп для SSO

Примечание

Раздел обязателен, если в **RuDesktop** параметр **Использовать для синхронизации** выключен — в этом случае группы пользователя берутся из токена. При включённой синхронизации группы запрашиваются через **API Keycloak**, и раздел можно пропустить

Чтобы группы пользователя передавались в JWT-токене, в **Keycloak** настраивается маппер **Group Membership**

1. Открыть созданного клиента в разделе Clients
2. Перейти во вкладку Client scopes
3. Открыть область с именем `<Client ID>-dedicated` (создаётся автоматически вместе с клиентом)
4. Перейти во вкладку Mappers и нажать на кнопку Configure a new mapper
5. Выбрать тип маппера **Group Membership**
6. Заполнить поля маппера:
   - **Name** — указать понятное имя, например `groups`
   - **Token Claim Name** — указать строго `groups`
   - **Full group path** — рекомендуется выключить (тогда группа передаётся как `support` — именно это значение нужно указывать в поле Группа в Keycloak локальной группы **RuDesktop**)
   - **Add to ID token** — включить
   - **Add to access token** — включить
   - **Add to userinfo** — включить
7. Нажать на кнопку Save

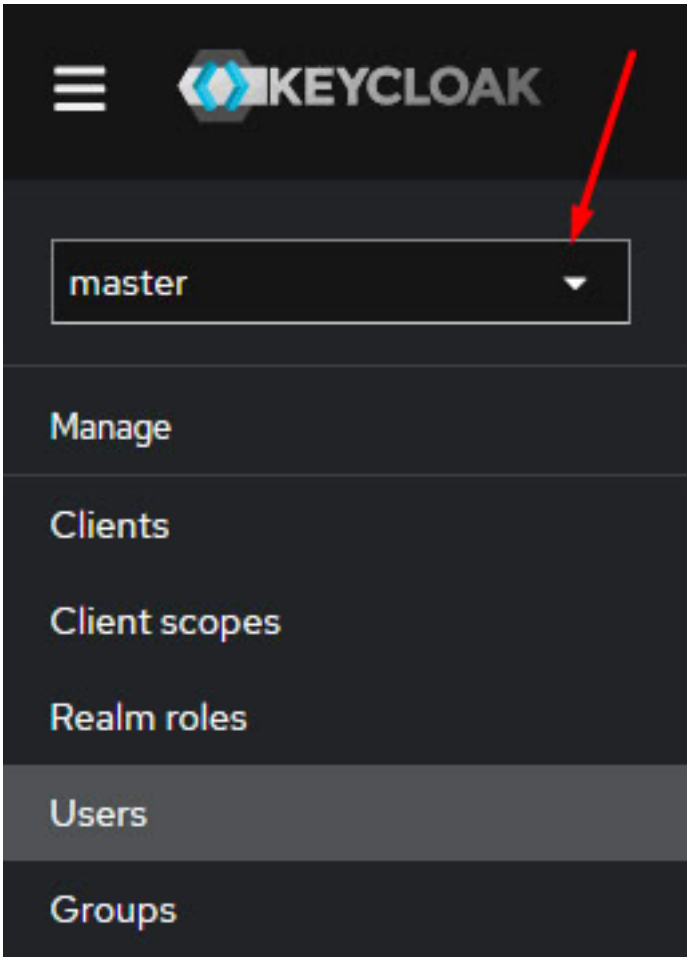
Важно

Если группы не передаются в токене и не доступны серверу **RuDesktop** при синхронизации, пользователь сможет пройти авторизацию, но попадёт только в группу по умолчанию

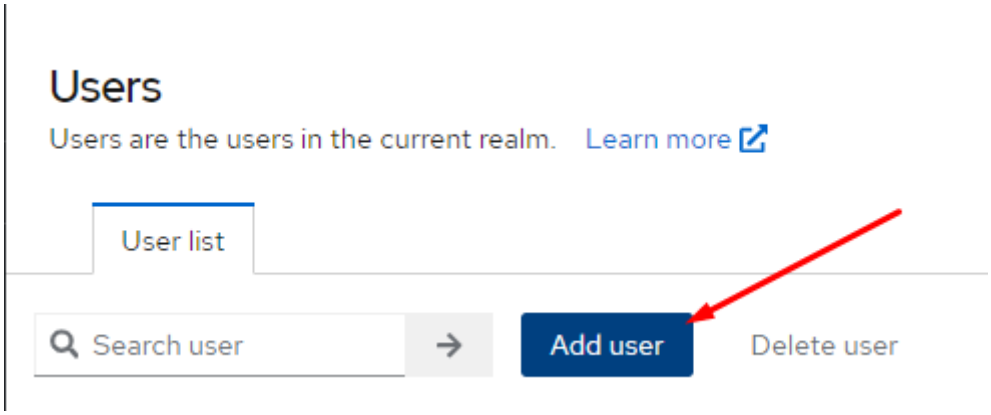
Создание Users

Этот раздел нужен, если в созданном Realm пока нет пользователей и их нужно создать вручную. При синхронизации с внешним каталогом (LDAP, Active Directory) пользователи появятся автоматически после настройки Identity Provider

1. Войти в административную панель **Keycloak**
2. Убедиться, что в выпадающем списке слева выбран нужный Realm
3. Открыть раздел Users в левом меню



4. Нажать на кнопку Add user



5. Заполнить форму создания пользователя:

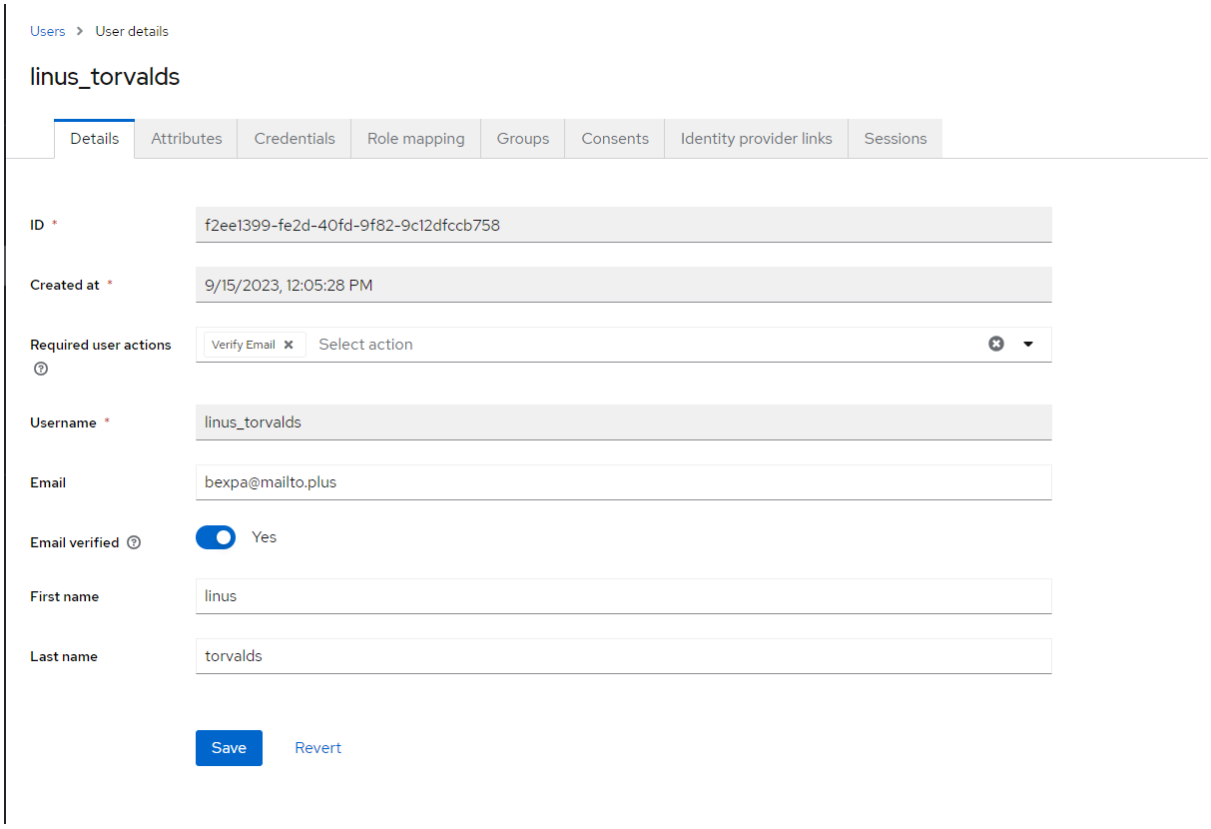
   5.1. **Username** — логин пользователя (используется для входа)

   5.2. **Email** — адрес электронной почты

   5.3. **First name** — имя

   5.4. **Last name** — фамилия

   5.5. Включить переключатель **Email verified**, если адрес уже подтверждён



6. Нажать на кнопку Create
7. На открывшейся странице пользователя перейти во вкладку Credentials и задать пароль:

    7.1. Нажать на кнопку Set password

    7.2. Ввести пароль и его подтверждение

    7.3. Переключатель **Temporary** оставить включённым, чтобы при первом входе пользователь сменил пароль самостоятельно

    7.4. Нажать на кнопку Save
8. При необходимости перейти во вкладку Groups и добавить пользователя в нужные группы **Keycloak** — именно эти группы будут передаваться в **RuDesktop** при авторизации

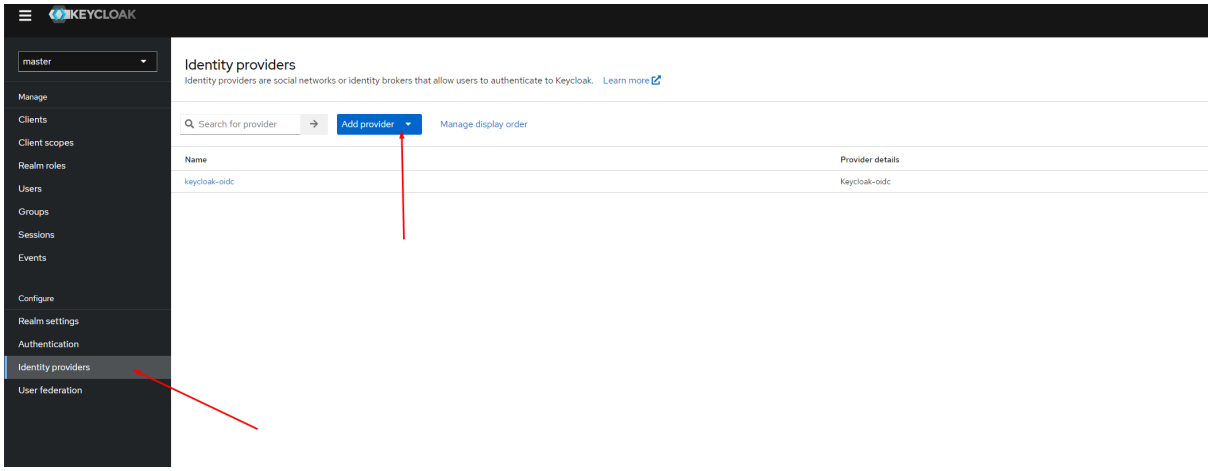
Настройка Identity Provider

Примечание

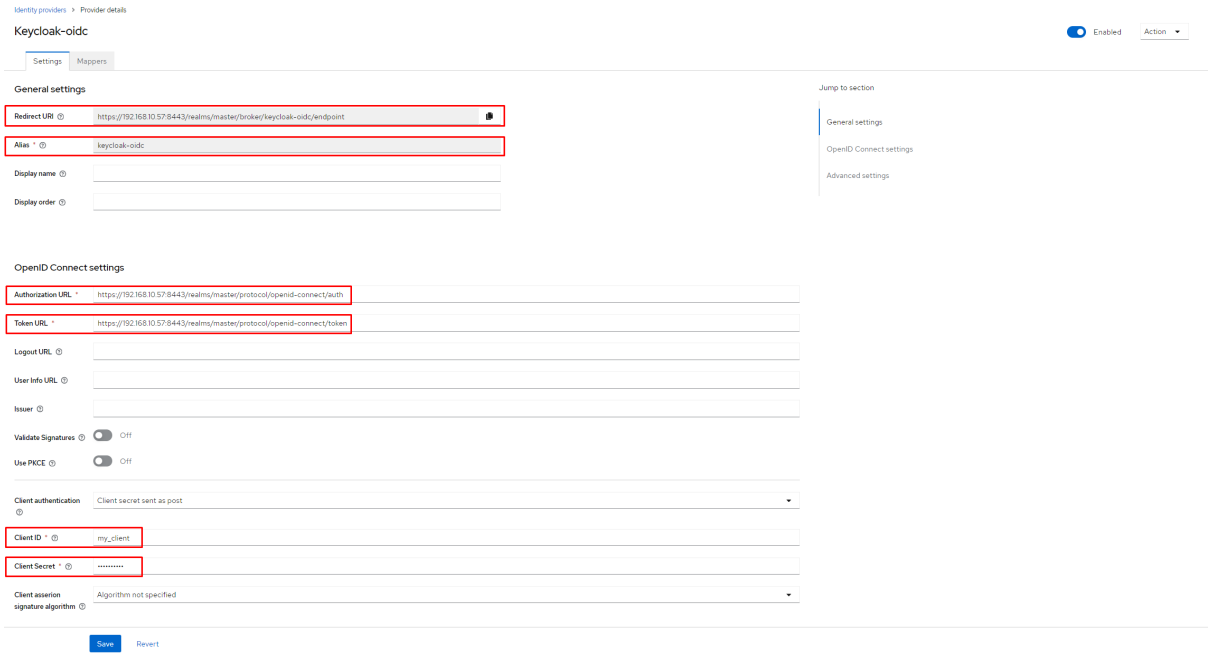
Раздел применяется, когда **Keycloak** должен делегировать проверку логина и пароля внешней системе (LDAP, Active Directory, другой OIDC-провайдер). Если пользователи создаются непосредственно в **Keycloak**, раздел можно пропустить

1. Открыть раздел Identity providers в левом меню

2. Выбрать нужный тип провайдера (например, `LDAP`, `Kerberos` или один из социальных провайдеров)



3. Задать настройки провайдера: адрес сервера, порт, протокол, маппинг атрибутов пользователя и т. д.



