Документация по продукту КриптоАРМ IDM

Версия 1.0

Документация КриптоАРМ IDM

КриптоАРМ IDM — это система класса Identity and Access Management (IAM / IDM), предназначенная для централизованного управления учетными записями и правами доступа пользователей в подключаемых информационных системах.

Здесь вы найдёте всё необходимое для успешной работы с системой.

Поиск и навигация

- **Используйте боковое меню** слева для перехода между разделами.
- **Следите за перекрёстными ссылками** в статьях — они ведут на связанные темы.

Обзор КриптоАРМ IDM — IDM система для управления идентификацией и доступом

КриптоАРМ IDM — это система класса Identity and Access Management (IAM / IDM), предназначенная для централизованного управления учетными записями и правами доступа пользователей в подключаемых информационных системах.

Содержание:

- Для каких задач подходит КриптоАРМ IDM
- Компоненты КриптоАРМ IDM
- Установка и настройка
- Основные модули КриптоАРМ IDM
- Смотрите также

Для каких задач подходит КриптоАРМ IDM

КриптоАРМ IDM предназначена для организаций, которым требуется централизованное управление доступом и учетными записями.

Система позволяет:

- управлять корпоративными пользователями и группами;
- строить организационную структуру (папки, подразделения, группы);
- синхронизировать пользователей из внешних систем;
- управлять ролями и доступами (RBAC);
- контролировать доступ к корпоративным ресурсам;
- объединять учетные записи из разных источников в единый профиль;
- обеспечивать единый вход в корпоративные системы.

Компоненты КриптоАРМ IDM

Система **КриптоАРМ IDM** состоит из двух взаимосвязанных компонентов: **ID** и **IDM**.

Компоненты работают совместно и образуют единую систему управления доступом и идентификацией.

ID отвечает за:

- авторизацию пользователей;
- управление профилями;
- способы входа;
- OAuth 2.0 и OpenID Connect;
- приложения и пользовательские сессии;
- личный кабинет пользователя;
- мини-виджет и каталог приложений.

> 💡 В экосистеме **КриптоАРМ IDM** система ID выступает как **Self Care Portal** для IDM — пользователь самостоятельно управляет своим профилем, настройками безопасности и персональными данными через интерфейс ID.
>
> 🔍 Подробнее о возможностях ID читайте в статье Описание системы ID.

IDM отвечает за корпоративное управление идентификацией и доступом:

- каталог пользователей;
- организационную структуру;
- группы и папки;
- RBAC-модель;
- корпоративные роли и ресурсы;
- синхронизацию пользователей через коннекторы.

Карта ответственности

Функция	ID	IDM
Аутентификация пользователей	✓	
Single Sign-On (SSO)	✓	
OAuth 2.0 / OpenID Connect	✓	
Управление профилем пользователя	✓	
Способы входа	✓	
Мини-виджет и личный кабинет	✓	
Каталог пользователей		✓
Организационная структура		✓
Группы и папки		✓

RBAC-модель	✓
Роли и ресурсы	✓
Коннекторы LDAP	✓
Импорт пользователей	✓
Сопоставление пользователей	✓

Установка и настройка КриптоАРМ IDM

Система **КриптоАРМ IDM** поставляется единым дистрибутивом, включающим оба компонента — **ID** и **IDM**.

При развертывании IDM автоматически устанавливаются и компоненты ID, используемые для аутентификации пользователей, управления профилями, приложениями и пользовательскими способами входа.

Подробное описание процесса установки и первого запуска приведено в инструкциях:

1. **Установка системы:**
   - Установка и первый запуск
   - Настройка переменных окружения
2. **Базовая настройка системы:**
   - Настройка системы (интерфейс, безопасность и доступ)
3. **Настройка компонентов ID, используемых в экосистеме IDM:**
   - Настройка профиля пользователя
   - Настройка способов входа
   - Настройка доверенных провайдеров
   - Настройка мини-виджета
   - Управление приложениями
   - Настройка шаблонов писем
   - Настройка уведомлений пользователей

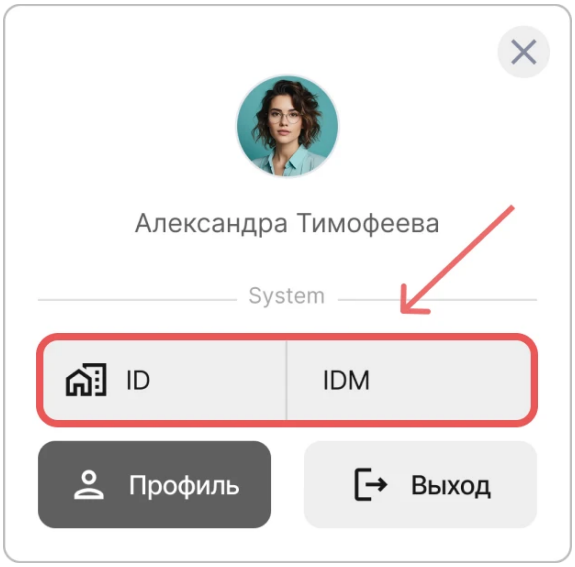
Доступ к IDM

Работа пользователя в IDM разделена между двумя интерфейсами:

Интерфейс	Назначение
ID	Вход в систему, профиль пользователя, способы входа, приложения
IDM	Управление каталогом, RBAC, коннекторами и корпоративной структурой

Переход в панель IDM осуществляется через мини-виджет системы.

Пример мини-виджета:



Для каждой организации и системы используется собственная панель IDM с отдельными настройками и структурой данных.

Основные модули КриптоАРМ IDM

Каталог

Каталог IDM представляет собой централизованную структуру хранения корпоративных пользователей, групп и подразделений.

Каталог поддерживает:

- папки и вложенные структуры;
- группы пользователей;
- корпоративные учетные записи;
- связи пользователей с внешними системами;
- импорт пользователей через коннекторы.

Структура каталога напоминает Active Directory или LDAP-каталог и позволяет организовать пользователей по подразделениям, проектам или организационным единицам.

RBAC

RBAC (Role-Based Access Control) — механизм ролевого управления доступом.

С помощью RBAC в IDM можно:

- создавать системы и ресурсы;
- назначать роли пользователям и группам;
- управлять доступом к корпоративным ресурсам;
- ограничивать доступ к приложениям на основе ролей.

RBAC-модель IDM интегрирована с приложениями компонента ID.

Коннекторы

Коннекторы обеспечивают интеграцию IDM с внешними корпоративными системами и каталогами пользователей.

Коннекторы используются для:

- импорта пользователей;
- синхронизации учетных записей;
- сопоставления пользователей;
- объединения учетных записей из разных систем;
- экспорта изменений обратно во внешние системы.

Лицензирование КриптоАРМ IDM

В IDM действует принцип: один коннектор — одна лицензия.

Это означает, что каждый подключенный внешний источник данных требует отдельной лицензии.

Подробная информация о лицензировании ID приведена в отдельной инструкции: Лицензирование ID.

> 💡 Добавление и привязка лицензии в IDM выполняется в настройках коннектора в разделе **Параметры подключения**.

Смотрите также

- Каталог в КриптоАРМ IDM — описание структуры каталога пользователей, групп и папок.
- RBAC модель в КриптоАРМ IDM — описание ролевой модели доступа, ресурсов, ролей и их связи с пользователями и группами.
- **Коннекторы в КриптоАРМ IDM — обзор коннекторов в КриптоАРМ IDM, включая принципы работы, типы интеграций и общую модель синхронизации с внешними системами.**

Как установить КриптоАРМ IDM

В этом руководстве вы узнаете, как установить SSO систему **КриптоАРМ IDM** через Docker на своем сервере. Мы пройдем весь путь — от подготовки окружения до первого входа администратора в систему.

Содержание:

- Требования к установке { #installation-requirements }

- Установка Docker и Docker Compose
- Установка системы
- Режимы запуска системы
- Учетные записи по умолчанию
- Первый вход в систему
- Полезные эндпоинты системы
- Смотрите также

Требования к установке

Системные требования сервера

Перед установкой системы **КриптоАРМ IDM** убедитесь, что ваша инфраструктура соответствует требованиям.

Системные требования зависят от планируемой нагрузки. Для тестовых сред достаточно минимальной конфигурации, для production-среды лучше использовать рекомендованные параметры.

Минимальная конфигурация

Компонент	Требования
Оперативная память (RAM)	4 ГБ
Дисковое пространство	50 ГБ SSD
Процессор (CPU)	2 ядра x86_64
Сетевой интерфейс	1 Гбит/с

Рекомендуемая конфигурация

Компонент	Требования
Оперативная память (RAM)	8 ГБ и более
Дисковое пространство	100 ГБ SSD/NVMe
Процессор (CPU)	4+ ядра x86_64
Сетевой интерфейс	1 Гбит/с и выше

> 💡 **Совет:** Для высоконагруженных систем с тысячами пользователей рекомендуется:

- 16+ ГБ оперативной памяти
- 8+ ядер процессора
- Использование NVMe дисков для максимальной скорости работы БД

Требования к программному обеспечению

Программное обеспечение

Компонент	Поддерживаемые версии	Дополнительная информация
Операционная	Ubuntu 18.04 LTS (Bionic Beaver),	Любой linux-дистрибутив

система	Ubuntu 20.04 LTS (Focal Fossa), Debian 11 (Bullseye)	с поддержкой Docker
Docker Engine	19.03+	-
Docker Compose	1.27+	-
Nginx/Apache	Любая современная версия	-

Общие требования

Для успешной установки и корректной работы **КриптоАРМ IDM** необходимо выполнить несколько условий:

- Наличие сервера с постоянным IP-адресом.
- Доступ ко всем рабочим станциям через порт, который будет использоваться для доступа к системе.
- Наличие сервера электронной почты (SMTP-сервера).
- Подключение к сервису должно осуществляться по протоколу HTTPS.

Установка Docker и Docker Compose

КриптоАРМ IDM разворачивается в виде набора Docker-контейнеров и может использоваться как корпоративный OAuth 2.0 Authorization Server и OpenID Connect Provider (IdP).

Документация Docker

Шаг 1. Установка Docker Engine

Для Ubuntu/Debian:

```
# Обновление пакетов
sudo apt update && sudo apt upgrade -y

# Установка зависимостей
sudo apt install -y apt-transport-https ca-certificates curl software-properties-common

# Добавление GPG-ключа Docker
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg

# Добавление репозитория
echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

# Установка Docker
sudo apt update
sudo apt install -y docker-ce docker-ce-cli containerd.io
```

```
# Проверка установки
sudo docker --version
```

Для CentOS/RHEL:

```
# Установка yum-utils
sudo yum install -y yum-utils

# Добавление репозитория Docker
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo

# Установка Docker
sudo yum install -y docker-ce docker-ce-cli containerd.io

# Запуск и автозагрузка Docker
sudo systemctl start docker
sudo systemctl enable docker

# Проверка установки
sudo docker --version
```

Шаг 2. Установка Docker Compose

```
# Скачивание Docker Compose
sudo curl -L "https://github.com/docker/compose/releases/latest/download/docker-
compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose

# Установка прав на исполнение
sudo chmod +x /usr/local/bin/docker-compose

# Проверка установки
docker-compose --version
```

> 💡 Требования к версиям: **Docker Engine 20.10+** и **Docker Compose 1.29+**. Для проверки используйте команды `docker --version` и `docker-compose --version`.

Установка системы

Шаг 1. Подготовка рабочей директории

Создайте и перейдите в директорию для установки:

```
# Создание директории
   mkdir cryptoarm-id && cd cryptoarm-id

# Проверка текущего пути
pwd  # Должно отобразить: /home/ваш_пользователь/trusted-id
```

Шаг 2. Загрузка конфигурационных файлов

Загрузите необходимые файлы конфигурации:

```
# Загрузка основных файлов
curl -O https://git.digtlab.ru/trusted/cryptoarm/id/-/raw/main/docker-compose.yaml
curl -O https://git.digtlab.ru/trusted/cryptoarm/id/-/raw/main/nginx.conf
curl -O https://git.digtlab.ru/trusted/cryptoarm/id/-/raw/main/build.sh
curl -O https://git.digtlab.ru/trusted/cryptoarm/id/-/raw/main/.env


# Проверка загрузки
ls -la
```

Скачанные файлы:

Файл	Назначение
docker-compose.yaml	Конфигурация Docker-контейнеров
nginx.conf	Настройки веб-сервера Nginx
build.sh	Скрипт настройки и сборки
.env	Переменные окружения и настройки

Шаг 3. Настройка прав доступа

Сделайте скрипт сборки исполняемым:

```
# Установка прав на скрипт сборки
chmod +x ./build.sh

# Проверка прав
ls -l build.sh
```

> ⚙ После установки рекомендуется выполнить базовую конфигурацию. Подробное описание всех параметров доступно в разделе Переменные окружения КриптоАРМ IDM.

Шаг 4. Настройка конфигурации

Отредактируйте файл `.env` с основными настройками:

```
# Открываем файл для редактирования (используйте nano или vim)
nano .env
```

Обязательные настройки:

```
# Основной домен системы
ID_HOST=id.example.ru  # Замените на ваш домен или IP

# Email администратора
ADMIN_MAIL=example@mail.ru  # Замените на реальный email
```

Шаг 5. Создание файла для хранения сертификатов

Создайте файл для хранения сертификатов и задайте права:

```
touch acme.json
chmod 600 acme.json
```

Шаг 6. Запуск скрипта сборки

Запустите скрипт настройки:

```
./build.sh
```

В результате выполнения в файле **nginx.conf** прописывается значение переменной **ID_HOST** и в файле **.env** прописываются переменные **CLIENT_ID** и **CLIENT_SECRET**.

Шаг 7. Запуск системы

Запустите проект:

```
docker compose up -d
```

Полезные команды Docker Compose

Команда	Описание	Пример использования
Просмотр логов	Отслеживание логов в реальном времени	`docker compose logs -f`
Остановка	Остановка всех контейнеров	`docker compose stop`
Запуск	Запуск остановленных контейнеров	`docker compose start`
Перезагрузка	Перезапуск всех контейнеров	`docker compose restart`
Статус	Просмотр состояния контейнеров	`docker compose ps`

Режимы запуска системы

В системе доступны три режима запуска проекта:

- **Production** — основной режим работы системы в рабочей среде.
- **Development** — режим для разработки и тестирования.
- **Safe-mode** — специальный режим для работы пользователя `root`. В этом режиме вход в систему разрешен только пользователю `root`, все остальные пользователи не могут авторизоваться.

Учетные записи по умолчанию

При установке системы автоматически создаются две учетные записи:

- `root` (логин: `root` / пароль: `changethis`): Учетная запись суперпользователя, которая игнорирует стандартные политики безопасности и способы аутентификации. Вход под `root` возможен только в режиме `safe-mode`.
- `admin` (логин: `admin` / пароль: `admin`): Административная учетная запись для первичного входа и настройки системы.

📌 Эти данные предоставляют полный доступ к системе. Обязательно измените пароль сразу после первого входа.

Первый вход в систему

Первый вход

Для входа в веб-интерфейс **КриптоАРМ IDM** необходимо перейти по адресу: `https://ID_HOST`.

1. На первом шаге виджета входа введите логин и нажмите **Войти**.
2. Введите пароль на втором шаге и нажмите **Войти**.

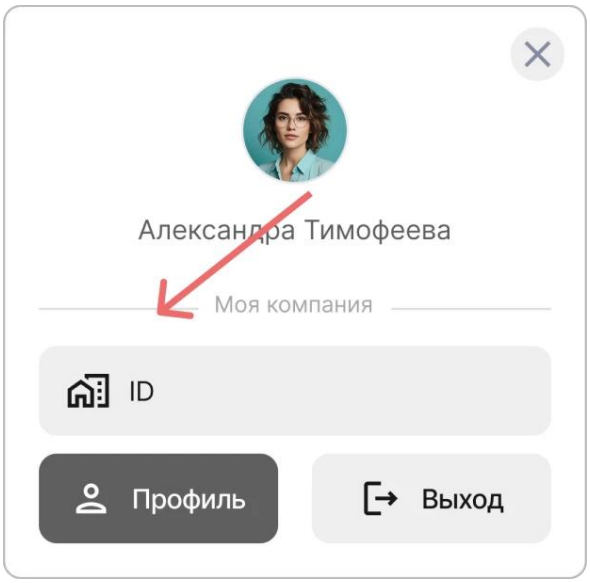
После авторизации произойдет переход в Профиль пользователя.

Переход в панель администратора

Настройки администрирования размещены в панели администратора.

Переход в панель администратора осуществляется через мини-виджет системы.

Пример мини-виджета:



Полезные эндпоинты системы

После успешной установки и настройки системы **КриптоАРМ IDM** вы можете использовать следующие URL для интеграции и ознакомления с API.

OpenID Connect Discovery

Стандартный endpoint для получения конфигурации OpenID Connect Provider (IdP) доступен по адресу:

```
https://ID_HOST/.well-known/openid-configuration
```

Замените `ID_HOST` на домен вашего сервера (значение переменной `ID_HOST` из файла **.env**). Этот документ содержит все необходимые данные для настройки клиентов:

- authorization_endpoint
- token_endpoint
- userinfo_endpoint
- jwks_uri
- issuer
- supported grant types, scopes и др.

Документация API (Swagger)

Интерактивная документация REST API доступна по адресу:

```
https://dev.trusted.plus
```

На этой странице описаны все доступные методы REST API для управления пользователями, клиентами, ролями и другими сущностями **КриптоАРМ IDM**. Документация позволяет тестировать запросы непосредственно из браузера.

Смотрите также

- Описание системы КриптоАРМ IDM — обзор функций системы **КриптоАРМ IDM**.
- Переменные окружения КриптоАРМ IDM — руководство по подготовке конфигурации перед запуском.
- Настройка системы — руководство по настройке интерфейса и доступа пользователей в систему.

Как настроить переменные окружения КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить переменные окружения **КриптоАРМ IDM** на вашем сервере. Мы подробно разберем все параметры — от базы данных и OIDC до кэша, почты и интерфейса, чтобы ваша система работала корректно с первого запуска.

Содержание:

- Общие переменные окружения
- Переменные окружения базы данных (PostgreSQL)
- Redis, сессии и OIDC cookies
- Ограничение скорости и логирование
- Метрики
- Смотрите также

> 💡 Чтобы изменить переменные окружения, нужно внести изменения в файл **docker-compose.yml**.

Общие переменные окружения

Эти переменные определяют базовое поведение и идентификацию сервиса.

Переменная	Описание	Значение по умолчанию
`NODE_ENV`	Среда выполнения приложения (`development` или `production`)	`production`
`DOMAIN`	Домен сервиса	—
`ADMIN_LOGIN`	Логин администратора	`root`
`ADMIN_PASSWORD`	Пароль администратора	`changethis`
`DELETE_PROFILE_AFTER_DAYS`	Количество дней, через которое профиль пользователя будет удален	`30`
`CLIENT_ID`	Уникальный идентификатор приложения (рекомендуется UUID)	—
`CLIENT_SECRET`	Уникальный секрет приложения (рекомендуется UUID)	—

> ⚠️ Переменные `CLIENT_ID` и `CLIENT_SECRET` используются для идентификации **КриптоАРМ IDM** как OAuth 2.0 / OpenID Connect клиента и должны храниться в секрете.

Переменные окружения базы данных (PostgreSQL)

Параметры для подключения к СУБД PostgreSQL.

Переменная	Описание	Значение по умолчанию
`POSTGRES_USER`	Имя пользователя для подключения к PostgreSQL	`user`
`POSTGRES_PASSWORD`	Пароль пользователя PostgreSQL	`password`
`POSTGRES_DB`	Название базы данных	`mydb`
`POSTGRES_HOST`	Хост базы данных	`localhost`
`POSTGRES_PORT`	Порт подключения к базе	`5432`
`DATABASE_URL`	Полная строка подключения в формате PostgreSQL	—

Redis, сессии и OIDC cookies

Настройки для хранения сессий, кэширования данных и безопасности аутентификации.

Переменная	Описание	Значение по умолчанию
`REDIS_HOST`	Хост Redis	`127.0.0.1`

`REDIS_PORT`	Порт Redis	`6379`
`OIDC_COOKIE_SECRET`	Секрет для подписи и проверки cookie	—
`OIDC_SESSION_TTL`	Время жизни сессии в секундах	`86400` (24 часа)

Ограничение скорости и логирование

Настройки для защиты от злоупотреблений и контроля логирования.

Переменная	Описание	Значение по умолчанию
`RATE_LIMIT`	Количество запросов для ограничения скорости	`15`
`RATE_LIMIT_TTL_SEC`	Период времени в секундах для лимита	`900`
`CONSOLE_LOG_LEVELS`	Уровни логирования для консоли	`log warn error`

Метрики

Переменная	Описание
`YANDEX_METRICA_ID`	ID для интеграции с Яндекс.Метрикой
`GOOGLE_METRICA_ID`	ID для интеграции с Google Analytics

Смотрите также

- Установка системы КриптоАРМ IDM — руководство по установке системы.
- **Настройка системы — руководство по настройке интерфейса и доступа пользователей в систему.**

Как настроить КриптоАРМ IDM: безопасность, интерфейс и доступ

В этом руководстве вы узнаете, как настроить интерфейс и локализацию **КриптоАРМ IDM**, создать типы приложений, управлять доступом пользователей, включить двухфакторную аутентификацию, а также настроить интеграции для логирования и мониторинга событий через **Sentry** и **Winston**.

Раздел предназначен для администраторов и специалистов по безопасности, которые хотят эффективно управлять настройками **КриптоАРМ IDM**.

Содержание:

- Интерфейс и локализация
- Безопасность и доступ
- Логирование
- Типы приложений
- Экспериментальные функции

- Смотрите также

  💡 Настройки системы размещены в панели ID. Для доступа к панели необходима роль **Администратор** сервиса. Как открыть панель ID →

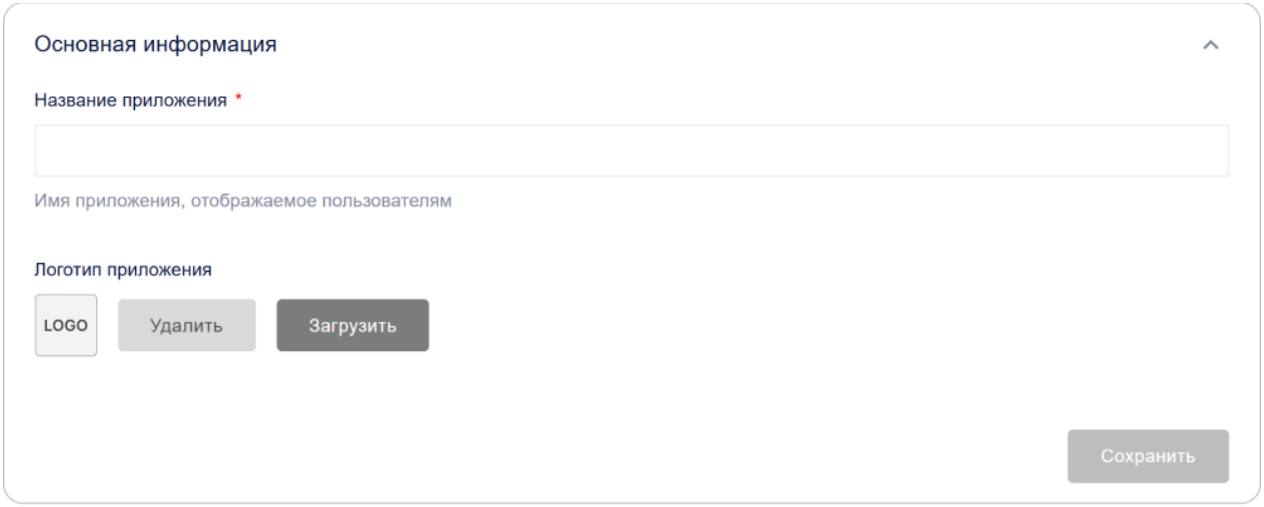
Интерфейс и локализация

Название системы и логотип

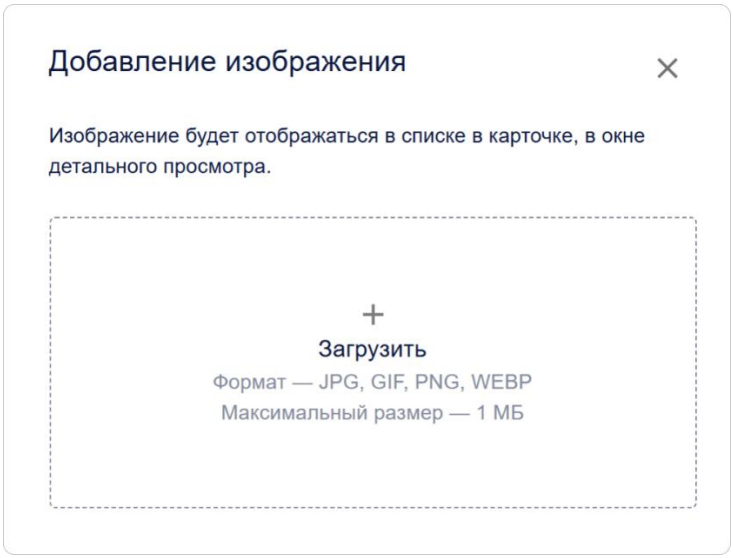
Название и логотип отображаются в интерфейсе системы **КриптоАРМ IDM**, а также в мини-виджете и виджете входа.

Чтобы настроить название и логотип:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Основная информация**.



3. Укажите новое название в поле **Название приложения**.
4. В блоке **Логотип приложения** нажмите **Загрузить** и выберите файл с логотипом.



⚡ Допустимые форматы: JPG, GIF, PNG, WEBP; максимальный размер 1 МБ.

5. Настройте отображение и нажмите **Применить**.

6. Нажмите **Сохранить**.

💡 **Совет:** Используйте SVG-формат для векторного логотипа, чтобы обеспечить четкое отображение на всех устройствах и разрешениях экрана.

Локализация

КриптоАРМ IDM поддерживает интерфейс на **шести языках**:

- Русский (ru)
- English (en)

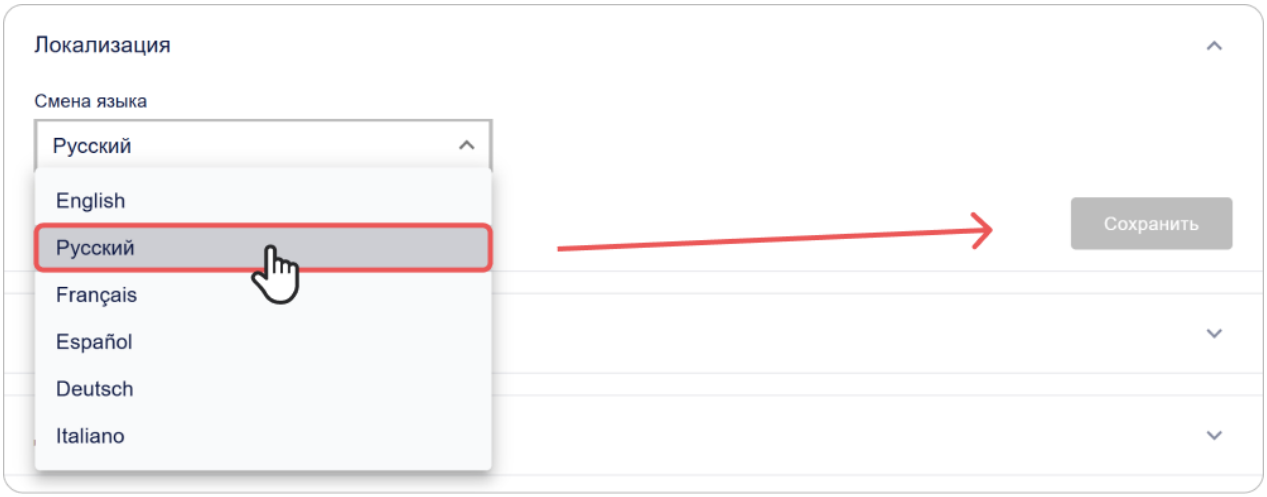
- Français (fr)
- Español (es)
- Deutsch (de)
- Italiano (it)

Выбранный язык влияет на отображение текста во всех интерфейсах **КриптоАРМ IDM**, включая виджет входа и мини-виджет.

Если вы используете дополнительные поля профиля пользователя и шаблоны писем — убедитесь, что они отображаются правильно.

Как изменить язык интерфейса

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Локализация** и выберите необходимый язык из списка.



3. Нажмите **Сохранить**.

Изменение языка произойдет автоматически, без перезапуска сервиса или обновления страницы.

> 🚨 **Предупреждение:** После смены языка все тексты в интерфейсе, включая системные сообщения и уведомления, будут отображаться на выбранном языке. Убедитесь, что ваши пользователи понимают выбранный язык.

Стилизация

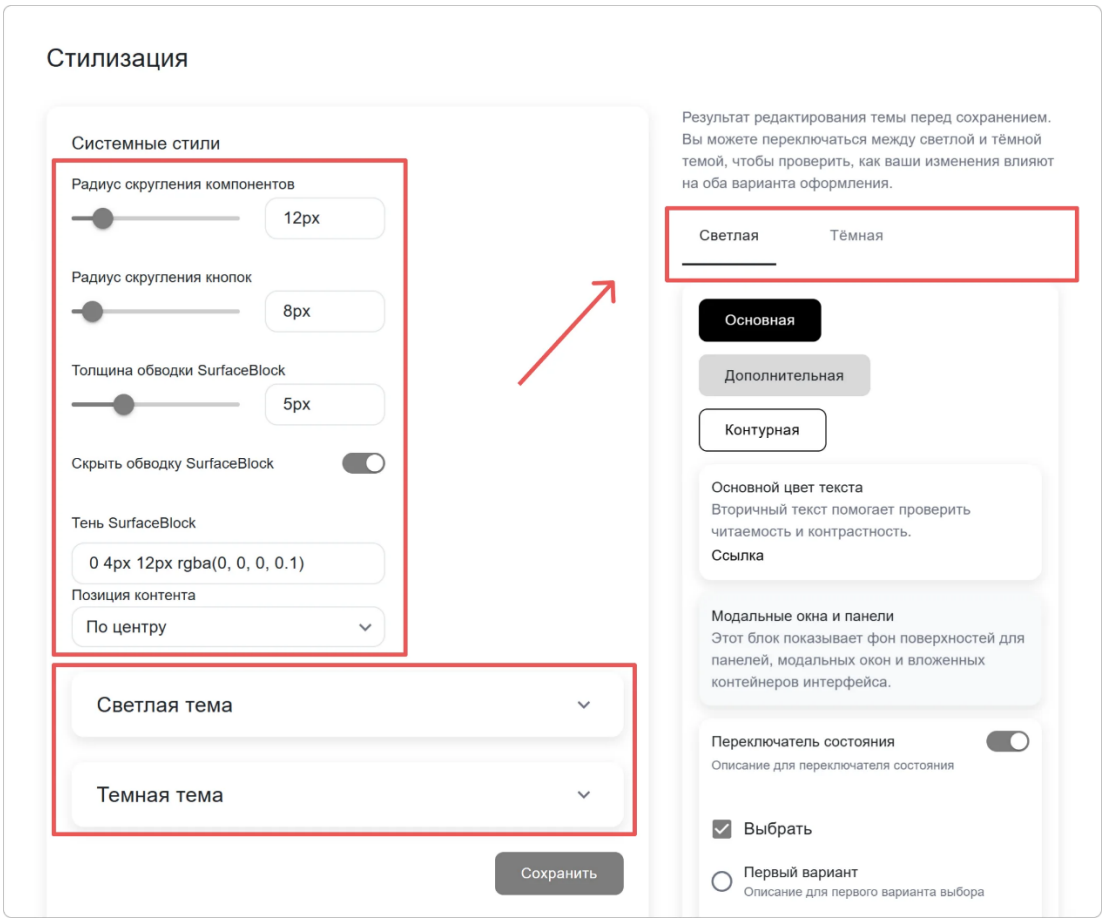
Раздел **Стилизация** позволяет настроить внешний вид системы: цвета, скругления, тени и поведение интерфейсных элементов (кнопок, карточек, вкладок и ссылок).

Настройки применяются ко всему интерфейсу и поддерживают отдельную конфигурацию для светлой и тёмной темы.

Настройка стилей

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Стилизация** и нажмите **Настроить**.

3. Настройте системные параметры:
   - **Радиус скругления компонентов** — Определяет радиус углов карточек, полей и меню. Чем больше значение — тем более “мягкие” углы.
   - **Радиус скругления кнопок** — Настраивает радиус углов всех кнопок. Можно связать с блоками, чтобы они выглядели одинаково.
   - **Толщина обводки SurfaceBlock** — Регулирует толщину границы вокруг компонентов. Работает только если включена внутренняя обводка SurfaceBlock.
   - **Скрыть обводку SurfaceBlock** — Показывает или скрывает границу блоков.
   - **Тень SurfaceBlock** — Добавляет тень под блоки и карточки для эффекта глубины (пример записи: `0 4px 12px rgba(0, 0, 0, 0.1)`).
   - **Позиция контента** - Позволяет выбрать, где на странице будет отображаться основной контент: слева, по центру или справа.
4. Укажите цвета для светлой и темной темы в HEX-формате.



5. Проверьте результат в области предпросмотра справа. Вы можете переключаться между светлой и тёмной темой, чтобы оценить изменения.
6. Нажмите **Сохранить**.

Копирайт и ссылка на справку

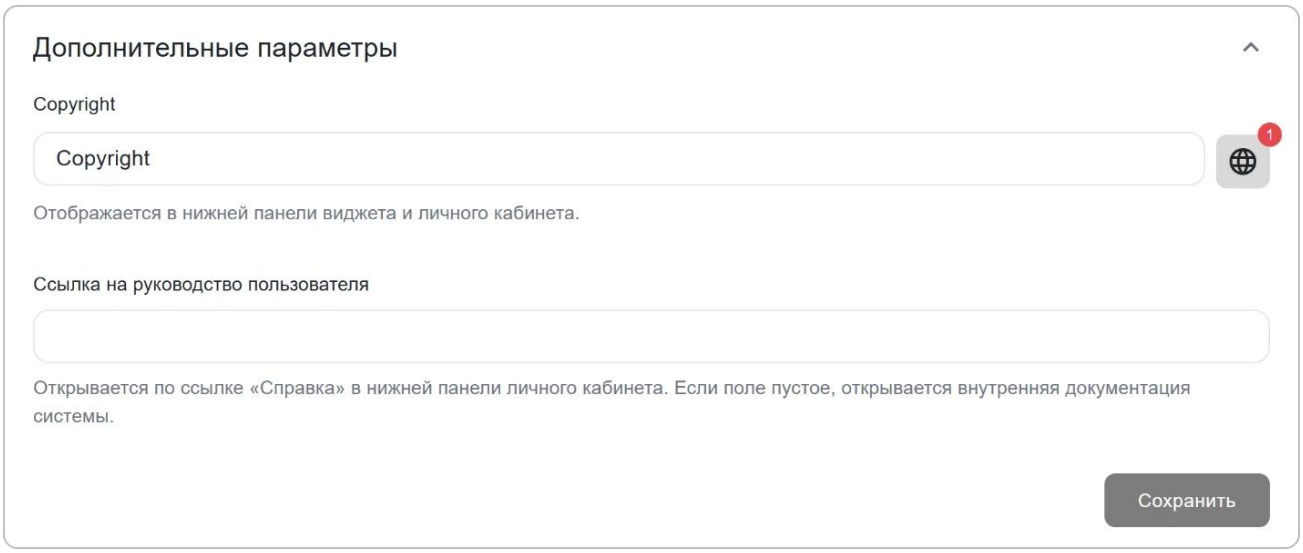
В блоке **Дополнительные параметры** можно настроить:

- **копирайт**, отображаемый в нижней панели виджета и интерфейса системы;
- **ссылку на руководство пользователя**, доступную по ссылке **Справка** в нижней панели интерфейса системы.

  ⚠️ Если ссылка на руководство не указана, при переходе по ссылке **Справка** открывается встроенная документация системы.

Как настроить копирайт и ссылку на справку

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Дополнительные параметры**.

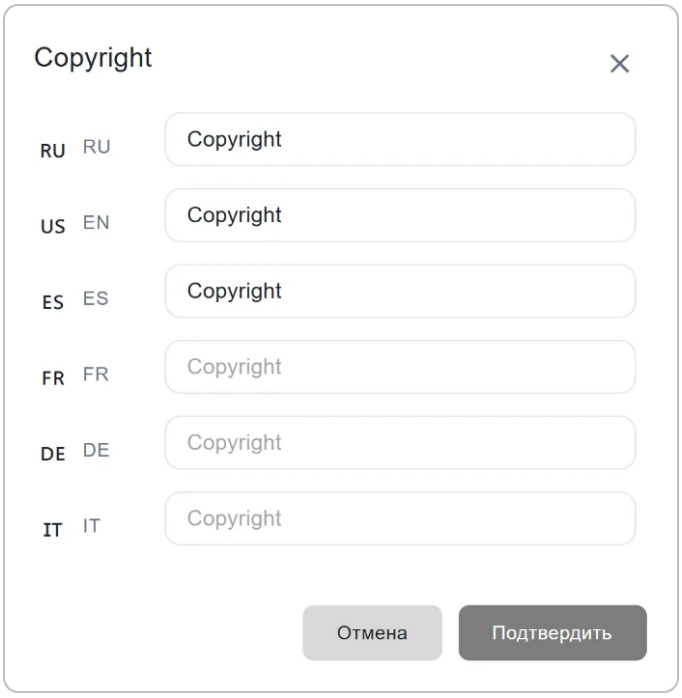


3. Укажите значение в поле **Copyright**.

   Для настройки значений на других языках не требуется менять язык системы.

   Нажмите на кнопку **Другие языки** и в открывшемся окне задайте значения для нужных локализаций.

   💡 Счётчик на кнопке **Другие языки** показывает количество добавленных переводов.



4. Укажите URL страницы с пользовательской документацией в поле **Ссылка на руководство пользователя**.
5. Нажмите **Сохранить**.

Безопасность и доступ

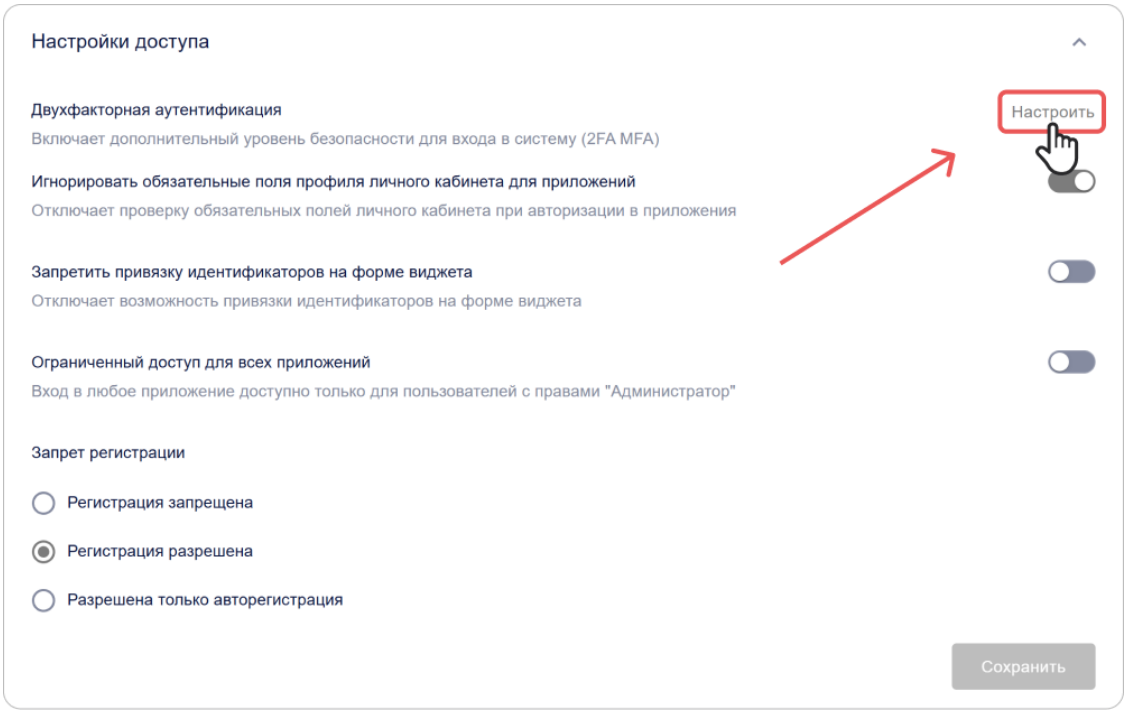
Настройки доступа

Двухфакторная аутентификация

Двухфакторная аутентификация (2FA) добавляет дополнительный уровень защиты при входе в систему. После ввода первого фактора (логин/пароль или другой способ аутентификации) пользователь должен подтвердить свою личность вторым фактором (телефон, электронная почта, WebAuthn).

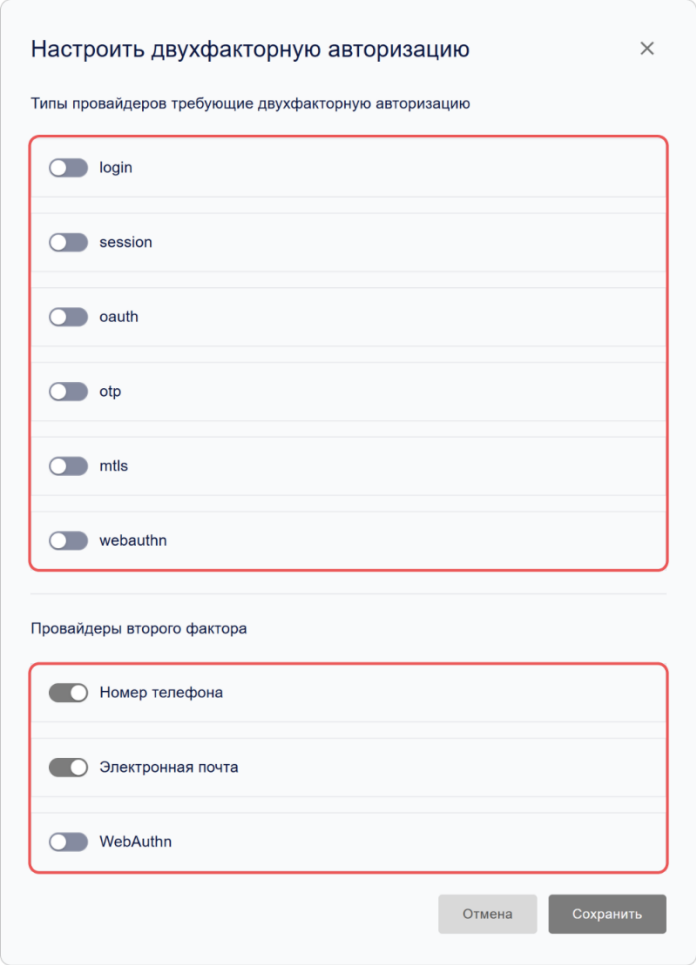
Чтобы настроить двухфакторную аутентификацию:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа** и нажмите **Настроить**.



3. Укажите провайдеры первого и второго факторов:

   - Провайдер **первого фактора** — основной способ аутентификации (логин/пароль или другой способ аутентификации).
   - Провайдер **второго фактора** — способ подтверждения личности (телефон, e-mail, WebAuthn).



4. Нажмите **Сохранить**.

Игнорирование обязательных полей профиля при входе в приложение

Некоторые поля профиля пользователя (например, телефон, почта и прочие) могут быть отмечены как обязательные для заполнения в профиле.

По умолчанию при авторизации в приложения **КриптоАРМ IDM** проверяет наличие всех обязательных полей и может приостанавливать вход, пока пользователь не заполнит недостающие данные. Настройка **Игнорировать обязательные поля профиля личного кабинета для приложений** позволяет отключить эту проверку.

Это может быть полезно, если организация использует внешние источники данных о пользователях и не требует заполнения профиля вручную.

Что будет при включении настройки:

- Пользователи смогут авторизоваться в приложениях, даже если их профиль в системе заполнен не полностью.
- Проверка обязательных полей выполняться не будет.
- В интерфейсе системы уведомления о незаполненных полях сохраняются.

Как включить настройку

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа**.
3. Включите переключатель **Игнорировать обязательные поля профиля личного кабинета для приложений**.
4. Нажмите **Сохранить**.

После применения настройки пользователи смогут проходить авторизацию без проверки обязательных полей профиля.

> 💡 **Рекомендация**: Включайте опцию только в том случае, если контроль полноты профиля осуществляется другими средствами.

Запрет привязки идентификаторов

Эта настройка запрещает пользователям самостоятельно привязывать новые внешние идентификаторы к своему профилю через виджет входа.

Чтобы запретить привязку:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа**.
3. Активируйте переключатель **Запретить привязку идентификаторов на форме виджета**.
4. Нажмите **Сохранить**.

Ограничения доступа

Эта настройка позволяет ограничить вход в приложение для всех пользователей, кроме **Администратор** сервиса. Все остальные пользователи не смогут авторизоваться.

> 🚨 **Важно:** при включении ограничения доступа все пользователи, кроме администраторов сервиса, потеряют возможность входа. Используйте настройку для технических работ или аварийных ситуаций.

Чтобы ограничить доступ:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа**.
3. Активируйте переключатель **Ограниченный доступ для всех приложений**.
4. Нажмите **Сохранить**.

Запрет регистрации

Эта настройка позволяет запретить создание новых аккаунтов в виджете входа.

Чтобы настроить запрет регистрации:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа**.

3. Выберите необходимую настройку:
   - **Регистрация запрещена** — полностью блокирует создание новых аккаунтов.
   - **Регистрация разрешена** (по умолчанию) — стандартный режим работы, пользователи могут создавать аккаунты самостоятельно.
4. Нажмите **Сохранить**.

Управление удаленными пользователями

Эта группа настроек определяет поведение системы с пользователями, которые были переведены в статус **Удален**. Вы можете разрешить или запретить самовосстановление таких учётных записей, а также задать срок, после которого пользователь будет окончательно удалён из базы данных.

> 💡 Статус **Удален** — это промежуточное состояние, в которое пользователь переводится при удалении. В этом статусе пользователь не может войти в систему, но его данные сохраняются.

Чтобы настроить удаление пользователей:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Дополнительные параметры**.
3. Найдите переключатель **Запретить восстановление УЗ из статуса УДАЛЕН** и установите нужное положение.
   - Если выключено, пользователь, после удаления своей учетной записи, сможет восстановить ее в личном кабинете.
   - Если включено, в личном кабинете пользователя пропадает кнопка восстановления.
4. В поле **Срок окончательного удаления пользователя** введите нужное значение (0, 1 или другое целое число).
   - **0** – пользователь удаляется немедленно после нажатия кнопки **Удалить**.
   - **1** – пользователь никогда не удаляется окончательно.
   - **Любое другое положительное число** (например, 30) – пользователь будет автоматически окончательно удален через указанное количество дней после перевода в статус **Удален**.
5. Нажмите **Сохранить**.

Технические параметры

Технические настройки, такие как идентификаторы клиента, параметры безопасности, URL-адреса авторизации, способы аутентификации клиента и параметры токенов и другие, находятся в разделе **Параметры приложения**.

> 📌 Ниже перечислены настройки, доступные для редактирования в панели администратора. Остальные параметры изменяются через конфигурационный файл.

Чтобы изменить параметры в панели администратора:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Параметры приложения**.
3. Настройте параметры:
   - Ограничение доступа
   - Время аутентификации
   - Токен доступа
   - Токен обновления
4. Нажмите **Сохранить**.

Описание параметров

Основные идентификаторы

Название	Параметр	Описание
Идентификатор (client_id)	`client_id`	Уникальный идентификатор приложения
Секретный ключ (client_secret)	`client_secret`	Конфиденциальный ключ приложения
Адрес приложения	-	Базовый URL сервиса **КриптоАРМ IDM** в формате `протокол://доменное имя:порт`

Ограничение доступа

Ограничивает вход в систему только пользователям с административными ролями.

Название	Описание
Ограниченный доступ	Если включено, доступ в систему будет разрешён только пользователям с правами **Администратор** сервиса

Возвратный URL

Название	Параметр	Описание
Возвратный URL #	`Redirect_uri`	URL, на который пользователь будет перенаправлен после успешной аутентификации

URL выхода из системы

Название	Параметр	Описание
URL выхода из системы #	`post_logout_redirect_uri`	URL, на который сервис будет перенаправлять пользователя после выхода. Если значение не указано, то используется `Redirect_uri`.

URL запроса аутентификации

Название	Параметр	Описание
URL запроса аутентификации	`request_uris`	Список URL для размещения JWT-

или восстановления после аутентификации #

запросов авторизации `Request Object`. Сервер извлекает JWT с указанного URL при авторизации.

Типы ответов

Название Параметр Описание

| **Тип ответов (response_types)** | `response_types` |

Определяет какие токены и коды возвращаются авторизационным сервером:

- `code` — только код авторизации - `id_token` — только ID токен - `code id_token` — код + ID токен - `code token` — код + токен доступа - `code id_token token` — код + ID токен + токен доступа - `none` — только подтверждение аутентификации

Типы предоставления доступа

Название Параметр Описание

| **Типы предоставления доступа (grant_types)** | `grant_types` |

Способы получения авторизации:

- `authorization code` — безопасный код через сервер клиента (рекомендуется); - `implicit` — прямое получение токена (для публичных клиентов) - `refresh_token` — обновление токена без повторного входа |

Метод аутентификации клиента

> 💡 Выбор метода зависит от требований безопасности и возможностей клиента. JWT-методы обеспечивают повышенную безопасность, так как не передают секрет напрямую.

Название Параметр Описание

| **Аутентификация клиента** | `token_endpoint_auth_method`, `introspection_endpoint_auth_method`, `revocation_endpoint_auth_method` |

Определяет метод аутентификации клиента при обращении к различным конечным точкам (`token`, `introspection`, `revocation`).

Доступные методы: - `none` — без учетных данных; - `client_secret_post` — учетные данные в теле запроса; - `client_secret_basic` — HTTP Basic Authentication; - `client_secret_jwt` — JWT, подписанный секретом клиента; - `private_key_jwt` — JWT, подписанный приватным ключом клиента.

|

Алгоритм подписи ID токена

Название Параметр Описание

| **Алгоритм подписи, используемый при создании подписанного ID-токена (id_token_signed_response_alg)** | `id_token_signed_response_alg` |

Указывает алгоритм, который используется для подписи ID токена.

`ID токен` — это JSON Web Token (JWT), который содержит утверждения (claims) о аутентификации пользователя |

Время аутентификации

Название	Параметр	Описание
Проверка наличия времени Аутентификации (require_auth_time)	`require_auth_time`	Если включено, в ID токене добавляется `auth_time` — время последней аутентификации пользователя

Дополнительные параметры безопасности

Название	Параметр	Описание

| Параметр для обеспечения безопасности передачи данных между клиентом и сервером авторизации | `require_signed_request_object` |

Указывает, требуется ли подписанный `Request Object` при отправке запроса на авторизацию.

`Request Object` — это способ безопасной передачи параметров авторизации от клиента к серверу авторизации, обычно в форме JWT (JSON Web Token).

Когда `require_signed_request_object` включен, клиент должен подписать `Request Object` с использованием заранее согласованного алгоритма подписи, который указан в конфигурации клиента.

|

Тип передачи идентификатора пользователя

Название	Параметр	Описание

| **Способ передачи ID пользователя в идентификационном токене (subject_type)** | `subject_type` | Определяет, как формируется `sub claim` в ID токене:

- `public` — один и тот же идентификатор для всех клиентов `- pairwise` — уникальный идентификатор для каждого клиента, повышает конфиденциальность

Токен доступа

Название	Параметр	Описание
Токен доступа (access_token_ttl)	`access_token_ttl`	Время жизни `access_token` в секундах

Токен обновления

Название	Параметр	Описание
Токен обновления (refresh_token_ttl)	`refresh_token_ttl`	Время жизни `refresh_token` в секундах

Журнал событий

В **Журнале** можно увидеть, откуда и с каких устройств пользователи заходили в систему или приложения.

Для каждого события доступен просмотр подробных сведений.

Параметр	Что содержит
Заголовок события	Категория действия
Дата и время	Точные временные метки
Приложение	Идентификатор (`client_id`) приложения
Пользователь	Идентификатор (`id`) пользователя
Устройство	Тип устройства и браузер
Местоположение	IP-адрес

Как перейти в журнал

1. Перейдите в панель ID.
2. Откройте вкладку **Журнал**.

Логирование

Sentry

Sentry — это платформа для мониторинга ошибок и производительности приложений.

> 📚 Официальный ресурс Sentry

Подключение **Sentry** позволяет:

- отслеживать ошибки и исключения в реальном времени;
- получать трассировки событий по пользователям;
- анализировать производительность системы.

Шаг 1. Создание проекта в Sentry

1. Перейдите на сайт Sentry.io.
2. Зарегистрируйтесь или войдите в свою учетную запись.
3. Создайте новый проект.

После создания проекта **Sentry** предоставит **DSN (Data Source Name)** — уникальный идентификатор для подключения **КриптоАРМ IDM** к **Sentry**.

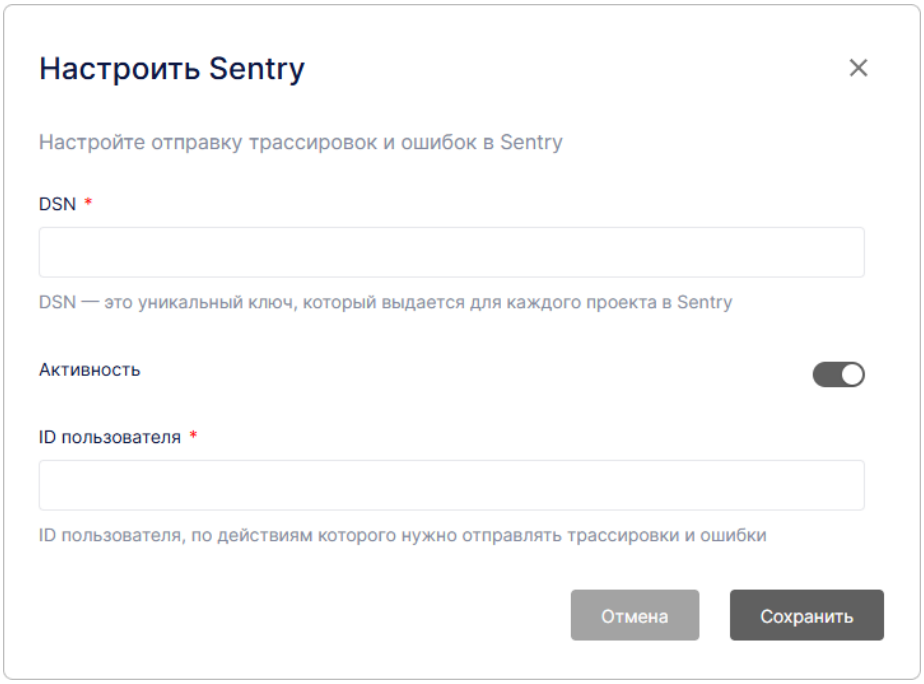
> 💡 **Совет**: Скопируйте **DSN (Data Source Name)**, чтобы не потерять его при переходе к следующему шагу.

Шаг 2. Подключение Sentry

Чтобы подключить **Sentry**:

1. Перейдите в панель ID → вкладка **Настройки**.

2. Раскройте блок **Логирование** и нажмите **Настроить** на панели **Sentry**.
3. В открывшейся форме подключения укажите:
   - **DSN** — уникальный идентификатор, созданный на **шаге 1**.
   - **Активность** — включите, чтобы начать отправку ошибок и трассировок в **Sentry**.
   - **ID пользователя** (при необходимости) — укажите, если нужно отслеживать ошибки и события по конкретным пользователям.



4. Нажмите **Сохранить**.

Winston

В **КриптоАРМ IDM** предусмотрена возможность экспорта логов во внешние системы через модуль логирования. Для этого используется конфигурируемый экспорт на базе логгера **Winston**.

📚 Официальный ресурс Winston

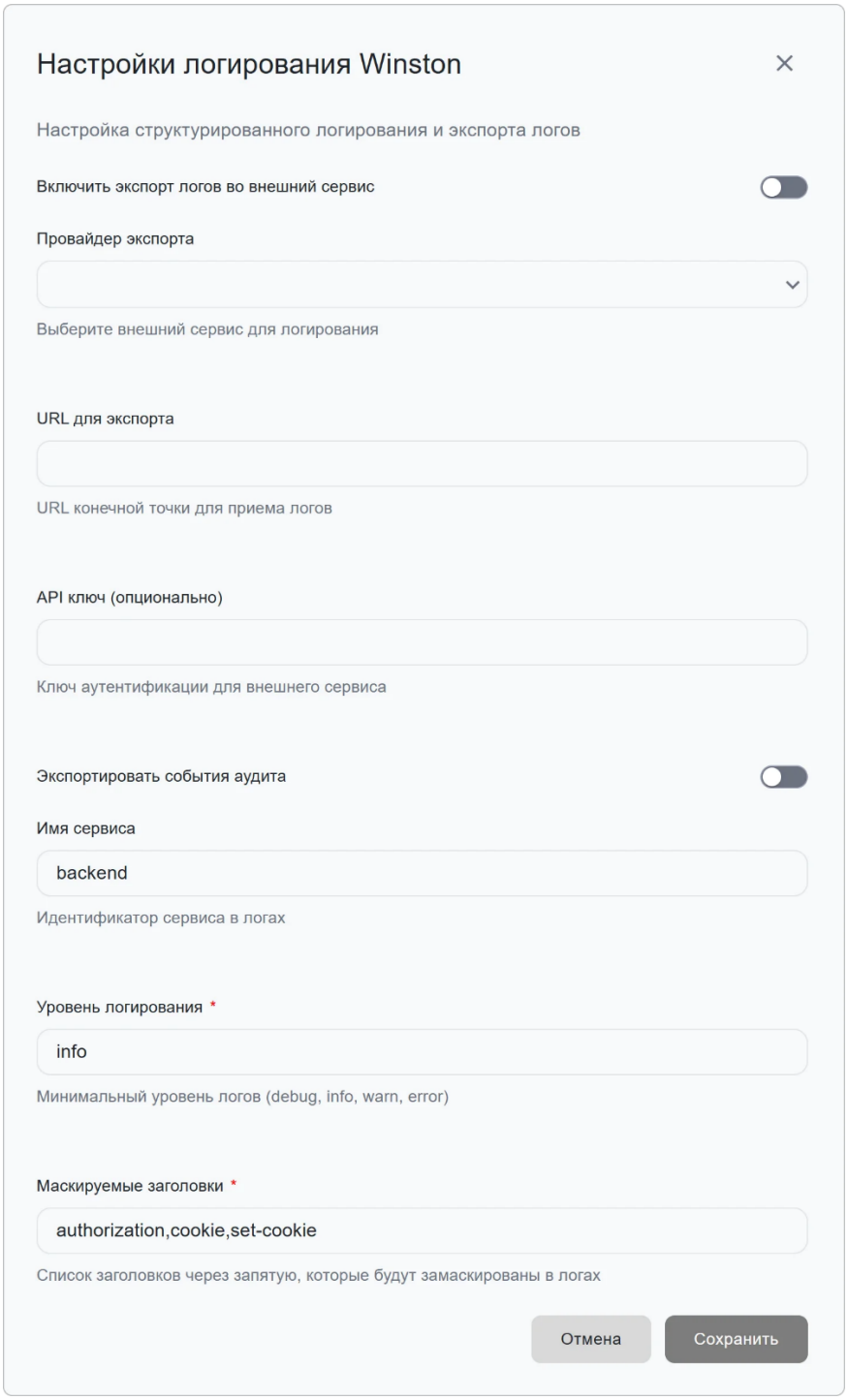
Экспорт логов позволяет:

- отправлять системные и прикладные логи во внешние системы;
- централизованно собирать логи из разных компонентов;
- интегрироваться с системами мониторинга (например, Loki, Graylog, HTTP-агрегаторы);
- настраивать уровень детализации логирования.

Как настроить экспорт логов

Чтобы подключить **Winston**:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Логирование** и нажмите **Настроить** на панели **Winston**.
3. В открывшейся форме подключения укажите:
   - **Включить экспорт логов во внешний сервис** — активирует отправку логов.
   - **Провайдер экспорта** — внешний сервис для логирования (Loki, HTTP, Graylog, Stdout).
   - **URL для экспорта** — URL конечной точки для приема логов.
   - **API ключ (опционально)** — ключ аутентификации для внешнего сервиса.
   - **Экспортировать события аудита** — включает отправку audit-событий.
   - **Уровень логирования** — минимальный уровень логов (`debug`, `info` (по умолчанию), `warn`, `error`).
   - **Маскируемые заголовки** — список HTTP-заголовков, которые будут скрыты в логах (по умолчанию: `authorization, cookie, set-cookie`)
4. Нажмите **Сохранить**.



Типы приложений

Типы приложений — это категории для систематизации приложений в **каталоге**. Они помогают организовать структуру и упростить навигацию пользователей.

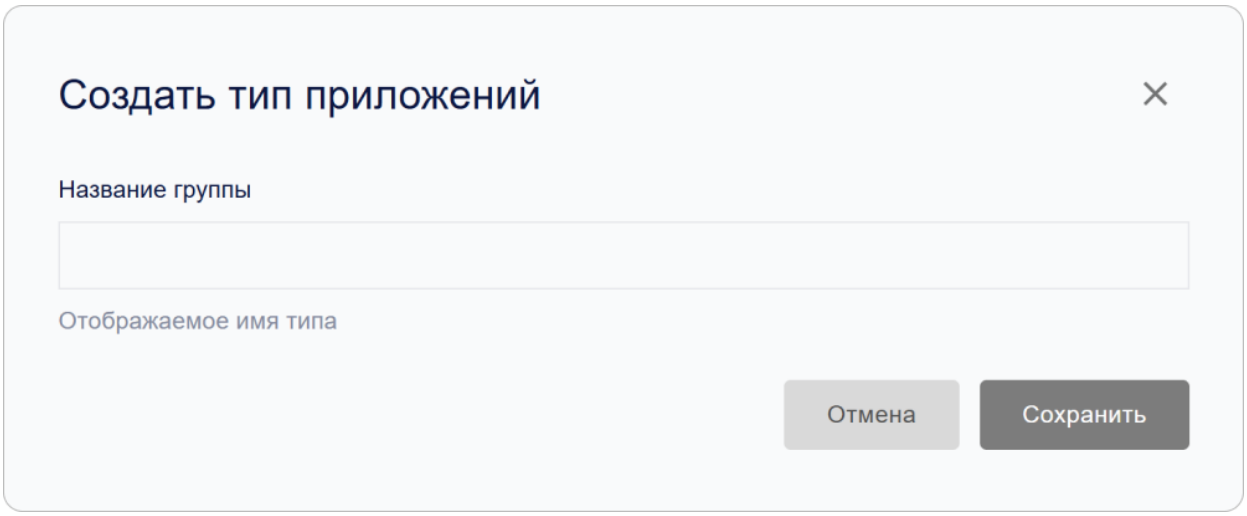
Зачем нужны типы:

- Помогают группировать приложения по категориям

- Упрощают поиск нужных приложений
- Помогают организовывать структуру каталога

Создание типа приложения

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Типы приложений** и нажмите **Настроить**.
3. В появившемся окне нажмите на кнопку **Создать** .
4. Откроется форма создания.



5. Укажите название типа.

   💡 Название типа должно быть уникальным в рамках системы.

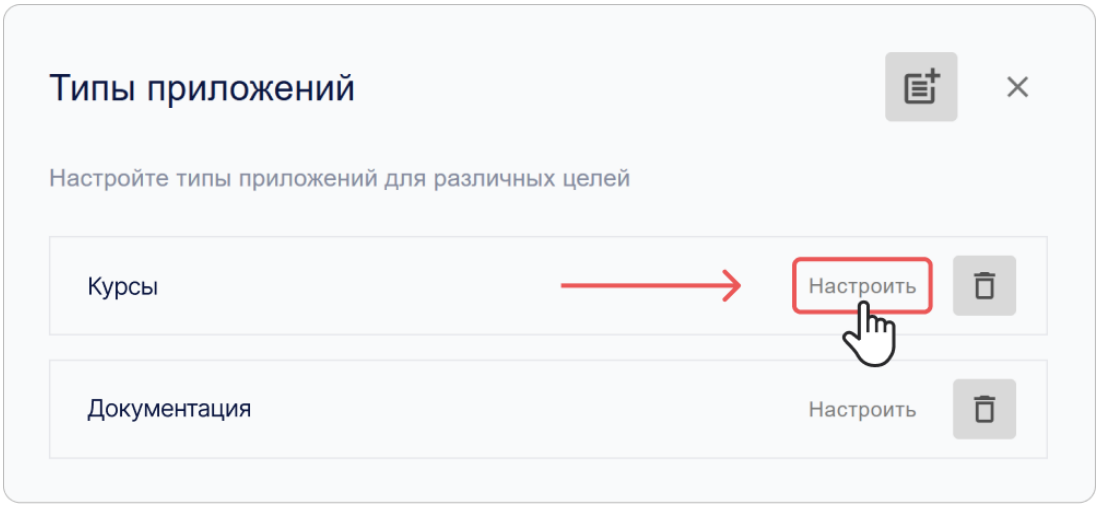
6. Нажмите **Сохранить**.

   Созданный тип отобразится в списке.

   💡 Назначение типа осуществляется при создании приложения.

Редактирование типа приложения

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Типы приложений** и нажмите **Настроить**.
3. Откроется окно со списком типов.



4. Нажмите на кнопку **Настроить** на панели с типом, который необходимо отредактировать.
5. Откроется форма редактирования.
6. Внесите необходимые изменения.
7. Нажмите **Сохранить**.

> 💡 После редактирования типа все связанные приложения автоматически получают обновленное название категории.

Удаление типа приложения

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Типы приложений** и нажмите **Настроить**.
3. Откроется окно со списком типов.
4. Нажмите на кнопку **Удалить** на панели с типом, который необходимо удалить.

Удаление происходит без дополнительного подтверждения.

> 💡 После удаления тип будет удалён из каталога, а приложения, у которых он был назначен, автоматически получат тип **Прочее**.

Экспериментальные функции

Экспериментальные функции — это новые возможности сервиса **КриптоАРМ IDM**, находящиеся на стадии тестирования и доработки.

Основные характеристики:

- Регулируются администратором сервиса
- Функционал может изменяться без предварительного уведомления
- Содержат недокументированные особенности работы
- Производительность и стабильность могут отличаться от основных функций

Раздел с экспериментальными функциями доступен по адресу: `https://ID_HOST/experimental`.

> 🚧 **Статус**: Экспериментальные функции могут быть удалены, изменены или переведены в основной функционал без предварительного уведомления.

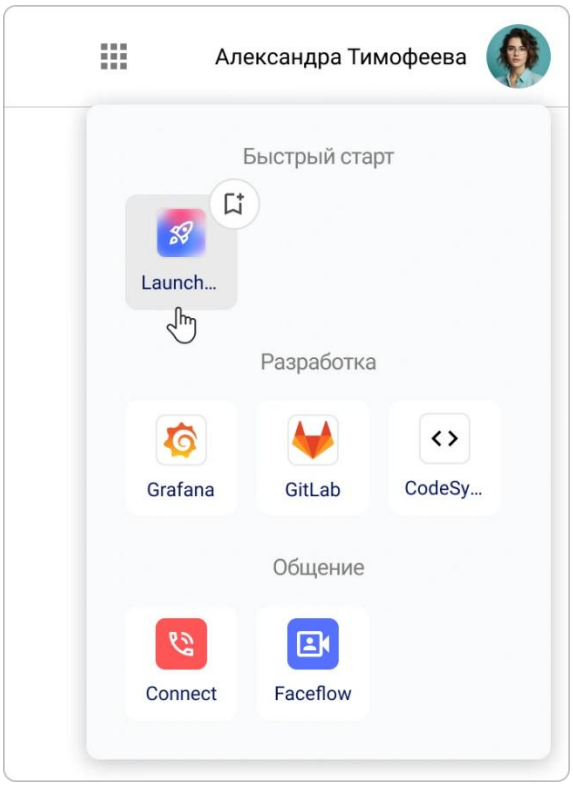
Какие функции доступны

1. **Визитка пользователя**
   - Цифровой аналог визитной карточки с контактными данными
   - Поддержка формата vCard для экспорта
   - Возможность делиться по ссылке или через QR-код

   Подробнее о визитке →

2. **Каталог приложений**
   - Централизованная площадка для приложений системы **КриптоАРМ IDM**
   - Содержит удобную систему категорий
   - Возможность добавлять приложения в избранные

   Подробнее о каталоге →



Смотрите также

- Настройка парольной политики и профиля пользователя — руководство по настройке профилей пользователей.

- Способы входа и настройка виджета входа — руководство по подключению и настройке внешних сервисов аутентификации.
- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.

Обзор КриптоАРМ ID — SSO система единого входа

КриптоАРМ ID — это Single Sign-On (SSO) система для централизованной аутентификации пользователей и управления доступом к корпоративным приложениям.

Система обеспечивает безопасную централизованную аутентификацию с поддержкой SSO, OAuth 2.0, OpenID Connect и двухфакторную проверку личности.

Для каких задач подходит КриптоАРМ ID

КриптоАРМ ID — система для организации централизованного входа пользователей на корпоративные информационные ресурсы с использованием единой учетной записи.

КриптоАРМ ID ориентирован на компании, которым требуется:

- **Единое окно входа** для внутренних и внешних сервисов
- **Централизованное управление доступом** для разных категорий пользователей (сотрудники, подрядчики, клиенты)
- **Повышенная безопасность** с поддержкой многофакторной аутентификации
- **Строгий контроль и аудит** действий пользователей
- **Безопасная интеграция** множества приложений с разными системами аутентификации

Основные возможности КриптоАРМ ID

1. Аутентификация и вход

Система обеспечивает централизованную аутентификацию и поддержку нескольких протоколов и методов аутентификации.

Поддерживаемые протоколы

- **OpenID Connect (OIDC)** — аутентификация пользователей и передача идентификационных данных
- **OAuth 2.0** — авторизация и управление доступом к ресурсам

Методы аутентификации

- **Базовые методы**: логин и пароль, электронная почта,
- **Внешние провайдеры идентификации**: социальные сети, доверенные корпоративные системы и другие сервисы,

- **Усиленные и беспарольные методы:** криптографическая аутентификация через **mTLS** (клиентские сертификаты) и **WebAuthn** (биометрия, аппаратные ключи), а также одноразовые пароли **TOTP/HOTP**.

Двухфакторная аутентификация (2FA / MFA)

КриптоАРМ ID поддерживает многофакторную аутентификацию (MFA), при которой доступ предоставляется только после успешного подтверждения личности пользователя несколькими независимыми факторами (знание, владение, биометрия).

2. Управление приложениями и пользователями

- **Создание и настройка приложений:** веб-приложения, нативные приложения
- **Кастомизация виджета:** настройка внешнего виджета аутентификации под бренд компании
- **Управление пользователями:** регистрация, приглашения, редактирование, блокировка, смена паролей

3. Организации

Организация — административная единица, объединяющая пользователей, приложения и политики доступа. Организации позволяют разделять данные, настройки и доступы между разными командами, подразделениями или клиентами внутри одной системы.

4. Безопасность и аудит

- **Разграничение прав доступа**
- **Подробное журналирование** всех событий и действий

5. Мини-виджет

Лёгкий JavaScript-компонент, который обеспечивает быстрый доступ к функциям аутентификации и информации о пользователе. Легко интегрируется в любые веб-сайты и интерфейсы. Позволяет переходить к профилю пользователя, панелям управления, приложениям и другим функциям системы **КриптоАРМ ID**.

Уровни доступа

В **КриптоАРМ ID** используется ролевая модель доступа, разделенная по уровням: система, организация и приложение. Каждый уровень определяет свои права и область действия пользователя.

Роль	Полномочия	Для кого предназначена
Администратор системы	Полный доступ ко всем приложениям, пользователям и глобальным настройкам	Суперпользователи и администраторы платформы
Управленец	Управление приложениями и способами входа своей организации/подразделения	Владельцы организаций/подразделений
Администратор	Управление конкретными	Разработчики,

приложения	приложениями и их пользователями	администраторы приложений
Участник	Управление своим профилем и разрешениями на доступ к личным данным	Обычные пользователи, сотрудники

Помимо ролей, в системе существуют типы пользователей, которые определяют способ их аутентификации и происхождение, а не уровень доступа:

- **Участник** — пользователь, созданный/зарегистрированный в системе.
- **Внутренний (корпоративный) пользователь** — пользователь, синхронизируемый через IDM-систему.
- **Доверенный пользователь** — пользователь, созданный через доверенный провайдер.

Модули системы КриптоАРМ ID

В **КриптоАРМ ID** доступ к функциям и настройкам системы разделён по уровням доступа. Для каждого уровня предусмотрена отдельная панель управления.

1. Профиль

Профиль предназначен для управления персональными данными пользователя и настройками доступа. Включает функции редактирования личной информации, настройки приватности, управления разрешениями приложений и просмотра журнала активности. Также модуль предоставляет доступ к каталогу публичных приложений.

2. Панель администратора

Панель администратора предназначена для централизованного управления системой **КриптоАРМ ID**. Включает функции настройки глобальных параметров системы, способов аутентификации и внешнего вида страницы входа. В панели можно управлять приложениями и учетными записями пользователей, а также отслеживать их активность через единый журнал событий.

3. Панель организации

Панель организации обеспечивает управление приложениями, способами аутентификации и политиками доступа в рамках организации. Включает настройку параметров организации, конфигурацию способов входа, управление приложениями организации и мониторинг активности пользователей.

4. Панель приложения

Панель приложения предназначена для администрирования отдельных приложений. Содержит функции управления настройками приложения, участниками и доступом пользователей к приложению.

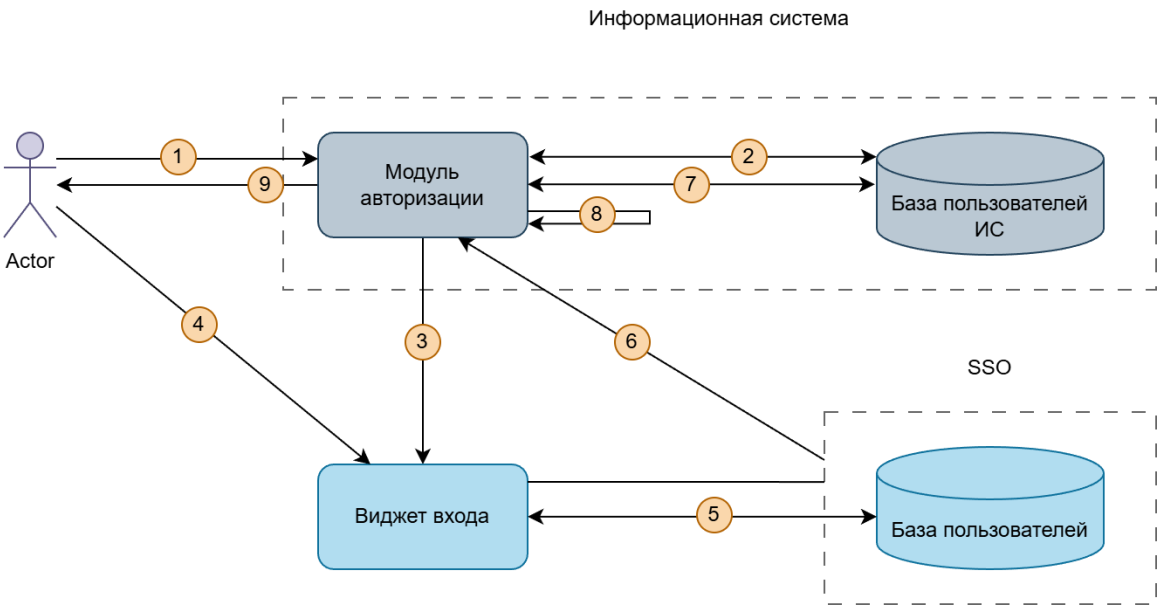
Доступ к панелям управления

Доступ к панелям осуществляется через **мини-виджет**. В зависимости от роли пользователя в системе в мини-виджете могут отображаться кнопки перехода:

- в панель администратора;
- в панель организации;
- в панель приложения;
- в профиль пользователя.

Концепция и принципы работы КриптоАРМ ID

Общая схема взаимодействия

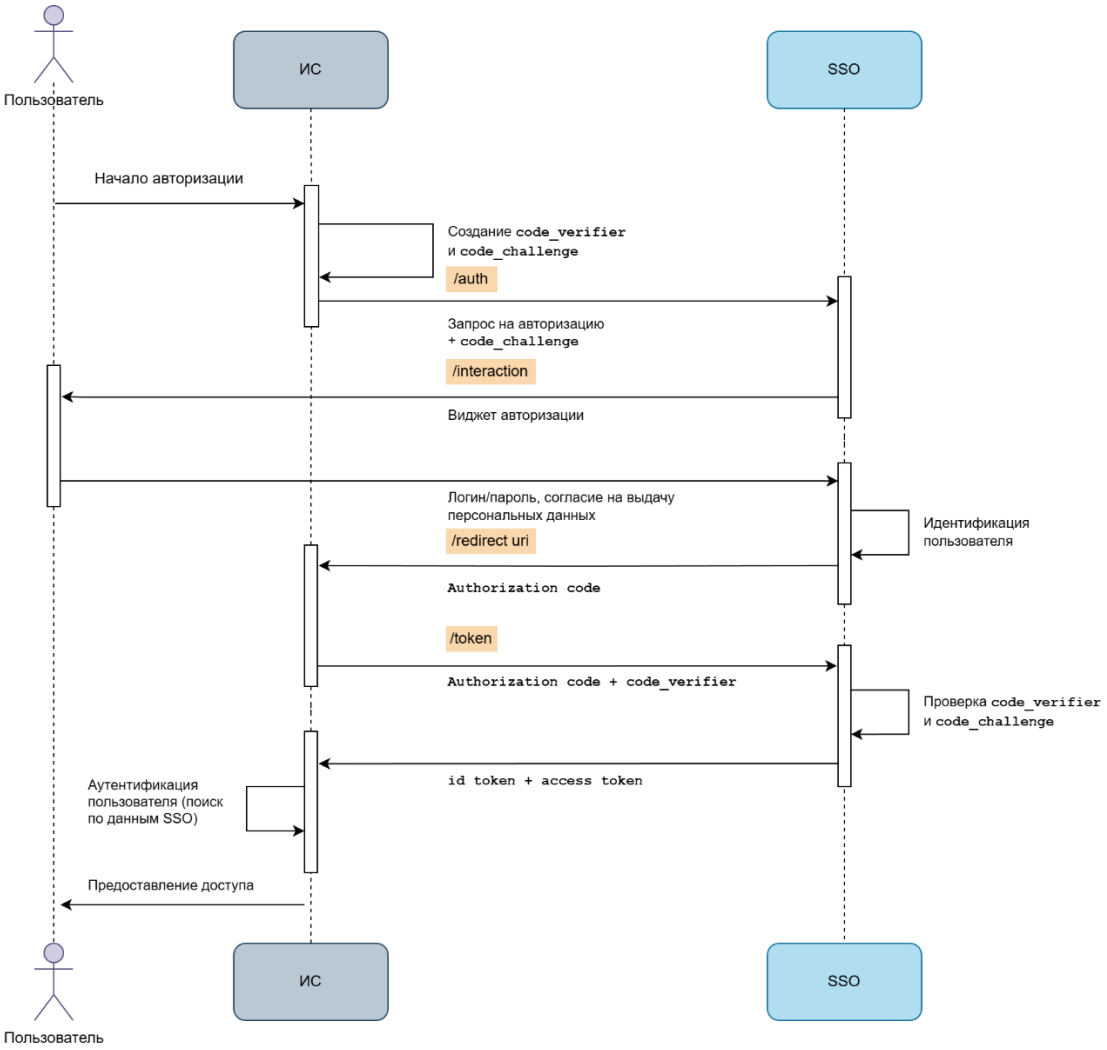


Последовательность взаимодействия:

1. **Запрос доступа** — пользователь обращается к информационной системе (ИС).
2. **Проверка в БД ИС** — система проверяет наличие пользователя.
3. **Перенаправление на виджет** — пользователь направляется в **КриптоАРМ ID**.
4. **Аутентификация** — пользователь проходит процедуру входа.
5. **Проверка в БД КриптоАРМ ID** — валидация учетных данных.
6. **Предоставление профиля** — возврат данных пользователя.
7. **Сопоставление в ИС** — поиск пользователя по данным из **КриптоАРМ ID**.
8. **Проверка прав** — авторизация в целевой системе.
9. **Предоставление доступа** — успешный вход в систему.

