- Яндекс 360 для бизнеса
- Что входит
- Переезд в Яндекс 360
  - Шаг 1. Подключение домена
  - Шаг 2. Подготовка аккаунтов
  - Шаг 3. Подготовка секрета
    - Microsoft 365
    - Microsoft 365 (EN)
    - Google Workspace
  - Шаг 4. Миграция писем
    - Microsoft 365 (Outlook)
    - Google Workspace (Gmail)
    - Microsoft Exchange Server по IMAP (Outlook)
    - Другой сервер
  - Шаг 5. Миграция файлов
    - Microsoft 365 (One Drive)
    - Microsoft 365 (SharePoint Online)
    - Google Workspace (Google Drive)
    - Google Workspace (Google Drive — общие диски)
    - Другой сервер
  - Шаг 6. Миграция задач
  - Шаг 7. Миграция досок
- Подключение домена
  - Регистрация домена
  - Делегирование домена на Яндекс
  - Подтверждение домена
  - Настройка DNS-записей
  - Проверка статуса домена
  - Управление доменами
    - Несколько доменов
    - Как заменить домен
    - Как удалить домен
  - Вопросы и ответы
- Сотрудники, подразделения и группы
  - Администраторы
  - Менеджеры
  - Сотрудники
    - Создать аккаунт
    - Пригласить пользователей

        - Загрузить список
    - Подразделения
    - Группы
- Офисы и переговорки
- Корпоративная почта
    - Первоначальная настройка
    - Почтовые адреса
        - Создать почтовый ящик
        - Адреса-синонимы (алиасы)
        - Рассылки по подразделениям и группам
        - Письма на несуществующие адреса
    - Совместный доступ к ящикам
        - Делегированные ящики
        - Общие ящики
    - Правила обработки писем
    - Нейрофильтр
    - Почтовые клиенты
    - Разрешенные и запрещенные отправители
    - Подключение шлюза
    - Архив писем
        - Включение и отключение архива
        - Поиск в архиве
        - Журнал действий с архивом
        - Вопросы и ответы
    - Решение проблем
- Мессенджер
    - Системные требования
    - MSI для Мессенджера
    - Боты и API
    - Пространства
    - Чаты подразделений
- MSI для Телемоста
- Доски
    - Вход и выход
    - Администрирование Досок
        - Пользователи
        - Управление командами
        - Управление досками
        - Журнал событий
        - Импорт
        - Навигация по файлам

- Доски on-premises
  - С чего начать
  - Тарификация
  - Пример развертывания
  - Установка
    - Системные требования
    - Архитектура приложения
    - Подготовка к установке
    - Конфигурирование и настройка
      - Параметры конфигурации приложения
      - Параметры секции s3 и настройка Object Storage
      - Настройка SSO
        - Настройка AD FS
        - Настройка Keycloak
        - Параметры секции sso
      - Настройка ClickHouse
    - Импорт досок из Miro
  - Обновление
  - Панель администратора
    - Введение
    - Раздел «Обзор»
    - Раздел «Пользователи»
    - Раздел «Команды»
    - Раздел «Доски»
    - Раздел «Журнал событий»
    - Раздел «Роли»
    - Раздел «LDAP»
    - Раздел «Импорты»
    - Раздел «Материалы»
    - Раздел «Инстансы»
    - Раздел «Мигратор»
  - Справочник API
    - Общее описание
    - Перечень методов API
    - Примеры использования методов API
  - О приложении
  - История изменений
- Сетевые настройки
- Управление организацией
  - Переключиться между организациями
  - Редактировать данные

    - Изменить владельца
    - Удалить организацию
    - Проблемы с доступом
- Связь с людьми не из организации
    - Внешние контакты
    - Гости
    - Федерации
- Общие диски
- Аудит-логи
- Безопасность
    - Как повысить безопасность
    - Двухфакторная аутентификация
    - Управление авторизацией на устройствах сотрудника
    - Защита исходящей почты от утечек
    - Сервисные приложения
    - API-сценарии
    - Соответствие требованиям
        - Реестр отечественного ПО
        - Обработка персональных данных
        - Стандарт безопасности ISO/IEC 27001
    - Единый вход (SSO)
        - Как подключить
            - Настройка Active Directory
            - Настройка Active Directory (EN)
            - Настройка Azure Active Directory
            - Настройка Azure Active Directory (EN)
            - Настройка Keycloak версии 18
            - Настройка Keycloak версии 19 и выше
            - Настройка Avanpost FAM
            - Настройка Multifactor
        - Синхронизация пользователей и групп с каталогом LDAP
        - Смена поставщика удостоверений (IdP)
        - Как отключить
    - Меры безопасности, принимаемые Яндекс 360
- Служба поддержки
    - Как работает служба поддержки
    - Связаться со службой поддержки

Онлайн-встреча «Знакомство с Яндекс 360 для бизнеса»

Приглашаем вас на онлайн-встречу «Знакомство с Яндекс 360 для бизнеса». На встрече вы узнаете про основные продукты, которые формируют единую коммуникационную платформу Яндекс 360, и увидите сквозные сценарии их применения.

Также на повестке:

1. Командная работа при помощи сервисов Яндекс 360.
2. Надежность и безопасность данных.
3. Бесшовный переход на Яндекс 360 для бизнеса.

Встреча будет актуальна для специалистов, перед которыми стоит задача поиска альтернативных решений в категории виртуального офиса для бизнеса.

Выбрать дату и зарегистрироваться

Переезд в Яндекс 360 для бизнеса

Мы собрали ответы на частые вопросы о том, как перенести данные вашей организации в Яндекс 360 для бизнеса из Google Workspace, Microsoft 365 и других платформ. Смотреть >

Что входит в Яндекс 360 для бизнеса

Чтобы перейти к Справке сервиса, выберите его в списке:

Почта

Корпоративная почта на домене вашей компании — клиенты и партнеры будут знать, кто им пишет. Администраторы могут подключать дополнительные адреса для сотрудников и отделов, настраивать правила обработки писем, сохранять переписки коллег в архив, находить удаленные письма.

Диск

Облачное хранилище файлов для каждого сотрудника. Загружать файлы и делиться ими можно с любого устройства, подключенного к интернету. Сотрудники могут настроить общий доступ к папке или открыть публичный доступ к файлам по ссылке. Администраторы могут увеличивать место на Диске для сотрудников организации.

Мессенджер

Сервис для корпоративного общения в закрытом контуре. Сотрудники могут переписываться в персональных и групповых чатах, читать каналы, пользоваться аудио- и видеозвонками. Администраторы могут автоматизировать внутренние процессы организации с помощью ботов.

Телемост

Видеовстречи и трансляции без ограничений по времени. Сотрудники могут приглашать участников и зрителей по ссылке, вести запись встречи, включать демонстрацию экрана и комментировать происходящее на встрече в групповом чате.

Рассылки

Конструктор писем об акциях и новостях для клиентов. Администраторы могут выбрать готовый шаблон письма или самостоятельно настроить оформление в корпоративном стиле.

Заметки

Сервис для быстрых записей и списков задач. Сотрудники могут записывать идеи, конспектировать встречи и прикреплять изображения к записям. Заметки сохранятся в облаке и не пропадут, если с компьютером или телефоном сотрудника что-то случится.

Календарь

Общий планировщик встреч и загрузки для всей компании. Сотрудники могут открывать коллегам доступ к своему календарю и создавать события исходя из занятости участников. Если у вашей организации есть офис, администраторы могут создавать переговорки, а сотрудники — бронировать их для встреч вживую.

Документы

Онлайн-редактор текстов, презентаций и таблиц. Сотрудники могут создавать документы на Диске вашей организации и редактировать их вместе с коллегами с компьютера или мобильного устройства.

Трекер

Сервис для управления проектами и рабочими процессами. Руководители могут распределять работу между сотрудниками и контролировать ее выполнение. Сотрудникам будет проще помнить про задачи, следить за сроками и приоритетами.

Вики

База знаний вашей организации. В ней можно хранить описания проектов, рабочие инструкции и другую информацию. Сотрудники могут редактировать страницы совместно.

Формы

Сервис, где вы можете создавать опросы, собирать отзывы, принимать заявки, проводить тесты и квизы. Ответы могут сохраняться на Вики или превращаться в задачи в Трекере.

Доски

Онлайн-пространство для совместной работы. Сотрудники могут создавать доски для проектов и редактировать их одновременно в режиме реального времени.

Яндекс Браузер для организаций с сервисами Яндекс 360 для бизнеса

Браузер с предустановленными сервисами, доступ к которым есть на Табло, боковой панели и панели задач. Браузер настраивается через интерфейс операционной системы или командную строку (терминал): можно задать единые параметры для всей организации или отдельных сотрудников.

Примечание

Сервисы Яндекс 360 для бизнеса обеспечивают безопасность при обработке персональных данных в соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных».

Шаг 1. Подключение домена

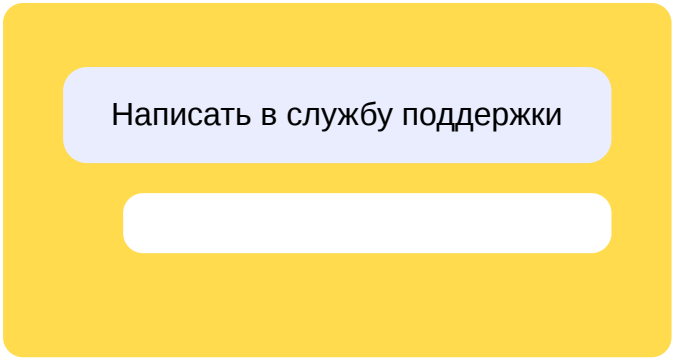
Чтобы создавать учетные записи и использовать корпоративную Почту, подключите к вашей организации домен.

Если вы собираетесь переносить письма и файлы из Google Workspace, Microsoft 365 или любой другой платформы, подключите к организации тот же домен, который вы использовали. Этот домен нужно сделать основным, иначе миграция не сработает.

1. Перейдите на страницу **Домены**.
2. Введите имя вашего домена, например `example.com`, и нажмите кнопку **Добавить домен**.
3. Подтвердите домен. Подтверждение нужно, чтобы никто не мог подключить домен без ведома его владельца.
   3.1. Рядом с именем домена нажмите **Подтвердить домен**.
   3.2. Подтвердите домен одним из способов. Как это сделать
   3.3. Дождитесь подтверждения домена.

> **Ограничение**
>
> Если вы подключаете к организации первый домен, до его подтверждения другие действия в Яндекс 360 для бизнеса будут заблокированы.

Полная инструкция по работе с доменами в Яндекс 360 для бизнеса приведена в разделе Подключение домена.



Шаг 2. Подготовка аккаунтов

Чтобы перенести файлы и письма, для всех сотрудников должны быть созданы аккаунты на вашем почтовом домене. Этими аккаунтами вы сможете управлять: задавать пароли, изменять персональные данные, блокировать и так далее.

Сначала добавьте аккаунты, затем приступайте к подготовке секрета (для Gmail и Outlook) и миграции писем и файлов.

Если вы используете систему управления доступом (например, Active Directory или Keycloak), настройте единый вход (SSO): после создания и настройки SAML-приложения аккаунты синхронизируются автоматически.

Внимание

Если вы уже добавили аккаунты вручную, то единый вход (SSO) включить не получится.

Если вы не используете единый вход (SSO), то можете подготовить аккаунты одним из способов:

Создать аккаунт

Добавьте сотрудников по одному — это удобно, если у вас небольшая организация.

Пригласить пользователей

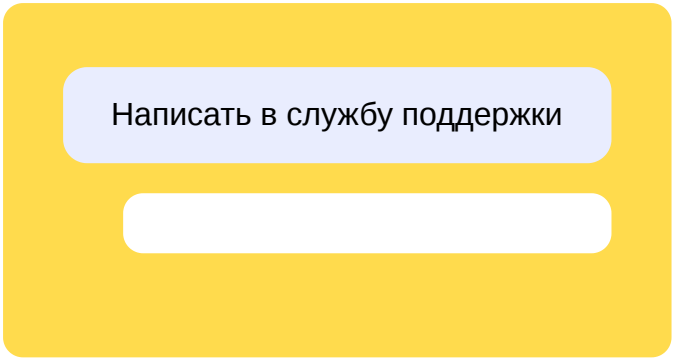
Пригласите сотрудников со своими аккаунтами на Яндексе.

Загрузить список

Создайте и загрузите CSV-файл с данными сотрудников — способ подойдет для больших организаций.

API Яндекс 360 для бизнеса

Управляйте аккаунтами посредством HTTP-запросов к REST API.


Написать в службу поддержки

Подготовка секрета в Microsoft 365

Файл секрета — это файл с ключом доступа. С его помощью Яндекс 360 для бизнеса подключается к Microsoft 365. Чтобы его подготовить, нужно зарегистрировать приложение в Microsoft Azure, затем создать новый секрет и сохранить его в файл.

Если вы работаете с англоязычным интерфейсом Microsoft Azure, воспользуйтесь инструкцией.

Шаг 1. Зарегистрируйте приложение в Microsoft Azure и создайте секреты

1. Откройте страницу регистрации приложений в MS Azure portal (требуется авторизация от имени администратора): https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade.
2. Нажмите **Новая регистрация**.
3. Введите данные:
   - В поле **Имя** введите название приложения, например *migration*.
   - В **Поддерживаемые типы учетных записей** выберите **Учетные записи только в этом каталоге организации (<название вашей организации>)**.
4. Нажмите **Зарегистрировать**.
5. Перейдите на вкладку **Обзор**. Скопируйте значение **Идентификатор приложения (клиент)** и сохраните в текстовом файле. Этот идентификатор понадобится на следующих этапах.

   Пример идентификатора:

   ```
   abcd1234-a1b2-1111-123a-absdfe
   ```

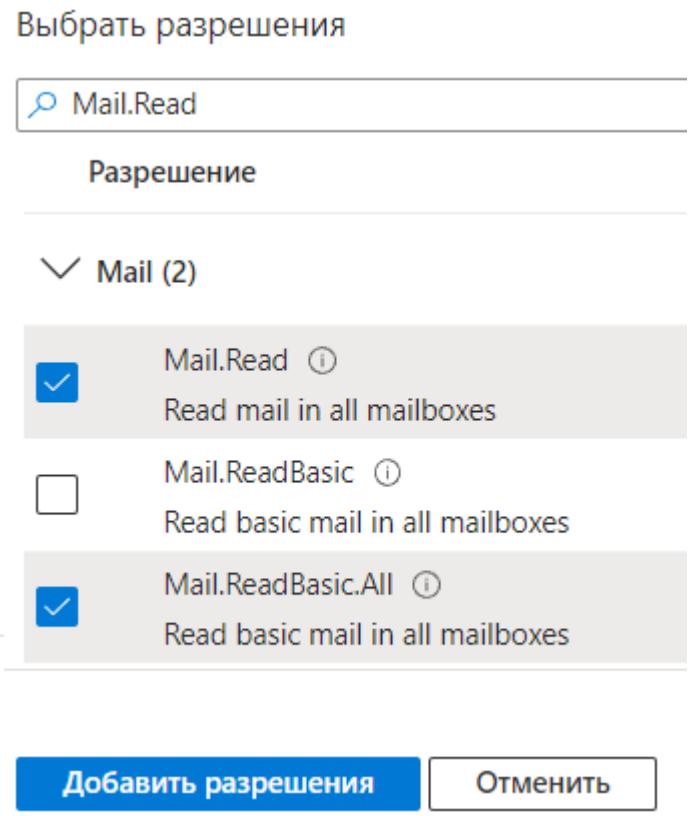
6. Перейдите на вкладку **Сертификаты и секреты** и создайте новый секрет для приложения миграции:
   6.1. Выберите **Секреты клиента** и нажмите **Новый секрет клиента**.
   6.2. На появившейся панели заполните поле **Описание** (например: *migration-secret*).
   6.3. Нажмите **Добавить**.
   6.4. Скопируйте секрет из поля **Значение** и сохраните в текстовом файле. Этот секрет понадобится на следующих этапах.

   Пример значения секрета:

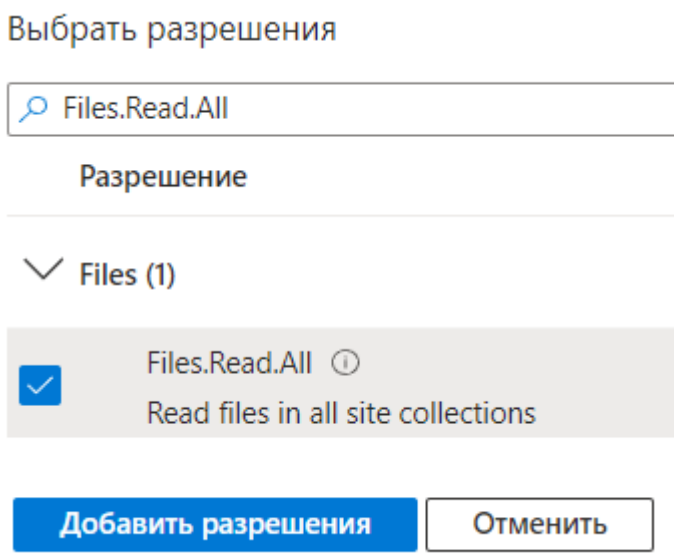
   ```
   ABCD2XYZ032-xyzXYZ032
   ```

7. Перейдите на вкладку **Разрешения API** и добавьте разрешения:
   7.1. Нажмите **Добавить разрешение**.
   7.2. Убедитесь, что на появившейся панели выбрана вкладка **Интерфейсы API Microsoft**. Нажмите **Microsoft Graph**.
   7.3. Выберите **Разрешения приложения**.
   7.4. Найдите следующие разрешения с помощью поиска, выберите их и нажмите кнопку **Добавить разрешения** для каждого раздела:

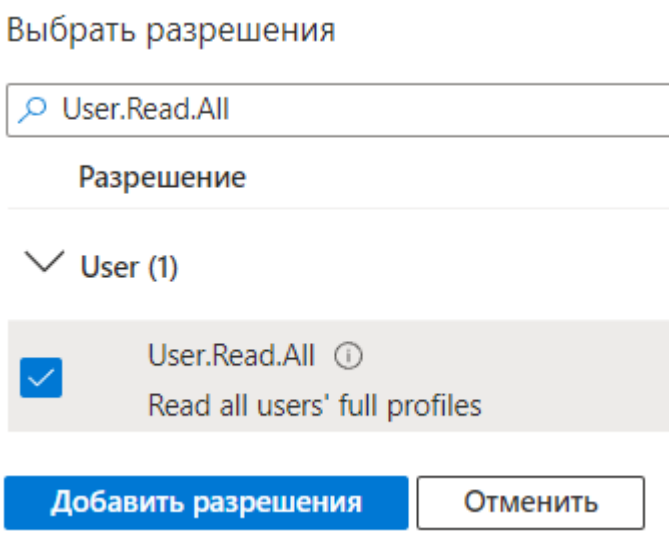
Mail: Mail.Read и Mail.ReadBasic.All (для переноса писем)



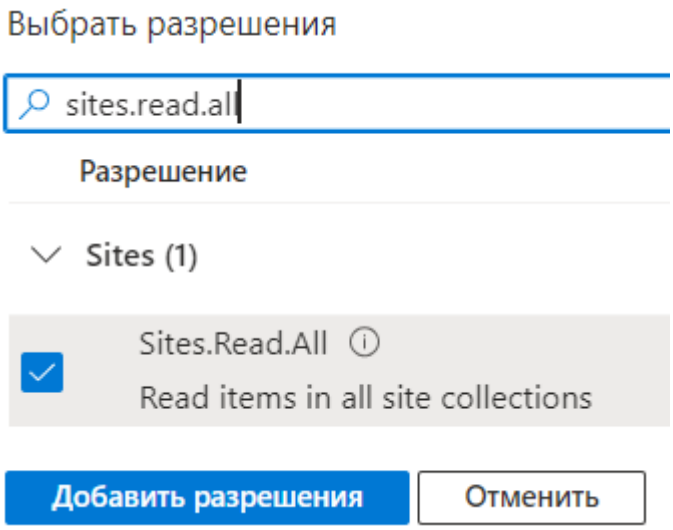
Files: Files.Read.All (для поиска и скачивания файлов с диска)



User.Read.All (для чтения списка пользователей)



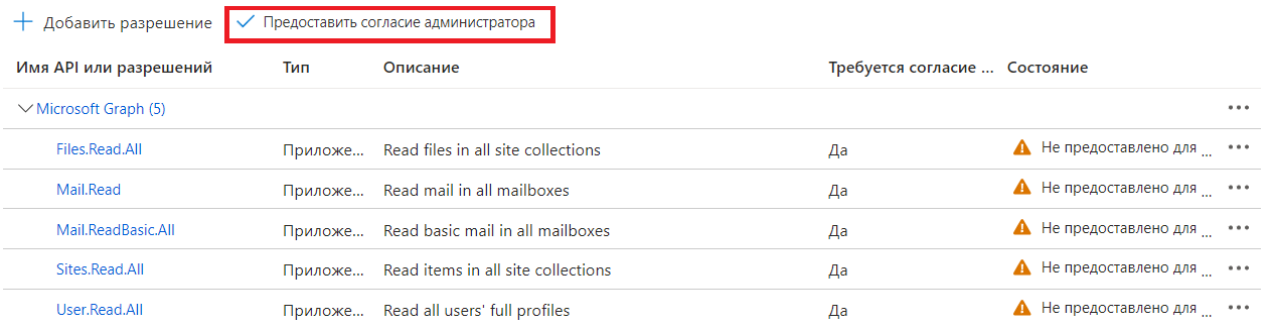
Sites.Read.All (для поиска и скачивания файлов из библиотек документов SharePoint Online)



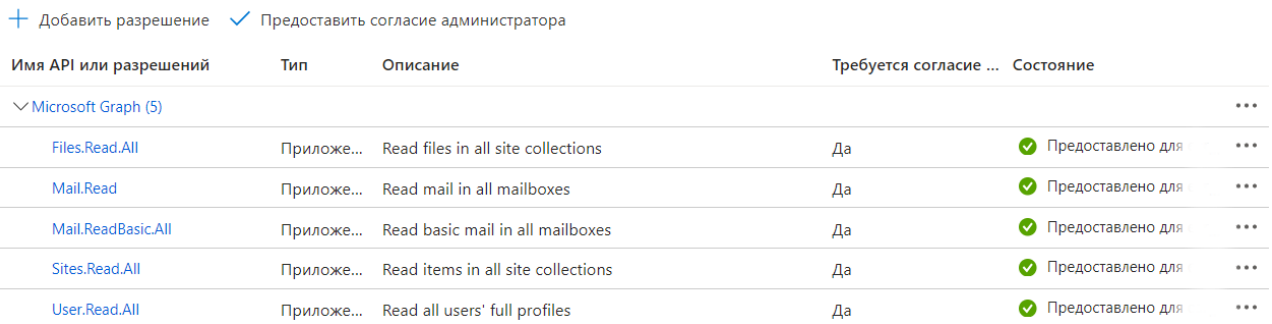
> **Внимание**
>
> Выберите все указанные выше разделы. Рекомендуется создавать один секрет, который будет использоваться и для писем, и для файлов. Если вы добавите разрешения только для писем (`Mail.Read` и `Mail.ReadBasic.All`), то не сможете запустить миграцию файлов с таким секретом.

7.5. Нажмите **Добавить разрешения**.

После этого разрешения будут добавлены, но не подтверждены:



Нажмите **Предоставить согласие администратора для <название вашей организации>** для подтверждения доступов приложения. В появившемся окне нажмите **Да**. Напротив каждого разрешения в колонке **Состояние** должен появиться значок ✅.



Шаг 2. Создайте файл секрета

1. Создайте файл `secret.json` в любом текстовом редакторе (например, в Блокноте) и скопируйте туда шаблон:

   ```
   {
   "client_id": "<client id>",
   "secret": "<secret>"
   }
   ```

2. Вместо `<client id>` вставьте значение **Идентификатор приложения (клиент)**, которое вы скопировали и сохранили в пункте 5 шага 1. Вместо `<secret>` вставьте **Значение** секрета, которое вы скопировали и сохранили в пункте 6.4 шага 1.

   Пример, как должно получиться:

   ```
   {
   "client_id": "abcd1234-a1b2-1111-123a-absdfe",
   "secret": "ABCD2~XYZ032-xyzXYZ032"
   }
   ```

3. Сохраните готовый файл с секретом. Можно приступать к миграции писем и файлов.

Написать в службу поддержки

Подготовка секрета в Microsoft 365 (английский интерфейс)

Файл секрета — это файл с ключом доступа. С его помощью Яндекс 360 для бизнеса подключается к Microsoft 365. Чтобы его подготовить, нужно зарегистрировать приложение в Microsoft Azure, затем создать новый секрет и сохранить его в файл.

Шаг 1. Зарегистрируйте приложение в Microsoft Azure и создайте секреты

1. Откройте страницу регистрации приложений в MS Azure portal (требуется авторизация от имени администратора): https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade.
2. Нажмите **New registration**.
3. Введите данные:
   - В поле **Name** введите название приложения, например *migration*.
   - В **Supported account types** выберите **Accounts in this organizational directory only (<название вашей организации>)**.
4. Нажмите **Register**.
5. Перейдите на вкладку **Overview**. Скопируйте значение **Application (client) ID** и сохраните в текстовом файле. Этот идентификатор понадобится на следующих этапах.

   Пример идентификатора:

   ```
   abcd1234-a1b2-1111-123a-absdfe
   ```

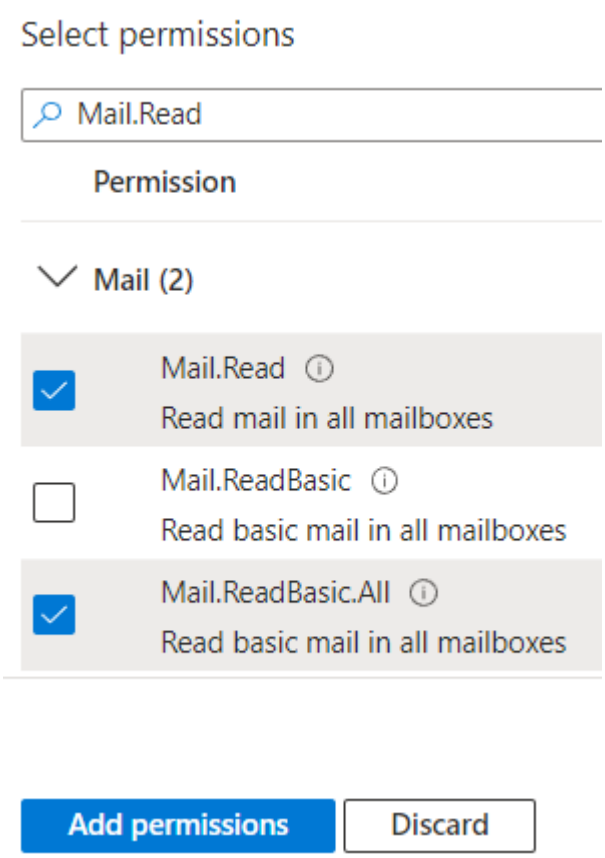
6. Перейдите на вкладку **Certificates & secrets** и создайте новый секрет для приложения миграции:
   6.1. Выберите **Client secrets** и нажмите **New client secret**.
   6.2. На появившейся панели заполните поле **description** (например: *migration-secret*).
   6.3. Нажмите **Add**.
   6.4. Скопируйте значение **Value** и сохраните в текстовом файле. Этот секрет понадобится на следующих этапах.

   Пример значения секрета:

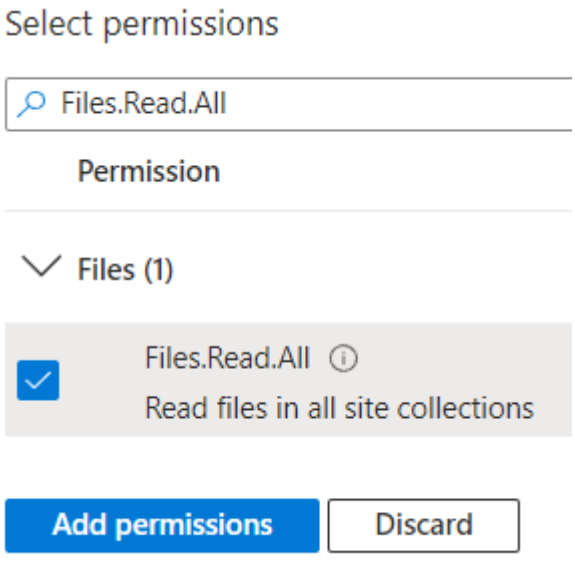
   ```
   ABCD2XYZ032-xyzXYZ032
   ```

7. Перейдите на вкладку **API permissions** и добавьте разрешения:
   7.1. Нажмите **Add a permission**.
   7.2. Убедитесь, что на появившейся панели выбрана вкладка Microsoft APIs. Нажмите **Microsoft Graph**.
   7.3. Выберите **Application permissions**.
   7.4. Найдите следующие разрешения с помощью поиска, выберите их и нажмите кнопку **Add permissions** для каждого раздела:

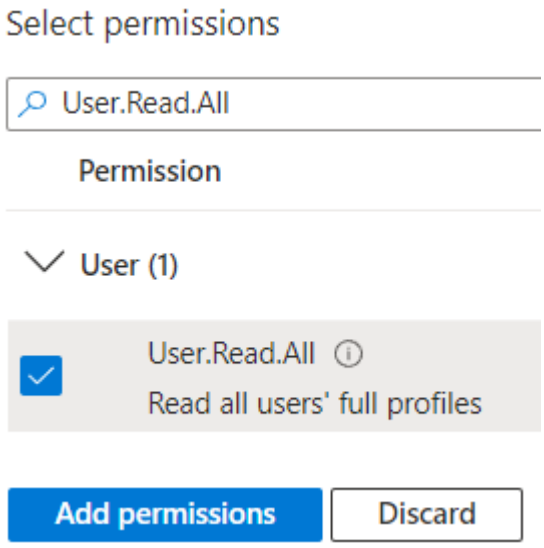
   Mail: Mail.Read и Mail.ReadBasic.All (для переноса писем)



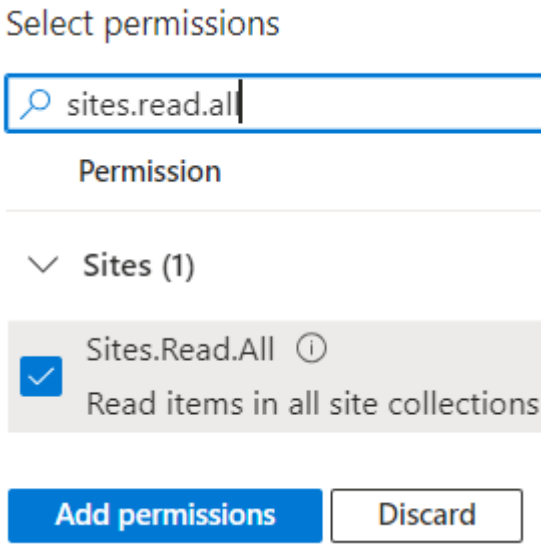
Files: Files.Read.All (для поиска и скачивания файлов с диска)



User.Read.All (для чтения списка пользователей)



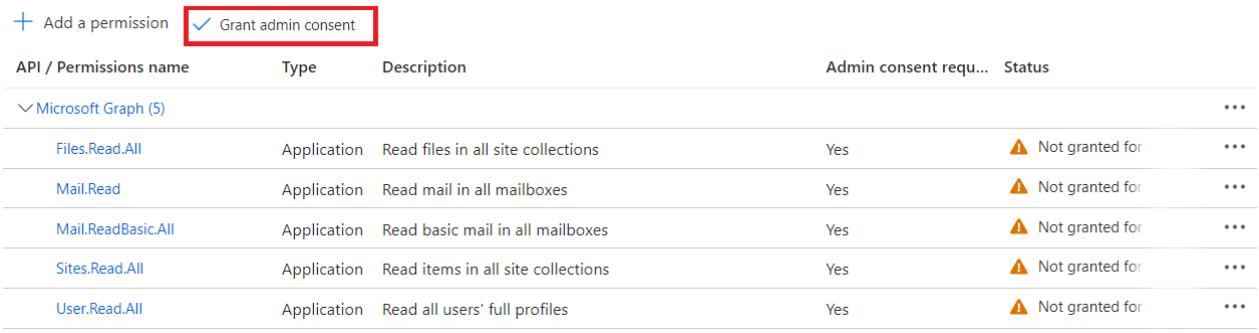
Sites.Read.All (для поиска и скачивания файлов из библиотек документов SharePoint Online)



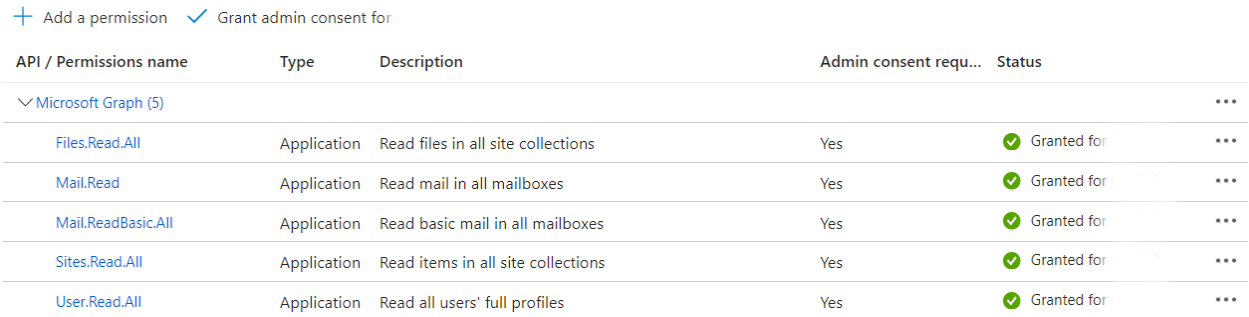
> **Внимание**
>
> Выберите все указанные выше разделы. Рекомендуется создавать один секрет, который будет использоваться и для писем, и для файлов. Если вы добавите разрешения только для писем (`Mail.Read` и `Mail.ReadBasic.All`), то не сможете запустить миграцию файлов с таким секретом.

7.5. Нажмите **Add permissions**.

После этого разрешения будут добавлены, но не подтверждены:



Нажмите **Grant/revoke admin consent for <название вашей организации>** для подтверждения доступов приложения. В появившемся окне нажмите **Yes**. Напротив каждого разрешения в колонке **Status** должен появиться значок ✅.



Шаг 2. Создайте файл секрета

1. Создайте файл `secret.json` в любом текстовом редакторе (например, в Блокноте) и скопируйте туда шаблон:

   ```
   {
   "client_id": "<client id>",
   "secret": "<secret>"
   }
   ```

2. Вместо `<client id>` вставьте значение **Application (client) ID**, которое вы скопировали и сохранили в пункте 5 шага 1. Вместо `<secret>` вставьте значение **Value**, которое вы скопировали и сохранили в пункте 6.4 шага 1.

   Пример, как должно получиться:

   ```
   {
   "client_id": "abcd1234-a1b2-1111-123a-absdfe",
   "secret": "ABCD2~XYZ032-xyzXYZ032"
   }
   ```

3. Сохраните готовый файл с секретом. Можно приступать к миграции писем и файлов.

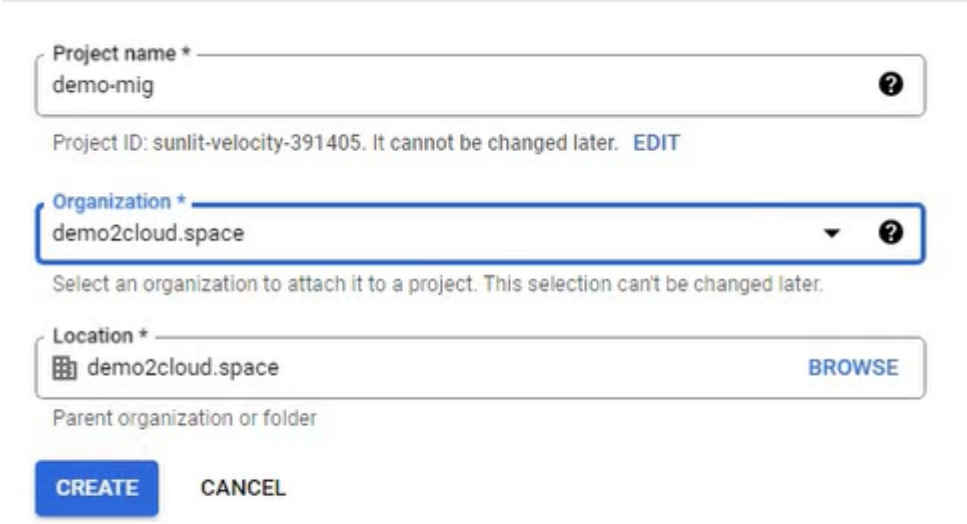
Написать в службу поддержки

Подготовка секрета в Google Workspace

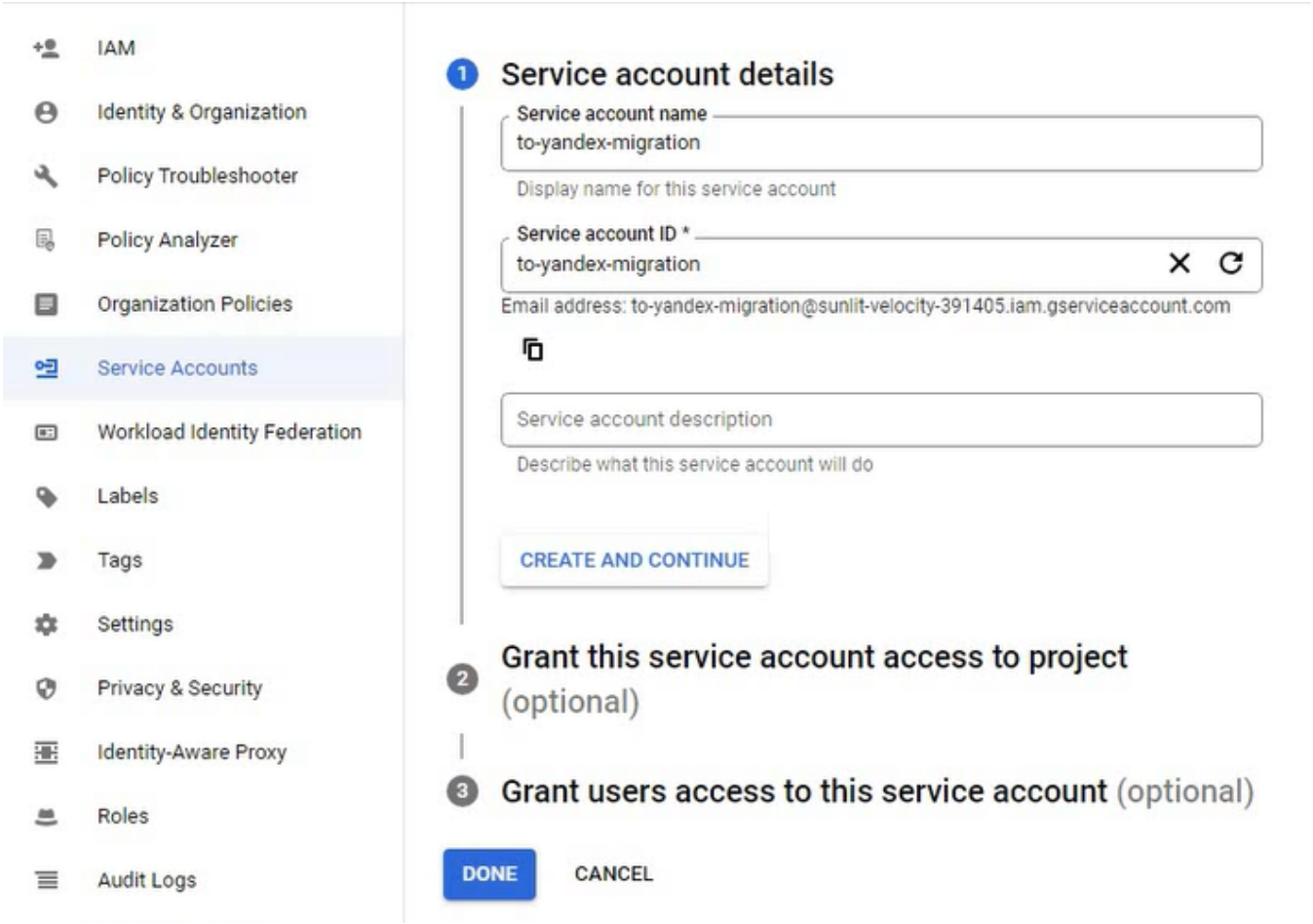
Файл секрета — это файл с ключом доступа. С его помощью Яндекс 360 для бизнеса подключается к Google Workspace. Чтобы его подготовить, нужно создать сервисный аккаунт в Google Workspace, затем создать новый секрет и сохранить его в файл.

Шаг 1. Создайте проект, аккаунт и ключ

1. Если у вас нет существующего проекта, создайте его:
   1.1. Перейдите на страницу Сервисные аккаунты Google.
   1.2. Нажмите кнопку **Create a project**.
   1.3. В поле **Project name** введите название проекта.
   1.4. В поле **Organization** выберите организацию, с которой хотите перенести данные.



   1.5. Нажмите кнопку **Create**. Дождитесь, пока обновится страница с новым проектом.
2. На панели сверху нажмите кнопку **Create service account**.
3. В поле **Service account name** введите имя учетной записи.
4. Нажмите **Create and continue**.



Необязательные этапы:

Предоставьте учетной записи доступ к проекту

> Пропустите этап **Grant this service account access to project** или настройте права доступа к проекту.

Предоставьте другим пользователям доступ к учетной записи

> Пропустите этап **Grant users access to project** или укажите пользователей, которым разрешаете управлять учетной записью.

5. Нажмите кнопку **Done**. Новая учетная запись сервисного аккаунта отобразится в списке.
6. Откройте учетную запись, скопируйте идентификационный номер **Unique ID** и сохраните его в текстовом файле. Номер понадобится на следующем шаге.

   Пример идентификационного номера:

   ```
   104585045394161743643
   ```

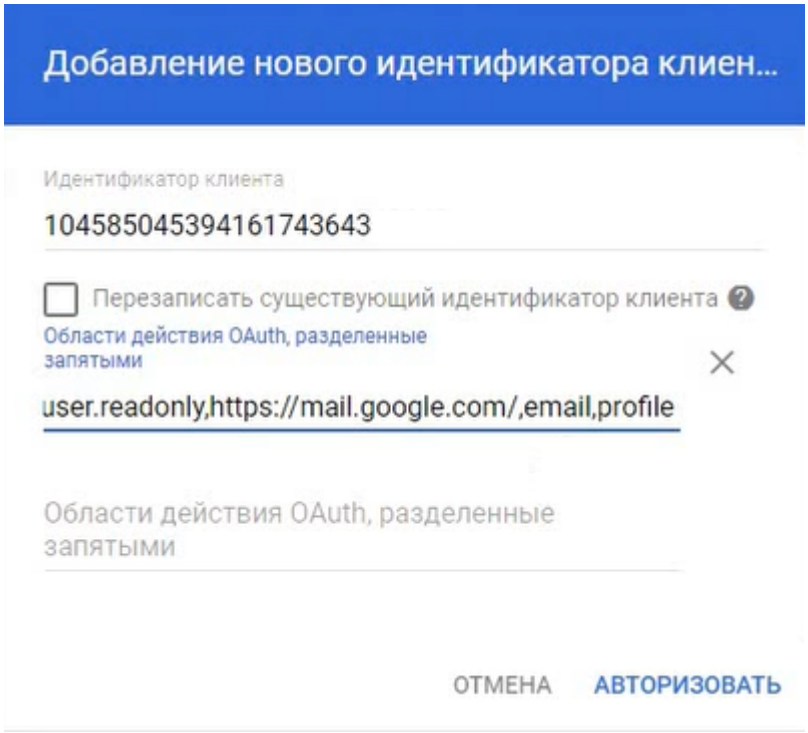
7. Перейдите на вкладку **Keys**.
8. Выберите **Add key** → **Create new key**.
9. В блоке **Key type** выберите формат **JSON**.
10. Нажмите кнопку **Create**, чтобы скачать ключ на компьютер.

Шаг 2. Настройте права доступа

1. Откройте консоль администратора Google.
2. Выберите **Безопасность** → **Управление доступом и данными** → **Управление API**.
3. Нажмите **Настроить делегирование доступа к данным в домене**.
4. В блоке **Клиенты API** нажмите **Добавить**.
5. В поле **Идентификатор клиента** укажите идентификационный номер учетной записи, который скопировали и сохранили в пункте 6 шага 1.
6. Скопируйте строку:

```
https://www.googleapis.com/auth/drive,https://www.googleapis.com/auth/admin.directo
```

7. Вставьте ее в поле **Области действия OAuth, разделенные запятыми**.

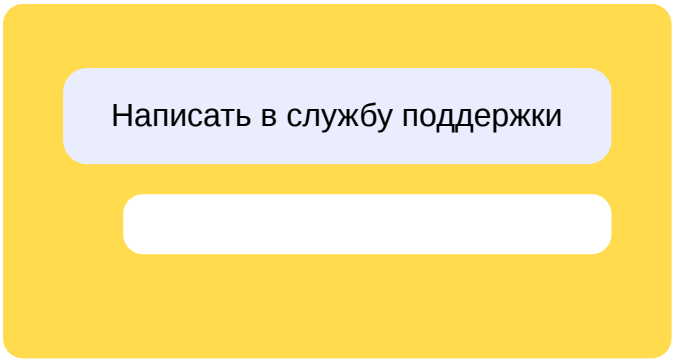


8. Нажмите кнопку **Авторизовать**.

Шаг 3. Включите доступ к проекту по API

1. На странице Admin SDK API в выпадающем списке **Select a project** выберите ваш проект и затем нажмите **Enable**.
2. На странице Google Drive API в выпадающем списке **Select a project** выберите ваш проект и затем нажмите **Enable**.
3. На странице Gmail API в выпадающем списке **Select a project** выберите ваш проект и затем нажмите **Enable**.

Когда вы завершите настройку проекта, можно приступать к миграции писем и файлов. Для запуска миграции потребуется файл с секретом, который вы скачали в пункте 10 шага 1.


Написать в службу поддержки

Microsoft 365 (Outlook)

Запуск миграции

1. Подготовьте секрет, подключите домен и подготовьте аккаунты сотрудников, если не сделали этого раньше.

   > **Примечание**
   >
   > Секрет применяется ко всем запущенным миграциям. Если вы уже запустили миграцию и после этого загружаете новый секрет, то он применится к этой миграции. При этом учитываются разрешения секрета: если новый секрет имеет доступ только к письмам (в разрешениях API добавлено `Mail.Read` и `Mail.ReadBasic.All`) и у вас запущена миграция файлов, она остановится.

2. В меню слева выберите **Общие настройки** → **Миграция**.
3. Выберите, что хотите перенести: нажмите **Миграция писем**.
4. Выберите, откуда хотите перенести почту: нажмите **Microsoft 365**.
5. Загрузите файл секрета и нажмите **Дальше**.
6. Укажите аккаунты, для которых нужно запустить миграцию:
   6.1. Скачайте шаблон CSV-файла.
   6.2. По образцу добавьте в файл данные сотрудников.

   Первая строка файла — заголовки полей аккаунта, не удаляйте ее. В каждой следующей строке файла должны быть указаны данные одного аккаунта в кавычках через точку с запятой.

   Обязательно укажите адреса исходных почтовых ящиков и логины сотрудников на вашем домене, в которые нужно перенести письма. Логины в столбце `yandex_login` могут не совпадать с именами учетных записей в Microsoft 365. Например, если вы создали сотрудника с логином `ivan.ivanov` в Яндекс 360 для бизнеса, а его исходный почтовый ящик — `i.ivanov@example.test`, то укажите `ivan.ivanov` в столбце `yandex_login`.

   У вас должен получиться файл со структурой:

   ```
   "yandex_login";"external_email"
   "ivan.ivanov";"i.ivanov@example.test"
   "marina.makarova";"m.makarova@example.test"
   ```

> **Примечание**
>
> Вы можете добавить до 20 000 логинов сотрудников в один файл. Если в организации больше сотрудников, можно запустить несколько миграций с разными CSV-файлами. Миграции будут выполняться параллельно.

6.3. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**).

> **Внимание**
>
> Если сохранить файл в другой кодировке, он будет распознан неправильно.

6.4. Нажмите кнопку **Загрузить CSV** и укажите ваш файл.

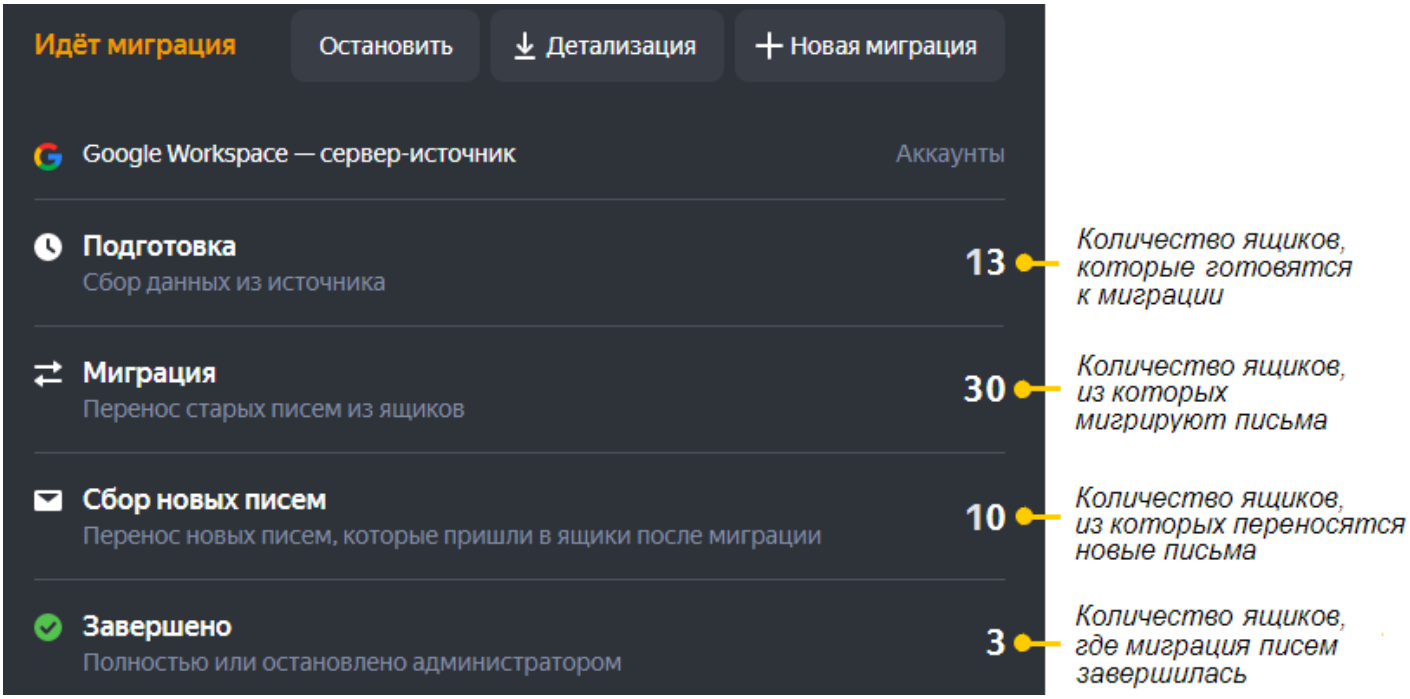
7. Нажмите **Запустить миграцию**.

В результате запуска вы увидите статус **Идет миграция**.

> **Примечание**
>
> Если вы планируете запускать миграцию несколько раз, перед каждым новым запуском сохраняйте файл с логами (его можно скачать, нажав кнопку **Детализация**). Если при миграции появятся ошибки, вы сможете отследить, при каком именно запуске это произошло.

Этапы миграции

Миграция происходит не сразу. Сбор данных займет от нескольких минут до двух часов, затем письма из исходных ящиков начнут появляться в ящиках Почты для бизнеса. Структура папок из исходных почтовых ящиков также копируется в целевые почтовые ящики.



Во время миграции напротив соответствующего этапа будет отображаться **0**. Если на этапе **Миграция** вы видите **0** — значит, перенос старых писем из ящиков завершен. Если вы хотите перенести только старые письма и не собирать новые, на этом этапе можно завершить миграцию вручную кнопкой **Остановить**.

> **Примечание**
>
> Если MX-запись указывает на ваш старый сервер, новые письма будут приходить в исходные ящики и будут перенесены позднее в ящики Почты для бизнеса. Чтобы письма перестали приходить на старый сервер, делегируйте домен или переключите MX-запись на сервер Яндекса.

Если вы не остановите миграцию на этом этапе вручную, письма, приходящие в ящики на старом сервере, будут постепенно переноситься в новые. Вы можете переключить MX-запись в любой момент: после этого новые письма будут приходить в ящики Почты для бизнеса, а не на старый сервер.

Что будет, если остановить миграцию

Остановятся все запущенные миграции и сбор новых писем из исходных почтовых ящиков в ящики Почты для бизнеса. Чтобы перенос писем продолжился, нужно запустить новую миграцию. При этом мигрируют новые письма, которые пришли в исходные ящики после того, как вы остановили предыдущую миграцию. Старые письма, которые уже мигрировали, не дублируются.

Что будет, если начать новую миграцию

Новая миграция будет идти параллельно с запущенными миграциями.

Решение проблем с миграцией

Ознакомьтесь с возможными ошибками при миграции и способами, как их исправить.

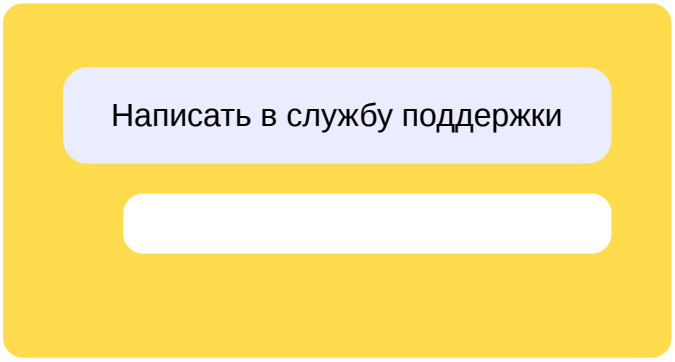
Загружен некорректный секрет

Проверьте корректность подготовки секрета.

В CSV-файле удалена или изменена первая строка

Скачайте шаблон CSV-файла и скопируйте из него первую строку в ваш CSV-файл. Убедитесь, что предыдущий импорт завершился, и запустите новый импорт с исправленным CSV-файлом.

Чтобы посмотреть отчет с подробным описанием ошибок, на странице активной миграции в правом верхнем углу нажмите кнопку **Детализация**. О способах исправления см. Отчет об ошибках миграции.



Google Workspace (Gmail)

1. Подготовьте секрет, подключите домен и подготовьте аккаунты сотрудников, если не сделали этого раньше.
2. В меню слева выберите **Общие настройки** → **Миграция**.
3. Выберите, что хотите перенести: нажмите **Миграция писем**.
4. Выберите, откуда хотите перенести почту: нажмите **Google Workspace**.
5. Загрузите файл секрета и нажмите **Дальше**.
6. Укажите аккаунты, для которых нужно запустить миграцию:
   6.1. Скачайте шаблон CSV-файла.
   6.2. По образцу добавьте в файл данные сотрудников.

   Первая строка файла — заголовки полей аккаунта. В каждой следующей строке файла должны быть указаны данные одного аккаунта в кавычках через точку с запятой.

   Обязательно должны быть указаны адреса исходных почтовых ящиков и логины сотрудников на вашем домене, в которые нужно перенести письма.

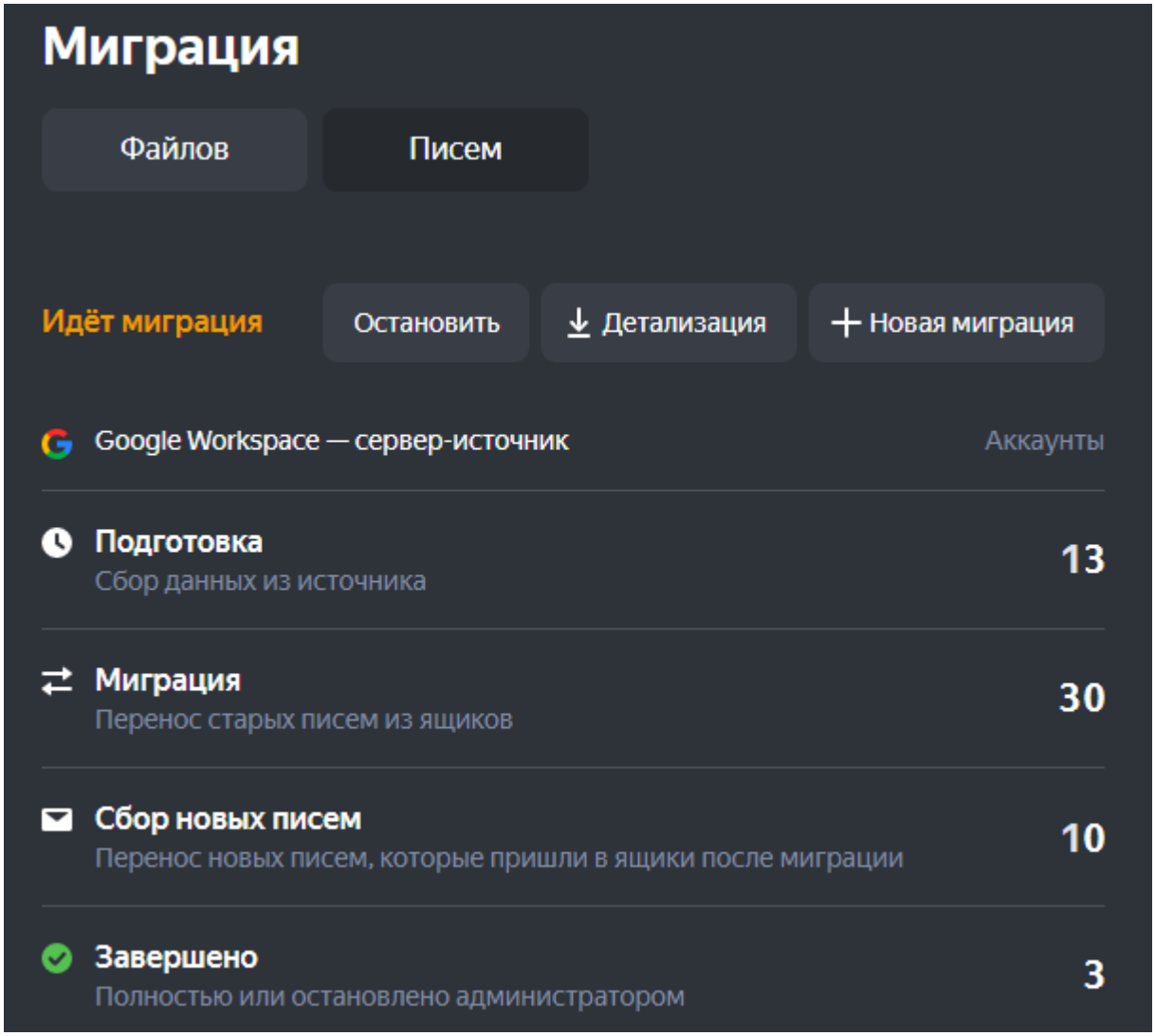
   > **Примечание**
   >
   > Вы можете добавить до 20 000 логинов сотрудников.

   6.3. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**).

   > **Внимание**
   >
   > Если сохранить файл в другой кодировке, он будет распознан неправильно.

   6.4. Нажмите кнопку **Загрузить CSV** и укажите ваш файл.
7. Нажмите **Запустить миграцию**.

В результате запуска вы увидите статус **Идет миграция**.



Примечание

Если вы планируете запускать миграцию несколько раз, перед каждым новым запуском сохраняйте файл с логами (его можно скачать, нажав кнопку **Детализация**). Если при миграции появятся ошибки, вы сможете отследить, при каком именно запуске это произошло.

Решение проблем с миграцией

Ознакомьтесь с возможными ошибками при миграции и способами, как их исправить.

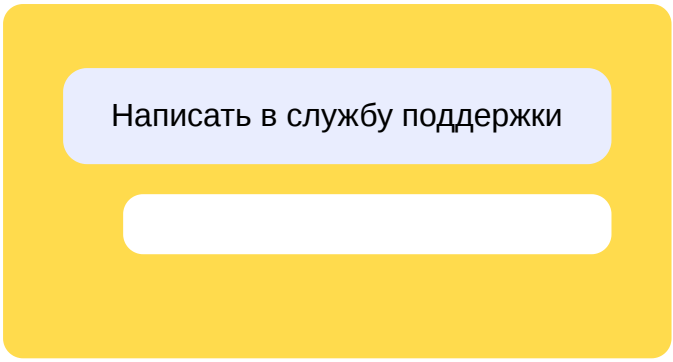
Загружен некорректный секрет

Проверьте корректность подготовки секрета.

В CSV-файле удалена или изменена первая строка

Скачайте шаблон CSV-файла и скопируйте из него первую строку в ваш CSV-файл. Убедитесь, что предыдущий импорт завершился, и запустите новый импорт с исправленным CSV-файлом.

Чтобы посмотреть отчет с подробным описанием ошибок, на странице активной миграции в правом верхнем углу нажмите кнопку **Детализация**. О способах исправления см. Отчет об ошибках миграции.


Написать в службу поддержки

Microsoft Exchange Server по IMAP (Outlook)

Письма сотрудников организации можно перенести из почтовых ящиков Exchange Server в Яндекс 360 для бизнеса по протоколу IMAP. Чтобы не собирать пароли всех пользователей, используйте отдельную учетную запись в локальной среде Active Directory и настройте для нее полный доступ к почтовым ящикам сотрудников.

Создание и настройка учетной записи для миграции

1. Подключите домен и подготовьте аккаунты сотрудников в Яндекс 360 для бизнеса, если не сделали этого раньше. Для этих аккаунтов будут созданы целевые почтовые ящики.
2. Убедитесь, что в Exchange Server включены и настроены служба IMAP4 и протокол SSL.
3. Создайте учетную запись для миграции в локальной среде Active Directory, например `migration@example.com`. Подключите почтовый ящик в Exchange Server для этой учетной записи.

   > **Совет**
   >
   > Создайте отдельную учетную запись для миграции без прав администратора Exchange. В последних версиях Exchange Server у администратора ограничен доступ к почтовым ящикам пользователей по протоколу IMAP, поэтому миграция может не работать.

4. Настройте для этой учетной записи права полного доступа к почтовым ящикам, которые нужно перенести.

   Доступ к одному ящику

   1. Откройте **Центр администрирования Exchange** в браузере.
   2. Перейдите в раздел **Получатели** → **Почтовые ящики**.
   3. Выберите нужный почтовый ящик.
   4. В появившемся окне свойств выберите **Делегирование почтового ящика**.
   5. В правой нижней части окна в разделе **Полный доступ** нажмите **Добавить**.
   6. В появившемся окне укажите учетную запись для миграции, например `migration@example.com`.
   7. Нажмите кнопку **ОК** — учетная запись добавится в раздел **Полный доступ**.
   8. В окне свойств почтового ящика нажмите кнопку **ОК**.

   Доступ к нескольким ящикам

   1. Откройте **Центр администрирования Exchange** в браузере.
   2. Перейдите в раздел **Получатели** → **Почтовые ящики**.
   3. Выберите почтовые ящики.

> **Примечание**
>
> Чтобы выбрать несколько ящиков подряд, нажмите на первый и последний ящики в диапазоне, удерживая при этом клавишу **Shift**. Чтобы выбрать несколько отдельных ящиков, удерживайте клавишу **Ctrl**.

4. В появившемся окне свойств выберите **Делегирование почтового ящика**.
5. В правой нижней части окна в разделе **Полный доступ** нажмите **Добавить**.
6. В появившемся окне укажите учетную запись для миграции, например `migration@example.com`.
7. Нажмите кнопку **ОК** — учетная запись добавится в раздел **Полный доступ**.
8. В окне свойств почтового ящика нажмите кнопку **ОК**.

Доступ ко всем ящикам

Используйте командную консоль Exchange (Exchange PowerShell).

1. Подключитесь к удаленному серверу Exchange.
2. Замените `migration@example.com` на вашу учетную запись для миграции и выполните командлет:

```
get-mailbox -ResultSize unlimited | Add-MailboxPermission -User
<migration@example.com> -AccessRights Fullaccess -InheritanceType all -
AutoMapping $false
```

Учетная запись для миграции получит права полного доступа ко всем почтовым ящикам организации в Exchange.

Подготовка CSV-файла

1. Скачайте шаблон CSV-файла.
2. По образцу добавьте в файл:
   2.1. Логин сотрудника в Яндекс 360 для бизнеса.
   2.2. Исходную учетную запись для миграции, например `example.com/migration/user`, где:
   - `example.com` — домен в Active Directory, под которым аутентифицируется пользователь исходного почтового ящика;
   - `migration` — имя учетной записи для миграции;
   - `user` — `Alias`-атрибут или `Mailnickname` исходного почтового ящика сотрудника в Microsoft Exchange Server.

   2.3. Пароль учетной записи администратора.

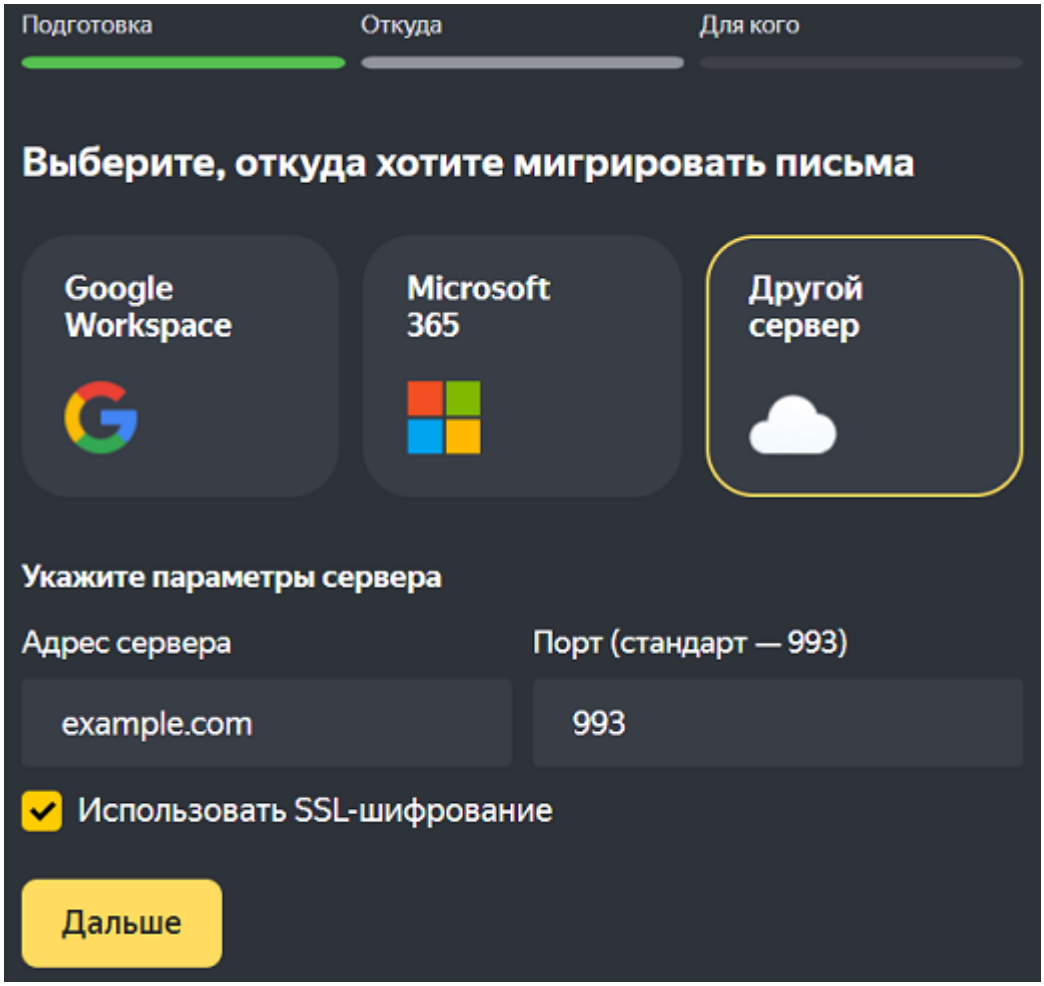
У вас должен получиться файл с такой структурой:

```
"yandex_login";"external_email";"external_password"
"user1";"example.com/migration/user1";"Password"
"user2";"example.com/migration/user2";"Password"
```

```
"user3";"example.com/migration/user3";"Password"
```

Запуск миграции

1. В меню слева выберите **Общие настройки → Миграция**.
2. Выберите, что хотите перенести: нажмите **Миграция писем**.
3. Выберите, откуда хотите перенести почту: нажмите **Другой сервер**.
4. Задайте параметры подключения:
   - доменное имя или IP-адрес почтового сервера;
   - порт сервера (например, 993);
   - включите SSL-шифрование.



5. Загрузите CSV-файл.
6. Нажмите **Запустить миграцию**.

Примечание

Если вы планируете запускать миграцию несколько раз, перед каждым новым запуском сохраняйте файл с логами (его можно скачать, нажав кнопку **Детализация**). Если при миграции появятся ошибки, вы сможете отследить, при каком именно запуске это произошло.

Решение проблем с миграцией

Ознакомьтесь с возможными ошибками при миграции и способами, как их исправить.

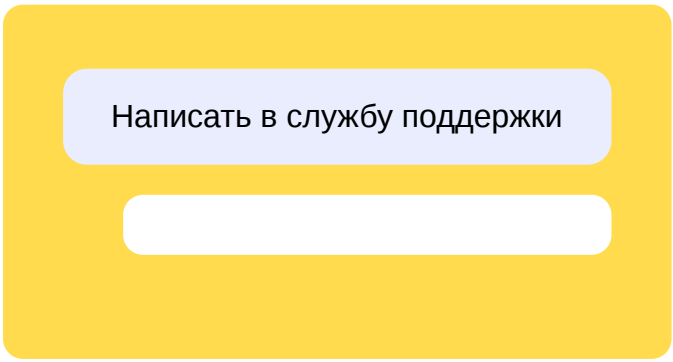
Ошибка аутентификации

Подключитесь к почтовому ящику пользователя от учетной записи для миграции. Используйте имя учетной записи из столбца **external_mail**, например `example.com/migration/user`, и пароль из столбца **external_password**. Если подключиться не удалось, проверьте настройки IMAP в Exchange Server и права полного доступа.

В CSV-файле удалена или изменена первая строка

Скачайте шаблон CSV-файла и скопируйте из него первую строку в ваш CSV-файл. Убедитесь, что предыдущий импорт завершился, и запустите новый импорт с исправленным CSV-файлом.

Чтобы посмотреть отчет с подробным описанием ошибок, на странице активной миграции в правом верхнем углу нажмите кнопку **Детализация**. О способах исправления см. Отчет об ошибках миграции.



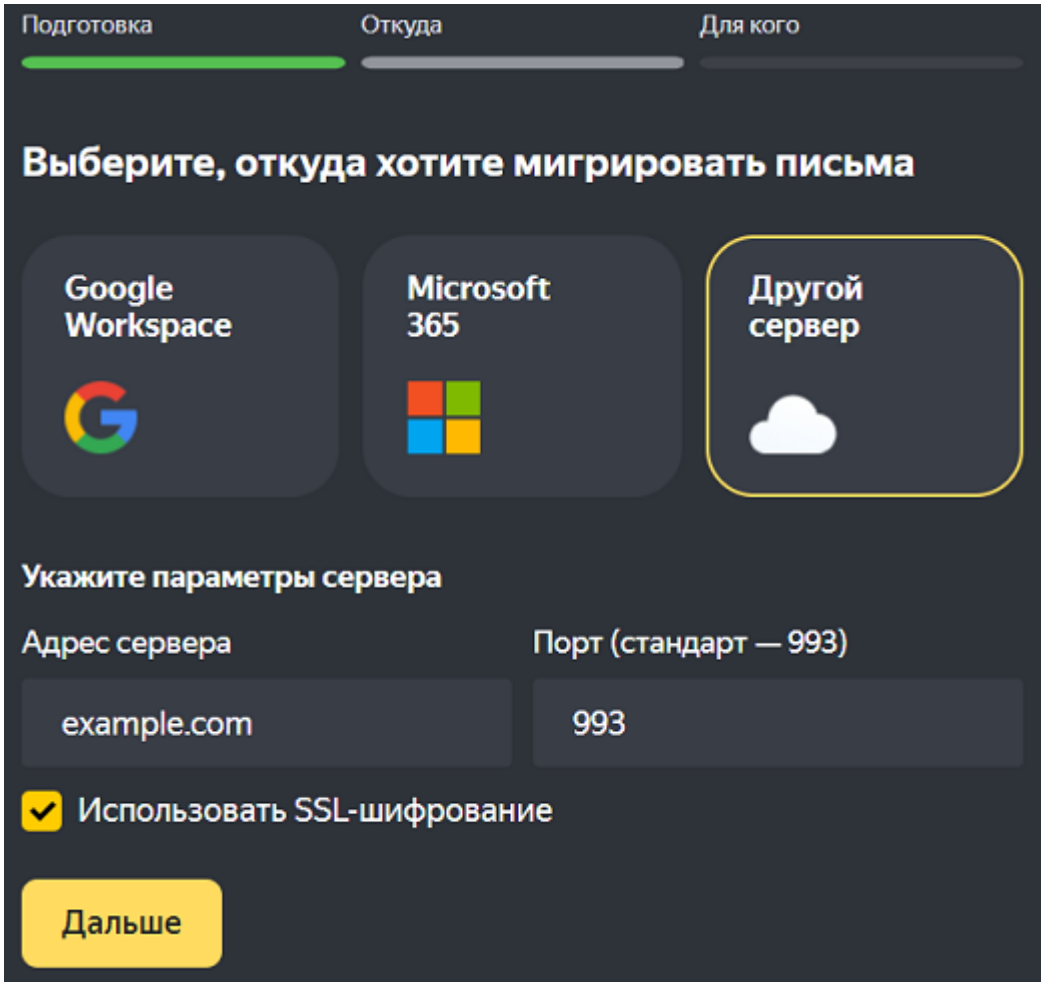
Другой сервер

Внимание

Вы можете импортировать почтовые ящики сотрудников, только если к организации подключен домен.

Чтобы импортировать почтовые ящики:

1. В меню слева выберите **Общие настройки** → **Миграция**.
2. Выберите, что хотите перенести сначала: письма или файлы.
3. Выберите, откуда хотите перенести почту: нажмите **Другой сервер**.
4. Задайте параметры подключения:
   - доменное имя или IP-адрес почтового сервера;
   - порт сервера (например, 993);
   - включите SSL-шифрование.



5. Укажите аккаунты, для которых нужно запустить миграцию:
   5.1. Скачайте шаблон CSV-файла.
   5.2. По образцу добавьте в файл почтовые адреса и пароли исходных почтовых ящиков, а также данные для создания ящиков в Почте для бизнеса.

Первая строка файла — заголовки полей аккаунта. В каждой следующей строке файла должны быть указаны данные одного аккаунта в кавычках через точку с запятой.

Обязательно должны быть указаны адрес и пароль исходного почтового ящика и логин аккаунта на вашем домене, в который нужно импортировать письма.

> **Примечание**
>
> Вы можете добавить до 20 000 логинов сотрудников.

5.3. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**).

> **Внимание**
>
> Если сохранить файл в другой кодировке, он будет распознан неправильно.

5.4. Нажмите кнопку **Загрузить CSV** и укажите ваш файл.

6. Нажмите **Запустить миграцию**.

> **Примечание**
>
> Если вы планируете запускать миграцию несколько раз, перед каждым новым запуском сохраняйте файл с логами (его можно скачать, нажав кнопку **Детализация**). Если при миграции появятся ошибки, вы сможете отследить, при каком именно запуске это произошло.

Решение проблем с миграцией

Ознакомьтесь с возможными ошибками при миграции и способами, как их исправить.

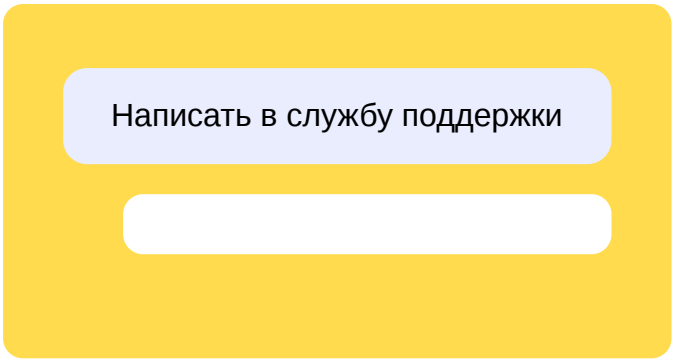
Указан неправильный пароль от исходного ящика

Попросите сотрудников настроить сбор писем из их исходных ящиков в новые. Это позволит завершить процесс миграции и убрать ошибку авторизации.

В CSV-файле удалена или изменена первая строка

Скачайте шаблон CSV-файла и скопируйте из него первую строку в ваш CSV-файл. Убедитесь, что предыдущий импорт завершился, и запустите новый импорт с исправленным CSV-файлом.

Чтобы посмотреть отчет с подробным описанием ошибок, на странице активной миграции в правом верхнем углу нажмите кнопку **Детализация**. О способах исправления см. Отчет об ошибках миграции.


Написать в службу поддержки

Microsoft 365 (One Drive)

Запуск миграции

1. Подготовьте секрет, подключите домен и подготовьте аккаунты сотрудников, если не сделали этого раньше.

   > **Примечание**
   >
   > Секрет применяется ко всем запущенным миграциям. Если вы уже запустили миграцию и после этого загружаете новый секрет, то он применится к этой миграции. При этом учитываются разрешения секрета: если новый секрет имеет доступ только к файлам и у вас запущена миграция писем, она остановится.

2. Выберите, откуда хотите перенести файлы: нажмите **Microsoft 365**.
3. Загрузите файл секрета и нажмите **Дальше**.
4. Укажите аккаунты, для которых нужно запустить миграцию:
   4.1. Скачайте шаблон CSV-файла.
   4.2. По образцу добавьте в файл логины сотрудников, для которых нужно перенести файлы.

   Первая строка файла — заголовки полей аккаунта, не удаляйте ее. В каждой следующей строке файла должны быть указаны данные одного аккаунта в кавычках через точку с запятой.

   Логины в столбце `yandex_login` должны совпадать с именами учетных записей в Microsoft 365. Например, для учетной записи `i.ivanov@example.test` укажите логин `i.ivanov` в столбце `yandex_login`.

   У вас должен получиться файл со структурой:

   ```
   "yandex_login";"external_email"
   "i.ivanov";"i.ivanov@example.test"
   "m.makarova";"m.makarova@example.test"
   ```

   > **В файле для миграции может быть не больше 20 000 строк**
   >
   > Если нужно мигрировать больше сотрудников, создайте дополнительный файл и запустите ещё одну миграцию. Она может идти параллельно с первой.

   4.3. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**).

> **Внимание**
>
> Если сохранить файл в другой кодировке, он будет распознан неправильно.

4.4. Нажмите кнопку **Загрузить CSV** и укажите ваш файл.

5. Нажмите **Запустить миграцию**.

   Миграция происходит не сразу. Сбор данных займет от нескольких минут до двух часов, затем файлы начнут появляться на Яндекс Диске. Если какие-то файлы на Яндекс Диске уже есть (например, были перенесены ранее), то сравниваются даты их последнего изменения в One Drive и Яндекс Диске и более старые версии заменяются новыми.

   После завершения миграции файлы не синхронизируются. Если в One Drive после запуска миграции появились новые файлы и вы хотите перенести их на Яндекс Диск, начните новую миграцию.

> **Примечание**
>
> Если вы планируете запускать миграцию несколько раз, перед каждым новым запуском сохраняйте файл с логами (его можно скачать, нажав кнопку **Детализация**). Если при миграции появятся ошибки, вы сможете отследить, при каком именно запуске это произошло.

Что будет, если остановить миграцию

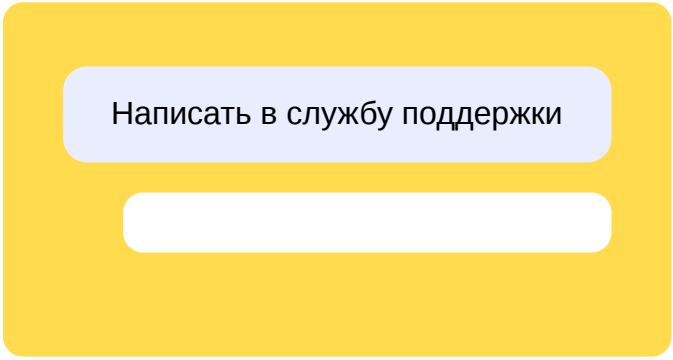
Остановятся все запущенные миграции.

Что будет, если начать новую миграцию

Новая миграция будет идти параллельно с запущенными миграциями.

Решение проблем с миграцией

Чтобы посмотреть отчет с подробным описанием ошибок, на странице активной миграции в правом верхнем углу нажмите кнопку **Детализация**. О способах исправления см. Отчет об ошибках миграции.



Библиотеки документов SharePoint Online

Вы можете скопировать содержимое библиотек документов из Microsoft SharePoint Online на личные Яндекс Диски пользователей Яндекс 360 для бизнеса или общие диски вашей организации.

Процесс и ограничения

Сколько библиотек можно копировать одновременно

В одном файле для миграции может быть не больше 20 000 строк. Для каждого сотрудника надо указать логин диска, откуда мигрируются данные, и логин общего или личного Яндекс Диска, куда данные должны попасть. Внутри файла логины не должны повторяться.

Если для одного логина надо скопировать несколько библиотек на Диск, делайте это в разных процессах. Такие миграции нужно запускать последовательно: копирование каждой следующей библиотеки должно начинаться после завершения предыдущей.

Куда копируются файлы

Во время миграции на Яндекс Диске пользователя создается отдельная папка. Содержимое библиотеки SharePoint копируется со всей структурой подпапок и файлов.

Как формируется имя и путь до папки

У каждой библиотеки документов есть уникальный URL. Он содержит:

- название тенанта (в примере ниже `tenantname`);
- семейство сайтов (в примере ниже `sites`);
- имя сайта (в примере ниже `examplesite`);
- имя подсайта, если есть (в примере ниже `subsite`);
- имя библиотеки документов (в примере ниже `Shared%20Documents`).

Из этих элементов формируется иерархия подпапок на Диске. Например, если путь до библиотеки документов имеет вид `https://tenantname.sharepoint.com/sites/examplesite/subsite/Shared%20Documents`, то на Диске будет создана структура подпапок `http://disk.yandex.ru/client/disk/tenantname/sites/examplesite/subsite/Shared%20Documents`.

Если вы используете библиотеку документов в корневом сайте (`root`), то она скопируется в папку вида `http://disk.yandex.ru/client/disk/tenantname/root/root/Shared%20Documents`.

Ограничения для копирования файлов

Для успешной миграции длина имени файла в библиотеке не должна превышать 255 символов. Файлы, которые не соответствуют этому условию, не будут скопированы. Перед миграцией проверьте содержимое библиотеки SharePoint на наличие таких файлов и переименуйте их.

Запуск миграции

1. Подготовьте секрет, подключите домен и подготовьте аккаунты сотрудников, если не сделали этого раньше.

   > **Примечание**
   >
   > Секрет применяется ко всем запущенным миграциям. Если вы уже запустили миграцию и после этого загружаете новый секрет, то он применится к этой миграции. При этом учитываются разрешения секрета: если новый секрет имеет доступ только к файлам и у вас запущена миграция писем, она остановится.

2. Убедитесь, что у каждого пользователя Яндекс 360 для бизнеса на Диске достаточно места для миграции файлов. Проверить свободное место на Диске пользователя можно в карточке сотрудника.
3. В кабинете организации выберите **Общие настройки** → **Миграция**.
4. Выберите вариант миграции:
   - **Файлы на персональных дисках**, если нужно перенести файлы на личные Диски пользователей Яндекс 360 для бизнеса.
   - **Файлы на общих дисках**, если если нужно перенести файлы на общие диски организации.
5. Выберите, откуда хотите мигрировать файлы: нажмите **Microsoft 365**.
6. Загрузите файл секрета и нажмите **Дальше**.
7. Подготовьте CSV-файл по инструкции.
8. Нажмите **Запустить миграцию**.

   Сбор данных займет от нескольких минут до двух часов, затем файлы начнут появляться на Яндекс Диске. Если какие-то файлы на Яндекс Диске уже есть (например, были перенесены ранее), то сравниваются даты их последнего изменения в SharePoint Online и Яндекс Диске и более старые версии заменяются новыми.

   После завершения копирования файлы больше не синхронизируются. Если в библиотеке SharePoint после завершения копирования появились новые файлы и вы хотите перенести их на Яндекс Диск, начните новую миграцию.

По итогу миграции проверьте, что количество скопированных файлов равно количеству файлов в источнике. Если вы планируете запускать процесс несколько раз, перед каждым новым запуском сохраняйте отчет по миграции. Если при миграции появятся ошибки, вы сможете отследить, при каком именно запуске это произошло.

Где посмотреть отчет по миграции

Чтобы скачать отчет, на странице активной миграции в правом верхнем углу нажмите кнопку **Детализация**. В отчете отражаются логи последнего запущенного процесса миграции, в которых описана детальная информация о количестве файлов, скопированных на личный Диск, и ошибках, возникших в процессе копирования.

Что будет, если остановить миграцию

Остановятся все запущенные миграции. Всё, что скопировано на момент завершения, сохранится.

Что будет, если начать новую миграцию

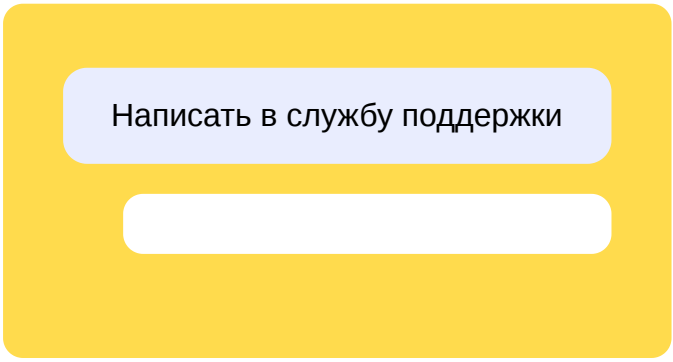
Если начать новую миграцию до завершения предыдущей, то новая миграция будет идти параллельно с уже запущенным процессом для всех личных Дисков.

Внимание

Запускать миграцию с файлом, содержащим логин, для которого уже был запущен процесс миграции, можно, только если первая миграция для этого логина завершилась. Статус завершения можно посмотреть в детализации.

Решение проблем с миграцией

Подробное описание ошибок, которые возникли в результате миграции, можно посмотреть в отчете по миграции. Со способами их исправления можно ознакомиться в разделе Отчет об ошибках миграции.



Google Workspace (Google Drive)

Запуск миграции

1. Подготовьте секрет, подключите домен и подготовьте аккаунты сотрудников, если не сделали этого раньше.
2. Убедитесь, что у каждого сотрудника на Диске достаточно места для миграции его файлов с сервера-источника.
3. В меню слева выберите **Общие настройки** → **Миграция**.
4. Выберите, что хотите перенести: нажмите **Миграция файлов**.
5. Выберите, откуда хотите перенести файлы: нажмите **Google Workspace**.
6. Загрузите файл секрета и нажмите **Дальше**.
7. Укажите аккаунты, для которых нужно запустить миграцию:
   7.1. Скачайте шаблон CSV-файла.
   7.2. По образцу добавьте в файл логины сотрудников, для которых нужно перенести файлы.

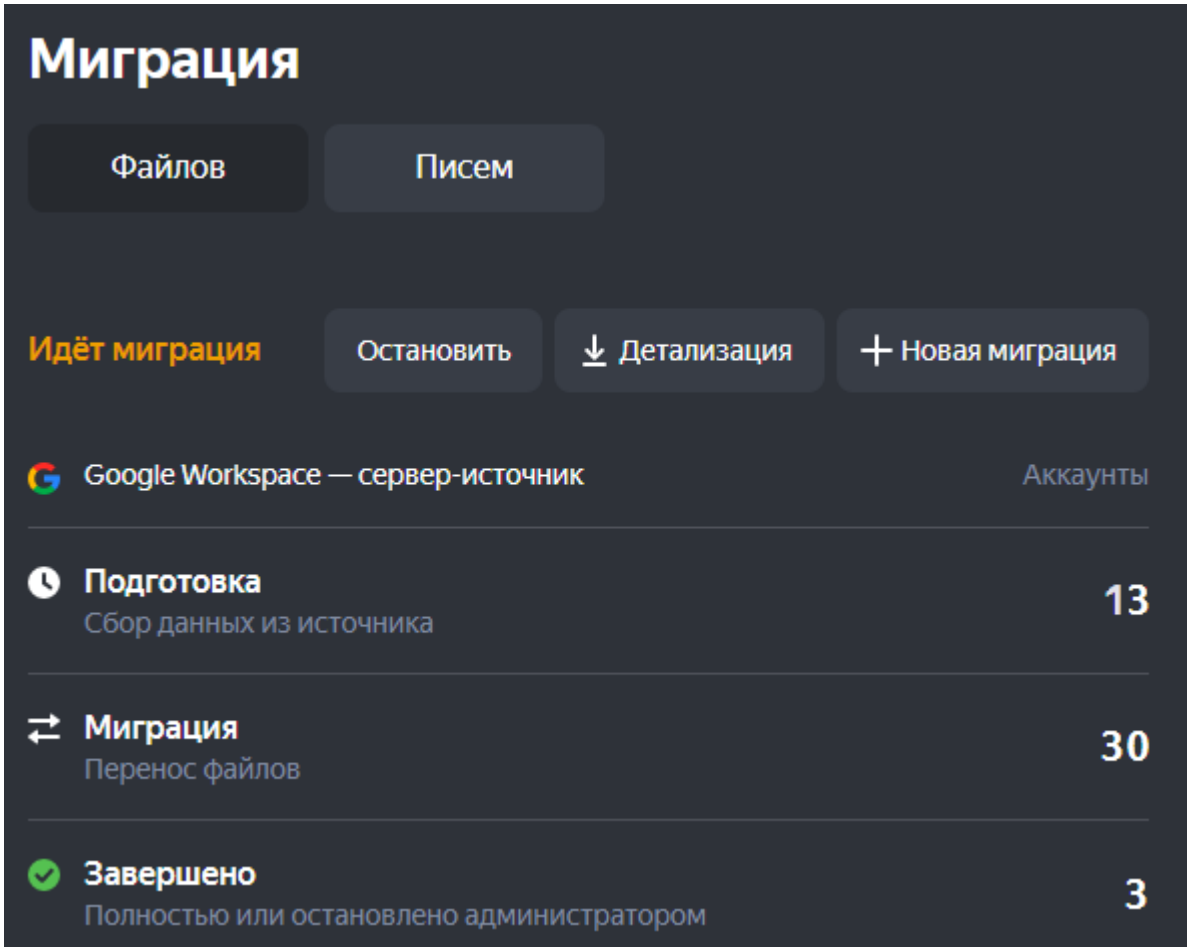
> **В файле для миграции может быть не больше 20 000 строк**
>
> Если нужно мигрировать больше сотрудников, создайте дополнительный файл и запустите ещё одну миграцию. Она может идти параллельно с первой.

   7.3. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**).

> **Внимание**
>
> Если сохранить файл в другой кодировке, он будет распознан неправильно.

   7.4. Нажмите кнопку **Загрузить CSV** и укажите ваш файл.
8. Нажмите **Запустить миграцию** — начнется перенос файлов.

В результате запуска вы увидите статус **Идет миграция**.



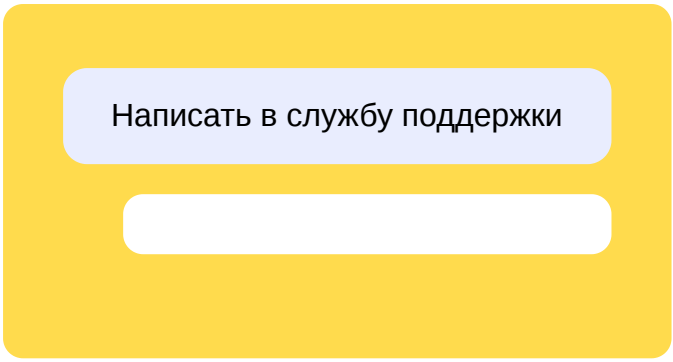
Если какие-то файлы на Яндекс Диске уже есть (например, были перенесены ранее), то сравниваются даты их последнего изменения в Google Drive и Яндекс Диске и более старые версии заменяются новыми.