4. Нажать на кнопку Save для сохранения настроек провайдера

Создание конфигурации в RuDesktop

1. Войти в административную панель RuDesktop
2. Открыть блок **Администрирование**
3. Нажать на пункт **Keycloak**
4. Нажать на кнопку Добавить Keycloak
5. Заполнить поля:
    5.1. Активировать галочку в чек-боксе **Включить**

5.2. При необходимости активировать чек-бокс **Использовать для SSO авторизации**

5.3. При необходимости активировать чек-бокс **Использовать для синхронизации**

5.4. Указать адрес сервера **Keycloak** в поле Адрес сервера

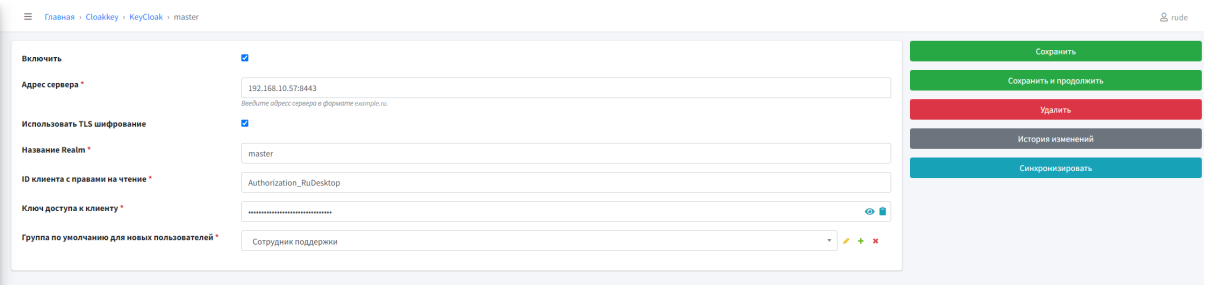
5.5. Если используется TLS шифрование, то активировать галочку в чек-боксе **Использовать TLS шифрование**

5.6. Указать название **Realm** в поле Название Realm

5.7. Указать ID клиента в поле ID клиента с правами на чтение

5.8. Указать **Client Secret** в поле Ключ доступа к клиенту

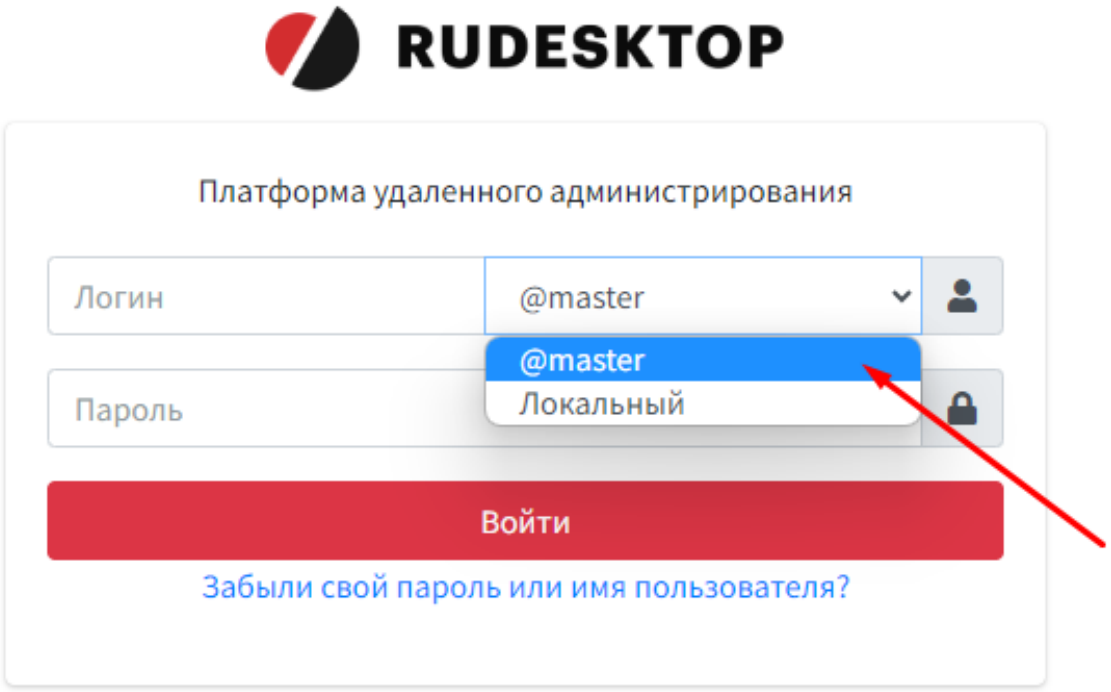
5.9. Выбрать из списка группу по умолчанию для новых пользователей в поле Группа по умолчанию для новых пользователей



6. Нажать на кнопку Сохранить и продолжить

Авторизация через Keycloak

1. Перейти на страницу авторизации
2. Выбрать Realm в поле выбора домена



3. Ввести Логин и Пароль
4. Нажать на кнопку Войти

Описание работы синхронизации и SSO

В этом разделе описано, что именно делает **RuDesktop** при синхронизации и при SSO авторизации, как формируется имя пользователя, что происходит с удалёнными учётными записями и как локальные группы связываются с группами **Keycloak**

Запуск синхронизации

Синхронизацию можно запустить:

- **Вручную** — кнопкой Синхронизировать на странице конфигурации **Keycloak** в **RuDesktop**
- **Через серверную команду** *rude keycloak sync* — удобно для запуска по расписанию через cron на стороне сервера

Примечание

Кнопка Синхронизировать доступна только для записей, у которых активирован чек-бокс **Использовать для синхронизации**

При SSO авторизации членство пользователя в группах обновляется отдельно — независимо от ручной или фоновой синхронизации (см. раздел *Как работает SSO авторизация*)

Формат имени пользователя в RuDesktop

Все пользователи, импортированные из **Keycloak**, сохраняются в **RuDesktop** под именем по шаблону `<username>@<realm_name>` — это исключает конфликты с локальными пользователями и с пользователями из других Realm

Например: пользователь `ivanov` из Realm `corp` будет сохранён в **RuDesktop** как `ivanov@corp`

Примечание

На странице авторизации пользователь вводит свой обычный логин **Keycloak** (без суффикса) — суффикс `@<realm_name>` подставляется сервером автоматически. Имя со суффиксом отображается в списке пользователей в административной панели **RuDesktop**

Что именно синхронизируется

При запуске синхронизации **RuDesktop** обращается к **API Keycloak** от имени сервисного аккаунта клиента и переносит данные в локальную базу в следующем порядке: сначала группы, затем пользователи и их членство в группах

Синхронизация групп

RuDesktop запрашивает у **Keycloak** полный список групп выбранного Realm и для каждой группы создаёт или обновляет соответствующую локальную группу в **RuDesktop**

Что переносится:

- **Имя группы** — записывается в поле Название локальной группы и одновременно в поле Группа в Keycloak, по которому происходит сопоставление при SSO авторизации
- **Полный путь группы** в **Keycloak** (например, `/parent/support`) — сохраняется в служебном поле локальной группы и используется для однозначной идентификации группы при последующих синхронизациях

Примечание

Иерархия групп **Keycloak** обходится рекурсивно: для каждой родительской группы синхронизируются все вложенные подгруппы. В **RuDesktop** все группы создаются как плоский список, но различаются по полному пути из **Keycloak** — это позволяет корректно различать группы с одинаковыми именами в разных ветках иерархии

Важно

Права доступа локальных групп **RuDesktop** при синхронизации **не изменяются**. Синхронизация только создаёт или обновляет запись о группе. Назначение прав остаётся за администратором **RuDesktop** — это сделано для того, чтобы иерархия и состав групп **Keycloak** не могли случайно изменить набор разрешений на сервере

Возможные результаты по каждой группе:

- `OK` — группа создана или уже существовала с теми же значениями
- `Conflict` — в **RuDesktop** уже есть группа с таким именем, но привязанная к другому пути или другому **Keycloak**. Такая группа пропускается, нужно либо переименовать локальную группу, либо удалить дубликат

Синхронизация пользователей

RuDesktop запрашивает у **Keycloak** список пользователей Realm и обрабатывает каждого пользователя, у которого включён флаг **Enabled** в **Keycloak**

Что переносится:

- **Username** — сохраняется в **RuDesktop** в формате `<username>@<realm_name>`, чтобы избежать конфликтов с локальными пользователями и пользователями из других Realms
- **First name** — имя
- **Last name** — фамилия
- **Email** — адрес электронной почты
- **Членство в группах** — для каждого пользователя **RuDesktop** запрашивает список групп через **API Keycloak** и привязывает пользователя к локальным группам по полному пути группы

Если у пользователя в **Keycloak** не указано ни одной группы и в конфигурации **RuDesktop** заполнено поле Группа по умолчанию для новых пользователей, пользователь добавляется в эту группу. Это позволяет новым сотрудникам сразу получать минимальный набор прав для входа в систему

Примечание

Пользователи с флагом **Enabled = false** в **Keycloak** при синхронизации пропускаются — соответствующие учётные записи в **RuDesktop** не создаются и не обновляются

Возможные результаты по каждому пользователю:

- `OK` — пользователь создан или обновлён
- `Not found` — пользователь не найден в **RuDesktop** при попытке обновления (редкая ситуация при гонке записей)
- `Conflict` — в **RuDesktop** уже есть пользователь с таким username, но связанный с другим Realm или с другой записью **Keycloak**

Что происходит с удалёнными или отключёнными пользователями

При синхронизации **RuDesktop** удаляет тех пользователей **Keycloak**, которых больше нет в свежем списке. Под удаление попадают:

- Пользователи, удалённые в **Keycloak**
- Пользователи с выключенным флагом **Enabled** в **Keycloak**

Важно

Удаление затрагивает только пользователей, импортированных из соответствующего **Keycloak** — локальные пользователи **RuDesktop** и пользователи из других конфигураций не трогаются. Если нужно временно ограничить доступ без удаления учётной записи, не отключайте пользователя в **Keycloak**, а исключите его из групп, дающих права в **RuDesktop**

Как работает SSO авторизация

При SSO авторизации **Keycloak** является источником проверки учетных данных пользователя:

1. Пользователь открывает страницу авторизации **RuDesktop**
2. Выбирает Realm, для которого включено использование **Keycloak** для авторизации
3. **RuDesktop** перенаправляет пользователя на авторизацию через **Keycloak** или проверяет учетные данные через настроенную интеграцию
4. После успешной проверки **Keycloak** возвращает серверу **RuDesktop** данные пользователя
5. **RuDesktop** создает пользователя, если его еще нет на сервере, или обновляет данные существующего пользователя
6. **RuDesktop** сопоставляет группы пользователя из **Keycloak** с локальными группами **RuDesktop**

7. Пользователь получает права, которые назначены его локальным группам на сервере **RuDesktop**

Важно

Для SSO авторизации в конфигурации **Keycloak** на сервере **RuDesktop** должен быть включен параметр **Использовать для SSO авторизации**

Связь группы Keycloak с локальной группой RuDesktop

Локальная группа **RuDesktop** используется для назначения прав, а группа **Keycloak** используется как внешний источник членства пользователя в этой группе

Чтобы связать группу **Keycloak** с локальной группой **RuDesktop**:

1. Открыть административную панель **RuDesktop**
2. Перейти в раздел **Организация** → *Группы*
3. Создать новую локальную группу или открыть существующую группу
4. На вкладке **Основная информация** заполнить поле Группа в Keycloak
5. В поле Группа в Keycloak указать название группы так, как оно передается из **Keycloak**

Подсказка

Для обычной связки локальной группы с группой **Keycloak** укажите имя группы, например `support`. Полный путь группы из **Keycloak** используется сервером **RuDesktop** при синхронизации отдельно и не является основным значением для поля Группа в Keycloak

6. Настроить права доступа локальной группы **RuDesktop**
7. Нажать на кнопку Сохранить

После этого при авторизации или синхронизации пользователь будет добавлен в локальную группу **RuDesktop**, если он состоит в соответствующей группе **Keycloak**

Примечание

Название группы в поле Группа в Keycloak должно совпадать с именем группы, которое **RuDesktop** получает от **Keycloak**. Например, если группа в **Keycloak** называется `support`, в поле Группа в Keycloak нужно указать `support`

Какие группы обновляются при SSO авторизации

При SSO авторизации **RuDesktop** обновляет членство пользователя только в тех локальных группах, которые связаны с **Keycloak** — то есть у которых заполнено поле Группа в Keycloak

Локальные группы с незаполненным полем Группа в Keycloak при входе не затрагиваются. Если администратор добавил пользователя в такую группу вручную, после SSO авторизации пользователь в ней останется

Параметр **Использовать для синхронизации** определяет, откуда **RuDesktop** получает список групп пользователя:

- Если параметр включен, группы запрашиваются через API **Keycloak**
- Если параметр выключен, группы берутся из токена авторизации **Keycloak**

Примечание

Вложенные группы AD при входе через Keycloak. Даже если в RuDesktop импортированы и родительская, и дочерняя группы, членство пользователя в дочерней группе само по себе не даёт прав родительской. Чтобы назначить эти права через SSO, проверьте, что Keycloak возвращает родительскую группу в списке групп самого пользователя: через API при включённой синхронизации или в поле `groups` токена доступа при выключенной. Если права назначаются через роль клиента RuDesktop, проверьте её в токене доступа в поле `resource_access.<client_id>.roles`, где `<client_id>` — идентификатор клиента RuDesktop в Keycloak

Например:

1. В **RuDesktop** есть две локальные группы: `Сотрудники поддержки` с незаполненным полем Группа в Keycloak и `Администраторы` со значением `admins` в этом поле
2. Администратор вручную добавил пользователя в обе группы
3. При SSO авторизации из **Keycloak** пришла только группа `admins`
4. Пользователь остаётся в группе `Сотрудники поддержки` — она не связана с **Keycloak**
5. Членство в группе `Администраторы` подтверждается данными из **Keycloak**. Если бы группа `admins` из **Keycloak** не пришла, пользователь был бы из неё исключён

Такое поведение позволяет одновременно управлять частью групп из **Keycloak** и назначать остальные вручную на сервере **RuDesktop**

Важно

Группы, которые **RuDesktop** создаёт автоматически по ролям клиента **Keycloak**, сразу получают заполненное поле Группа в Keycloak с именем роли. Это значит, что они управляются из **Keycloak**: при следующем входе без соответствующей роли пользователь будет из такой группы исключён

Если пользователь не получил ожидаемую группу после SSO авторизации:

- Добавьте пользователя в соответствующую группу на стороне **Keycloak**
- Проверьте, что группа передается в токене, если параметр **Использовать для синхронизации** выключен
- Проверьте, что группа доступна через API **Keycloak**, если параметр **Использовать для синхронизации** включен
- Убедитесь, что значение в поле Группа в Keycloak совпадает со значением группы, которое получает **RuDesktop**

Предупреждение

Для связанных групп источником членства становится **Keycloak**. Если пользователя добавили вручную в группу с заполненным полем Группа в Keycloak, но соответствующей группы нет в **Keycloak**, после входа пользователь будет из неё исключён

Проверка настройки

Если после настройки SSO пользователь авторизуется, но не получает нужные права, проверьте:

- Пользователь создан и активен в **Keycloak**
- Пользователь состоит в нужной группе **Keycloak**
- Для клиента **Keycloak** настроена передача групп
- Группа передается в токене или доступна серверу **RuDesktop** при синхронизации
- Значение группы из **Keycloak** совпадает со значением в поле Группа в Keycloak
- В локальной группе **RuDesktop** настроены нужные права доступа
- В конфигурации **Keycloak** на сервере **RuDesktop** включен параметр **Использовать для SSO авторизации**
- Если параметр **Использовать для синхронизации** выключен, нужные группы передаются в токене авторизации
- Если параметр **Использовать для синхронизации** включен, нужные группы доступны через API **Keycloak**

Типовые ошибки

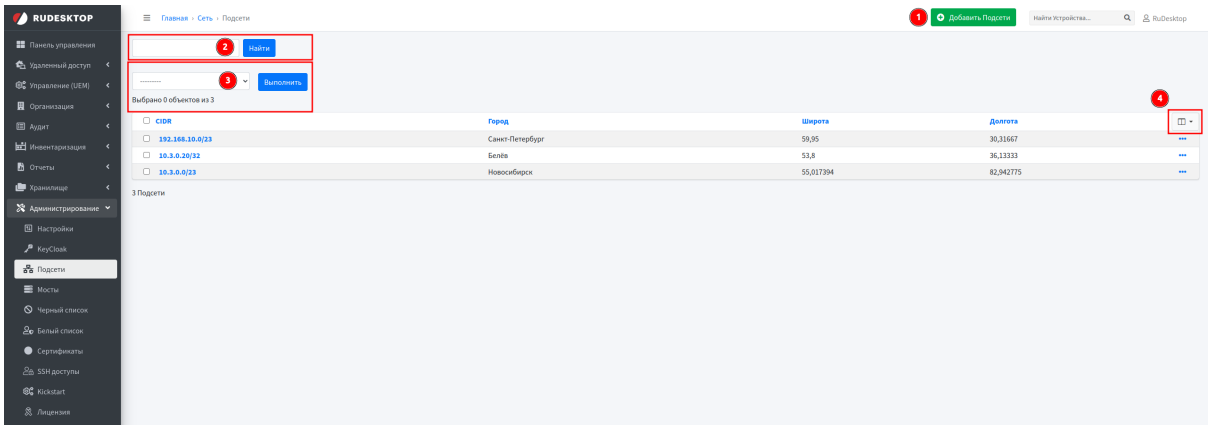
При настройке интеграции чаще всего встречаются следующие ошибки:

- В поле Группа в Keycloak указан полный путь группы, например `/support`, хотя для сопоставления ожидается имя группы `support`
- Пользователь вручную добавлен в локальную группу **RuDesktop**, связанную с **Keycloak**, но на стороне **Keycloak** не состоит в соответствующей группе — при входе такое членство снимается
- Для клиента **Keycloak** не настроен маппер групп, поэтому **RuDesktop** не получает список групп пользователя
- Параметр **Использовать для синхронизации** выключен, но нужная группа не передается в токене авторизации **Keycloak**
- Новому пользователю назначается группа по умолчанию, но у этой группы нет прав, необходимых для работы
- Локальную группу связали с **Keycloak** «на будущее», заполнив поле Группа в Keycloak, — с этого момента её состав определяется внешней системой, а не ручными назначениями

2.16.3 Подсети

Описание страницы

Подсети — эта страница предназначена для регистрации правил, по которым **RuDesktop** определяет геопозицию устройства по его IP-адресу



Как это работает

Каждое правило сопоставляет диапазон IP-адресов (CIDR-подсеть) с городом и координатами. Если IP-адрес устройства попадает в одну из зарегистрированных подсетей, **RuDesktop** записывает соответствующую геопозицию в данные устройства

Геопозиция используется для:

- отображения устройств на карте
- подбора ближайшего *моста* при подключении к удалённому филиалу
- статистики по локациям подключений

Примечание

Если устройство имеет публичный IP-адрес, его геопозиция определяется автоматически по встроенной базе геолокации сервера. Подсети нужны для устройств с приватными адресами (например, во внутренней корпоративной сети) — там автоматическое определение не работает

Подробности о настройке базы геолокации — на странице *Настройка определения геолокации*

Создание подсети

Для добавления подсети необходимо:

1. На странице **«Подсети»** нажать на кнопку Добавить подсеть
2. Заполнить поля:
    1. CIDR — диапазон IP-адресов в формате CIDR, например `192.168.10.0/23`

        Важно

        Укажите адрес сети, например `192.168.10.0/24`. В одной подсети может быть не более 65 536 адресов. Если диапазон больше (например, `0.0.0.0/0`), форма покажет ошибку при сохранении. Каждую подсеть можно добавить только один раз

    2. Город — город, в котором расположена подсеть. По выбранному городу подставляются координаты

        Подсказка

        Если нужного города нет в списке, его можно добавить, нажав на кнопку справа от списка

    3. Широта и Долгота — координаты подсети

        Подсказка

        При выборе города из списка координаты заполняются автоматически. Если город не выбран, координаты можно ввести вручную

        Примечание

        - Для поля Широта допустимы значения от `-90` до `90`

- Для поля Долгота допустимы значения от `-180` до `180`

3. Нажать на кнопку Сохранить или Сохранить и продолжить

Поиск и фильтрация

Для поиска подсетей используется поле поиска

Важно

Поиск работает по CIDR, названию города, широте и долготе

Для выполнения поиска необходимо заполнить поле поиска и нажать на кнопку Найти

Таблица

В таблице отображаются следующие столбцы:

1. CIDR — диапазон подсети
2. Город — выбранный город
3. Широта — широта подсети
4. Долгота — долгота подсети

Операции

При нажатии на кнопку в правой части таблицы открывается контекстное меню

Доступные действия:

1. Редактировать — открыть страницу редактирования подсети
2. Удалить — удалить подсеть
3. История изменений — открыть историю изменений подсети

Массовые действия

Для выбранных подсетей доступно действие:

1. Удалить выбранные подсети — удаление выбранных подсетей

Важно

В зависимости от прав пользователя действие может быть недоступно

Для выполнения действия необходимо отметить подсети в таблице, выбрать действие Удалить выбранные подсети и нажать на кнопку Выполнить

Предупреждение

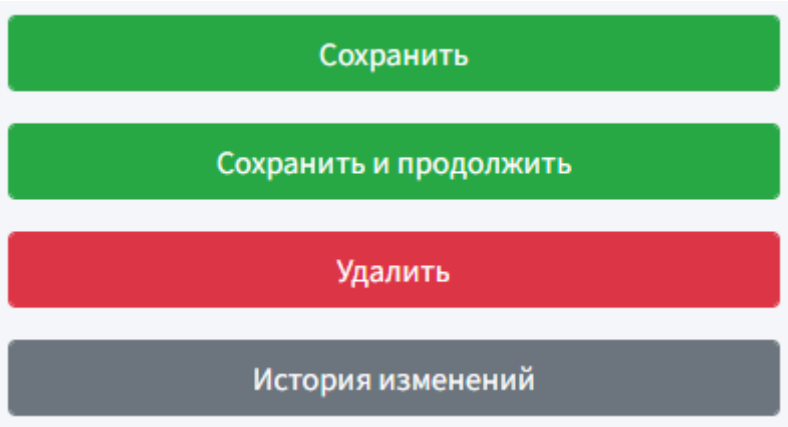
При удалении подсети **RuDesktop** также удаляет геопозиции устройств, которые были определены через эту подсеть. Геопозиция таких устройств станет неизвестной, пока не появится новое подходящее правило или устройство не получит публичный IP-адрес

Свойства подсети

Редактирование

При нажатии на кнопку Редактировать откроется страница свойств подсети

Меню действий



Доступные действия:

1. Сохранить — сохранить изменения и вернуться на страницу **«Подсети»**
2. Сохранить и продолжить — сохранить изменения и остаться на странице редактирования
3. Удалить — удалить подсеть
4. История изменений — просмотреть историю изменений подсети

Пример

Предположим, во внутренней корпоративной сети `192.168.10.0/23` находятся рабочие станции московского офиса. У этих устройств приватные IP-адреса, и автоматически определить их местоположение по внешним базам геолокации нельзя — для этого создаётся правило подсети

1. На странице **«Подсети»** нажать на кнопку Добавить подсеть
2. Заполнить поля:
    1. CIDR — `192.168.10.0/23`
    2. Город — выбрать `Москва` из списка
    3. Широта и Долгота — заполнятся автоматически

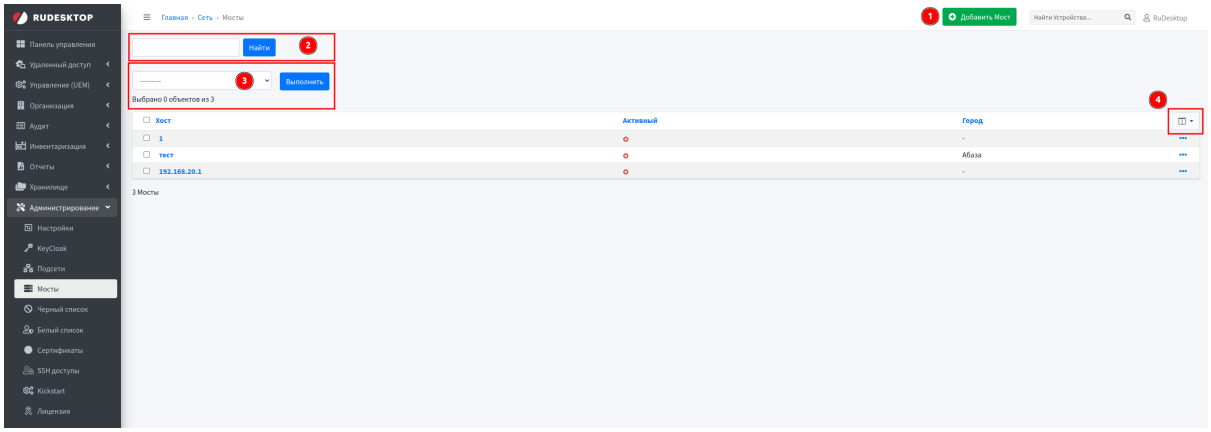
3. Нажать на кнопку Сохранить

После сохранения у устройств с IP-адресами из диапазона `192.168.10.0/23` поле **«Геопозиция»** будет заполнено координатами Москвы

2.16.4 Мосты

Описание страницы

Мосты — эта страница предназначена для регистрации серверов-ретрансляторов, через которые клиенты в удалённых филиалах подключаются к главному серверу **RuDesktop**



Как это работает

Мост — это отдельный сервер **RuDesktop**, развёрнутый в географически удалённой точке. Клиенту, подключающемуся к главному серверу, по координатам подбирается ближайший активный мост, и трафик подключения проходит через него — это сокращает сетевую задержку для удалённых филиалов

Запись о мосте на главном сервере хранит:

- адрес моста (FQDN или IP с портом)
- признак активности — выключенные мосты не используются для маршрутизации
- географическую привязку — город или явно заданные координаты

Примечание

Установка и настройка самого сервера-моста описана в разделе *Настройка мостов*. На странице **«Мосты»** регистрируется уже развёрнутый мост, чтобы главный сервер знал о нём и учитывал при маршрутизации

После добавления, изменения или удаления моста сервер автоматически обновляет список для следующих подключений

Создание моста

Для добавления моста необходимо:

1. На странице **«Мосты»** нажать на кнопку Добавить мост
2. Заполнить поля:
    1. Хост — адрес моста в формате `hostname:port` или `ip:port`, например `nsk.rude.ru:443`

        Важно

        Адрес должен быть уникальным — нельзя добавить два моста с одинаковым `Хост`

    2. Активный — включает использование моста при маршрутизации. Снимите флаг, чтобы временно вывести мост из работы без удаления записи
    3. Город — город, в котором физически расположен мост. По выбранному городу подставляются координаты для расчёта ближайшего моста к клиенту

        Подсказка

        Если нужного города нет в списке, его можно добавить, нажав на кнопку справа от списка

    4. Широта и Долгота — координаты моста

        Подсказка

        При выборе города из списка координаты заполняются автоматически. Если город не выбран, координаты можно ввести вручную

3. Нажать на кнопку Сохранить или Сохранить и продолжить

Поиск и фильтрация

Для поиска мостов используется поле поиска

Важно

Поиск работает по адресу моста (поле Хост) и по названию города

Для выполнения поиска необходимо заполнить поле поиска и нажать на кнопку Найти

Таблица

В таблице отображаются следующие столбцы:

1. Хост — адрес моста
2. Активный — состояние моста
3. Город — выбранный город

Операции

При нажатии на кнопку в правой части таблицы открывается контекстное меню

Доступные действия:

1. Редактировать — открыть страницу редактирования моста
2. Удалить — удалить мост
3. История изменений — открыть историю изменений моста

Массовые действия

Для выбранных мостов доступны действия:

1. Удалить выбранные мосты — удаление выбранных мостов
2. Экспортировать выбранные мосты — экспорт выбранных мостов

Примечание

При экспорте необходимо дополнительно выбрать формат файла

Важно

В зависимости от прав пользователя отдельные действия могут быть недоступны

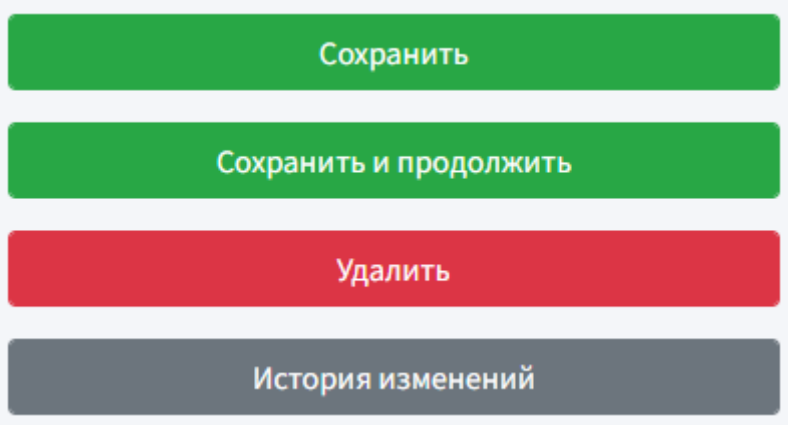
Для выполнения действия необходимо отметить мосты в таблице, выбрать нужное действие и нажать на кнопку Выполнить

Свойства моста

Редактирование

При нажатии на кнопку Редактировать откроется страница свойств моста

Меню действий



Доступные действия:

1. Сохранить — сохранить изменения и вернуться на страницу **«Мосты»**
2. Сохранить и продолжить — сохранить изменения и остаться на странице редактирования
3. Удалить — удалить мост
4. История изменений — просмотреть историю изменений моста

Пример

Предположим, у компании два филиала: один в Москве, другой в Новосибирске. Главный сервер **RuDesktop** находится в Москве по адресу `msk.rude.ru`. Необходимо обеспечить сотрудникам из Новосибирска подключение с минимальной задержкой

1. Развернуть сервер-мост в Новосибирске по адресу `nsk.rude.ru` по инструкции *Настройка мостов*
2. Зарегистрировать мост на главном сервере:
    1. На странице **«Мосты»** нажать на кнопку Добавить мост
    2. Заполнить следующие поля:
        1. Хост — заполнить значение, например: `nsk.rude.ru:443`
        2. Активный — активировать чекбокс
        3. Город — выбрать город из списка, например: `Новосибирск`
        4. Широта — заполнится автоматически
        5. Долгота — заполнится автоматически
    3. Нажать на кнопку Сохранить или Сохранить и продолжить для сохранения моста

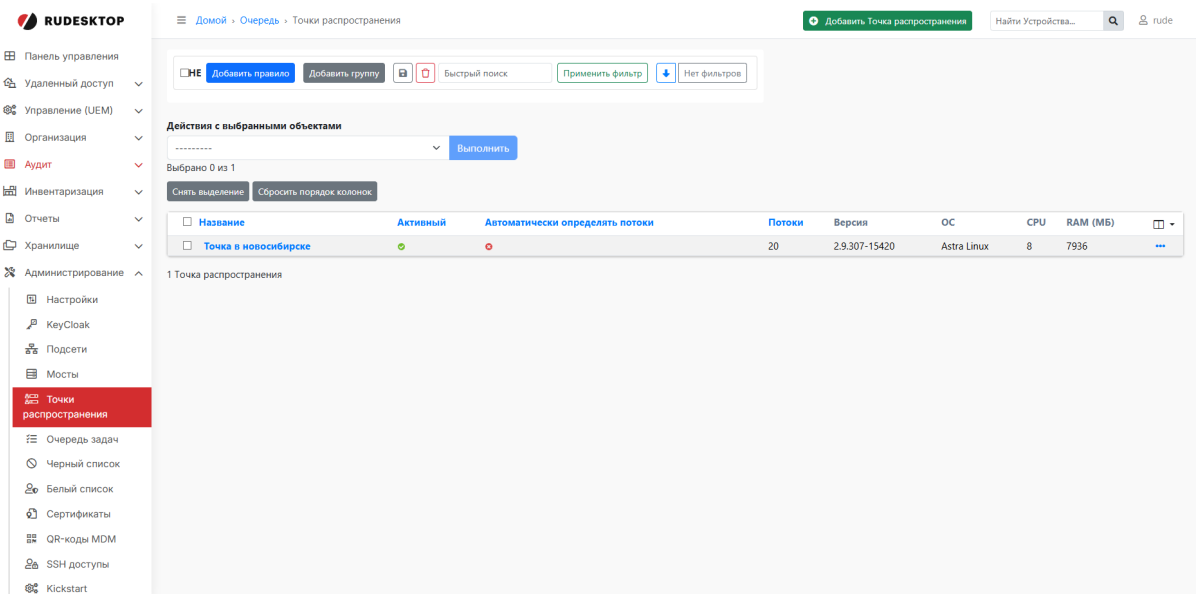
После сохранения главный сервер начнёт направлять подключения новосибирских клиентов через мост `nsk.rude.ru`