📌 **Требования для интеграции:** Для подключения информационной системы к **КриптоАРМ ID** необходимо наличие базы данных пользователей и модуля авторизации, поддерживающего OpenID Connect или OAuth 2.0.

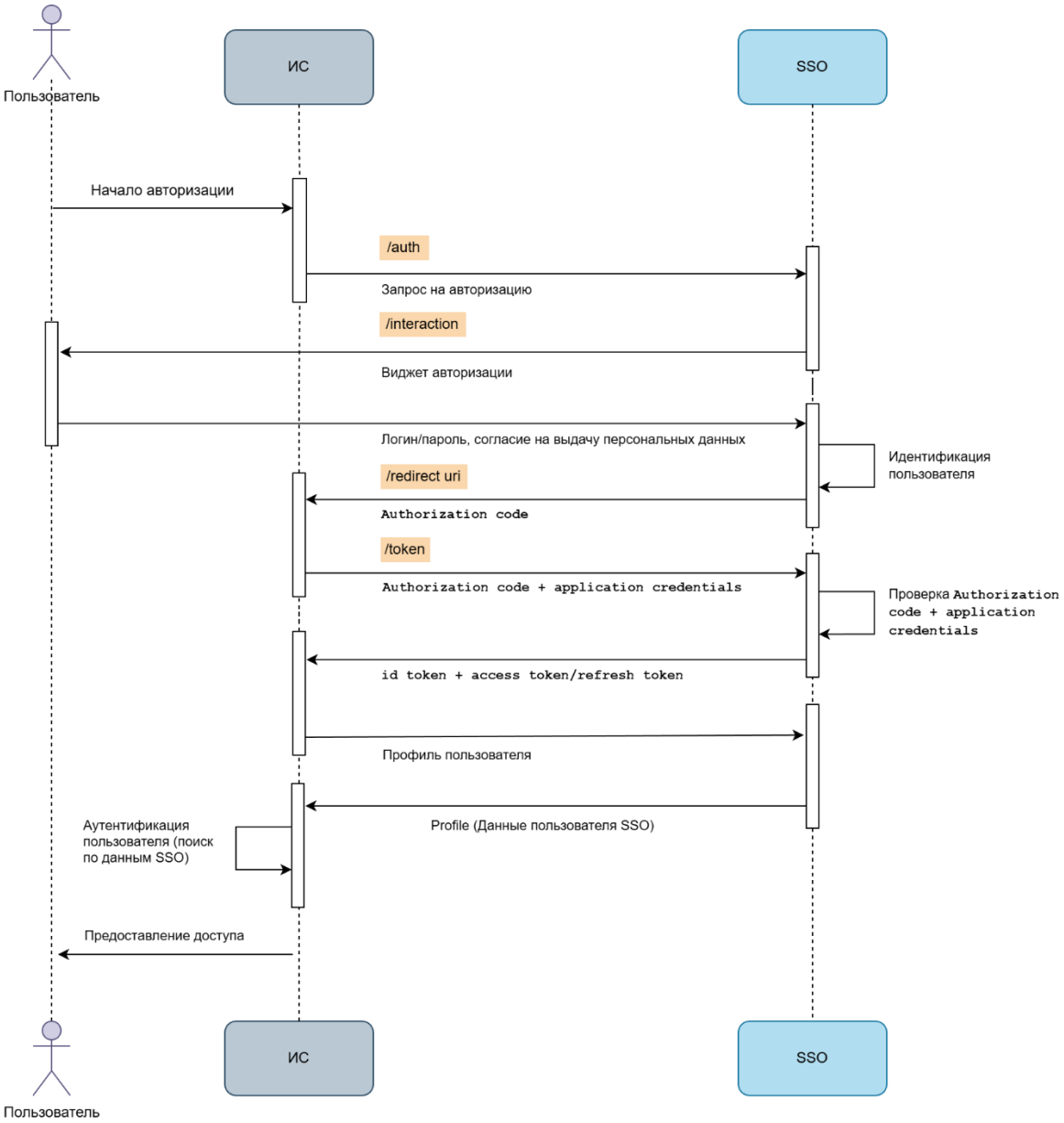
Схема авторизации по OpenID Connect



Ключевые этапы OIDC:

1. Пользователь обращается к ИС.
2. ИС (клиент) генерирует `code_verifier` и `code_challenge`.
3. ИС перенаправляет пользователя на `/authorize` **КриптоАРМ ID**.
4. Пользователь перенаправляется на виджет авторизации **КриптоАРМ ID**.
5. Пользователь вводит логин/пароль и предоставляет согласие на передачу данных.
6. Выполняется проверка пользователя в БД **КриптоАРМ ID**.
7. Перенаправление пользователя обратно в ИС (клиент) с `Authorization code`.
8. ИС отправляет запрос на `/token` в **КриптоАРМ ID**.
9. Проверка `code_challenge` and `code_verifier` в **КриптоАРМ ID**.
10. Предоставление в ИС `id token`, содержащего профиль пользователя **КриптоАРМ ID**, и `access token` (опционально `refresh token`).
11. Аутентификация пользователя ИС.
12. Пользователь получает доступ к ИС.

Схема авторизации по OAuth 2.0

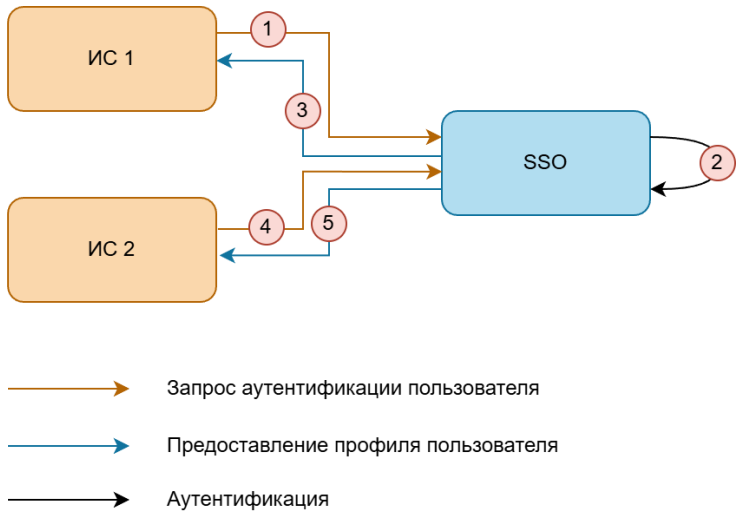


Особенности OAuth 2.0 потока:

1. Пользователь обращается к ИС.
2. ИС перенаправляет пользователя на `/authorize` **КриптоАРМ ID**.
3. Пользователь перенаправляется на виджет авторизации **КриптоАРМ ID**.
4. Пользователь вводит логин/пароль и предоставляет согласие на передачу данных.
5. Выполняется проверка пользователя в БД **КриптоАРМ ID**.
6. **КриптоАРМ ID** перенаправляет пользователя обратно в ИС с `Authorization code` на `Redirect_URI`.
7. ИС отправляет запрос на `token` по `Authorization code`.
8. **КриптоАРМ ID** валидирует запрос.

9. **КриптоАРМ ID** возвращает токены `id token` и `access token` (опционально `refresh token`).
10. ИС запрашивает профиль пользователя.
11. **КриптоАРМ ID** предоставляет профиль пользователя.
12. ИС валидирует ответы и устанавливает локальную сессию пользователя.
13. Пользователь получает доступ к ИС.

Схема Single sign-on (SSO)



Типичный сценарий:

1. Запрос доступа к ИС1.
2. Аутентификация пользователя в **КриптоАРМ ID**.
3. Предоставление профиля пользователя **КриптоАРМ ID** в ИС1.
4. Запрос доступа к ИС2.
5. Предоставление профиля пользователя **КриптоАРМ ID** в ИС2 без повторной процедуры аутентификации пользователя.

🚀 **Готовы начать?** Переходите к руководству по установке системы.

Смотрите также

- Установка системы КриптоАРМ ID — руководство по установке системы.
- Переменные окружения КриптоАРМ ID — руководство по подготовке конфигурации перед запуском.
- Настройка системы — руководство по настройке интерфейса и доступа пользователей в систему.

Управление организацией в КриптоАРМ IDM

В **КриптоАРМ IDM** организации служат основной структурной единицей для управления доступом к приложениям, разделения сотрудников по подразделениям и

ведения аудита активности пользователей. В этом руководстве мы рассмотрим, как создавать организации и настраивать способы входа.

Содержание:

- Основные понятия об организациях
- Доступ к панели организации
- Настройка организации
- Управление пользователями
- Удаление организации
- Смотрите также

Основные понятия об организациях

Организация в **КриптоАРМ IDM** — это структурная единица, которая позволяет:

- **Разграничивать доступ** к приложениям между подразделениями или проектами,
- **Настраивать корпоративные способы входа**,
- **Вести централизованный аудит** активности пользователей,
- **Управлять приложениями** в рамках одной компании,
- **Настраивать брендинг** (логотип, название) для виджетов входа.

> 💡 Организации идеально подходят для компаний, которым нужно управлять несколькими приложениями и группами пользователей с единой точки контроля.

Доступ к панели организации

Панель организации предназначена для управления настройками, приложениями и пользователями организации.

В панели организации доступны следующие разделы:

- **Настройки** — параметры организации, способы входа, кастомизация виджета авторизации.
- **Приложения** — управление приложениями организации.
- **Пользователи** — управление пользователями организации.
- **Журнал** — история активности пользователей организации.

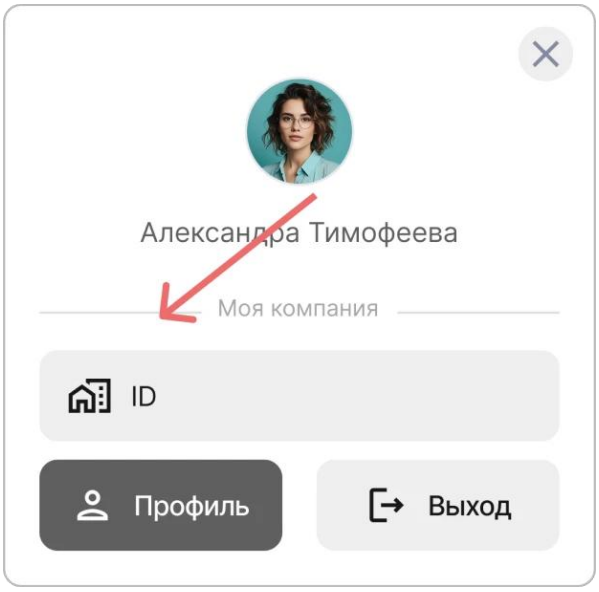
Как попасть в панель организации КриптоАРМ IDM

> ⚠️ Для доступа в панель организации необходимы полномочия **Управленец**. Обратитесь к администратору сервиса для их получения.

Чтобы открыть панель управления организацией:

1. Авторизуйтесь в **КриптоАРМ IDM**.
2. Нажмите на свое имя в правом верхнем углу окна.

3. В открывшемся окне мини-виджета нажмите на кнопку **ID**.



Вы будете перенаправлены в панель организации.

Настройка организации

Для организации доступны следующие настройки:

- **Общие параметры** — название, описание и логотип организации, которые отображаются в интерфейсе системы, виджете входа и мини-виджете.
- **Способы входа** — настройка доступных методов аутентификации для пользователей организации.
- **Уведомления** — настройка оповещения пользователя о различных событиях при входе в систему или приложения.
- **Доверенные провайдеры** — подключение корпоративных провайдеров идентификации.

Эти параметры позволяют адаптировать организацию под внутренние правила компании, требования безопасности и сценарии использования.

Настройка названия и логотипа

Название и логотип отображаются в интерфейсе системы **КриптоАРМ IDM**, а также в мини-виджете.

Чтобы настроить название и логотип:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Основная информация**.
3. Укажите новое название в поле **Название приложения**.
4. В разделе **Логотип приложения** нажмите **Загрузить** и выберите файл с логотипом.

⚡ Допустимые форматы: JPG, GIF, PNG, WEBP; максимальный размер 1 МБ.

5. Настройте область отображения логотипа.

6. Нажмите **Сохранить**.

Управление пользователями

Пользователи организации в **КриптоАРМ IDM** — все учетные записи, связанные с организацией, включая внутренних (корпоративных) пользователей, доверенных пользователей и участников, зарегистрированных через способы входа организации.

Через панель организации можно управлять пользователями: просматривать список, назначать права доступа, блокировать, управлять публичностью и отслеживать активность.

> 🔍 Операции с пользователями описаны в отдельной инструкции: Управление пользователями в КриптоАРМ IDM.

Удаление организации

Удаление организации в **КриптоАРМ IDM** выполняется только через администратора сервиса.

Это ограничение связано с тем, что организация является структурной единицей системы и может включать приложения, пользователей, способы входа и другие зависимости.

Как происходит удаление

Для удаления организации необходимо обратиться к администратору сервиса и инициировать процедуру удаления.

После подтверждения удаления:

- организация полностью удаляется из системы;
- все пользователи, связанные с организацией, удаляются из системы;
- доступ к приложениям и данным организации становится недоступен.

⚠️ Удаление организации является необратимой операцией. Восстановление данных после удаления невозможно.

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.
- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как работает лицензирование КриптоАРМ IDM

В этом руководстве мы расскажем про **лицензирование КриптоАРМ IDM**: какие функции требуют лицензии, какие возможности предоставляет базовая лицензия и лицензия на доверенный провайдер, как правильно выполнить активацию лицензии и привязать ее к доверенному провайдеру.

Содержание:

- На какие функции требуется лицензия
- Активация лицензии
- Смотрите также

На какие функции требуется лицензия

С помощью лицензий в **КриптоАРМ IDM** регулируется доступ к дополнительным возможностям, таким как: авторизация через SSO и подключение доверенных источников данных.

Варианты лицензий:

1. **Базовая лицензия**
   - Разблокирует авторизацию пользователей через любые провайдеры.
   - Позволяет подключить один доверенный провайдер к источнику данных.
   - Может быть бессрочной или с ограниченным сроком действия.
   - Для работы системы нужна только одна такая лицензия.
2. **Лицензия на доверенный провайдер**

- Позволяет подключать дополнительные доверенные провайдеры (по одной лицензии на каждый).
- Может быть бессрочной или с ограниченным сроком действия.

💡 **Для быстрого старта:** достаточно одной базовой лицензии. Она включает авторизацию и один доверенный провайдер. Остальное можно докупать по мере необходимости.

Лицензия	Авторизация	Подключение доверенных провайдеров	Особенности
Без лицензии	❌ Недоступна	❌ Недоступно	Можно запускать и настраивать систему, создавать пользователей
Базовая лицензия	✅ Доступна	✅ 1 доверенный провайдер	Бессрочная или с ограничением, только одна лицензия нужна для работы системы
Лицензия на доверенный провайдер	–	✅ 1 доверенный провайдер	Бессрочная или ограниченная по времени

⚠️ **Примечание**: Лицензии действуют только для соответствующих глобальных версий. Убедитесь, что цифра в начале номера лицензии совпадает с вашей версией системы.

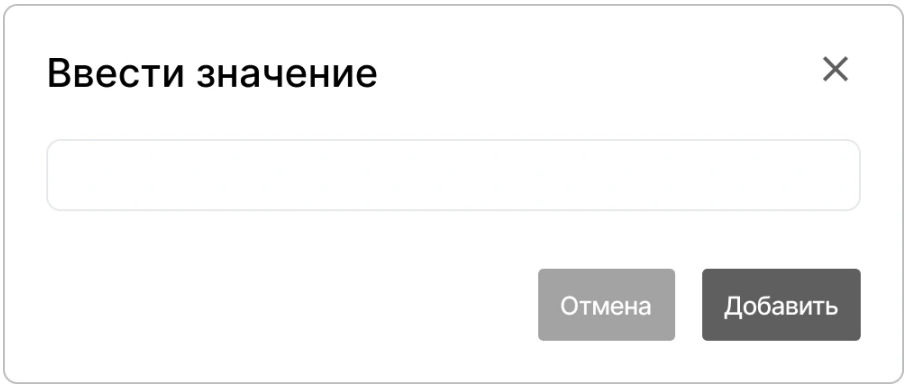
Активация лицензии

Добавление ключа

Чтобы добавить лицензионный ключ для базовой лицензии или лицензии на доверенный провайдер:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Лицензии** и нажмите **Добавить**.

3. Введите лицензионный ключ и нажмите **Добавить**.

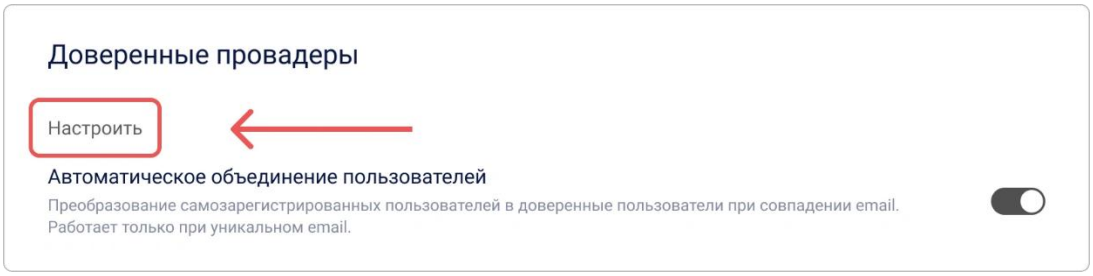


💡 **Совет**: Лицензионный ключ можно добавить в форме редактирования провайдера.

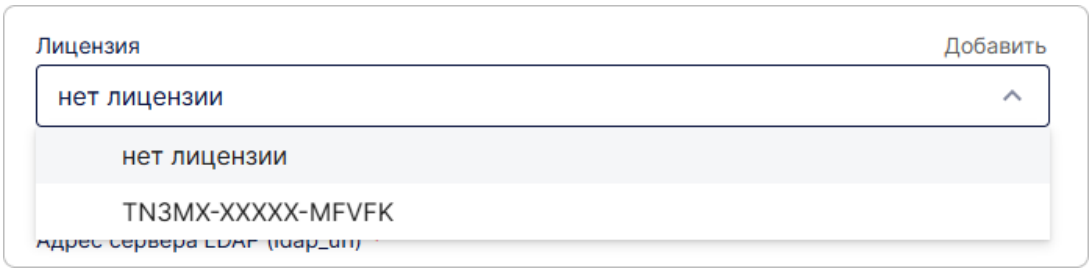
Привязка ключа к способу входа

Чтобы привязать лицензию:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Доверенные провайдеры**.
3. Нажмите на кнопку **Настроить**.



4. Откроется окно со списком провайдеров.
5. Нажмите кнопку **Настроить** на панели с провайдером, к которому необходимо привязать лицензию.
6. Откроется форма редактирования.
7. В настройке **Лицензия** выберите ключ из выпадающего списка.



💡 **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

💡 **Особые условия:** Если адреса подключения провайдеров совпадают, допускается привязка нескольких таких провайдеров к одной лицензии.

8. Нажмите **Сохранить** в форме редактирования.

Лицензия привязывается к способу входа.

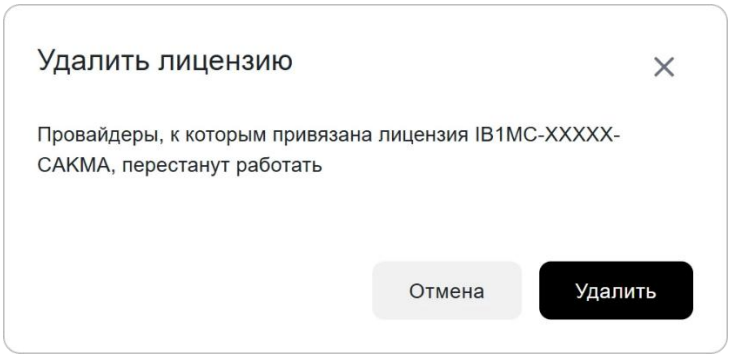
📌 Если срок действия лицензии истечёт или ключ будет удалён, связанный способ входа будет автоматически отключён, и пользователи не смогут авторизоваться через него.

Удаление ключа из системы

Чтобы удалить ключ из системы:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Лицензии**.
3. Нажмите на кнопку **Удалить** на панели с лицензионным ключом, который требуется удалить из системы.

4. Подтвердите действие в модальном окне.



Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.

Как настроить профиль пользователя КриптоАРМ IDM

В этом руководстве мы расскажем, как настроить профиль пользователя и парольную политику в **КриптоАРМ IDM**. Вы научитесь управлять полями профиля, валидацией полей и настраивать подтверждение адреса электронной почты и телефона.

Содержание:

- Парольная политика
- Основные поля профиля
- Дополнительные поля профиля
- Правила валидации полей профиля и пароля
- Подтверждение электронной почты
- Подтверждение номера телефона
- Смотрите также

> 💡 Настройки системы размещены в панели ID. Для доступа к панели необходима роль **Администратор** сервиса. Как открыть панель ID →

Парольная политика

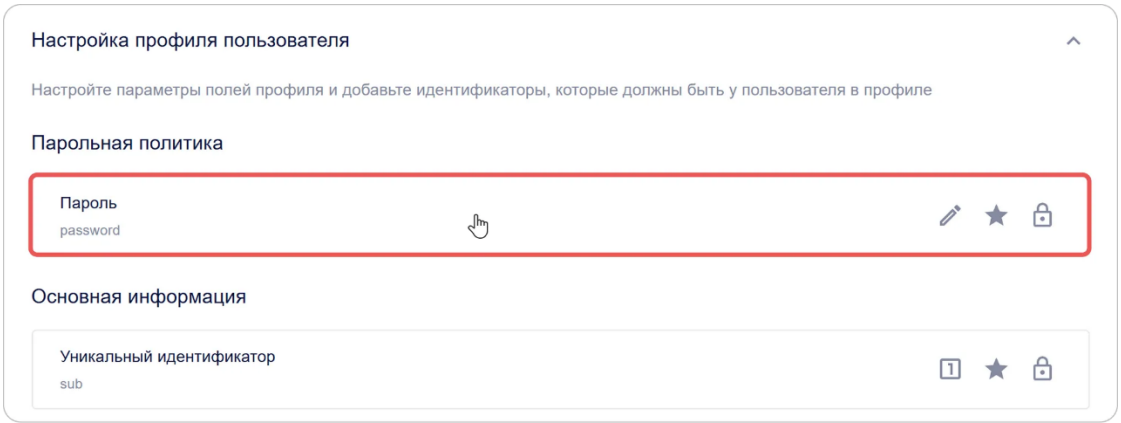
Парольная политика в КриптоАРМ IDM — это набор правил, определяющих требования к сложности и безопасности паролей пользователей. Она помогает защитить учетные записи от взлома и несанкционированного доступа.

Установленные правила применяются:

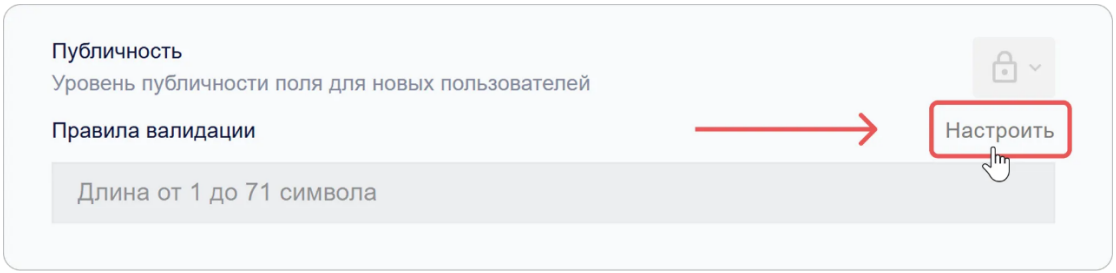
- при создании пароля в виджете регистрации,
- при восстановлении пароля в виджете входа,
- при смене пароля в профиле пользователя.

Как настроить правила парольной политики

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя** и нажмите на **Пароль**.



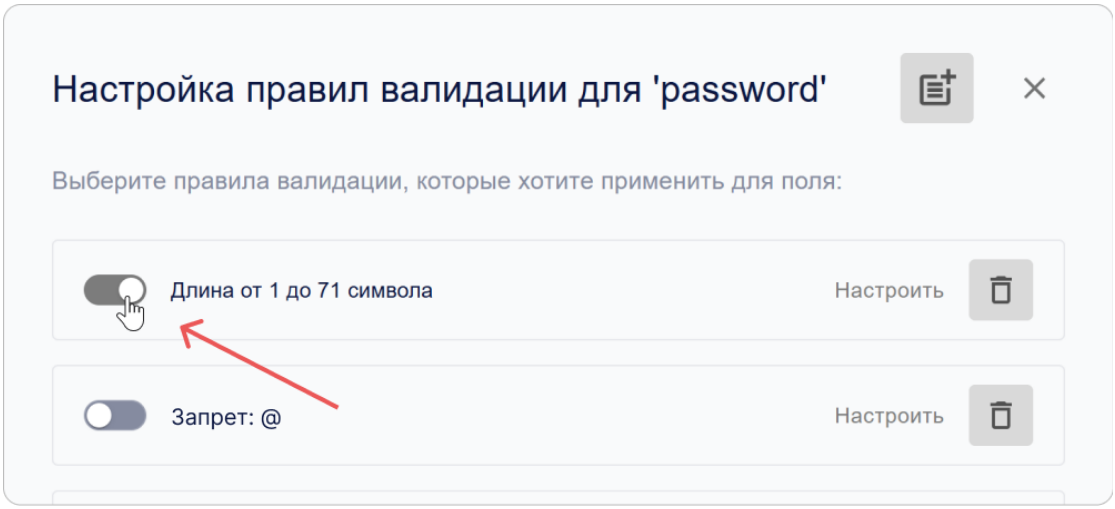
3. В появившемся окне нажмите **Настроить**.



4. Откроется окно со списком доступных правил проверки.

   🔗 Про создание и настройку правил валидации полей профиля читайте в инструкции Правила валидации полей профиля пользователя.

5. Отметьте флажками правила, которые нужно применить к паролю.



6. Закройте окно со списком правил.

7. Нажмите **Сохранить** в форме редактирования поля.

Изменения применяются автоматически.

Теперь выбранные вами правила будут использоваться для проверки сложности пароля пользователя.

> ⚠️ **Примечание**: Новые правила применяются только к создаваемым и изменяемым паролям. Существующие пароли остаются без изменений.

Рекомендации по безопасности

Чтобы обеспечить надёжную защиту учетных записей, рекомендуется включить следующие параметры:

Рекомендация	Пример правила
Минимальная длина пароля — не менее 8 символов	`Минимальная длина = 8`
Использование букв разного регистра	`Содержит строчные и прописные символы`

Обязательное наличие цифр	`Содержит хотя бы одну цифру`
Обязательное наличие спецсимволов	`Содержит специальные символы (!@#$% и т. п.)`

Основные поля профиля пользователя

Основные поля профиля — это обязательные системные атрибуты, которые создаются автоматически для каждого пользователя при его регистрации. Они формируют базовую структуру профиля и обеспечивают корректную работу механизмов аутентификации, идентификации и связи между системами.

Список основных полей

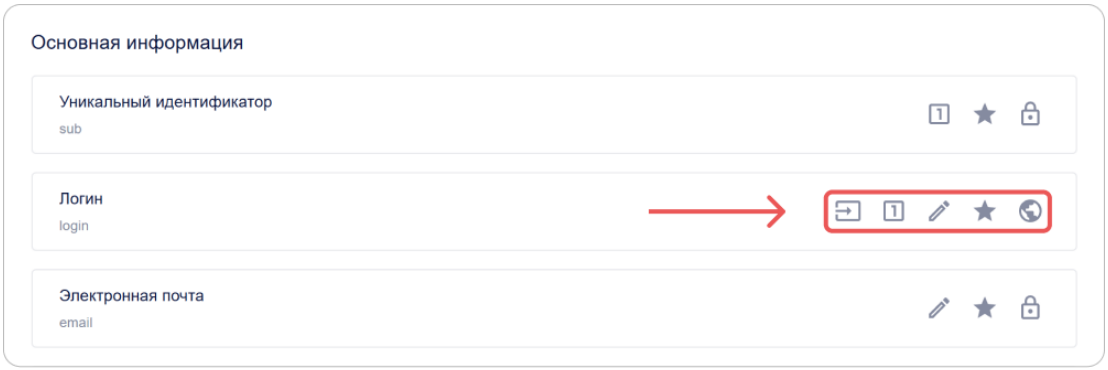
📌 Список основных полей фиксирован. Добавление, переименование или удаление этих полей недоступно.

Поле	Идентификатор
Идентификатор	`sub`
Логин	`login`
Электронная почта	`email`
Имя	`given_name`
Фамилия	`family_name`
Телефон	`phone_number`
Дата рождения	`birthdate`
Публичное имя	`nickname`
Фото	`picture`
Согласие на обработку данных	`data_processing_agreement`

Обозначения настроек

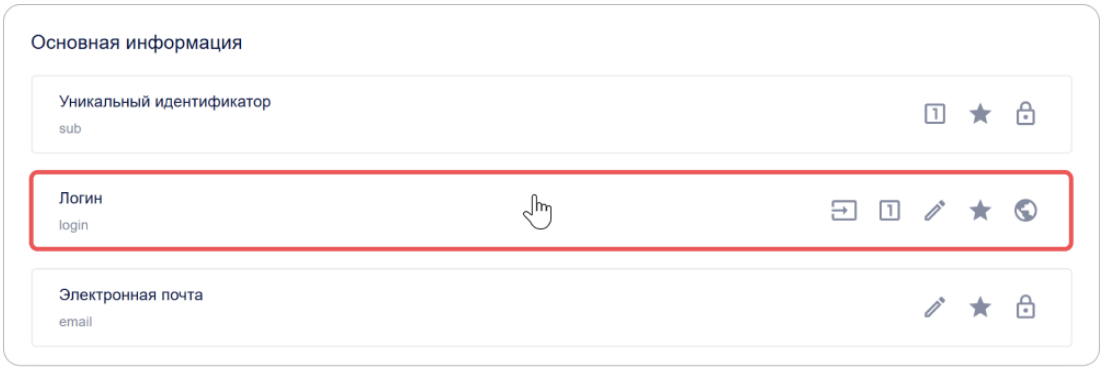
В интерфейсе для каждого поля доступен быстрый просмотр настроек поля в виде идентификаторов:

Иконка	Параметр
	Поле доступно пользователю для редактирования
	Поле обязательно для заполнения
	Значение поля должно быть уникальным
	Уровень публичности поля
	Поле можно использовать как логин при входе



Как настроить основное поле

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с полем, которое необходимо настроить.



4. В открывшейся форме укажите:
   - параметры,
   - правила валидации.
5. Сохраните изменения в форме редактирования.

Параметры основного поля

Название	Описание
Название	Название поля. Недоступно для редактирования.
Описание поля	Название поля в интерфейсе. Недоступно для редактирования.
Использовать в качестве логина	Позволяет авторизоваться с использованием данного поля. Доступно для настройки в полях **Логин**, **Электронная почта** и **Номер телефона**
Активность	Определяет обязательное наличие поля в профиле пользователя. Неизменяемый параметр.
Редактируемость	Разрешает пользователю изменять значение поля в своём профиле.
Обязательность	Требует заполнения поля при регистрации или входе. Без

	него аутентификация невозможна.
Уникальность	Проверяет, чтобы значение поля не повторялось среди всех профилей.
Публичность	Определяет, кому будут доступны данные пользователя:: - **Доступно только вам** - данные приватны и доступны только пользователю. - **Доступно по запросу** - данные пользователя доступны для сторонних систем после его согласия; - **Доступно всем** - данные публичны всегда для сторонних систем, не требуют согласия на доступ к данным. Данные, которые будут передаваться сторонней системе по хешу электронной почты (по аналогии с сервисом Gravatar).
Настройки подтверждения электронной почты	Предназначено для настройки параметров для подтверждения адреса электронной почты в профиле пользователя. 🔗 Подробное описание настроек в инструкции Настройки подтверждения электронной почты.
Настройки подтверждения номера телефона	Предназначено для настройки параметров для подтверждения номера телефона в профиле пользователя. 🔗 Подробное описание настроек в инструкции Настройки подтверждения электронной почты.
Правила валидации	Набор правил проверки корректности введённых данных. 🔗 Подробное описание в инструкции Настройка правил валидации.

Дополнительные поля профиля пользователя

Дополнительные поля профиля — это пользовательские атрибуты, которые можно создавать для хранения любых специфических данных, не входящих в стандартный набор.

Они помогают адаптировать профиль под конкретные задачи:

- хранить внутренние идентификаторы, должности, роли, отделы и т.д.
- статусы проверки данных и другие бизнес-атрибуты.

Обозначения настроек

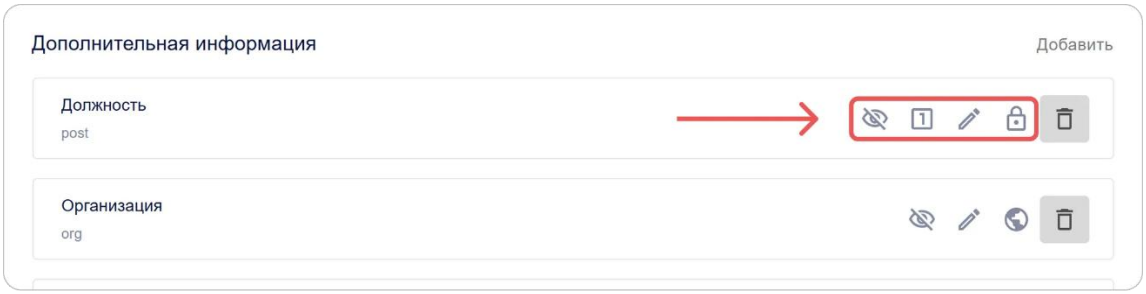
В интерфейсе для каждого поля доступен быстрый просмотр настроек поля в виде идентификаторов:

Иконка	Параметр
	Поле доступно пользователю для редактирования
	Поле обязательно для заполнения

Значение поля должно быть уникальным

Уровень публичности поля

Активность поля



Добавление дополнительного поля

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя** .
3. Нажмите кнопку **Добавить** в разделе **Дополнительная информация**.
4. В открывшейся форме укажите:
   - параметры,
   - правила валидации.
5. Нажмите **Сохранить**.

Редактирование дополнительного поля

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с дополнительным полем, настройки которого необходимо изменить.
4. В открывшейся форме отредактируйте параметры и правила валидации.
5. Нажмите **Сохранить**.

💡 Изменения вступают в силу сразу и применяются ко всем профилям, где используется данное поле.

Удаление дополнительного поля

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите кнопку **Удалить** , напротив поля, которое нужно удалить.

⚠️ **Примечание**: При удалении поля все сохраненные в нем данные пользователей будут безвозвратно утеряны.

Параметры дополнительного поля

Название	Описание
Описание поля	Название поля в системе
Активность	Определяет, отображается ли поле в профиле пользователя
Редактируемость	Разрешает пользователю изменять значение поля самостоятельно
Обязательность	Требует заполнения поля при регистрации или входе в систему. Без заполненного поля пользователь не сможет войти в систему.
Уникальность	Проверяет, чтобы значение не повторялось среди всех профилей
Публичность	Настраивает, кому будет доступно поле: - **Доступно только вам** - данные приватны и доступны только пользователю. - **Доступно по запросу** - данные пользователя доступны для сторонних систем после его согласия; - **Доступно всем** - данные публичны всегда для сторонних систем, не требуют согласия на доступ к данным. Данные, которые будут передаваться сторонней системе по хешу электронной почты (по аналогии с сервисом Gravatar).
Атрибут vCard	Позволяет сопоставить поле с атрибутом при экспорте профиля в формат vCard
Значение по умолчанию	Устанавливает предзаполненное значение при создании профиля
Правила валидации	Определяют логику проверки введённого значения. 🔗 Подробнее в инструкции Настройка правил валидации.

Правила валидации полей профиля пользователя и пароля

Правила валидации полей — это набор проверок, по которым система оценивает корректность данных, вводимых пользователем.

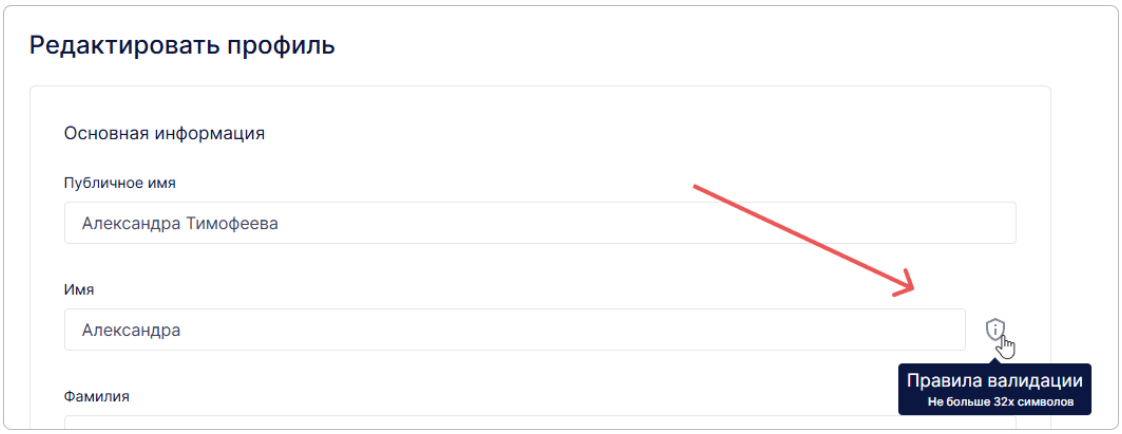
Вы можете задать собственные правила для:

- пароля аккаунта,

- основных полей профиля пользователя,
- дополнительных полей профиля пользователя.

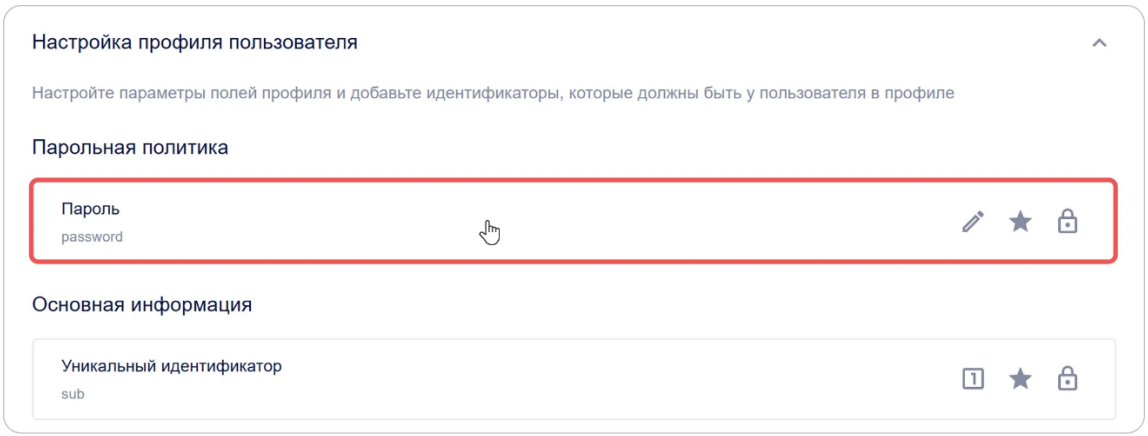
Такие проверки позволяют повысить качество данных, например, не допускать некорректные email-адреса, номера телефонов или пароли без спецсимволов.

Заданные правила валидации отображаются в интерфейсе. Например, в форме редактирования профиля около основного или дополнительного поля появляется специальная иконка, при наведении на которую открывается список заданных правил.

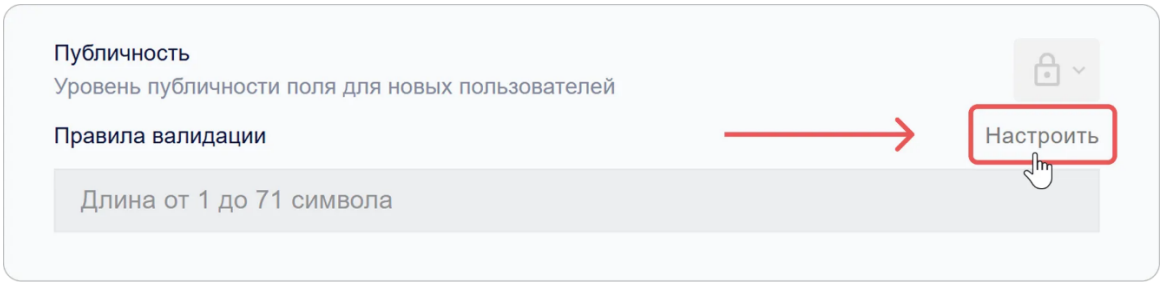


Создание правила

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с паролем, основным или дополнительным полем.

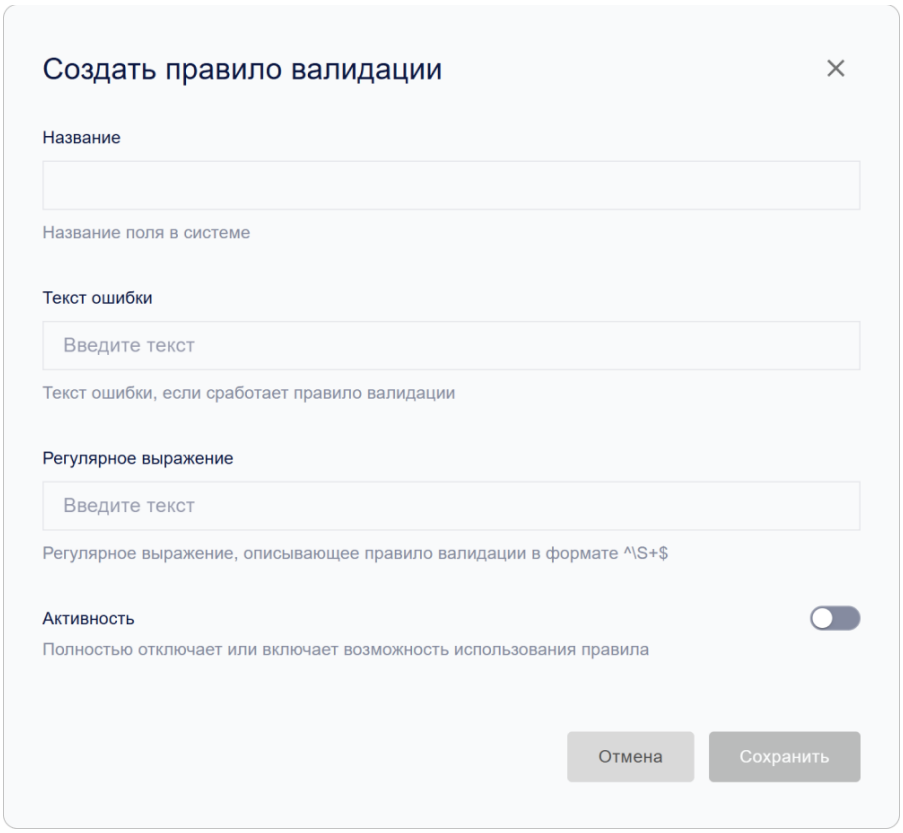


4. Откроется форма редактирования.
5. Нажмите **Настроить** в разделе **Правила валидации**.



6. В открывшемся окне со списком правил валидации нажмите на кнопку **Добавить** .

7. Откроется форма создания правила.



8. Заполните поля правила:

   - **Название**;

   - **Текст ошибки** — сообщение, которое будет отображаться при срабатывании правила;

   - **Регулярное выражение** — выражение, которому должно соответствовать значение в поле;

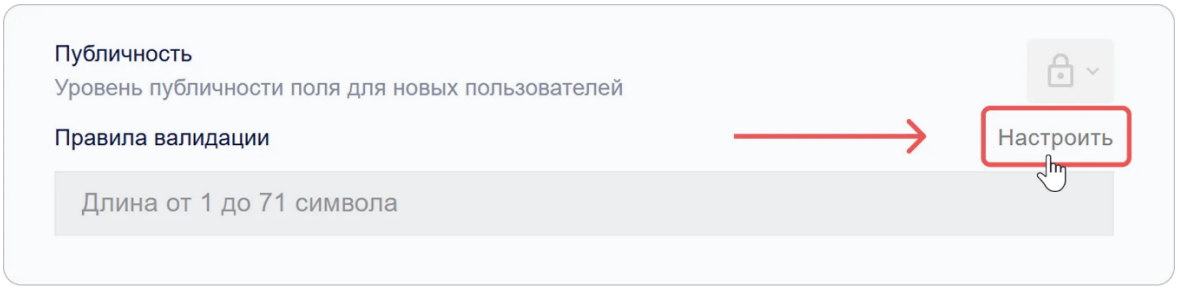
- **Активность** — при включении данное правило можно выбрать для валидации поля. Неактивные правила недоступны для выбора и игнорируются при проверке значений в поле.

9. Нажмите **Сохранить**.

Созданное правило добавится в список правил и станет доступно для настройки валидации полей.

Редактирование правила

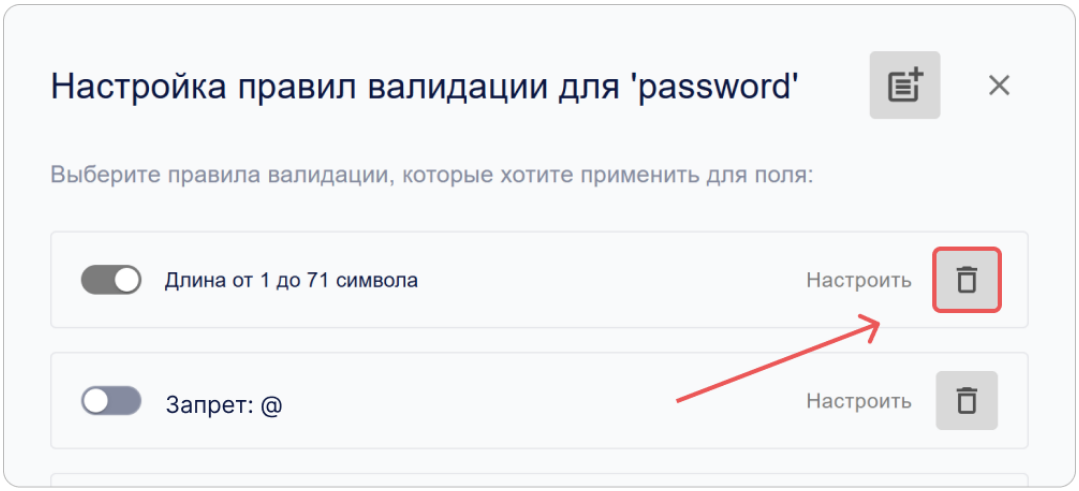
1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с основным или дополнительным полем.
4. Откроется форма редактирования.
5. Нажмите **Настроить** в разделе **Правила валидации**.
6. Откроется окно со списком правил валидации.
7. На панели с правилом нажмите кнопку **Настроить** .



8. В открывшейся форме редактирования измените необходимые поля.
9. Нажмите **Сохранить**.

Удаление правила

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с основным или дополнительным полем.
4. Откроется форма редактирования.
5. Нажмите **Настроить** в разделе **Правила валидации**.
6. Откроется окно со списком правил валидации.
7. На панели с правилом нажмите кнопку **Удалить** .

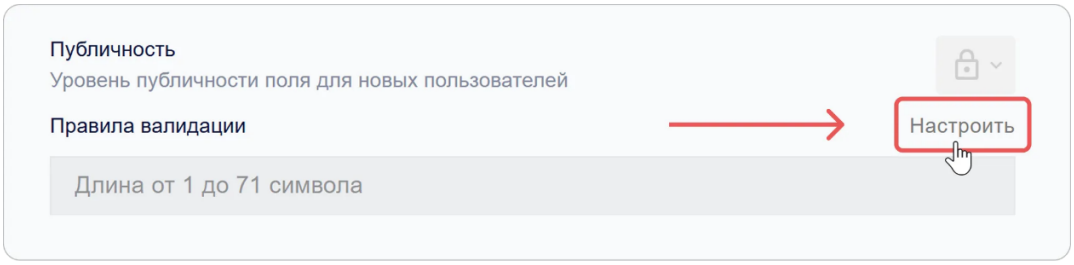


Изменения применяются автоматически.

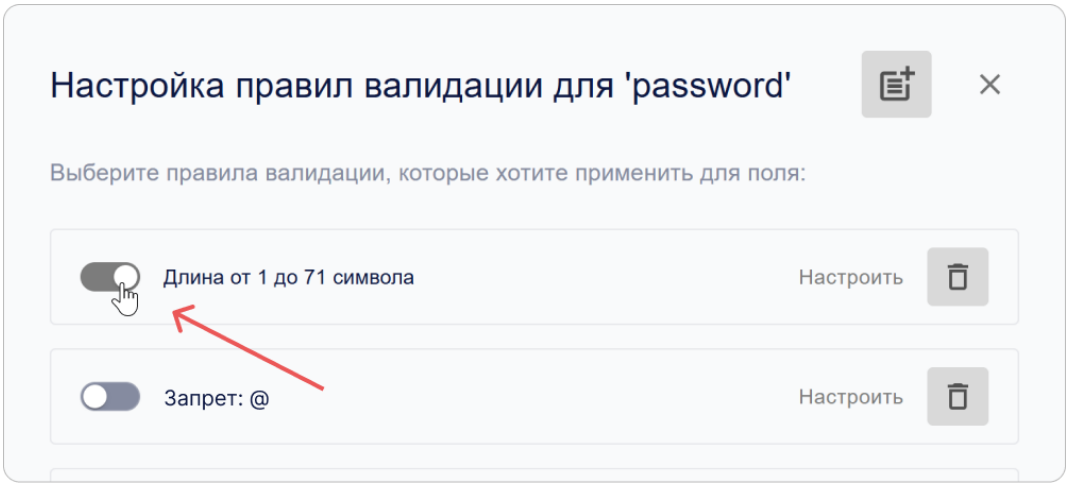
Как добавить правило в поле профиля пользователя

Чтобы настроить правила валидации в основном или дополнительном поле:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с основным или дополнительным полем.
4. Откроется форма редактирования.
5. Нажмите **Настроить** в разделе **Правила валидации**.



6. Откроется окно со списком правил валидации.



7. Установите флажок напротив правил, которые необходимо применить к выбранному полю.

8. Закройте окно со списком правил.

Изменения применяются автоматически.

Настройки подтверждения электронной почты

Подтверждение электронной почты в КриптоАРМ IDM — это механизм проверки достоверности адреса, указанного пользователем при регистрации, авторизации или изменении данных профиля.

После указания адреса система отправляет письмо с кодом подтверждения или уникальной ссылкой. Пользователь должен перейти по ссылке или ввести код — после этого адрес считается подтверждённым.

Такая проверка обеспечивает:

- защиту от регистрации с некорректными или чужими адресами;
- безопасность доступа к учётной записи;
- возможность использовать электронную почту для восстановления доступа и уведомлений;
- контроль за актуальностью контактных данных пользователей.

Добавление настройки

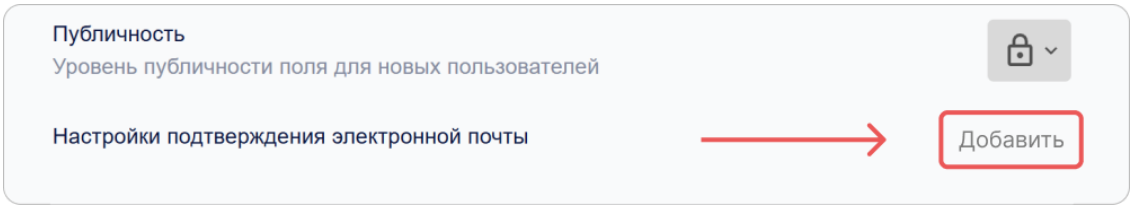
1. Перейдите в панель ID → вкладка **Настройки**.

2. Раскройте блок **Настройка профиля пользователя**.

3. Нажмите на панель **Электронная почта**.

4. Откроется форма редактирования.

5. В разделе **Настройки подтверждения электронной почты** нажмите **Добавить**.



6. В открывшемся окне укажите параметры:

Параметр	Описание
Основной почтовый адрес	Основной адрес электронной почты, с которого будут отправляться автоматические письма
Псевдоним отправителя (alias)	Имя отправителя, которое будет отображаться в поле «От»
Адрес сервера исходящей почты	Адрес smtp-сервера
Порт сервера исходящей почты	Порт для smtp-сервера
Пароль почты	Обычный пароль или пароль приложения, который создается в настройках аккаунта почтового сервиса
Публичный способ входа	Почта будет использоваться для входа в приложения с помощью одноразовых паролей
Изображение почты	Иконка, которая будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**
Время жизни кода подтверждения	Время жизни кодов подтверждения адреса электронной почты в секундах

7. Нажмите **Сохранить**.

💡 Для отправки тестового сообщения нажмите **Отправить**  . Эта функция позволяет проверить корректность настроек почтового сервиса (SMTP и других параметров) перед использованием его в рабочей среде.

Настройка шаблонов уведомлений

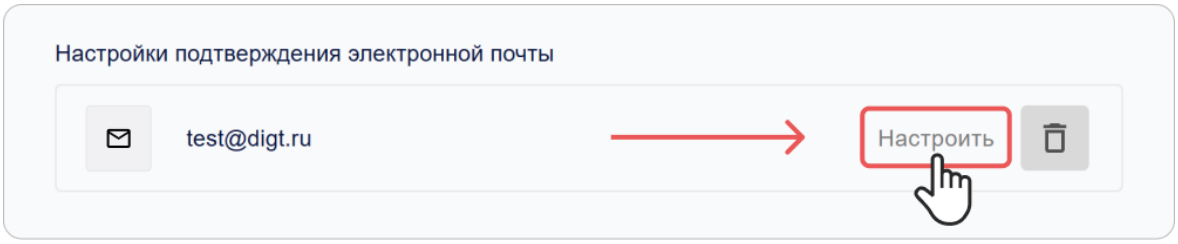
После создания настройки подтверждения электронной почты можно настроить внешний вид и содержимое писем, которые отправляет система **КриптоАРМ IDM**.

🔍 Подробнее о настройке шаблонов читайте в инструкции Настройка шаблонов email-уведомлений

Редактирование настройки

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Электронная почта**.
4. Откроется форма редактирования.

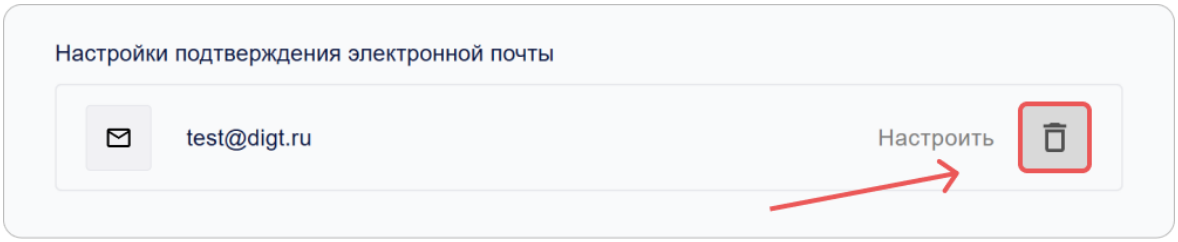
5. В разделе **Настройки подтверждения электронной почты** нажмите кнопку **Настроить**.



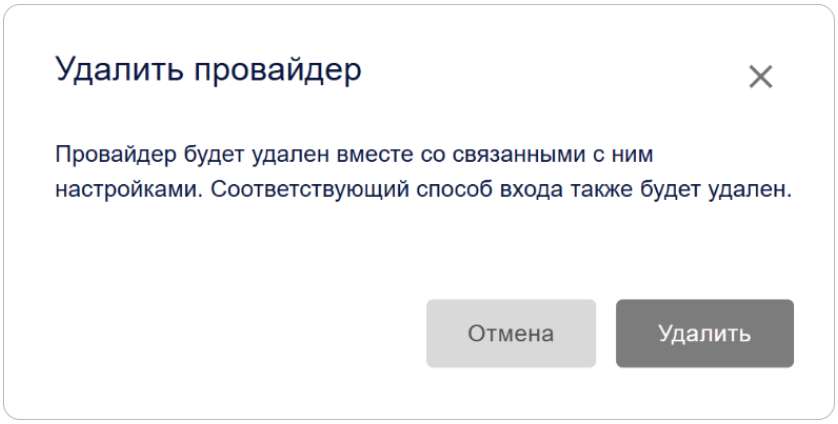
6. Откроется форма редактирования.
7. Внесите необходимые изменения.
8. Нажмите **Сохранить**.

Удаление настройки

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Электронная почта**.
4. Откроется форма редактирования.
5. Нажмите кнопку **Удалить** в разделе **Настройки подтверждения электронной почты**.



6. Подтвердите действие в модальном окне.



Настройки подтверждения номера телефона

Подтверждение номера телефона в КриптоАРМ IDM — это механизм проверки достоверности контактного номера, указанного пользователем при регистрации, входе или изменении профиля.

После ввода номера система отправляет пользователю проверочный код или инициирует автоматический звонок. Пользователь вводит полученный код, подтверждая, что указанный номер действительно принадлежит ему.

Такая проверка выполняет несколько ключевых функций:

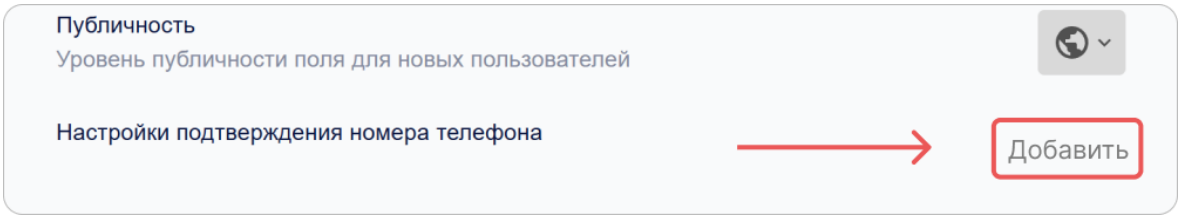
- предотвращает использование недействительных или чужих номеров;
- обеспечивает дополнительный уровень защиты учётной записи;
- позволяет использовать номер для входа по одноразовому коду;
- гарантирует корректную работу уведомлений, связанных с безопасностью.

В текущей версии **КриптоАРМ IDM** подтверждение номеров реализуется через интеграцию с сервисом Авторизация по звонку платформы **Kloud.One**. Для работы этого механизма требуется настроить подключение к **Kloud.One**, указав идентификатор и секрет клиента.

> 💡 **Совет:** перед сохранением настройки убедитесь, что приложение корректно зарегистрировано в **Kloud.One** и указанные данные (`client_id` и `client_secret`) действительны. Без этого подтверждение номеров не будет работать.
>
> 📚 Документация Kloud.One

Добавление настройки

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Номер телефона**.
4. Откроется форма редактирования.
5. В разделе **Настройки подтверждения номера телефона** нажмите **Добавить**.



6. В появившемся окне задайте необходимые параметры:

Параметр	Название	Описание
Базовый адрес авторизации	`issuer`	Адрес приложения Авторизация по звонку. В текущей версии —

(issuer)		`<https://flashcall.kloud.one>`
Идентификатор ресурса (client_id)	`client_id`	Идентификатор приложения, созданного в сервисе Авторизация по звонку
Секретный ключ (Client_secret)	`client_secret`	Секретный ключ приложения, созданного в сервисе Авторизация по звонку
Использовать для входа по коду	-	Номер телефона будет использоваться для входа в приложения с помощью одноразовых паролей
Изображение телефона	-	Иконка, которая будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**

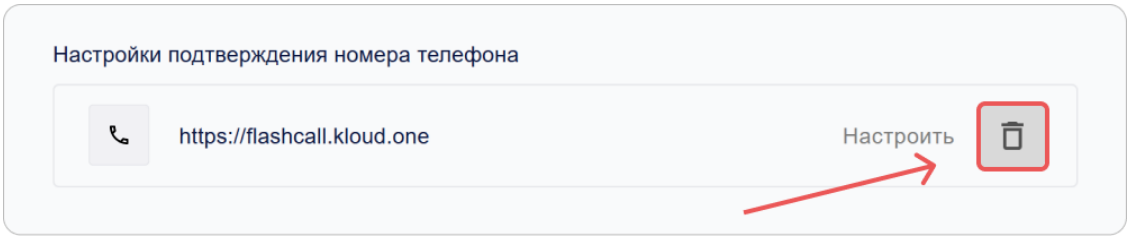
7. Нажмите **Сохранить**.

Редактирование настройки

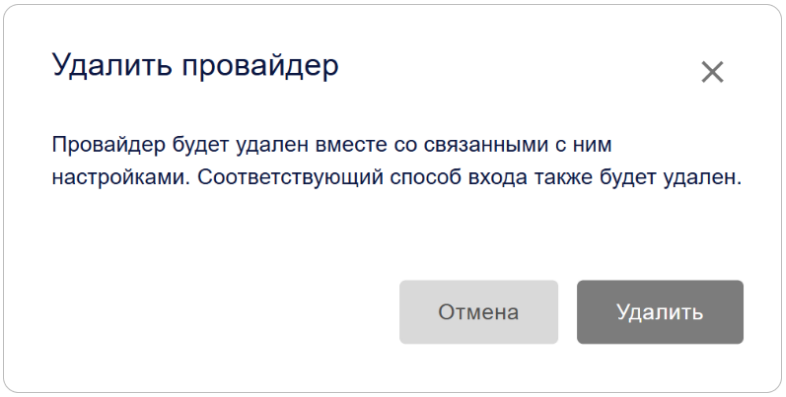
1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Номер телефона**.
4. Откроется форма редактирования.
5. В разделе **Настройки подтверждения номера телефона** нажмите **Настроить**.
6. Откроется форма редактирования.
7. Внесите необходимые изменения.
8. Нажмите **Сохранить**.

Удаление настройки

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Номер телефона**.
4. Откроется форма редактирования.
5. Нажмите **Удалить** в разделе **Настройки подтверждения номера телефона**.



6. Подтвердите действие в модальном окне.



Смотрите также

- Способы входа и настройка виджета входа — руководство по подключению и настройке внешних сервисов аутентификации.
- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.
- **Управление пользователями — руководство по управлению учетными записями пользователей.**

Как настроить способы входа в КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить способы входа в **КриптоАРМ IDM**, включая стандартные OAuth-провайдеры и усиленные методы аутентификации (WebAuthn, mTLS, TOTP). Мы также расскажем, как правильно настроить и оформить виджет авторизации, чтобы сделать вход в систему безопасным и удобным для пользователей.

Содержание:

- Обзор способов входа
- Управление способами входа
- Настройка виджета входа
- Смотрите также

Обзор способов входа

Способ входа — это метод аутентификации пользователей, позволяющий им авторизоваться в системе или подключенных приложениях. Это ключевой элемент системы единого входа, обеспечивающий гибкую и безопасную идентификацию.

Типы провайдеров аутентификации в КриптоАРМ IDM

В **КриптоАРМ IDM** поддерживаются следующие типы способов входа:

- **Базовые методы**: логин и пароль, электронная почта,
- **Внешние провайдеры идентификации**: социальные сети, доверенные корпоративные системы и другие сервисы,
- **Усиленные и беспарольные методы:** криптографическая аутентификация через **mTLS** (клиентские сертификаты), **WebAuthn** (биометрия, аппаратные ключи), одноразовые пароли **TOTP/HOTP**, а также вход через приложение **КриптоАРМ** с использованием пользовательского сертификата.

Комбинируйте способы входа для повышения безопасности. Реализуйте **двухфакторную аутентификацию**, при которой после ввода первого фактора (логин, пароль или другой способ) пользователь должен подтвердить свою личность с помощью второго фактора (телефон, электронная почта или WebAuthn). Как настроить двухфакторную аутентификацию →

Уровни управления и публичность способов входа

Способы входа могут создаваться на разных уровнях управления:

- Уровень сервиса – действует для всего сервиса;
- Уровень организации – действует в рамках конкретной компании;
- Уровень приложения – действует только для отдельного приложения.

Для способов входа, созданных на уровне **сервиса** или **организации**, можно настраивать **публичность** — определять, где именно они будут доступны.

Тип способа входа	Настройка публичности	Где доступен	Управление
Создан в панели администратора	✓ Да	Панель администратора и все приложения сервиса	Управляется только из **панели администратора**
Создан в организации	✓ Да	Все приложения данной организации	Управляется только из **панели организации**
Создан в приложении	✗ Нет	Только в этом приложении	Управляется в **настройках приложения**

Управление способами входа

Создание нового способа входа

Для большинства популярных сервисов в **КриптоАРМ IDM** предусмотрены готовые шаблоны с настройками. Они упрощают процесс подключения, так как содержат предзаполненные параметры, специфичные для каждого провайдера.

Процесс настройки включает три шага:

1. **Подготовка:** получите `Client ID` и `Client Secret` в сервисе-поставщике.
2. **Настройка в КриптоАРМ IDM:** создайте провайдер соответствующего типа.

Обратитесь к отдельной инструкции по настройке выбранного провайдера:

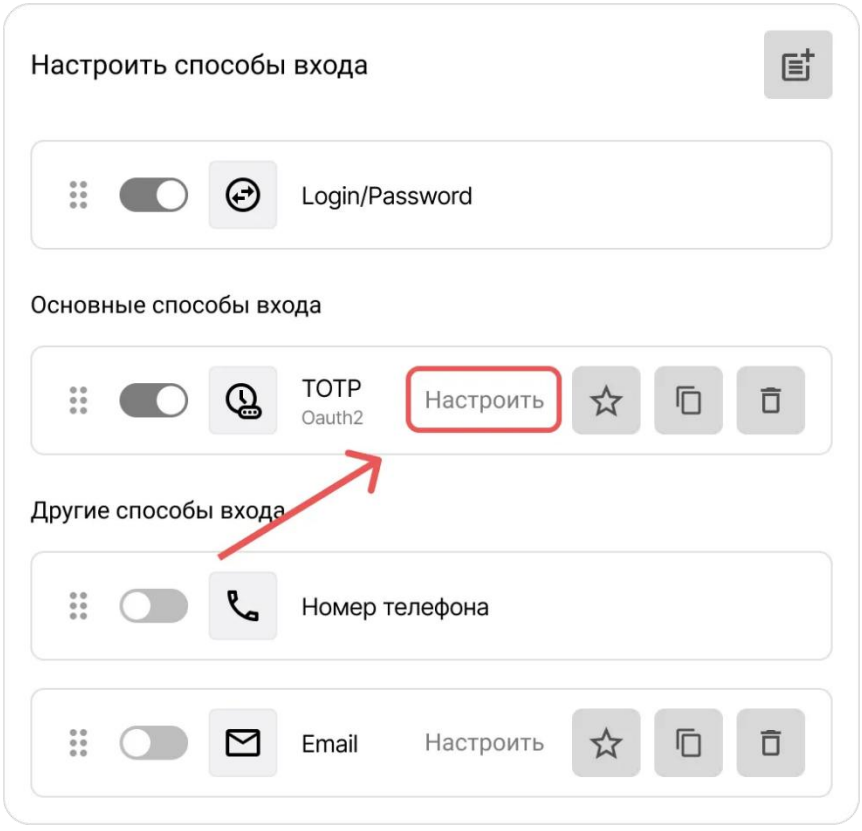
- **Электронная почта**: Email
- **Социальные сети:** ВКонтакте, Mail.ru, Яндекс
- **Универсальный:** OpenID Connect (для любых OIDC-совместимых систем)
- **Усиленные методы:** mTLS, КриптоАРМ (mTLS с поддержкой ГОСТ), WebAuthn, TOTP, HOTP

3. **Размещение на виджете:** добавьте способ входа на форму входа, доступную пользователям системы.

Редактирование существующего способа входа

Если необходимо обновить настройки существующего способа входа:

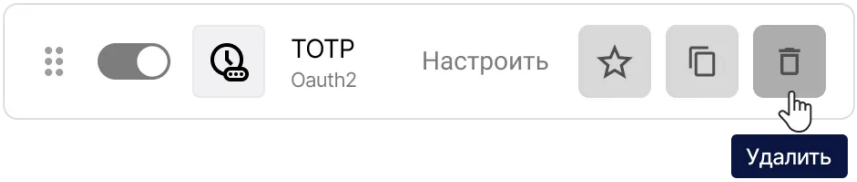
1. Перейдите в панель ID → раздел **Настройки**.
2. Нажмите **Настроить** в блоке **Способы входа**.
3. Откроется окно со списком созданных способов входа.
4. Нажмите кнопку **Настроить** на панели со способом входа, который необходимо отредактировать.



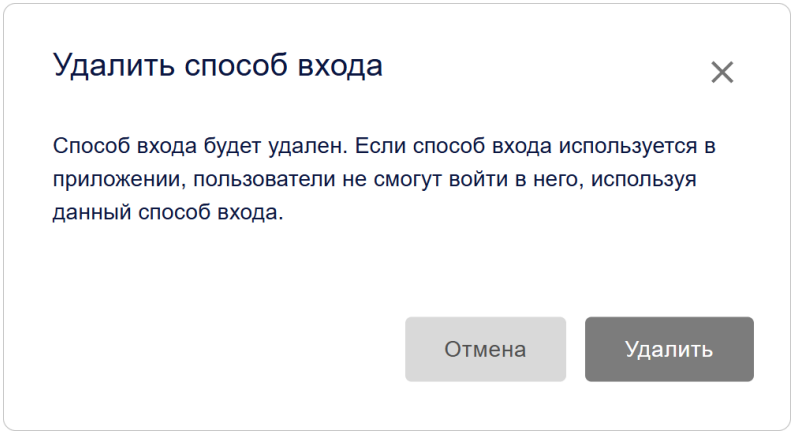
5. Откроется форма редактирования.
6. Внесите необходимые изменения.
7. Нажмите **Сохранить**.

Удаление способа входа

1. Перейдите в панель ID → раздел **Настройки**.
2. Раскройте блок **Способы входа**.
3. Нажмите **Настроить**.
4. Откроется окно со списком созданных способов входа.
5. Нажмите на кнопку **Удалить** , размещенную на панели со способом входа, который необходимо удалить.



6. Подтвердите действие в модальном окне.

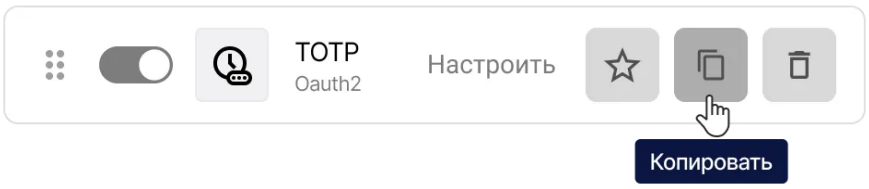


После успешного удаления способ входа исчезнет из виджетов всех связанных приложений.

Копирование настроек способа входа

Копирование настроек позволяет создать новый способ на основе ранее созданного.

1. Скопируйте настройки способа входа по кнопке **Копировать** , расположенной на панели со способом входа.



2. Далее откройте форму создания нового способа входа по шаблону с аналогичным типом и нажмите **Вставить** .

   ⚠️ **Примечание**: При несовпадении типов новый провайдер может работать некорректно.

Настройка обязательного идентификатора в профиле пользователя

Идентификаторы — это внешние сервисы, которые пользователь добавил в свой профиль или через которые он когда-либо входил в систему.

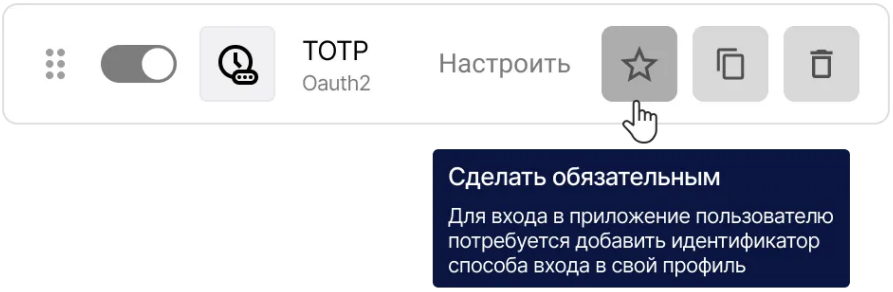
Список доступных для добавления идентификаторов формируется из способов входа в **КриптоАРМ IDM** с активной настройкой публичности.

- Если способ входа настроен как **публичный**, он появится в списке доступных для добавления в профиле пользователя.
- Размещать этот способ входа на виджете приложения необязательно — он может быть доступен в профиле даже без кнопки на главном экране входа.
- Пользователь также может добавить идентификатор во время входа через виджет, если такой способ входа доступен.

В **КриптоАРМ IDM** можно настроить требование обязательной привязки идентификатора внешнего аккаунта к профилю пользователя. В этом случае при входе в приложение у пользователя, не имеющего привязанного идентификатора, появится запрос на его добавление к профилю.

Как сделать идентификатор обязательным

1. Перейдите в панель ID → раздел **Настройки**.
2. Раскройте блок **Способы входа** и нажмите **Настроить**.
3. Откроется окно со списком созданных способов входа.
4. Нажмите на кнопку **Сделать обязательным** на панели со способом входа, который необходимо сделать обязательным.



Настройка применяется без дополнительного подтверждения.

💡 **Совет**: При повторном клике на кнопку **Сделать обязательным** наличие идентификатора в профиле станет необязательным.

Настройка виджета входа

Что такое виджет входа?

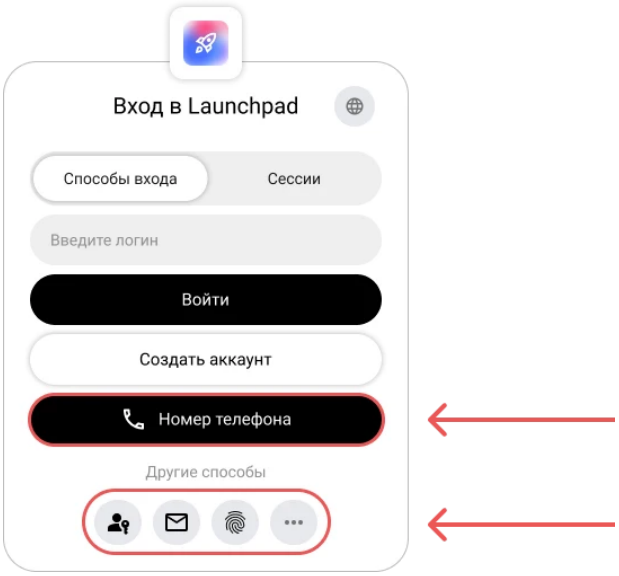
Виджет входа — это форма авторизации, которая отображается пользователю при попытке входа в приложение или систему **КриптоАРМ IDM**, если он ещё не прошёл аутентификацию.

Виджет поддерживает:

- классический вход по логину и паролю,
- вход через различные провайдеры,
- гибкую настройку внешнего вида и структуры,
- группировку способов входа.

В виджете способы входа делятся на:

- **Основные способы** — отображаются в виде отдельных кнопок под кнопкой **Войти** и используются чаще всего.
- **Дополнительные способы** — размещены в блоке **Другие способы** в виде компактных кнопок, чтобы не перегружать интерфейс.



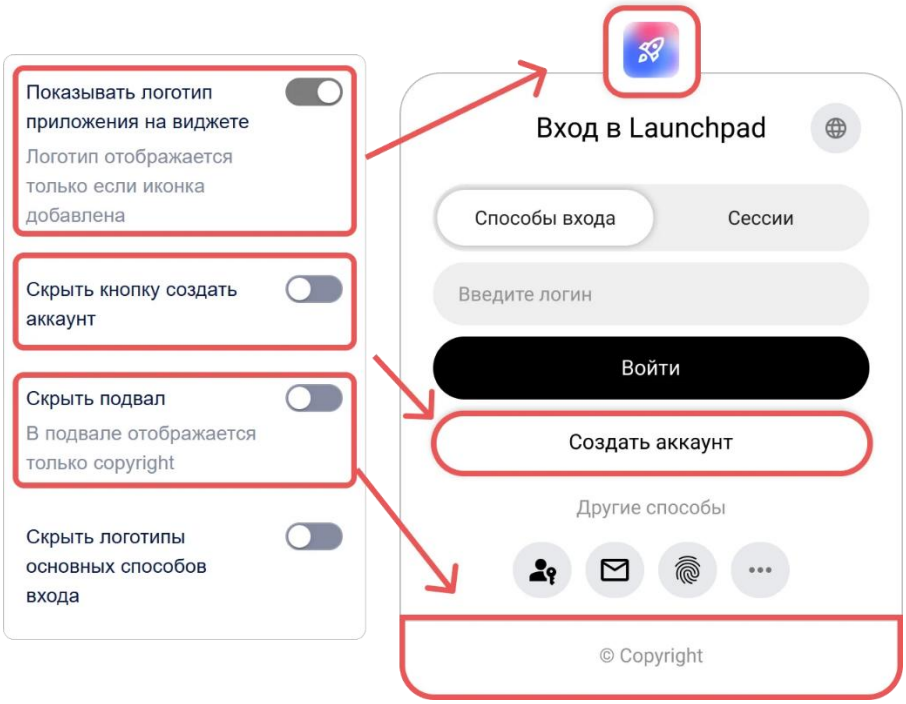
💡 **Виджет входа** — это первое, что видит пользователь при авторизации, поэтому важно, чтобы он соответствовал визуальному стилю компании и был максимально понятен.

Настройка внешнего вида виджета

Чтобы настроить внешний вид виджета:

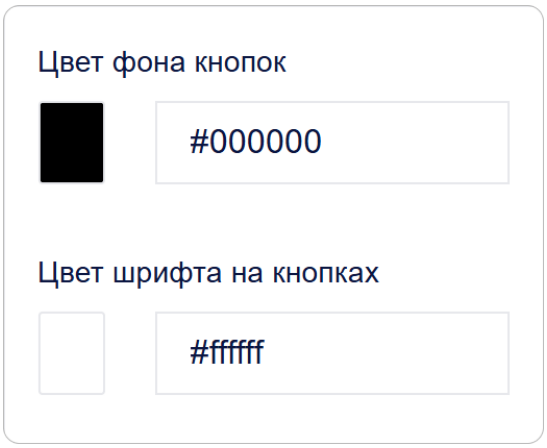
1. Перейдите в панель ID → раздел **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.