Примечание

Если вы планируете запускать миграцию несколько раз, перед каждым новым запуском сохраняйте файл с логами (его можно скачать, нажав кнопку **Детализация**). Если при миграции появятся ошибки, вы сможете отследить, при каком именно запуске это произошло.

Решение проблем с миграцией

Чтобы посмотреть отчет с подробным описанием ошибок, на странице активной миграции в правом верхнем углу нажмите кнопку **Детализация**. О способах исправления см. Отчет об ошибках миграции.


Написать в службу поддержки

Общие Диски Google Drive

Вы можете скопировать содержимое общих Дисков из Google WorkSpace на личные Яндекс Диски пользователей Яндекс 360 для бизнеса или на общие диски вашей организации.

Процесс и ограничения

Ограничения на одновременное копирование

В одном файле для миграции может быть не больше 20 000 строк. Для каждого сотрудника надо указать логин диска, откуда мигрируются данные, и логин общего или личного Яндекс Диска, куда данные должны попасть. Внутри файла логины не должны повторяться.

Если для логина надо скопировать несколько общих дисков на один личный Диск, делайте это в разных процессах. Такие миграции нужно запускать последовательно: миграция для каждого следующего общего диска должна начинаться после завершения миграции предыдущего.

Куда копируются файлы

Во время копирования общих дисков Google Drive на личном Яндекс Диске пользователя создается отдельная папка. Содержимое общего диска Google Drive копируется со всей структурой подпапок и файлов.

Как формируется имя и путь до папки

У каждого общего диска Google Drive есть:

- имя (не уникально на Google Drive);
- идентификатор (уникален на Google Drive).

На основе этих двух параметров составляется уникальное имя папки на Яндекс Диске. Например, если общий диск называется `SharedDisk`, а его идентификатор `1qazXSW23edcVFR45tg`, то имя папки на личном Яндекс Диске, в который перенесется все содержимое общего диска, будет `SharedDisk_1qazXSW23edcVFR45tg`.

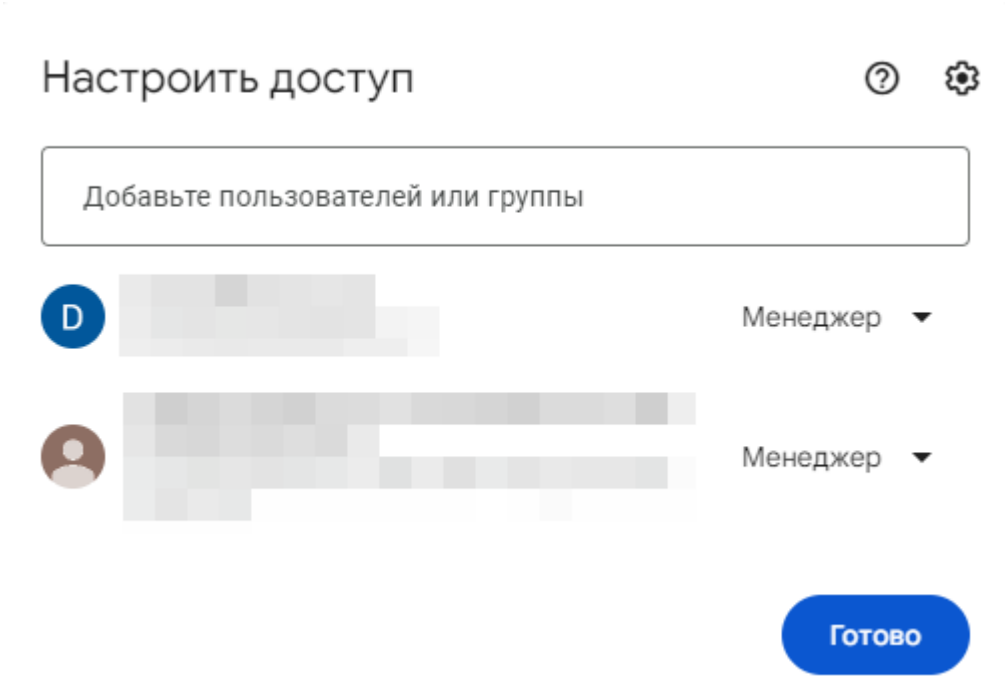
Ограничения для копирования файлов

Для успешной миграции длина имени файла на общем диске не должна превышать 255 символов. Файлы, которые не соответствуют этому условию, не будут скопированы. Перед миграцией проверьте содержимое общих дисков Google Drive на наличие таких файлов и переименуйте их.

Запуск миграции

1. Подготовьте секрет, подключите домен и подготовьте аккаунты сотрудников, если не сделали этого раньше.
2. Сервисной учетной записи, которую вы получили при подготовке секрета на нужные общие диски, выдайте права «Менеджер». Для этого:
   2.1. Перейдите в раздел **Приложение** → **Google Workspace** → **Диск и Документы** → **Управление общими дисками**.

2.2. На нужном диске нажмите **Управление пользователями** и добавьте сервисную учетную запись с правами «Менеджер».



2.3. Повторите предыдущий шаг для всех дисков, которые планируете мигрировать.

3. Убедитесь, что у каждого пользователя Яндекс 360 для бизнеса на Диске достаточно места для миграции файлов с общего диска Google Drive. Проверить свободное место на Диске пользователя можно в карточке сотрудника.
4. В кабинете организации выберите **Общие настройки** → **Миграция**.
5. Выберите вариант миграции:
   - **Файлы на персональных дисках**, если нужно перенести файлы на личные Диски пользователей Яндекс 360 для бизнеса.
   - **Файлы на общих дисках**, если если нужно перенести файлы на общие диски организации.
6. Выберите, откуда хотите мигрировать файлы: нажмите **Google Workspace**.
7. Загрузите файл секрета и нажмите **Дальше**.
8. Подготовьте CSV-файл по инструкции.
9. Нажмите кнопку **Загрузить CSV** и укажите ваш файл.
10. Нажмите **Запустить миграцию** — начнется перенос файлов.

    В результате запуска вы увидите статус **Идёт миграция**.

    Сбор данных займет от нескольких минут до двух часов, затем файлы начнут появляться на Яндекс Диске. Если какие-то файлы на Яндекс Диске уже есть (например, были перенесены ранее), то сравниваются даты их последнего изменения в Google Drive и Яндекс Диске и более старые версии заменяются новыми.

    После завершения копирования файлы больше не синхронизируются. Если в библиотеке SharePoint после завершения копирования появились новые файлы и вы хотите перенести их на Яндекс Диск, начните новую миграцию.

По итогу миграции проверьте, что количество скопированных файлов равно количеству файлов в источнике. Если вы планируете запускать процесс несколько раз, перед каждым новым запуском

сохраняйте отчет по миграции. Если при миграции появятся ошибки, вы сможете отследить, при каком именно запуске это произошло.

Где посмотреть отчет по миграции

Чтобы скачать отчет, на странице активной миграции в правом верхнем углу нажмите кнопку **Детализация**. В отчете отражаются логи последнего запущенного процесса миграции, в которых описана детальная информация о количестве файлов, скопированных на личный Диск, и ошибках, возникших в процессе копирования.

Что будет, если остановить миграцию

Остановятся все запущенные миграции. Всё, что скопировано на момент завершения, сохранится.

Что будет, если начать новую миграцию

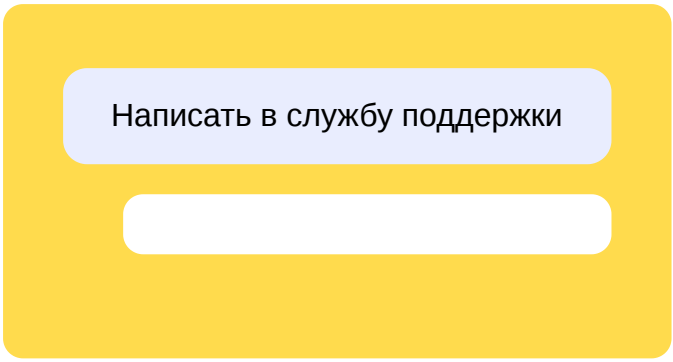
Если начать новую миграцию до завершения предыдущей, то новая миграция будет идти параллельно с уже запущенным процессом для всех личных или общих дисков.

Внимание

Запускать миграцию с файлом, содержащим логин, для которого уже был запущен процесс миграции, можно, только если первая миграция для этого логина завершилась. Статус завершения можно посмотреть в детализации.

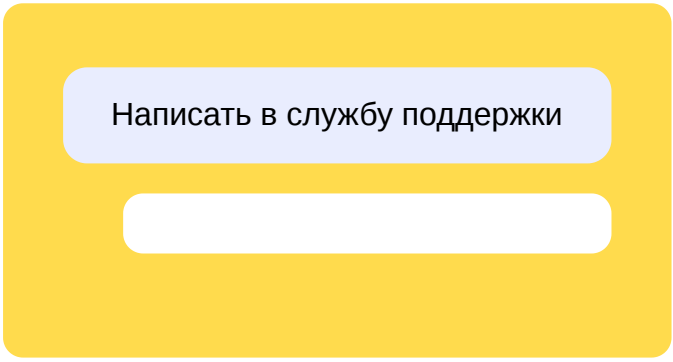
Решение проблем с миграцией

Подробное описание ошибок, которые возникли в результате миграции, можно посмотреть в отчете по миграции. Со способами их исправления можно ознакомиться в разделе Отчет об ошибках миграции.



Другой сервер

1. Подключите домен и подготовьте аккаунты сотрудников, если не сделали этого раньше.
2. Попросите сотрудников перенести файлы самостоятельно: скачать все файлы на компьютер, а затем загрузить в облако с помощью программы Яндекс Диск для компьютера. О том, как работать с программой, см. в Справке.



Как подготовить CSV-файл для миграции

Миграция из личных дисков Google Drive или One Drive

На какие диски в Яндекс 360 для бизнеса вы хотите перенести файлы?

На личные Диски сотрудников

1. Скачайте шаблон и заполните его.

   Как заполнять

   Первая строка файла — заголовки полей аккаунта, не удаляйте ее. В каждой следующей строке файла укажите данные в кавычках через точку с запятой:

   - `yandex_login` — логины сотрудников, на чьи личные Диски будете мигрировать файлы.

     Важно: для миграции из One Drive логины должны совпадать с именами учетных записей в Microsoft 365. Например, для учетной записи `i.ivanov@example.test` укажите логин `i.ivanov`.

     Если мигрируете из Google Drive, этого правила можно не придерживаться.
   - `external_email` — здесь нужно указать почту пользователя, с которой он входит учетную запись. В Microsoft 365 она ещё называется UserPrincipalName (UPN) — найти её можно в центре администрирования, в разделе Пользователи → Активные пользователи. Другие email пользователя не подойдут.

   > **В файле для миграции может быть не больше 20 000 строк**
   >
   > Если нужно мигрировать больше сотрудников, создайте дополнительный файл и запустите ещё одну миграцию. Она может идти параллельно с первой.

   Что должно получиться

   ```
   "yandex_login";"external_email"
   "i.ivanov";"i.ivanov@example.test"
   "m.makarova";"m.makarova@example.test"
   ```

2. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**). Если сохранить файл в другой кодировке, он будет распознан неправильно.

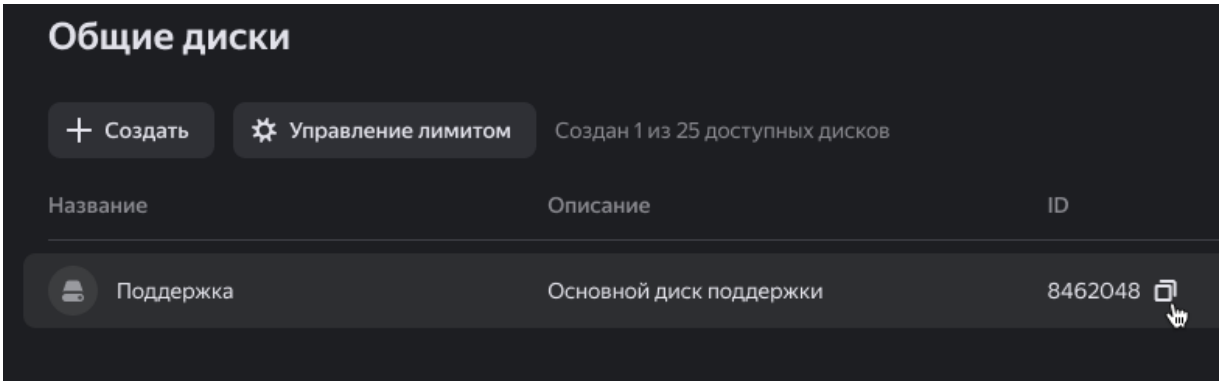
На общие диски организации

1. Скачайте шаблон и заполните его.

   Как заполнять

Первая строка файла — заголовки полей аккаунта, не удаляйте ее. В каждой следующей строке файла укажите данные в кавычках через точку с запятой:

- `yandex_disk_id` — идентификатор общего диска вашей организации, куда вы хотите мигрировать файлы. Его можно скопировать в разделе Общие диски:



- `external_email` — здесь нужно указать почту пользователя, с которой он входит учетную запись. В Microsoft 365 она ещё называется UserPrincipalName (UPN) — найти её можно в центре администрирования, в разделе Пользователи → Активные пользователи. Другие email пользователя не подойдут.

> **В файле для миграции может быть не больше 20 000 строк**
>
> Если нужно мигрировать больше сотрудников, создайте дополнительный файл и запустите ещё одну миграцию. Она может идти параллельно с первой.

Что должно получиться

```
"yandex_disk_id";"external_email"
"12345678";"i.ivanov@example.test"
"87654321";"m.makarova@example.test"
```

2. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**). Если сохранить файл в другой кодировке, он будет распознан неправильно.

Миграция из общих дисков Google Drive или из библиотек документов MS SharePoint Online

На какие диски в Яндекс 360 для бизнеса вы хотите перенести файлы?

На личные Диски сотрудников

1. Скачайте нужный шаблон:
   - Для миграции из MS SharePoint Online. Скачать.
   - Для миграции из Google Drive. Скачать.
2. Заполните его.

Как заполнять

Первая строка файла — заголовки полей аккаунта, не удаляйте ее. В каждой следующей строке файла укажите данные в кавычках через точку с запятой:

- `yandex_login` — логины сотрудников, на чьи личные Диски будете мигрировать файлы.

  Важно: для миграции из SharePoint Online логины должны совпадать с именами учетных записей в Microsoft 365. Например, для учетной записи `i.ivanov@example.test` укажите логин `i.ivanov`.

  Если мигрируете из Google Drive, этого правила можно не придерживаться.
- `drive_id` — для миграции из Microsoft SharePoint Online укажите URL библиотеки документов, например `https://tenantname.sharepoint.com/sites/examplesite/subsite/Shared%20Documents`.

  Для миграции из Google Drive укажите уникальные идентификаторы дисков. Идентификатор диска можно найти в адресной строке браузера:

  1. Откройте общий диск в Google Drive.
  2. Перейдите в адресную строку браузера и скопируйте конец ссылки после слеша. Например, в ссылке `https://drive.google.com/drive/u/0/folders/1qazXSW23edcVFR45tg` содержится идентификатор `1qazXSW23edcVFR45tg`.
  3. Если в идентификаторе есть дефисы, удалите их, чтобы остались только цифры и буквы.

> **В файле для миграции может быть не больше 20 000 строк**
>
> Если нужно мигрировать больше сотрудников, создайте дополнительный файл и запустите ещё одну миграцию. Она может идти параллельно с первой.

Что должно получиться

Для миграции из Microsoft SharePoint Online:

```
"yandex_login";"drive_id"
"i.ivanov";"https://tenantname.sharepoint.com/sites/examplesite/subsite/Shared%
"m.makarova";"https://tenantname.sharepoint.com/sites/examplesite/subsite/Share
```

Для миграции из Google Drive:

```
"yandex_login";"drive_id"
"i.ivanov";"1qazXSW23edcVFR45tg"
"m.makarova";"2qazXSW34edcVFR56tg"
```

3. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**). Если сохранить файл в другой кодировке, он будет распознан неправильно.

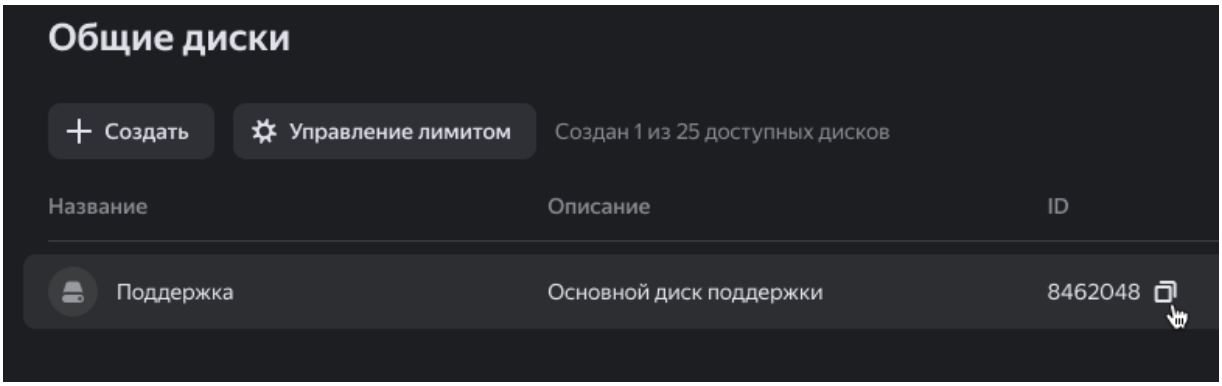
На общие диски организации

1. Скачайте шаблон и заполните его.

   Как заполнять

   Первая строка файла — заголовки полей аккаунта, не удаляйте ее. В каждой следующей строке файла укажите данные в кавычках через точку с запятой:

   - `yandex_disk_id` — идентификатор общего диска вашей организации, куда вы хотите мигрировать файлы. Его можно скопировать в разделе Общие диски:

   - `drive_id` — для миграции из Microsoft SharePoint Online укажите URL библиотеки документов, например `https://tenantname.sharepoint.com/sites/examplesite/subsite/Shared%20Documents`.

     Для миграции из Google Drive укажите уникальные идентификаторы дисков. Идентификатор диска можно найти в адресной строке браузера:

     1. Откройте общий диск в Google Drive.
     2. Перейдите в адресную строку браузера и скопируйте конец ссылки после слеша. Например, в ссылке `https://drive.google.com/drive/u/0/folders/1qazXSW23edcVFR45tg` содержится идентификатор `1qazXSW23edcVFR45tg`.
     3. Если в идентификаторе есть дефисы, удалите их, чтобы остались только цифры и буквы.

   > **В файле для миграции может быть не больше 20 000 строк**
   >
   > Если нужно мигрировать больше сотрудников, создайте дополнительный файл и запустите ещё одну миграцию. Она может идти параллельно с первой.

   Что должно получиться

   Для миграции из Microsoft SharePoint Online:

   ```
   "yandex_disk_id";"drive_id"
   "12345678";"https://tenantname.sharepoint.com/sites/examplesite/subsite/Shared%
   ```

```
"23456789";"https://tenantname.sharepoint.com/sites/examplesite/subsite/Shared%
```

Для миграции из Google Drive:

```
"yandex_disk_id";"drive_id"
"12345678";"1qazXSW23edcVFR45tg"
```

2. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**). Если сохранить файл в другой кодировке, он будет распознан неправильно.

Написать в службу поддержки

Миграция досок

Можно перенести доски из Miro, чтобы продолжать работать с ними в Яндекс Досках.

Для Досок в режиме on-premises другая инструкция

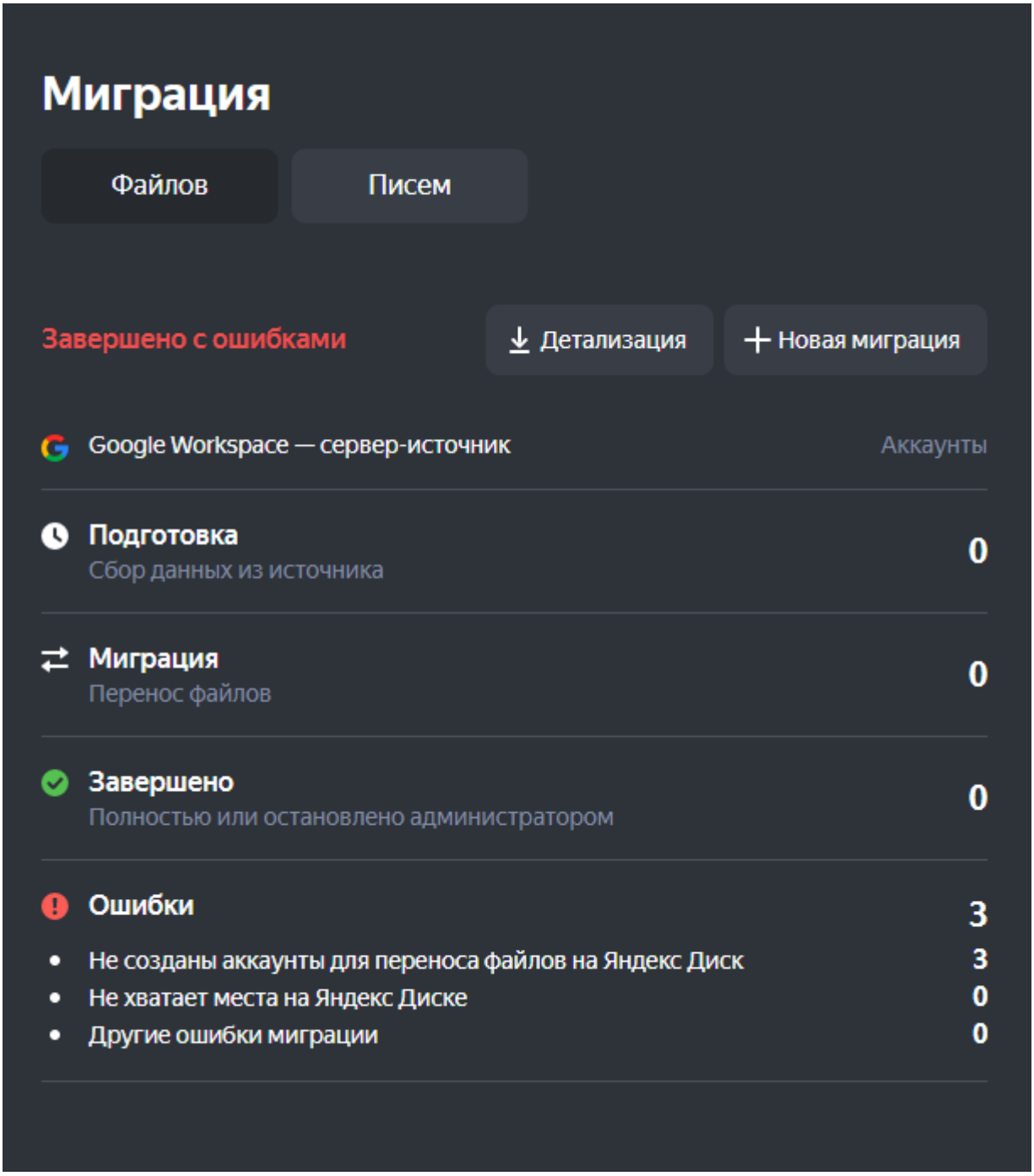
Эта статья о миграции досок через веб-интерфейс. О том, как импортировать доски из Miro в режиме on-premises читайте в разделе Настройка импорта досок из Miro.

Если у вас есть доступ к доскам через аккаунт администратора Miro, вы можете перенести все доступные доски или попросить сотрудников перенести доски самостоятельно с помощью импорта. Перейти к инструкции в Справке Яндекс Досок

Если вы не нашли ответа на свой вопрос в Справке Яндекс Досок, заполните короткую форму — мы ответим вам на почту.

Отчет об ошибках миграции

Количество ошибок и их общее описание отображаются в разделе **Общие настройки** → **Миграция**.



Чтобы посмотреть подробный отчет, нажмите кнопку **Детализация**.

Значение полей в отчете об ошибках

Миграция Почты

- **login** — логин сотрудника, у которого возникла ошибка миграции;
- **status** — статус миграции;
- **error_reason** — текст ошибки;

- **external_mailbox_messages_count** — количество сообщений во внешнем ящике на момент создания миграции (первичного запуска миграции для этого ящика);
- **collected_messages_count** — количество сообщений, перенесенных в Яндекс Почту;
- **failed_to_collect_messages_count** — количество сообщений, которые не удалось перенести;
- **latest_sync_ts** — дата и время последнего запуска цикла синхронизации для почтового ящика (если запусков не было, содержит фразу `collecting not started yet`);
- **latest_create_ts** — дата и время загрузки csv-файла с указанным логином сотрудника в мастер миграции.

Миграция Диска

- **login** — логин сотрудника, у которого возникла ошибка миграции;
- **status** — статус миграции;
- **error reason** — текст ошибки;
- **yandex_disk_quota** — квота в Яндекс Диске;
- **external_disk_files_size** — суммарный размер файлов на внешнем диске на момент создания миграции (первичного запуска миграции);
- **external_disk_files_count** — количество файлов на внешнем диске на момент создания миграции (первичного запуска миграции);
- **latest_touch_ts** — дата и время последнего запуска цикла миграции для пользователя (если миграция не стартовала, содержит фразу `migration not started yet`);
- **latest_create_ts** — дата и время загрузки csv-файла с указанным логином сотрудника в мастер миграции.

Ошибки запуска миграции

Ошибки загрузки секрета Google

Ошибки загрузки секрета Microsoft

Общие ошибки

Ошибки загрузки секрета Google

Текст ошибки	Решение

Client is unauthorized to retrieve access tokens using this method, or client not authorized for any of the scopes requested	1. Убедитесь, что включили доступ к проекту по API в ресурсах Admin SDK API, Google Drive API и Gmail API. 2. Запустите миграцию заново (нажмите кнопку **Новая миграция**). Если доступ к проекту включен, но ошибка появилась — обратитесь в службу поддержки Google.
Access Not Configured. Drive API has not been used in project ... before or it is disabled	1. Убедитесь, что правильно подготовили файл секрета. 2. Если в файле все верно, попробуйте создать новый сервисный аккаунт и секретный ключ. 3. Запустите миграцию заново (нажмите кнопку **Новая миграция**).

Текст ошибки	Решение
The domain administrators have disabled Drive apps	1. Убедитесь, что правильно подготовили файл секрета. 2. Проверьте доступ к Google Drive. 3. Запустите миграцию заново (нажмите кнопку **Новая миграция**).
Invalid credentials	1. Убедитесь, что правильно подготовили файл секрета. 2. Проверьте токен доступа к Google Drive. 3. Запустите миграцию заново (нажмите кнопку **Новая миграция**).
Disabled_client: The OAuth client was disabled...	1.

Application with identifier '...' was not found in the directory '...' This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant.	1. Убедитесь, что в файле секрета верно указали домен и идентификатор приложения, или подготовьте новый секрет. 2. Запустите миграцию заново (нажмите кнопку **Новая миграция**).
AADSTS7000215: Invalid client secret provided. Ensure the secret being sent in the request is the client secret value...	
AADSTS90013: Invalid input received from the user	Чаще всего ошибки возникают из-за неверного идентификатора и значения секрета. 1. Создайте новый файл секрета заново. 2. Запустите миграцию (нажмите кнопку **Новая миграция**) с новым файлом секрета.
Either scp or roles claim need to be present in the token	

AADSTS7000222: The provided client secret keys for app '73e871c4-2970-4aef-a0ff-7b0797cc46d1' are expired...	1. Создайте файл секрета заново. 2. Запустите миграцию (нажмите кнопку **Новая миграция**) с новым

Текст ошибки	**Решение**
Login error (при миграции с других серверов)	1. Убедитесь, что правильно указали логин и пароль в CSV-файле и включили доступ по IMAP или POP3 в настройках ящика. 2. Запустите миграцию (нажмите кнопку **Новая миграция**) не раньше чем через 1 час, чтобы не сработала защита от взлома почтового ящика.

Connection error	1. Убедитесь, что при авторизации верно ввели адрес сервера, логин и пароль (актуально для миграции с другого сервера). 2. Попробуйте авторизоваться с этими данными в почтовой программе, например в Mozilla Thunderbird. 3. Если вы верно заполнили все поля в программе, но проблема остается, обратитесь в службу поддержки сервера, с которого переносите данные.
SSL handshake error	1. Проверьте, используется ли SSL-шифрование в исходном сервере. 2. Если SSL-шифрование используется, на вкладке **Миграция** в блоке **Другие серверы** включите опцию **Использовать SSL-шифрование**. Если SSL-шифрование не используется, отключите эту опцию. 3. Запустите миграцию заново (нажмите кнопку **Новая миграция**).

Forbidden	1. Проверьте доступы к API в Google Workspace или в Microsoft Azure. Если доступов не хватает — добавьте их. 2. Запустите миграцию заново (нажмите кнопку **Новая миграция**).
Not Found	1. Убедитесь, что правильно указали адрес исходного почтового ящика. 2. Запустите миграцию заново (нажмите кнопку **Новая миграция**). Если адрес исходного почтового ящика — это рассылка, перенести данные из него не получится.
Session expired, login again	1. Дождитесь, пока миграция завершится для всех аккаунтов. 2. Запустите новую миграцию только для аккаунтов, с которыми возникла проблема.

Login error (при миграции с серверов Google или Microsoft)	Исправьте разрешения для сервисного аккаунта — для этого обратитесь в службу поддержки сервера, с которого переносите данные.
ExternalUserNotFound	1. Убедитесь, что правильно указали исходный логин пользователя. 2. Запустите миграцию заново (нажмите кнопку **Новая миграция**).
DiskTemporaryError	Если в отчете много аккаунтов с такой ошибкой, запустите миграцию заново (нажмите кнопку **Новая**

Текст ошибки	**Решение**

Содержит фразу **HTTPSConnectionPool** **Пример** HTTPSConnectionPool(host='login.microsoftonline.com', port=443): Read timed out. (read timeout=None)	Если в отчете много аккаунтов с такой ошибкой, запустите миграцию заново (нажмите кнопку **Новая миграция**). Если проблема с некоторыми аккаунтами: 1. Дождитесь, пока миграция завершится для всех аккаунтов. 2. Нажмите кнопку **Новая миграция** и запустите ее только для аккаунтов, с которыми возникла проблема.

Подключение домена

Чтобы пользоваться сервисами Яндекс 360 для бизнеса, организации нужен **домен** — собственный адрес в интернете. По такому адресу обычно располагаются сайт организации (например, `www.example.com`) и ее электронная почта (например, `markov@example.com`).

> **Яндекс 360 не работает без домена**
>
> Для работы с сервисами Яндекс 360 домен понадобится в любом случае — даже если вы не планируете иметь сайт или пользоваться корпоративной почтой.

Чтобы получить в свое владение домен, его нужно зарегистрировать у регистратора, а затем подключить к организации в Яндекс 360.

Один домен может быть подключен **только к одной организации**. Если у вас несколько бизнесов и несколько организаций, понадобится несколько доменов.

При этом подключить несколько доменов к одной организации можно: один из них станет основным, а другие — алиасами (синонимами). В чем разница?

Как перенести домен из одной организации в другую?

Для этого отключите его от старой организации и подключите к новой. Как удалить домен

Последовательность действий

Есть два способа подключения домена к Яндексу: с автоматической настройкой и с ручной настройкой. Второй способ позволяет настроить домен более гибко. Если вы не знаете, какой способ выбрать, воспользуйтесь автоматической настройкой.

Чтобы домен был настроен автоматически, его нужно делегировать Яндексу.

Таким образом, последовательность действий выглядит так:

Чтобы пройти каждый этап, воспользуйтесь инструкциями:

- Как зарегистрировать домен
- Как подтвердить владение доменом
- Как настроить домен
- Как делегировать домен
- Как убедиться, что домен подключен

Написать в службу поддержки

Регистрация домена

Если у вашей организации пока нет собственного домена, перед подключением к Яндекс 360 его нужно зарегистрировать.

Не регистрируйте домен организации на физическое лицо

Если сотрудник, зарегистрировавший домен, уволится, вы потеряете доступ к управлению доменом — то есть фактически перестанете быть его владельцем.

Чтобы зарегистрировать домен, выберите любого регистратора и следуйте его инструкциям.

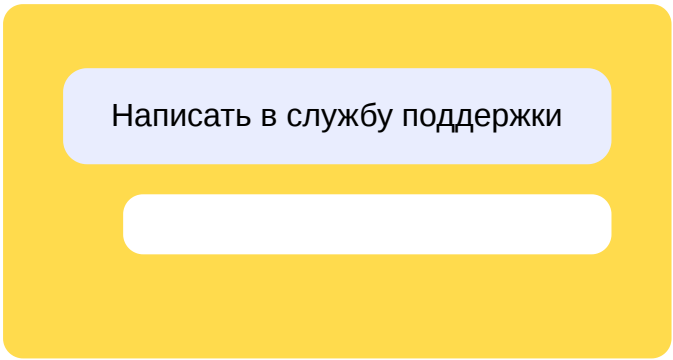
Регистрация домена — платная услуга, стоимость которой зависит от множества факторов и определяется регистратором. Регистрацию домена нужно каждый год продлевать — тоже платно. Не забывайте продлевать регистрацию, чтобы не лишиться своего домена.

Инструкции по регистрации домена в базах знаний разных регистраторов

- «Рег.ру»
- RU-CENTER
- «Регистратор R01»
- Beget
- Webnames.ru («Регтайм»)
- masterhost
- Nethouse

Можно ли воспользоваться услугами регистратора не из этого списка?

Конечно. Это просто примеры.



Делегирование домена

Делегирование домена на Яндекс — это передача Яндексу управления DNS-записями домена.

Делегирование упрощает подключение домена к Яндекс 360: если домен делегирован, его не нужно вручную настраивать.

Делегирование подойдет, если вы хотите как можно проще и быстрее настроить организацию и не планируете создавать вокруг домена какую-то сложную конфигурацию.

Важно

Делегируйте домен только **после** подтверждения. Как подтвердить домен

Как делегировать домен на Яндекс

Вам нужно добавить для своего домена два DNS-сервера Яндекса:

- Первичный сервер `dns1.yandex.net.`
- Вторичный сервер `dns2.yandex.net.`

Если в настройках делегирования есть поля для ввода IP-адресов, оставьте их пустыми.

Указать эти DNS-серверы вы можете в своем личном кабинете на сайте регистратора, поэтому конкретные инструкции доступны в базах знаний регистраторов:

- «Рег.ру»
- «Регистратор R01»
- Webnames.ru («Регтайм»)
- masterhost
- Nethouse

DNS-записи обновляются не мгновенно

Это занимает до 72 часов.

Смогу ли я управлять DNS-записями после делегирования — например, добавить новые?

Да, это можно будет делать в кабинете организации.

Написать в службу поддержки

Подтверждение домена

Прежде чем подключить домен к вашей организации, Яндексу нужно убедиться в том, что вы действительно являетесь владельцем этого домена.

Есть несколько способов подтвердить домен.

- Самый простой способ, доступный сразу после регистрации домена, — создать специальную **временную DNS-запись**. Такая запись может служить подтверждением владения доменом, так как доступ к управлению DNS-записями есть только у владельца.
- Если к вашему домену уже подключен **хостинг**, вы можете подтвердить домен, разместив на нем специальный HTML-файл или добавив тег в существующий.

Как получить данные для подтверждения домена

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Общие настройки** → **Домены**.
3. Впишите имя домена и нажмите **Добавить домен**.
4. Выберите способ подтверждения и следуйте инструкции на экране.

Как добавить данные к своему домену

Подтверждение с помощью DNS-записи

Чтобы добавить подтверждающую DNS-запись, вам нужно открыть панель управления DNS на сайте регистратора. Панели разных регистраторов немного отличаются друг от друга, но принцип всегда один и тот же.

Если возникнут вопросы, воспользуйтесь инструкцией, предоставленной регистратором:

- «Рег.ру»
- «Регистратор R01»
- Beget
- Webnames.ru («Регтайм»)
- masterhost
- Nethouse

Если вашего регистратора нет в списке, найдите инструкцию в его базе знаний.

DNS-записи обновляются не мгновенно

Это занимает до 72 часов.

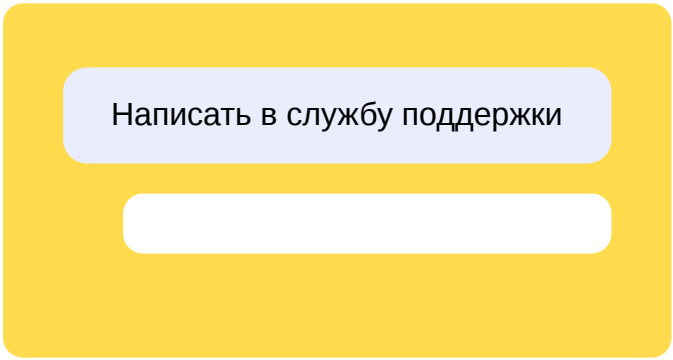
Подтверждение с помощью файла или тега

Чтобы подтвердить владение доменом этим способом, добавьте тег или файл по инструкции в кабинете.

Технически этот процесс ничем не отличается от других поправок, которые вы вносите на свой сайт, — просто воспользуйтесь привычными инструментами.

Что делать, если домен делегирован, но не подтвержден

> Чтобы подтвердить такой домен, нужно отменить делегирование: вернуть первичный и вторичный DNS-серверы, которые по умолчанию предлагает регистратор. После этого нужно пройти процедуру подтверждения домена, а затем делегировать домен заново.



Настройка DNS-записей

Чтобы зарегистрированным доменом можно было пользоваться — например, принимать и отправлять электронную почту или сделать сайт, — нужно создать для него ресурсные записи DNS. С помощью таких записей владелец домена указывает, какие именно сервисы должны отвечать за те или иные функции домена.

Подробнее

> Например, владелец организации «Мой бизнес» выбрал для нее домен `example.com`. Он зарегистрировал домен у регистратора и теперь `example.com` принадлежит «Моему бизнесу».
>
> Но сама по себе регистрация домена не привязывает его ни к какому-то почтовому сервису, ни к хостингу с сайтом организации. Чтобы получать почту, отправляемую на `example.com`, владелец должен указать данные почтового сервиса в настройках своего домена.

Как настраивать DNS-записи

Вы можете управлять DNS-записями:

- в личном кабинете на сайте регистратора — если домен не делегирован на Яндекс; Что значит «делегирован»?
- в кабинете организации — если домен делегирован на Яндекс.

Домен не делегирован

Конкретный порядок действий зависит от того, какой именно регистратор обслуживает ваш домен. Инструкции доступны в базах знаний регистраторов:

- «Рег.ру»
- «Регистратор R01»
- Beget
- Webnames.ru («Регтайм»)
- masterhost
- Nethouse

> **DNS-записи обновляются не мгновенно**
>
> Это занимает до 72 часов.

Домен делегирован

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Общие настройки** → **Домены**.
3. В блоке нужного домена нажмите **Управлять DNS-записями**.

Как настроить записи для электронной почты

Можно просто делегировать домен на Яндекс

Настроить почтовые DNS-записи можно автоматически — для этого достаточно делегировать домен на Яндекс. Как это сделать?

Если вы уже делегировали домен, дополнительно настраивать почту вам не нужно — все необходимые DNS-записи созданы автоматически.

Для работы почты нужны три записи:

Тип	Хост	Значение	TTL
MX	@	mx.yandex.net	21600
TXT	mail._domainkey	{уникальный ключ}	21600
TXT	@	v=spf1 redirect=_spf.yandex.net	21600

Чтобы сформировать, добавить и проверить каждую из них, воспользуйтесь подробными инструкциями:

- Как создать MX-запись
- Как создать SPF-запись
- Как создать подпись DKIM

Как настроить записи для сайта

Если вы хотите, чтобы домен служил адресом сайта вашей организации, нужно создать DNS-записи типов **A** и **AAAA**.

- Как создать A-запись и AAAA-запись

Написать в службу поддержки

MX-запись

MX-запись указывает на сервер, принимающий почту для вашего домена. Чтобы вашу почту обрабатывал сервер Яндекса, нужно создать MX-запись, указывающую на этот сервер.

Если вы делегировали домен на серверы Яндекса, MX-запись будет настроена автоматически.

Добавить MX-запись

Общая инструкция по настройке MX-записи

1. Войдите в панель управления доменом (зоной DNS) на сайте компании, которая предоставляет вам DNS-хостинг.
2. Удалите существующие MX-записи.
3. Создайте новую MX-запись со следующими значениями полей (в разных панелях управления названия полей могут различаться):
   - **Значение** — `mx.yandex.net.`

     Точка в конце имени сервера обязательна, если ваша панель управления не добавляет ее по умолчанию.
   - **Приоритет** — `10`

     Если приоритет со значением `10` не предусмотрен в панели управления, укажите любой другой отличный от нуля приоритет.
   - **Имя поддомена** (или **Хост**) — `@`

     В некоторых панелях управления вместо символа `@` нужно указать имя вашего домена (например, `example.org.`). Если вам не удается указать ни `@`, ни имя домена, оставьте это поле пустым.

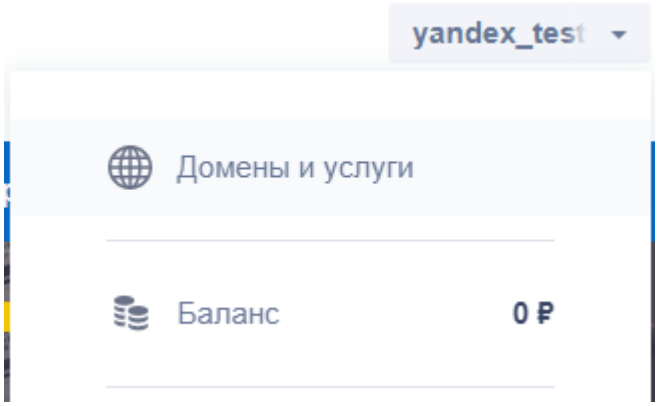
     Если это поле отсутствует в панели управления, можно его не указывать.
   - Если требуется заполнить поле **TTL**, укажите `21600`.
4. Подождите, пока изменения вступят в силу. Может потребоваться до 72 часов, чтобы DNS-серверы в интернете обменялись данными о новых DNS-записях.

   Чтобы обновить статус, в Яндекс 360 для бизнеса перейдите на страницу **Домены**, затем нажмите **Подтвердить домен** рядом с нужным доменом и нажмите кнопку **Проверить**. Статус изменится, если данные на стороне DNS-хостинга уже обновились.

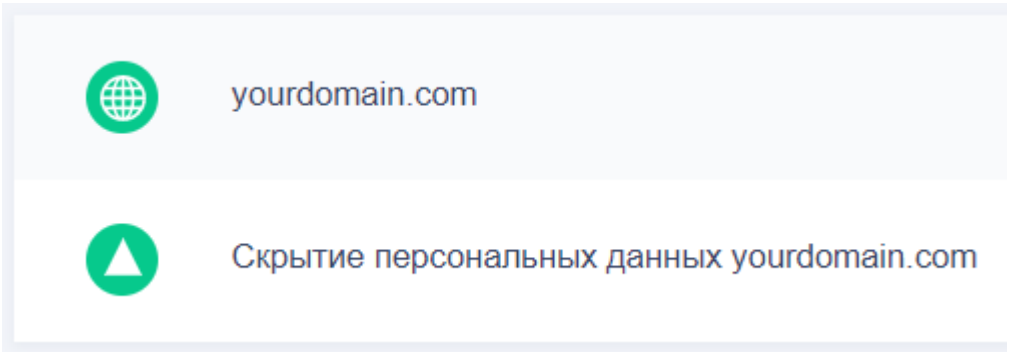
Инструкции по настройке MX-записи у некоторых хостинг-провайдеров

reg.ru

1. Откройте страницу https://www.reg.ru/ и войдите в ваш аккаунт.
2. Нажмите кнопку с вашим логином и выберите **Домены и услуги**.



3. Нажмите ссылку с именем нужного домена. Откроется страница **Управление**.



4. Выберите **DNS-серверы и управление зоной**.
5. Удалите существующие MX-записи.
6. Добавьте новую MX-запись со следующими значениями полей:
   - **Subdomain** — `@`
   - **Mail Server** — `mx.yandex.net.`
   - **Priority** — `10`

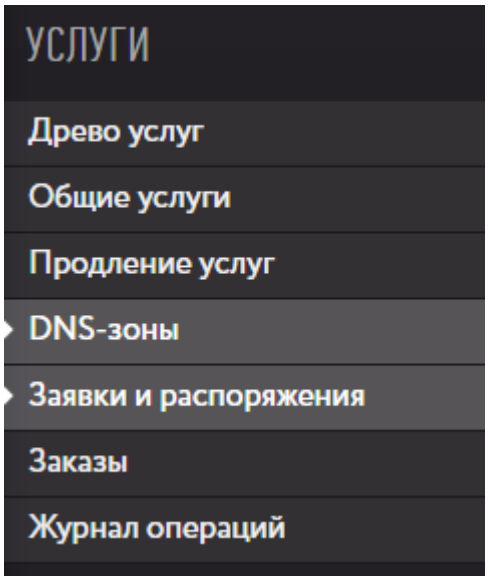
7. Подождите, пока изменения вступят в силу. Может потребоваться до 72 часов, чтобы DNS-серверы в интернете обменялись данными о новых DNS-записях.

   Чтобы обновить статус, в Яндекс 360 для бизнеса перейдите на страницу **Домены**, затем нажмите **Подтвердить домен** рядом с нужным доменом и нажмите кнопку **Проверить**. Статус изменится, если данные на стороне DNS-хостинга уже обновились.

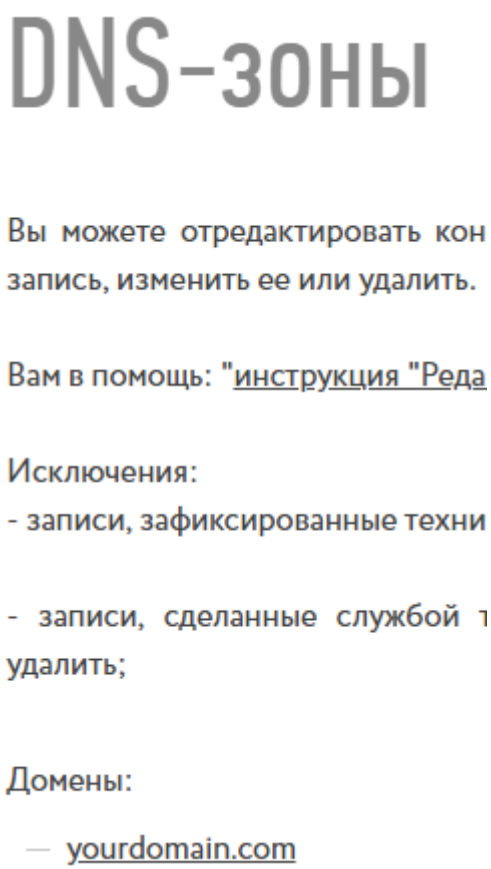
masterhost.ru

1. Откройте страницу https://cp.masterhost.ru и войдите в ваш аккаунт.

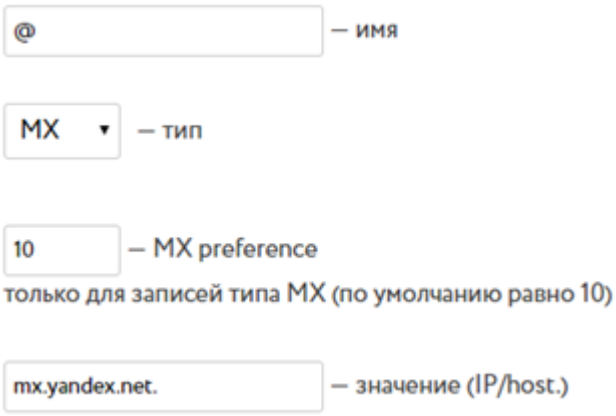
2. На панели справа выберите **DNS-зоны**.



3. Нажмите ссылку с именем нужного домена. Откроется страница **Просмотр DNS-зоны**.

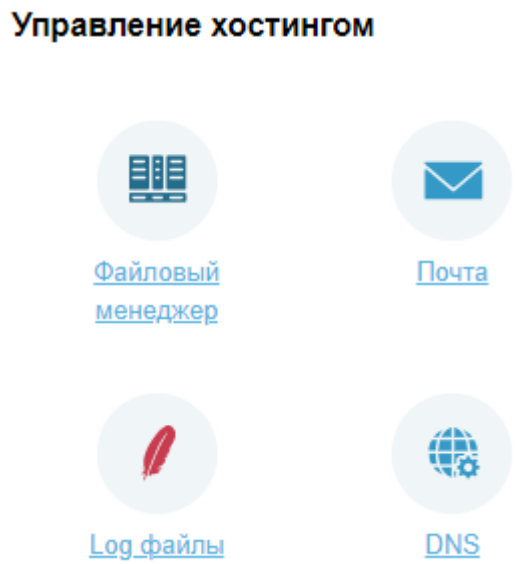


4. Добавьте новую MX-запись со следующими значениями полей:
   - **имя** — `@`
   - **тип** — `MX`
   - **MX preference** — `10`
   - **значение (IP/host.)** — `mx.yandex.net.`

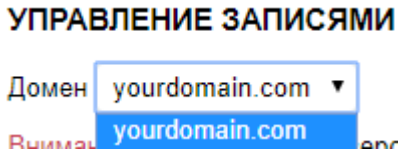


sweb.ru

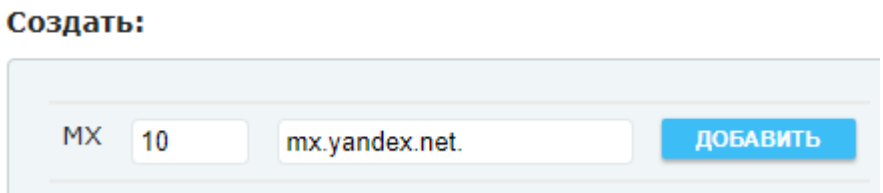
1. Откройте страницу https://mcp.sweb.ru/ и войдите в ваш аккаунт.
2. В разделе **Управление хостингом** нажмите ссылку **DNS**.



3. В выпадающем списке выберите нужный домен.



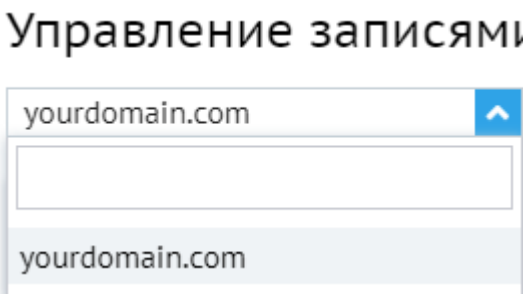
4. Добавьте новую MX-запись со следующими значениями полей:
   - Приоритет — `10`
   - Значение — `mx.yandex.net.`



beget.com

1. Откройте страницу https://cp.beget.com/ и войдите в ваш аккаунт.
2. Нажмите ссылку **DNS**.

3. В выпадающем списке выберите нужный домен.



4. В нижней части страницы найдите строку с нужным доменом и нажмите на значок . DNS-записи домена станут доступными для редактирования.
5. Добавьте новую MX-запись со следующими значениями полей:
   - **preference** — `10`
   - **exchange** — `mx.yandex.net.`

Собственные инструкции провайдеров по настройке DNS-записей:

- Timeweb
- NetAngels
- 1Gb.ru
- Hostinger
- RedDock

Проверить, правильно ли настроена MX-запись

Чтобы избежать проблем с отправкой или получением почты, проверьте правильность настройки DNS-записей. Это можно сделать, например, с помощью сервиса https://www.digwebinterface.com или другой dig-утилиты.

1. Откройте страницу https://www.digwebinterface.com.
2. В поле **Hostnames or IP addresses** укажите имя вашего домена, например `example.org`.
3. В поле **Type** выберите **MX** и нажмите кнопку **Dig**.

Ответ должен иметь вид:

```
example.org.  20755 IN MX 10 mx.yandex.net.
```

Если сервер не отвечает на запрос, ответ не совпадает с нужным или в ответе присутствуют лишние записи, значит, MX-запись настроена некорректно. Настройте ее по инструкции.

Внимание

Прежде чем повторно проверять DNS-записи, подождите 72 часа. За это время DNS-серверы в интернете обновят данные о записях.

Написать в службу поддержки

SPF-запись

SPF-запись помогает снизить риск того, что письмо, отправленное с адреса на вашем домене, попадет в спам у адресата. Чтобы настроить SPF-запись, нужно создать TXT-запись со списком серверов, которые отвечают за отправку почты с вашего домена.

Если вы делегировали домен на серверы Яндекса, SPF-запись будет настроена автоматически.

Общая инструкция по настройке SPF-записи

1. Войдите в панель управления доменом (зоной DNS) на сайте компании, которая предоставляет вам DNS-хостинг.
2. SPF-запись помогает снизить риск того, что письмо, отправленное с адреса на вашем домене, попадет в спам у адресата. Чтобы настроить SPF-запись, нужно создать TXT-запись со списком серверов, которые отвечают за отправку почты с вашего домена.
   - **Значение** — `v=spf1 redirect=_spf.yandex.net`

     Если вы хотите отправлять письма не только с серверов Яндекса, укажите дополнительные серверы в таком формате:

     ```
     v=spf1 ip4:IP-1 ip4:IP-2 ip4:IP-3 include:_spf.yandex.net ~all
     ```

     Где `IP-1`, `IP-2`, `IP-3` — IP-адреса дополнительных серверов.
   - **Имя поддомена** (или **Хост**) — `@`

     В некоторых панелях управления вместо символа `@` нужно указать имя вашего домена (например, `example.org.`). Если вам не удается указать ни `@`, ни имя домена, оставьте это поле пустым.

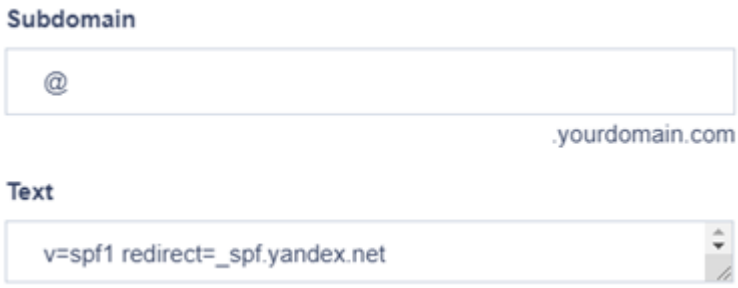
     Если это поле отсутствует в панели управления, можно его не указывать.
   - Если требуется заполнить поле **TTL**, укажите `21600`.
3. Подождите, пока изменения вступят в силу. Может потребоваться до 72 часов, чтобы DNS-серверы в интернете обменялись данными о новых DNS-записях.

   Чтобы обновить статус, в Яндекс 360 для бизнеса перейдите на страницу **Домены**, затем нажмите **Подтвердить домен** рядом с нужным доменом и нажмите кнопку **Проверить**. Статус изменится, если данные на стороне DNS-хостинга уже обновились.

Инструкции по настройке SPF-записи у некоторых хостинг-провайдеров

reg.ru

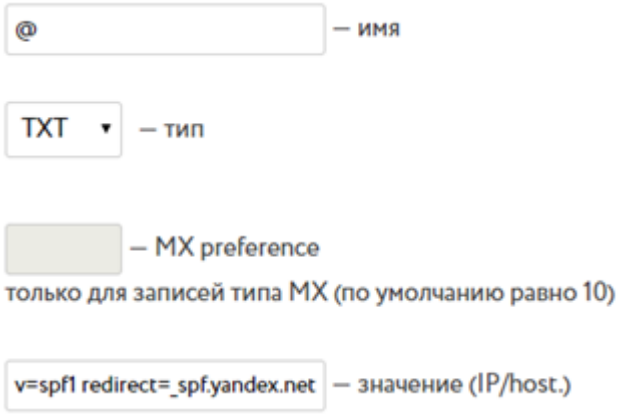
1. Добавьте новую TXT-запись со следующими значениями полей:
   - **Subdomain** — `@`
   - **Text** — `v=spf1 redirect=_spf.yandex.net`



masterhost.ru

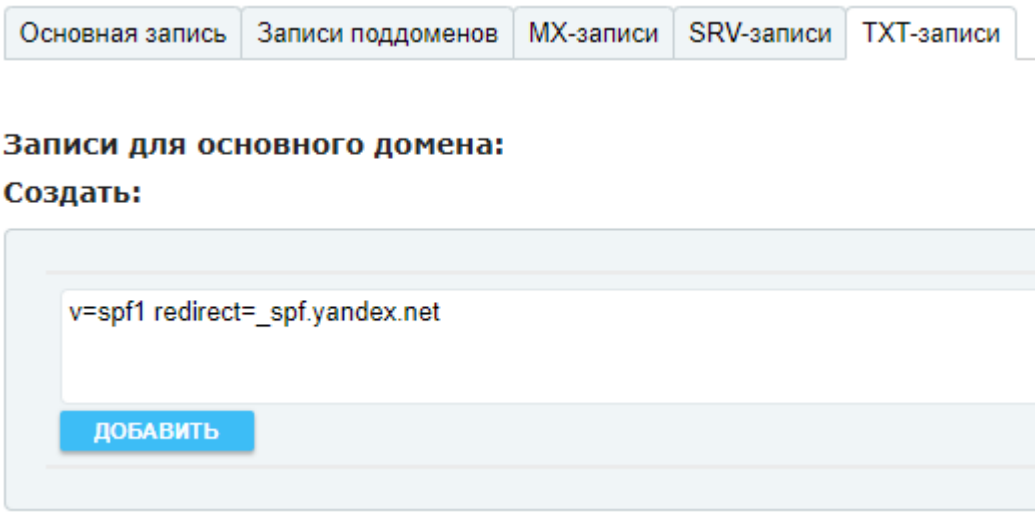
1. Добавьте новую TXT-запись со следующими значениями полей:
   - **имя** — `@`
   - **тип** — `TXT`
   - **значение (IP/host.)** — `v=spf1 redirect=_spf.yandex.net`

   Поле **MX preference** оставьте пустым.



sweb.ru

1. В разделе **Записи для основного домена** добавьте новую TXT-запись. В поле укажите `v=spf1 redirect=_spf.yandex.net`.

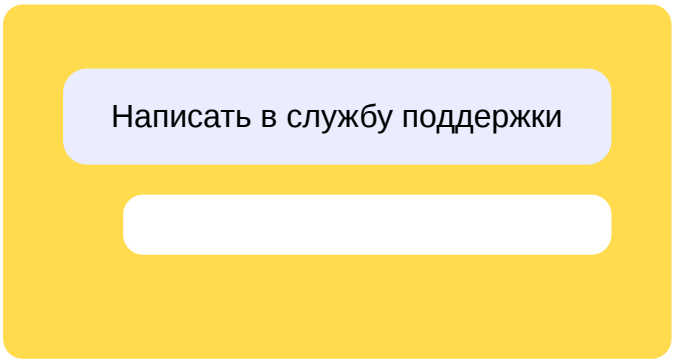


beget.com

1. Добавьте новую TXT-запись, в поле **txt data** укажите `v=spf1 redirect=_spf.yandex.net`.

Собственные инструкции провайдеров по настройке DNS-записей:

- Timeweb
- Hostinger
- RedDock



DKIM-подпись

Если вы делегировали домен на серверы Яндекса, DKIM-подпись с публичным ключом будет настроена автоматически.

Общая инструкция по настройке DKIM-подписи

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Домены**.
3. Рядом с именем домена, для которого вы хотите добавить подпись, нажмите **Настроить DKIM**.

   Если нужного домена нет в списке, убедитесь, что он подключен и подтвержден.
4. В блоке **Настройка DKIM-подписи** скопируйте значение публичного ключа для вашего домена.
5. Войдите в панель управления доменом (зоной DNS) на сайте компании, которая предоставляет вам DNS-хостинг.
6. Создайте TXT-запись со следующими значениями полей (в разных панелях управления названия полей могут различаться):
   - **Имя поддомена** (или **Хост**) — `mail._domainkey`. В некоторых панелях управления DNS для публичного ключа DKIM необходимо также указывать домен, например `mail._domainkey.yourdomain.tld`.
   - Значение — текст публичного ключа, который вы скопировали из блока **Настройка DKIM-подписи** в настройках домена.

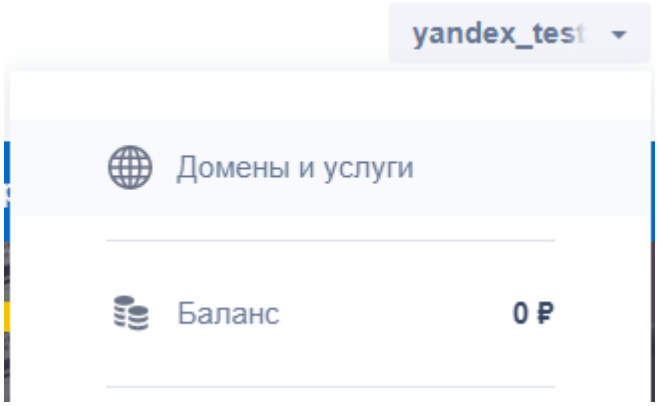
     Например, `v=DKIM1; k=rsa; t=s; p=MIGfMA0GCSEBtaCOteH4EBqJlKpe...`
   - Если требуется заполнить поле **TTL**, укажите `21600`.
7. Подождите, пока изменения вступят в силу. Может потребоваться до 72 часов, чтобы DNS-серверы в интернете обменялись данными о новых DNS-записях.

   Чтобы обновить статус, в Яндекс 360 для бизнеса перейдите на страницу **Домены**, затем нажмите **Подтвердить домен** рядом с нужным доменом и нажмите кнопку **Проверить**. Статус изменится, если данные на стороне DNS-хостинга уже обновились.

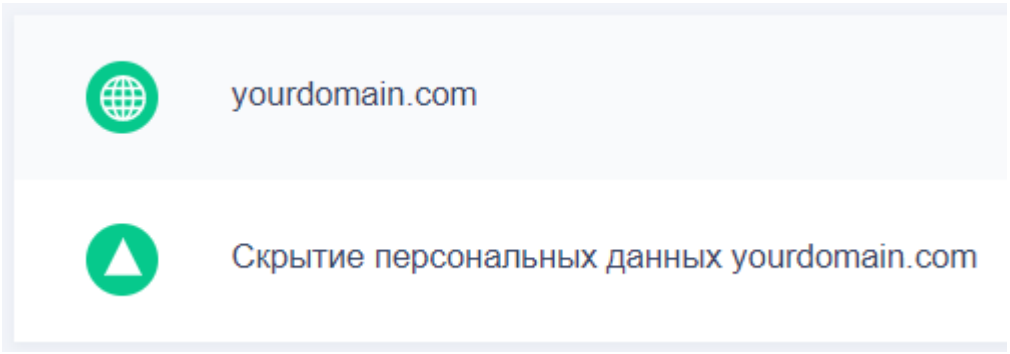
Инструкции по настройке DKIM-подписи у некоторых хостинг-провайдеров

reg.ru

1. Перейдите на страницу настройки домена в Почте для бизнеса и скопируйте значение публичного ключа для вашего домена (см. в общей инструкции по настройке DKIM-подписи).
2. Откройте страницу https://www.reg.ru/ и войдите в ваш аккаунт.
3. Нажмите кнопку с вашим логином и выберите **Домены и услуги**.

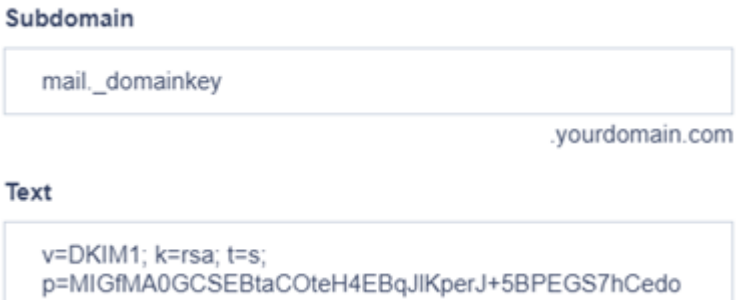


4. Нажмите ссылку с именем нужного домена. Откроется страница **Управление**.



5. Выберите **DNS-серверы и управление зоной**.
6. Добавьте новую TXT-запись со следующими значениями полей:
   - **Subdomain** — `mail._domainkey`
   - **Text** — значение публичного ключа, полученное на странице настройки домена в Почте для бизнеса.

   Например, `v=DKIM1; k=rsa; t=s; p=MIGfMA0GCSEBtaCOteH4EBqJlKpe...`



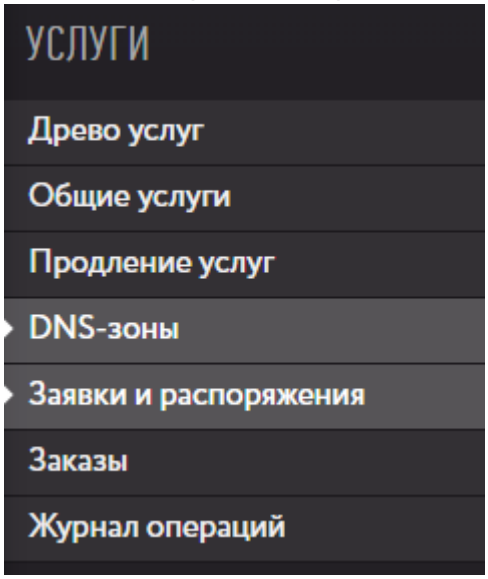
7. Подождите, пока изменения вступят в силу. Может потребоваться до 72 часов, чтобы DNS-серверы в интернете обменялись данными о новых DNS-записях.

   Чтобы обновить статус, в Яндекс 360 для бизнеса перейдите на страницу **Домены**, затем нажмите **Подтвердить домен** рядом с нужным доменом и нажмите кнопку **Проверить**. Статус изменится, если данные на стороне DNS-хостинга уже обновились.

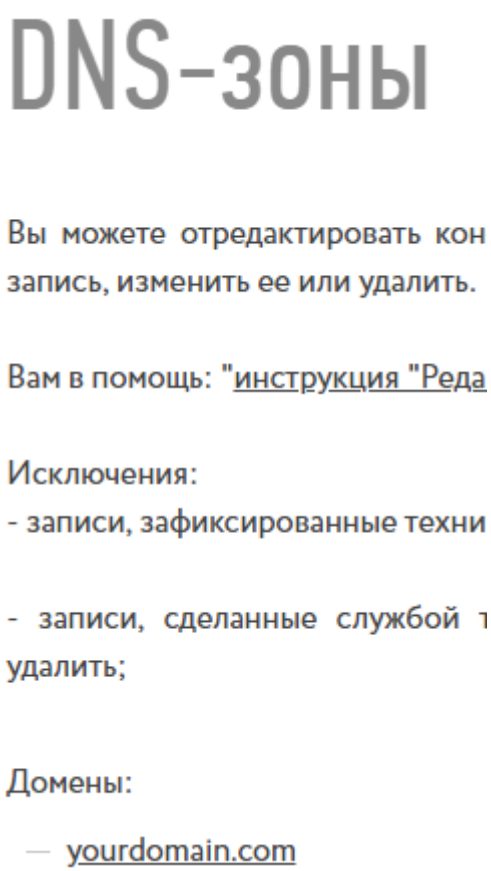
masterhost.ru

1. Перейдите на страницу настройки домена в Почте для бизнеса и скопируйте значение публичного ключа для вашего домена (см. в общей инструкции по настройке DKIM-подписи).
2. Откройте страницу https://cp.masterhost.ru и войдите в ваш аккаунт.

3. На панели справа выберите **DNS-зоны**.



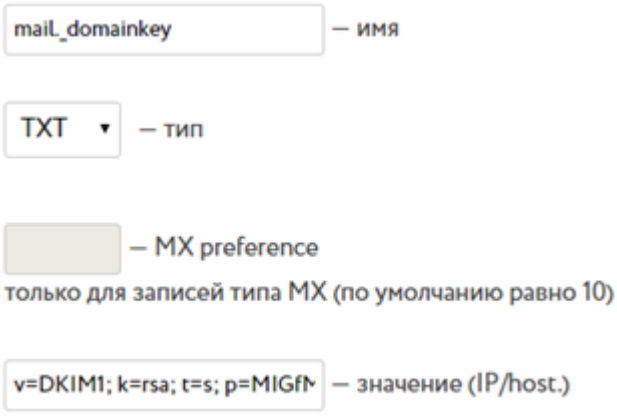
4. Нажмите ссылку с именем нужного домена. Откроется страница **Просмотр DNS-зоны**.



5. Добавьте новую TXT-запись со следующими значениями полей:
   - **имя** — `mail._domainkey`
   - **тип** — `TXT`
   - **значение (IP/host.)** — значение публичного ключа, полученное на странице настройки домена в Почте для бизнеса.

   Например, `v=DKIM1; k=rsa; t=s; p=MIGfMA0GCSEBtaCOteH4EBqJlKpe...`

   Поле **MX preference** оставьте пустым.

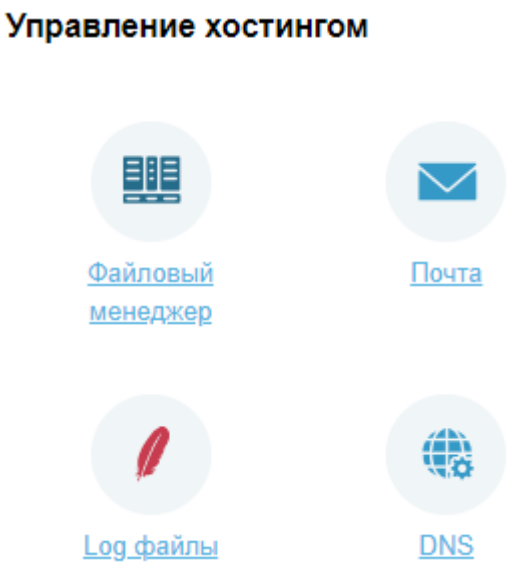


6. Подождите, пока изменения вступят в силу. Может потребоваться до 72 часов, чтобы DNS-серверы в интернете обменялись данными о новых DNS-записях.

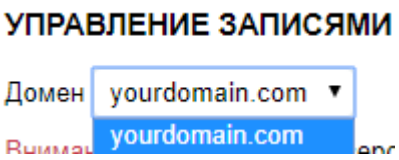
   Чтобы обновить статус, в Яндекс 360 для бизнеса перейдите на страницу **Домены**, затем нажмите **Подтвердить домен** рядом с нужным доменом и нажмите кнопку **Проверить**. Статус изменится, если данные на стороне DNS-хостинга уже обновились.

sweb.ru

1. Перейдите на страницу настройки домена в Почте для бизнеса и скопируйте значение публичного ключа для вашего домена (см. в общей инструкции по настройке DKIM-подписи).
2. Откройте страницу https://mcp.sweb.ru/ и войдите в ваш аккаунт.
3. В разделе **Управление хостингом** нажмите ссылку **DNS**.



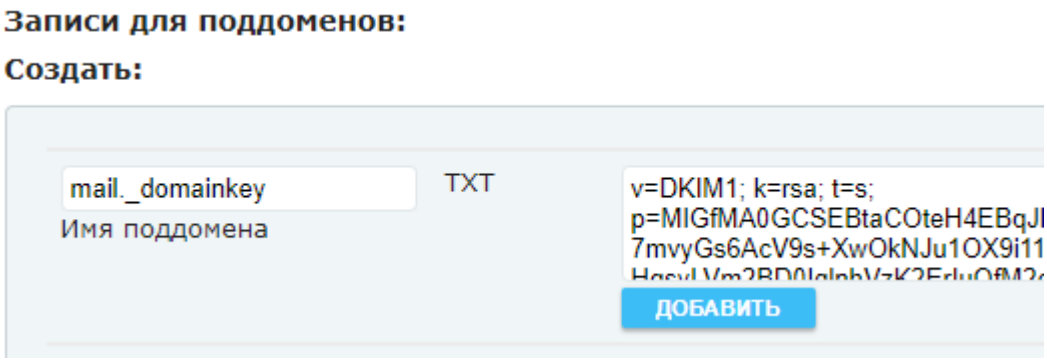
4. В выпадающем списке выберите нужный домен.



5. Добавьте новую TXT-запись в разделе **Записи для поддоменов** со следующими значениями полей:
   - **Имя поддомена** — `mail._domainkey`

- **TXT** — значение публичного ключа, полученное на странице настройки домена в Почте для бизнеса.

Например, `v=DKIM1; k=rsa; t=s; p=MIGfMA0GCSEBtaCOteH4EBqJlKpe...`



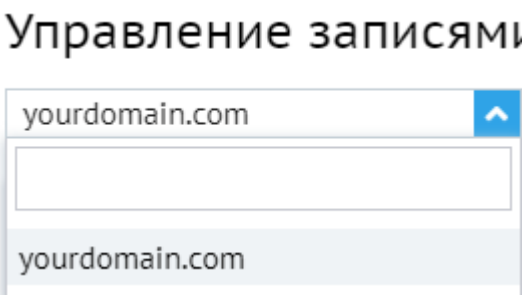
6. Подождите, пока изменения вступят в силу. Может потребоваться до 72 часов, чтобы DNS-серверы в интернете обменялись данными о новых DNS-записях.

   Чтобы обновить статус, в Яндекс 360 для бизнеса перейдите на страницу **Домены**, затем нажмите **Подтвердить домен** рядом с нужным доменом и нажмите кнопку **Проверить**. Статус изменится, если данные на стороне DNS-хостинга уже обновились.

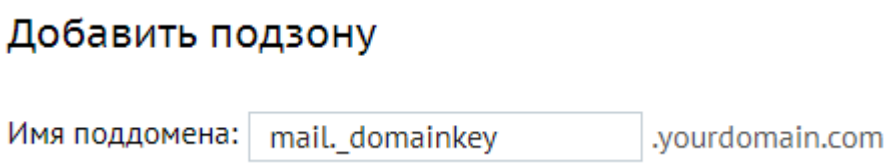
beget.com

1. Перейдите на страницу настройки домена в Почте для бизнеса и скопируйте значение публичного ключа для вашего домена (см. в общей инструкции по настройке DKIM-подписи).
2. Откройте страницу https://cp.beget.com/ и войдите в ваш аккаунт.
3. Нажмите ссылку **DNS**.

4. В выпадающем списке выберите нужный домен.



5. Нажмите ссылку **Добавить подзону**. Откроется дополнительное окно.
6. Добавьте поддомен с именем `mail._domainkey`. Появится сообщение об успешном создании поддомена.



7. В нижней части страницы найдите строку с добавленным поддоменом и нажмите на значок . DNS-записи поддомена станут доступными для редактирования.
8. Удалите A-запись, добавленную по умолчанию.
9. Добавьте новую TXT-запись, в поле **txt data** которой укажите значение публичного ключа, полученное на странице настройки домена в Почте для бизнеса.

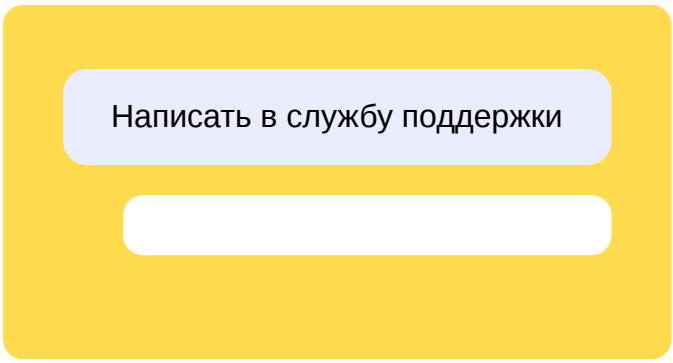
   Например, `v=DKIM1; k=rsa; t=s; p=MIGfMA0GCSEBtaCOteH4EBqJlKpe...`

10. Подождите, пока изменения вступят в силу. Может потребоваться до 72 часов, чтобы DNS-серверы в интернете обменялись данными о новых DNS-записях.

    Чтобы обновить статус, в Яндекс 360 для бизнеса перейдите на страницу **Домены**, затем нажмите **Подтвердить домен** рядом с нужным доменом и нажмите кнопку **Проверить**. Статус изменится, если данные на стороне DNS-хостинга уже обновились.

Собственные инструкции провайдеров по настройке DNS-записей:

- Timeweb
- Hostinger
- RedDock



A-запись

Чтобы по адресу вашего домена открывался сайт, настройте для домена A-запись и (или) AAAA-запись.

A-запись указывает IP-адрес сервера, на котором расположен ваш сайт, в формате IPv4. AAAA-запись служит для той же цели, но содержит адрес сервера в формате IPv6.

Если вы делегировали домен на серверы Яндекса, A-запись и AAAA-запись должны быть настроены в Яндекс 360 для бизнеса. При подключении домена к организации существующие DNS-записи автоматически копируются на страницу домена в Яндекс 360 для бизнеса. Если этого не произошло или если вы хотите добавить новый сайт, создайте A-запись и AAAA-запись в DNS-редакторе Яндекс 360 для бизнеса.

Настройка A-записи и AAAA-записи

1. Под аккаунтом администратора организации перейдите на страницу **Домены**.
2. Создайте A-запись и задайте значения полей:
   - **Тип** — A.
   - **Хост**:
     - Чтобы указать IP-адрес сайта для основного домена (например, `example.org`), введите символ `@`.
     - Чтобы указать IP-адрес сайта для поддомена, введите часть имени поддомена, которая отделена от имени основного домена точкой. Например, для поддомена `sub.example.org` укажите `sub`.
   - В поле **Адрес IPv4/IPv6** укажите IP-адрес сервера, на котором находится сайт. Например, `203.0.113.45`.
   - **TTL** — `21600`.
3. Если у сайта несколько IP-адресов, создайте такие же A-записи для каждого IP-адреса.
4. Чтобы создать AAAA-запись, выполните такие же шаги, как для создания A-записи. В качестве значения AAAA-записи указывайте IP-адрес сервера в формате IPv6, например `2a02:4b7:b070:7310::1:8`.
5. Подождите, пока изменения вступят в силу. Может потребоваться до 72 часов, чтобы DNS-серверы в интернете обменялись данными о новых DNS-записях.

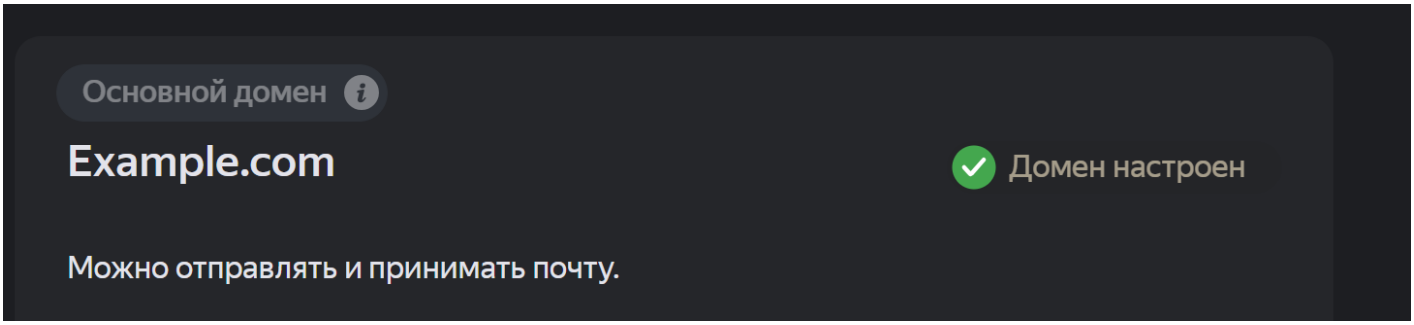
   Чтобы обновить статус, в Яндекс 360 для бизнеса перейдите на страницу **Домены**, затем нажмите **Подтвердить домен** рядом с нужным доменом и нажмите кнопку **Проверить**. Статус изменится, если данные на стороне DNS-хостинга уже обновились.

Написать в службу поддержки

Как убедиться, что домен подключен

После того как вы настроили или делегировали домен, убедитесь в том, что он успешно подключен к вашей организации.

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Общие настройки** → **Домены**.
3. Посмотрите статус домена. Если все в порядке, вы увидите надпись «Домен настроен».



Написать в службу поддержки

Домены-алиасы (синонимы)

К одной организации в Яндекс 360 можно подключить несколько доменов — один из них будет **основным**, а остальные — **алиасами** (синонимами).

Например, после ребрендинга в качестве алиаса можно добавить прежний домен организации, чтобы не терять почту от старых клиентов.

Вся почта, отправленная на домен-алиас, будет попадать в соответствующие почтовые ящики сотрудников. В свою очередь, сотрудник может выбрать, с какого адреса отправить то или иное письмо.

Как добавить алиас

Процесс добавления алиаса не отличается от добавления первого домена:

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Общие настройки** → **Домены**.
3. Впишите имя домена и нажмите **Добавить домен**.
4. Настройте и подтвердите домен или делегируйте его. Что это значит?

Чем алиас отличается от основного домена

- По умолчанию электронная почта отправляется с основного домена.
- Основной домен используется в интерфейсе кабинета организации и сервисов Яндекс 360 — например, при создании аккаунта сотрудника или в окне создания встречи.
- Основной домен нельзя удалить, то есть отключить от организации.

Как заменить основной домен организации

1. Подключите новый домен как алиас.
2. Нажмите ⋮ в блоке этого домена и выберите **Сделать основным**.

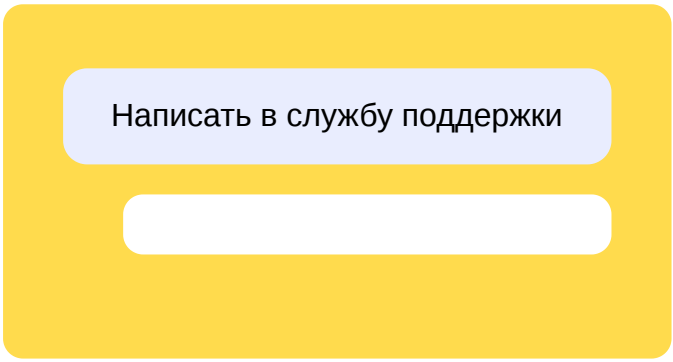
После этого старый домен можно будет либо отключить от организации, либо оставить в качестве алиаса.

Что произойдет после смены домена с почтовыми ящиками сотрудников и адресами переговорок:

- Почтовые ящики сотрудников вашей организации будут перенесены на новый основной домен. Все данные в почтовых ящиках сохранятся.
- Старый домен в почтовых адресах переговорок поменяется на новый основной домен. Например, вы решили изменить домен `company1.ru` на `company2.ru`. Почтовый адрес `meeting-room@company1.ru` для переговорки «Meeting room» изменится на `meeting-room@company2.ru`. Старый адрес переговорки во встречах тоже поменяется на новый.

Примечание

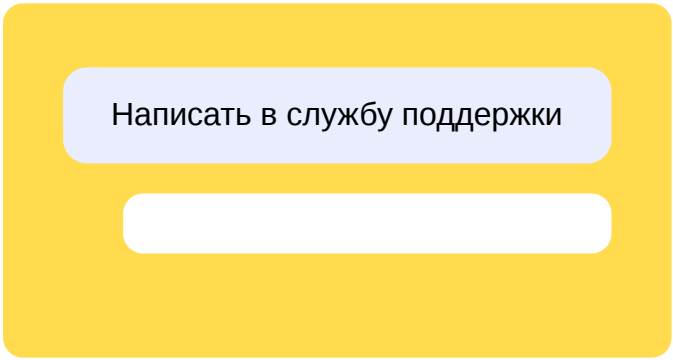
Если после смены домена внешний участник отредактирует встречу, бронирование переговорки с новым адресом отменится. Это не произойдет, если встречу отредактирует сотрудник организации.



Как заменить домен в организации

Чтобы заменить домен, вначале нужно подключить новый домен, а затем отключить старый.

1. Добавьте новый домен в качестве алиаса по инструкции.
2. Сделайте новый домен основным. Как это сделать
3. Удалите прежний домен. Как это сделать



Как отключить домен от организации

Если нужно удалить алиас

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Общие настройки** → **Домены**.
3. В блоке с нужным доменом нажмите кнопку ⋮, а затем — **Удалить**.
4. Подтвердите удаление.

Если нужно удалить основной домен

Чтобы домен можно было отключить от организации, он должен перестать быть **основным доменом**. Для этого нужен домен-алиас.

К организации подключены другие домены

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Общие настройки** → **Домены**.
3. Выберите среди алиасов домен, который станет основным.
4. В блоке с этим доменом нажмите кнопку ⋮, а затем — **Сделать основным**.

После этого бывший основной домен станет алиасом, и его можно будет удалить.

Основной домен — единственный

Вначале подключите к организации домен-алиас. Как это сделать

Что делать, если никаких других доменов нет, а освободить основной нужно

> В таком случае освободить домен можно через удаление организации. Как удалить организацию

После того как домен будет добавлен:

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Общие настройки** → **Домены**.
3. Выберите добавленный домен-алиас.
4. В блоке с этим доменом нажмите кнопку ⋮, а затем — **Сделать основным**.

После этого бывший основной домен станет алиасом, и его можно будет удалить.

Написать в службу поддержки

Администраторы

Администраторы — это сотрудники, у которых есть права на управление настройками организации в Яндекс 360 для бизнеса. В частности, администраторы могут:

- добавлять и удалять других администраторов;
- выполнять различные действия с аккаунтами сотрудников;
- выстраивать структуру организации, в частности создавать подразделения, добавлять в них сотрудников и назначать руководителей;
- объединять сотрудников в группы, например для работы над крупной задачей или с одним заказчиком;
- назначать сотрудников на роли менеджеров;
- увеличивать место на Диске отдельным сотрудникам;
- становиться плательщиками — пополнять баланс организации в Яндекс 360 для бизнеса с банковской карты.

По умолчанию владелец организации становится ее главным администратором. Владельца организации нельзя удалить, но можно изменить.

Добавить

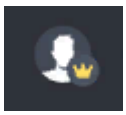
Вы можете выдать права администратора любому сотруднику вашей организации:

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выделите сотрудника и нажмите → **Сделать администратором**.

Просмотреть

Чтобы узнать, кто может управлять настройками организации:

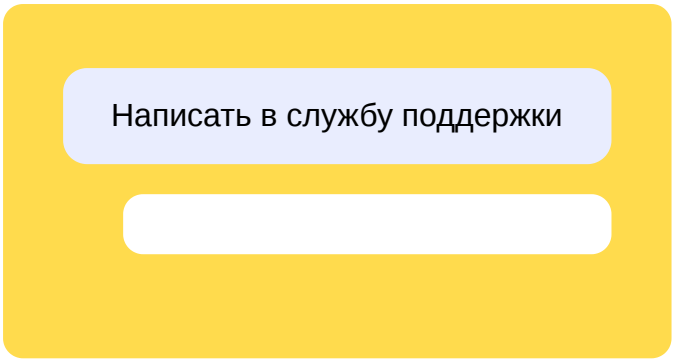
1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. В строке пользователей с правами администратора отображается значение **Администратор**, а их портреты отмечены специальным значком:



Удалить

Вы можете отозвать права любого администратора, кроме владельца организации:

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выделите сотрудника и нажмите → **Отозвать права администратора**.


Написать в службу поддержки

Менеджеры

Менеджер — это роль сотрудника, которая дает ему возможность управлять отдельной группой настроек в Яндекс 360 для бизнеса.

Администратор может назначить сотрудников на следующие роли:

- Менеджер правил для писем — может настраивать правила, по которым Почта автоматически обрабатывает входящие письма. Узнать о настройке правил
- Менеджер архива писем — имеет доступ к архиву писем, который содержит письма сотрудников организации.
- Менеджер федераций — может отправлять и принимать запросы на связь с другими организациям.
- - Менеджер аудит-логов — может просматривать события в аудит-логах сервисов Яндекс 360 для бизнеса. Как просматривать логи
- Менеджер оплаты и тарифов — может управлять тарифом, оплачивать услуги Яндекс 360 для бизнеса и менять реквизиты организации. Перейти в Справку по тарифам и оплате.
- Менеджер пользователей — может выполнять различные действия с аккаунтами сотрудников: добавлять, редактировать, блокировать, удалять, объединять в подразделения и группы. Но менеджер пользователей не может сбрасывать пароли сотрудников и удалить аккаунт владельца организации.
- Менеджер безопасности — может просмотреть, с каких устройств сотрудники организации вошли в сервисы Яндекс 360 для бизнеса, самостоятельно выйти из аккаунта сотрудника на любом устройстве или завершить все сессии сотрудника. Как управлять авторизацией на устройствах сотрудников

Один сотрудник может совмещать несколько ролей менеджера. На одну роль может быть назначено несколько сотрудников.

Назначить на роль менеджера

Назначить на одну роль

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Роли и доступы**.
3. Наведите указатель на роль, на которую хотите назначить сотрудников, и нажмите **Назначить** справа от ее описания. Или выберите роль и нажмите **Назначить** на открывшейся странице роли.
4. Начните писать имя или фамилию в поле для поиска и выберите сотрудника из выпадающего списка. Вы можете выбрать несколько человек, которых хотите назначить на роль.
5. Нажмите **Назначить**. Выбранные сотрудники отобразятся в списке на странице роли и у них появится доступ к соответствующим настройкам.

Назначить на одну или сразу несколько ролей

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Роли и доступы**.
3. Нажмите **Назначить** вверху страницы.
4. Заполните поля в окне назначения на роли:

- выберите из списка нужные роли;
- выберите сотрудников: для каждого сотрудника начните писать имя или фамилию в поле для поиска и выберите нужный вариант из выпадающего списка.

5. Нажмите **Назначить**. Выбранные сотрудники отобразятся в списке на странице роли и у них появится доступ к соответствующим настройкам.

Просмотреть роли сотрудника

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите сотрудника, чтобы просмотреть информацию о нем. Все назначенные роли будут указаны в разделе **Роль**.

Отозвать роль

Отозвать роль у одного сотрудника

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Роли и доступы**.
3. Выберите роль, которую хотите отозвать у сотрудника.
4. В списке сотрудников на странице роли найдите того, у которого хотите отозвать роль. Можно воспользоваться полем поиска в правой верхней части окна — начните писать имя или фамилию и в списке останутся только те сотрудники, которые удовлетворяют условиям поиска.
5. Наведите указатель на сотрудника, нажмите значок ⋮ в правой части строки и выберите **Отозвать роль**.
6. Подтвердите отзыв роли.

Отозвать роль сразу у нескольких сотрудников

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Роли и доступы**.
3. Выберите роль, которую хотите отозвать у сотрудников.
4. В списке сотрудников на странице роли отметьте тех, у которых хотите отозвать роль.
5. Нажмите **Отозвать роль** вверху страницы.
6. Проверьте список сотрудников и подтвердите отзыв роли.

Написать в службу поддержки

Сотрудники

При работе в Яндекс 360 для бизнеса вы можете выполнять различные действия с аккаунтами сотрудников: добавлять новые и удалять те, что больше не нужны, выполнять поиск по данным сотрудников и просматривать их карточки, а также редактировать и блокировать аккаунты, зарегистрированные на почтовом домене вашей организации.

Добавить

Чтобы начать совместную работу в Яндекс 360 для бизнеса, добавьте сотрудников в вашу организацию. Для этого можно воспользоваться одним из способов.

Создать аккаунты вручную

Если к вашей организации подключен домен, в разделе **Пользователи** → **Сотрудники** вы можете быстро добавить новые аккаунты. В этом случае аккаунты создаются на вашем домене.

В таких доменных аккаунтах вы сможете:

- менять данные сотрудника, например удалять или добавлять почтовые алиасы;
- импортировать письма из почтовых ящиков ваших сотрудников на других серверах;
- перемещать отделы внутри организации.

Подробнее о том, как создать доменный аккаунт вручную, см. в разделе Создать аккаунт.

После создания аккаунтов на домене организации настроить единый вход (SSO) не получится.

Пригласить сотрудников

Вы можете пригласить пользователей присоединиться к вашей организации с личными аккаунтами на Яндексе. При этом вам не нужно подключать почтовый домен. Аккаунты приглашенных сотрудников нельзя редактировать и блокировать, но можно просматривать и удалять. Подробнее о том, как пригласить сотрудников в организацию, см. в разделе Пригласить пользователей.

Загрузить список сотрудников

Вы можете скачать шаблон CSV-файла, заполнить данные сотрудников и загрузить его. Такой способ подойдет, если нужно добавить большое количество аккаунтов. Подробнее о том, как это сделать, см. в разделе Загрузить список.

Подключить единый вход (SSO)

С помощью технологии единого входа на базе SAML 2.0 вы можете организовать вход в сервисы Яндекс 360 через вашу систему управления доступом (например, Active Directory или Keycloak). Так сотрудникам не придется запоминать новые логин и пароль, а вам — заводить для них отдельные аккаунты в Яндекс 360 для бизнеса. Для подключения единого входа (SSO) нужно, чтобы в организации не было доменных аккаунтов сотрудников.

Найти

В разделе **Пользователи** → **Сотрудники** имеется строка поиска, с помощью которой можно быстро находить сотрудников. Просто введите имя, фамилию или электронную почту нужного вам человека.