2.16.5 Точки распространения

Доступны только в UEM версии

Описание страницы

Точки распространения — эта страница предназначена для создания узлов, на которых будут запускаться фоновые задачи, такие как выполнение политик и прочее



Важно

Страница доступна при наличии лицензии с функциями UEM

Как это работает

Точка распространения — отдельный узел, на котором запускается сервис **RuDesktop** в режиме исполнителя фоновых задач. Главный сервер передаёт ему задачи (например, выполнение политик), а сами задачи выполняются на этом узле — это позволяет вынести нагрузку с главного сервера и распределить её между несколькими исполнителями

Параметры точки распространения, заданные в веб-интерфейсе, применяются на узле автоматически каждые 5 минут

Примечание

Установка и базовая настройка самого узла-исполнителя описана в разделе *Настройка точки распространения*. На странице **«Точки распространения»** регистрируется уже развёрнутый узел и задаются его параметры работы

Какие задачи выполняются на точке распространения

На точки распространения выносится не любая фоновая работа, а только:

- **выполнение политик** — запуск плейбуков на устройствах (задача **«Запуск плейбука»** в *очереди задач*);
- **кэширование и удаление файлов** — подготовка и очистка локальных копий файлов (задачи **«Кэширование файла»** и **«Удаление кэшированного файла»**).
- **публикация PXE-образов** — загрузка ISO с главного сервера, формирование локального PXE-меню и запуск PXE/SMB на точке, выбранной в свойствах образа ОС.
- **PXE-миграция** — сбор и восстановление данных выполняются на точке, выбранной для целевого образа ОС; данные хранятся в её SMB-каталоге.

Остальные операции выполняются **только на главном сервере** и на точки распространения не передаются: генерация и отправка отчётов, экспорт данных, сбор инвентаризационных отчётов и оповещения.

Распределение задач между точками распространения

Если к главному серверу подключено несколько точек распространения, задачи распределяются между ними по доступности:

- **Выполнение политики** передаётся на **любую свободную точку распространения** — задачу забирает та точка, которая первой освободилась. Жёсткой привязки задачи к конкретной точке или филиалу нет: это балансировка нагрузки, а не маршрутизация по расположению устройств. Какая точка выполнила задачу, видно в *очереди задач* в столбце **«Точка распространения»**
- **Кэширование файла** выполняется **на каждой активной точке распространения** — при запуске кэширования создаётся отдельная задача для каждой точки, чтобы локальная копия файла была на всех из них
- **Публикация PXE-образа** имеет жёсткую привязку к точке, выбранной в свойствах образа. Задачу не может выполнить другая свободная точка
- **PXE-миграция** выполняется на той же точке, на которой опубликован выбранный целевой образ. Другой исполнитель эту миграцию не подхватывает

Примечание

Так как выполнение политики может достаться любой точке, файл, используемый в политике, желательно закэшировать на всех точках распространения — тогда любая из них сможет отдать его устройству без обращения к главному серверу. Если файла на точке не окажется, она догрузит его с главного сервера в момент выполнения

Поведение при выключении или недоступности точки

- **Выключенная точка** (снят флаг Активный) не получает новых задач и не участвует в кэшировании файлов
- **Недоступная (офлайн) точка**: задачи, адресованные именно ей (кэширование и удаление файлов), остаются в *очереди задач* и выполняются, когда точка снова выходит на связь. Выполнение политик при этом не останавливается — их подхватывают другие активные точки распространения
- Задача публикации PXE на недоступной точке также остаётся в очереди. До её успешного завершения образ не получает признак **«Опубликовано»**

Важно

Нельзя изменить IPv4 адрес или снять флаг Активный, пока на точке есть опубликованные образы либо выполняются операции публикации. Сначала снимите все образы с публикации

Создание точки распространения

Для добавления точки распространения необходимо:

1. На странице **«Точки распространения»** нажать на кнопку Добавить точку распространения
2. На вкладке **«Основная информация»** заполнить поля:
    1. Название — название точки распространения
    2. IPv4 адрес — IPv4-адрес узла, на котором развёрнут исполнитель

        Важно

        Поле должно содержать корректный IPv4-адрес — значение проверяется при сохранении

    3. Активный — включает или выключает точку распространения. Выключенная точка не получает новых задач
    4. Автоопределение потоков — автоматически рассчитывает количество одновременно выполняемых задач по формуле:

        ```
        потоки = (число ядер − средняя нагрузка в покое) × 2.5
        ```

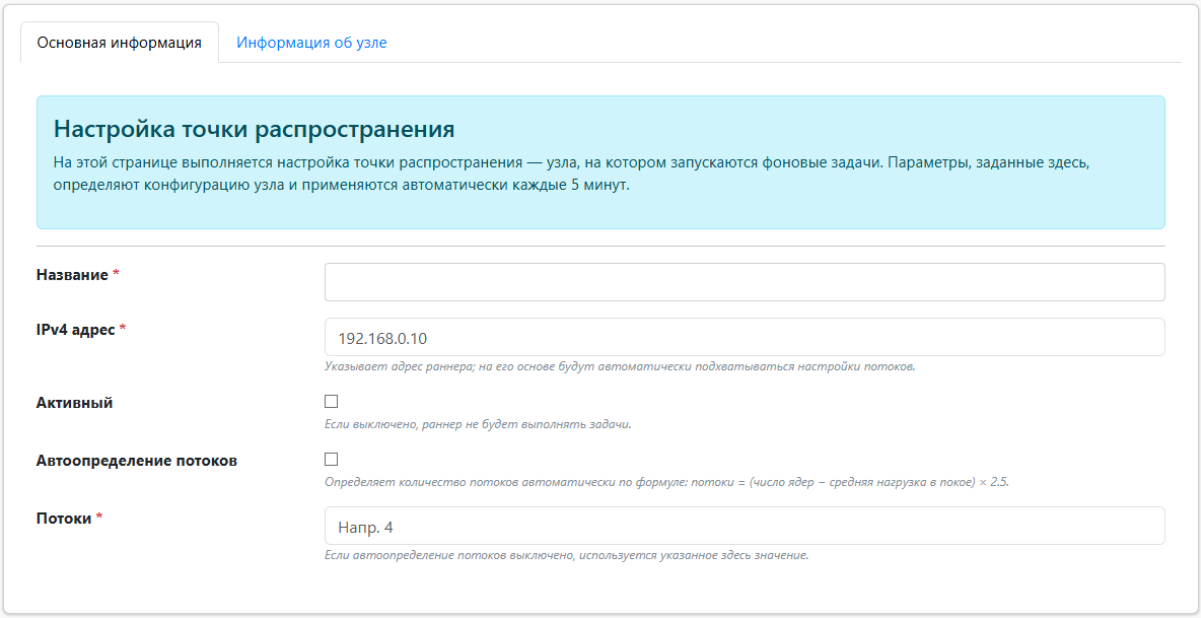
        Примечание

        При включённом автоопределении поле Потоки блокируется и показывает текущее рассчитанное значение, полученное от узла

5. Потоки — количество потоков вручную (используется только при выключенном автоопределении)

3. Нажать на кнопку Сохранить или Сохранить и продолжить

Основная информация



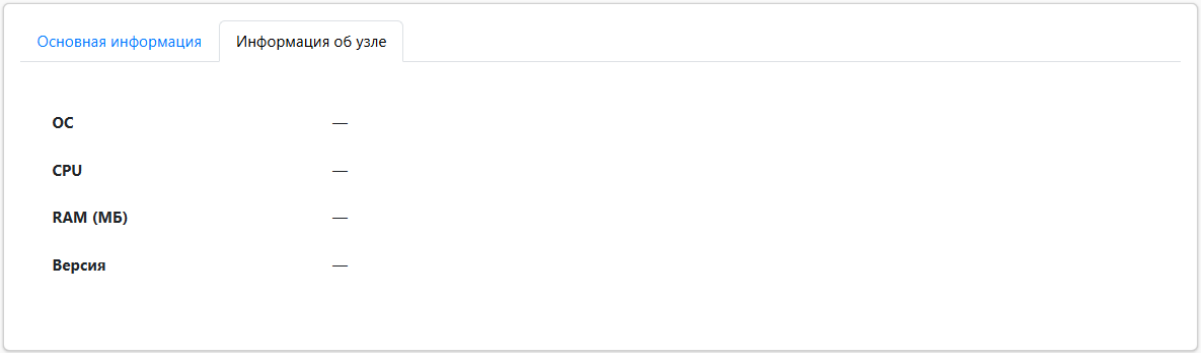
Информация об узле

Вкладка содержит информацию, которую узел отправляет на главный сервер автоматически. Все поля доступны только для просмотра:

- ОС — наименование операционной системы узла
- CPU — количество ядер процессора
- RAM (МБ) — объём оперативной памяти в мегабайтах
- Версия — версия сервера **RuDesktop**, установленного на узле

Примечание

Если на странице данные не отображаются, узел не выходит на связь с главным сервером — нужно проверить установку и настройку сервиса по инструкции *Настройка точки распространения*



Поиск и фильтрация

На странице не предусмотрены отдельные фильтры и поле поиска

Таблица

В таблице отображаются следующие столбцы:

1. Название — название точки распространения
2. Активный — состояние точки распространения
3. Автоматически определять потоки — признак автоматического определения потоков
4. Потоки — количество потоков
5. Версия — версия сервера **RuDesktop**
6. ОС — наименование операционной системы
7. CPU — количество ядер процессора
8. RAM (МБ) — объём оперативной памяти

Примечание

В столбце Потоки при включённом автоопределении отображается текущее рассчитанное значение

Операции

При нажатии на кнопку в правой части таблицы открывается контекстное меню

Доступные действия:

1. Редактировать — открыть страницу редактирования точки распространения
2. Удалить — удалить точку распространения
3. История изменений — открыть историю изменений

Массовые действия

Для выбранных точек распространения доступны действия:

1. Удалить выбранные точки распространения — удаление выбранных точек распространения
2. Экспортировать выбранные точки распространения — экспорт выбранных точек распространения

Примечание

При экспорте необходимо дополнительно выбрать формат файла

Важно

В зависимости от прав пользователя отдельные действия могут быть недоступны

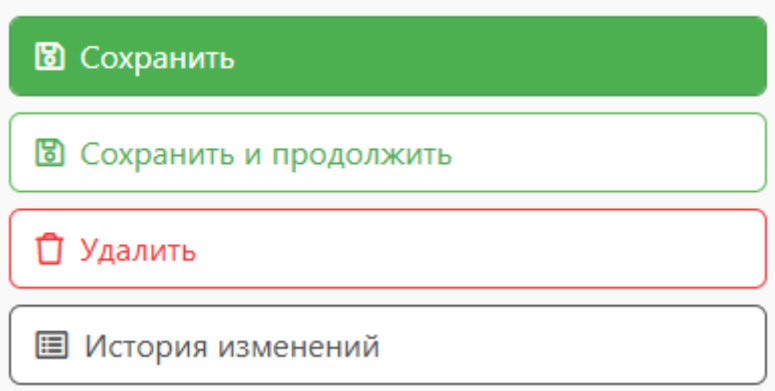
Для выполнения действия необходимо отметить записи в таблице, выбрать нужное действие и нажать на кнопку Выполнить

Свойства точки распространения

Редактирование

При нажатии на кнопку Редактировать откроется страница свойств точки распространения

Меню действий



Доступные действия:

1. Сохранить — сохранить изменения и вернуться на страницу **«Точки распространения»**
2. Сохранить и продолжить — сохранить изменения и остаться на странице редактирования
3. Удалить — удалить точку распространения
4. История изменений — просмотреть историю изменений

Пример

Предположим, на отдельном сервере по адресу `192.168.10.10` развёрнут узел-исполнитель **RuDesktop** по *инструкции*. Чтобы зарегистрировать его на главном сервере и поручить выполнение фоновых задач:

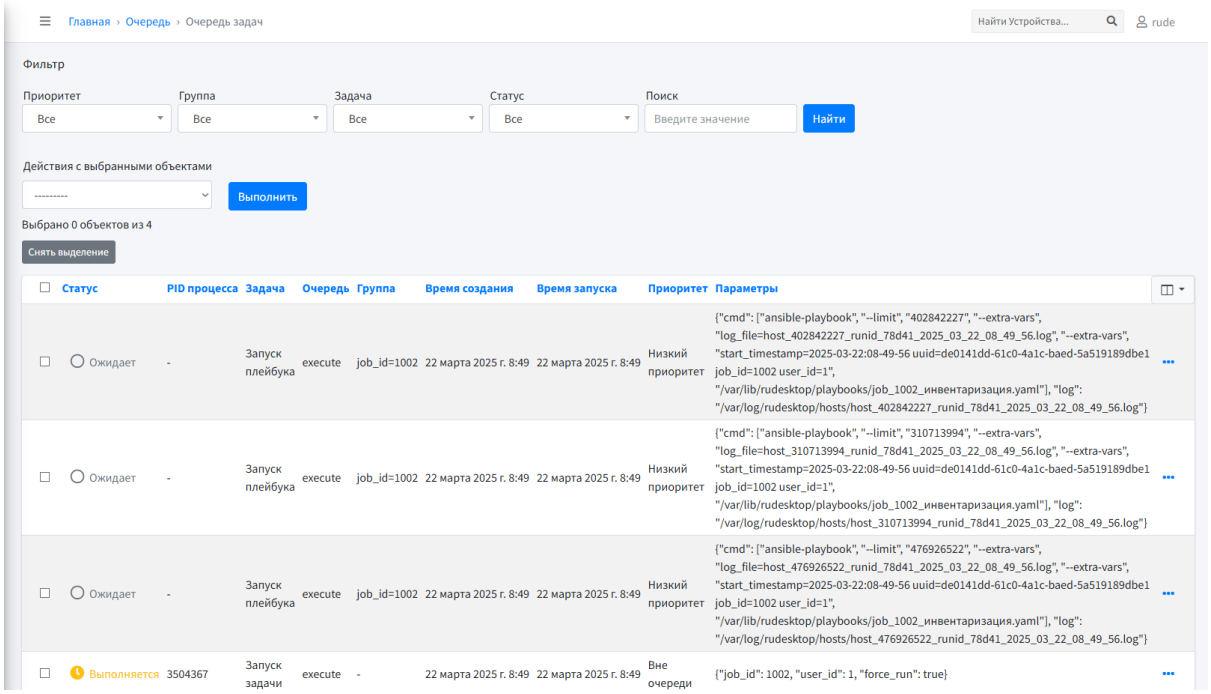
1. На странице **«Точки распространения»** нажать на кнопку Добавить точку распространения
2. Заполнить следующие поля:
    1. Название — указать `Точка распространения 1`
    2. IPv4 адрес — `192.168.10.10`
    3. Активный — активировать чекбокс
    4. Автоопределение потоков — активировать чекбокс (количество потоков узел рассчитает сам)
3. Нажать кнопку Сохранить