3. Откроется окно **Настроить внешний вид виджета**.
4. В первом блоке задаются ключевые визуальные элементы:
   - **Заголовок виджета** — Отображается в верхней части формы. Для отображения названия приложения в заголовке виджета используйте переменную `APP_NAME`.
   - **Обложка виджета** — Фоновое изображение формы авторизации.
   - **Режим автоподстановки обложки на виджетах приложений**:
     - **Отключено** — Используется обложка приложения,
     - **По умолчанию** — Только для приложений без обложки,
     - **Принудительный** — Применяется ко всем приложениям.
5. Во втором блоке настройте видимость элементов формы входа:
   - **Показывать логотип приложения на виджете** — При включении отображает логотип рядом с названием приложения. Используется изображение из раздела Основная информация.
   - **Скрыть кнопку создать аккаунт** — При включении скрывает кнопку создания аккаунта из виджета.
   - **Скрыть подвал** — При включении скрывает подвал виджета с копирайтом.
   - **Скрыть логотипы основных способов входа** — При включении скрывает логотипы способов входа из группы **Основные**.

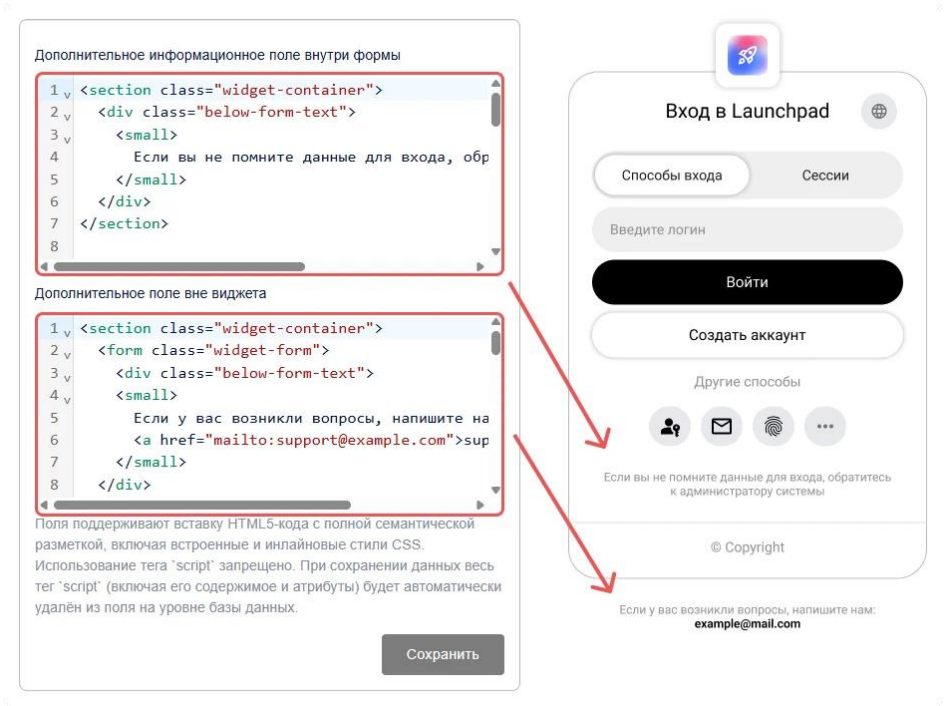


6. В третьем блоке настройте дизайн кнопок:

- **Цвет фона кнопок** — Цветовая схема для фона кнопки (hex-код).
- **Цвет шрифта на кнопках** — Задается цветовая схема для текста кнопки (hex-код).



7. При необходимости укажите текст:
   - **Дополнительное информационное поле внутри формы** — Дополнительный текст, который будет отображаться в нижней части виджета,
   - **Дополнительное информационное поле вне виджета** — Дополнительный текст, который будет отображаться под виджетом.



Поля поддерживают вставку HTML5-кода с полной семантической разметкой, включая встроенные и инлайновые стили CSS. Использование тега `script`

запрещено. При сохранении данных весь тег `script` (включая его содержимое и атрибуты) будет автоматически удалён из поля на уровне базы данных.

8. Нажмите **Сохранить**, чтобы применить изменения.

💡 В разделе **Превью** можно посмотреть результаты изменений.

Добавление и отключение способов входа на виджете

Чтобы настроить отображение способа входа в виджете:

1. Перейдите в панель ID → раздел **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. Включите или отключите переключатели для нужных способов входа.
4. При необходимости настройте группы способов входа.

⚠️ **Примечание**:

1. Невозможно отключить способ входа **Логин/пароль**. При отключении всех способов входа автоматически включается способ входа **Логин/пароль**, поскольку в виджете должен быть хотя бы один способ для входа.
2. Отключение способа входа с виджета не удаляет способ входа из системы.

Смотрите также

- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.
- Управление организацией — руководство по работе с организацией в **КриптоАРМ IDM**.
- **Регистрация и вход пользователей — инструкция по созданию аккаунта, входу с помощью логина/пароля и внешних сервисов аутентификации.**

Как настроить доверенные провайдеры в КриптоАРМ IDM

Узнайте, как подключить доверенные провайдеры в **КриптоАРМ IDM** и обеспечить безопасную корпоративную аутентификацию пользователей на основе внешних систем.

Содержание:

- Что такое доверенные провайдеры?
- Управление доверенными провайдерами
- Автоматическое объединение профилей пользователей
- Смотрите также

Что такое доверенные провайдеры?

Доверенные провайдеры — это внешние корпоративные или государственные системы (например, Active Directory, 1С), которые выступают **источником верифицированных данных** о пользователе.

Ключевые особенности:

1. При входе через доверенный провайдер автоматически создается пользователь в **КриптоАРМ IDM**, профиль которого содержит данные пользователя внешней системы.
2. Профиль пользователя, созданный через доверенный провайдер, не доступен для редактирования пользователю.
3. При авторизации доверенного пользователя его профиль автоматически синхронизируется с внешней системой. Это происходит независимо от того, какой провайдер был использован для входа.

Поддерживаемые доверенные провайдеры

В **КриптоАРМ IDM** поддерживаются следующие доверенные провайдеры:

- **LDAP (Active Directory)** — вход по учетным данным пользователя службы каталогов Active Directory;
- **ALD Pro** — вход по учетным данным пользователя службы каталогов ALD Pro;
- **1С** — вход по учетным данным пользователя системы 1С.

Уровни управления

Доверенные провайдеры, как и способы входа, могут создаваться на разных уровнях системы **КриптоАРМ IDM** в зависимости от уровня доступа пользователя. Подробнее читайте в инструкции Как настроить способы входа.

Управление доверенными провайдерами

Создание нового провайдера

Для большинства популярных сервисов и корпоративных систем в **КриптоАРМ IDM** предусмотрены готовые шаблоны с настройками. Они упрощают процесс подключения, так как содержат предзаполненные параметры, специфичные для каждого провайдера.

Процесс настройки включает три шага:

1. **Подготовка:** настройка на стороне доверенной системы.
2. **Настройка в КриптоАРМ IDM:** создание провайдера соответствующего типа.
3. **Размещение на виджете:** добавление созданного провайдера на форму входа, доступную пользователям системы.

Обратитесь к отдельной инструкции по настройке выбранного провайдера:

- Как подключить вход через LDAP,

- Как подключить вход через 1С,
- Как подключить вход через ALD Pro.

> **Важно:**
> Для подключения доверенного провайдера требуется лицензия.
> Подробнее о лицензировании.

Редактирование существующего провайдера

Если необходимо обновить настройки существующего провайдера:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Нажмите **Настроить** в блоке **Доверенные провайдеры**.
3. Откроется окно со списком созданных провайдеров.
4. Нажмите кнопку **Настроить** на панели с провайдером, который необходимо отредактировать.
5. Откроется форма редактирования.
6. Внесите необходимые изменения.
7. Нажмите **Сохранить**.

Удаление провайдера

1. Перейдите в панель ID → вкладка **Настройки**.
2. Нажмите **Настроить** в блоке **Доверенные провайдеры**.
3. Откроется окно со списком созданных провайдеров.
4. Нажмите на кнопку **Удалить**  , размещенную на панели с провайдером, который необходимо удалить.
5. Подтвердите действие в модальном окне.

После успешного удаления способ входа исчезнет из виджетов всех связанных приложений.

Копирование настроек провайдера

Копирование настроек позволяет создать новый провайдер на основе ранее созданного.

1. Скопируйте настройки провайдера по кнопке **Копировать**  , расположенной на панели со способом входа.
2. Далее откройте форму создания нового провайдера по шаблону с аналогичным типом и нажмите **Вставить**  .

   ⚠ **Примечание**: При несовпадении типов новый провайдер может работать некорректно.

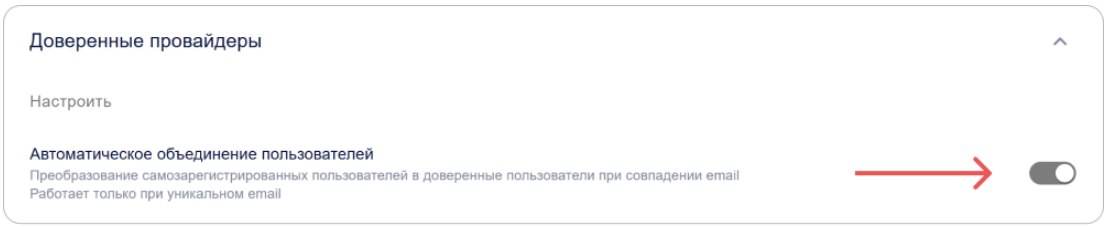
Автоматическое объединение профилей пользователей

Функция **Автоматическое объединение пользователей** автоматически объединяет профили самозарегистрированных пользователей с профилями из доверенных систем при **совпадении email**.

> ⚠️ **Ограничения**: Функция работает только при уникальном адресе электронной почты в профилях самозарегистрированных пользователей. Перед активацией выполните проверку дубликатов профилей.

Чтобы включить автоматическое объединение пользователей:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Доверенные провайдеры**.
3. Активируйте переключатель **Автоматическое объединение пользователей**.



> 💡 После активации система начнёт автоматически связывать профили при первой авторизации через доверенный источник.

Смотрите также

- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.
- Управление организацией — руководство по работе с организацией в **КриптоАРМ IDM**.
- **Регистрация и вход пользователей — инструкция по созданию аккаунта, входу с помощью логина/пароля и внешних сервисов аутентификации.**

Управление пользователями КриптоАРМ IDM

В этом руководстве вы узнаете, как создавать и редактировать профили пользователей в **КриптоАРМ IDM**, назначать им роли и права доступа, блокировать и удалять аккаунты, завершать активные сеансы, управлять публичностью и экспортировать данные профиля.

Содержание:

- Создание пользователя
- Просмотр и редактирование профиля пользователя

- Управление данными профиля
- Доступ и безопасность
- Статус аккаунта
- Удаление пользователя
- Смотрите также

Создание пользователя

В **КриптоАРМ IDM** возможны несколько способов регистрации пользователей:

- самостоятельная регистрация через виджет,
- ручное создание пользователей.

> 💡 Если организация использует инсталляцию **КриптоАРМ IDM** как внутреннюю корпоративную систему и одновременно предоставляет возможность самостоятельной регистрации внешним пользователям, рекомендуется создавать сотрудников через механизм внутренних пользователей.

В данной инструкции мы рассмотрим, как создать пользователя вручную:

1. Перейдите в панель ID → вкладка **Пользователи**.
2. Нажмите на кнопку **Создать пользователя**  .
3. Откроется форма создания пользователя.
4. На форме создания заполните поля профиля:
   - **Публичное имя** — отображаемое имя пользователя в системе;
   - **Имя** — имя и отчество пользователя;
   - **Фамилия** — фамилия пользователя;
   - **Логин** — должен быть уникальным для сервиса, в дальнейшем с его помощью можно авторизоваться;
   - **Электронная почта** — адрес должен быть уникальным для сервиса, в дальнейшем с его помощью можно авторизоваться;
   - **Создать email как подтвержденный** — если настройка отключена, адрес электронной почты будет добавлен как неподтвержденный. Неподтвержденный адрес нельзя использовать для входа в систему,

получения уведомлений и восстановления доступа к аккаунту. Администратор может позже подтвердить адрес вручную из профиля пользователя.

- **Номер телефона** — должен быть уникальным для сервиса, в дальнейшем с его помощью можно авторизоваться;

- **Создать телефон как подтвержденный** — по аналогии с почтовым адресом: если настройка отключена, номер телефона добавляется как неподтвержденный;

- **Пароль** — должен соответствовать парольной политике, заданной в настройках сервиса.

  🔗 Подробнее в инструкции Настройка парольной политики.

- **Требовать смены пароля при следующей авторизации** — пользователь будет перенаправлен на экран смены пароля при следующем входе через виджет.

- **Дата рождения**;

- **Фото профиля**.

5. Нажмите **Сохранить**.

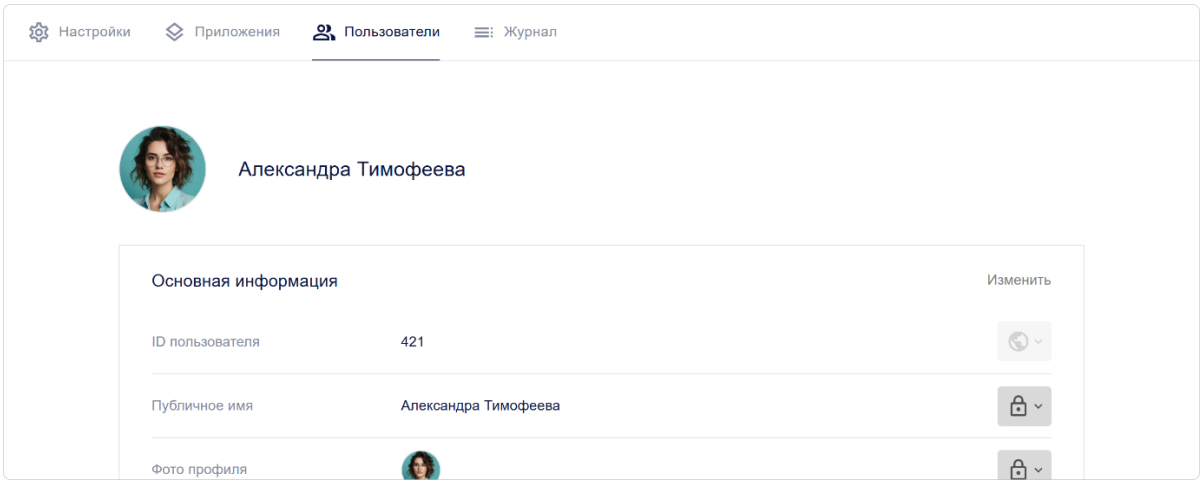
   💡 Профиль пользователя может содержать дополнительные поля.

Просмотр и редактирование профиля пользователя

Просмотр профиля пользователя

Чтобы получить детальную информацию об аккаунте, откройте его профиль.

1. Перейдите в панель ID → вкладка **Пользователи**.
2. Нажмите на панель с пользователем, профиль которого необходимо просмотреть.
3. Откроется профиль пользователя с детальной информацией: контактные данные, идентификаторы, настройки публичности.



Редактирование данных профиля

Для внесения изменений в профиль пользователя:

1. Перейдите в панель ID → вкладка **Пользователи**.
2. Откройте профиль пользователя.
3. Нажмите **Изменить** в блоке **Основная информация**.
4. В открывшейся форме **Редактировать пользователя** внесите необходимые изменения.
5. Нажмите **Сохранить**.

Управление данными профиля

Управление идентификаторами профиля

В разделе **Идентификаторы** профиля пользователя отображаются способы входа пользователя, которые он добавил самостоятельно или использовал для входа в приложение или в систему **КриптоАРМ IDM**. Администратор может настроить публичность идентификатора и удалить его из профиля пользователя.

> 💡 **Важно:** Добавлять новые идентификаторы может только владелец аккаунта. Подробнее в руководстве Идентификаторы внешних сервисов.

Чтобы удалить идентификатор:

1. Перейдите в панель ID → вкладка **Пользователи**.
2. Откройте профиль пользователя.
3. Нажмите **Удалить** на панели со способом входа, который необходимо удалить из профиля.

Идентификатор будет немедленно удален из профиля.

Настройка публичности полей профиля

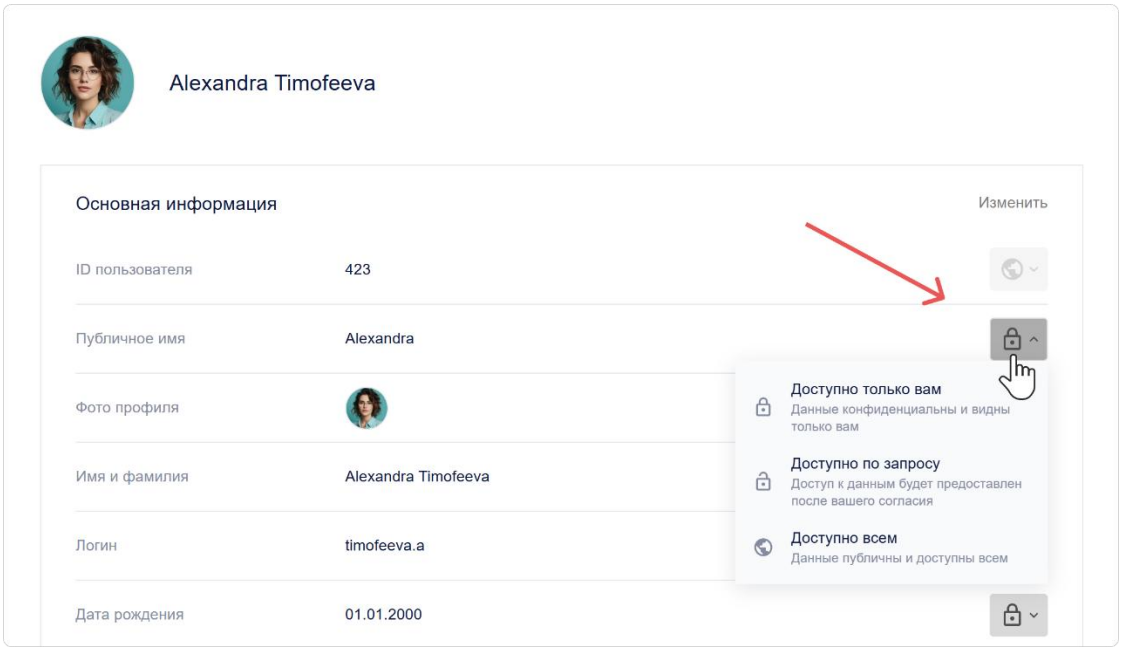
В каждом поле профиля можно настроить уровень публичности, определяющий, кто сможет видеть эту информацию. Доступны настройки для основных и дополнительных данных о пользователе, а также для способов входа.

Уровни публичности

Уровень	Иконка	Описание
Доступно только вам		Данные не передаются в сторонние системы и доступны только пользователю.
Доступно по запросу		Данные доступны в сторонних системах, с которыми настроена интеграция **КриптоАРМ IDM**. Для доступа к данным требуется согласие пользователя.
Доступно всем		Данные публичны всегда. Для доступа к ним не требуется согласие пользователя.

Как изменить публичность поля профиля

1. Перейдите в панель ID → вкладка **Пользователи**.
2. Откройте профиль пользователя.
3. Нажмите на текущую иконку публичности рядом с полем.
4. В выпадающем меню выберите новый уровень.



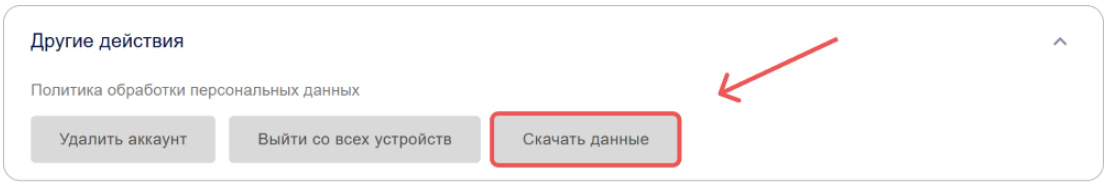
Изменение применяется мгновенно.

Экспорт данных профиля

КриптоАРМ IDM позволяет экспортировать все данные профиля в JSON формате.

Чтобы скачать данные профиля:

1. Перейдите в панель ID → вкладка **Пользователи**.
2. Откройте профиль пользователя.
3. Раскройте блок **Другие действия**.



4. Выберите действие **Скачать данные**.
5. Загрузка JSON-файла начнется автоматически.

Структура экспортированного файла

Экспортированный файл содержит полный список данных пользователя:


```
{
  "user": {
    "id": 1573,
    "email": "ivanov.petr89@mail.com",
    "birthdate": "1992-11-14T15:22:11.123Z",
    "family_name": "Иванов",
    "given_name": "Петр",
```

```
    "nickname": "Петя",
    "login": "petr_ivanov92",
    "phone_number": "+79991234567",
    "picture": "public/images/profile/3f7b21d8e4c2a6f1b2c9d3a0e5f7b1c4",
    "public_profile_claims_oauth": "id email family_name given_name picture",
    "public_profile_claims_gravatar": "family_name given_name email picture",
    "blocked": false,
    "deleted": null,
    "custom_fields": {
      "country": "Россия"
    },
    "password_updated_at": "2025-10-12T08:45:33.222Z"
  },
  "role": "ADMIN"
}
```

Доступ и безопасность

Завершение сеансов пользователя

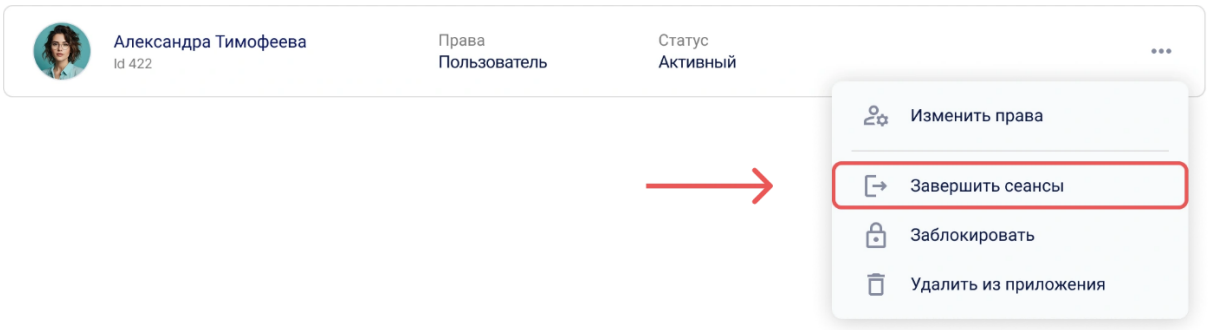
Функция принудительного завершения всех активных сессий — важный инструмент безопасности. Используйте его в случае утери устройства, подозрения на взлом аккаунта или для немедленного обновления токенов доступа.

> 📌 Эта операция немедленно аннулирует все access- и refresh-токены пользователя, завершая все его текущие сессии во всех приложениях. Пользователю потребуется войти заново.

Как завершить сеансы пользователя

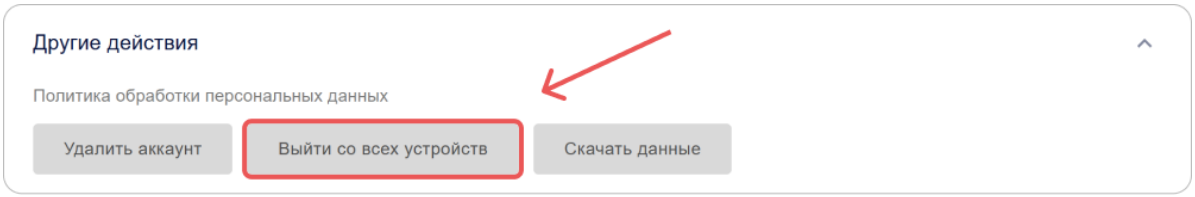
Способ 1: Из общего списка пользователей

1. Перейдите в панель ID → вкладка **Пользователи**.
2. Нажмите **Завершить сеансы** в меню действий с пользователем.



Способ 2: Из профиля пользователя

1. Перейдите в панель ID → вкладка **Пользователи**.
2. Нажмите **Завершить сеансы** в профиле пользователя в блоке **Другие действия**.



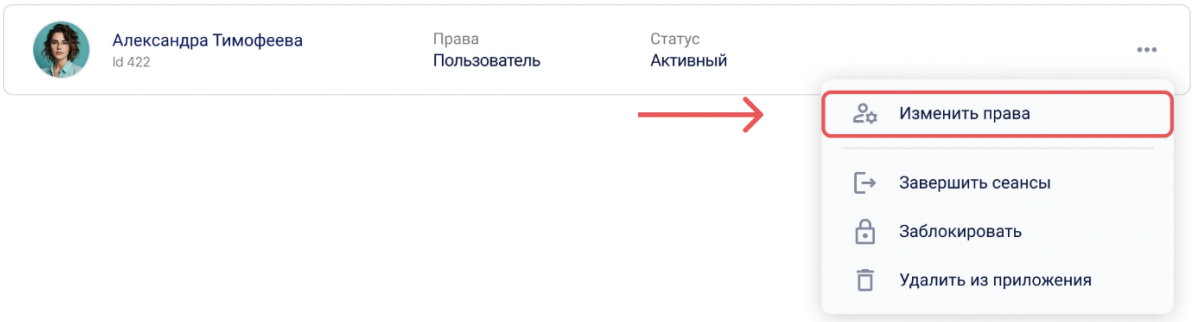
Что происходит после подтверждения:

- **Все активные сессии** пользователя завершаются
- **Токены доступа** (`access_token`) становятся недействительными
- **Токены обновления** (`refresh_token`) аннулируются
- Пользователю потребуется **войти заново** при следующем обращении к приложению

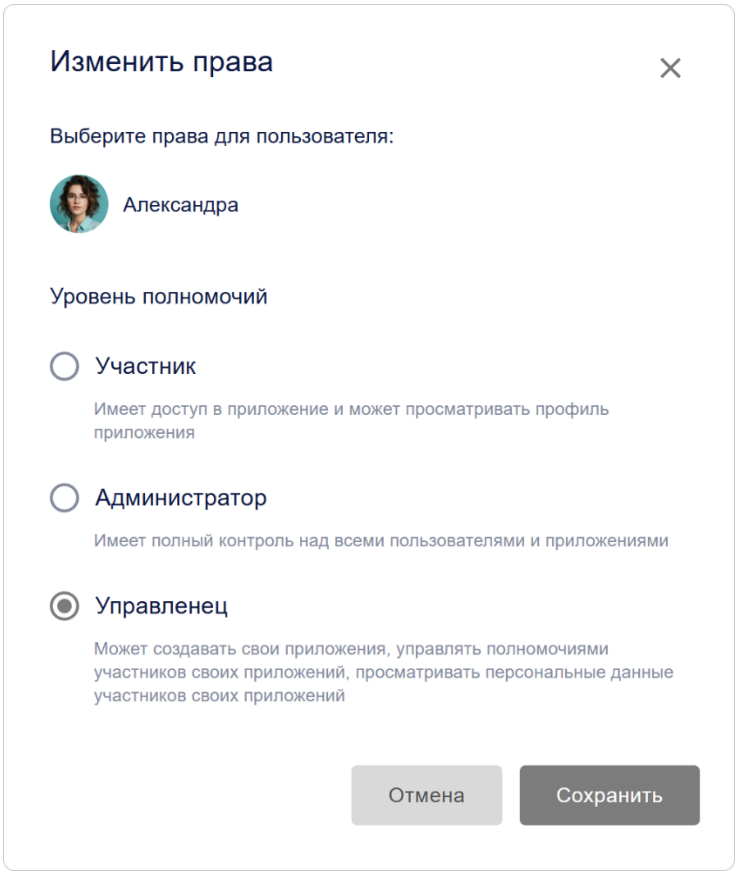
📌 Эта операция не блокирует пользователя. Он сможет авторизоваться снова.

Назначение и изменение полномочий пользователя

1. Перейдите в панель ID → вкладка **Пользователи**.
2. Вызовите меню действий по кнопке **Еще** для пользователя, права которого необходимо изменить.
3. Выберите действие **Изменить права**.



4. В открывшемся окне выберите необходимую роль и нажмите **Сохранить**.



Пользователь получит выбранную роль и соответствующие ей права.

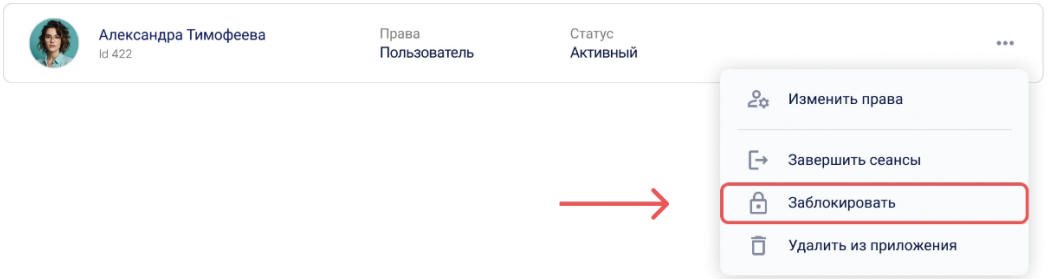
Статус аккаунта

Блокирование пользователей КриптоАРМ IDM

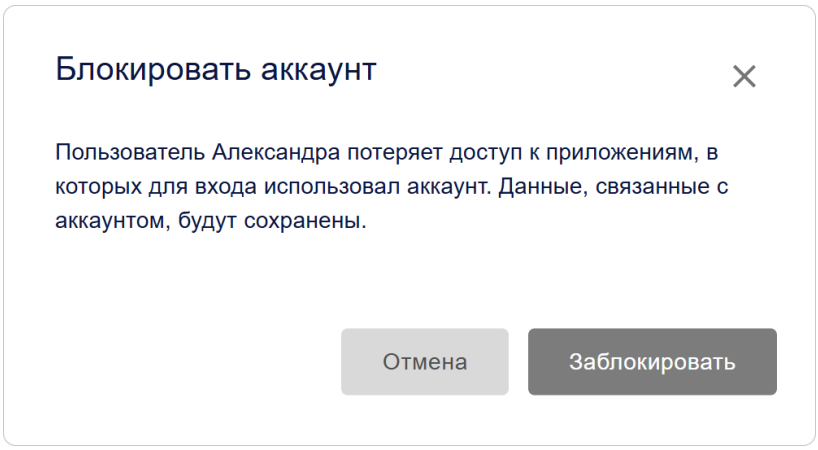
Блокировка запрещает доступ ко всем сервисам, использующим **КриптоАРМ IDM** для входа.

Чтобы заблокировать пользователя:

1. Вызовите меню действий с активным пользователем в одном из интерфейсов:
   - В меню действий с пользователем в профиле приложения.
   - В меню действий с пользователем на вкладке **Пользователи**.

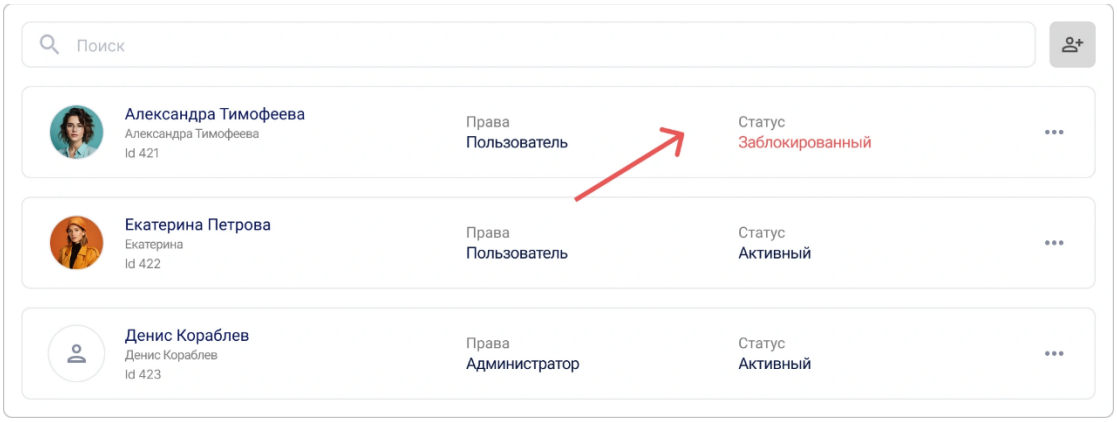


2. Выберите действие **Блокировать в КриптоАРМ IDM**.
3. Подтвердите действие в модальном окне.



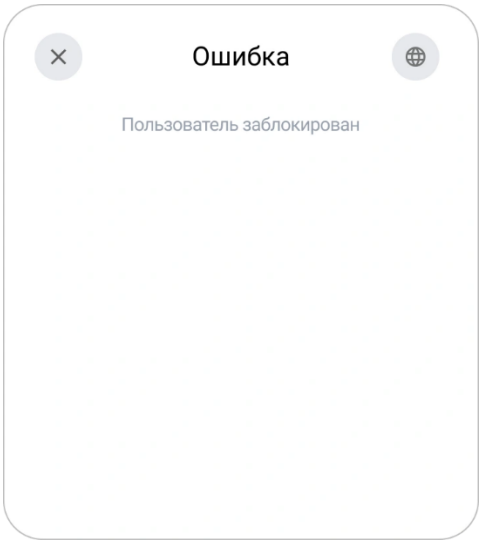
Что происходит после блокировки:

- Статус пользователя изменится на **Заблокированный**.



- Заблокированный пользователь не сможет войти в приложение.

  При попытке входа будет отображаться следующий виджет:



Разблокирование пользователей КриптоАРМ IDM

Чтобы разблокировать пользователя:

1. Вызовите меню действий с заблокированным пользователем в одном из интерфейсов:
   - В меню действий с пользователем в профиле приложения.
   - В меню действий с пользователем на вкладке **Пользователи**.
2. Выберите действие **Разблокировать в КриптоАРМ IDM**.
3. Подтвердите действие в модальном окне.

После подтверждения действия статус пользователя изменится на **Активный**.

Удаление пользователя

Администратор может навсегда удалить пользователя. После подтверждения удаления аккаунт и все данные исчезнут безвозвратно. Пользователь потеряет доступ ко всем приложениям, где использовался его аккаунт **КриптоАРМ IDM**.

> 💡 Пользователь может самостоятельно удалить свой аккаунт через личный профиль. Удаление реализовано с **механизмом отсрочки**. В течение определенного времени пользователь может восстановить доступ к своему аккаунту. Подробнее об этом можно узнать в инструкции Профиль пользователя.

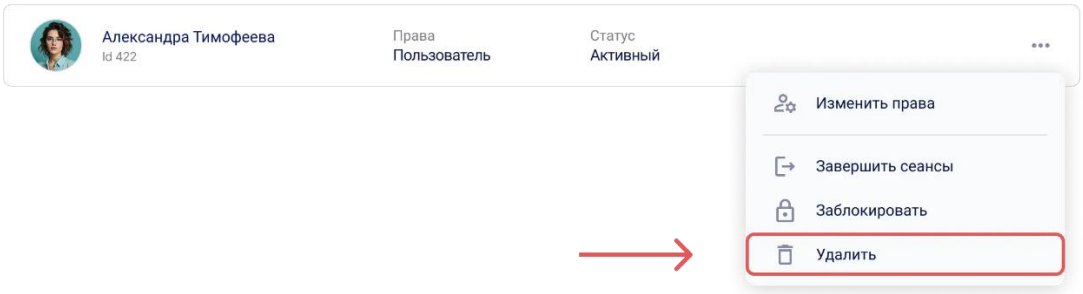
Как удалить пользователя КриптоАРМ IDM

> 💡 **Альтернатива**: Рассмотрите возможность **блокировки аккаунта** вместо удаления, если есть вероятность восстановления доступа.

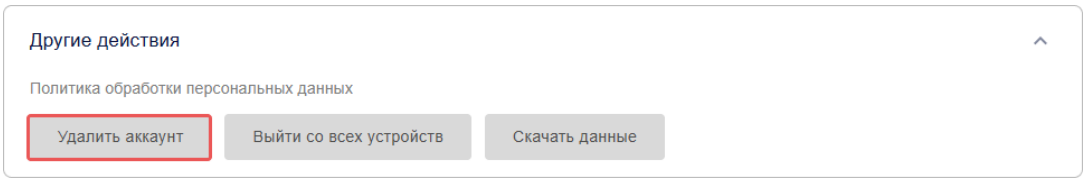
Чтобы удалить пользователя:

1. Нажмите **Удалить аккаунт** в одном из интерфейсов:

– В меню действий с пользователем на вкладке **Пользователи**.



– В профиле пользователя в блоке **Другие действия**.



2. Подтвердите действие в модальном окне.

После подтверждения пользователь будет удален.

Что происходит после удаления:

- Приложения, где удаляемый пользователь является единственным владельцем, будут безвозвратно удалены.
- Все данные аккаунта стираются без возможности восстановления после окончательного удаления.
- Пользователь теряет доступ ко всем интегрированным сервисам.

Смотрите также

- Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.
- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.
- Управление организацией — руководство по работе с организацией в **КриптоАРМ IDM**.

Как настроить и подключить мини-виджет КриптоАРМ IDM

В этом руководстве вы узнаете, как подключить и настроить мини-виджет **КриптоАРМ IDM** на вашем веб-ресурсе. Вы научитесь настраивать параметры аутентификации, отображение профиля пользователя, кнопки входа и меню, а также кастомизировать внешний вид виджета, чтобы он гармонично вписывался в дизайн вашего проекта.

Содержание:

- Что такое мини-виджет?
- Конфигурация виджета
- Настройка отображения профиля
- Настройка кнопки входа
- Параметры кнопок меню
- Стилизация мини-виджета
- Индивидуальная стилизация кнопок меню
- Смотрите также

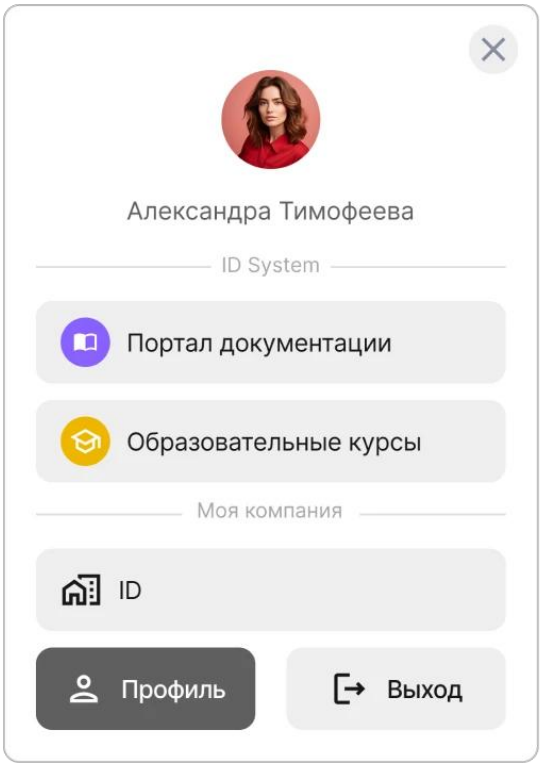
Что такое мини-виджет?

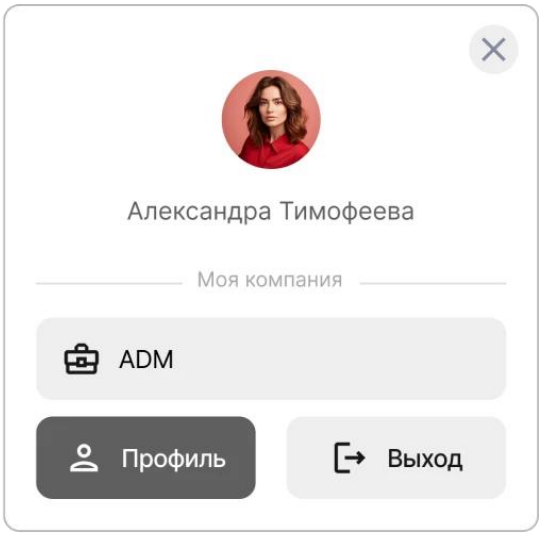
Мини-виджет — это меню с данными о пользователе и важными функциями. В нем доступны профиль, панель управления системой, организацией, приложением, а также выход из системы. Также здесь можно разместить приложение для быстрого доступа. Виджет открывается при клике на аватар пользователя в правом верхнем углу экрана.

Мини-виджет представляет из себя лёгкий JavaScript-компонент для аутентификации пользователей в сервисе **КриптоАРМ IDM**. Он работает по стандартам OIDC/OAuth2, PKCE и может быть встроен в любые веб-сайты или интерфейсы — от простого HTML до SPA на React или Vue.

> 💡 Чтобы добавить приложение в мини-виджет включите переключатель **Отображать в мини-виджете** в настройках приложения.

Примеры виджетов:





Конфигурация виджета

Обязательные параметры

Для базовой работы виджета необходимо указать три ключевых параметра:

Параметр	Тип	Описание	Пример
`appId`	`string`	Уникальный идентификатор приложения в Trusted	`"MTnOOTdx85FgNbOFy2nUsH"`
`backendUrl`	`string`	URL вашего backend API	`"http://localhost:3001"`
`redirectUrl`	`string`	URL для перенаправления после авторизации	`"http://localhost:3000/login"`

Дополнительные параметры

Для расширенной настройки доступны опциональные параметры:

Параметр	Тип	Описание	Значение по умолчанию
`issuer`	`string`	URL Trusted SSO сервера	`"https://id.kloud.one"`
`withOutHomePage`	`boolean`	Автоматический редирект на авторизацию	`false`
`getTokenEndPoint`	`string`	Endpoint для получения токена	`"/api/oidc/token"`
`getUserInfoEndPoint`	`string`	Endpoint для получения данных пользователя	`"/api/oidc/me"`
`scopes`	`string[]`	OAuth2 разрешения	`["openid", "lk", "profile"]`
`profile`	`IProfileConfig`	Настройки профиля пользователя	См. раздел ниже
`loginButton`	`ICustomMenuButton`	Настройки кнопки входа	См. раздел ниже
`menuButtons`	`ICustomMenuButton[]`	Массив дополнительных кнопок	См. раздел ниже
`customStyles`	`ICustomStyles`	Глобальные стили виджета	См. раздел ниже

Базовый пример подключения

```
import { TrustedWidget, TrustedWidgetConfig } from "trusted-widget";

const newConfig: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  issuer: "https://id.kloud.one",
  withOutHomePage: false,
  getTokenEndPoint: "/api/oidc/token",
  getUserInfoEndPoint: "/api/oidc/me",
};

// Использование компонента
<TrustedWidget config={newConfig} />;
```

Настройка отображения профиля

Параметры конфигурации профиля

Профиль пользователя — это компонент, который содержит аватар и имя пользователя.

Параметр	Тип	Описание	Значение по умолчанию
`isHideText`	`boolean`	Скрыть отображение имени пользователя	`false`
`wrapper`	`IComponentStyles`	Стили контейнера профиля (только цвета)	См. раздел стилей
`button`	`IComponentStyles`	Стили кнопки-аватара пользователя (только цвета)	См. раздел стилей

> ⚠️ **Важно:** Для настроек профиля (`profile.wrapper` и `profile.button`) можно изменять только цвета (`color.text`, `color.background`, `color.hover`) и скрывать имя пользователя (`isHideText`). Другие параметры стилизации (такие как `borderRadius`, `padding`, `position`) не применяются к профилю.

Пример настройки профиля

```
// Пример: Только аватар без текста
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  profile: {
    isHideText: true, // Скрыть имя, показывать только аватар
  },
};
```

Настройка кнопки входа

Кнопка входа отображается для неавторизованных пользователей. Вы можете настроить её текст, иконку и стили.

Параметры кнопки входа

Параметр	Тип	Описание	Значение по умолчанию
`text`	`string`	Текст кнопки входа	`"Войти"`
`type`	`string`	Тип кнопки	`"login"`
`icon`	`string | React.ReactElement`	Ссылка на изображение или React элемент	`null`
`customStyles`	`IComponentStyles`	Индивидуальные стили для кнопки	См. раздел стилей

Пример конфигурации

```
// Пример: Кнопка с кастомной иконкой
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  loginButton: {
    text: "Войти через Trusted",
    type: "login",
    icon: "https://id.kloud.one/favicon.ico", // Пользовательская иконка
  },
};

// Пример: Простая текстовая кнопка без иконки
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  loginButton: {
    text: "Войти",
    type: "login",
    customStyles: {
      isHideIcon: true, // Скрыть иконку
    },
  },
};
```

Параметры кнопок меню

Обязательные параметры

Параметр	Тип	Описание	Пример
`text`	`string`	Отображаемое название кнопки	`"TestService"`

`link`	`string`	Ссылка на страницу для перехода	`"https://test.com"`

Дополнительные параметры

Параметр	Тип	Описание	Значение по умолчанию
`icon`	`string | React.ReactElement`	Ссылка на изображение или React элемент	`null`
`customStyles`	`IComponentStyles`	Индивидуальные стили для кнопки	См. раздел стилей

Пример конфигурации

```
import { TrustedWidget, TrustedWidgetConfig } from "trusted-widget";

const newConfig: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  menuButtons: [
    {
      text: "TestService",
      link: "https://test.com",
      icon: "https://image.png", // | <Icon />
    },
  ],
};
```

Стилизация мини-виджета

Виджет поддерживает детальную кастомизацию внешнего вида через объект `customStyles`. Вы можете управлять цветами, скруглениями, отступами и выравниванием всех элементов.

Структура объекта стилей

```
customStyles: {
  global: {
    borderRadius: "8px",         // Глобальное скругление
    color: { /* цвета */ }       // Глобальные цвета
  },
  components: {
    primaryButton: { /* стили */ },   // Основные кнопки
    secondaryButton: { /* стили */ }, // Второстепенные кнопки
    accountButton: { /* стили */ }    // Кнопки меню аккаунта
  }
}
```

Параметры кастомных стилей

Глобальные стили

Параметр	Тип	Описание	Пример
`global.borderRadius`	`string`	Скругление углов для всех элементов	`"12px"`
`global.color`	`IComponentStyles`	Глобальные цвета	См. ниже

Стили компонентов

Параметр	Тип	Описание	Назначение
`components.primaryButton`	`IComponentStyles`	Стиль основной кнопки	Кнопка “Войти”, “Профиль”
`components.secondaryButton`	`IComponentStyles`	Стиль второстепенной кнопки	Кнопка “Выход”
`components.accountButton`	`IComponentStyles`	Стиль кнопок меню аккаунта	Кнопки в выпадающем меню

Параметры стилей компонентов IComponentStyles

Параметр	Тип	Описание	Пример
`color.text`	`string`	Цвет текста и иконки (HEX)	`"#ffffff"`
`color.background`	`string`	Цвет фона (HEX)	`"#1976d2"`
`color.hover`	`string`	Цвет фона при наведении (HEX)	`"#1565c0"`
`borderRadius`	`string`	Скругление углов элемента	`"8px"`
`padding`	`string`	Внутренние отступы	`"8px 16px"`
`position`	`"left" | "center"`	Выравнивание контента в кнопке	`"center"`
`isHideIcon`	`boolean`	Скрыть иконку в кнопке	`false`

Наследование стилей

Виджет имеет умную систему наследования стилей для кнопки `secondaryButton`:

- **Если заданы стили только для `primaryButton`**, то они автоматически применяются и к `secondaryButton`, но с большей прозрачностью (через уменьшение opacity).
- **Если заданы отдельные стили для `secondaryButton`**, то прозрачность применяться не будет — используются только явно указанные параметры.

Пример конфигурации стилей

Пример настройки глобальных стилей

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
```

```
  redirectUrl: "http://localhost:3000/login",
  // Дефолтные значения для глобальных стилей
  customStyles: {
    global: {
      color: {
        text: "#666666",
        background: "#ffffff",
      },
      borderRadius: "8px",
    },
    components: {
      accountButton: {
        color: {
          text: "#fff",
          background: "#efefef",
          hover: undefined, // если не задан применяется filter: brightness(90%)
        },
        position: "left",
        isHideIcon: false,
      },
      primaryButton: {
        color: {
          text: "#ffffff",
          background: "#b5262f",
          hover: undefined, // если не задан применяется filter: brightness(90%)
        },
        position: "left",
        isHideIcon: false,
      },
      // secondaryButton не задан — будет использоваться стиль primaryButton с
прозрачностью (opacity:0.5)
    },
  },
};
```

Пример полной конфигурации стилей

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  // Настройки профиля
  profile: {
    isHideText: false,
    wrapper: {
      color: {
        text: "#333333",
        background: "#f8f9fa",
      },
    },
    button: {
      color: {
        text: "#333333",
```

```
        background: "transparent",
        hover: "rgba(0, 0, 0, 0.08)",
      },
    },
  },
};
```

Пример полной конфигурации с кнопкой входа

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  // Кнопка входа с иконкой
  loginButton: {
    text: "Войти",
    type: "login",
    icon: "https://id.kloud.one/favicon.ico",
    customStyles: {
      color: {
        text: "#ffffff",
        background: "#4CAF50",
        hover: "#45a049",
      },
      borderRadius: "8px",
      padding: "10px 20px",
    },
  },
};
```

Пример полной конфигурации с глобальными стилями и меню

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  // Глобальные стили
  customStyles: {
    global: {
      borderRadius: "8px",
    },
    components: {
      primaryButton: {
        color: {
          text: "#ffffff",
          background: "#4CAF50",
          hover: "#45a049",
        },
        position: "center",
        isHideIcon: false,
      },
      secondaryButton: {
        color: {
          text: "#4CAF50",
```

```
        background: "transparent",
        hover: "#f1f8e9",
      },
      position: "center",
      isHideIcon: false,
    },
    accountButton: {
      color: {
        text: "#333333",
        background: "#ffffff",
        hover: "#f5f5f5",
      },
      position: "left",
      isHideIcon: false,
    },
  },
},
};
```

Индивидуальная стилизация кнопок меню

Для каждой кнопки в `menuButtons` можно задать индивидуальные стили через свойство `customStyles` типа `IComponentStyles`.

Пример с индивидуальными стилями для кнопок

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  menuButtons: [
    {
      text: "Личный кабинет",
      link: "https://my-account.com",
      icon: "https://icons.com/profile.png",
      customStyles: {
        color: {
          text: "#ffffff",
          background: "#4CAF50", // Зеленый фон
          hover: "#45a049", // Темно-зеленый при наведении
        },
        borderRadius: "8px",
        padding: "8px 16px",
        position: "center",
      },
    },
    {
      text: "Настройки",
      link: "https://settings.com",
      icon: "https://icons.com/settings.png",
      customStyles: {
```

```
        color: {
          text: "#333333",
          background: "#f5f5f5", // Светло-серый фон
          hover: "#e0e0e0", // Серый при наведении
        },
        borderRadius: "6px",
        padding: "6px 12px",
        position: "left",
      },
    },
    {
      text: "Поддержка",
      link: "https://support.com",
      customStyles: {
        color: {
          text: "#ffffff",
          background: "#FF5722", // Оранжевый фон
          hover: "#E64A19", // Темно-оранжевый при наведении
        },
        borderRadius: "4px",
        padding: "10px 20px",
        position: "center",
        isHideIcon: true, // Скрыть иконку для этой кнопки
      },
    },
  ],
};
```

Приоритет применения стилей

1. **Индивидуальные стили кнопки** (`customStyles` в объекте кнопки) — высший приоритет
2. **Стили accountButton** (`customStyles.components.accountButton`) — если не заданы индивидуальные
3. **Дефолтные стили** — если не заданы предыдущие

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  // Если у кнопки НЕТ customStyles, то для menuButtons применяются стили
accountButton
  customStyles: {
    components: {
      // дефолтные стили accountButton
      accountButton: {
        color: {
          text: "#666666",
          background: "#efefef",
          hover: undefined, // если не задан применяется filter: brightness(90%)
        },
        position: "left",
      },
```

```
    },
  },
};
```

Принципы стилизации мини-виджета

Принцип	Что это значит	Где и как это применить
Централизованное управление	Все настройки внешнего вида задаются через три ключевых объекта конфигурации.	Настройте общий вид в `customStyles`, профиль — в `profile`, кнопку входа — в `loginButton`.
Гибкая настройка профиля	Внешний вид блока с именем и аватаром авторизованного пользователя настраивается отдельно.	Используйте `profile.wrapper` для фона и `profile.button` для кнопки-аватара. Учтите, что здесь работают только настройки цвета.
Настройка кнопки входа	Стили кнопки, которую видят неавторизованные пользователи, настраиваются независимо.	Задайте текст, иконку и стили в объекте `loginButton` и его свойстве `customStyles`.
Структура цветов	Цветовая схема для любого элемента описывается единообразно.	Всегда используйте вложенный объект `color` с полями `text`, `background` и `hover` (например, `color: {text: "#fff", background: "#1976d2"}`).
Управление отображением	Можно легко скрывать текстовые метки или иконки.	Используйте флаги `isHideText` (скрыть текст) и `isHideIcon` (скрыть иконку) в стилях компонента.
Гибкое выравнивание	Содержимое внутри кнопок можно выровнять по левому краю или по центру.	Задайте свойство `position: "left"` или `position: "center"` в стилях нужной кнопки.
Умное наследование	Система сама заполняет пробелы в конфигурации, используя логичные значения по умолчанию.	- Для `secondaryButton`: если стили не заданы, он унаследует `primaryButton` с добавлением прозрачности.- Для `hover`: если цвет не указан, к фону при наведении применится `filter: brightness(90%)`.
Fallback-система	Кнопки в выпадающем меню используют общие стили, если для них не заданы индивидуальные.	Если у кнопки в `menuButtons` нет своего `customStyles`, к ней автоматически применяются стили из `accountButton`.

Глобальное скругление	Единое значение скругления углов можно задать для всех элементов виджета.	Укажите `customStyles.global.borderRadius` (например, `"8px"`), и оно повлияет на кнопки и модальные окна.
Индивидуальная кастомизация	Любую кнопку в меню можно стилизовать совершенно уникально.	Добавьте объект `customStyles` для конкретного элемента в массиве `menuButtons`.

Смотрите также

- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.
- Управление организацией — руководство по работе с организацией в **КриптоАРМ IDM**.
- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как создать и настроить приложение в КриптоАРМ IDM

В этом руководстве вы узнаете, как создавать и настраивать OAuth 2.0 и OIDC приложения в **КриптоАРМ IDM**. Мы подробно разберём создание web- и native-приложений, настройку виджета входа, управление пользователями и доступом.

Содержание:

- Создание приложения
- Настройка приложения
- Управление приложением
- Полный справочник параметров приложения
- Смотрите также

Создание приложения

Создание веб-приложения OAuth

> **Веб-приложение** — это стандартное приложение, которое работает в браузере пользователя и взаимодействует с **КриптоАРМ IDM** по протоколам OAuth 2.0 и OpenID Connect.

Чтобы создать веб-приложение:

1. Перейдите в панель ID → вкладка **Приложения**.

2. Нажмите кнопку **Создать**  .
3. Откроется форма создания приложения.
4. Укажите обязательные параметры приложения:
   - **Название приложения**,
   - **Адрес приложения** в формате `протокол://доменное имя:порт`,
   - **Возвратный URL #** (`redirect_uris`) — адрес, на который пользователь переадресовывается после авторизации,
   - **URL выхода из системы #** (`post_logout_redirect_uris`) — адрес, на который переадресовывается пользователь после выхода.

     🔍 Полный справочник параметров →
5. Нажмите **Создать**.

💡 При создании формируются дополнительные поля приложения, которые можно посмотреть и отредактировать в настройках:

- **Идентификатор (client_id)** — используется для идентификации приложения;
- **Секретный ключ (client_secret)** — используется для аутентификации подлинности приложения, когда приложение запрашивает доступ к аккаунту пользователя. Секретный ключ должен быть известен только приложению.

Создание нативного OAuth-приложения

Нативное приложение — это приложение, которое разработано специально для определённой операционной системы.

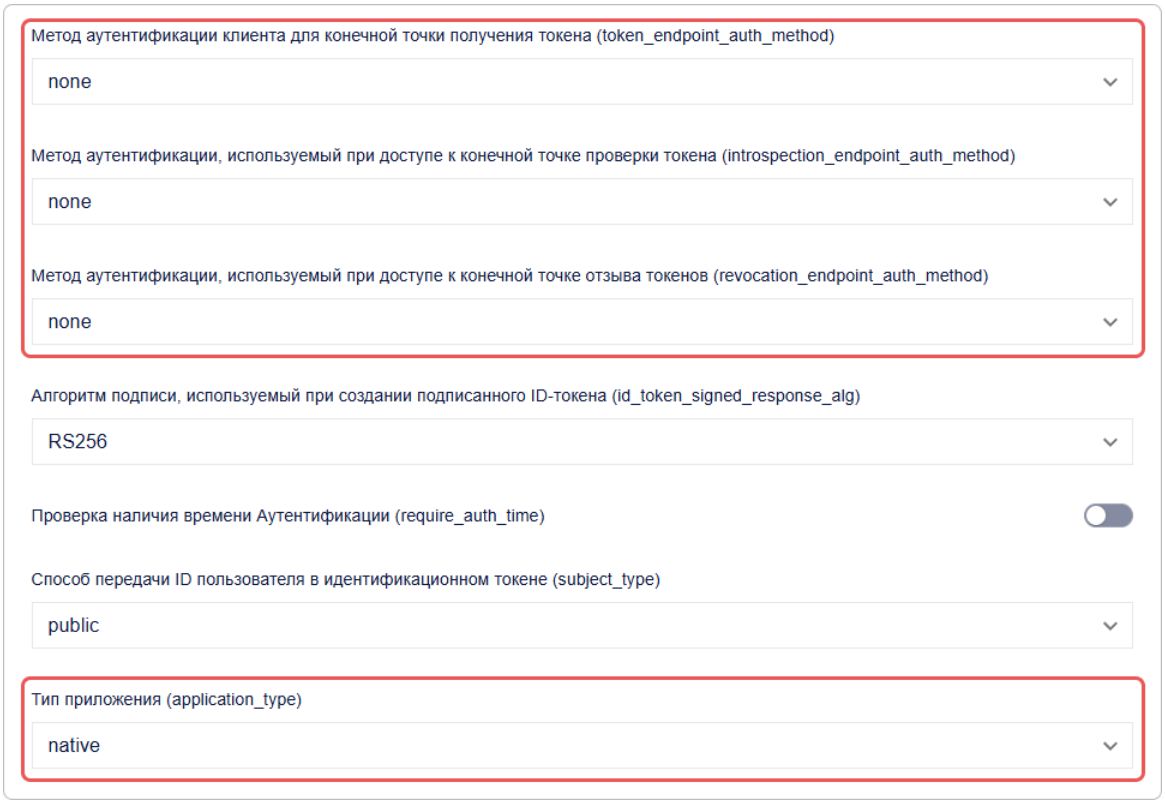
Чтобы создать нативное приложение:

1. Перейдите в панель ID → вкладка **Приложения**.
2. Нажмите кнопку **Создать**  .
3. Откроется форма создания приложения.
4. Укажите обязательные параметры приложения:
   - **Название приложения**,
   - **Адрес приложения** — локальный адрес приложения в формате `myapp://callback` (требуется для завершения создания, но **не используется** в нативных приложениях),
   - **Возвратный URL #** (`redirect_uris`) — локальный адрес, на который будет возвращён пользователь после авторизации, например, `myapp://callback`,

- **URL выхода из системы** # (`post_logout_redirect_uris`) — локальный адрес переадресации после выхода (например: myapp://logout).

  🔍 Полный справочник параметров →

5. Нажмите **Создать**.
6. Откройте созданное приложение и нажмите на **Редактировать** ⚙.
7. В открывшейся форме редактирования:
   - Выберите `native` в настройке **Тип приложения**;
   - Выберите none в настройках с методами аутентификации.



8. Сохраните изменения.

Дальше настройте авторизацию на стороне вашего приложения:

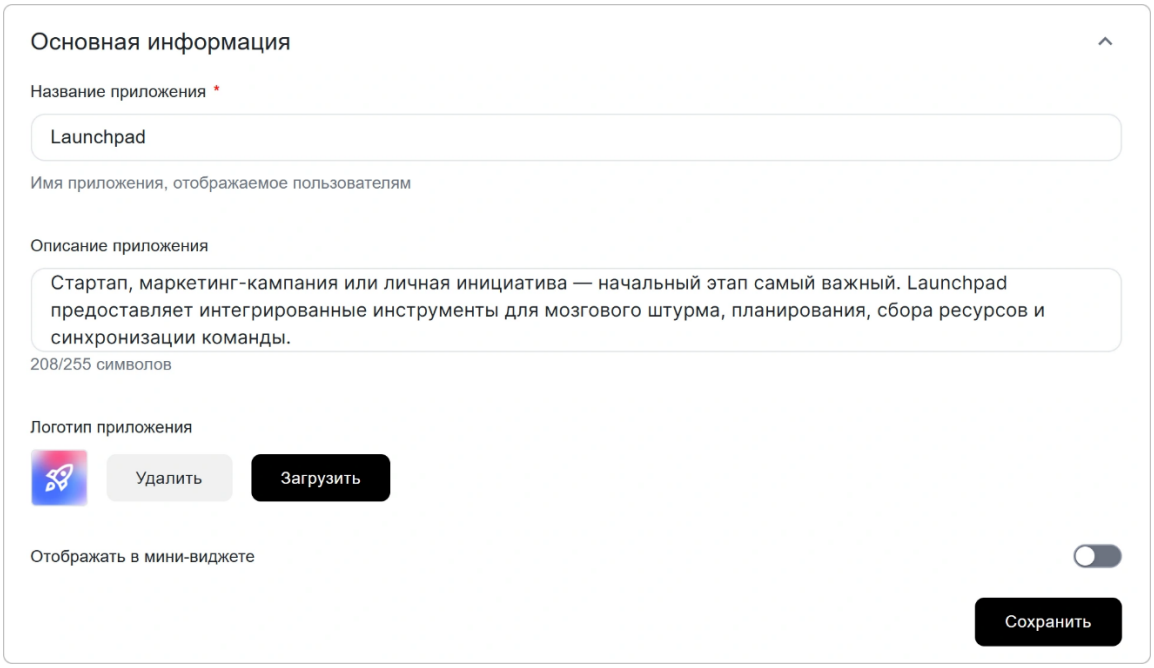
- используйте PKCE (Proof Key for Code Exchange) при запросе авторизационного кода;
- используйте ранее указанный `redirect_uri` для обработки результата авторизации;
- выполняйте обновление токена по протоколу OAuth 2.0.

Настройка приложения

После создания приложения необходимо выполнить первичную настройку, чтобы оно корректно отображалось в интерфейсе и было доступно пользователям **КриптоАРМ IDM**. На этом этапе можно задать базовые параметры приложения — описание, логотип, ключевые настройки доступа и отображение приложения в каталоге и виджете входа. Эти параметры формируют «лицо» приложения для пользователей и влияют на то, как оно будет восприниматься и использоваться в системе.

Настройка основной информации

1. Перейдите в панель ID → вкладка **Приложения**.
2. Нажмите на панель с приложением, которое необходимо отредактировать.
3. В открывшемся окне нажмите на кнопку **Редактировать** .
4. Раскройте блок **Основная информация** и укажите основные сведения о приложении:
   - **Название приложения** — отображается в интерфейсе системы и виджете входа,



   - **Описание приложения** — описание, отображаемое в интерфейсе сервиса **КриптоАРМ IDM**,
   - **Логотип приложения** — логотип в формате JPG, GIF, PNG, WEBP. Максимальный размер - 1 МБ.
   - **Отображать в мини-виджете** — если активно, добавляет приложение в мини-виджет для быстрого перехода к нему. Мини-виджет легко

интегрируется в любые веб-сайты и интерфейсы. Ознакомьтесь с инструкцией Как настроить и подключить мини-виджет →.

5. Сохраните изменения.

Настройка отображения в каталоге

🔬 **Каталог** — экспериментальная функция. Доступность регулируется администратором системы.

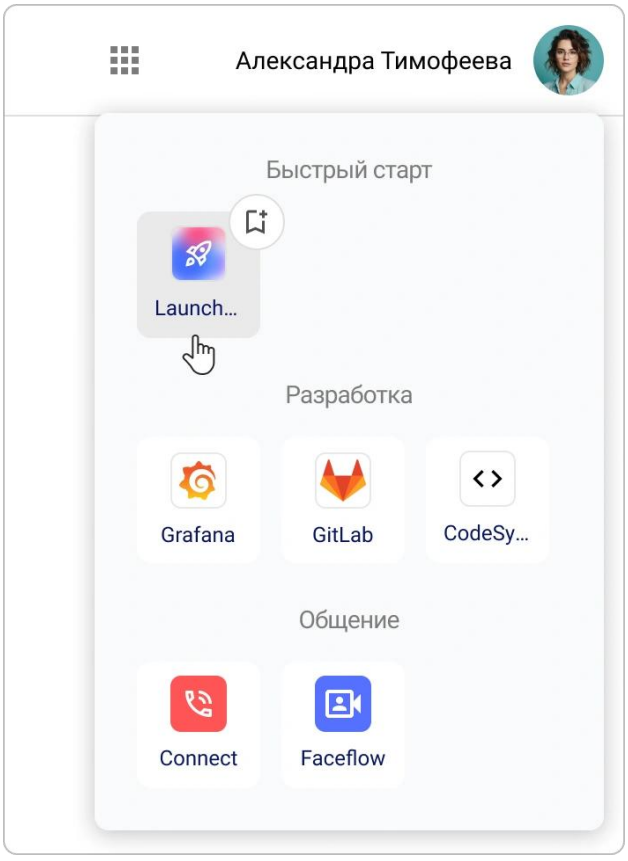
Каталог — это централизованный маркетплейс всех приложений, доступных в экосистеме **КриптоАРМ IDM**.

Каталог объединяет все публичные приложения в одном месте, что позволяет быстро находить нужные приложения, просматривать названия и описания, получать доступ к приложениям без необходимости запоминать сложные ссылки или пути.

Для удобства все приложения в каталоге разделены по типам. Они помогают организовать структуру и упростить навигацию пользователей. Типы приложений создаются и настраиваются администраторами системы.

В каталоге пользователь видит название приложения, логотип и тип приложения и может быстро перейти к приложению.

Пример отображения приложений в каталоге:



Как добавить приложение в каталог

1. Перейдите в панель ID → вкладка **Приложения**.

2. Откройте настройки приложения.
3. Раскройте блок **Каталог**.
4. Настройте параметры публикации:
   - **Тип приложения** — категория приложения в каталоге;
   - **Отображать в каталоге** — включает отображение приложения в каталоге.
5. Сохраните изменения.

После сохранения приложение станет доступно пользователям в каталоге системы **КриптоАРМ IDM**.

Правила отображения приложений в мини-виджете и каталоге

В **КриптоАРМ IDM** список приложений в мини-виджете и каталоге может включать:

- **Системные приложения** – добавляются и настраиваются администратором системы.
- **Приложения организации** – создаются и настраиваются управленцем в рамках конкретной организации.

Отображение зависит от того, где используется виджет:

- **В интерфейсе самой системы** – пользователь организации видит системные приложения и приложения своей организации (при условии, что для каждого из них включены соответствующие настройки отображения).
- **В виджете, встроенном в веб-ресурс** – действует тот же принцип: показываются как системные, так и организационные приложения.

Настройка обязательных полей профиля пользователя

Некоторым приложениям для корректной работы требуется доступ к определённым данным пользователя — например, имени, адресу электронной почты, номеру телефона или дополнительным полям профиля.

В настройках приложения можно указать список полей, которые пользователь обязан предоставить при авторизации.

Как работают обязательные поля

Если приложение запрашивает обязательные поля:

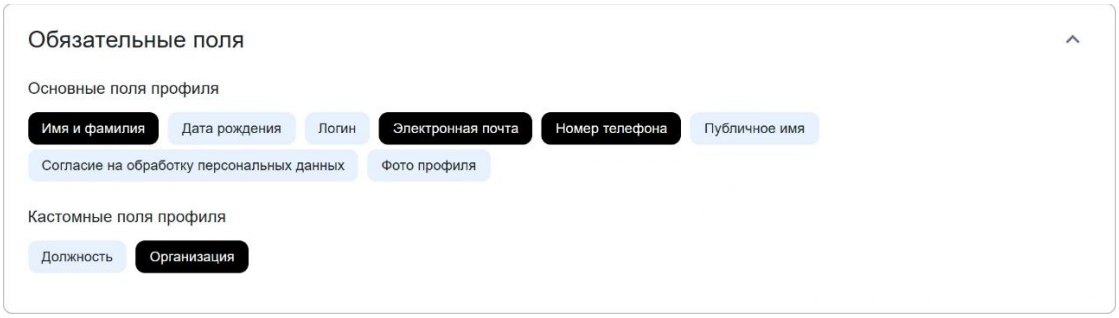
- пользователь должен заполнить отсутствующие поля перед входом в приложение;
- пользователь должен предоставить приложению доступ к этим данным.

Если нужное поле отсутствует в профиле пользователя, система предложит заполнить его во время авторизации в приложении.

Если поля присутствуют в профиле, но для них установлен уровень публичности **Доступно только вам**, пользователю будет предложено изменить этот уровень на **Доступно по запросу**, чтобы приложение смогло получить доступ к данным.

Как настроить обязательные поля

1. Перейдите в панель ID → вкладка **Приложения**.
2. Откройте настройки приложения.
3. Раскройте блок **Обязательные поля**.
4. Выберите поля, которые приложение должно получать от пользователя.



Настройка способов входа и виджета

Способ входа — это метод аутентификации пользователей, позволяющий им авторизоваться в приложениях.

В организации могут использоваться как публичные способы входа, так и способы входа, созданные для данной организации.

Вы можете:

- Использовать **публичные способы входа**, настроенные администратором **КриптоАРМ IDM**,
- Добавлять **собственные способы входа** только для вашей организации,
- Настраивать **публичность** — определять, где будут доступны ваши способы входа,
- Настраивать **обязательные** идентификаторы для пользователей.

  ⚠️ **Ограничения:** редактировать публичные способы входа могут только администраторы **КриптоАРМ IDM**.

  🔍 Подробные инструкции по созданию, редактированию и удалению способов входа приведены в основном руководстве: Настройка способов входа.

Настройка виджета входа

Виджет входа — это форма авторизации, которую видят пользователи при попытке войти именно в **это приложение**. Его настройки позволяют адаптировать внешний вид и способы входа под бренд и потребности вашего сервиса.

Чтобы открыть настройки виджета:

1. Перейдите в панель ID → вкладка **Приложения**.
2. Откройте настройки приложения.
3. Найдите блок **Способы входа** и нажмите **Настроить**.

Что можно настроить:

- **Заголовок и обложка** — адаптируйте под бренд приложения,
- **Цветовая схема** — цвета кнопок, соответствующие вашему дизайну,
- **Способы входа** — выберите, какие провайдеры показывать,
- **Информационные блоки** — добавьте правила использования или ссылки.

> 📚 **Полное руководство по всем настройкам:**
> Для детального ознакомления со всеми параметрами и возможностями кастомизации перейдите к полному руководству по настройке виджета входа →.

Настройка уведомлений пользователя

В **КриптоАРМ IDM** можно создавать уведомления, которые отображаются пользователю после авторизации в приложение.

Уведомления могут быть использованы для:

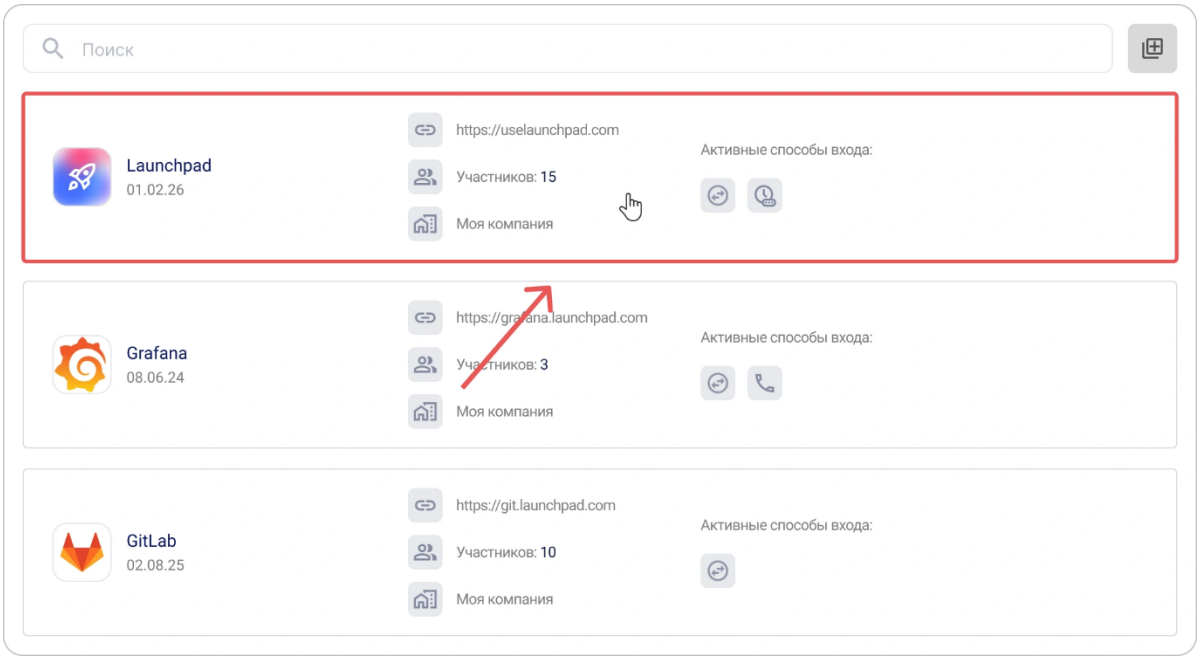
- информирования о важных изменениях;
- публикации правил или регламентов;
- отображения технических сообщений;
- уведомления о новых возможностях или обновлениях;
- обязательного ознакомления пользователей с информацией.

> 🔍 Подробная инструкция по созданию и управлению уведомлениями доступна в руководстве Как настроить уведомления пользователей.

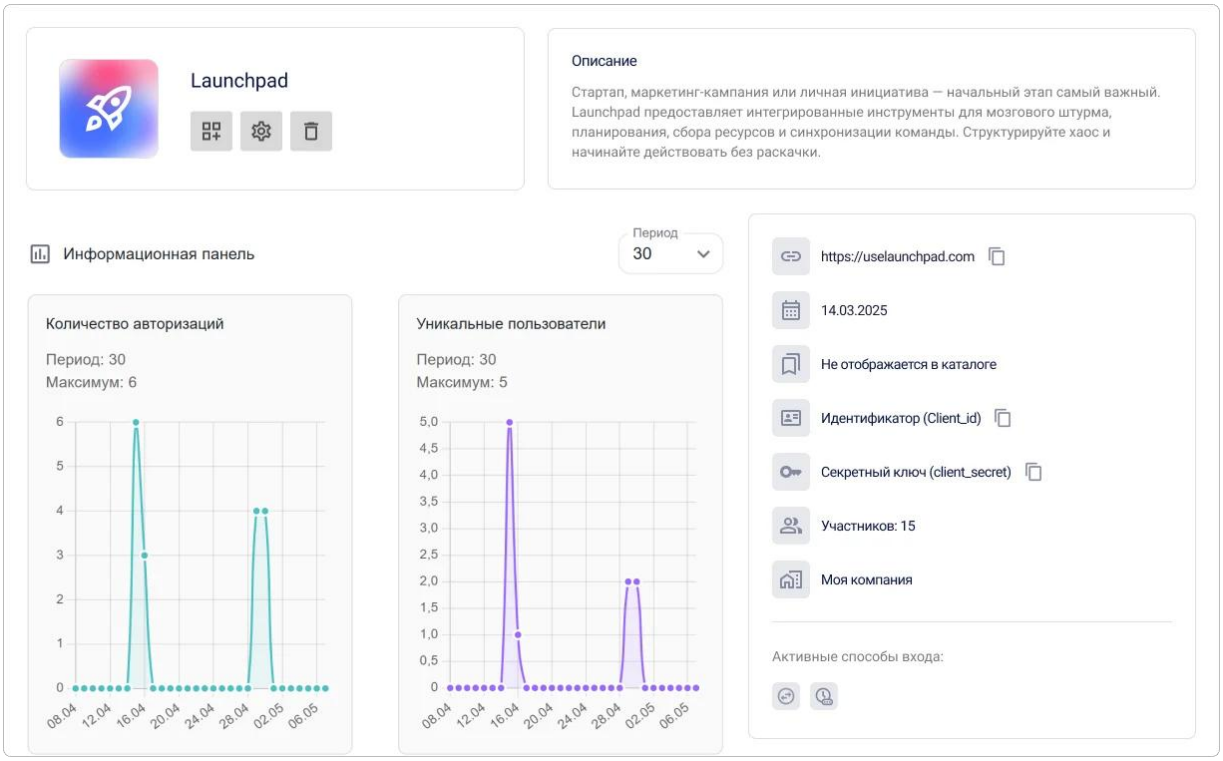
Управление приложением

Просмотр приложения

1. Перейдите в панель ID → вкладка **Приложения**.
2. Нажмите на панель с приложением, профиль которого необходимо просмотреть.



3. Откроется форма с профилем приложения.



Метрики приложения

В профиле приложения доступен блок со статистикой использования за выбранный период. Метрики помогают оценить активность пользователей и популярность способов входа.

Доступны следующие показатели:

- **Количество авторизаций** — общее число успешных входов в приложение;
- **Уникальные пользователи** — количество пользователей, которые авторизовались в приложении хотя бы один раз за выбранный период;
- **Популярность способов входа** — статистика использования различных способов входа, добавленных в виджет.

Для просмотра статистики:

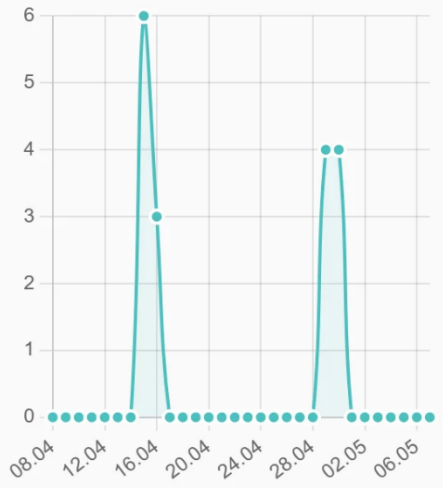
1. Перейдите в панель ID → вкладка **Приложения**.
2. Откройте настройки приложения.
3. В блоке **Информационная панель** выберите период отображения метрик.
4. Ознакомьтесь с графиками и показателями активности.