Выберите сотрудника в списке, чтобы открыть его карточку. В ней отображаются:

- контактные и персональные данные сотрудника;
- подразделения и группы, в которых он состоит;
- размер свободного места на его Диске. В карточке сотрудника вы можете подключить дополнения к тарифу.

Изменить

Чтобы изменить аккаунт пользователя на вашем домене:

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Наведите указатель на сотрудника, нажмите значок и выберите действие:
   - **Редактировать** — редактировать данные сотрудника, кроме логина.
   - **Изменить пароль** — задать для сотрудника новый пароль. В этом случае сотруднику потребуется заново войти в аккаунт на всех устройствах и принять условия использования сервисов Яндекса.

> **Примечание**
>
> После смены пароля в аккаунте Яндекс ID пользователя сбросятся настройки:
>
> - контрольный вопрос;
> - номер телефона;
> - вход по паролю и одноразовому паролю.

Некоторые данные пользователей с доменной почтой, например публичное имя сотрудника, можно изменять только через API.

Удалить

> **Внимание**
>
> Если вы удалите аккаунт, созданный на вашем домене, сотрудник потеряет все данные на Яндекс Диске и в Яндекс Почте. Восстановить данные будет невозможно. Если вы удалите приглашенного сотрудника с аккаунтом на Яндексе, пользователь потеряет доступ к организации. Если сотрудник был добавлен в подразделения и группы, он удалится из них.

Чтобы удалить сотрудника организации:

1. Войдите в аккаунт администратора организации.

2. Перейдите на страницу **Сотрудники**.
3. Выделите сотрудника, нажмите значок ⋮ и выберите **Удалить**.

Заблокировать или разблокировать

Администратор может заблокировать доступ к сервисам для определённого сотрудника, например, если его данные попали к злоумышленникам. Заблокированный сотрудник не сможет пользоваться Почтой и другими сервисами, подключенными к организации, но вся информация о его аккаунте сохранится. После разблокировки сотрудник сможет продолжить работу.

Внимание

Некоторые функции Почты продолжат работать даже после блокировки. Что продолжит работать

Чтобы заблокировать или разблокировать сотрудника:

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Наведите указатель на пользователя, нажмите значок ⋮ и выберите **Заблокировать** или **Разблокировать**.

Также можно удалить сотрудника из подразделения и группы, если он был туда добавлен.

Работа Почты после блокировки

Правила пересылки писем и доступа для делегатов продолжат работать в Почте сотрудника даже после его блокировки.

Чтобы отключить пересылку, войдите в почтовый ящик пользователя или воспользуйтесь API. Как отключить пересылку через API

Чтобы отключить доступ для делегатов, используйте API. Как отключить делегирование через API

Написать в службу поддержки

Создать аккаунт

Ограничение

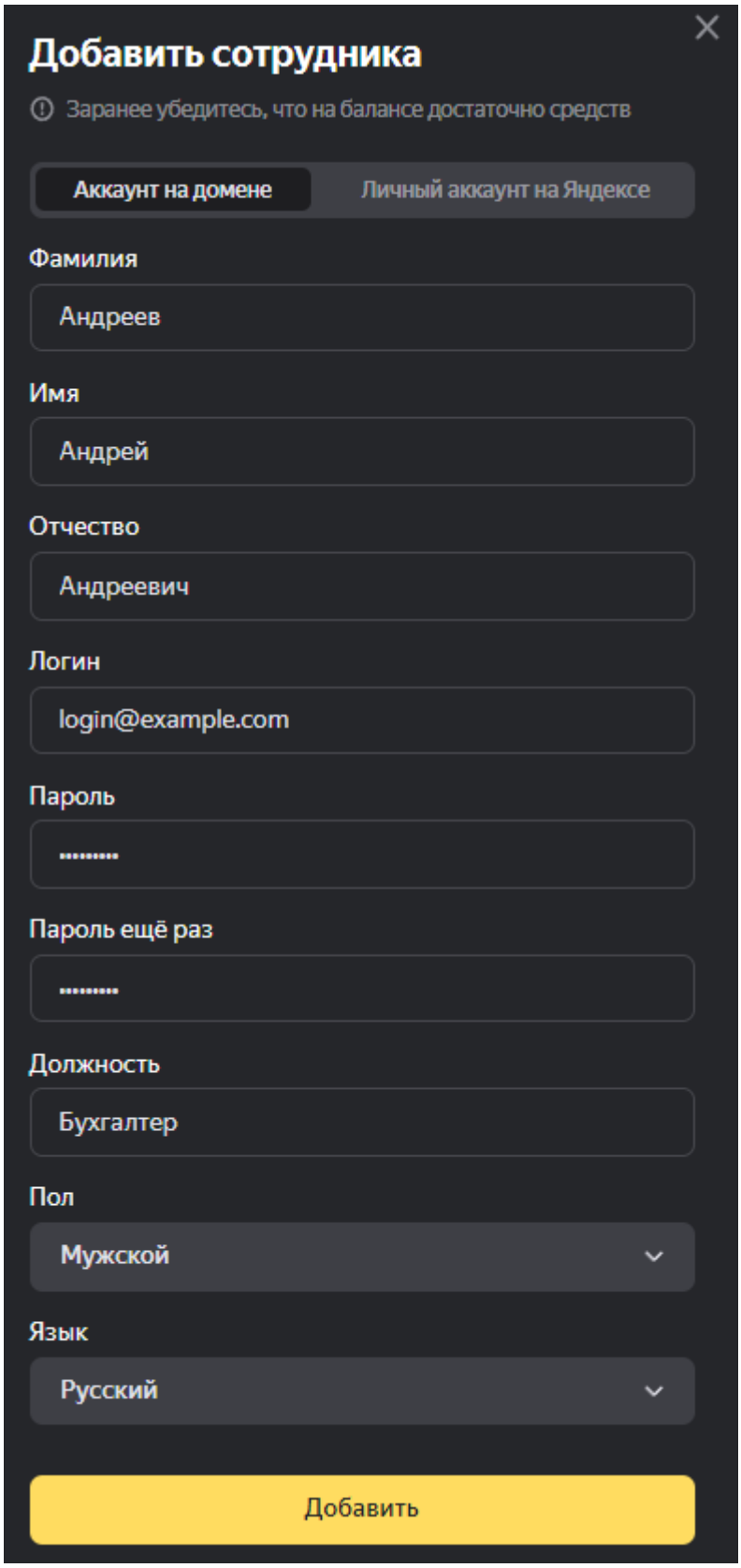
Вы можете создавать аккаунты пользователей, только если к организации подключен домен и у вас на балансе достаточно средств для оплаты тарифа с учетом новых пользователей.

После создания аккаунтов на домене организации настроить единый вход не получится.

Чтобы сотрудники вашей компании могли использовать сервисы Яндекс 360 для бизнеса, создайте для них аккаунты в организации.

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Нажмите кнопку **Добавить сотрудника**.
4. В окне **Добавить сотрудника** введите данные сотрудника.

   Пример

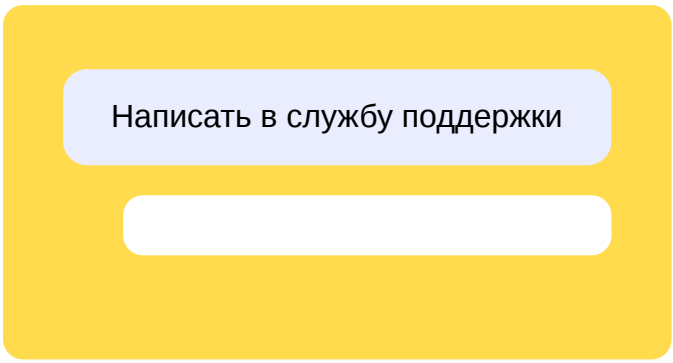


Значение поля **Логин** станет почтовым адресом сотрудника на вашем домене, например `login@example.com`.

При добавлении сотрудника вы можете указать для него подразделение и группу — и тогда он автоматически появится в структуре вашей организации. Подробнее см. в разделах Подразделения и Группы.

5. Нажмите кнопку **Сохранить**.

Для авторизации в сервисах Яндекс 360 сотруднику нужно будет вводить свой полный почтовый адрес (например, `login@example.com`) и пароль.



Пригласить пользователей

Вы можете пригласить пользователей присоединиться к вашей организации со своими аккаунтами на Яндексе. Чтобы пригласить пользователей, не обязательно подключать почтовый домен.

Внимание

На балансе должно быть достаточно средств для оплаты тарифа с учетом новых сотрудников. Если вы хотите добавить в организацию больше 1000 участников, напишите в службу поддержки через форму внизу страницы.

У приглашенных пользователей не будет почтового ящика на вашем домене. При этом приглашенные пользователи смогут использовать все сервисы Яндекс 360 для бизнеса, подключенные к организации.

Пригласить пользователя в организацию можно с помощью ссылки. По одной ссылке можно пригласить только одного сотрудника.

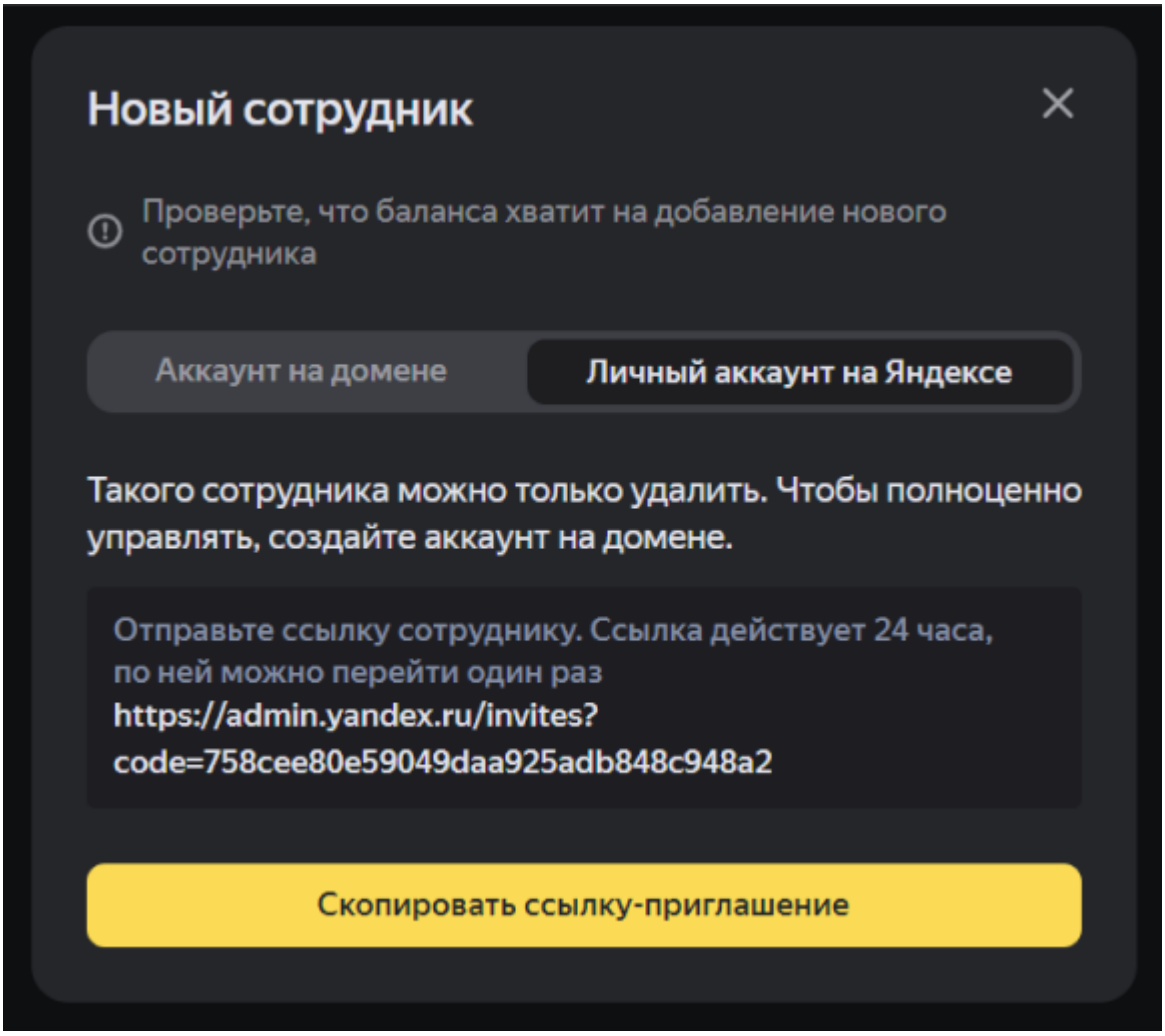
Чтобы получить ссылку для приглашения пользователя:

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники** и нажмите кнопку **Добавить**.
3. Откроется окно **Новый сотрудник**. Если у вас не подключен единый вход (SSO), перед этим выберите в открывшемся меню **Пригласить по ссылке**.
4. Скопируйте ссылку из окна **Новый сотрудник** и отправьте сотруднику, которого нужно пригласить в организацию.

Чтобы пригласить нескольких пользователей, получите для каждого из них отдельную ссылку. Для этого закройте окно **Новый сотрудник** и снова нажмите кнопку **Добавить**.

Чтобы присоединиться к организации, пользователю нужно авторизоваться в аккаунте Яндекса, который он будет использовать для работы, и перейти по ссылке. После этого пригласительная ссылка станет недействительной.

Ссылка действует только 24 часа. Если срок действия ссылки истечет, получите новую ссылку.



Написать в службу поддержки

Загрузить список

Внимание

Вы можете создавать аккаунты пользователей, только если к организации подключен домен и у вас на балансе достаточно средств для оплаты тарифа с учетом новых пользователей.

Чтобы сотрудники вашей компании могли использовать сервисы Яндекс 360 для бизнеса, создайте для них аккаунты в организации.

Загрузите CSV-файл со списком сотрудников:

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Нажмите кнопку **Добавить сотрудника**.
4. Скачайте шаблон CSV-файла.
5. По образцу добавьте в файл данные сотрудников.

   Первая строка файла — заголовки полей аккаунта. В каждой следующей строке файла должны быть указаны данные одного аккаунта в кавычках через точку с запятой. Всего в файл можно добавить до 20 000 строк с данными аккаунтов сотрудников.

   Обязательно должны быть указаны логины сотрудников на вашем домене, в которые будет происходить миграция.
6. Сохраните CSV-файл в кодировке UTF-8 (в Microsoft Excel нажмите **Сохранить как** → **CSV-UTF8**).

   Внимание

   Если сохранить файл в другой кодировке, он будет распознан неправильно.
7. Нажмите кнопку **Выбрать CSV-файл** и укажите ваш файл.
8. Нажмите **Загрузить список**. Добавленные сотрудники отобразятся в списке **Пользователи**. Если во время загрузки возникли ошибки, после завершения нажмите значок и посмотрите логи.

Написать в службу поддержки

Подразделения

В Яндекс 360 для бизнеса вы можете воссоздать структуру вашей организации: создать подразделения и добавить в них сотрудников. Это повысит наглядность работы, выстроит иерархию сотрудников в организации и поможет разграничить их полномочия. Иерархическая структура может быть любого уровня вложенности.

Если к организации подключен почтовый домен, для каждого подразделения можно создать адрес рассылки, чтобы отправлять письма сразу всем сотрудникам подразделения.

Действия с подразделениями

На вкладке **Подразделения** вы можете добавлять новые и редактировать созданные ранее подразделения, а также перемещать их в структуре вашей организации и удалять, когда они больше не нужны.

Добавить

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Подразделения**.
4. В правой части строки на том уровне структуры, куда нужно добавить новое подразделение, нажмите значок . Если подразделений еще нет, в центре экрана нажмите **Добавить**.
5. В окне **Добавить подразделение** введите название подразделения, его краткое описание и адрес рассылки (если к организации подключен почтовый домен).
6. Нажмите кнопку **Сохранить**.

Редактировать

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Подразделения**.
4. Выделите подразделение, в конце строки нажмите значок и выберите **Редактировать**.
5. В окне **Редактировать подразделение** внесите нужные изменения и нажмите **Сохранить**.

Переместить

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Подразделения**.
4. Выделите подразделение, в конце строки нажмите значок и выберите **Переместить**.

5. Укажите, куда нужно переместить подразделение, и нажмите кнопку **Переместить**.

Удалить

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Подразделения**.
4. Выделите подразделение, в конце строки нажмите значок и выберите **Удалить**.

> **Примечание**
>
> Вы не можете удалить подразделение, в котором есть сотрудники. Удалите сотрудников из подразделения, а затем удалите его.

Действия с сотрудниками подразделений

Вы можете добавлять сотрудников в подразделения и удалять сотрудников из подразделений в случае увольнения или перевода в другой отдел.

Добавить

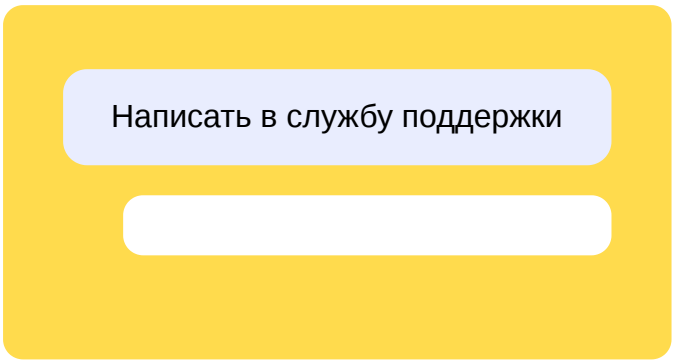
1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Подразделения**.
4. Выделите подразделение, в конце строки нажмите значок и выберите **Добавить сотрудников**.
5. Выберите сотрудников из списка и нажмите кнопку **Добавить сотрудников**.

> **Примечание**
>
> Сотрудник может числиться только в одном подразделении.

Удалить

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Подразделения**.
4. Выделите и разверните нужное подразделение, чтобы увидеть список его сотрудников.
5. Выделите сотрудника, которого нужно удалить, и в конце строки нажмите значок .

6. Подтвердите удаление сотрудника из подразделения.



Группы

Чтобы объединить сотрудников разных отделов (например для работы над крупной задачей или с одним клиентом), вы можете создать группу. Можно выстраивать иерархические структуры групп любого уровня вложенности. В одной группе рекомендуется объединять не более 10 000 участников.

Если к организации подключен почтовый домен, для группы можно создать адрес рассылки, чтобы отправлять письма сразу всем ее участникам — например, когда вы планируете большую встречу в Календаре и хотите пригласить на нее более 100 человек.

Действия с группами

> **Примечание**
>
> Управлять группой могут только администраторы.

На вкладке **Группы** вы можете добавлять новые и редактировать созданные ранее группы, а также перемещать их в дереве и удалять, когда они больше не нужны.

Добавить

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Группы**.
4. В правой части строки на том уровне структуры, куда нужно добавить новую группу, нажмите значок . Если групп еще нет, нажмите **Добавить** в центре экрана.
5. В окне **Добавить группу** введите название группы, ее краткое описание и адрес рассылки (если к организации подключен почтовый домен).
6. Нажмите кнопку **Сохранить**.

Редактировать

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Группы**.
4. Выделите группу, в конце строки нажмите значок и выберите **Редактировать**.
5. В окне **Редактировать группу** внесите нужные изменения и нажмите **Сохранить**.

Переместить

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.

3. Выберите вкладку **Группы**.
4. Выделите группу, в конце строки нажмите значок и выберите **Переместить**.
5. Укажите, куда нужно переместить группу, и нажмите кнопку **Переместить**.

Удалить

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Группы**.
4. Выделите группу, в конце строки нажмите значок и выберите **Удалить**.

> **Примечание**
>
> При удалении группы аккаунты ее участников сохраняются.

Действия с участниками группы

> **Примечание**
>
> Управлять участниками могут только администраторы.

Вы можете добавлять сотрудников в группы и удалять сотрудников из групп, если они больше не участвуют там.

В одной группе может состоять до 10 000 сотрудников. При подсчете общего количества сотрудников в группе учитывается членство сотрудника как в верхнеуровневой группе, так и во всех вложенных, если они есть.

Добавить

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Группы**.
4. Выделите группу, в конце строки нажмите значок и выберите **Добавить сотрудников**.
5. Выберите сотрудников из списка и нажмите кнопку **Добавить сотрудников**.

Примечание

Один и тот же сотрудник может быть участником нескольких групп.

Удалить

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Сотрудники**.
3. Выберите вкладку **Группы**.
4. Выделите и разверните нужную группу, чтобы увидеть список ее сотрудников.
5. Выделите сотрудника, которого нужно удалить, и в конце строки нажмите значок .
6. Подтвердите удаление сотрудника из группы.

Написать в службу поддержки

Переезд в Яндекс 360 для бизнеса

Мы собрали ответы на частые вопросы о том, как перенести данные вашей организации в Яндекс 360 для бизнеса из Google Workspace, Microsoft 365 и других платформ. Смотреть >

Офисы и переговорки

Эта возможность доступна в тарифах **Основной**, **Продвинутый** и всех версиях тарифа **Корпоративный** из новой линейки, а также тарифах **Оптимальный** и **Расширенный** из старой.

Если в офисах вашей компании есть специальные помещения для проведения рабочих встреч (переговорки), добавьте их в Яндекс 360 для бизнеса, чтобы сотрудники могли бронировать переговорки прямо при создании встречи в календаре.

Каждая переговорка привязывается к определенному офису: если у компании несколько филиалов в разных городах или офисы в разных зданиях, сотрудникам удобнее сначала указать нужный офис, а затем выбирать из доступных переговорок.

Если во встрече участвуют коллеги из разных офисов, можно забронировать одновременно несколько переговорок.

Бронирование переговорки доступно любому сотруднику с аккаунтом на домене организации, а также сотрудникам связанной организации, которая входит в федерации.

Как добавить офис и переговорки

Чтобы добавлять переговорки, сначала добавьте хотя бы один офис.

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Офисы и переговорки**.
3. На вкладке **Офисы** нажмите **Добавить**. Если в списке уже есть офисы, кнопка будет в правом верхнем углу, а если добавляете первый — в центре экрана.
4. Укажите название офиса, город, в котором он находится, и адрес.
5. Нажмите **Сохранить**.

Теперь можно добавить переговорку:

1. Перейдите на вкладку **Переговорки** и нажмите **Добавить**. Если в списке уже есть переговорки, кнопка будет в правом верхнем углу, а если добавляете первую — в центре экрана.
2. Укажите название переговорки, логин, офис, этаж и вместимость — это обязательные поля. Поле **Описание** можно не заполнять.
3. Включите опцию **Переговорка доступна для бронирования**, если хотите, чтобы сотрудники могли добавлять ее во встречи.
4. Нажмите кнопку **Сохранить**.

Для одной организации можно добавить не более 10 офисов и 100 переговорок.

Как отредактировать данные

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Офисы и переговорки**.
3. Выберите вкладку и наведите указатель на офис или переговорку, которые хотите изменить.
4. Нажмите значок и выберите **Редактировать**.
5. Внесите изменения и нажмите **Сохранить**.

Как удалить офис или переговорку

Удаление необратимо

Если удалить переговорку, забронировать ее для новых встреч будет нельзя.

Если удалить офис, удалятся и все переговорки внутри него — в том числе из встреч, для которых они были забронированы. Это действие нельзя отменить.

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Офисы и переговорки**.
3. Выберите вкладку и наведите указатель на офис или переговорку, которые хотите удалить.
4. Нажмите значок и выберите **Удалить**.
5. Подтвердите действие.

Как сотрудникам бронировать переговорку из сторонних программ

Если сотрудник использует не Яндекс Календарь, а почтовую программу или приложение календаря, которые синхронизируются с Яндекс Календарем по протоколу CalDAV, передайте ему почтовый адрес переговорки вида `логин@основной-домен-организации.ru`. Как настроить такую синхронизацию

Узнать почтовый адрес переговорки

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Офисы и переговорки**.
3. Выберите вкладку **Переговорки** и нажмите строку с нужной переговоркой.
4. Скопируйте адрес из поля **Почта**.

Инструкция для сотрудника

Чтобы забронировать переговорку, добавьте почтовый адрес переговорки, полученный у администратора организации, в список обязательных участников встречи.

Если переговорка свободна, вы получите письмо о том, что приглашение на встречу принято. Если занята, вам придет отказ от участия во встрече, а переговорка удалится из списка участников. Такие письма можно отключить по инструкции, но без них вы не узнаете, удалось ли забронировать переговорку.

С аккаунтом владельца организации можно создавать и редактировать переговорки, но бронировать нельзя. Для бронирования перейдите в аккаунт на домене организации.

Как создать событие и забронировать переговорку в Яндекс Календаре

Написать в службу поддержки

Первоначальная настройка

Совет

Выполнить настройку, описанную на этой странице, можно автоматически — для этого достаточно **делегировать** домен на Яндекс. Как это сделать?

Если вы уже делегировали домен, дополнительно настраивать почту вам не нужно — все необходимые DNS-записи созданы автоматически.

Чтобы письма, адресованные вашей организации, приходили в ящики на корпоративной Яндекс Почте, понадобятся несколько DNS-записей для вашего домена.

Как настроить DNS-записи

Для работы почты нужны три записи:

Тип	Хост	Значение	TTL
MX	@	mx.yandex.net.	21600
TXT	mail._domainkey	{уникальный ключ}	21600
TXT	@	v=spf1 redirect=_spf.yandex.net	21600

Конкретный набор шагов разный у разных регистраторов. Воспользуйтесь инструкциями:

- Как создать MX-запись
- Как создать SPF-запись
- Как создать подпись DKIM

После создания или редактирования записи подождите несколько часов — обновление записей происходит не мгновенно.

Написать в службу поддержки

Почтовые адреса

В этом разделе собраны инструкции по настройке почтовых адресов, используемых в организации.

- Как сделать сотруднику дополнительный адрес (алиас)
- Как сделать адрес-рассылку, чтобы письма получали несколько сотрудников
- Как получать письма, отправленные на несуществующие адреса

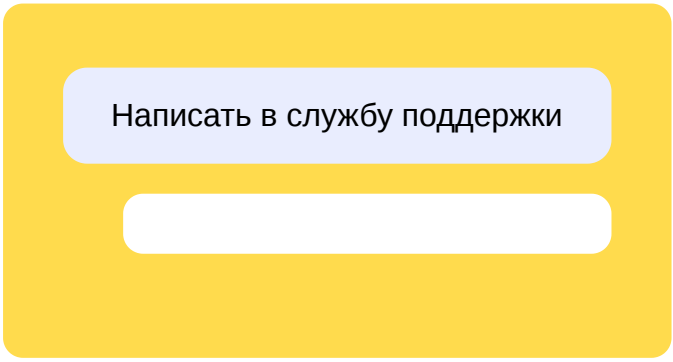
Как создать почтовый ящик

Почтовый ящик — это часть аккаунта сотрудника. Чтобы создать новый почтовый ящик, вам нужно зарегистрировать нового сотрудника. Как это сделать?

Совет

Возможно, для решения вашей задачи не нужно создавать новый ящик, а достаточно создать **адрес-синоним** или запустить **рассылку**.

Чтобы изучить эти возможности, прочтите статьи об адресах-синонимах (алиасах) и о рассылках по подразделениям.



Адреса-синонимы (алиасы)

Примечание

Это статья об адресах-алиасах **внутри одного домена**. О доменах-алиасах рассказано в разделе Домены.

У почтового ящика в Яндекс Почте может быть несколько адресов:

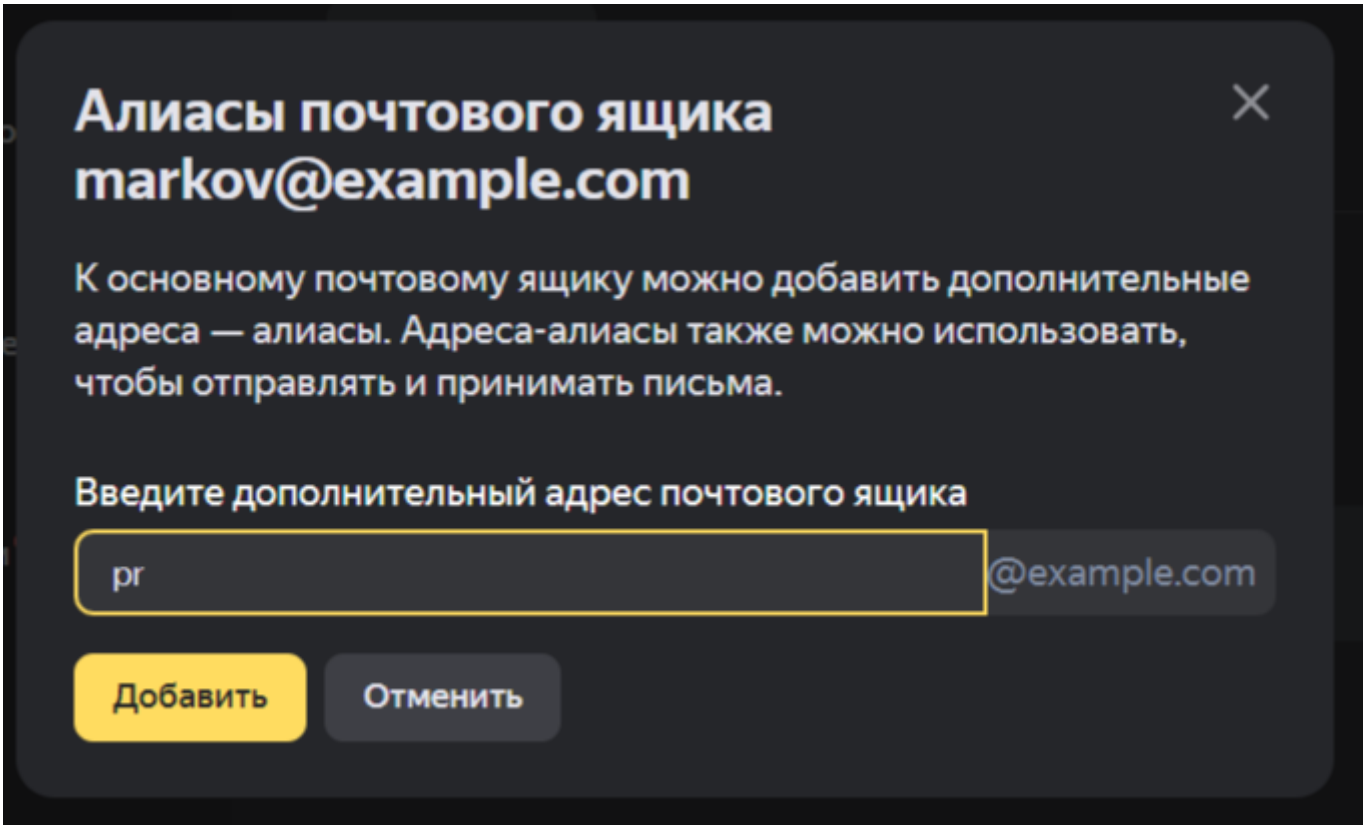
- **Основной адрес**, который задается при регистрации сотрудника.
- Дополнительные адреса — **алиасы**, которые могут быть добавлены потом. Если у сотрудника есть адреса-алиасы, он может использовать их для входа. У одного ящика может быть до **10** алиасов.

Зачем это нужно

Например, у вас есть сотрудник Игорь Марков с основным адресом `markov@example.com`. Он работает PR-менеджером. Вы хотите, чтобы почта, отправленная на адрес `pr@example.com`, приходила в его личный почтовый ящик.

В таком случае вы можете добавить алиас `pr@example.com` к основному адресу. После этого Игорь сможет:

- читать письма, отправленные на `pr@example.com`, прямо в своем рабочем почтовом ящике;
- отправлять письма с адреса `pr@example.com`;
- входить в Яндекс 360, используя алиас в качестве логина.



Как добавить алиас

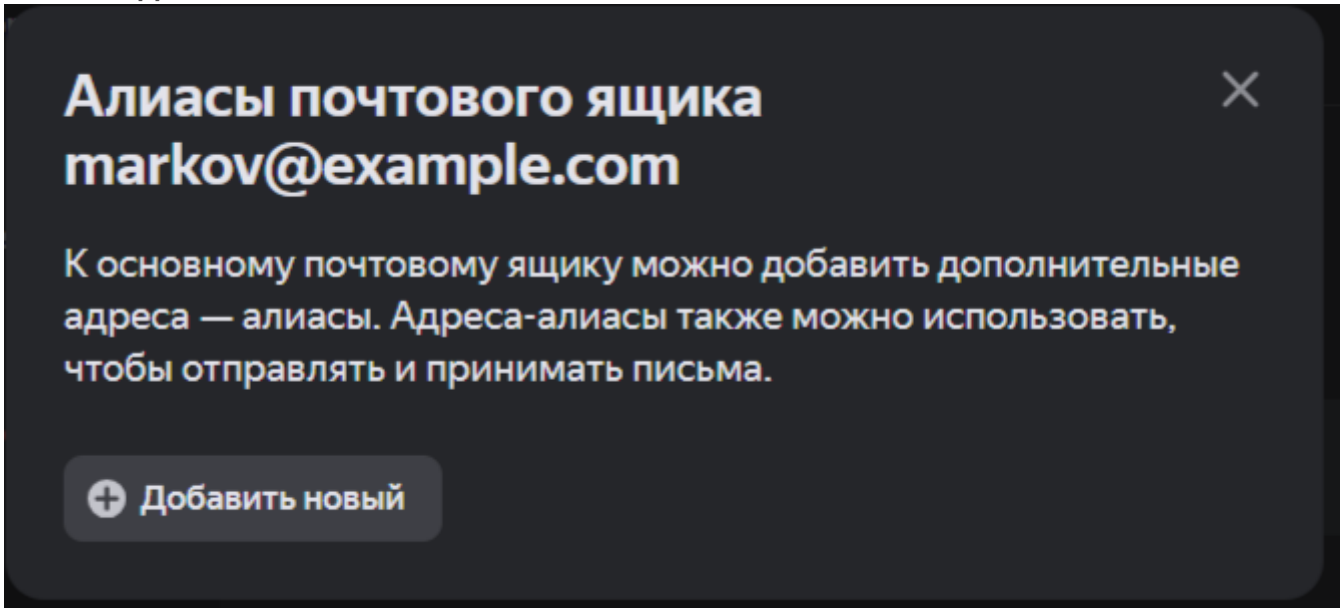
Примечание

Эта инструкция подходит, если вы управляете аккаунтами сотрудников с помощью Яндекс 360. Если у вас настроена автоматическая синхронизация с собственной службой каталогов (например, Active Directory), добавляйте алиас через нее.

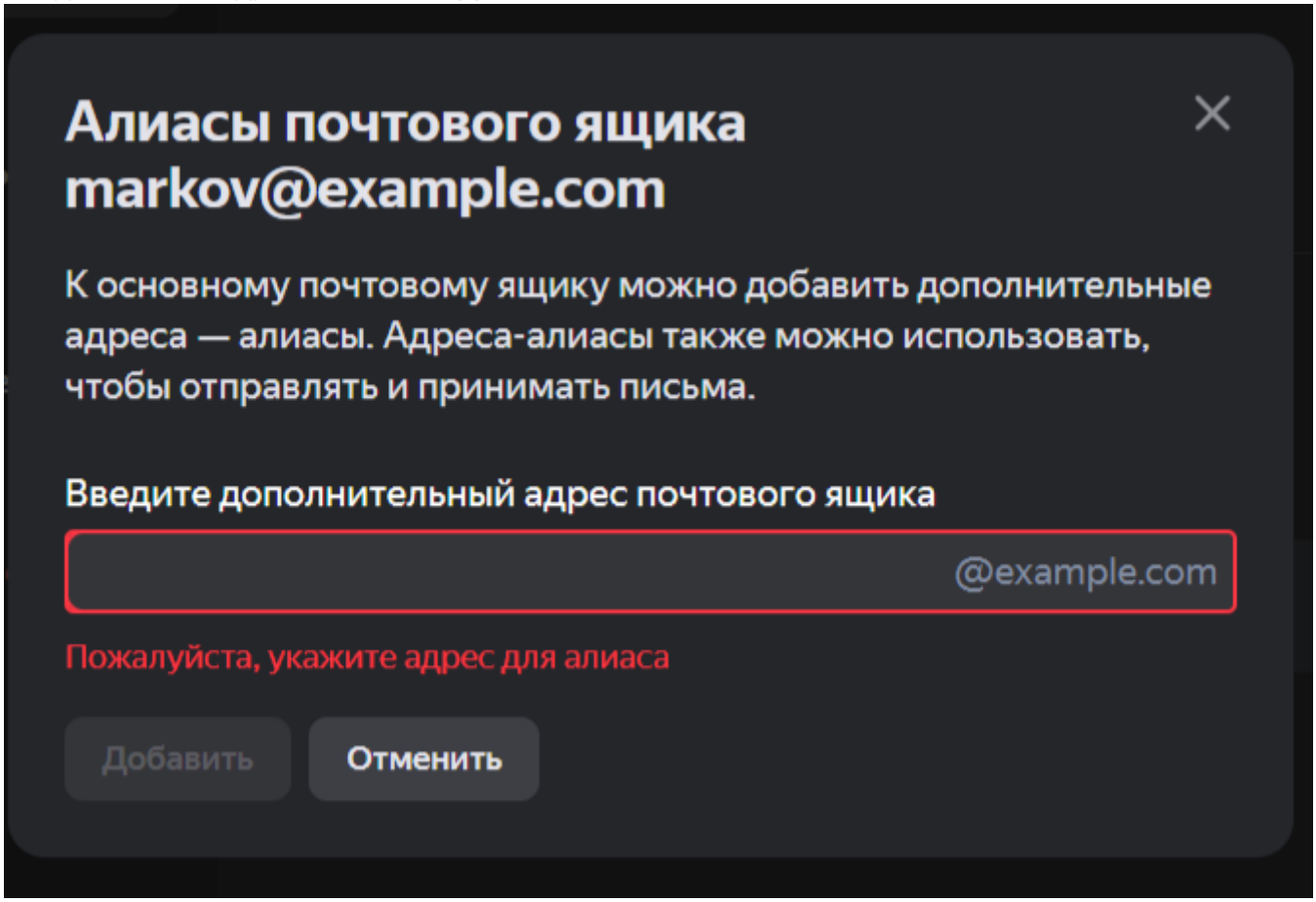
Как управлять синхронизацией с Active Directory

1. Откройте admin.yandex.ru.
2. Выберите **Сотрудники**.
3. Найдите в списке нужного сотрудника и нажмите на его имя.
4. Нажмите на три точки в правом верхнем углу карточки сотрудника и выберите **Редактировать алиасы**.

5. Нажмите **Добавить новый**.



6. Введите новый адрес и нажмите **Добавить**.



Как удалить алиас

> **Примечание**
>
> Эта инструкция подходит, если вы управляете аккаунтами сотрудников с помощью Яндекс 360. Если у вас настроена автоматическая синхронизация с собственной службой каталогов (например, Active Directory), добавляйте алиас через нее.
>
> Как управлять синхронизацией с Active Directory

1. Откройте admin.yandex.ru.
2. Выберите **Сотрудники**.
3. Найдите в списке нужного сотрудника и нажмите на его имя.
4. Нажмите на три точки в правом верхнем углу карточки сотрудника и выберите **Редактировать алиасы**.

5. Наведите мышью на нужный алиас и нажмите на крестик.

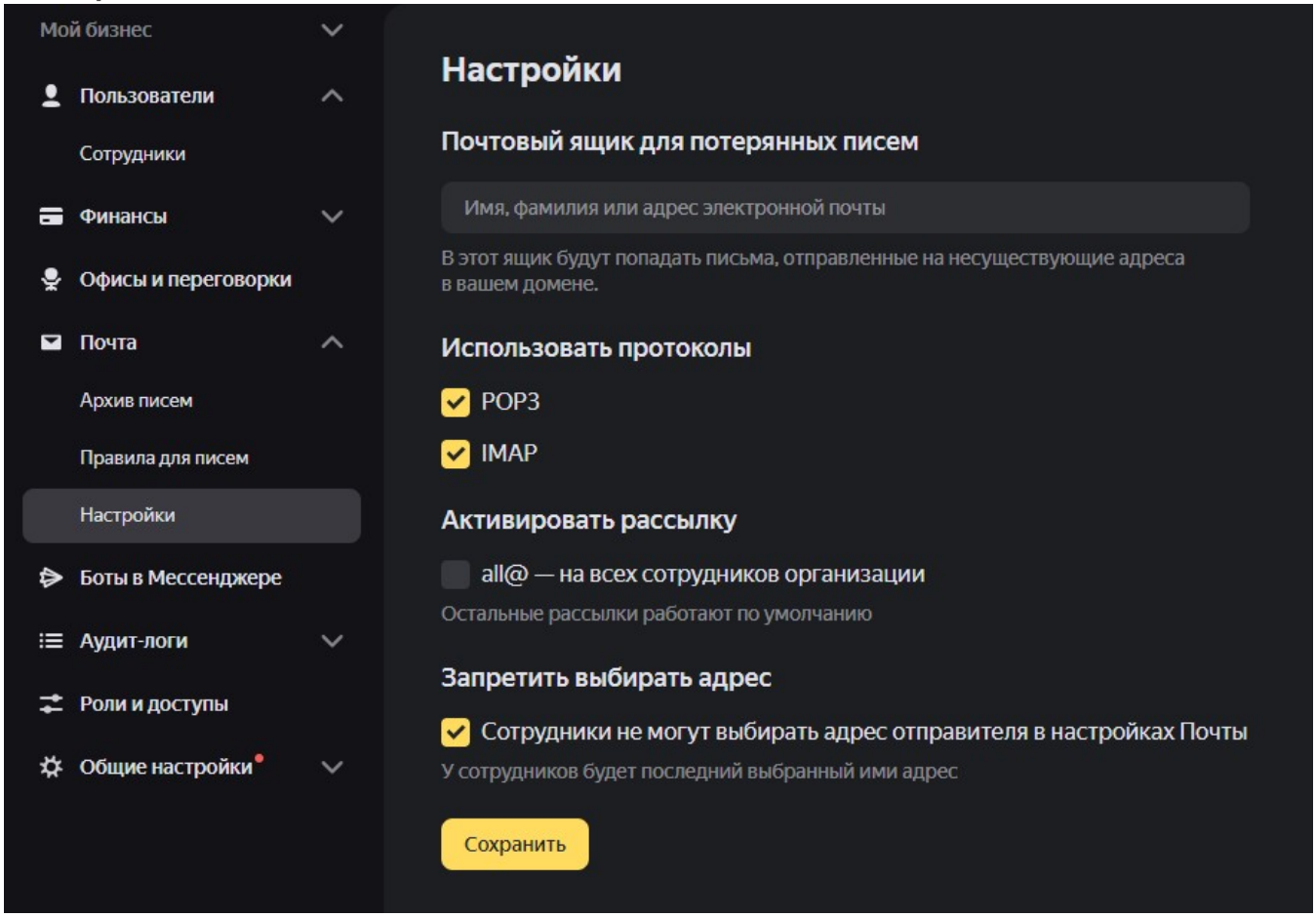
Запрет на использование алиасов

Если вы хотите, чтобы каждый сотрудник организации использовал для работы только один адрес, вы можете **запретить переключение между алиасами**. Такой запрет затрагивает как именные, так и доменные алиасы.

Обратите внимание: у каждого сотрудника в качестве единственного останется тот адрес, который был выбран в настройках Почты в момент введения запрета. Изменить его можно будет только по API с помощью запроса `POST org/{orgId}/mail/users/{userId}/settings/sender_info` (документация).

Как установить запрет

1. Откройте admin.yandex.ru и выберите **Почта** → **Настройки**.
2. Поставьте галочку напротив **Сотрудники не могут выбирать адрес отправителя в настройках Почты**.



Вопросы и ответы

Смогут ли сотрудники пользоваться алиасом, работая с почтой через почтовый клиент?

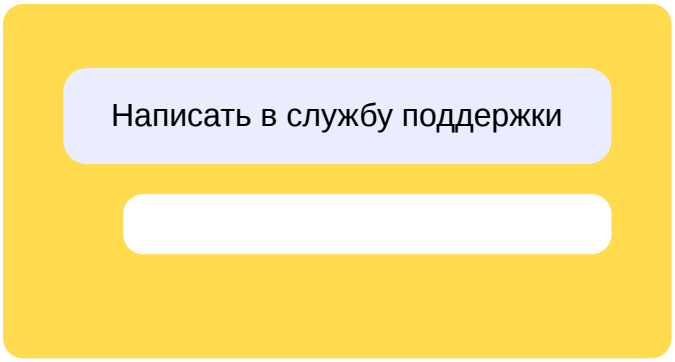
Да.

Чтобы получать такую почту, ничего дополнительно настраивать не надо.

Чтобы отправлять почту с адреса-алиаса, почтовый клиент нужно донастроить.

Можно ли один и тот же алиас прикрепить к нескольким почтовым ящикам?

Нет. Чтобы письмо получали сразу несколько сотрудников, создайте рассылку. Инструкция


Написать в службу поддержки

Рассылки по подразделениям и группам

Вы можете настроить корпоративную почту так, чтобы письма на определенный адрес получали несколько сотрудников. Например, чтобы все менеджеры отдела продаж читали почту `sales@example.com`.

Для этого нужно, чтобы все получатели писем относились к одному подразделению или группе.

Как создать рассылку

1. Создайте новую группу или подразделение по инструкциям из раздела Сотрудники, подразделения и группы. При создании укажите нужный адрес рассылки.
2. Добавьте в эту группу или подразделение нужных получателей.

Если все нужные адресаты уже состоят в одной группе или подразделении, ничего нового создавать не нужно — просто добавьте адрес рассылки в свойствах этой группы или подразделения.

Отправители рассылок

По умолчанию на адреса почтовых рассылок можно писать всем. Однако для каждой рассылки вы можете ограничить список пользователей, у которых есть такое право. Для этого нужно задать список разрешенных отправителей рассылки. Это нужно для того, чтобы исключить ситуации, когда любой пользователь может написать письмо на адрес рассылки или случайно отправить ответ на рассылку всем ее участникам.

Если пользователь, которого нет в списке разрешенных отправителей рассылки, напишет письмо на ее адрес, то оно никуда не уйдет. Так произойдет, даже если в полях **Кому**, **Копия** и **Скрытая копия** содержатся другие адреса, на которые у пользователя есть право отправлять письма. Яндекс Почта проинформирует о том, что письмо не было отправлено.

Когда для рассылки на группу или подразделение задан список разрешенных отправителей:

- на адрес такой рассылки не смогут писать пользователи, аккаунты которых созданы не на доменах организаций в Яндекс 360 для бизнеса;
- на такую группу или подразделение не получится отправить приглашение из Яндекс Календаря.

Как задать список разрешенных отправителей или добавить в него сотрудников

Задать список отправителей можно с помощью запроса к API. Таких запросов может быть несколько — список каждый раз будет дополняться теми, кого вы укажете в новом запросе.

1. Подготовьтесь к работе с API .
   1.1. Получите OAuth-токен, который позволит управлять доступом и авторизацией:
      - Воспользуйтесь инструкцией на странице Доступ к API. При создании приложения выберите следующие доступы:
        - `ya360_admin:mail_read_mail_list_permissions` и `ya360_admin:mail_write_mail_list_permissions` — для отправки запросов на добавление разрешенных отправителей рассылок;

- `directory:read_groups` — для отправки запросов на просмотр информации о группах, в том числе идентификаторах рассылок;
- `directory:read_departments` — для отправки запросов на просмотр информации о подразделениях, в том числе идентификаторах рассылок;
- `directory:read_users` — для отправки запросов на просмотр информации о сотрудниках организации.

- Если OAuth-приложение уже создано, но у него нет нужных прав доступа, добавьте их и получите новый токен по инструкции.

1.2. Ознакомьтесь с порядком отправки запросов к API, если вы не имели такого опыта ранее.

Как составлять и отправлять HTTP-запросы

Для формирования запроса вам необходимо знать:

- HTTP-метод — он определяет какую именно операцию вы собираетесь выполнить, например, получить информацию с сервера или обновить ее.
- URL запроса — это адрес ресурса, на который отправляется запрос.
- Заголовки — передают дополнительную информацию, например, об аутентификации или форматах данных.
- Тело запроса — необязательная часть, которая используется в некоторых методах (например, POST) для передачи конкретных данных.

Отправка HTTP-запросов может выполняться различными способами в зависимости от того, какой инструмент или язык программирования вы используете. Одним из таких способов является отправка запросов с помощью cURL.

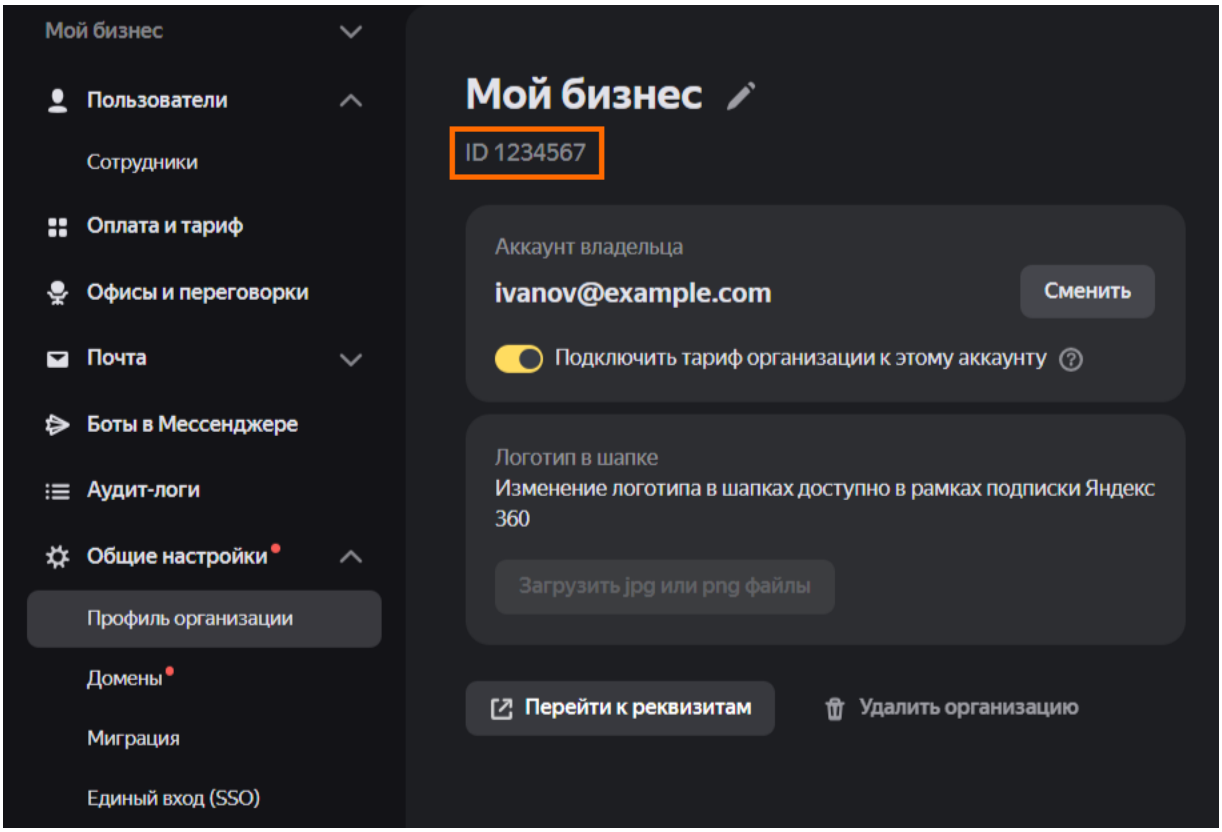
Чтобы отправить любой запрос из этого раздела с помощью cURL, если вы работаете на Windows:

1. Подготовьте команду: скопируйте приведенный пример в любой редактор и подставьте в места, обозначенные фигурными скобками, нужную информацию.
2. Откройте папку, в которой лежит файл с телом запроса, если оно есть в примере. Если тела нет, отправлять запрос можно из любой папки.
3. Нажмите на пустое место в адресной строке.
4. Напишите туда `cmd` и нажмите клавишу Enter.
5. Откроется окно «Командная строка». Вставьте в него готовую команду и нажмите Enter.

2. Получите необходимые идентификаторы.

2.1. Определите идентификатор вашей организации: откройте admin.yandex.ru и выберите **Общие настройки** → **Профиль организации**. Идентификатор будет указан под названием организации.

Скриншот



2.2. Выясните идентификатор рассылки, для которой надо создать список отправителей. Это можно сделать с помощью запросов к API Яндекс 360 для бизнеса.

- **Для рассылки на группу**

Для рассылки на группу

Компонент запроса	Значение
HTTP-метод	`GET`

URL запроса

```
https://api360.yandex.net/directory/v1/org/{ОРГАНИЗАЦИЯ}/groups
```

где `{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1.

Заголовки

```
Authorization: OAuth {OAUTH-TOKEN}
```

где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1.1.

в документации API.

Для рассылки на подразделение

Для рассылки на подразделение

Компонент запроса	Значение
HTTP-метод	`GET`

URL запроса

```
https://api360.yandex.net/directory/v1/org/{ОРГАНИЗАЦИЯ}/departments
```

где `{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1.

Заголовки

```
Authorization: OAuth {OAUTH-TOKEN}
```

где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1.1.

```
curl -X GET -H "Authorization: OAuth {OAUTH-TOKEN}"
https://api360.yandex.net/directory/v1/org/{ОРГАНИЗАЦИЯ}/departments
```

Как отправить команду, если вы работаете на Windows, описано на шаге 1.2.

Идентификатор рассылки придет в поле `emailId` ответа на запрос — в массиве `departments` найдите часть, которая содержит описание нужного вам подразделения (его название будет указано в поле `name`, а адрес почтовой рассылки — в поле `email`), и скопируйте значение из поля `emailId`.

Полное описание запроса на получение списка подразделений организации можно посмотреть в документации API.

2.3. Определите идентификаторы тех, кому вы планируете предоставить право писать на рассылку.

○ **Сотрудники**

Сотрудники

По API

Компонент запроса	Значение
HTTP-метод	`GET`
URL запроса	`https://api360.yandex.net/directory/v1/org/{ОРГАНИЗАЦИЯ}/users` где `{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1.
Заголовки	`Authorization: OAuth {OAUTH-TOKEN}` где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1.1.

Отправить запрос можно с помощью команды `curl` такого вида:

```
curl -X GET -H "Authorization: OAuth {OAUTH-TOKEN}"
```

```
https://api360.yandex.net/directory/v1/org/{ОРГАНИЗАЦИЯ}/users
```

Как отправить команду, если вы работаете на Windows, описано на шаге 1.2.

Идентификаторы сотрудников возвращаются в поле `id` ответа на запрос — в массиве `users` найдите часть, которая содержит описание нужного вам сотрудника (его имя и фамилия будут указаны в поле `name`, а логин — в поле `nickname`), и скопируйте значение из поля `id`.

Полное описание запроса на получение списка сотрудников организации можно посмотреть в документации API.

В интерфейсе кабинета организации

1. Перейдите в кабинет организации Яндекс 360 для бизнеса admin.yandex.ru.
2. Выберите **Пользователи** → **Сотрудники**.
3. Найдите строчку нужного сотрудника и нажмите на его имя.
4. Правой кнопкой нажмите на логин сотрудника и скопируйте адрес ссылки.
5. Вставьте адрес в любой текстовый редактор. Идентификатор сотрудника — это часть адреса после `uid=`.

Группы

Группы

Идентификаторы групп можно получить из ответа на запрос на получение списка групп организации. Порядок отправки этого запроса описан в разделе "Для рассылки на группу" на шаге 2.2. Идентификатор каждой группы возвращается в поле `id` массива `groups`.

Подразделения

Подразделения

Идентификаторы групп можно получить из ответа на запрос на получение списка групп организации. Порядок отправки этого запроса описан в разделе "Для рассылки на подразделение" на шаге 2.2. Идентификатор каждого подразделения возвращается в поле `id` массива `departments`.

Организация

Организация

Порядок получения идентификатора организации описан на шаге 2.1.

Отдельному общему ящику нельзя дать разрешение писать на рассылку

С адресов общих ящиков можно отправлять письма на адрес рассылки, только если для этого адреса рассылки:

- список разрешенных отправителей не задан;
- право писать на рассылку задано сразу для всей организации. Если же для рассылки задан список разрешенных отправителей, писать на ее адрес с общих ящиков не получится.

3. Сформируйте и отправьте запрос на добавление разрешенных отправителей.

3.1. Подготовьте список тех, кто может писать на рассылку. Для этого в любом текстовом редакторе создайте файл с телом запроса — например, с именем `permissions-list.json`. Структура файла будет аналогична такой:

```
{
   "role_actions": [
      {
         "type": "grant",
         "roles": [
            "mail_list_sender"
         ],
         "subjects": [
            {
               "type": "organization",
               "id": 1234567,
               "org_id": 1234567
            },
            {
               "type": "department",
               "id": 777,
               "org_id": 1234567
            },
            {
               "type": "group",
               "id": 555,
               "org_id": 1234567
            },
            {
               "type": "user",
               "id": 1150000062907856,
               "org_id": 1234567
            },
            {
               "type": "user",
               "id": 1150000062907859,
               "org_id": 1234567
            }
         ]
      }
```

```
    ]
}
```

Измените файл так, чтобы он содержал информацию о той организации, ее подразделениях, группах или сотрудниках, которым вы предоставляете право писать на рассылку. Каждого из них опишите конструкцией, содержащей следующие поля по аналогии с примером:

Параметр	Тип данных	Описание
`type`	Строка	Тип того, кому предоставляется право писать на рассылки: - `organization` — вся организация; - `department` — подразделение; - `group` — группа; - `user` — пользователь. Конструкций с типами `department`, `group` и `user` в файле может быть несколько. Значение `organization` означает, что право писать на адрес рассылки будет у всех сотрудников организации (в том числе с адресов общих ящиков), а внешние контакты писать на рассылку не смогут.
`id`	Целое число	Идентификатор того, кому предоставляется право писать на рассылки. Идентификаторы вы получили на шаге 2.3.

`org_id`	Целое число	Идентификатор организации. В поле указывается: ▪ идентификатор вашей организации для тех сотрудников, групп и подразделений, которые принадлежат ей; ▪ «0» для внешних контактов, которые не принадлежат организации.

3.2.

Компонент запроса	Значение
HTTP-метод	`POST`

URL
запроса

омощью команды `curl`

```
https://cloud-
api.yandex.net/v1/admin/org/{ОРГАНИЗАЦИЯ}/mail-
lists/{РАССЫЛКА}/update-permissions
```

```
-H "Content-Type:
/cloud-
{РАССЫЛКА}/update-
```

где

но на шаге 1.2.

4. Прое

4.1.

`{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1;

Компонент запроса	Значение
HTTP-метод	`GET`

URL
запроса

```
https://cloud-
api.yandex.net/v1/admin/org/{ОРГАНИЗАЦИЯ}/mail-
lists/{РАССЫЛКА}/permissions
```

можно с помощью

```
s://cloud-
ССЫЛКА}/permissions
```

где

на шаге 1.2.

4.2.

`{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1;

перечень всех
которых направлялись в

`{РАССЫЛКА}` — идентификатор рассылки, для которой необходимо задать список пользователей с правами на отправку, полученный на шаге 2.2.

Как удал

1. Вклю
выда

Пример

которым ранее было
n следующего формата:

```
https://cloud-
api.yandex.net/v1/admin/org/1234567/mail-
lists/1150000045826541/permissions
```

```
{
                ]
            }
        ]
}
```

Структура этого файла аналогична структуре файла из шага 3.1, который задает список разрешенных отправителей. Разница в том, что в поле `role_actions.type` указывается другой тип действия: не `grant` — предоставление прав, а `revoke` — отзыв прав.

2. Отправьте запрос к API по инструкции из шага 3.2, где в качестве тела запроса укажите файл `permissions-list-del.json`.

Как перезаписать список разрешенных отправителей

1. Сост охраните его в файле `perm`

Заголовки

```
Authorization: OAuth {OAUTH-TOKEN}
```

где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1.1.

```
{
                "id": 888,
                "org_id": 1234567
            },
            {
                "type": "group",
                "id": 444,
                "org_id": 1234567
            },
            {
                "type": "user",
                "id": 1150000062901254,
                "org_id": 1234567
            }
        ]
    }
  ]
}
```

Структура этого файла аналогична структуре файла из шага 3.1, который задает список разрешенных отправителей. Разница в том, что в поле `role_actions.type` указывается другой тип действия: не `grant` — предоставление прав, а `overwrite` — перезапись списка прав.

Действие `overwrite` распространяется только на те типы, которые присутствуют в запросе

Вы можете перезаписать разрешенных отправителей сразу для всех значений `type` или только некоторых из них. То есть, если вы хотите перезаписать только перечень подразделений, которым разрешена отправка на адрес рассылки, включите в файл только блоки с типом `department` — остальные типы, например сотрудники и группы, останутся без изменений.

2. Отправьте запрос к API по инструкции из шага 3.2, где в качестве тела запроса укажите файл `permissions-list-new.json`.

Как снова разрешить писать на рассылку всем или отменить это разрешение

Параметр `type` может также принимать значение `anonymous`, которое означает, что писать на рассылку может любой пользователь. Чтобы разрешить писать на рассылку всем, добавьте блок с этим типом в список разрешенных отправителей с помощью действия `overwrite`. Отправители с другими типами могут оставаться в списке — это не вызовет конфликтов.

1. Сформируйте файл `permissions-list-all.json` следующего содержания:

```
{
   "role_actions": [
      {
         "type": "overwrite",
         "roles": [
            "mail_list_sender"
         ],
         "subjects": [
            {
               "type": "anonymous",
               "id": 0
            }
         ]
      }
   ]
}
```

2. Отправьте запрос к API по инструкции из шага 3.2, где в качестве тела запроса укажите файл `permissions-list-all.json`.

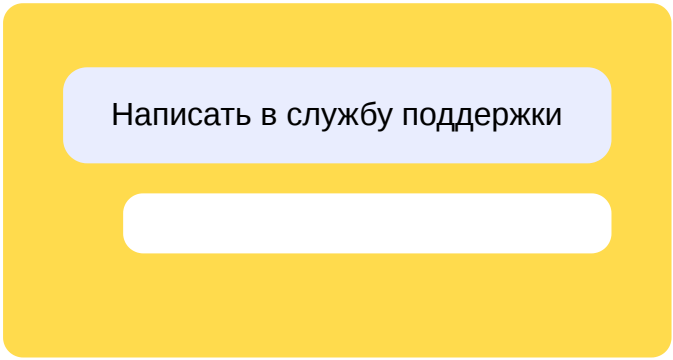
Чтобы повторно ограничить список отправителей, исключите блок с типом `anonymous` из списка с помощью действия `revoke`:

1. Сформируйте файл `permissions-list-del-all.json` следующего содержания:

```
{
   "role_actions": [
      {
         "type": "revoke",
         "roles": [
            "mail_list_sender"
         ],
         "subjects": [
            {
               "type": "anonymous",
               "id": 0
            }
         ]
      }
```

```
    ]
}
```

2. Отправьте запрос к API по инструкции из шага 3.2, где в качестве тела запроса укажите файл `permissions-list-del-all.json`.



Ящик для писем, отправленных на несуществующие адреса

Вы можете настроить получение писем, которые направлены на адреса:

- относящиеся к вашему домену,
- но не зарегистрированные в вашей корпоративной почте.

Пример

> Вы зарегистрировали домен example.com и зарегистрировали три адреса: markov@example.com, pr@example.com и secretary@example.com.
>
> Технически отправитель может написать на любой адрес, а не только на эти три — например, на info@example.com или smith@example.com.

По умолчанию Яндекс Почта не принимает и не сохраняет такие письма, но это поведение можно изменить.

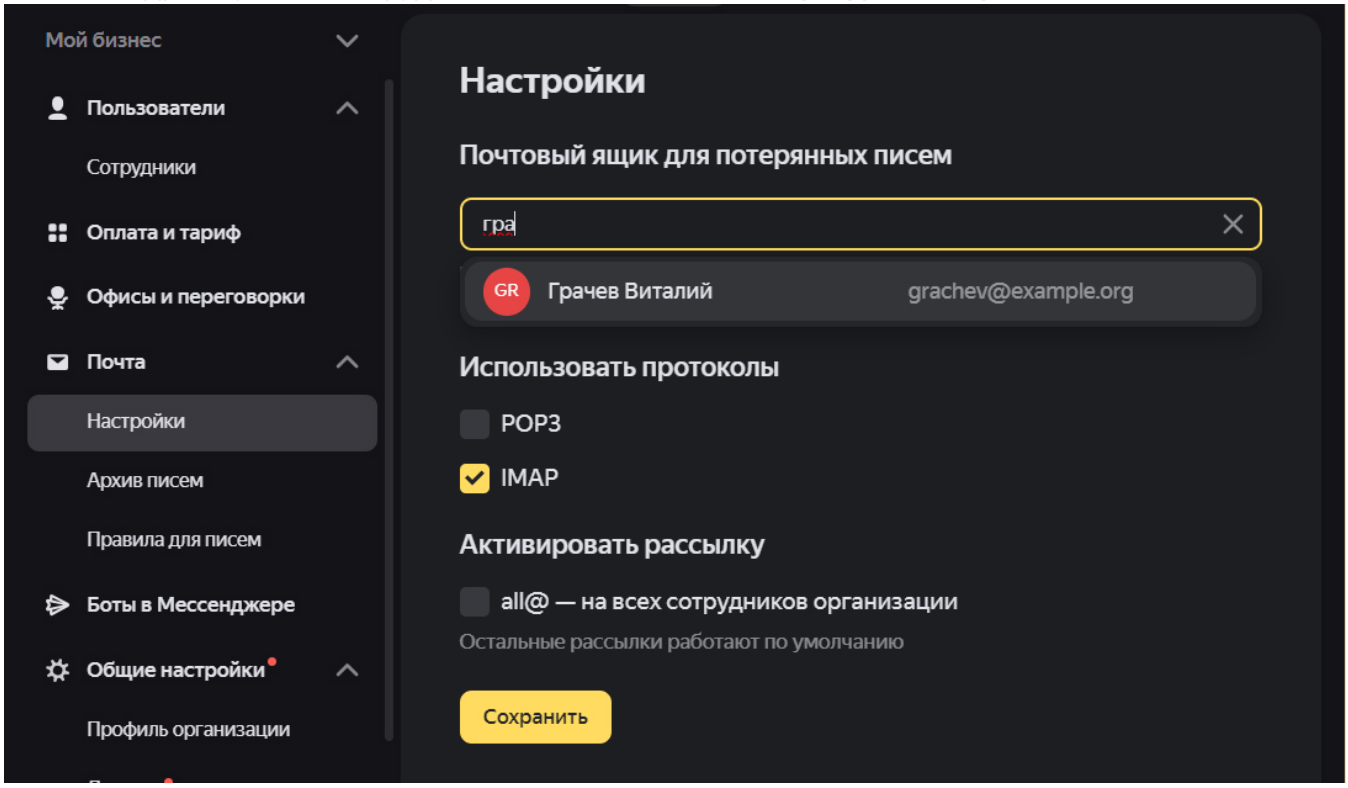
Зачем это нужно

> Настройка позволит вам не пропускать никакую корреспонденцию, адресованную организации, даже если отправитель — например, клиент — не знал конкретного адреса или ошибся при наборе.

Как получать такие письма

Письма, отправленные на несуществующие адреса, можно собирать в любой почтовый ящик организации — например, принадлежащий секретарю.

1. Откройте admin.yandex.ru и выберите **Почта** → **Настройки**.
2. Укажите адрес нужного сотрудника в поле **Почтовый ящик для потерянных писем**.



Можно ли где-то найти письма, отправленные до выполнения этой настройки?

Нет. Если ящик для сбора таких писем не указан, Яндекс Почта их не сохраняет.

Написать в службу поддержки

Совместный доступ: общие и делегированные ящики

Делегированный ящик — ящик пользователя, к которому настроены права доступа для коллег, например на время отпуска владельца. Делегировать можно ящик любого сотрудника.

Общий ящик — ящик, у которого нет конкретного владельца, им могут пользоваться сразу несколько сотрудников организации.

О предоставлении доступа сотрудников читайте в разделах Общие ящики и Делегированные ящики. Вы также можете настроить доступ к общим и делегированным ящикам через API.

Лимиты

Параметр	Делегированные ящики	Общие ящики
Количество ящиков в организации	2500	2500
Количество ящиков (не считая своего), к которым может иметь доступ один пользователь	40 (общий лимит)	
Количество пользователей (не считая владельца), которые могут иметь доступ к одному ящику	40	40

Возможности пользователей

С чужими ящиками пользователи могут работать:

- В веб-интерфейсе Яндекс Почты. Инструкция по настройке совместного доступа в веб-версии
- В почтовых программах. Инструкция по настройке почтовых программ

Режимы отправки писем

Существует два режима отправки писем из общих или делегированных ящиков:

- «Отправить от имени» (Send on behalf) — в заголовке письма указывается, что оно отправлено другим сотрудником от имени владельца делегированного ящика (или от имени общего ящика). То есть получатель видит фактического отправителя письма. Например, если сотрудник Алексей Иванов отправляет письмо от имени своего начальника Сергея Петрова, получатель увидит примерно следующее: «От имени Сергея Петрова, Алексей Иванов».

- «Отправить как» (Send as) — для получателя письмо выглядит так, как будто владелец делегированного ящика отправил его лично. Например, если сотрудник Алексей Иванов отправляет письмо из ящика своего начальника Сергея Петрова, получатель увидит только имя Сергея Петрова. В случае отправки письма с общего ящика получатель также не увидит имя фактического отправителя — у него отобразиться только имя общего ящика.

Пользователь может выбрать режим отправки, если:

- он отправляет письмо из почтовой программы;
- программа поддерживает возможность такого выбора;
- пользователь назначен на роль, которая дает ему право на отправку в обоих режимах.

В веб-интерфейсе Яндекс Почты можно отправлять письма только в режиме «Отправить как».

Действия, доступные сотрудникам

Вы можете выбрать следующие действия, которые будут доступны сотруднику в общем или делегированном ящике:

Ограниченная отправка писем по SMTP (роль в API `shared_mailbox_half_sender`)

Пользователь с такой ролью может отправлять письма по протоколу SMTP только в режиме «Отправить от имени».

Отправка писем по SMTP (роль в API `shared_mailbox_sender`)

Роль позволяет отправлять письма по протоколу SMTP как в режиме «Отправить от имени», так и в режиме «Отправить как».

Управление ящиком в IMAP-клиенте (роль в API `shared_mailbox_imap_admin`)

Пользователь с такой ролью имеет полный доступ на управление содержимым почтового ящика по протоколу IMAP: ему доступны чтение, разметка и удаление писем, а также управление папками. Права на отправку писем роль не дает.

Владение ящиком (роль в API `shared_mailbox_owner`)

Роль предоставляет полные права на ящик, аналогичные тем, которые есть у владельца:

- В почтовых программах:
  - управление ящиком в IMAP-клиенте: чтение, разметка, удаление писем, управление папками;
  - отправка писем по SMTP: как в режиме «Отправить от имени», так и в режиме «Отправить как».
- В веб-версии Яндекс Почты:
  - управление ящиком: чтение, разметка, удаление писем, управление папками;
  - отправка писем в режиме «Отправить как».

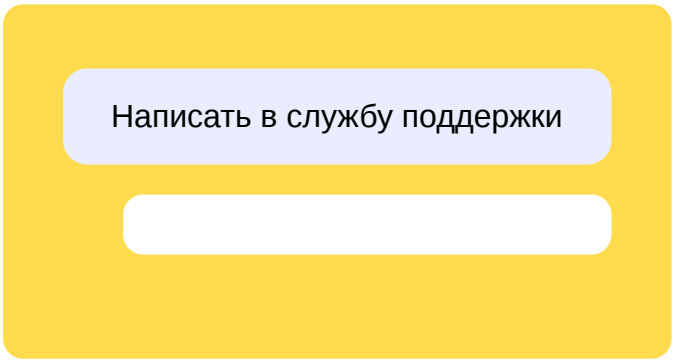
Уведомления

Когда у какого-либо сотрудника появляется доступ к другому почтовому ящику, Яндекс 360 для бизнеса направляет два уведомления об этом: сотруднику, для которого настраивается доступ, и на электронный адрес ящика, к которому предоставляется доступ. Такие же уведомления

отправляются, если вы меняете права доступа для сотрудника или отключаете ему доступ к другому ящику совсем.

Если вы настраиваете доступ сотрудника к почтовому ящику через API, вы можете указать, кому необходимо отправлять письма-уведомления об изменении прав. В запросе это регулируется параметром `notify`, который может принимать следующие значения:

- `all` — сотруднику, для которого настраивается доступ, а также на электронный адрес ящика, к которому предоставляется доступ (значение по умолчанию);
- `delegates` — только сотруднику, для которого настраивается доступ;
- `none` — никому.



Совместный доступ: общие и делегированные ящики

Делегированный ящик — почтовый ящик, к которому настроены права доступа для других сотрудников. Это может быть полезно, если, например, сотрудник уходит в отпуск и нужно отвечать клиентам от его имени.

Общий ящик — ящик, у которого нет конкретного владельца: им пользуются несколько сотрудников, например из одного отдела.

Как предоставить доступ

Управление доступом к общим и делегированным ящикам пока осуществляется только по API.

Порядок настройки и предоставления доступа описан в разделах Делегированные ящики и Общие ящики.

Лимиты

Параметр	Делегированные ящики	Общие ящики
Количество ящиков в организации	200	50
Количество ящиков (не считая своего), к которым может иметь доступ один пользователь	10 (общий лимит)	
Количество пользователей (не считая владельца), которые могут иметь доступ к одному ящику	10	10

Роли сотрудников

- Для доступа сотрудника к другому ящику в веб-интерфейсе Яндекс Почты нужна одна из ролей:
  - *Просмотр ящика в веб-версии* (`shared_mailbox_imap_reader`) — пользователь с такой ролью имеет права на чтение и разметку писем в веб-интерфейсе Яндекс Почты.

- *Редактирование ящика в веб-версии* (`shared_mailbox_imap_editor`) — пользователь с такой ролью имеет права на чтение, разметку и удаление писем в веб-интерфейсе Яндекс Почты.
- *Управление ящиком в веб-версии* (`shared_mailbox_imap_admin`) — пользователь с такой ролью имеет полный доступ на управление содержимым почтового ящика в веб-интерфейсе Яндекс Почты: чтение, разметка и удаление писем, управление папками и настройка ящика.

Права на отправку писем роли этой группы не дают.

- Для доступа сотрудника к другому ящику в почтовых программах (по IMAP) требуется роль
  - *Управление ящиком в IMAP-клиенте* (`shared_mailbox_imap_admin`) — пользователь с такой ролью имеет полный доступ на управление содержимым почтового ящика по протоколу IMAP: чтение, разметка и удаление писем, а также управление папками.

  Права на отправку писем роль не дает.
- Для возможности отправки писем с адреса другого ящика у сотрудника должна быть одна из ролей:
  - *Ограниченная отправка писем* (`shared_mailbox_half_sender`) — пользователь с такой ролью может отправлять письма только в почтовых программах (по SMTP) и только в режиме «Отправить от имени».
  - *Отправка писем* (`shared_mailbox_sender`) — роль позволяет отправлять письма и в веб-интерфейсе Яндекс Почты (доступен режим «Отправить как»), и в почтовых программах по SMTP (доступны режима «Отправить от имени» и «Отправить как»).

  Для отправки писем в веб-интерфейсе Яндекс Почты у сотрудника, помимо роли, которая разрешает отправку писем, должна также быть роль, которая обеспечивает доступ к почтовому ящику.
- Максимальный набор прав содержит роль
  - *Владение ящиком* (`shared_mailbox_owner`) — она предоставляет полные права на ящик, аналогичные тем, которые есть у владельца:
    - управление ящиком в IMAP-клиенте и в веб-интерфейсе Яндекс Почты: чтение, разметка, удаление писем, управление папками;
    - отправка писем по SMTP (в режимах «Отправить от имени» и «Отправить как») и в веб-интерфейсе Яндекс Почты (в режиме «Отправить как»).

  Эта роль включает в себя права всех остальных ролей.

Схематично взаимосвязь ролей указана в таблице:

Группа ролей	**В веб-интерфейсе Яндекс Почты**	**Через почтовые клиенты** (по протоколам IMAP и SMTP)

Доступ к ящику	Требуется одна из ролей: • *Просмотр ящика в веб-версии* • *Редактирование ящика в веб-версии* • *Управление ящиком в веб-версии*	Регулируется единственной ролью: • *Управление ящиком в IMAP-клиенте*
Отправка писем	Регулируется единственной ролью: • *Отправка писем* (режим «Отправить как»)	Требуется одна из ролей: • *Ограниченная отправка писем* (режим «Отправить от имени») • *Отправка писем* (режимы «Отправить от имени» и «Отправить как»)

Когда у какого-либо сотрудника появляется доступ к другому почтовому ящику, Яндекс 360 для бизнеса формирует два уведомления об этом: сотруднику, для которого настраивается доступ, и на электронный адрес ящика, к которому предоставляется доступ.

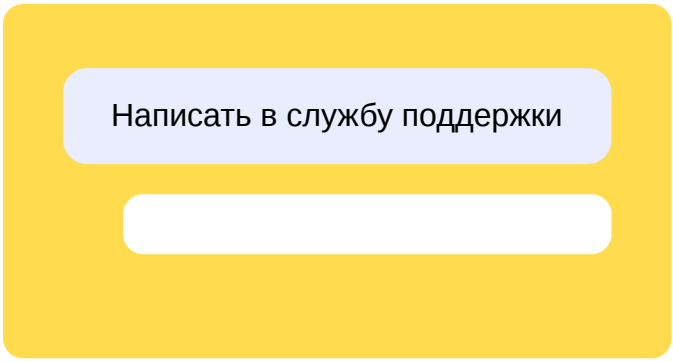
При настройке доступа сотрудника к почтовому ящику через API, вы можете указать, кому необходимо отправлять письма-уведомления об изменении прав. В запросе это регулируется параметром `notify`, который может принимать следующие значения:

- `all` — сотруднику, для которого настраивается доступ, а также на электронный адрес ящика, к которому предоставляется доступ (значение по умолчанию);
- `delegates` — только сотруднику, для которого настраивается доступ;
- `none` — никому.

Как помочь сотруднику настроить почту

Сотрудник может получить доступ к другому ящику через почтовый клиент — Microsoft Outlook, Mozilla Thundebird или Почта для macOS. Настройка этих программ описана в разделе Совместный доступ к ящикам в почтовых программах.

Инструкция по работе с делегированными ящиками в веб-интерфейсе Яндекс Почты содержится в разделе Совместный доступ в Почте: общие и делегированные ящики.


Написать в службу поддержки

Делегированные ящики

Делегированный ящик — ящик, к которому настроены права доступа для других сотрудников. Это может быть полезно, если, например, сотрудник уходит в отпуск и нужно отвечать клиентам от его имени.

Делегировать можно только ящики, аккаунты владельцев которых созданы на домене организации.

Чтобы начать работать с делегированным ящиком:

Количество делегированных ящиков в организации и количество ящиков, к которым может быть доступ у одного сотрудника, ограничено. Об ограничениях читайте в разделе Лимиты на странице Совместный доступ.

Управлять делегированными ящиками можно также по API. Как это сделать

Включить для ящика возможность его делегирования

Когда вы включаете какому-либо ящику возможность делегирования, этот ящик считается делегированным, даже если к нему не настроен доступ других сотрудников. Когда совместный доступ к ящику больше не нужен, выключите возможность его делегирования, чтобы он не влиял на доступный лимит.

Чтобы включить возможность делегирования:

1. В кабинете организации перейдите в раздел **Почта** → **Делегированные ящики**.
2. Нажмите кнопку **+ Добавить**.
3. Начните вводить имя, фамилию или электронный адрес владельца того ящика, которому хотите включить возможность делегирования, и выберите нужного сотрудника из выпадающего списка.
4. Нажмите **Добавить** — выбранный ящик появится в списке делегированных.

Настроить доступ к ящику

Доступ других сотрудников можно настроить только к ящику, который добавлен в список делегированных.

1. В кабинете организации перейдите в раздел **Почта** → **Делегированные ящики**.
2. Выберите делегированный ящик, к которому хотите дать доступ сотрудникам, или наведите указатель на строку с этим ящиком и нажмите ⋮ справа.
3. Нажмите кнопку **Настроить доступ**.
4. Начните вводить имя, фамилию или электронный адрес сотрудника, которому хотите предоставить доступ, и выберите нужного пользователя из выпадающего списка.
5. Отметьте действия, которые будут доступны сотруднику. Описание действий содержится в разделе Возможности пользователей.
6. Нажмите **Сохранить** — сотрудник, которому вы предоставили доступ, появится в списке.

Если достигнут лимит на количество доступных сотруднику ящиков

В этом случае чтобы подключить новый ящик, отключите доступ к любому из уже ненужных

общих или делегированных ящиков.

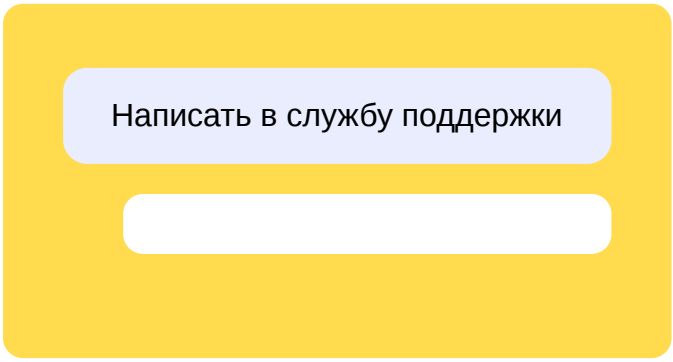
Когда вы настраиваете доступ, отключаете его или меняете список доступных действий сотрудника, Яндекс 360 для бизнеса направляет два письма-уведомления об этом: на почту сотруднику, для которого предоставлен доступ, и на адрес владельца делегированного ящика.

Помочь сотруднику настроить ящик

Порядок настройки делегированных ящиков в веб-интерфейсе Яндекс Почты описан в Справке для пользователей в разделе Совместный доступ в Почте. Как настроить доступ к делегированному ящику через почтовый клиент (Microsoft Outlook, Mozilla Thundebird или Почта для macOS) читайте в Инструкции по настройке почтовых программ.

Выключить для ящика возможность его делегирования

1. В кабинете организации перейдите в раздел **Почта** → **Делегированные ящики**.
2. Наведите указатель на строку с ящиком, для которого хотите выключить возможность делегирования, и нажмите ⋮ справа.
3. Нажмите **Удалить из делегированных**.
4. Подтвердите удаление ящика из списка делегированных — доступ к этому ящику останется только у владельца.



Управление делегированными ящиками по API

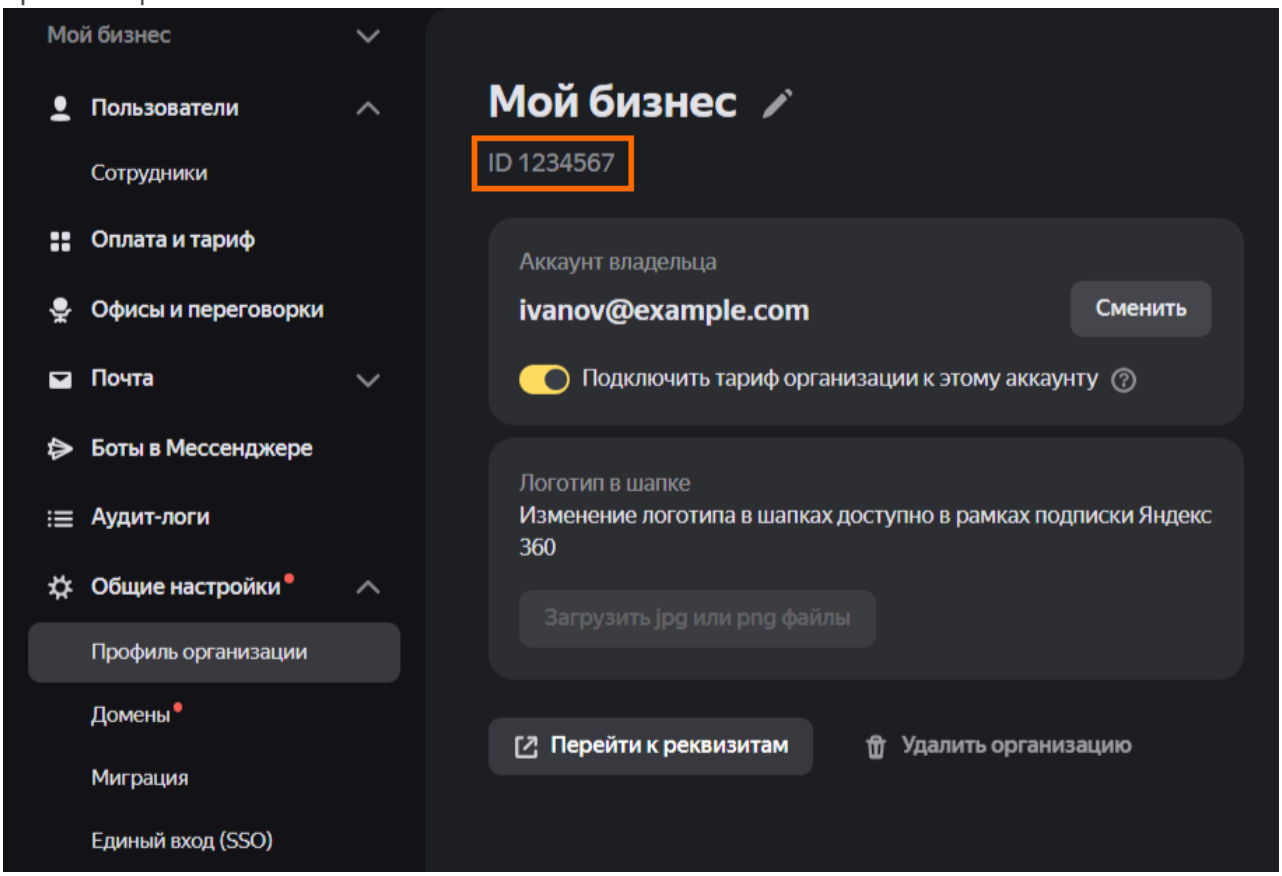
Делегированный ящик — ящик, к которому настроены права доступа для других сотрудников. Это может быть полезно, если, например, сотрудник уходит в отпуск и нужно отвечать клиентам от его имени.

Делегировать можно только ящики, аккаунты владельцев которых созданы на домене организации.

Процесс делегирования

Шаг 1. Подготовьтесь к работе с API

1. Для работы с API вам потребуется OAuth-токен, который можно получить после создания приложения в сервисе Яндекс OAuth.
   - Если у вас еще нет OAuth-приложения, то для его создания и получения токена воспользуйтесь инструкцией на странице Доступ к API. При создании приложения выберите права `ya360_admin:mail_read_shared_mailbox_inventory` и `ya360_admin:mail_write_shared_mailbox_inventory`.
   - Если у вас уже есть OAuth-приложение для работы с API Яндекс 360 для бизнеса, то добавьте ему права на просмотр и изменение настроек доступа к почтовым ящикам, а затем получите новый OAuth-токен по инструкции.
2. Соберите данные, которые потребуются для API-запросов.
   2.1. Определите идентификатор организации: откройте admin.yandex.ru и выберите **Общие настройки** → **Профиль организации**. Идентификатор будет написан под названием организации.

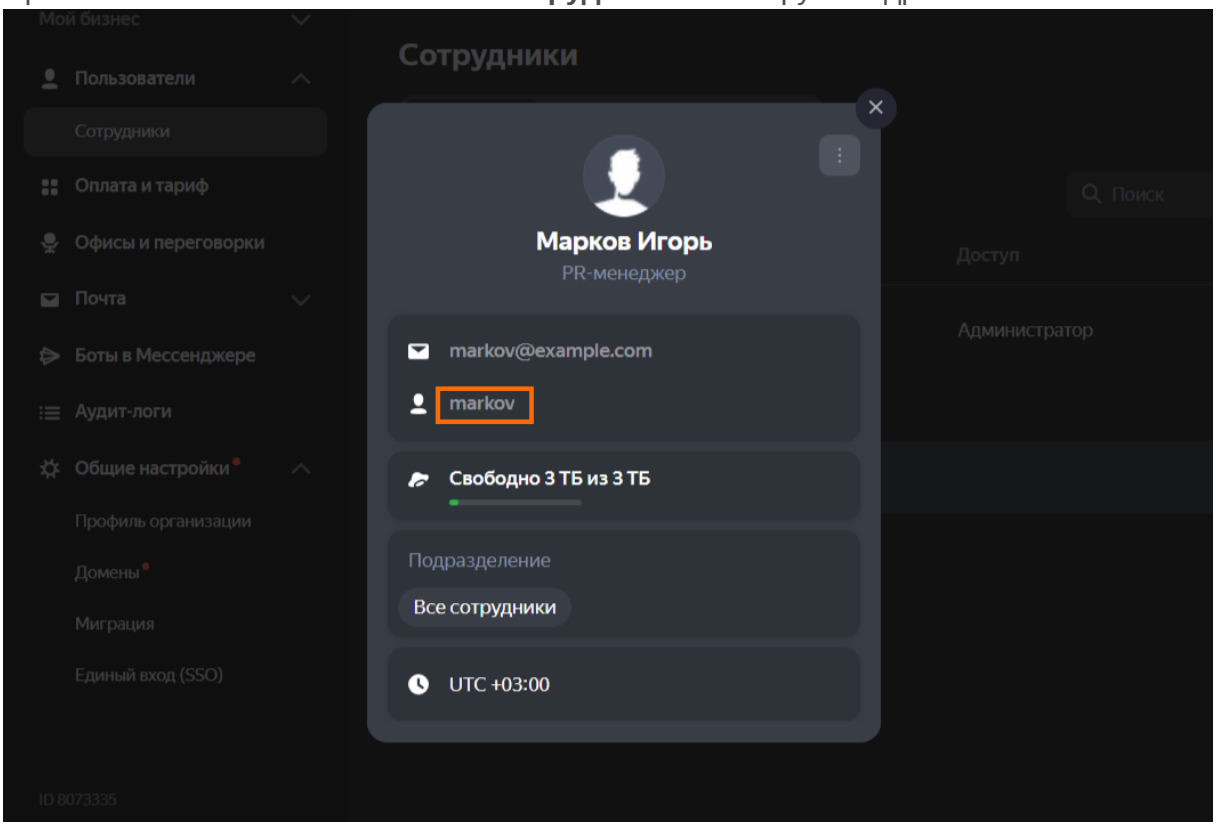


   2.2. Определите идентификатор сотрудника, которому нужно предоставить доступ. Чтобы определить идентификатор:

2.2.1. Выберите **Пользователи** → **Сотрудники**.

2.2.2. Найдите строчку нужного сотрудника и нажмите на его имя.

2.2.3. Правой кнопкой нажмите на **логин сотрудника** и скопируйте адрес ссылки.



2.2.4. Вставьте адрес в любой текстовый редактор. Идентификатор — это часть адреса после `uid=`. Например, из адреса

```
https://staff.yandex.ru/bb?org_id=5487632&uid=2260000054273165
```

получится идентификатор `2260000054273165`.

А можно ли определить идентификаторы сотрудников тоже по API?

Конечно. Есть запрос, который возвращает их список. Посмотреть документацию

Шаг 2. Включите для ящика возможность его делегирования

Примечание

Количество делегированных ящиков в организации ограничено. О существующих ограничениях читайте в разделе Лимиты на странице Совместный доступ.

Когда вы включаете какому-либо ящику возможность делегирования, этот ящик считается делегированным, даже если к нему не настроен доступ других сотрудников. Когда совместный доступ к ящику больше не нужен, выключите возможность его делегирования, чтобы он не влиял на доступный лимит.

1. Подготовьте файл с именем `resource.json`, который будет содержать данные для запроса. Это можно сделать в любом текстовом редакторе. В файле укажите идентификатор владельца ящика, для которого надо включить возможность делегирования, в следующем формате:

   ```
   {
      "resourceId": "{ВЛАДЕЛЕЦ}"
   }
   ```

   где `{ВЛАДЕЛЕЦ}` — идентификатор владельца делегируемого ящика, полученный на шаге 2.2 инструкции «Подготовка к работе с API».

2. С помощью запроса к API включите делегирование ящика:
   - HTTP-метод: `PUT`
   - URL запроса:

     ```
     https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/delegated
     ```

     где `{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1 инструкции «Подготовка к работе с API».

     Пример

     ```
     https://api360.yandex.net/admin/v1/org/1234567/mailboxes/delegated
     ```

   - Заголовки:

     ```
     Authorization: OAuth {OAUTH-TOKEN}
     Content-Type: application/json
     ```

     где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1 инструкции «Подготовка к работе с API».
   - Тело запроса: содержится в файле `resource.json`, созданном на шаге 1 этой инструкции.