В течение 5 минут узел получит параметры конфигурации и начнёт принимать задачи. На вкладке **«Информация об узле»** появятся ОС, число ядер, объём памяти и версия сервера — это означает, что точка распространения вышла на связь

2.16.6 Очередь задач

Описание страницы

Очередь задач — страница предназначена для просмотра текущих фоновых задач и их остановки. Создание, редактирование и ручное удаление задач со страницы недоступны — управление осуществляется только через действие «Остановить»



Как это работает

Задачи в очередь попадают автоматически — например, при выполнении *политик* UEM, синхронизации с *доменами* и *Keycloak*, фоновых операциях экспорта или массовых действиях со страниц веб-интерфейса

Каждая задача забирается из очереди фоновым воркером сервера **RuDesktop**:

- Если у задачи есть параметр Точка распространения — задача выполняется на узле-исполнителе (см. *Точки распространения*)
- Если точка распространения не указана — задача выполняется на главном сервере

Порядок обработки задач определяется приоритетом: задачи с большим приоритетом забираются из очереди раньше, при равных приоритетах — по времени создания

Возможные статусы задачи:

- Ожидает — задача создана и ждёт свободного воркера
- В процессе — задача взята воркером и выполняется

Возможные значения приоритета:

- Вне очереди — служебный приоритет (1000) для задач, запущенных принудительно (например, через действие «Запустить вне очереди» на странице политик)
- Критический приоритет (10)
- Высокий приоритет (7)
- Средний приоритет (5)
- Низкий приоритет (0) — приоритет по умолчанию

Поиск и фильтрация

Для фильтрации задач можно использовать:

1. Приоритет — фильтрация по уровню приоритета (включая `Вне очереди`)
2. Группа — фильтрация по группе задач (используется для пакетной обработки связанных задач, например, всех задач одной политики)
3. Задача — фильтрация по типу задачи
4. Статус — фильтрация по статусу выполнения
5. Поле поиска — поиск по параметрам задачи, группе, приоритету и названию задачи

Для выполнения поиска необходимо заполнить поля или часть полей и нажать на кнопку Найти

Таблица

В таблице отображаются следующие столбцы:

1. Статус — статус выполнения задачи (`Ожидает` или `В процессе`)
2. Точка распространения — узел, на котором выполняется задача. Значение является ссылкой на страницу свойств точки распространения. Для задач, выполняемых на главном сервере, отображается -

3. PID процесса — идентификатор процесса в операционной системе. Заполняется только для задач в статусе `В процессе`
4. Задача — отображаемое название задачи
5. Очередь — имя очереди, в которой находится задача (по умолчанию `default`)
6. Группа — идентификатор группы связанных задач, например `policy_id=42` для всех задач одной политики
7. Время создания — момент попадания задачи в очередь
8. Время запуска — момент, начиная с которого задача доступна к выполнению (для отложенных задач может быть в будущем)
9. Приоритет — приоритет задачи
10. Параметры — JSON с аргументами и метаданными запуска

Операции

При нажатии на кнопку в правой части таблицы открывается контекстное меню с действием:

- Остановить — снять задачу с выполнения и удалить её из очереди

Примечание

Поведение действия зависит от текущего статуса задачи:

- Для задачи в статусе Ожидает — задача удаляется из очереди до начала выполнения
- Для задачи в статусе В процессе — **RuDesktop** завершает процесс по `PID` (вместе со всеми его дочерними процессами), затем удаляет запись из очереди

Важно

Для выполнения одиночного действия Остановить требуется право `Может запускать политики`

Массовые действия

Для выбранных задач доступно действие:

1. Остановить задачи — остановка и удаление выбранных задач из очереди

Важно

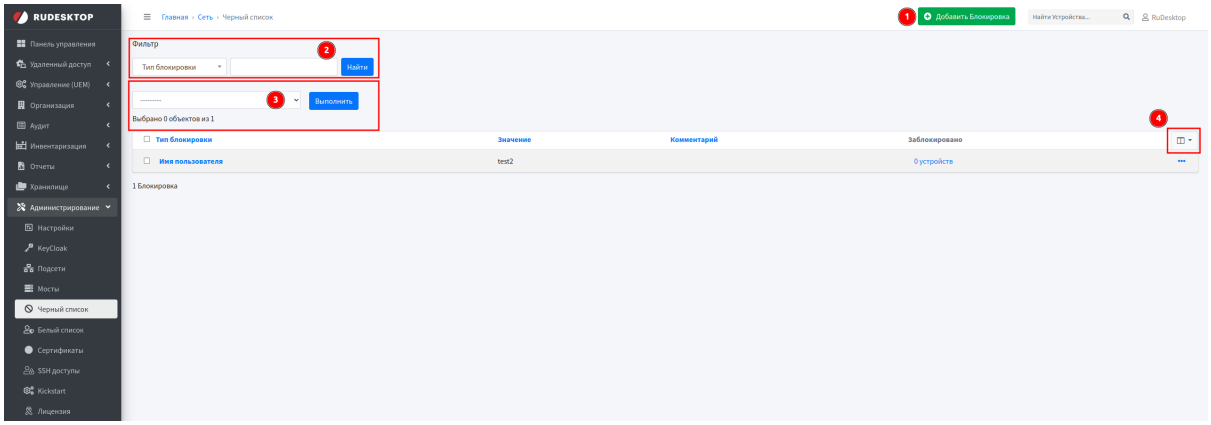
Массовое действие Остановить задачи доступно при наличии стандартных прав Изменение/Удаление на задачи. Для одиночного действия Остановить дополнительно требуется право `Может запускать политики`

Для выполнения действия необходимо отметить задачи в таблице, выбрать действие Остановить задачи и нажать на кнопку Выполнить

2.16.7 Черный список

Описание страницы

Черный список — эта страница предназначена для запрета подключения устройств к серверу по различным признакам



Как это работает

Блокировка может быть настроена по одному из следующих признаков:

- **IP-адрес**
- **Адрес сети**
- **Уникальный код**
- **Имя пользователя**
- **Название хоста**

Важно

Правила **Черного списка** имеют приоритет над *Белым списком*: если устройство одновременно подходит под обе категории, подключение запрещается

Параметры блокировки

При создании и редактировании блокировки используются следующие поля:

1. `Тип блокировки` — признак, по которому выполняется блокировка
2. `Значение` — конкретное значение для выбранного типа блокировки
3. `Комментарий` — дополнительная информация о причине блокировки

Подсказка

- Значения для типов `IP-адрес`, `Уникальный код` (UUID устройства), `Имя пользователя` и `Название хоста` можно посмотреть в свойствах конкретного устройства на странице *Устройства*
- Для типа `Адрес сети` необходимо указать IPv4-подсеть в формате CIDR, например: `192.168.1.0/24`

Примечание

Особенности заполнения поля `Значение`:

- Для `IP-адрес` поддерживается только IPv4-адрес
- Для `Адрес сети` поддерживается только IPv4-подсеть в формате CIDR
- Для `Имя пользователя` значение должно соответствовать правилам имени пользователя в системе
- Для `Уникальный код` и `Название хоста` значение должно быть непустым
- При сохранении значение приводится к нижнему регистру независимо от типа блокировки
- Нельзя создать две одинаковые блокировки с одним и тем же типом и значением

Создание блокировки

Для добавления блокировки необходимо:

1. На странице **«Черный список»** нажать на кнопку Добавить блокировку
2. Выбрать `Тип блокировки`
3. Заполнить поле `Значение`
4. При необходимости заполнить поле `Комментарий`

5. Нажать кнопку Сохранить или Сохранить и продолжить

Поиск и фильтрация

Для поиска блокировок можно использовать:

1. `Тип блокировки` — фильтрация блокировок по их типу
2. `Поле поиска` — поиск по значению блокировки

Для выполнения поиска необходимо указать одно или несколько значений фильтра и нажать на кнопку Найти

Таблица и действия

В таблице отображаются следующие столбцы:

1. `Тип блокировки` — тип, по которому произведена блокировка
2. `Значение` — значение, по которому произведена блокировка
3. `Комментарий` — комментарий, оставленный при добавлении блокировки
4. `Заблокировано` — количество устройств, соответствующих выбранному правилу блокировки

> **Подсказка**
>
> При нажатии на количество произойдет переход на страницу *Устройства* со списком устройств, соответствующих данной блокировке

Для каждой записи доступны действия:

1. `Редактировать` — открыть страницу редактирования блокировки
2. `Удалить` — удалить блокировку
3. `История изменений` — открыть историю создания и изменения блокировки

Массовые действия

Для выбранных записей доступны действия:

1. `Удалить выбранные черные списки` — удаление выбранных блокировок
2. `Экспортировать выбранные черные списки` — экспорт выбранных блокировок

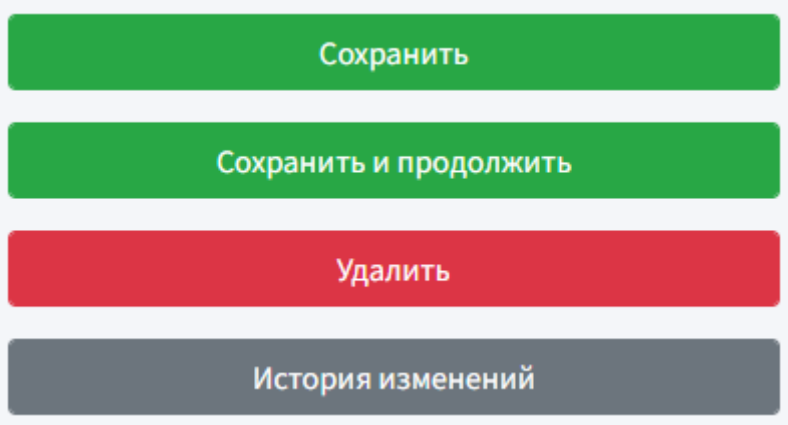
> **Примечание**
>
> Для экспорта необходимо дополнительно выбрать формат файла

Важно

В зависимости от прав пользователя отдельные действия могут быть недоступны

Редактирование и удаление

При открытии блокировки доступны следующие действия:



1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Черный список»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление черного списка и перенаправляет на страницу **«Черный список»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления черного списка
2. После подтверждения удаления черного списка произойдет переход на страницу **«Черный список»** и появится уведомление Успешно удалена блокировка

4. История изменений — отображает все изменения, выполненные для этого черного списка

Пример

Для добавления черного списка по названию хоста устройства необходимо:

1. На странице **«Черный список»** нажать на кнопку Добавить блокировку
2. В поле `Тип блокировки` выбрать `Название хоста`
3. В поле `Значение` указать имя хоста устройства, например: `office-pc-01`

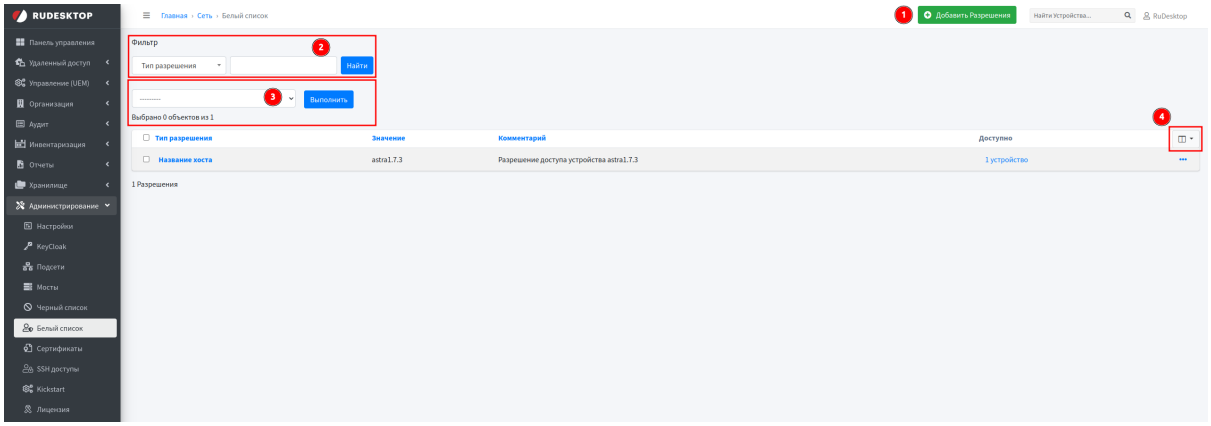
4. При необходимости заполнить поле `Комментарий`
5. Нажать кнопку Сохранить

После сохранения блокировки устройство с именем хоста `office-pc-01` не сможет подключиться к серверу

2.16.8 Белый список

Описание страницы

Белый список — эта страница предназначена для настройки разрешения подключения устройств к серверу по различным признакам



Как это работает

Разрешение может быть настроено по одному из следующих признаков:

- **IP-адрес**
- **Адрес сети**
- **Уникальный код**
- **Имя пользователя**
- **Название хоста**

Важно

- Если **Белый список** пуст, подключение разрешено всем устройствам
- Если в **Белом списке** есть записи, подключение разрешено только устройствам, соответствующим хотя бы одному правилу
- Правила *Черного списка* имеют приоритет над **Белым списком**: если устройство одновременно подходит под обе категории, подключение запрещается

Параметры разрешения

При создании и редактировании разрешения используются следующие поля:

1. Тип разрешения — признак, по которому выполняется разрешение
2. Значение — конкретное значение для выбранного типа разрешения
3. Комментарий — дополнительная информация о причине разрешения

Подсказка

- Значения для типов IP-адрес, Уникальный код (UUID устройства), Имя пользователя и Название хоста можно посмотреть в свойствах конкретного устройства на странице *Устройства*
- Для типа Адрес сети необходимо указать IPv4-подсеть в формате CIDR, например: 192.168.1.0/24

Примечание

Особенности заполнения поля Значение:

- Для IP-адрес поддерживается только IPv4-адрес
- Для Адрес сети поддерживается только IPv4-подсеть в формате CIDR
- Для Имя пользователя значение должно соответствовать правилам имени пользователя в системе
- Для Уникальный код и Название хоста значение должно быть непустым
- При сохранении значение приводится к нижнему регистру независимо от типа разрешения
- Нельзя создать два одинаковых разрешения с одним и тем же типом и значением

Создание разрешения

Для добавления разрешения необходимо:

1. На странице **«Белый список»** нажать на кнопку Добавить разрешение
2. Выбрать Тип разрешения
3. Заполнить поле Значение
4. При необходимости заполнить поле Комментарий
5. Нажать кнопку Сохранить или Сохранить и продолжить

Поиск и фильтрация

Для поиска разрешений можно использовать:

1. `Тип разрешения` — фильтрация разрешений по их типу
2. `Поле поиска` — поиск по значению разрешения

Для выполнения поиска необходимо указать одно или несколько значений фильтра и нажать на кнопку Найти

Таблица и действия

В таблице отображаются следующие столбцы:

1. `Тип разрешения` — тип, по которому произведено разрешение
2. `Значение` — значение, по которому произведено разрешение
3. `Комментарий` — комментарий, оставленный при добавлении разрешения
4. `Доступно` — количество устройств, соответствующих выбранному правилу разрешения

> **Подсказка**
>
> При нажатии на количество произойдет переход на страницу *Устройства* со списком устройств, соответствующих данному правилу разрешения

Для каждой записи доступны действия:

1. `Редактировать` — открыть страницу редактирования разрешения
2. `Удалить` — удалить разрешение
3. `История изменений` — открыть историю создания и изменения разрешения

Массовые действия

Для выбранных записей доступны действия:

1. `Удалить выбранные белые списки` — удаление выбранных разрешений
2. `Экспортировать выбранные белые списки` — экспорт выбранных разрешений

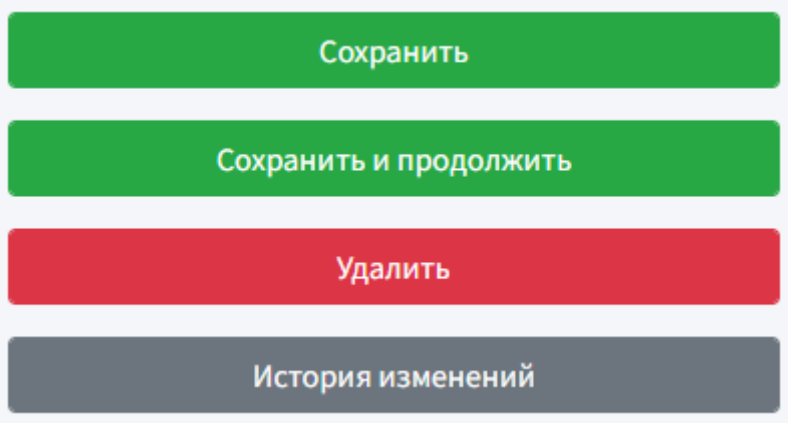
> **Примечание**
>
> Для экспорта необходимо дополнительно выбрать формат файла

Важно

В зависимости от прав пользователя отдельные действия могут быть недоступны

Редактирование и удаление

При открытии разрешения доступны следующие действия:



1. Сохранить — производит сохранение внесенных изменений и перенаправляет на страницу **«Белый список»**
2. Сохранить и продолжить — производит сохранение внесенных изменений и позволяет остаться на странице редактирования для выполнения дальнейших операций
3. Удалить — производит удаление белого списка и перенаправляет на страницу **«Белый список»**

Примечание

1. После нажатия на кнопку Удалить откроется страница подтверждения удаления белого списка
2. После подтверждения удаления белого списка произойдет переход на страницу **«Белый список»** и появится уведомление Успешно удалено разрешение

4. История изменений — отображает все изменения, выполненные для этого белого списка

Пример

Для добавления белого списка по названию хоста устройства необходимо:

1. На странице **«Белый список»** нажать на кнопку Добавить разрешение
2. В поле `Тип разрешения` выбрать `Название хоста`
3. В поле `Значение` указать имя хоста устройства, например: `office-pc-01`

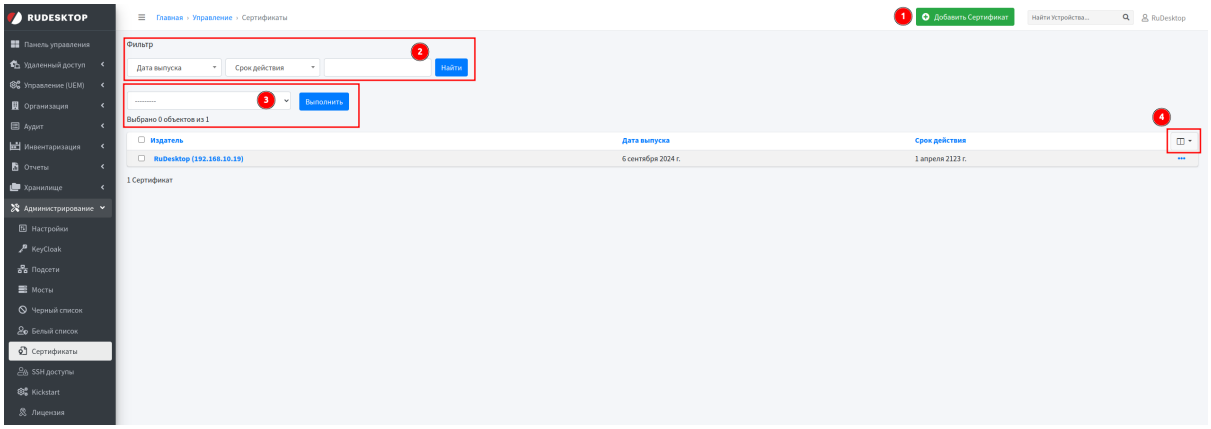
4. При необходимости заполнить поле `Комментарий`
5. Нажать кнопку Сохранить

После сохранения разрешения устройство с именем хоста `office-pc-01` сможет подключиться к серверу

2.16.9 Сертификаты

Описание страницы

Сертификаты — эта страница предназначена для управления корневыми сертификатами в формате PEM



Как это работает

На странице отображаются корневые сертификаты, добавленные в хранилище сервера **RuDesktop**. Сертификаты используются для проверки подлинности подключений к серверу и компонентам инфраструктуры — например, при настройке *мостов*, когда мост использует собственный центр сертификации

Важно

- После установки сервера **RuDesktop** автоматически создаётся основной сертификат
- При открытии страницы список сертификатов автоматически синхронизируется с хранилищем сервера
- Основной сертификат сервера **RuDesktop** помечается как защищённый и не может быть изменён или удалён

Создание сертификата

Для добавления сертификата необходимо:

1. На странице **«Сертификаты»** нажать на кнопку Добавить сертификат
2. В поле Сертификат вставить содержимое сертификата в формате PEM:

```
-----BEGIN CERTIFICATE-----
[тело сертификата]
-----END CERTIFICATE-----
```

3. Нажать кнопку Сохранить или Сохранить и продолжить

После сохранения **RuDesktop** автоматически разбирает сертификат и заполняет поля:

- Издатель — имя издателя сертификата
- Дата выпуска — дата выпуска сертификата
- Срок действия — дата окончания срока действия сертификата
- Информация — подробная расшифровка содержимого сертификата

Примечание

Особенности работы с сертификатами:

- Поддерживается только формат PEM
- Нельзя добавить сертификат, содержимое которого уже есть в системе
- При добавлении некорректного сертификата сохранение не выполняется — отображается ошибка валидации
- Если сертификат относится к текущему хосту **RuDesktop**, он автоматически помечается как защищённый

Поиск и фильтрация

Для поиска сертификатов можно использовать:

1. `Дата выпуска` — фильтрация сертификатов по дате выпуска
2. `Срок действия` — фильтрация сертификатов по дате окончания срока действия
3. `Поле поиска` — поиск по издателю сертификата

Для выполнения поиска необходимо указать одно или несколько значений фильтра и нажать на кнопку Найти

Таблица

В таблице отображаются следующие столбцы:

1. Издатель — издатель сертификата
2. Дата выпуска — дата выпуска сертификата
3. Срок действия — дата окончания срока действия сертификата

Операции

При нажатии на кнопку в правой части таблицы открывается контекстное меню

Доступные действия:

1. Редактировать — открыть страницу редактирования сертификата
2. Удалить — удалить сертификат
3. История изменений — открыть историю создания и изменения сертификата

Примечание

Для защищённого системного сертификата действия редактирования и удаления недоступны

Массовые действия

Для выбранных записей доступны действия:

1. Удалить выбранные сертификаты — удаление выбранных сертификатов
2. Экспортировать выбранные сертификаты — экспорт выбранных сертификатов

Примечание

Для экспорта сертификатов доступен только формат `pem`

Важно

- В зависимости от прав пользователя отдельные действия могут быть недоступны
- Защищённый системный сертификат нельзя удалить массовым действием

Свойства сертификата

При открытии сертификата отображаются разделы:

1. Сертификат — содержимое сертификата в формате PEM
2. Информация — подробная расшифровка содержимого сертификата

Примечание

Для защищённого системного сертификата поле Сертификат доступно только для просмотра, действия редактирования и удаления заблокированы

Меню действий

Для обычного сертификата доступны следующие действия:

1. Сохранить — сохранить изменения и вернуться на страницу **«Сертификаты»**
2. Сохранить и продолжить — сохранить изменения и остаться на странице сертификата
3. Удалить — удалить сертификат и вернуться на страницу **«Сертификаты»**
4. История изменений — отобразить все изменения, выполненные для этого сертификата

Примечание

После подтверждения удаления произойдёт переход на страницу **«Сертификаты»** и появится уведомление Успешно удален сертификат

Пример

Для добавления собственного сертификата (например, корневого сертификата моста) необходимо:

1. На странице **«Сертификаты»** нажать на кнопку Добавить сертификат
2. Вставить содержимое сертификата в формате PEM в поле Сертификат
3. Нажать кнопку Сохранить

После сохранения сертификат появится в таблице со значениями издателя, даты выпуска и срока действия

2.16.10 QR-коды MDM

Доступны только в MDM версии

Описание страницы

QR-коды MDM - эта страница предназначена для создания и управления QR-кодами, которые используются для автоматической настройки устройств при первичной инициализации в системе управления мобильными устройствами (MDM). Сканирование такого кода позволяет устройству получить все необходимые параметры для подключения к серверу MDM, настройки Wi-Fi и применения политик безопасности

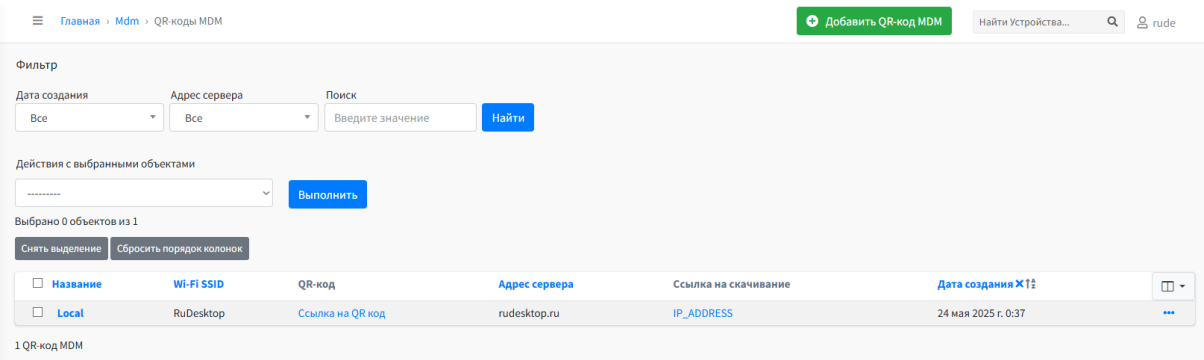
Важно

Страница доступна при наличии лицензии с функциями MDM

Для просмотра изображения QR-кода по прямой ссылке необходимо войти на сервер в браузере

Неавторизованный запрос перенаправляется на страницу входа

При настройке Android покажите код в авторизованном браузере администратора и сканируйте его с устройства



Как это работает

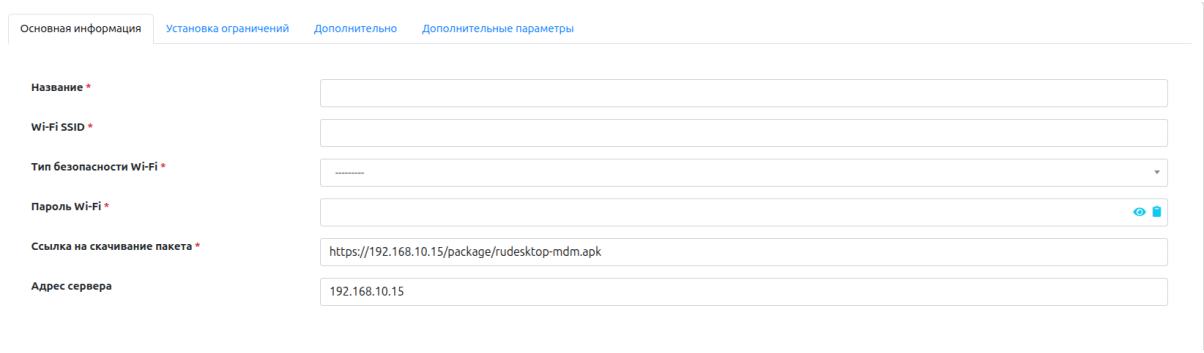
QR-код используется для автоматической настройки устройства при первичной инициализации в MDM. После сканирования устройство получает параметры подключения к Wi-Fi, адрес сервера **RuDesktop** и дополнительные ограничения

Параметры QR-кода

При создании и редактировании QR-кода используется многостраничная форма. Форма состоит из пяти вкладок, каждая из которых отвечает за определённый набор параметров

Основная информация

На этой вкладке задаются основные параметры для подключения устройства к сети и серверу **RuDesktop**



Доступные поля:

1. Название - внутреннее наименование QR-кода для удобства идентификации в списке
2. Wi-Fi SSID - имя (идентификатор) беспроводной сети, к которой должно подключиться устройство

> **Важно**
>
> Обратите внимание на формат указания SSID в зависимости от производителя устройства:
>
> - Для планшетов **Kvadra** имя Wi-Fi сети необходимо указывать **в двойных кавычках**, например: `"rudesktop-wi-fi"`
>
>   Это обязательное условие для успешной установки подключения
> - Для всех остальных устройств кавычки не требуются, имя указывается обычным текстом, например: `rudesktop-wi-fi`
>
> Несоблюдение этого правила может привести к ошибке подключения устройства к Wi-Fi сети при сканировании QR-кода

3. Тип безопасности Wi-Fi - выбор протокола безопасности для Wi-Fi сети

   Доступны варианты:

   - `Открытая сеть (без пароля)`
   - `WPA/WPA2/WPA3/PSK`
   - `WEP`
   - `EAP`
4. Пароль Wi-Fi - пароль для доступа к выбранной беспроводной сети
5. Ссылка на скачивание пакета - URL-адрес, по которому устройство сможет скачать пакет .apk клиента **RuDesktop**

> **Подсказка**
>
> Поле заполняется автоматически по адресу текущего сервера и имеет вид `https://АДРЕС_СЕРВЕРА/package/rudesktop-mdm.apk`
>
> При необходимости значение можно отредактировать и указать собственную ссылку на пакет регистрации

6. Адрес сервера - адрес сервера **RuDesktop**, к которому клиент должен подключиться после установки

Подсказка

Адрес подставляется автоматически с учётом настройки **«Порт подключения клиентов»**

Если порт отличается от 443, указать его в формате `host:port`, например `rd.example.org:8443`

Без явно указанного порта клиент будет подключаться к 443

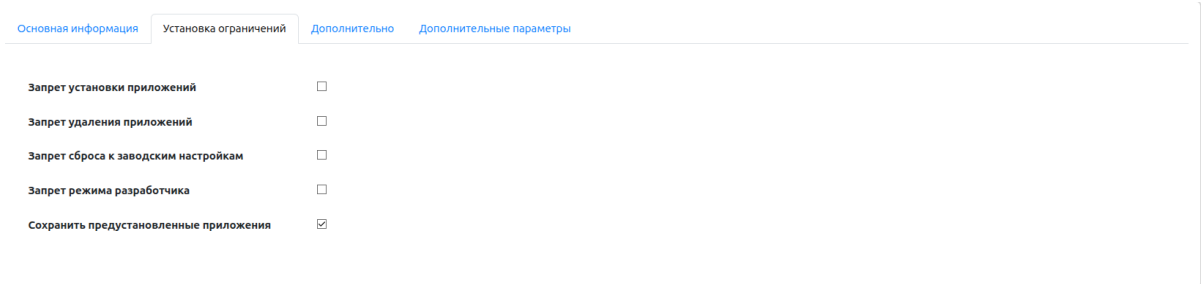
Это адрес подключения клиента, а поле **«Ссылка на скачивание пакета»** содержит отдельный полный URL загрузки APK