Информационная панель

Период
30

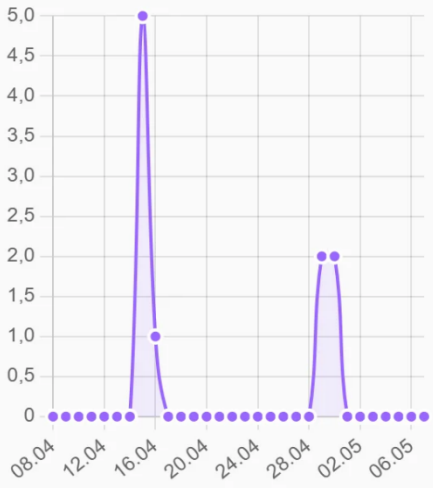
Количество авторизаций

Период: 30
Максимум: 6



Уникальные пользователи

Период: 30
Максимум: 5



Популярность способов входа

Период: 30
Всего авторизаций: 17

handleFillRequired **35,3 %**
6 / 17

session **29,4 %**
5 / 17

CREDENTIALS **23,5 %**
4 / 17

ALDPRO **5,9 %**
1 / 17

registration **5,9 %**
1 / 17

Приглашения в приложения

Механизм приглашений позволяет ограничить доступ к приложению и предоставлять его только заранее выбранным пользователям. Это удобно, если приложение предназначено для **закрытого круга пользователей**.

Включение ограничения доступа

Чтобы сделать приложение доступным только для приглашенных пользователей:

1. Перейдите в панель ID → вкладка **Приложения**.
2. Откройте настройки приложения.
3. Раскройте блок **Параметры приложения**.
4. Включите настройку **Запрет доступа для внешних пользователей**
5. Сохраните изменения.

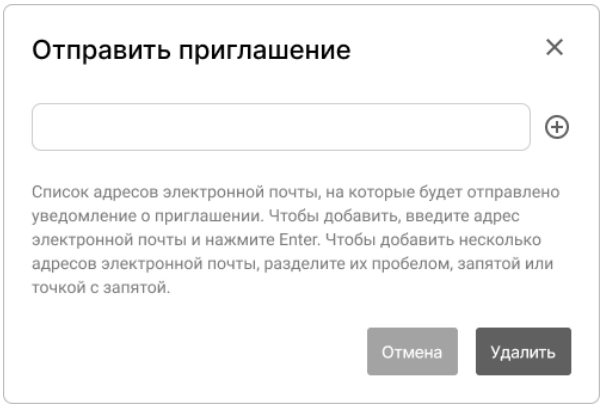
Что происходит после включения:

- Участники приложения — могут войти как обычно.
- Неприглашенные пользователи — видят сообщение об отказе в доступе.
- Новые пользователи — могут войти только после получения приглашения.

Отправка приглашений пользователям

Чтобы отправить приглашение пользователю:

1. Перейдите в панель ID → вкладка **Приложения**.
2. Откройте настройки приложения.
3. Нажмите кнопку **Пригласить**.
4. В открывшемся окне укажите email-адреса пользователей:
   - введите адрес и нажмите **Enter**, либо кнопку ⊕;
   - для добавления нескольких адресов используйте разделители: пробел, запятую `,`, точку с запятой `;`.



5. Нажмите **Отправить**.

На указанные адреса отправляется письмо с ссылкой для быстрого перехода в приложение.

> 💡 Приглашения будут активны до отмены или принятия.

Что видят пользователи

Пользователь, получивший приглашение, получает письмо с ссылкой для входа в приложение. Приглашение также отображается в разделе **Запросы** личного профиля пользователя. Принять приглашение можно двумя способами: перейдя по ссылке из письма или выбрав приглашение в разделе **Запросы**.

> 🔍 Как принять приглашение в приложение →

Приглашение защищено механизмом проверки: оно действует только для того почтового адреса, на который было отправлено. Пользователь должен войти в систему именно под этим адресом, чтобы принять приглашение. Это предотвращает передачу доступа другим лицам.

Если пользователь еще не зарегистрирован в системе, ему необходимо зарегистрироваться, указав тот же почтовый адрес, на который пришло приглашение. После успешной регистрации доступ к приложению предоставляется автоматически.

Просмотр списка отправленных приглашений

1. Перейдите в панель ID → вкладка **Приложения**.
2. Откройте профиль приложения.
3. Раскройте раздел **Список отправленных приглашений в приложение**.

Для каждого приглашения в списке отображается:

- Адрес получателя,
- Дата отправки.

Отмена приглашения

Если нужно отозвать отправленное приглашение:

1. Найдите приглашение в списке отправленных.
2. Нажмите кнопку **Удалить** на панели с приглашением.
3. Подтвердите отмену приглашения.

Последствия отмены:

- Ссылка в письме становится недействительной,
- Пользователь не сможет принять приглашение.

Пользователи приложения

Пользователи приложения (участники) — это пользователи системы **КриптоАРМ IDM**, которые предоставили вашему приложению разрешение на доступ к своим данным.

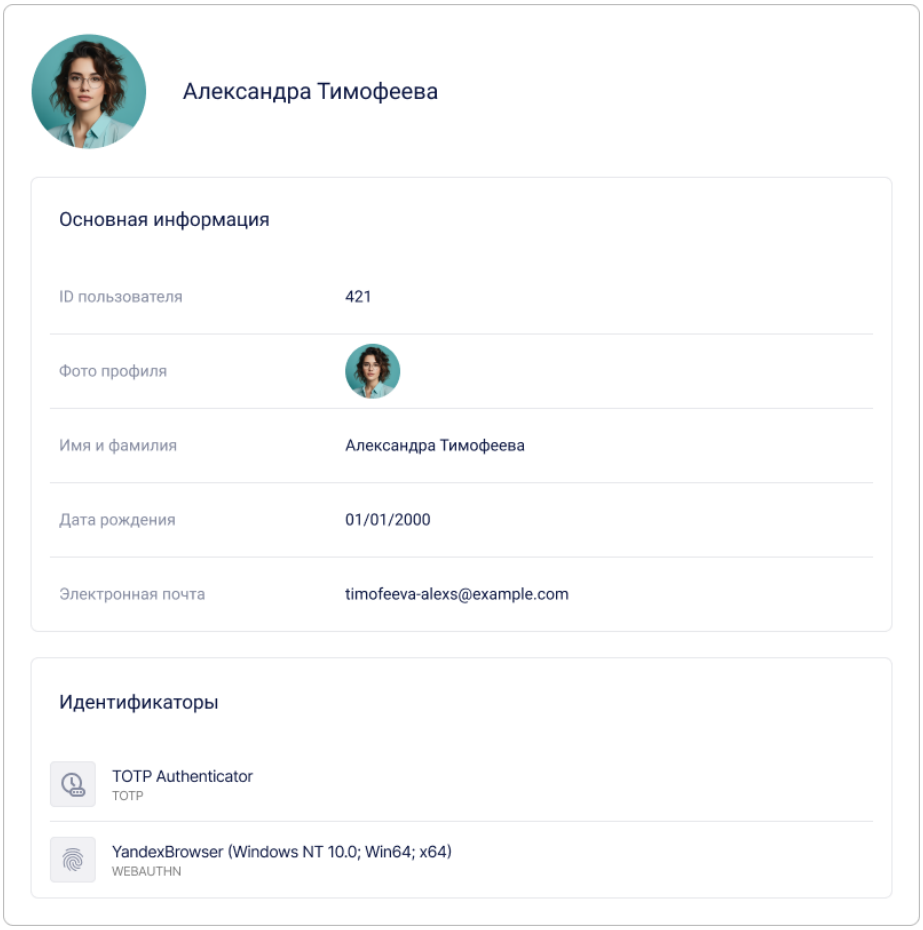
Как пользователь становится участником:

1. Пользователь впервые обращается к вашему приложению.
2. Система перенаправляет его на виджет входа **КриптоАРМ IDM**.
3. Пользователь проходит аутентификацию и **дает согласие** на доступ к запрашиваемым данным.
4. Приложение получает токен доступа, а пользователь добавляется в список участников.

> 💡 **Важно:** Управление участниками приложения происходит в рамках самого **приложения**. Действия не влияют на глобальный аккаунт пользователя в **КриптоАРМ IDM**, а только на его связь с конкретным приложением.

Просмотр участников приложения

1. Перейдите в панель ID → вкладка **Приложения**.
2. Нажмите на панель с нужным приложением.
3. Откроется профиль приложения с общей информацией.
4. В профиле приложения найдите раздел с участниками.
5. Нажмите на панель с пользователем, профиль которого необходимо просмотреть.
6. Откроется профиль пользователя, содержащий перечень данных, доступ к которым предоставил пользователь.

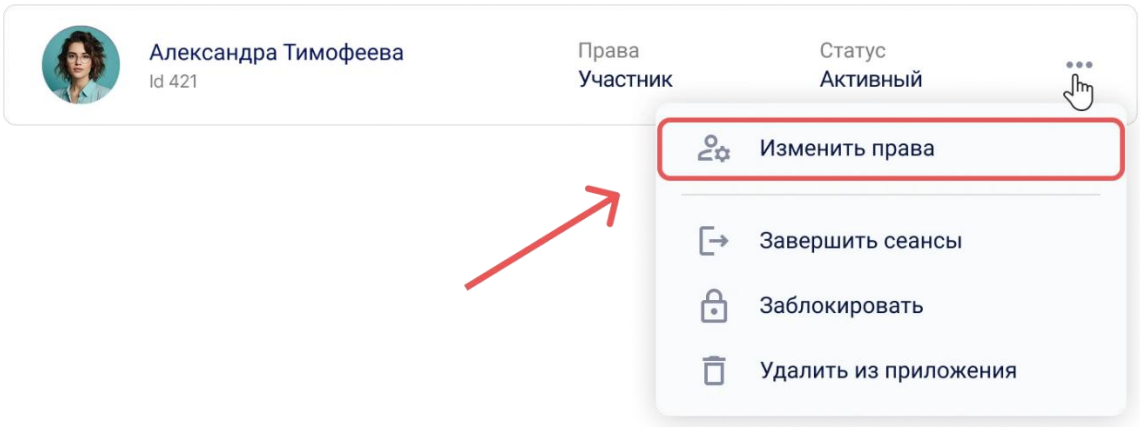


Назначение администратора приложения

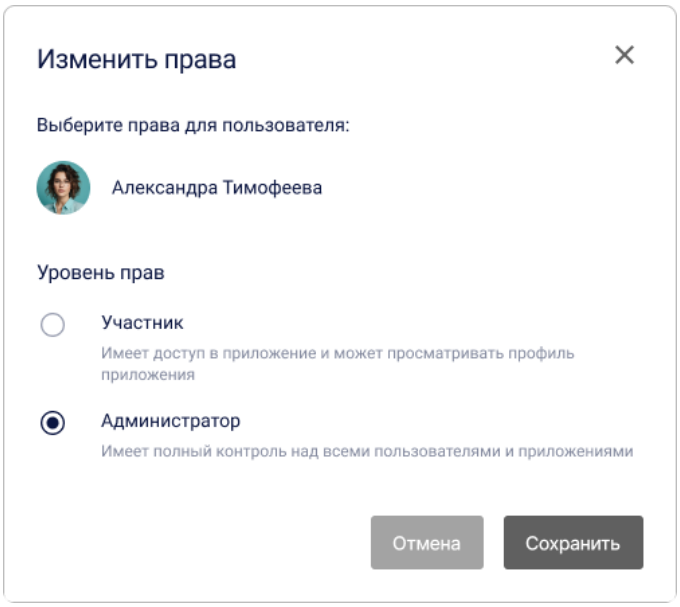
Когда это нужно: Чтобы делегировать права управления приложением доверенным пользователям. Администраторы приложения могут управлять его настройками и пользователями.

Чтобы назначить администратора приложения:

1. Перейдите в панель ID → вкладка **Приложения**.
2. Нажмите на панель с приложением.
3. Откроется профиль приложения.
4. Вызовите меню действий для пользователя, которому необходимо изменить полномочия.



5. Выберите действие **Изменить права**.
6. В появившемся окне выберите уровень полномочий **Администратор**.



7. Нажмите **Сохранить**.

После сохранения изменений полномочия пользователя в приложении будут изменены.

✅ **Что изменится:**

- Пользователь получит доступ в панель администрирования приложения,
- Сможет управлять настройками приложения и его пользователями,
- Не получит доступ к другим приложениям или настройкам организации/сервиса.

⚠️ **Безопасность:** Назначайте права администратора только доверенным пользователям. Администратор приложения может удалять других пользователей и изменять настройки интеграции.

Завершение сеансов пользователя в приложении

Когда это нужно: При подозрении на компрометацию аккаунта, утечке устройства или для принудительного обновления токенов доступа.

Чтобы завершить сеансы пользователя:

1. Перейдите в панель ID → вкладка **Приложения**.
2. Нажмите на панель с приложением.
3. Откроется профиль приложения.
4. Вызовите меню действий для пользователя, которому необходимо завершить все сеансы.
5. Выберите действие **Завершить сеансы**.
6. Подтвердите действие в модальном окне.

После подтверждения все сессии и токены для пользователя будут удалены.

✅ **Что происходит после подтверждения:**

- **Все активные сессии** пользователя в этом приложении завершаются
- **Токены доступа** (`access_token`) становятся недействительными
- **Токены обновления** (`refresh_token`) аннулируются
- Пользователю потребуется **войти заново** при следующем обращении к приложению

  📌 Эта операция не блокирует пользователя. Он сможет авторизоваться снова.

Удаление пользователя из приложения

Когда это нужно: Когда пользователю больше не нужен доступ к приложению, при увольнении сотрудника или по запросу пользователя.

Чтобы удалить пользователя из приложения:

1. Перейдите в панель ID → вкладка **Приложения**.
2. Нажмите на панель с приложением.
3. Откроется профиль приложения.
4. Вызовите меню действий для пользователя, которого необходимо удалить из приложения.
5. Выберите действие **Удалить пользователя**.
6. Подтвердите действие в модальном окне.

После подтверждения пользователь будет удален из приложения.

✅ **Что происходит после удаления:**

- Пользователь **исчезает** из списка участников приложения
- Все его **токены доступа** к этому приложению аннулируются
- При следующем обращении к приложению ему **снова покажут запрос на согласие**
- **Глобальный аккаунт** пользователя в **КриптоАРМ IDM** остается нетронутым

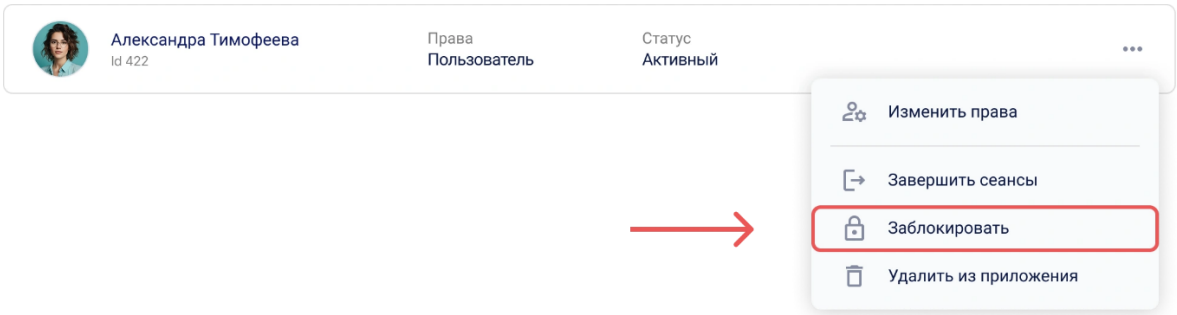
Блокировка пользователя в приложении

Когда это нужно: Для полного и постоянного запрета доступа пользователя к приложению без возможности восстановления.

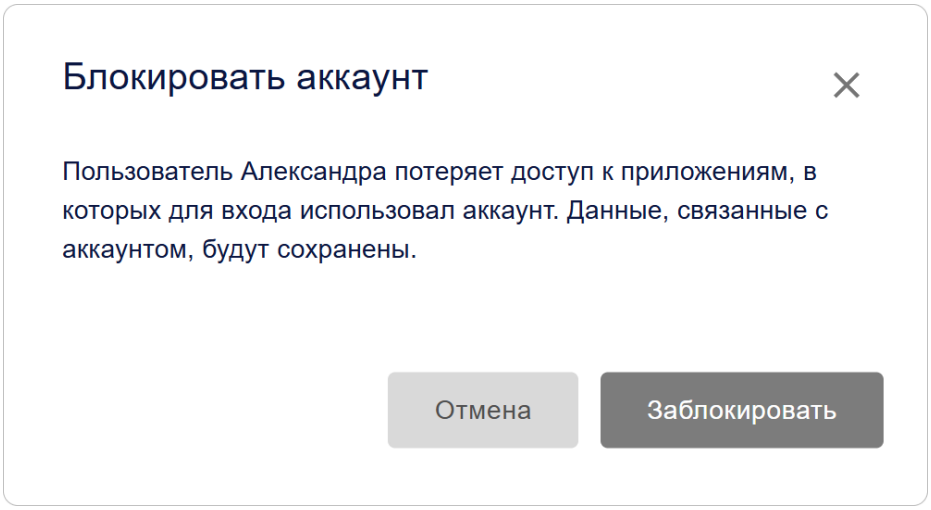
Блокировка — это более серьезное действие, чем удаление. Заблокированный пользователь не сможет получить доступ к приложению.

Чтобы заблокировать пользователя:

1. Вызовите меню действий с активным пользователем в профиле приложения.



2. Выберите действие **Блокировать в КриптоАРМ IDM**.
3. Подтвердите действие в модальном окне.



Что происходит после блокировки:

- Статус пользователя изменится на **Заблокированный**.
- Заблокированный пользователь не сможет войти в приложение.

Разблокирование пользователей КриптоАРМ IDM

Чтобы разблокировать пользователя:

1. Вызовите меню действий с заблокированным пользователем в профиле приложения.

2. Выберите действие **Разблокировать в КриптоАРМ IDM**.
3. Подтвердите действие в модальном окне.

После подтверждения действия статус пользователя изменится на **Активный**.

Удаление приложения

> ⚠️ **Внимание:** Удаление приложения — необратимая операция. Все связанные данные будут удалены из системы.

Чтобы удалить приложение:

1. Перейдите в панель ID → вкладка **Приложения**.
2. Откройте профиль приложения.
3. Нажмите на кнопку **Удалить**  .
4. Подтвердите действие в модальном окне.

После подтверждения действия приложение удалится из **КриптоАРМ IDM**.

Полный справочник параметров приложения

Основные идентификаторы

Название	Параметр	Описание	Тип	Обязательность
Идентификатор (client_id)	`client_id`	Уникальный идентификатор приложения	Текст	Генерируется автоматически
Секретный ключ (client_secret)	`client_secret`	Приватный ключ клиента. Необходимо хранить в безопасности.	Текст	Генерируется автоматически
Адрес приложения	-	URL веб-ресурса, на котором будет использоваться вход через **КриптоАРМ IDM**	Текст в формате `протокол://доменное имя:порт`	✓

Настройки доступа

Название	Параметр	Описание	Тип	По умолчанию
Ограниченный доступ	-	Если включено, вход в приложение будет доступен только для пользователей с	Переключатель (`Вкл`/`Выкл`)	`Выкл`

		правами **Администратор**		
Запрет доступа для внешних пользователей	-	Если включено, доступ к приложению будет только у участников или по приглашениям	Переключатель (Вкл/Выкл)	Выкл

Возвратный URL

Название	Параметр	Описание	Обязательность
Возвратный URL #	`redirect_uri`	URL, на который **КриптоАРМ IDM** будет перенаправлять пользователя после аутентификации. После того как пользователь аутентифицируется и даст согласие на доступ к своим данным, сервер перенаправляет пользователя обратно на **Redirect_uri** с кодом авторизации, ID токеном или другой информацией, в зависимости от запрошенного **response_type**.	✓

URL выхода из системы

Название	Параметр	Описание	Обязательность
URL выхода из системы #	`post_logout_redirect_uri`	URL, на который сервис будет перенаправлять пользователя после выхода. Если значение не указано, то используется **Возвратный URL (Redirect_uri)**	✗

URL запроса аутентификации

Название	Параметр	Описание	Обязательность
URL запроса аутентификации или восстановления после аутентификации #	`request_uris`	Список URL, где размещены JWT-запросы авторизации. Когда система отправляет запрос на авторизацию серверу, она может просто указать параметр `request_uri`, который ссылается на один из URL-адресов, определенных в этом списке. Сервер затем извлекает объект запроса JWT по этому URL для обработки запроса.	✗

Тип ответов

Название	Параметр	Описание

Тип ответов (response_types)	`response_types`	Определяет, какие токены возвращаются клиенту. • `code` — только код авторизации; • `id_token` — только ID токен; • `code id_token` — код и ID токен; • `code token` — получит код авторизации и токен доступа; • `code id_token token` — полный набор; • `none` — используется, когда не требуется получения кода авторизации, токена доступа или ID токена через перенаправление. Может быть полезным в случаях, когда необходимо подтвердить аутентификацию пользователя, но не требуется доступ к его данным.

Типы предоставления доступа

Название	Параметр	Описание
Типы предоставления доступа (grant_types)	`grant_types`	Способ получения авторизации для доступа к защищенным ресурсам. `authorization code` — стандартный и безопасный метод; - `implicit` — устаревающий вариант без серверного обмена; - `refresh_token` — обновление токена без повторного входа.

Методы аутентификации

Название	Параметр	Описание
Метод аутентификации клиента для конечной точки получения токена (token_endpoint_auth_method)	`token_endpoint_auth_method`	Метод, который клиент использует для аутентификации при обращении к `token endpoint` сервера авторизации. • `none` - не предоставляет учетные данные при обращении к `token endpoint`. Этот метод используется, когда клиент не может конфиденциально хранить учетные данные или когда аутентификация не требуется; - `client_secret_post` - отправляет свои учетные данные в теле запроса; - `client_secret_basic` - использует HTTP Basic Authentication, отправляя свои учетные данные в заголовке запроса; - `client_secret_jwt` - подписывает JWT (JSON Web Token) с использованием своего секрета и отправляет его в качестве учетных

данных; - `private_key_jwt` - подписывает JWT с использованием своего приватного ключа и отправляет его в качестве учетных данных.

Выбор метода аутентификации зависит от требований безопасности приложения и способности клиента безопасно хранить свои учетные данные. Например, методы `client_secret_jwt` и `private_key_jwt` обеспечивают более высокий уровень безопасности, так как используют асимметричное шифрование и позволяют избежать передачи секретов клиента через сеть.

Методы аутентификации

Название	Параметр	Описание
Метод аутентификации, используемый при доступе к конечной точке проверки токена (introspection_endpoint_auth_method)	`introspection_endpoint_auth_method`	Метод, который клиент использует при обращении к `introspection endpoint`. Эта конечная точка используется для проверки состояния токена доступа и получения информации о нем. – `none` - не предоставляет учетные данные при обращении к introspection endpoint; – `client_secret_post` - отправляет свои учетные данные в теле запроса; – `client_secret_basic` - использует HTTP Basic Authentication, отправляя свои учетные данные в заголовке запроса; – `client_secret_jwt` - подписывает JWT (JSON Web Token) с использованием своего секрета и отправляет его в качестве учетных данных; – `private_key_jwt` - подписывает JWT с использованием своего приватного ключа и отправляет его в качестве учетных данных. Выбор метода зависит от требований безопасности и возможностей клиента. Например, методы, использующие JWT, обеспечивают дополнительный уровень безопасности за счет использования подписанных токенов, что предотвращает необходимость передачи секретов клиента через сеть.
Метод	`introspection_`	Определяет метод аутентификации, который

аутентификации, используемый при доступе к конечной точке отзыва токенов (revocation_endpoint_auth_method)	`endpoint_auth_method`	клиент использует при обращении к `revocation endpoint`. Эта конечная точка используется для отзыва токенов доступа или обновления токенов. Этот метод обычно совпадает с методами, используемыми для `token endpoint` и `introspection endpoint`. `none` - не предоставляет учетные данные при обращении к revocation endpoint; – client_secret_post - отправляет свои учетные данные в теле запроса; – client_secret_basic - использует HTTP Basic Authentication, отправляя свои учетные данные в заголовке запроса; – client_secret_jwt - подписывает JWT (JSON Web Token) с использованием своего секрета и отправляет его в качестве учетных данных; – private_key_jwt - подписывает JWT с использованием своего приватного ключа и отправляет его в качестве учетных данных.

Алгоритм подписи ID токена

Название	Параметр	Описание
Алгоритм подписи, используемый при создании подписанного ID-токена (id_token_signed_response_alg)	`id_token_signed_response_alg`	Указывает алгоритм, который используется для подписи ID токена. **ID токен** — это JSON Web Token (JWT), который содержит утверждения (`claims`) о аутентификации пользователя

Проверка наличия времени аутентификации

Название	Параметр	Описание
Проверка наличия времени Аутентификации (require_auth_time)	`require_auth_time`	Указывает, должен ли сервер авторизации предоставить время аутентификации пользователя в ID токене. Если этот параметр включен, сервер авторизации включает в ID токен утверждение `auth_time`, которое представляет собой время, когда пользователь в последний раз выполнил

аутентификацию

Способ передачи ID пользователя

Название	Параметр	Описание
Способ передачи ID пользователя в идентификационном токене (subject_type)	`subject_type`	

Определяет способ, которым идентификатор пользователя (`sub claim`) представляется клиенту. Этот параметр влияет на то, как пользовательские идентификаторы генерируются и управляются.

- `public` - идентификатор пользователя является одинаковым для всех клиентов. Это означает, что каждый клиент будет видеть один и тот же `sub claim` для пользователя; - `pairwise` - идентификатор пользователя уникален для каждого клиента. Это обеспечивает большую конфиденциальность, так как разные клиенты не смогут связать активность пользователя между собой. `pairwise` часто используется в сценариях, где необходимо защитить приватность пользователя от различных клиентов.

Тип приложения

Название	Параметр	Описание
Тип приложения (application_type)	`application_type`	

Определяет платформу, для которой предназначено приложение:

- `web` - веб-приложение, выполняемое в браузере; - `native` - нативное приложение, установленное на устройстве.

Токен доступа

Название	Параметр	Описание
Токен доступа (access_token_ttl)	`access_token_ttl`	Время жизни `access_token` в секундах

Токен обновления

Название	Параметр	Описание
Токен обновления (refresh_token_ttl)	`refresh_token_ttl`	Время жизни `refresh_token` в секундах

Смотрите также

- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.
- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.

Как настроить шаблоны писем

В этом руководстве вы узнаете, как настроить шаблоны почтовых писем в **КриптоАРМ IDM**, включая использование переменных и настройку локализации для каждого типа уведомлений.

Содержание:

- О шаблонах
- Где используются шаблоны
- Где настраиваются шаблоны
- Использование переменных
- Как настроить шаблоны
- Смотрите также

О шаблонах

Шаблоны писем — это заготовки электронных писем, которые содержат предустановленное форматирование и элементы оформления. Они используются для автоматической отправки уведомлений (например, при регистрации, восстановлении пароля и других событиях).

С их помощью можно:

- настраивать текст и оформление писем;
- адаптировать письма под бренд организации или приложения;
- использовать разные языки (локализацию);
- подставлять динамические данные (имя пользователя, ссылки, коды и т.д.);
- управлять письмами для разных сценариев (регистрация, восстановление доступа, подтверждение и другие события).

Где используются шаблоны

Шаблоны применяются во всех автоматических почтовых уведомлениях системы **КриптоАРМ IDM**.

Каждое письмо формируется автоматически на основе выбранного шаблона.

Доступные типы писем:

Тип письма	Событие	Назначение
Регистрация	`account_create`	Приветственное письмо новому пользователю
Код подтверждения	`confirmation_code`	Письмо с кодом подтверждения
Ссылка подтверждения	`confirmation_link`	Письмо с верификационной ссылкой
Изменение пароля	`password_change`	Уведомление о смене пароля

Запрос восстановления пароля	`password_recover`	Письмо с кодом подтверждения
Приглашение	`invite`	Письмо с приглашением в приложение

Где настраиваются шаблоны

Настройка шаблонов выполняется в рамках базового провайдера **Email**.

Способ входа **Email** может быть настроен на разных уровнях: системы, организации или приложения.

Соответственно, редактирование шаблонов писем доступно:

- администратору системы — при настройке подтверждения электронной почты в профиле пользователя или в способе входа, созданном на уровне системы;
- администратору организации — в способе входа организации;
- администратору приложения — в почтовом провайдере приложения.

> 🔍 Подробнее про создание и настройку способа входа **Email** читайте в инструкции Как подключить вход по электронной почте.

Использование переменных

Для формирования динамического содержимого используется шаблонизатор **Mustache**.

> 🔗 Официальная документация Mustache

Шаблонизатор используется для:

- Подстановки данных пользователя (`{{user.name}}`),
- Динамического формирования ссылок (`{{confirmation_link}}`),
- Условного отображения блоков.

Примеры переменных:

Переменная	Описание
`{{user.name}}`	Имя пользователя
`{{user.email}}`	Адрес электронной почты пользователя
`{{confirmation_code}}`	Код подтверждения
`{{confirmation_link}}`	Ссылка подтверждения
`{{app.name}}`	Название системы / приложения / организации

> 📌 Шаблоны писем используют данные того уровня, на котором создан почтовый провайдер. Например, если провайдер создан на уровне системы — в письмах будут использоваться название и параметры системы; если на уровне

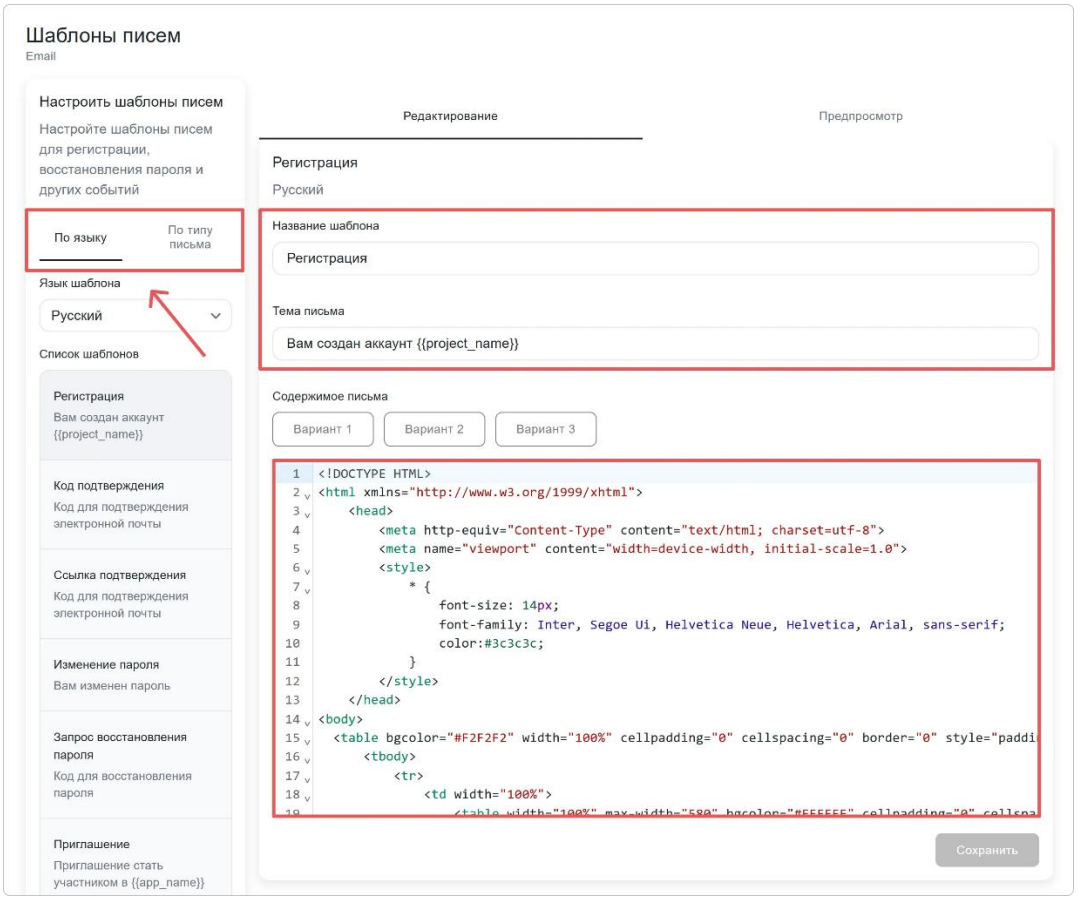
организации — данные организации; если на уровне приложения — данные конкретного приложения.

Как настроить шаблон

1. Перейдите в панель ID.
2. Откройте форму редактирования способа входа **Email**.
3. Найдите блок **Настроить шаблоны писем** и нажмите **Настроить**.
4. В открывшейся форме редактирования выберите режим отображения:
   - **по языку** — редактирование шаблонов для каждой локализации;
   - **по типу письма** — редактирование одного шаблона для всех языков.
5. На вкладке **Редактирование** настройте:
   - **Название шаблона**,
   - **Тема письма**,
   - **Содержимое письма**.

   Доступны три преднастроенных варианта оформления: светлый, тёмный и цветной.

   💡 Используйте HTML-разметку и переменные в формате `{{variable_name}}`. Убедитесь, что используемые переменные совпадают с доступными полями профиля пользователя, чтобы избежать ошибок при отправке письма.



6. На вкладке **Предпросмотр** проверьте отображение шаблона.
7. Нажмите **Сохранить**.

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.
- **Уведомления при входе — руководство по настройке уведомлений, отображаемых пользователю после аутентификации.**

Как настроить уведомления пользователей

В этом руководстве вы узнаете, как работают уведомления в **КриптоАРМ IDM**, как их создавать и редактировать, а также как управлять показом и архивированием для разных типов пользователей.

Содержание:

- Как работают уведомления

- Создание уведомления
- Редактирование уведомления
- Архивирование уведомлений
- Смотрите также

Как работают уведомления

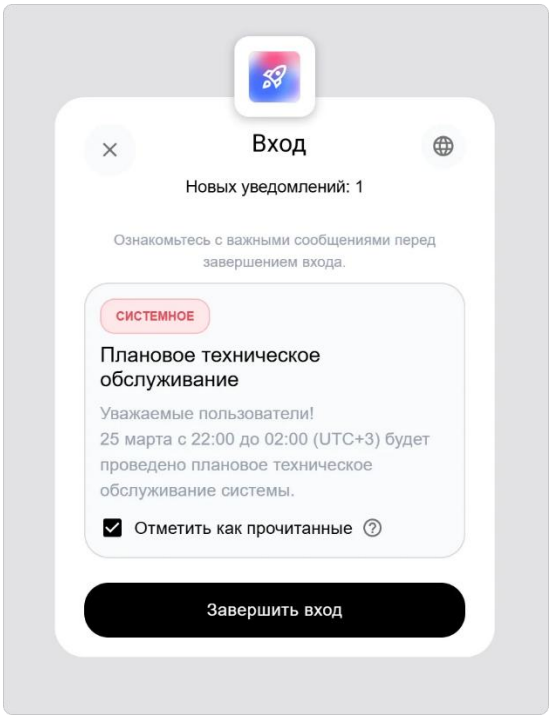
Уведомления предназначены для информирования пользователей о важных событиях, изменениях или требованиях. Поддерживаются уведомления для пользователей системы, организаций и приложений.

После аутентификации в системе, приложение организации или конкретное приложение пользователю отображается окно с уведомлением. Уведомления отображаются последовательно — по одному за раз:

- Сначала показываются **системные уведомления**,
- затем — **организационные**,
- после них — уведомления **приложения**.

Каждое уведомление помечается соответствующим лейблом.

Пример уведомления:



Пользователь может отметить уведомление как прочитанное с помощью чекбокса **Отметить как прочитанное**. После отметки уведомление больше не отображается при последующих входах. Если уведомление не отмечено, оно будет отображаться повторно при каждом входе.

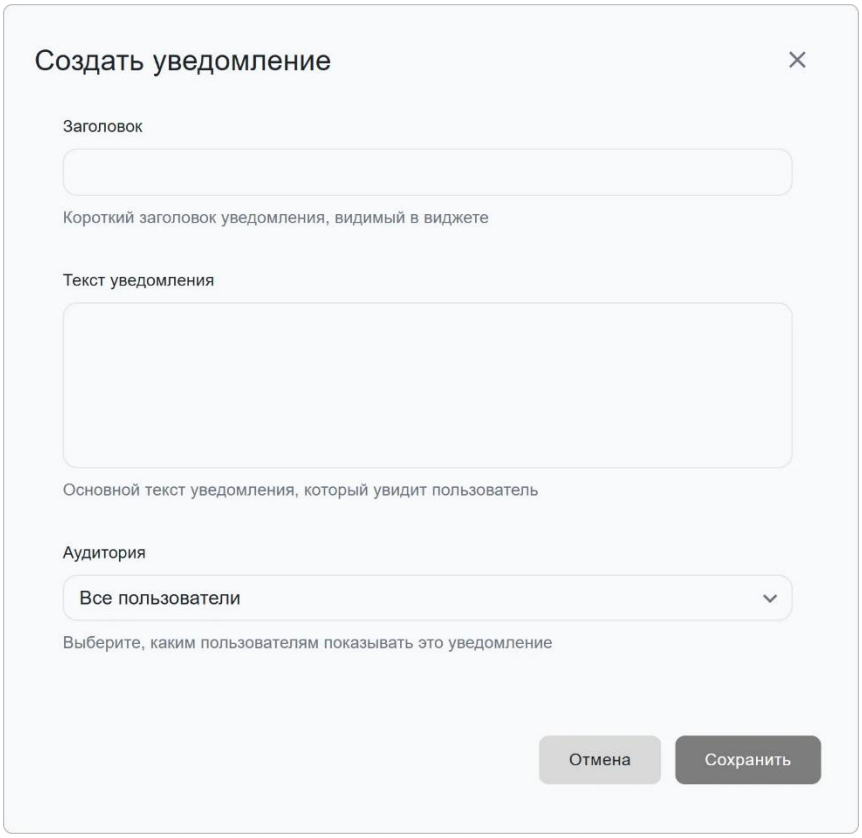
Для каждого уведомления доступна статистика прочтения, которая отображается на панели уведомления в списке уведомлений. Для каждого активного уведомления администратор может увидеть:

- количество пользователей, прочитавших уведомление;
- количество пользователей, которые ещё не прочитали уведомление.

Эти данные помогают оценить охват и эффективность уведомления.

Создание уведомления

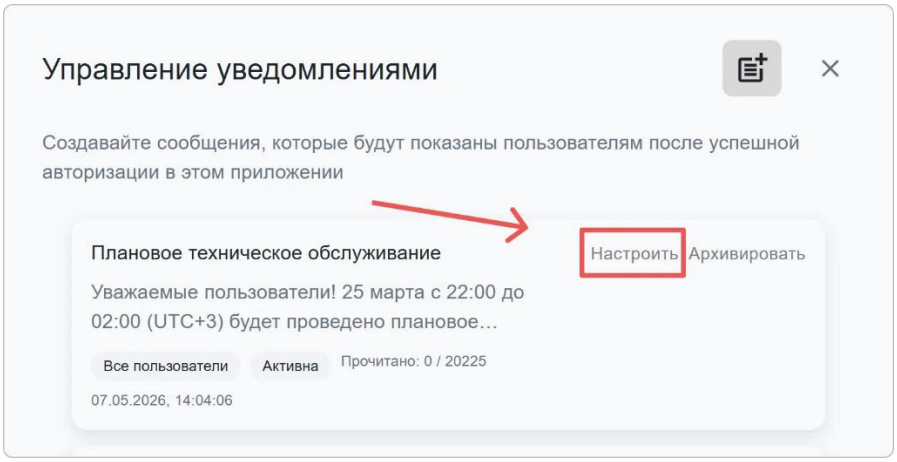
1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Уведомления** и нажмите **Настроить**.
3. В открывшемся окне нажмите **Создать**  .
4. Укажите параметры уведомления:
   - **Заголовок** — короткий заголовок, видимый в виджете;
   - **Текст уведомления** — основной текст, который увидит пользователь;
   - **Аудитория** — пользователи, которым будет показано уведомление:
     - **Все пользователи** — уведомление отображается всем пользователям;
     - **Новые пользователи** — только новым пользователям после регистрации;
     - **Существующие пользователи** — всем пользователям, кроме новых;
     - **Список пользователей** — выбор конкретных пользователей.



5. Нажмите **Создать**.

Редактирование уведомления

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Уведомления** и нажмите **Настроить**.



3. На панели нужного уведомления нажмите **Настроить**.
4. Внесите изменения и сохраните их.

⚠️ Изменение уведомления не сбрасывает статус «прочитано» для пользователей, которые уже отметили его.

Архивирование уведомлений

Архивирование позволяет убрать уведомление из активного показа без полного удаления. Архивированное уведомление больше не показывается пользователям и не учитывается в текущей статистике, но сохраняется в истории.

После архивирования уведомление:

- перестает отображаться пользователям;
- сохраняется в архиве;
- остается доступным для просмотра администраторам.

Как архивировать уведомление

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Уведомления** и нажмите **Настроить**.
3. На панели нужного уведомления нажмите **Архивировать**.
4. Подтвердите действие в модальном окне.

После подтверждения уведомление будет помечено как неактивное.

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление приложениями — руководство по созданию, настройке и управлению OAuth 2.0 и OpenID Connect (OIDC) приложениями.
- **Шаблоны писем — руководство по настройке шаблонов почтовых писем.**

Как управлять личным профилем КриптоАРМ IDM

Профиль в КриптоАРМ IDM — ваш центр управления данными и безопасностью аккаунта.

В этом руководстве вы узнаете, как управлять личным профилем в **КриптоАРМ IDM**: редактировать данные и настройки приватности, обновлять пароль, контролировать доступ приложений, просматривать журнал активности и экспортировать данные профиля.

Содержание:

- Управление личным профилем
- Разрешения приложений и OAuth-доступ
- Приглашения в закрытые приложения

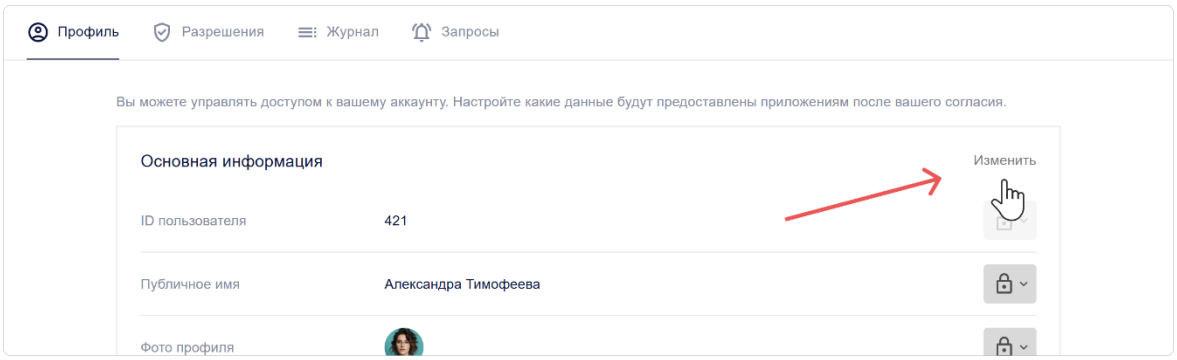
- Каталог приложений
- Журнал активности и история входов
- Смотрите также

Управление личным профилем

Ваш профиль содержит основную информацию для идентификации в системе. В зависимости от способа регистрации некоторые поля могут быть недоступны для редактирования. Если вам нужно их отредактировать, свяжитесь с администратором сервиса.

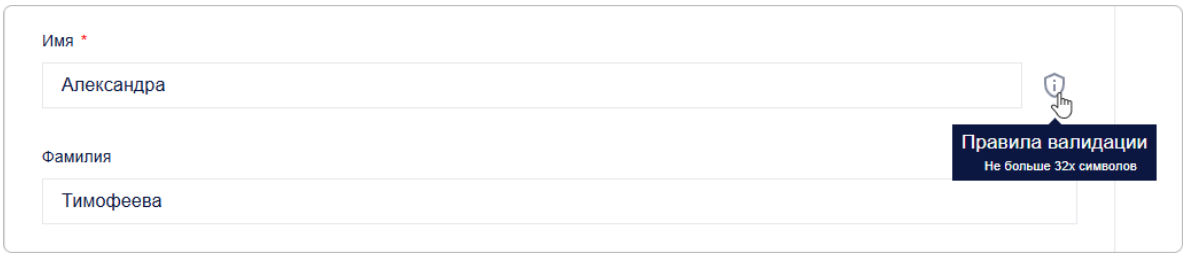
Изменение персональной информации

1. Перейдите в свой **Профиль**.
2. Нажмите **Изменить** в блоке **Основная информация**.



3. Внесите необходимые изменения в открывшейся форме.

   Для некоторых полей установлены правила валидации. Будьте внимательны при внесении изменений.



4. Нажмите **Сохранить**.

   📌 **Важно:** Профиль можно сохранить даже с незаполненными обязательными полями. При следующем входе система запросит недостающие данные.

Добавление фото профиля

Вы можете загрузить фото с устройства или использовать аватар из привязанных внешних сервисов.

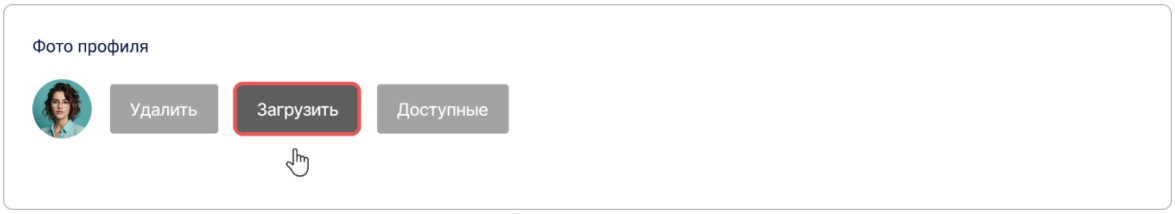
1. Перейдите в свой **Профиль**.

2. Нажмите **Изменить** в блоке **Основная информация**.

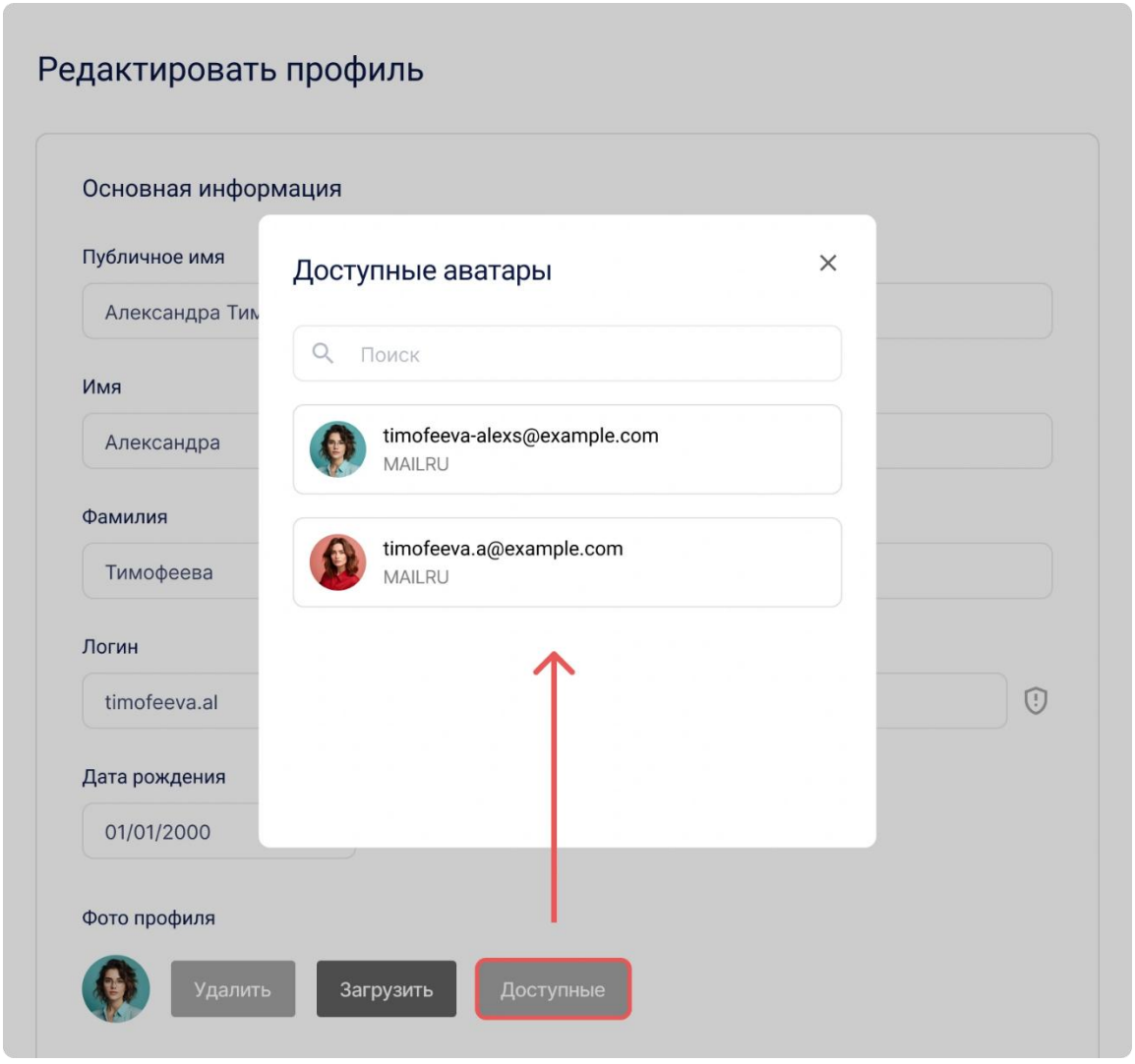
3. Откроется форма редактирования.

4. Добавьте фото одним из способов:

   – Нажмите кнопку **Загрузить** и укажите путь к файлу с фото,



   – Нажмите кнопку **Доступные** и выберите фото из внешней системы.



📌 Если в профиле нет привязанных идентификаторов внешних систем с фото, то кнопка **Доступные** будет скрыта.

💡 **Совет**: Чтобы удалить фото, нажмите на кнопку **Удалить** в блоке **Фото профиля**.

5. Нажмите **Сохранить** в форме редактирования.

Управление контактными данными

В профиле пользователя **КриптоАРМ IDM** можно добавить несколько номеров телефонов и адресов электронной почты.

Один из контактов можно назначить **основным (контактным)**. Такой контакт может быть использован:

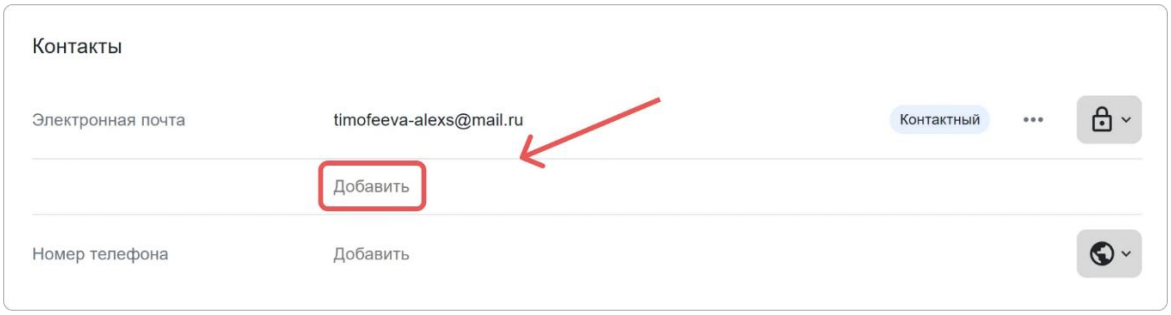
- для входа в систему;
- для получения уведомлений;
- для передачи приложениям при запросе доступа к данным.

Добавление нового адреса

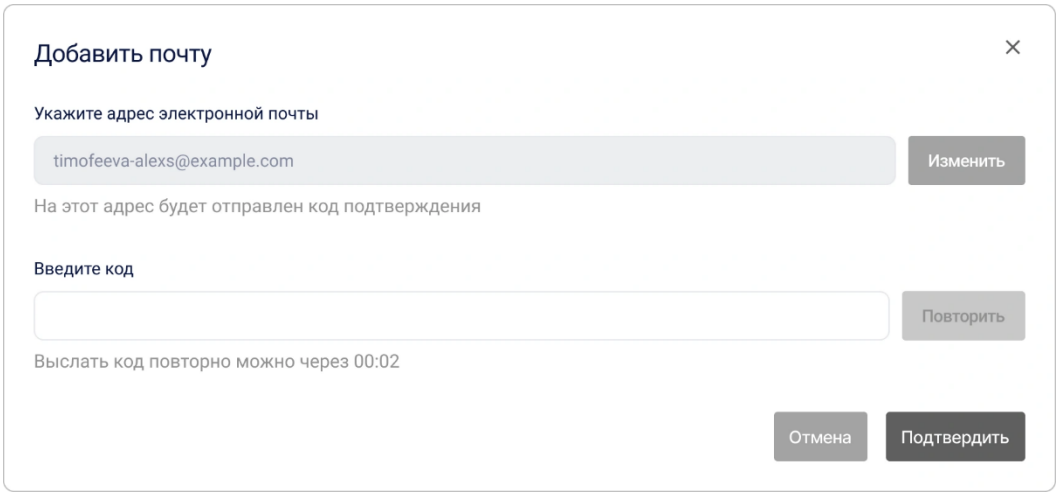
💡 Для электронной почты требуется подтверждение — ввод одноразового кода или переход по ссылке из письма.

1. Перейдите в свой **Профиль**.

2. Найдите блок **Контакты** и нажмите **Добавить** на панели **Электронная почта**.



3. Откроется форма добавления.



4. Введите почту и нажмите **Получить код**.

   На указанный адрес будет направлено письмо с кодом подтверждения.

5. Введите код и нажмите **Подтвердить**, либо перейдите по ссылке из письма.

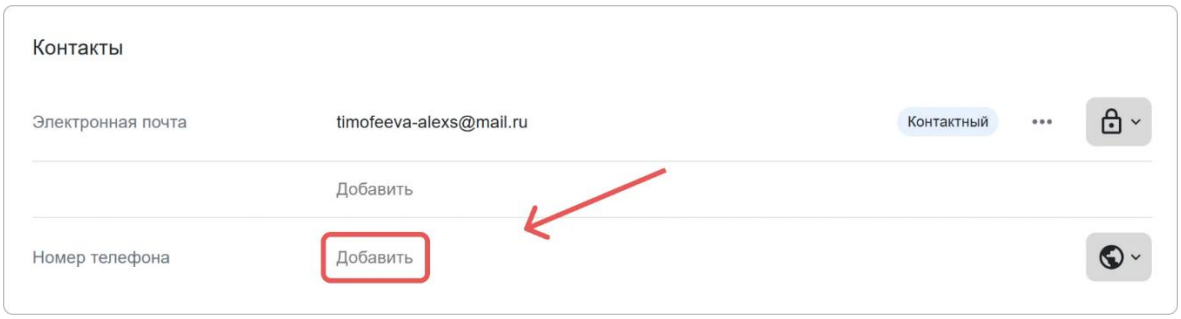
После подтверждения адрес появится в списке доступных адресов электронной почты.

> 💡 **Совет**: Чтобы удалить почту, нажмите на кнопку **Удалить** на панели **Электронная почта**.

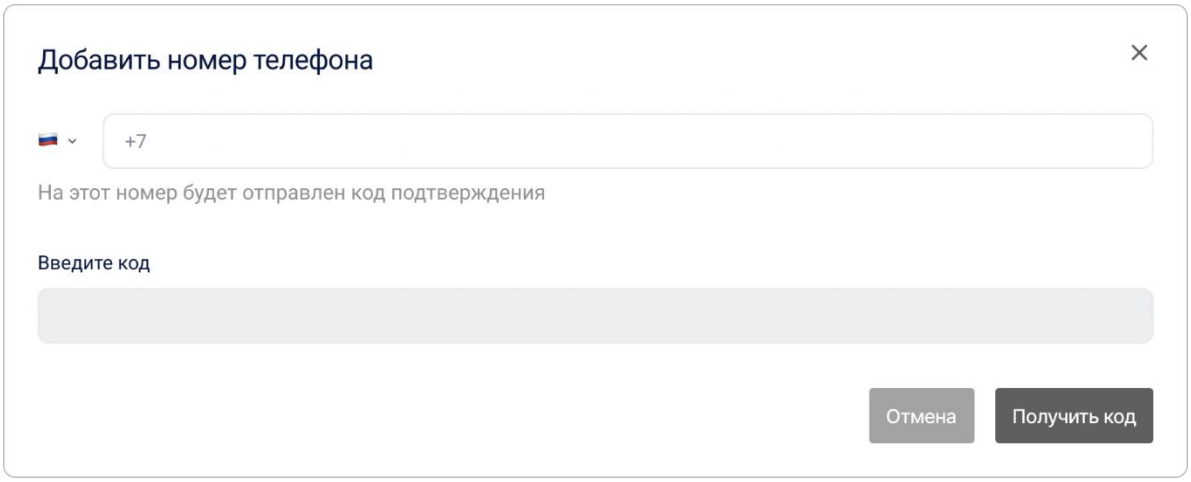
Добавление номера телефона

> 💡 Для номера телефона требуется подтверждение - ввод одноразового кода из SMS или входящего звонка.

1. Перейдите в свой **Профиль**.
2. Найдите блок **Контакты** и нажмите **Добавить** на панели **Номер телефона**.



3. Откроется форма редактирования.



4. Введите номер и нажмите **Получить код**.

   На указанный номер будет направлено SMS или звонок.

5. Введите код подтверждения и нажмите **Подтвердить**.

   💡 **Совет**: Чтобы удалить телефон, нажмите на кнопку **Удалить** на панели **Номер телефона**.

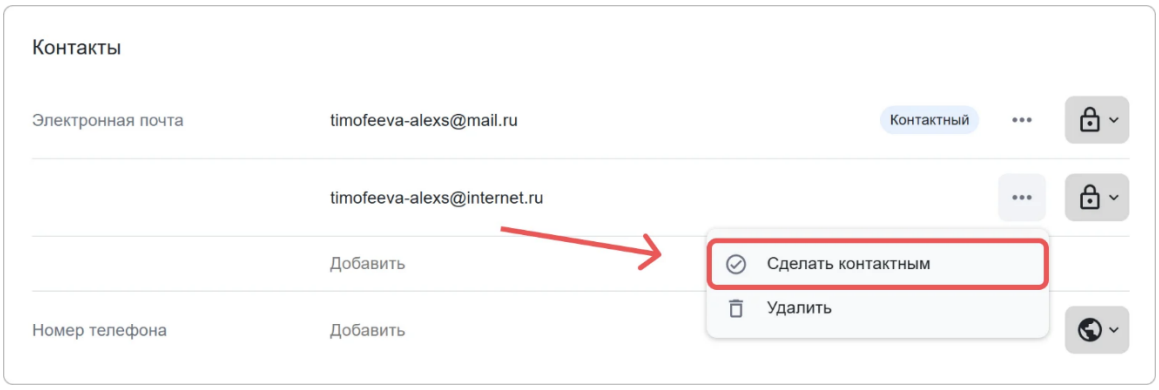
Назначение контактного способа связи

Чтобы назначить контактный способ связи (почтовый адрес или номер телефона):

1. Перейдите в свой **Профиль**.

2. Найдите блок **Контакты** и откройте меню действий для нужного контакта.

3. Выберите действие **Сделать контактным**.



4. После этого выбранный адрес станет основным контактным адресом профиля.

   📌 Только один адрес электронной почты и номер телефона могут быть контактными одновременно.

Подтверждение контактного способа связи

Некоторые контактные данные могут быть добавлены в профиль автоматически — например, администратором системы.

Если контакт еще не подтвержден, рядом с ним отображается соответствующий статус. До подтверждения такой контакт нельзя использовать для входа, получения уведомлений и восстановления доступа к аккаунту.

Чтобы подтвердить контакт:

1. Перейдите в свой **Профиль**.

2. В блоке **Контакты** найдите неподтвержденный контакт.

3. Нажмите **Подтвердить**.

4. Завершите подтверждение:

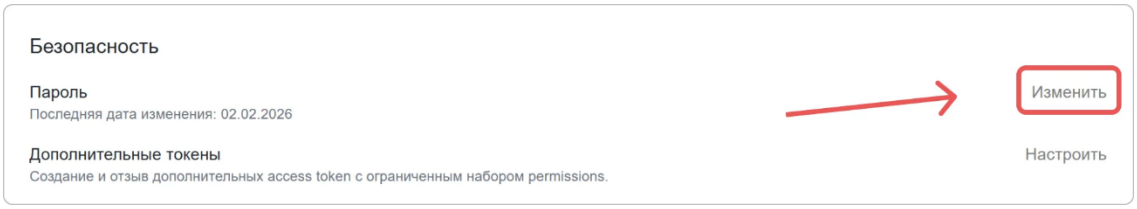
   - для почтового адреса — через код или ссылку из письма;
   - для телефона — через SMS-код или входящий звонок.

После успешного подтверждения статус контакта обновится автоматически.

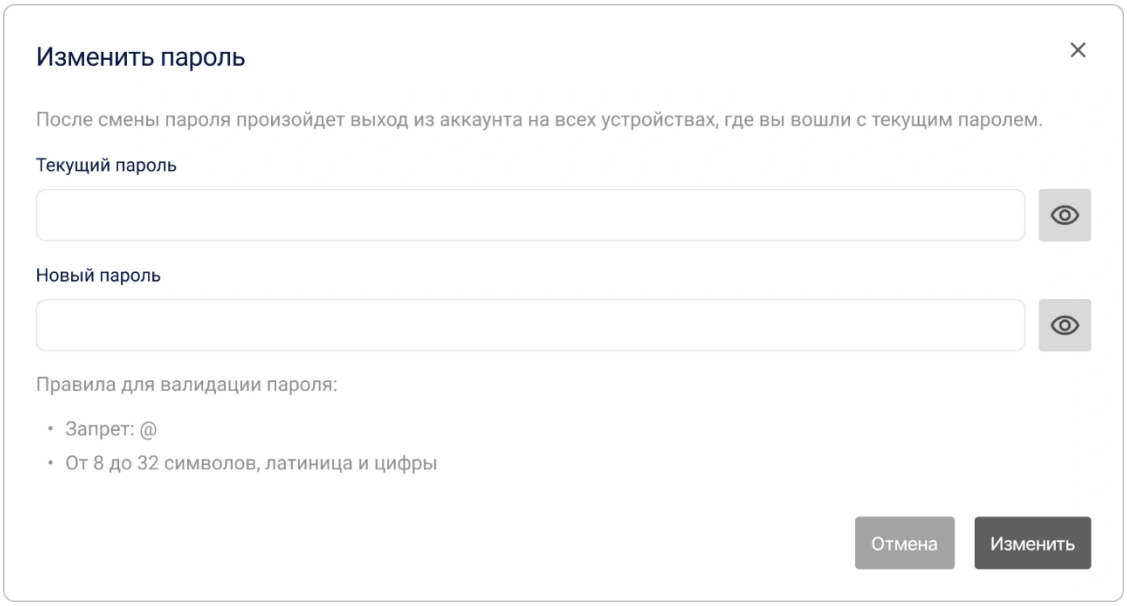
Смена пароля

1. Перейдите в свой **Профиль**.

2. Нажмите **Изменить** в блоке **Безопасность**.



3. В открывшемся окне укажите текущий пароль и новый пароль.



После смены пароля произойдет выход из системы. Для продолжения работы необходимо заново авторизоваться, используя новый пароль.

Токены доступа

В **КриптоАРМ IDM** пользователи могут создавать токены доступа — специальные ключи, которые позволяют выполнять действия через API от имени пользователя.

Токены удобно использовать для:

- интеграций с внешними сервисами;
- автоматизации действий (скрипты, API-запросы);
- предоставления ограниченного доступа без передачи учетных данных пользователя.

Каждый токен имеет:

- собственный срок действия;
- набор разрешений (scope), определяющий доступные операции.

  💡 Токен предоставляет доступ только к тем действиям, которые разрешены при его создании.

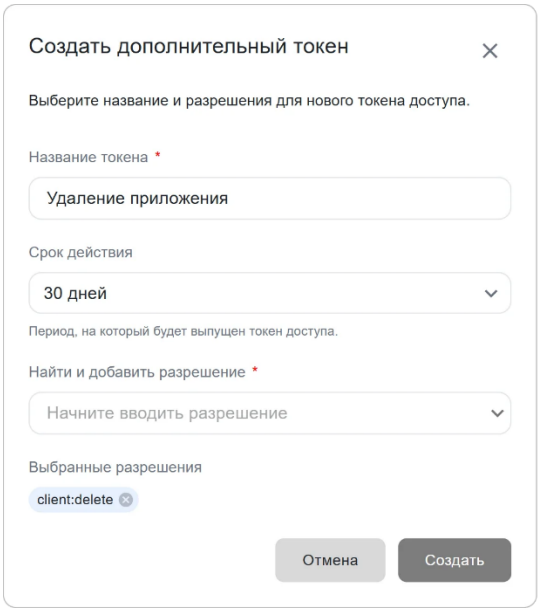
Создавать токены могут:

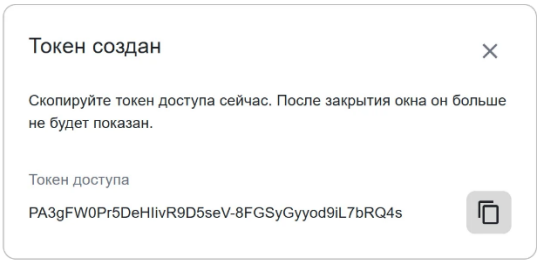
- сам пользователь — для своего аккаунта;
- администратор — для пользователя.

Создание токена доступа

1. Перейдите в свой **Профиль**.
2. Откройте блок **Безопасность** → **Дополнительные токены** и нажмите **Настроить**.
3. В открывшемся окне нажмите **Создать дополнительный токен** +.

4. Укажите параметры токена:
   - **Название токена** — произвольное имя для удобства идентификации;
   - **Срок действия** — период, в течение которого токен будет действителен (1 час, 1 день, 7 дней, 30 дней);
   - **Разрешения** — выберите одно или несколько разрешений из списка.



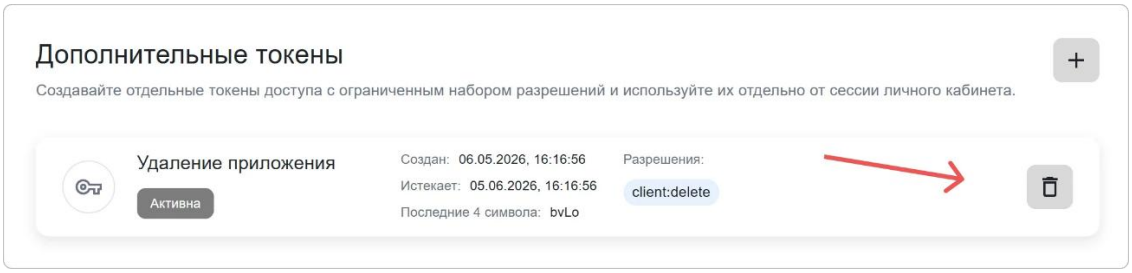


5. Нажмите **Создать**.
6. Скопируйте значение токена в открывшемся окне. Значение токена отображается только один раз. После закрытия окна его нельзя будет посмотреть повторно.

   💡 Рекомендуется хранить токен в безопасном месте и не передавать его третьим лицам

Отзыв (удаление) токена доступа

1. Перейдите в свой **Профиль**.
2. Откройте блок **Безопасность** → **Дополнительные токены** и нажмите **Настроить**.
3. Нажмите **Отозвать токен** на панели с токеном.



4. Подтвердите действие.

После отзыва токен становится недействительным и не может быть использован повторно.

Настройка публичности

Вы можете самостоятельно контролировать, какая информация будет доступна другим пользователям или сторонним системам. Это осуществляется через настройку публичности поля.

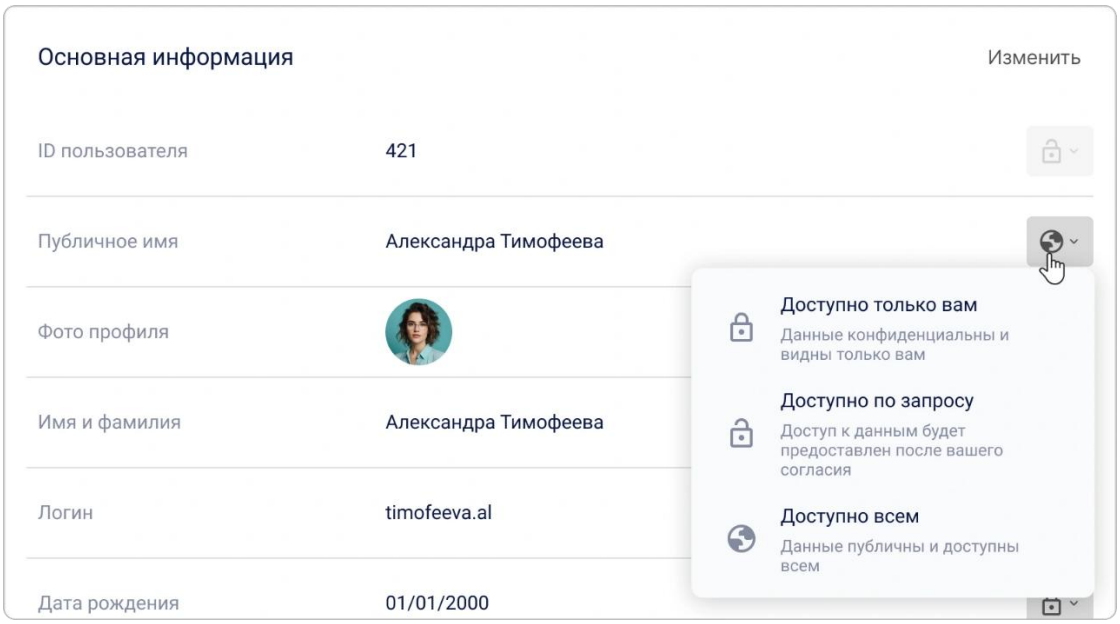
Эта настройка позволяет определять публичность для каждого поля в блоках **Основная информация**, **Дополнительная информация** и **Идентификаторы**.

Уровни публичности

Уровень	Иконка	Описание
Доступно только вам		Данные не передаются в сторонние системы и доступны только вам.
Доступно по запросу		Данные доступны в сторонних системах, с которыми настроена интеграция КриптоАРМ IDM. Для доступа к данным требуется ваше согласие.
Доступно всем		Данные публичны всегда. Для доступа к ним не требуется вашего согласия.

Как настроить публичность поля

1. Перейдите в свой **Профиль**.
2. Нажмите на кнопку для настройки публичности рядом с полем.
3. Выберите необходимый уровень.



В зависимости от выбранного значения значение поля в профиле становится публичным или приватным.

Настройка применяется без дополнительного подтверждения.

Управление идентификаторами внешних сервисов

Идентификаторы — внешние сервисы, которые вы добавили в свой профиль или через которые вы когда-либо входили в приложения или систему **КриптоАРМ IDM**.

Список доступных для добавления идентификаторов в профиле формируется из публичных способов входа, созданных в **КриптоАРМ IDM**.

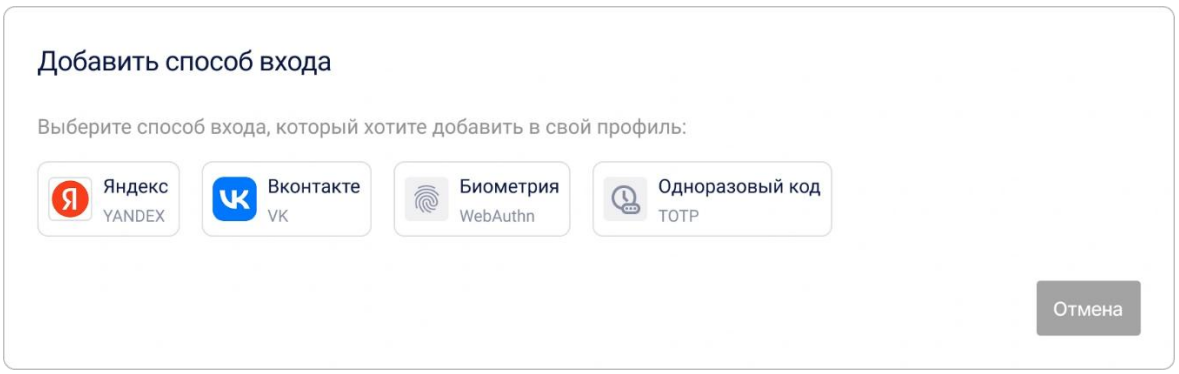
> 🔍 Доступные для привязки идентификаторы настраиваются в панели администратора.
>
> 💡 Вы можете входить в приложения, используя идентификаторы, при условии, что они добавлены на виджет входа.

Добавление нового идентификатора

1. Перейдите в свой **Профиль**.

2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите внешний сервис.



4. Пройдите аутентификацию в сервисе.

   После успешного входа в аккаунт внешнего сервиса, идентификатор будет привязан в профиле.

   > 💡 **Совет**: Если идентификатор внешнего сервиса уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Удаление идентификатора

1. Перейдите в свой **Профиль**.

2. Нажмите для идентификатора, который необходимо удалить.

3. Выберите действие **Удалить**.

Идентификатор будет **немедленно удален** из профиля.

Настройка публичного профиля

Публичный профиль — публичные данные, доступные для просмотра другим участникам системы **КриптоАРМ IDM** и подключенным приложениям. Он позволяет контролировать, какая информация о пользователе видна другим без необходимости предоставления полного доступа к аккаунту.

Просмотр публичного профиля

1. Перейдите в свой **Профиль**.
2. Нажмите на кнопку **Публичные данные** в блоке **Приватность профиля**.
3. Откроется окно с публичным профилем, который содержит данные с уровнем **Доступно всем**.

Скачивание данных публичного профиля

📌 Данные публичного профиля экспортируются в файл формата **vCard**.

1. Перейдите в свой **Профиль**.
2. Нажмите на кнопку **Публичные данные** в блоке **Приватность профиля**.
3. Откроется окно **Публичный профиль** с данными, для которых установлен уровень **Доступно всем**.
4. Нажмите кнопку **Экспортировать vCard** .
5. Запустится загрузка файла.

Пример файла **vCard** с публичными данными профиля:

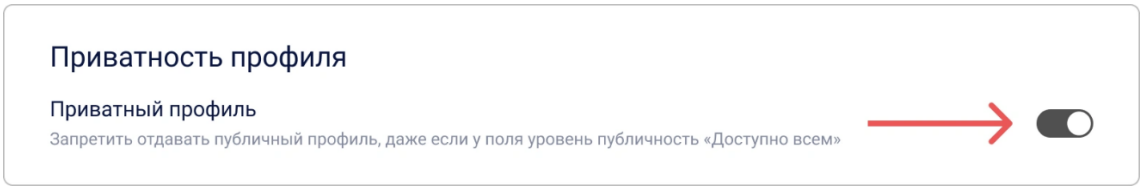
```
BEGIN:VCARD
VERSION:3.0
FN:Timofeeva Alex
N:Timofeeva;Alex;;;
PHOTO:https://service-
adress/public/images/profile/90211313d753e1d1b83ab19ecfd4af5e
EMAIL:timofeeva-alexs@mail.ru
UID:null
REV:2025-05-26T12:52:24.630Z
END:VCARD
```

Отключение публичного профиля

> 💡 **Совет**: Вы можете запретить передачу публичных данных профиля, которые имеют уровень публичности «Доступно всем».

1. Перейдите в свой **Профиль**.

2. Активируйте переключатель **Приватный профиль** в блоке **Приватность профиля**.



Настройка применяется без дополнительного подтверждения.

После активации настройки данные с уровнем публичности «Доступно всем» стают доступны только по запросу.

Цифровая визитка личного профиля

> 🔬 **Экспериментальная функция**: Доступность регулируется администратором системы.

Визитка в КриптоАРМ IDM — это современная цифровая замена бумажной визитке, доступная по уникальной ссылке.

Содержимое визитки:

- Фотография профиля,
- Имя и фамилия,
- Контактные данные (email, телефон),
- Дата рождения.

Особенности:

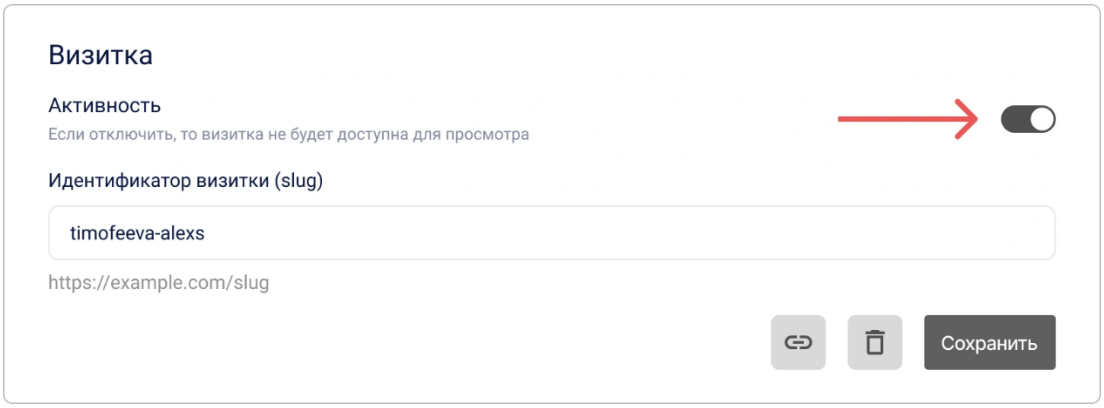
- Данные отображаются независимо от настроек их публичности.
- Визитка доступна по уникальной ссылке: `https://<ваш-сервис>/api/cards/<идентификатор>`.
- Поддерживается экспорт визитки в формате **vCard** для интеграции в различные приложения.

Активность визитки

Для визитки доступна настройка активности.

1. Перейдите в свой **Профиль**.

2. В блоке **Визитка** активируйте переключатель **Активность**.



Убедитесь, что теперь ваша визитка доступна. Для этого перейдите по ссылке: `https://<your-domain>/api/cards/<идентификатор>`:

Настройка персонализированного адреса ссылки

Чтобы ссылка на визитку была короче и легко запоминалась, можно задать собственный уникальный идентификатор.

1. Перейдите в свой **Профиль**.
2. В блоке **Визитка** укажите новый идентификатор.
3. Нажмите **Сохранить**.

> 💡 Идентификатор должен быть уникальным в системе и содержать только латинские буквы, цифры и дефисы.

Как поделиться визиткой

1. Перейдите в свой **Профиль**.
2. В блоке **Визитка**:
   - Нажмите **Открыть QR-код** и отсканируйте код камерой устройства.
   - Кнопку **Скопировать ссылку**, чтобы скопировать адрес ссылки на визитку.

Дополнительные действия с личным профилем

Завершение всех сеансов

Функция принудительного завершения всех активных сессий — важный инструмент безопасности. Используйте его в случае утери устройства, подозрения на взлом аккаунта или для немедленного обновления токенов доступа.

> 📌 Эта операция немедленно аннулирует все access- и refresh-токены, завершая ВСЕ его текущие сессии во всех приложениях.

Чтобы завершить все активные сеансы:

1. Перейдите в свой **Профиль**.
2. Раскройте блок **Другие действия** и выберите **Выйти со всех устройств**.

После этого потребуется **войти заново** на всех устройствах.

Скачивание данных личного профиля

КриптоАРМ IDM позволяет экспортировать все данные профиля в JSON формате.