   Если вы работаете на Windows, то отправить запрос на включение возможности делегирования ящика можно с помощью команды `curl` такого вида:

   ```
   curl -X PUT -H "Authorization: OAuth {OAUTH-TOKEN}" -H "Content-Type:
   application/json" -d "@resource.json"
   https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/delegated
   ```

   где
   `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1 инструкции «Подготовка к работе

с API»;
`resource.json` — файл с телом запроса, созданный на шаге 1 этой инструкции;
`{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1 инструкции «Подготовка к работе с API».

Я не понимаю, как это сделать

1. Подготовьте команду: скопируйте пример в любой редактор, вставьте в указанные места токен и идентификаторы.
2. Откройте папку, в которой лежит файл `resource.json`.
3. Нажмите на пустое место в адресной строке.
4. Напишите туда `cmd` и нажмите клавишу Enter.
5. Откроется окно «Командная строка». Вставьте в него готовую команду и нажмите Enter.

3. Проанализируйте полученный ответ: в случае успешного выполнения запроса в ответе вы получите статус `200 OK` с указанием идентификатора почтового ящика, возможность делегирования которого включена.

Шаг 3. Предоставьте доступ к ящику

Чтобы к почтовому ящику можно было настроить доступ других сотрудников, сначала нужно включить возможность его делегирования.

Групповые операции на предоставление доступов пока не поддерживаются. За один запрос можно предоставить, изменить или удалить право доступа только для одного сотрудника к одному почтовому ящику. Но вы можете одновременно направить несколько таких запросов.

1. Подготовьте файл с именем `roles.json`, который будет содержать данные для запроса. Это можно сделать в любом текстовом редакторе. В файле укажите роли сотрудника, которому открывается доступ к ящику. Описание ролей приведено в разделе Роли и права доступа.

   Пример файла `roles.json`:

   ```
   {
      "roles": [
         "shared_mailbox_imap_admin",
         "shared_mailbox_half_sender"
      ]
   }
   ```

   В списке должна присутствовать одна из ролей `shared_mailbox_sender` либо `shared_mailbox_owner`, потому что они отвечают за чтение почты.

2. С помощью запроса к API предоставьте доступ сотрудникам к делегированному ящику:
   - HTTP-метод: `POST`
   - URL запроса:

```
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/set/{ВЛАДЕЛЕЦ}?
actorId={СОТРУДНИК С ДОСТУПОМ}&notify={ПАРАМЕТР ОТПРАВКИ УВЕДОМЛЕНИЙ}
```

где
`{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1 инструкции «Подготовка к работе с API»;
`{ВЛАДЕЛЕЦ}` — идентификатор владельца ящика, полученный на шаге 2.2 инструкции «Подготовка к работе с API»;
`{СОТРУДНИК С ДОСТУПОМ}` — идентификатор сотрудника, которому нужно предоставить доступ к ящику, полученный на шаге 2.2 инструкции «Подготовка к работе с API»;
`{ПАРАМЕТР ОТПРАВКИ УВЕДОМЛЕНИЙ}` — параметр, который определяет, кому необходимо отправить письмо-уведомление об изменении прав доступа к ящику. Возможные значения: `all`, `delegates`, `none`. Описание значений параметра приведены в разделе Уведомления.

Пример

```
https://api360.yandex.net/admin/v1/org/1234567/mailboxes/mailboxes/set/2260
actorId=3340000075421587&notify=all
```

- Заголовки:

```
Authorization: OAuth {OAUTH-TOKEN}
Content-Type: application/json
```

где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1 инструкции «Подготовка к работе с API».

- Тело запроса: содержится в файле `roles.json`, созданном на шаге 1 этой инструкции.

Если вы работаете на Windows, то отправить запрос на предоставление доступа ящика можно с помощью команды `curl` такого вида:

```
curl -X POST -H "Authorization: OAuth {OAUTH-TOKEN}" -H "Content-Type:
application/json" -d "@roles.json"
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/set/{ВЛАДЕЛЕЦ}?
actorId={СОТРУДНИК С ДОСТУПОМ}&notify={ПАРАМЕТР ОТПРАВКИ УВЕДОМЛЕНИЙ}
```

где
`{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1 инструкции «Подготовка к работе с API»;
`roles.json` — файл с телом запроса, созданный на шаге 1 этой инструкции;
`{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1 инструкции «Подготовка к работе с API»;
`{ВЛАДЕЛЕЦ}` — идентификатор владельца ящика, полученный на шаге 2.2 инструкции

«Подготовка к работе с API»;
`{СОТРУДНИК С ДОСТУПОМ}` — идентификатор сотрудника, которому нужно предоставить доступ к ящику, полученный на шаге 2.2 инструкции «Подготовка к работе с API»;
`{ПАРАМЕТР ОТПРАВКИ УВЕДОМЛЕНИЙ}` — параметр, который определяет, кому необходимо отправить письмо-уведомление об изменении прав доступа к ящику. Возможные значения: `all`, `delegates`, `none`. Описание значений параметра приведены в разделе Уведомления.

3. Проанализируйте полученный ответ: в случае успешного выполнения запроса в ответе вы получите статус `200 OK` и идентификатор задачи на изменение прав. Сохраните полученный идентификатор.
4. Чтобы убедиться, что доступ предоставлен, выполните еще один запрос, подставив в него идентификатор задачи:

   ```
   curl -X GET -H "Authorization: OAuth {OAUTH-TOKEN}"
   https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/tasks/{ID ЗАДАЧИ}
   ```

   В ответ вы получите статус задачи на изменение прав. Права успешно изменены, если в ответе пришло значение `complete`.

Шаг 4. Помогите сотрудникам с настройкой почты

Инструкция по настройке почтовых клиентов содержится в разделе Совместный доступ к ящикам в почтовых программах.

Изменение права доступа к ящику

Чтобы изменить права доступа сотрудника к ящику, выполните пункты инструкции по предоставлению доступа, заменив перечень ролей в файле `roles.json`.

Отключение от делегированного ящика

Отключить доступ к ящику

Чтобы отключить доступ к ящику конкретному сотруднику, выполните пункты инструкции по предоставлению доступа, только в файле с перечнем доступных ролей `roles.json` укажите пустой список:

```
{
   "roles": []
}
```

Когда вы отзываете доступ у одного сотрудника, ящик продолжает считаться делегированным, даже если доступ к ящику остался только у его владельца. Чтобы ящик перестал быть делегированным, нужно выключить возможность его делегирования.

Выключить для ящика возможность его делегирования

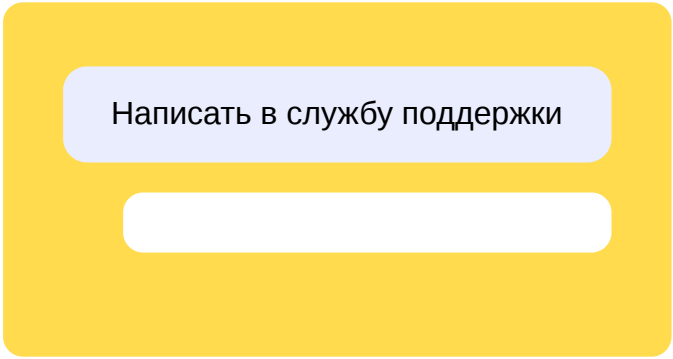
Выключить возможность делегирования ящика можно с помощью DELETE-запроса:

```
curl -X DELETE -H "Authorization: OAuth {OAUTH-TOKEN}"
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/delegated/{ВЛАДЕЛЕЦ}
```

Когда вы выключаете возможность делегирования ящика, у всех сотрудников, которые имеют доступ к этому ящику, такой доступ отзывается.

Документация API

Полное описание всех методов для управления доступом вы найдете в документации.



Общие ящики

Общий ящик — ящик, у которого нет конкретного владельца: им пользуются несколько сотрудников, например из одного отдела.

Создать общий ящик в организации можно, только если у нее подключен домен. Как подключить домен

Чтобы начать работать с общим ящиком:

Количество общих ящиков в организации и количество сотрудников, у которых может быть доступ к одному общему ящику, ограничено. Об ограничениях читайте в разделе Лимиты на странице Совместный доступ.

Управлять общими ящиками можно также по API. Как это делать

Создать ящик

1. В кабинете организации перейдите в раздел **Почта** → **Общие ящики**.
2. Нажмите кнопку **+ Создать**.
3. Задайте параметры общего ящика:
   - Название — имя ящика, которое будут видеть отправители и получатели писем. Оно должно быть уникальным для вашей организации и содержать не менее двух символов.
   - Логин — часть электронного адреса общего ящика до символа `@`. Адрес будет выглядеть так: `login@your-domain.ru`, где `login` — логин, который вы придумаете, `your-domain.ru` — домен вашей организации.
   - Описание — краткая информацию об общем ящике, которая поможет понять, для чего он используется.
4. Нажмите **Создать** — выбранный ящик появится в списке.

Название и описание общего ящика можно в дальнейшем изменить. Логин ящика отредактировать нельзя.

Настроить доступ к ящику

1. В кабинете организации перейдите в раздел **Почта** → **Общие ящики**.
2. Выберите общий ящик, к которому хотите дать доступ сотрудникам, или наведите указатель на строку с этим ящиком и нажмите справа.
3. Нажмите **Настроить доступ**.
4. Начните вводить имя, фамилию или электронный адрес сотрудника, которому хотите предоставить доступ, и выберите нужного пользователя из выпадающего списка.
5. Отметьте действия, которые будут доступны сотруднику. Описание действий содержится в разделе Возможности пользователей.
6. Нажмите **Сохранить**.

Если достигнут лимит на количество доступных сотруднику ящиков

В этом случае чтобы подключить новый ящик, отключите доступ к любому из уже ненужных

общих или делегированных ящиков.

Когда вы настраиваете доступ к общему ящику, отключаете его или меняете список доступных действий сотрудника, Яндекс 360 для бизнеса направляет два письма-уведомления об этом: на почту сотруднику, для которого предоставлен доступ, и на адрес общего ящика, к которому предоставлен доступ.

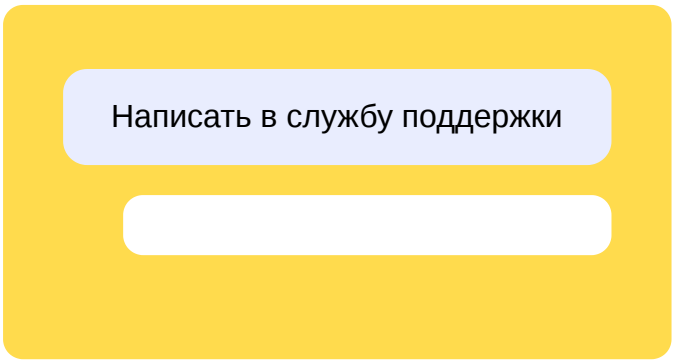
Помочь сотруднику настроить ящик

Порядок настройки общих ящиков в веб-интерфейсе Яндекс Почты описан в Справке для пользователей в разделе Совместный доступ в Почте. Как настроить доступ к общему ящику через почтовый клиент (Microsoft Outlook, Mozilla Thundebird или Почта для macOS) читайте в Инструкции по настройке почтовых программ.

Удалить ящик

При удалении общего ящика все письма в нем удаляются навсегда, восстановить их не получится. Чтобы удалить общий ящик со всем содержимым:

1. В кабинете организации перейдите в раздел **Почта** → **Общие ящики**.
2. Выберите в списке ящик, который хотите удалить, или наведите указатель на строку с этим ящиком
3. Справа от названия ящика нажмите ⋮.
4. Выберите **Удалить**.
5. Подтвердите удаление.



Управление общими ящиками по API

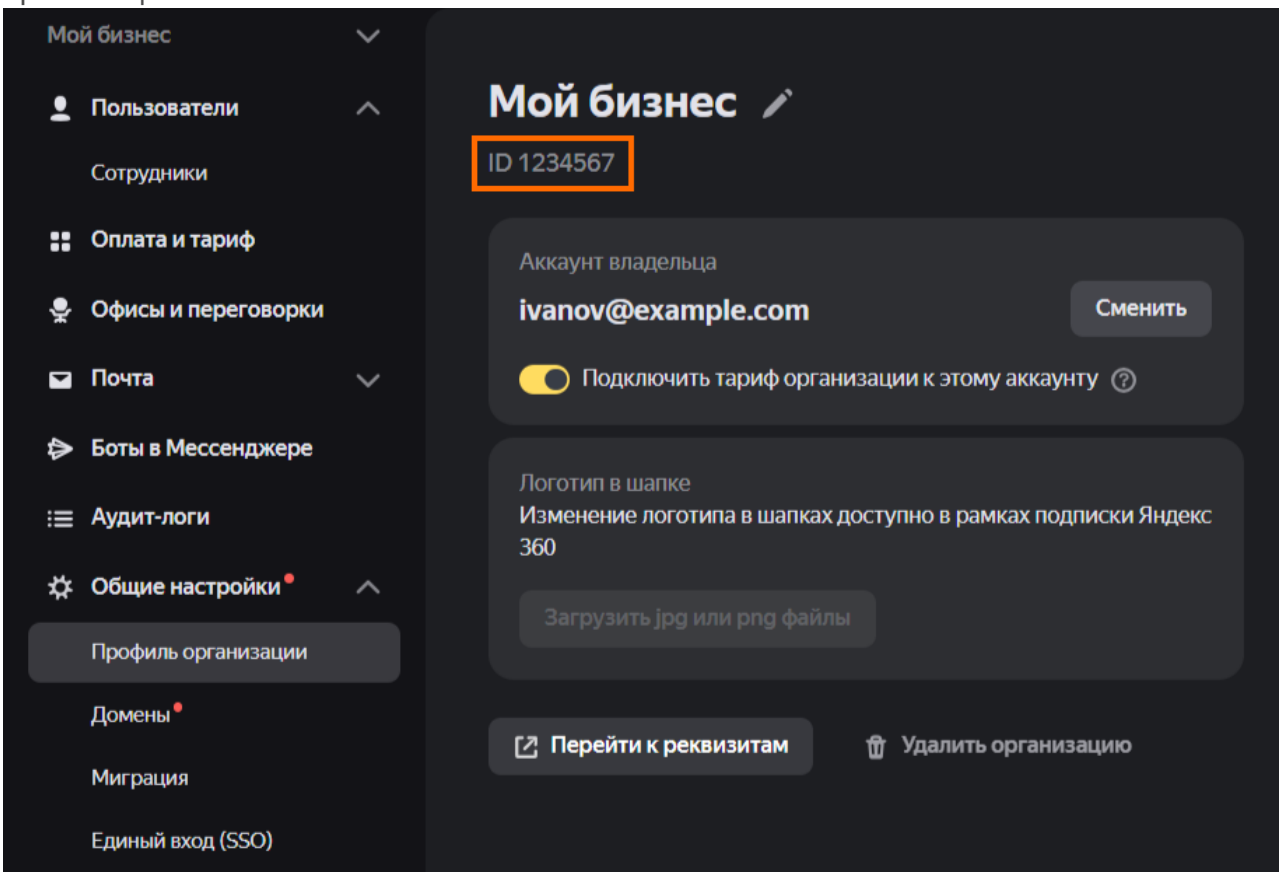
Общий ящик — ящик, у которого нет конкретного владельца: им пользуются несколько сотрудников, например из одного отдела.

Если у организации не подключен домен, создать общие ящики не получится. Как подключить домен

Создание и настройка общего ящика

Шаг 1. Подготовьтесь к работе с API

1. Для работы с API вам потребуется OAuth-токен, который можно получить после создания приложения в сервисе Яндекс OAuth.
   - Если у вас еще нет OAuth-приложения, то для его создания и получения токена воспользуйтесь инструкцией на странице Доступ к API. При создании приложения выберите права `ya360_admin:mail_read_shared_mailbox_inventory` и `ya360_admin:mail_write_shared_mailbox_inventory`.
   - Если у вас уже есть OAuth-приложение для работы с API Яндекс 360 для бизнеса, то добавьте ему права на просмотр и изменение настроек доступа к почтовым ящикам, а затем получите новый OAuth-токен по инструкции.
2. Соберите данные, которые потребуются для API-запросов.
   2.1. Определите идентификатор организации: откройте admin.yandex.ru и выберите **Общие настройки** → **Профиль организации**. Идентификатор будет написан под названием организации.

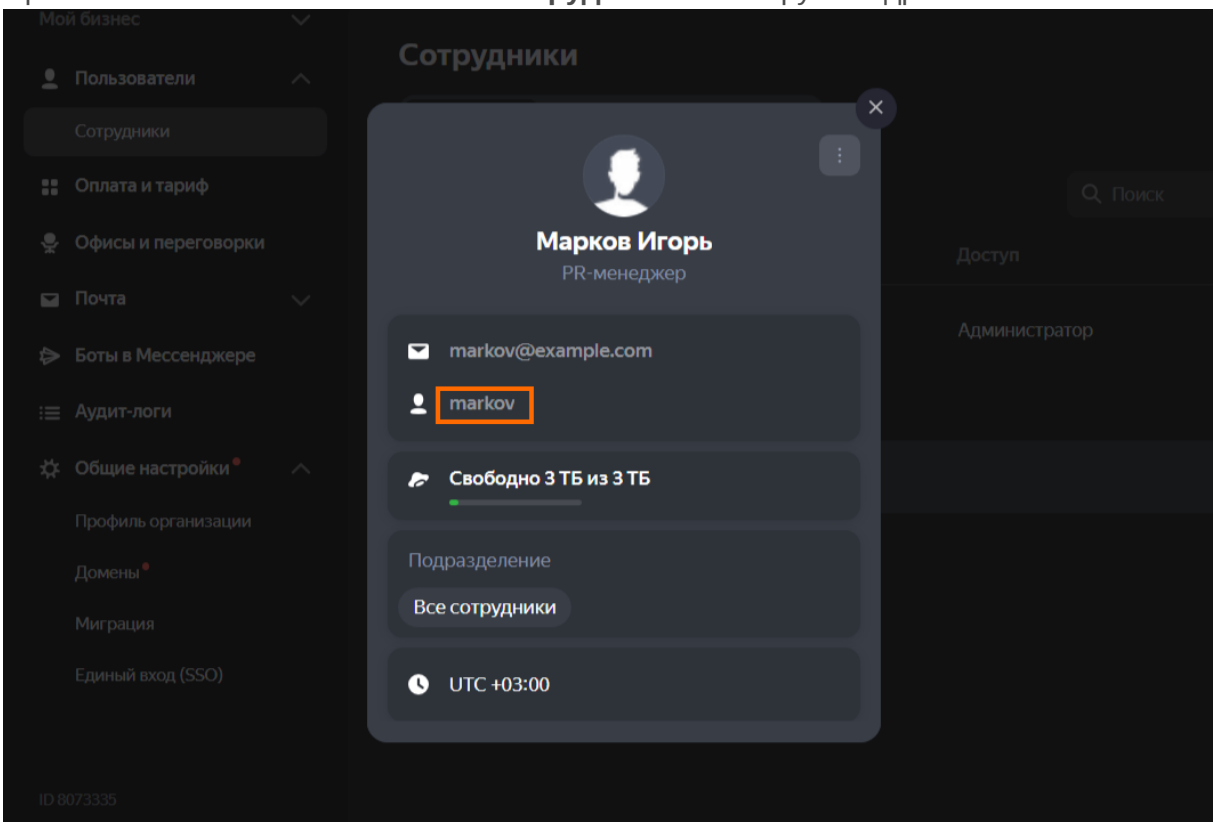


   2.2. Определите идентификатор сотрудника, которому нужно предоставить доступ. Чтобы определить идентификатор:

2.2.1. Выберите **Пользователи** → **Сотрудники**.

2.2.2. Найдите строчку нужного сотрудника и нажмите на его имя.

2.2.3. Правой кнопкой нажмите на **логин сотрудника** и скопируйте адрес ссылки.



2.2.4. Вставьте адрес в любой текстовый редактор. Идентификатор — это часть адреса после `uid=`. Например, из адреса

```
https://staff.yandex.ru/bb?org_id=5487632&uid=2260000054273165
```

получится идентификатор `2260000054273165`.

А можно ли определить идентификаторы сотрудников тоже по API?

Конечно. Есть запрос, который возвращает их список. Посмотреть документацию

Шаг 2. Создайте общий ящик

1. Подготовьте файл с именем `parameters.json`, который будет содержать данные для запроса. Это можно сделать в любом текстовом редакторе. В файле укажите параметры создаваемого общего ящика в следующем формате:

```
{
   "email": "{АДРЕС}",
   "name": "{ИМЯ}",
   "description": "{ОПИСАНИЕ}"
}
```

где
`{АДРЕС}` — адрес электронной почты общего ящика;
`{ИМЯ}` — имя общего ящика;
`{ОПИСАНИЕ}` — краткое описание общего ящика.

2. Сформируйте и отправьте запрос на создание общего ящика:
   - HTTP-метод: `PUT`
   - URL запроса:

     ```
     https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/shared
     ```

     где `{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1 инструкции «Подготовка к работе с API».

     Пример

     ```
     https://api360.yandex.net/admin/v1/org/1234567/mailboxes/shared
     ```

   - Заголовки:

     ```
     Authorization: OAuth {OAUTH-TOKEN}
     Content-Type: application/json
     ```

     где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1 инструкции «Подготовка к работе с API».
   - Тело запроса: содержится в файле `parameters.json`, созданном на шаге 1 этой инструкции.

Если вы работаете на Windows, то отправить запрос на разрешение делегирования ящика можно с помощью команды `curl` такого вида:

```
curl -X PUT -H "Authorization: OAuth {OAUTH-TOKEN}" -H "Content-Type:
application/json" -d "@parameters.json"
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/shared
```

где
`{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1 инструкции «Подготовка к работе с API»;
`parameters.json` — файл с телом запроса, созданный на шаге 1 этой инструкции;
`{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1 инструкции «Подготовка к работе с API».

Я не понимаю, как это сделать

1. Подготовьте команду: скопируйте пример в любой редактор, вставьте в указанные места токен и идентификаторы.
2. Откройте папку, в которой лежит файл `parameters.json`.
3. Нажмите на пустое место в адресной строке.
4. Напишите туда `cmd` и нажмите клавишу Enter.
5. Откроется окно «Командная строка». Вставьте в него готовую команду и нажмите Enter.

3. Проанализируйте полученный ответ: в случае успешного выполнения запроса в ответе вы получите статус `200 OK` с указанием идентификатора созданного общего ящика. Сохраните этот идентификатор.

Шаг 3. Предоставьте доступ

Групповые операции на предоставление доступов пока не поддерживаются. За один запрос можно предоставить, изменить или удалить право доступа только для одного сотрудника к одному почтовому ящику. Но вы можете одновременно направить несколько таких запросов.

1. Подготовьте файл с именем `roles.json`, который будет содержать данные для запроса. Это можно сделать в любом текстовом редакторе. В файле укажите роли сотрудника, которому открывается доступ к ящику. Описание ролей приведено в разделе Роли и права доступа.

   Пример файла `roles.json`:

   ```
   {
      "roles": [
         "shared_mailbox_imap_admin",
         "shared_mailbox_half_sender"
      ]
   }
   ```

   В списке должна присутствовать одна из ролей `shared_mailbox_sender` либо `shared_mailbox_owner`, потому что они отвечают за чтение почты.
2. С помощью запроса к API предоставьте доступ сотрудникам к общему ящику:
   - HTTP-метод: `POST`
   - URL запроса:

     ```
     https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/set/{ЯЩИК}?
     actorId={СОТРУДНИК С ДОСТУПОМ}&notify={ПАРАМЕТР ОТПРАВКИ УВЕДОМЛЕНИЙ}
     ```

     где
     `{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1 инструкции «Подготовка к работе с API»;
     `{ЯЩИК}` — идентификатор общего ящика, созданного по инструкции Создание ящика;
     `{СОТРУДНИК С ДОСТУПОМ}` — идентификатор сотрудника, которому нужно предоставить доступ к ящику, полученный на шаге 2.2 инструкции «Подготовка к работе с API»;

`{ПАРАМЕТР ОТПРАВКИ УВЕДОМЛЕНИЙ}` — параметр, который определяет, кому необходимо отправить письмо-уведомление об изменении прав доступа к ящику. Возможные значения: `all`, `delegates`, `none`. Описание значений параметра приведены в разделе Уведомления.

Пример

```
https://api360.yandex.net/admin/v1/org/1234567/mailboxes/mailboxes/set/2260
actorId=3340000075421587&notify=all
```

- Заголовки:

```
Authorization: OAuth {OAUTH-TOKEN}
Content-Type: application/json
```

где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1 инструкции «Подготовка к работе с API».

- Тело запроса: содержится в файле `roles.json`, созданном на шаге 1 этой инструкции.

Если вы работаете на Windows, то отправить запрос на разрешение делегирования ящика можно с помощью команды `curl` такого вида:

```
curl -X POST -H "Authorization: OAuth {OAUTH-TOKEN}" -H "Content-Type:
application/json" -d "@roles.json"
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/set/{ЯЩИК}?
actorId={СОТРУДНИК С ДОСТУПОМ}&notify={ПАРАМЕТР ОТПРАВКИ УВЕДОМЛЕНИЙ}
```

где
`{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 1 инструкции «Подготовка к работе с API»;
`roles.json` — файл с телом запроса, созданный на шаге 1 этой инструкции;
`{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.1 инструкции «Подготовка к работе с API»;
`{ЯЩИК}` — идентификатор общего ящика, созданного по инструкции Создание ящика;
`{СОТРУДНИК С ДОСТУПОМ}` — идентификатор сотрудника, которому нужно предоставить доступ к ящику, полученный на шаге 2.2 инструкции «Подготовка к работе с API»;
`{ПАРАМЕТР ОТПРАВКИ УВЕДОМЛЕНИЙ}` — параметр, который определяет, кому необходимо отправить письмо-уведомление об изменении прав доступа к ящику. Возможные значения: `all`, `delegates`, `none`. Описание значений параметра приведены в разделе Уведомления.

3. Проанализируйте полученный ответ: в случае успешного выполнения запроса в ответе вы получите статус `200 OK` и идентификатор задачи на изменение прав. Сохраните полученный идентификатор.
4. Чтобы убедиться, что доступ предоставлен, выполните еще один запрос, подставив в него идентификатор задачи:

```
curl -X GET -H "Authorization: OAuth {OAUTH-TOKEN}"
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/tasks/{ID ЗАДАЧИ}
```

В ответ вы получите статус задачи на изменение прав. Права успешно изменены, если в ответе пришло значение `complete`.

Шаг 4. Помогите сотрудникам с настройкой почты

Инструкция по настройке почтовых клиентов содержится в разделе Совместный доступ к ящикам в почтовых программах.

Отключение доступа

Чтобы отключить доступ к ящику конкретному сотруднику, выполните пункты инструкции по предоставлению доступа, только в файле с перечнем доступных ролей `roles.json` укажите пустой список:

```
{
   "roles": []
}
```

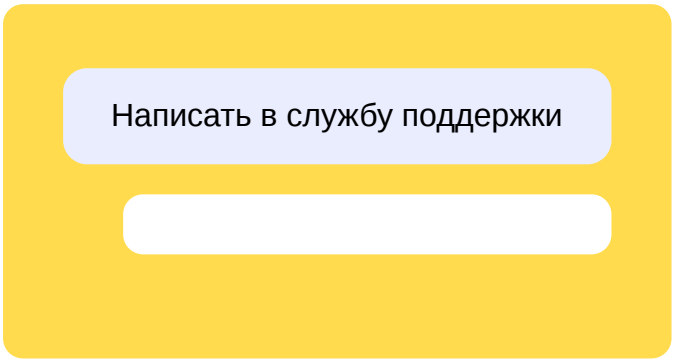
Удаление ящика

Удалить общий ящик можно с помощью DELETE-запроса:

```
curl -X DELETE -H "Authorization: OAuth {OAUTH-TOKEN}"
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mailboxes/shared/{ЯЩИК}
```

Документация API

Полное описание всех методов для управления доступом вы найдете в документации.



Правила обработки писем

Эта возможность доступна в тарифах **Основной**, **Продвинутый** и всех версиях тарифа **Корпоративный** из новой линейки, а также тарифах **Оптимальный** и **Расширенный** из старой.

Администраторы организации и менеджеры правил для писем могут настраивать правила, по которым Почта будет обрабатывать письма сотрудников автоматически: пересылать на другой адрес или удалять из ящика получателя. Настроить правила можно только для ящиков на домене организации.

Перед включением обработки писем обязательно проконсультируйтесь с юристом своей организации. Он скажет, нужно ли в вашем случае собирать согласия сотрудников на доступ к данным.

Правила можно создавать, редактировать, перемещать в списке, чтобы менять приоритет, и удалять, если они больше не нужны.

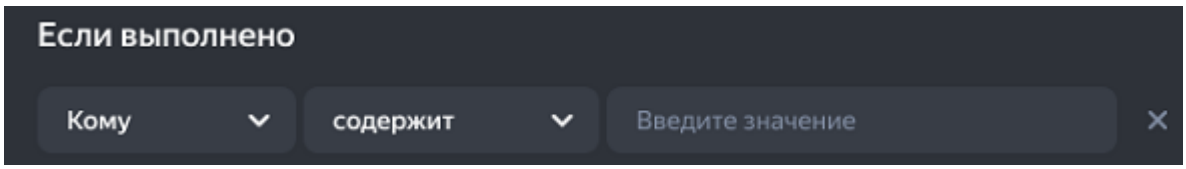
Ограничения

- Правила начинают работать через 10 минут после их создания. Если вы отредактируете условия или порядок выполнения правил, они начнут работать по-другому также через 10 минут.
- Всего можно добавить не более 200 правил и не более чем для 30 действий одновременно. Например, вы можете добавить одно правило, по которому в ящике сотрудника удаляются письма, и второе, по которому письма пересылаются на 29 других адресов, — это 30 действий в сумме.

Создать простое правило

Например, сотрудник ушел в отпуск, и нужно дублировать все письма, которые ему приходят, на ящик другого коллеги.

1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Почта** → **Правила для писем**.
3. Нажмите кнопку **Добавить**.
4. В блоке **Если выполнено** составьте условие для обработки писем. Выберите **Кому** → **содержит** и укажите электронную почту того, кто будет в отпуске.



Выберите параметр

Насколько строго должно соблюдаться условие

Введите значение выбранного параметра

Правило может состоять из одного или нескольких условий. В каждом условии есть параметр, его значение и то, насколько строго выполняется условие. Подробнее о том, как правильно составить условие, см. в специальной статье.

5. В блоке **То это письмо** выберите **Переслать на адрес** и укажите адрес коллеги, который будет получать письма.
6. Нажмите кнопку **Создать правило**.

Создать сложное правило

Добавить несколько условий

Добавить вложенную группу условий

Добавить несколько условий

Например, сотрудник получает письма от коллег и коммерческие предложения от клиентов компании. Чтобы в его отпуске пересылать другому коллеге только коммерческие предложения, настройте два условия, которые будут выполняться одновременно:

1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Почта** → **Правила для писем**.
3. Нажмите кнопку **Добавить**.
4. В блоке **Если выполнено** выберите **Все условия**, чтобы условия выполнялись одновременно.
5. Составьте условия для обработки писем (задаются так же, как для простых правил). Выберите **Кому** → **содержит** и укажите электронную почту того, кто будет в отпуске.
6. Нажмите кнопку + **условие**.
7. Задайте второе условие: **Тема** → **содержит** и введите «коммерческое предложение».
8. В блоке **То это письмо** выберите **Переслать на адрес** и укажите адрес коллеги, который будет получать письма.
9. Нажмите кнопку **Создать правило**.

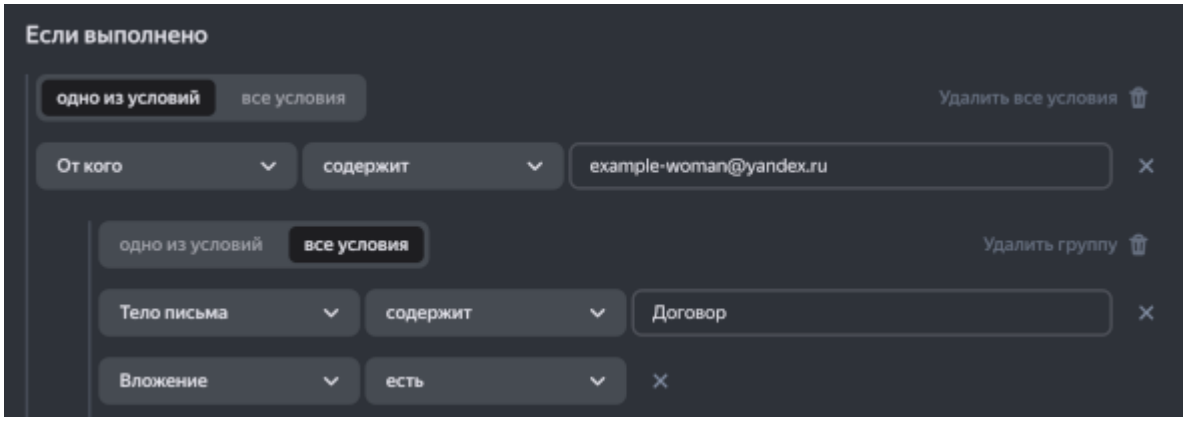
Добавить вложенную группу условий

Группы пригодятся, чтобы объединить условия, которые должны выполняться одновременно. Можно добавлять группы до четырех уровней вложенности.

Например, сотруднику приходят письма от коллег, от конкретного клиента компании, а еще он отвечает всем клиентам на вопросы о договорах (если в письме приложен файл). Сотрудник уходит в отпуск, и вы хотите настроить правила так, чтобы письма от конкретного клиента компании, а также вопросы о договорах пересылались другому сотруднику. Для этого нужно добавить одно обычное условие, а также два условия, объединенных в группу:

1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Почта** → **Правила для писем**.
3. Нажмите кнопку **Добавить**.

4. В блоке **Если выполнено** выберите **одно из условий**.
5. Составьте условия для обработки писем. Выберите **От кого** → **содержит** и укажите электронную почту клиента, от которого приходят письма.
6. Нажмите кнопку + **группа условий**.
7. Задайте условия:
   - **Тело письма** → **содержит** и введите «Договор»;
   - **Вложение** → **есть**.



8. В блоке **То это письмо** выберите **Переслать на адрес** и укажите адрес коллеги, который будет получать письма вместо того, кто в отпуске.
9. Нажмите кнопку **Создать правило**.

Задать порядок выполнения правил

Правила выполняются по порядку: чем выше правило в списке, тем раньше оно выполнится. Если для нескольких правил с одинаковыми условиями были заданы действия, которые не могут выполняться одновременно, то сработает правило, расположенное выше в списке.

Переместить правило

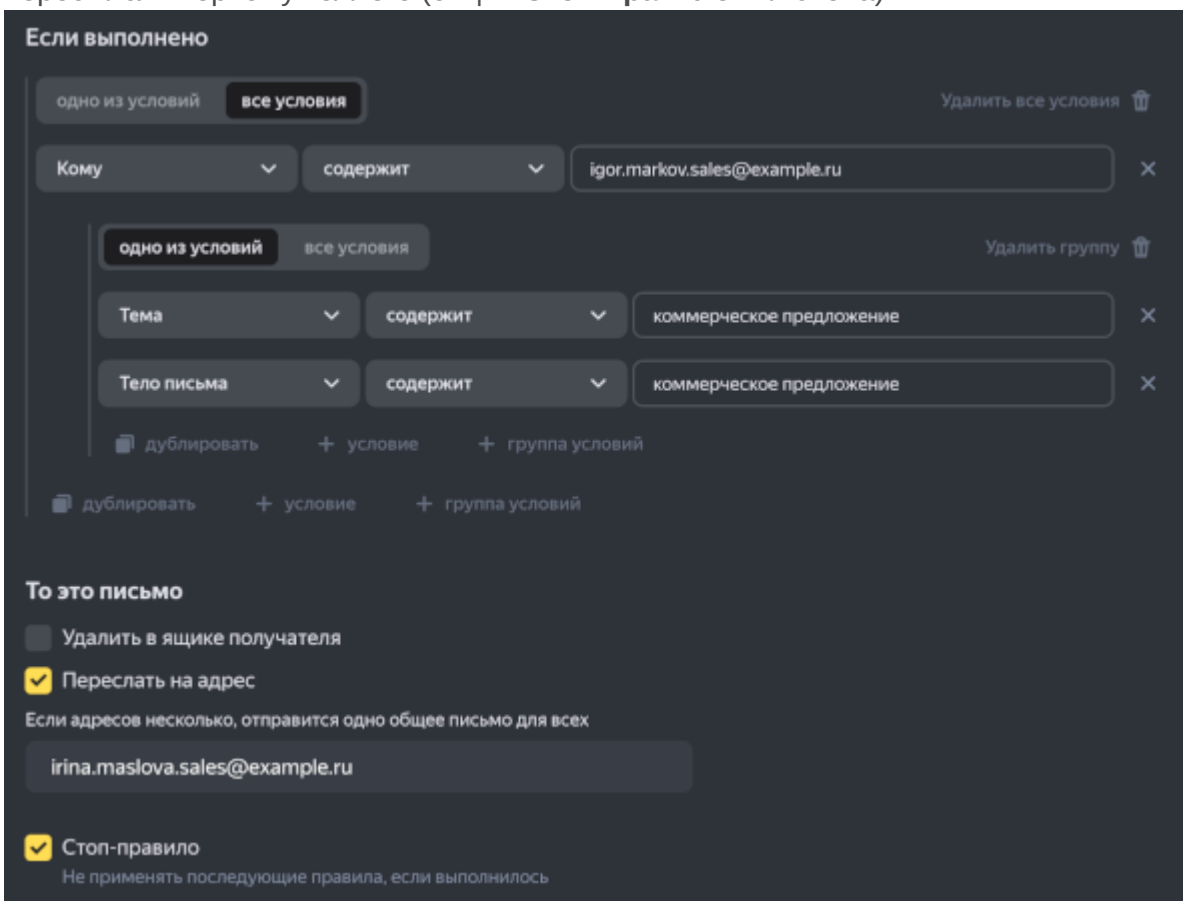
1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Почта** → **Правила для писем**.
3. Нажмите кнопку **Редактировать**.
4. Слева от правила нажмите значок ⠿ и, удерживая его, переместите правило на позицию выше или ниже.
5. Нажмите кнопку **Сохранить изменения**.

Включить стоп-правило

Если правило, в котором включена опция **Стоп-правило**, сработает, то правила, расположенные ниже, выполняться не будут. Если правило с опцией не сработает, то выполнятся все правила, расположенные ниже.

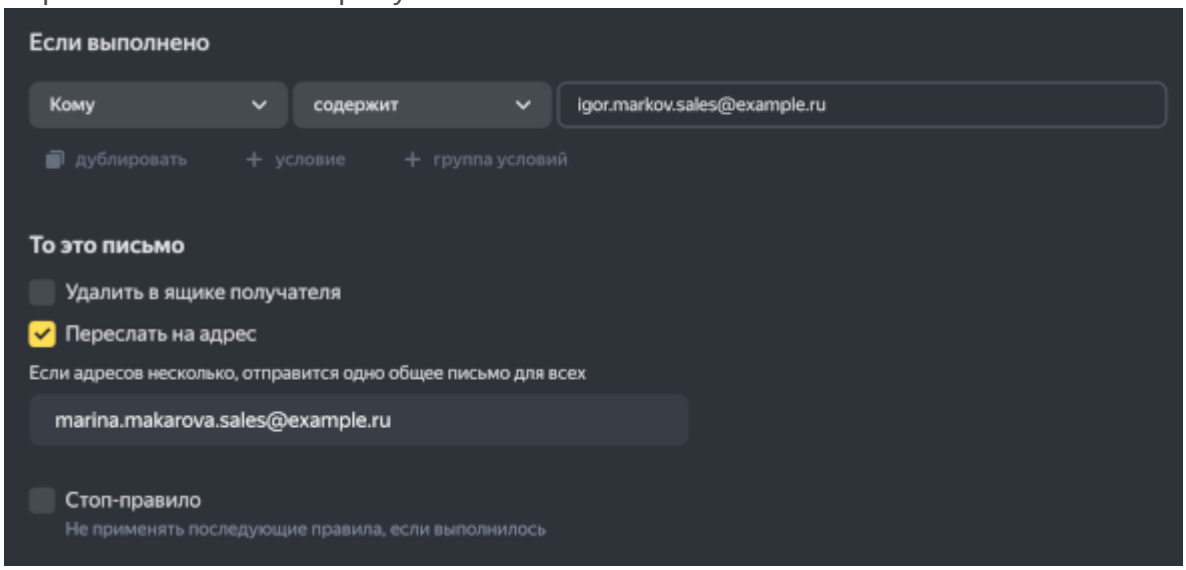
Например, сотрудник получает коммерческие предложения от клиентов компании и письма от коллег. На время отпуска его обязанности разделили: один коллега будет работать с коммерческими предложениями, а другой — отвечать на остальные письма. Создайте два разных правила:

1. Письма для сотрудника в отпуске, которые содержат фразу «коммерческое предложение», пересылать первому коллеге (опция **Стоп-правило** включена):



   Задайте правило и нажмите кнопку **Создать правило**.

2. Пересылать письма второму коллеге:



   Задайте правило и нажмите кнопку **Создать правило**. Так как это правило расположено ниже того, в котором включена опция **Стоп-правило**, пересылаться будут все письма, кроме коммерческих предложений.

Редактировать правило

1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Почта** → **Правила для писем**.
3. Нажмите кнопку **Редактировать**.
4. Справа от нужного правила нажмите значок .

5. Отредактируйте правило и нажмите кнопку **Сохранить изменения**.

Удалить правило

1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Почта** → **Правила для писем**.
3. Нажмите кнопку **Редактировать**.
4. Справа от правила нажмите значок . Чтобы удалить все действующие правила, нажмите кнопку **Удалить все**.
5. Нажмите кнопку **Сохранить изменения**.

Написать в службу поддержки

Нейрофильтр в Почте

Нейрофильтр выбирает письма среди входящих за последние 7 дней и коротко пересказывает их суть. Администраторы организации могут включать Нейрофильтр в ящиках сотрудников, чтобы важные письма всегда были на виду. Как работать с Нейрофильтром в Почте

Это безопасно

Нейрофильтр не запоминает содержание писем, не обучается на полученных данных и никуда их не передает.

Ограничения

Включать и отключать Нейрофильтр можно только для ящиков на домене организации.

Как включить

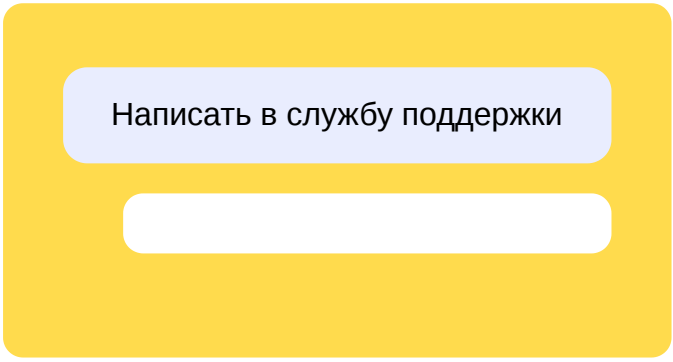
1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Почта** → **Настройки**.
3. В блоке **Нейрофильтр** включите опцию **Нейрофильтр в Почте**.
4. Нажмите **Сохранить**.

Нейрофильтр начнет показывать пересказы важных писем в течение часа.

Как отключить

Вы можете отключить Нейрофильтр во всех ящиках на вашем домене — он перестанет работать, даже если в настройках Почты сотрудников опция Нейрофильтра будет включена.

1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Почта** → **Настройки**.
3. В блоке **Нейрофильтр** выключите опцию **Нейрофильтр в Почте**.
4. Нажмите **Сохранить**.



Как верно составить условие

Чтобы правило работало корректно, необходимо верно составить его условие. В условии указываются параметр, строгость выполнения условия и значение параметра.

Параметры и значения

Параметр	Что указать в значении параметра	Пример значения параметра
От кого	Адрес отправителя	igor.markov.sales@example.ru
Кому или копия	Адрес получателя или адрес получателя копии письма	irina.maslova.sales@example.ru
Кому	Адрес получателя	irina.maslova.sales@example.ru
Копия	Адрес получателя копии письма	marketing@example.ru
Тема	Тема письма	Встреча с руководителем
Тело письма	Текст письма	Завтра обсуждаем новый план продаж.
Вложение	Название вложенного файла	plan.pdf
Заголовок	Служебная информация о письме	To: irina.maslova.sales@example.ru

Строгость выполнения условий

Существует шесть степеней строгости:

совпадает

Какие письма попадут в фильтр	Для каких параметров применимо	Пример выполнения
Письма, параметры которых строго соответствуют указанному значению или в адресе, или в имени пользователя.	**Кому** **От кого** **Копия** **Кому или копия**	Если для параметра **От кого** задано значение адреса `igor.markov.sales@example.ru` или значение имени «Игорь Марков», то в обоих случаях в фильтр попадет письмо от отправителя «Игорь Марков» с адресом `igor.markov.sales@example.ru`.
Письма, параметры которых строго соответствуют указанному значению.	**Тема** **Тело письма** **Вложение** **Заголовок**	Если для параметра **Тема** задано значение «план продаж», то в фильтр попадет письмо с темой «План продаж».
Письма, текст которых соответствует указанному значению, а также содержит сочетание с указанным значением в оформленном или неоформленном виде.	**Тело письма**	Если для параметра **Тело письма** задано значение «график работы», то в фильтр попадут и письма с текстом «График работы на февраль», и письма с текстом «Мы переходим на новый ***график работы***».

не совпадает с

Какие письма попадут в фильтр	Для каких параметров применимо	Пример выполнения

Письма, параметры которых строго не соответствуют указанному значению или в адресе, или в имени пользователя.	**Кому** **От кого** **Копия** **Кому или копия**	Если для параметра **От кого** задано значение адреса `igor.markov.sales@example.ru` или значение имени «Игорь Марков», то в обоих случаях в фильтр попадут все письма, кроме писем от отправителя «Игорь Марков» с адресом `igor.markov.sales@example.ru`.
Письма, параметры которых строго не соответствуют указанному значению.	**Тема** **Тело письма** **Вложение** **Заголовок**	Если для параметра **Тема** задано значение «поставщик», то в фильтр попадут все письма, кроме писем с темами «Новый поставщик» и «Поставщик сменил реквизиты».
Письма, текст которых не соответствует указанному значению, а также не содержит сочетание с указанным значением в оформленном или неоформленном виде.	**Тело письма**	Если для параметра **Тело письма** задано значение «договор поставки», то в фильтр попадут все письма, кроме писем с текстом «Подпишите договор поставки» и «***Договор поставки № 1152-В***».

содержит

Какие письма попадут в фильтр	Для каких параметров применимо	Пример выполнения

Письма, параметры которых содержат указанное значение или сочетание с этим значением в адресе или в имени пользователя.	**Кому** **От кого** **Копия** **Кому или копия**	Если для параметра **От кого** задано значение адреса `igor.markov.sales` или значение имени «Игорь», то в обоих случаях в фильтр попадет письмо от отправителя «Игорь Марков» с адресом `igor.markov.sales@example.ru`.
Письма, параметры которых содержат сочетания с этим значением и его словоформы.	**Тема** **Тело письма** **Вложение** **Заголовок**	Если для параметра **Тема** задано значение «Договор поставки», то в фильтр попадут письма с темами «Договор поставки» и «Соглашение к договору поставки». Письма с темами «Договор от Маркова» и «Подпишите договор» в фильтр не попадут.
Письма, текст которых содержит указанное	**Тело письма**	Если для параметра **Тело письма** задано значение «договор», то в фильтр попадут

не содержит

Какие письма попадут в фильтр	**Для каких параметров применимо**	**Пример выполнения**
Письма, параметры которых не содержат указанное значение или сочетание с этим значением в адресе или в имени пользователя.	**Кому** **От кого** **Копия** **Кому или копия**	Если для параметра **От кого** задано значение адреса `igor.markov.sales` или значение имени «Игорь», то в обоих случаях в фильтр попадут все письма, кроме писем от отправителя «Игорь Марков» с адресом `igor.markov.sales@exapmle.ruuacomcom.trkzuz`.

Письма, параметры которых не содержат сочетания с этим значением и его словоформы.	**Тема** **Тело письма** **Вложение** **Заголовок**	Если для параметра **Тема** задано значение «Договор поставки», то в фильтр попадут письма с темами «Договор подряда» и «Сегодня заключаем договор». Письма с темами «Договор поставки» и «Подписание договора поставки» в фильтр не попадут.
Письма, текст которых не содержит указанное значение или сочетание с этим значением в оформленном или неоформленном виде.	**Тело письма**	Если для параметра **Тело письма** задано значение «Договор поставки», то в фильтр попадут все письма, кроме писем с текстом «***Договор поставки № 1152-В***» и «Сегодня мы подпишем договор поставки».

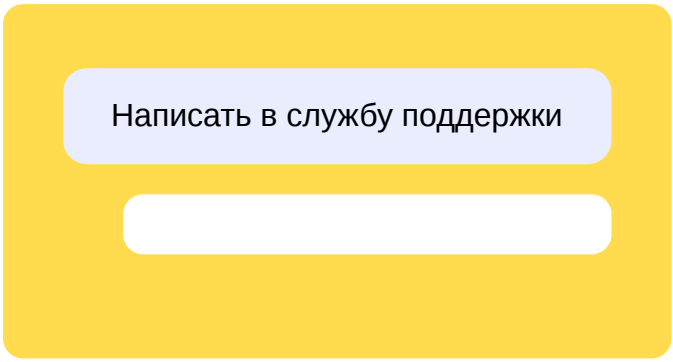
есть

Какие письма попадут в фильтр	Для каких параметров применимо	Пример выполнения
Письма, параметры которых содержат любое значение, кроме пустого.	**Заголовок** **Вложение**	Если для параметра **Вложение** или **Заголовок** задано условие **есть**, то в фильтр попадут все письма с вложениями или заголовком.

нет

Какие письма попадут в фильтр	Для каких параметров применимо	Пример выполнения

Письма, параметры которых содержат	**Заголовок**	Если для параметра **Вложение** или **Заголовок** задано условие **нет**,



Работа через почтовые клиенты

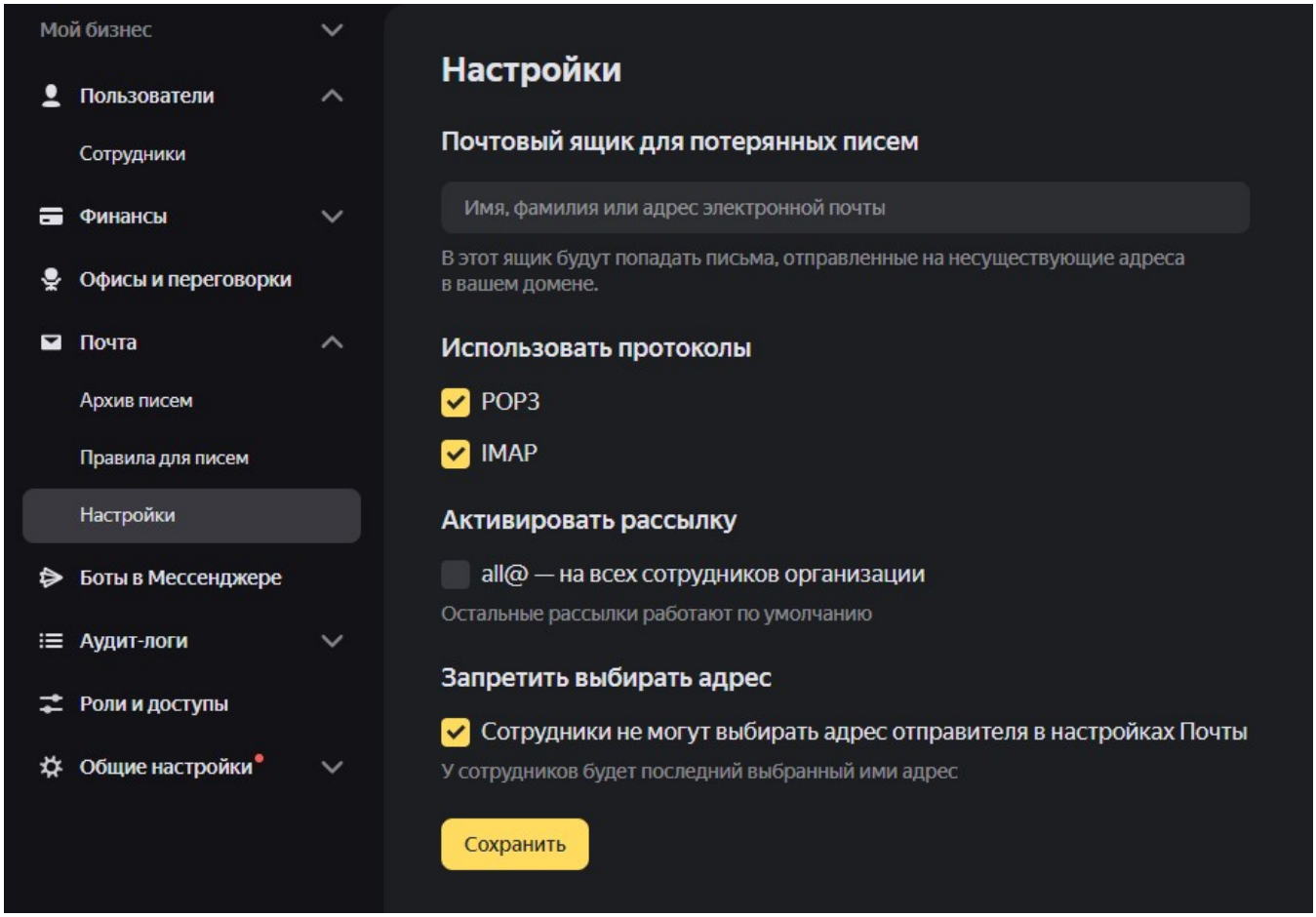
Рекомендуемый способ работы с Яндекс Почтой — веб-интерфейс mail.yandex.ru, веб-приложение и официальное мобильное приложение. Там пользователи получают доступ к функциям, которых нет в почтовых программах, — таким, как отложенная отправка писем, напоминания, быстрое добавление вложений с Диска.

Если веб-интерфейс и приложение не отвечают требованиям вашей организации, вы можете настроить работу с корпоративной почтой через почтовые клиенты. Для этого нужно включить почтовые протоколы и отправить пользователям инструкции по настройке.

Включение почтовых протоколов

Чтобы почтовые клиенты могли подключаться к серверам Яндекса и обмениваться с ними почтой, нужно включить один из предназначенных для этого почтовых протоколов.

1. Откройте admin.yandex.ru и выберите **Почта** → **Настройки**.
2. В блоке **Использовать протоколы** поставьте галочки напротив тех, которые собираетесь использовать. Если не знаете, какой выбрать, включите IMAP.



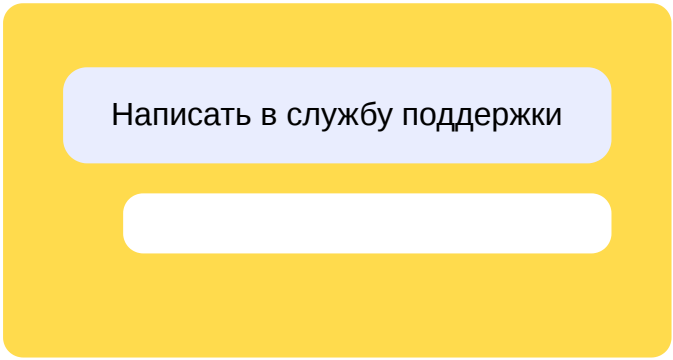
Совет

Если ваши сотрудники не пользуются почтовыми клиентами, держите оба протокола выключенными — так будет правильно с точки зрения безопасности.

Инструкции для пользователей

Инструкции по настройке разных версий почтовых программ собраны в Справке для пользователей.

Обратите внимание: инструкции описывают подключение только по протоколу IMAP.



Веб-приложение — это удобный способ пользоваться веб-интерфейсом почты, доступный в Яндекс Браузере. О том, как его установить, читайте в Справке Яндекс Браузера.

У Яндекс Почты есть приложение для iOS и для Android. Скачать.

Разрешенные и запрещенные отправители

Для защиты от нежелательной почты вы можете добавить отправителей в список запрещенных — по почтовому адресу, домену, IP-адресу или подсети. Так вы сможете заблокировать сообщения из определенных источников, даже если они проходят проверку Спамообороной.

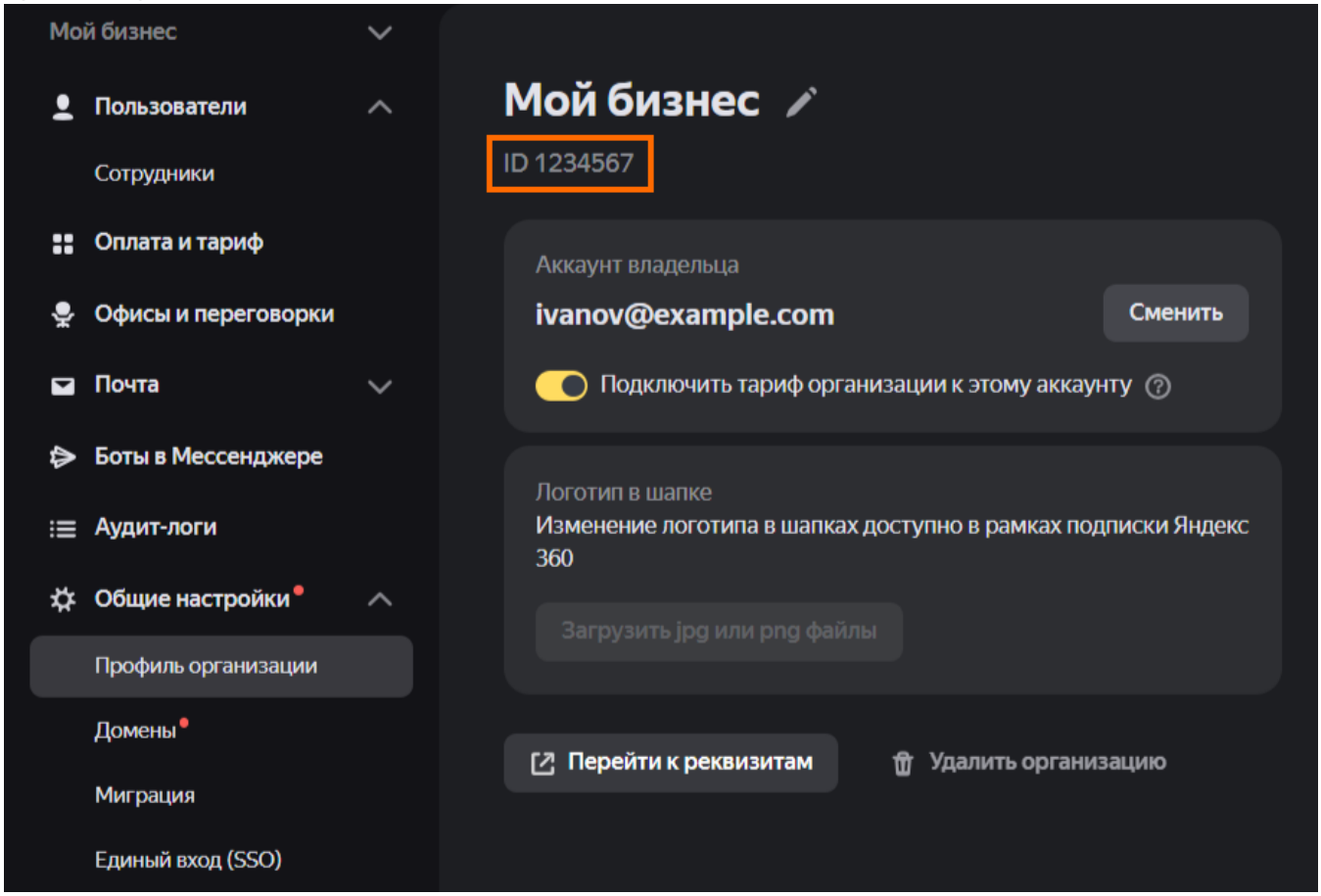
> Эта возможность доступна в тарифах **Основной**, **Продвинутый** и всех версиях тарифа **Корпоративный** из новой линейки, а также тарифах **Оптимальный** и **Расширенный** из старой.

Прежде чем начать

Управление списками разрешенных и запрещенных отправителей пока доступно только через API и осуществляется при помощи Правил доменной политики.

1. Для работы с API вам потребуется OAuth-токен, который можно получить после создания приложения в сервисе Яндекс OAuth.
   - Если у вас еще нет OAuth-приложения, то для его создания и получения токена воспользуйтесь инструкцией на странице Доступ к API. При создании приложения выберите права `ya360_admin:mail_write_routing_rules` и `ya360_admin:mail_read_routing_rules`.
   - Если у вас уже есть OAuth-приложение для работы с API Яндекс 360 для бизнеса, то добавьте ему права доступа для работы с доменными политиками и правилами обработки писем, а затем получите новый OAuth-токен по инструкции.
2. Определите идентификатор организации: откройте admin.yandex.ru и выберите **Общие настройки** → **Профиль организации**. Идентификатор будет написан под названием

организации.



Как просмотреть список правил

1. Сформируйте и отправьте GET-запрос:

   ```
   curl -X GET -H "Authorization: OAuth {oauth_token}"
   https://api360.yandex.net/admin/v1/org/{orgId}/mail/routing/policies
   ```

   В код подставьте значения:

   - `{orgId}` — идентификатор организации;
   - `{oauth_token}` — OAuth-токен.

2. Ответ на запрос возвращает перечень правил, в которых содержатся списки разрешенных и запрещенных отправителей.

Как добавить отправителя в список

Вы можете добавить отправителя в существующее правило или задать новое правило.

Внимание

Добавление новых адресов и правил происходит путем перезаписи данных. Чтобы внести изменения и не потерять уже созданные правила, нужно выгрузить текущий список правил, отредактировать его и загрузить обновленный список заново.

1. Сформируйте и отправьте GET-запрос:

```
curl -X GET -H "Authorization: OAuth {oauth_token}" -o body.json
https://api360.yandex.net/admin/v1/org/{orgId}/mail/routing/policies
```

   В код подставьте значения:

   - `{orgId}` — идентификатор организации;
   - `{oauth_token}` — OAuth-токен.

2. Список существующих правил будет сохранен в файл `body.json`.
3. Откройте файл в любом редакторе. Пример содержимого:

```
{
    "rules": [
        {
            "name": {название},
            "description": {описание},
            "enabled": {активность},
            "condition": {
                "email_from_filter": {
                    "list": [
                        "username@domain.ru",
                        "username@my.domain.ru",
                        "username@SOME.DOMAIN",
                        "username@other.domain.ru"
                    ]
                }
            },
            "action": {
                "type": {действие},
                "options": {
                    "force": {отметка}
                }
            }
        }
    ]
}
```

   Здесь:
   `{название}` — название правила, например `"Запрещенные почтовые адреса"`;
   `{описание}` — краткое описание правила, в котором можно дать пояснение, например `"Отклонить нежелательные письма"`;
   `{активность}` — нужно ли включить правило: `true` — правило включено, `false` — правило выключено;
   `{действие}` — какое действие будет выполнено: `reject` — отклонить письмо, `accept` — принять письмо;
   `{отметка}` — нужно ли поставить принятому письму дополнительную отметку: `spam` —

пометить письмо как спам, `ham` — не считать письмо спамом, даже если Спамооборона Почты пометила его как спам. Параметр используется, только если `type=accept`.

Для каждого правила в параметре `condition` может быть указано только одно из условий со списком:

- `email_from_filter` — список адресов электронной почты;
- `ip_filter` — список IP-адресов и подсетей;
- `domain_filter` — список доменов (значения в этом списке могут содержать символ подстановки `*` для обозначения любых поддоменов для домена более высокого уровня. Пример).

4. Добавьте отправителя в подходящий список существующего правила или задайте новое правило. Порядок правил в списке имеет значение: чем выше правило к началу списка, тем выше его приоритет.

   Пример готового файла с несколькими правилами

```
{
    "rules": [
        {
            "name": "Запрещенные почтовые адреса",
            "description": "Отклонить нежелательные письма",
            "enabled": true,
            "condition": {
                "email_from_filter": {
                    "list": [
                        "username@domain.ru",
                        "username@my.domain.ru",
                        "username@SOME.DOMAIN",
                        "username@other.domain.ru"
                    ]
                }
            },
            "action": {
                "type": "reject"
            }
        },
        {
            "name": "Запрещенные домены",
            "description": "Отклонить нежелательные письма",
            "enabled": true,
            "condition": {
                "domain_filter": {
                    "list": [
                        "SOME.DOMAIN",
                        "other.domain.ru",
                        "*.download"
                    ]
                }
            },
```

```
            "action": {
                "type": "reject"
            }
        },
        {
            "name": "Разрешенные IP-адреса",
            "description": "IP-адреса партнеров",
            "enabled": true,
            "condition": {
                "ip_filter": {
                    "list": [
                        "44.33.22.11",
                        "255.255.0.0/16"
                    ]
                }
            },
            "action": {
                "type": "accept"
            }
        },
        {
            "name": "Подозрение на спам",
            "description": "Поместить в папку спам",
            "enabled": true,
            "condition": {
                "ip_filter": {
                    "list": [
                        "55.55.33.33"
                    ]
                }
            },
            "action": {
                "type": "accept",
                "options": {
                    "force": "spam"
                }
            }
        }
    ]
}
```

5. Сохраните файл.
6. Сформируйте и отправьте PUT-запрос:

```
curl -X PUT -H "Authorization: OAuth {oauth_token}" -H "Content-Type:
application/json" -d "@body.json"
https://api360.yandex.net/admin/v1/org/{orgId}/mail/routing/policies
```

В код подставьте значения:

- `{orgId}` — идентификатор организации;
- `{oauth_token}` — OAuth-токен.

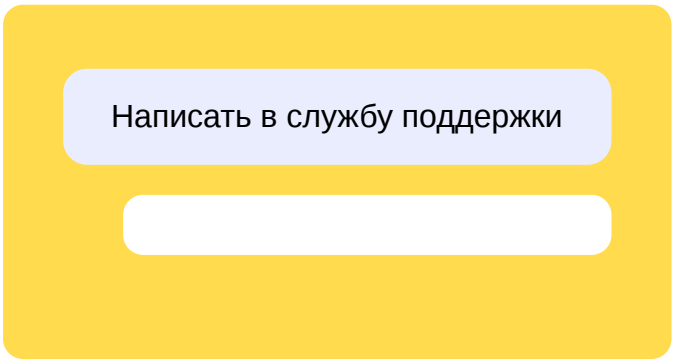
7. Результатом успешного запроса является ответ с кодом 200.

Я не понимаю, как отправлять запросы

1. Подготовьте запрос: скопируйте пример в любой редактор, вставьте в указанные места токен и идентификатор.
2. Откройте папку, в которую будет сохранен файл `body.json`.
3. Нажмите на пустое место в адресной строке.
4. Напишите туда `cmd` и нажмите **Enter**.
5. Откроется окно «Командная строка». Вставьте в него готовый запрос и нажмите **Enter**.

Документация API

Полное описание всех методов для управления списками разрешенных и запрещенных отправителей вы найдете в документации.



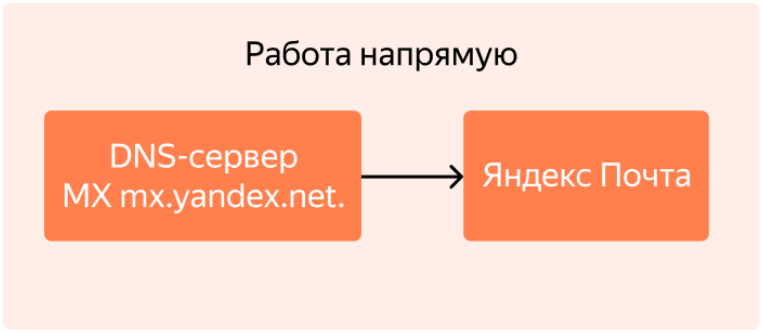
Подключение шлюза

Если вам нужно как-то обрабатывать корпоративную почту, прежде чем она попадет в почтовые ящики сотрудников, вы можете использовать почтовый шлюз.

Зачем это может быть нужно

> Например, для подключения стороннего антиспам-решения. Кроме того, такая настройка позволяет реализовать **гибридную конфигурацию почты**: разместить ящики части пользователей на вашем внутреннем почтовом сервере (например, Exchange), а другой части — в Яндекс Почте. В этом случае входящее письмо вначале приходит на ваш собственный сервер. Если на нем находится подходящий ящик, письмо попадает в него. Если хотя бы одного из получателей письма на сервере нет, оно отправляется дальше — в Яндекс Почту.

Для этого нужно перенаправить почту в шлюз, а уже из него передавать ее Яндекс Почте:



Обратите внимание: если шлюз настроен, через него маршрутизируется **вся почта**, включая письма от сотрудника сотруднику, письма на рассылки и так далее.

Как настроить работу через шлюз

Совет

Этот раздел содержит описание принципа, но не подробную пошаговую инструкцию: конкретные шаги зависят от задачи, которую нужно решить.

Если вы пока не знаете, как настраиваются шлюзы для почты, воспользуйтесь конфигурацией по умолчанию — без шлюза.

1. Измените MX-запись своего домена так, чтобы она указывала на ваш шлюз.
2. На стороне шлюза создайте правило пересылки входящей почты на DNS-запись `mx.yandex.net`.
3. При необходимости добавьте адрес шлюза в белый список — объяснение и инструкцию смотрите в следующем разделе.

Если на шлюзе работает стороннее антиспам-решение

В этом случае к письмам, определенным в спам, нужно добавлять специальный заголовок. При получении от шлюза письма с таким заголовком Яндекс Почта будет помещать его в папку **Спам** в почтовом ящике пользователя.

Настройте шлюз таким образом, чтобы при пересылке писем на Яндекс он добавлял к нежелательным письмам заголовок `X-Yandex-ExternalGate-Spam: YES`.

Список разрешенных источников входящей почты

Вы можете добавить адрес своего шлюза или какого-то другого сервера в список разрешенных IP-адресов. После этого почта, пришедшая из этого источника, не будет проходить проверку Спамообороной. Это может быть полезно, например, в таких случаях:

- Вы используете сторонний продукт для защиты от спама и полностью ему доверяете.
- Вы сконфигурировали гибридную систему: часть почтовых ящиков расположены на внутреннем почтовом сервере, и он пересылает в Яндекс Почту письма, которые сам не смог обработать.
- Вы заказываете эмуляцию фишинговой атаки, чтобы проверить, готовы ли сотрудники противостоять злоумышленникам.

Совет

Мы рекомендуем не отказываться от Спамообороны, даже если вы уверены в стороннем защитном решении.

Как добавить адрес в список разрешенных источников

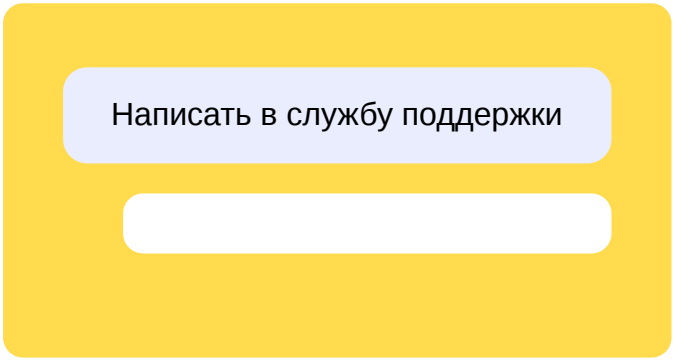
Добавить адрес в список разрешенных источников можно только по API.

В списке могут быть как конкретные IP-адреса (например, `77.88.21.249`), так и целые подсети (например, `77.88.54.0/23` или `2a02:6b8::/32`).

Для управления списком используйте запросы из группы «Список антиспама». Описание запросов приведено в документации API Яндекс 360.

Почему с подключенным шлюзом не отображаются портреты

Если у вас настроен почтовый шлюз, MX-запись домена указывает на него, а не на сервер Яндекса. Из-за этого портреты, установленные в аккаунтах на Яндексе, не будут отображаться в письмах сотрудников с учетными записями на домене вашей организации.



Архив писем

Эта возможность доступна в тарифах **Основной**, **Продвинутый** и всех версиях тарифа **Корпоративный** из новой линейки, а также тарифах **Оптимальный** и **Расширенный** из старой.

Архив — это инструмент, который сохраняет копии всех писем, отправленных и полученных сотрудниками организации. В архив попадают письма только из тех почтовых ящиков, которые созданы на домене организации.

При необходимости уполномоченный сотрудник может получить к этим письмам доступ.

- Как включить или отключить архив
- Как искать в архиве
- Как посмотреть, кто и что искал в архиве

Написать в службу поддержки

Включение и отключение архива

Внимание

Перед включением архива обязательно проконсультируйтесь с юристом своей организации. Он скажет, нужно ли в вашем случае собирать согласия сотрудников на доступ к данным.

По умолчанию доступ к письмам через архив **выключен**.

После включения архива в него попадет вся почта сотрудников, чьи почтовые ящики были созданы на домене организации. Обратите внимание: письма, которые были **удалены владельцами ящиков до включения архива**, восстановить уже не получится.

Как включить архив

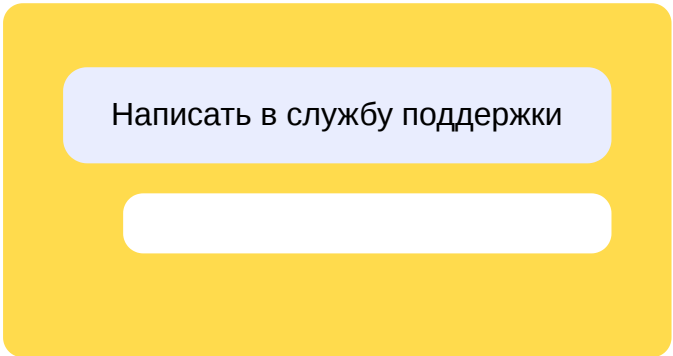
1. Откройте admin.yandex.ru.
2. Выберите **Почта** → **Архив писем**.
3. Нажмите **Подключить**.
4. Подтвердите подключение.

Как выключить архив

1. Откройте admin.yandex.ru.
2. Выберите **Почта** → **Архив писем**.
3. Нажмите на три точки возле заголовка **Архив писем**.
4. Подтвердите отключение.

Если включить архив обратно в течение месяца, он сохранит созданные поиски и их результаты.

Спустя месяц архив будет удален вместе со всеми поисками.



Поиск в архиве

Чтобы найти в архиве письма, нужно создать в нем новый **поиск**.

Каждый поиск выводит письма, соответствующие определенному фильтру. Например, можно создать поиск, выводящий все письма из определенного ящика, или поиск, выводящий все письма с определенными словами.

Результаты всех созданных поисков всегда доступны в архиве, но они не обновляются. Чтобы получить обновленную выдачу по тому же запросу, нужно создать новый поиск с такими же параметрами.

Как создать поиск

Откройте архив писем:

1. Откройте admin.yandex.ru.
2. Выберите **Почта** → **Архив писем**.

Если вы хотите выполнить простой поиск по ключевым словам, напишите запрос в поле **Поиск в письмах сотрудников** и нажмите **Найти**. В результате будет создан поиск с простейшим фильтром.

В некоторых случаях может понадобиться более точная настройка фильтрации. Чтобы задать параметры поиска, нажмите кнопку . Вот какие свойства писем можно использовать:

- Наличие вложений.
- Расположение в заданных ящиках. Если поиск происходит по подразделению или группе, можно исключить из него часть ящиков. Например, найти все письма отдела продаж за исключением писем секретаря.
- Временной интервал.
- Поля **От**, **Кому**, **Копия** и **Скрытая копия**.

После нажатия кнопки **Найти** новый поиск появится в списке.

Как смотреть результаты поиска

1. Откройте admin.yandex.ru.
2. Выберите **Почта** → **Архив писем**.
3. Нажмите на поиск, результаты которого нужно посмотреть.
4. Нажмите на письмо, которое нужно посмотреть.
5. При необходимости архивную копию письма можно переслать — например, руководителю или аудитору. Для этого нажмите кнопку **Переслать** над текстом письма.

Совет

Поискам можно давать названия, чтобы было удобнее ориентироваться в их списке. Чтобы переименовать поиск, откройте его и нажмите на карандаш возле его названия.

Как запустить тот же поиск повторно

Каждый поиск срабатывает один раз. Выдача не обновляется по мере того, как сотрудники получают и отправляют новые письма.

Чтобы получить обновленную выдачу, создайте новый поиск с теми же параметрами.

1. Откройте admin.yandex.ru.
2. Выберите **Почта** → **Архив писем**.
3. Нажмите на поиск, который нужно повторить.
4. Нажмите **Клонировать поиск**.
5. Проверьте параметры поиска — в первую очередь поле **За период**. Если нужно, измените их.
6. Нажмите **Найти**.

Почему я не нахожу нужных писем в архиве?

Самые вероятные причины такие:

- Вы задали слишком строгие условия поиска.
- Вы пытаетесь найти письма, которые владелец ящика удалил **до включения архива**.
- Вы пытаетесь найти письма сотрудника, который был удален из организации.

Написать в службу поддержки

Журнал действий с архивом

Все действия с архивом писем записываются в журнал. В журнале всегда можно посмотреть, кто и что искал.

1. Откройте admin.yandex.ru.
2. Выберите **Логи управления**.
3. Перейдите на вкладку **Архив писем**.
4. Если нужно, настройте фильтр: можно выбрать сотрудника, тип события и период.

> **Внимание**
>
> При увольнении сотрудника его действия **сохраняются в логе**. При этом в фильтре по сотрудникам есть только действующие сотрудники. Если администратор, действия которого нужно найти, уволился, не пытайтесь задать его в фильтре по сотрудникам. Для поиска соответствующих событий воспользуйтесь другими фильтрами.

5. Чтобы посмотреть подробную информацию о событии, нажмите на него.

Написать в службу поддержки

Вопросы и ответы

Останутся ли в архиве копии писем, если сотрудник удалит их из ящика?

Да.

Доступны ли в архиве письма сотрудников, аккаунты которых заблокированы?

Да.

Сохраняются ли в архиве письма сотрудников, чьи аккаунты удалены?

Нет.

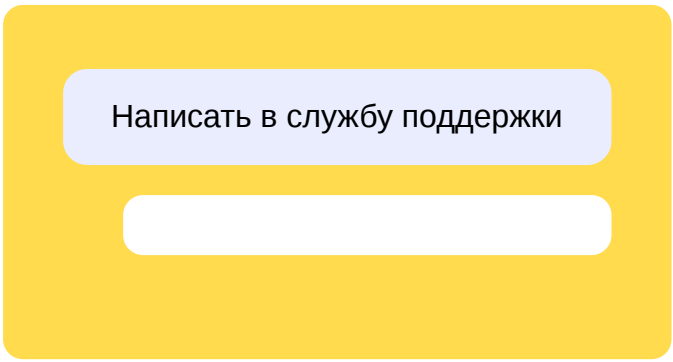
Попадают ли в архив письма сотрудников, использующих почтовые клиенты?

Да. Единственное исключение — в архив не попадет письмо, отправленное через SMTP и не синхронизированное по IMAP.

Почему я не нахожу нужных писем в архиве?

Самые вероятные причины такие:

- Вы задали слишком строгие условия поиска.
- Вы ищете по импортированным ящикам. В архив попадают письма только из тех почтовых ящиков, которые созданы на домене организации.
- Вы пытаетесь найти письма, которые владелец ящика удалил **до включения архива**.
- Вы пытаетесь найти письма сотрудника, который был удален из организации.



Решение проблем

Не могу получать письма и отправлять их из почтового ящика на своем домене

Большинство проблем с почтой связаны с неправильными настройками почтового домена. Убедитесь, что все настройки выполнены верно:

Шаг 1. Проверьте срок регистрации домена

Проверьте срок регистрации домена с помощью любого WHOIS-сервиса, например https://www.whois.com:

1. Перейдите на страницу WHOIS-сервиса.
2. В строке поиска введите имя вашего домена, например `example.org`.
3. Убедитесь, что дата, которая указана в строке **Expires On:**, еще не наступила.

Если срок регистрации домена истек, обратитесь к регистратору, чтобы продлить его.

Шаг 2. Проверьте DNS-записи домена

Проверьте правильность настройки DNS-записей. Это можно сделать, например, с помощью сервиса https://www.digwebinterface.com или другой dig-утилиты.

MX

1. Откройте страницу https://www.digwebinterface.com.
2. В поле **Hostnames or IP addresses** укажите имя вашего домена, например `example.org`.
3. В поле **Type** выберите **MX** и нажмите кнопку **Dig**.

Ответ должен иметь вид:

```
example.org.  20755 IN MX 10 mx.yandex.net.
```

Если сервер не отвечает на запрос, ответ не совпадает с нужным или в ответе присутствуют лишние записи, значит, MX-запись настроена некорректно. Настройте ее по инструкции.

Примеры некорректных ответов и способы их исправить

Ответ	Как исправить

`example.org.  20755 IN MX 10 mx.yandex.net.` `example.org.  12345 IN MX 12 somevalue.somedomain.tld`	Удалите лишние записи и оставьте только одну, с приоритетом `10` и значением `mx.yandex.net`.
`example.org. 12345 IN MX 12 somevalue.somedomain.tld`	Удалите эту запись и настройте правильную по инструкции.
В ответе ничего нет.	Скорее всего, запись на вашем домене совсем не настроена. Настройте ее по инструкции. Если запись настроена, но не отображается в ответе, обратитесь в службу поддержки вашего хостинга.

Внимание

Прежде чем повторно проверять DNS-записи, подождите 72 часа. За это время DNS-серверы в интернете обновят данные о записях.

SPF

1. Откройте страницу https://www.digwebinterface.com.

2. В поле **Hostnames or IP addresses** укажите имя вашего домена, например `example.org`.
3. В поле **Type** выберите **TXT** и нажмите кнопку **Dig**.

Ответ должен иметь вид:

```
example.org. 21600 IN TXT "v=spf1 redirect=_spf.yandex.net"
```

или

```
example.org. 21600 IN TXT "v=spf1 ip4:IP-1 ip4:IP-2 ip4:IP-3
include:_spf.yandex.net ~all"
```

Если сервер не отвечает на запрос, ответ не совпадает с нужным или в ответе присутствуют лишние записи, значит, SPF-запись настроена некорректно. Настройте ее по инструкции.

Внимание

Прежде чем повторно проверять DNS-записи, подождите 72 часа. За это время DNS-серверы в интернете обновят данные о записях.

DKIM

1. Откройте страницу https://www.digwebinterface.com.
2. В поле **Hostnames or IP addresses** укажите имя поддомена `mail._domainkey` для вашего домена, например `mail._domainkey.example.org`.
3. В поле **Type** выберите **TXT** и нажмите кнопку **Dig**.

Ответ должен иметь вид:

```
mail._domainkey.example.org. 21599 IN TXT "v=DKIM1\; k=rsa\; t=s\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDlk+IUXTHUIumVpG1S0vwFuwO9AC2aRrJj21MLj7xvO
```

Если сервер не отвечает на запрос, ответ не совпадает с нужным или в ответе присутствуют лишние записи, значит, DKIM-подпись настроена некорректно. Настройте ее по инструкции.

Внимание

Прежде чем повторно проверять DNS-записи, подождите 72 часа. За это время DNS-серверы в интернете обновят данные о записях.

Если вы убедились, что срок регистрации домена не истек и все его настройки верны, поищите возможную причину в разделе Проблемы с получением и отправкой писем в Справке Яндекс Почты.

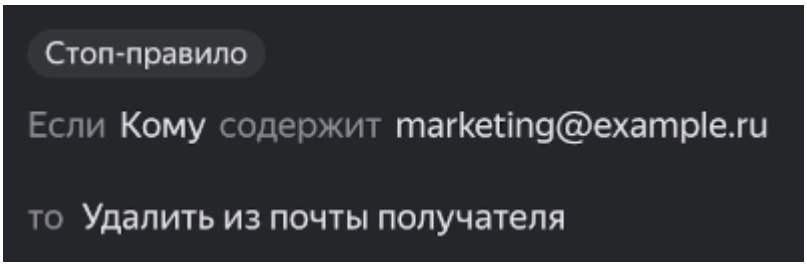
Мои письма не доходят до получателя или попадают в спам

Если вы отправляете с вашего почтового ящика большое количество писем, система безопасности Яндекс Почты может принять ваши письма за спам и заблокировать отправку писем. Подробнее об ограничениях на отправку писем и о требованиях к почтовым рассылкам читайте в разделе Отправить много писем в Справке Яндекс Почты.

Если вы не делали массовых рассылок, попробуйте определить причину проблемы с помощью пошаговой инструкции Не отправляются письма в Справке Яндекс Почты.

Я настроил правила для рассылок, но письма не доходят получателям

Например, вы задали правило, согласно которому письмо, отправленное на определенную рассылку, должно удалиться в ящике получателя:



Если правило сработало, а в адресатах письма были и другие рассылки, для которых либо письма должны были доставиться, либо правила не были настроены, то такие письма не дойдут получателям ни одной рассылки. Чтобы письма дошли, нужно изменить условия правила.

Подробнее о том, как добавлять правила, читайте в разделе Правила обработки писем.

Получатели не видят тему моего письма

Такая проблема может возникать при отправке писем с сайта через функцию `mail()` в PHP. Если в теме письма используется только кодировка UTF-8, Яндекс Почта ее не распознает.

Чтобы получатели видели тему письма, ее нужно перекодировать. Для этого используйте функцию `mb_encode_mimeheader`, укажите кодировку `UTF-8`, в которую нужно преобразовать текст, и метод кодировки Base64 `"B"`.

Например, замените такой код:

```
$subject = "Тема письма";
```

на такой:

```
$subject = mb\_encode\_mimeheader("Тема письма", "UTF-8", "B");
```

Если это не помогло

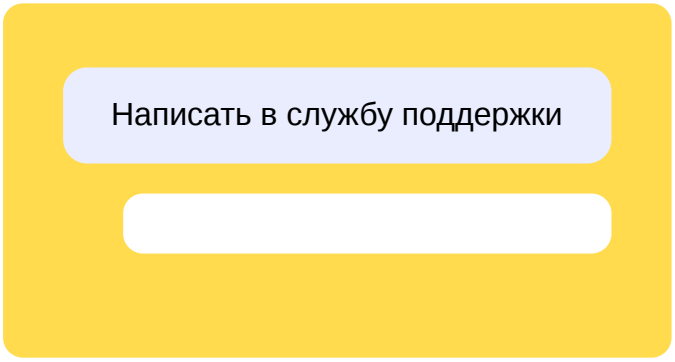
Перекодируйте тему письма с помощью функции `base64_encode()` и добавьте специальные текстовые метки.

Например, замените такой код:

```
$subject = "Тема письма";
```

на такой:

```
$subject = '=?utf-8?B?'.base64\_encode("Тема письма").'?=';
```



Системные требования

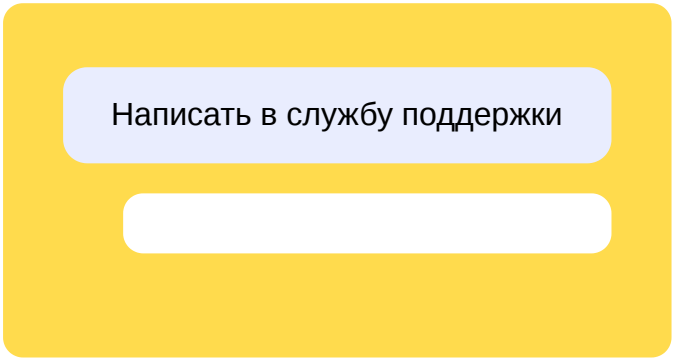
Для разных устройств и браузеров, чтобы общаться в Мессенджере.

Для установки

	Приложение	Браузер
Компьютер	• 64-разрядные Windows 10 или macOS 10.10 (Yosemite) или выше • Intel Pentium 4 (для Windows) или Intel 64x (для macOS) или выше • 512 МБ оперативной памяти или больше	• Яндекс Браузер 19 • Google Chrome 79 • Edge 79 • Firefox 78 • Opera 85 • Safari 13 И их более высокие версии.

Телефон	Android 7.0 или iOS 14.1 или выше	
		• Android WebView 79 • Google Chrome 79
	Приложение	**Браузер**
Компьютер	• 64-разрядные Windows 10 или macOS 10.10 (Yosemite) или выше • Intel Pentium 4 (для Windows) или Intel 64x (для macOS) или выше • 512 МБ оперативной памяти или больше	• Яндекс Браузер 19 • Google Chrome 79 • Edge 79 • Firefox 78 • Opera 85 И их более высокие версии.

Телефон	Android 7.0 или iOS 14.1 или выше



Установка, обновление и удаление Мессенджера через MSI

С помощью MSI можно установить Мессенджер на компьютеры с 64-битной Windows 10 или более высокими версиями. Для более старых или 32-битных Windows такой способ установки не подойдёт.

С MSI-файлом системные администраторы могут установить приложение как сразу всем сотрудникам организации, так и выбранным пользователям.

Как установить

Важно: если на компьютерах сотрудников уже есть приложение Мессенджера, установленное из файла `.exe`, сначала его нужно удалить.

С помощью MSI можно установить Мессенджер обычным или тихим способом. По умолчанию приложение установится с включенным автообновлением — при установке это можно отключить:

1. Скачайте MSI-файл по ссылке.
2. Запустите командную строку от имени администратора.
3. Напишите команду `msiexec /i "путь к файлу Yandex_Messenger.msi"`, а затем допишите через пробел нужные параметры:
   - `MSIINSTALLPERUSER=0`, чтобы установить Мессенджер для всех сотрудников.

     Приложение установится в папку *C:\ProgramFiles\Yandex Messenger*. Чтобы выбрать другую папку для установки, допишите параметр `APPINSTALLDIR="полный путь к папке"`.
   - `/qn /quiet`, чтобы запустить тихую установку без всплывающих окон.
   - `AUTOUPDATEENABLED=0`, чтобы отключить автоматическое обновление и в дальнейшем обновлять Мессенджер вручную. Этот параметр всегда можно поменять на `AUTOUPDATEENABLED=1` — чтобы приложение снова обновлялось автоматически.
   - `INSTALLLEVEL=2`, чтобы вообще не устанавливать компонент автоматического обновления.
   - `AUTOLAUNCH=1`, чтобы Мессенджер запустился после установки.

     Примеры команд

     `msiexec /i "C:\Downloads\Yandex_Messenger.msi" MSIINSTALLPERUSER=0` — обычная установка в папку *C:\ProgramFiles\Yandex Messenger*. После установки Мессенджер нужно будет запустить вручную.

     `msiexec /i "C:\Downloads\Yandex_Messenger.msi" MSIINSTALLPERUSER=0 APPINSTALLDIR="C:\Users\user\Folder" /qn /quiet` — тихая установка в папку *C:\Users\user\Folder\Yandex Mesenger*. Мессенджер запустится после установки.
4. Нажмите клавишу **Enter**.

Можно ли установить Мессенджер не всем, а только определенным сотрудникам?

> Да. Запустите установщик MSI локально или удаленно на компьютерах тех сотрудников, кто будет пользоваться Мессенджером:

1. Скачайте MSI-файл по ссылке.
2. Запустите командную строку от имени администратора.
3. Напишите команду `msiexec /i "путь к файлу Yandex_Messenger.msi" MSIINSTALLPERUSER=1`. Мессенджер установится в папку *C:\Users\user\AppData\Local\Programs\Yandex Messenger*. Чтобы выбрать другую папку для установки, допишите `APPINSTALLDIR="полный путь к этой папке"`.
4. Если нужно запустить Мессенджер после установки, допишите к команде `AUTOLAUNCH=1`.

   Примеры команд

   `msiexec /i "C:\Downloads\Yandex_Messenger.msi" MSIINSTALLPERUSER=1` — Мессенджер установится в папку *C:\Users\user\AppData\Local\Programs\Yandex Messenger*. Запустить приложение можно будет вручную.

   `msiexec /i "C:\Downloads\Yandex_Messenger.msi" MSIINSTALLPERUSER=1 APPINSTALLDIR="C:\Users\user\Folder"` — Мессенджер установится в папку *C:\Users\user\Folder\Yandex Mesenger* и запустится после установки.
5. Нажмите клавишу **Enter**.

Мессенджер, установленный таким способом, будет обновляться автоматически.

Как обновить

По умолчанию при любом способе установки с помощью файла MSI Мессенджер обновляется автоматически.

Чтобы обновлять его вручную, нужно:

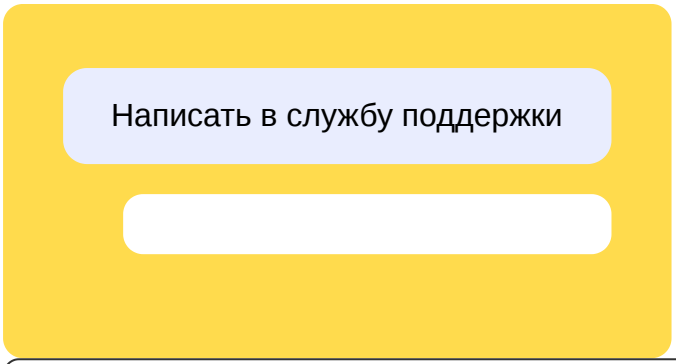
- отключить автообновление одним из параметров;
- проверять наличие обновления по ссылке. Номер актуальной версии указан после *ru.yandex.yamb*, обновления выходят раз в 1-2 недели;
- скачивать актуальную версию файла и повторять установку.