Проверить оба адреса из сети, в которой будет регистрироваться устройство

Успешная загрузка APK ещё не подтверждает доступность порта подключения клиента

Установка ограничений

На этой вкладке настраиваются политики безопасности и ограничения, которые будут автоматически применены к устройству после его регистрации в MDM



Здесь представлен список опций, которые можно активировать с помощью переключателей:

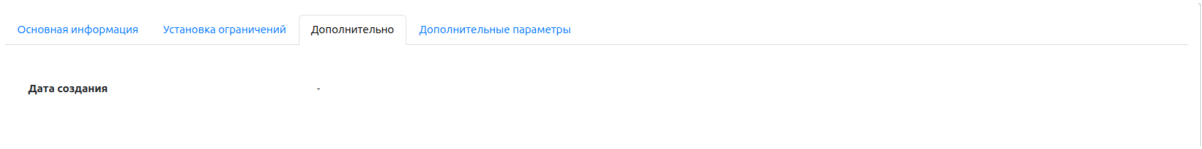
- Запрет установки приложений - запрещает пользователю устанавливать новые приложения на устройстве
- Запрет удаления приложений - запрещает пользователю удалять существующие приложения на устройстве
- Запрет сброса к заводским настройкам - предотвращает сброс устройства до состояния, в котором оно было с завода
- Запрет режима разработчика - отключает доступ к настройкам для разработчиков
- Сохранить предустановленные приложения - обеспечивает сохранение приложений, установленных производителем

Примечание

Активированные на этой вкладке ограничения будут переданы на устройство вместе с QR-кодом и применены автоматически

Дополнительно

На этой вкладке отображается служебная информация о QR-коде



Здесь находится только одно поле:

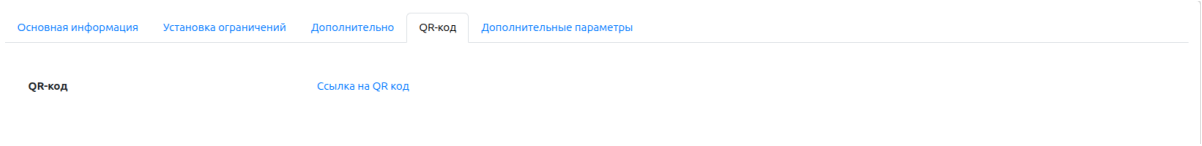
- Дата создания - метка времени, показывающая, когда был создан данный QR-код

Примечание

Это поле является информационным и недоступно для редактирования

QR-код

На этой вкладке отображается сгенерированное изображение QR-кода



Вкладка содержит:

- QR-код - графическое представление кода, которое можно сканировать для настройки устройства

Подсказка

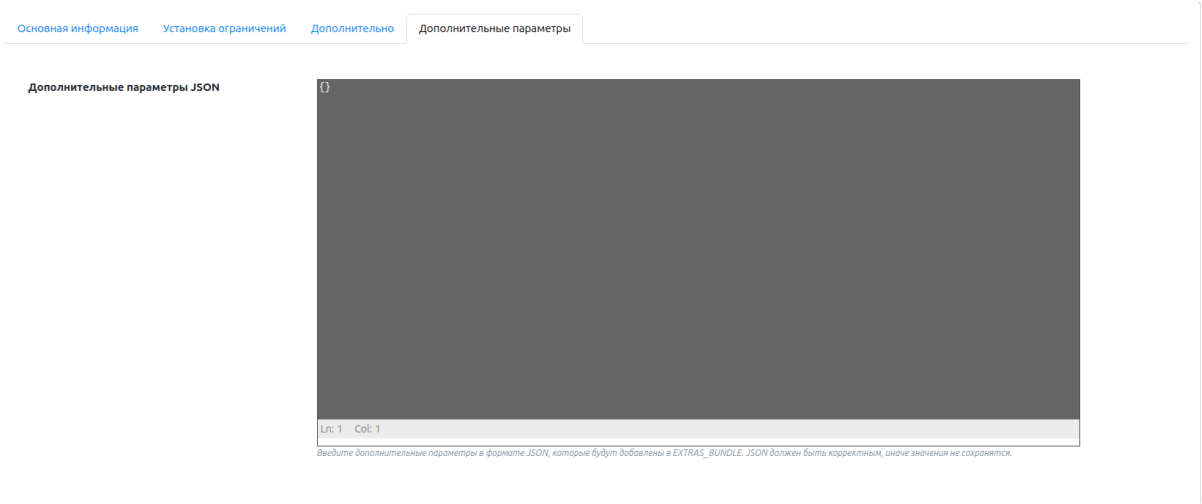
Изображение можно сохранить на диск, чтобы распечатать или встроить в инструкцию для пользователей

Примечание

Вкладка **«QR-код»** появляется только после первого сохранения QR-кода

Дополнительные параметры

На этой вкладке можно передать на устройство произвольные данные в структурированном виде



Здесь расположено поле:

- Дополнительные параметры JSON - текстовое поле для ввода пользовательских данных в формате JSON

> **Важно**
>
> Значение должно быть указано в корректном формате JSON

Для запрета сброса настроек Wi-Fi, мобильной сети и Bluetooth после регистрации добавить параметр:

```
{"disable_network_reset": true}
```

Требуются Android 6 или новее и MDM-клиент с поддержкой этого параметра. Это ограничение не выполняет сброс сети. Для изменения ограничения на уже зарегистрированном устройстве использовать *политику управления сбросом сети*

> **Важно**
>
> Более подробно как это работает можно прочитать в кейсе Предустановка приложений через QR-код

Создание QR-кода

Для создания QR-кода необходимо:

1. На странице **«QR-коды MDM»** нажать на кнопку Добавить QR-код MDM
2. На вкладке **«Основная информация»** заполнить обязательные параметры подключения
3. При необходимости настроить вкладки **«Установка ограничений»** и **«Дополнительные параметры»**

4. Нажать на кнопку Сохранить или Сохранить и продолжить

Поиск и фильтрация

Для удобства навигации по списку QR-кодов предусмотрен фильтр:

1. Дата создания - фильтрация QR-кодов по дате создания
2. Адрес сервера - фильтрация QR-кодов по адресу сервера
3. Поле поиска - поиск по названию компонента, адресу сервера и значению `Wi-Fi SSID`

Для применения фильтра необходимо нажать кнопку Найти

Таблица

Таблица содержит список всех созданных QR-кодов со следующими столбцами:

1. Название - внутреннее имя, присвоенное QR-коду при создании
2. Wi-Fi SSID - имя сети Wi-Fi, зашитое в QR-код
3. QR-код - ссылка на изображение QR-кода
4. Адрес сервера - адрес сервера **RuDesktop**
5. Ссылка на скачивание - ссылка на .apk клиента **RuDesktop**
6. Дата создания - дата и время генерации кода

Операции

При нажатии на кнопку в правой части таблицы открывается контекстное меню. **Доступные действия:**

1. Редактировать - открыть форму редактирования параметров QR-кода
2. Удалить - удалить QR-код
3. История изменений - просмотр истории изменений данного QR-кода

Массовые действия

Для выбранных QR-кодов доступны действия:

1. Удалить выбранные - удаление отмеченных QR-кодов
2. Экспортировать выбранные - экспорт параметров выбранных QR-кодов в файл

Примечание

При выборе экспорта потребуется указать формат файла

Важно

Набор доступных действий зависит от прав текущего пользователя

Для выполнения действия необходимо отметить QR-коды в таблице, выбрать нужное действие и нажать на кнопку Выполнить

Свойства QR-кода

Редактирование

При нажатии на кнопку Редактировать откроется форма с теми же вкладками, что и при создании. После первого сохранения дополнительно появляется вкладка **«QR-код»** с готовым изображением

Меню действий

На странице редактирования доступны следующие действия:

1. Сохранить - сохранить изменения и вернуться к списку QR-кодов
2. Сохранить и продолжить - сохранить изменения и оставить форму открытой
3. Удалить - удалить текущий QR-код
4. История изменений - отобразить историю изменений данного QR-кода

Пример

Для создания QR-кода, который подключит устройство к Wi-Fi сети, установит клиент **RuDesktop** и направит его на указанный сервер, необходимо:

1. На странице **«QR-коды MDM»** нажать кнопку Добавить QR-код MDM
2. На вкладке **«Основная информация»** заполнить поля:
   - Название - `Wi-Fi`
   - Wi-Fi SSID - `Network`
   - Тип безопасности Wi-Fi - выбрать `WPA/WPA2/WPA3/PSK`
   - Пароль Wi-Fi - `Password123`
   - Адрес сервера - указать `test.server.local`
3. Перейти на вкладку **«Установка ограничений»** и активировать опцию **Запрет сброса к заводским настройкам**
4. Нажать кнопку Сохранить

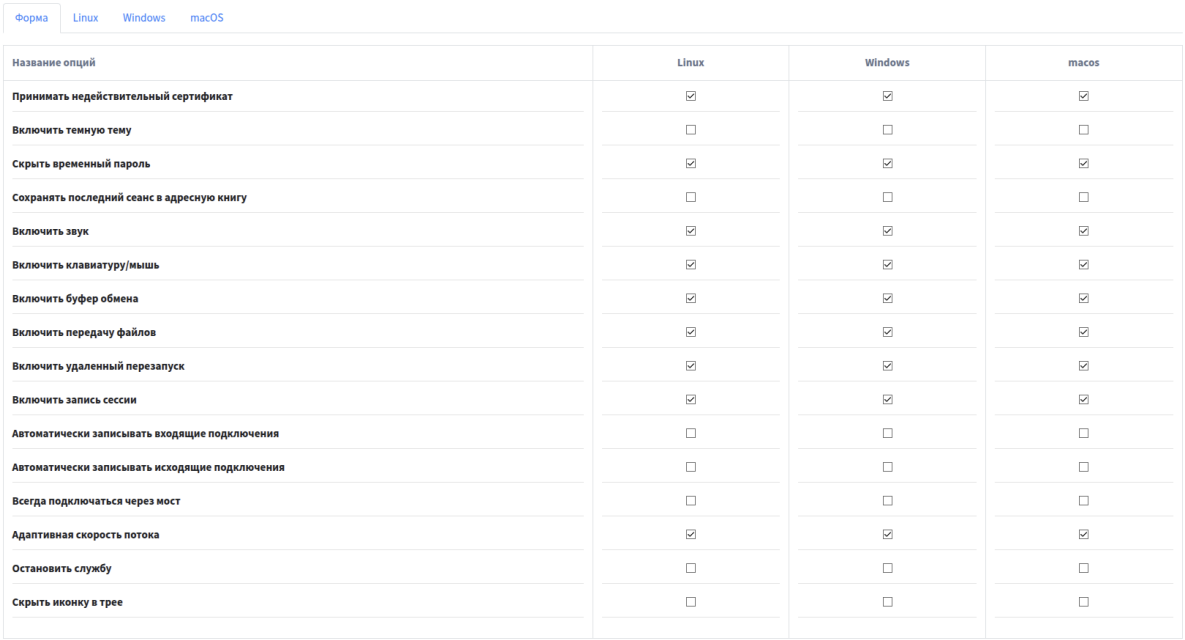
Система создаст QR-код и перенаправит на список, где он будет отображаться под названием `Wi-Fi`. Для просмотра и скачивания изображения нужно нажать на Ссылка на QR код в столбце `QR-код`

После сканирования этого QR-кода устройство автоматически подключится к Wi-Fi сети `Network`, на нём будет установлен клиент **RuDesktop** с подключением к серверу `test.server.local`, а также будет активирован запрет на сброс настроек

2.16.11 Kickstart

Описание страницы

Kickstart — это набор параметров клиента **RuDesktop**, который сервер централизованно применяет к подключённым устройствам. Параметры задаются один раз для каждой поддерживаемой платформы (Windows, Linux, macOS) и распространяются либо при первой установке клиента, либо вручную через кнопку Применить настройки



Как это работает

Параметры на странице соответствуют опциям клиента **RuDesktop** — например, тёмная тема, разрешение на буфер обмена, автоматическая запись сессий и т. д. Каждый параметр включается отдельно для каждой ОС: Windows, Linux, macOS

При сохранении формы **RuDesktop** генерирует для каждой платформы скрипт настройки клиента. Этот скрипт:

- автоматически выполняется на устройстве при первой установке клиента **RuDesktop**
- может быть применён вручную к уже установленным клиентам через кнопку Применить настройки

Помимо стандартных параметров, в скрипт можно добавить произвольные команды (см. *Платформенные вкладки*) — например, очистку временных файлов или создание каталогов

Важно

Kickstart переопределяет настройки клиента на устройстве. Снятая галочка задаёт выключенное значение соответствующего параметра, а не возвращает его к значению по умолчанию

Для применения изменений сохранить форму и нажать Применить настройки для нужных устройств или групп

Параметры Kickstart

На вкладке **«Форма»** содержится набор параметров клиента под каждую платформу. Параметры разделены на две группы — **«Настройки клиента»** управляют постоянным поведением приложения, **«Преднастройки подключения»** задают режим, который применяется к каждой новой исходящей сессии

Настройки клиента

Эти настройки позволяют настроить клиент

1. Принимать недействительный сертификат — позволяет автоматически принять новый сертификат сервера **RuDesktop** при его сбросе
2. Включить темную тему — после применения настроек включает тёмную тему

   Подсказка

   При снятой галочке применяется светлая тема

3. Числовой временный пароль — временный пароль будет генерироваться только из цифр

   Примечание

   При снятой галочке используются цифры и буквы. На постоянный пароль настройка не влияет

4. Открывать новые подключения в отдельном окне — новые подключения открываются в отдельных окнах клиента

   Подсказка

   При снятой галочке новые подключения открываются во вкладках

5. Скрыть временный пароль — скрыть временный пароль в пользовательском интерфейсе

6. Сохранять последний сеанс в адресную книгу — при активации этого пункта устройства, к которым было выполнено подключение, будут сохраняться автоматически в адресную книгу
7. Включить звук — позволяет включить или отключить звук удаленного устройства при подключении к нему
8. Включить клавиатуру/мышь — разрешить подключенному устройству управлять компьютером с помощью клавиатуры и мыши
9. Включить буфер обмена — разрешить подключенному устройству использовать буфер обмена
10. Включить передачу файлов — разрешить подключенному устройству использовать передачу файлов
11. Всегда открывать корень файловой системы при передаче файлов — при открытии передачи файлов сразу отображать корень файловой системы
12. Включить удаленный перезапуск — разрешить подключенному устройству выполнять перезагрузку устройства
13. Включить запись сессии — разрешить подключенному устройству выполнять запись сессии
14. Автоматически записывать входящие подключения — при активации данного пункта все входящие подключения будут записываться
15. Автоматически записывать исходящие подключения — при активации данного пункта все исходящие подключения будут записываться
16. Всегда подключаться через мост — при активации этого пункта подключение будет происходить через сервер (по умолчанию используется P2P)
17. Адаптивная скорость потока — при активации этой настройки приложение будет адаптировать качество трансляции удаленного рабочего стола в зависимости от скорости вашего интернет-соединения
18. Остановить службу — отключение службы

> **Важно**
>
> Принимать и выполнять подключения к устройствам будет невозможно, так как служба будет выключена

19. Скрыть иконку в трее — не отображать иконку клиента **RuDesktop** в трее

Преднастройки подключения

Эти настройки позволяют настроить преднастройки клиента при первом подключении к устройству

1. Показать удаленный курсор — после подключения
2. Отключить звук — отключить звук удаленного устройства для оператора
3. Режим конфиденциальности — блокировка экрана и устройств ввода удаленного устройства

4. Блокировка экрана после завершения сеанса — блокировка пользовательской сессии после завершения сеанса
5. Показать качество — отобразить информацию о качестве изображения
6. Режим просмотра — заблокировать собственные устройства ввода для удаленного устройства, такие как клавиатура и мышь
7. Отключить обои aero на время сеанса — отключить тему Aero и обои рабочего стола для повышения скорости отклика

Важно

1. При нажатии на имя параметра происходит следующее:
    - `Установка галочек`: При нажатии на имя параметра отмечаются галочками все доступные платформы
    - `Снятие галочек`: При повторном нажатии галочки снимаются
2. При нажатии на имя платформы происходит следующее:
    - `Установка галочек`: При нажатии на имя платформы отмечаются галочками все доступные параметры
    - `Снятие галочек`: При повторном нажатии галочки снимаются

Эти функции позволяют быстро выбрать или отменить выбор всех параметров или платформ одновременно, что упрощает работу с параметрами

Платформенные вкладки

Помимо галочек **«Форма»**, у каждой платформы есть отдельная вкладка с текстовым редактором для добавления произвольных команд. Команды выполняются на устройстве после применения Kickstart-скрипта и позволяют, например, подготовить каталоги, очистить временные файлы или установить дополнительные пакеты

Команды записываются на стандартном языке оболочки соответствующей ОС:

- **Windows** — PowerShell или CMD
- **Linux** — bash
- **macOS** — bash или zsh

Примеры:

```
# Пример для Windows
& "C:\Windows\system32\cmd.exe" /c del /q /s "C:\Users\rude\
 ↪AppData\Local\Temp\*"

# Пример для Linux
mkdir /home/rude/Downloads/test
```

Важно

Команды выполняются с правами учётной записи, под которой работает клиент **RuDesktop** на устройстве. Если требуется повышение прав, используйте соответствующие средства ОС (`sudo`, `runas` и т. п.)