Этот файл содержит всю информацию, относящуюся к вашему профилю в **КриптоАРМ IDM**, а также сведения о внешних аккаунтах, которые вы добавили в качестве способов входа, независимо от того, установлен ли для них параметр публичности.

Чтобы скачать данные профиля:

1. Перейдите в свой **Профиль**.
2. Раскройте блок **Другие действия** и выберите **Скачать данные**.
3. Загрузка JSON-файла начнется автоматически.

Политика обработки персональных данных

Ознакомьтесь с документом о том, как **КриптоАРМ IDM** обрабатывает ваши данные.

Чтобы ознакомиться с политикой:

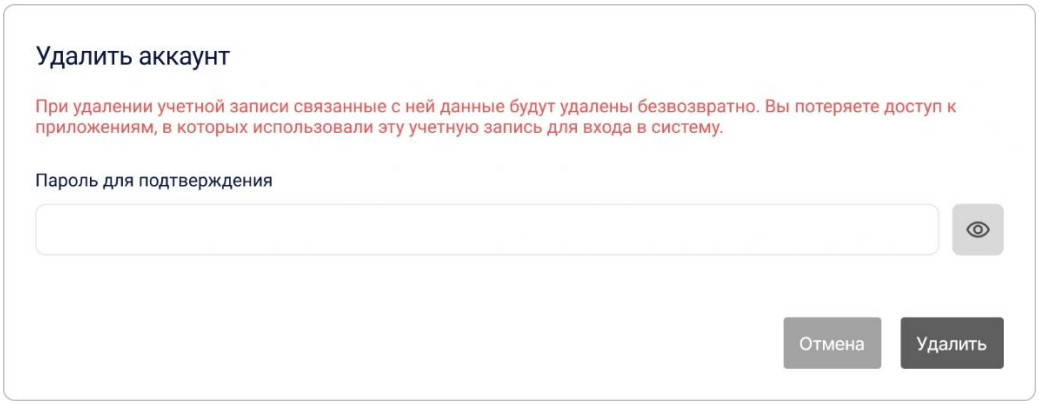
1. Перейдите в свой **Профиль**.
2. Раскройте блок **Другие действия** и выберите **Политика обработки ПДн**.
3. Запустится скачивание файла с политикой.

Удаление и восстановление аккаунта

Удаление аккаунта в **КриптоАРМ IDM** — необратимая операция, после которой восстановить данные будет невозможно. Система использует механизм отсроченного удаления: ваш аккаунт помечается на удаление, но остается доступным для восстановления в течение определенного времени. Это сделано для защиты от случайного удаления и дает вам время передумать.

Чтобы удалить аккаунт:

1. Перейдите в свой **Профиль**.
2. Раскройте блок **Другие действия** и выберите действие **Удалить аккаунт**.
3. В открывшемся окне введите пароль от аккаунта для подтверждения действия и нажмите **Удалить**.



Что происходит:

- Аккаунт помечается на удаление
- Вы автоматически выходите из системы
- В течение определенного времени доступно восстановление аккаунта

В течение определенного времени после удаления аккаунта у вас есть возможность восстановить доступ к нему. Для этого вам нужно заново авторизоваться в **КриптоАРМ IDM**, после этого нажать **Восстановить аккаунт**.

> 💡 Восстановление аккаунта доступно только при авторизации в **КриптоАРМ IDM**. При входе в приложение через сервис **КриптоАРМ IDM** восстановление аккаунта недоступно.

Разрешения приложений и OAuth-доступ

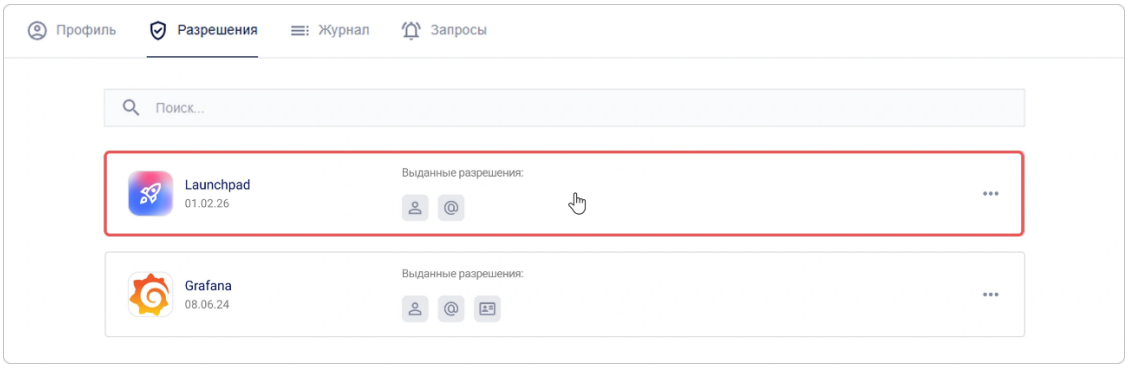
Разрешения — это права, которые вы предоставляете внешним приложениям для доступа к определенным данным вашего профиля **КриптоАРМ IDM**. Вы можете в любой момент ограничить доступ, завершить активные сеансы или полностью отозвать разрешения.

Все приложения, имеющие доступ к вашим данным, отображаются в **Профиле** на вкладке **Разрешения**.

Переход в приложение из списка разрешений

Чтобы быстро открыть приложение, которому вы ранее предоставили доступ:

1. Перейдите в свой **Профиль** → вкладка **Разрешения**.

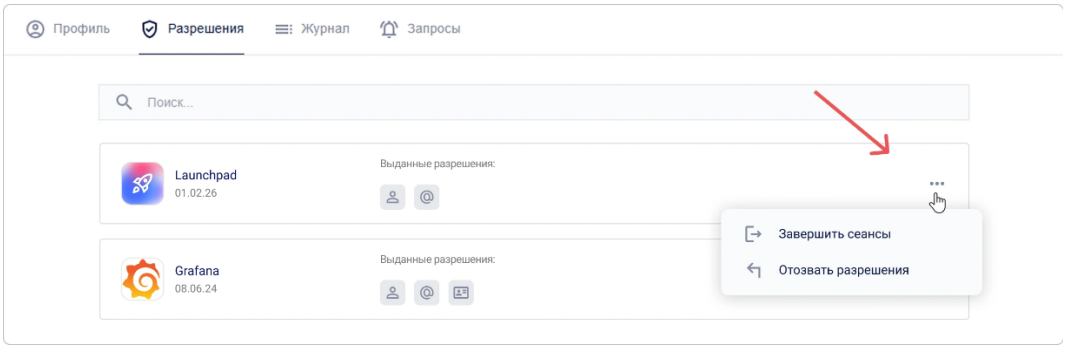


2. Нажмите на **название приложения** в списке.
3. Произойдет автоматический переход в выбранное приложение.

Завершение активных сеансов приложения

Если вы хотите немедленно завершить все сессии в конкретном приложении:

1. Перейдите в свой **Профиль** → вкладка **Разрешения**.
2. Вызовите меню действий для приложения, в котором необходимо завершить сеансы.
3. Выберите действие **Завершить сеансы**.



4. Подтвердите действие в модальном окне.

Что произойдет: Все активные сессии в этом приложении будут завершены. При следующем обращении к приложению потребуется **повторная авторизация**.

Завершение сеансов полезно, если вы подозреваете несанкционированный доступ или использовали приложение на общем устройстве.

Отзыв разрешений у приложения

Чтобы полностью запретить приложению доступ к вашим данным:

1. Перейдите в свой **Профиль** → вкладка **Разрешения**.

2. Вызовите меню действий для приложения, у которого необходимо отозвать разрешения.
3. Выберите действие **Отозвать разрешение**.
4. Подтвердите действие в модальном окне.

Последствия: Приложение **потеряет доступ** ко всем данным вашего профиля. При следующем входе система запросит **новое согласие** на доступ.

Приглашения в закрытые приложения

Приглашение — это способ получить доступ к закрытому приложению. Администратор приложения отправляет приглашение на вашу электронную почту, после чего вы сможете войти в приложение, недоступное для остальных пользователей.

Как получить приглашение?

Приглашение приходит двумя способами:

1. **По электронной почте**: Вы получите письмо с приглашением и ссылкой для быстрого перехода в приложение.
2. **В вашем профиле КриптоАРМ IDM**: в разделе **Запросы** появляется новое приглашение.

Как принять приглашение?

Вы можете принять приглашение любым удобным способом.

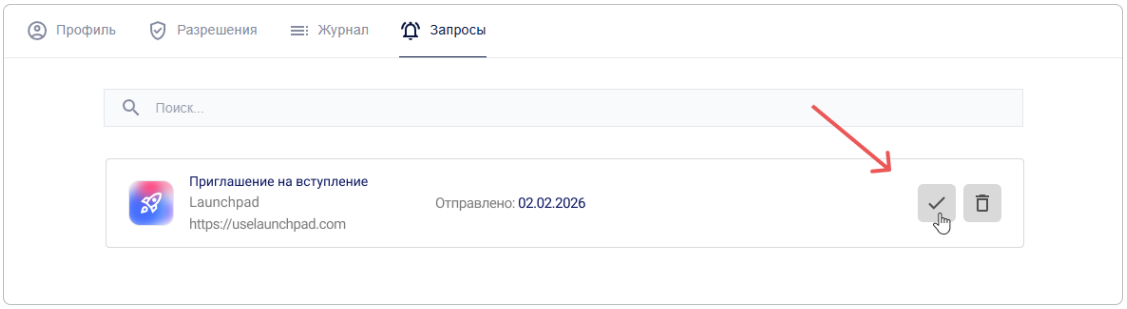
Способ 1: Принять приглашение из письма

1. Откройте письмо с приглашением.
2. Нажмите на ссылку в письме.
3. Далее возможны два варианта:
   - если вы уже авторизованы в системе — вы сразу попадёте в приложение;
   - если вы не авторизованы — выполните вход в систему.

   🔐 Вход необходимо выполнить **под тем аккаунтом**, к которому привязан email, указанный в приглашении.

Способ 2: Принять приглашение из профиля

1. Перейдите в свой **Профиль** → вкладка **Запросы**.
2. Найдите нужное приглашение в списке.
3. Нажмите кнопку **Принять**.



После этого доступ к приложению будет активирован, и вы сможете перейти в него.

Если у вас ещё нет аккаунта

Если вы получили приглашение, но ещё не зарегистрированы в системе **КриптоАРМ IDM**:

1. Перейдите по ссылке из письма с приглашением.
2. Зарегистрируйтесь в системе **КриптоАРМ IDM**.
3. При регистрации укажите тот же почтовый адрес, на который было отправлено приглашение.
4. После завершения регистрации вы автоматически получите доступ к приложению.

Каталог приложений

> 🔬 **Экспериментальная функция**: Доступность регулируется администратором системы.

Что такое каталог?

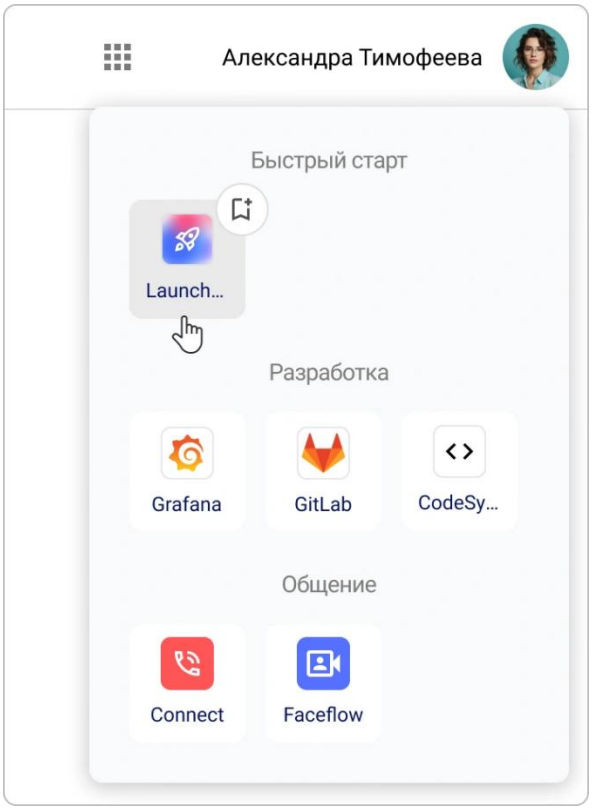
Каталог — это централизованный маркетплейс всех приложений, доступных в экосистеме **КриптоАРМ IDM**.

Каталог объединяет все публичные приложения в одном месте, что позволяет быстро находить нужные приложения, просматривать названия и описания, получать доступ к приложениям без необходимости запоминать сложные ссылки или пути.

Приложения из каталога можно добавить в избранные. Для быстрого доступа все избранные приложения отображаются в левой боковой панели.

Как использовать приложения из каталога?

1. Нажмите на кнопку .
2. Откроется окно со списком приложений, добавленных в каталог.



3. Выберите нужное приложение в каталоге.
4. Произойдет автоматический редирект на страницу приложения.
5. Пройдите аутентификацию в приложении с помощью **КриптоАРМ IDM** и предоставьте приложению доступ к своим данным.

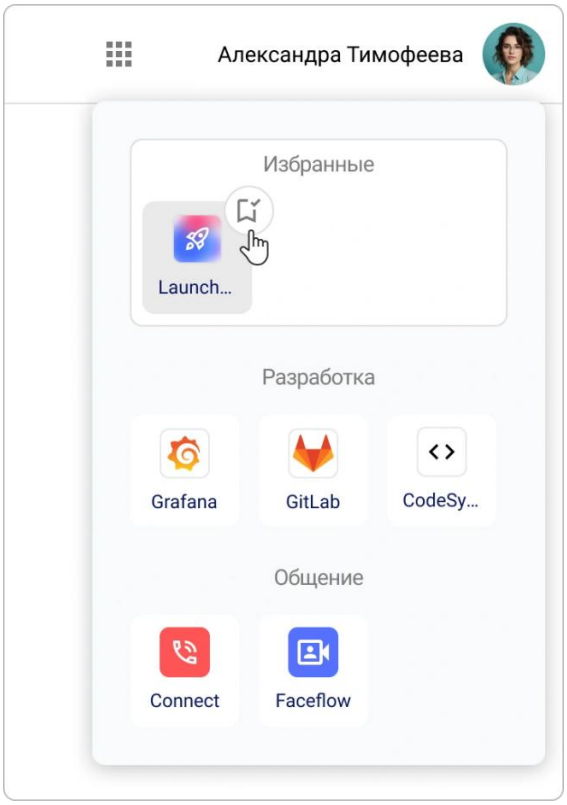
Теперь вы сможете входить в приложение с вашим профилем **КриптоАРМ IDM**.

Действия в каталоге

Добавление приложения в избранные

1. Нажмите на кнопку **Каталог приложений** .
2. Откроется окно со списком приложений, добавленных в каталог.
3. Нажмите на кнопку , размещенную рядом с приложением, которое необходимо добавить в избранные.

   Приложение будет добавлено в избранные и отобразится в соответствующей группе.



Удаление приложения из избранных

1. Нажмите на кнопку **Каталог приложений** .
2. Откроется окно со списком приложений, добавленных в каталог.
3. Нажмите на кнопку , размещенную рядом с приложением, которое необходимо удалить из избранных.

Приложение будет удалено из избранных и пропадет из бокового меню.

Журнал активности и история входов

Журнал активности — это инструмент безопасности, который позволяет отслеживать откуда и с каких устройств вы заходили в **КриптоАРМ IDM** или приложения.

Детализация событий

Для каждого события доступен просмотр подробных сведений.

Параметр	Что содержит
Заголовок события	Категория действия
Дата и время	Точные временные метки
Приложение	Идентификатор (client_id) приложения
Пользователь	Идентификатор (id) пользователя
Устройство	Тип устройства и браузер

Местоположение IP-адрес

Как просмотреть журнал активности?

1. Перейдите в свой **Профиль**.
2. Откройте вкладку **Журнал**.

Смотрите также

- Регистрация и вход пользователей — инструкция по созданию аккаунта, входу с помощью логина/пароля и внешних сервисов аутентификации.

Регистрация, вход и восстановление пароля в КриптоАРМ IDM

В этом руководстве вы узнаете, как создать аккаунт в **КриптоАРМ IDM**, войти в систему с помощью логина и пароля или через внешние сервисы, а также безопасно восстановить доступ к профилю при необходимости.

Содержание:

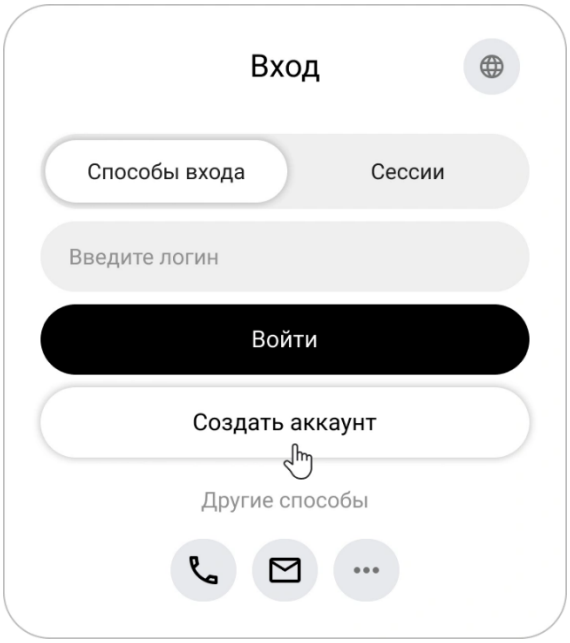
- Регистрация нового аккаунта
- Вход по логину и паролю
- Вход через внешние сервисы
- Быстрый вход для аутентифицированных пользователей
- Восстановление пароля
- Смотрите также

Регистрация нового аккаунта

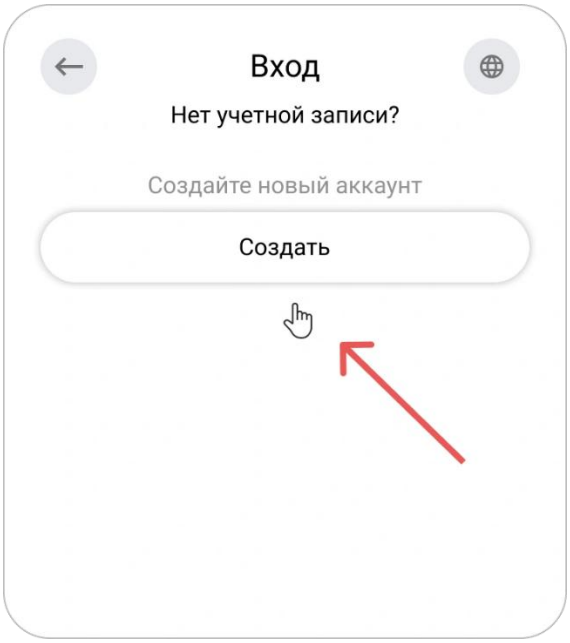
Где доступна регистрация

Функция создания аккаунта может быть доступна в двух случаях:

1. **На форме входа**;



2. **На форме выбора действий при входе через способ входа**, если указанный идентификатор не привязан ни к одному профилю в **КриптоАРМ IDM**

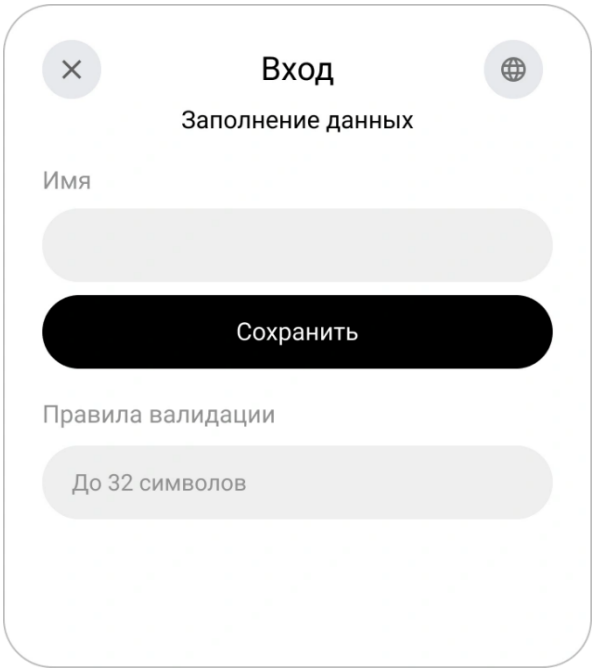


💡 **Дизайн форм** может отличаться в зависимости от настроек конкретного приложения

Как создать аккаунт в КриптоАРМ IDM

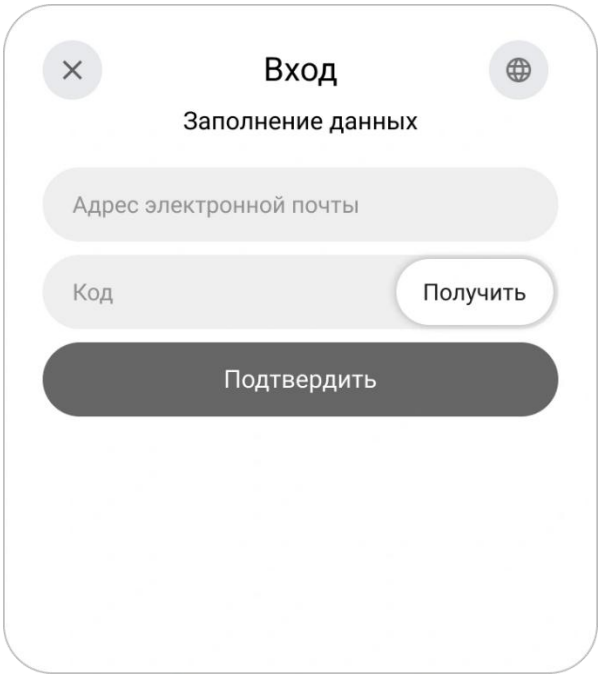
1. Нажмите **Создать аккаунт** на форме входа или выбора действий.
2. Введите необходимые данные в регистрационной форме.

   Пример окна для ввода имени:



3. Если система запросит e-mail — укажите адрес, не привязанный к другим пользователям.

4. Введите код или перейдите по ссылке из письма, отправленного на указанную почту.



💡 Если подтверждение выполняется по ссылке, окно ввода кода можно закрыть.

5. При первом входе в приложение разрешите доступ к необходимым данным.

После выполнения шагов аккаунт будет создан, и произойдет вход в систему.

> 🔗 Если регистрация начата через внешний сервис, идентификатор внешней системы автоматически привяжется к новому профилю. Его можно будет использовать для последующих входов.

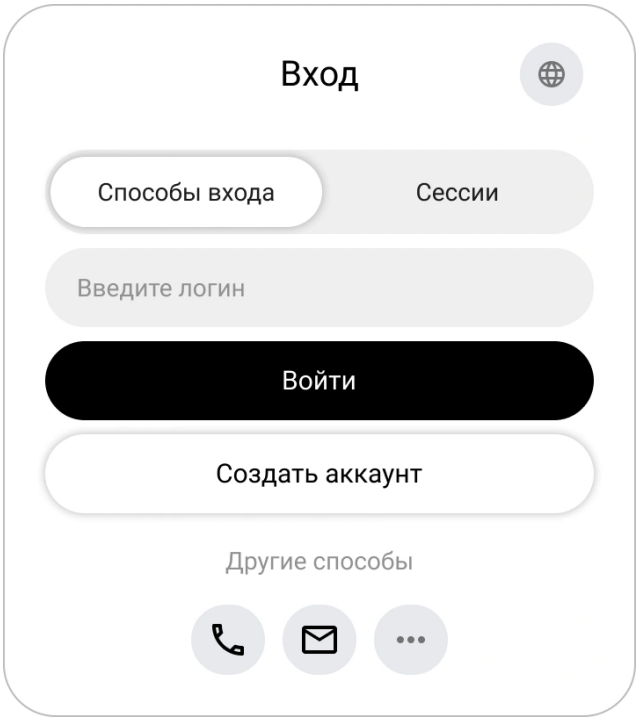
Вход по логину и паролю

Вы можете авторизоваться в приложении с помощью учетной записи **КриптоАРМ IDM**.

> 📌 **Примечание**: В некоторых приложениях вход по паролю может быть отключен. В этом случае используйте внешние способы входа.

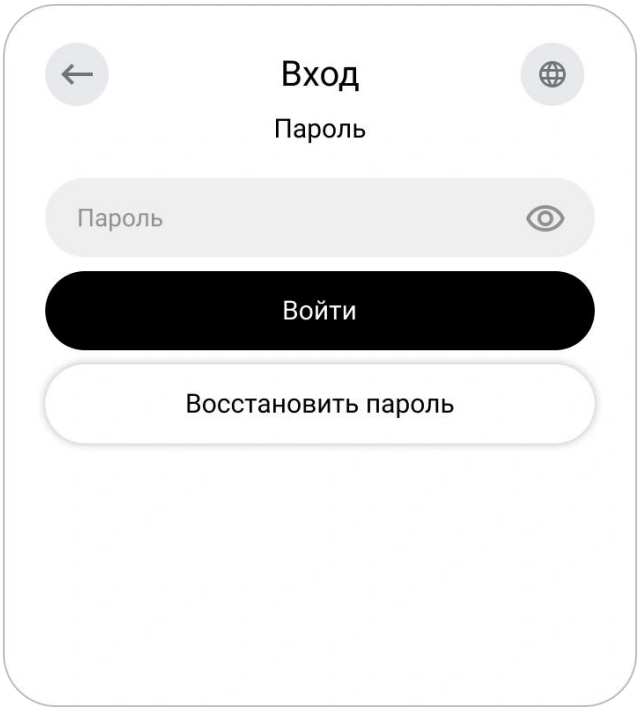
Чтобы войти в систему:

1. На первом шаге виджета входа введите данные для идентификации (например, логин, e-mail или номер телефона) и нажмите **Войти**.



2. Введите пароль на втором шаге и нажмите **Войти**.

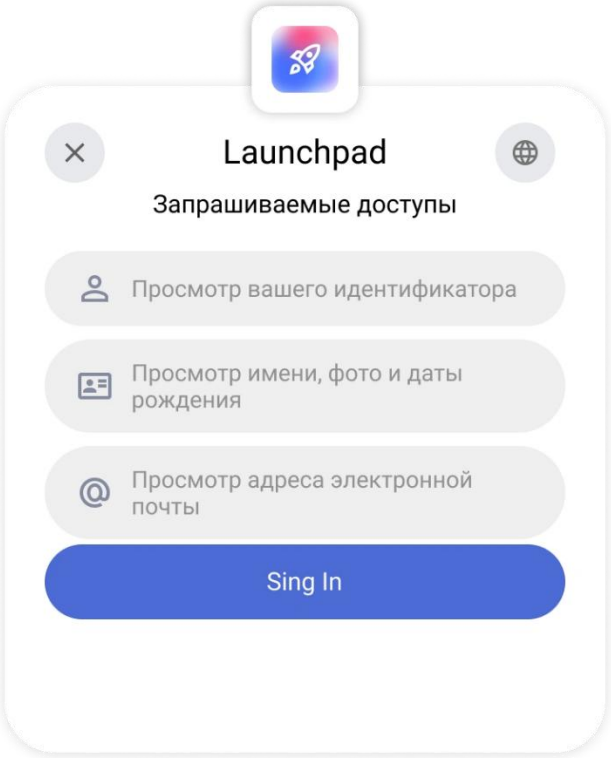
> 💡 Если вы допустили ошибку при вводе данных, следуйте подсказкам на экране.



После успешной аутентификации:

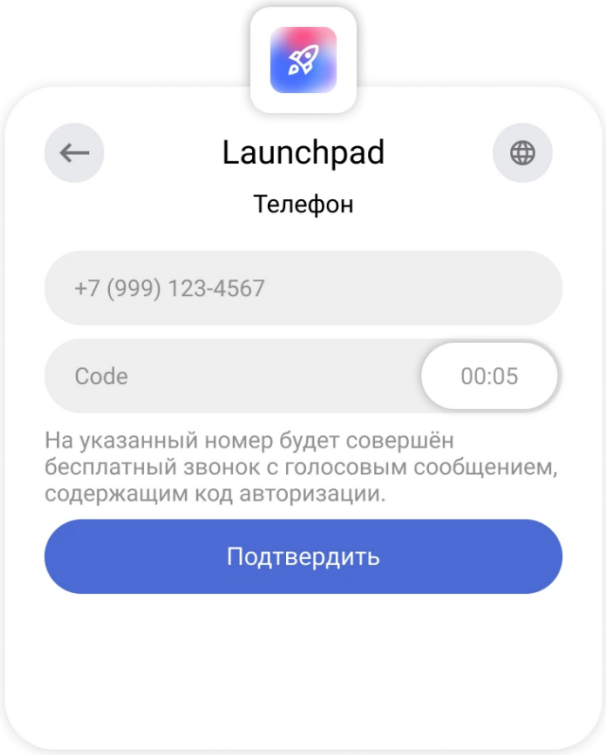
- при первом входе откроется форма подтверждения доступа к данным;

  Пример формы с запросом доступа к данным профиля:



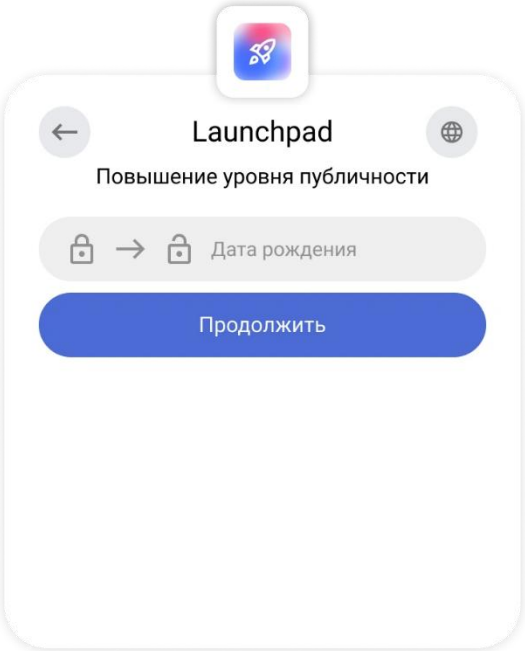
- если приложению требуются обязательные поля профиля, система запросит их заполнение;

Пример запроса номера телефона:



- если данные скрыты настройками приватности, будет предложено изменить уровень доступа.

  Пример изменения приватности даты рождения:



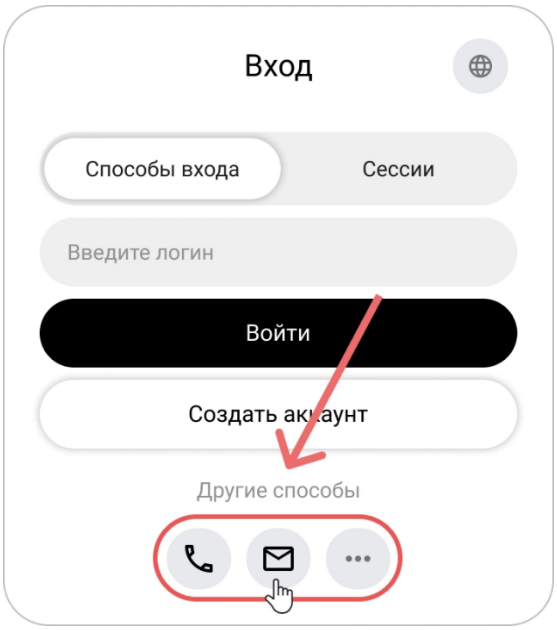
💡 Если вы переходили по ссылке на конкретную страницу, после авторизации вы будете автоматически возвращены на неё — повторно искать раздел не потребуется.

Вход через внешние сервисы

К внешним сервисам идентификации (или способам входа) относятся социальные сети и внешние сервисы (Yandex, Mail, Вконтакте и др.).

Чтобы войти через внешний сервис:

1. Выберите нужный способ входа в виджете.



2. Пройдите авторизацию в выбранном сервисе, используя доступные способы для социальных сетей.

3. При первом входе откроется форма запроса доступа к данным. Предоставьте согласие на доступ к своим данным.

Быстрый вход для аутентифицированных пользователей

Если вы уже выполняли вход в **КриптоАРМ IDM** в своём браузере, повторная авторизация не потребуется.

Возможны два сценария входа:

Автоматический вход

Если в браузере активна только одна сессия пользователя, вход произойдёт автоматически — без отображения формы выбора аккаунта.

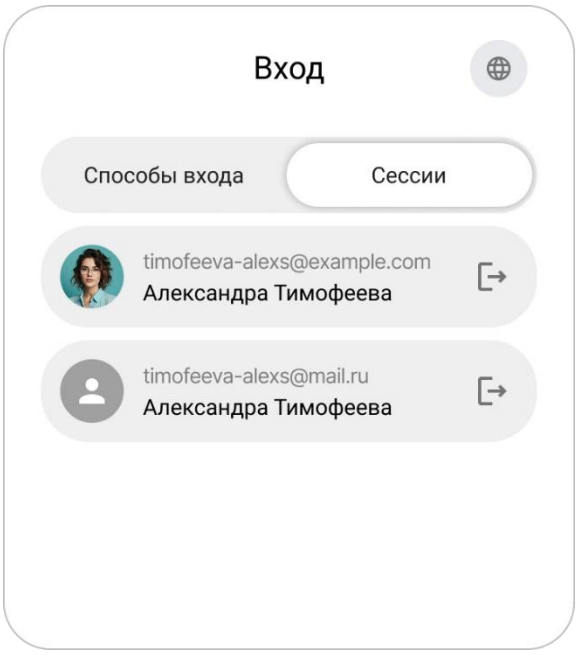
💡 Это называется сквозной (автоматической) аутентификацией и позволяет сразу продолжить работу.

⚠️ Автоматический вход работает только для приложений. При входе в систему всегда отображается окно выбора аккаунта — даже если активна одна сессия.

Выбор аккаунта

Если в браузере сохранено несколько сессий, откроется окно выбора аккаунта:

1. Нажмите на имя пользователя.



2. После выбора пользователя произойдёт вход.

Дополнительно:

- Чтобы войти под другим пользователем, выберите **Способы входа** и пройдите авторизацию другим пользователем.

- Чтобы завершить текущую сессию, нажмите кнопку **Выйти из аккаунта**.

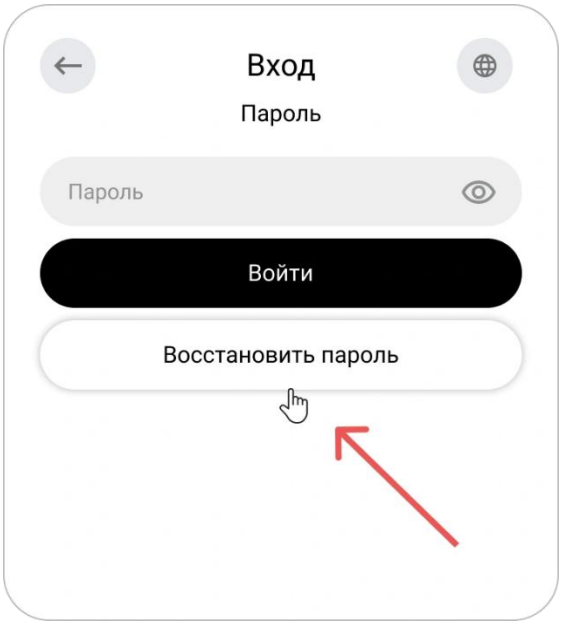
Восстановление пароля

Если вы забыли пароль от своей учётной записи в **КриптоАРМ IDM**, вы можете легко его восстановить.

Как восстановить пароль в КриптоАРМ IDM

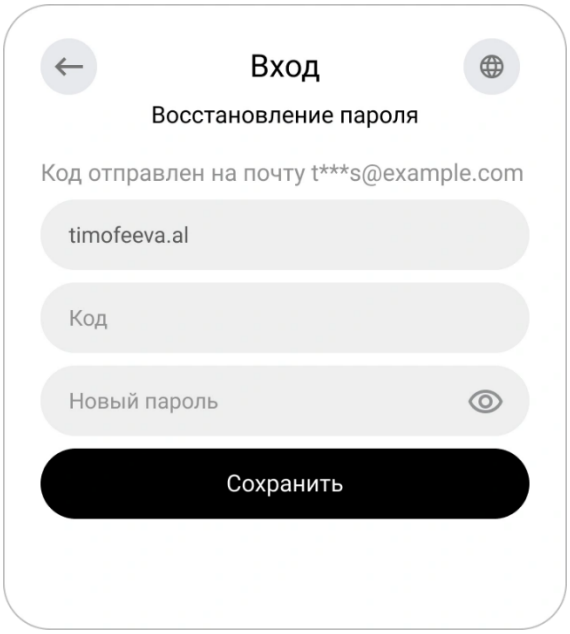
1. На первом шаге виджета входа введите данные для идентификации (например, логин, e-mail или номер телефона) и нажмите **Войти**.

2. На следующем шаге выберите **Восстановить пароль**.



3. На вашу почту будет направлено письмо с кодом подтверждения.
4. Введите код из письма.

   ⚠️ Код действует ограниченное время. Если срок действия истёк, запросите новый код.



5. Задайте новый пароль и нажмите **Сохранить**.

После обновления пароля вход будет выполнен автоматически.

   ✅ Пароль успешно восстановлен, теперь вы можете использовать новую комбинацию при входе в систему.

Смотрите также

- Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.

Как подключить вход через LDAP в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить доверенный провайдер аутентификации **LDAP (Lightweight Directory Access Protocol)** или **Active Directory** к системе **КриптоАРМ IDM**, настроить сопоставление атрибутов, проверить доступность внешней системы и интегрировать кнопку входа на виджет авторизации.

Доверенный провайдер **LDAP** предназначен для организации входа в информационные системы по данным учетных записей пользователей системы **LDAP**.

Шаг 1. Настройка на стороне внешней системы

На стороне внешнего LDAP/Active Directory необходимо подготовить учетную запись, которая будет использоваться для подключения коннектора.

Рекомендуется использовать сервисную учетную запись с правами на чтение каталога пользователей и (при необходимости) изменение паролей.

Учетная запись должна:

- иметь право на выполнение LDAP-запросов к каталогу;
- иметь доступ к области поиска, указанной в параметре `ldap_base`;
- при необходимости — иметь право на изменение пользовательских атрибутов (например, при включенной синхронизации паролей).

> 💡 В большинстве случаев используется отдельная сервисная учетная запись, а не административный пользователь домена.

Шаг 2. Настройка в КриптоАРМ IDM

В сервисе **КриптоАРМ IDM** необходимо создать доверенный провайдер по шаблону **LDAP**:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Доверенные провайдеры** и нажмите **Настроить**.
3. В открывшемся окне нажмите на кнопку **Создать**  .

4. Откроется окно со списком шаблонов.
5. Выберите шаблон провайдера **LDAP**.
6. В форме создания заполните поля или вставьте скопированные значения из ранее созданного доверенного провайдера **LDAP**:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Адрес сервера LDAP (ldap_url)** — Адрес сервера LDAP в формате `ldaps://example.com`.
   - **База поиска (ldap_base)** — Объект каталога, начиная с которого будет производиться поиск. Должен быть корректным DN, например, `dc=example,dc=com`.
   - **Домен LDAP (ldap_domain)** — Имя домена, которому принадлежат пользователи.
   - **Фильтр поиска (ldap_filter)** — Фильтр для поиска учетной записи пользователя.
   - **Сопоставление атрибутов LDAP (ldap_mapping)** — Соответствие атрибутов профиля пользователя **КриптоАРМ IDM** с атрибутами в LDAP. Формат: `trusted_id_attribute:ldap_attribute` (например, `given_name:givenName`, `family_name:sn`, `email:mail`, `picture:photo`). Подробнее о правилах →
   - **Логин администратора (ldap_admin_dn)** — Логин администратора LDAP.
   - **Пароль администратора (ldap_admin_pwd)** — Пароль администратора LDAP.

   Дополнительные настройки

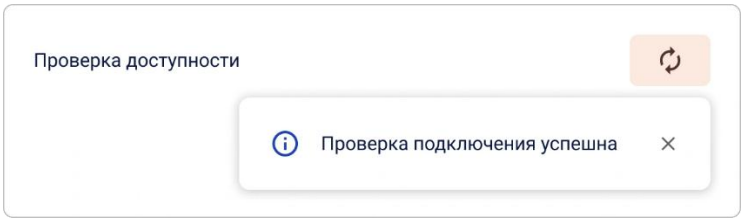
   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
   - **Запретить сброс пароля** — Пользователь не сможет сменить пароль от учетной записи внешней системы. В виджете входа кнопка **Сменить пароль** будет скрыта.
7. Нажмите **Сохранить**.

После успешного создания провайдер отобразится в списке.

Шаг 3. Проверка доступности внешней системы

Проверка доступности — это встроенный инструмент, который позволяет убедиться, что указанные параметры подключения к доверенному провайдеру настроены корректно и сервис успешно взаимодействует с внешней системой.

После заполнения параметров провайдера нажмите кнопку **Проверка доступности**. Система выполнит тестовый запрос на указанные конечные точки провайдера.



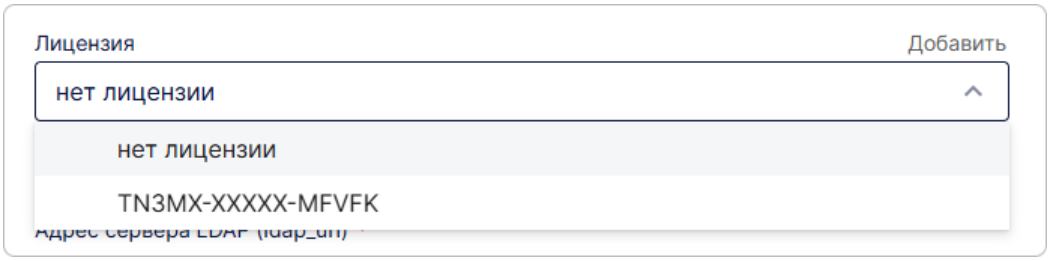
В результате проверки возможны два варианта ответа:

- ✅ **Проверка подключения успешна** — соединение установлено, параметры конфигурации корректны.
- ❌ **Ошибка проверки подключения** — возникла ошибка соединения. В этом случае проверьте правильность указанных URL и корректность клиентских ключей или токенов.

  💡 Рекомендуется выполнять проверку после каждого изменения настроек, чтобы убедиться, что параметры указаны корректно перед сохранением.

Шаг 4. Привязка лицензии

1. В общем списке провайдеров найдите созданный способ входа и нажмите **Настроить**.
2. В **Лицензия** выберите ключ из выпадающего списка.



   💡 **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

3. Сохраните изменения по кнопке **Сохранить**.

Шаг 5. Добавление на виджет

Чтобы пользователи увидели кнопку входа на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом способа входа.

Правила сопоставления атрибутов

Сопоставление атрибутов позволяет настроить сопоставление поля профиля пользователя **КриптоАРМ IDM** с атрибутом пользователя в **Active Directory**.

Если значение поля не задано, используется значение по умолчанию:

- `given_name:givenName`,
- `family_name:sn`,
- `email:mail`.

Основные поля пользователя КриптоАРМ IDM

Поле	Описание
`sub`	Идентификатор пользователя
`email`	Адрес электронной почты
`phone_number`	Номер телефона
`nickname`	Публичное имя
`given_name`	Имя
`family_name`	Фамилия
`login`	Логин
`birthdate`	Дата рождения
`picture`	Фото профиля

Особенности сопоставления атрибутов

1. **Дополнительные поля**:
   - Допускается настройка сопоставления на дополнительные поля профиля пользователя. В таком случае в качестве поля профиля **КриптоАРМ IDM** указывается **Название** дополнительного поля.
2. **Особенности работы с логином**
   - Можно задать сопоставление на поле **Логин**, для того, чтобы логины пользователя в **КриптоАРМ IDM** и во внешней системе совпадали. В этом случае логин во внешней системе должен иметь уникальное значение.

- Если в сопоставлении атрибутов отсутствует настройка сопоставления на поле **Логин**, или логин уже используется для другого пользователя, то при автоматической регистрации пользователю присваивается внутренний логин, сгенерированный системой.

3. **Сопоставление с условием «или»**

   - В поле **Сопоставление атрибутов** для доверенных провайдеров можно задать несколько возможных атрибутов через дефис, чтобы использовать значение из одного, если в другом оно отсутствует.
   - Пример записи: `<поле_КриптоАРМ IDM>:<атрибут1>-<атрибут2>`

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.

Как подключить вход через 1С в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить доверенный провайдер аутентификации **1С** к системе **КриптоАРМ IDM**, настроить сопоставление атрибутов, проверить доступность внешней системы и интегрировать кнопку входа на виджет авторизации.

Доверенный провайдер **1С** предназначен для организации входа в информационные системы по данным (логин/пароль) учетных записей пользователей системы **1С**.

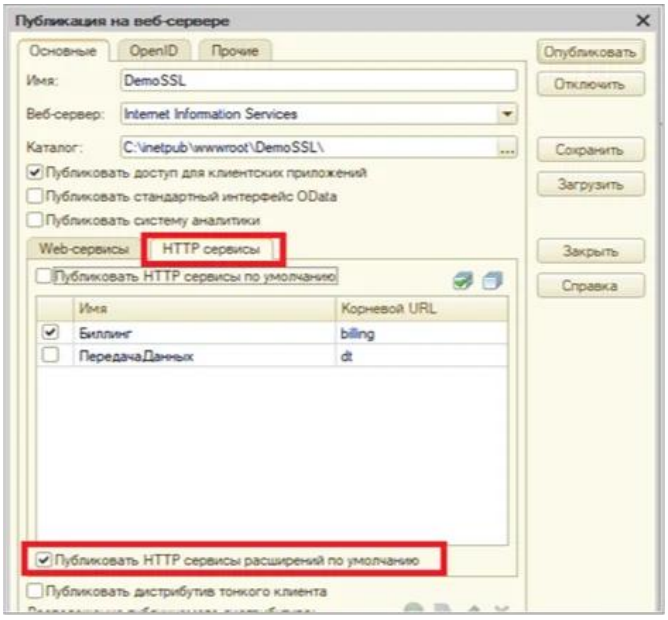
Шаг 1. Настройка на стороне внешней системы

1. Установите расширение конфигурации **1С**.

   Взаимодействие с информационной базой **1С** реализовано через расширение конфигурации (файл расширения предоставляется отдельно), и осуществляется с использованием http-сервисов.

   Расширение конфигурации предоставляется технической поддержкой **КриптоАРМ IDM**.

2. Опубликуйте http-сервисы приложения на web-сервере для работы с расширением.



3. Установите признак **Публиковать HTTP сервисов расширения по умолчанию** для работы http-сервисов расширения.

   Для проверки корректности публикации http-сервисов проверяется файл публикации (**.vrd**) на web-сервере. Файл публикации должен содержать свойство `publishExtensionsByDefault`, равное значению `true`.

```
</ws>
<httpServices publishByDefault="false"
              publishExtensionsByDefault="true">
        <service name="Биллинг"
                 rootUrl="billing"
                 enable="true"
                 reuseSessions="autouse"
                 sessionMaxAge="20"
                 poolSize="10"
                 poolTimeout="5"/>
        <service name="ПередачаДанных"
                 rootUrl="dt"
```

4. Создайте пользователя, учетные данные которого будут использоваться для авторизации запросов (допускается пользователь без прав).

Шаг 2. Настройка в КриптоАРМ IDM

В сервисе **КриптоАРМ IDM** необходимо создать доверенный провайдер по шаблону **1С**.

Чтобы создать провайдер:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Доверенные провайдеры** и нажмите **Настроить**.
3. В открывшемся окне нажмите на кнопку **Создать** .
4. Откроется окно со списком шаблонов.

5. Выберите шаблон провайдера **1С**.

6. В форме создания заполните поля или вставьте скопированные значения из ранее созданного доверенного провайдера **1С**:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Адрес сервера 1С** — Название опубликованной базы в формате: `http(s)://[сервер]:[порт]/[база]`.
   - **Логин администратора 1С** — Логин пользователя 1С, учетные данные которого будут использоваться для авторизации запросов (допускается пользователь без прав).
   - **Пароль администратора 1С** — Пароль пользователя 1С.
   - **Сопоставление атрибутов 1С** — Соответствие атрибутов профиля пользователя **КриптоАРМ IDM** с атрибутами в 1С. Формат: `trusted_id_attribute:1C_attribute` (например, `given_name:givenName`, `family_name:sn`, `email:mail`, `picture:photo`). Подробнее о правилах →

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
   - **Запретить сброс пароля** — Пользователь не сможет сменить пароль от учетной записи внешней системы. В виджете входа кнопка **Сменить пароль** будет скрыта.

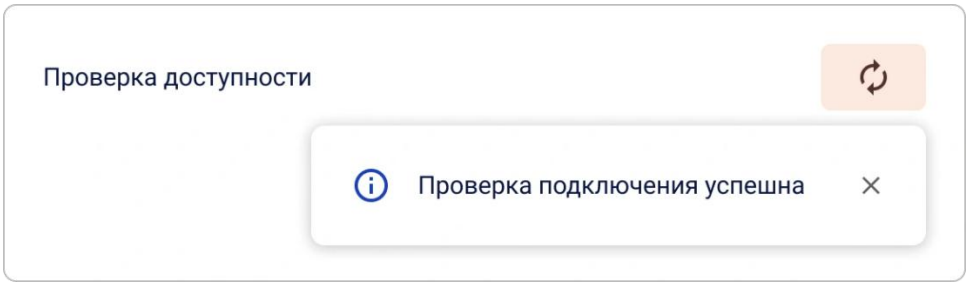
7. Нажмите **Сохранить**.

После успешного создания провайдер отобразится в списке.

Шаг 3. Проверка доступности внешней системы

Проверка доступности — это встроенный инструмент, который позволяет убедиться, что указанные параметры подключения к доверенному провайдеру настроены корректно и сервис успешно взаимодействует с внешней системой.

После заполнения параметров провайдера нажмите кнопку **Проверка доступности**. Система выполнит тестовый запрос на указанные конечные точки провайдера.



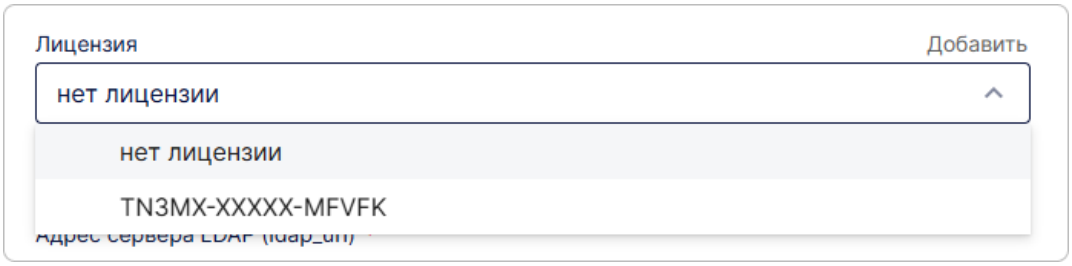
В результате проверки возможны два варианта ответа:

- ✅ **Проверка подключения успешна** — соединение установлено, параметры конфигурации корректны.
- ❌ **Ошибка проверки подключения** — возникла ошибка соединения. В этом случае проверьте правильность указанных URL и корректность клиентских ключей или токенов.

  💡 Рекомендуется выполнять проверку после каждого изменения настроек, чтобы убедиться, что параметры указаны корректно перед сохранением.

Шаг 4. Привязка лицензии

1. В общем списке провайдеров найдите созданный способ входа и нажмите **Настроить**.
2. В **Лицензия** выберите ключ из выпадающего списка.



   💡 **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

3. Сохраните изменения по кнопке **Сохранить**.

Шаг 5. Добавление на виджет

Чтобы пользователи увидели кнопку входа на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом способа входа.

Правила сопоставления атрибутов

Сопоставление атрибутов позволяет настроить сопоставление поля профиля пользователя **КриптоАРМ IDM** с атрибутом пользователя в **1С**.

Если значение поля не задано, используется значение по умолчанию:

- `given_name:firstName`,
- `family_name:lastName`,
- `email:email`,
- `picture:photo`.

Основные поля пользователя КриптоАРМ IDM

Поле	Описание
`sub`	Идентификатор пользователя
`email`	Адрес электронной почты
`phone_number`	Номер телефона
`nickname`	Публичное имя
`given_name`	Имя
`family_name`	Фамилия
`login`	Логин
`birthdate`	Дата рождения
`picture`	Фото профиля

Особенности сопоставления атрибутов

1. **Дополнительные поля**:
   - Допускается настройка сопоставления на дополнительные поля профиля пользователя. В таком случае в качестве поля профиля **КриптоАРМ IDM** указывается **Название** дополнительного поля.
2. **Особенности работы с логином**
   - Можно задать сопоставление на поле **Логин**, для того, чтобы логины пользователя в **КриптоАРМ IDM** и во внешней системе совпадали. В этом случае логин во внешней системе должен иметь уникальное значение.
   - Если в сопоставлении атрибутов отсутствует настройка сопоставления на поле **Логин**, или логин уже используется для другого пользователя, то при автоматической регистрации пользователю присваивается внутренний логин, сгенерированный системой.
3. **Сопоставление с условием «или»**
   - В поле **Сопоставление атрибутов** для доверенных провайдеров можно задать несколько возможных атрибутов через дефис, чтобы использовать значение из одного, если в другом оно отсутствует.

- Пример записи: `<поле_КриптоАРМ IDM>:<атрибут1>-<атрибут2>`

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как подключить вход через ALD Pro в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить доверенный провайдер аутентификации **ALD Pro** к системе **КриптоАРМ IDM**, настроить сопоставление атрибутов, проверить доступность внешней системы и интегрировать кнопку входа на виджет авторизации.

Доверенный провайдер **ALD Pro** предназначен для организации входа в информационные системы по данным учетных записей пользователей системы **ALD Pro**.

Шаг 1. Настройка на стороне внешней системы

На стороне внешней системы ALD Pro необходимо подготовить учетную запись, которая будет использоваться для подключения коннектора.

Рекомендуется использовать сервисную учетную запись с правами на чтение каталога пользователей и (при необходимости) изменение паролей.

Учетная запись должна:

- иметь права на чтение каталога пользователей;
- иметь права на чтение групп и организационной структуры;
- при необходимости — с правами изменения атрибутов пользователей (для экспорта).

> 💡 В большинстве случаев используется отдельная сервисная учетная запись, а не административный пользователь домена.

Шаг 2. Настройка в КриптоАРМ IDM

В сервисе **КриптоАРМ IDM** необходимо создать доверенный провайдер по шаблону **ALD Pro**:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Доверенные провайдеры** и нажмите **Настроить**.
3. В открывшемся окне нажмите на кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон провайдера **ALD Pro**.
6. В форме создания заполните поля или вставьте скопированные значения из ранее созданного доверенного провайдера **ALD Pro**:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Адрес сервера ALD Pro (aldpro_url)** — Адрес сервера ALD Pro в формате `ALD Pros://example.com`.
   - **База поиска (aldpro_base)** — Объект каталога, начиная с которого будет производиться поиск. Должен быть корректным DN, например, `dc=example,dc=com`.
   - **Домен ALD Pro (aldpro_domain)** — Имя домена, которому принадлежат пользователи.
   - **Фильтр поиска (aldpro_filter)** — Фильтр для поиска учетной записи пользователя.
   - **Сопоставление атрибутов ALD Pro (aldpro_mapping)** — Соответствие атрибутов профиля пользователя **КриптоАРМ IDM** с атрибутами в ALD Pro. Формат: `trusted_id_attribute:ALD Pro_attribute` (например, `given_name:givenName`, `family_name:sn`, `email:mail`, `picture:photo`). Подробнее о правилах →
   - **Логин администратора (aldpro_admin_dn)** — Логин администратора ALD Pro.
   - **Пароль администратора (aldpro_admin_pwd)** — Пароль администратора ALD Pro.

   Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
- **Запретить сброс пароля** — Пользователь не сможет сменить пароль от учетной записи внешней системы. В виджете входа кнопка **Сменить пароль** будет скрыта.

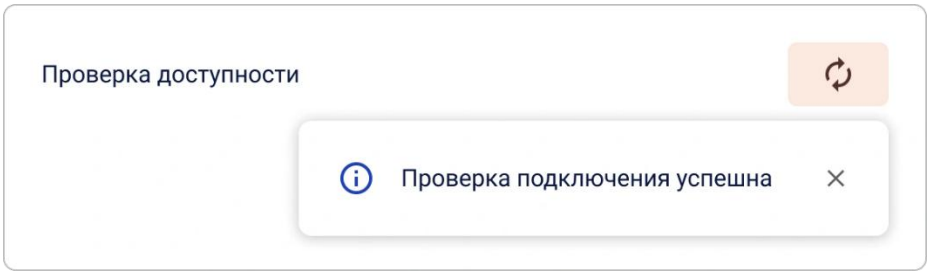
7. Нажмите **Сохранить**.

После успешного создания провайдер отобразится в списке.

Шаг 3. Проверка доступности внешней системы

Проверка доступности — это встроенный инструмент, который позволяет убедиться, что указанные параметры подключения к доверенному провайдеру настроены корректно и сервис успешно взаимодействует с внешней системой.

После заполнения параметров провайдера нажмите кнопку **Проверка доступности**. Система выполнит тестовый запрос на указанные конечные точки провайдера.



В результате проверки возможны два варианта ответа:

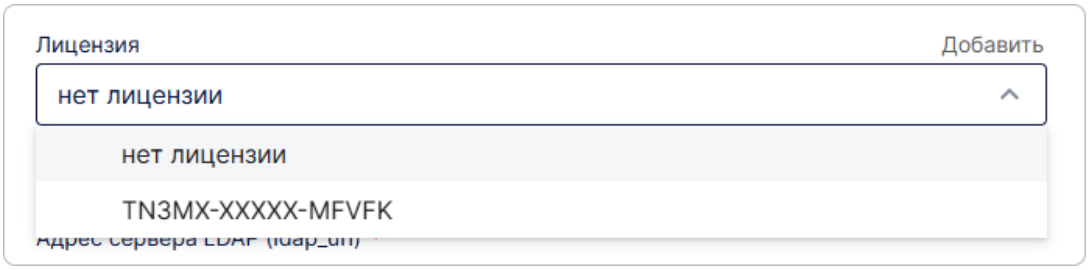
- ✅ **Проверка подключения успешна** — соединение установлено, параметры конфигурации корректны.
- ❌ **Ошибка проверки подключения** — возникла ошибка соединения. В этом случае проверьте правильность указанных URL и корректность клиентских ключей или токенов.

  💡 Рекомендуется выполнять проверку после каждого изменения настроек, чтобы убедиться, что параметры указаны корректно перед сохранением.

Шаг 4. Привязка лицензии

1. В общем списке провайдеров найдите созданный способ входа и нажмите **Настроить**.

2. В **Лицензия** выберите ключ из выпадающего списка.



💡 **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

3. Сохраните изменения по кнопке **Сохранить**.

Шаг 5. Добавление на виджет

Чтобы пользователи увидели кнопку входа на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом способа входа.

Правила сопоставления атрибутов

Сопоставление атрибутов позволяет настроить сопоставление поля профиля пользователя **КриптоАРМ IDM** с атрибутом пользователя в **ALD Pro**.

Если значение поля не задано, используется значение по умолчанию:

- `given_name:givenName`,
- `family_name:sn`,
- `email:mail`.

Основные поля пользователя КриптоАРМ IDM

Поле	Описание
`sub`	Идентификатор пользователя
`email`	Адрес электронной почты
`phone_number`	Номер телефона
`nickname`	Публичное имя
`given_name`	Имя
`family_name`	Фамилия
`login`	Логин
`birthdate`	Дата рождения

`picture` Фото профиля

Особенности сопоставления атрибутов

1. **Дополнительные поля**:
   - Допускается настройка сопоставления на дополнительные поля профиля пользователя. В таком случае в качестве поля профиля **КриптоАРМ IDM** указывается **Название** дополнительного поля.
2. **Особенности работы с логином**
   - Можно задать сопоставление на поле **Логин**, для того, чтобы логины пользователя в **КриптоАРМ IDM** и во внешней системе совпадали. В этом случае логин во внешней системе должен иметь уникальное значение.
   - Если в сопоставлении атрибутов отсутствует настройка сопоставления на поле **Логин**, или логин уже используется для другого пользователя, то при автоматической регистрации пользователю присваивается внутренний логин, сгенерированный системой.
3. **Сопоставление с условием «или»**
   - В поле **Сопоставление атрибутов** для доверенных провайдеров можно задать несколько возможных атрибутов через дефис, чтобы использовать значение из одного, если в другом оно отсутствует.
   - Пример записи: `<поле_КриптоАРМ IDM>:<атрибут1>-<атрибут2>`

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как подключить вход через ЕСИА в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить доверенный провайдер аутентификации **ЕСИА** к системе **КриптоАРМ IDM**. Этот способ входа предназначен для организации входа в информационные системы с помощью учетной записи портала **Госуслуг**. Оператор системы — **Минцифры России**.

В текущей реализации **КриптоАРМ IDM** для подписи и проверки запросов используется приложение КриптоАРМ Сервер.

Шаг 1. Настройка на стороне внешней системы

Подключите свою компанию по инструкции.

Шаг 2. Настройка КриптоАРМ Сервер

1. Скачайте и установите **КриптоАРМ Сервер** на выделенный сервер
2. Настройте сертификаты:
   - Установите сертификат КЭП вашей организации
   - Проверьте срок действия сертификата
3. **Проверьте доступность**:
   - Запустите сервис КриптоАРМ Сервер
   - Убедитесь, что эндпоинты подписи и проверки доступны

После настройки КриптоАРМ Сервер вам понадобятся:

- **Адрес получения подписи запроса** (например: `http://ваш-сервер:порт/sign`)
- **Адрес проверки подписи запроса** (например: `http://ваш-сервер:порт/verify`)
- **Сертификат** КЭП вашей организации

🔍 Технические вопросы интеграции рассмотрены в Методических рекомендациях по использованию ЕСИА.

Шаг 3. Настройка в КриптоАРМ IDM

В сервисе **КриптоАРМ IDM** необходимо создать провайдер по шаблону **ЕСИА**.

Чтобы создать провайдер **ЕСИА**:

1. Перейдите в панель ID → вкладка **Настройки**.
2. Раскройте блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите на кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон провайдера **ЕСИА**.
6. В открывшейся форме создания провайдера заполните параметры провайдера:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.

- **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

Параметры

- **Идентификатор ресурса (client_id)** — Уникальный идентификатор подключаемого ресурса.
- **Пароль** — Пароль от ключевого контейнера ключа подписи.
- **Сертификат подписи и проверки запросов** — Сертификат ключа квалифицированной электронной подписи, выпущенной для подключаемой информационной системы. Необходимо указать путь к файлу с сертификатом.
- **Адрес получения подписи запроса (sign_endpoint)** — Ресурс, который подписывает запрос.
- **Адрес проверки подписи запроса (verify_endpoint)** — Ресурс, который проверяет подпись ответа от ЕСИА.

Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

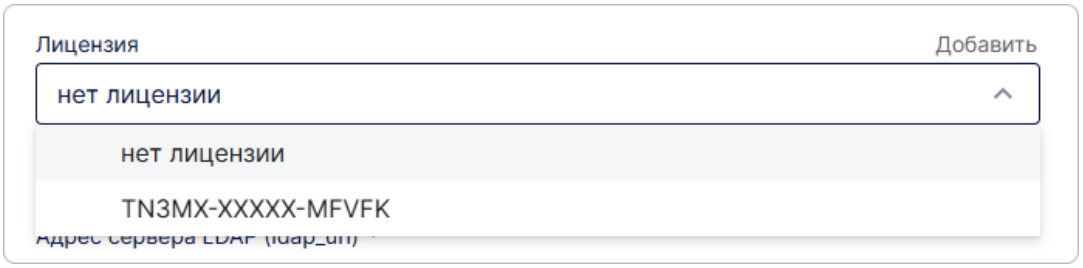
7. Нажмите **Сохранить**.

После успешного создания провайдер отобразится в списке.

Шаг 4. Привязка лицензии

1. В общем списке провайдеров найдите созданный способ входа и нажмите **Настроить**.

2. В **Лицензия** выберите ключ из выпадающего списка.



💡 **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

3. Сохраните изменения по кнопке **Сохранить**.

Шаг 5. Добавление на виджет

Чтобы пользователи увидели кнопку входа на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом способа входа.

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.

Как подключить вход через КриптоАРМ в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить вход по сертификату с помощью приложения **КриптоАРМ** в системе **КриптоАРМ IDM**.

Настройка входа через **КриптоАРМ** состоит из нескольких ключевых этапов:

- Общая информация
- Варианты конфигурации
- Настройка входа через КриптоАРМ для администраторов КриптоАРМ IDM
- Привязка клиентского сертификата для пользователей КриптоАРМ IDM
- Смотрите также

Общая информация

КриптоАРМ — это способ входа в **КриптоАРМ IDM** с использованием клиентского сертификата и локально установленного приложения **КриптоАРМ**.

> 📌 Поскольку криптографические операции выполняются на стороне приложения **КриптоАРМ**, а не в браузере, вход возможен из любого современного браузера без установки дополнительных криптографических плагинов.

При выборе этого способа входа на странице авторизации браузер инициирует запуск приложения **КриптоАРМ**, установленного на устройстве пользователя. В открывшемся

приложении пользователь выбирает личный сертификат, после чего выполняется криптографическая операция подтверждения личности.

Результат проверки передается в систему **КриптоАРМ IDM**, где выполняется сопоставление с открытой частью ключа, сохраненной в профиле пользователя. Если данные совпадают, пользователь успешно проходит аутентификацию и получает доступ к системе.

Для использования этого способа входа необходимо:

- установить и настроить локальное приложение **КриптоАРМ** и криптопровайдер **КриптоПро CSP** на устройствах пользователей;
- создать и активировать провайдер **КриптоАРМ** в интерфейсе **КриптоАРМ IDM**;
- добавить открытые ключи сертификатов пользователей в их профили **КриптоАРМ IDM**;
- *опционально для коробочной версии*: настроить веб-сервер для централизованной валидации сертификатов и обработки запросов.

  🔍 Приложение **КриптоАРМ** можно скачать на официальном сайте разработчика: https://cryptoarm.ru/products/cryptoarm/

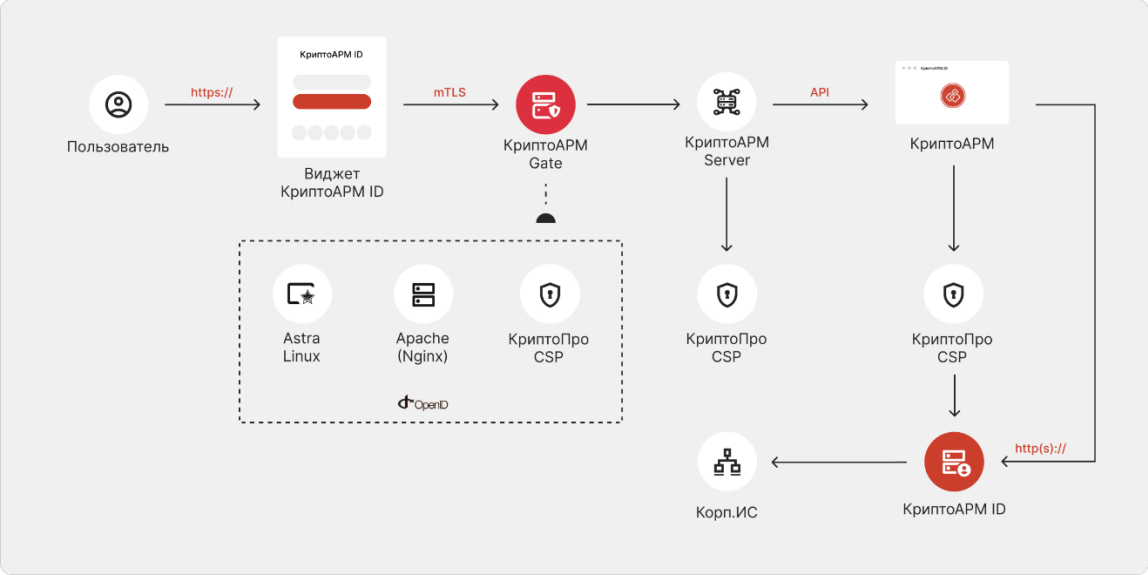
Варианты конфигурации (доступно для коробочной версии)

В зависимости от требований к инфраструктуре, вы можете выбрать подходящую схему развертывания:

- **Настройка с поддержкой ГОСТ.** Если ваша инфраструктура требует использования сертификатов с российскими криптоалгоритмами ГОСТ, необходимо настроить веб-сервер с поддержкой ГОСТ (например, Apache с модулями от КриптоПро).
- **Использование КриптоАРМ Gate с поддержкой ГОСТ.** Для сложных сценариев, требующих гибкой маршрутизации запросов и централизованной проверки цепочек сертификатов с алгоритмами ГОСТ, рекомендуется использовать продукт **КриптоАРМ Gate**. Он выступает в роли промежуточного звена, принимая запросы от приложения и перенаправляя их на указанный защищенный URL, при этом может выполнять дополнительную валидацию сертификатов.

Все варианты поддерживают стандартную процедуру аутентификации пользователей через приложение **КриптоАРМ**.

Пример двухсторонней аутентификации по протоколу **mTLS** с поддержкой ГОСТ и дополнительными политиками аутентификации **КриптоАРМ Gate**:



Настройка входа через КриптоАРМ для администраторов КриптоАРМ IDM

Шаг 1. Создание провайдера КриптоАРМ

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать** .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **КриптоАРМ**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, чтобы этот способ входа можно было добавить в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
   - **Защищенный URL (issuer)** — Адрес точки входа.
   - **Сопоставление атрибутов КриптоАРМ** — Сопоставление атрибутов профиля пользователя с данными сертификата в формате:

`given_name:givenname`, `family_name:sn`, `email:email`, `nickname:cn`. Подробнее о правилах →

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 2. Добавление провайдера КриптоАРМ на виджет

Чтобы пользователи увидели кнопку **КриптоАРМ** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **КриптоАРМ**.

Правила сопоставления атрибутов

Сопоставление атрибутов позволяет настроить, какие данные из клиентского сертификата будут записываться в поля профиля пользователя **КриптоАРМ IDM**. При каждой успешной аутентификации через **КриптоАРМ** система может автоматически обновлять данные профиля значениями из сертификата.

Допускается настройка сопоставления на основные и дополнительные поля профиля пользователя.

> 💡 Рекомендуется указывать только те поля, которые действительно должны обновляться из сертификата. Например, если `email` пользователей управляется отдельно, сопоставление `email:email` можно удалить.
>
> 📌 Названия атрибутов сертификата зависят от используемого удостоверяющего центра и структуры сертификатов. Перед настройкой рекомендуется проверить состав полей в сертификате пользователя.

Привязка клиентского сертификата для пользователей КриптоАРМ IDM

> 📌 Инструкция предназначена для пользователей, которым необходимо выполнить вход в систему через **КриптоАРМ**.

Шаг 1. Импорт личного сертификата в приложении КриптоАРМ

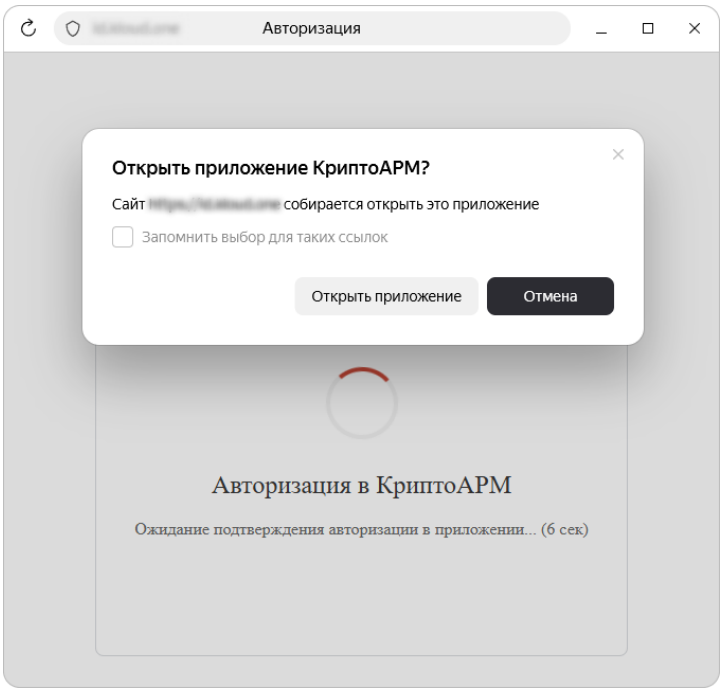
Перед привязкой сертификата в профиле необходимо установить личный сертификат в приложении КриптоАРМ.

Подробнее про установку сертификатов читайте в инструкции Как установить сертификаты в КриптоАРМ на портале документации cryptoarm.ru.

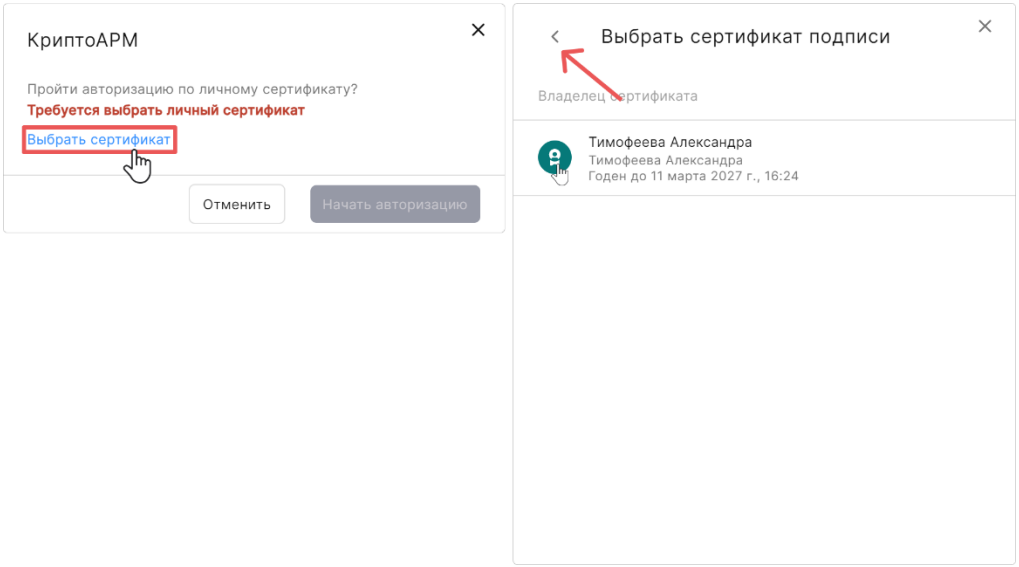
Шаг 2. Добавление идентификатора в профиль

1. Перейдите в свой **Профиль**.
2. Нажмите **Добавить** в блоке **Идентификаторы**.

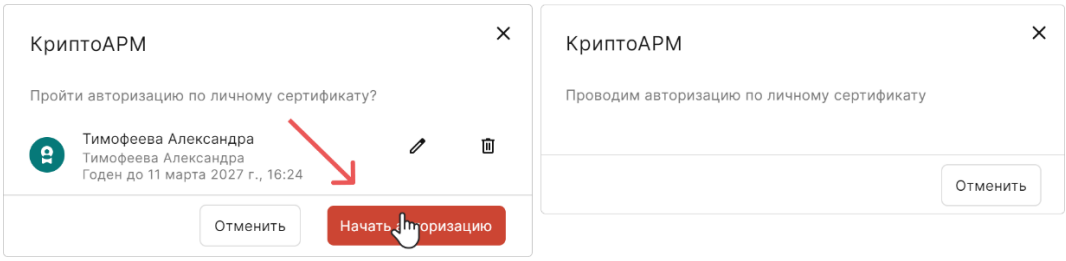
3. В открывшемся окне выберите способ входа **КриптоАРМ**.
4. При необходимости подтвердите открытие приложения **КриптоАРМ**.



5. Выберите сертификат, установленный на предыдущем шаге.



6. Нажмите **Начать авторизацию**.
7. При необходимости подключите токен к устройству и введите PIN-код.
8. Дождитесь окончания авторизации.



> 💡 **Совет**: Если идентификатор уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Шаг 3. Проверка

1. Перейдите на страницу входа с включенным способом входа **КриптоАРМ**.
2. Выберите иконку способа входа **КриптоАРМ**.
3. При необходимости подтвердите открытие приложения **КриптоАРМ**.
4. В открывшемся приложении укажите сертификат, привязанный в профиле.
5. Дождитесь окончания авторизации.

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.

Как подключить вход по электронной почте в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить аутентификацию с помощью электронной почты в своей организации или приложении. Способ входа Email будет использован для отправки email-уведомлений, таких как письма о регистрации, восстановлении пароля и других событиях.

Настройка входа через **Email** состоит из нескольких шагов:

- Шаг 1. Создание способа входа
- Шаг 2. Добавление на виджет
- Шаг 3. Настройка шаблонов уведомлений

Шаг 1. Создание способа входа

1. Перейдите в панель ID → вкладка **Настройки**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **Email**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Основной почтовый адрес** — Основной почтовый адрес, который будет использоваться для рассылки писем.
   - **Псевдоним отправителя (alias)** — Имя отправителя, которое будет отображаться в поле «От».
   - **Адрес сервера исходящей почты** — Адрес сервера исходящей почты.
   - **Порт сервера исходящей почты** — Порт сервера исходящей почты.
   - **Пароль почты** — Обычный пароль или пароль приложения, который создается в настройках аккаунта почтового сервиса.
   - **Время жизни кода подтверждения** — Время жизни кода подтверждения для почтового сервиса в секундах.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.

   💡 Для отправки тестового сообщения нажмите **Отправить**  . Эта функция позволяет проверить корректность настроек почтового сервиса (SMTP и других параметров) перед использованием его в рабочей среде.
7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 2. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через Email** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.

2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **Email**.

Шаг 3. Настройка шаблонов писем

После подключения способа входа **Email** система сможет отправлять пользователям письма: подтверждение регистрации, восстановление пароля, одноразовые коды подтверждения и другие уведомления.

Внешний вид и содержимое таких писем настраиваются через шаблоны уведомлений.

> 🔍 Подробнее о настройке шаблонов читайте в инструкции Настройка шаблонов email-уведомлений

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как подключить вход через HOTP в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить аутентификацию по одноразовым паролям **HOTP** к системе **КриптоАРМ IDM**.

Кому подходит эта инструкция:

- Администраторам — для настройки метода входа в системе.
- Пользователям — для привязки **HOTP** к своему профилю.

Настройка входа через **HOTP** состоит из нескольких ключевых этапов:

- Настройка аутентификации для администраторов
- Привязка HOTP для пользователей

Общая информация

HOTP (HMAC-based One-Time Password) — это алгоритм генерации одноразовых паролей на основе секретного ключа и счетчика, который увеличивается при каждом

успешном использовании кода. Это широко используется для двухфакторной аутентификации, добавляя уровень безопасности поверх стандартного логина и пароля.

Главное отличие **HOTP** от **HOTP** — коды не зависят от времени. Каждое использование кода увеличивает счетчик, и сервер проверяет введенный код относительно текущего значения счетчика.

> 💡 Для создания способа входа основанного на **TOTP** воспользуйтесь инструкцией Как подключить вход через TOTP.