Как удалить

Откройте командную строку, напишите `msiexec /x "путь к файлу Yandex_Messenger.msi"` и нажмите клавишу **Enter**.

Пример команды

`msiexec /x "C:\Downloads\Yandex_Messenger.msi"`



Переезд в Яндекс 360 для бизнеса

Мы собрали ответы на частые вопросы о том, как перенести данные вашей организации в Яндекс 360 для бизнеса из Google Workspace, Microsoft 365 и других платформ. Смотреть >

Боты в Мессенджере

Эта возможность доступна в тарифах **Основной**, **Продвинутый** и всех версиях тарифа **Корпоративный** из новой линейки, а также тарифах **Оптимальный** и **Расширенный** из старой.

Администратор организации может создавать ботов для Яндекс Мессенджера и управлять ими. Боты могут автоматизировать внутренние процессы организации, создавать групповые чаты и уведомлять администратора о событиях в них.

Боты в Мессенджере взаимодействуют только с сотрудниками организации.

Создать бота

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Боты в Мессенджере**.
3. Нажмите кнопку **Создать бота**.
4. В появившемся окне введите **Имя** бота, загрузите фото.
5. Нажмите кнопку **Создать**. Токен бота будет сформирован автоматически и скопирован в буфер обмена.
6. Сохраните токен в надежном месте. С помощью OAuth-токена бот авторизует все операции.

Примечание

Яндекс Мессенджер не хранит токены ботов. Просмотреть токен позже не получится. Если вы потеряете токен, то сможете его перевыпустить. Предыдущий токен при этом будет отозван.

Добавить несколько ботов

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Боты в Мессенджере**.
3. В правом верхнем углу нажмите кнопку **Добавить бота**.
4. В появившемся окне введите **Имя** бота, загрузите фото.
5. Нажмите кнопку **Создать**. Токен бота будет сформирован автоматически и скопирован в буфер обмена.
6. Сохраните токен в надежном месте. С помощью OAuth-токена бот авторизует все операции.

Настроить бота

В разделе **Боты в Мессенджере** можно выполнить простые действия с ботами: изменить имя и фото бота или добавить вебхук. Подробные настройки ботов описаны в документации API Мессенджера**.** Если вы потеряли токен бота, его можно перевыпустить.

Изменить имя или фото

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Боты в Мессенджере**.
3. Выделите бота и нажмите кнопку **Настроить**.
4. Внесите изменения и нажмите кнопку **Сохранить**.

Добавить вебхук

Если добавить вебхук, все обновления будут отправляться в виде POST-запроса по указанному адресу. Чтобы добавить вебхук:

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Боты в Мессенджере**.
3. Выделите бота и нажмите кнопку **Настроить**.
4. В поле **Вебхук** введите URL-адрес бота и нажмите кнопку **Сохранить**.

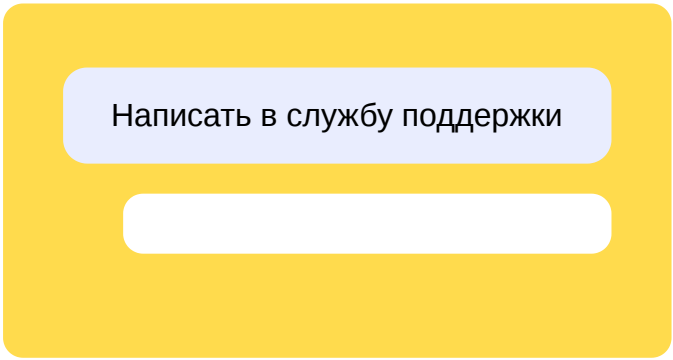
Перевыпустить токен

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Боты в Мессенджере**.
3. Выделите бота и нажмите кнопку **Настроить**.

4. Нажмите кнопку **Перевыпустить токен**. Токен бота будет сформирован автоматически и скопирован в буфер обмена.
5. Сохраните токен в надежном месте. С помощью OAuth-токена бот авторизует все операции.

Удалить бота

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Боты в Мессенджере**.
3. Выделите бота, который больше не нужен.
4. Нажмите кнопку **Удалить**.



Пространства

Пространства созданы для общения внутри организации.

Рабочее и личное

Если ваша компания зарегистрирована в Яндекс 360 для бизнеса, вам доступны два вида пространства в Мессенджере:

- *Личное* — общение с людьми вне организации.
- *Рабочее* — пространство для общения сотрудников внутри компании. Если человек работает в двух организациях, у него будет два независимых рабочих пространства.
  - Если компания зарегистрирована после 1 июля 2022 года, рабочее пространство включено по умолчанию. Переключитесь на пространство вашей организации.
  - Если компания зарегистрирована до 1 июля 2022 года, у вас может не быть рабочего пространства, попросите администратора его подключить.

Как переключаться между пространствами

1. Нажмите (или **Настройки** в iOS).
2. В блоке **Пространства** выберите нужное.

Особенности рабочего пространства

Рабочее пространство закрыто от внешних пользователей:

- Отображаются контакты только из адресной книги Яндекс 360 для бизнеса.
- В чат не могут войти внешние пользователи, даже если у них есть прямая ссылка.

Здесь созданы все условия для работы:

- В чат можно добавить не только отдельных сотрудников, но и подразделения или группы. Все изменения в штате, которые отражаются в Яндекс 360 для бизнеса, автоматически отображаются в рабочем пространстве.
- В профиле пользователя видны отдел и рабочие группы сотрудника.
- Пользователям доступны все функции Мессенджера: общение в чатах, создание каналов, звонки и обмен файлами.

Как подключить рабочее пространство

> **Примечание**
>
> Подключить рабочее пространство может только администратор.

Подайте заявку на подключение в службу поддержки. После подачи заявки в рабочее пространство будут перенесены все приватные и групповые чаты между сотрудниками. Чаты, где есть внешние

пользователи, не переносятся. Администратор может перенести их вручную, удалив внешних пользователей.

Как перенести чат в рабочее пространство

> **Примечание**
>
> Перенести чат может только его администратор.

Если в чате есть внешние пользователи, Мессенджер не перенесет его в закрытое пространство из соображений безопасности. Перенесите чат вручную:

1. Удалите из чата внешних пользователей.
2. Справа вверху нажмите ⋮ (в iOS •••) и выберите **Перенести чат**.

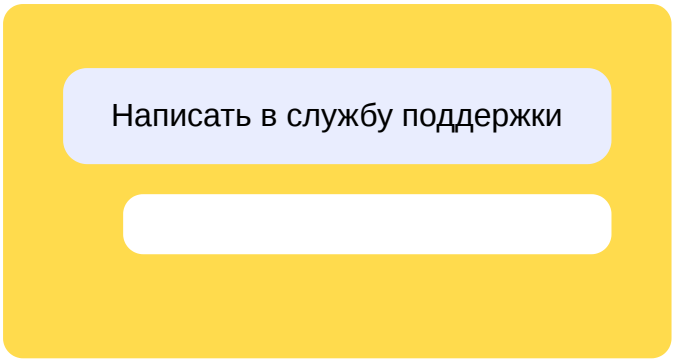
Вопросы и ответы

Пропали рабочие чаты, не могу найти коллег в поиске

Возможно, вы не переключились на рабочее пространство. Чтобы в него перейти:

1. Нажмите ⚙ (или **Настройки** в iOS).
2. В блоке **Пространства** выберите нужное.

Если вы заметили публикацию или комментарий, нарушающие правила, или считаете, что ваше сообщение было удалено по ошибке, напишите в службу поддержки.



Чат на основе группы или подразделения

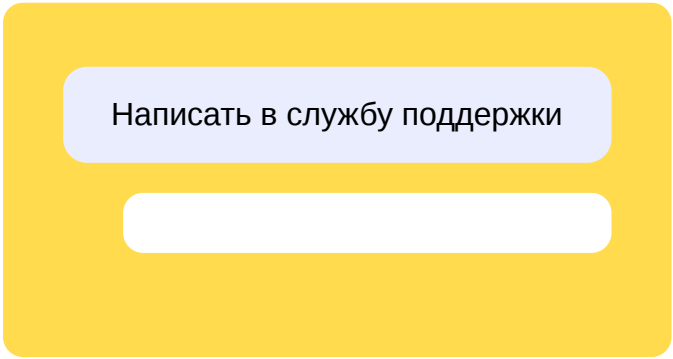
Вы можете создать чат или канал для сотрудников определенной группы или подразделения, не добавляя всех по одному. Такие чаты можно делать на основе групп, созданных вручную, через API и в результате синхронизации с каталогом LDAP. Как настроить синхронизацию

Как создать

1. В Мессенджере нажмите → **Новый групповой чат**.
2. Укажите название чата и нажмите **Добавить участников**.
3. Введите название группы или подразделения и нажмите на него в списке.
4. Выберите **Создать чат**. В него автоматически попадут все сотрудники из выбранной группы.

Чтобы пригласить группу или подразделение в уже существующий чат, нажмите → **Добавить участников**. Введите название нужного отдела и нажмите **Добавить**.

После удаления сотрудника из группы в кабинете организации у него пропадет доступ к групповому чату, а при добавлении нового сотрудника доступ к чату появится автоматически. Как удалить или добавить сотрудника



Установка, обновление и удаление Телемоста через MSI

С помощью MSI можно установить Телемост на компьютеры с 64-битной Windows 10 или более высокими версиями. Для более старых или 32-битных Windows такой способ установки не подойдёт.

С MSI-файлом системные администраторы могут установить приложение как сразу всем сотрудникам организации, так и выбранным пользователям.

Как установить

Важно: если на одном компьютере несколько учетных записей с установленной из файле `.exe` программой Телемоста, сначала ее нужно удалить из каждой учетной записи.

Если на компьютере одна учетная запись, то удалять программу Телемоста перед запуском установки через MSI не нужно.

С помощью MSI можно установить Телемост в обычном или тихом режиме:

1. Скачайте установочный MSI-файл по ссылке.
2. Запустите командную строку от имени администратора.
3. Напишите команду `msiexec /i "путь к файлу YandexTelemostSetup_9999.msi"`, а затем допишите через пробел нужные параметры:
   - `/qn`, чтобы запустить тихую установку без всплывающих окон.
   - `ALLUSERS="1" MSIINSTALLPERUSER=""`, чтобы установить Телемост для всех сотрудников. **Если вы запускаете тихую установку, обязательно укажите эти праметры.**
   - `SKIP_LAUNCH=1`, чтобы не запускать Телемост сразу после установки.
   - `NODESKTOPSHORTCUT=1`, чтобы не создавать ярлык на рабочем столе. Если не указывать этот параметр, ярлык создастся на рабочих столах всех пользователей.

     Пример команды

     `msiexec /i "C:\Downloads\YandexTelemostSetup_9999.msi" /qn ALLUSERS="1" MSIINSTALLPERUSER="" SKIP_LAUNCH=1` — тихая установка для всех пользователей без запуска после установки.
4. Нажмите клавишу **Enter**.

Программа установится в папку `C:\Program Files\Yandex\YandexTelemost`.

Можно ли установить Телемост не всем, а только определенным сотрудникам?

Да. Запустите установщик MSI локально или удаленно в учетных записях тех сотрудников, кто будет пользоваться Телемостом:

1. Скачайте установочный MSI-файл по ссылке.
2. Запустите командную строку **не от имени администратора**. Важно: если запустить командную строку от имени администратора, то Телемост установится для всех учетных записей независимо от того, какие параметры вы укажете.
3. Напишите команду `msiexec /i "путь к файлу YandexTelemostSetup_9999.msi" ALLUSERS=2 MSIINSTALLPERUSER="1"`, а затем допишите через пробел нужные параметры,

например `NODESKTOPSHORTCUT=1`, чтобы не создавать ярлык на рабочем столе.

4. Нажмите клавишу **Enter**.

Телемост установится в папку `C:\Users\%USERNAME%\AppData\Local\Programs\Yandex\YandexTelemost`.

Как обновить

По умолчанию при любом способе установки с помощью файла MSI Телемост обновляется автоматически. Если автообновление по каким-либо причинам не сработало, можно повторно установить программу по инструкции.

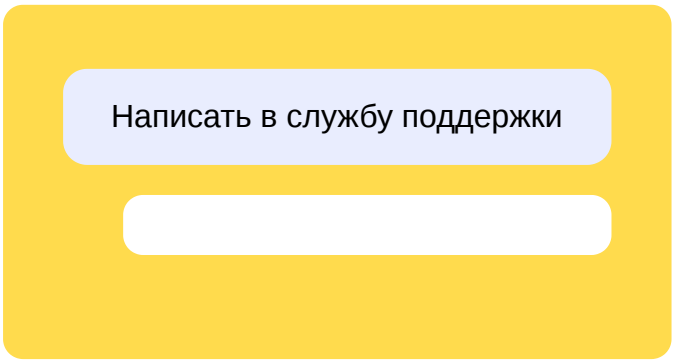
Обновлять Телемост вручную не рекомендуется, потому что при этом будут прерваны текущие сессии всех пользователей.

Как удалить

Откройте командную строку, напишите `msiexec /x "путь к файлу YandexTelemostSetup_9999.msi"` и нажмите клавишу **Enter**.

Пример команды

```
msiexec /x "C:\YandexTelemostSetup_9999.msi"
```



Вход и выход

Как войти

Чтобы начать работу с онлайн-досками в пространстве компании, войдите в Доски с помощью Яндекс ID, привязанного к организации.

1. Перейдите по ссылке boards.yandex.ru.
2. В правом верхнем углу страницы нажмите **Войти**.
3. Введите логин и пароль и нажмите **Войти**.
4. Выберите **Рабочее** и нажмите на название своей компании.

Как выйти

Чтобы выйти из Досок или сменить аккаунт:

1. В левом верхнем углу личного кабинета нажмите на свое имя.
2. Нажмите **Выйти из аккаунта**.

Администрирование Яндекс Досок

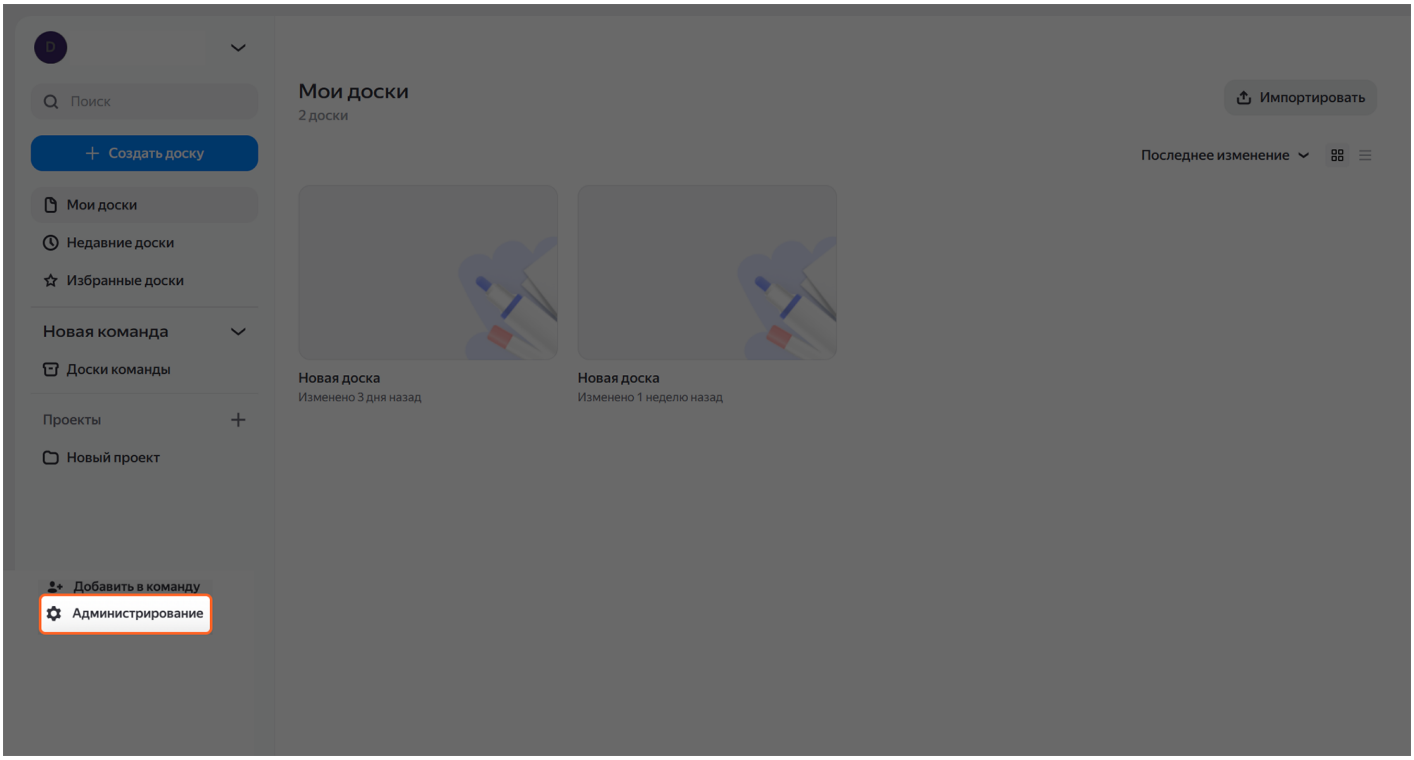
Вы можете управлять пространством организации в Досках в разделе **Администрирование**. В нем вам доступна информация про сотрудников, команды, доски и файлы. Также через него можно отслеживать события и активность сотрудников в пространстве организации.

Кто и где управляет Досками

Управление пространством Досок доступно не в кабинете организации, а в разделе **Администрирование** в Досках. В него могут попасть только администраторы вашей организации. Как назначить администратора

Как начать администрировать

Чтобы попасть в раздел **Администрирование**, войдите в Доски с помощью Яндекс ID, привязанного к организации. Затем в левом нижнем углу личного кабинета нажмите **Администрирование**. Как войти в Доски



Управление пользователями

Вы можете посмотреть информацию об активных сотрудниках и тех, кто удален из пространства организации. Для этого перейдите в раздел **Пользователи**.

Как посмотреть действия пользователя

Все действия сотрудников записываются в журнал событий. Там вы можете отслеживать все, что делают сотрудники в пространстве организации.

Чтобы посмотреть действия:

1. В списке пользователей найдите нужного сотрудника.
2. Нажмите на три точки справа от него.
3. Выберите действия, которые хотите посмотреть:
    - **Действия пользователя** — все действия пользователя в пространстве организации.
    - **Действия над пользователем** — все действия над пользователем со стороны других сотрудников. Например добавление пользователя в команду.

Как передать доски другому сотруднику

Вы можете передать все доски одного сотрудника другому. Например, если сотрудник уволился, а на его досках есть нужная организации информация.

Чтобы передать доски сотрудника другому:

1. В разделе **Пользователи** найдите сотрудника, доски которого хотите передать.
2. Нажмите на три точки справа от него.
3. Нажмите **Передать данные**.
4. Введите логин пользователя, которому передаете доски.
5. Нажмите **Сохранить**.

Управление командами

Вы можете просматривать список команд, создавать, настраивать, переименовывать и удалять их. Для этого перейдите в раздел **Команды**.

Как посмотреть доски команды

Вы можете посмотреть список досок, созданных конкретной командой. Для этого:

2. В списке команд найдите нужную и нажмите на три точки справа от нее.
3. Нажмите **Доски команды**. Откроется список досок, созданных этой командой.

Как посмотреть действия команды

Вы можете открыть список всех действий команды, например, если вам нужно узнать, когда участники послений раз работали над проектом.

Чтобы посмотреть все действия команды:

1. Найдите в списке команд нужную.
2. Нажмите на три точки справа от нее.
3. Нажите **Действия команды**. Откроется журнал событий этой команды.

Как изменить роли участников

Вы можете менять роли участников в командах. Какие бывают роли

Чтобы изменить роль участника команды:

1. В списке команд найдите нужную и нажмите на три точки справа от нее.
2. Нажмите **Участники команды**.
3. В открывшемся окне измените роли участников.

Как переименовать команду

1. В списке команд найдите нужную и нажмите на три точки справа от нее.
2. Нажмите **Переименовать**.
3. Введите новое название команды.

Как удалить команду

Если вы удалите команду, доступ к доскам останется у всех ее участников.

Чтобы удалить команду:

1. В списке команд найдите нужную и нажмите на три точки справа от нее.
2. Нажмите **Удалить**.
3. Введите новое название команды.

Управление досками

Вы можете управлять всеми досками в пространстве организации. Для этого перейдите в раздел **Доски**. В нем можно просматривать, переименовывать и удалять доски, а также просматривать журнал событий каждой доски.

Как посмотреть действия с доской

Вы можете посмотреть все действия с конкретной доской, например, если вам нужно узнать, кто последний ее редактировал.

Чтобы открыть список действий с доской:

1. Найдите в списке досок нужную.
2. Справа от нее нажмите на три точки.
3. Нажмите **Действия с доской**. Откроется журнал событий этой доски.

Как включить гостевой доступ

Чтобы ваши сотрудники могли поделиться доской с пользователями не из вашей организации, включите гостевой доступ. Для этого:

1. Найдите в списке досок нужную.
2. Справа от нее нажмите на три точки.
3. Нажмите **Включить гостевой доступ**.

Если вам нужно посмотреть список досок с включеным гостевым доступом, нажмите на выпадающее меню над списком досок и выберите **Гостевой доступ**. В таблице с досками отобразятся только те, которыми можно делиться с внешними пользователями.

Как переименовать или удалить доску

Вы можете изменить название доски или удалить ее. Для этого:

1. Найдите в списке досок нужную.
2. Справа от нее нажмите на три точки.
3. Нажмите **Переименовать** или **Удалить**.

Журнал событий

В журнале событий вы сможете следить за событиями и активностью сотрудников в Досках. Это может быть полезно при инцидентах и выявлении нарушений безопасности. Журнал событий работает аналогично аудит-логам.

Какие события записываются

В журнале событий записываются все действия производимые в пространстве организации.

Чтобы посмотреть список конкретных событий:

1. Нажмите на выпадающий список над таблицей со всеми событиями.
2. Выберите, какие события вам нужно найти:
    - **Команда создана** — формирование новой команды в системе.
    - **Команда отредактирована** — изменение параметров или настроек существующей команды.
    - **Команда удалена** — удаление команды из системы.
    - **Участник команды создан** — добавление нового участника в команду.
    - **Участник команды изменен** — обновление данных или ролей существующего участника команды.
    - **Участник команды удален** — удаление участника из команды.
    - **Доска создана** — создание новой доски для работы или проектов.
    - **Доска изменена** — редактирование параметров или содержимого доски.
    - **Доска удалена** — удаление доски из системы.
    - **Гостевой доступ включен** — предоставление доступа к доске для внешних пользователей.
    - **Гостевой доступ выключен** — ограничение доступа к доске для внешних пользователей.
    - **Доска Miro импортирована** — добавление доски из Miro в Яндекс Доски.
    - **Проект в команде создан** — создание нового проекта внутри команды.
    - **Проект в команде изменен** — внесение изменений в параметры или статус существующего проекта.
    - **Проект в команде удален** — удаление проекта из списка проектов команды.
    - **Пользователь создан** — регистрация нового пользователя в системе.
    - **Пользователь изменен** — обновление данных пользователя, например, изменение логина или имени.
    - **Пользователь удален** — удаление сотрудника из пространства организации.
    - **Пользователь восстановлен** — восстановление учетной записи пользователя после ее удаления.
    - **Перенесли данные пользователя** — передача досок одного сотрудника другому.
    - **Пользователь авторизовался** — вход пользователя в пространтсво организации.
    - **Пользователь разлогинился** — выход пользователя из пространства организации.
    - **Файл загружен** — добавление файла на доску или в проект.
    - **Файл удален** — удаление файла с доски.

Поиск по событиям

Вы можете искать события по параметрам. Если ищите какое-то конкретное событие, установите фильтр по инструкции и введите в поиск по разделу, например, название доски или команды с которой это событие связанно.

Как узнать детали события

Если вам нужно посмотреть подробную информацию о событии, откройте детализированную информацию о нем. Для этого:

1. В списке событий найдите нужное.
2. Нажмите на три точки справа от него.
3. Нажмите **Детали**. Откроется окно с подробной информацией.

Управление импортом досок

Вы можете управлять импортом досок из Miro и Pruffme. Для этого перейдите в раздел **Импорт**. В нем отображается список всех досок, импортированных из Miro и Pruffme, с указанием статуса импорта.

Как перезапустить импорт

Если доска по какой-то причине не импортировалась или импортировалась с ошибками, вы можете повторно запустить импорт.

Чтобы перезапустить:

1. Найдите в списке доску, которую не получилось импортировать.
2. Нажмите на три точки справа от нее.
3. Нажмите **Переобработать**. Импорт доски начнется заново.

Навигация по файлам

Вы можете быстро искать файлы, которые загружены на доски. Для этого перейдите в раздел **Материалы**. В нем отображаются все изображения, презентации и вложения, добавленные сотрудниками на доски.

Как найти файл

Вы можете посмотреть список файлов конкретного типа, например только изображения.

Чтобы открыть список файлов определенного типа:

1. Нажмите на выпадающий список над таблицей со всеми файлами.
2. Выберите, какие файлы вам нужно найти. В списке отобразятся только они.

Если вы нашли нужный файл и хотите узнать, какие еще файлы загружены сотрудником, нажмите три точки справа от файла и выберите **Все материалы пользователя**. Также можно открыть список всех файлов загруженных на доску с найденным вами файлом. Для этого выберите **Все материалы доски**.

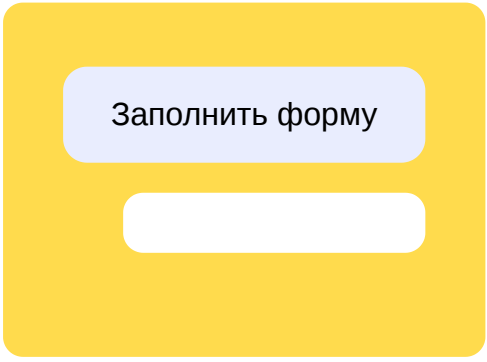
С чего начать

В отличие от обычного способа установка Яндекс Досок способом on-premises позволяет работать с сервисом в закрытом контуре компании. Чтобы протестировать работу с Досками этим способом, вы можете получить 2 бесплатные лицензии. Для этого:

1. Заполните форму внизу страницы. С вами свяжется менеджер и уточнит детали подключения.
2. Получите лицензии и выполните инсталляцию по инструкции.

Если сервис подойдет для решения ваших задач, вы можете перейти с бесплатной тестовой версии на коммерческую, выбрав срок действия и количество лицензий, которые нужны вашему бизнесу. Для этого:

1. Свяжитесь с менеджером, который вас консультировал.
2. Заключите договор и оплатите счет.
3. Получите лицензии и активируйте их.



Тарификация Яндекс Досок при подключении on-premises

При подаче заявки на подключение вы фиксируете с менеджером количество лицензий, необходимых вашей организации. Лицензия для одного сотрудника стоит 800 ₽ в месяц. Только сотрудникам с лицензией доступна совместная работа.

В зависимости от версии Яндекс Досок, которая развернута на ваших серверах, распределение оплаченных лицензий между пользователями происходит по-разному. Начиная с версии 1.11.1, администратор может выдавать и отзывать лицензии.

> Чтобы узнать, какая версия Яндекс Досок у вас установлена, нажмите на имя пользователя в левом верхнем углу экрана.
> Как перейти на новую версию, читайте в разделе Обновление.

Распределение лицензий

Версия 1.11.1 и выше

Лицензии распределяются среди пользователей с помощью отметки **Оплаченный**. Отметить пользователя может только администратор.

Чтобы выдать лицензию пользователю:

1. В личном кабинете зайдите в раздел **Администрирование** → **Пользователи**.
2. Установите отметку **Оплаченный** для нужного сотрудника.

Если администратор снимет отметку **Оплаченный** с сотрудника, его лицензия освободится. Вместо него можно будет назначить нового пользователя. Перераспределять лицензии можно в любое время.

Пример лицензирования в версии 1.11.1

> Общая численность организации: 150 человек.
> Пользователи, отмеченные администратором: 100 человек.
> Итог: только эти 100 человек считаются пользователями с лицензией.

Версия 1.10.2 и ниже

Все подтвержденные пользователи могут получить полный доступ к приложению. Если сотрудник откроет любую доску, он автоматически получит одну из оплаченных лицензий. Передать выданную лицензию другому пользователю невозможно.

Пример лицензирования в версии 1.10.2

> Общая численность организации: 150 человек.
> Из них 100 человек авторизовались и перешли на доску.
> Итог: все эти 100 человек считаются пользователями с лицензией.

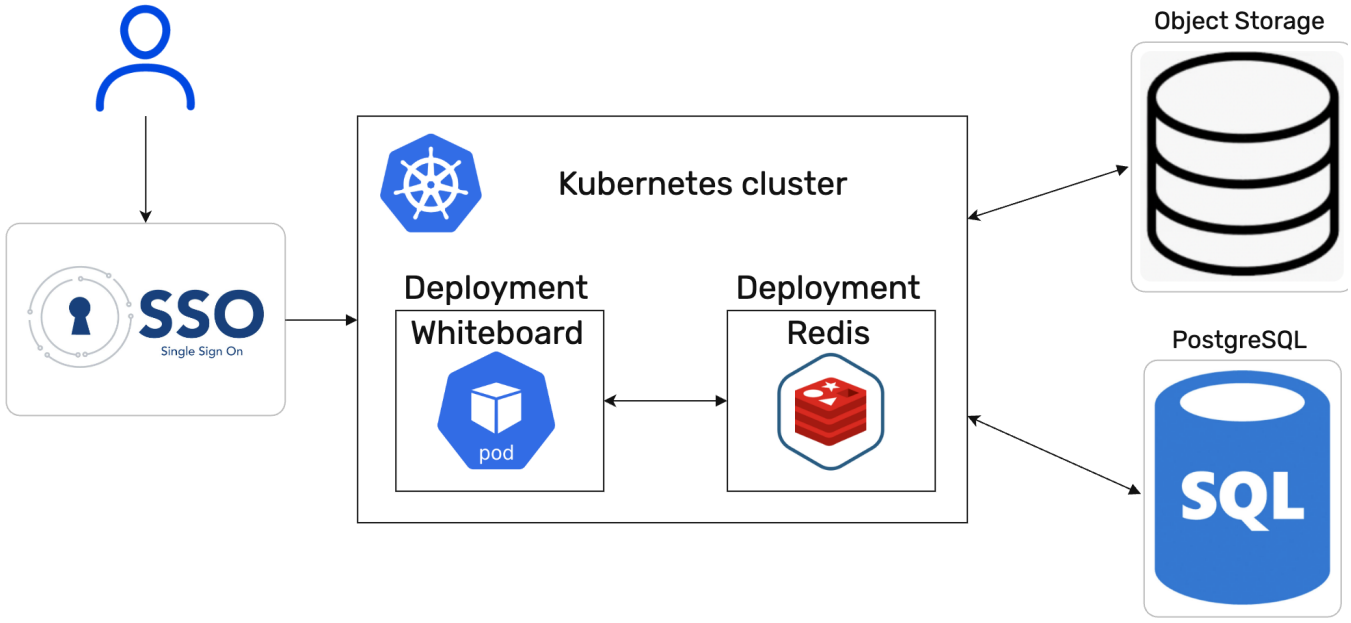
Как изменить количество лицензий

Для изменения количества лицензий свяжитесь с менеджером отдела продаж. Он сообщит вам подробности и сделает запрос на ключ с новым количеством лицензий.

Пример развертывания

В статье описано развертывание Досок в Kubernetes с помощью менеджера пакетов Helm в облачном хранилище Yandex Cloud. В качестве смежных сервисов выбраны СУБД PostgreSQL, система идентификации AD FS, использующая протокол SAML, или Keycloak с поддержкой протокола OpenID для организации единого входа (SSO), а также объектное хранилище Yandex Object Storage.

Схема взаимодействия компонентов



Вы можете воспользоваться приведенной ниже конфигурацией с минимальным набором параметров, чтобы протестировать приложение. Если Доски подойдут для выполнения ваших задач, приобретите лицензии и разверните аналогичную структуру внутри вашего контура или продолжайте использовать облачный вариант.

Важно

Устанавливая программное обеспечение, вы соглашаетесь с условиями лицензионного соглашения с конечным пользователем.

Шаг 1. Подготовка к установке

1. Создайте кластер базы данных PostgreSQL.

   Пример того, как создать кластер PostgreSQL в облаке Яндекса, описан в Справке Yandex Cloud.
2. Настройте Object Storage и создайте в нем бакет.

   Объектное хранилище используется Досками для хранения файлов, в том числе загружаемых пользователями. Как начать работать с Yandex Object Storage, описано в Справке Yandex Cloud.

3. Сконфигурируйте сервер вашего провайдера идентификации.

   SAML (AD FS)

   Инструкция содержится в разделе Конфигурирование AD FS.

   OpenID (Keycloak)

   Инструкция содержится в разделе Конфигурирование Keycloak.

4. Подготовьте данные для задания параметров SSO.

   SAML (AD FS)

   Сохраните данные сертификата X509 по инструкции из раздела Настройка AD FS.

   OpenID (Keycloak)

   Воспользуйтесь инструкцией из раздела Настройка Keycloak.

5. Подготовьтесь к работе с Kubernetes:
   5.1. Создайте кластер Kubernetes.

   Пример того, как создать кластер Kubernetes и группу узлов в этом кластере, используя облако Яндекса, описан в Справке Yandex Cloud.

   5.2. Установите менеджер пакетов Helm.

   На macOS это можно сделать при помощи команды:

   ```
   brew install helm
   ```

   Порядок установки на другие системы описан в документации к Helm.

   5.3. Зарезервируйте IP-адрес вашего балансировщика нагрузки.

   Балансировщик нагрузки используется сервисом для распределения трафика. Как зарезервировать IP-адрес при использовании Yandex Cloud, описано в Справке.

   5.4. Настройте DNS-запись типа A для вашего домена и укажите в ней IP-адрес балансировщика.

   Вы можете создать A-запись:

   - В личном кабинете на сайте регистратора — если домен не делегирован на Яндекс. Что значит «делегирован»?
   - В кабинете организации Яндекс 360 для бизнеса по инструкции — если домен делегирован на Яндекс.

Шаг 2. Получение и настройка пакета Helm

1. Скачайте ZIP-файл с примером пакета Helm и распакуйте архив. Скачать

   Пакет содержит в себе:

   - папку `templates` с шаблонами манифестов Kubernetes;
   - файл `chart.yaml` — чарт для развертывания сервиса в Kubernetes;

- файл `values.yaml` со списком конфигурационных параметров.

2. Задайте значения для параметров конфигурации — в текстовом редакторе откройте файл `values.yaml` и отредактируйте его, указав значения параметров в соответствии с комментариями.

   Содержание файла `values.yaml`

```
image:
  repository: docker-registry.pruffme.com/whiteboard
  pullPolicy: IfNotPresent

# Первый запуск chart выполняется с --set install=true
install: false

resources:
  limits:
    memory: 6Gi
    cpu: "6"
  requests:
    memory: 512Mi
    cpu: "0.8"

# Сертификат TLS и приватный ключ. Имеют маску по домену
tls:
  crt: |-
    -----BEGIN CERTIFICATE-----
    MII***=
    -----END CERTIFICATE-----
  key: |-
    -----BEGIN PRIVATE KEY-----
    MII***=
    -----END PRIVATE KEY-----


# Доменное имя, по которому обращаются пользователи
domain: boards.domain.ru

# IP-адрес балансировщика нагрузки
loadBalancerIP: xx.xx.xx.xx

# Ключ лицензии
license: "demo"

# Тип СУБД, используемой в качестве основной (mongodb или postgres)
mainDatabaseType: postgres

# Порты контейнера приложения
ports:
  # Внешний порт, по которому обращаются конечные пользователи приложения
(ingress)
```

```
  https: 443
  # Внутренний порт, на котором приложение ожидает подключения
  inner: 443

livenessProbe:
  enabled: false
  path: /
  initialDelaySeconds: 30
  periodSeconds: 10
  timeoutSeconds: 5
  failureThreshold: 3
  successThreshold: 1
readinessProbe:
  enabled: false
  path: /
  initialDelaySeconds: 30
  periodSeconds: 10
  timeoutSeconds: 5
  failureThreshold: 5
  successThreshold: 1

# Параметры mongodb, СУБД и pod. Применяются, если mainDatabaseType ==
mongodb
mongodb:
  # Если используется внешняя СУБД mongodb, установите значение path, а также
укажите relatedContainers.mongodb.enabled: false в строке 208
  # Формат path: "mongodb://username:password@whiteboard-mongodb-
hostname:27017"
  path: ""
  # Имя базы данных
  database: "whiteboard"


# Параметры postgres, СУБД. Применяются, если mainDatabaseType == postgres
postgres:
  user: "pruffme"
  database: "editboard"
  password: "password"
  host: "host.net"
  port: 6432
  max: 20
  idleTimeoutMillis: 300000
  connectionTimeoutMillis: 200000
  maxUses: 7500

# Параметры redis
redis:
  enabled: true
  port: 6379
  pass: ""
  name: "whiteboard-redis"
```

```yaml
# Параметры clickhouse
clickhouse:
  enabled: false
  # Установите значение url, если используется внешняя СУБД clickhouse
  # Формат url: "http://whiteboard-clickhouse/
  url: ""
  # Следующие значения для подключения к СУБД (внешней или внутри pod), создания и настройки pod, создания БД
  ports:
    http: 8123
  database: "pruffme"
  username: "pruffme"
  password: "pruffme"
  flushNumber: 1

# Параметры S3 Object Storage
s3:
  # Версия AWS SDK
  version: 2
  # Идентификатор доступа пользователя. Используется вместе с секретным ключом для аутентификации запросов к хранилищу
  accessKey: "***"
  # Секретный ключ пользователя. Выступает в паре с идентификатором доступа для создания подписанных запросов
  secretKey: "***"
  # Название контейнера, который используется для хранения данных
  bucket: "boards"
  # URL сервиса хранилища
  endpoint: "https://storage.yandexcloud.net"
  # Регион, в котором расположено хранилище
  region: "ru-central1"
  # Часть URL в начале ссылки на файл. Обычно это путь к bucket
  publicPrefix: "https://storage.yandexcloud.net/boards/"
  # Параметр, который указывает, нужно ли использовать старый стиль при формировании пути к объектам в S3
  s3ForcePathStyle: false
  # Версия API, которую следует использовать при работе с S3
  apiVersion: "latest"
  # Список расширений файлов, которые поддерживаются для хранения. Позволяет ограничить типы файлов, которые могут быть загружены пользователями
  extensions:
    - "png"
    - "jpeg"
    - "jpg"
    - "pdf"
    - "docx"
    - "doc"
    - "xlsx"
    - "xls"
    - "pptx"
    - "ppt"
    - "mp4"
```

```
    - "mp3"
  acl: "public-read"

jwtkey: "testtest"

# Список модулей и их параметры
modules:
  test:
    enabled: true
    apiPartner: "test"
    apiKey: "1234567890abcdefgh1234567890abcd"
  sso:
    enabled: true
    moduleType: "sso"
    type: "saml"
    entryPoint: "https://adfs.domain.ru/adfs/ls"
    issuer: "https://boards.domain.ru/sso/"
    cert: "adfs/cert.crt"
    callbackUrl: "https://boards.domain.ru/sso/callback"
    fieldId: "nameID"
    fieldName: "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
    exitUrl: "https://boards.domain.ru"
    apiPartner: "sso"
    apiKey: "sso"
    x509:
      createSecret: true
      certificate: |
        -----BEGIN CERTIFICATE-----
        MII***==
        -----END CERTIFICATE-----
    admins:
      - "admin@domain.ru"

# Параметры резервных копий досок
dump:
  enabled: false
  # Время ожидания (в часах) после последнего изменения доски, по истечении
которого будет сделан снэпшот (моментальный снимок)
  dumpDashboardsWait: 1
  # Время (в часах) после создания последнего снэпшота, по истечении которого
будет автоматически создаваться резервная копия
  dumpDashboardsInterval: 6


# Параметры логирования действий во внешние системы
logs:
  enabled: false
  # Путь к файлу, в который будет записываться события из раздела "Журнал
событий" в формате CEF
  cefLog: "/home/user/log.cef"
  # Вывод логов в syslog
  syslog:
```

```
    ip: "127.0.0.1"
    port: 514
  # Список ID событий, которые не будут фиксироваться в логах
  skiplogs:
    - 11

# Параметры импорта объектов из Miro
miro:
  enabled: false
  # Клиентский номер приложения Miro (https://developers.miro.com/docs/try-out-the-web-sdk)
  clientId: "********"
  # Секретный ключ приложения
  secret: "****************"
  # Параметр, который задает, нужно ли сохранять в таблицу dashboards_import_tasks_items исходные объекты из Miro
  debug: true


# Данные для создания подов (pods) дополнительных сервисов в Kubernetes
# Указываются, если вы используете эти сервисы при работе с основным приложением и если такие поды еще не существуют в вашем контуре
relatedContainers:
  mongodb:
    enabled: false
    # Параметры mongodb для создания pod и подключения к нему
    image: mongodb/mongodb-community-server:6.0-ubi8
    name: whiteboard-mongodb
    port: 27017
    rootPassword: "whiteboard"
    username: "whiteboard"
    password: "whiteboard"
    persistence:
      enabled: true
      storageClass: "standard"
      accessModes:
        - ReadWriteOnce
      size: 10Gi
      pv:
        # persistent volume – создаётся только для локального тестирования (например, minikube), размещается на хосте
        create: false
        name: pv-001
        path: "/data/pv-001/"
  minio:
    # Параметры minio для создания pod и подключения к нему
    enabled: false
    image: bitnami/minio:latest
    name: "whiteboard-minio"
    storageHostname: storage.whiteboard.test
    rootUser: minio-root-user-whiteboard
    rootPassword: minio-root-insecured-password
```

```
    ports:
      api: 9000
      dashboard: 9001
    persistence:
      enabled: true
      storageClass: "standard"
      accessModes:
        - ReadWriteOnce
      size: 10Gi
      pv:
        # persistent volume – создаётся только для локального тестирования
(например, minikube), размещается на хосте
        create: false
        name: pv-002
        path: "/data/pv-002/"
  clickhouse:
    # Параметры clickhouse для создания pod и подключения к нему
    enabled: false
    image: clickhouse/clickhouse-server
    name: "whiteboard-clickhouse"
    persistence:
      enabled: true
      storageClass: "standard"
      accessModes:
        - ReadWriteOnce
      size: 10Gi
      pv:
        # persistent volume – создаётся только для локального тестирования
(например, minikube), размещается на хосте
        create: false
        name: pv-003
        path: "/data/pv-003/"

testJob:
  enabled: false
```

Подробное описание всех параметров приведено в разделе Описание параметров конфигурации приложения. Минимальный набор параметров, который обеспечивает работоспособность системы, приведен ниже.

2.1. Поле `image.repository` — адрес образа Яндекс Досок:

```
image:
    repository: <ССЫЛКА_НА_ОБРАЗ>
```

где `<ССЫЛКА_НА_ОБРАЗ>` — это адрес стандартного расположения образа: `docker-registry.pruffme.com/whiteboard`.

`whiteboard` содержит образ, который включает минимальный набор для запуска Яндекс Досок.

Если стандартное расположение образа напрямую недоступно

Ссылку на образ можно получить с помощью Container Registry.

1. Создайте реестр в Container Registry.

   Вы можете использовать Yandex Container Registry и работать с ним в облаке Яндекса: в консоли управления Yandex Cloud в списке сервисов выберите **Container Registry**, нажмите кнопку **Создать реестр** и задайте имя реестра. Полную информацию о порядке работы с Yandex Container Registry можно найти в документации Yandex Cloud.
2. Установите OrbStack — он понадобится для работы с Container Registry. На macOS это можно сделать при помощи команды:

   ```
   brew install orbstack
   ```

   Порядок установки на другие системы описан в документации к OrbStack.
3. Получите образ Яндекс Досок одним из способов:
   - Скачайте образ по ссылке `docker-registry.pruffme.com/whiteboard` при помощи Docker:

     ```
     docker pull docker-registry.pruffme.com/whiteboard
     ```

   - В случае, если репозиторий недоступен, получите образ в виде TAR-архива.
     1. Скачайте TAR-архив с образом по ссылке https://whiteboard.hb.ru-msk.vkcs.cloud/docker/whiteboard.tar:

        ```
        wget "https://whiteboard.hb.ru-
        msk.vkcs.cloud/docker/whiteboard.tar"
        ```

     2. Загрузите контейнер:

        ```
        docker load < whiteboard.tar
        ```
        ```
        ```
4. Загрузите образ Яндекс Досок в Container Registry.

   Если вы используете Yandex Container Registry:

   4.1. Присвойте скачанному Docker-образу тег вида `cr.yandex/<ИДЕНТИФИКАТОР_РЕЕСТРА>/<ИМЯ_DOCKER-ОБРАЗА>:<ТЕГ>:`.

   Например,

```
docker tag whiteboard
cr.yandex/<ИДЕНТИФИКАТОР_РЕЕСТРА>/whiteboard:latest
```

где `<ИДЕНТИФИКАТОР_РЕЕСТРА>` — идентификатор реестра из п.1.

4.2. Загрузите Docker-образ в репозиторий Container Registry:

```
docker push cr.yandex/<ИДЕНТИФИКАТОР_РЕЕСТРА>/whiteboard:latest
```

Инструкции для других систем могут отличаться.

После этого в файле `values.yaml` можно будет использовать ссылку на образ из Container Registry.

Например,

```
image:
    repository: cr.yandex/<ИДЕНТИФИКАТОР_РЕЕСТРА>/whiteboard:latest
```

2.2. Поля `tls.crt` и `tls.key` — сертификат TLS и приватный ключ вашего домена:

```
tls:
    crt: |-
        -----BEGIN CERTIFICATE-----
        MII***=
        -----END CERTIFICATE-----
    key: |-
        -----BEGIN PRIVATE KEY-----
        MII***=
        -----END PRIVATE KEY-----
```

2.3. Поле `domain` — адрес вашего домена:

```
domain: <ВАШ_ДОМЕН>
```

где вместо `<ВАШ_ДОМЕН>` укажите имя домена, на котором будет работать приложение.

2.4. Поле `loadBalancerIP` — IP-адрес вашего балансировщика нагрузки:

```
loadBalancerIP: XX.XX.XX.XX
```

где `XX.XX.XX.XX` — IP-адрес балансировщика, который вы зарезервировали в п.5.3. на шаге подготовки.

2.5. Поле `license` — лицензионный ключ. На этапе тестирования Яндекс Досок on-premises в этом поле можно указать значение `demo`:

```
license: "demo"
```

2.6. Поле `mainDatabaseType` — тип базы данных:

```
mainDatabaseType: postgres
```

2.7. Поле `postgres` — параметры базы данных PostgreSQL:

```
postgres:
    user: "pruffme"
    database: "editboard"
    password: "password"
    host: "host.net"
    port: 6432
```

2.8. Поле `s3` — параметры подключения к созданному в облачном хранилище бакету.

```
s3:
    version: 2
    accessKey: "***"
    secretKey: "***"
    bucket: "boards"
    endpoint: "https://storage.yandexcloud.net"
    region: "ru-central1"
    publicPrefix: "https://storage.yandexcloud.net/boards/"
    s3ForcePathStyle: false
```

2.9. Поле `modules.sso` — параметры модуля SSO:

SAML (AD FS)

```
modules:
    sso:
        enabled: true
        moduleType: "sso"
        type: "saml"
        entryPoint: "https://<ДОМЕН_СЕРВЕРА_AD_FS>/adfs/ls"
        issuer: "https://<ВАШ_ДОМЕН>/sso/"
        cert: "adfs/cert.crt"
        callbackUrl: "https://<ВАШ_ДОМЕН>/sso/callback"
        fieldId: "nameID"
        fieldName:
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
```

```
        exitUrl: "https://<ВАШ_ДОМЕН>"
        apiPartner: "sso"
        apiKey: "sso"
        x509:
            createSecret: true
            certificate: |
                -----BEGIN CERTIFICATE-----
                MII***==
                -----END CERTIFICATE-----
        admins:
            - "admin@domain.ru"
```

где укажите:

- вместо `<ДОМЕН_СЕРВЕРА_AD_FS>` — адрес домена, на котором развернута служба AD FS;
- вместо `<ВАШ_ДОМЕН>` — адрес вашего домена;
- в поле `x509.certificate` — данные сертификата X.509, которые вы сохранили в п.4. на шаге подготовки;
- в поле `sso.admins` — адреса администраторов вашей организации, которые получат доступ к администрированию Досок.

OpenID (Keycloak)

```
modules:
    sso:
        enabled: true
        module_type: "sso"
        type: "auth2"
        callback_url: "https://<ВАШ_ДОМЕН>/sso/callback"
        authorization_url:
"https://<ДОМЕН_СЕРВЕРА_KEYCLOAK>/realms/[realm_ID]/protocol/openid-
connect/auth"
        token_url:
"https://<ДОМЕН_СЕРВЕРА_KEYCLOAK>/realms/[realm_ID]/protocol/openid-
connect/token"
        info_url:
"https://<ДОМЕН_СЕРВЕРА_KEYCLOAK>/realms/[realm_ID]/protocol/openid-
connect/userinfo"
        scope: "openid profile email"
        authorization_type: "Bearer"
        field_id: "email"
        field_name: "name"
        client_id: "[client_id]"
        client_secret: "[client_secret]"
        whiteboard_api_partner: "kc"
        whiteboard_api_key: "kc_key"
        admins:
            - "admin@domain.ru"
```

где укажите:

- вместо `<ВАШ_ДОМЕН>` — адрес вашего домена;
- в полях `authorization_url`, `token_url`, `info_url` и `client_secret` — данные для задания параметров SSO, которые вы сохранили в п.4. на шаге подготовки;
- в поле `client_id` — идентификатор вашего приложения Досок из поля **Client ID** Keycloak, который вы сохранили в п.3. на шаге подготовки;
- в поле `sso.admins` — адреса администраторов вашей организации, которые получат доступ к администрированию Досок.

При использовании протокола OpenID помимо описания параметров SOO в файле `values.yaml` необходимо переопределить параметры в файле, который используется для создания ConfigMap в Kubernetes. Откройте файл `configmap-config.yaml` и замените код, содержащий параметры SSO, на блок следующего содержания:

```
not_var{{- if .Values.modules.sso.enabled }}
    "sso":{
        "module_type": "{{ .Values.modules.sso.module_type }}",
        "type": "{{ .Values.modules.sso.type }}",
        "callback_url": "{{ .Values.modules.sso.callback_url }}",
        "whiteboard_api_partner": "{{
.Values.modules.sso.whiteboard_api_partner }}",
        "whiteboard_api_key": "{{ .Values.modules.sso.whiteboard_api_key
}}",
        "authorization_url": "{{ .Values.modules.sso.authorization_url }}",
        "token_url": "{{ .Values.modules.sso.token_url }}",
        "info_url": "{{ .Values.modules.sso.info_url }}",
        "scope": "{{ .Values.modules.sso.scope }}",
        "authorization_type": "{{ .Values.modules.sso.authorization_type
}}",
        "field_id": "{{ .Values.modules.sso.field_id }}",
        "field_name": "{{ .Values.modules.sso.field_name }}",
        "client_id": "{{ .Values.modules.sso.client_id }}",
        "client_secret": "{{ .Values.modules.sso.client_secret }}",
        "admins":{{ .Values.modules.sso.admins | toJson }}
        },
not_var{{- end }}
```

Шаг 3. Запуск в режиме установки и конфигурирование

1. Запустите терминал и перейдите в папку с распакованным архивом.
2. Запустите приложение в режиме установки.

   На режим установки указывает значение `true` параметра `install`. Запуск можно произвести с помощью команды:

```
helm install whiteboard . --set install=true
```

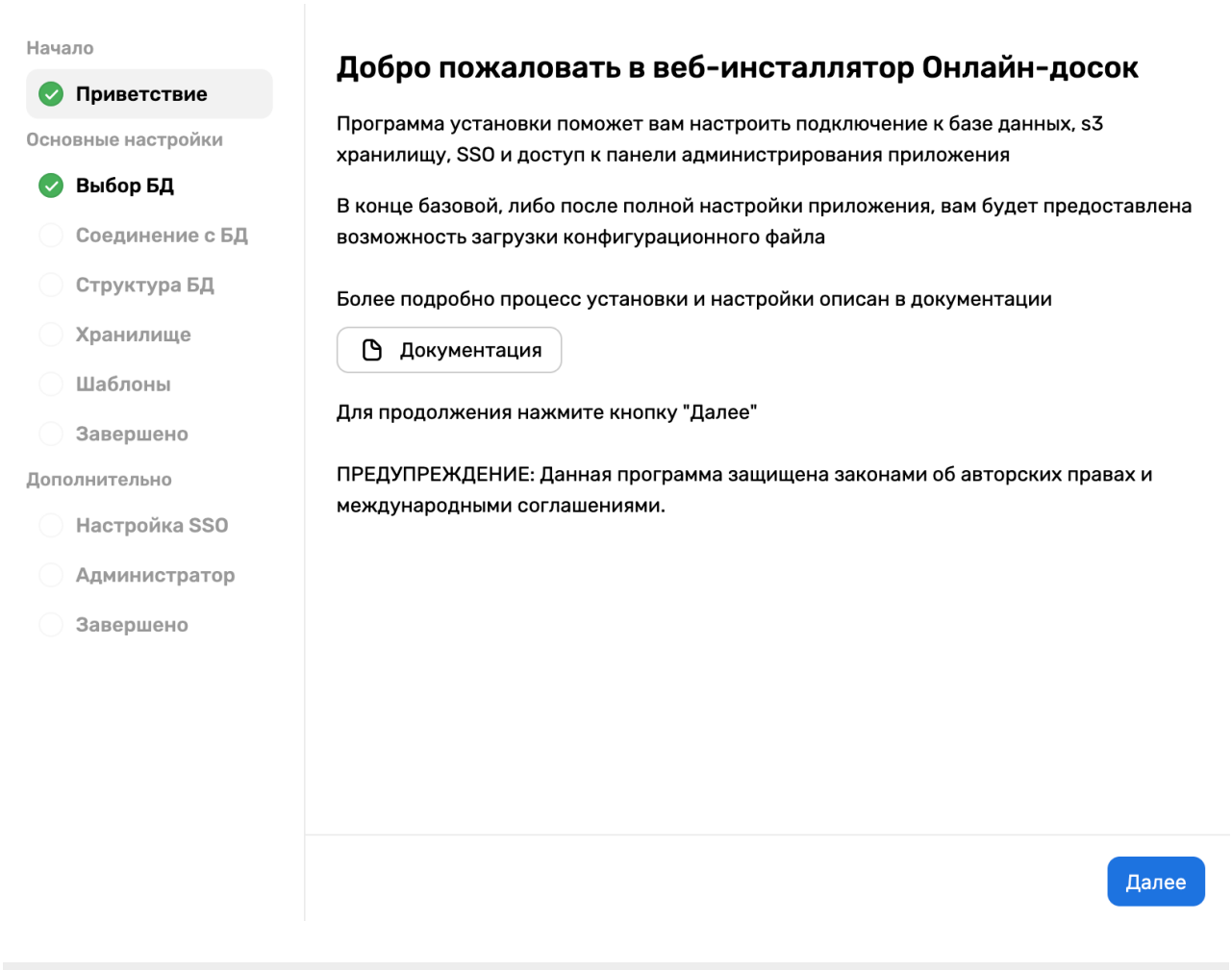
3. Сконфигурируйте настройки сервера с помощью веб-инсталлятора. Большинство параметров будут предзаполнены на основании данных из файла `values.yaml`.

   3.1. Запустите веб-инсталлятор.

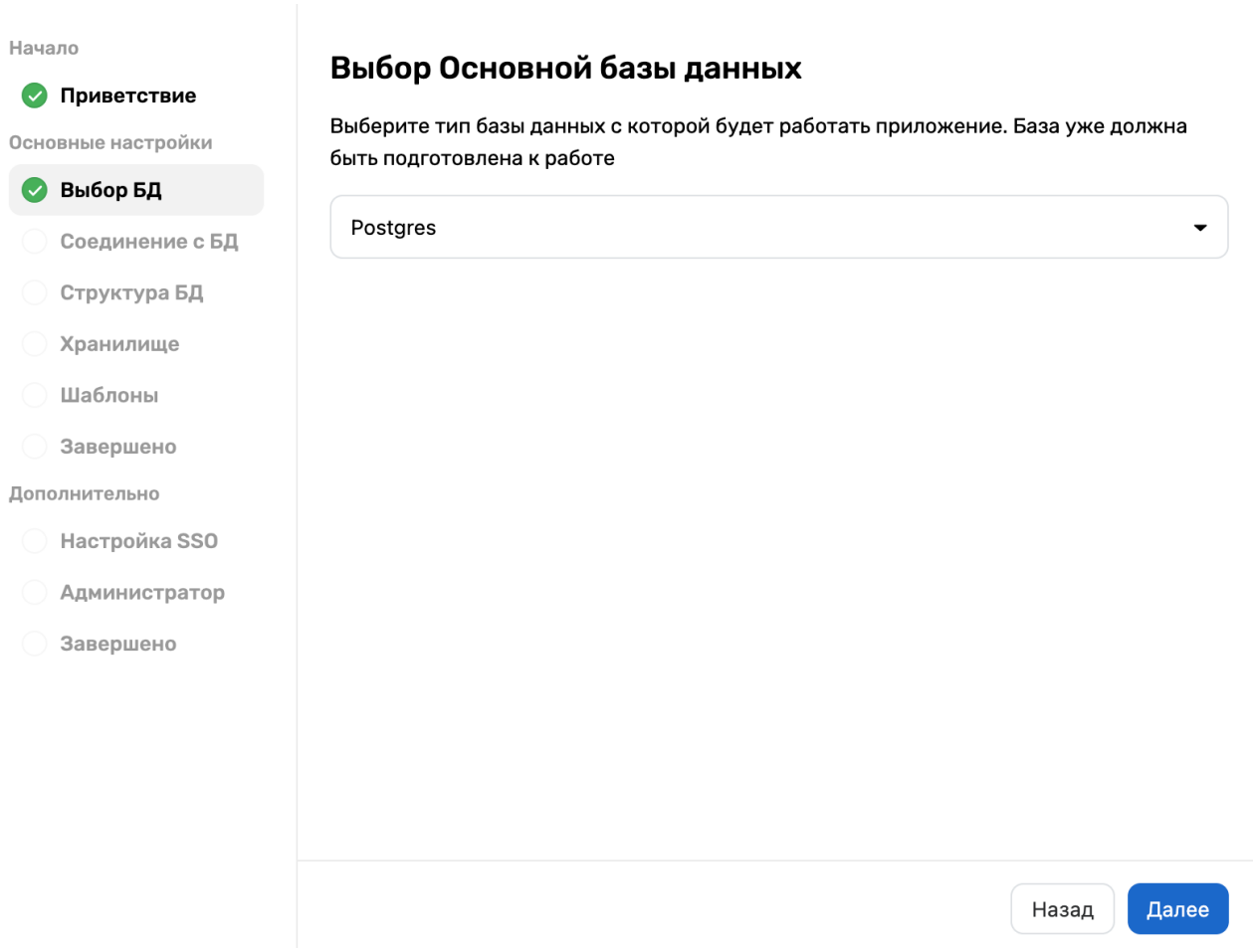
   Для этого перейдите по ссылке `https://<АДРЕС_СЕРВЕРА_ДОСОК>`, где вместо `<АДРЕС_СЕРВЕРА_ДОСОК>` — укажите адрес сервера Яндекс Досок, который доступен:

   - по IP-адресу балансировщика, зарезервированного в п.5.3 на шаге подготовки;
   - по домену, к которому вы привязали IP-адрес балансировщика п.5.4 на шаге подготовки.
     Подставьте в адрес одно из этих значений.

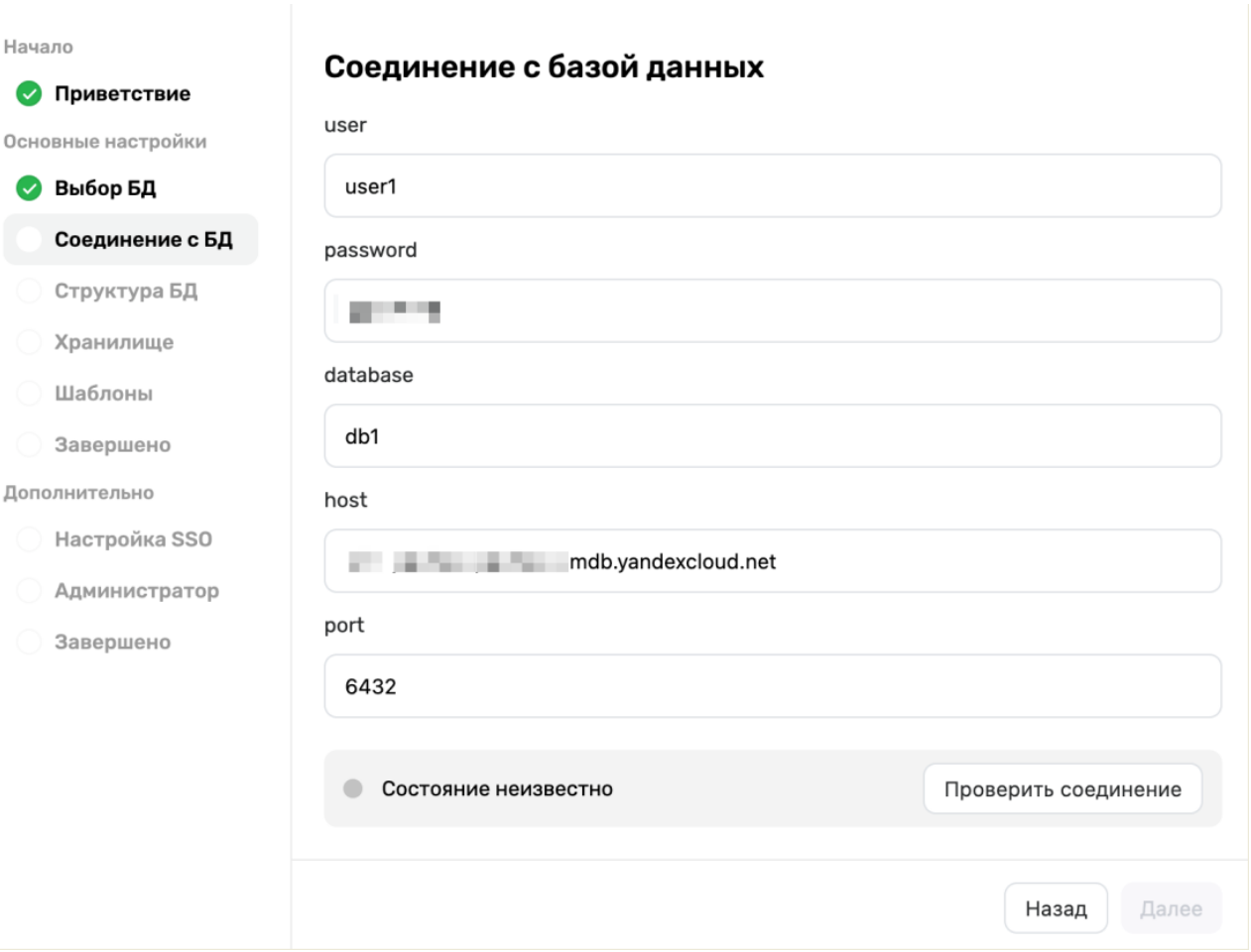
   3.2. В окне приветствия нажмите **Далее**.



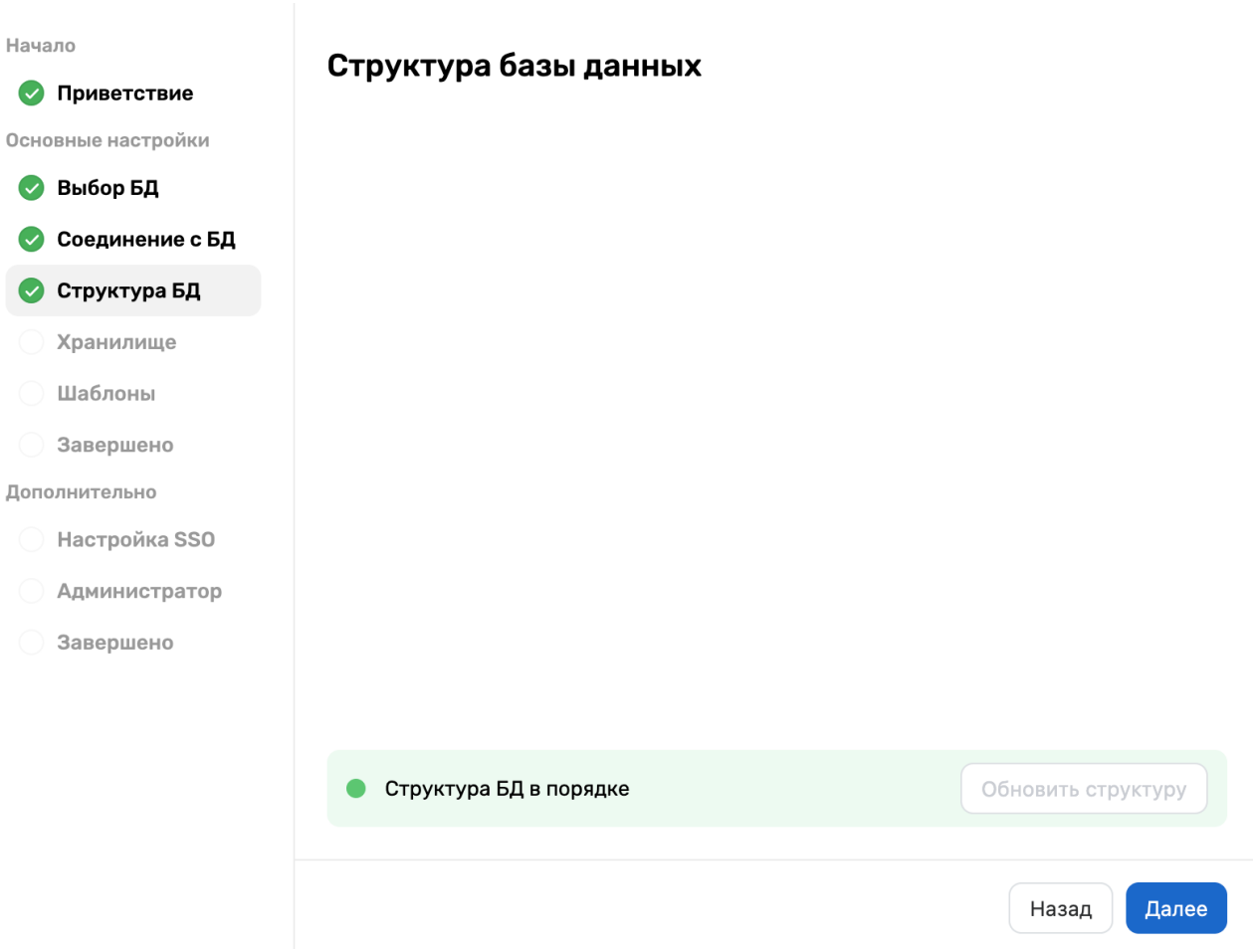
   3.3. Выберите базу данных Postgres и нажмите **Далее**.



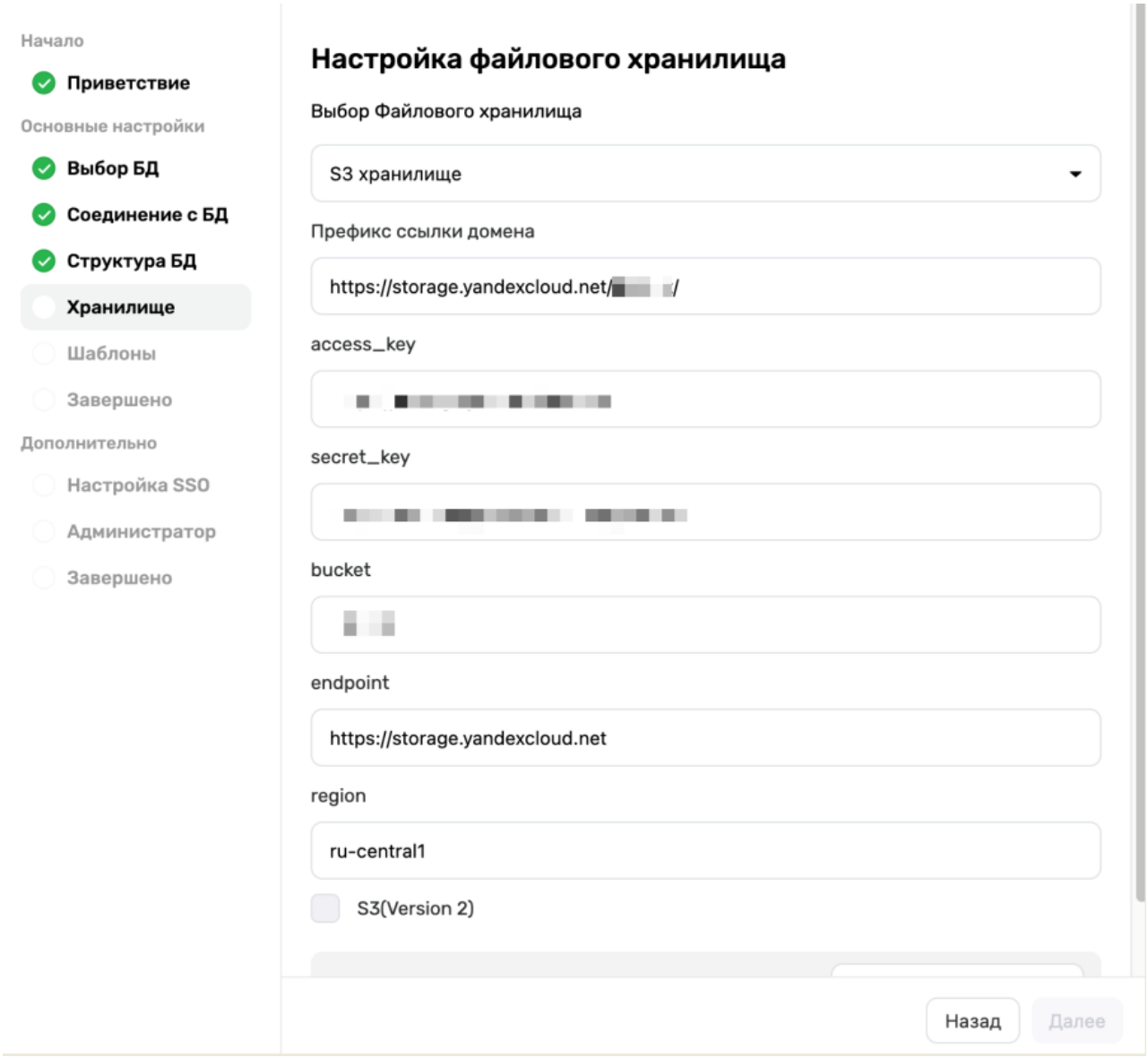
3.4. Проверьте параметры подключения к БД и проверьте соединение.



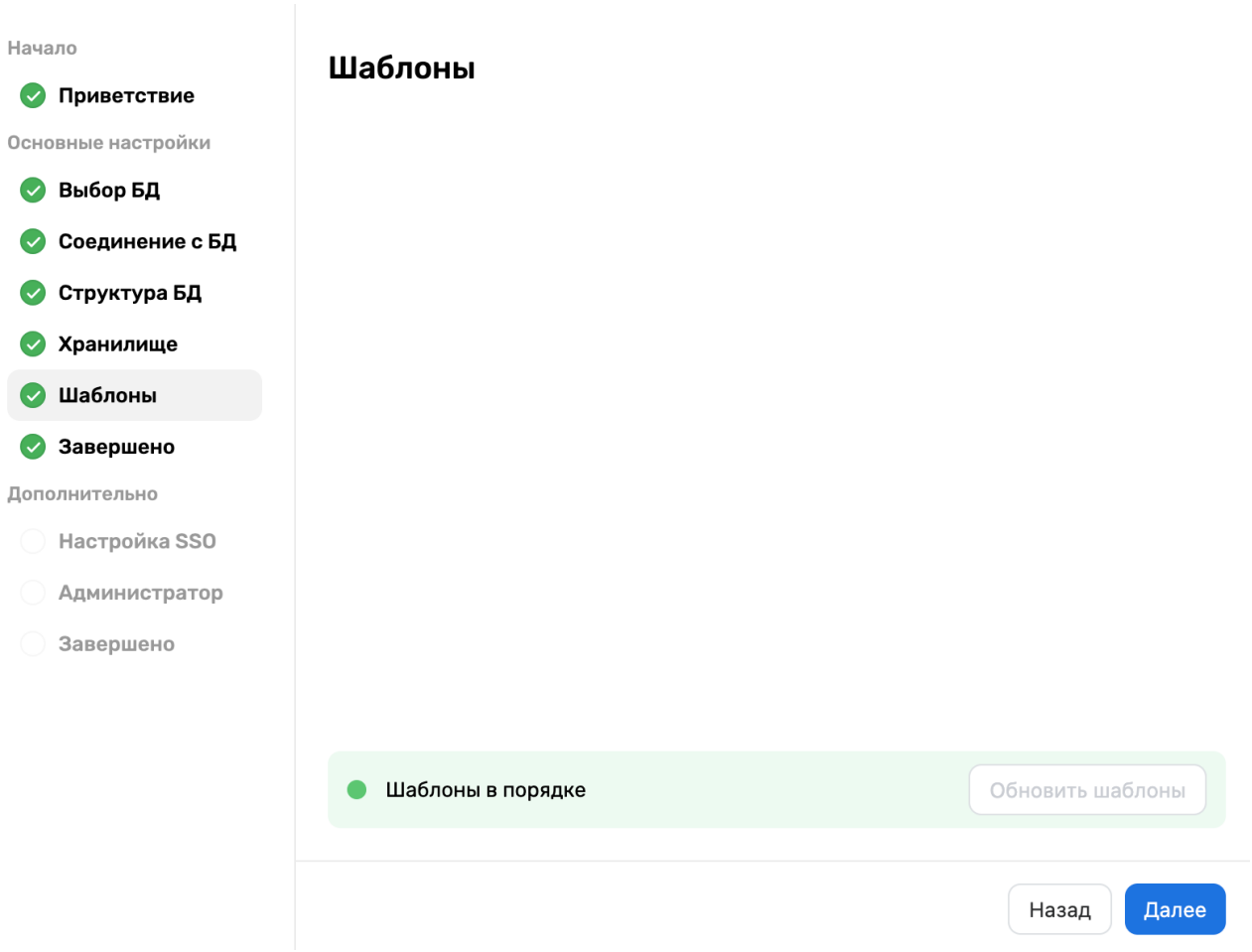
3.5. Обновите структуру базы данных.



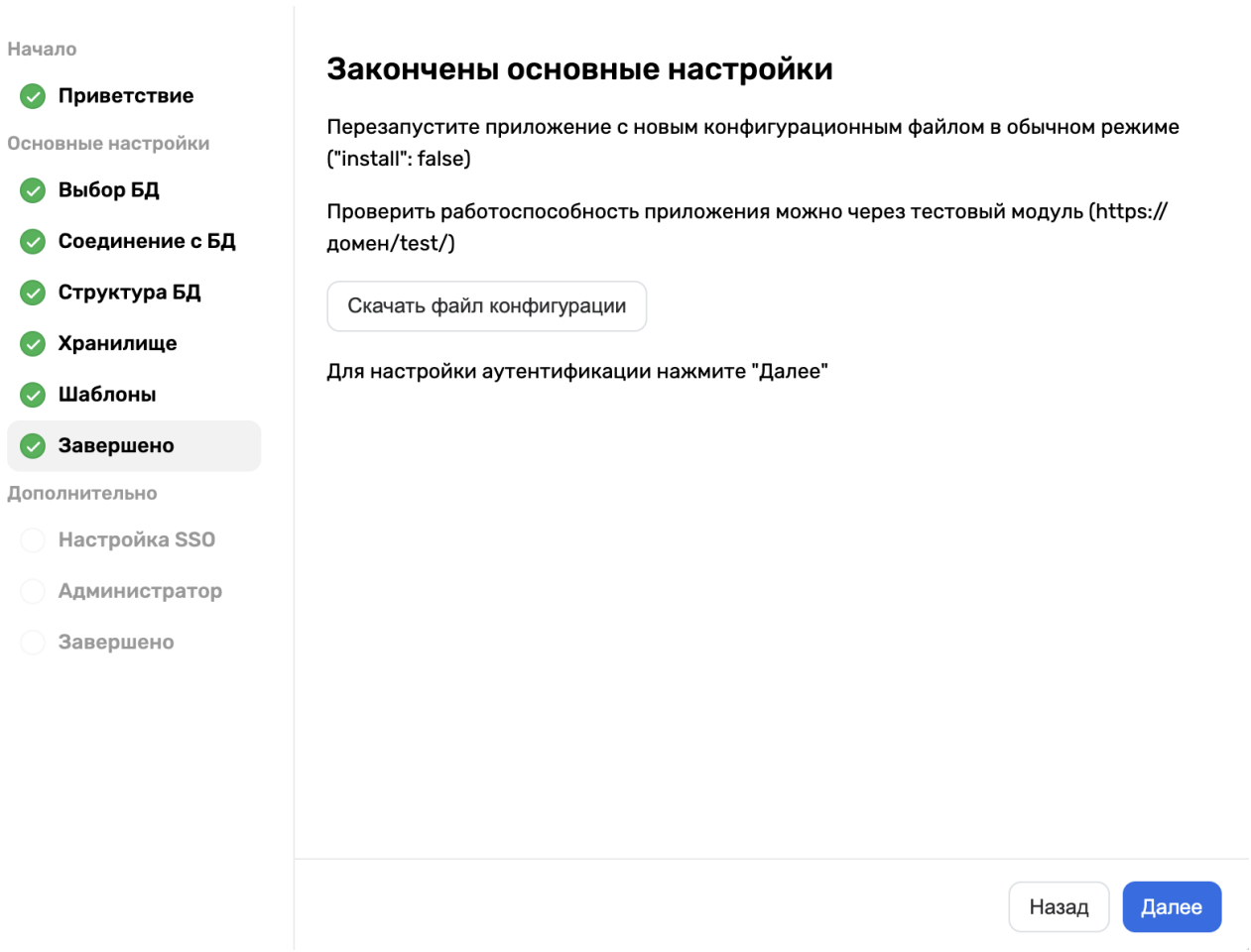
3.6. Проверьте настройки объектного хранилища.



3.7. Обновите шаблоны.

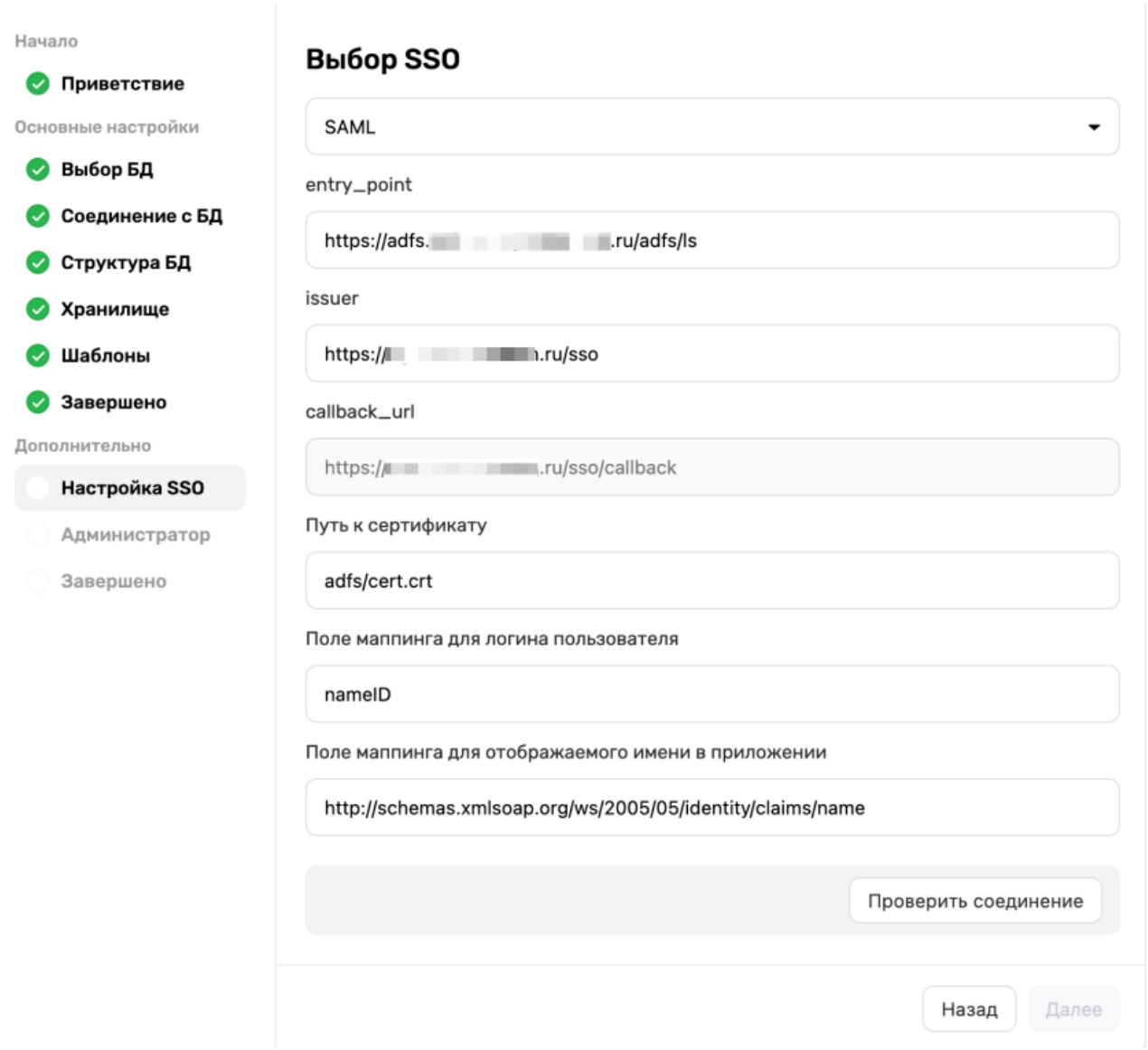


3.8. Подтвердите завершение основной настройки.

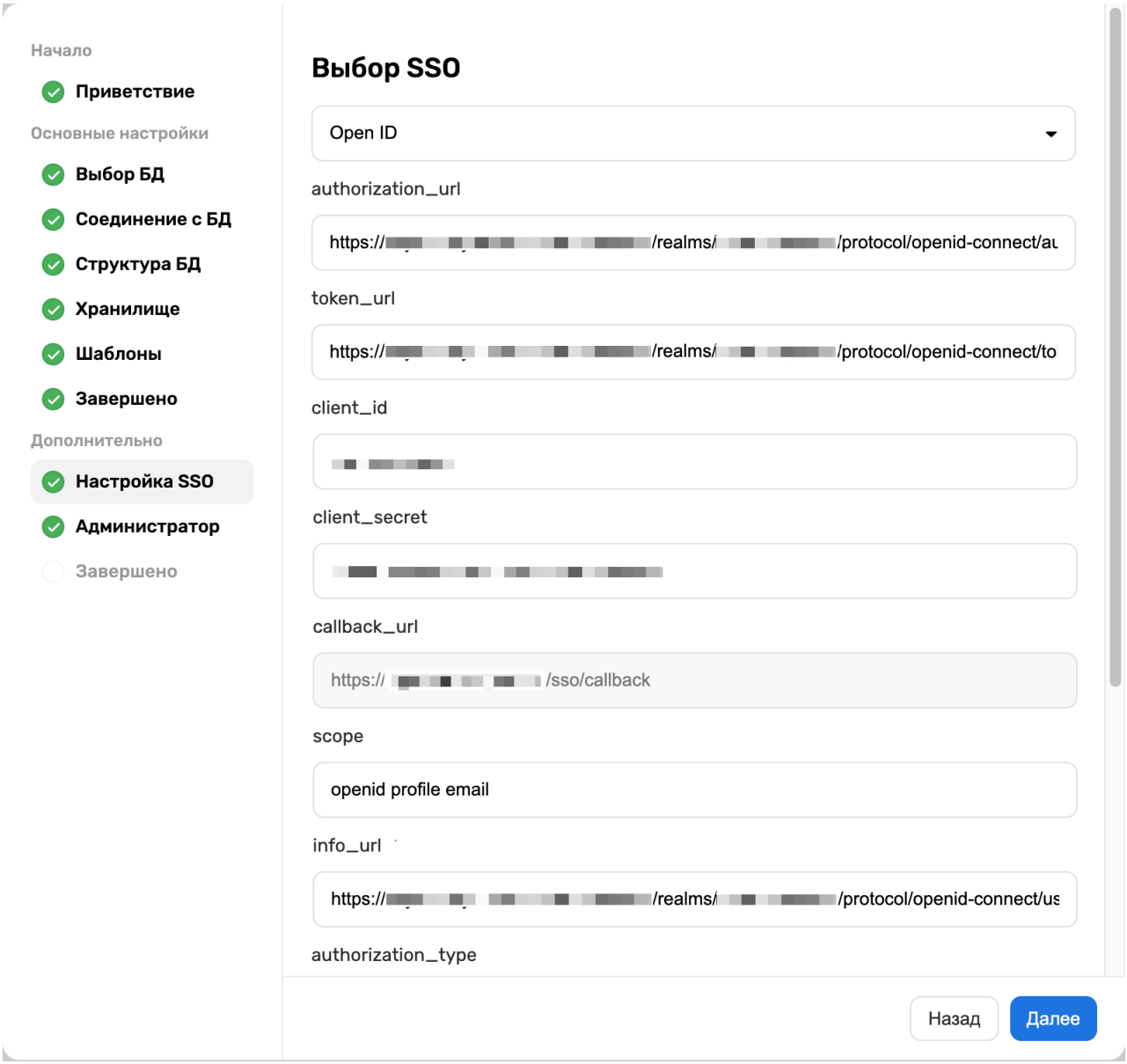


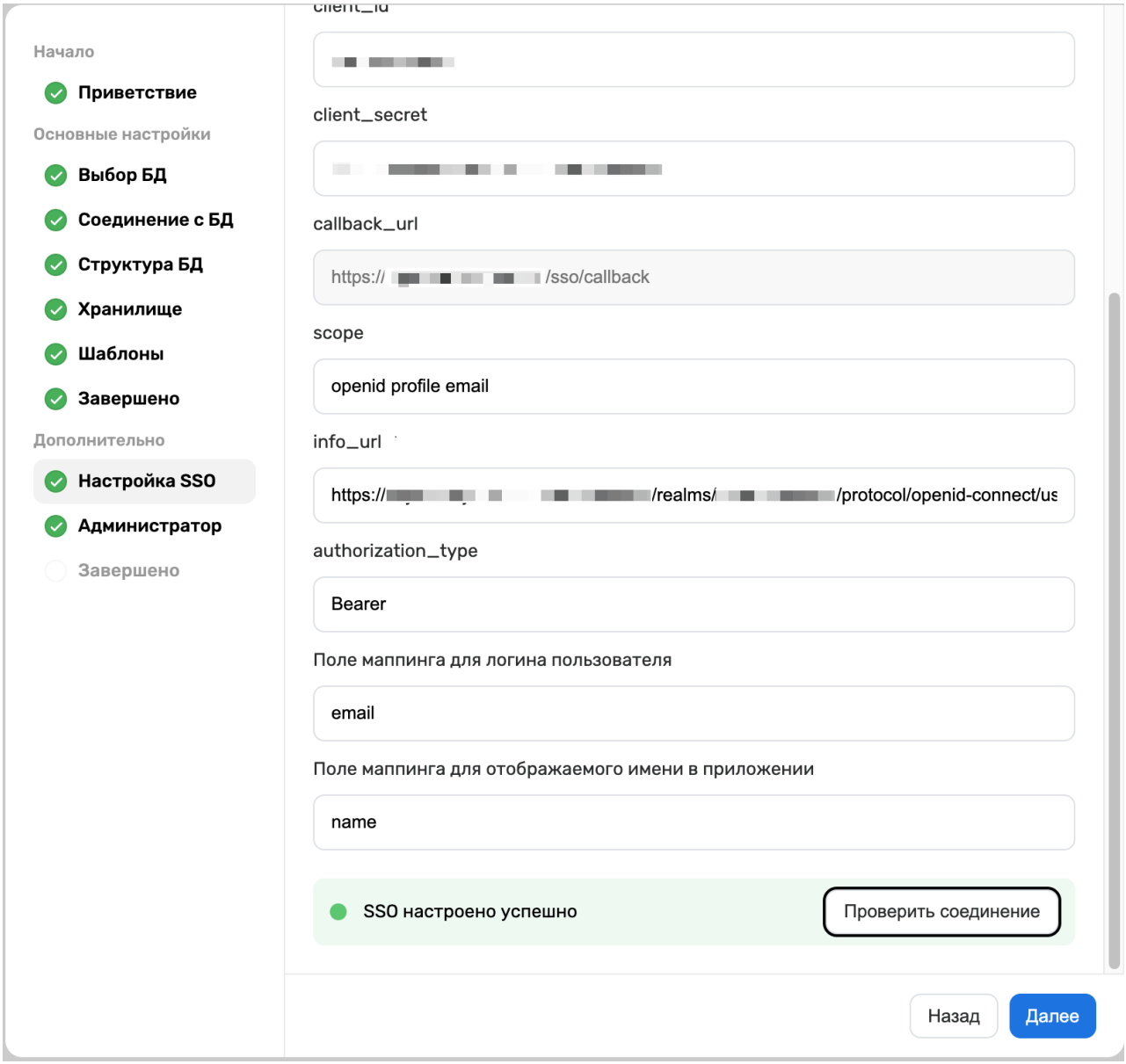
3.9. Проверьте параметры SSO.