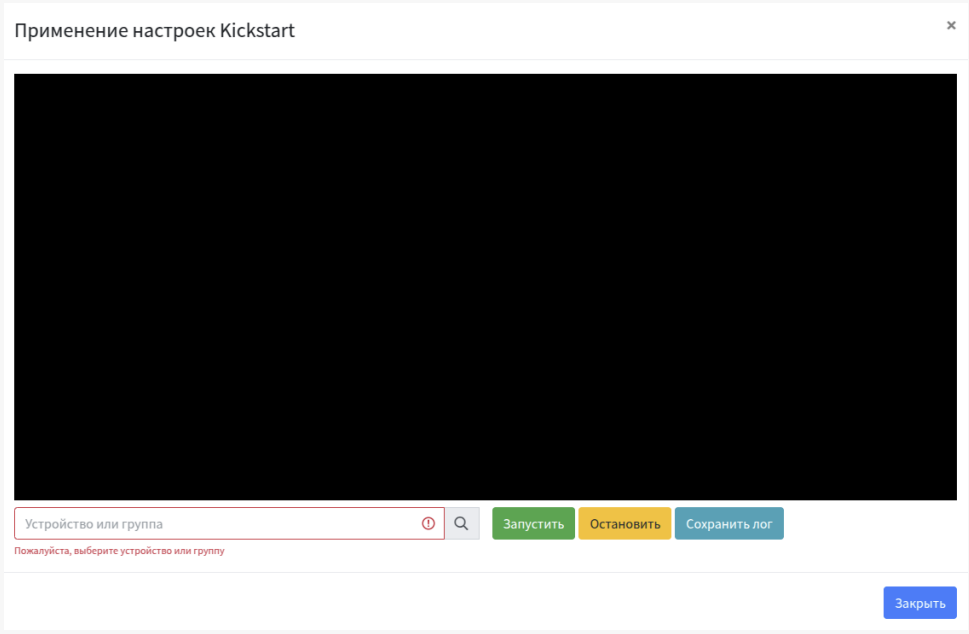
Применение настроек

Для применения настроек Kickstart необходимо:

1. Нажать на кнопку Применить настройки

Подсказка

После этого откроется окно для выбора устройств или группы устройств для применения настроек



2. Нажать на поле Устройство или группа и выбрать в появившемся меню устройство или группу устройств

Важно

Чтобы выполнить применение настроек для всех подключенных к серверу устройств, в меню необходимо выбрать пункт Все

3. После выбора устройств или группы необходимо нажать на кнопку Запустить

Примечание

После запуска в окне терминала должны появиться логи выполнения. Это означает, что процесс применения настроек успешно запущен

Подсказка

Вы можете управлять процессом применения настроек следующими способами:

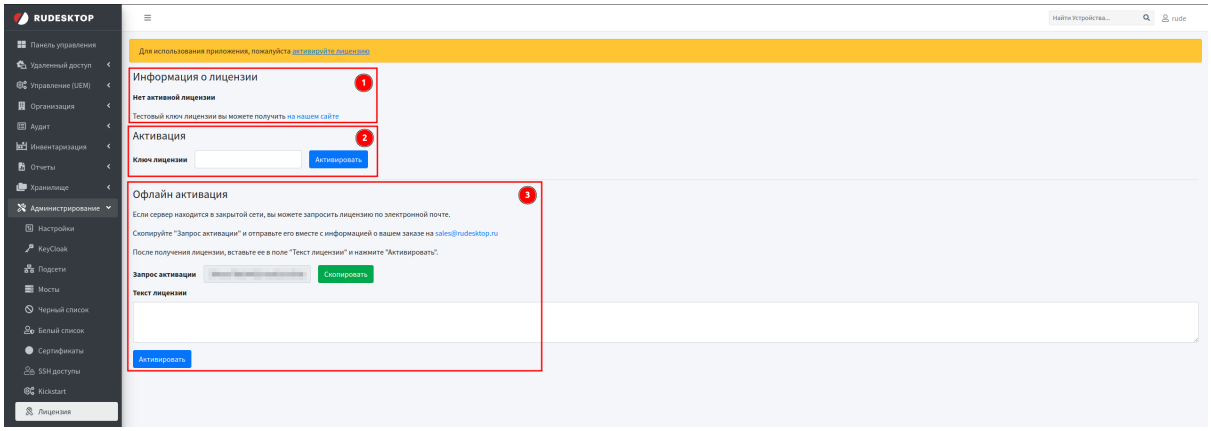
- `Остановка процесса`: Для остановки применения настроек нажмите на кнопку Остановить
- `Сохранение логов`: Чтобы сохранить лог выполнения процесса, нажмите на кнопку Сохранить лог

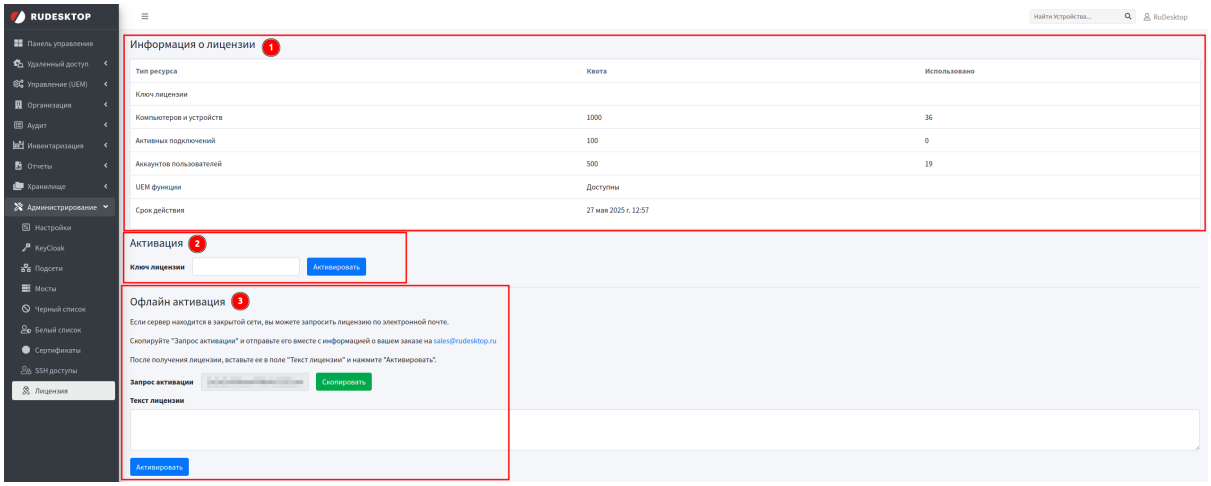
Эти функции позволяют контролировать процесс применения настроек и сохранять важные записи логов для последующего анализа

2.16.12 Лицензия

Описание страницы

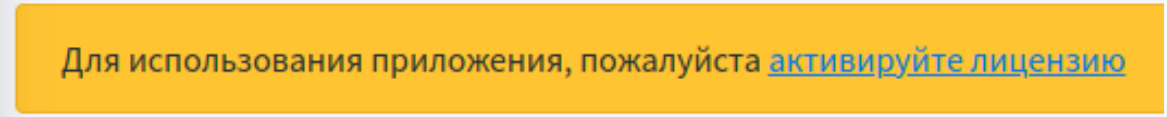
Лицензия — эта страница предназначена для активации и отображения информации о лицензии





Примечание

Если лицензия не активирована, на всех страницах будет показано уведомление с просьбой выполнить активацию



В уведомлении есть ссылка, которая при нажатии открывает страницу **«Лицензия»**

Как это работает

Лицензия определяет лимиты ресурсов и доступные функции сервера **RuDesktop**:

- максимальное количество подключаемых устройств
- максимальное количество одновременных подключений
- максимальное количество учётных записей пользователей
- доступность модулей UEM (управление политиками) и MDM (управление мобильными устройствами)
- срок действия

Активация выполняется одним из двух способов:

- **Онлайн** — сервер обращается к серверу активации **RuDesktop** напрямую, требуется доступ в интернет
- **Офлайн** — администратор отправляет запрос активации в письме, получает ответный лицензионный текст и вставляет его в форму на сервере

После успешной активации данные о лицензии кэшируются и сразу отображаются на странице

Важно

При активации лицензии без модуля **UEM** все фоновые задачи UEM-политик автоматически отключаются. Это нужно учитывать при переходе с UEM-лицензии на лицензию без UEM — ранее назначенные политики останутся, но не будут запускаться по расписанию

Параметры лицензии

В блоке информации об активной лицензии отображаются следующие параметры:

- Ключ лицензии — уникальный ключ активной лицензии
- Компьютеров и устройств — лимит подключаемых к серверу устройств и количество уже подключённых
- Активных подключений — лимит одновременных активных подключений и текущее количество активных подключений
- Аккаунтов пользователей — лимит учётных записей и количество уже созданных
- UEM функции — доступность модуля управления политиками
- MDM функции — доступность модуля управления мобильными устройствами
- Срок действия — дата и время окончания срока лицензии. Для бессрочной лицензии в поле отображается значение **«Не ограничен»**
- Версия лицензии — версия лицензионного контракта

Примечание

Для пробной (trial) лицензии в интерфейсе дополнительно отображается отметка **«Триальная версия»**. Пробная лицензия имеет ограниченный срок действия — после истечения сервер переходит в режим без активной лицензии

Активация лицензии

Подсказка

Ключ лицензии предоставляется менеджерами по продажам после покупки

Онлайн активация

Используется, если сервер имеет доступ в интернет — **RuDesktop** обращается к серверу активации напрямую и сохраняет результат

В блоке онлайн активации отображаются:

- Поле Ключ лицензии для ввода ключа
- Кнопка Активировать

Чтобы активировать лицензию в онлайн режиме:

1. В поле Ключ лицензии вставить полученный ключ
2. Нажать на кнопку Активировать

После успешной активации страница автоматически обновится и отобразит параметры новой лицензии

Офлайн активация

Используется, если сервер находится в закрытой сети без доступа к интернету. В этом случае активация выполняется через обмен текстовыми блоками: сервер генерирует запрос активации с привязкой к своему уникальному идентификатору, а отдел продаж выдаёт лицензионный текст для этого идентификатора

В блоке офлайн активации отображаются:

- Поле Запрос активации с уникальным запросом активации (генерируется автоматически на основе идентификатора сервера)
- Иконка копирования рядом с полем Запрос активации
- Поле Текст лицензии для вставки полученного лицензионного текста
- Кнопка Активировать

Чтобы активировать лицензию в офлайн режиме:

1. В поле Запрос активации скопировать значение, нажав на иконку копирования
2. Отправить скопированное значение и приобретённый ключ лицензии в письме на `sales@rudesktop.ru`
3. Получить ответное письмо с лицензионным текстом
4. Вставить лицензионный текст из ответного письма в поле Текст лицензии
5. Нажать на кнопку Активировать

После успешной активации страница автоматически обновится и отобразит параметры новой лицензии

> **Важно**
>
> Лицензионный текст выдаётся под конкретный сервер — попытка активировать его на другом сервере (с другим идентификатором) приведёт к ошибке. Если потребовалось перенести лицензию на другой сервер, обратитесь к менеджерам по продажам

Администрирование — раздел для настройки сервера **RuDesktop** на низком уровне: глобальные параметры (SMTP, мессенджеры, безопасность, мониторинг), интеграция с **KeyCloak**, маршрутизация (мосты, подсети), очередь фо-

новых задач, чёрный/белый списки подключений, сертификаты, QR-коды для MDM, профили Kickstart и управление лицензией

Подсказка

Раздел **«Администрирование»** доступен при использовании локального сервера **Удаленный доступ** или **Управление конфигурациями (UEM)**. Часть страниц (например, *Лицензия*, *Настройки*) видна только суперпользователю или пользователю с правом **Настройки → Просмотр**

Настройки

Глобальные настройки сервера

KeyCloak

Интеграция с KeyCloak для SSO

Подсети

Привязка диапазонов IP к геопозиции

Мосты

Серверы-ретрансляторы для удалённых филиалов

Точки распространения

Серверы для распространения файлов и пакетов

Очередь задач

Просмотр и управление фоновыми задачами сервера

Черный список

Запрет подключения устройств по различным признакам

Белый список

Разрешение подключения устройств по различным признакам

Сертификаты

Корневые сертификаты для проверки клиентов

QR-коды MDM

Подготовка устройств к управлению через MDM

Kickstart

Профили преднастройки клиента RuDesktop

Лицензия

Состояние и параметры активной лицензии

Руководство пользователя - описание работы в веб-интерфейсе сервера **RuDesktop**: вход и регистрация, навигация и панель управления, удалённый доступ к устройствам и сессии, централизованное управление через политики и задачи (UEM), сканирование сети, установка и обновления ОС, организационная структура (пользователи, группы, домены, подразделения), журналы аудита, инвентаризация ресурсов, отчёты и аналитика, хранилище файлов, а также настройки сервера и интеграций

Подсказка

Каждая страница раздела содержит блок **«Как это работает»** с кратким описанием логики работы и описание доступной функциональности - фильтров, массовых действий, столбцов таблицы, операций контекстного меню и свойств объекта

Регистрация

Регистрация на сервере

Авторизация

Авторизация на сервере и восстановление пароля

Панель управления

Дашборды и загрузка клиентов

Портал самообслуживания

Запросы в техническую поддержку и установка приложений из магазина

Удаленный доступ

Удаленные устройства, сессии и их свойства

Управление (UEM)

Политики, задачи и обращения

Сканирование сети
Обнаружение устройств и установка клиента RuDesktop

Обновления ОС
Поиск и офлайн-установка обновлений Windows

Установка OS
Образы OS, миграции и задачи миграции

Организация
Группы, домены и пользователи

Аудит
Описание логов

Инвентаризация
Описание справочника ресурсов УД

Отчеты
Построение и экспорт отчетов

Хранилище
Репозитории и файлы

Администрирование
Настройка и интеграции с сервером