Основные компоненты:

- **Сервер аутентификации** — сервер, который генерирует секретный ключ и проверяет введенные коды,учитывая счетчик.
- **Аутентификатор** — приложение, хранящее секретный ключ и текущий счетчик, генерирующее одноразовые пароли.
- **Секретный ключ** — общая для сервера и приложения база, используемая для генерации кодов.

Процесс работы HOTP

1. **Предварительная настройка**
   - Администратор создает способ входа **HOTP** и активирует его для виджетов нужных приложений.
   - Пользователь в своем профиле добавляет новый идентификатор **HOTP**, сканируя QR-код с секретным ключом через приложение-аутентификатор.
2. **Генерация и проверка кода**
   - Приложение-аутентификатор вычисляет одноразовый пароль на основе секретного ключа и текущего значения счетчика с использованием алгоритма `SHA1`, `SHA256` или `SHA512`.
   - Когда пользователь вводит код на форме входа, сервер вычисляет ожидаемый код по тому же секрету и текущему счетчику.
   - Если код совпадает, сервер увеличивает счетчик и предоставляет доступ пользователю.

> 🚨 **Важно**: **HOTP** не зависит от времени, поэтому синхронизация часов не требуется.

Настройка аутентификации для администраторов

Шаг 1. Создание способа входа

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .

4. Откроется окно со списком шаблонов.
5. Выберите шаблон **HOTP**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Количество цифр** — Количество цифр в одноразовом пароле (обычно 6).
   - **Начальное значение счётчика** — Текущий счетчик (не редактируемое).
   - **Алгоритм** — Алгоритм хеширования (`SHA1`, `SHA256` или `SHA512`) (обычно `SHA-1`).

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 2. Добавление провайдера HOTP на виджет

Чтобы пользователи увидели кнопку **HOTP** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **HOTP**.

Привязка HOTP для пользователей

> 📌 Инструкция предназначена для пользователей, которым необходимо выполнить вход в систему через **HOTP**.

Шаг 1. Установка приложения-аутентификатора

На ваше мобильное устройство необходимо установить приложение, которое генерирует HOTP-коды.

Шаг 2. Добавление HOTP-идентификатора в профиль

1. Перейдите в свой **Профиль**.
2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите способ входа **HOTP**.
4. Отсканируйте QR-код с помощью приложения-аутентификатора.
5. Введите код из приложения и подтвердите.

> 💡 **Совет**: Если идентификатор уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Шаг 3. Проверка

1. Перейдите на страницу входа с включенным способом входа **HOTP**.
2. Выберите иконку способа входа **HOTP**.
3. Откроется форма для ввода кода. Не закрывая страницу, откройте приложение-аутентификатор на своем телефоне.
4. Найдите сервис, соответствующий **КриптоАРМ IDM** (или названию приложения) и введите свой логин и 6-значный код в поле на форме входа.
5. Нажмите кнопку **Подтвердить**.

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как подключить вход через Mail.ru в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить аутентификацию с помощью аккаунта **Mail.ru** к системе **КриптоАРМ IDM**. Этот способ входа позволяет пользователям входить в приложения с помощью учётной записи сервиса **Mail.ru**.

Настройка входа через **Mail.ru** состоит из трёх ключевых этапов, которые выполняются в двух разных системах:

- Шаг 1. Настройка приложения в Mail.ru
- Шаг 2. Создание способа входа
- Шаг 3. Добавление на виджет
- Параметры способа входа
- Смотрите также

Шаг 1. Настройка приложения в Mail.ru

Перед настройкой способа входа в **КриптоАРМ IDM** необходимо зарегистрировать ваше приложение в кабинете разработчика **Mail.ru** и получить ключи доступа:

1. Зарегистрируйтесь или авторизуйтесь на сайте Mail.ru.

2. Перейдите в личный кабинет управления приложениями.

3. Нажмите **Создать приложение**.

4. В открывшейся форме создания укажите:

   - **Название проекта**,
   - **Фото** (при необходимости),
   - **Все redirect_uri** — возвратный URL #1 (`Redirect_uri`) в формате `https://<адрес инсталляции>/api/interaction/code`.

5. Нажмите кнопку **Подключить сайт**.

6. На следующем шаге формы в блоке **Платформы** выберите **Web**.

7. Нажмите **Сохранения изменения**.

8. Скопируйте значения полей **ID Приложения/Client ID** и **Секрет/Client Secret**. Они понадобятся при создании приложения в **КриптоАРМ IDM**.

Шаг 2. Создание способа входа

Теперь, имея ключи от **Mail.ru**, создадим соответствующий провайдер в системе **КриптоАРМ IDM**.

1. Перейдите в панель ID → вкладка **Настройки**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.

3. В открывшемся окне нажмите кнопку **Создать**  .

4. Откроется окно со списком шаблонов.
5. Выберите шаблон **Mail.ru**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры аутентификации

   - **Идентификатор ресурса (client_id)** — Вставьте скопированный **ID Приложения** (`Client ID`).
   - **Секретный ключ (client_secret)** — Вставьте скопированный **Секрет** (`Client Secret`).
   - **Возвратный URL(Redirect URI)** — Поле заполнится автоматически на основе вашего домена.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через Mail.ru** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **Mail.ru**.

Параметры способа входа

Основная информация

Название	Описание	Тип	Ограничения

Имя	Название, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**	Текст	Макс. 50 символов
Описание	Краткое описание, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**	Текст	Макс. 255 символов
Логотип	Изображение, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM** и виджете входа	JPG, GIF, PNG или WEBP	Макс. размер: 1 МБ

Параметры аутентификации

Название	Параметр	Описание
Идентификатор ресурса (client_id)	`Client_id`	ID приложения, созданного в **Mail.ru**
Секретный ключ (client_secret)	`Client_secret`	Сервисный ключ доступа приложения, созданного созданного в **Mail.ru**
Возвратный URL(Redirect URI) (не редактируемое)	`Redirect URI`	Адрес **КриптоАРМ IDM**, на который пользователь перенаправляется после аутентификации в стороннем сервисе

Дополнительные настройки

Название	Описание
Публичный способ входа	При активации настройки: - Способ входа станет доступен для добавления в другие приложения сервиса. - Способ входа станет доступен для добавления в качестве идентификатора внешнего сервиса в профиле пользователя.
Публичность	Задает уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как подключить вход по протоколу mTLS в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить аутентификацию **mTLS** к системе **КриптоАРМ IDM**.

Настройка входа через **mTLS** состоит из нескольких ключевых этапов:

1. Настройка mTLS-аутентификации для администраторов **КриптоАРМ IDM**
   - Шаг 1. Настройка Nginx для mTLS
   - Шаг 2. Создание провайдера mTLS
   - Шаг 3. Добавление провайдера mTLS на виджет
2. Привязка клиентского сертификата для пользователей **КриптоАРМ IDM**
   - Шаг 1. Установка клиентского сертификата в браузере
   - Шаг 2. Добавление идентификатора в профиль
   - Шаг 3. Проверка

Общая информация

mTLS (Mutual TLS) — способ аутентификации, основанный на взаимной проверке сертификатов клиента и сервера.

Этот способ обеспечивает высокий уровень доверия и безопасности, так как вход в систему возможен только при наличии у пользователя действительного сертификата, подписанного доверенным центром сертификации (CA).

mTLS особенно полезен для корпоративных или чувствительных систем, где требуется минимизировать риск несанкционированного доступа.

Процесс работы mTLS

1. **Инициация соединения:** Клиент отправляет запрос к серверу **КриптоАРМ IDM**.
2. **Запрос сертификата клиента:** Сервер требует предоставления клиентского сертификата.
3. **Отправка клиентского сертификата:** Клиент предоставляет свой сертификат, подписанный доверенным CA.
4. **Проверка сертификата на сервере:**
   - Сервер сверяет сертификат с основным CA.
   - Проверяет срок действия, подпись и соответствие требованиям безопасности.
5. **Аутентификация пользователя:**
   - Если сертификат валиден, сервер сопоставляет его с учетной записью пользователя и разрешает доступ.
   - Если сертификат невалиден или отсутствует — доступ отклоняется.
6. **Установление защищенного канала:** После успешной проверки сертификата устанавливается **шифрованное соединение**, и пользователь получает доступ.

Настройка mTLS-аутентификации для администраторов КриптоАРМ IDM

Для работы **mTLS** необходимо:

- создать и активировать провайдер **mTLS** в интерфейсе **КриптоАРМ IDM**;
- установить клиентские сертификаты на устройства пользователей и в их профили **КриптоАРМ IDM**;
- *опционально для коробочной версии*: настроить веб-сервер **Nginx**, чтобы он принимал только запросы, подписанные доверенным сертификатом.

Шаг 1. Настройка Nginx для mTLS

Перед добавлением провайдера в **КриптоАРМ IDM** необходимо подготовить конфигурацию **Nginx**:

1. Откройте файл конфигурации `nginx.local.conf`.

2. Добавьте новый `server` блок:

   Пример конфигурации:

```
server {
   server_name local.trusted.com;
   listen 3443 ssl;

   # Сертификаты сервера
   ssl_certificate         certs/local.trusted.com.pem;
   ssl_certificate_key     certs/local.trusted.com-key.pem;

   # Сертификат корневого CA для проверки клиентских сертификатов
   ssl_client_certificate  certs/ca-bundle.crt;
   ssl_verify_client on;
   ssl_verify_depth 3;

   # Настройки сессии и протоколов
   ssl_session_timeout 10m;
   ssl_session_cache shared:SSL:10m;
   ssl_protocols TLSv1.2 TLSv1.3;

   # Ограничение доступа на основной путь, mTLS разрешен только для
/api/mtls
   location / {
       return 404 "mTLS endpoints only. Use port 443 for regular access.";
   }

   # Настройка проксирования запросов на backend
   location /api/mtls {
       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-Proto $scheme;
```

```
        # Передача информации о клиентском сертификате
        proxy_set_header X-SSL-Client-Verify $ssl_client_verify;
        proxy_set_header X-SSL-Client-DN $ssl_client_s_dn;
        proxy_set_header X-SSL-Client-Serial $ssl_client_serial;
        proxy_set_header X-SSL-Client-Fingerprint $ssl_client_fingerprint;
        proxy_set_header X-SSL-Client-Issuer $ssl_client_i_dn;

        # Проксирование на backend
        proxy_pass http://backend;
        proxy_redirect off;
    }
}
```

3. Перезапустите **Nginx** после внесения изменений.

Описание параметров

Параметр	Назначение
`ssl_certificate`	Сертификат сервера, используемый для HTTPS.
`ssl_certificate_key`	Закрытый ключ сервера.
`ssl_client_certificate`	Корневой сертификат CA для проверки клиентских сертификатов.
`ssl_verify_client on`	Включение обязательной проверки клиентских сертификатов.
`ssl_verify_depth`	Максимальная глубина цепочки проверки сертификатов клиента.
`ssl_session_timeout`	Время жизни SSL-сессии.
`ssl_protocols`	Разрешённые версии TLS.
`proxy_set_header X-SSL-Client-*`	Передача информации о клиентском сертификате на backend.

- Разместите серверные сертификаты (`.pem` и ключ) и корневой CA (`ca-bundle.crt`) в удобной директории, например `certs/`.
- Путь к сертификатам укажите в конфигурации **Nginx**.

Шаг 2. Создание провайдера mTLS

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **mTLS**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.

- **Описание** (опционально) — Краткое описание.
- **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

Дополнительные настройки

- **Публичный способ входа** — Включите, чтобы этот способ входа можно было добавить в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
- **Точка входа mTLS соединения (issuer)** — Адрес точки входа.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление провайдера mTLS на виджет

Чтобы пользователи увидели кнопку **mTLS** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **mTLS**.

Привязка клиентского сертификата для пользователей КриптоАРМ IDM

📌 Инструкция предназначена для пользователей, которым необходимо выполнить вход в систему через **mTLS**.

Шаг 1. Установка клиентского сертификата в браузере

Перед установкой убедитесь, что у вас есть файл сертификата в формате `.p12` или `.pfx`.

Этот файл должен содержать:

- ваш персональный сертификат,
- закрытый ключ,
- и цепочку доверия (если требуется).

Установка в Google Chrome / Microsoft Edge

1. Откройте браузер **Chrome** или **Edge**.
2. Перейдите в **Настройки** → **Конфиденциальность и безопасность**.
3. Найдите раздел **Безопасность**.
4. Нажмите **Управление сертификатами**.
5. Перейдите на вкладку **Личное** / **Ваши сертификаты**.
6. Нажмите **Импорт…**.
7. В мастере импорта нажмите **Далее**.

8. Нажмите **Обзор** и выберите ваш файл `.p12` или `.pfx`.
9. Введите пароль, который вы получили с сертификатом.
10. Выберите **Поместить все сертификаты в следующее хранилище**.
11. Нажмите **Обзор** и выберите **Личное**.
12. Нажмите **Далее** → **Готово**.
13. При появлении предупреждения безопасности нажмите **Да**.

После успешной установки сертификат появится в списке на вкладке **Личное** / **Ваши сертификаты**.

Установка в Mozilla Firefox

1. Откройте меню **Firefox** → **Настройки**
2. Перейдите в раздел **Приватность и защита**
3. Прокрутите вниз до **Сертификаты**
4. Нажмите **Показать сертификаты…**
5. Перейдите на вкладку **Ваши сертификаты**
6. Нажмите **Импорт…**
7. Выберите ваш файл `.p12` или `.pfx`
8. Введите пароль к сертификату
9. Нажмите **ОК**

После успешной установки сертификат появится в списке на вкладке **Ваши сертификаты**.

> ⚠️ Сертификаты нужно устанавливать только на доверенные устройства и строго следить за сохранностью пароля.

> 💡 После установки сертификата, при входе через **mTLS**, браузер автоматически предложит выбрать соответствующий сертификат для аутентификации.

Шаг 2. Добавление идентификатора в профиль

1. Перейдите в свой **Профиль**.
2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите способ входа **mTLS**.
4. Выберите сертификат, установленный на предыдущем шаге.

> 💡 **Совет**: Если идентификатор уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Шаг 3. Проверка

1. Перейдите на страницу входа с включенным способом входа **mTLS**.
2. Выберите иконку способа входа **mTLS**.
   - **Первый вход**: система может запросить выбор клиентского сертификата.
   - **Повторные входы**: аутентификация выполняется автоматически с использованием ранее выбранного сертификата.

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.

Как подключить вход через OpenID Connect в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить аутентификацию **OpenID Connect** к системе **КриптоАРМ IDM**.

Настройка входа через **OpenID Connect** состоит из трёх ключевых этапов, которые выполняются в двух разных системах:

- Шаг 1. Настройка на стороне внешней системы
- Шаг 2. Создание способа входа
- Шаг 3. Добавление на виджет
- Описание параметров
- Смотрите также

Шаг 1. Настройка на стороне внешней системы

1. Создайте приложение во внешнем сервисе идентификации.
2. Скопируйте значения полей **ID Приложения/Client ID** и **Секрет/Client Secret**. Они понадобятся при создании приложения в **КриптоАРМ IDM**.

Шаг 2. Создание способа входа

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.

3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **OpenID Connect**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры аутентификации

   - **Идентификатор ресурса (client_id)** — Вставьте скопированный **ID Приложения** (`Client ID`).
   - **Секретный ключ (client_secret)** — Вставьте скопированный **Секрет** (`Client Secret`).
   - **Возвратный URL(Redirect URI)** — Поле заполнится автоматически на основе вашего домена.
   - **Базовый адрес сервера авторизации (issuer)** — Адрес сервиса внешней идентификации.
   - **Адрес авторизации (authorization_endpoint)** — Адрес, на который пользователь переадресовывается для авторизации.
   - **Адрес выдачи токена (token_endpoint)** — Ресурс, обеспечивающий выдачу токенов.
   - **Адрес получения информации о пользователе (userinfo_endpoint)** — Ресурс, который возвращает информацию о текущем пользователе.
   - **Запрашиваемые разрешения (scopes)** — Перечень разрешений, которые должны быть получены при обращении к поставщику идентификации. Для добавления разрешения введите его имя и нажмите **Enter**.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через OpenID Connect** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **OpenID Connect**.

Описание параметров

Основная информация

Название	Описание	Тип	Ограничения
Имя	Название, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**	Текст	Макс. 50 символов
Описание	Краткое описание, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**	Текст	Макс. 255 символов
Логотип	Изображение, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM** и виджете входа	JPG, GIF, PNG или WEBP	Макс. размер: 1 МБ

Параметры аутентификации

Название	Параметр	Описание
Идентификатор ресурса (client_id)	`client_id`	ID приложения, созданного во внешней системе
Секретный ключ (client_secret)	`client_secret`	Сервисный ключ доступа приложения, созданного созданного на стороне внешней системы
Возвратный URL(Redirect URI) (не редактируемое)	`redirect URI`	Адрес **КриптоАРМ IDM**, на который пользователь перенаправляется после аутентификации в стороннем сервисе
Базовый адрес сервера авторизации (issuer)	`issuer`	Адрес сервиса внешней идентификации
Адрес авторизации (authorization_endpoint)	`authorization_endpoint`	Адрес, на который пользователь переадресовывается для авторизации
Адрес выдачи токена (token_endpoint)	`token_endpoint`	Ресурс, обеспечивающий выдачу токенов

Адрес получения информации о пользователе (userinfo_endpoint)	`userinfo_endpoint`	Ресурс, который возвращает информацию о текущем пользователе
Запрашиваемые разрешения (scopes)	-	Перечень разрешений, которые должны быть получены при обращении к поставщику идентификации. Для добавления разрешения введите его имя и нажмите **Enter**.

Дополнительные настройки

Название	Описание
Публичный способ входа	При активации настройки: - Способ входа станет доступен для добавления в другие приложения сервиса. - Способ входа станет доступен для добавления в качестве идентификатора внешнего сервиса в профиле пользователя.
Публичность	Задает уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.

Как подключить вход через TOTP в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить аутентификацию по одноразовым паролям **TOTP** к системе **КриптоАРМ IDM**.

Кому подходит эта инструкция:

- **Администраторам** — для настройки метода входа в системе.
- **Пользователям** — для привязки **TOTP** к своему профилю.

Настройка входа через **TOTP** состоит из нескольких ключевых этапов:

- Настройка аутентификации для администраторов
- Привязка TOTP для пользователей

Общая информация

TOTP (Time-based One-Time Password) — это алгоритм генерации одноразовых паролей, действительных в течение короткого промежутка времени.

> 💡 Для создания способа входа основанного на **HOTP** воспользуйтесь инструкцией Как подключить вход через HOTP.

Главное отличие **TOTP** от **HOTP** — генерация пароля на основе текущего времени. При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (обычно — 30 секунд).

Основные компоненты:

- **Сервер аутентификации** — сервер, который генерирует секретный ключ и проверяет введенные коды.
- **Аутентификатор** — приложение, хранящее секретный ключ и генерирующее текущий OTP.
- **Секретный ключ** — общая для сервера и приложения база, используемая для генерации кодов.

Процесс работы TOTP

1. **Предварительная настройка**
   - Администратор создает способ входа **TOTP** и активирует его для виджетов нужных приложений.
   - Пользователь в своем профиле добавляет новый идентификатор **TOTP**, сканируя QR-код с секретным ключом через приложение-аутентификатор.
2. **Генерация и проверка кода**
   - Приложение-аутентификатор вычисляет одноразовый пароль на основе секретного ключа и текущего временного интервала (обычно 30 секунд) с использованием алгоритма `SHA1`, `SHA256` или `SHA512`.
   - Когда пользователь вводит код на форме входа, сервер повторно вычисляет ожидаемый код по тому же секрету и текущему времени.
   - Если введенный код совпадает с ожидаемым, пользователю предоставляется доступ.

> 🚨 **Важно**: Время на устройстве пользователя и на сервере должно быть синхронизировано. Несовпадение времени — самая частая причина отказа кода. Для компенсации небольшой разницы во времени сервер может принимать коды из соседних временных интервалов (обычно ±1 интервал).

Настройка аутентификации для администраторов

Шаг 1. Создание способа входа

1. Перейдите в панель ID → вкладка **Настройки**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **TOTP**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Количество цифр** — Количество цифр в одноразовом пароле (обычно 6).
   - **Период действия** — Время действия одноразового пароля в секундах (рекомендуется 30).
   - **Алгоритм** — Алгоритм хеширования (`SHA1`, `SHA256` или `SHA512`) (обычно `SHA-1`).

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 2. Добавление провайдера TOTP на виджет

Чтобы пользователи увидели кнопку **TOTP** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **TOTP**.

Привязка TOTP для пользователей

📌 Инструкция предназначена для пользователей, которым необходимо выполнить вход в систему через **TOTP**.

Шаг 1. Установка приложения-аутентификатора

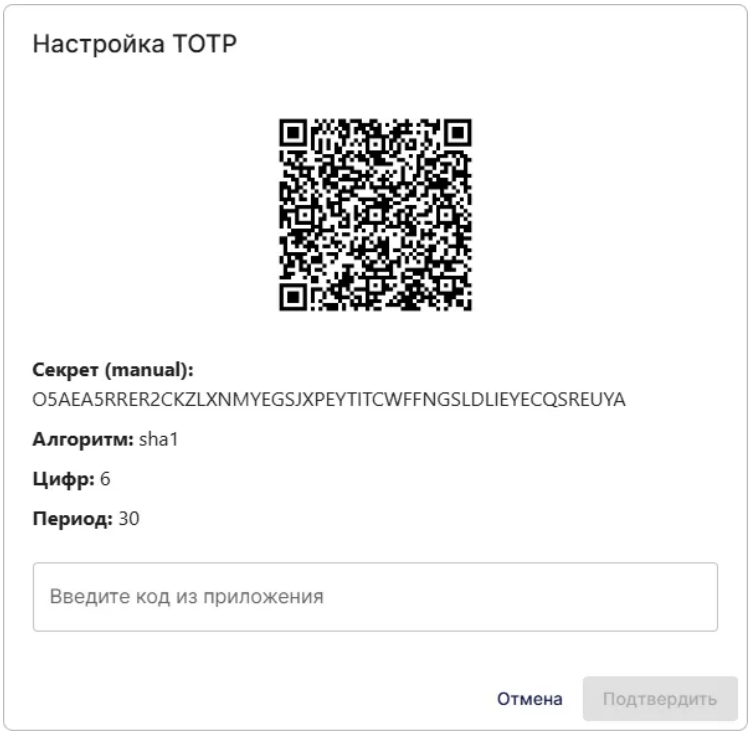
На ваше мобильное устройство необходимо установить приложение, которое генерирует TOTP-коды.

> 💡 Убедитесь, что время на вашем мобильном устройстве настроено автоматически (через сеть). Неправильное время — самая частая причина того, что коды не принимаются.

Шаг 2. Добавление TOTP-идентификатора в профиль

1. Перейдите в свой **Профиль**.
2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите способ входа **TOTP**.
4. Отсканируйте QR-код с помощью приложения-аутентификатора.



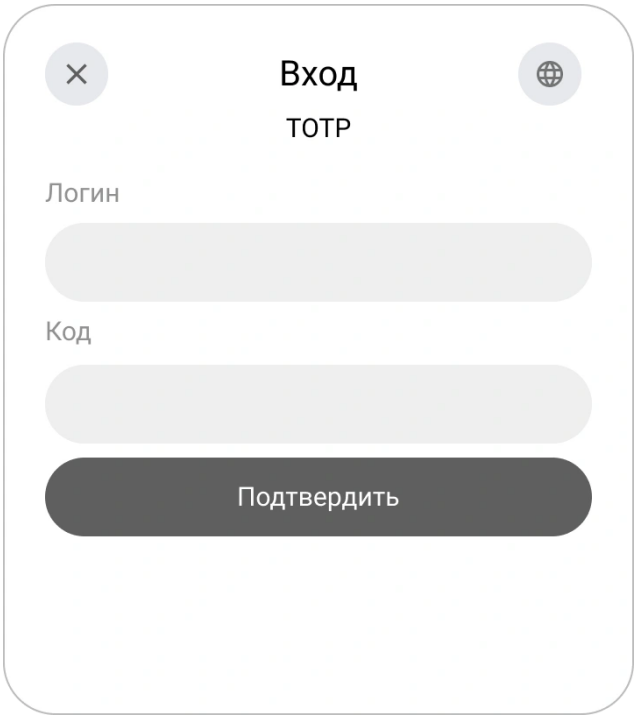
5. Введите код из приложения и подтвердите.

> 💡 **Совет**: Если идентификатор уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Шаг 3. Проверка

1. Перейдите на страницу входа с включенным способом входа **TOTP**.

2. Выберите иконку способа входа **TOTP**.
3. Откроется форма для ввода кода.
4. Введите свой логин.



5. Не закрывая страницу, откройте приложение-аутентификатор на своем телефоне. Скопируйте 6-значный код и вставьте его в форму.
6. Нажмите кнопку **Подтвердить**.

   Если код не принимается: Убедитесь, что время на вашем телефоне и сервере синхронизировано. Попробуйте подождать генерации следующего кода (новый появится через 30 секунд). Если проблема не исчезает, обратитесь к администратору.

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.

- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как подключить вход через ВКонтакте в КриптоАРМ IDM

📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить аутентификацию с помощью аккаунта **Вконтакте** к системе **КриптоАРМ IDM**. Этот способ входа позволяет пользователям входить в приложения с помощью учётной записи сервиса **Вконтакте**.

Настройка входа через **Вконтакте** состоит из трёх ключевых этапов, которые выполняются в двух разных системах:

- Шаг 1. Настройка приложения во Вконтакте
- Шаг 2. Создание способа входа
- Шаг 3. Добавление на виджет
- Описание параметров
- Смотрите также

Шаг 1. Настройка приложения во Вконтакте

Перед настройкой способа входа в **КриптоАРМ IDM** необходимо зарегистрировать ваше приложение в кабинете разработчика **Вконтакте** и получить ключи доступа:

1. Зарегистрируйтесь или авторизуйтесь в сети ВКонтакте.

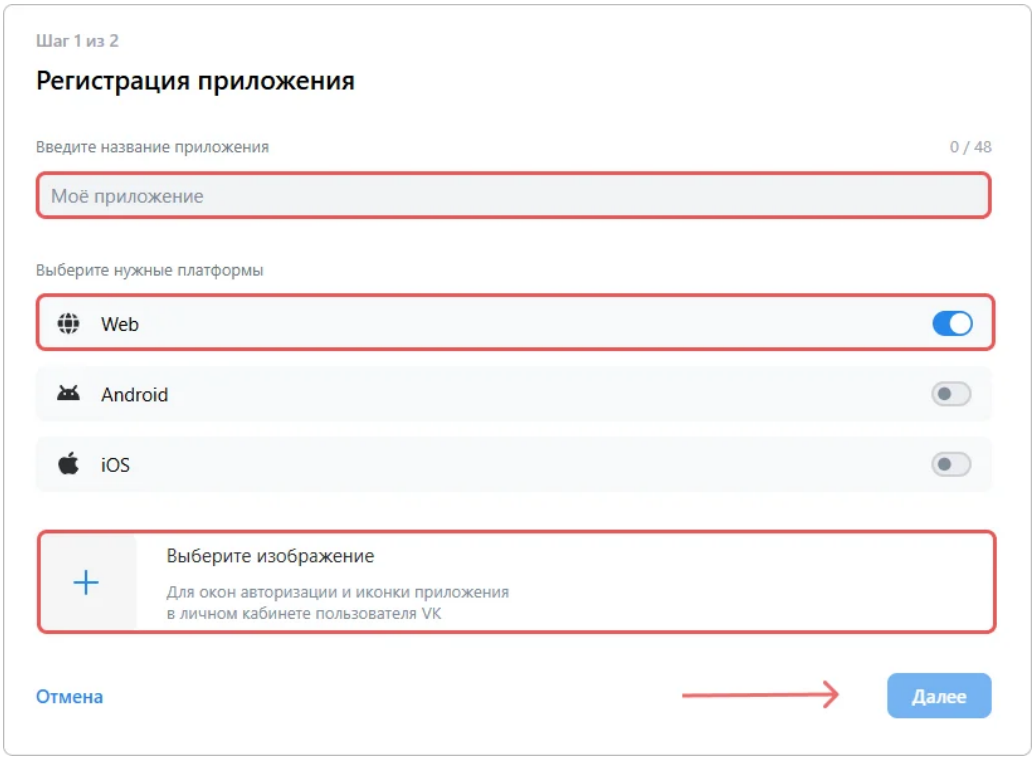
2. Откройте dev.vk.com и перейдите по ссылке для создания приложения с типом **Сайт**.

3. На первом шаге формы регистрации приложения:

   – Введите название приложения;

   – Выберите платформу **Web**;

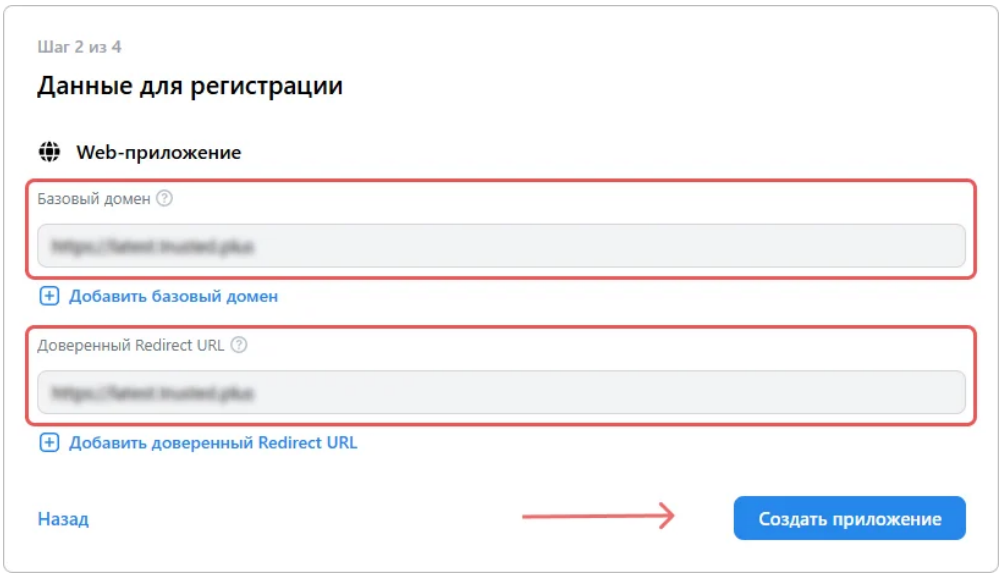
   – Добавьте изображение (при необходимости).



4. На втором шаге формы регистрации приложения укажите:

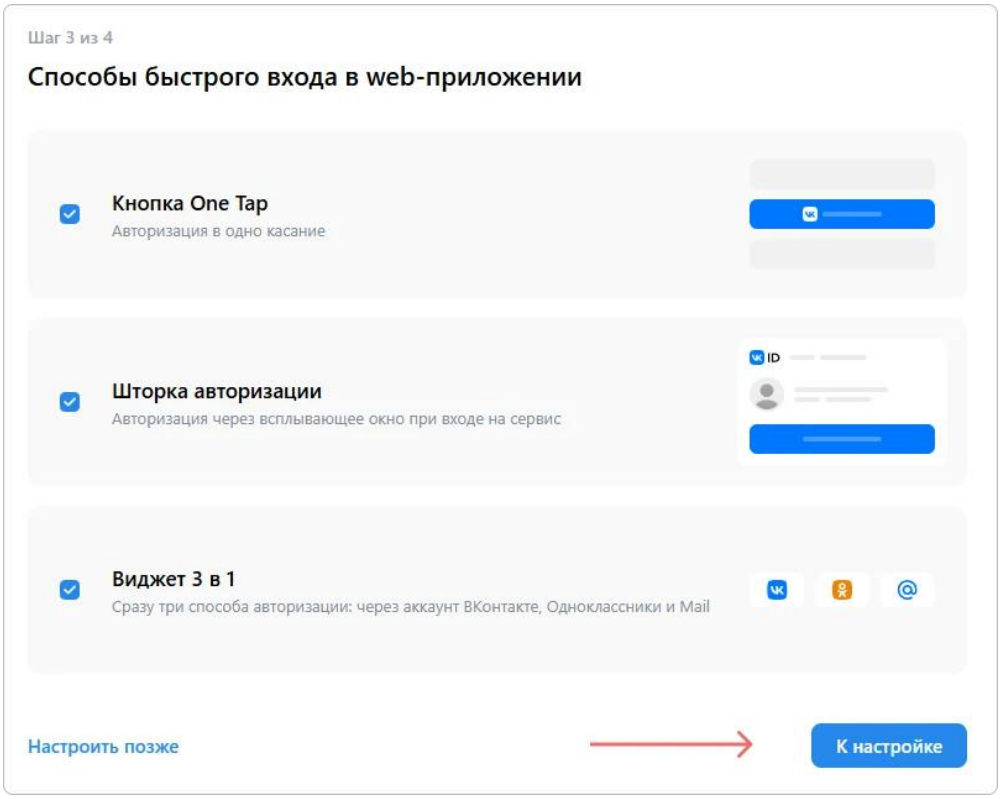
   – **Базовый домен** - адрес инсталляции сервиса **КриптоАРМ IDM**;

   – **Доверенный Redirect URL** - возвратный URL (`Redirect_uri`) в формате `https://<адрес инсталляции>/api/interaction/code`.

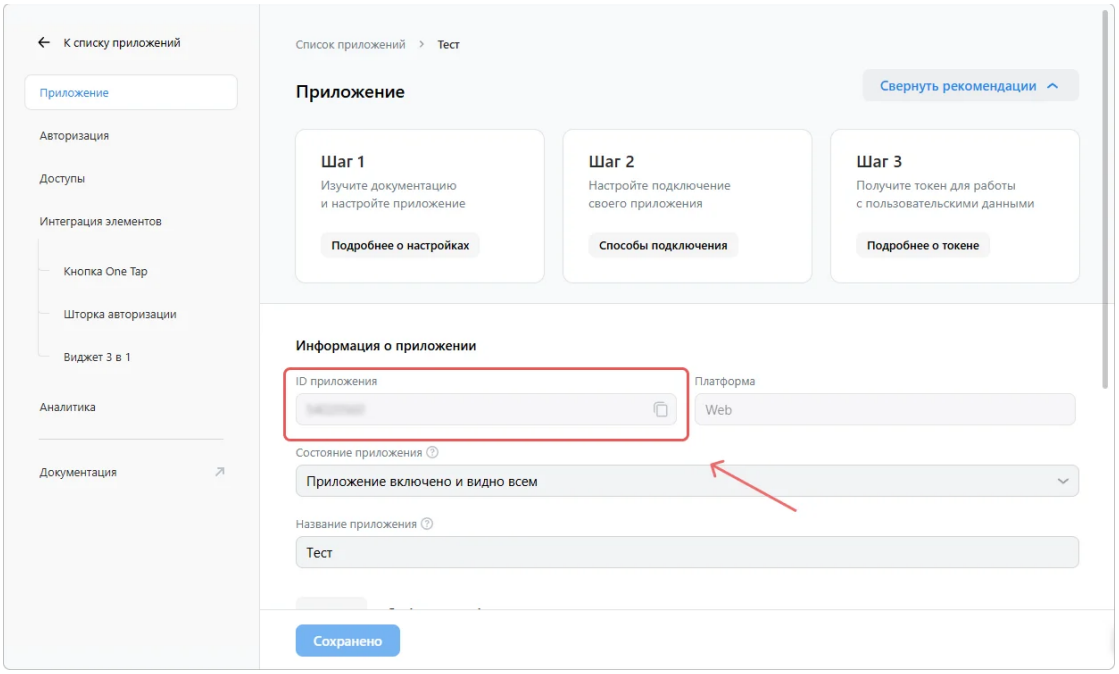


5. Нажмите **Создать приложение**.

6. На третьем шаге с настройкой способов быстрого входа нажмите **К настройке**.



7. Скопируйте значения полей **ID Приложения/Client ID** и **Секрет/Client Secret**. Они понадобятся при создании приложения в **КриптоАРМ IDM**.



Шаг 2. Создание способа входа

Теперь, имея ключи от **Вконтакте**, создадим соответствующий провайдер в системе **КриптоАРМ IDM**.

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **Вконтакте**.
6. Заполните форму создания:

   Основная информация

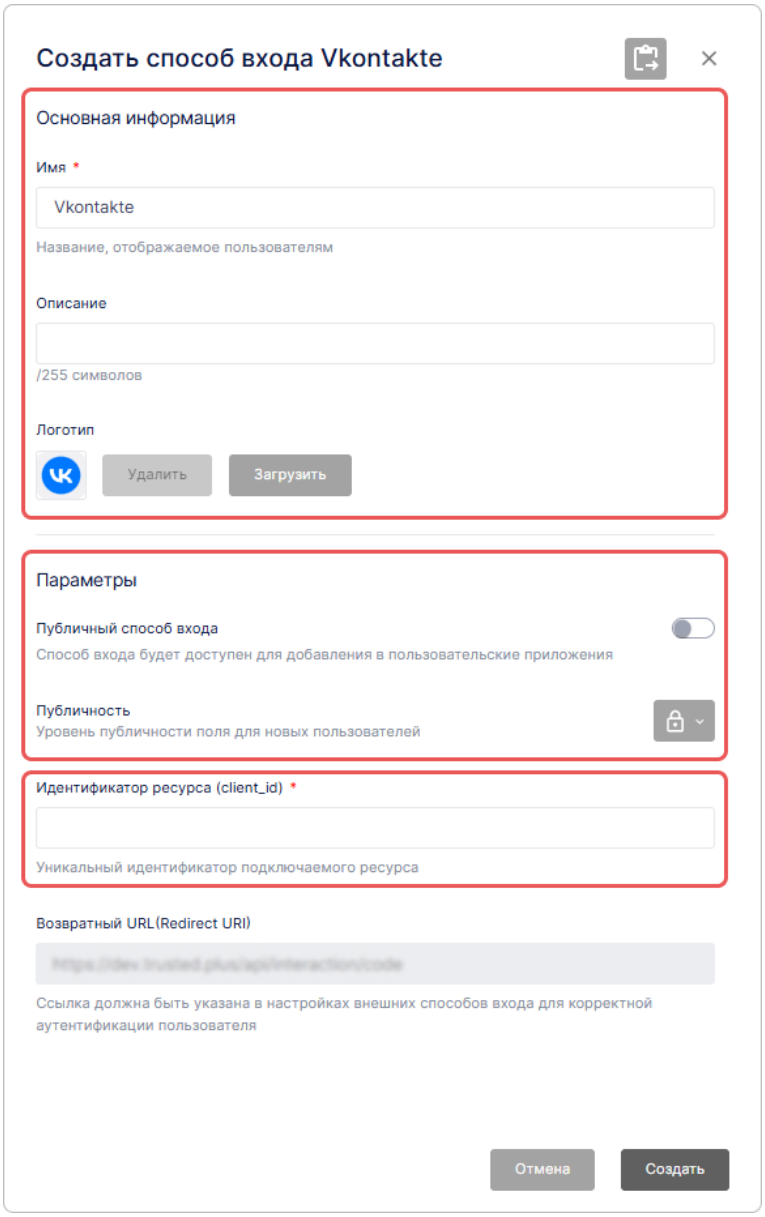
   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку или будет использована стандартная.

   Параметры аутентификации

   - **Идентификатор ресурса (client_id)** — Вставьте скопированный **ID Приложения** (`Client ID`).
   - **Секретный ключ (client_secret)** — Вставьте скопированный **Секрет** (`Client Secret`).
   - **Возвратный URL(Redirect URI)** — Поле заполнится автоматически на основе вашего домена.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.



7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через Вконтакте** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **Вконтакте**.

Описание параметров

Основная информация

Название	Описание	Тип	Ограничения
Имя	Название, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**	Текст	Макс. 50 символов
Описание	Краткое описание, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**	Текст	Макс. 255 символов
Логотип	Изображение, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM** и виджете входа	JPG, GIF, PNG или WEBP	Макс. размер: 1 МБ

Параметры аутентификации

Название	Параметр	Описание
Идентификатор ресурса (client_id)	`Client_id`	ID приложения, созданного в **ВКонтакте**
Возвратный URL(Redirect URI) (не редактируемое)	`Redirect URI`	Адрес **КриптоАРМ IDM**, на который пользователь перенаправляется после аутентификации в стороннем сервисе

Дополнительные настройки

Название	Описание
Публичный способ входа	При активации настройки: - Способ входа станет доступен для добавления в другие приложения сервиса. - Способ входа станет доступен для добавления в качестве идентификатора внешнего сервиса в профиле пользователя.
Публичность	Задает уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.

- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как подключить вход по протоколу WebAuthn в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить аутентификацию **WebAuthn** к системе **КриптоАРМ IDM**.

Содержание:

- Общая информация
- Настройка WebAuthn-аутентификации для администраторов
- Добавление ключа для пользователя
- Смотрите также

Общая информация

WebAuthn (Web Authentication) — стандарт аутентификации, который позволяет пользователям входить в систему без пароля, используя надёжные методы проверки:

- биометрия (Face ID, Touch ID);
- аппаратные ключи безопасности;
- встроенные модули безопасности устройств.

WebAuthn входит в спецификацию **FIDO2**, поддерживается всеми современными браузерами.

> 🔐 **WebAuthn** можно использовать как основной способ входа, либо как дополнительный — для многофакторной аутентификации.

Процесс работы WebAuthn

1. **Регистрация пользователя:**
   - Пользователь создает ключ аутентификации.
   - Устройство генерирует пару ключей: публичный ключ сохраняется в системе, а приватный остается только у пользователя.
2. **Инициация входа:**
   - Пользователь выбирает способ входа **WebAuthn** на веб-ресурсе.
   - Сервер отправляет вызов (`challenge`) для подтверждения идентичности.
3. **Аутентификация пользователя:**
   - Устройство или токен подписывает `challenge` приватным ключом.
   - Сервер проверяет подпись с помощью сохраненного публичного ключа.
   - Если подпись корректна — пользователь получает доступ.

4. **Установление защищенного канала:** После успешной аутентификации пользователь входит в систему без передачи пароля через сеть.

Настройка WebAuthn-аутентификации для администраторов

Шаг 1. Создание способа входа

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **WebAuthn**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, чтобы этот способ входа можно было добавить в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
   - **Использовать внешние ключи безопасности** — Включите, если необходимо использовать только внешние ключи (NFC, QR, USB-устройства и т.п.). По умолчанию применяется только встроенная биометрия устройства (Face ID, Touch ID, Windows Hello и т.п.).
7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 2. Добавление провайдера WebAuthn на виджет

Чтобы пользователи увидели кнопку **WebAuthn** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **WebAuthn**.

Добавление ключа для пользователя

Шаг 1. Добавление ключа на устройство

Регистрация ключа **WebAuthn** — это процесс, при котором создаётся связка публичного и приватного ключей и привязывается к конкретному пользователю.

Чтобы использовать вход по **WebAuthn**, пользователю необходимо сначала зарегистрировать ключ — это может быть встроенный аутентификатор (например, **Touch ID**, **Face ID** или **Windows Hello**), либо внешний физический ключ безопасности.

Во время добавления ключа создаётся уникальная криптографическая пара — **публичный** и **приватный ключи**.

- Приватный ключ надёжно сохраняется на устройстве пользователя и никогда не передаётся в сеть.
- Публичный ключ сохраняется на сервере **КриптоАРМ IDM** и используется для последующей проверки подлинности при входе.

После регистрации ключа пользователю необходимо добавить идентификатор **WebAuthn** в своем профиле **КриптоАРМ IDM**.

Шаг 2. Добавление идентификатора в профиль

1. Перейдите в свой **Профиль**.
2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите способ входа **WebAuthn**.
4. В системном окне укажите ранее зарегистрированный ключ.

> 💡 **Совет**: Если идентификатор уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.

- **Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.**

Как подключить вход через Яндекс в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке способов входа. Подробнее читайте в инструкции Способы входа и настройка виджета.

В этом руководстве вы узнаете, как подключить аутентификацию с помощью аккаунта **Яндекс** к системе **КриптоАРМ IDM**. Этот способ входа позволяет пользователям входить в приложения с помощью учётной записи сервиса **Яндекс**.

Настройка входа через **Яндекс** состоит из трёх ключевых этапов, которые выполняются в двух разных системах:

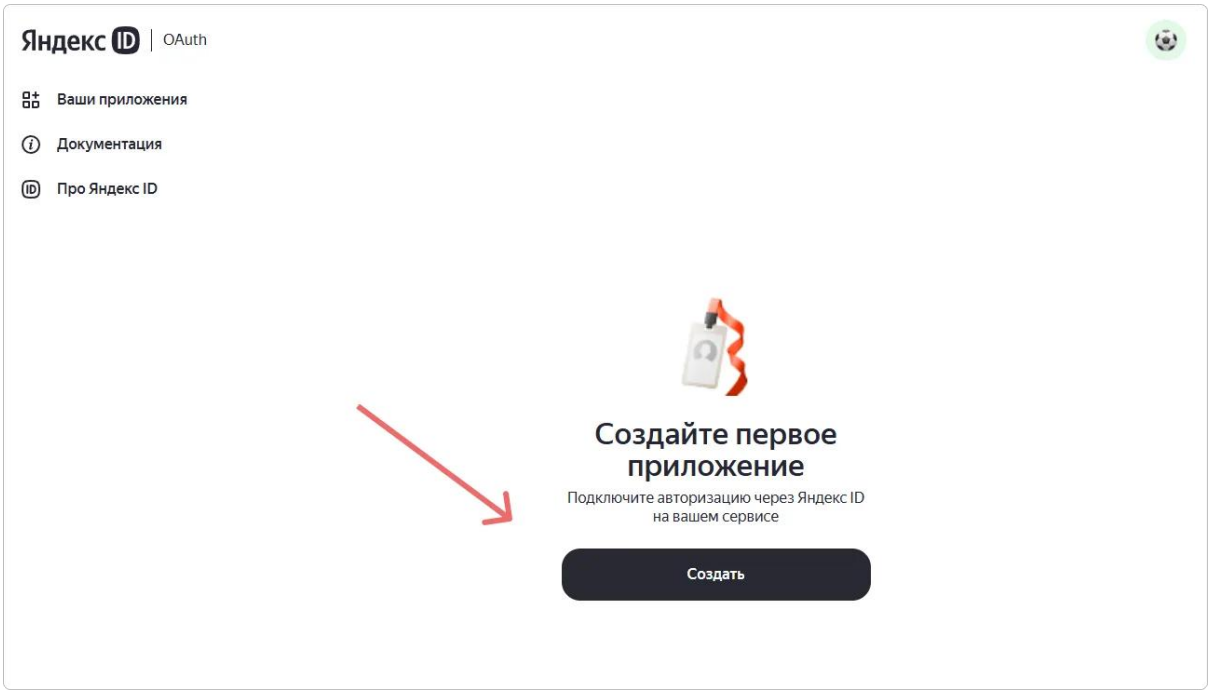
- Шаг 1. Настройка приложения в Яндекс
- Шаг 2. Создание способа входа
- Шаг 3. Добавление на виджет
- Описание параметров
- Смотрите также

Шаг 1. Настройка приложения в Яндекс

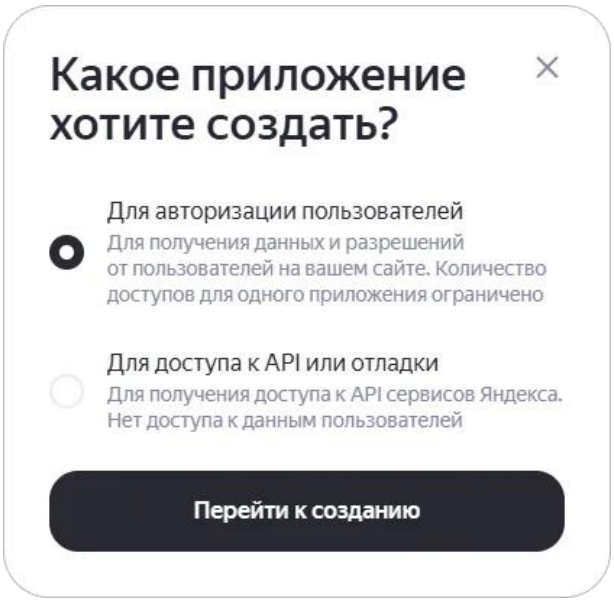
Перед настройкой способа входа в **КриптоАРМ IDM** необходимо зарегистрировать ваше приложение в кабинете разработчика **Яндекс** и получить ключи доступа:

1. Зарегистрируйтесь или авторизуйтесь в сервисе Яндекс OAuth.

2. Нажмите кнопку **Создать**.



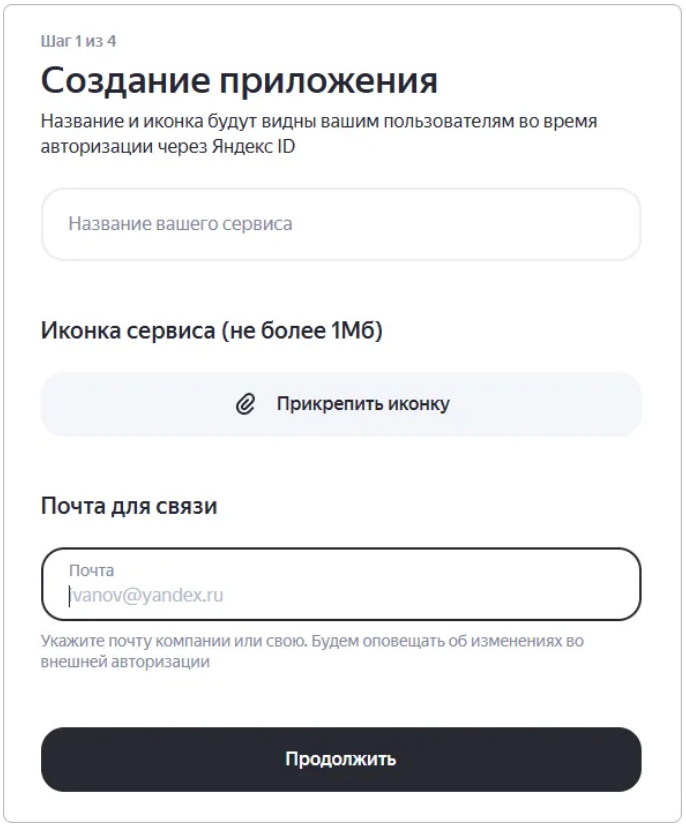
3. Выберите вариант **Для авторизации пользователей** и нажмите **Перейти к созданию**.



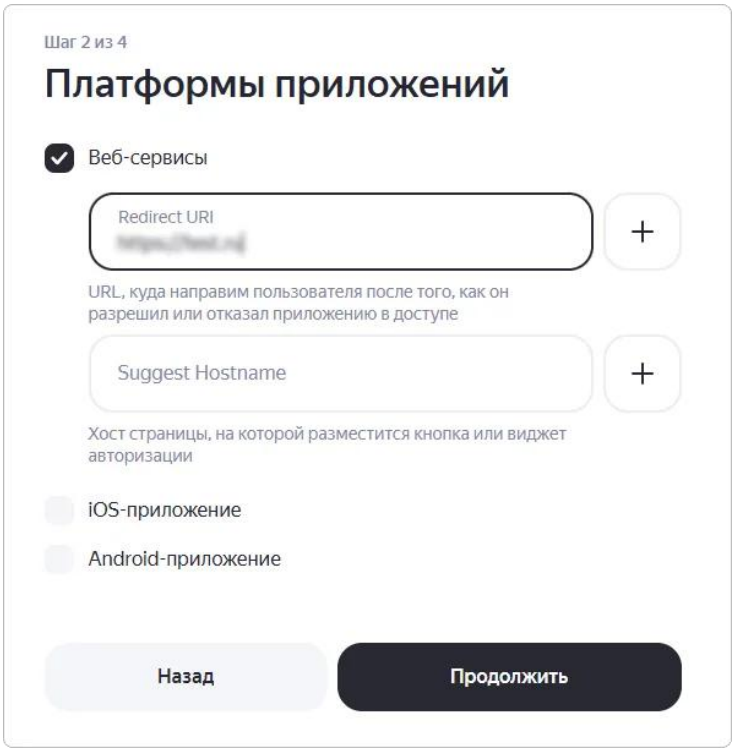
4. Откроется форма создания.

5. На первом шаге формы укажите:

   - **Название сервиса**,
   - **Иконку сервиса**,
   - **Электронную почту**.

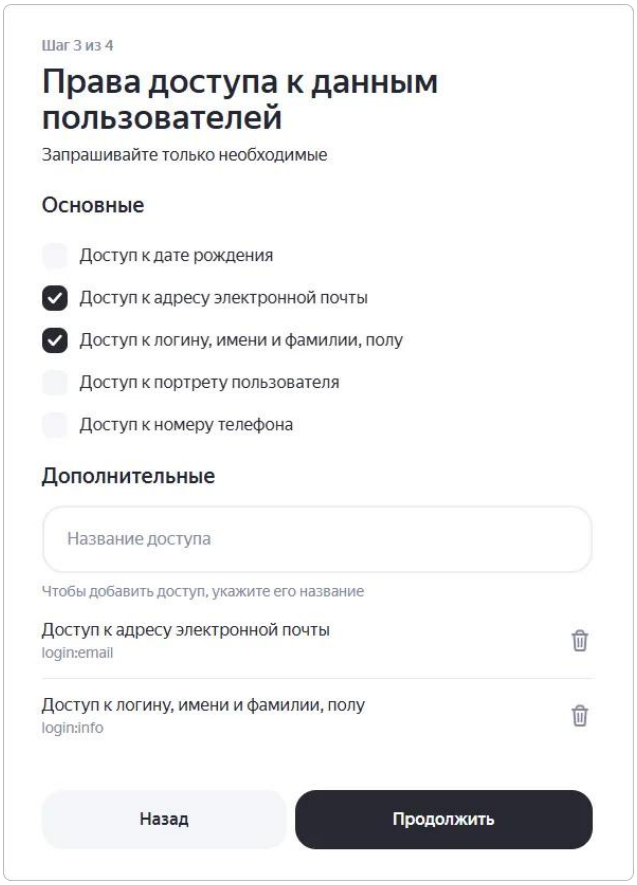


6. На втором шаге установите чекбокс **Веб-сервисы** и укажите **Возвратный URL #1** (`Redirect_uri`) в формате `https://<your-domain>/api/interaction/code`.

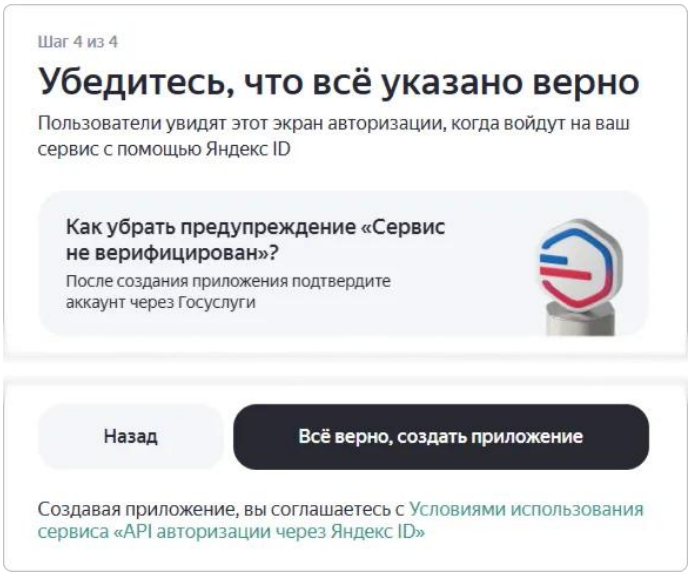


7. На третьем шаге установите чекбоксы:

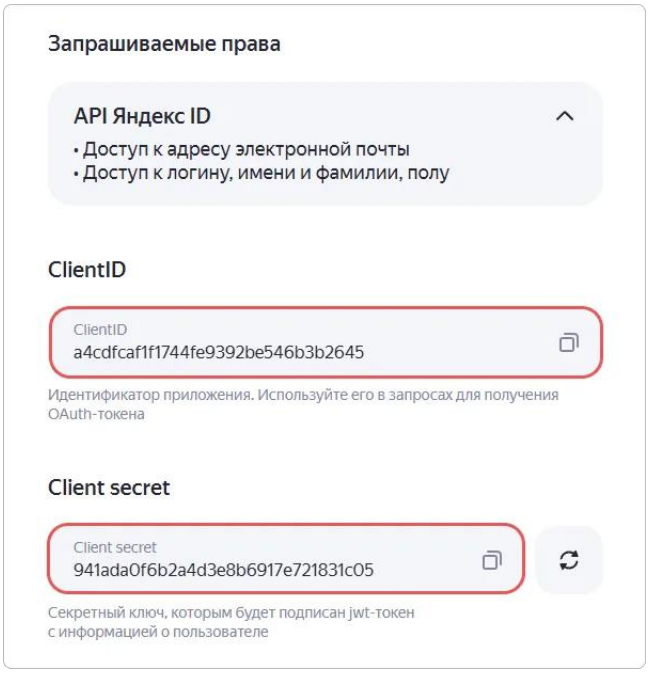
- **Доступ к адресу электронной почты**;
- **Доступ к логину, имени и фамилии, полу**.



8. На четвертом шаге подтвердите создание приложения.



9. Скопируйте значения полей **ID Приложения/Client ID** и **Секрет/Client Secret**. Они понадобятся при создании приложения в **КриптоАРМ IDM**.



Шаг 2. Создание способа входа

Теперь, имея ключи от **Яндекс**, создадим соответствующий провайдер в системе **КриптоАРМ IDM**.

1. Перейдите в панель ID → вкладка **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать** .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **Яндекс**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры аутентификации

   - **Идентификатор ресурса (client_id)** — Вставьте скопированный **ID Приложения** (`Client ID`).
   - **Секретный ключ (client_secret)** — Вставьте скопированный **Секрет** (`Client Secret`).

- **Возвратный URL(Redirect URI)** — Поле заполнится автоматически на основе вашего домена.

Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через Яндекс** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

   Проверка: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **Яндекс**.

Описание параметров

Основная информация

Название	Описание	Тип	Ограничения
Имя	Название, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**	Текст	Макс. 50 символов
Описание	Краткое описание, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM**	Текст	Макс. 255 символов
Логотип	Изображение, которое будет отображаться в интерфейсе сервиса **КриптоАРМ IDM** и виджете входа	JPG, GIF, PNG или WEBP	Макс. размер: 1 МБ

Параметры аутентификации

Название	Параметр	Описание
Идентификатор ресурса (client_id)	`Client_id`	ID приложения, созданного в **Яндекс**
Секретный ключ (client_secret)	`Client_secret`	Секретный ключ доступа приложения, созданного созданного в **Яндекс**
Возвратный	`Redirect URI`	Адрес **КриптоАРМ IDM**, на который

URL(Redirect URI) (не редактируемое)	пользователь перенаправляется после аутентификации в стороннем сервисе

Дополнительные настройки

Название	Описание
Публичный способ входа	При активации настройки: - Способ входа станет доступен для добавления в другие приложения сервиса. - Способ входа станет доступен для добавления в качестве идентификатора внешнего сервиса в профиле пользователя.
Публичность	Задает уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя

Смотрите также

- Способы входа и настройка виджета входа — руководство по способам входа и настройке виджета входа.
- Управление организациями — руководство по работе с организациями системы **КриптоАРМ IDM**.
- Личный профиль и управление разрешениями приложений — руководство по управлению личным профилем.

Как настроить интеграцию 1С с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **1С:Предприятие** через систему **КриптоАРМ IDM**.

Преимущества интеграции:

- **Единый вход** — пользователи входят в 1С с учетными данными **КриптоАРМ IDM**
- **Централизованное управление** — управление доступом через **КриптоАРМ IDM**
- **Безопасность** — использование OAuth 2.0 и OpenID Connect
- **Упрощение** — не нужно запоминать отдельные пароли для 1С

Поддерживаемые версии 1С — 1С:Предприятие 8.3.10 и выше.

Настройка входа через **КриптоАРМ IDM** состоит из нескольких ключевых этапов, которые выполняются в двух разных системах.

- Шаг 1. Создание приложения
- Шаг 2. Настройка системы 1С
- Шаг 3. Проверка подключения

Шаг 1. Создание приложения

1. Авторизуйтесь или зарегистрируйтесь в системе **КриптоАРМ IDM**.

2. Создайте приложение с настройками:

Поле	Значение
Адрес приложения	`<Адрес опубликованной базы 1С>`
Возвратный URL #1 (Redirect_uri)	`<Адрес опубликованной базы 1С>/authform.html`
URL выхода из системы #1 (post_logout_redirect_uri)	`<Адрес опубликованной базы 1С>/exit.html`

🔍 Подробнее о создании приложений читайте в инструкции.

3. Откройте настройки приложения и скопируйте значения:
   - **Идентификатор** (`client_id`),
   - **Секретный ключ** (`client_secret`).

   Эти данные понадобятся для настройки системы **1С**.

Шаг 2. Настройка системы 1С

1. Опубликуйте информационную базу на веб-сервере.

   🔗 Подробное руководство по публикации доступно в документации 1С.

2. Откройте .vrd-файл опубликованной базы. В конец добавьте запись между тегами `openidconnect`:

```
<httpServices poolTimeout="5"/>
<openidconnect>
    <providers>
        <![CDATA[
        {
            "name": "Digit",
            "title": "Digit",
            "authenticationClaimName": "email",
            "endSessionEndpoint": "<Адрес инсталляции
системы>/api/oidc/session/end",
            "discovery": "<Адрес инсталляции системы>/api/oidc/.well-
known/openid-configuration",
            "authenticationUserPropertyName": "email",
            "clientconfig": {
                "authority": "<Адрес инсталляции системы>/api/oidc/",
                "client_id": "",
                "client_secret": "",
                "redirect_uri": "",
                "post_logout_redirect_uri": "",
                "scope": "openid email",
                "response_type": "code"
            }
        }
        ]]>
    </providers>
```

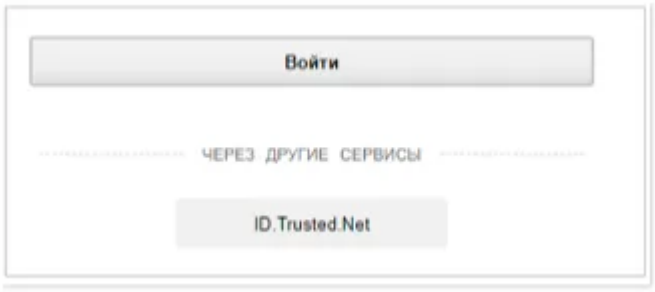
```
    <allowStandardAuthentication>true</allowStandardAuthentication>
</openidconnect>
```

где

Параметр	Назначение
`scope`	Список запрашиваемых разрешений (`openid email`)
`endSessionEndpoint`	`<Адрес инсталляции системы>/api/oidc/session/end`
`discovery`	`<Адрес инсталляции системы>/api/oidc/.well-known/openid-configuration`
`authority`	`<Адрес инсталляции системы>/api/oidc/`
`authenticationClaimName`	Поле для сопоставления пользователей
`authenticationUserPropertyName`	Дополнительное поле сопоставления

Шаг 3. Проверка подключения

1. Откройте опубликованную базу **1С** в браузере.
2. На форме входа появится кнопка «Войти через КриптоАРМ IDM».



3. Нажмите на кнопку — откроется окно авторизации **КриптоАРМ IDM**.

4. После успешного входа вы будете перенаправлены обратно в базу 1С.

Как настроить интеграцию 1С-Битрикс с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **Битрикс** через систему **КриптоАРМ IDM**.

> 📌 Битрикс — это платформа для управления бизнес-процессами, разработанная компанией **1С-Битрикс**.

Преимущества интеграции:

- **Единый вход** — сотрудники входят в Битрикс с учетными данными **КриптоАРМ IDM**
- **Централизованное управление** — управление доступом через **КриптоАРМ IDM**
- **Безопасность** — OAuth 2.0 и многофакторная аутентификация
- **Автоматизация** — автоматическая регистрация и синхронизация пользователей

Настройка входа через **КриптоАРМ IDM** состоит из нескольких ключевых этапов, которые выполняются в двух разных системах.

- Шаг 1. Создание приложения
- Шаг 2. Настройка системы Битрикс
- Шаг 3. Проверка подключения

Шаг 1. Создание приложения

1. Авторизуйтесь в системе **КриптоАРМ IDM**.

2. Создайте приложение с настройками:

Поле	Значение
Адрес приложения	Адрес инсталляции системы Битрикс
Возвратный URL #1 (Redirect_uri)	`<адрес инсталляции Битрикс>/bitrix/tools/oauth/trustedid.php`

   🔍 Подробнее о создании приложений читайте в инструкции.

3. Откройте настройки приложения и скопируйте значения:

   - **Идентификатор** (`client_id`),
   - **Секретный ключ** (`client_secret`).

   Эти данные понадобятся для настройки **Битрикс**.

Шаг 2. Настройка системы Битрикс

Установка модуля «Trusted ID»

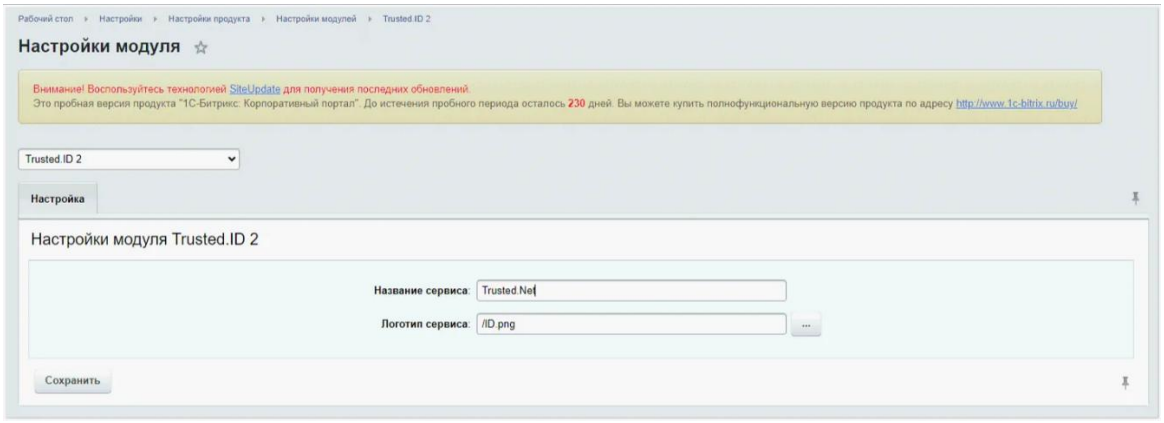
1. В административной части **Битрикс** установите модуль **Trusted ID**.

2. Перейдите в настройки модуля: **Администрирование → Настройки → Настройки продукта → Настройки модулей → Trusted ID**

3. Заполните поля:

   - **Название сервиса** — текст, который будет отображаться при наведении на логотип на форме авторизации.

   - **Логотип сервиса** — иконка для формы авторизации.

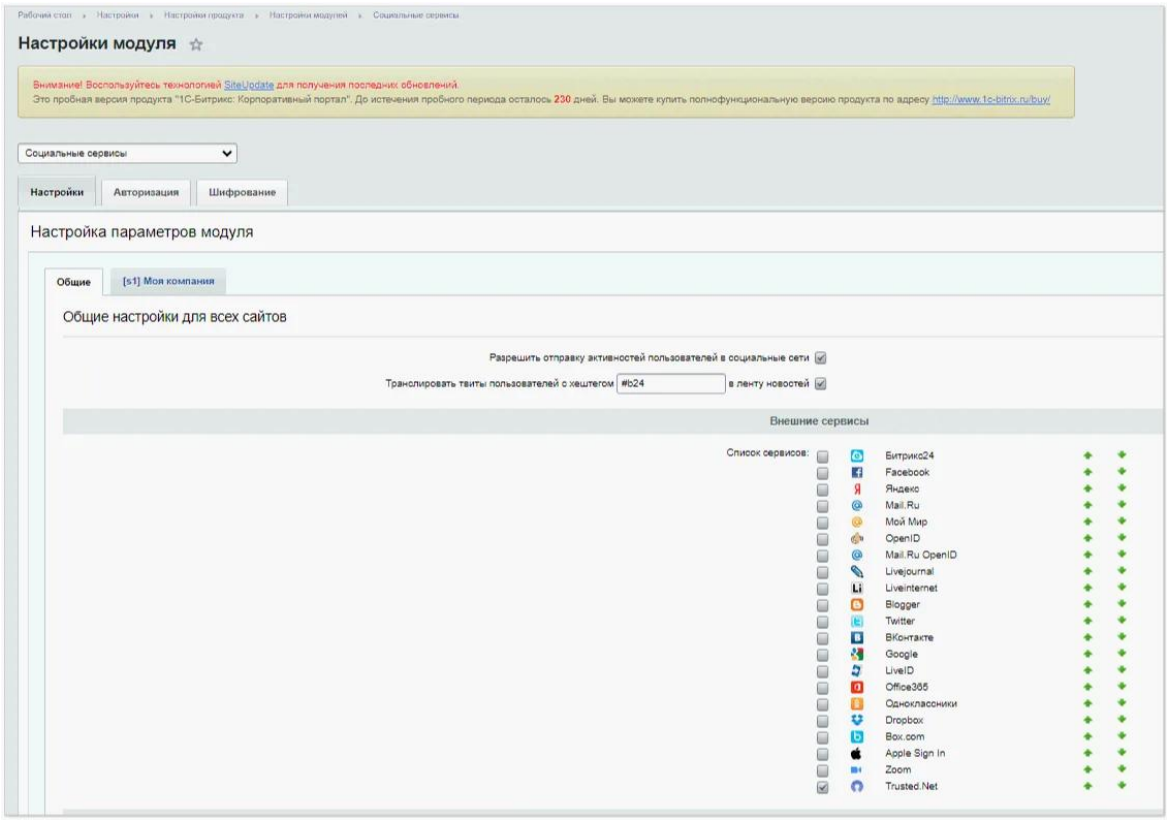


4. Сохраните изменения.

Настройка социальных сервисов

1. Перейдите к настройкам параметров модуля: **Администрирование → Настройки → Настройки продукта → Настройки модулей → Социальные сервисы**.

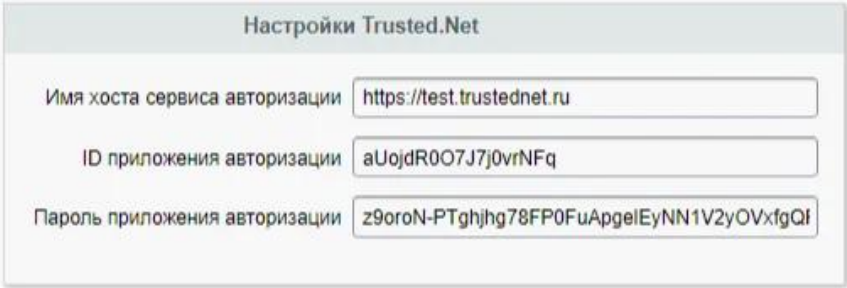
2. В разделе **Внешние сервисы** включите флаг для настроенного названия сервиса **Trusted ID**.



Привязка приложения

1. В настройках модуля укажите параметры приложения, созданного в **КриптоАРМ IDM**:

Параметр	Значение
Адрес сервиса	URL вашей инсталляции КриптоАРМ IDM
ID приложения авторизации	`Client_id`, скопированный из приложения КриптоАРМ IDM
Пароль приложения авторизации	`client_secret`, скопированный из приложения КриптоАРМ IDM



2. Примените изменения.

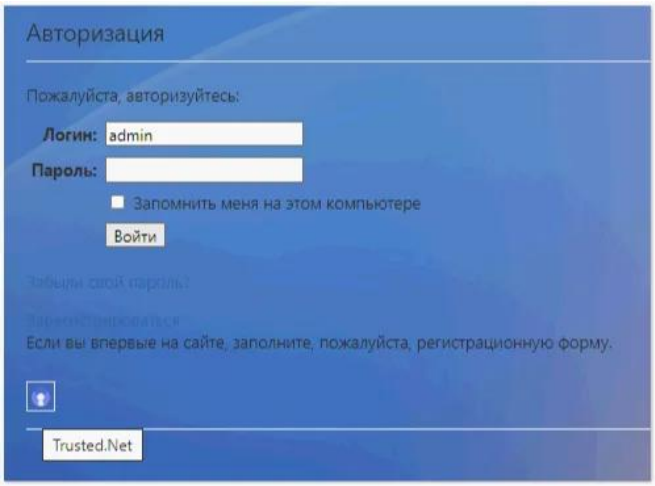
Настройка регистрации пользователей

Если требуется автоматическая регистрация новых пользователей через **КриптоАРМ IDM**:

1. В настройках главного модуля **Битрикс** перейдите в раздел **Регистрация и авторизация**.
2. Убедитесь, что флаг **Позволять ли пользователям регистрироваться самостоятельно?** активен.

Шаг 3. Проверка подключения

1. Откройте форму авторизации вашего сайта на **Битрикс**.
2. Должна появиться кнопка **Войти через КриптоАРМ IDM**:



3. Нажмите на кнопку — откроется окно авторизации **КриптоАРМ IDM**.

4. После успешного входа вы будете перенаправлены обратно в Битрикс.

Как настроить интеграцию Контур.Толк с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **Контур.Толк** через систему **КриптоАРМ IDM**.

> 📌 Контур.Толк — сервис для проведения видеоконференций с возможностью записи, планированием, интеграцией с телефонией и многим другим. Обеспечивает удобное и безопасное общение сотрудников друг с другом и с партнерами, в формате видео-аудио конференций.

Настройка входа через **КриптоАРМ IDM** состоит из нескольких ключевых этапов, которые выполняются в двух разных системах.

- Общее описание интеграции
- Шаг 1. Создание приложения
- Шаг 2. Настройка системы Контур.Толк
- Шаг 3. Проверка подключения

Общее описание интеграции

SSO (Single Sign-On) позволяет централизованно управлять входом пользователей:

- Аутентификация выполняется через корпоративную систему.
- Пользователям не нужно создавать отдельный аккаунт в Контур.Толк.
- Для интеграции используется протокол **Authorization Code Flow** через **OpenID Connect** или **OAuth 2.0**.

Контур.Толк поддерживает следующие ключевые атрибуты и конечные точки:

Категория	Параметр	Описание	Пример/Значение
Основные параметры	`authorization_endpoint`	URL для аутентификации	`https://id.kloud.one/api/oidc/auth`
	`device_authorization_endpoint`	URL для авторизации устройств	`https://id.kloud.one/api/oidc/device/auth`
	`claims_parameter_supported`	Поддержка параметра claims	`false`
	`claims_supported`	Поддерживаемые атрибуты	`["sub","email","name","picture",...]`

		в токене	
Методы аутентификации	code_challenge_methods_supported	Методы для PKCE	["S256"]
	end_session_endpoint	URL выхода	https://id.kloud.one/api/oidc/session/end
	grant_types_supported	Поддерживаемые типы OAuth 2.0	["implicit","authorization_code",...]
	id_token_signing_alg_values_supported	Алгоритмы подписи ID токена	["RS256"]
Дополнительно	issuer	Идентификатор сервера	https://id.kloud.one
	jwks_uri	URL JWKS	https://id.kloud.one/api/oidc/jwks
	registration_endpoint	URL регистрации клиента	https://id.kloud.one/api/oidc/reg
	response_modes_supported	Режимы ответа	["form_post","fragment","query"]
	response_types_supported	Типы ответов	["code token","code id_token",...]
	scopes_supported	Поддерживаемые scopes	["openid","email","profile",...]
	subject_types_supported	Типы субъектов	["public","pairwise"]
Конечные точки	token_endpoint	URL получения токена	https://id.kloud.one/api/oidc/token
	userinfo_endpoint	URL информации о пользователе	https://id.kloud.one/api/oidc/me
	introspection_endpoint	URL проверки токена	https://id.kloud.one/api/oidc/token/introspection

	`revocation_endpoint`	URL отзыва токена	`https://id.kloud.one/api/oidc/token/revocation`
Методы аутентификации конечных точек	`token_endpoint_auth_methods_supported`	Методы аутентификации	`["client_secret_basic",...]`
	`introspection_endpoint_auth_methods_supported`	Для интроспекции	`["client_secret_basic",...]`
	`revocation_endpoint_auth_methods_supported`	Для отзыва токенов	`["client_secret_basic",...]`
Алгоритмы	`claim_types_supported`	Типы атрибутов	`normal`

Шаг 1. Создание приложения

1. Авторизуйтесь ив системе **КриптоАРМ IDM**.
2. Создайте новое приложение с настройками:

Параметр	Значение
Адрес приложения	`<адрес инсталляции Контур.Толк>`
Redirect_uri #1	`<адрес инсталляции Контур.Толк>/login/callback`

🔍 Подробнее о создании приложений читайте в инструкции по управлению приложениями.

3. Откройте настройки приложения и скопируйте значения:
   - **Идентификатор** (`Client_id`)
   - **Секретный ключ** (`client_secret`)

Шаг 2. Настройка системы Контур.Толк

Настройка на стороне Контур.Толк требует взаимодействия с технической поддержкой сервиса:

1. Отправьте запрос в техподдержку **Контур.Толк** на подключение системы единого входа (SSO). В запросе укажите:
   - `CLIENT_ID` приложения, созданного в **КриптоАРМ IDM**
   - `CLIENT_SECRET` приложения
2. После подтверждения техподдержкой, параметры приложения будут привязаны к вашему пространству в Контур.Толк.

Шаг 3. Проверка подключения

1. Откройте страницу входа в **Контур.Толк**.
2. Убедитесь, что появилась кнопка **Вход через КриптоАРМ IDM**.
3. Попробуйте войти с учётной записью корпоративного пользователя:
   - После нажатия кнопки система перенаправит вас на страницу аутентификации **КриптоАРМ IDM**.
   - Введите корпоративные учетные данные.
4. **Проверьте, что после успешной аутентификации вы попадаете в своё пространство в Контур.Толк.**

Как настроить интеграцию GitLab с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **GitLab** через систему **КриптоАРМ IDM**.

> 📌 GitLab — это веб-платформа для управления проектами и репозиториями программного кода, работа которой основана на популярной системе контроля версий **Git**.

Настройка входа через **КриптоАРМ IDM** состоит из нескольких ключевых этапов, которые выполняются в двух разных системах.

- Шаг 1. Создание приложения
- Шаг 2. Настройка системы GitLab
- Шаг 3. Проверка работы интеграции

Шаг 1. Создание приложения

1. Авторизуйтесь в системе **КриптоАРМ IDM**.
2. Создайте приложение с настройками:
   - **Адрес приложения** - адрес инсталляции системы **GitLab**;
   - **Возвратный URL #1 (`Redirect_uri`)** - `<адрес инсталляции GitLab>/users/auth/oauth2_generic/callback`.

   > 🔍 Подробнее о создании приложений читайте в инструкции.
3. Откройте настройки приложения и скопируйте значения полей:
   - **Идентификатор** (`Client_id`),
   - **Секретный ключ** (`client_secret`).

Шаг 2. Настройка системы GitLab

Настройка авторизации пользователей сервиса **GitLab** через **КриптоАРМ IDM** происходит в файле конфигурации **GitLab gitlab.rb**, расположенного в папке конфигурации сервиса (/config).

1. Откройте файл конфигурации **gitlab.rb** в режиме редактирования и перейти к блоку **OmniAuth Settings**.