SAML (AD FS)

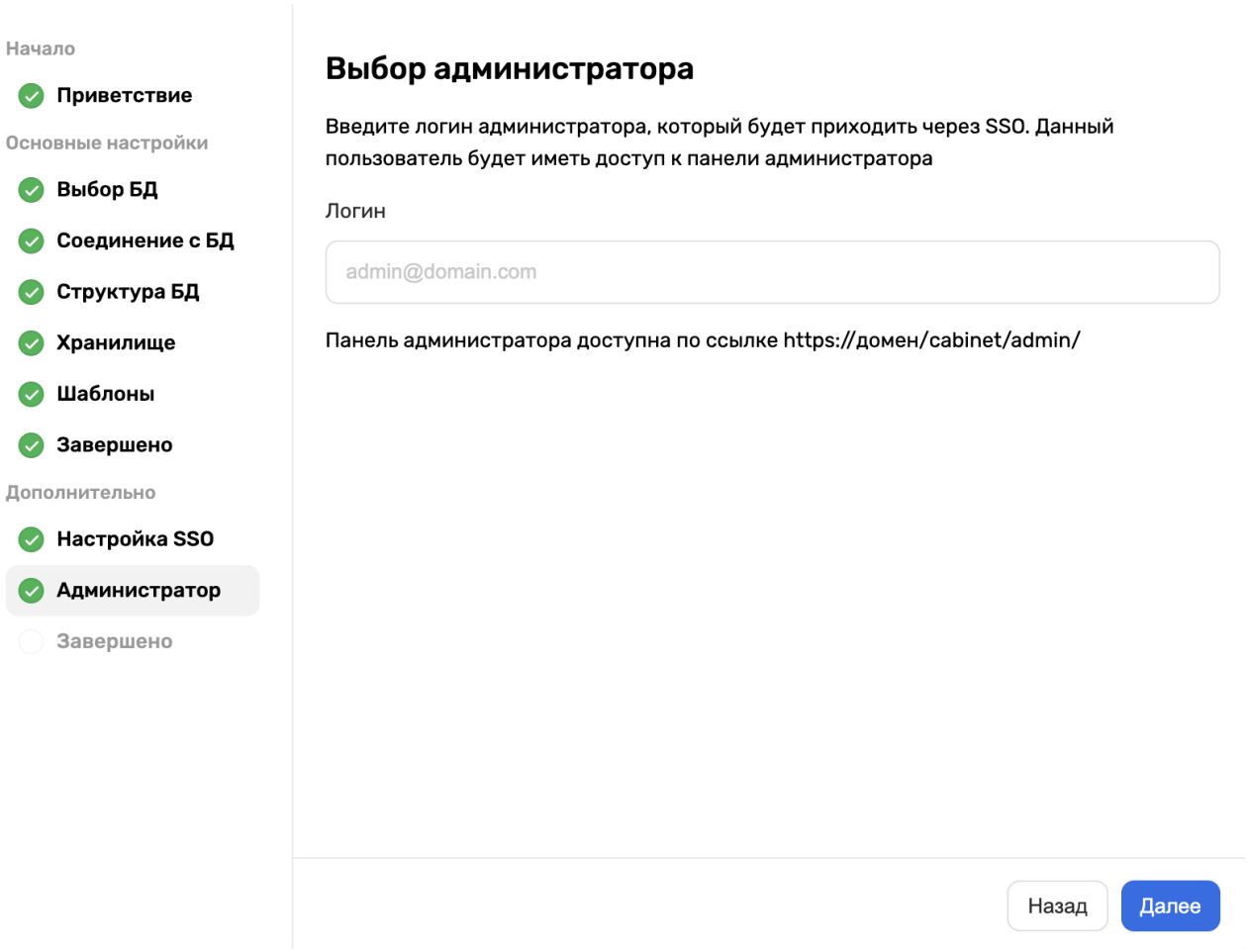


OpenID (Keycloak)

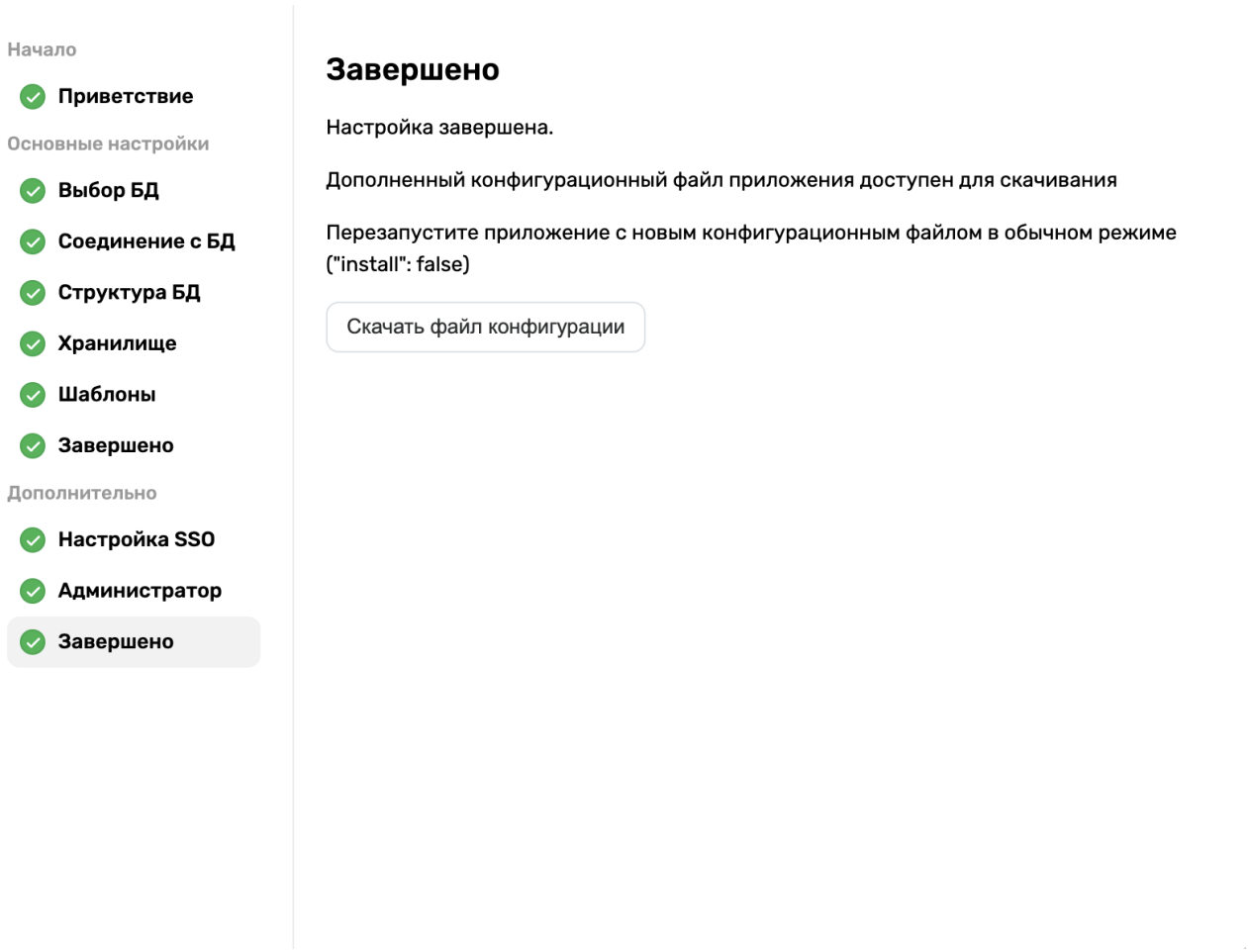

Начало
Приветствие
Основные настройки
Выбор БД
Соединение с БД
Структура БД
Хранилище
Шаблоны
Завершено
Дополнительно
Настройка SSO
Администратор
Завершено
Выбор SSO
Open ID
authorization_url
https://[redacted]/realms/[redacted]/protocol/openid-connect/au
token_url
https://[redacted]/realms/[redacted]/protocol/openid-connect/to
client_id
client_secret
callback_url
https://[redacted]/sso/callback
scope
openid profile email
info_url
https://[redacted]/realms/[redacted]/protocol/openid-connect/us
authorization_type
Назад
Далее



3.10. Если список администраторов вы задали в файле `values.yaml`, то в окне выбора администратора никаких дополнительных действий совершать не нужно, даже если поле **Логин** пустое.



3.11. Подтвердите завершение конфигурирования приложения.



Шаг 4. Обновление чарта и запуск в основном режиме

1. Обновите существующий чарт в кластере Kubernetes и установите для параметра `install` значение `false`:

   ```
   helm upgrade whiteboard . --set install=false
   ```

2. Перезапустите приложение.

   2.1. Получите список всех развертываний (Deployment):

   ```
   kubectl get deploy
   ```

   2.2. Перезапустите Deployment приложения Досок:

   ```
   kubectl rollout restart deployment/<DEPLOYMENT-NAME>
   ```

   где `<DEPLOYMENT-NAME>` — имя нужного развертывания, например `deployment-whiteboard`.

3. Проверьте работоспособность сконфигурированного приложения.
   - Основная версия личного кабинета доступна по ссылке `https://<ВАШ_ДОМЕН>/cabinet/`, где `<ВАШ_ДОМЕН>` — адрес домена, который вы указали в поле `domain` файла `values.yaml`.
   - Если по какой-то причине вы не смогли настроить SSO, но при этом хотите проверить работу сервера, то вы можете это сделать при помощи тестового модуля по ссылке `https://<ВАШ_ДОМЕН>/test/`.

Системные требования

Запуск тестового стенда

Такой тестовый стенд рассчитан ориентировочно на 50 пользователей. Минимальные системные требования для тестирования приложения:

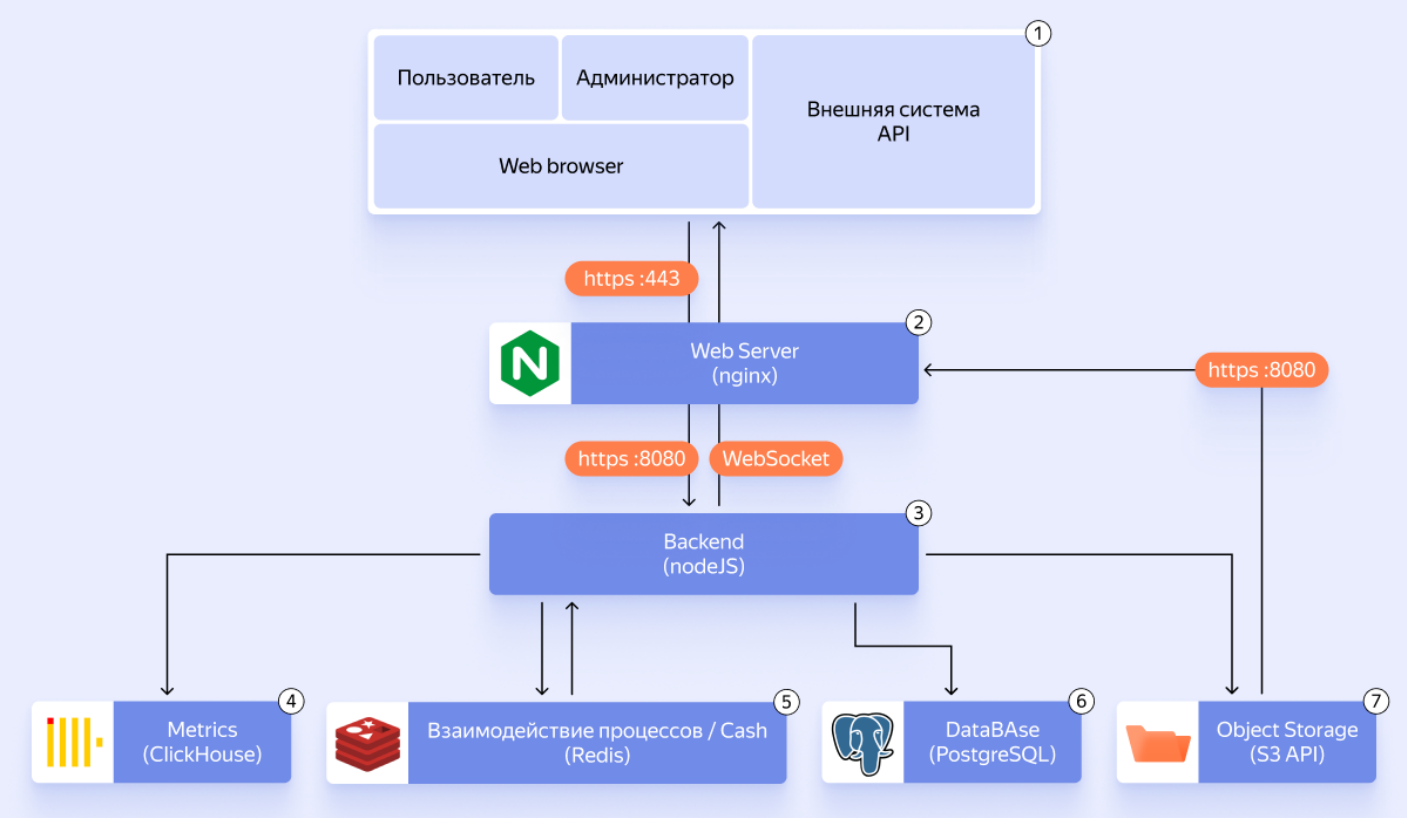
Параметр	Требования для тестового стенда
Платформа	Intel ice Lake
Процессор	2 ядра (vCPU)
Оперативная память	2 ГБ (RAM)
Место на диске	96 ГБ (HDD)
База данных	PostgreSQL 16
Операционная система	Astra Linux 1.7 или иная ОС с поддержкой Kubernetes (например, Ubuntu)
Провайдеры идентификации	• Keycloak (протокол SAML или OAuth 2.0); • Active Directory Federation Services (SAML); • Microsoft Active Directory (LDAP).

Развертывание приложения

Минимальные системные требования для развертывания приложения:

Параметр	Требования для развертывания
Платформа	Intel ice Lake
Процессор	Минимум 6 ядер (CPU)
Оперативная память	Минимум 8 ГБ (RAM)
Место на диске	Минимум 40 ГБ (Storage)
База данных	PostgreSQL 16
Операционная система	Astra Linux 1.7 или иная ОС с поддержкой Kubernetes (например, Ubuntu)
Провайдеры идентификации	• Keycloak (протокол SAML или OAuth 2.0); • Active Directory Federation Services (SAML); • Microsoft Active Directory (LDAP).

Архитектура приложения



1. **Клиент**
   В роли клиентов приложения могут выступать:
   - Пользовательский веб-браузер: Интерфейс, с которым взаимодействуют пользователи.
   - Внешняя система: Программы и сервисы, которые используют API для подачи запросов и взаимодействия с приложением.
2. **Веб-сервер**
   Nginx 1.18 отвечает за прием входящих HTTPS-запросов, перенаправление запросов на сервер приложения по HTTP, балансировку нагрузки между различными экземплярами сервера приложения, кеширование статического контента.
3. **Сервер приложения**
   Node.js 14.18.0 приложение, обрабатывающее бизнес-логику и взаимодействующее с другими компонентами системы. Обрабатывает входящие запросы по HTTP на порт 8080, поступающих от веб-сервера. Формирует ответы и отправляет их обратно через веб-сервер к клиенту. Используется многопроцессная архитектура для масштабирования нагрузки (запускается отдельный процесс для каждого ядра процессора).
4. **Агрегация статистики**
   ClickHouse обеспечивает хранение и обработку статистических данных. Например, позволяет сохранять информацию о количестве активных пользователей за день или месяц, количестве созданных объектов и т.д.
5. **Межпроцессное взаимодействие**
   Redis 2.8.0: Хранилище данных в памяти, используемое для обмена данными между процессами. Обеспечивает синхронизацию и координации между процессами, работающими

на разных ядрах процессора. Кеширует данные для ускорения доступа и уменьшения нагрузки на базы данных.

6. **Хранение структурированных данных**
   PostgreSQL используется для хранения досок, команд и проектов.
7. **Файловое хранилище**
   S3-совместимое хранилище, работающее по AWS SDK v2 и v3. Служит для размещения пользовательских файлов различного типа (изображения, документы, медиа-файлы).

Подготовка к установке

Яндекс Доски on-premises в процессе своей работы взаимодействуют с другими программами и сервисами. Это значит, что перед началом установки Досок необходимо выполнить подготовительные шаги, которые позволят установить и настроить выбранные вами для работы с Досками инструменты.

В инструкциях ниже в качестве примера установки отдельных таких программ даны ссылки на документацию Yandex Cloud. На примере настройки этих программ в облачном хранилище вы сможете понять примерный порядок работы с ними в вашем кластере.

Установка базы данных

Приложение поддерживает работу с PostgreSQL. Базу данных можно установить как на то же устройство, куда вы будете устанавливать Яндекс Доски, так и на другое.

После установки и подключения к PostgreSQL создайте нового пользователя и базу данных:

```
CREATE DATABASE my_database;
CREATE USER my_user WITH ENCRYPTED PASSWORD 'my_password';
GRANT ALL PRIVILEGES ON DATABASE my_database TO my_user;
```

Данные `my_user` и `my_password` понадобятся при работе с веб-инсталлятором.

Пример того, как создать кластер PostgreSQL в Yandex Cloud, описан в Справке Yandex Cloud. Вы можете пользоваться сервисами в облаке Яндекса на этапе тестирования Досок.

Создание Object Storage

Object Storage используется Досками для хранения данных. Настройте и запустите объектное хранилище. Это может быть сделано в облачной платформе (AWS в Yandex Object Storage или MinIO) либо на собственном сервере.

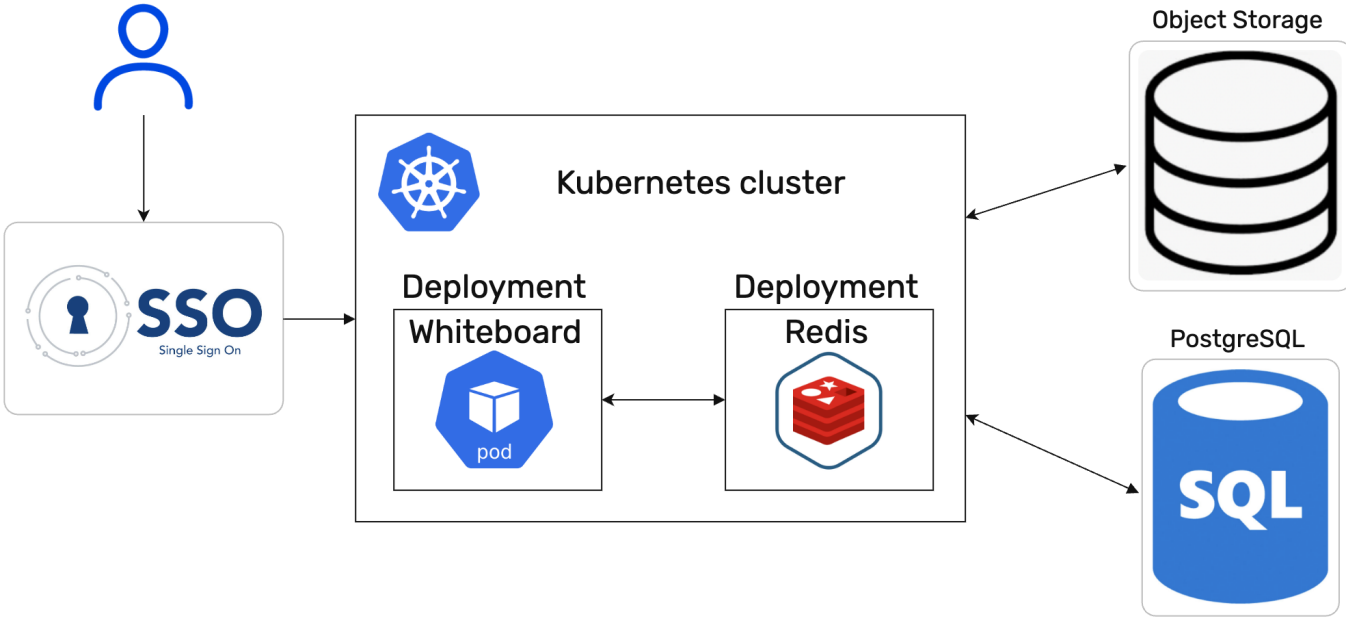
Как начать работать с Yandex Object Storage, описано в Справке Yandex Cloud.

Установка инструментов для работы с контейнеризированными приложениями

Kubernetes

Создайте кластер Kubernetes.

Пример возможной схемы взаимодействия компонентов при использовании Kubernetes для развертывания Досок



Пример того, как создать кластер Kubernetes в Yandex Cloud и группу узлов в этом кластере, описан в Справке.

Helm

Кроме кластера Kubernetes в некоторых вариантах установки вам может потребоваться менеджер пакетов Helm. Если вы выбрали метод установки Досок с помощью Helm:

1. Установите Helm.

   На macOS это можно сделать при помощи команды:

   ```
   brew install helm
   ```

   Порядок установки на другие системы описан в документации к Helm.
2. После запуска Helm в режиме установки, также запустится балансировщик нагрузки. Для дальнейшей настройки Яндекс Досок вам потребуется IP-адрес этого балансировщика. Узнать IP-адрес балансировщика можно при помощи команды:

   ```
   helm get svc
   ```

3. Для вашего домена настройте DNS-запись типа A и укажите в ней IP-адрес балансировщика.

   Вы можете создать A-запись:

   - в личном кабинете на сайте регистратора — если домен не делегирован на Яндекс; Что значит «делегирован»?
   - в кабинете организации Яндекс 360 для бизнеса по инструкции — если домен делегирован на Яндекс.

Описание параметров конфигурации приложения

В зависимости от сценария использования параметры конфигурации приложения могут существенно изменяться. В данном примере рассмотрен один из вариантов стандартной тестовой настройки config.json, содержание которого формируется на основании параметров, заданных в файле `values.yaml` из установочного пакета Helm.

```
{
    "install":false,
    "domain":"whiteboard.mycorp.com",
    "hostname":"whiteboard.mycorp.com",
    "license":"demo",
    "cert":{
        "crt":"/ssl/cert.crt",
        "key":"/ssl/cert.key"
    },
    "type":[
        "api",
        "socket",
        "upload",
        "coordinator",
        "admin"
    ],
    "master_process":0,
    "priority":1,
    "split_port":true,
    "inner_port":443,
    "https_port":443,
    "postgres":{
        "user":"user",
        "database":"db",
        "password":"passwd",
        "host":"xxxxx.mdb.yandexcloud.net",
        "port":6432,
        "max":20,
        "idleTimeoutMillis":300000,
        "connectionTimeoutMillis":200000,
        "maxUses":7500
    },
    "redis":{
        "host":"whiteboard-redis",
        "port": 6379,
        "pass":""
    },
    "s3":{
        "access_key":"access_key",
        "secret_key":"secret_key",
        "bucket":"bucket",
        "endpoint":"https://storage.yandexcloud.net",
        "region":"ru-central1",
```

```
        "public_prefix":"https://storage.yandexcloud.net/bucket/",
        "version":2,
        "version":2,

        "s3ForcePathStyle":false,
        "apiVersion":"latest",
        "extensions":
["png","jpeg","jpg","pdf","docx","doc","xlsx","xls","pptx","ppt","mp4","mp3"],
        "acl":"public-read"
    },
    "jwtkey":"testtest",
    "network":"eth0",
    "modules":{
        "sso":{
            "module_type": "sso",
            "type": "auth2",
            "callback_url": "https://whiteboard.mycorp.com/sso/callback",
            "whiteboard_api_partner": "kc",
            "whiteboard_api_key": "kc_key",
            "authorization_url":
"https://keycloak.yandex360tech.ru:8443/realms/realm_name/protocol/openid-
connect/auth",
            "token_url":
"https://keycloak.yandex360tech.ru:8443/realms/realm_name/protocol/openid-
connect/token",
            "info_url":
"https://keycloak.yandex360tech.ru:8443/realms/realm_name/protocol/openid-
connect/userinfo",
            "scope": "openid profile email",
            "authorization_type": "Bearer",
            "field_id": "email",
            "field_name": "name",
            "client_id": "brds",
            "client_secret": "client_secret",
            "admins":["name@yourdomain.ru"]
            },
        "test":{
            "whiteboard_api_partner":"test",
            "whiteboard_api_key":"1234567890abcdefgh1234567890abcd",
            "db_users_only": true
        }
    },
    "recording":{
        "ffmpeg_path":"/usr/bin/ffmpeg",
        "ffmpeg_audio_codec":"aac"
    },
    "cabinet":{
        "path":"cabinet"
    }
}
```

Значения параметров конфигурации приложения

Примечание

Некоторые секции конфигурации рассмотрены подробнее в соответствующих разделах
SSO - Настройка SSO
Object Storage - Настройка Object Storage

Параметр	Описание	Тип данных
install	Режим установки. Если `true`, то создается БД, коллекций в ней, а также импорт шаблонов. `false` — для обычного запуска. Нельзя удалять из конфигурации	Логический
license	Для хранения лицензионного ключа	Строка
hash	Хеш имя сервера (например название данного сервера)	Строка
hostname	Имя хоста на котором работает приложение	Строка
domain	Доменное имя на котором работает приложение	Строка
version	Текущая версия приложения	Строка
cert	Путь до сертификатов cert.crt и cert.key	Объект
type	Массив с перечнем ролей сервера	Массив
master_process	Параметр для управления процессами приложения	Число
priority	Требует настройки, только если сервер имеет роль `redis` или `coordinator`	Число
split_port	Служебный параметр	Логический
clickhouse	Настройка подключения к ClickHouse	Объект
inner_port	Порт для внутреннего трафика приложения	Число
https_port	Порт для защищенного HTTPS трафика. По нему отправляем запросы к приложению	Число
redis	Настройки подключения к Redis, включая хост, порт и пароль	Объект
jwtkey	Ключ для генерации и верификации JWT токенов	Строка

network	Сетевой интерфейс, который используется приложением	Строка
modules	Конфигурация модулей приложения. Например test модуль или SSO	Объект
recording	Настройки для записи медиа, включая путь к ffmpeg и используемый аудиокодек	Объект
s3	Конфигурация для подключения к хранилищу S3	Объект
cabinet	Путь к основной версии личного кабинета*	Объект
dump	Настройка свойств резервных копий досок*	Объект
logs	Настройка свойств логирования действий во внешние системы*	Объект
miro	Настройка параметров для импорта объектов из Miro*	Объект
ldap	Управление периодичностью синхронизации по LDAP	Объект

Расширенное описание для вложенных секций

Описание секции `cert`

```
    "cert": {
        "crt": "/conf/ssl/cert.crt",
        "key": "/conf/ssl/cert.key"
    },
```

Параметр	Описание	Тип данных
crt	Путь до открытого ключа	Строка
key	Путь до закрытого ключа	Строка

Описание секции `type`

```
    "type":[
        "api",
        "socket",
        "upload",
        "clickhouse",
        "redis",
        "admin",
        "avp",
```

```
        "coordinator",
        "convert_video",
        "convert_documents",
        "miro"
    ],
```

Параметр	Описание	Тип данных
`api`	Фронт сервера. Отвечают за распределение по сокетам	Строка
`socket`	WebSocket сервер	Строка
`upload`	Сервер, на который загружаем файлы и выгружаем в s3 хранилище	Строка
`clickhouse`	Сервер, на который отправляются статистику для агрегации и обработки	Строка
`redis`	Устанавливается для одного сервера, через который предполагается обрабатывать запросы от остальных частей приложения. Если несколько серверов, то у каждого должен быть свой `priority`	Строка
`coordinator`	Служит для выполнения единых cron задач (например, автоматическое удаление неактивных пользователей или синхронизации LDAP)	Строка
`admin`	Сервер для администрирования приложения, мониторинга и статистики	Строка
`avp`	Сервер с установленным антивирусным ПО	Строка
`convert_video`	Сервер на котором выполняется обработка видеоматериалов	Строка
`convert_documents`	Сервер на котором выполняется обработка документов (pdf и т.д.)	Строка
`miro`	Сервер на котором выполняется импорт и обработка досок из Miro	Строка

Описание секции `redis`

```
    "redis": {
        "host": "127.0.0.1",
        "port": 6379,
```

```
        "pass": "vMotn8dZTGddfhdfzcvndDN0tj0********"
    },
```

Параметр	Описание	Тип данных
`host`	ip адрес используемого Redis сервера	Строка
`port`	Порт работы Redis	Число
`pass`	Пароль для подключения к Redis, может быть произвольным	Строка

Описание секции `clickhouse`

```
    "clickhouse": {
        "url": "http://137.139.132.2/",
        "port": 8123,
        "database": "clickhouse",
        "username": "default",
        "password": "DefaultPassword"
    },
```

Либо

```
    "clickhouse": {
        "disabled" : true
    },
```

Параметр	Описание	Тип данных
`url`	ip адрес используемого ClickHouse сервера	Строка
`port`	Порт работы ClickHouse	Число
`database`	Название базы к которой выполняется подключение	Строка
`username`	Имя пользователя ClickHouse, которое будет использоваться для подключения к базе данных	Строка
`password`	Пароль для пользователя, указанного в параметре `username`	Строка
`disabled`	Параметр отвечает за включение или отключение поиска подключения к базе ClickHouse. Если не используется подключение к ClickHouse, установить значение `true`	Строка

Описание секции `modules`

```
"modules": {
        "test": {
            "whiteboard_api_partner": "test",
            "whiteboard_api_key": "1234567890abcdefgh1234567890abcd"
        },
        "sso": {
            ...
        }
    },
```

Параметр	Описание	Тип данных
`test`	Модуль для базовой проверки работоспособности приложения	Объект
`sso`	Модуль для настройки доменной авторизации. Описан отдельно в разделе Настройка SSO	Объект
(другие модули в зависимости от сборки приложения)	В некоторых случаях могут быть добавлены и иные модули, созданные с использованием API приложения	Объект

Описание секции `recording`

```
    "recording": {
        "ffmpeg_path": "/usr/bin/ffmpeg",
        "ffmpeg_audio_codec": "aac"
    },
```

Параметр	Описание	Тип данных
`ffmpeg_path`	Путь к исполняемому файлу ffmpeg. Например `/usr/bin/ffmpeg`	Строка
`ffmpeg_audio_codec`	Выбор аудио кодека AAC при использовании ffmpeg. По умолчанию `aac`	Строка

Описание секции `cabinet`

Параметр `cabinet` не является обязательным для версии приложения от 1.6.0 и выше

```
"cabinet": {
    "path": "cabinet"
}
```

Параметр	Описание	Тип данных
`path`	Составная часть, которая используется для формирования URL к основной версии личного кабинета	Строка

Описание секции `dump`

```
"dump": {
    "dump_dashboards_interval":6,
    "dump_dashboards_wait":1
}
```

Параметр	Описание	Тип данных
`dump_dashboards_interval`	Интервал в часах автоматического создания после отсутствия изменений указанный в dump_dashboards_wait	Число
`dump_dashboards_wait`	Время ожидания в часах, через сколько после последнего изменения будет сделан снапшот	Число

Описание секции `logs`

```
"logs":{
    "cef_log":"/home/user/log.cef",
    "syslog":{
        "ip":"127.0.0.1",
        "port":"514"
    },
    "skiplogs":[11]
}
```

Параметр	Описание	Тип данных
`cef_log`	Путь к файлу в который будет записываться события из раздела «Журнал событий» в формате CEF	Строка
`syslog`	Позволяет включить вывод логов в syslog	Логический или Объект
`skiplogs`	Можно указать список ID событий, которые не будут фиксироваться в логах	Массив (Число)

Описание ID событий в журнале логирования

ID	Описание
10	Команда создана
11	Команда отредактирована
12	Команда удалена
21	Участник команды создан
22	Участник команды изменен
23	Участник команды удален
31	Доска создана
32	Доска изменена
33	Доска удалена
34	Гостевой доступ включен
35	Гостевой доступ выключен
37	Доска Miro импортирована
40	Проект в команде создан
41	Проект в команде изменен
42	Проект в команде удален
50	Пользователь создан
51	Пользователь изменен

52	Пользователь удален
53	Пользователь восстановлен
54	Для пользователя изменен логин
60	Пользователь авторизовался
61	Пользователь разлогинился
70	Роль добавлена
71	Роль изменена
72	Роль удалена
80	Вложение загружено
81	Вложение удалено
105	LDAP соединение создано
106	LDAP соединение удалено
110	LDAP правило создано
111	LDAP правило изменено
112	LDAP правило удалено
120	LDAP администратор создан
121	LDAP администратор удален

Описание секции `miro`

```
"miro":{
     "clientId":"********",
     "secret":"****************",
     "debug":true
 }
```

Параметр	Описание	Тип данных
`clientId`	Клиентский номер приложения Miro (https://developers.miro.com/docs/try-out-the-web-sdk)	Строка
`secret`	Секретный ключ приложения	Строка

`debug`	Сохранять или нет в таблицу dashboards_import_tasks_items исходные объекты из Миро	Логический

Подробнее о настройке механизма импорта можно узнать на данной странице

Описание секции `ldap`

```
"ldap": {
    "interval": 120,
    "debug": true
}
```

Параметр	Описание	Тип данных
`interval`	Количество секунд между запуском процедуры синхронизации по LDAP	Число
`debug`	Показ расширенной информации во время выполнения операции	Логический

Дополнительные параметры приложения (версия 1.8.0 +)

postgres

```
"postgres": {
    "user": "postgres",
    "database": "postgres",
    "password": "PruffmeTest",
    "host": "editboard.mycorp.com",
    "port": "5432"
},
```

Параметр	Описание	Тип данных
`postgres`	Количество секунд между запуском процедуры синхронизации по LDAP	Объект
`user`	Имя пользователя PostgreSQL, которое будет использоваться для подключения к базе данных	Строка
`database`	Название базы данных, к которой будет осуществляться подключение	Строка

`password`	Пароль для пользователя, указанного в параметре user	Строка
`host`	Адрес сервера, на котором размещена база данных	Строка
`port`	Номер порта, который используется для подключения к базе данных	Строка

```
{
    ...
    "serveradmin":"all",
    ...
}
```

Параметр	Описание	Тип данных
`serveradmin`	Если выставлено all, то доступ к разделу «Инстансы» и «Мигратор» предоставляется всем администраторам системы. Для того, чтобы ограничить доступ к данному разделу определенными администраторами, необходимо указать их логины в массиве (["example.admin@editboard.com"])	Массив (Строка) / Строка

admin_stat_interval

```
{
    ...
    "admin_stat_interval" : 30,
    ...
}
```

Параметр	Описание	Тип данных
`admin_stat_interval`	Интервал в секундах между записями мгновенной статистики (пользователи, запушенные доски в моменте)	Число

preventcentral

```
{
    ...
    "preventcentral" : true,
    ...
}
```

Параметр	Описание	Тип данных
`preventcentral`	Управляет возможность включать и отключать страницу выбора SSO	Логический

Дополнительные параметры приложения (версия 1.10.0 +)

whiteboard_properties

```
{
    ...
    "modules": {
        "sso": {
            ...
            "whiteboard_properties":{
                "objects":{
                    "menu":{
                        "disable_links":true
                    }
                },
                "media":{
                    "hide_presentation":true,
                    "hide_video":false,
                    "hide_audio":true,
                    "hide_youtube":true,
                    "hide_attachment":true
                },
                "comments":{
                    "disable_links":true,
                    "input_options":{
                        "hide_record_video":true,
                        "hide_record_audio":true,
                        "hide_record_screen":false,
                        "hide_audio": false,
                        "hide_video": true,
                        "hide_photos": false,
                        "hide_files": true,
                        "hide_add_presentation":true,
                        "attachment_extensions":[
                            "png","jpeg","jpg",
                            "pdf",
                            "docx","doc","xlsx","xls",
                            "pptx","ppt",
                            "mp4","mp3",
                            "zip"
                        ]
                    }
                }
```

```
            },
            ...
        }
    },
    ...
}
```

Параметр	Описание	Тип данных
`whiteboard_properties`	Секция для настройки доступности в приложения функционала, такого как ссылки и вложения	Объект
`objects`	Настраивает доступность функционала в для объектов	Объект
`menu`	Область настройки. В данном случае это контекстное меню	Объект
`disable_links`	Управляет доступностью функционала закрепления гиперссылок на объектах доски	Логический
`media`	Область настройки. В данном случае настраивает какие типы медиа материалов будут доступны через инструмент «Материалы»	Объект
`hide_presentation`	Скрывает отображение медиа материалов типа "Презентация"	Логический
`hide_video`	Скрывает отображение медиа материалов типа "Видео"	Логический
`hide_audio`	Скрывает отображение медиа материалов типа "Аудио"	Логический
`hide_youtube`	Скрывает отображение медиа материалов типа «Видео из внешних источников (YouTube)»	Логический
`hide_attachment`	Скрывает отображение медиа материалов типа "Вложения"	Логический
`comments`	Область настройки. В данном случае настраивает какие типы медиа материалов будут доступны через инструмент «Комментарий»	Объект

`disable_links`	Управляет доступностью функционала гиперссылок в сообщениях. Если установлено в `true`, то ссылки преобразовываются в текст	Логический
`input_options`	Настройка меню для поля ввода в окне комментария	Объект
`hide_record_audio`	Управляет возможностью добавлять голосовые заметки в комментарий	Логический
`hide_record_screen`		Логический
`hide_audio`	Управляет возможностью добавлять запись экрана в комментарий	Логический
`hide_video`	Управляет возможностью добавлять видео в комментарий	Логический
`hide_photos`	Управляет возможностью добавлять фото в комментарий	Логический
`hide_files`	Управляет возможностью добавлять вложения в комментарий	Логический
`hide_add_presentation`	Управляет возможностью добавлять презентации в комментарий	Логический
`attachment_extensions`	Список разрешенных в качестве вложений расширений файлов	Массив (Строка)

```
    ...
    "guest_access" : "all",
    ...
}
```

Параметр	Описание	Тип данных
`guest_access`	Глобальная настройка гостевого доступа в приложении. `whiteboard` - гостевой доступ выставляется только для определенных досок администратором системы. `all` - гостевой доступ выставляется любым создателем доски. `no` - отключения гостевого доступа в системе	Строка

import

```
{
    ...
```

```
    "import":{
        "miro":{
            "clientId":"345***",
            "secret":"oikau***",
            "debug":true,
            "threads":5
        },
        "pruffme":true
    },
    ...
}
```

Параметр	Описание	Тип данных
`import`	Единая область настройки импорта в приложении	Объект
`miro`	Настройки для работа импорта из Miro	Объект
`pruffme`	Управление возможностью производить импорт досок, созданных на Pruffme.com	Логический

http_info_key

```
{
    ...
    "http_info_key":"info_key_example"
    ...
}
```

Параметр	Описание	Тип данных
`http_info_key`	Предоставление доступа к данным о нагрузке на инстанс (/info), только если в `query string` передано значение `http_info_key`	Строка

Настройка Object Storage

S3 (AWS SDK v3)

Пример настройки при использовании Yandex Object Storage

```
    "s3":{
        "access_key":"YCAJEZZ2WQyqGTL**********",
        "secret_key":"YCPC1C9iW_LJLc7bMvgY9LiCl4O6vC**********",
        "bucket":"s3-v3-pruffme",
        "endpoint":"https://storage.yandexcloud.net",
        "public_prefix":"https://storage.yandexcloud.net/s3-v3-pruffme/",
        "region":"ru-central1",
        "extensions": [
            "png",
            "jpeg",
            "jpg",
            "pdf",
            "docx",
            "doc",
            "xlsx",
            "xls",
            "pptx",
            "ppt",
            "mp4",
            "mp3"
        ]
    },
```

Описание параметров

Параметр	Описание	Тип данных
access_key	Идентификатор доступа пользователя. Используется вместе с секретным ключом для аутентификации запросов к хранилищу	Строка
secret_key	Секретный ключ пользователя. Выступает в паре с идентификатором доступа для создания подписанных запросов	Строка
bucket	Название контейнера, который используется для хранения данных	Строка
endpoint	URL-адрес сервиса хранилища	Строка

public_prefix	Находится в начале ссылки на файл, когда генерируется URL. Обычно это путь к bucket	Строка
region	Регион, в котором расположено хранилище	Строка
extensions	Список расширений файлов, которые поддерживаются для хранения. Это позволяет ограничить типы файлов, которые могут быть загружены	Строка

Пример настройки при использовании MinIO и второй версии AWS SDK

```
    "s3":{
        "version": 2,
        "access_key": "tQemfrt5ne**********",
        "secret_key": "8zeNaP0z3m5fAKs8vcrWOorjN2pGax**********",
        "bucket": "pruffme",
        "endpoint": "https://editboard.mycorp.com:9000",
        "region": "ru-1",
        "public_prefix": "https://editboard.mycorp.com:9000/pruffme/",
        "s3ForcePathStyle": true,
        "apiVersion": "latest"
    },
```

Описание параметров

Параметр	Описание	Тип данных
version	Указывает версию AWS SDK	Число
access_key	Идентификатор доступа пользователя. Используется вместе с секретным ключом для аутентификации запросов к хранилищу	Строка
secret_key	Секретный ключ пользователя. Выступает в паре с идентификатором доступа для создания подписанных запросов	Строка
bucket	Название контейнера, который используется для хранения данных	Строка
endpoint	URL-адрес сервиса хранилища	Строка
public_prefix	Находится в начале ссылки на файл, когда генерируется URL. Обычно это путь к bucket	Строка
region	Регион, в котором расположено хранилище	Строка

s3ForcePathStyle	Параметр, указывающий на необходимость использования старого стиля формирования путей к объектам в S3	Логический
apiVersion	Версия API, которую следует использовать при работе с S3	Строка

При данном варианте использования объектного хранилища, файлы можно сохранять непосредственно в локальной папке.

```
    "s3":{
        "type":"localfolder",
        "storage_dir":"/storage",
        "public_prefix":"https://editboard.mycorp.com/storage/",
        "skiphttp": true,
        "extensions":[
            "png","jpeg","jpg",
            "pdf",
            "docx","doc","xlsx","xls",
            "pptx","ppt",
            "mp4","mp3"
        ]
    },
```

Особенности использования

Изменение в конфигурации nginx

Добавить в раздел `server` для порта `443` \

```
location /storage {
    alias /storage;
    try_files $uri $uri/ /index.html;
}
```

Изменения команды запуска Docker:

```
docker run -it \
    --rm \
    -p 443:443 \
    -e TZ=Europe/Moscow \
    -v /editboard-conf:/conf \
    -v /editboard-logs/nginx:/var/log/nginx \
    -v /editboard-logs/app:/root/.pm2/logs \
    -v /mnt/editboard-storage:/storage \
    --name editboard docker-registry.pruffme.com/editboard:latest
```

Описание параметров

Параметр	Описание	Тип данных
type	Параметр, который указывает на режим использования объектного хранилища в режиме локальной папки. Специфичен и используется только для LocalFolder	Строка
storage_dir	Путь к папке в которую сохраняются файлы. Специфичен и используется только для LocalFolder	Строка
public_prefix	Находится в начале ссылки на файл, когда генерируется URL. Обычно это путь к bucket	Строка
skiphttp	Изменяет механику проверки работоспособности хранилища	Логический
extensions	Список расширений файлов, которые поддерживаются для хранения. Это позволяет ограничить типы файлов, которые могут быть загружены	Строка

Новые параметры для версии 1.8.0 и выше

```
"s3":{
    "acl": "public-read",
    ...
},
```

Параметр	Описание	Тип данных
acl	Access Control List Bucket. `public-read` - устанавливает разрешение на чтение для всех пользователей	Строка

Возможные ошибки при настройке

Ошибка чтения из Object Storage

Описание ситуации

- Пользователь может загружать изображения и файлы на доску, но они не открываются.
- Ссылки сформированы корректно.
- Файлы не открываются по прямой ссылке.

Решение: в настройках бакета установить для анонимного доступа префикс / с правами на чтение

Невалидная ссылка на файлы и изображения

Описание ситуации

- Пользователь может загружать изображения и файлы на доску, но они не открываются.
- В MinIO в бакете на анонимный доступ есть префикс / на ro и выше.

Решение: проверить пути в PostreSQL. Для загруженных файлов пути можно увидеть в коллекции `users_media`; для шаблонов `dashboards_templates`

Подробнее о том, как формируется ссылка

> Как происходит склейка URL изображения\файла, которое использует приложение `public_prefix` + `${MODULE_PARTNER_NAME}` + `ids_path` + `file_name`
>
> Например:
>
> `public_prefix` + `${MODULE_PARTNER_NAME}` + `ids_path` + `file_name`
>
> https://board.test.com/s3/editboard/test/846d0a0c1655d714fd2c6172a1cdd366/ea92bf3bcfb9a57f0d14faa04603207b/4abdef04c1cae7005d8f997e01ad2154.png

Пути до файлов шаблонов прописываются во время установки, поэтому если имя бакета было изменено, то нужно:

- изменить их в базе через запрос;
- удалить базу и запустить приложение в режиме установки. После этого сделать стандартный запуск.

Не загружаются файлы (версия 1.8.11)

Пример конфигурации `nginx.conf` при обновлении на 1.8.11 с предыдущих версий приложения.

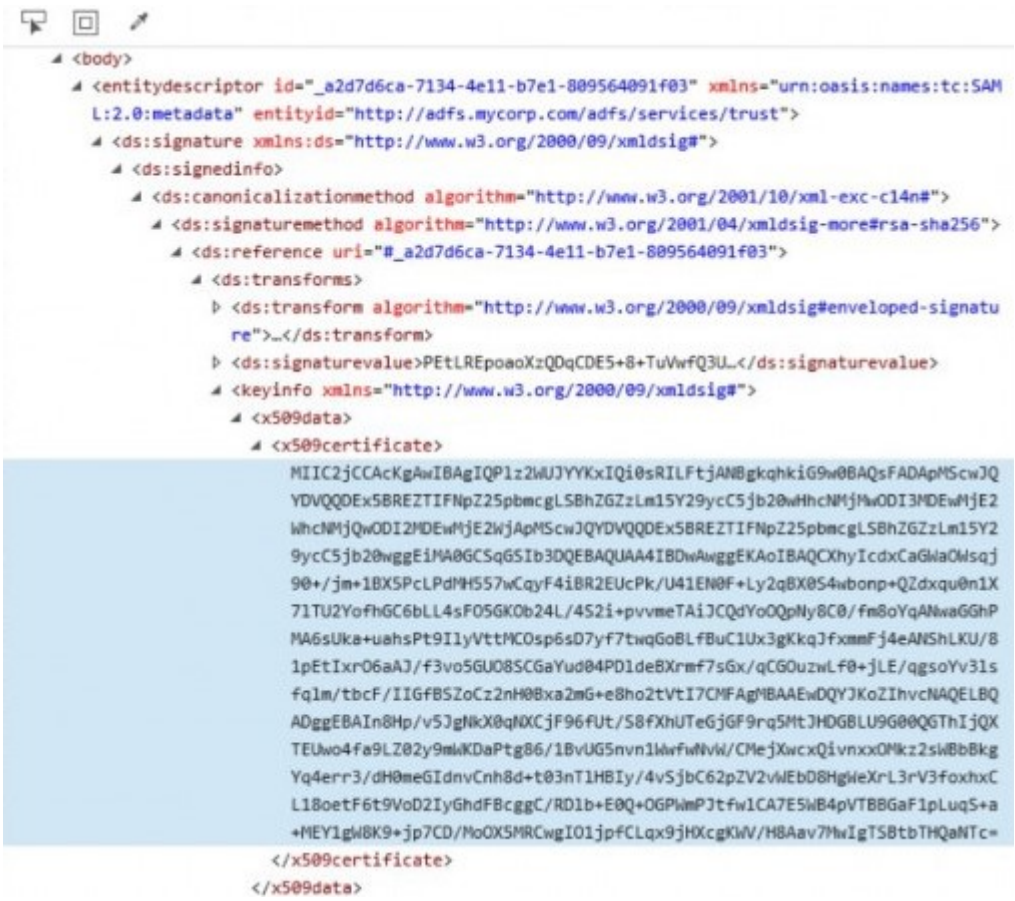
Основные изменения, которые необходимо внести в `nginx.conf` приложения:

```
 server {
    ...
        location / {
            ...
            add_header 'Access-Control-Allow-Headers'
'Range,Accept,Authorization,Cache-Control,Content-Type,DNT,If-Modified-Since,Keep-
Alive,Origin,User-Agent,X-Mx-ReqToken,X-Requested-With,X-File-Name,source-
origin,presentation,dashboard,position,parent,unconvertable,sid,hash,participant,owner,
            ...
```

Настройка AD FS

Подготовка сертификата

1. Перейдите на страницу по адресу `https://adfs.<ДОМЕН_СЕРВЕРА_AD_FS>/federationmetadata/2007-06/federationmetadata.xml`, где вместо `<ДОМЕН_СЕРВЕРА_AD_FS>` подставьте адрес домена, на котором развернута служба AD FS, и скачайте XML-файл с ключом.
2. Откройте файл в текстовом редакторе и скопируйте данные из тега `<X509Certificate>`.



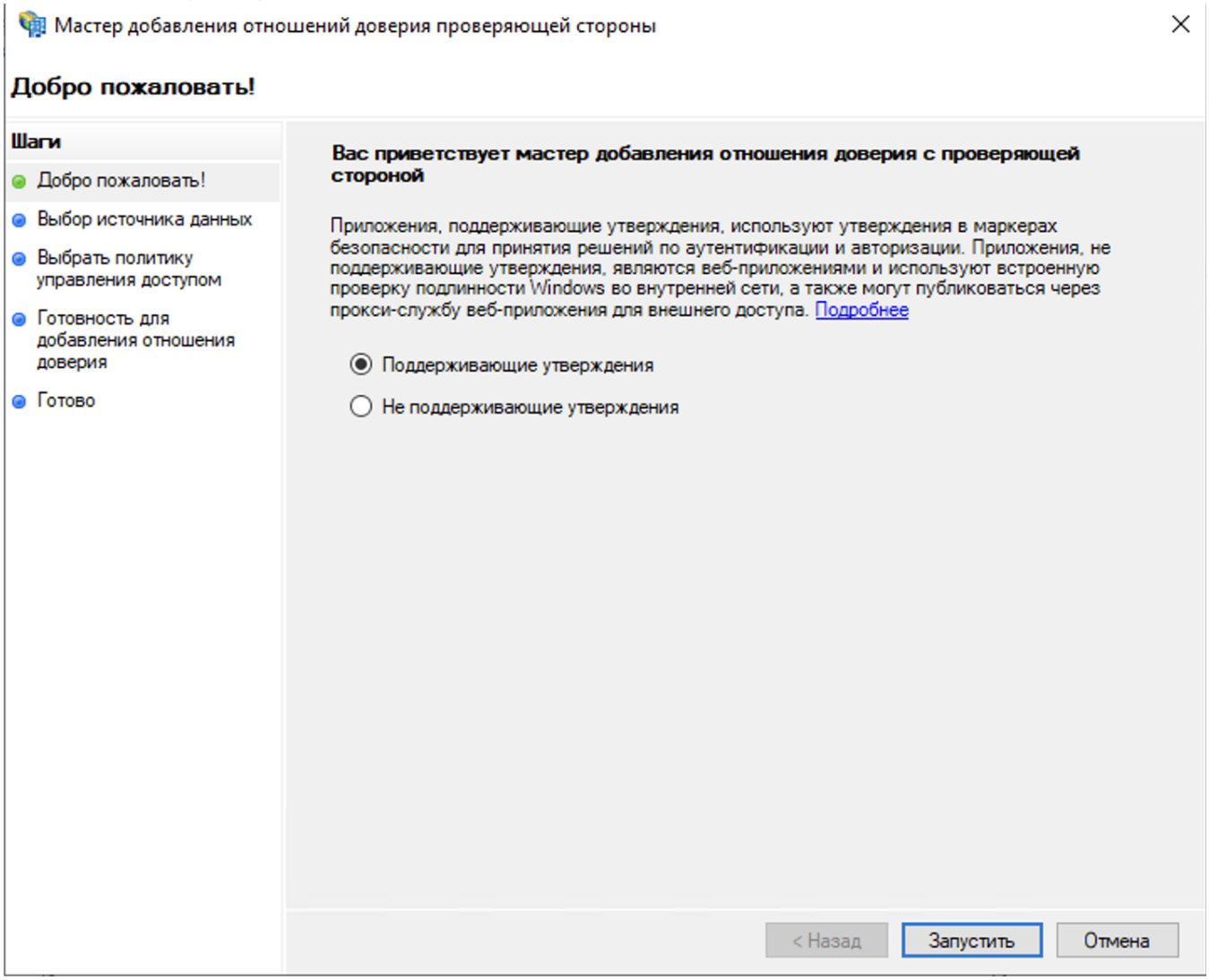
> **Примечание**
>
> В некоторых случаях `X509Certificate` может содержать более одного сертификата. Важно удостоверится, что содержимое файла ключа приложения корректно. Например, если вы сталкиваетесь с ошибкой `Failed to read asymmetric key`.

3. Сохраните данные сертификата в любом удобном виде, например в текстовом файле. Они понадобятся для задания параметров конфигурации Досок.

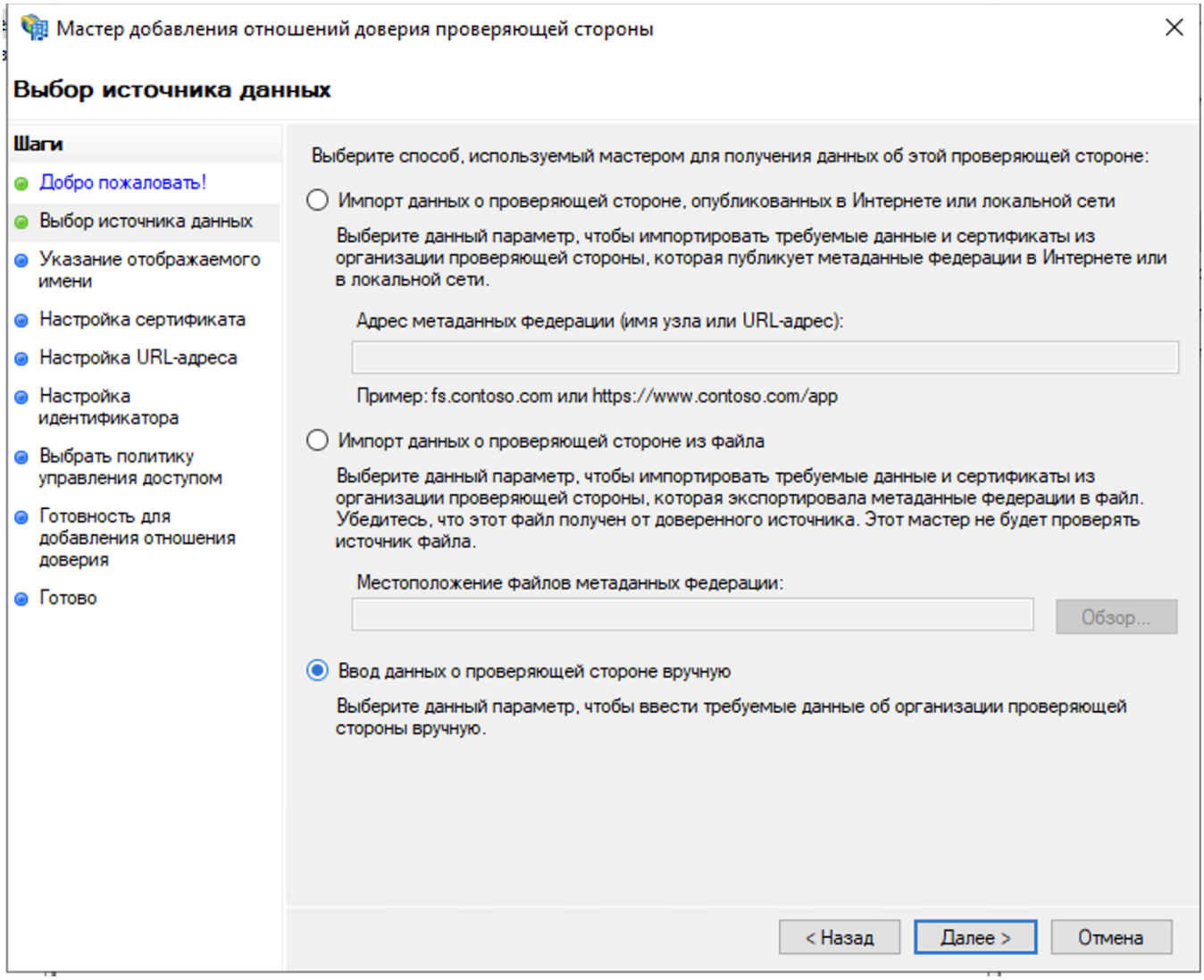
Конфигурирование AD FS

Добавление отношения доверия проверяющий стороны

1. В диспетчере сервера нажмите **Средства** и выберите **Управление AD FS**.
2. В разделе **Действия** нажмите кнопку **Добавить отношение доверия с проверяющей стороной**.
3. На странице приветствия выберите **Поддерживающие утверждения** (Claims aware) и нажмите кнопку **Запустить**.

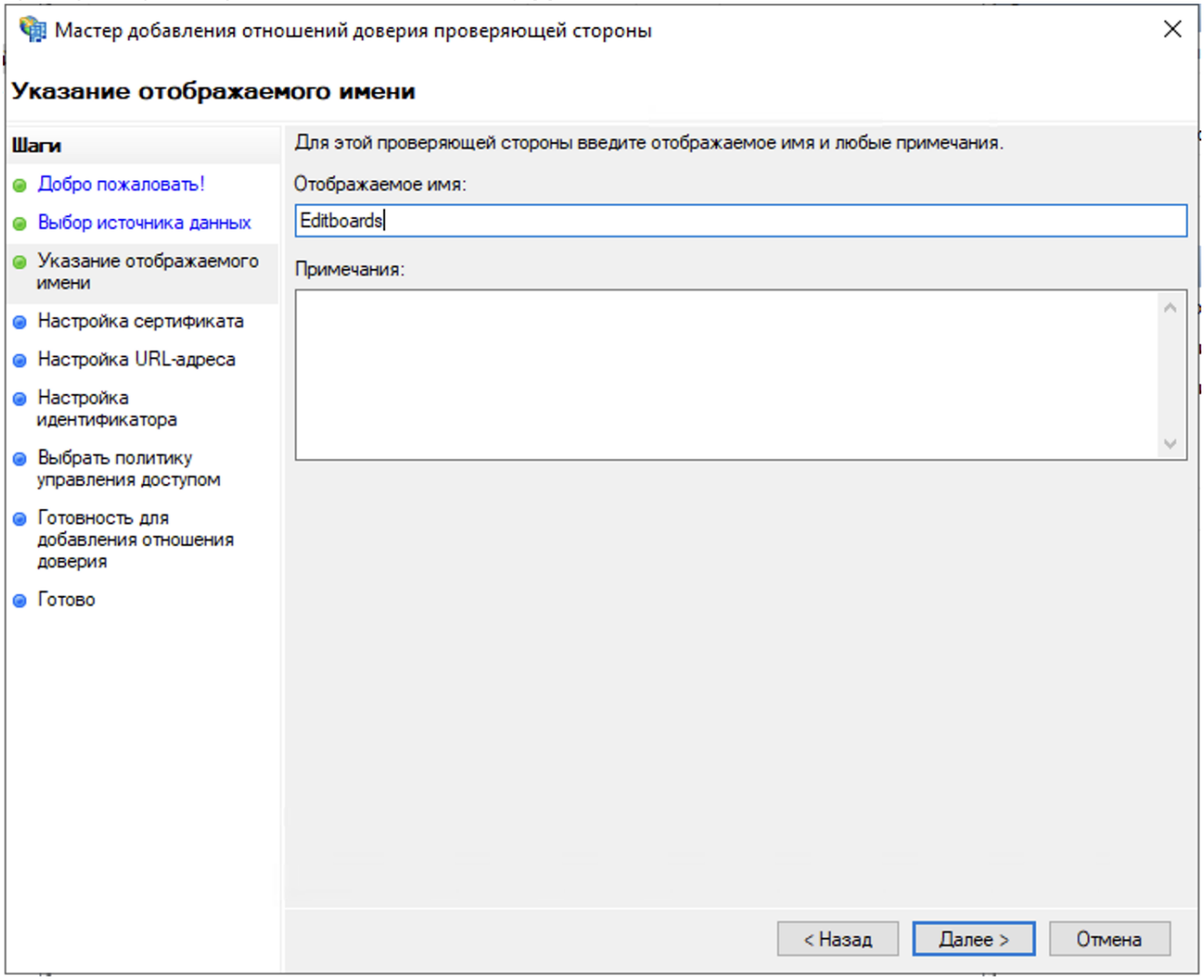


4. На странице **Выбор источника данных** отметьте **Ввод данных о проверяющей стороне вручную** (Enter data about the relying party manually), а затем нажмите кнопку **Далее**.

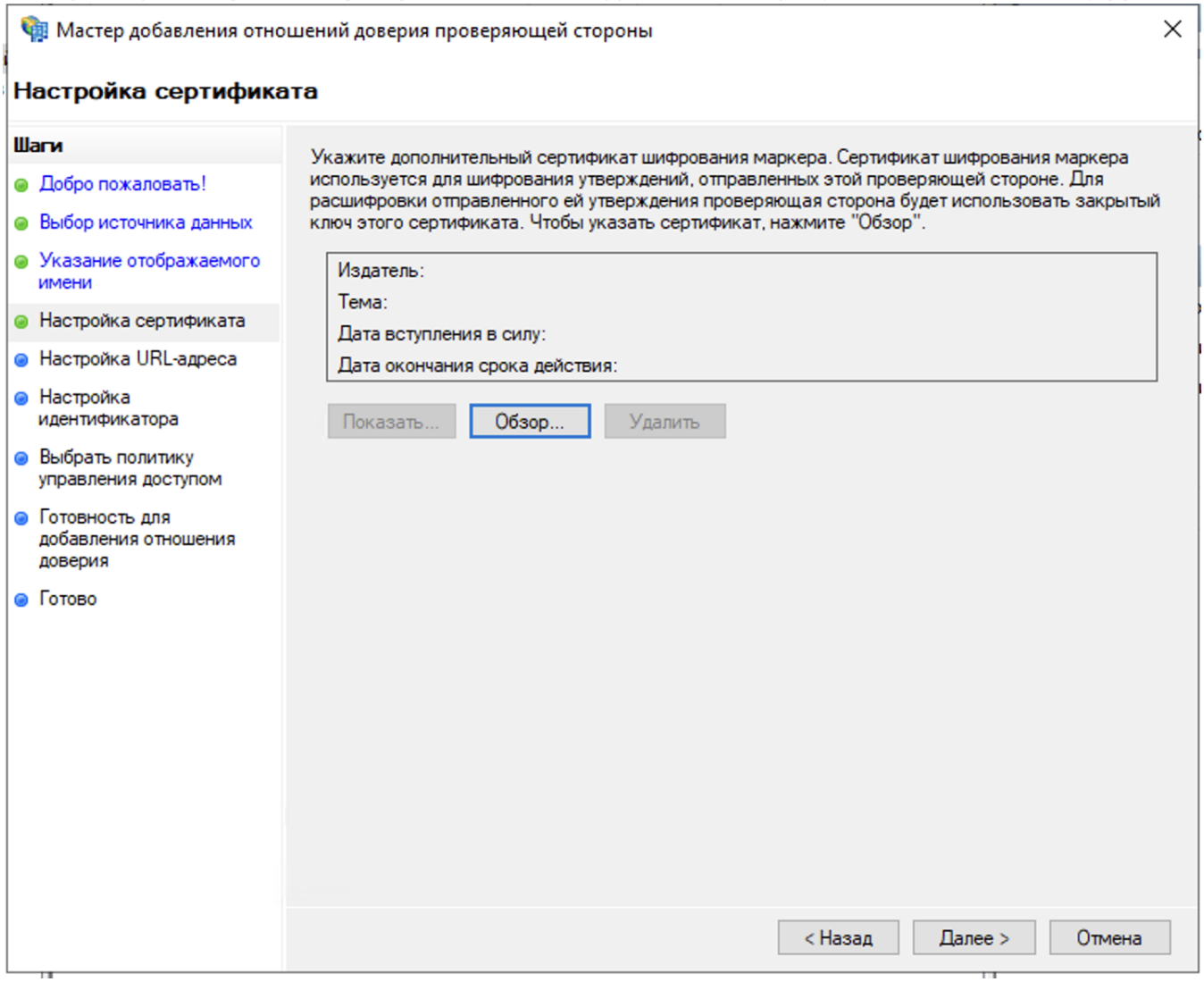


5. На странице **Указание отображаемого имени** (Specify Display Name) введите имя в поле **Отображаемое имя**. В поле **Примечания** введите описание для этого отношения доверия с

проверяющей стороной и нажмите кнопку **Далее**.

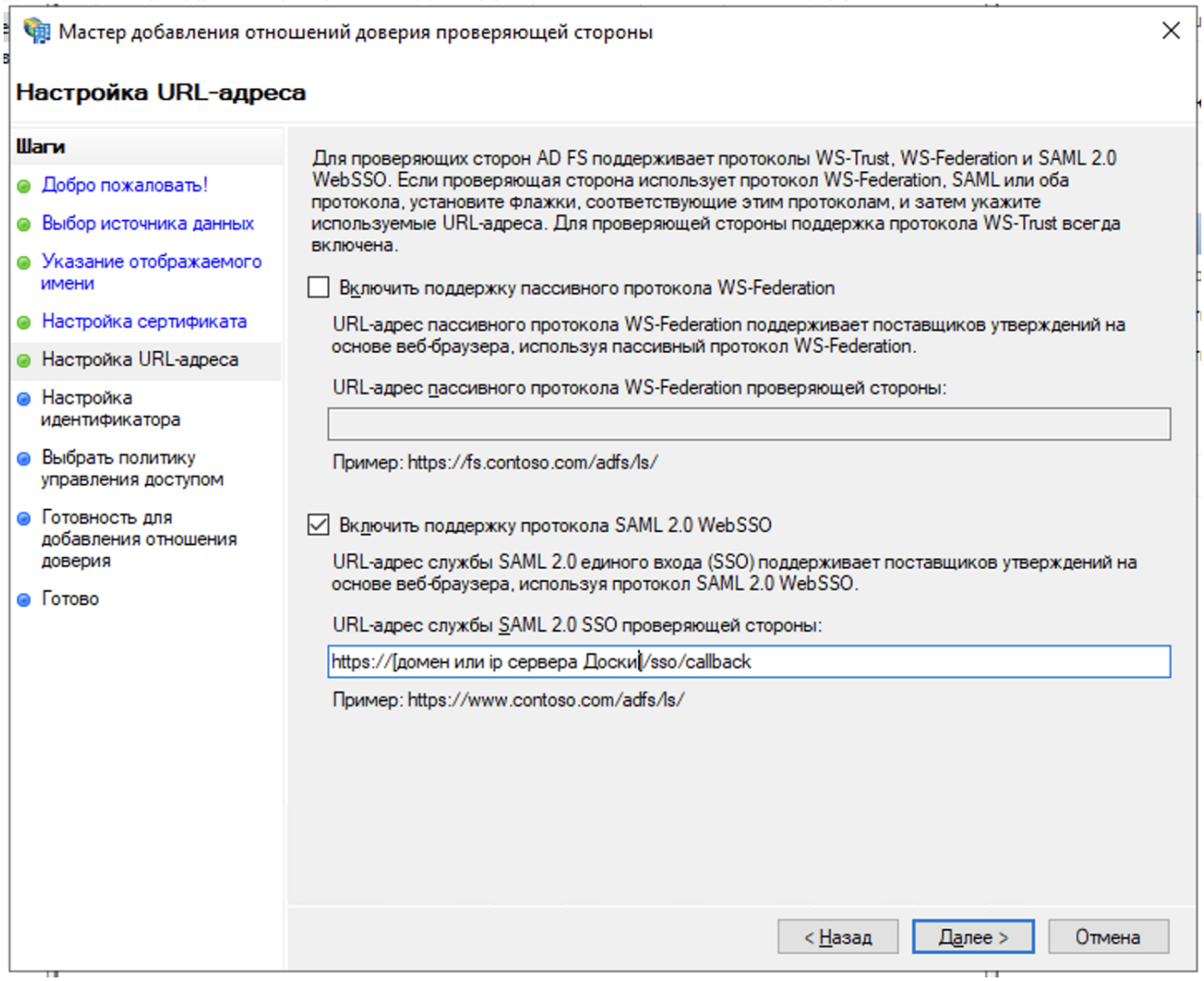


6. На странице **Настройка сертификата**, никаких действий не требуется, нажмите кнопку **Далее**.



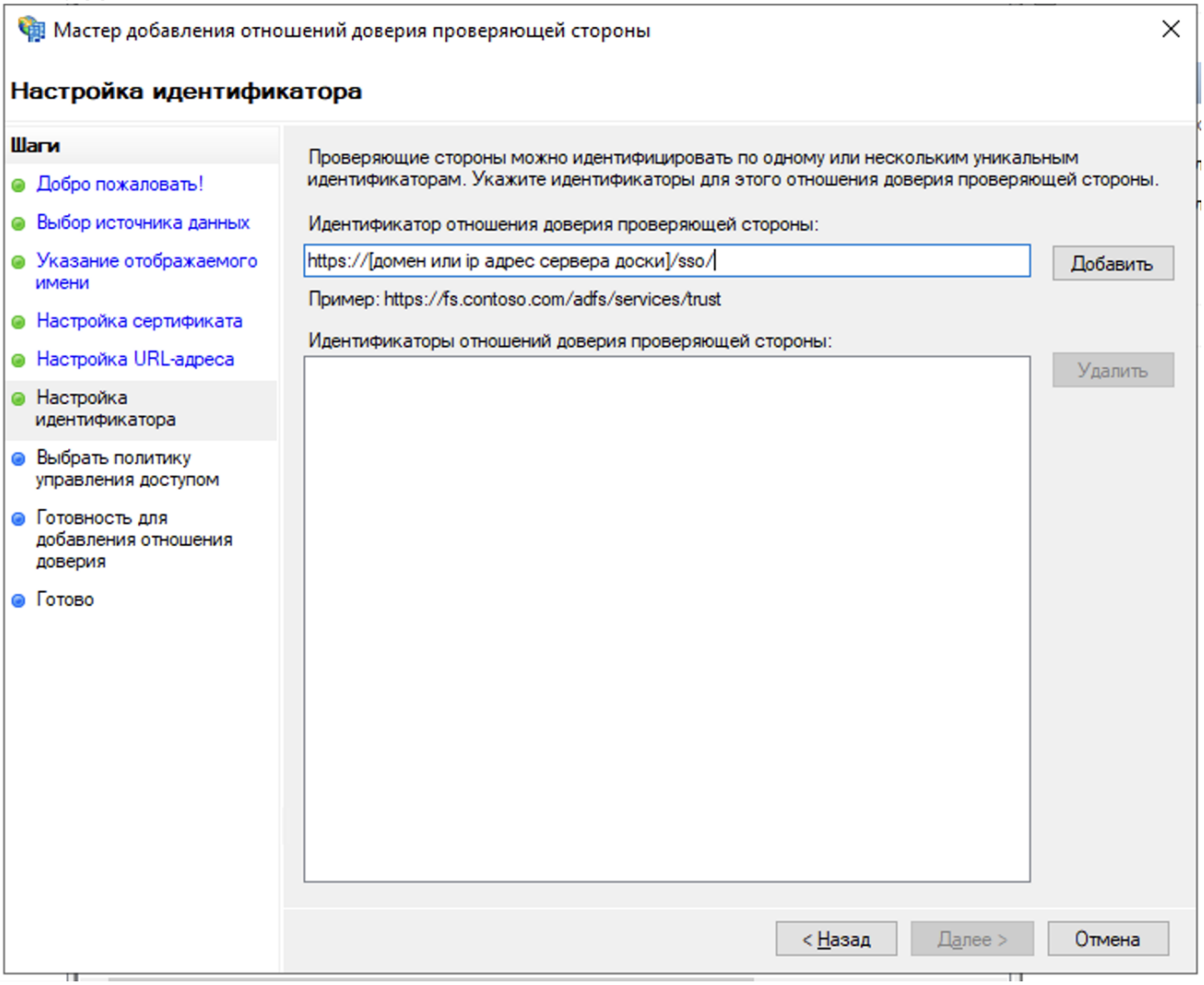
7. На странице **Настройка URL-адреса** включите поддержку протокола SAML 2.0 WebSSO, укажите URL `https://<СЕРВЕР_ДОСОК>/sso/callback`, где вместо `<СЕРВЕР_ДОСОК>` подставьте

домен или ip адрес сервера с Яндекс Досками, и нажмите кнопку **Далее**.

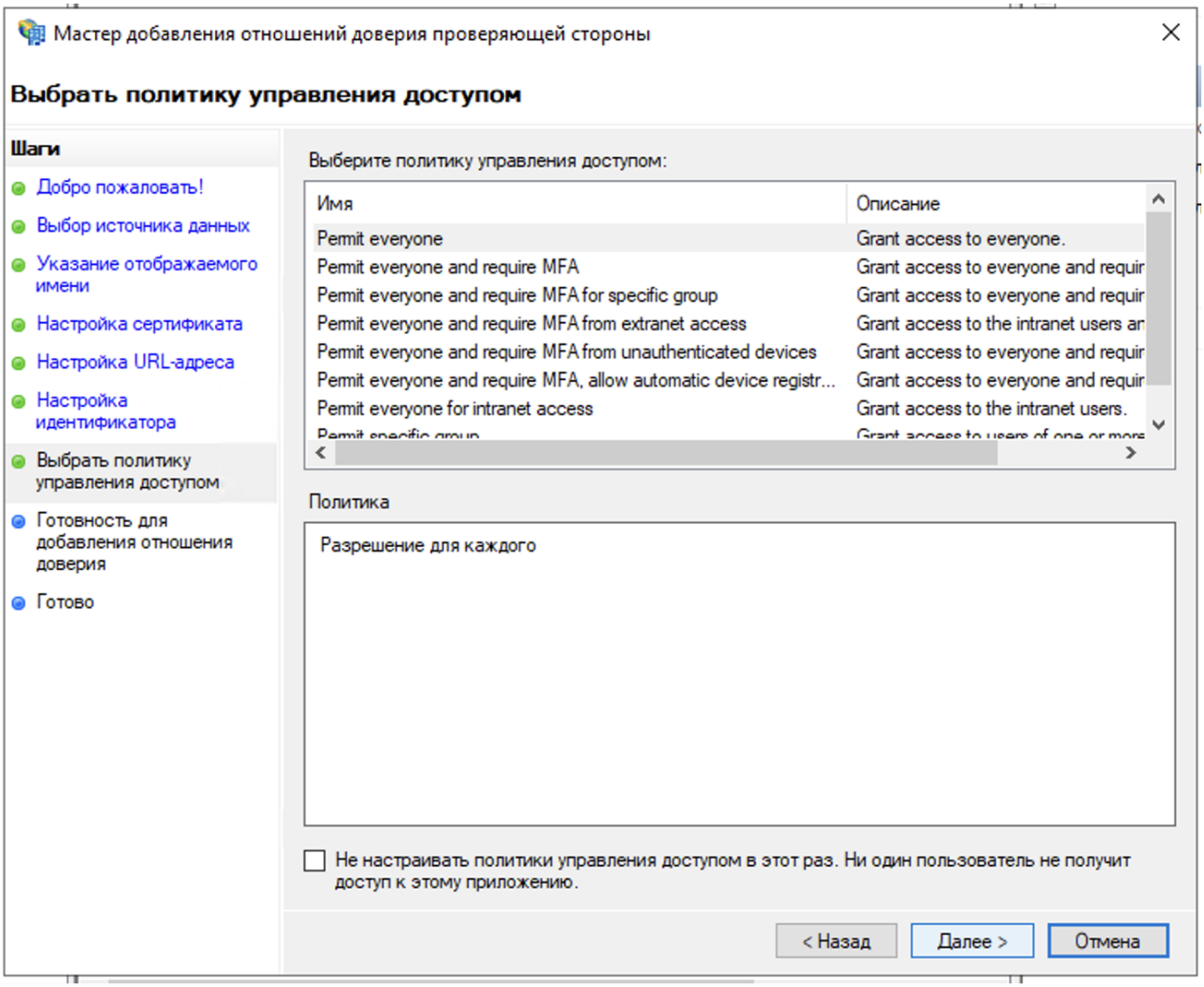


8. На странице **Настройка идентификатора** укажите один идентификатор проверяющей стороны вида `https://<СЕРВЕР_ДОСОК>/sso/` и нажмите кнопку **Добавить**, затем нажмите

кнопку **Далее**.

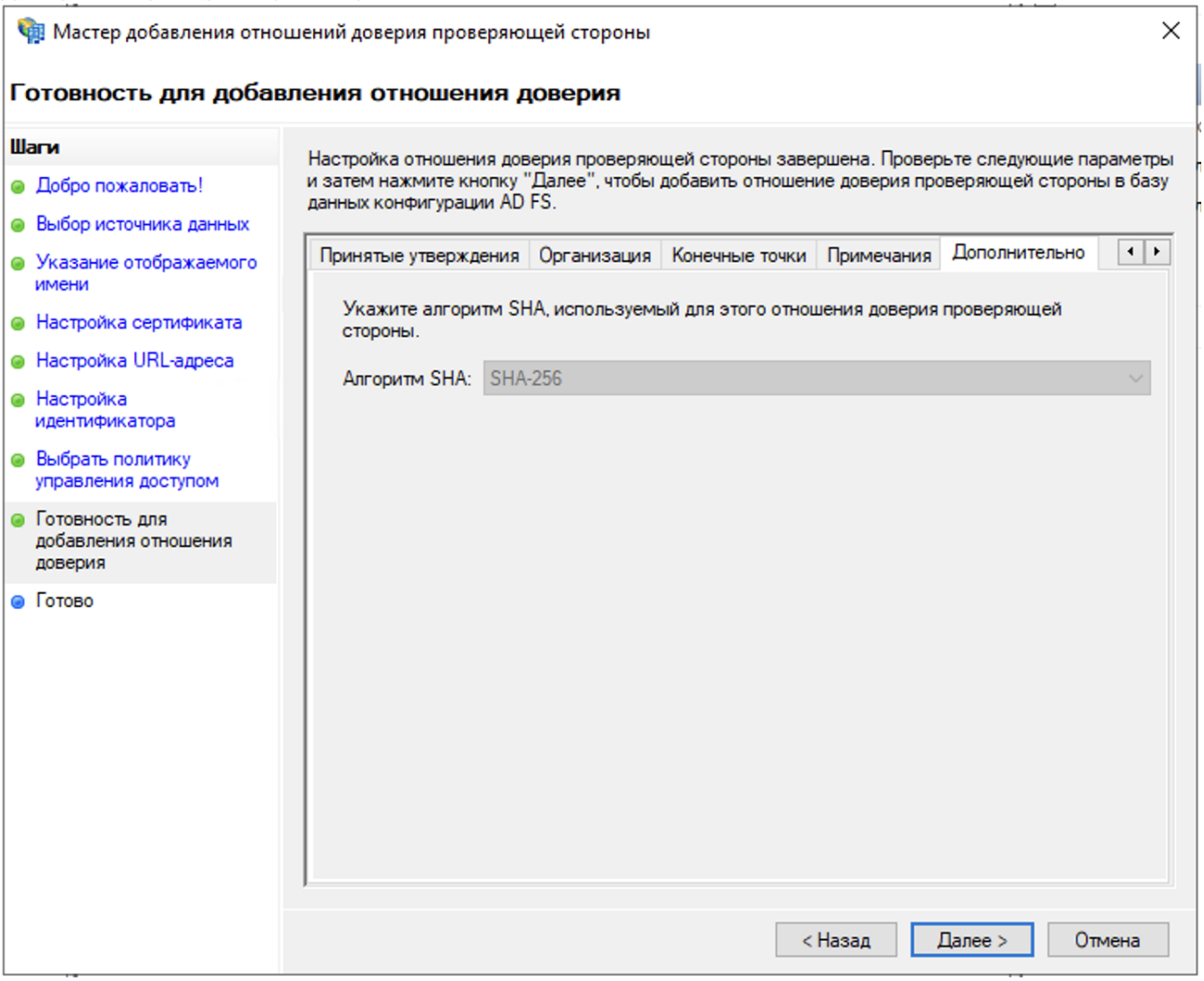


9. На странице **Выбрать политику управления доступом** (Choose Access Control Policy) выберите политику **Разрешение для каждого** (Permit everyone) и нажмите кнопку **Далее**.

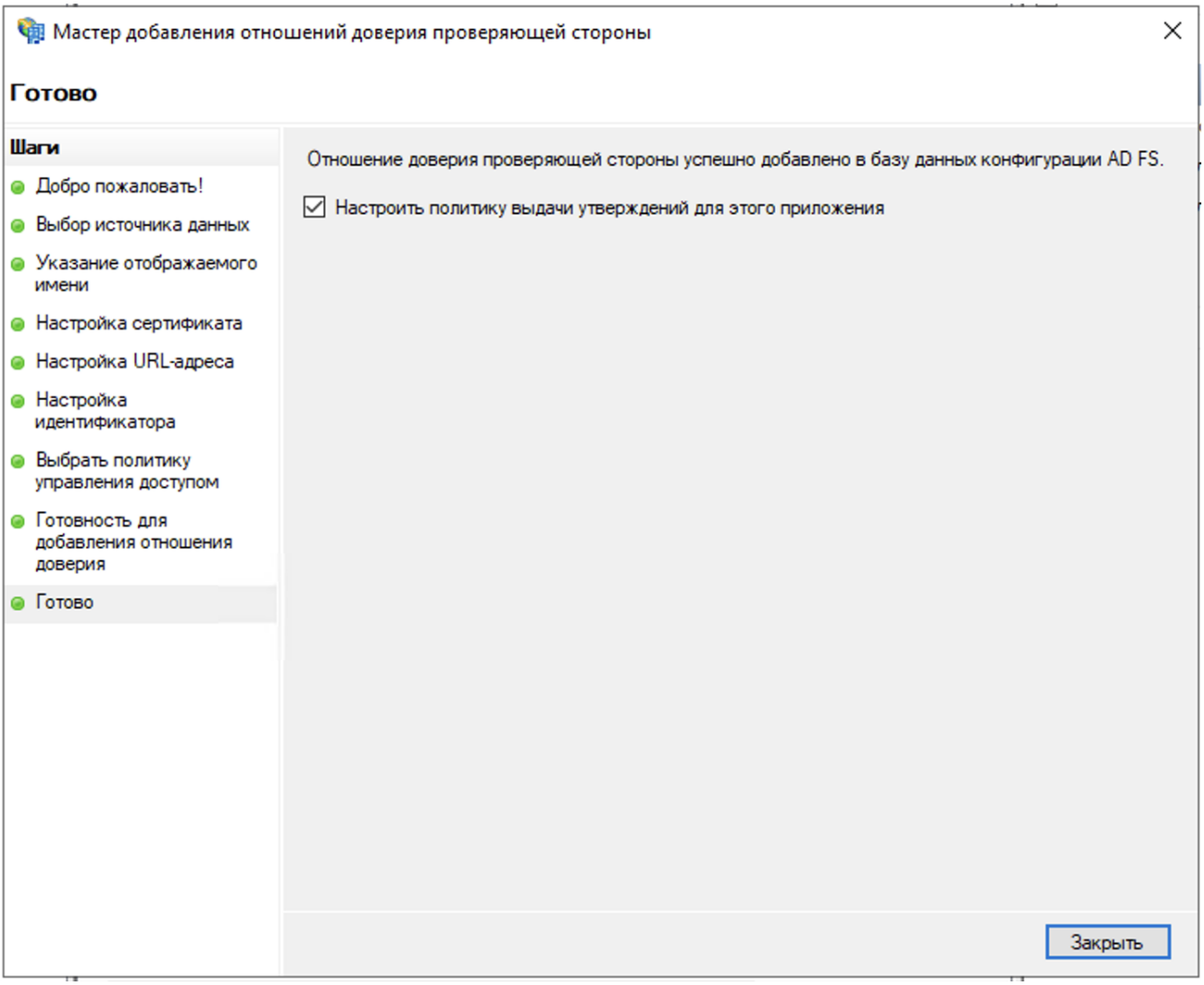


10. На странице **Готовность для добавления отношения доверия** (Ready to Add Trust) проверьте параметры и нажмите кнопку **Далее**, чтобы сохранить сведения об отношении

доверия с проверяющей стороной.

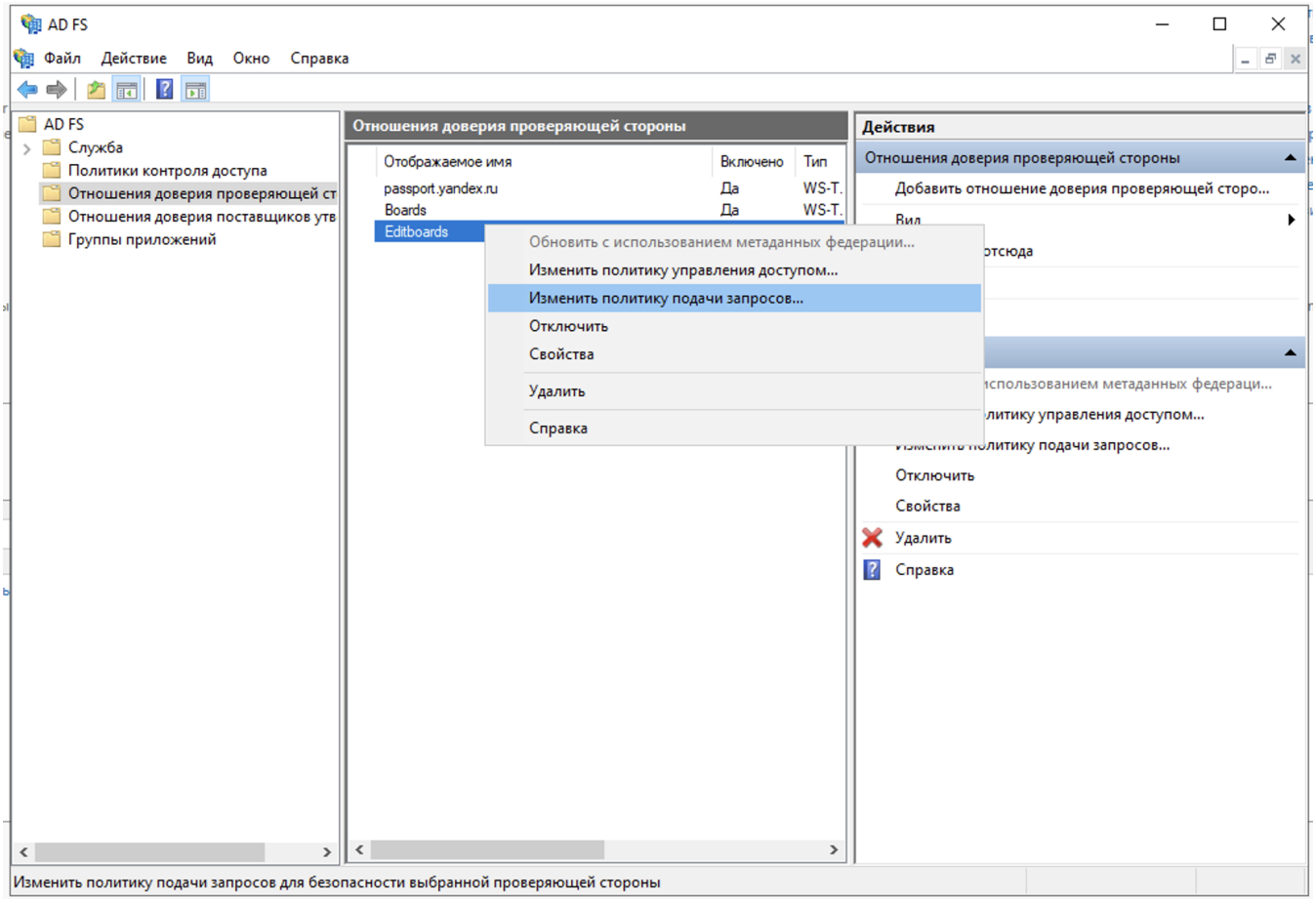


11. На странице **Готово** нажмите кнопку **Закрыть**. После этого автоматически откроется диалоговое окно **Изменение правил утверждений**.

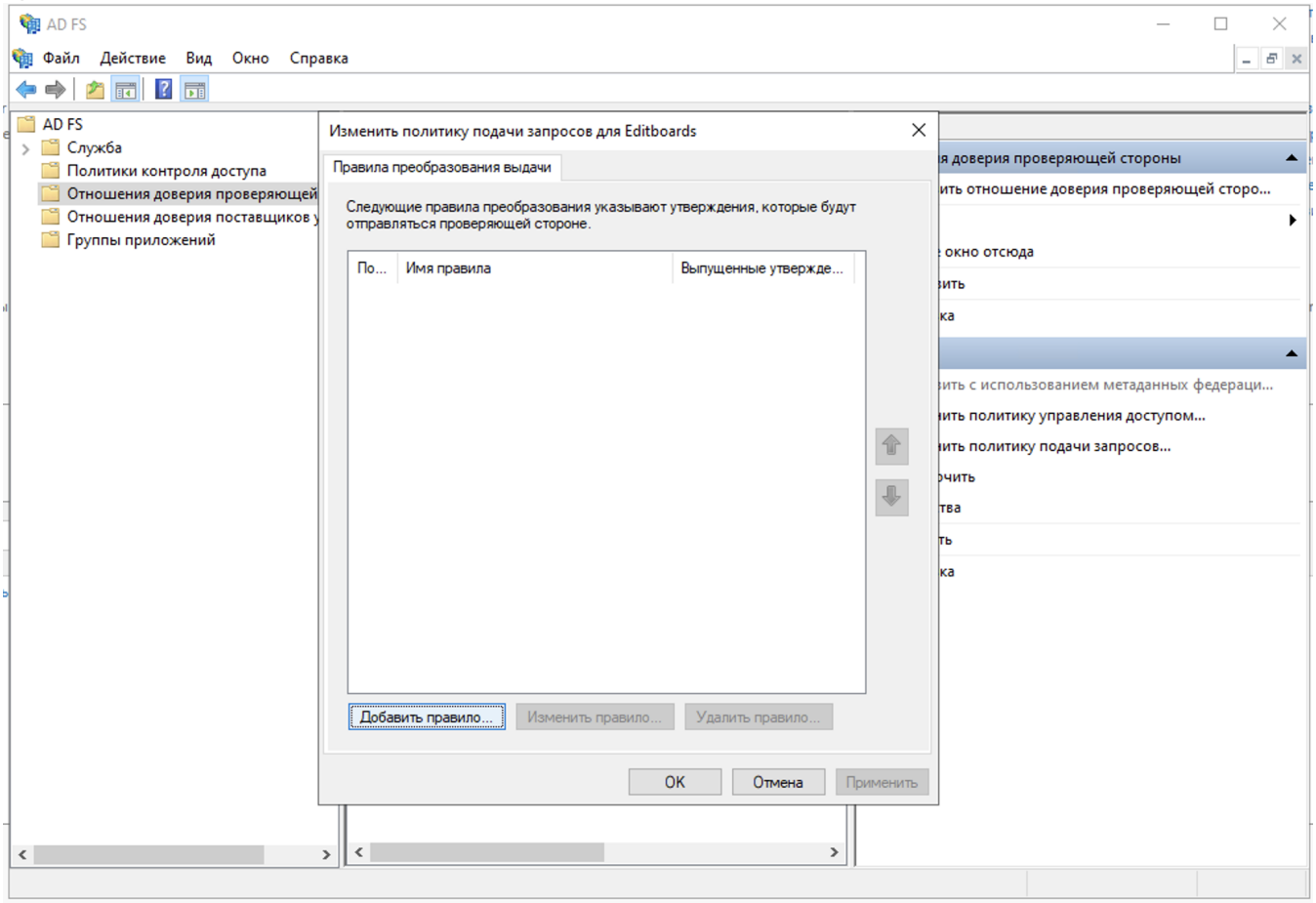


Создание правила для отправки атрибутов LDAP в качестве утверждений для доверия проверяющей стороны

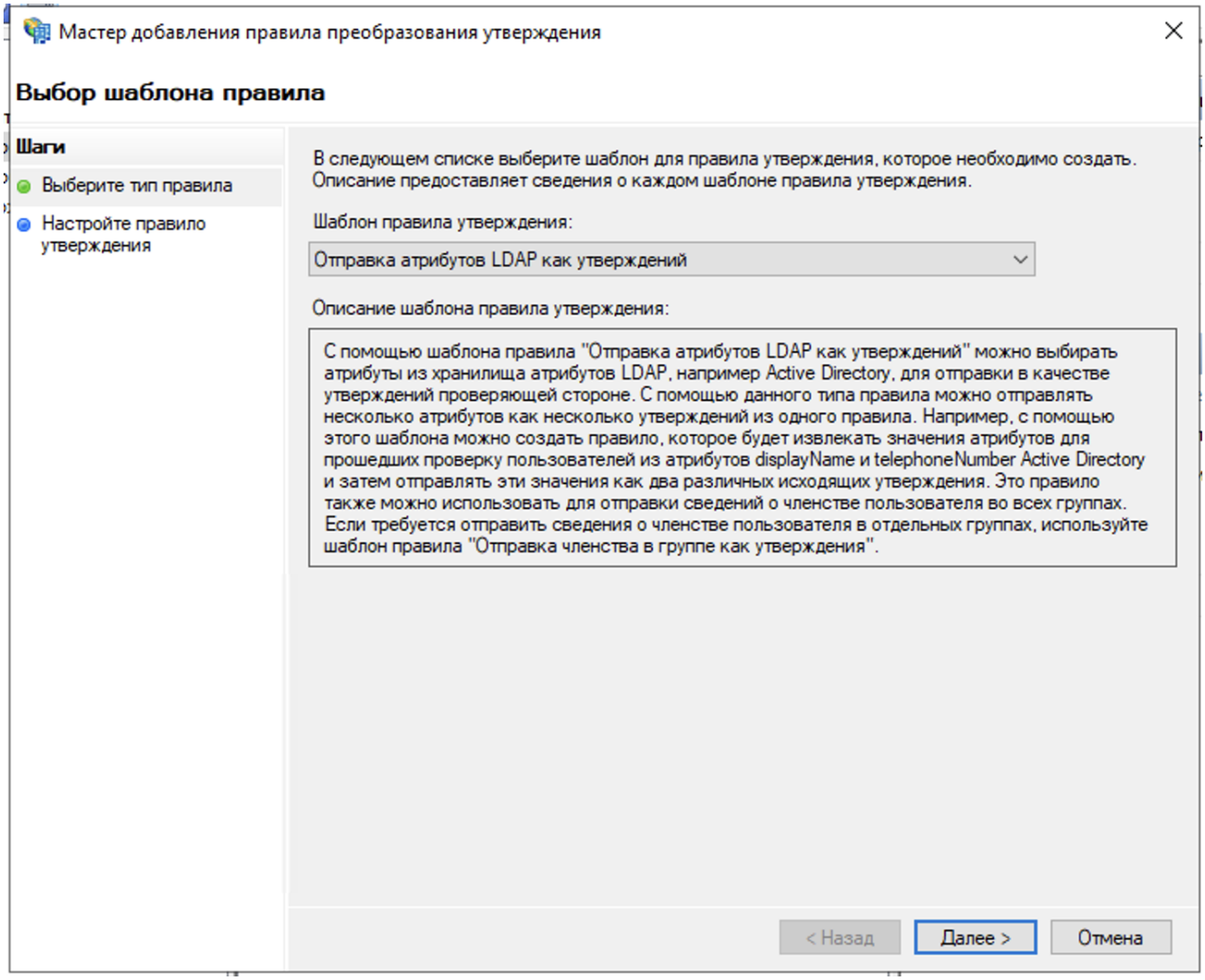
1. В диспетчере сервера выберите **Средства** и далее **Управление AD FS**.
2. В дереве консоли в разделе AD FS выберите **Отношения доверия проверяющей стороны**.
3. Выберите нужное доверие и в контекстном меню нажмите **Изменить политику подачи запросов**.