2. Задайте следующие значения для параметров:

```
    gitlab_rails['omniauth_enabled'] = true
    gitlab_rails['omniauth_allow_single_sign_on'] = ['oauth2_generic',
'<НазваниеСистемыКриптоАРМ IDM>']
    gitlab_rails['omniauth_block_auto_created_users'] = false
```

Значение gitlab_rails['omniauth_providers'] должно выглядеть следующим образом:

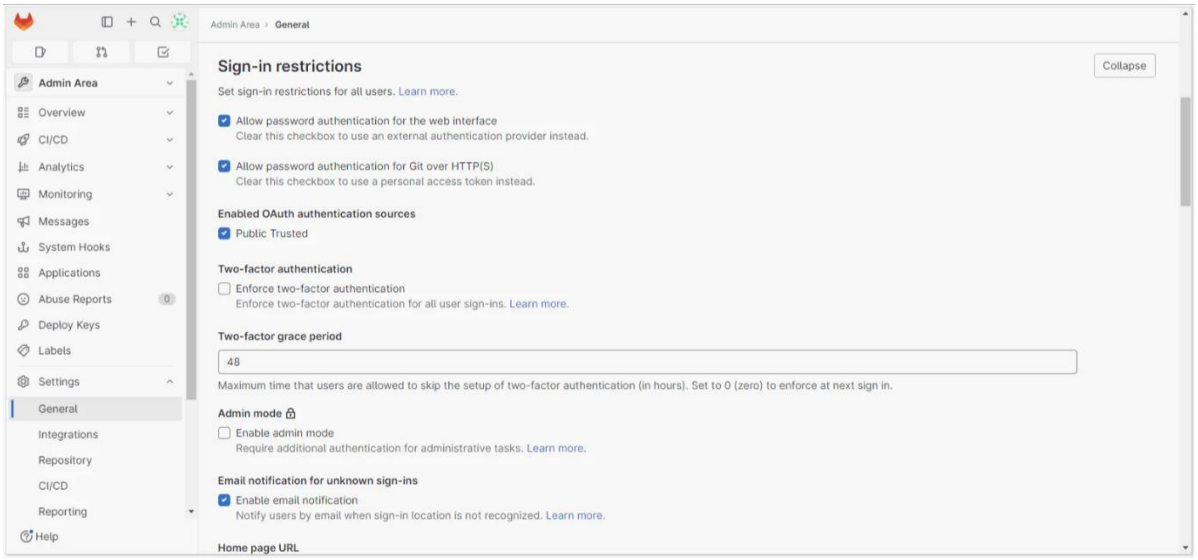
```
    gitlab_rails['omniauth_providers'] = [
    {
    'name' => 'oauth2_generic',
    'app_id' => '<Client_id приложения, созданного в КриптоАРМ IDM>',
    'app_secret' => '<Client_secret приложения, созданного в КриптоАРМ
IDM>',
    'args' => {
    client_options: {
    'site' => 'https://<Адрес системы КриптоАРМ IDM>/',
    'authorize_url' => '/api/oidc/auth',
    'user_info_url' => '/api/oidc/me',
    'token_url' => '/api/oidc/token'
    },
    user_response_structure: {
    root_path: [],
    id_path: ['sub'],
    attributes: { email:'email',  name:'nickname' },
    },
    scope: 'openid profile email',
    'name' => '<НазваниеСистемыКриптоАРМ IDM>’
    }
    }
    ]
```

```
### OmniAuth Settings
###! Docs: https://docs.gitlab.com/ee/integration/omniauth.html

gitlab_rails['omniauth_enabled'] = true
gitlab_rails['omniauth_allow_single_sign_on'] = ['oauth2_generic', '          TrustedRu']
# gitlab_rails['omniauth_sync_email_from_provider'] = 'saml'
# gitlab_rails['omniauth_sync_profile_from_provider'] = ['saml']
# gitlab_rails['omniauth_sync_profile_attributes'] = ['email']
# gitlab_rails['omniauth_auto_sign_in_with_provider'] = 'saml'
gitlab_rails['omniauth_block_auto_created_users'] = false
# gitlab_rails['omniauth_auto_link_ldap_user'] = false
# gitlab_rails['omniauth_auto_link_saml_user'] = false
# gitlab_rails['omniauth_external_providers'] = ['twitter', 'google_oauth2']

gitlab_rails['omniauth_providers'] = [
  {
    'name' => 'oauth2_generic',
    'app_id' => 'DjfyT                ',
    'app_secret' => 'dtYR7yDUYkJ36qQ                                                                  ',
    'args' => {
      client_options: {
        'site' => 'https://test.trusted.plus', # including port if necessary
        'authorize_url' => '/api/oidc/auth',
        'user_info_url' => '/api/oidc/me',
        'token_url' => '/api/oidc/token'
      },
      user_response_structure: {
        root_path: [],
        id_path: ['sub'],
        attributes: { email:'email',  name:'nickname' }, # if the nickname attribute of a user is called 'username'
      },
      scope: 'openid profile email',
      'name' => 'TestTru          '
    }
  }
]
```

3. Перезапустите сервис **GitLab** для применения новых настроек.

4. При необходимости, зайдите под администратором в интерфейсную часть сервиса **GitLab**. Перейдите в настройки по пути **Admin (Admin Area) — Settings-General**.

   На открывшейся странице в блоке **Sign-in restrictions** установите флаг напротив в дочернем блоке **Enabled OAuth authentication sources**.



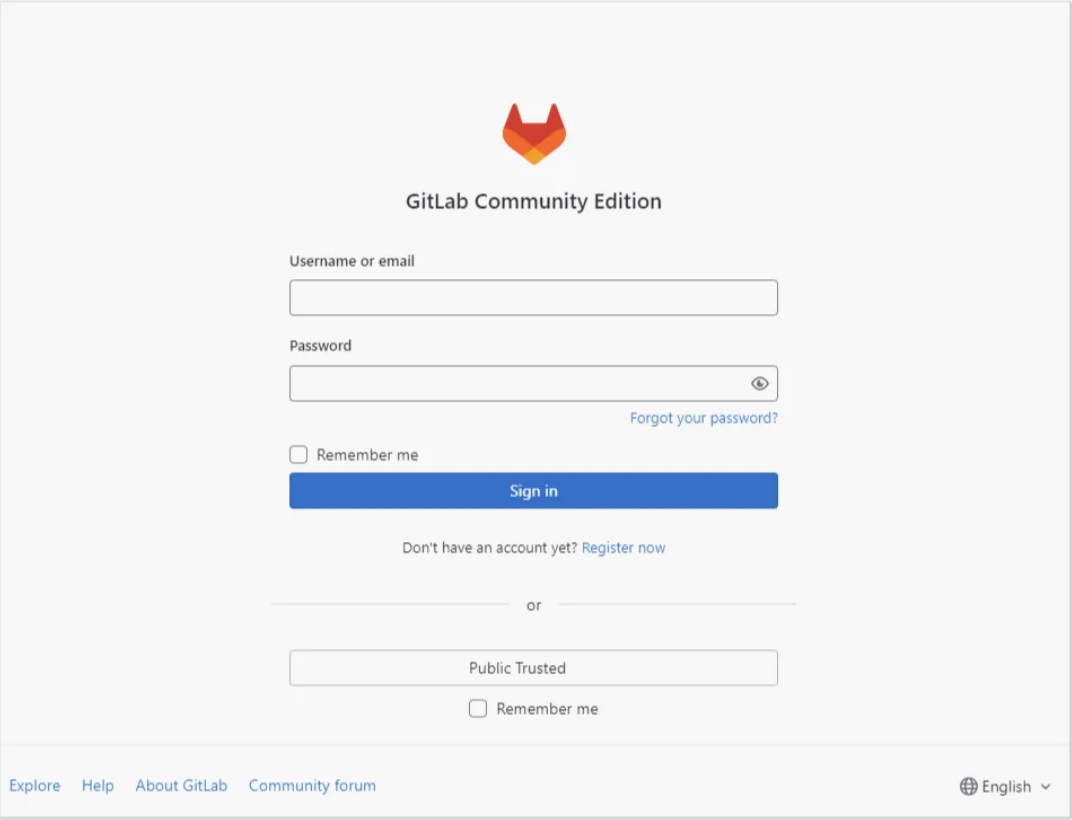
Шаг 3. Проверка работы интеграции

1. Откройте страницу входа в **GitLab**.

2. Убедитесь, что появилась кнопка **Вход через КриптоАРМ IDM**.

3. Нажмите на кнопку и выполните вход с корпоративной учётной записью:

   - Система перенаправит вас на страницу аутентификации **КриптоАРМ IDM**.
   - Введите свои корпоративные учетные данные.



4. После успешной аутентификации вы должны быть перенаправлены обратно в **GitLab** и автоматически авторизованы в своём аккаунте.

Как настроить интеграцию Grafana с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **Grafana** через систему **КриптоАРМ IDM**.

> 📌 Grafana — свободная программная система визуализации данных, ориентированная на данные систем ИТ-мониторинга.

Настройка входа через **КриптоАРМ IDM** состоит из нескольких ключевых этапов, которые выполняются в двух разных системах.

- Шаг 1. Создание приложения
- Шаг 2. Настройка системы Grafana
- Шаг 3. Проверка подключения

Шаг 1. Создание приложения

1. Авторизуйтесь в системе **КриптоАРМ IDM**.

2. Создайте приложение с настройками:

   - **Адрес приложения** - адрес инсталляции системы **Grafana**;
   - **Возвратный URL #1 (Redirect_uri)** - `<адрес инсталляции Grafana>/login/generic_oauth`.

   🔍 Подробнее о создании приложений читайте в инструкции.

3. Откройте настройки приложения и скопируйте значения полей:

   - **Идентификатор** (`Client_id`),
   - **Секретный ключ** (`client_secret`).

Шаг 2. Настройка системы Grafana

Настройка авторизации через **КриптоАРМ IDM** выполняется в файле конфигурации **grafana.ini**, который на Linux обычно находится по пути: `/etc/grafana/grafana.ini`.

1. Откройте файл **grafana.ini** в режиме редактирования.

2. Найдите или добавьте блок `[auth.generic_oauth]` и задайте следующие параметры:

```
[auth.generic_oauth]
enabled = true
name = <НазваниеСистемыКриптоАРМ IDM>
allow_sign_up = true
client_id = <Client_id приложения, созданного в КриптоАРМ IDM>
client_secret = <Client_secret приложения, созданного в КриптоАРМ IDM>
scopes = openid profile email
empty_scopes = false
email_attribute_name = email:email
email_attribute_path = data.email
login_attribute_path = data.login
name_attribute_path = data.givenName
auth_url = https://<Адрес системы КриптоАРМ IDM>/api/oidc/auth
token_url = https://<Адрес системы КриптоАРМ IDM>/api/oidc/token
api_url = https://<Адрес системы КриптоАРМ IDM>/api/oidc/me
```

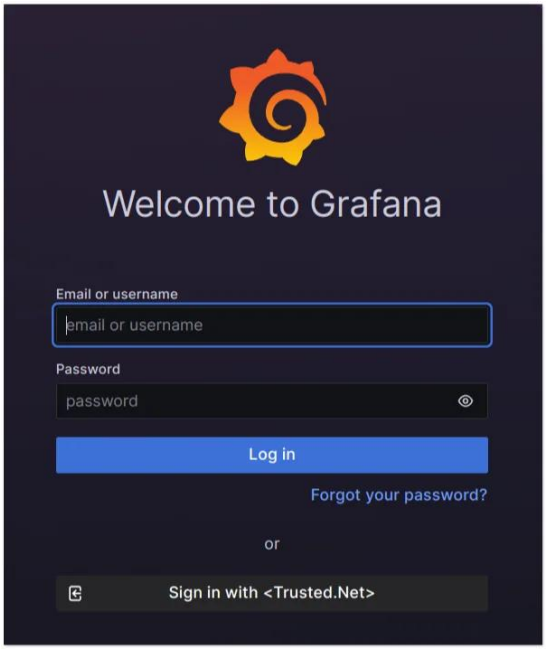
```
enabled = true
name = <НазваниеСистемыTrusted.ID>
allow_sign_up = true
client_id = BCfS65FnItNpo0XobyKTd
client_secret = y0ThHD_#qEm{hjJrNqlxhU#B%?PsYw9St{LICbfgEMecXSmEp-mNybMrxjGgrTyS5Eszdfk_nTsX#}Df2Bsb%p
scopes = openid profile email
empty_scopes = false
email_attribute_name = email:email
email_attribute_path = data.email
login_attribute_path = data.login
name_attribute_path = data.givenName
auth_url = https://<Адрес системы Trusted.ID>/api/oidc/auth
token_url = https://<Адрес системы Trusted.ID>/token
api_url = https://<Адрес системы Trusted.ID>/api/oidc/me
```

3. Перезапустите сервис **Grafana** для применения новых настроек.

```
sudo systemctl restart grafana-server
```

Шаг 3. Проверка подключения

1. Откройте страницу входа в **Grafana**.
2. Убедитесь, что появилась кнопка **Вход через КриптоАРМ IDM**.
3. Нажмите на кнопку и выполните вход, используя корпоративные учетные данные:
   - Вы будете перенаправлены на страницу аутентификации **КриптоАРМ IDM**;
   - После успешного входа вы попадёте обратно в **Grafana**, авторизованным пользователем.



Как настроить интеграцию Moodle с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **Moodle** через систему **КриптоАРМ IDM**.

📌 Moodle — система управления образовательными электронными курсами (электронное обучение).

Настройка входа через **КриптоАРМ IDM** состоит из нескольких ключевых этапов, которые выполняются в двух разных системах:

- Шаг 1. Создание приложения
- Шаг 2. Настройка системы Moodle
- Шаг 3. Проверка подключения

Шаг 1. Создание приложения

1. Авторизуйтесь в системе **КриптоАРМ IDM**.

2. Создайте приложение с настройками:

   - **Адрес приложения** - адрес инсталляции системы **Moodle**;

   - **Возвратный URL #1 (Redirect_uri)** - `<адрес инсталляции Moodle>/admin/oauth2callback.php`.

   Подробнее о создании приложений читайте в инструкции.

3. Откройте настройки приложения и скопируйте значения полей:

   - **Идентификатор** (`Client_id`),
   - **Секретный ключ** (`client_secret`).

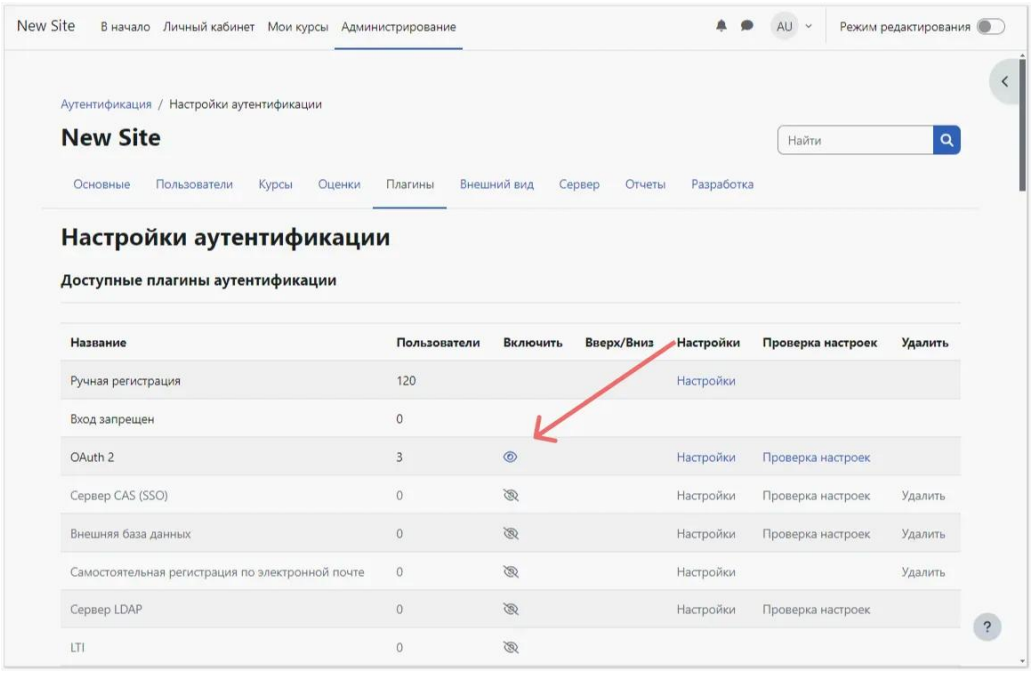
Шаг 2. Настройка системы Moodle

Для настройки авторизации пользователей требуются права администратора в **Moodle**.

Включение плагина OAuth2

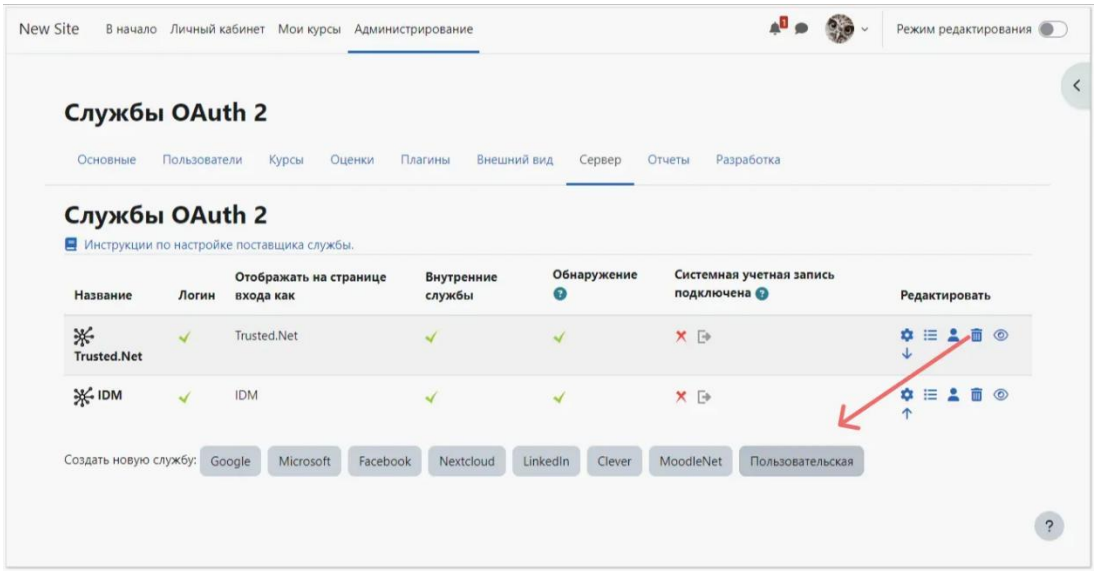
1. Авторизуйтесь в **Moodle** с административными правами.

2. Перейдите в **Администрирование - Плагины - Аутентификация** и активируйте плагин **Oauth 2**, включив его в столбце **Включить**.



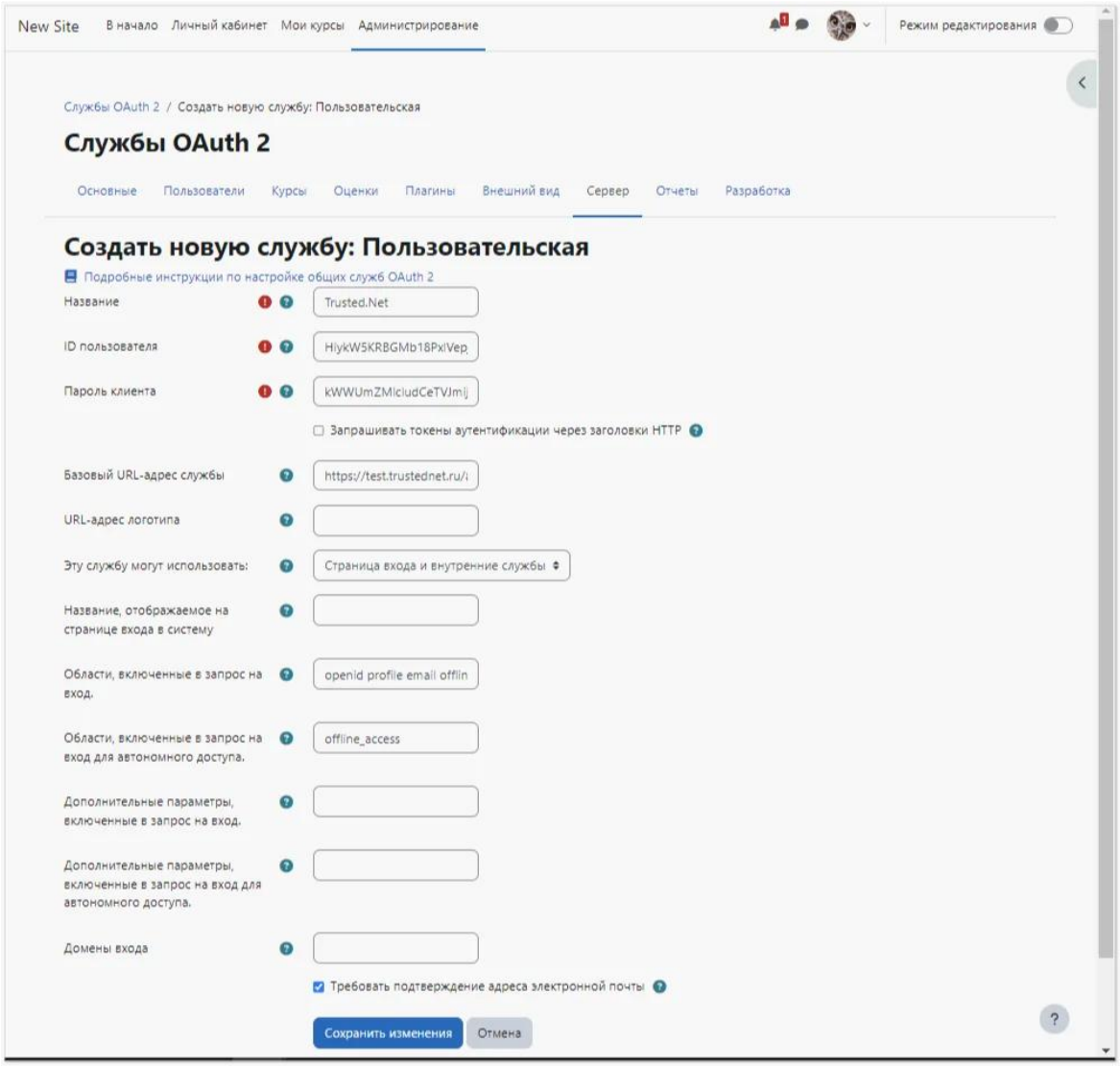
Создание пользовательского провайдера

1. Перейдите в раздел **Администрирование → Сервер → Службы OAuth2**.
2. Нажмите кнопку **Пользовательская**.



3. Откроется форма создания провайдера.
4. Заполните поля:
   - **Название** — любое отображаемое название сервиса;
   - **ID пользователя** — `Client_id` приложения **КриптоАРМ IDM**;
   - **Пароль клиента** — `Client_secret` приложения **КриптоАРМ IDM**;
   - **Базовый URL-адрес службы** — `<Адрес КриптоАРМ IDM>/api/oidc`;
   - **Эту службу могут использовать — Страница входа и внутренние службы**;

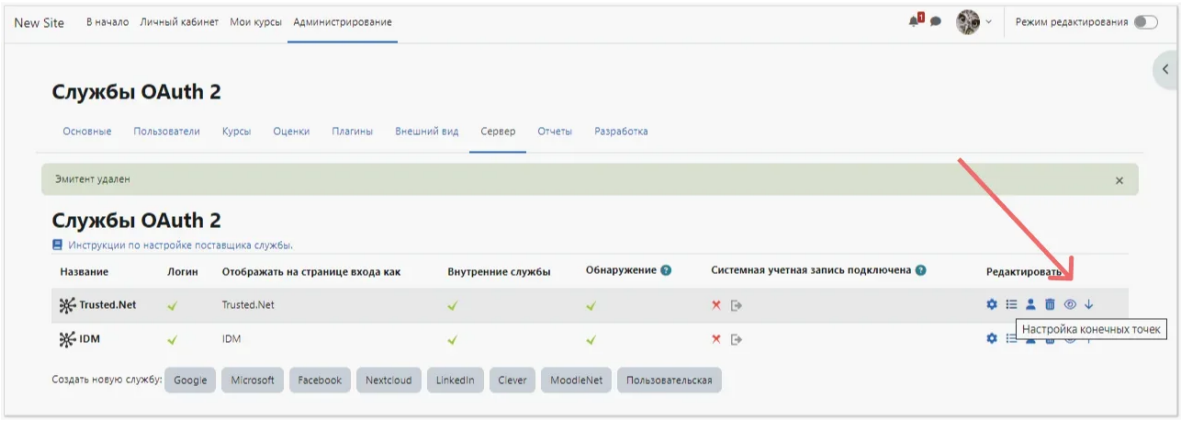
- **Области, включенные в запрос на вход** — `openid profile email offline_access`;
- **Области, включенные в запрос на вход для автономного доступа** — `offline_access`.



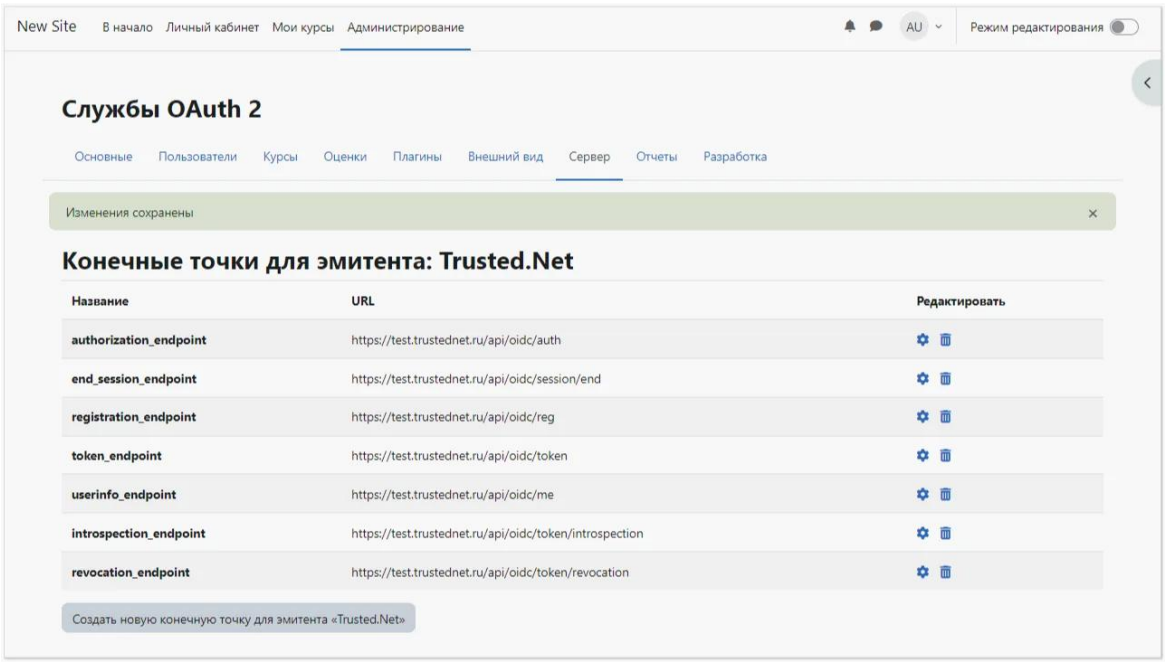
5. Сохраните изменения.

Настройка конечных точек

1. Нажмите **Настройки конечных точек** в столбце **Редактировать**.



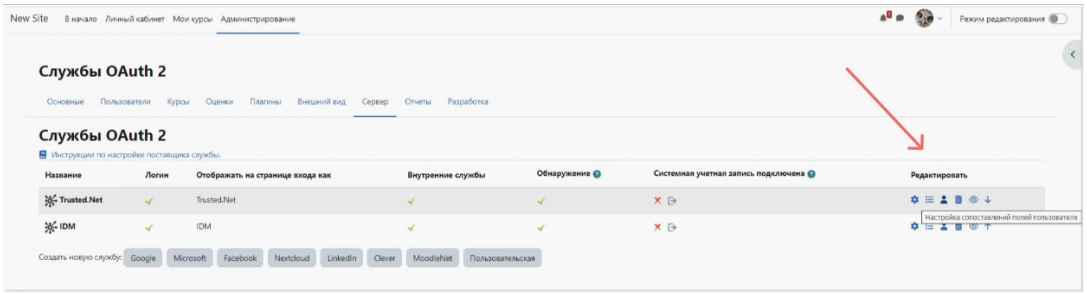
2. В случае, если все данные были введены корректно, настройки автоматически заполнятся.



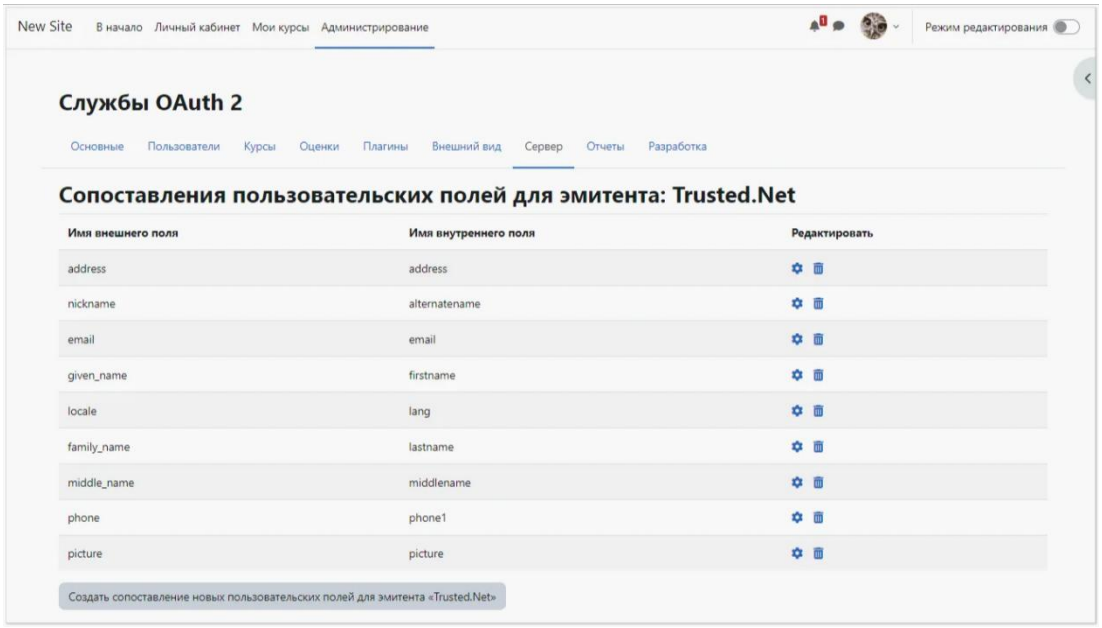
При необходимости можно заполнить URL конечных точек вручную. Список доступных URL см. по адресу: `https://<Адрес сервиса КриптоАРМ IDM>/api/oidc/.well-known/openid-configuration`

Настройка сопоставления полей пользователя

1. Нажмите **Настройка сопоставлений полей пользователя** в столбце **Редактировать**.



2. В случае, если все данные были введены корректно, настройки автоматически заполнятся.



При необходимости сопоставления можно настроить вручную.

Настройка отправки почты в Moodle

В случае, когда в СДО требуется отправка писем пользователям, то необходимо выполнить настройки почты (если ранее не были заданы):

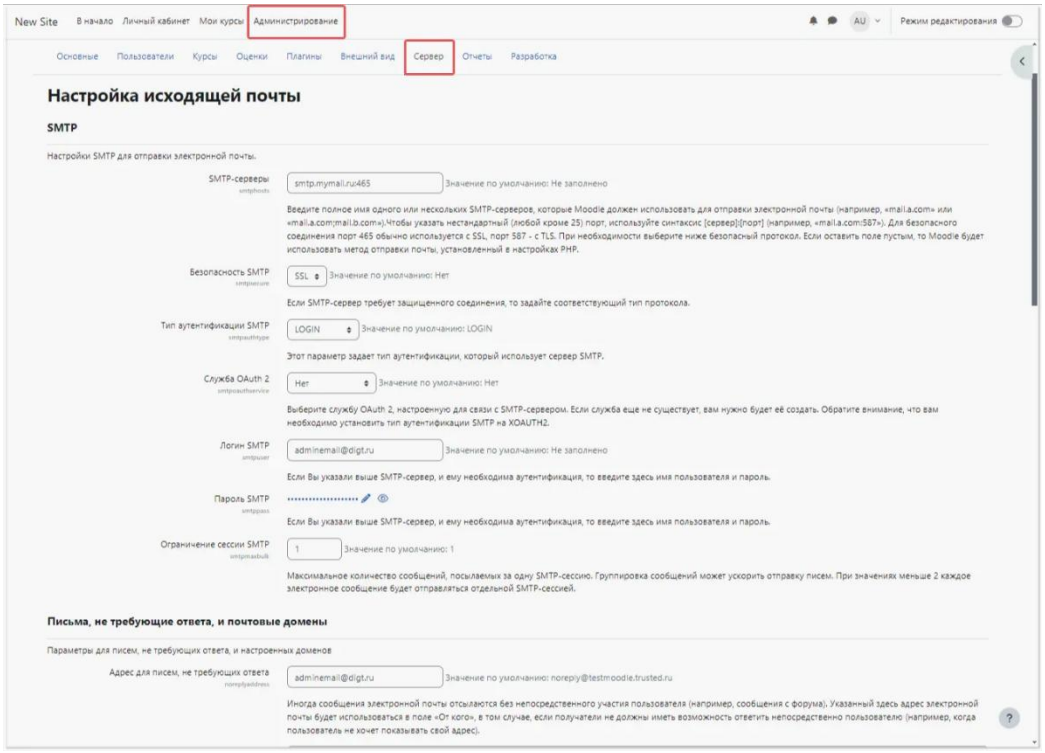
1. Перейдите в **Администрирование → Сервер → Электронная почта → Настройка исходящей почты**.

2. Заполните поля:

   - **SMTP-серверы** — полное имя smtp-сервера, включая порт через двоеточие;

   - **Безопасность SMTP** — выбрать значение из списка;

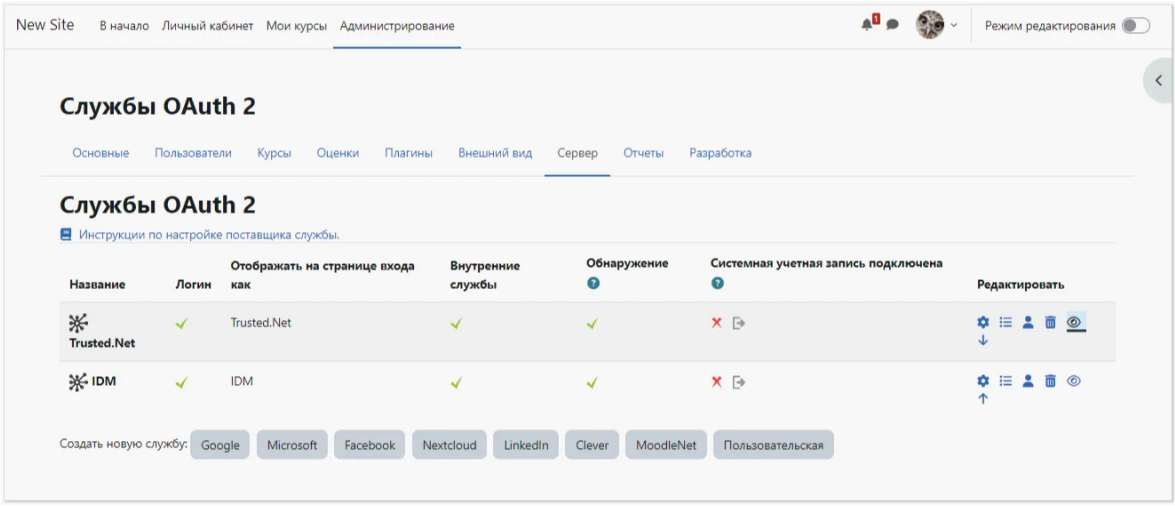
   - **Тип аутентификации SMTP** — выбрать нужное значение. В случае выбора типа аутентификации **LOGIN**, заполнить поля **Логин SMTP** и **Пароль SMTP**. Поле **Адрес для писем, не требующих ответа** рекомендуется заполнить во избежание потенциальных проблем при отправке писем.



💡 Связывание пользователя СДО Moodle с пользователем КриптоАРМ IDM происходит по адресу электронной почты. Отсутствие email в профиле КриптоАРМ IDM приведет к невозможности авторизации в Moodle. Удаление ранее привязанного к Moodle почтового ящика в КриптоАРМ IDM и добавление нового почтового ящика приведет к созданию нового пользователя в Moodle.

Шаг 3. Проверка подключения

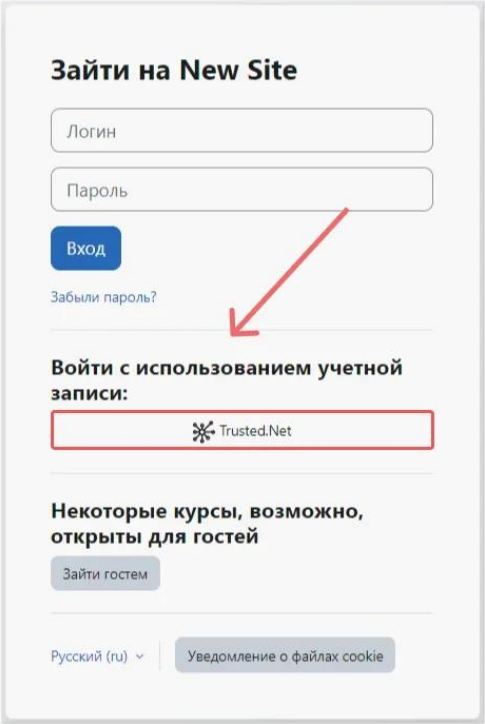
1. Вернитесь в список **Служб OAuth 2** и убедитесь, что созданный провайдер активен.



2. Откройте страницу входа в **Moodle**.

3. Убедитесь, что появилась кнопка **Вход через КриптоАРМ IDM**.

4. Нажмите на кнопку и выполните вход, используя корпоративные учетные данные:
   - Вы будете перенаправлены на страницу аутентификации **КриптоАРМ IDM**;
   - После успешного входа вы попадёте обратно в **Moodle**, авторизованным пользователем.



Как настроить интеграцию МТС Линк с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **МТС Линк** через систему **КриптоАРМ IDM**.

> 📌 МТС Линк — экосистема сервисов для бизнес-коммуникаций и совместной работы, объединяющая звонки, видеоконференции, чаты и управление задачами.

Настройка входа через **КриптоАРМ IDM** состоит из двух ключевых этапов, которые выполняются в двух разных системах.

- Шаг 1. Создание приложения
- Шаг 2. Настройка системы МТС Линк

Шаг 1. Создание приложения

1. Авторизуйтесь в системе **КриптоАРМ IDM**.

2. Создайте приложение с настройками:

- **Адрес приложения** - адрес инсталляции системы **МТС Линк**;

- **Возвратный URL #1 (Redirect_uri)** - `<адрес инсталляции МТС Линк>/api/oauth/return`.

🔍 Подробнее о создании приложений читайте в инструкции.

3. Перейдите в настройки приложения и скопируйте значения полей:

   - **Идентификатор** (`Client_id`),
   - **Секретный ключ** (`client_secret`).

Шаг 2. Настройка системы МТС Линк

Для корректной работы требуется подтверждение домена в **МТС Линк**. Подтверждение необходимо, чтобы только сотрудники организации могли использовать домен для SSO. Подробное описание в статьях Подтверждение домена для SSO и Настройка SSO.

Включение и настройка SSO

1. Авторизуйтесь в **МТС Линк**.

2. Перейдите в раздел **Бизнес** → **Настройки SSO**.

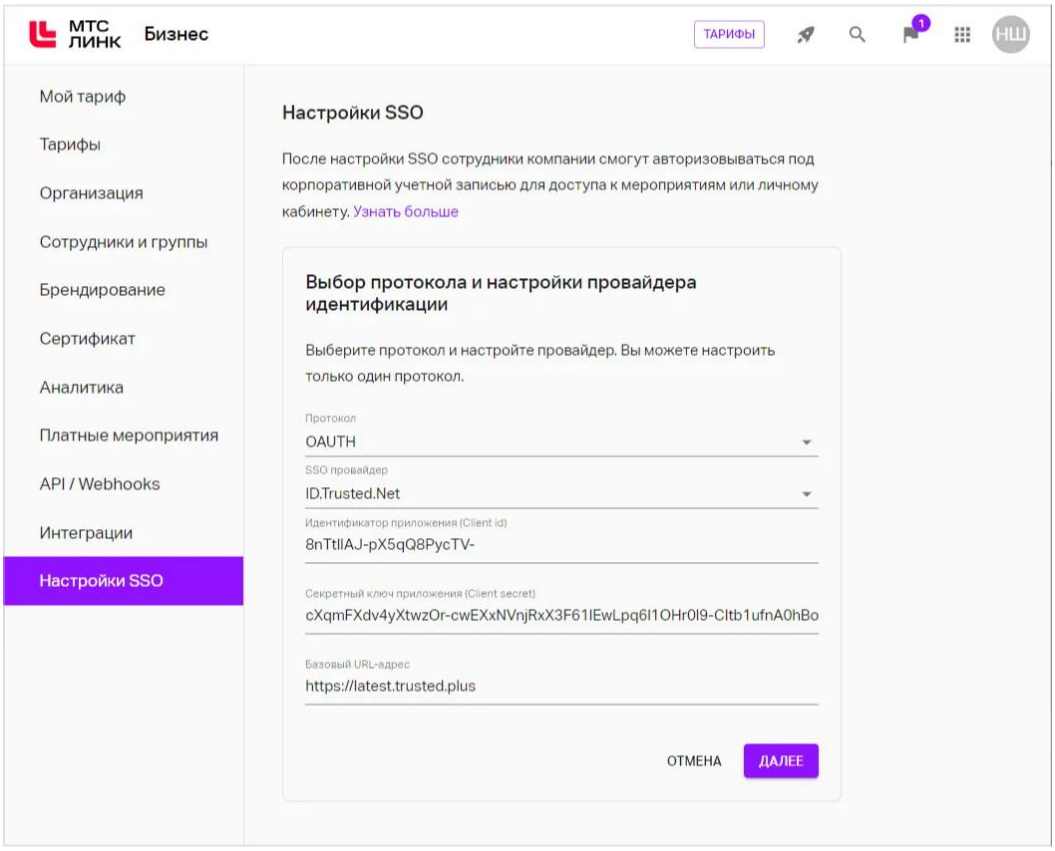
3. Откроется форма настройки.

4. Укажите настройки:

   - Протокол → **OAuth**,
   - SSO провайдер → **ID.КриптоАРМ IDM**,
   - Идентификатор приложения (`Client id`) — идентификатор приложения, созданного в **КриптоАРМ IDM**;

   - Секретный ключ приложения (`Client secret`) — секретный ключ приложения, созданного в **КриптоАРМ IDM**;

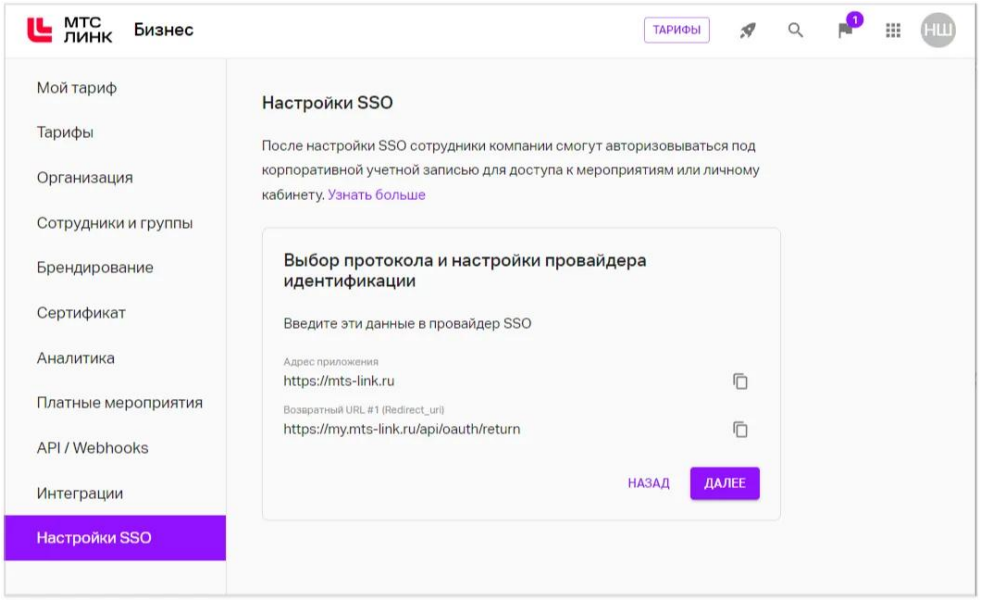
   - Базовый URL-адрес — укажите адрес сервиса **КриптоАРМ IDM**.



5. Нажмите **Далее**:

Проверка параметров Redirect URI

Убедитесь, что значение параметров **Адрес приложения** и **Возвратный URL (`Redirect_uri`)** соответствуют значениям, что указаны в настройках **КриптоАРМ IDM**.

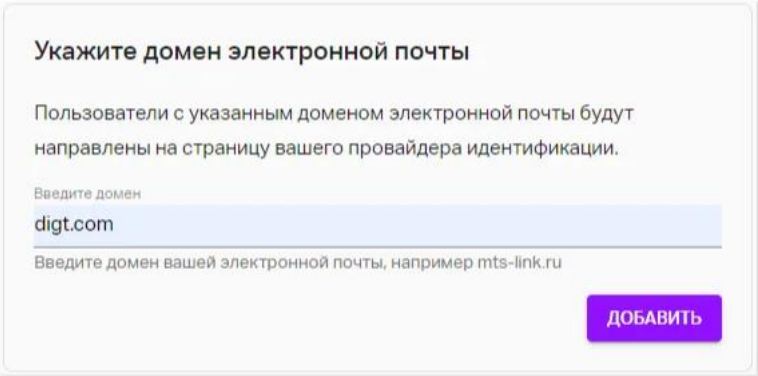


Если они отличаются — скопируйте актуальные значения из **МТС Линк** и вставьте их в настройки вашего приложения **КриптоАРМ IDM**.

Добавление корпоративного домена

1. В личном кабинете **МТС Линк** укажите домен электронной почты, чтобы пользователи с этим доменом направлялись на страницу провайдера идентификации **КриптоАРМ IDM**.

2. Нажмите **Добавить**, чтобы пользователи с этим доменом перенаправлялись для входа через **КриптоАРМ IDM**.



Проверка корректности настройки

1. В разделе **Настройки SSO** нажмите кнопку **Проверить работу**.

2. Откроется окно входа через КриптоАРМ IDM. Успешная авторизация подтверждает корректность интеграции.

Как настроить интеграцию Nextcloud с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **Nextcloud** через систему **КриптоАРМ IDM**.

> 📌 Nextcloud — экосистема сервисов для бизнес-коммуникаций и совместной работы, объединяющая звонки, видеоконференции, чаты и управление задачами.

Настройка входа с помощью **КриптоАРМ IDM** состоит из двух ключевых этапов, которые выполняются в двух разных системах.

- Шаг 1. Создание приложения
- Шаг 2. Настройки на стороне Nextcloud
- Шаг 3. Проверка подключения

Шаг 1. Создание приложения

1. Авторизуйтесь в **КриптоАРМ IDM**.

2. Создайте новое приложение, в котором укажите:

- **Адрес приложения** - адрес инсталляции системы **Nextcloud**. Например: `https://<адрес инсталляции Nextcloud>`.

- **Возвратный URL #1** (`Redirect_uri`) - адрес в формате `https://<адрес инсталляции Nextcloud>/api/oauth/return`.

  🔍 Подробнее о создании приложений читайте в инструкции.

3. Откройте настройки приложения и скопируйте значения полей:

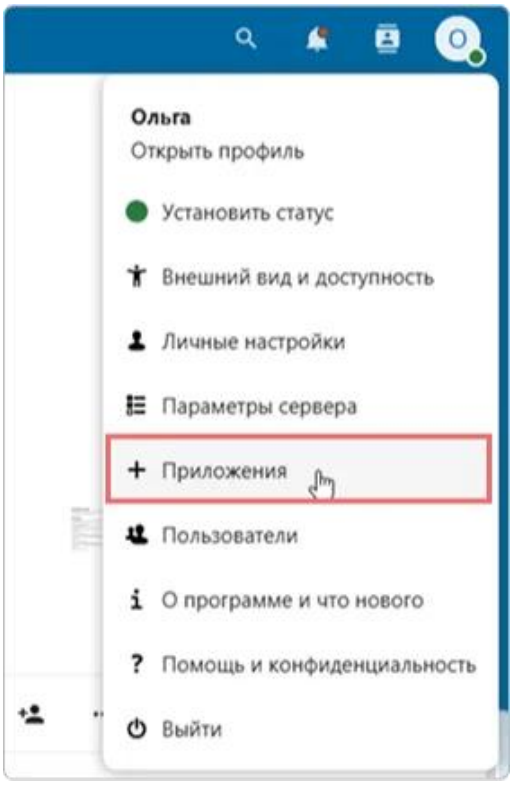
   - **Идентификатор** (`Client_id`),
   - **Секретный ключ** (`client_secret`).

Шаг 2. Настройки на стороне Nextcloud

1. Авторизуйтесь в **Nextcloud** с правами администратора.

2. Установите приложение **Social Login**. Это приложение позволяет пользователям входить в систему **Nextcloud** с использованием учетных записей сторонних сервисов. Подробнее о приложении читайте на apps.nextcloud.com.

   - Перейдите в раздел **Приложения** → **Социальное и связь**.



   - Нажмите **Скачать и включить** для приложения **Social Login**.

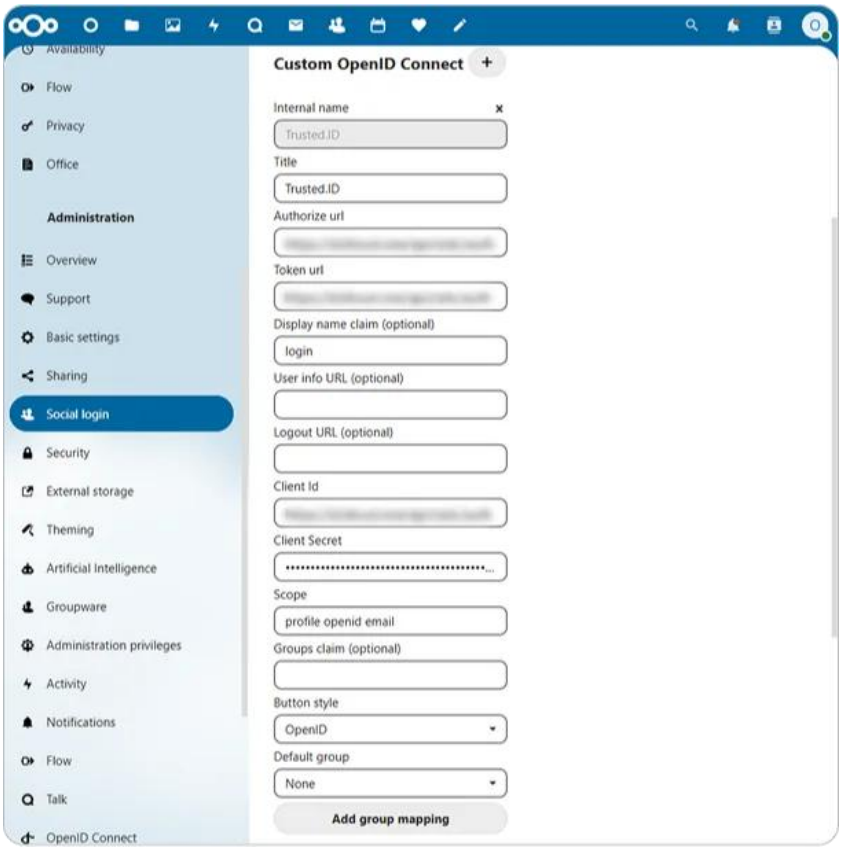
После установки приложения в разделе **Параметры сервера** появится подраздел **Social login**.

3. Перейдите в раздел **Параметры сервера** → подраздел **Social login** (Социальный вход).

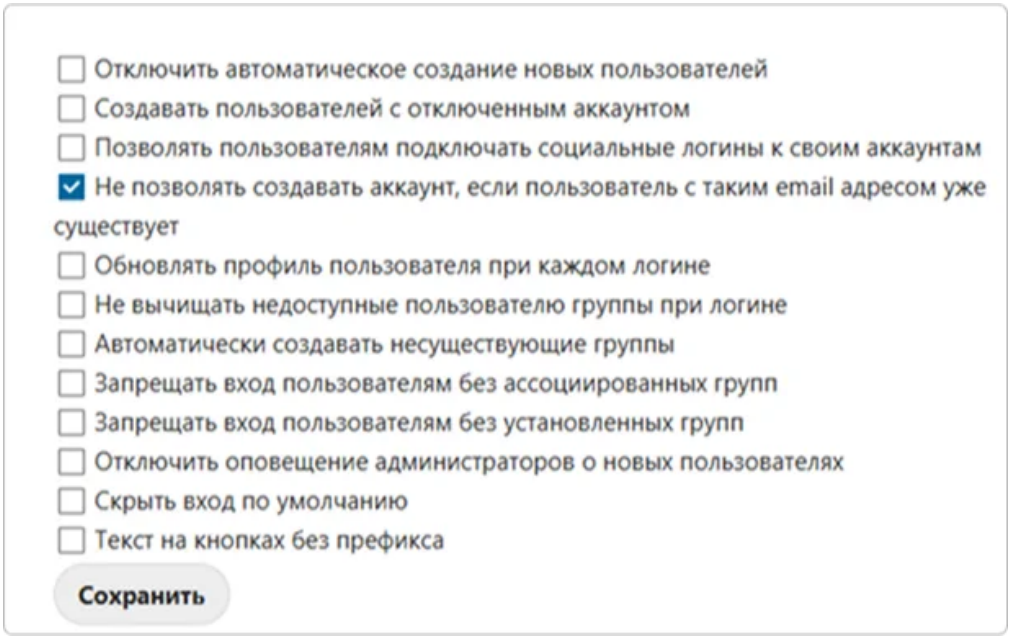
4. Нажмите кнопку + рядом с полем **Custom OpenID Connect** (Пользовательское подключение OpenID).

5. Заполните параметры подключения:

   - **Внутреннее имя** - укажите внутреннее название сервиса аутентификации, которое будет отображаться в настройках **Nextcloud**.
   - **Название** - укажите название сервиса аутентификации, понятное пользователям. Название будет отображаться на кнопке страницы аутентификации и в настройках **Nextcloud**.
   - **Authorize url** - укажите URL для авторизации. Например, `https://<адрес инсталляции КриптоАРМ IDM>/api/oidc/auth`.
   - **URL token** - укажите URL для получения токена доступа. Например, `https://<адрес инсталляции КриптоАРМ IDM>/api/oidc/token`.
   - **Client id** - укажите значение, созданное на **шаге 1**.
   - **Client Secret** - укажите значение, созданное на **шаге 1**.
   - **Scope** - укажите необходимые разрешения для получения данных. Обязательный scope - `openid` и стандартный scope - `profile` . При указании нескольких разрешений разделите их пробелом. Например: `profile email openid`.



6. При необходимости выставите дополнительные настройки:



После завершения всех шагов в виджете авторизации **Nextcloud** отобразится кнопка входа для **КриптоАРМ IDM**.

Шаг 3. Проверка подключения

1. Откройте страницу входа в **Nextcloud**.
2. Убедитесь, что появилась кнопка **Вход через КриптоАРМ IDM**.
3. Нажмите на кнопку и выполните вход, используя корпоративные учетные данные:
   - Вы будете перенаправлены на страницу аутентификации **КриптоАРМ IDM**;
   - После успешного входа вы попадёте обратно в **Nextcloud**, авторизованным пользователем.

Как настроить интеграцию Rocket.Chat с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **Rocket.Chat** через систему **КриптоАРМ IDM**.

> 📌 Rocket.Chat — это платформа для обмена сообщениями с открытым исходным кодом, предназначенная для командной работы и коммуникации. Она предоставляет функционал, аналогичный таким сервисам, как **Slack** или **Microsoft Teams**, но с возможностью самостоятельного развертывания на собственном сервере.

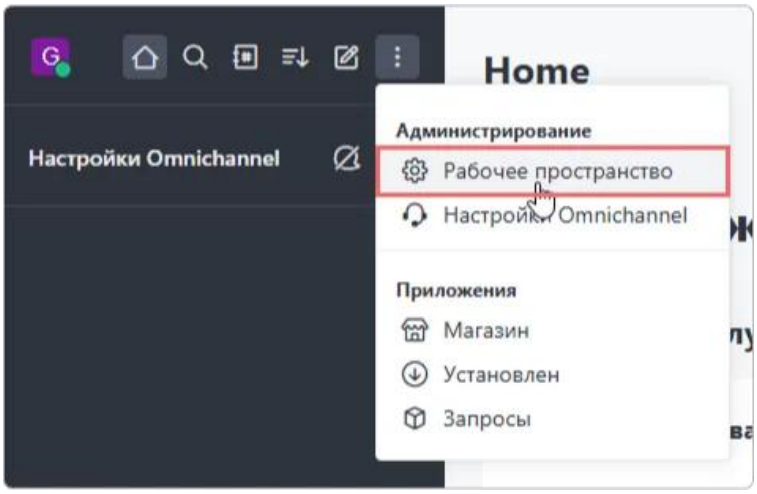
Настройка входа через **КриптоАРМ IDM** состоит из нескольких ключевых этапов, которые выполняются в двух разных системах:

- Шаг 1. Создание подключения в Rocket.Chat
- Шаг 2. Создание приложения
- Шаг 3. Настройка подключения в Rocket.Chat
- Шаг 4. Проверка подключения

Шаг 1. Создание подключения в Rocket.Chat

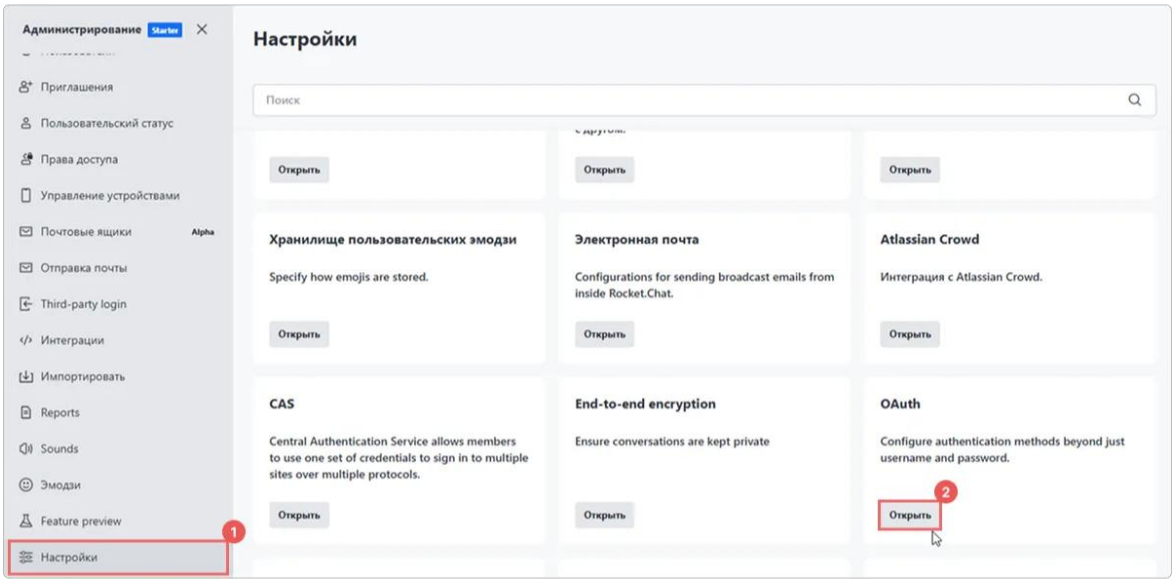
1. Авторизуйтесь в **Rocket.Chat** с правами администратора.

2. Вызовите меню и выберите пункт **Рабочее пространство**.

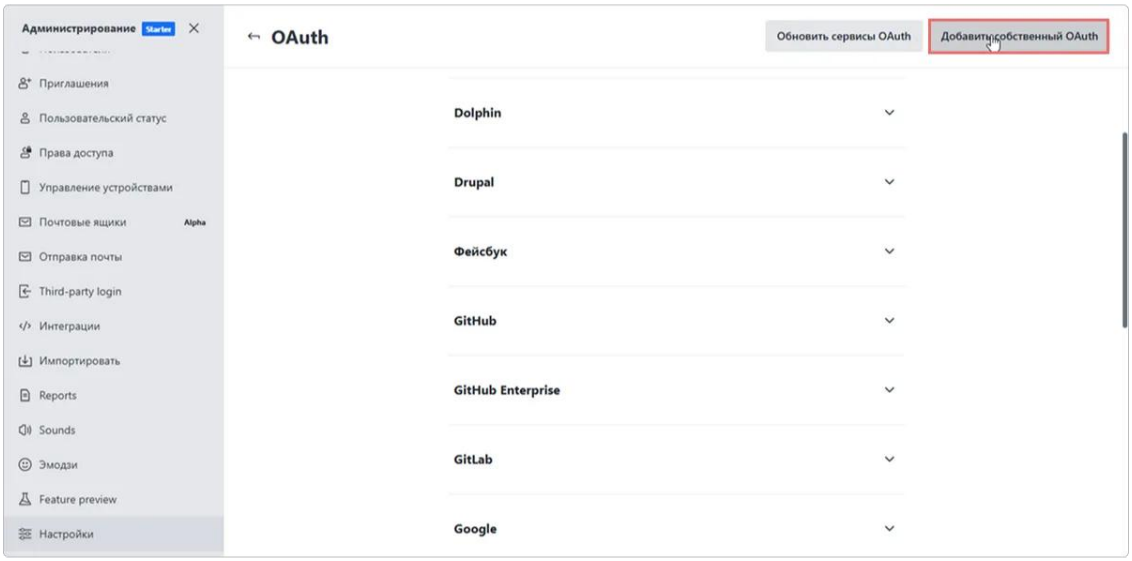


3. Откроется раздел **Администрирование**.

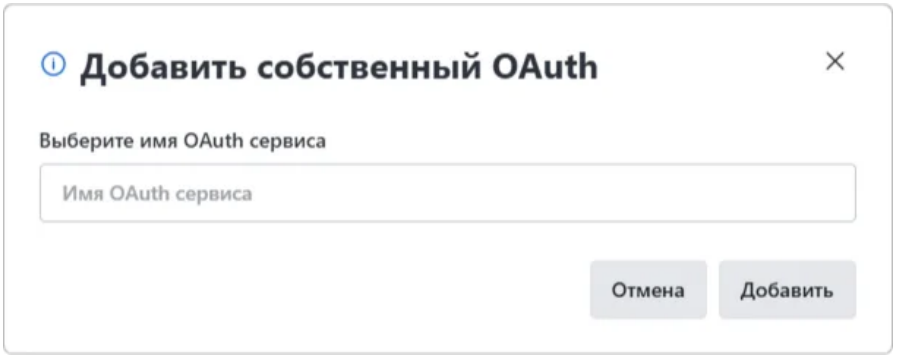
4. Перейдите в подраздел **Настройки** и нажмите **Открыть** в блоке **OAuth**.



5. Нажмите кнопку **Добавить собственный OAuth**.

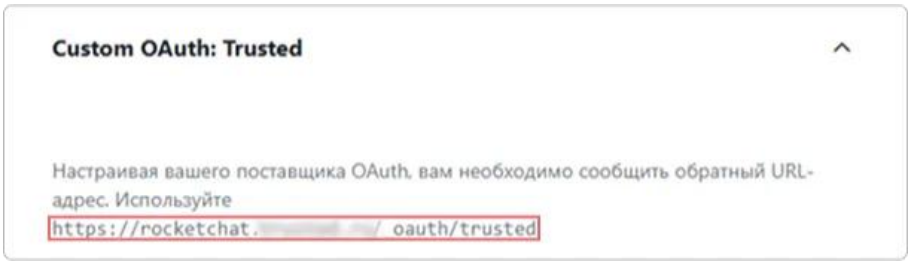


6. В появившемся окне укажите уникальное название для подключаемого **OAuth сервиса** и нажмите **Добавить**.



7. Созданное подключение отобразится в общем списке подключений. Если этого не произошло, обновите страницу в браузере.

8. Раскройте настройки подключения и скопируйте **Возвратный URL-адрес**.



Шаг 2. Создание приложения

1. Авторизуйтесь в **КриптоАРМ IDM**.

2. Создайте новое приложение, в котором укажите:

- **Адрес приложения** - адрес инсталляции **Rocket.Chat**;

- **Возвратный URL #1 (Redirect_uri)** - вставьте скопированное значение из созданного подключения в **Rocket.Chat**.

  🔍 Подробнее о создании приложений читайте в инструкции.

3. Откройте настройки приложения и скопируйте значения полей:

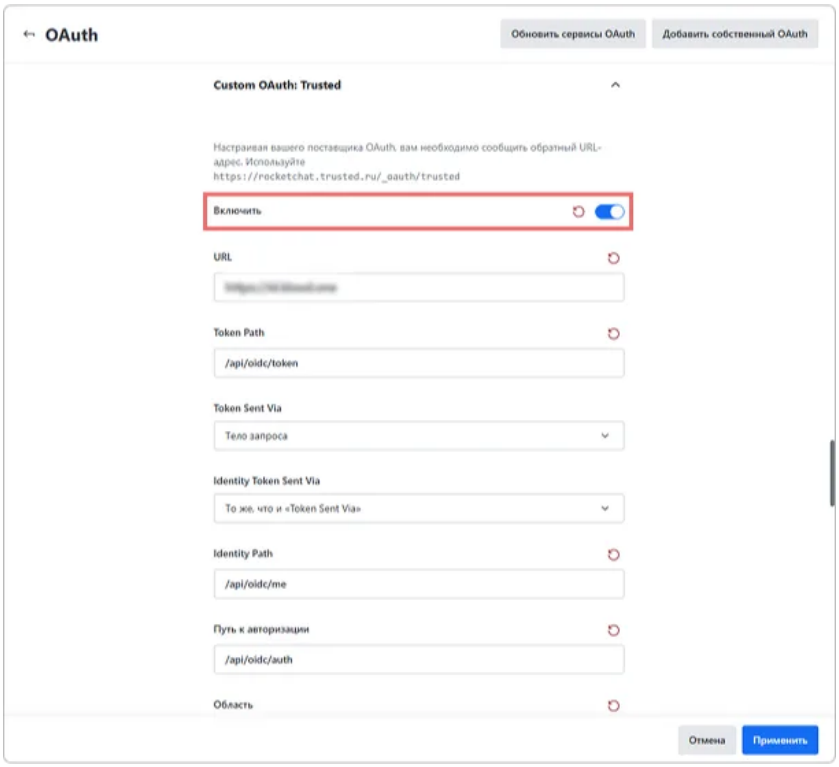
   - **Идентификатор** (`Client_id`),
   - **Секретный ключ** (`client_secret`).

Шаг 3. Настройка подключения в Rocket.Chat

1. Вернитесь в **Rocket.Chat**.

2. Откройте настройки подключения, созданного на шаге 1.

3. Активируйте переключатель **Включить** для активации работы подключения, либо активируйте позже после настройки всех параметров.



4. Укажите параметры подключения:

   - **URL** — URL-адрес сервиса КриптоАРМ IDM. Например: `https://<адрес инсталляции КриптоАРМ IDM>`
   - **Token Path** — это часть URL-адреса Token Endpoint, которая указывает путь для получения токенов. Например: **/api/oidc/token**.

- **Identity Path** — конечная точка с информацией о пользователе. Например: **/api/oidc/me**.
- **Authorize Path** (Путь к авторизации) - путь от конечной точки авторизации. Например: **/api/oidc/auth**.
- **Scope** (Область) — необходимые разрешения для получения данных. Обязательный scope - **openid** и стандартный scope - **profile** . При указании нескольких разрешений разделите их пробелом. Например: **profile email openid**.
- **Id** (Идентификатор) - Идентификатор (`Client_id`). Скопируйте значение, созданное на шаге 2.
- **Secret** (Ключ) — Секретный ключ (`Client_secret`). Скопируйте значение, созданное на шаге 2.

5. Укажите остальные настройки. С подробным описанием настроек можно ознакомиться на портале документации docs.rocket.chat.

6. Сохраните настройки подключения.

После завершения всех шагов в виджете авторизации **Rocket.Chat** отобразится кнопка входа для **КриптоАРМ IDM**.

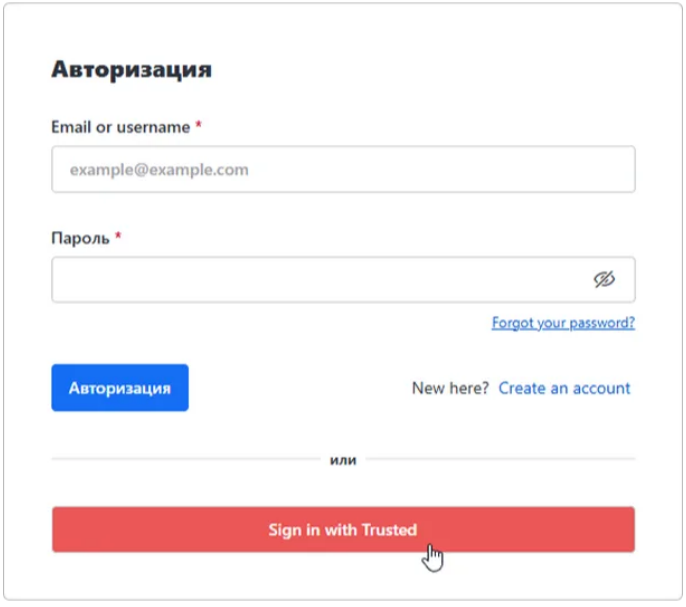
Шаг 4. Проверка подключения

1. Откройте страницу входа в **Rocket.Chat**.

2. Убедитесь, что появилась кнопка **Вход через КриптоАРМ IDM**.

3. Нажмите на кнопку и выполните вход, используя корпоративные учетные данные:

   - Вы будете перенаправлены на страницу аутентификации **КриптоАРМ IDM**;
   - После успешного входа вы попадёте обратно в **Rocket.Chat**, авторизованным пользователем.



Как настроить интеграцию Sentry с КриптоАРМ IDM

В этом руководстве вы узнаете, как настроить единый вход (SSO) в **Sentry** через систему **КриптоАРМ IDM**.

Sentry — это платформа для мониторинга и отслеживания ошибок в приложениях. Она помогает разработчикам выявлять, анализировать и исправлять ошибки в реальном времени, улучшая качество программного обеспечения.

Базовая версия продукта не поддерживает аутентификацию через **OpenID Connect**. Чтобы реализовать эту функцию, можно использовать дополнительное решение — sentry-auth-oidc. Это специальный провайдер, который обеспечивает интеграцию **OpenID Connect** с **Sentry** и позволяет настроить единый вход (SSO) в системе.

Настройка входа через **КриптоАРМ IDM** состоит из нескольких ключевых этапов, которые выполняются в двух разных системах:

- Шаг 1. Создание приложения
- Шаг 2. Установка sentry-auth-oidc
- Шаг 3. Проверка подключения

Шаг 1. Создание приложения

1. Авторизуйтесь или зарегистрируйтесь **КриптоАРМ IDM**.

2. Создайте приложение с настройками:

Поле	Значение
Адрес приложения	Адрес инсталляции системы **Sentry**
Возвратный URL #1 (Redirect_uri)	`<адрес инсталляции>/auth/sso`

   🔍 Подробнее о создании приложений читайте в инструкции.

3. Откройте настройки приложения и скопируйте значения полей:
   - **Идентификатор** (`Client_id`),
   - **Секретный ключ** (`client_secret`).

Шаг 2. Установка sentry-auth-oidc

1. Для установки провайдера выполните консольную команду:

   ```
   $ pip install sentry-auth-oidc
   ```

   или создайте Shell-скрипт с содержимым

   ```
   #!/bin/bash
   set -euo pipefail
   apt-get update
   pip install sentry-auth-oidc
   ```

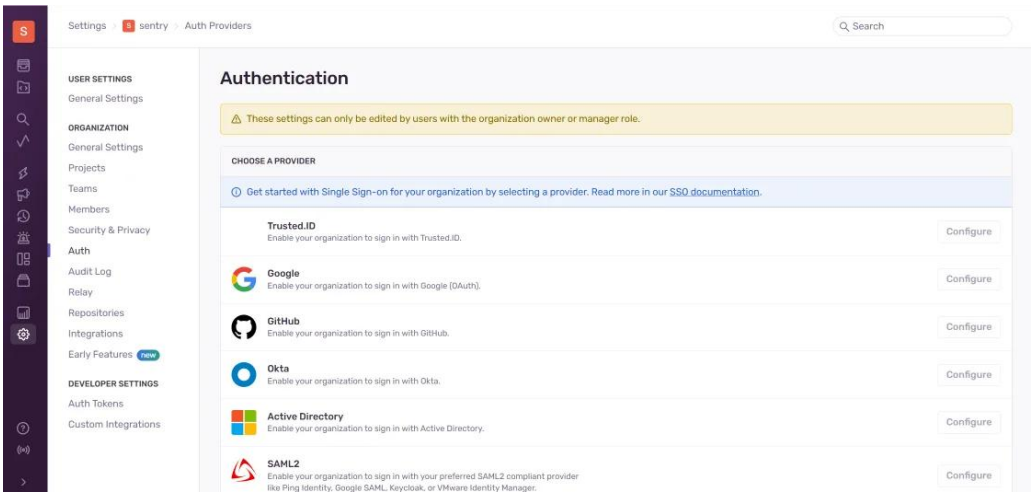
и запустите его из каталога `<путь к Sentry>/sentry/`.

2. После установки провайдера отредактируйте файл конфигурации **Sentry** `sentry.conf.py`. В файле конфигурации добавьте блок переменных с параметрами **OIDC_CLIENT_ID** и **OIDC_CLIENT_SECRET**, скопированными из приложения **КриптоАРМ IDM**.

```
##################
# OIDC #
##################

#SENTRY_MANAGED_USER_FIELDS = ('email', 'first_name', 'last_name',
'password', )

OIDC_CLIENT_ID = "client id из приложения КриптоАРМ IDM"
OIDC_CLIENT_SECRET = "client secret из приложения КриптоАРМ IDM"
OIDC_SCOPE = "openid email profile"
OIDC_DOMAIN = "https://<адрес КриптоАРМ IDM>/api/oidc"
OIDC_ISSUER = "имя модуля для выставления разрешений"
```

После этого запустите скрипт, который лежит в корне проекта **Sentry** `install.sh`, дождитесь исполнения скрипта и запустите проект.

3. Перейдите в панель администратора **Sentry** по адресу `https://<путь к Sentry>/settings/sentry/` и выберите раздел **Auth**. Далее выберите приложение **КриптоАРМ IDM**.



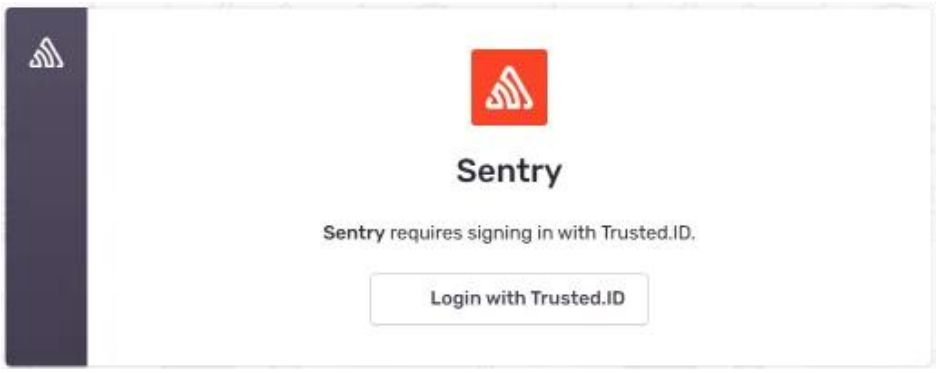
Выставите все необходимые настройки и сохраните изменения. После этого будет включена авторизация с помощью **КриптоАРМ IDM**, а вход по логину/паролю будет отключен.

Шаг 3. Проверка подключения

1. Откройте страницу входа в **Sentry**.

2. Убедитесь, что появилась кнопка **Вход через КриптоАРМ IDM**.

3. Нажмите на кнопку и выполните вход, используя корпоративные учетные данные:
   - Вы будете перенаправлены на страницу аутентификации **КриптоАРМ IDM**;
   - После успешного входа вы попадёте обратно в **Sentry**, авторизованным пользователем.



Каталог в КриптоАРМ IDM

В этой инструкции вы узнаете, как устроен каталог IDM, зачем нужны папки и группы, как управлять пользователями — создавать, перемещать, блокировать, удалять и отслеживать их связи с внешними системами в **КриптоАРМ IDM**.

Содержание:

- Что такое каталог IDM
- Управление папками
- Управление группами
- Управление пользователями
- Смотрите также

Что такое каталог IDM

Каталог IDM — это централизованная структура хранения пользователей, групп и организационных единиц в системе **КриптоАРМ IDM**.

Каталог используется для:

- построения корпоративной структуры;
- управления учетными записями пользователей;
- организации подразделений и групп;
- синхронизации данных из внешних систем;
- управления ролями и доступом.

По принципу работы каталог IDM напоминает LDAP-каталог или Active Directory и выступает единым источником корпоративных идентификационных данных.

Структура каталога

После установки IDM в системе автоматически создается базовая структура каталога.

Каталог представляет собой древовидную иерархию, которая может содержать:

- папки;
- группы;
- пользователей;
- вложенные организационные единицы.

Такая структура позволяет организовывать корпоративные данные по подразделениям, филиалам, проектам или любым другим организационным принципам.

В каталоге IDM папки и группы выполняют разные задачи.

Элемент	Назначение
Папка	Формирует организационную структуру
Группа	Используется для логического объединения пользователей

Корневая структура

В корне каталога располагается системная группа **IDM**, которая является основой всей структуры пользователей.

Внутри группы автоматически создается системная группа **Guests**.

Группа Guests

Группа **Guests** предназначена для пользователей, зарегистрировавшихся самостоятельно и еще не включенных в корпоративную структуру организации.

Например:

- внешние пользователи;
- подрядчики;
- клиенты;
- пользователи самостоятельной регистрации.

После привязки пользователя к корпоративной структуре или внешней системе пользователь может быть перемещен в соответствующую папку или группу организации.

Управление папками

Папки используются для построения организационной структуры компании.

С их помощью можно организовывать:

- подразделения;
- филиалы;
- отделы;
- проекты;
- организационные единицы.