4. В диалоговом окне **Изменить политику подачи запросов** в разделе **Правила преобразования выдачи** нажмите кнопку **Добавить правило**, чтобы запустить мастер правил.

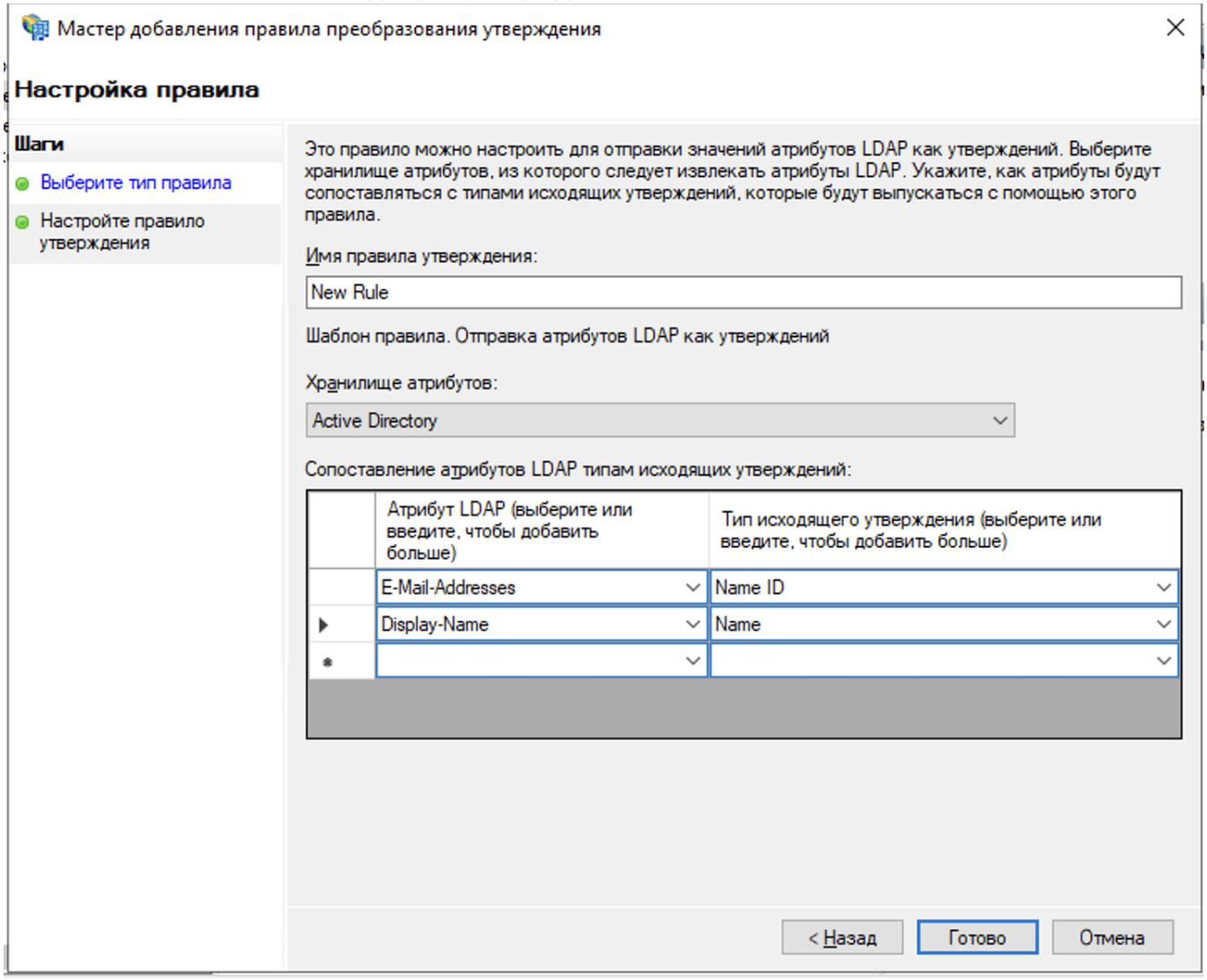


5. На странице **Выбор шаблона правила** в поле **Шаблон правила утверждения** выберите в списке **Отправка атрибутов LDAP как утверждений** и нажмите кнопку **Далее**.



6. На странице **Настройка правила** в поле **Имя правила утверждения** введите отображаемое имя для этого правила, выберите хранилище атрибутов, а затем выберите атрибут LDAP и

сопоставьте его с типом исходящего утверждения.

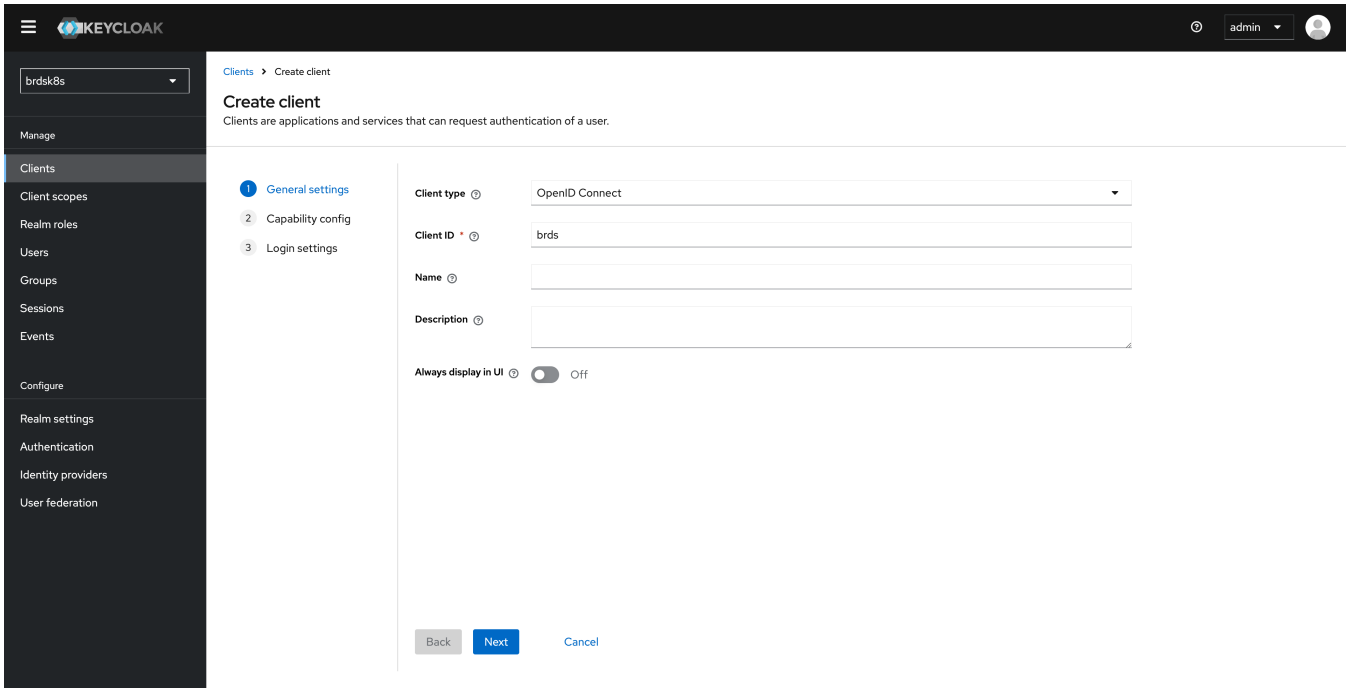


7. Нажмите кнопку **Готово**.
8. В диалоговом окне **Изменение правил утверждений** нажмите кнопку **ОК**, чтобы сохранить правило.

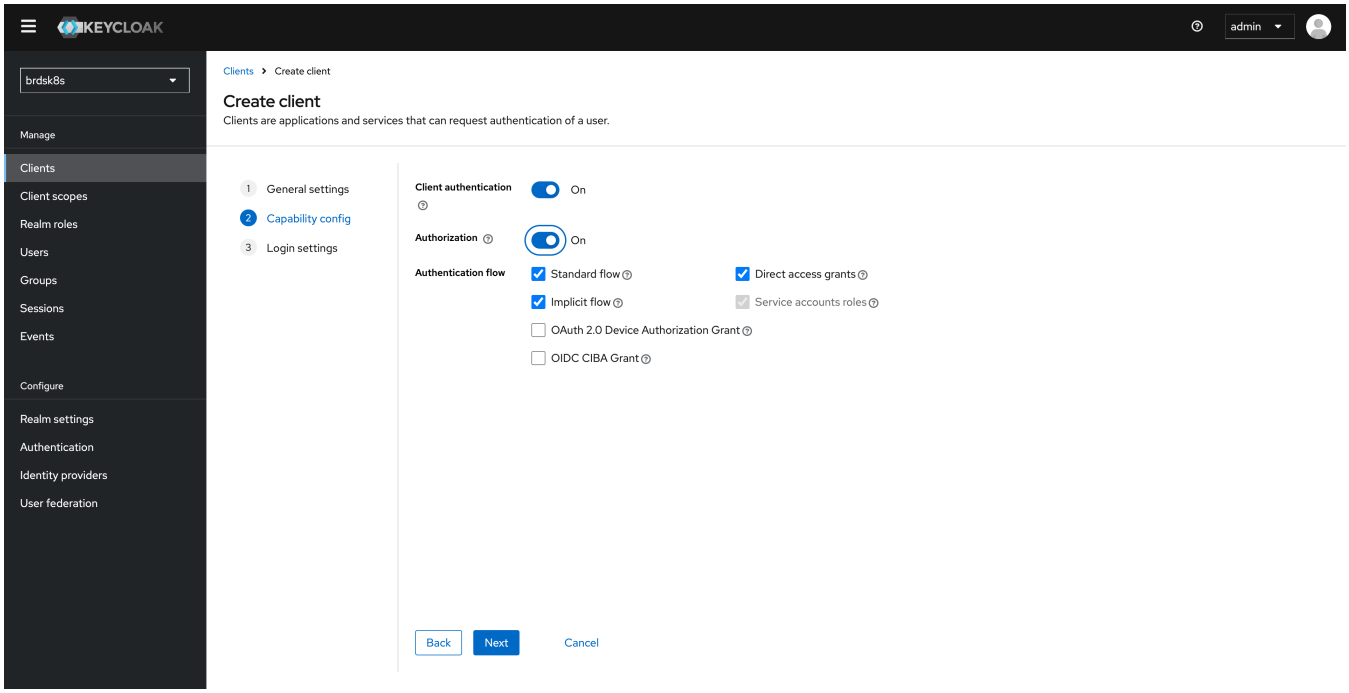
Настройка Keycloak

Конфигурирование Keycloak

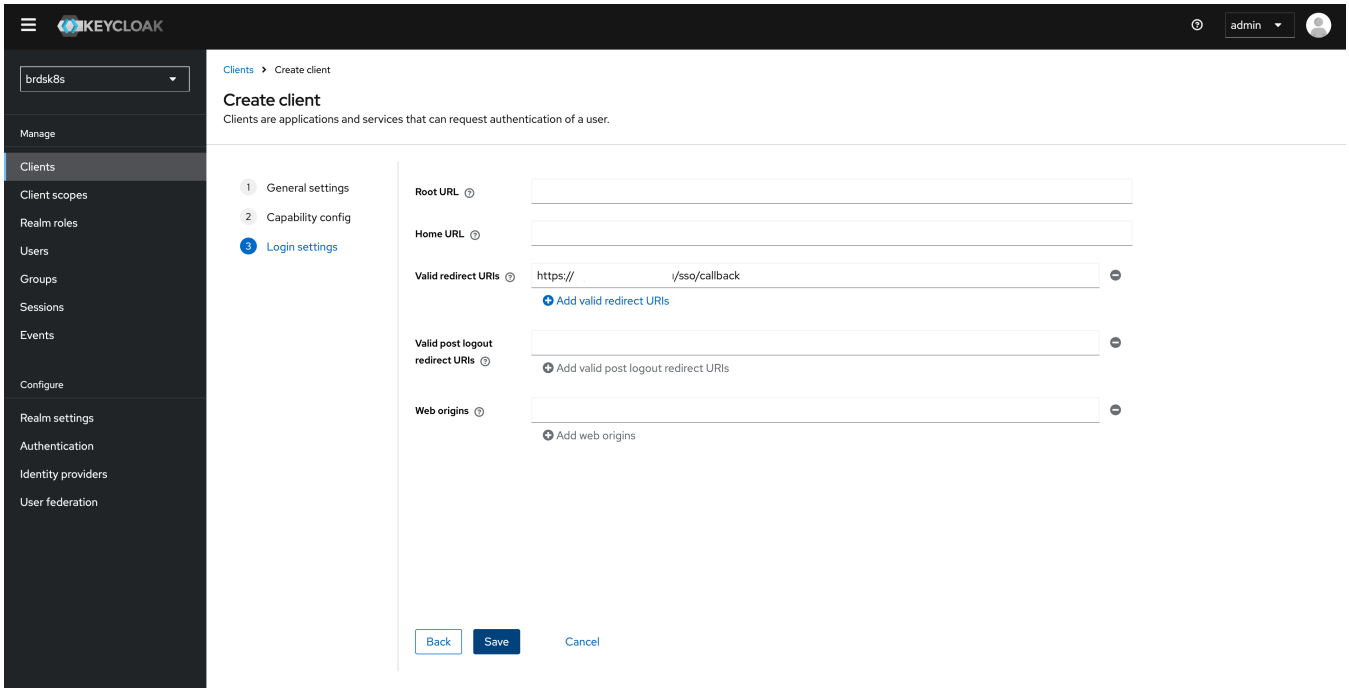
1. На панели слева выберите **Clients** и нажмите кнопку **Create Client**.
2. В разделе **General settings**:
   2.1. В поле **Client type** выберите **OpenID Connect**.
   2.2. Придумайте уникальный идентификатор вашего приложения Досок и введите его в поле **Client ID**. Идентификатор может содержать буквенно-цифровые символы, а также символы подчеркивания (_) и дефисы (-); пробелы и специальные символы не допускаются.
   Запомните или сохраните в любом текстовом файле значение **Client ID** — оно понадобится вам при задании параметров SSO в установочном пакете Helm.
   2.3. Нажмите **Next**.



3. В разделе **Capability config**:
   3.1. Включите опции **Client authentication** и **Authorization**.
   3.2. В поле **Authentication flow** отметьте **Standard flow**, **Direct access grants** и **Implicit flow**.
   3.3. Нажмите **Next**.



4. В разделе **Login settings**:
   4.1. В поле **Valid Redirect URIs** укажите URL, на который SSO-провайдер перенаправит пользователя после успешной аутентификации (например, `"https://<ВАШ_ДОМЕН>/sso/callback"`, где `<ВАШ_ДОМЕН>` — адрес вашего домена).
   4.2. Если ваши сотрудники пользуются сервисом Яндекс Доски не только на российском домене, нажмите **Add valid redirect URIs** и дополнительно добавьте URL языковых доменов.

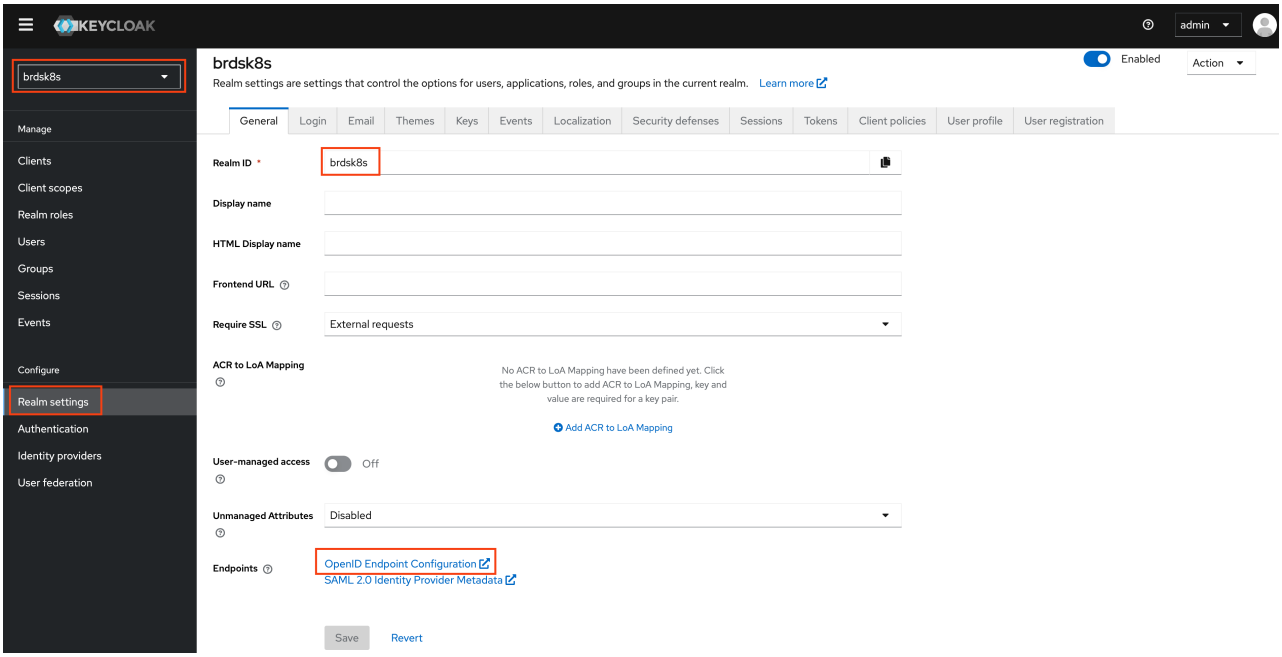


Получение данных для Helm

Для задания параметров SSO в установочном пакете Helm понадобятся адреса конечных точек и секретный ключ.

1. Получите URL, необходимые для аутентификации:
   1.1. На панели слева выберите **Realm settings**.
   1.2. В поле **Realm ID** введите значение, соответствующее вашей рабочей области.

1.3. Нажмите **OpenID Endpoint Configuration** внизу окна, чтобы открыть список конфигурационных параметров.

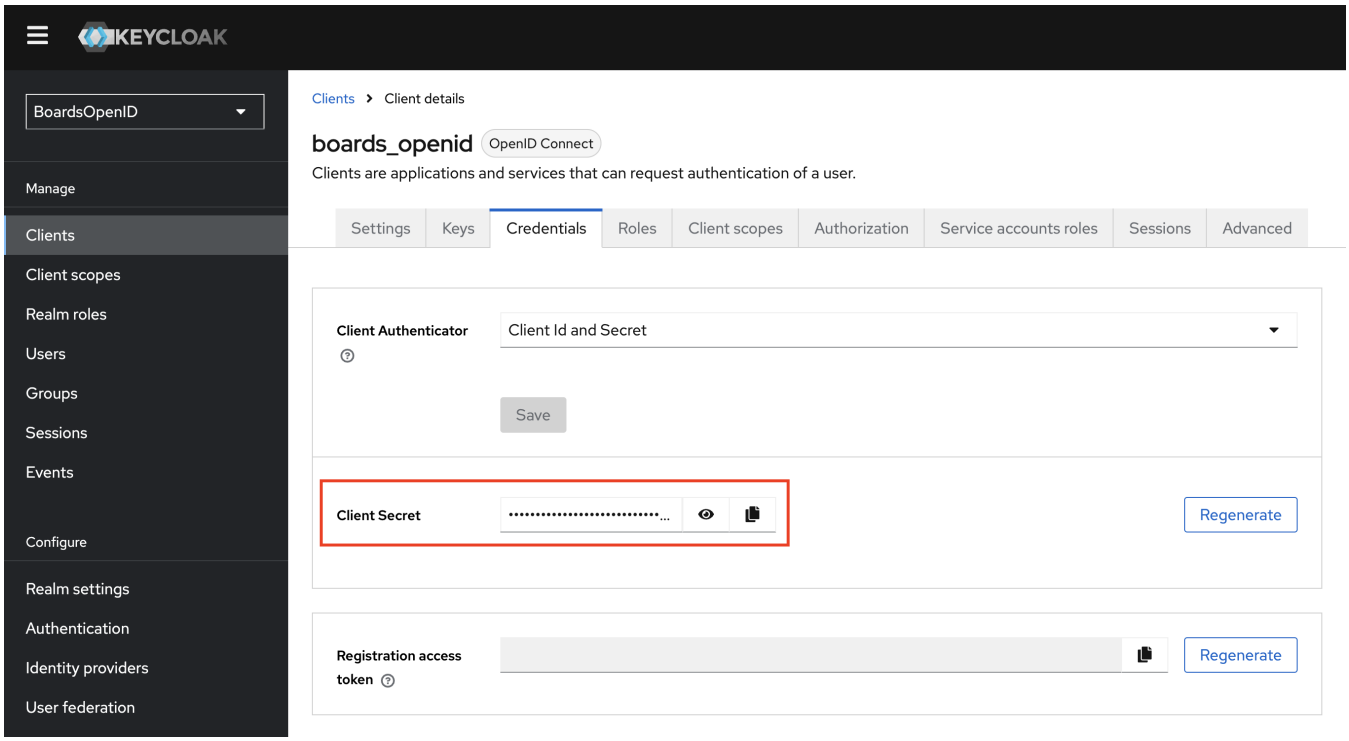


1.4. Сохраните значения полей **authorization_endpoint**, **token_endpoint** и **userinfo_endpoint** в любом текстовом файле.

2. Получите Client Secret:

2.1. На панели слева выберите **Clients** и перейдите на вкладку **Credentials**.

2.2. Скопируйте значение из поля **Client Secret** и также сохраните его в текстовом файле.



Настройка SSO

Приложение позволяет для организации единого входа использовать один из протоколов `SAML` или `OpenID`.

Модуль SOO в `values.yaml`

Пример настройки полей `modules.sso` в файле `values.yaml` из установочного пакета Helm:

SAML

```
sso:
    enabled: true
    module_type: "sso"
    type: "saml"
    entry_point: "https://<ДОМЕН_СЕРВЕРА_AD_FS>/adfs/ls"
    issuer: "https://<ВАШ_ДОМЕН>/sso/"
    cert: "adfs/cert.crt"
    callback_url: "https://<ВАШ_ДОМЕН>/sso/callback"
    field_id: "nameID"
    field_name: "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
    exit_url: "https://<ВАШ_ДОМЕН>"
    whiteboard_api_partner: "sso"
    whiteboard_api_key: "sso"
    x509:
        create_secret: true
        certificate: |
            -----BEGIN CERTIFICATE-----
            MII***==
            -----END CERTIFICATE-----
    admins:
        - "admin@domain.ru"
```

OpenID

```
sso:
    enabled: true
    module_type: "sso"
    type: "auth2"
    callback_url: "https://<ВАШ_ДОМЕН>/sso/callback"
    authorization_url:
"https://<ДОМЕН_СЕРВЕРА_KEYCLOAK>/realms/[realm_ID]/protocol/openid-connect/auth"
    token_url: "https://<ДОМЕН_СЕРВЕРА_KEYCLOAK>/realms/[realm_ID]/protocol/openid-
connect/token"
    info_url: "https://<ДОМЕН_СЕРВЕРА_KEYCLOAK>/realms/[realm_ID]/protocol/openid-
connect/userinfo"
    scope: "openid profile email"
    authorization_type: "Bearer"
    field_id: "email"
```

```
    field_name: "name"
    client_id: "[client_id]"
    client_secret: "[client_secret]"
    whiteboard_api_partner: "kc"
    whiteboard_api_key: "kc_key"
    admins:
        - "admin@domain.ru"
```

Описание параметров модуля

SAML

Параметр	Описание	Тип данных
sso	Название модуля. Произвольное значение (необязательно “sso”). Участвует в формировании URI	Строка
enabled	Статус активации группы параметров: `true` — включено; `false` — выключено	Логический
module_type	Тип модуля. Маркирует данную секцию как используемую для модуля SSO	Строка
type	Тип используемого протокола для SSO, в данном случае `saml`	Строка
entry_point	Адрес, по которому расположен сервис аутентификации, например AD FS	Строка
issuer	Уникальный идентификатор вашего сервиса SSO у провайдера. Это значение используется провайдером для идентификации приложения, инициирующего запрос аутентификации. Вместо `<ВАШ_ДОМЕН>` укажите адрес вашего домена	Строка

cert	Путь к сертификату безопасности, используемому для проверки подлинности сообщений SAML	Строка
callback_url	URL, на который SSO-провайдер перенаправит пользователя после успешной аутентификации. Вместо `<ВАШ_ДОМЕН>` укажите адрес вашего домена	Строка
field_id	Указывает на поле в данных SAML Assertion, которое содержит уникальный идентификатор пользователя (в данном случае, адрес электронной почты)	Строка
field_name	Указывает на поле в данных SAML Assertion, содержащее имя пользователя. Это поле используется приложением для отображения имени или других данных пользователя	Строка
exit_url	URL, на который пользователь будет перенаправлен после выхода из системы или завершения сессии SSO. Вместо `<ВАШ_ДОМЕН>` укажите адрес вашего домена	Строка
whiteboard_api_partner	Произвольное значение. Используется для разделения области видимости документов, если в системе используется несколько доменов	Строка
whiteboard_api_key	Произвольное значение. Ключ API для доступа к ресурсам определенного apiPartner	Строка
x509.create_secret	Признак того, что для аутентификации используется сертификат в формате X.509	Логический

x509.certificate	Данные сертификата X.509	Строка
admins	Адреса администраторов вашей организации, которые получат доступ к администрированию Досок	Массив
use_teams	Необязательный параметр. Определяет режим личного кабинета: `true` — основная версия ЛК; `false` — упрощенная версия	Логический

Параметр	**Описание**	**Тип данных**
sso	Название модуля. Произвольное значение (необязательно “sso”). Участвует в формировании URI	Строка
enabled	Статус активации группы параметров: `true` — включено; `false` — выключено	Логический
module_type	Задает тип модуля. Маркирует данную секцию как используемую для модуля SSO	Строка
type	Тип используемого протокола для SSO, в данном случае `auth2`	Строка
callback_url	URL, на который SSO-провайдер перенаправит пользователя после успешной аутентификации. Вместо `<ВАШ_ДОМЕН>` укажите адрес вашего домена	Строка

authorization_url	URL, на который необходимо перенаправить пользователя для начала процесса аутентификации через OAuth 2.0. Подставьте в это поле значение **authorization_endpoint**, которое вы сохранили на шаге 1.4 при получении параметров SSO из Keycloak	Строка
token_url	URL, который используется для обмена авторизационного кода на токен, обеспечивающий доступ к защищенным ресурсам пользователя. Подставьте в это поле значение **token_endpoint**, которое вы сохранили на шаге 1.4 при получении параметров SSO из Keycloak	Строка
info_url	URL, по которому приложение может запросить данные о пользователе, используя полученный токен доступа. Это позволяет извлечь информацию о пользователе после аутентификации/ Подставьте в это поле значение **userinfo_endpoint**, которое вы сохранили на шаге 1.4 при получении параметров SSO из Keycloak	Строка
scope	Указывает область действия запрашиваемых разрешений. Значение `null` означает, что конкретные разрешения не указаны или используются значения по умолчанию. При работе с openid для корректной работы приложения заполняется следующим образом `"scope" : "openid profile email"`	Строка
authorization_type	Указывает на тип используемой аутентификации. Возможны значения: `Bearer`, `token`	Строка

field_id	Наименование поля, которое содержит идентификатор пользователя, получаемый от OAuth-провайдера. Это значение используется для идентификации пользователя в приложении	Строка
field_name	Наименование поля, которое содержит имя пользователя, получаемое от OAuth-провайдера. Это значение используется для представления пользователя в приложении	Строка
client_id	Уникальный идентификатор клиента, выданный OAuth-провайдером при регистрации приложения. Укажите значение **Client ID**, которое вы ввели на шаге 2.2 при конфигурировании Keycloak	Строка
client_secret	Секретный ключ, выданный вместе с client_id, необходимый для обеспечения безопасности при обмене данными между приложением и OAuth-сервером. Укажите значение **Client Secret**, которое вы сохранили на шаге 2.2 при получении параметров SSO из Keycloak	Строка
whiteboard_api_partner	Произвольное значение. Используется для разделения области видимости документов, если в системе используется несколько доменов	Строка
whiteboard_api_key	Произвольное значение. Ключ API для доступа к ресурсам определенного whiteboard_api_partner	Строка
admins	Адреса администраторов вашей организации, которые получат доступ к администрированию	Массив

Дополнительные поля

```
"sso":{
    "module_type":"sso",
```

use_teams	Необязательный параметр. Определяет режим личного кабинета: `true` — основная версия ЛК, `false` — упрощенная версия	Логический

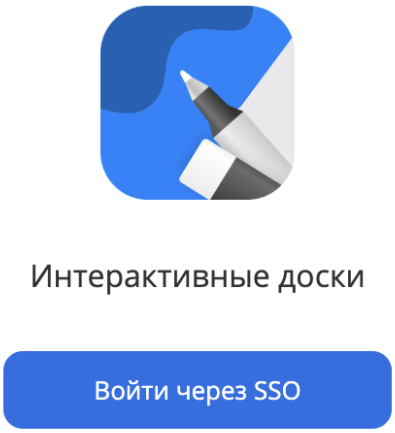
```
        ]
    }
```

Параметр	Описание	Тип данных
db_users_only	Если параметр включен, то в кабинет могут попасть только те пользователи, что уже есть в базе данных. До версии 1.7.0 В базу данных добавлялись автоматически все пользователи прошедшие авторизацию	Логический
admins	Позволяет задать начальный список авторизованных администраторов	Массив(Строка)

Работа с несколькими модулями

Если необходимо обеспечить несколько точек для аутентификации пользователей, можно добавить необходимое количество конфигураций SSO в раздел `modules` файла `values.yaml`.

В этом случае при переходе в приложение пользователям будет предоставляться выбор, каким способом проводить аутентификацию.



Модуль SOO в `configmap-config.yaml`

Помимо описания параметров SOO в файле `values.yaml` необходимо переопределить параметры SSO в файле, который используется для создания ConfigMap в Kubernetes. Откройте файл `configmap-config.yaml` и замените код, содержащий параметры SSO, на блок следующего содержания:

SAML

```
"sso": {
    "module_type": "{{ .Values.modules.sso.module_type }}",
    "type": "{{ .Values.modules.sso.type }}",
    "entry_point": "{{ .Values.modules.sso.entry_point }}",
    "issuer": "{{ .Values.modules.sso.issuer }}",
    "cert": "{{ .Values.modules.sso.cert }}",
    "callback_url": "{{ .Values.modules.sso.callback_url }}",
    "field_id": "{{ .Values.modules.sso.field_id }}",
    "field_name": "{{ .Values.modules.sso.field_name }}",
    "exit_url": "{{ .Values.modules.sso.exit_url }}",
    "whiteboard_api_partner": "{{ .Values.modules.sso.api_partner }}",
    "whiteboard_api_key": "{{ .Values.modules.sso.api_key }}"
},
```

OpenID

```
"sso": {
    "module_type": "{{ .Values.modules.sso.module_type }}",
    "type": "{{ .Values.modules.sso.type }}",
    "callback_url": "{{ .Values.modules.sso.callback_url }}",
    "authorization_url": "{{ .Values.modules.sso.authorization_url }}",
    "token_url": "{{ .Values.modules.sso.token_url }}",
    "info_url": "{{ .Values.modules.sso.info_url }}",
    "scope": "{{ .Values.modules.sso.scope }}",
    "authorization_type": "{{ .Values.modules.sso.authorization_type }}",
    "field_id": "{{ .Values.modules.sso.field_id }}",
    "field_name": "{{ .Values.modules.sso.field_name }}",
    "client_id": "{{ .Values.modules.sso.client_id }}",
    "client_secret": "{{ .Values.modules.sso.client_secret }}",
    "whiteboard_api_partner": "{{ .Values.modules.sso.whiteboard_api_partner }}",
    "whiteboard_api_key": "{{ .Values.modules.sso.whiteboard_api_key }}",
    "admins":{{ .Values.modules.sso.admins | toJson }}
},
```

Возможные ошибки при настройке

Несовпадение ключей

Ошибки вида:

```
8|whiteboard | /sso/callback SAML endpoint hit
8|whiteboard | Ошибка аутентификации: Error: Failed to read asymmetric key
```

или

```
8|whiteboard | /sso/callback SAML endpoint hit
8|whiteboard | Ошибка аутентификации: Error: Invalid signature
```

свидетельствует о несовпадении ключей между сервером и приложением. Проверьте ключи на соответсвие. Если в метаданных содержится несколько ключей, то необходимо проверить их все.

Другие ошибки протоколов

SAML

Если при использовании модуля SSO браузер возвращает следующую ошибку:

`{error: -1}`

```
0|whiteboard  | /sso/callback SAML endpoint hit
0|whiteboard  | User authenticated {
0|whiteboard  | issuer: 'http://adfs.mycorp.com/adfs/services/trust',
```

проверьте правильность заполнения следующих полей:

```
"field_id": "http://schemas.xmlsoap.org/claims/EmailAddress",
"field_name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name",
```

OpenID

Ошибка, связанная с токеном:

```
editboard  | 0|whiteboard  | /sso/callback endpoint hit
editboard  | 0|whiteboard  | 2024-02-16 18:10:37)accessToken: {содержимое токена}
editboard  | 0|whiteboard  | Ошибка аутентификации: [AxiosError: Request failed with
status code 401] {
editboard  | 0|whiteboard  |   code: 'ERR_BAD_REQUEST',
```

может возникать в случаях, когда выбран неверный `"authorization_type"` в секции SSO. Тип, использованный в токене и ожидаемый приложением, должны иметь полное соответствие.

Настройка конфигурации ClickHouse

> **Примечание**
>
> Реализация может отличаться в зависимости от особенностей архитектуры кластера

Операции со стороны ClickHouse

Пример создания базы (общий случай)

```
CREATE DATABASE pruffme ENGINE = Atomic;

CREATE TABLE pruffme.actions_online (`eventDate` Date, `eventTime` DateTime,
`service` String, `serviceProcess` Int32 DEFAULT CAST(0, 'Int32'), `duration` Int32
DEFAULT CAST(0, 'Int32'), `action` String, `number` Int32 DEFAULT CAST(0, 'Int32'),
`values` Int32 DEFAULT CAST(0, 'Int32')) ENGINE = Distributed('default', 'pruffme',
'actions_online_table', rand()) ;
CREATE TABLE pruffme.actions_online_table (`eventDate` Date, `eventTime` DateTime,
`service` String, `serviceProcess` Int32 DEFAULT CAST(0, 'Int32'), `duration` Int32
DEFAULT CAST(0, 'Int32'), `action` String, `number` Int32 DEFAULT CAST(0, 'Int32'),
`values` Int32 DEFAULT CAST(0, 'Int32')) ENGINE = MergeTree() PARTITION BY
toYYYYMM(eventDate) PRIMARY KEY action ORDER BY action SETTINGS index_granularity =
8192 ;
CREATE TABLE pruffme.objects_online (`eventDate` Date, `eventTime` DateTime,
`service` String, `serviceProcess` Int32 DEFAULT CAST(0, 'Int32'), `partner` String,
`presentation` String, `dashboard` String, `duration` Int32 DEFAULT CAST(0, 'Int32'),
`object` String, `number` Int32 DEFAULT CAST(0, 'Int32')) ENGINE =
Distributed('default', 'pruffme', 'objects_online_table', rand()) ;
CREATE TABLE pruffme.objects_online_table (`eventDate` Date, `eventTime` DateTime,
`service` String, `serviceProcess` Int32 DEFAULT CAST(0, 'Int32'), `partner` String,
`presentation` String, `dashboard` String, `duration` Int32 DEFAULT CAST(0, 'Int32'),
`object` String, `number` Int32 DEFAULT CAST(0, 'Int32')) ENGINE = MergeTree()
PARTITION BY toYYYYMM(eventDate) PRIMARY KEY dashboard ORDER BY dashboard SETTINGS
index_granularity = 8192 ;
CREATE TABLE pruffme.opens_stat (`eventDate` Date, `eventTime` DateTime, `partner`
String, `participant` String, `userNative` String, `ip` String, `service` String,
`serviceProcess` Int32 DEFAULT CAST(0, 'Int32'), `type` Int32 DEFAULT CAST(0,
'Int32'), `presentation` String, `creator` String, `creatorNative` String) ENGINE =
Distributed('default', 'pruffme', 'opens_stat_table', rand()) ;
CREATE TABLE pruffme.opens_stat_table (`eventDate` Date, `eventTime` DateTime,
`partner` String, `participant` String, `userNative` String, `ip` String, `service`
String, `serviceProcess` Int32 DEFAULT CAST(0, 'Int32'), `type` Int32 DEFAULT CAST(0,
'Int32'), `presentation` String, `creator` String, `creatorNative` String) ENGINE =
MergeTree() PARTITION BY toYYYYMM(eventDate) PRIMARY KEY participant ORDER BY
participant SETTINGS index_granularity = 8192 ;
CREATE TABLE pruffme.participants_online (`eventDate` Date, `eventTime` DateTime,
`partner` String, `presentation` String, `dashboard` String, `participant` String,
```

```
`service` String, `serviceProcess` Int32 DEFAULT CAST(0, 'Int32'), `duration` Int32
DEFAULT CAST(0, 'Int32'), `editor` Int8, `moderator` Int8, `userNative` String)
ENGINE = Distributed('default', 'pruffme', 'participants_online_table', rand()) ;
CREATE TABLE pruffme.participants_online_table (`eventDate` Date, `eventTime`
DateTime, `partner` String, `presentation` String, `dashboard` String, `participant`
String, `service` String, `serviceProcess` Int32 DEFAULT CAST(0, 'Int32'), `duration`
Int32 DEFAULT CAST(0, 'Int32'), `editor` Int8, `moderator` Int8, `userNative` String)
ENGINE = MergeTree() PARTITION BY toYYYYMM(eventDate) PRIMARY KEY dashboard ORDER BY
dashboard SETTINGS index_granularity = 8192 ;
```

Дополнительно (1.10.0 и выше)

Необходимо кроме основного скрипта создания базы, выполнить добавление `countable`

```
ALTER TABLE pruffme.participants_online_table ADD COLUMN IF NOT EXISTS `countable`
Int8 DEFAULT 1;
```

Добавление пользователя и установка для него прав доступа

```
CREATE USER pruffme IDENTIFIED WITH plaintext_password BY 'pruffme';
GRANT ALL ON pruffme.* TO pruffme;
```

Настройка приложения

Добавляем в файл конфигурации приложения `config.json` следующие параметры:

`"clickhouse"` в `"type": []`

Пример

```
    "type": [
        "api",
        "socket",
        "upload",
        "clickhouse",
        "coordinator"
    ],
```

Кроме этого добавляем новую секцию "clickhouse" с параметрами для подключения к ClickHouse

```
    "clickhouse":{
        "url":"http://my.clickhouse.addr/",
        "port":8123,
        "database":"pruffme",
        "username":"pruffme",
```

```
        "password":"pruffme"
    }
```

Пример в общей конфигурации

```
    ....
    "priority": 1,
    "redis": {
        "host": "127.0.0.1",
        "port": 6379,
        "pass":
"0498320e6a7840e45th06380e291eb21cfatyuefc3b4d22c83dd7d34161150000"
    },
    "clickhouse": {
        "url": "http://121.139.121.2/",
        "port": 8123,
        "database": "test",
        "username": "default",
        "password": "DefaultPassword"
    },
    "jwtkey": "testtest",
    ...
```

Совет

На время тестирования, проверить работает ли подключение к clickhouse, можно добавить параметр config.clickhouse.flush_number:1
Таким образом данные о действиях в базе будут появляться сразу, после единичного действия

Настройка импорта досок из Miro

Создание и подключение приложения для импорта

Для настройки импорта досок из Miro в наше приложение необходимо выполнить следующие шаги:

1. Получение аккаунта разработчика на портале разработчик Miro

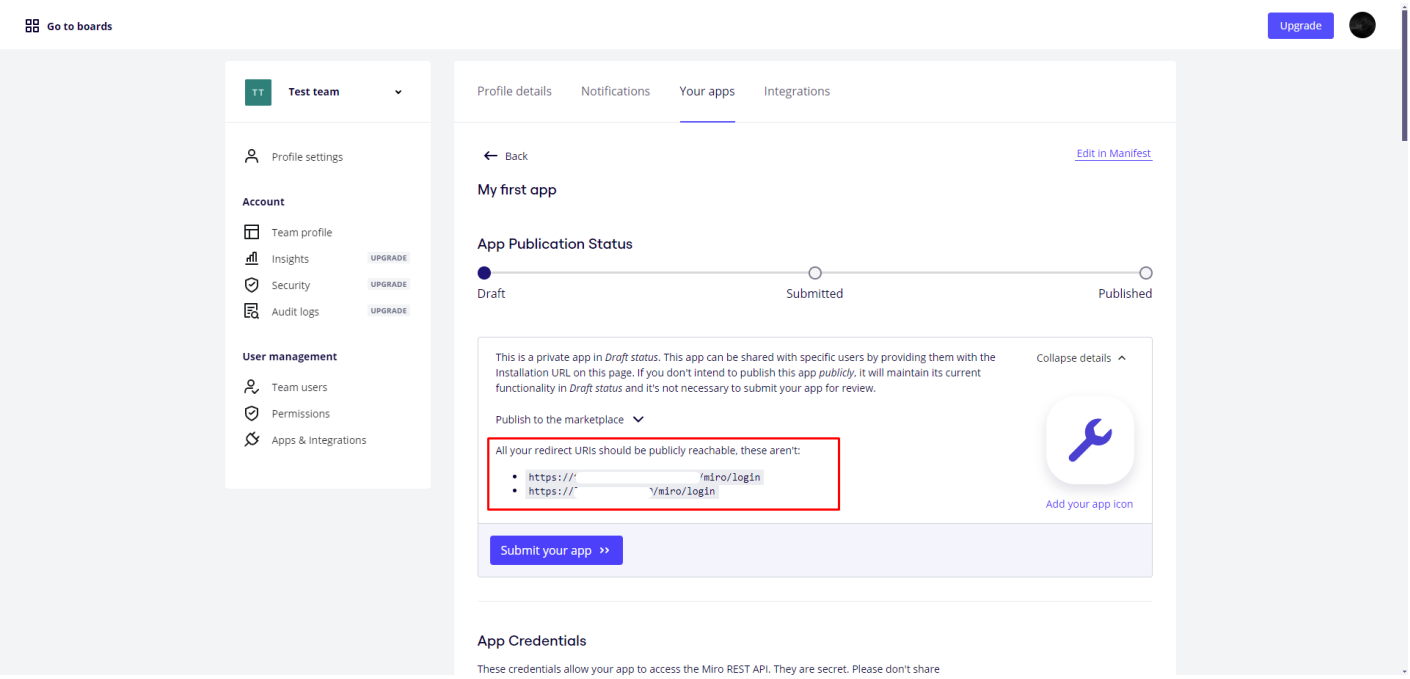
Перейдите на портал разработчиков Miro и зарегистрируйте свой аккаунт как аккаунт разработчика.

2. Создание приложения в Miro

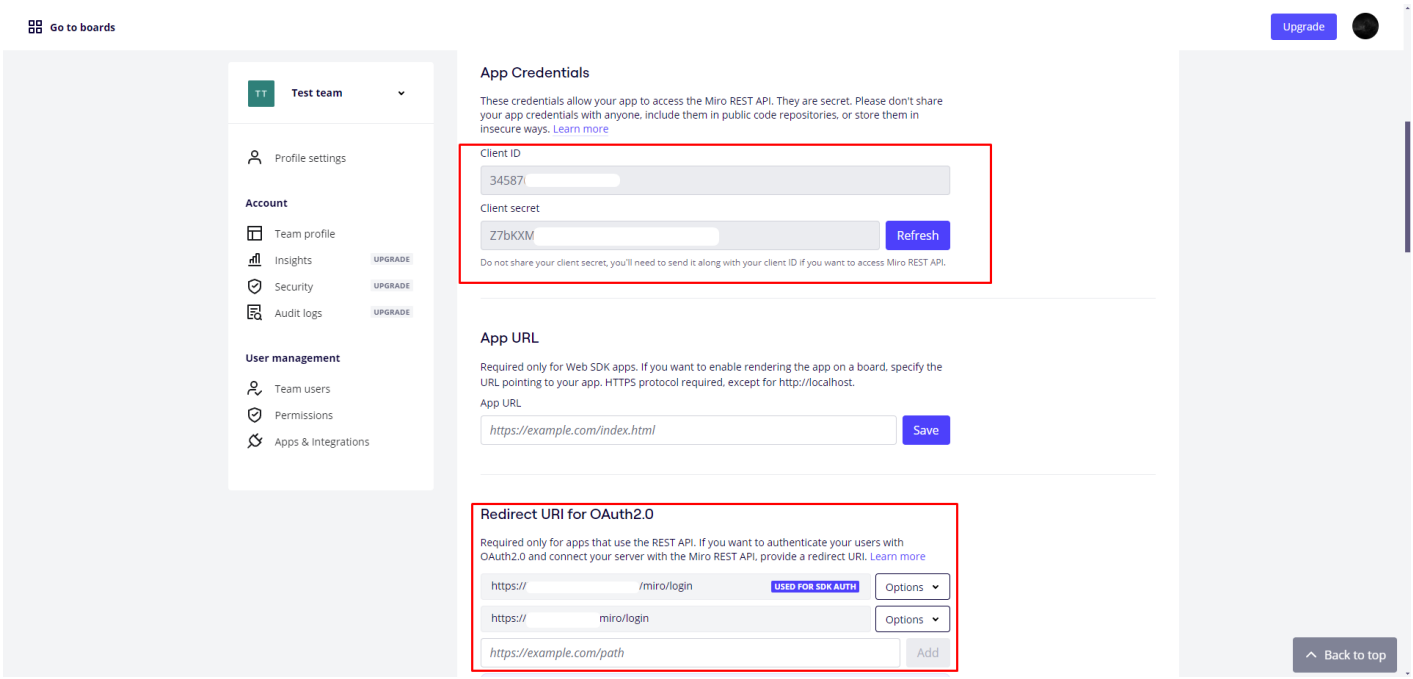
Перейдите в раздел `Your apps` и выберите `Create a new app`. Название приложения может быть произвольным.

3. Настройка приложения

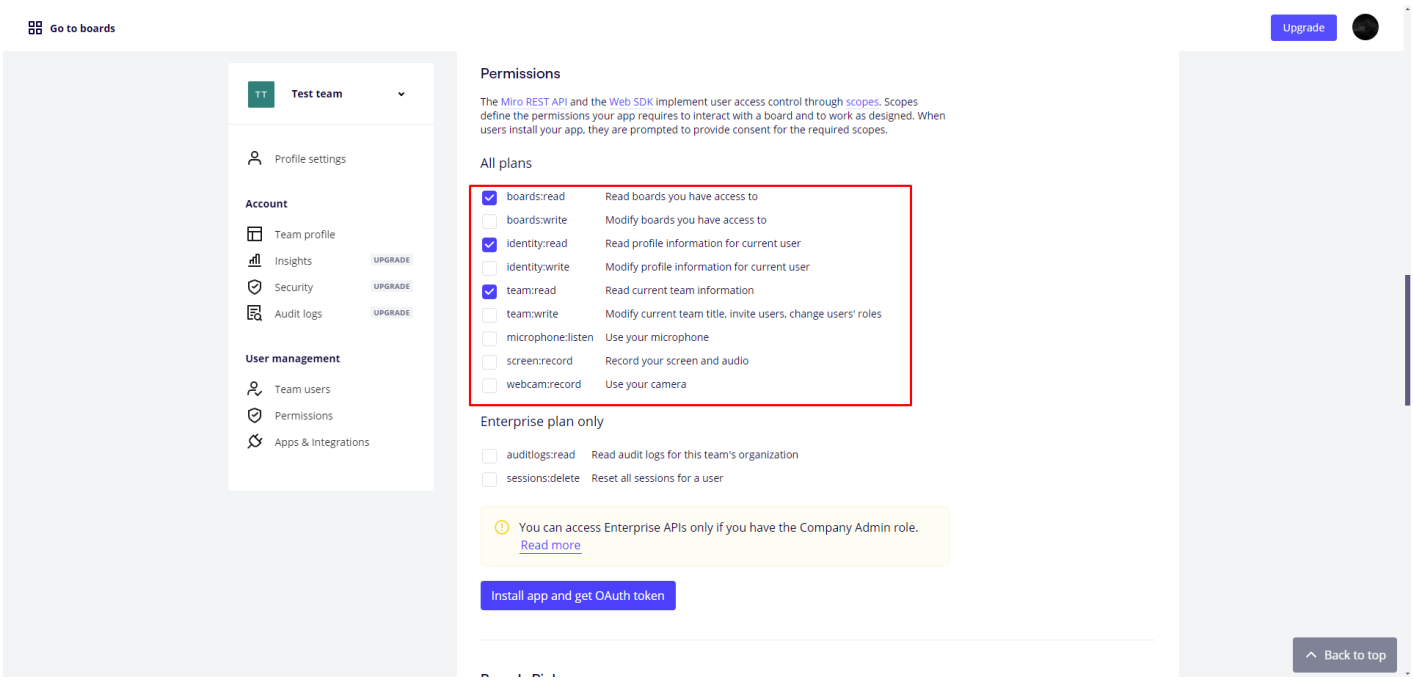
- **App URL**: Очистите это поле и нажмите `Save`. Этот параметр не нужен.
- **Redirect URI for OAuth2.0**: Обязательно укажите URI. Принцип его формирования таков: `https://${domain}/miro/login`.
  `domain` — равен значению `domain` из конфигурационного файла приложения (config.json)



- **App Credentials**: В этом разделе содержатся необходимые нам `clientId` и `secret`.



- **Permissions**: Выставьте для приложения следующие разрешения:
  - `boards:read`
  - `identity:read`
  - `team:read`



- **App Publication Status**: Статус приложения может оставаться в состоянии `Draft`, это не мешает работе импорта.

4. Настройки в config.json

В корневой секции файла `config.json` добавьте следующую запись:

```
"miro": {
    "clientId": "********",
    "secret": "****************",
    "debug": true
}
```

В поле `clientId` впишите значение `Client ID` из настроек вашего приложения Miro.
В поле `secret` впишите значение `Client secret` из настроек вашего приложения Miro.

Возможные неполадки и их исправление

Ошибка "error":"Cant authorize"

- Проверьте доступность для следующий ресурсов из контейнера приложения:
  https://api.miro.com
  https://miro.com

Для этого запустите curl из контейнера с приложением:

```
kubectl exec -it <имя-пода> -- /bin/bash
```

После входа в под, используйте curl для проверки доступности ресурсов:

```
curl -v https://api.miro.com
```

```
curl -v https://miro.com
```

В случае ошибок при выполнении запроса, необходимо обеспечить приложению доступ до указанных ресурсов

- Повышение значения параметра `proxy_read_timeout` до 300
- Включение `access log` в конфигурации nginx приложения,в случае, если необходима дополнительная информация

Импортированные доски не обрабатываются

В `configmap-config.yaml` не указан необходимый тип сервера.

```
"type": [
  "api",
  "socket",
  "upload",
  "redis",
  "admin",
  "coordinator",
  "convert_documents",
```

```
    "convert_video",
    "miro"<<<
    ],
```

Обновление приложения

Для обновления приложения, развернутого с помощью Helm в Kubernetes:

1. Откройте терминал и перейдите в директорию с распакованным архивом Helm.
2. Обновите релиз в Kubernetes с помощью команды:

```
helm upgrade <RELEASE> <CHART> -f values.yaml
```

где `<RELEASE>` — имя релиза, а `<CHART>` — путь к чарту.

Чтобы узнать значения `<RELEASE>` и `<CHART>`, выполните команду получения списка релизов:

```
helm list
```

Эта команда выведет таблицу с установленными релизами в текущем Kubernetes-кластере. В графе `NAME` будет указано имя релиза (`<RELEASE>`), а в графе `CHART` — текущая версия чарта, использованного для развертывания.

3. Получите список всех развертываний (Deployment) с помощью команды:

```
kubectl get deploy
```

4. Перезапустите нужное развертывание Досок с помощью команды:

```
kubectl rollout restart deployment/<DEPLOYMENT-NAME>
```

где `<DEPLOYMENT-NAME>` — имя нужного развертывания, например `deployment-whiteboard`.

Панель администрирования

Панель администратора предоставляет удобный интерфейс для управления всеми аспектами системы. Она включает в себя различные разделы, каждый из которых отвечает за определенные функции и возможности.

Перечень разделов:

Пользователи

В разделе «Пользователи» можно управлять учетными записями пользователей. Здесь отображается список всех пользователей в виде таблицы с возможностью сортировки по столбцам, фильтрации по состоянию, а также доступен поиск по пользователям. Для каждого пользователя доступны действия, такие как просмотр досок, команд, журналов событий, редактирование и удаление.

Команды

Раздел «Команды» позволяет управлять командами. Список команд также представлен в виде таблицы с возможностью сортировки и поиска. Можно создавать новые команды, а также выполнять различные действия с существующими командами: просматривать участников и их роли, детали команды, доски команды, действия команды, переименовывать и удалять команды.

Доски

В разделе «Доски» можно управлять всеми досками в системе. Список досок представлен в виде таблицы с возможностью сортировки и поиска. Доступны действия, такие как просмотр журнала событий доски, переименование и удаление доски.

Журнал событий

Раздел «Журнал событий» предоставляет доступ к истории всех событий в системе. События отображаются в виде таблицы с возможностью сортировки и фильтрации по типу, а также поиска. Доступен просмотр детализированной информации о каждом событии.

Роли

В разделе «Роли» можно управлять ролями пользователей. Список ролей представлен в виде таблицы. Можно создавать новые роли, редактировать существующие роли (переименовывать и изменять права), а также удалять роли.

LDAP

Раздел «LDAP» позволяет управлять подключениями и аутентификацией через LDAP. Здесь можно создавать новые подключения, проверять их работоспособность, редактировать правила и назначать права администратора для групп.

История импорта

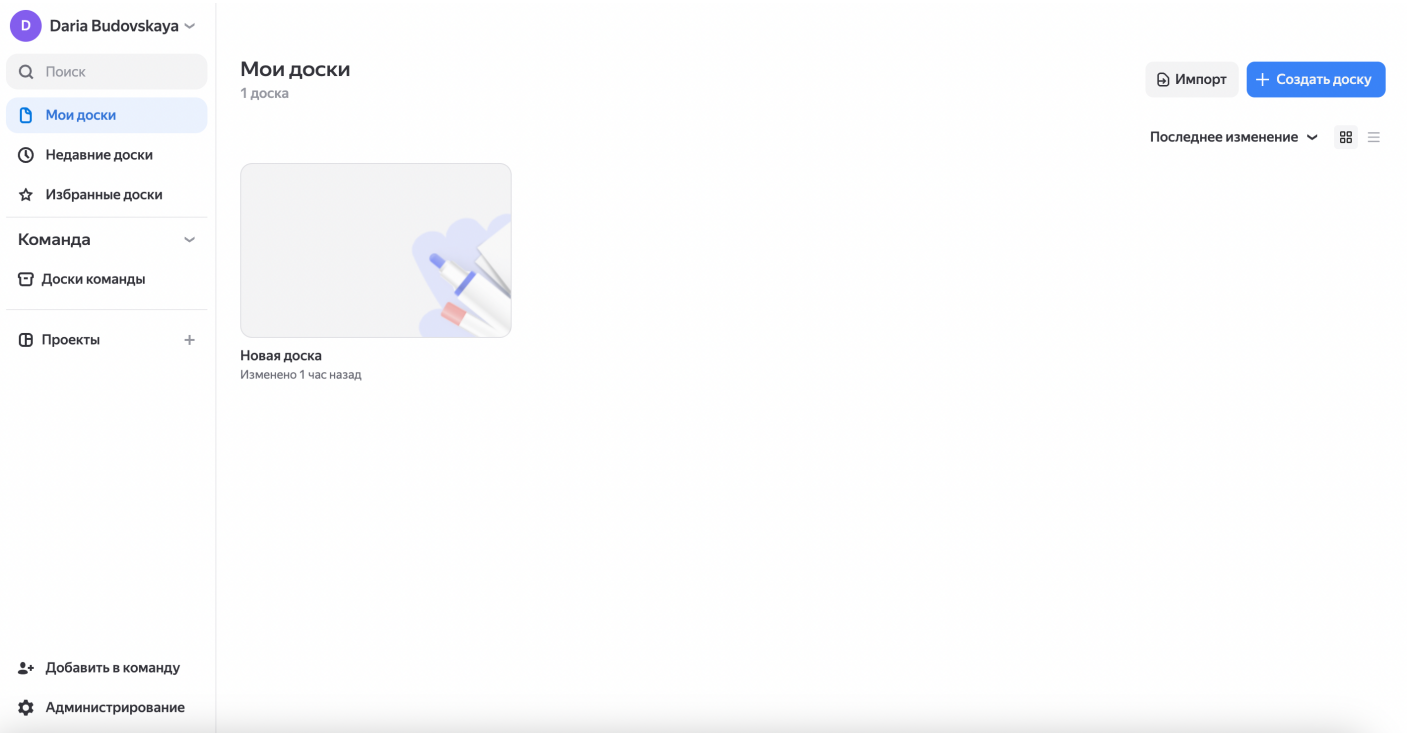
В разделе «История импорта» отображается история запуска импорта досок из Miro. В таблице отображаются логин пользователя, имя доски, конечный статус выполнения операции и дата события.

Материалы

Раздел «Материалы» позволяет управлять загруженными файлами. Список материалов представлен в виде таблицы с возможностью поиска и фильтрации по типам (изображение, видео, YouTube, аудио, вложение, презентация, скрытое изображение). Доступны действия, такие как просмотр всех материалов, загруженных пользователем, и просмотр всех материалов, использованных на доске.

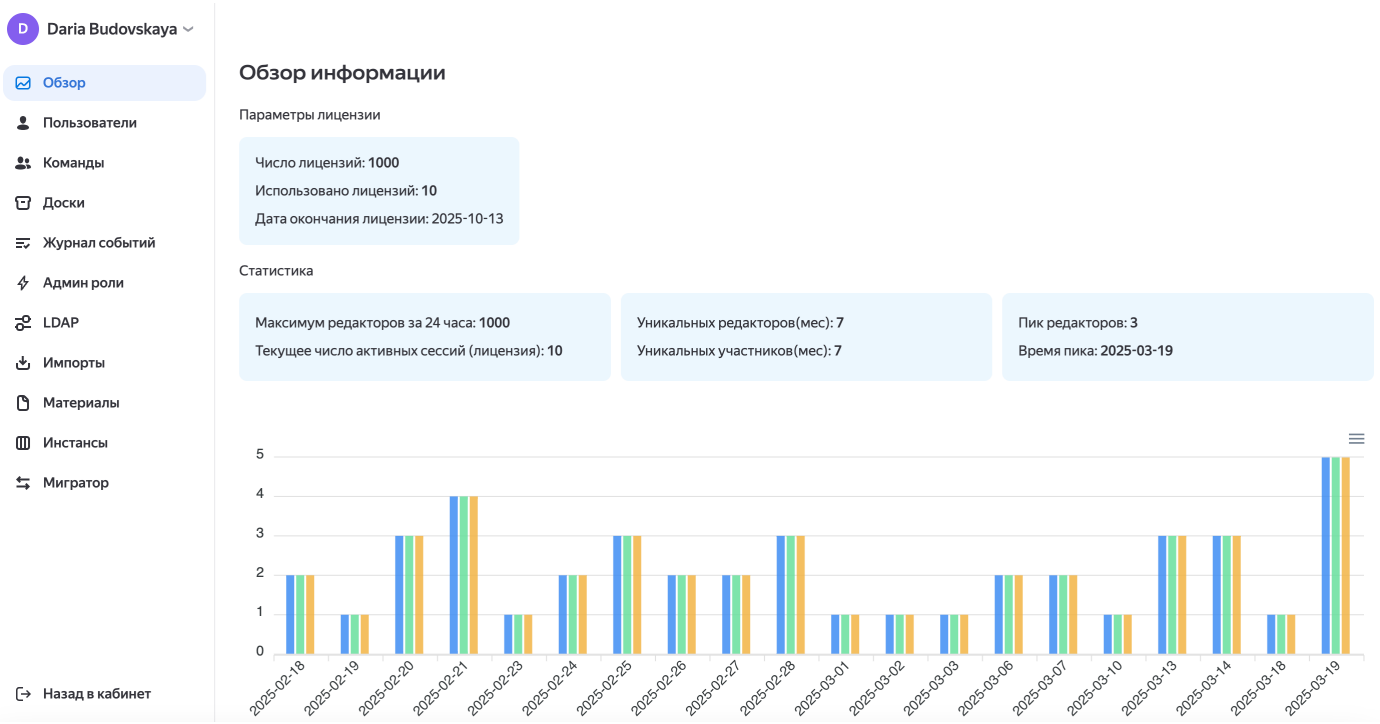
Панель администратора обеспечивает полный контроль над всеми элементами системы, позволяя легко управлять пользователями, командами, досками, событиями и другими аспектами.

Чтобы перейти в панель администратора, необходимо кликнуть на соответствующую иконку в нижнем левом углу интерфейса личного кабинета приложения



Обзор информации

В данном разделе представлена информация о лицензии, количестве активных редакторов, обработке медиа файлов и импорте из Miro.



Пользователи

В данном разделе представлена возможность управления пользователями системы. Список пользователей отображается в виде таблицы, с возможностью сортировки по столбцам. Функционал раздела включает следующие возможности:

Фильтр по состоянию пользователей

Есть возможность фильтрации пользователей по следующим состояниям:

- Действующие
- Удаленные
- Администраторы
- Операторы (роли)

Создание пользователя

Возможность добавления нового пользователя в систему.

Поиск по пользователям

Возможность поиска пользователей по различным параметрам.

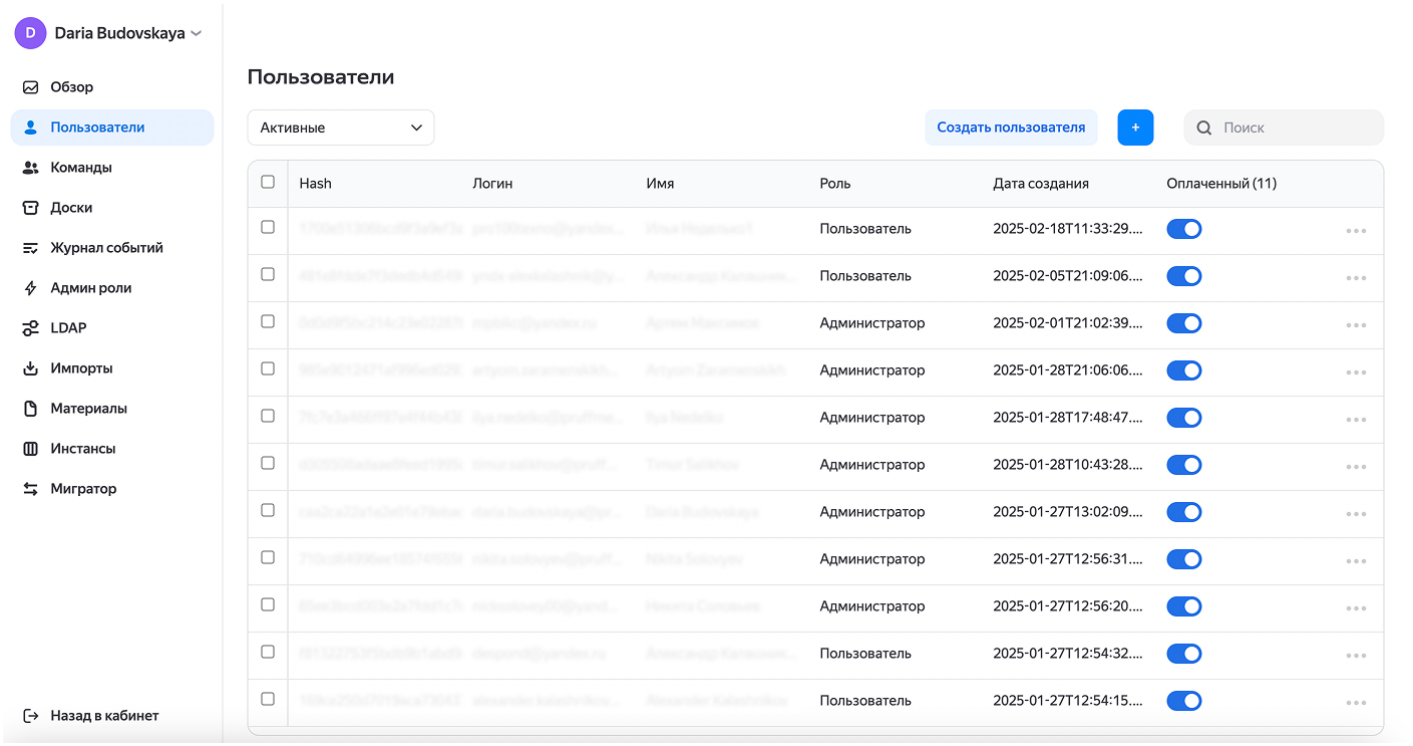
Действия с пользователями

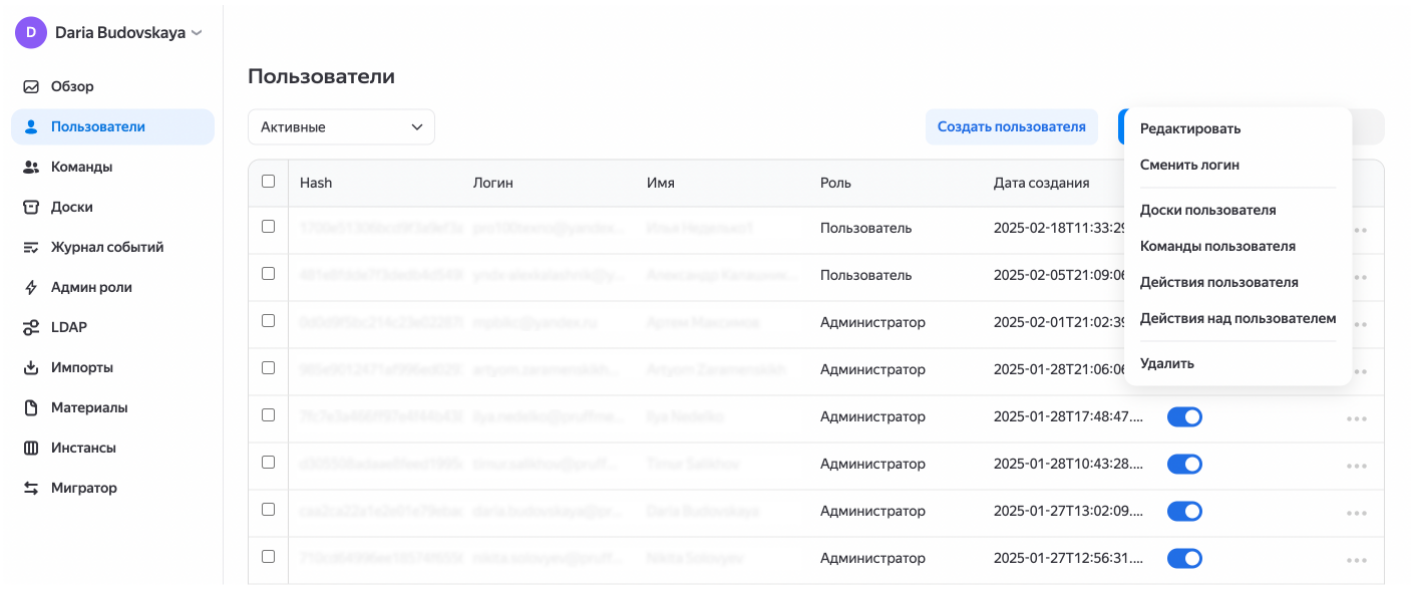
В дополнительном меню для каждого пользователя можно выполнить следующие действия:

- **Посмотреть доски пользователя**: Переход в раздел «Доски» для просмотра досок, связанных с пользователем.
- **Команды пользователя**: Переход в раздел «Команды» для просмотра команд, в которые входит пользователь.
- **Действия пользователя**: Переход в раздел «Журнал событий» для просмотра действий, совершенных пользователем.
- **Редактировать**: Редактирование данных пользователя, например изменить его имя или роль.
- **Смена логина**: Для версии 1.10.4 и выше. Позволяет изменить логин пользователя и получить новый идентификатор в системе для него.

> **Пример**
>
> Если замена логина у пользователя (А) происходит на пользователя (Б), который уже существует в системе, то весь контент пользователя (А) будет закреплен за пользователем (Б). А именно: доски, команды, проекты, медиаматериалы.
> В случае, если оба пользователя были в одной команде, то пользователь (Б) получит те же права, что были у пользователя (А). То есть, если пользователь (А) был владельцем, то им станет пользователь (Б). Однако, если пользователь (Б) изначально был создателем в команде, а пользователь (А) был участником, то пользователь (Б) перестанет владеть командой.

- **Удалить**: Удаление пользователя из системы.


Daria Budovskaya
Обзор
Пользователи
Команды
Доски
Журнал событий
Админ роли
LDAP
Импорты
Материалы
Инстансы
Мигратор
Назад в кабинет
Пользователи
Активные
Создать пользователя
+
Поиск
Hash
Логин
Имя
Роль
Дата создания
Оплаченный (11)
Пользователь 2025-02-18T11:33:29....
Пользователь 2025-02-05T21:09:06....
Администратор 2025-02-01T21:02:39....
Администратор 2025-01-28T21:06:06....
Администратор 2025-01-28T17:48:47....
Администратор 2025-01-28T10:43:28....
Администратор 2025-01-27T13:02:09....
Администратор 2025-01-27T12:56:31....
Администратор 2025-01-27T12:56:20....
Пользователь 2025-01-27T12:54:32....
Пользователь 2025-01-27T12:54:15....


Daria Budovskaya
Обзор
Пользователи
Команды
Доски
Журнал событий
Админ роли
LDAP
Импорты
Материалы
Инстансы
Мигратор
Пользователи
Активные
Создать пользователя
Редактировать
Сменить логин
Доски пользователя
Команды пользователя
Действия пользователя
Действия над пользователем
Удалить
Hash
Логин
Имя
Роль
Дата создания
Пользователь
Пользователь
Администратор
Администратор
Администратор
Администратор
Администратор
Администратор

Команды

В данном разделе представлена возможность управления командами приложения. Функционал включает следующие возможности:

Вывод списка команд

Список команд отображается в виде таблицы, с возможностью сортировки по столбцам.

Создание команды

Возможность добавления новой команды в систему.

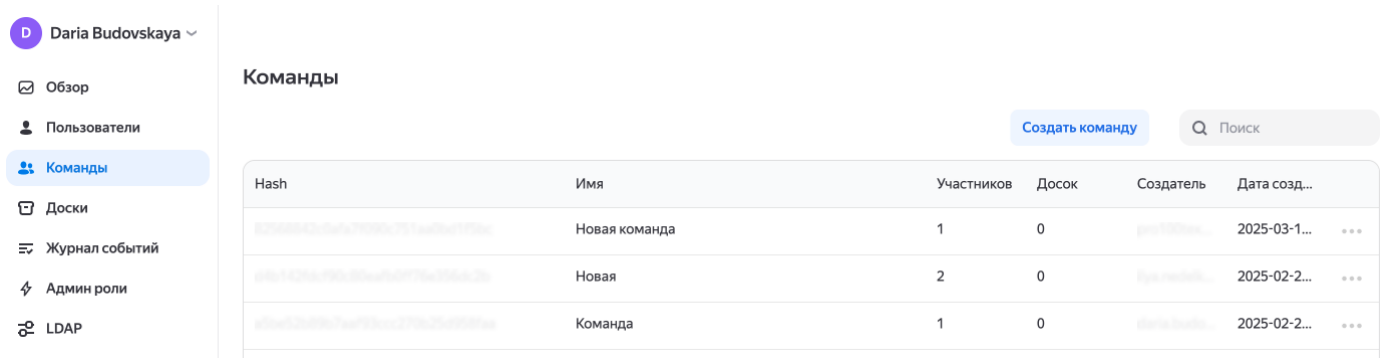
Поиск по командам

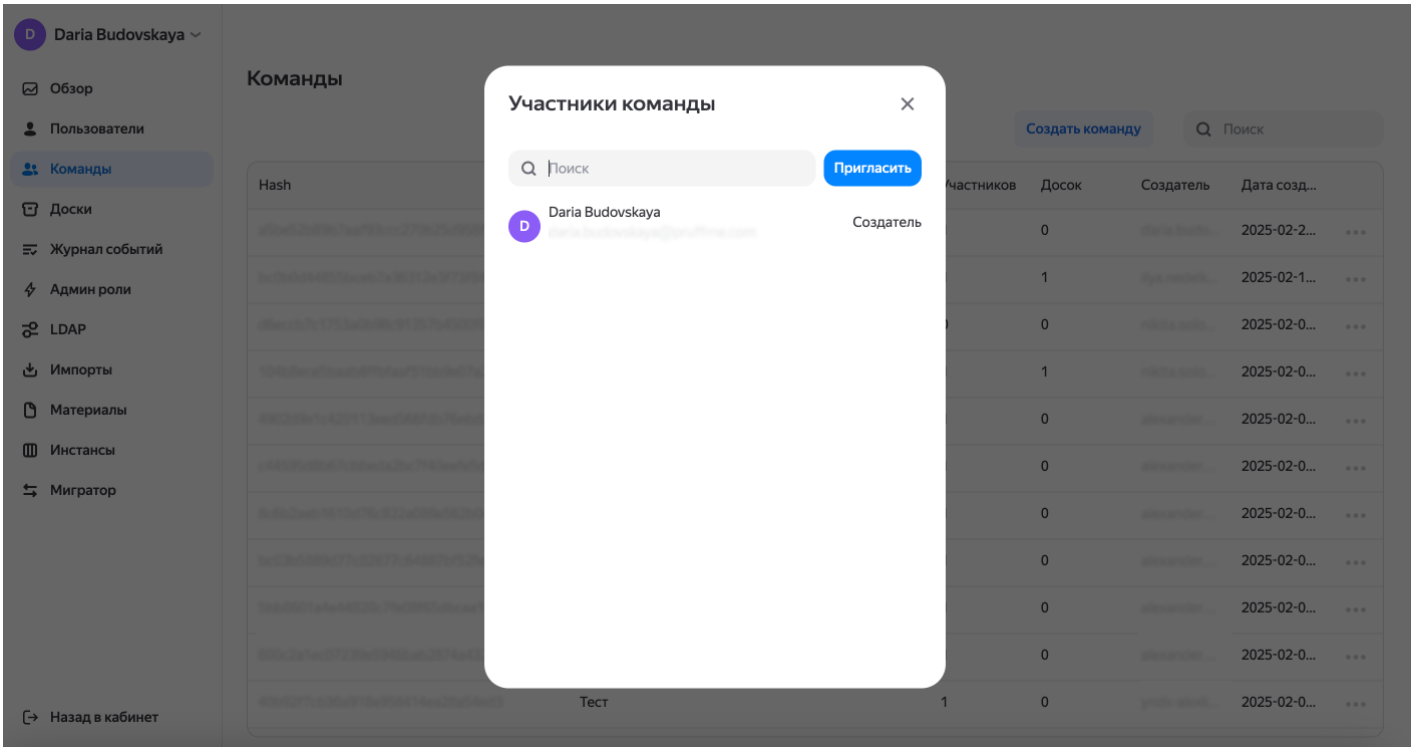
Возможность поиска команд по различным параметрам.

Действия с командами

В дополнительном меню для каждой команды можно выполнить следующие действия:

- **Участники команды**: Переход к списку участников команды с указанием их текущих ролей.
- **Детали команды**: Отображение всей информации о команде.
- **Доски команды**: Переход в раздел «Доски» для просмотра досок, созданных данной командой.
- **Действия команды**: Переход в раздел «Журнал событий» для отображения всех действий, совершенных в рамках данной команды.
- **Переименовать**: Изменение названия команды.
- **Удалить**: Удаление команды из системы.




Daria Budovskaya
Обзор
Пользователи
Команды
Доски
Журнал событий
Админ роли
LDAP
Импорты
Материалы
Инстансы
Мигратор
Назад в кабинет
Команды
Создать команду
Поиск
Hash
Участников
Досок
Создатель
Дата созд...
Участники команды
Поиск
Пригласить
Daria Budovskaya
Создатель
Тест
1
0
2025-02-0...

Доски

В данном разделе представлена возможность управления досками системы. Функционал включает следующие возможности:

Вывод списка досок

Список досок отображается в виде таблицы с возможностью сортировки по столбцам.

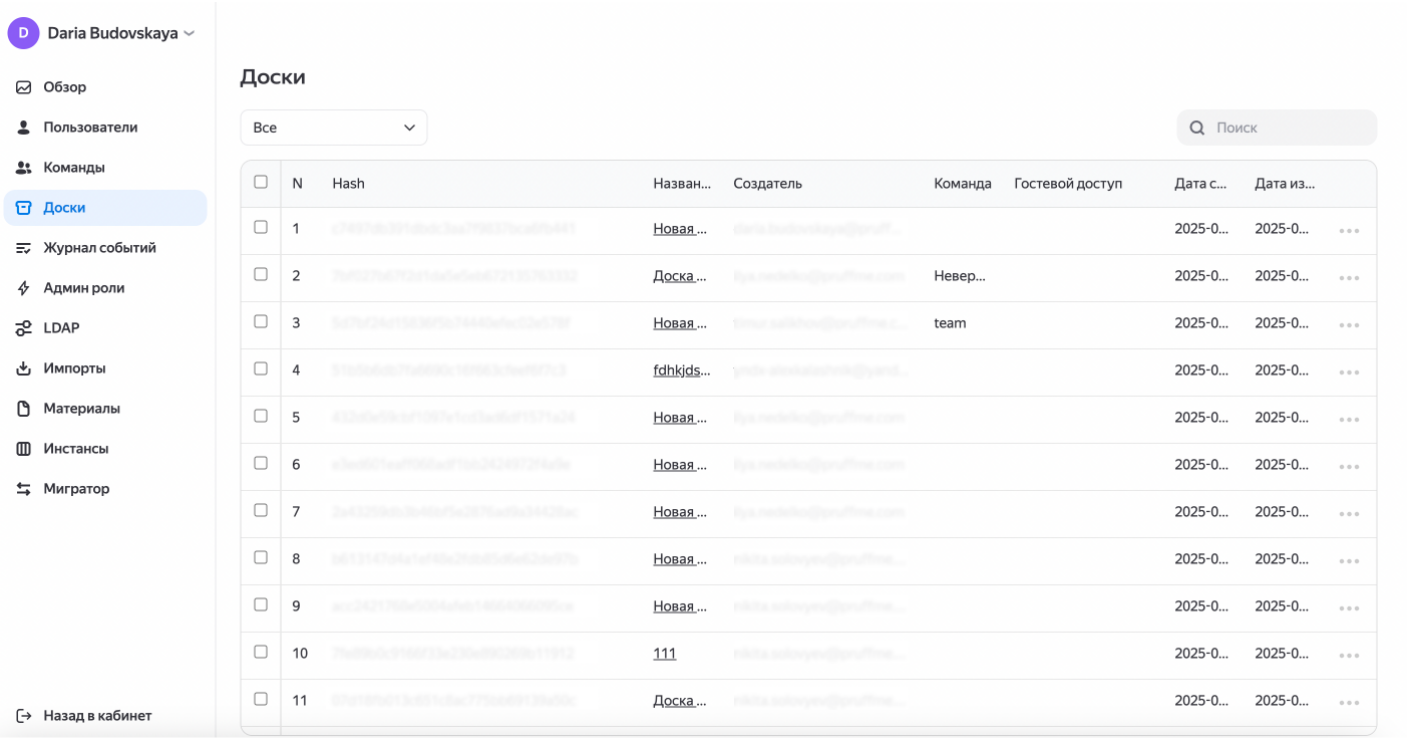
Поиск по доскам

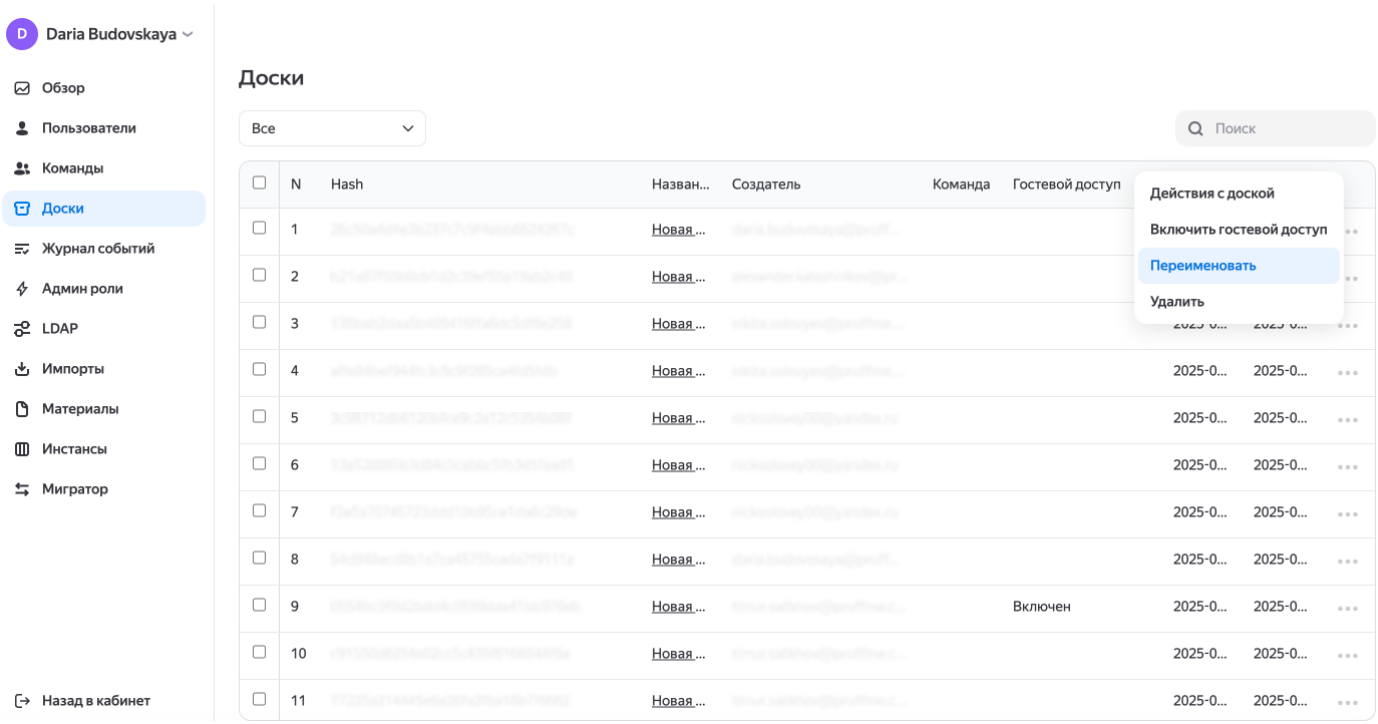
Возможность поиска досок по различным параметрам.

Действия с досками

В дополнительном меню для каждой доски можно выполнить следующие действия:

- **Действия с доской**: Переход в раздел «Журнал событий» для отображения всех действий, совершенных с данной доской.
- **Переименовать доску**: Изменение названия доски.
- **Удалить**: Удаление доски из системы.




Daria Budovskaya
Обзор
Пользователи
Команды
Доски
Журнал событий
Админ роли
LDAP
Импорты
Материалы
Инстансы
Мигратор
Назад в кабинет
Доски
Все
Поиск
N
Hash
Назван...
Создатель
Команда
Гостевой доступ
Действия с доской
Включить гостевой доступ
Переименовать
Удалить
Включен

Журнал событий

В данном разделе представлена возможность управления и просмотра событий системы. Функционал включает следующие возможности:

Вывод списка событий

Список событий отображается в виде таблицы, с возможностью сортировки по столбцам.

Фильтрация событий по типу

Есть возможность фильтровать события по различным типам.

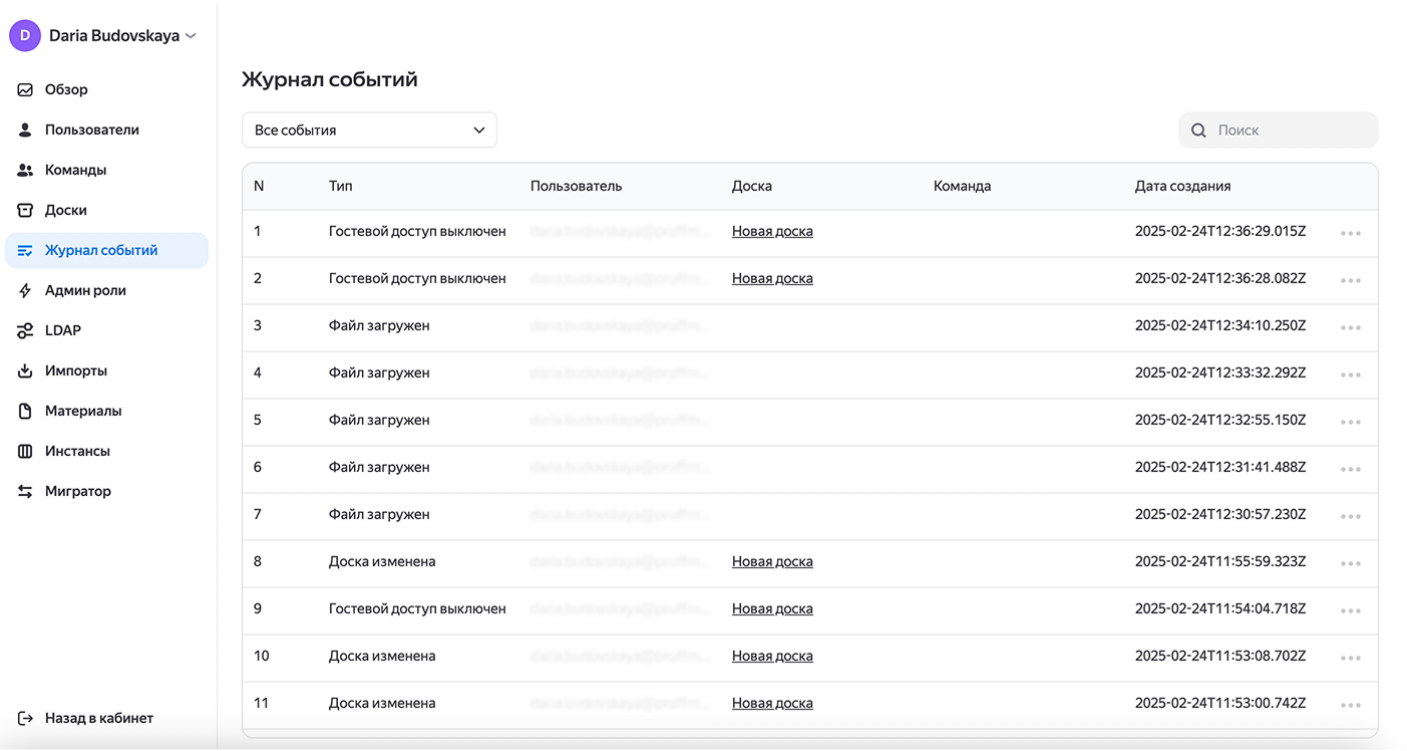
Поиск по событиям

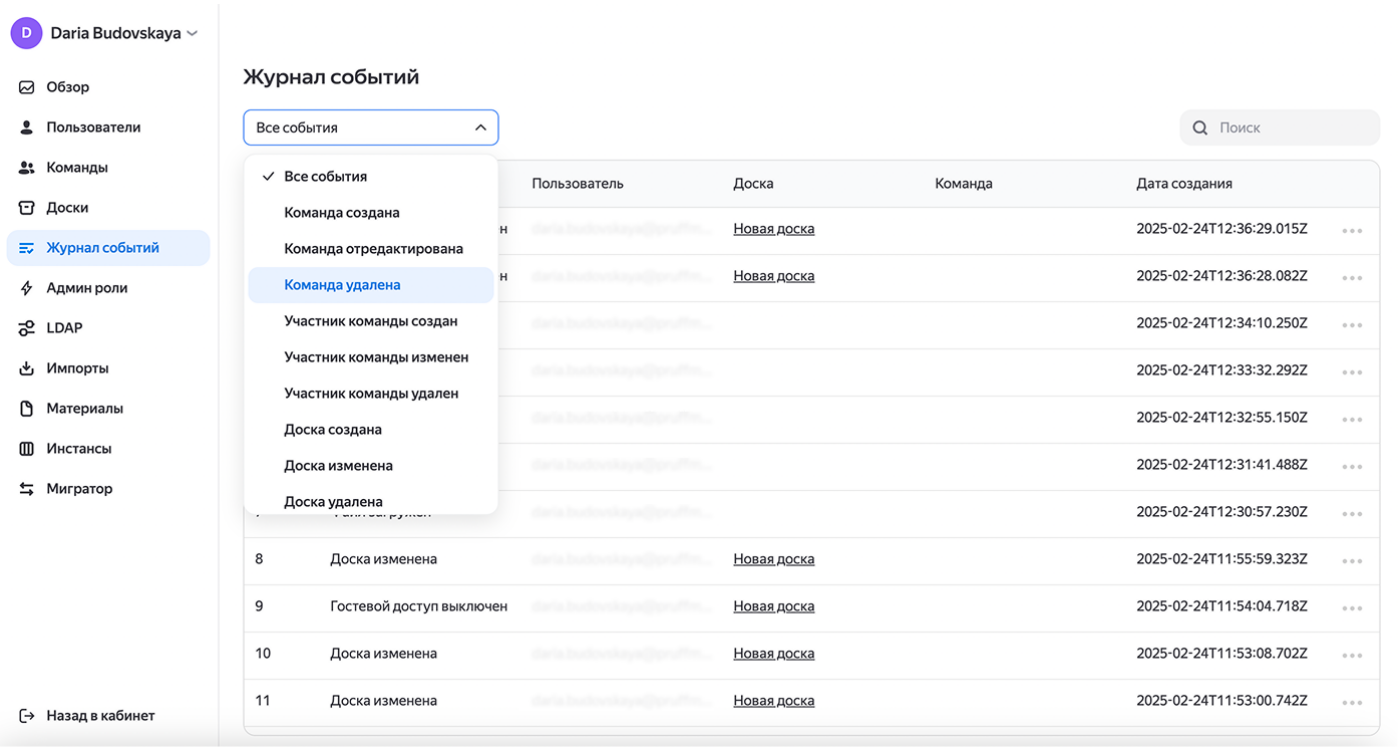
Возможность поиска событий по различным параметрам.

Действия с событиями

В дополнительном меню для каждого события можно выполнить следующие действия:

- **Просмотр детализированной информации**: Переход к подробной информации о событии.




Daria Budovskaya
Обзор
Пользователи
Команды
Доски
Журнал событий
Админ роли
LDAP
Импорты
Материалы
Инстансы
Мигратор
Назад в кабинет
Журнал событий
Все события
Поиск
Все события
Команда создана
Команда отредактирована
Команда удалена
Участник команды создан
Участник команды изменен
Участник команды удален
Доска создана
Доска изменена
Доска удалена
Пользователь
Доска
Команда
Дата создания
Новая доска
2025-02-24T12:36:29.015Z
2025-02-24T12:36:28.082Z
2025-02-24T12:34:10.250Z
2025-02-24T12:33:32.292Z
2025-02-24T12:32:55.150Z
2025-02-24T12:31:41.488Z
2025-02-24T12:30:57.230Z
8 Доска изменена Новая доска 2025-02-24T11:55:59.323Z
9 Гостевой доступ выключен Новая доска 2025-02-24T11:54:04.718Z
10 Доска изменена Новая доска 2025-02-24T11:53:08.702Z
11 Доска изменена Новая доска 2025-02-24T11:53:00.742Z

Роли

В данном разделе представлена возможность управления ролями в системе. Функционал включает следующие возможности:

Вывод списка ролей

Список ролей отображается в виде таблицы.