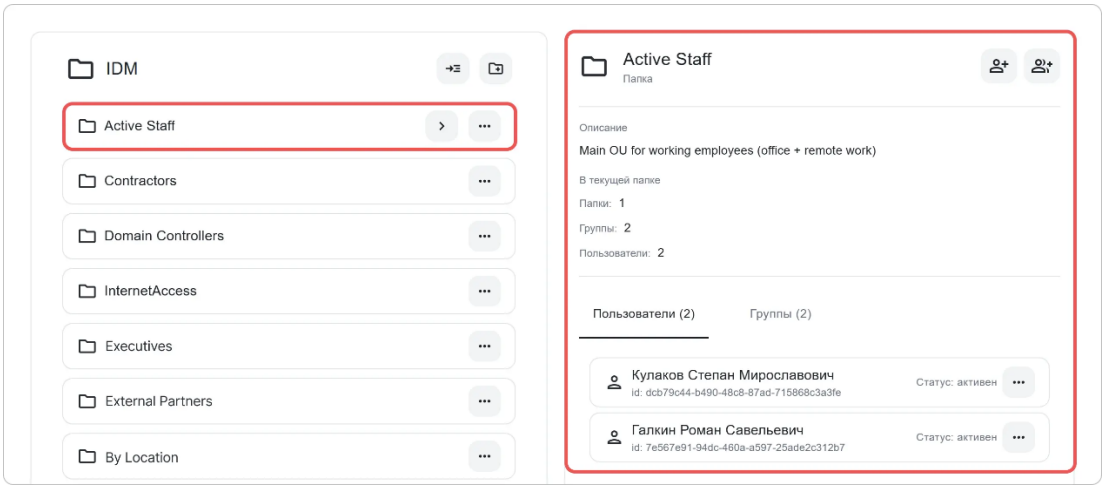
Папки могут содержать:

- другие папки;
- группы;
- пользователей.

Просмотр папки

Чтобы просмотреть содержимое папки:

1. Перейдите в панель **IDM** → **Каталог**.
2. Нажмите на нужную папку в списке.
3. В области справа откроется содержимое папки:
   - на вкладке **Пользователи** отображаются пользователи, находящиеся в данной папке;
   - на вкладке **Группы** — группы, созданные внутри папки.

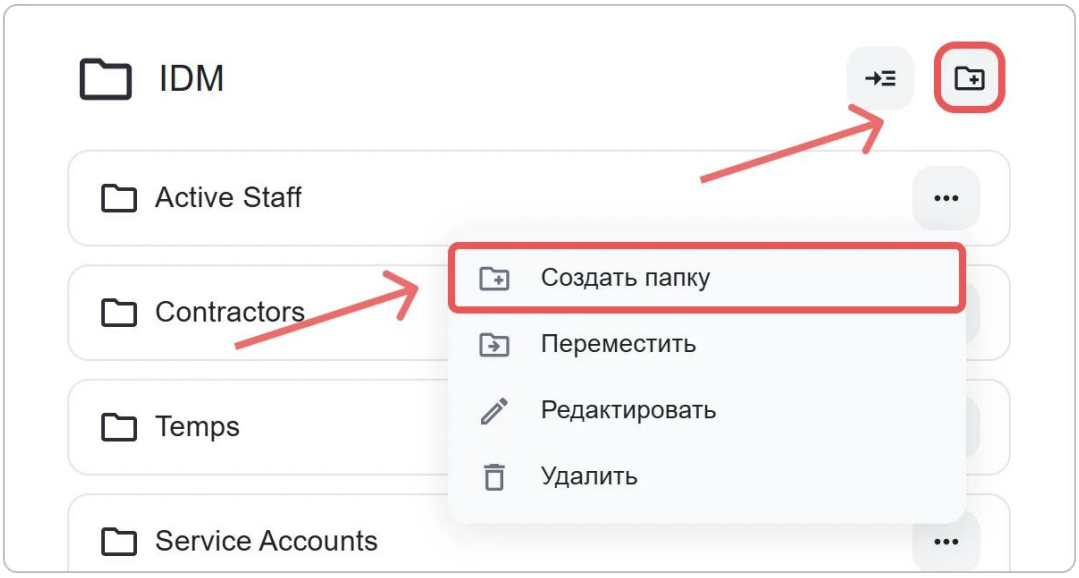


💡 Для просмотра вложенных папок нажмите кнопку  на панели с родительской папкой. После этого в списке будут отображены все дочерние папки.

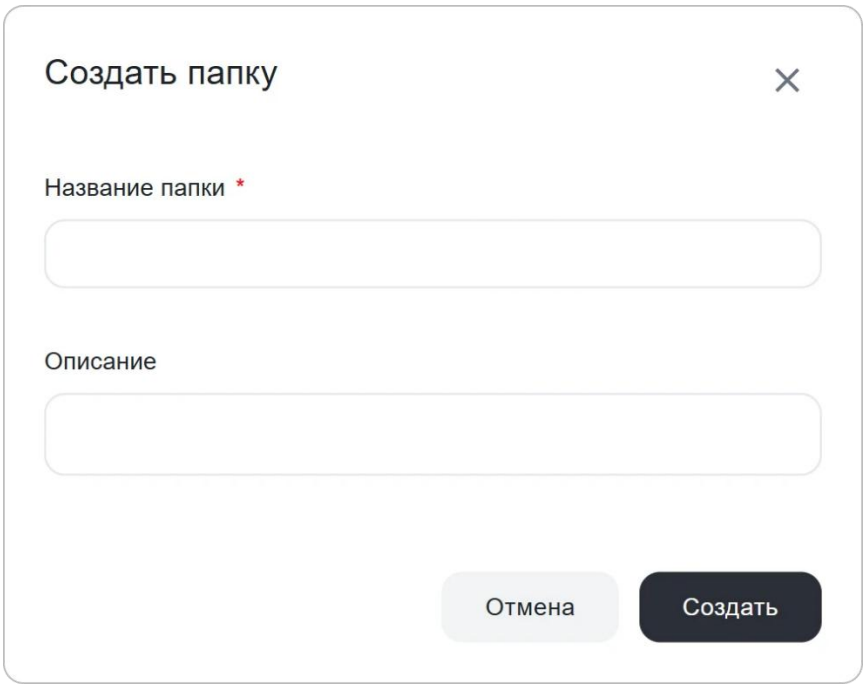
Создание папки

1. Перейдите в панель **IDM** → **Каталог**.
2. Создайте папку одним из способов:
   - Для создания папки в корне каталога нажмите на кнопку  .

- Для создания вложенной папки откройте меню действий по кнопке **Еще** на панели с нужной папкой и выберите действие **Создать папку**.



3. В открывшемся окне укажите параметры папки:
   - **Название** — отображаемое имя папки;
   - **Описание** — дополнительная информация о назначении папки (необязательно).



4. Нажмите **Создать**.

После сохранения папка появится в выбранном разделе каталога IDM.

Перемещение папки

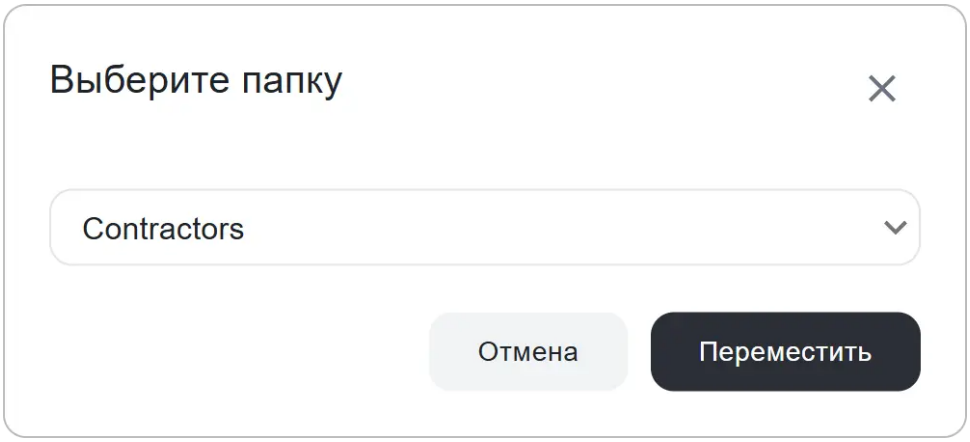
Папки можно перемещать между разделами каталога для изменения организационной структуры.

При перемещении сохраняются все вложенные объекты:

- пользователи;
- группы;
- подпапки.

Чтобы переместить папку:

1. Перейдите в панель **IDM** → **Каталог**.
2. Откройте меню действий по кнопке **Еще** на панели с нужной папкой и выберите действие **Переместить**.
3. В открывшемся окне введите название родительской папки.



4. Нажмите **Переместить**.

Редактирование папки

Для папки можно изменить название и описание.

Чтобы изменить параметры папки:

1. Перейдите в панель **IDM** → **Каталог**.
2. Откройте меню действий по кнопке **Еще** на панели с нужной папкой и выберите действие **Редактировать**.
3. В открывшемся окне укажите новые параметры папки.
4. Сохраните изменения.

Удаление папки

> ⚠️ При удалении папки удаляются все вложенные объекты, включая подпапки, группы и пользователей.

Чтобы удалить папку:

1. Перейдите в панель **IDM → Каталог**.
2. Откройте меню действий по кнопке **Еще** на панели с нужной папкой и выберите действие **Удалить**.
3. Подтвердите действие в открывшемся окне.

Управление группами

Группы используются для логического объединения пользователей.

Например:

- сотрудники отдела;
- участники проекта;
- пользователи с одинаковыми ролями;
- команды сопровождения.

Группы не влияют на организационную структуру пользователя и используются преимущественно для управления доступом.

При удалении группы пользователи не удаляются из системы.

Создание группы

Чтобы создать группу:

1. Перейдите в панель **IDM → Каталог**.
2. Выберите нужную папку.
3. В области справа нажмите кнопку **Создать группу**  .
4. В открывшемся окне укажите параметры группы:
   - **Название** — отображаемое имя группы;
   - **Описание** — дополнительная информация о назначении группы (необязательно).
5. Нажмите **Создать**.

После сохранения группа появится в выбранной папке каталога IDM.

Перемещение группы

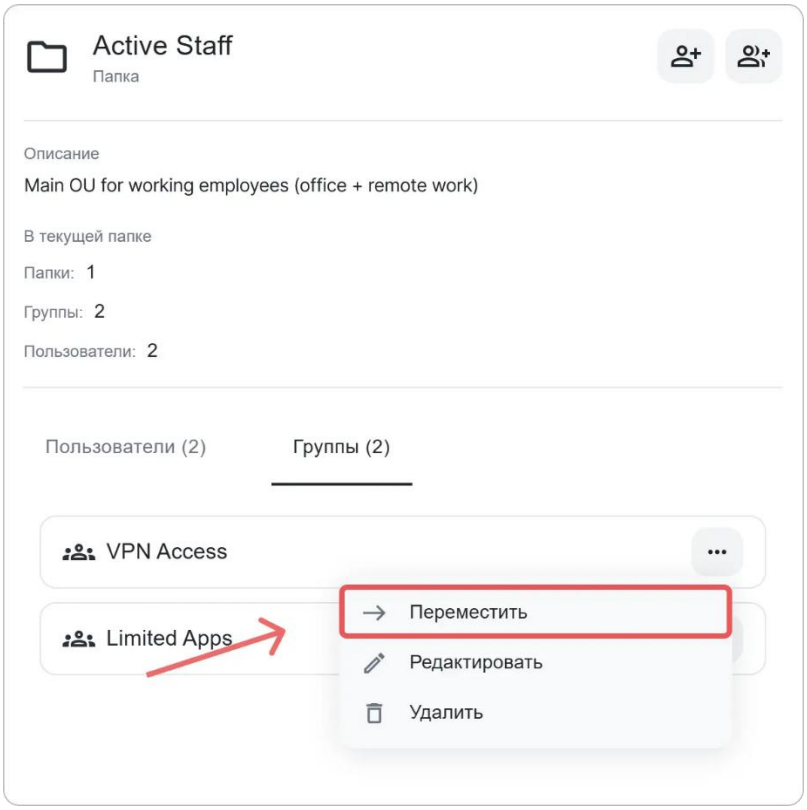
Группы можно перемещать между папками каталога.

> 💡 Перемещение группы не влияет на пользователей, входящих в нее. Состав группы и назначенные связи сохраняются.

Чтобы переместить группу:

1. Перейдите в панель **IDM → Каталог**.

2. Откройте папку, в которой находится нужная группа.
3. Перейдите на вкладку **Группы**.
4. Откройте меню действий по кнопке **Еще** на панели с нужной группой и выберите действие **Переместить**.



5. В открывшемся окне введите название папки, в которую необходимо переместить группу.
6. Нажмите **Переместить**.

После подтверждения группа будет отображаться в новой папке каталога.

Редактирование группы

Для группы можно изменить название и описание.

Чтобы изменить параметры группы:

1. Перейдите в панель **IDM → Каталог**.
2. Откройте папку, в которой находится нужная группа.
3. Перейдите на вкладку **Группы**.
4. Откройте меню действий по кнопке **Еще** на панели с нужной группой и выберите действие **Редактировать**.
5. В открывшемся окне укажите новые параметры группы.
6. Нажмите **Сохранить**.

После сохранения изменения будут применены сразу для всех пользователей и связей группы.

Удаление группы

При удалении группы:

- группа удаляется из каталога;
- пользователи сохраняются;
- связи пользователей не изменяются.

> ⚠ Удаление группы не влияет на положение пользователей в организационной структуре и не удаляет их из системы.

Чтобы удалить группу:

1. Перейдите в панель **IDM** → **Каталог**.
2. Откройте папку, в которой находится нужная группа.
3. Перейдите на вкладку **Группы**.
4. Откройте меню действий по кнопке **Еще** на панели с нужной группой и выберите действие **Удалить**.
5. Подтвердите действие в открывшемся окне.

После подтверждения группа будет безвозвратно удалена из каталога IDM.

Управление пользователями

Пользователь IDM представляет собой корпоративную учетную запись, которая может быть связана с несколькими внешними системами одновременно.

Пользователи могут быть:

- созданными вручную;
- импортированными через коннекторы;
- зарегистрированными самостоятельно;
- связанными с внешними каталогами.

Каждый пользователь может быть размещен в определенной папке каталога и входить в одну или несколько групп.

Связи пользователей с внешними системами

IDM поддерживает объединение учетных записей пользователей, полученных из разных внешних систем и каталогов.

При импорте пользователей через коннекторы IDM анализирует правила сопоставления и автоматически связывает найденные учетные записи с существующим корпоративным профилем пользователя.

Это позволяет:

- избежать дублирования пользователей;
- централизованно управлять доступом;
- поддерживать единый профиль сотрудника;
- работать одновременно с несколькими внешними системами.

Все связанные учетные записи отображаются в карточке пользователя в блоке **Связи с системами**. При необходимости связь с отдельной внешней системой можно разорвать без удаления пользователя из каталога IDM. Подробнее читайте в Просмотр связей пользователя.

Создание пользователя

Пользователи IDM могут:

- создаваться вручную;
- импортироваться через коннекторы.

При ручном создании пользователь сразу добавляется в выбранную папку каталога и становится частью корпоративной структуры.

Чтобы создать пользователя вручную:

1. Перейдите в панель **IDM** → **Каталог**.
2. Выберите папку, в которой необходимо создать пользователя.
3. В области справа нажмите кнопку **Создать пользователя**  .
4. В открывшемся окне заполните данные учетной записи пользователя.

   🔍 Поля профиля пользователя и правила их заполнения аналогичны системе ID. Подробнее см. инструкцию Создание пользователя в ID.
5. Нажмите **Сохранить**.

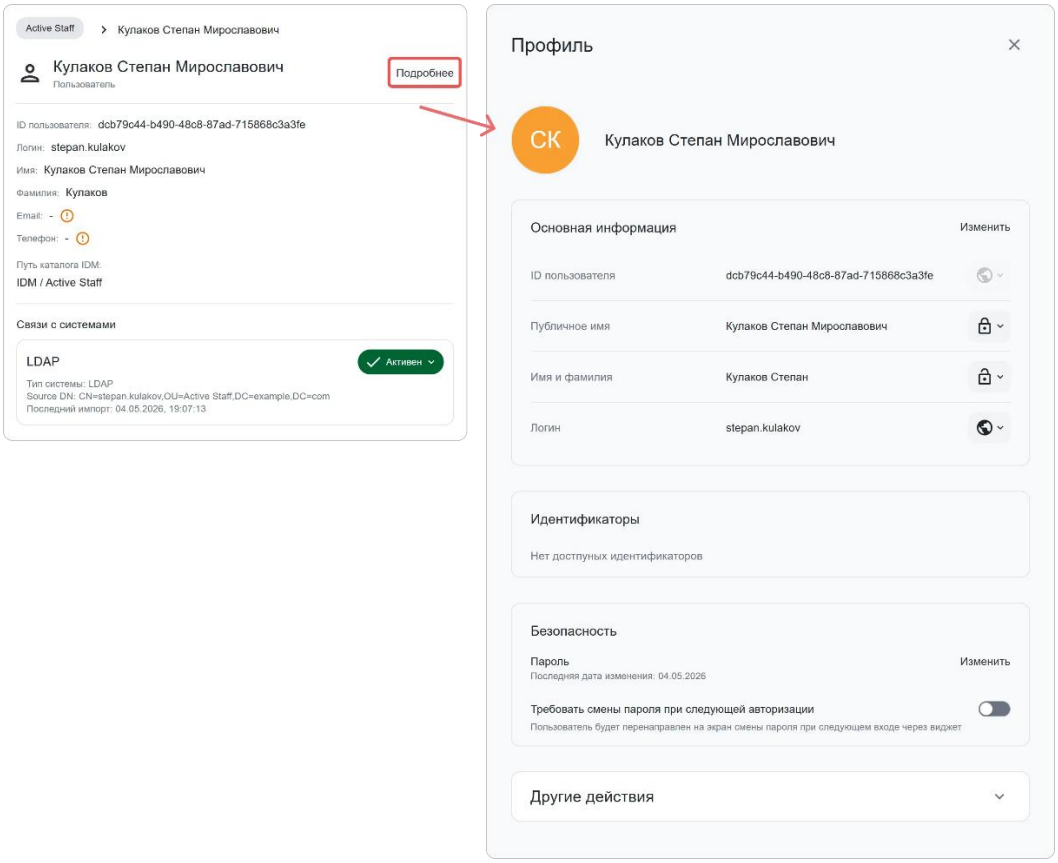
После создания пользователь появится в выбранной папке каталога IDM.

Просмотр сведений о пользователе

Чтобы просмотреть сведения о пользователе:

1. Перейдите в панель **IDM** → **Каталог**.
2. Откройте папку, в которой находится пользователь.
3. На вкладке **Пользователи** нажмите на панель нужного пользователя.
4. После этого откроется окно со сведениями о пользователе, в котором отображаются:
   - идентификатор пользователя;
   - логин;
   - имя и фамилия;

- email и телефон;
- расположение пользователя в каталоге IDM;
- связи пользователя с внешними системами.



Для перехода к полному профилю пользователя нажмите кнопку **Подробнее**.

Полный профиль пользователя позволяет:

- редактировать данные профиля;
- управлять публичностью полей;
- просматривать идентификаторы;
- завершать пользовательские сеансы;
- удалять учетную запись.

📌 Подробнее о работе с профилем пользователя читайте в инструкции Управление данными профиля ID.

Просмотр связей пользователя

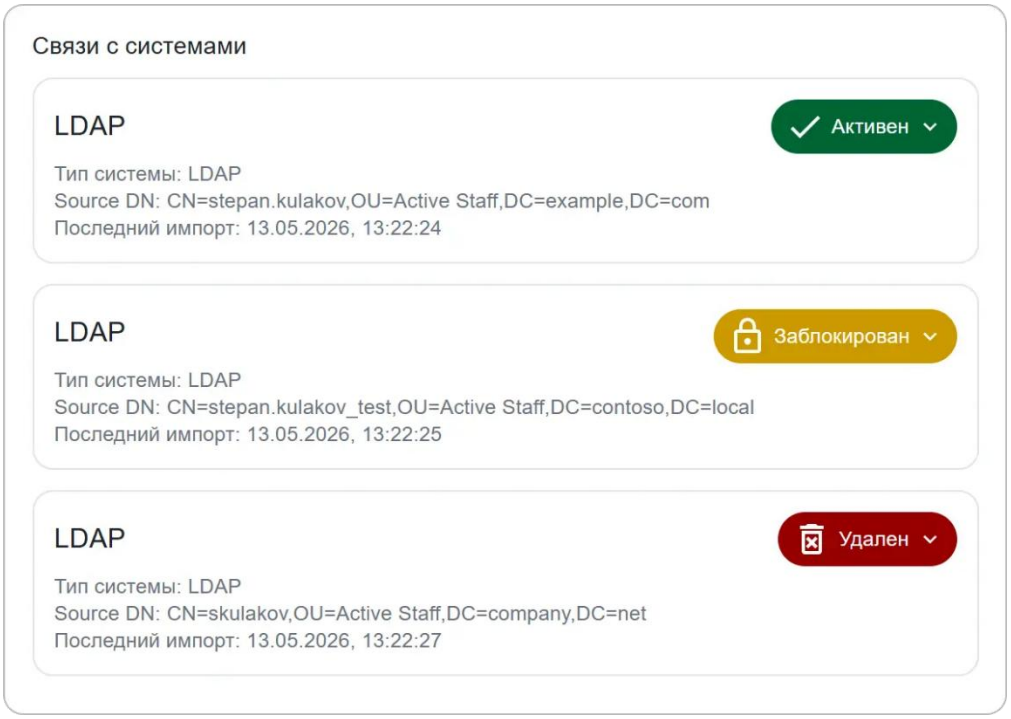
Один пользователь IDM может одновременно иметь несколько связанных систем.

Чтобы просмотреть связи пользователя:

1. Перейдите в панель **IDM** → **Каталог**.
2. Откройте папку, в которой находится пользователь.
3. На вкладке **Пользователи** нажмите на панель нужного пользователя.
4. В блоке **Связи с системами** просмотрите список подключенных систем.

Для каждой связи отображается информация о внешней системе и связанной учетной записи пользователя:

- **Активен** — Связь с внешней системой активна. Синхронизация пользователей и данных выполняется в штатном режиме.
- **Заблокирован** — Связь отключена. Синхронизация данных по данной связи блокируется в обе стороны — изменения не импортируются из внешней системы и не экспортируются обратно.
- **Удален** — Учетная запись пользователя была удалена во внешней системе. Связь с пользователем IDM автоматически разрывается и получает статус **Удален**.



Разрыв связи с внешней системой

При необходимости связь пользователя с отдельной внешней системой можно разорвать.

После разрыва связи:

- пользователь останется в каталоге IDM;
- связь с выбранной системой будет удалена;
- импортированные данные из этой системы перестанут синхронизироваться для данного пользователя.

Чтобы разорвать связь:

1. В блоке **Связи с системами** откройте меню действий нужной связи.
2. Выберите действие **Заблокирован**.
3. Подтвердите действие в открывшемся окне.

Перемещение пользователя

Пользователя можно перемещать между папками каталога.

Перемещение позволяет изменять положение пользователя в организационной структуре компании.

1. Перейдите в панель **IDM** → **Каталог**.
2. Откройте папку, в которой находится пользователь.
3. На вкладке **Пользователи** откройте меню действий с нужным пользователем и выберите действие **Переместить**.
4. В открывшемся окне введите название папки, в которую необходимо переместить пользователя.
5. Нажмите **Переместить**.

После подтверждения пользователь будет отображаться в новой папке каталога.

Блокировка пользователя

Блокировка пользователя временно запрещает доступ ко всем связанным системам, приложениям и корпоративным ресурсам.

После блокировки:

- пользователь не сможет авторизоваться в подключенных системах;
- доступ к ресурсам и ролям будет ограничен;
- учетная запись останется в каталоге IDM;
- связи с внешними системами и группами сохранятся.

> 💡 Блокировка подходит для временного ограничения доступа без удаления учетной записи и потери связей пользователя.

Чтобы заблокировать пользователя:

1. Перейдите в панель **IDM** → **Каталог**.
2. Откройте папку, в которой находится пользователь.
3. На вкладке **Пользователи** откройте меню действий с нужным пользователем и выберите действие **Заблокировать**.
4. Подтвердите действие в открывшемся окне.

После подтверждения пользователь будет переведен в статус заблокированного.

Удаление пользователя

Удаление пользователя полностью удаляет учетную запись из каталога IDM.

При удалении:

- удаляются связи пользователя;
- удаляются корпоративные назначения;
- пользователь теряет доступ ко всем ресурсам.

⚠ Удаление пользователя является необратимой операцией.

Чтобы удалить пользователя:

1. Перейдите в панель **IDM → Каталог**.
2. Откройте папку, в которой находится пользователь.
3. На вкладке **Пользователи** откройте меню действий с нужным пользователем и выберите действие **Удалить**.
4. Подтвердите действие в открывшемся окне.

После подтверждения учетная запись будет полностью удалена из каталога IDM.

Смотрите также

- Обзор КриптоАРМ IDM — общая информация о системе IDM, её назначении и компонентах.
- RBAC модель в КриптоАРМ IDM — описание ролевой модели доступа, ресурсов, ролей и их связи с пользователями и группами.
- **Коннекторы в КриптоАРМ IDM — обзор коннекторов в КриптоАРМ IDM, включая принципы работы, типы интеграций и общую модель синхронизации с внешними системами.**

RBAC в КриптоАРМ IDM

В этом руководстве вы узнаете, что такое RBAC, как он реализован в **КриптоАРМ IDM**, научитесь управлять системами, ресурсами, ролями, а также назначать доступ пользователям и группам.

Содержание:

- Основные понятия RBAC
- Как работает RBAC в КриптоАРМ IDM
- Управление системами RBAC
- Управление ресурсами
- Управление ролями
- Назначение пользователей и групп
- Наследование прав
- Влияние RBAC на приложения ID
- Смотрите также

Основные понятия RBAC

RBAC (Role-Based Access Control) — это механизм ролевого управления доступом в **КриптоАРМ IDM**, который позволяет централизованно управлять правами пользователей и групп в корпоративных системах.

RBAC-модель определяет:

- к каким ресурсам пользователь может получить доступ;
- какие действия ему разрешены;
- через какие роли предоставляются права;
- какие пользователи и группы участвуют в системе доступа.

В **КриптоАРМ IDM** RBAC тесно интегрирован с системой **ID** и может использоваться для ограничения входа в приложения.

RBAC-модель в **КриптоАРМ IDM** строится из нескольких ключевых сущностей.

Сущность	Назначение
Система	Логическая область управления доступом
Ресурс	Объект, к которому предоставляется доступ
Роль	Набор разрешений внутри системы
Пользователь	Учетная запись IDM
Группа	Объединение пользователей для массового назначения прав

Как работает RBAC в КриптоАРМ IDM

RBAC в **КриптоАРМ IDM** работает по следующему принципу:

1. Создается система RBAC.
2. Внутри системы создаются ресурсы и роли.
3. Пользователям или группам назначаются роли.
4. Роли предоставляют доступ к ресурсам.
5. При авторизации система проверяет назначенные роли и определяет доступ пользователя.

RBAC позволяет централизованно управлять доступом без необходимости вручную назначать права каждому пользователю.

Управление системами RBAC

Система RBAC — это контейнер, внутри которого объединяются ресурсы, роли и назначения пользователей.

В качестве системы могут использоваться:

- корпоративные приложения;

- внутренние сервисы;
- порталы;
- информационные системы.

В **КриптоАРМ IDM** системы RBAC связаны с приложениями из ID.

> 💡 В ID приложение отвечает за авторизацию и вход пользователя, а в IDM это же приложение выступает как сущность RBAC для управления доступом.

Каждая система может включать:

- список ресурсов;
- набор ролей;
- пользователей;
- группы пользователей;
- правила доступа.

Создание системы

1. Перейдите в панель **IDM** → **RBAC**.
2. Нажмите на кнопку **Создать систему**  .
3. Укажите параметры системы:
   - **Название системы** — отображаемое имя системы;
   - **Описание** — дополнительная информация о системе (необязательно);
   - **Адрес системы** — URL системы, которое будет использоваться в RBAC.
4. Нажмите **Создать**.

Удаление системы

1. Перейдите в панель **IDM** → **RBAC**.
2. Нажмите на кнопку **Удалить**  на панели с нужной системой.
3. Подтвердите действие в открывшемся окне.

Управление ресурсами

Ресурс — это объект доступа внутри системы RBAC.

Ресурсы используются для разграничения доступа пользователей и групп к отдельным компонентам системы или приложения.

В качестве ресурсов могут выступать:

- разделы приложения;
- административные панели;
- внутренние сервисы;
- модули системы;
- бизнес-функции.

Создание ресурса

1. Перейдите в панель **IDM → RBAC**.
2. Откройте нужную систему и перейдите на вкладку **Ресурсы**.
3. Нажмите кнопку **Добавить** в списке ресурсов.
4. Укажите название и описание ресурса.
5. Нажмите **Создать**.

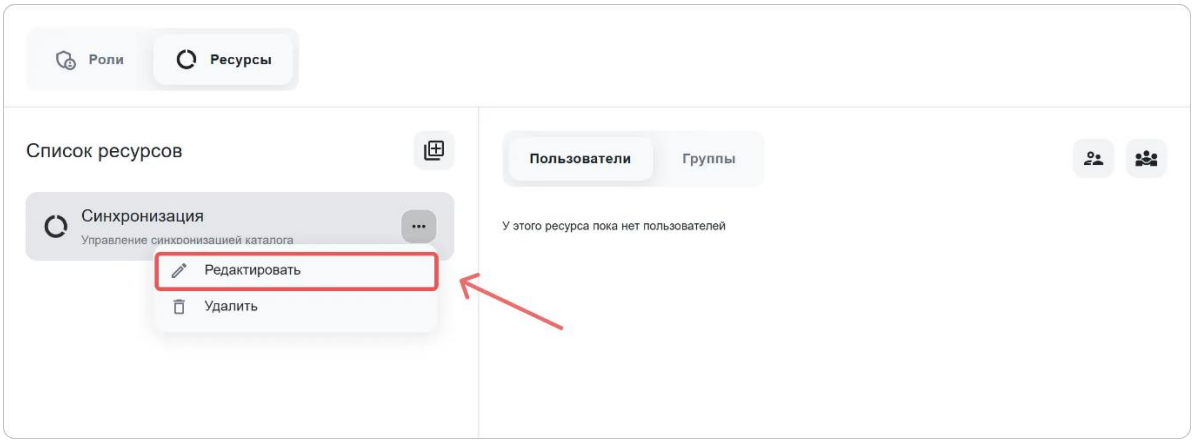
После создания ресурс появится в списке ресурсов системы и станет доступен для назначения ролей, пользователей и групп.

Редактирование ресурса

У ресурса можно изменить название и описание.

Чтобы изменить параметры ресурса:

1. Перейдите в панель **IDM → RBAC**.
2. Откройте нужную систему и перейдите на вкладку **Ресурсы**.
3. Откройте меню действий по кнопке **Еще** на панели с нужным ресурсом.
4. Выберите действие **Редактировать**.



5. В открывшемся окне укажите новые параметры ресурса.
6. Сохраните изменения.

Удаление ресурса

Удаление ресурса отменяет все связанные с ним назначения пользователей, групп и ролей.

> ⚠️ После удаления ресурс перестанет участвовать в проверке доступа. Пользователи, ранее имевшие доступ через этот ресурс, потеряют соответствующие права.

1. Перейдите в панель **IDM → RBAC**.
2. Откройте нужную систему и перейдите на вкладку **Ресурсы**.

3. Откройте меню действий по кнопке **Еще** на панели с нужным ресурсом.
4. Выберите действие **Удалить**.
5. Подтвердите действие в открывшемся окне.

Управление ролями

Роль — это логическое объединение прав доступа внутри системы.

Роли позволяют управлять доступом не для каждого пользователя отдельно, а сразу для группы пользователей с одинаковыми обязанностями.

Примеры ролей:

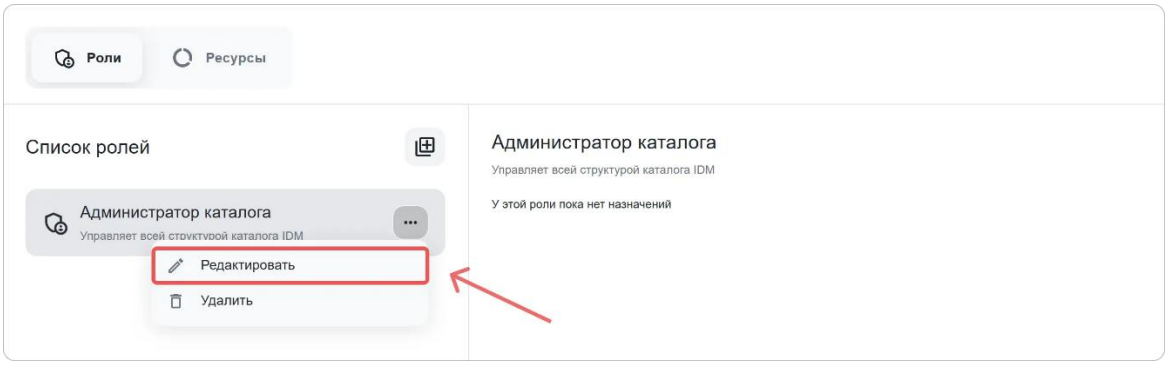
- Администратор;
- Менеджер;
- Руководитель;
- Сотрудник;
- Аудитор.

Создание роли

1. Перейдите в панель **IDM** → **RBAC**.
2. Откройте нужную систему и перейдите на вкладку **Роли**.
3. Нажмите **Добавить роль** .
4. Укажите название и описание роли.
5. Сохраните изменения.

Редактирование роли

1. Перейдите в панель **IDM** → **RBAC**.
2. Откройте нужную систему и перейдите на вкладку **Роли**.
3. Откройте меню действий по кнопке **Еще** на панели с нужной ролью.
4. Выберите действие **Редактировать**.



5. В открывшемся окне укажите новые параметры роли.
6. Сохраните изменения.

Удаление роли

1. Перейдите в панель **IDM → RBAC**.
2. Откройте нужную систему и перейдите на вкладку **Роли**.
3. Откройте меню действий по кнопке **Еще** на панели с нужной ролью.
4. Выберите действие **Удалить**.
5. Подтвердите действие в открывшемся окне.

Назначение пользователей и групп

В **КриптоАРМ IDM** доступ может назначаться:

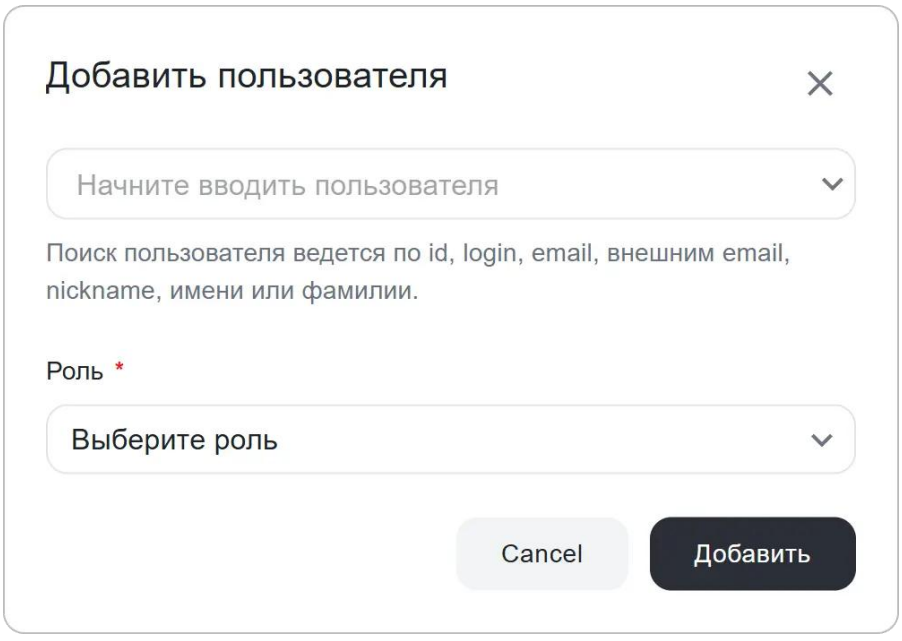
- отдельным пользователям;
- группам пользователей IDM.

Назначение через группы позволяет автоматически предоставлять доступ сразу нескольким пользователям.

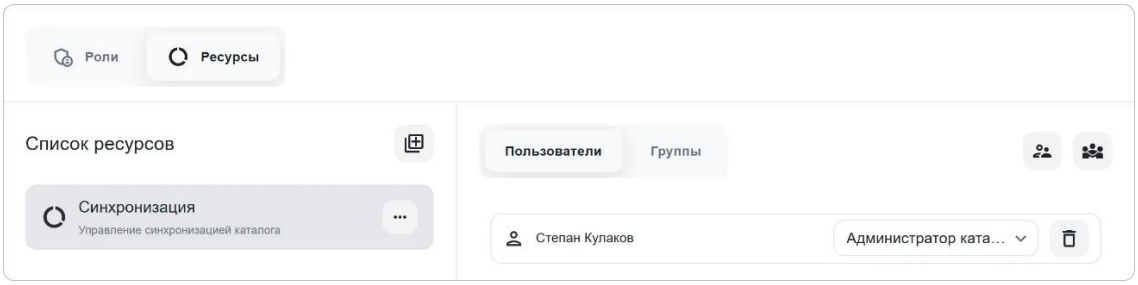
Назначение пользователя

Чтобы назначить пользователя на ресурс:

1. Перейдите в панель **IDM → RBAC**.
2. Откройте нужную систему и перейдите на вкладку **Ресурсы**.
3. В области справа перейдите на вкладку **Пользователи**.
4. Нажмите кнопку **Добавить пользователя** .
5. В открывшемся окне укажите пользователя и выберите роль.



6. Нажмите **Добавить**.

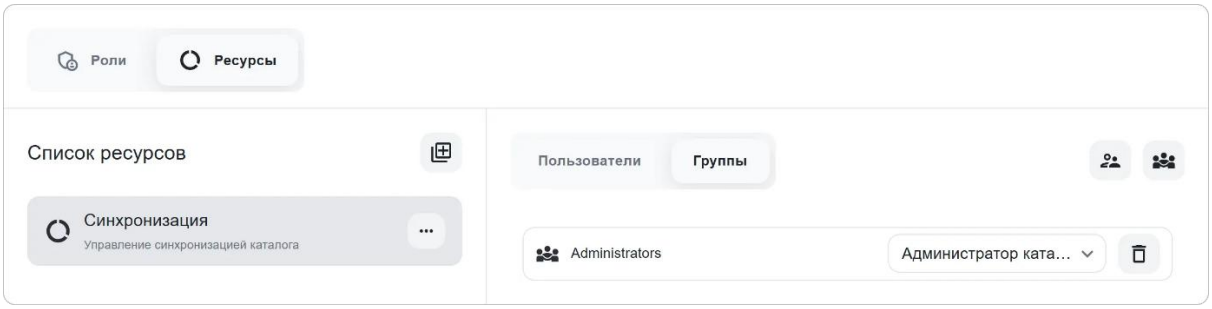


После назначения пользователь получит соответствующий доступ.

Назначение группы

Чтобы назначить группу на ресурс:

1. Перейдите в панель **IDM → RBAC**.
2. Откройте нужную систему и перейдите на вкладку **Ресурсы**.
3. В области справа перейдите на вкладку **Пользователи**.
4. Нажмите кнопку **Добавить группу** .
5. В открывшемся окне укажите группу и выберите роль.
6. Нажмите **Добавить**.



После назначения все пользователи группы получат соответствующий доступ.

> 💡 Чтобы удалить назначенного пользователя или группу из ресурса, нажмите **Удалить** на панели соответствующего пользователя или группы.
>
> 💡 Для изменения роли выберите новую роль в выпадающем списке на панели пользователя или группы.

Наследование прав

RBAC в **КриптоАРМ IDM** поддерживает наследование прав через группы.

Это означает:

- если роль назначена группе;

- все пользователи группы автоматически получают доступ;
- при добавлении нового пользователя в группу права применяются автоматически.

Наследование упрощает администрирование крупных корпоративных структур и снижает количество ручных операций.

Влияние RBAC на приложения ID

RBAC напрямую влияет на доступ пользователей к приложениям ID.

Это одна из ключевых особенностей экосистемы **КриптоАРМ IDM**.

Как это работает

Если приложение существует только в ID:

- пользователь может авторизоваться в приложении;
- доступ регулируется механизмами ID.

Если для приложения создается RBAC-модель в IDM:

- вход начинает контролироваться RBAC;
- пользователь должен иметь соответствующую роль или назначение;
- при отсутствии доступа авторизация будет запрещена.

Что происходит при отсутствии назначений

Если для приложения:

- создана RBAC-система;
- созданы ресурсы;
- но пользователю не назначен доступ,

то пользователь не сможет войти в приложение даже при успешной аутентификации через ID.

Таким образом:

- **ID** отвечает за аутентификацию пользователя;
- **IDM** отвечает за авторизацию и контроль доступа.

> 💡 ID и IDM образуют единую IAM-экосистему, где ID выполняет роль Identity Provider, а IDM — централизованной системы управления корпоративным доступом.

Смотрите также

- Обзор КриптоАРМ IDM — общая информация о системе IDM, её назначении и компонентах.

- Каталог в КриптоАРМ IDM — описание структуры каталога пользователей, групп и папок.
- **Коннекторы в КриптоАРМ IDM — обзор коннекторов в КриптоАРМ IDM, включая принципы работы, типы интеграций и общую модель синхронизации с внешними системами.**

Коннекторы в КриптоАРМ IDM

В этом руководстве вы узнаете, что такое коннекторы в **КриптоАРМ IDM**. Узнаете, чем они отличаются от доверенных провайдеров. Научитесь создавать и настраивать коннекторы, управлять правилами сопоставления пользователей, импортом и экспортом данных, а также отслеживать историю запусков.

Содержание:

- Что такое коннекторы
- Список коннекторов
- Создание коннектора
- Настройка коннектора
- История запусков
- Удаление коннектора
- Смотрите также

Что такое коннекторы

Коннекторы в **КриптоАРМ IDM** предназначены для интеграции с внешними корпоративными каталогами и системами управления пользователями. Они позволяют автоматически импортировать, синхронизировать и связывать учетные записи пользователей между IDM и внешними источниками данных.

С помощью коннекторов можно централизованно управлять корпоративными пользователями, объединять учетные записи из разных систем и поддерживать актуальность данных без ручного администрирования.

Коннекторы позволяют:

- импортировать пользователей из внешних систем;
- синхронизировать изменения профилей;
- автоматически создавать корпоративные учетные записи;
- связывать учетные записи из разных систем;
- экспортировать изменения обратно во внешнюю систему;
- поддерживать актуальность организационной структуры.

Принцип работы коннектора

Синхронизация через коннекторы включает несколько этапов:

1. Подключение к внешнему каталогу.
2. Получение пользователей и организационной структуры.
3. Сопоставление учетных записей.
4. Создание или обновление пользователей IDM.
5. Обновление связей пользователей.
6. Экспорт изменений (при необходимости).

Во время синхронизации IDM создает связи между корпоративным профилем пользователя и внешними системами.

Один пользователь IDM может иметь несколько связей одновременно.

Поддерживаемые типы коннекторов

В текущей версии **КриптоАРМ IDM** поддерживаются коннекторы:

- LDAP;
- ALD Pro.

Отличия коннекторов от доверенных провайдеров

В экосистеме **КриптоАРМ IDM** существуют два механизма интеграции с внешними системами:

Возможность	Доверенный провайдер ID	Коннектор IDM
Авторизация пользователя	✓	
Создание пользователя при первом входе	✓	
Автоматический импорт пользователей без входа		✓
Синхронизация профиля пользователя	✓ При авторизации	✓ По расписанию и вручную
Централизованный импорт пользователей		✓
Сопоставление пользователей	Ограничено	✓
Объединение учетных записей		✓
Работа с организационной структурой		✓
RBAC и корпоративный каталог		✓
Экспорт изменений во внешнюю систему		✓

Доверенные провайдеры предназначены в первую очередь для аутентификации пользователей.

При использовании доверенного провайдера:

- пользователь появляется в системе только после первого входа;
- первоначальная линковка выполняется через авторизацию;
- пользователь должен самостоятельно пройти вход через внешний провайдер.

Такой подход подходит небольшим организациям и простым сценариям интеграции.

Коннекторы IDM подходят для корпоративных сценариев с централизованным управлением пользователями и синхронизацией каталогов.

IDM самостоятельно:

- подключается к внешней системе;
- импортирует пользователей;
- создает корпоративные учетные записи;
- выполняет сопоставление пользователей;
- объединяет учетные записи из разных систем.

После импорта пользователь уже существует в IDM и может авторизоваться через доступные способы входа без необходимости первичной авторизации через провайдер.

Список коннекторов

В разделе **Коннекторы** отображается сводная информация по каждому подключению. Она позволяет быстро оценить состояние синхронизации без перехода в настройки коннектора.

Каждый коннектор отображается в виде карточки со следующими параметрами:

Основная информация

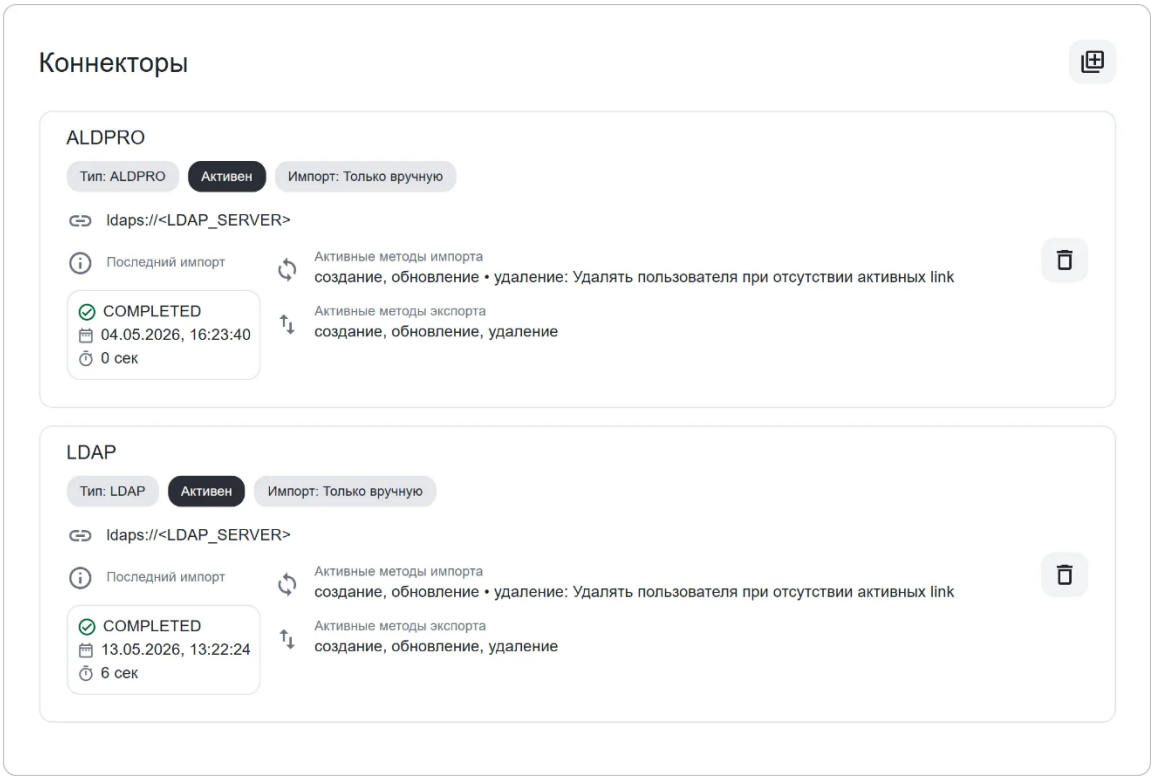
- **Имя коннектора** — название подключения
- **Тип** — тип источника данных
- **Состояние активности** — активен или отключен
- **Адрес сервера** — URL подключения

Режим синхронизации

- **Импорт** — режим выполнения импорта
- **Активные методы импорта** — какие операции выполняются при импорте
- **Активные методы экспорта** — какие операции выполняются при экспорте

Последний запуск синхронизации

- **Статус выполнения**
- **Дата и время последнего запуска**
- **Длительность выполнения**



Создание коннектора

1. Перейдите в панель **IDM → Коннекторы**.
2. Нажмите кнопку **Добавить** .
3. Создайте коннектор необходимого типа.

   Обратитесь к отдельной инструкции:

   - LDAP
   - ALD Pro
4. Сохраните изменения.

Настройка коннектора

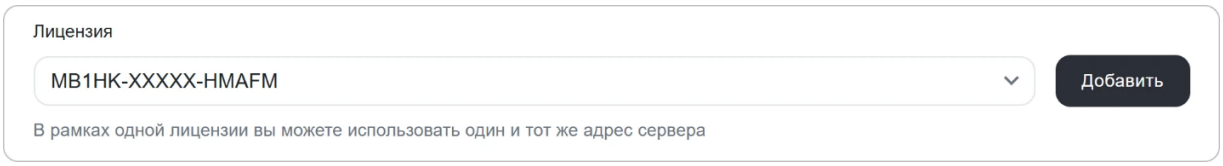
Как открыть настройки коннектора

Настройки коннектора доступны в панели IDM и позволяют управлять синхронизацией, правилами сопоставления, расписанием и параметрами подключения.

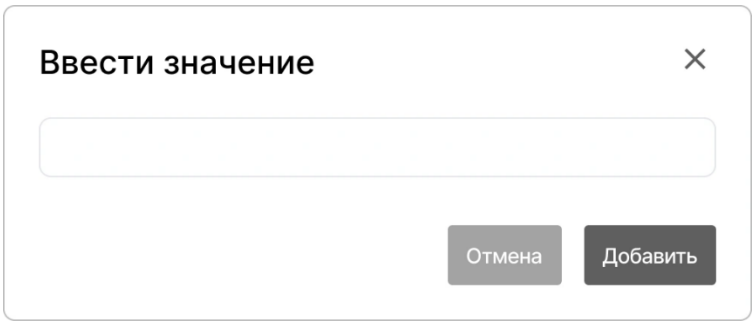
1. Перейдите в панель **IDM**
2. Откройте вкладку **Коннекторы**.
3. В списке выберите нужный коннектор.
4. Нажмите на карточку коннектора, чтобы открыть его настройки.

Привязка лицензии

1. Откройте настройки нужного коннектора.
2. Раскройте блок **Параметры подключения**.
3. В поле **Лицензия** добавьте лицензию одним из способов:
   - Выберите ключ из выпадающего списка (если лицензия уже сохранена в системе),



   - Нажмите **Добавить** и в открывшемся окне введите лицензионный ключ.



4. Сохраните изменения.

Режим синхронизации

Режим синхронизации определяет, какие операции выполняются при запуске коннектора — импорт, экспорт или их варианты с полной перезаписью данных.

Он влияет только на обработку данных и не определяет время запуска.

Чтобы настроить режим синхронизации:

1. Откройте настройки нужного коннектора.
2. В первом блоке установите необходимые настройки:

Параметр	Описание
Импортировать	Выполняет стандартный импорт данных согласно правилам сопоставления пользователей.
Импортировать (перезапись данных)	Полностью перезаписывает данные пользователя данными из внешней системы. Используется как режим полной синхронизации.
Экспортировать	Передает изменения пользователей в внешнюю систему согласно правилам экспорта.
Экспортировать (перезапись данных)	Полностью перезаписывает данные во внешней системе данными из IDM. Используется для приведения внешней

системы к состоянию IDM.

💡 Режимы с перезаписью выполняют полную синхронизацию данных и могут изменять записи во внешней системе или в IDM.

Изменения сохраняются автоматически

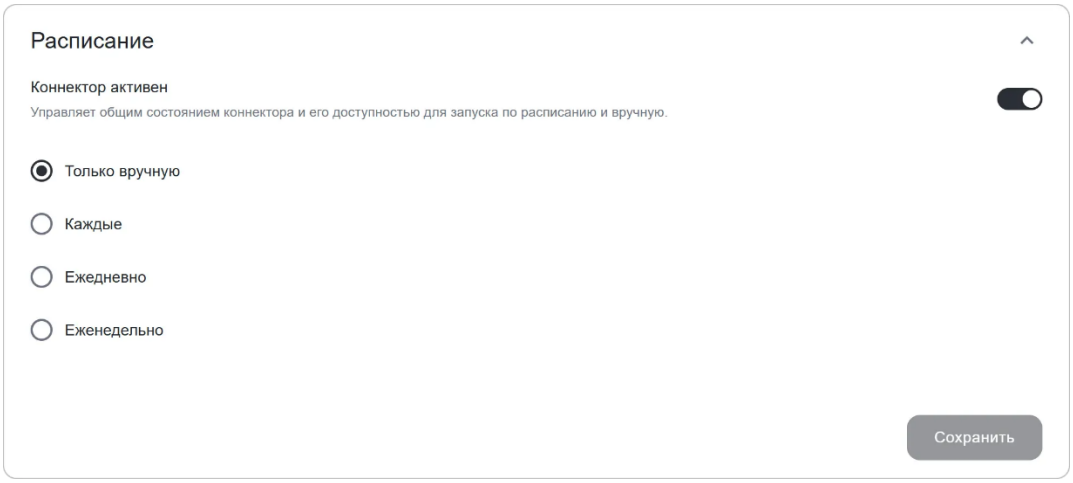
Расписание синхронизации

Расписание синхронизации определяет, когда коннектор выполняет операции импорта и экспорта. Оно не влияет на логику обработки данных — только задаёт момент запуска синхронизации.

Использование расписания позволяет автоматически поддерживать актуальность данных между IDM и внешними системами без ручного запуска.

Чтобы настроить расписание:

1. Откройте настройки нужного коннектора.
2. Раскройте блок **Расписание**.



3. Включите или отключите коннектор с помощью параметра **Коннектор активен**.

💡 Если коннектор неактивен, автоматические и ручные запуски синхронизации недоступны.

4. Установите необходимые настройки режима:

Режим	Описание
Только вручную	Синхронизация выполняется только по инициативе пользователя. Автоматические запуски отключены.
Каждые	Синхронизация запускается с заданным интервалом времени (например, каждые 15 минут или 1 час).
Ежедневно	Синхронизация выполняется один раз в день в указанное время.
Еженедельно	Синхронизация выполняется один раз в неделю в

выбранные дни и время.

5. Нажмите **Сохранить**.

Правила сопоставления пользователей

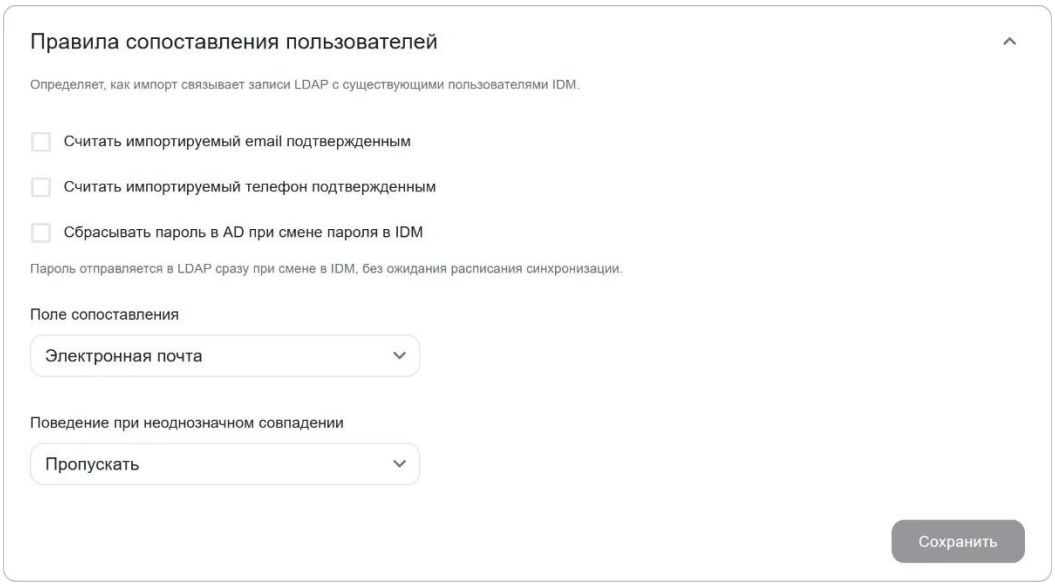
Правила сопоставления определяют, как IDM связывает записи из внешних систем с существующими учетными записями в каталоге.

Сопоставление позволяет:

- избежать дублирования пользователей;
- объединять учетные записи.

Чтобы настроить сопоставление:

1. Откройте настройки нужного коннектора.
2. Раскройте блок **Правила сопоставления пользователей**.



3. Установите параметры обработки данных:
   - **Считать импортируемый email подтвержденным** — электронный адрес, полученный из внешней системы, автоматически считается подтверждённым;
   - **Считать импортируемый телефон подтвержденным** — телефон, полученный из внешней системы, автоматически считается подтверждённым;
   - **Сбрасывать пароль при смене пароля в IDM** — пароль отправляется во внешнюю систему сразу при смене в IDM, без ожидания расписания синхронизации.
4. Выберите **поле сопоставления**:
   - Электронная почта,
   - Логин,

- Фамилия,
- Имя.

💡 Рекомендуется использовать уникальные идентификаторы (например, почта или логин) для предотвращения ложных совпадений.

5. Настройте **поведение при неоднозначном совпадении**:
   - **Пропускать** — запись не будет импортирована;
   - **Считать ошибкой** — импорт завершится с ошибкой;
   - **Создавать отдельно** — будет создан новый пользователь без объединения.
6. Нажмите **Сохранить**.

Настройка импорта

Импорт позволяет автоматически создавать и обновлять пользователей IDM на основе данных внешнего каталога.

Чтобы настроить импорт:

1. Откройте настройки нужного коннектора.
2. Раскройте блок **Параметры импорта**.
3. Включите или отключите импорт с помощью настройки **Включить импорт**.
4. Настройте, как система обрабатывает данные при получении из внешнего каталога:
   - **Создание новых пользователей** — при обнаружении новых записей во внешней системе пользователи создаются в IDM.
   - **Обновление существующих пользователей** — данные существующих пользователей обновляются в соответствии с правилами сопоставления.
5. Выберите правило обработки пользователей, удаленных во внешней системе:
   - **Только link -> Deleted** — помечает связь с внешней системой как удалённую, пользователь в IDM сохраняется;
   - **Удалять пользователя при отсутствии активных link** — пользователь удаляется из IDM, если отсутствуют активные связи с внешними системами;
   - **Всегда помечать пользователя удаленным** — Пользователь сохраняется, но получает статус «Удалён».
6. Настройте дублирование структуры:
   - **Дублировать структуру каталогов** — создаёт и обновляет папки в IDM в соответствии с внешней системой;
   - **Дублировать структуру групп** — синхронизирует группы пользователей из внешней системы.
7. Укажите параметры производительности:
   - **Многопоточность** — включает параллельную обработку данных;

- **Размер chunk** — определяет количество записей, обрабатываемых за один цикл.

8. Нажмите **Сохранить**.

Настройка экспорта

Экспорт позволяет передавать изменения из IDM во внешнюю систему, обеспечивая синхронизацию данных в обратном направлении.

> 📌 Доступность экспорта зависит от типа коннектора и настроек внешней системы.

Чтобы настроить экспорт:

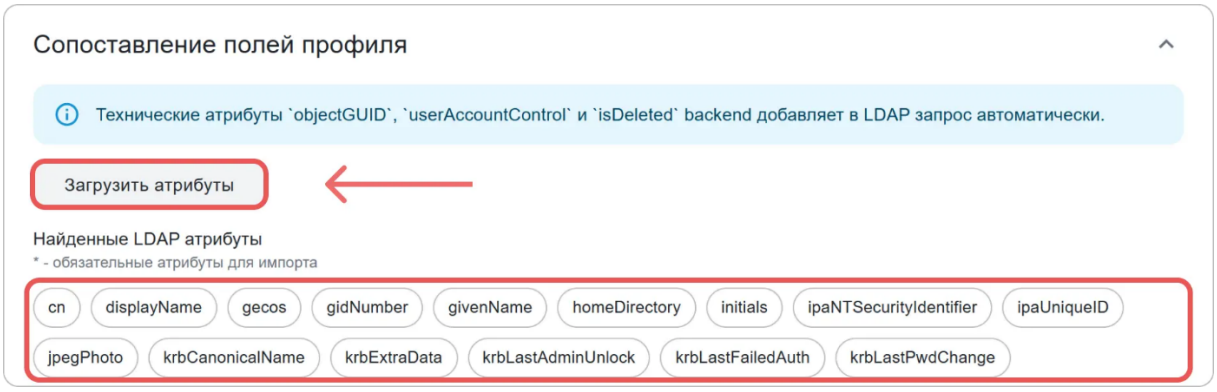
1. Откройте настройки нужного коннектора.
2. Раскройте блок **Параметры экспорта**.
3. Включите или отключите экспорт с помощью настройки **Включить экспорт**.
4. Настройте поведение при передаче данных:
   - **Создавать отсутствующие записи во внешней системе** — добавляет отсутствующие записи во внешней системе;
   - **Обновлять существующие записи во внешней системе** — синхронизирует изменения существующих записей;
   - **Удалять удалённые в IDM записи из внешней системы** — удаляет во внешней системе записи, удалённые в IDM (если поддерживается системой).
5. Настройте дублирование структуры:
   - **Дублировать IDM-структуру каталогов**;
   - **Дублировать IDM-структуру групп**.
6. Укажите параметры производительности:
   - **Многопоточность** — включает параллельную обработку данных;
   - **Размер chunk** — определяет количество записей, обрабатываемых за один цикл.
7. Нажмите **Сохранить**.

Сопоставление полей профиля

Сопоставление полей профиля определяет, как данные пользователя в IDM связываются с атрибутами пользователя внешней системы при импорте и экспорте.

> 📌 Технические атрибуты `objectGUID`, `userAccountControl` и `isDeleted` backend добавляет в запрос автоматически.

Для удобства настройки сопоставления используйте кнопку **Загрузить атрибуты** — она подгружает доступные поля из подключенной системы.



Добавление правила

1. Откройте настройки нужного коннектора.
2. Раскройте блок **Сопоставление полей профиля**.
3. В разделе **Правила импорта** или **Правила экспорта** нажмите **Добавить правило**.
4. В появившемся блоке укажите параметры правила:
   - **Поле профиля** — атрибут пользователя IDM;
   - **Атрибут внешней системы** — поле во внешней системе;
   - **Вес** — приоритет правила (чем выше, тем важнее правило при конфликте);
   - **Нормализация** — обработка значения перед сравнением или записью. Доступные варианты: `trim` (удаляет пробелы в начале и в конце строки), `lowercase` (приводит строку к нижнему регистру), `uppercase` (приводит строку к верхнему регистру), `digits_only` (оставляет только цифры, удаляя все остальные символы).

5. Нажмите **Сохранить**.

💡 Чтобы удалить правило, нажмите **Удалить** в строке соответствующего правила.

Активность правила

Каждое правило сопоставления может быть включено или отключено без удаления из конфигурации.

- **Включено** — правило применяется при импорте и экспорте данных.
- **Выключено** — правило игнорируется, значение передаётся без изменений.

💡 Отключение правила удобно для временного изменения логики сопоставления без потери настроек и без необходимости повторной настройки.

История запусков

IDM сохраняет историю всех запусков коннектора. История позволяет контролировать выполнение синхронизации, анализировать результаты импорта и экспорта, а также диагностировать ошибки подключения и обработки данных.

Для каждого запуска отображаются:

- тип операции (импорт или экспорт);
- статус выполнения;
- дата и время запуска;
- длительность выполнения;
- количество обработанных записей;
- количество ошибок.

Показатели:

Параметр	Описание
fetched	Количество записей, полученных из внешней системы
created	Количество созданных пользователей
updated	Количество обновленных пользователей
skipped	Количество пропущенных записей
deactivated	Количество деактивированных пользователей
errors	Количество ошибок обработки
duration	Общее время выполнения синхронизации

Скачивание отчета

Для каждого запуска доступна кнопка **Скачать отчет**.

Отчет выгружается в формате JSON и содержит полную техническую информацию о выполнении синхронизации:

- идентификатор задачи;
- тип запуска;
- время начала и завершения;
- статистику обработки;
- сведения об ошибках;
- параметры синхронизации;
- диагностические метаданные.

Пример структуры отчета:

```
{
  "job_id": "cmolhevco001g1gb2zyqnaj2a",
  "status": "COMPLETED",
  "trigger": "MANUAL",
  "started_at": "2026-04-30T12:50:23.160Z",
  "finished_at": "2026-04-30T12:50:25.581Z",
  "summary": {
    "fetched": 8,
    "created": 1,
    "updated": 7,
    "skipped": 0,
    "deactivated": 0,
    "errors": 0
  },
  "errors": [],
  "meta": {
    "duration_ms": 2239,
    "full_resync": true,
    "sync_direction": "IMPORT"
  }
}
```

Удаление коннектора

Коннектор можно удалить как из его настроек, так и напрямую из списка коннекторов.

Способ 1. Удаление из настроек коннектора

1. Откройте настройки нужного коннектора.
2. Раскройте блок **Другие действия**.
3. Нажмите на кнопку **Удалить коннектор**.
4. Подтвердите действие в открывшемся окне.

Способ 2. Удаление из списка коннекторов

1. Перейдите в панель **IDM** → **Коннекторы**.
2. Нажмите кнопку  на панели с нужным коннектором.
3. Подтвердите действие в открывшемся окне.

> ⚠️ При удалении коннектора удаляется только его конфигурация и история синхронизации.
>
> 💡 Пользователи, группы и папки, ранее импортированные в IDM, не удаляются автоматически и продолжают существовать в каталоге IDM как обычные объекты системы.

Смотрите также

- Обзор КриптоАРМ IDM — общая информация о системе IDM, её назначении и компонентах.

- Каталог в КриптоАРМ IDM — описание структуры каталога пользователей, групп и папок.
- RBAC модель в КриптоАРМ IDM — описание ролевой модели доступа, ресурсов, ролей и их связи с пользователями и группами.
- Подключение ALD Pro-коннектора — инструкция по подключению коннектора к системе ALD Pro.
- **Подключение LDAP-коннектора — инструкция по подключению коннектора к системе LDAP.**

Подключение коннектора ALD Pro в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке коннекторов. Общая информация доступна в инструкции Коннекторы в КриптоАРМ IDM.

ALD Pro-коннектор позволяет подключить внешнюю систему ALD Pro к **КриптоАРМ IDM** для импорта, экспорта и синхронизации пользователей.

Содержание:

- Шаг 1. Подготовка внешней системы
- Шаг 2. Создание коннектора
- Шаг 3. Привязка лицензии
- Шаг 4. Настройка коннектора
- Рекомендуемые правила сопоставления полей профиля
- Смотрите также

Шаг 1. Подготовка учетной записи в ALD Pro

На стороне внешней системы ALD Pro необходимо подготовить учетную запись, которая будет использоваться для подключения коннектора.

Рекомендуется использовать сервисную учетную запись с правами на чтение каталога пользователей и (при необходимости) изменение паролей.

Учетная запись должна:

- иметь права на чтение каталога пользователей;
- иметь права на чтение групп и организационной структуры;
- при необходимости — с правами изменения атрибутов пользователей (для экспорта).

> 💡 В большинстве случаев используется отдельная сервисная учетная запись, а не административный пользователь домена.

Шаг 2. Создание коннектора

1. Перейдите в панель **IDM → Коннекторы**.

2. Нажмите кнопку **Добавить**  .

3. В открывшемся окне укажите обязательные параметры для подключения:

   - **Имя коннектора**,
   - **Тип коннектора**: **ALD Pro**,
   - **Адрес сервера ALDPRO (aldpro_url)**,
   - **База поиска (aldpro_base)**,
   - Учетные данные администратора: **Логин администратора (aldpro_admin_dn)** и **Пароль администратора (aldpro_admin_pwd)**.

   💡 Поле **Лицензия** можно заполнить позже. Подробнее — в разделе Привязка лицензии.

4. Нажмите **Создать**.

Параметры коннектора

Параметр	Обязательное	Описание
Имя коннектора	✓	Отображаемое название коннектора в интерфейсе IDM. Используется для идентификации подключения.
Тип коннектора	✓	Тип внешней системы
Коннектор активен	✗	Включает или отключает коннектор. Неактивный коннектор не участвует в синхронизации.
Лицензия	✓	Лицензия, назначенная коннектору
Адрес сервера ALDPRO (aldpro_url)	✓	Адрес сервера в формате `ldaps://example.com`
База поиска (aldpro_base)	✓	DN-объект каталога, начиная с которого выполняется поиск
Фильтр поиска (aldpro_filter)	✗	LDAP-фильтр для поиска учетных записей
Источник LDAP/AD	✗	Логический идентификатор директории
База домена (domain_base_dn)	✗	Используется для tombstone-поиска удалённых объектов. Можно указать DN (`DC=corp,DC=local`) или домен (`corp.local`).
Логин администратора (aldpro_admin_dn)	✓	Учетная запись для подключения к LDAP.
Пароль администратора (aldpro_admin_pwd)	✓	Пароль учетной записи администратора LDAP.
Область поиска	✗	Определяет глубину поиска объектов
Размер страницы	✗	Количество объектов в одном запросе
Время ожидания	✗	Максимальное время ожидания ответа

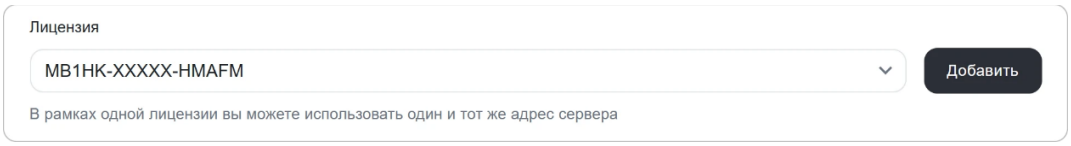
(миллисекунды)		сервера
Проверять TLS сертификат	✗	Проверка TLS/SSL-сертификата сервера

Шаг 3. Привязка лицензии

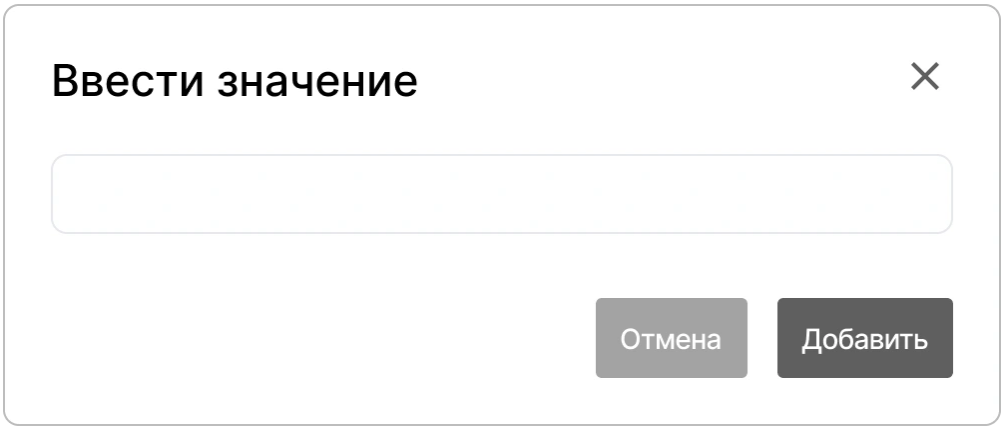
1. При создании коннектора найдите поле **Лицензия**. Если коннектор уже создан, откройте его настройки и перейдите в раздел **Параметры подключения** → **Лицензия**.

2. Добавьте лицензию одним из способов:

   – Выберите ключ из выпадающего списка (если лицензия уже сохранена в системе),



   – Нажмите **Добавить** и в открывшемся окне введите лицензионный ключ.



3. Сохраните изменения.

Шаг 4. Настройка коннектора

После создания коннектора выполните настройку в соответствии с инструкциями:

- Режим синхронизации
- Расписание синхронизации
- Правила сопоставления пользователей
- Настройка импорта
- Настройка экспорта
- Сопоставление полей профиля

Рекомендуемые правила сопоставления полей профиля

При интеграции ALD Pro-каталогов рекомендуется использовать следующие сопоставления:

Поле IDM	ALD Pro атрибут
`email`	`mail`
`login`	`uid` / `cn`
`family_name`	`sn`
`given_name`	`givenName`
`phone_number`	`telephoneNumber`

Использование этих правил помогает:

- избежать дублирования пользователей;
- корректно объединять учетные записи;
- минимизировать ошибки сопоставления;
- поддерживать единый формат данных профиля.

Смотрите также

- Обзор КриптоАРМ IDM — общая информация о системе IDM, её назначении и компонентах.
- Каталог в КриптоАРМ IDM — описание структуры каталога пользователей, групп и папок.
- RBAC модель в КриптоАРМ IDM — описание ролевой модели доступа, ресурсов, ролей и их связи с пользователями и группами.
- **Коннекторы в КриптоАРМ IDM — обзор коннекторов в КриптоАРМ IDM, включая принципы работы, типы интеграций и общую модель синхронизации с внешними системами.**

Подключение коннектора LDAP в КриптоАРМ IDM

> 📋 Эта инструкция входит в серию статей по настройке коннекторов. Общая информация доступна в инструкции Коннекторы в КриптоАРМ IDM.

LDAP-коннектор позволяет подключить внешнюю LDAP/Active Directory систему к **КриптоАРМ IDM** для импорта, экспорта и синхронизации пользователей.

Содержание:

- Шаг 1. Подготовка внешней системы
- Шаг 2. Создание коннектора
- Шаг 3. Привязка лицензии
- Шаг 4. Настройка коннектора
- Рекомендуемые правила сопоставления полей профиля

- Смотрите также

Шаг 1. Подготовка учетной записи в LDAP

На стороне внешнего LDAP/Active Directory необходимо подготовить учетную запись, которая будет использоваться для подключения коннектора.

Рекомендуется использовать сервисную учетную запись с правами на чтение каталога пользователей и (при необходимости) изменение паролей.

Учетная запись должна:

- иметь право на выполнение LDAP-запросов к каталогу;
- иметь доступ к области поиска, указанной в параметре `ldap_base`;
- при необходимости — иметь право на изменение пользовательских атрибутов (например, при включенной синхронизации паролей).

> 💡 В большинстве случаев используется отдельная сервисная учетная запись, а не административный пользователь домена.

Шаг 2. Создание коннектора

1. Перейдите в панель **IDM** → **Коннекторы**.
2. Нажмите кнопку **Добавить**  .
3. В открывшемся окне укажите обязательные параметры для подключения:
   - Имя коннектора,
   - Тип коннектора: **LDAP**,
   - Адрес сервера LDAP (`ldap_url`),
   - База поиска (`ldap_base`),
   - Учетные данные администратора: логин (`ldap_admin_dn`) и пароль (`ldap_admin_pwd`).

   > 💡 Поле **Лицензия** можно заполнить позже. Подробнее — в разделе Привязка лицензии.
4. Нажмите **Создать**.

Параметры коннектора

Параметр	Обязательное	Описание
Имя коннектора	✓	Отображаемое название коннектора в интерфейсе IDM. Используется для идентификации подключения.
Тип коннектора	✓	Тип внешней системы
Коннектор активен	✗	Включает или отключает коннектор. Неактивный коннектор не участвует в

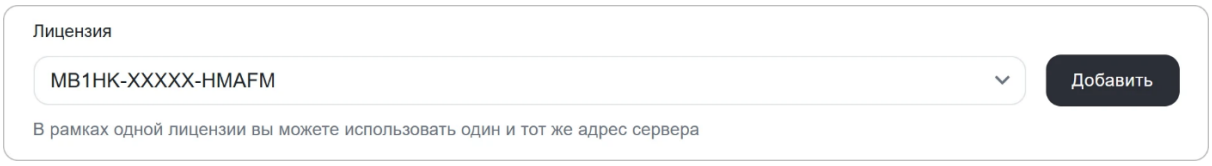
		синхронизации.
Лицензия	✓	Лицензия, назначенная коннектору
Адрес сервера LDAP (ldap_url)	✓	Адрес LDAP-сервера в формате `ldaps://example.com`
База поиска (ldap_base)	✓	DN-объект каталога, начиная с которого выполняется поиск
Фильтр поиска (ldap_filter)	✗	LDAP-фильтр для поиска учетных записей
Источник LDAP/AD	✗	Логический идентификатор директории
База домена (domain_base_dn)	✗	Используется для tombstone-поиска удалённых объектов. Можно указать DN (`DC=corp,DC=local`) или домен (`corp.local`).
Логин администратора (ldap_admin_dn)	✓	Учетная запись для подключения к LDAP.
Пароль администратора (ldap_admin_pwd)	✓	Пароль учетной записи администратора LDAP.
Область поиска	✗	Определяет глубину поиска объектов
Размер страницы	✗	Количество объектов в одном запросе
Время ожидания (миллисекунды)	✗	Максимальное время ожидания ответа сервера
Проверять TLS сертификат	✗	Проверка TLS/SSL-сертификата сервера

Шаг 3. Привязка лицензии

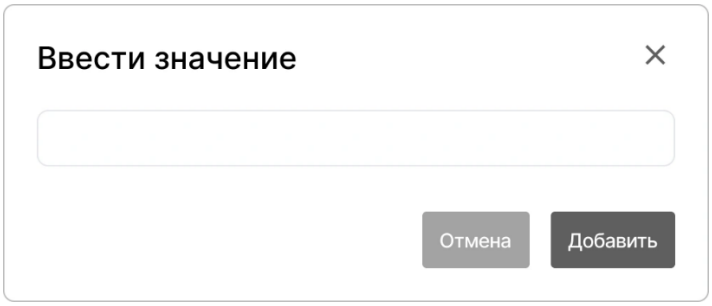
1. При создании коннектора найдите поле **Лицензия**. Если коннектор уже создан, откройте его настройки и перейдите в раздел **Параметры подключения** → **Лицензия**.

2. Добавьте лицензию одним из способов:

   – Выберите ключ из выпадающего списка (если лицензия уже сохранена в системе),



   – Нажмите **Добавить** и в открывшемся окне введите лицензионный ключ.



3. Сохраните изменения.

Шаг 4. Настройка коннектора

После создания коннектора выполните настройку в соответствии с инструкциями:

- Режим синхронизации
- Расписание синхронизации
- Правила сопоставления пользователей
- Настройка импорта
- Настройка экспорта
- Сопоставление полей профиля

Рекомендуемые правила сопоставления полей профиля

При интеграции LDAP-каталогов рекомендуется использовать следующие сопоставления:

Поле IDM	LDAP атрибут	Рекомендуемая нормализация
`email`	`mail`	`trim`, `lowercase`
`login`	`sAMAccountName`	`trim`
`family_name`	`sn`	`trim`
`given_name`	`givenName`	`trim`
`phone_number`	`telephoneNumber`	`digits_only`

Использование этих правил помогает:

- избежать дублирования пользователей;
- корректно объединять учетные записи;
- минимизировать ошибки сопоставления;
- поддерживать единый формат данных профиля.

Смотрите также

- Обзор КриптоАРМ IDM — общая информация о системе IDM, её назначении и компонентах.

- Каталог в КриптоАРМ IDM — описание структуры каталога пользователей, групп и папок.
- RBAC модель в КриптоАРМ IDM — описание ролевой модели доступа, ресурсов, ролей и их связи с пользователями и группами.
- Коннекторы в КриптоАРМ IDM — обзор коннекторов в КриптоАРМ IDM, включая принципы работы, типы интеграций и общую модель синхронизации с внешними системами.