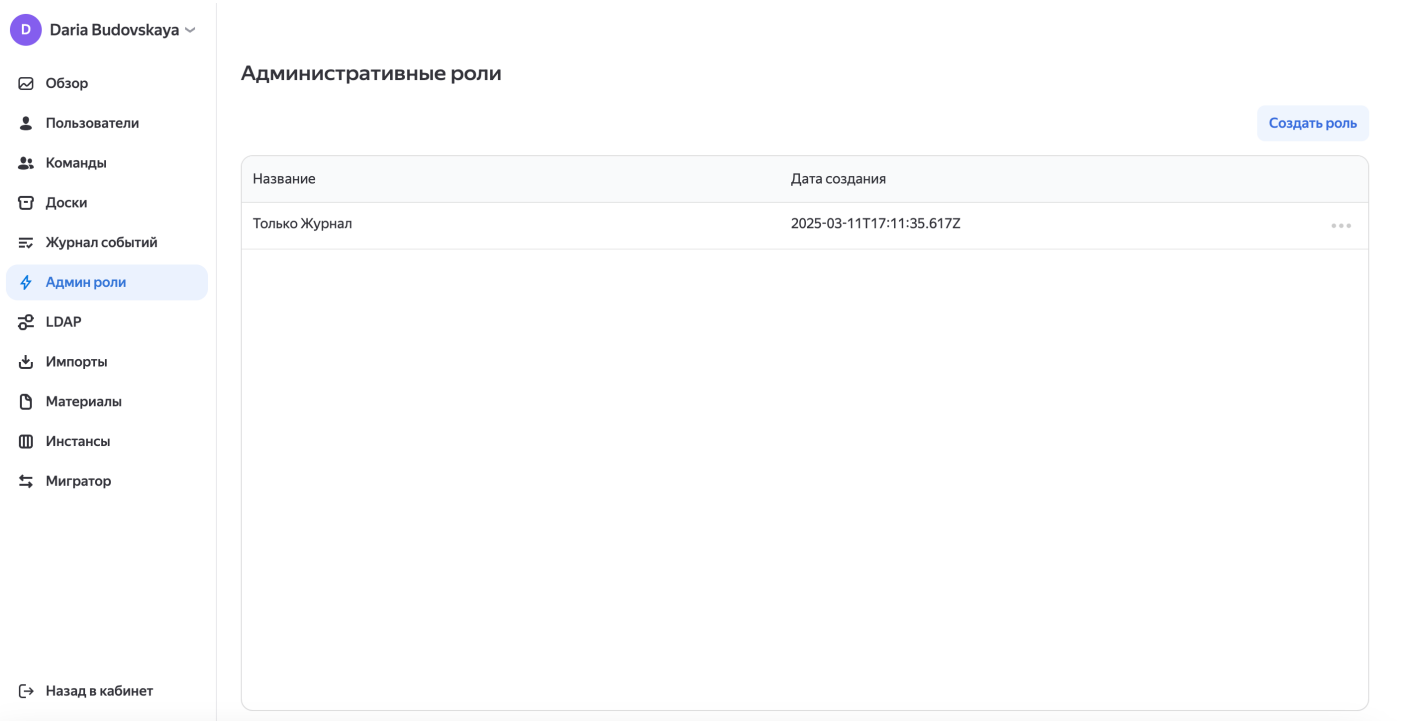
Создание роли

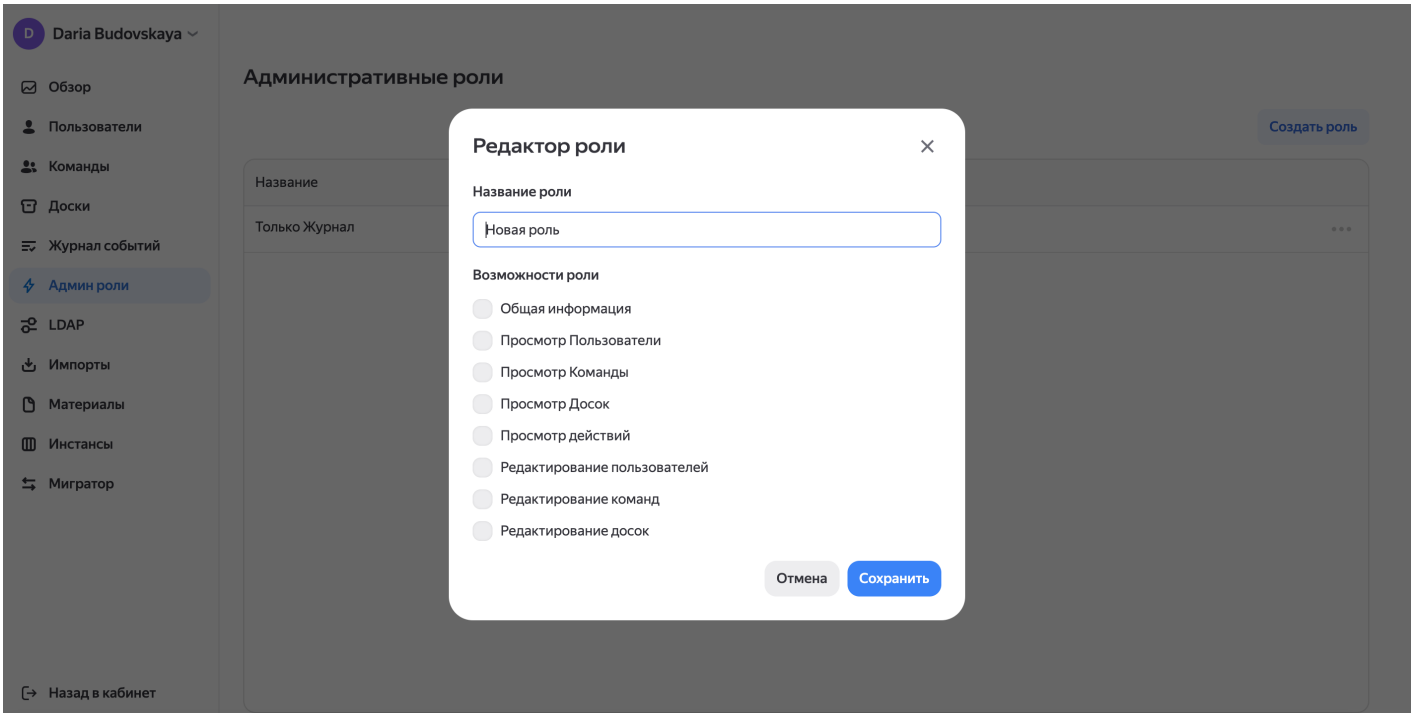
Возможность добавления новой роли в систему. Новая роль может быть настроена в соответствии с потребностями пользователей.

Действия с ролями

В дополнительном меню для каждой роли можно выполнить следующие действия:

- **Редактировать**: Переименование роли и изменение прав в рамках выбранной роли.
- **Удалить**: Удаление роли из системы.




Daria Budovskaya
Обзор
Пользователи
Команды
Доски
Журнал событий
Админ роли
LDAP
Импорты
Материалы
Инстансы
Мигратор
Назад в кабинет
Административные роли
Создать роль
Название
Только Журнал
Редактор роли
Название роли
Новая роль
Возможности роли
Общая информация
Просмотр Пользователи
Просмотр Команды
Просмотр Досок
Просмотр действий
Редактирование пользователей
Редактирование команд
Редактирование досок
Отмена
Сохранить

LDAP

В данном разделе представлена возможность управления правилами подключения и аутентификации через LDAP. Функционал включает следующие возможности:

Вывод списка правил

Список правил отображается в виде таблицы.

Создание и проверка подключения по LDAP

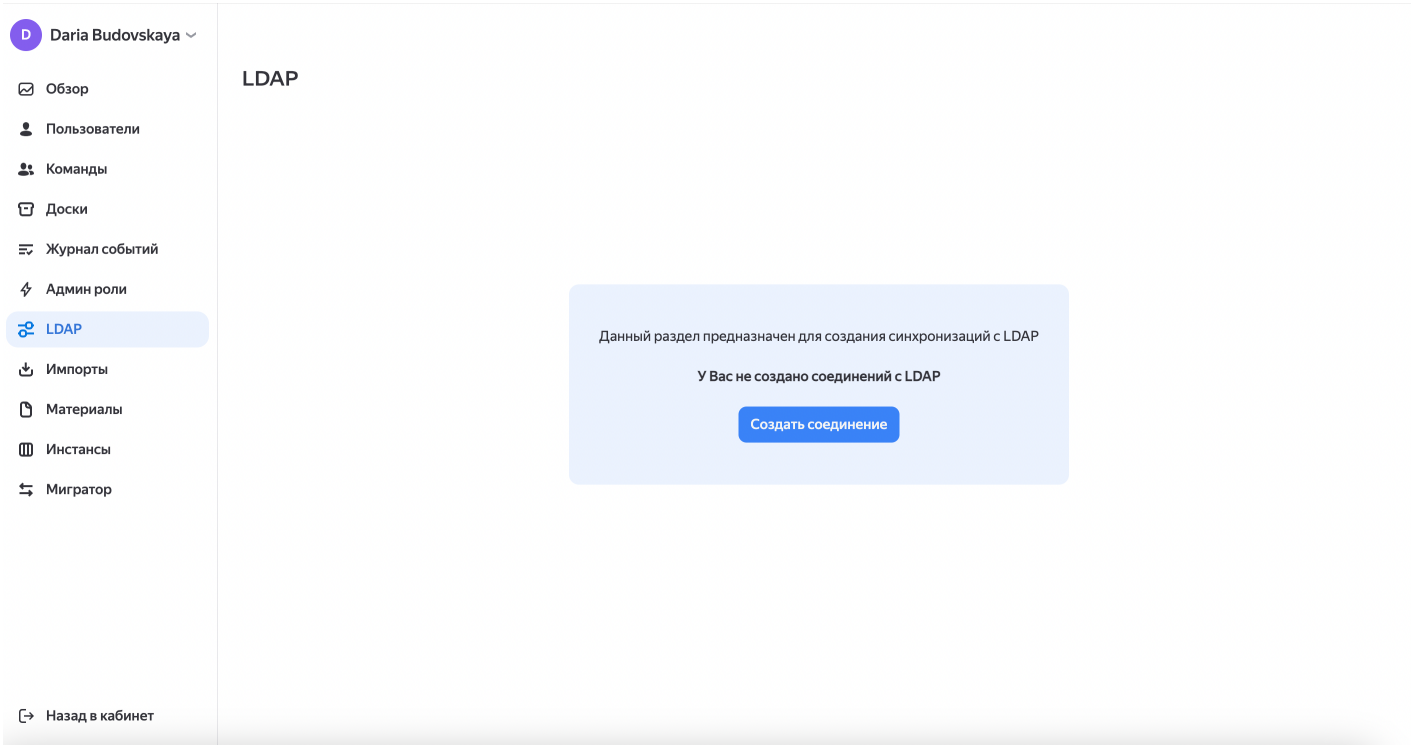
Возможность создания нового подключения по LDAP и проверки его работоспособности.

Редактирование списка правил

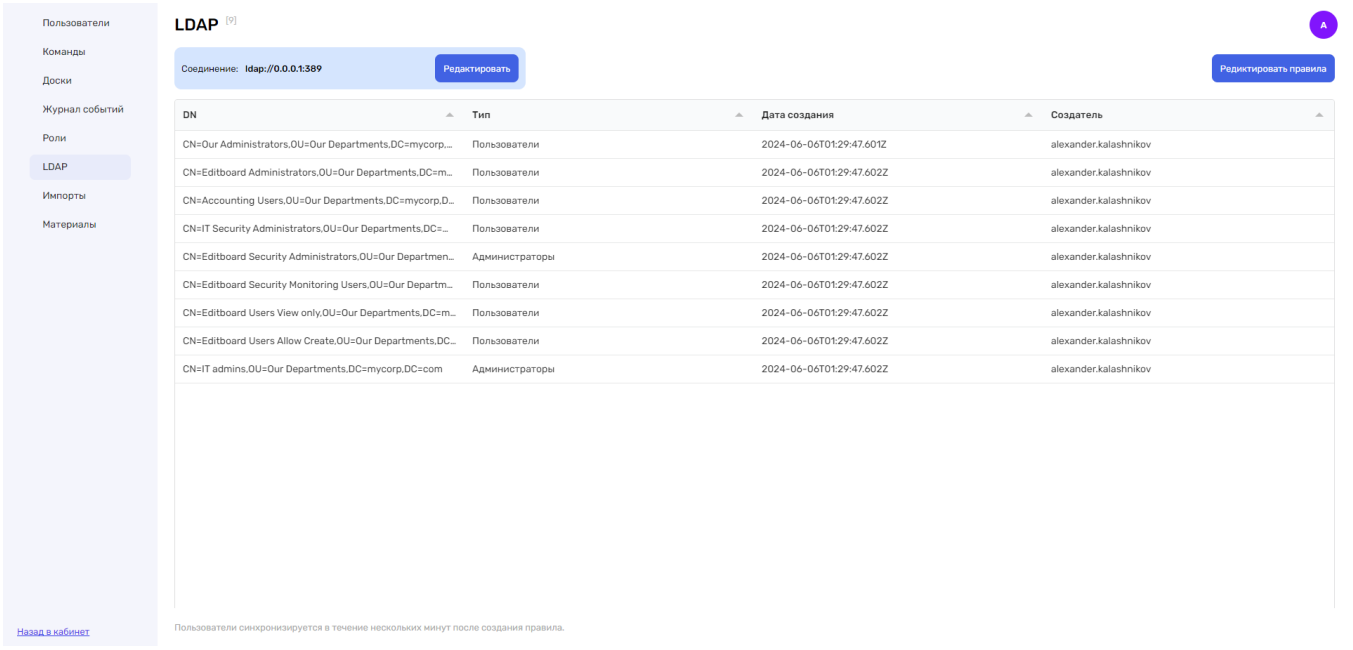
Возможность редактирования существующих правил LDAP.

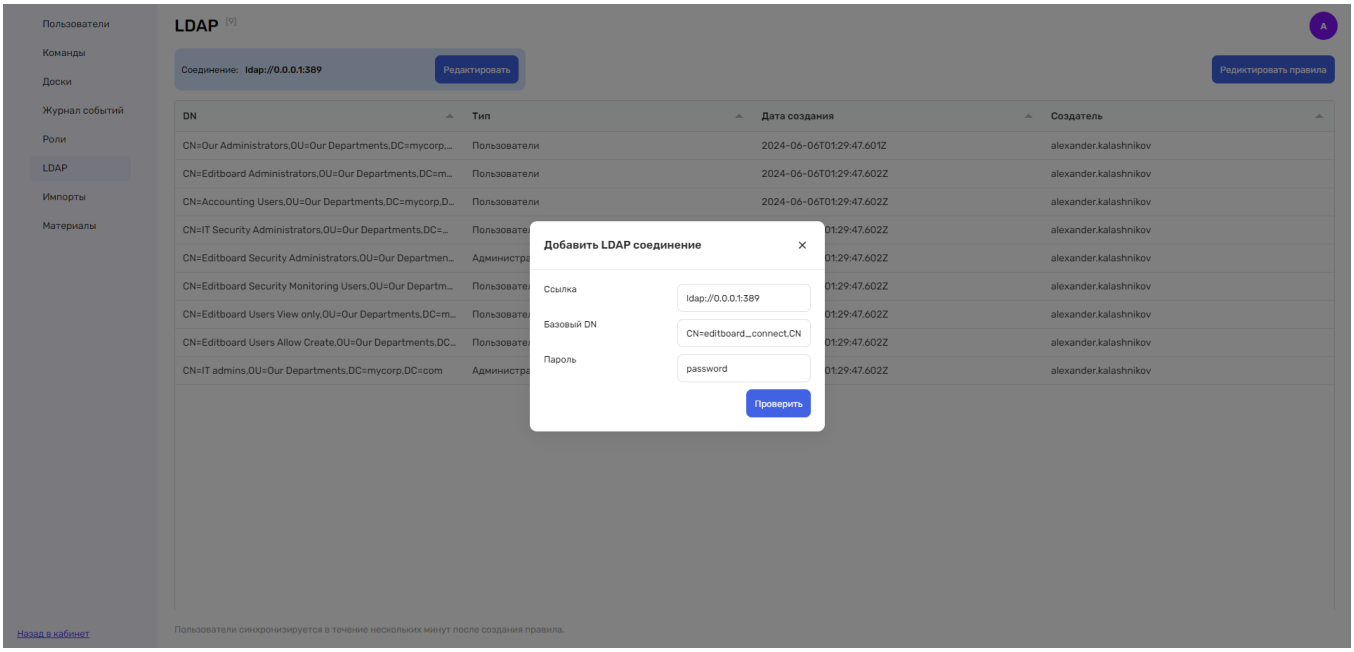
Установка прав администратора для группы

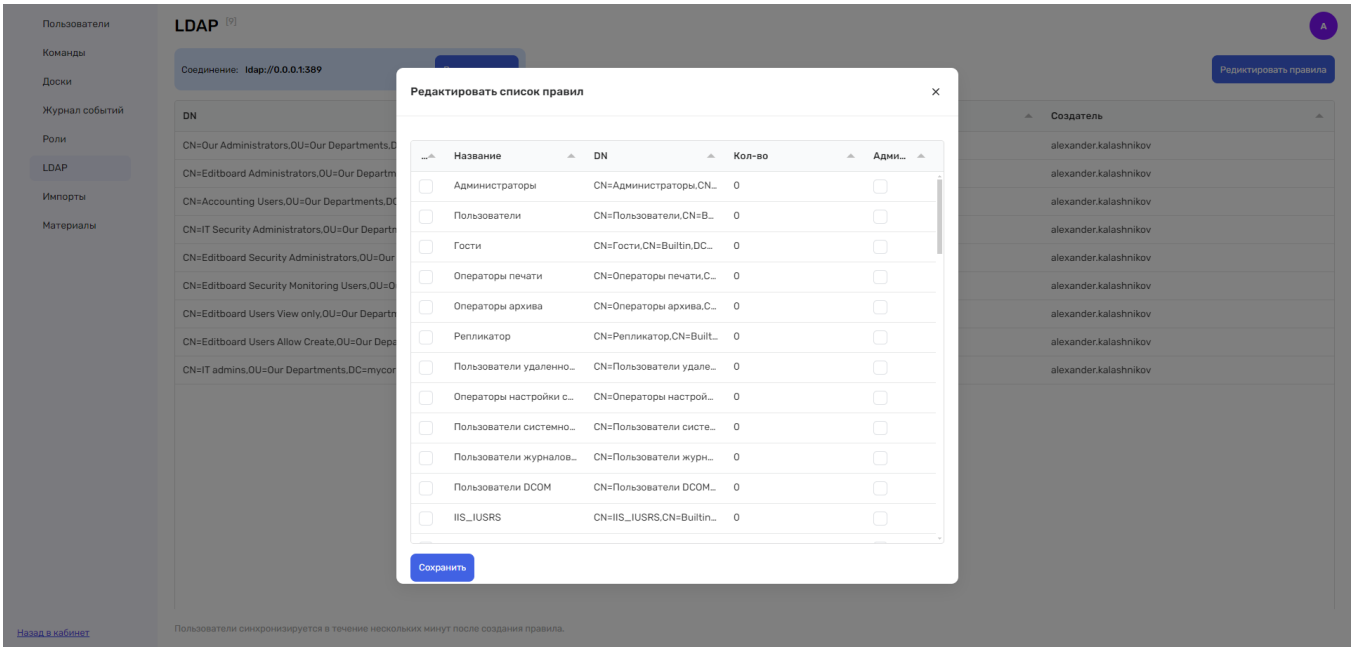
Возможность установки прав администратора для выбранной группы.



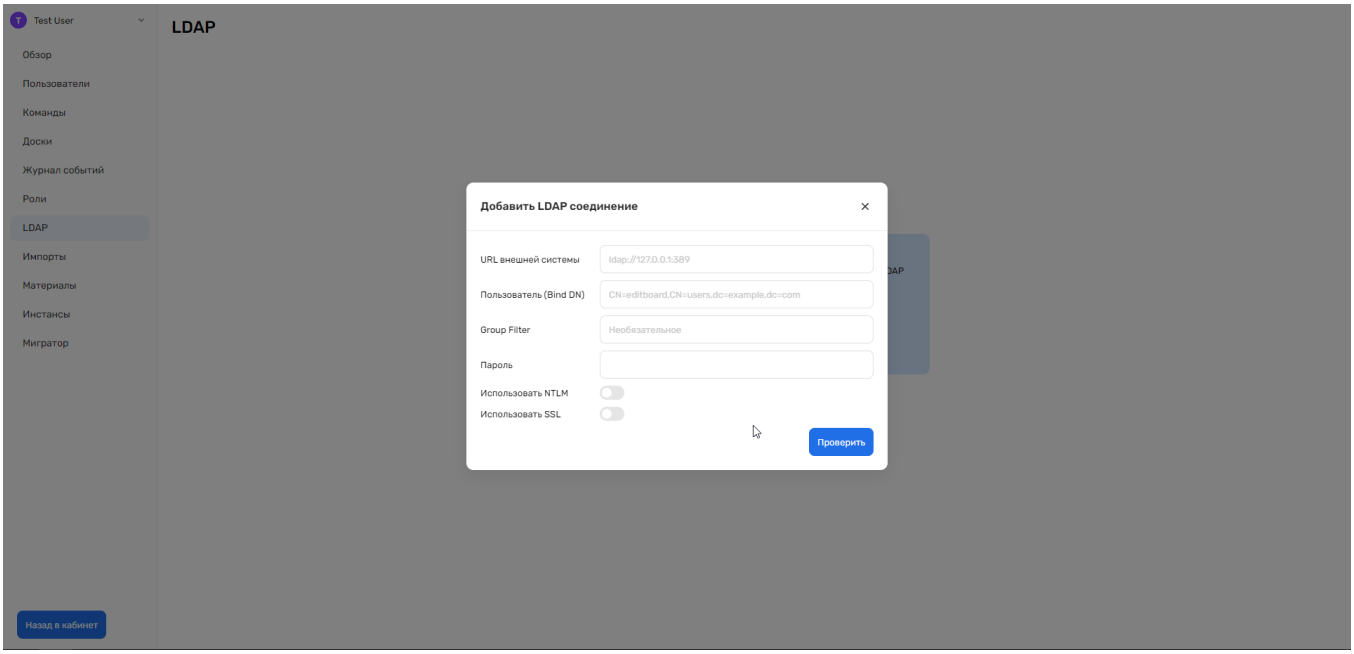
Интерфейс создания и редактирования соединения в версии 1.7.8 и ниже


Пользователи
Команды
Доски
Журнал событий
Роли
LDAP
Импорты
Материалы
LDAP [9]
Соединение: ldap://0.0.0.1:389
Редактировать
Редиктировать правила
DN
Тип
Дата создания
Создатель
CN=Our Administrators,OU=Our Departments,DC=mycorp,...
Пользователи
2024-06-06T01:29:47.601Z
alexander.kalashnikov
CN=Editboard Administrators,OU=Our Departments,DC=m...
Пользователи
2024-06-06T01:29:47.602Z
alexander.kalashnikov
CN=Accounting Users,OU=Our Departments,DC=mycorp,D...
Пользователи
2024-06-06T01:29:47.602Z
alexander.kalashnikov
CN=IT Security Administrators,OU=Our Departments,DC=...
Пользователи
2024-06-06T01:29:47.602Z
alexander.kalashnikov
CN=Editboard Security Administrators,OU=Our Departmen...
Администраторы
2024-06-06T01:29:47.602Z
alexander.kalashnikov
CN=Editboard Security Monitoring Users,OU=Our Departm...
Пользователи
2024-06-06T01:29:47.602Z
alexander.kalashnikov
CN=Editboard Users View only,OU=Our Departments,DC=m...
Пользователи
2024-06-06T01:29:47.602Z
alexander.kalashnikov
CN=Editboard Users Allow Create,OU=Our Departments,DC...
Пользователи
2024-06-06T01:29:47.602Z
alexander.kalashnikov
CN=IT admins,OU=Our Departments,DC=mycorp,DC=com
Администраторы
2024-06-06T01:29:47.602Z
alexander.kalashnikov
Назад в кабинет
Пользователи синхронизируется в течение нескольких минут после создания правила.


Пользователи
Команды
Доски
Журнал событий
Роли
LDAP
Импорты
Материалы
LDAP [9]
Соединение: ldap://0.0.0.1:389
Редактировать
Редиктировать правила
DN
Тип
Дата создания
Создатель
Добавить LDAP соединение
Ссылка
ldap://0.0.0.1:389
Базовый DN
CN=editboard_connect,CN
Пароль
password
Проверить
Назад в кабинет
Пользователи синхронизируется в течение нескольких минут после создания правила.



Интерфейс создания и редактирования соединения в версии 1.8.0 и выше



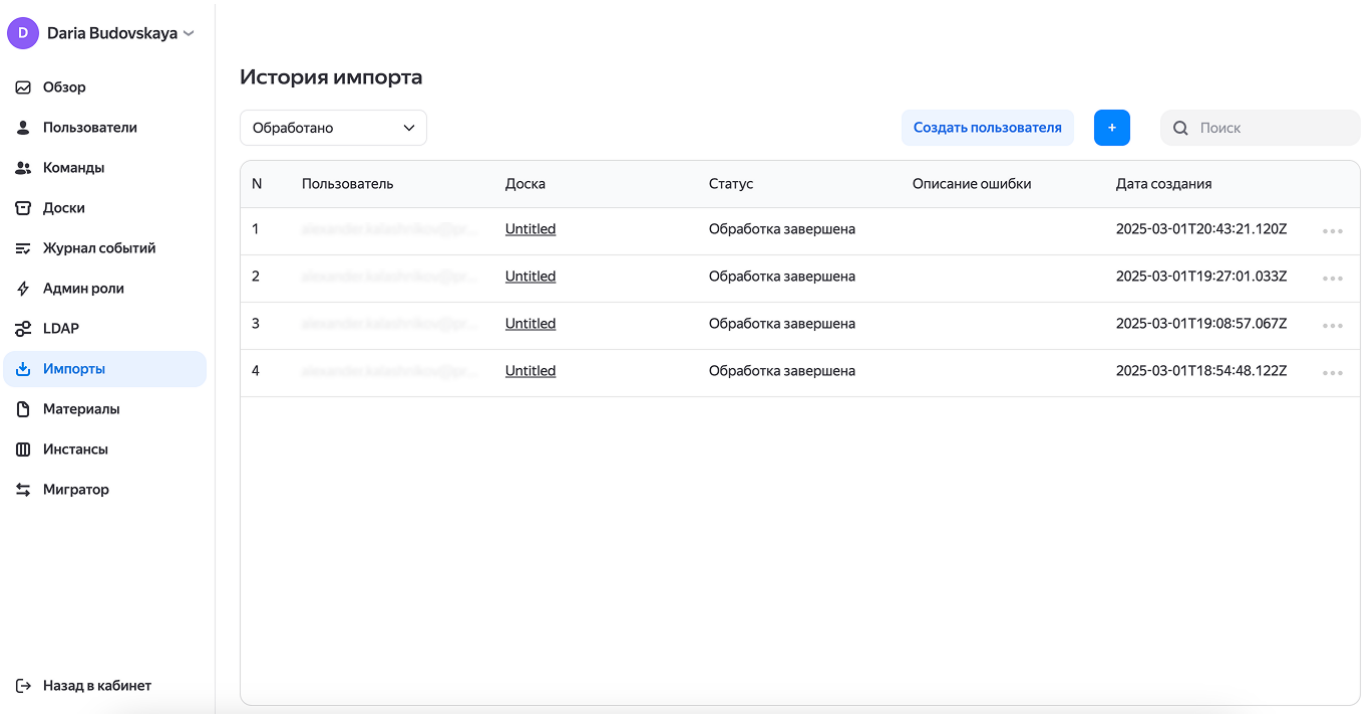
История импорта

В данном разделе представлена возможность просмотра истории запуска импорта досок из Miro в виде таблицы. Функционал включает следующие возможности:

Отображаемые данные

В таблице отображаются следующие данные:

- Логин пользователя, запустившего импорт.
- Имя доски.
- Конечный статус выполнения операции.
- Дата события.



Материалы

В данном разделе представлена возможность просмотра загруженных файлов в приложении. Функционал включает следующие возможности:

Поиск

Возможность поиска материалов по различным параметрам.

Фильтрация по типам

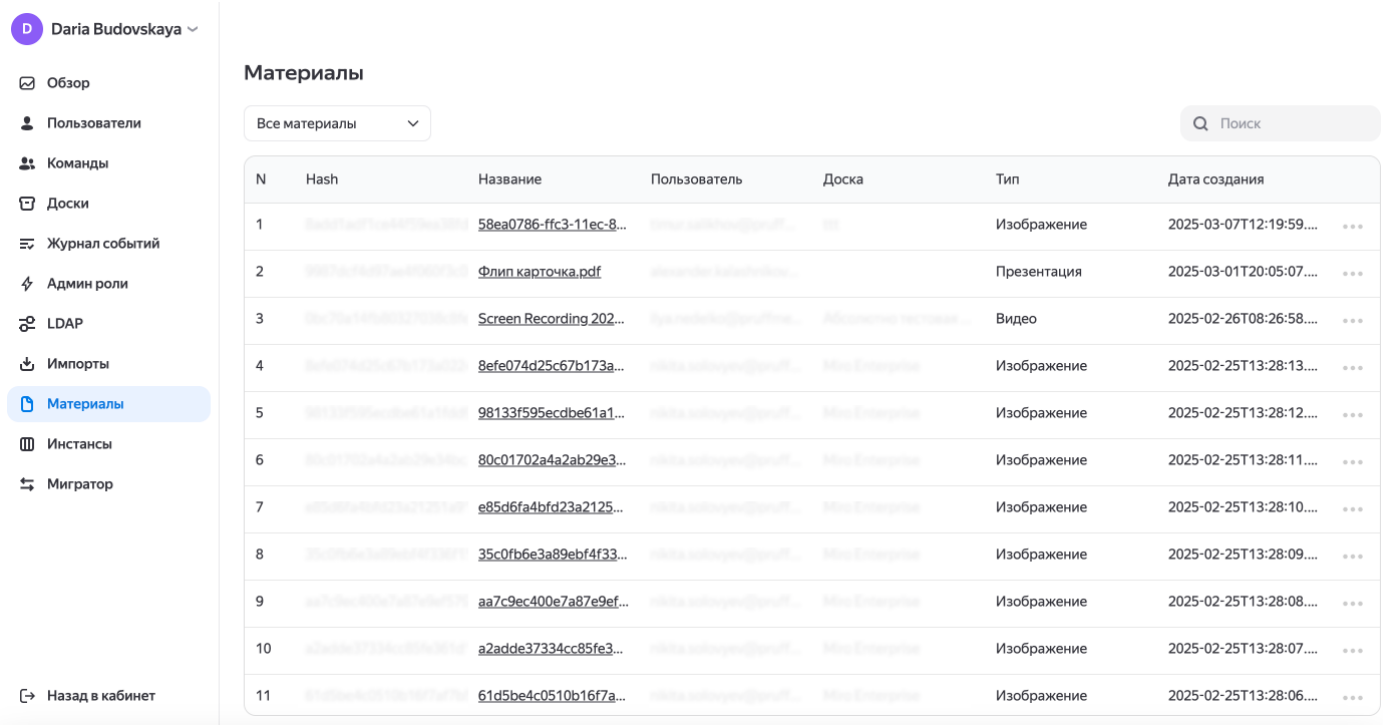
Возможность фильтрации материалов по следующим типам:

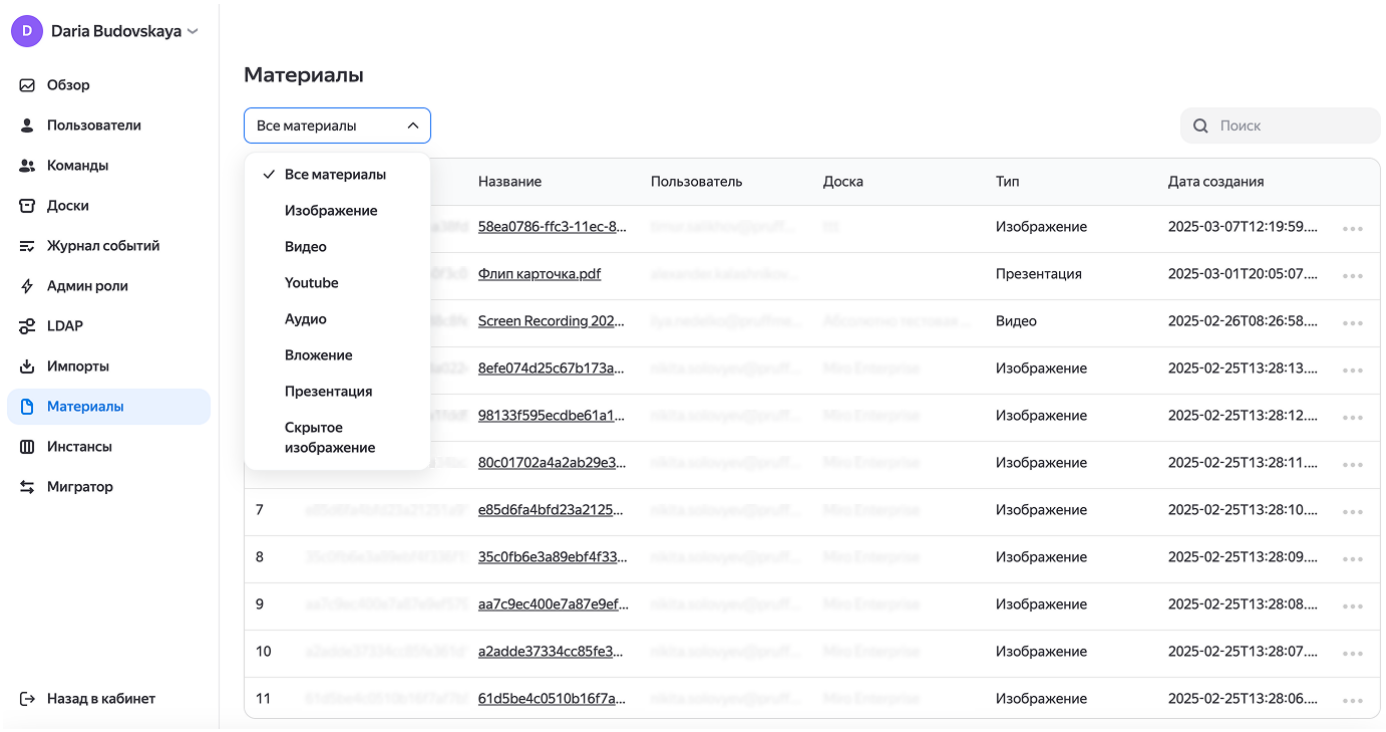
- Все материалы
- Изображение
- Видео
- YouTube
- Аудио
- Вложение
- Презентация
- Скрытое изображение

Действия с материалами

В дополнительном меню для каждого материала можно выполнить следующие действия:

- **Просмотреть все материалы, которые загрузил данный пользователь**: Переход к списку всех материалов, загруженных пользователем.
- **Просмотреть все материалы, использованные на данной доске**: Переход к списку всех материалов, использованных на указанной доске.




Daria Budovskaya
Обзор
Пользователи
Команды
Доски
Журнал событий
Админ роли
LDAP
Импорты
Материалы
Инстансы
Мигратор
Назад в кабинет
Материалы
Все материалы
Все материалы
Изображение
Видео
Youtube
Аудио
Вложение
Презентация
Скрытое изображение
Поиск
Название
Пользователь
Доска
Тип
Дата создания
58ea0786-ffc3-11ec-8...
Изображение
2025-03-07T12:19:59....
Флип карточка.pdf
Презентация
2025-03-01T20:05:07....
Screen Recording 202...
Видео
2025-02-26T08:26:58....
8efe074d25c67b173a...
Изображение
2025-02-25T13:28:13....
98133f595ecdbe61a1...
Изображение
2025-02-25T13:28:12....
80c01702a4a2ab29e3...
Изображение
2025-02-25T13:28:11....
7
e85d6fa4bfd23a2125...
Изображение
2025-02-25T13:28:10....
8
35c0fb6e3a89ebf4f33...
Изображение
2025-02-25T13:28:09....
9
aa7c9ec400e7a87e9ef...
Изображение
2025-02-25T13:28:08....
10
a2adde37334cc85fe3...
Изображение
2025-02-25T13:28:07....
11
61d5be4c0510b16f7a...
Изображение
2025-02-25T13:28:06....

Инстансы

В данном разделе представлена возможность визуализировать данные о нагрузке на сервера приложения по таким параметрам как:

- CPU
- RAM
- Количество пользователей

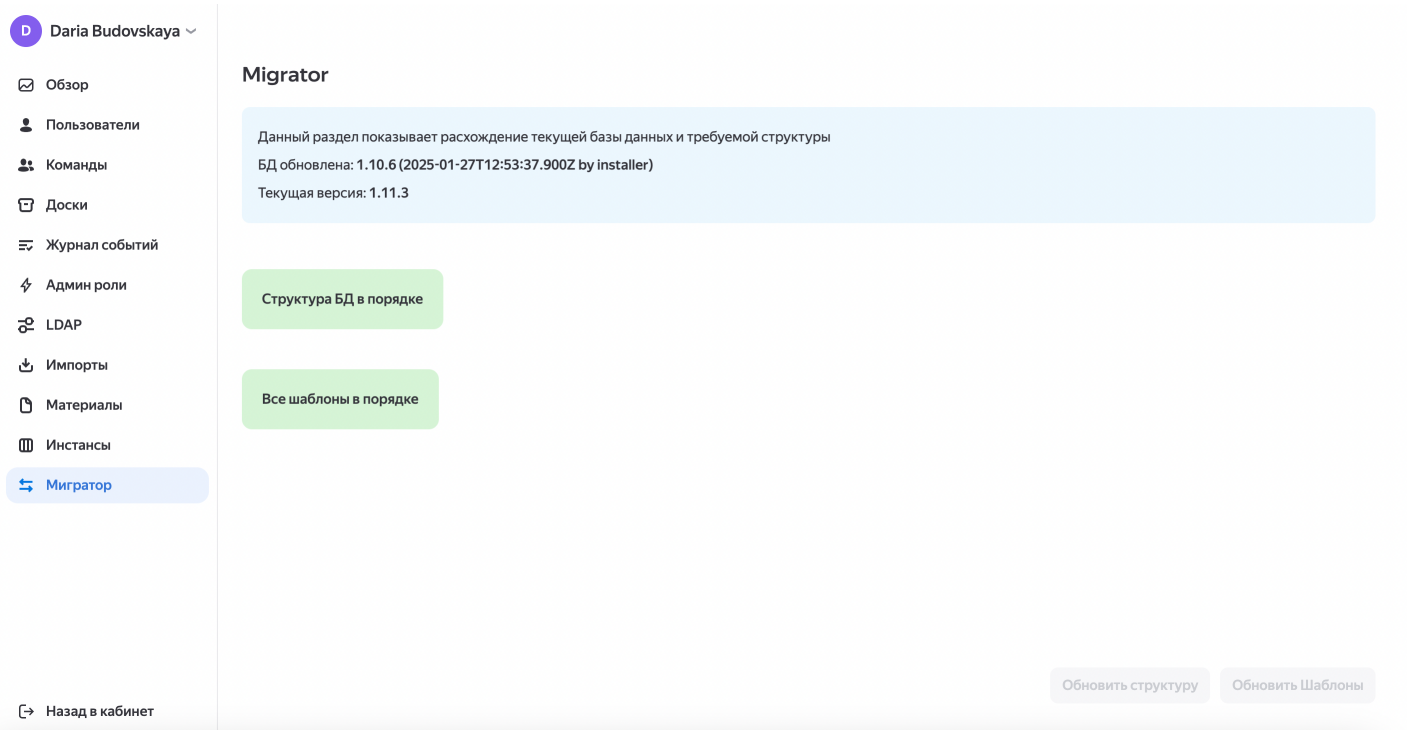
Доступ к данному разделу выставляется отдельно при помощи параметра `serveradmin`

Параметр	Описание	Тип данных
`serveradmin`	Если выставлено `all`, то доступ к разделу «Инстансы» и «Мигратор» предоставляется всем администраторам системы. Для того, чтобы ограничить доступ к данному разделу определенными администраторами, необходимо указать их логины в массиве (`["example.admin@editboard.com"]`)	Массив (Строка) / Строка

Мигратор

В данном разделе представлена возможность актуализации состояния базы данных после обновления приложения. Также есть возможность обновить шаблоны.
Доступ к данному разделу выставляется отдельно при помощи параметра `serveradmin`

Параметр	Описание	Тип данных
`serveradmin`	Если выставлено `all`, то доступ к разделу «Инстансы» и «Мигратор» предоставляется всем администраторам системы. Для того, чтобы ограничить доступ к данному разделу определенными администраторами, необходимо указать их логины в массиве (`["example.admin@editboard.com"]`)	Массив (Строка)



Общение описание API

Формат запросов

```
Host: https://${domain}/api
Authorization: Bearer ${Bearer-токен}
{
   Тело запроса в формате JSON
}
```

Методы

Запросы к API на текущий момент используют POST метод

Пример использования

Получение информации о досках, которые созданы конкретным пользователем

Для получения задачи используйте HTTP-запрос с методом `POST`

Формат запроса

Заголовки

Host

Адрес узла, предоставляющего API:

`https://testbox.editboard.team/api`

Authorization

Bearer-токен, например:

`Bearer eyJhbGciOiJIU6IkpXVCJ9**********`

Тело запроса

```
{
    "action": "get-boards",
    "limit": 50,
    "user": "editboard1@testbox.editboard.team"
}
```

Параметр	Описание	Тип данных

action	Идентификатор метода	Строка
limit	Максимальное количество элементов в массиве, которые будет возвращено за один запрос	Число
user	Логин пользователя	Строка

Формат ответа

Запрос выполнен успешно

В случае успешного выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON


```
{
    "result": {
        "presentations": [
            {
                "hash": "2ebafae8d476484a5753d39149b5363c",
                "name": "Test1",
                "access_type": 10,
                "creationdate": "2024-04-04T17:01:15.605Z",
                "updatedate": "2024-04-04T17:01:15.605Z",
                "user": "editboard1@testbox.editboard.team",
                "dashboards": [
                    "cecc45de5915350da585ffeec3fc4ce0"
                ]
            },
            {
                "hash": "1fff2b673bb9391538f03635dbdffc5c",
                "name": "Test5",
                "access_type": 10,
                "creationdate": "2024-04-04T17:01:14.002Z",
                "updatedate": "2024-04-04T17:01:14.002Z",
                "user": "editboard1@testbox.editboard.team",
                "dashboards": [
                    "7b6925fd297110c29ee9ee8155c192af"
                ]
            }
        ],
        "cursor": null
    }
}
```


Параметры ответа

Параметр	Описание	Тип данных

presentations	Массив досок, которые созданы указанным в запросе пользователем	Объект
hash	Хеш доски	Строка
name	Имя доски	Строка
access_type	Тип доступа к доске. 10 - доступ по списку участников команды	Число
creationdate	Дата создания доски	Строка
updatedate	Дата внесения последних изменений на доску	Строка
user	Логин пользователя	Строка
dashboards	Идентификатор доски. Используется в некоторых API запросах. Например в `get-items` или `update-items`	Строка
cursor	Последний элемент в массиве, который был возвращен в ответе на запрос. Используется для партиционирования больших запросов	Строка

Запрос выполнен с ошибкой

В данном случае выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON

```
{
    "error": {
        "code": 102,
        "description": "WRONG_KEY"
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. В данном случае проблема в токене	Число
description	Описание ошибки	Строка

```
{
    "error": {
        "code": 101,
        "description": "WRONG_ACTION"
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. В данном случае проблема в неверном идентификаторе запроса	Число
description	Описание ошибки	Строка

Получение токена для выполнения запросов

Для получения задачи используйте HTTP-запрос с методом `POST`

Формат запроса

Заголовки

Host

Адрес узла, предоставляющего API:

`https://testbox.editboard.team/api`

Authorization

Bearer-токен, например:

`Bearer eyJhbGciOiJIU6IkpXVCJ9*************`

Тело запроса

```
{
    "action": "get-access-token",
    "content": {
    "livetime": 3600
    },
    "partner": "editboard",
    "key": "c822c1b63853ed273b89687ac505f9fa"
}
```

Параметр	Описание	Тип данных
action	Идентификатор метода	Строка
content	Объект в котором содержаться необходимые для получения данные	Объект

livetime	Время жизни токена	Число
partner	Идентификатор области видимости документов	Строка
key	Ключ API для доступа к ресурсам определенного partner	Строка

Запрос выполнен успешно

В случае успешного выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON

```
{
    "token": "eyJhbGciOiJIUzI1NiI****************"
}
```

Параметры ответа

Параметр	Описание	Тип данных
token	Токен для использования в запросах к API	Строка

Запрос выполнен с ошибкой

В данном случае выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON

```
{
    "error": {
        "code": 102,
        "description": "WRONG_KEY"
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. Проверьте корректность указанных в запросе данных	Число
description	Описание ошибки	Строка

Перечень методов API

Совет

Важно следить за валидностью используемого токена при запросах. `102` - код ошибки при выполнении запроса. который указывает на проблемы с используемым для запроса токеном

Получение информации о досках, которые созданы конкретным пользователем

Для получения задачи используйте HTTP-запрос с методом `POST`

Формат запроса

Заголовки

Host

Адрес узла, предоставляющего API:

`https://testbox.editboard.team/api`

Authorization

Bearer-токен, например:

`Bearer eyJhbGciOiJIU6IkpXVCJ9*************`

Тело запроса

```
{
    "action": "get-boards",
    "limit": 50,
    "user": "editboard1@testbox.editboard.team"
}
```

Параметр	Описание	Тип данных
action	Идентификатор метода	Строка
limit	Максимальное количество элементов в массиве, которые будет возвращено за один запрос	Число
user	Логин пользователя	Строка

Формат ответа

Запрос выполнен успешно

В случае успешного выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON


```
{
    "result": {
        "presentations": [
            {
                "hash": "2ebafae8d476484a5753d39149b5363c",
                "name": "Test1",
                "access_type": 10,
                "creationdate": "2024-04-04T17:01:15.605Z",
                "updatedate": "2024-04-04T17:01:15.605Z",
                "user": "editboard1@testbox.editboard.team",
                "dashboards": [
                    "cecc45de5915350da585ffeec3fc4ce0"
                ]
            },
            {
                "hash": "1fff2b673bb9391538f03635dbdffc5c",
                "name": "Test5",
                "access_type": 10,
                "creationdate": "2024-04-04T17:01:14.002Z",
                "updatedate": "2024-04-04T17:01:14.002Z",
                "user": "editboard1@testbox.editboard.team",
                "dashboards": [
                    "7b6925fd297110c29ee9ee8155c192af"
                ]
            }
        ],
        "cursor": null
    }
}
```


Параметры ответа

Параметр	Описание	Тип данных
presentations	Массив досок, которые созданы указанным в запросе пользователем	Объект
hash	Хеш доски	Строка
name	Имя доски	Строка

access_type	Тип доступа к доске. 10 - доступ по списку участников команды	Число
creationdate	Дата создания доски	Строка
updatedate	Дата внесения последних изменений на доску	Строка
user	Логин пользователя	Строка
dashboards	Идентификатор доски. Используется в некоторых API запросах. Например в `get-items` или `update-items`	Строка
cursor	Последний элемент в массиве, который был возвращен в ответе на запрос. Используется для партиционирования больших запросов	Строка

Запрос выполнен с ошибкой

В данном случае выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON

```
{
    "error": {
        "code": 102,
        "description": "WRONG_KEY"
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. В данном случае проблема в токене	Число
description	Описание ошибки	Строка

```
{
    "error": {
        "code": 101,
        "description": "WRONG_ACTION"
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. В данном случае проблема в неверном идентификаторе запроса	Число

description	Описание ошибки	Строка

Получение информации о контенте на доске

Для получения задачи используйте HTTP-запрос с методом `POST`

Формат запроса

Host

Адрес узла, предоставляющего API:

`https://testbox.editboard.team/api`

Authorization

Bearer-токен, например:

`Bearer eyJhbGciOiJIU6IkpXVCJ9**********`

Тело запроса

```
{
    "action" : "get-items",
    "presentation" : "d590ac8fb13e4746dd1cf47db9b5aba4",
    "dashboard" : "99427592908ab618ea1be2ebeaacd9e1",
}
```

Параметр	Описание	Тип данных
action	Идентификатор метода	Строка
presentation	Хеш доски	Строка
dashboard	Идентификатор доски	Строка

Формат ответа

Запрос выполнен успешно

В случае успешного выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON

```
{
    "result": {
        "items": [
            {
                "hash": "ade871cdd2901a25802accbdb7de9d15",
```

```
                "type": "shape",
                "value": "<p>test</p>",
                "parent": "DASHBOARD",
                "geometry": {
                    "x": "992",
                    "y": "370",
                    "width": "609",
                    "height": "512",
                    "as": "geometry"
                },
                "creationdate": "2024-04-04T16:06:22.552Z"
            }
        ],
        "cursor": null
    }
}
```


Параметры ответа

Параметр	Описание	Тип данных
items	Массив с перечнем фигур размещенных на доске	Объект
type	Тип фигуры	Строка
value	Текстовое содержимое фигуры	Строка
parent	Родительский объект в котором размещена фигура. DASHBOARD - это основной родительский элемент	Строка
geometry	Объект с геометрическими свойствами фигуры	Объект
creationdate	Время создания фигуры	Строка
user	Логин пользователя	Строка
cursor	Последний элемент в массиве, который был возвращен в ответе на запрос. Используется для партиционирования больших запросов	Строка

Запрос выполнен с ошибкой

В данном случае выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON


```
{
    "error": {
        "code": 251,
```

```
        "description": "No dashboard"
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. В данном случае не существует доски с указанными параметрами (идентификатор)	Число
description	Описание ошибки	Строка

```
{
    "error": {
        "code": 250,
        "description": "No presentation"
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. В данном случае не существует доски с указанными параметрами (хеш презентации)	Число
description	Описание ошибки	Строка

Обновление содержимого фигуры на доске

Для получения задачи используйте HTTP-запрос с методом `POST`

Формат запроса

Заголовки

Host

Адрес узла, предоставляющего API:

`https://testbox.editboard.team/api`

Authorization

Bearer-токен, например:

`Bearer eyJhbGciOiJIU6IkpXVCJ9**********`

Тело запроса

```
{
    "action" : "update-item",
    "presentation" : "2ebafae8d476484a5753d39149b5363c",
    "dashboard" : "cecc45de5915350da585ffeec3fc4ce0",
    "item" : {
        "hash" : "dd5cd5029671f39ccb39b29cb09d2aaa",
        "value" : "test"
    }
}
```

Параметр	Описание	Тип данных
action	Идентификатор метода	Строка
presentation	Хеш доски	Число
item	Фигура, в которой необходимо изменить содержимое	Объект
hash	Хеш фигуры	Строка
value	Передаваемое значение	Строка

Формат ответа

Запрос выполнен успешно

В случае успешного выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON

```
{
    "result": true
}
```

Параметры ответа

Параметр	Описание	Тип данных
result	Результат выполнения запроса	Логический

Запрос выполнен с ошибкой

В данном случае выполнения запроса API возвращает ответ с кодом 200 OK

Тело ответа содержит результаты в формате JSON

```
{
    "code": 252,
    "description": "No item"
}
```

Параметр	Описание	Тип данных
code	Код ошибки. Объекта с данным хешом не существует	Число
description	Описание ошибки	Строка

```
{
    "error": {
        "code": 99,
        "description": "Invalid json"
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. Ошибка в формате запроса	Число
description	Описание ошибки	Строка

```
{
    "error": {
        "code": 251,
        "description": "No dashboard"
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. В данном случае не существует доски с указанными параметрами (идентификатор)	Число
description	Описание ошибки	Строка

```
{
    "error": {
        "code": 250,
        "description": "No presentation"
```

```
    }
}
```

Параметр	Описание	Тип данных
code	Код ошибки. В данном случае не существует доски с указанными параметрами (хеш презентации)	Число
description	Описание ошибки	Строка

Примеры использования методов API

В данном разделе представлены примеры модулей использующих API приложения. Инструкция по их использованию также содержится в архиве

NodeJS

- Архив с исходным кодом

Java

- Архив с исходным кодом

Функциональные возможности и особенности приложения

- Приложение поддерживает AstraLinux, Ubuntu и другие операционные системы, обеспечивающие работу контейнеризации.
- Приложение можно развернуть с использованием Kubernetes с применением helm chart по запросу.
- Поддерживается интеграцию с другими on-premises решениями.
- Поддерживается шифрование данных между всеми узлами приложения.
- Приложение работает с базой данных PostgreSQL.
- Поддерживается работа в нескольких инстансах.
- Приложение разработано с учетом принципов отказоустойчивости.
- Приложение может полноценно функционировать в изолированной инфраструктуре.
- Поддерживается работа с syslog.
- Приложение поддерживает SAML, OpenID и LDAPS для реализации единого входа (SSO).
- Поддерживаются механизмы многофакторной аутентификации для повышения безопасности.
- Возможна загрузка пользователей из Active Directory.
- Все учетные записи в приложении персонифицированы.

Сетевые параметры

Порт	Назначение	Протокол	Трафик	Шифрование	Алгоритм шифрования	Тип	Комментарий
`443`	Внешний доступ к приложению через nginx (HTTPS) со стороны клиента	TLS (HTTPS)	Внешний	Да (TLS 1.2 или 1.3)	ECDHE-RSA-AES256-GCM-SHA384	H	Порт может быть изменен в конфигурации nginx
`8080`	Внутренние экземпляры backend-приложения (по числу CPU)	HTTPS	Внутренний	Да (TLS 1.3)	TLS_AES_256_GCM_SHA384	H	Прокси через nginx, порт зависит от числа процессов и настройки приложения. Например 8080–8087
`9000`	Обращения к внешнему хранилищу (S3 API, AWS v2 или v3)	HTTPS (S3 API)	Внешний	Да	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 и др.	H	Используется как endpoint для доступа к объектному хранилищу

`541`	Отправка логов на syslog-сервер	UDP или TCP	Внешний или внутренний	Зависит от конфигурации	Зависит от конфигурации	H	Может быть как TCP, так и UDP. TLS обычно не включен
`6379`	Redis (in-memory key-value хранилище)	Redis протокол	Внутренний	Нет	Не применяется	H	Требует включения TLS для соответствия ИБ
`5432`	PostgreSQL (БД приложения)	PostgreSQL	Внутренний	Нет	Не применяется	H	Приложение не поддерживает работу с TLS
`389`	LDAP	LDAP (TCP)	Внешний или внутренний	Нет	Не применяется	H	Без шифрования, для поиска пользователей
`636`	LDAPS	LDAP over TLS	Внешний или внутренний	Да	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 и др.	H	TLS-версия LDAP, используется для безопасной аутентификации

История изменений

1.11.5 (20.03.2025)

Прочее

- Расширен перечень логируемых действий для приложения.
- Повышена стабильность в работе приложения.
- Небольшие улучшения интерфейса приложения.

1.11.4 (20.03.2025)

Импорт

Добавлен импорт из Miro конкретной доски по ссылке.

Прочее

- Интерфейс приложение приведен в соответствие с дизайн-системой.
- Улучшена обработка вставки внешних ссылок.

1.11.2 (20.03.2025)

Прочее

- Улучшен интерфейс приложения.
- Исправлены некоторые ошибки отображения в панели администратора.

1.11.1 (02.02.2025)

Доступ к приложению

Изменилась политика выдачи лицензий. Теперь администратор может вручную назначать пользователей, которые будут иметь полнофункциональный доступ к приложению в разделе **Пользователи**. Также предусмотрено точечное отключение лицензии для пользователей.

Улучшения и исправление ошибок

- Улучшено взаимодействие при помощи клавиатуры с модальными окнами интерфейса.
- Визуальная переработка системы уведомлений в панели администратора.
- Исправлена ситуация, когда у некоторых пользователей дважды открывался интерфейс создания LDAP.
- Исправлена ошибка с некорректным редиректом по клику на аватарку в комментариях.
- Исправлена ошибка отображения названий проектов и команд в которых применялись спецсимволы.
- Исправлена проблема, которая не позволяла отключать маркированный список для текстовых элементов.

Прочее

Небольшие улучшения интерфейса приложения.

1.10.6 (19.01.2025)

Доступ к приложению

Добавлена возможность использовать в качестве логина записи с одним DC, а не только с двумя.

Функционал приложения

Добавлена функция наследования стиля шрифта для инструмента **Текст** (цвет, семейство, размер, цвет фона шрифта).

Прочее

- Повышение стабильности в работе приложения.
- Небольшие улучшения интерфейса приложения.

1.10.4 (17.12.2024)

Функционал приложения

- Возможность перемещать объект, по которому производится голосование.
- Повышение удобства использования инструмента **Комментарий**.
- Обновлен интерфейс создания шаблонов, а также библиотека шаблонов.
- Повышение стабильности работы инструментов **Интеллектуальная карта**, **Стрелка** и **Таблица**.
- Улучшено взаимодействие с объектами в режиме мультивыбора (перемещения).

Доступ к приложению

Возможность настраивать гостевой доступ на уровне приложения.

Панель администратора

- Добавлено отображение даты окончания действия лицензии.
- Улучшена система сбора пользовательской статистики в панели администратора.
- Добавление логирования загрузки файлов.
- Добавлена механика смены логина пользователя в панели администратора.

Работа с базами данных

Добавлена поддержка длинных логинов пользователей.

Прочее

Общие исправление и улучшения пользовательского интерфейса.

Адреса и порты, используемые Яндекс 360

Если в вашей компании настроена защищенная корпоративная сеть, разрешите входящий и исходящий трафик для подсетей Яндекса.

Шаг 1. Откройте порты

Откройте внешние порты для входящего и исходящего трафика:

TCP:

- `80`
- `443`
- `3478`

UDP:

- `80`
- `443`
- `3478`
- `10000`
- `20000-23000`

Шаг 2. Разрешите доступ к диапазонам IP-адресов

Откройте доступ ко всем подсетям, которые используются Яндексом:

- `5.45.192.0/18`
- `5.255.192.0/18`
- `37.9.64.0/18`
- `37.9.82.144/28`
- `37.9.102.64/28`
- `37.140.128.0/18`
- `77.88.0.0/18`
- `77.88.7.48/28`
- `84.252.160.0/19`
- `87.250.224.0/19`
- `90.156.176.0/22`
- `93.158.128.0/18`
- `95.108.128.0/17`
- `141.8.128.0/18`
- `178.154.128.0/18`
- `185.32.187.0/24`
- `185.206.164.0/22`

- `213.180.192.0/19`
- `2a02:6b8:0:2001::/64`
- `2a02:6b8:0:1a0b::/64`
- `2a02:6b8:11d:c::/64`

Шаг 3. Разрешите доступ к адресам подключений

Откройте доступ ко всем адресам, даже если планируете пользоваться только одним из сервисов.

- `api.messenger.yandex.net`
- `avatars.mds.yandex.net`
- `backend.messenger.yandex.ru`
- `calendar.yandex.ru`
- `calendar.360.yandex.ru`
- `cloud-api.yandex.net`
- `disk.yandex.ru`
- `disk.360.yandex.ru`
- `docs.yandex.ru`
- `docs.360.yandex`
- `docviewer.360.yandex.ru`
- `download.messenger.yandex.ru`
- `files.messenger.yandex.net`
- `files.messenger.yandex.ru`
- `goloom.strm.yandex.net`
- `images.messenger.yandex.net`
- `mail.yandex.ru`
- `mail.360.yandex.ru`
- `messenger.yandex.ru`
- `messenger.360.yandex.ru`
- `mc.yandex.ru`
- `passport.yandex.ru`
- `push.yandex.ru`
- `stun.rtc.yandex.net`
- `telemost.yandex.ru`
- `telemost.360.yandex.ru`
- `tools.messenger.yandex.net`
- `translate.yandex.net`
- `turn.webrtc.yandex.net`
- `uniproxy.messenger.yandex.ru`
- `yandex.ru`

- `yastatic.net`

Написать в службу поддержки

Переезд в Яндекс 360 для бизнеса

Мы собрали ответы на частые вопросы о том, как перенести данные вашей организации в Яндекс 360 для бизнеса из Google Workspace, Microsoft 365 и других платформ. Смотреть >

Управление организацией

Профиль организации настраивают ее администраторы и владелец, который по умолчанию является главным администратором.

В настройках профиля вы можете:

- создавать, удалять организации и переключаться между ними;
- редактировать данные организации, в том числе логотип и название;
- менять владельца.

Чтобы настроить профиль организации:

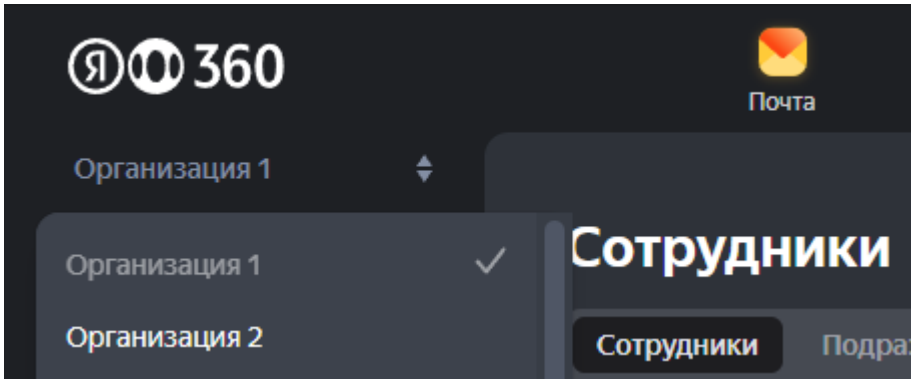
1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Профиль организации**.
3. Если вы являетесь администратором сразу нескольких организаций, переключитесь на нужную организацию на панели слева.

Написать в службу поддержки

Переключиться между организациями

Если вы администратор нескольких организаций в Яндекс 360 для бизнеса, вы можете переключаться между ними.

- Чтобы сменить организацию, нажмите на название текущей организации на панели слева и выберите организацию, на которую нужно переключиться.

  Если в вашем браузере открыто несколько страниц с настройками организации, обновите эти страницы. После этого на них отобразятся данные организации, на которую вы переключились.
- Чтобы создать новую организацию, нажмите на название текущей организации и внизу выберите **Создать организацию**.

Написать в службу поддержки

Редактировать данные

Чтобы изменить название вашей организации, загрузить логотип и настроить тариф для владельца:

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Профиль организации**.
3. Измените название:
   3.1. Нажмите значок рядом с названием организации.
   3.2. Введите новое название и нажмите кнопку **Сохранить**.

> **Примечание**
>
> Вы также можете изменить название организации на странице **Оплата и тариф**.

4. Добавьте логотип вашей организации на верхнюю панель:
   4.1. В разделе **Логотип в шапке** нажмите **Загрузить jpg или png файлы**.
   4.2. Выберите на вашем компьютере файл с логотипом организации.

> **Примечание**
>
> Размер изображения должен быть не меньше 100 × 100 и не больше 1024 × 1024. Размер файла не должен превышать 7 МБ.

5. Подключите или отключите тариф организации у владельца — в зависимости от того, нужны ли ему платные сервисы.

> **Примечание**
>
> Опция доступна только для владельца — пользователя с аккаунтом вида `login@yandex.ru`.

Написать в службу поддержки

Изменить владельца

По умолчанию владелец организации в Яндекс 360 для бизнеса — это ее создатель. Он также считается владельцем всех подключенных к организации доменов.

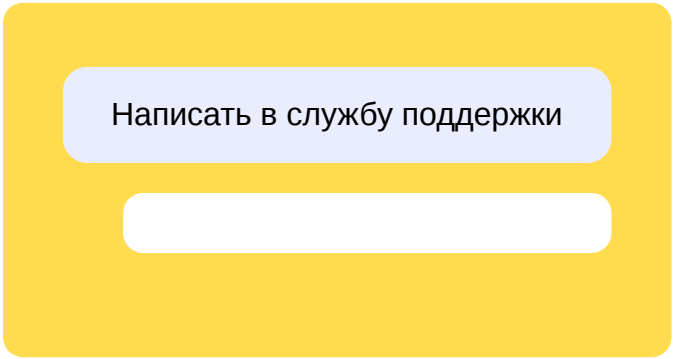
Владелец может передать свое право владения другому человеку — как сотруднику организации, так и внешнему пользователю с аккаунтом на Яндексе вида `login@yandex.ru`. Для этого:

1. Войдите в аккаунт администратора организации.
2. Перейдите на страницу **Профиль организации**.
3. В поле **Аккаунт владельца** нажмите кнопку **Сменить**.
4. Введите электронную почту нового владельца и нажмите **Далее**.
5. Нажмите **Сменить владельца**, чтобы подтвердить передачу владения.

Прежний владелец сохранит права администратора, но больше не будет считаться владельцем организации и подключенных к ней доменов, а значит, не сможет самостоятельно восстановить свое право владения.

Восстановить доступ к организации при потере аккаунта

Если вы потеряли доступ к аккаунту владельца организации, вы можете попробовать самостоятельно его восстановить. Посмотреть возможные способы можно в разделе Проблемы с доступом.



Удалить организацию

Если вы больше не хотите работать с сервисами Яндекс 360 для бизнеса, то можете просто перестать пользоваться своей организацией или удалить ее.

Организацию можно удалить самостоятельно, только если выполнены все перечисленные условия:

- Баланс организации (договора) равен нулю.
- Организация не является реферальным партнером Яндекс 360. Для удаления такой организации обратитесь к партнерскому менеджеру.
- Организация подключилась к Яндекс 360 для бизнеса не через партнера. Для удаления такой организации обратитесь к партнеру, через которого вы подключались.

Как удалить организацию

Тариф оплачен

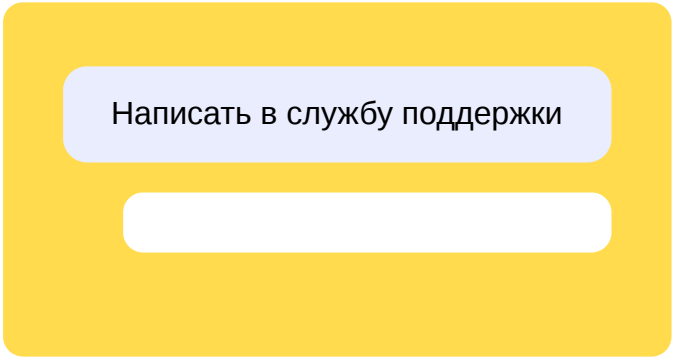
1. Выберите нужную организацию в списке ваших организаций.
2. На вкладке **Оплата и тариф** проверьте, что баланс организации (договора) равен нулю.
3. В разделе **Общие настройки** → **Профиль организации** нажмите кнопку **Удалить организацию**.
4. Подтвердите удаление и нажмите кнопку **Удалить**.
5. Дождитесь удаления организации.

Тариф не оплачен

Если вы уже создали организацию, но еще не оплатили тариф:

1. Выберите нужную организацию в списке ваших организаций.
2. На вкладке **Оплатите** внизу страницы нажмите кнопку **Удалить организацию**.
3. Подтвердите удаление и нажмите кнопку **Удалить**.
4. Дождитесь удаления организации.

Если у вас будут вопросы, напишите нам.



Проблемы с доступом

Если вы потеряли доступ к аккаунту владельца организации, вы можете попробовать самостоятельно его восстановить.

Не помню логин владельца организации

- Если вы привязали номер телефона к аккаунту или недавно заходили в свой аккаунт с этого же компьютера и браузера, откройте страницу Восстановление логина и следуйте инструкциям.
- Если вы переписывались с этого адреса с друзьями, родными или коллегами, попробуйте связаться с ними, например, через социальные сети. Возможно, они вспомнят ваш адрес или найдут письма от вас в своих почтовых ящиках и смогут сообщить вам, с какого адреса они были отправлены.

Не помню пароль владельца организации

Если вы корректно указали имя и фамилию при регистрации и привязали номер телефона к аккаунту, откройте страницу восстановления пароля и следуйте инструкциям.

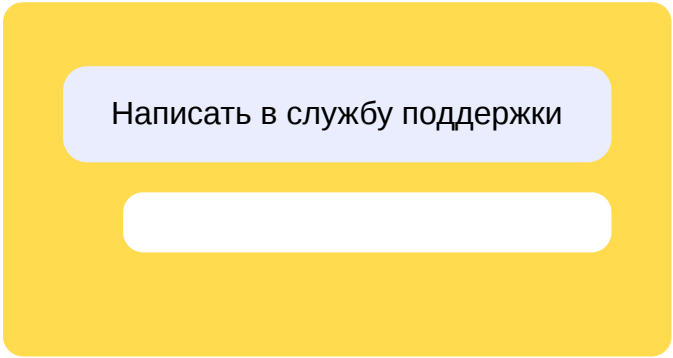
Если вы видите сообщение о том, что адрес почты или номер телефона неправильный, проверьте, не опечатались ли вы при вводе. Если корректно введенный номер все-таки не подходит, постарайтесь вспомнить, какие еще адреса или номера вы могли привязать к аккаунту.

Не удается восстановить аккаунт владельца организации

Если вы не можете вспомнить логин или пароль от аккаунта, с помощью которого создавали организацию в Яндекс 360 для бизнеса, восстановите доступ с помощью другого аккаунта:

1. Зарегистрируйте новый аккаунт на Яндексе.
2. Подтвердите, что вы действительно являетесь владельцем организации. Для этого заполните форму восстановления доступа.
3. Подтвердите владение доменом одним из предложенных в форме способов.

Если вы все сделали правильно, права на организацию перейдут на новый аккаунт. При этом все данные организации сохранятся.



Связь с людьми не из организации

Если вашим сотрудникам часто нужно общаться с людьми из других организаций, вы можете добавить их в список контактов или выдать им доступ к корпоративным каналам связи.

Внешние контакты

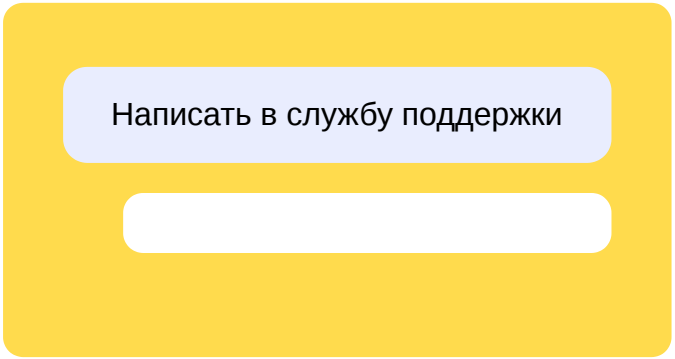
Чтобы ваши сотрудники могли находить людей из других организаций в Почте, Календаре и Диске, вы можете добавить их в качестве внешних контактов. Такие контакты не получат доступ к данным компании — они просто появятся в списке контактов. Как добавить

Гости

Гости - это внешние контакты, с которыми можно общаться в рабочих переписках Мессенджера. Вы сами решаете, в какие рабочие чаты добавить гостя, а в какие — нет. Самостоятельно написать сотрудникам, создать чат или выйти из него он не сможет. Чтобы добавить гостя в организацию, отправьте ему приглашение. Как пригласить

Федерации

Чтобы сотрудники из разных компаний могли беспрепятсвенно общаться по рабочим вопросам, объедините организации в федерацию. Сотрудники компаний получат доступ к общим контактам в Почте, Календаре и Мессенджере. Как создать федерацию



Внешние контакты

Внешние контакты — это пользователи не из вашей организации. Ими могут быть сотрудники компаний-партнеров, подрядчики, клиенты или заказчики. Добавьте внешние контакты в Яндекс 360 для бизнеса, чтобы ваши сотрудники могли быстрее находить нужных людей в Почте, Календаре и Диске — например, когда пишут письма, добавляют участников встреч или настраивают общий доступ к папкам.

Вы можете добавить до 200 000 внешних контактов для одной организации.

Добавить

Загрузить списком

Добавить в вашу организацию сразу несколько внешних контактов можно с помощью CSV-файла.

1. Скачайте шаблон CSV-файла, который вы сможете использовать как образец.
   1.1. Откройте кабинет организации **admin.yandex.ru**.
   1.2. В меню слева выберите **Пользователи** → **Внешние контакты**.
   1.3. Если вы впервые добавляете внешние контакты, нажмите кнопку **Загрузить список** в центре экрана.

   Если у вашей организации уже есть внешние контакты, над таблицей с ними нажмите кнопку **Добавить** и выберите **Загрузить списком**.
   1.4. Нажмите **Шаблон** и сохраните файл к себе на устройство.
2. На основе шаблона сформируйте новый файл для загрузки списка контактов.
   2.1. Заполните скачанный файл своими данными:
   - Первую строку оставьте неизменной — это заголовки полей.
   - По образцам в строках 2–6 добавьте в файл данные внешних контактов. Строки с образцами удалите.

   Описание полей:

N	Поле	Что содержит	Комментарий
1	last_name	Фамилия	
2	first_name	Имя	
3	middle_name	Отчество	

4	title	Должность	
5	company	Компания	
6	address	Почтовый адрес	
7	department	Подразделение	
8	phone_number	Номер телефона	
9	is_main_phone_number	Признак основного телефона	Возможные значения: - `true` — основной; - `false` — дополнительный. Основной номер может быть только один.

10	phone_number_type	Тип телефонного номера	Возможные значения: ▪ `work` — рабочий телефон; ▪ `mobile` — мобильный телефон; ▪ `ip` — IP-телефон; ▪ для прочих телефонных номеров оставьте поле незаполненным.
11	email	Адрес электронной почты	Должен быть уникальным во всем списке внешних контактов.
12	is_main_email	Признак основного электронного адреса	Возможные значения: ▪ `true` — основной; ▪ `false` — дополнительный. Основной электронный адрес может быть только один.

При

13	email_type	Тип электронного адреса	Возможные значения: ▪ `work` — рабочая почта; ▪ для личной почты оставьте поле незаполненным.

Добавить дополнительные электронные адреса или номера телефонов к контакту, который уже есть в списке внешних контактов вашей организации, можно только при его редактировании в интерфейсе Яндекс 360 для бизнеса. Как редактировать внешний контакт в интерфейсе

2.2. Сохраните CSV-файл в кодировке UTF-8.

Внимание

Если сохранить файл в другой кодировке, он будет распознан неправильно.

2.3. Убедитесь, что в файле не больше 1000 строк, а его размер — до 10 МБ. Если файл большой, разбейте его на несколько файлов поменьше.

3. Загрузите подготовленный список.

3.1. Откройте кабинет организации **admin.yandex.ru**.

3.2. В меню слева выберите **Пользователи** → **Внешние контакты**.

3.3. Если вы впервые добавляете внешние контакты, нажмите кнопку **Загрузить список** в центре экрана.

Если у вашей организации уже есть внешние контакты, над таблицей с ними нажмите кнопку **Добавить** и выберите **Загрузить списком**.

3.4. Нажмите кнопку **Выбрать CSV-файл** и укажите ваш файл.

3.5. Нажмите **Загрузить список** и дождитесь окончания загрузки. Добавленные пользователи отобразятся в списке **Внешние контакты**.

Если во время загрузки возникли ошибки, данные из файла не загрузятся. Исправьте их и попробуйте загрузить список снова.

Создать контакт вручную

1. Откройте кабинет организации **admin.yandex.ru**.

2. В меню слева выберите **Пользователи** → **Внешние контакты**.
3. Если вы впервые добавляете внешние контакты, нажмите кнопку **Добавить вручную** в центре экрана.

   Если у вашей организации уже есть внешние контакты, над их списком нажмите кнопку **Добавить** и выберите **Создать вручную**.
4. Заполните поля карточки внешнего контакта:
   - Поля с фамилией, именем и электронной почтой обязательны для заполнения.
   - Для электронной почты, рабочего, мобильного и IP-телефона помимо основных вы можете добавить до 15 дополнительных значений. Для этого нажмите справа от нужного поля.
   - Все адреса электронной почты у контактов должны быть уникальными.
5. Проверьте введенную информацию и нажмите **Добавить**.
6. Если при вводе допущены ошибки, система укажет на поля, значения в которых надо исправить. Отредактируйте их и снова нажмите **Добавить**.

   Если все заполнено правильно, пользователь появится в списке внешних контактов.

Найти

В правом верхнем углу раздела **Внешние контакты** находится строка поиска. Начните вводить известные данные человека, которого вы хотите найти: имя, фамилию, отчество, электронную почту или название компании, в которой он работает. На экране появится список подходящих внешних контактов.

Выберите пользователя в списке, чтобы открыть его карточку. В ней отображаются все данные, которые добавлены для этого контакта. Если для него зарегистрированы дополнительные номера телефонов или адреса электронной почты, то для их просмотра нажмите **Показать еще** в карточке.

Редактировать

1. Откройте кабинет организации **admin.yandex.ru**.
2. В меню слева выберите **Пользователи** → **Внешние контакты**.
3. Наведите указатель на нужный контакт. Если необходимо воспользуйтесь поиском по списку. Порядок поиска описан в разделе Найти.
4. В правой части строки нажмите значок и выберите **Редактировать**.
5. Измените данные контакта и нажмите кнопку **Сохранить**.

Удалить

1. Откройте кабинет организации **admin.yandex.ru**.
2. В меню слева выберите **Пользователи** → **Внешние контакты**.
3. Наведите указатель на нужный контакт. Если необходимо воспользуйтесь поиском по списку. Порядок поиска описан в разделе Найти.
4. В правой части строки нажмите значок и выберите **Удалить**.
5. Подтвердите удаление.
6. Контакт пропадет из списка. Файлы по ссылке на Диске, которыми поделились с этим контактом, и встречи в Календаре, на которые он приглашен, останутся ему доступны. Закрыть

доступ к файлам и удалить из встреч можно вручную.

Примечание

Удаление контакта может занимать до одного часа.

Внешние контакты в Почте, в Календаре и Диске

Контакты, которые не состоят в вашей организации, помечаются флагом `внешний`. Обращайте внимание на такую отметку, когда отправляете письма, добавляете участников встреч или приглашаете людей в общую папку. Это снизит вероятность того, что вы по ошибке поделитесь закрытой информацией с сотрудником другой организации.

Внешние контакты отображаются:

В Почте

- Когда выбираете получателей и просматриваете информацию о них.
  Как выбирать получателей при написании письма
- В результатах поиска по письмам.
  Как искать по письмам

Примечание

Если вы синхронизируете контакты в почтовой программе для компьютера и в ней перестали отображаться общие и внешние контакты, настройте синхронизацию заново.
Что делать, если из адресной книги пропали некоторые контакты

В Календаре

- Когда добавляете участников события или просматриваете информацию о них.
  Как пригласить участников на событие

В Диске

- Когда настраиваете общий доступ к папке.
  Как настроить общий доступ к папке

Написать в службу поддержки

Гости

Эта возможность доступна в тарифах **Минимальный**, **Основной**, **Продвинутый**, **Корпоративный** и **Корпоративный + Управление организацией** из новой линейки, а также тарифе **Оптимальный** из старой. О покупке тарифа читайте в Справке по тарифам и оплате.

Гости — это внешние контакты, с которыми ваши сотрудники могут общаться в рабочих чатах Мессенджера. Это удобно, если нужно связаться с несколькими сотрудниками другой организации или подрядчиками.

Пригласить одного гостя

Чтобы отправить приглашение, в кабинете организации перейдите в раздел **Внешние контакты и гости** → **Гости** → **Добавить** → **Пригласить вручную**. Заполните все поля и нажмите **Пригласить**.

Приглашение придет пользователю на указанную почту — оно действительно в течение трех дней. Если пользователь не авторизуется за это время, приглашение нужно будет отправить снова.

Пригласить сразу много

Добавить сразу несколько гостей можно с помощью CSV-файла.

1. Откройте кабинет организации admin.yandex.ru.
2. В меню слева выберите **Пользователи** → **Внешние контакты и гости** → **Гости**.
3. Нажмите **Добавить** → **Загрузить списком**.
4. Нажмите **Шаблон** и сохраните файл к себе на устройство.
5. Заполните скачанный файл:

   Содержание полей и правила заполнения

Поле	Что содержит
last_name	Фамилия
first_name	Имя
middle_name	Отчество

position	Должность
company	Компания
phone_number	Номер телефона
email	Адрес электронной почты

- Разделитель полей в файле — запятая.
- Электронная почта должна быть уникальной. Если в файле будет содержаться адрес почты, который уже есть в списке гостей, такой файл вызовет ошибку загрузки.
- Чтобы добавить дополнительные электронные адреса или номера телефонов к контакту, введите его в следующей строке.

6. Сохраните CSV-файл в кодировке UTF-8. В другой кодировке он будет распознан неправильно.
7. Убедитесь, что в файле не больше 1000 строк, а его размер — до 10 МБ.
8. В кабинете организации нажмите **Выбрать CSV-файл** и укажите ваш файл.
9. Нажмите **Загрузить список**. Добавленные пользователи получат письмо-приглашение на почту, которое нужно принять в течение трех дней.

Как удалить гостя

1. Откройте admin.yandex.ru.
2. В меню слева выберите **Пользователи** → **Внешние контакты и гости** → **Гости**.
3. Выберите гостя, которого хотите удалить, и в конце строки нажмите ⋮ → 🗑.

После удаления у гостя пропадут все рабочие чаты вашей организации.

Написать в службу поддержки

Федерации

Эта возможность доступна в тарифах для крупных организаций **Корпоративный + Управление организацией** и **Корпоративный Максимум**, а также тарифах **Оптимальный** и **Расширенный** из старой линейки.

Федерация — это несколько организаций, связанных между собой. С помощью федераций сотрудники из разных компаний могут вместе работать в сервисах Яндекс 360: ставить друг другу встречи, переписываться, созваниваться и быстро находить друг друга в контактах Почты, Мессенджера и Календаря.

Добавлять и удалять организации в федерации может администратор или менеджер федераций.

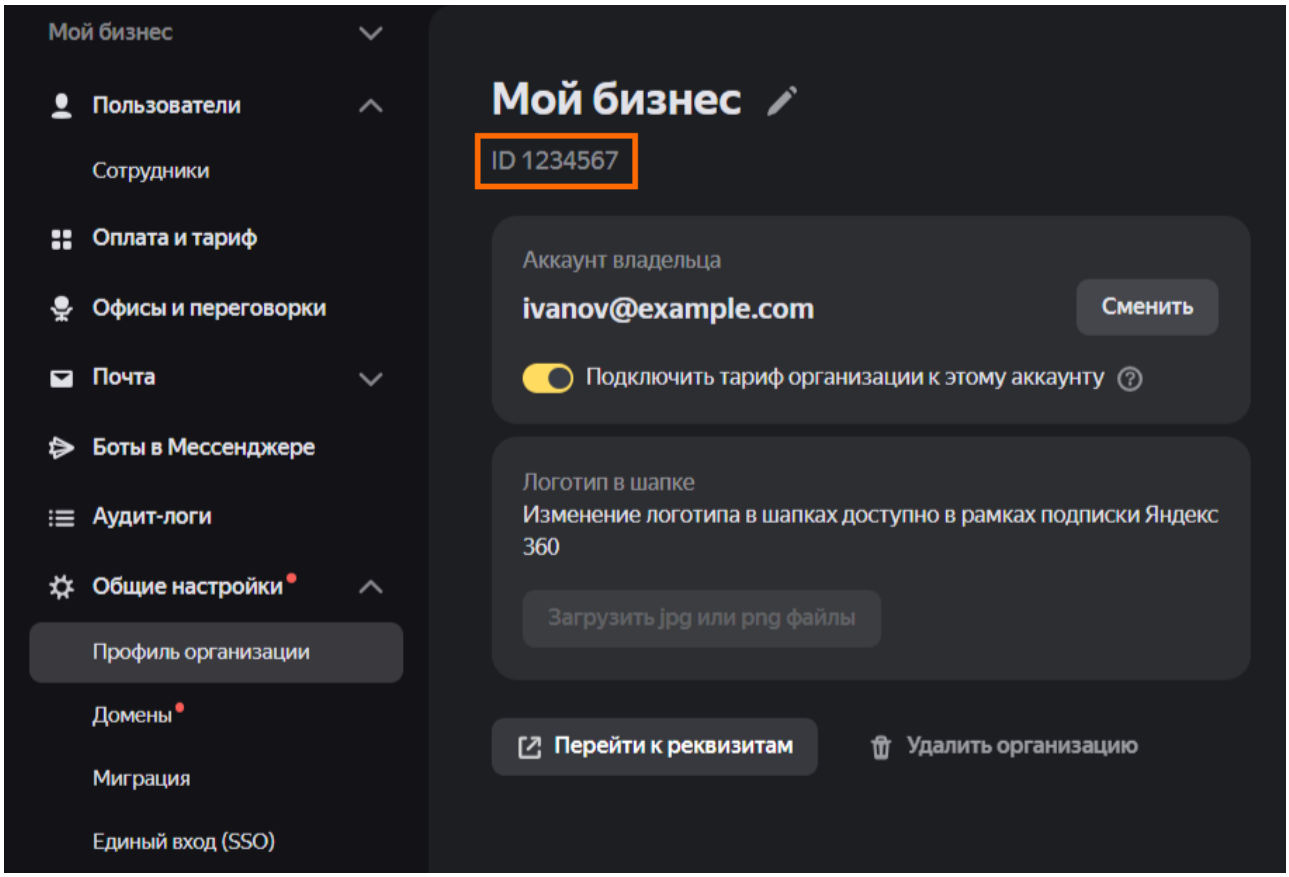
Связать две организации в федерацию

Чтобы организации связались, одна должна отправить запрос, а другая — принять его. Для этого:

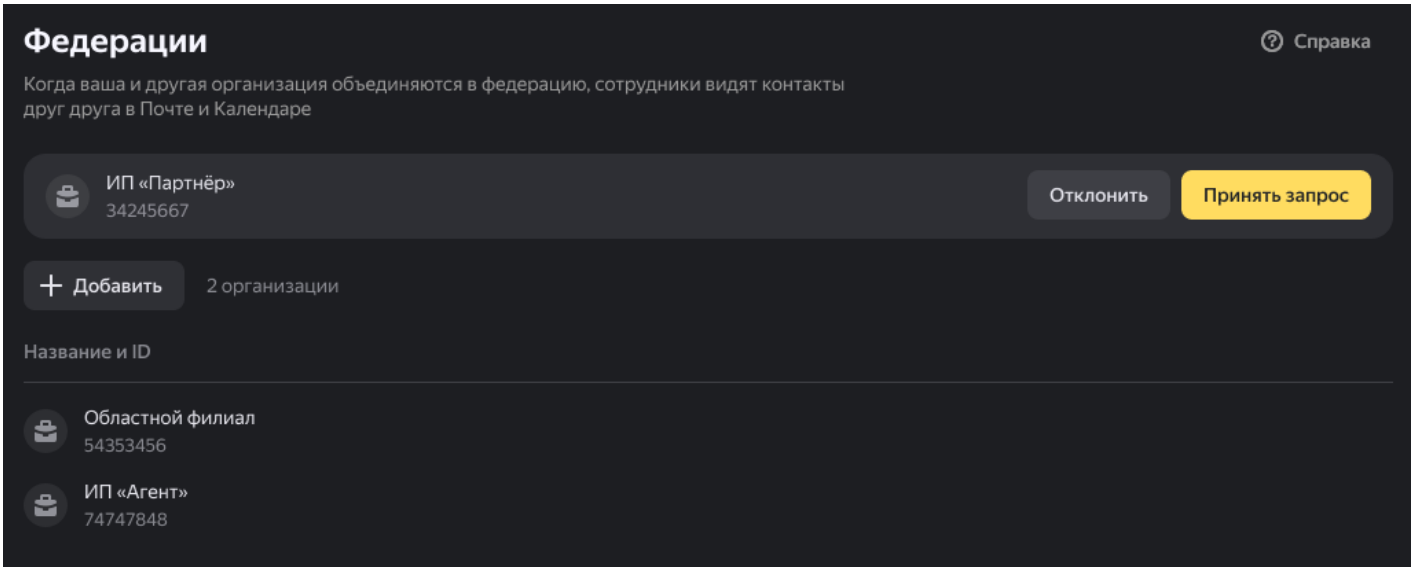
1. Откройте admin.yandex.ru и выберите **Федерации**.
2. Нажмите **Добавить**.
3. Укажите ID организации, которую хотите добавить в федерацию.

   Как определить ID организации

   Узнать индентификатор другой организации можно у ее администратора — ID написан под названием организации в разделе **Общие настройки** → **Профиль организации**.



4. Нажмите **Отправить запрос**. Организация будет добавлена, когда ее администратор примет запрос в разделе **Федерации**.



Связать три и более организации в федерацию

Чтобы связать больше двух организаций, каждая должна добавить остальные.

Например, у вас в кабинете есть три организации: А, Б и В. Чтобы сотрудники всех трех организаций смогли видеть контакты друг друга, добавьте их в федерации:

1. Переключитесь на организацию А и отправьте запросы Б и В.
2. Переключитесь на организацию Б, примите запрос от А и отправьте запрос В.
3. Переключитесь на организацию В и примите запросы от А и Б.

Возможности сотрудников в федерации

Когда вы добавите организацию в федерации, сотрудники будут видеть контакты друг друга и смогут:

В Почте

- Добавлять получателей из другой организации через подсказки при вводе.
- Писать любому сотруднику другой организации через адресную книгу.
- Находить контакты другой организации в поиске по письмам.

В Календаре

- Приглашать участников из другой организации на встречи.
- Бронировать переговорки другой организации.

В Мессенджере

- Переписываться в личных и групповых чаты в рабочем пространстве федерации.
- Находить друг друга в поиске.
- Обмениваться файлами.
- Звонить друг другу.

Удалить организацию из федерации

Связь между двумя организациями может быть разорвана по инициативе любой из них — подтверждение второй не требуется. При этом сотрудники больше не будут видеть друг друга среди контактов в Почте, Мессенджере и Календаре. Уже созданные общие встречи не пропадут.

1. Откройте admin.yandex.ru и выберите **Федерации**.
2. Выделите организацию, которую хотите удалить из федерации, и в конце строки нажмите .
3. Подтвердите удаление.

Написать в службу поддержки

Общие диски

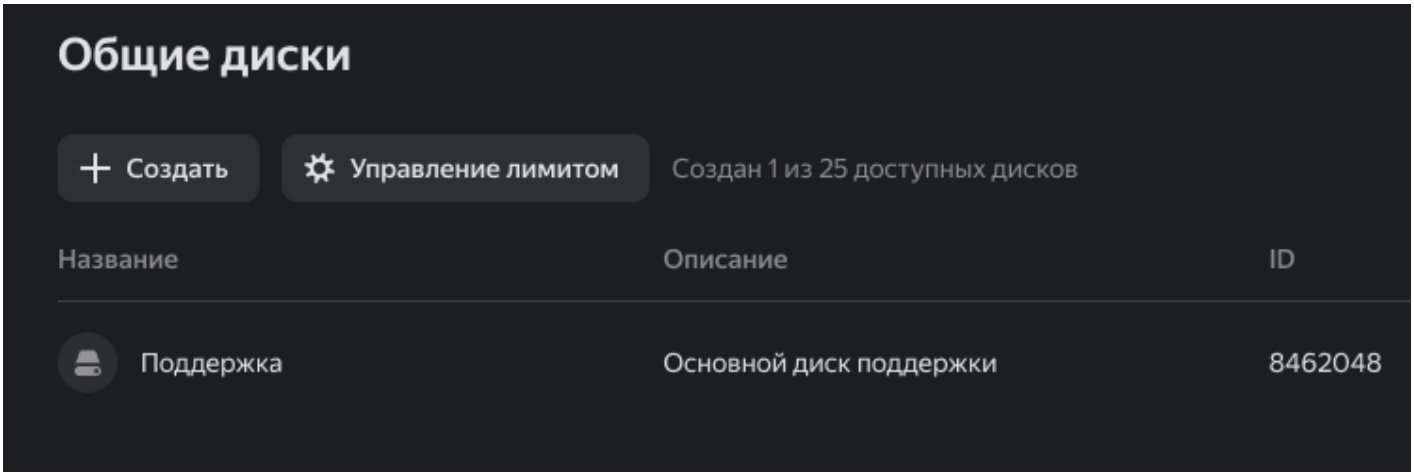
Общие диски — это специальные папки на Яндекс Диске, в которых можно хранить файлы, работать над ними совместно с коллегами и искать нужную информацию.

Размер одного общего диска — 1 ТБ. Для организации можно подключить любое количество таких дисков.

> **Примечание**
>
> Подключение общих дисков — это дополнительная услуга, которая не входит в стандартные тарифы Яндекс 360 для бизнеса и приобретается отдельно. О покупке дополнений читайте в Справке по тарифам и оплате.

Использовать общие диски можно **только в веб-версии Диска** на странице disk.yandex.ru и только сотрудникам, чьи аккаунты созданы на домене организации.

В мобильном приложении и программе для компьютера общие диски недоступны. Сотрудники с аккаунтами на других доменах, в том числе `yandex.ru`, не могут пользоваться общими дисками даже в веб-версии.



Порядок настройки общих дисков:

- Покупка общих дисков описана в Справке по тарифам и оплате.
- В кабинете организации вы можете управлять оплаченными общими дисками:
  - создавать диски в пределах подключенного лимита;
  - настраивать доступ сотрудникам, группам и подразделениям без указания ролей;
  - очищать корзину;
  - удалять общие диски.
- Общим диском могут пользоваться только те сотрудники, которым выдан доступ к нему. Работа сотрудников с общими дисками описана в Справке Яндекс Диска для бизнеса.

Управлять общими дисками организации и файлами и папками на них можно также по API. О том, как это делать, читайте в документации REST API Яндекс Диска.

Создать

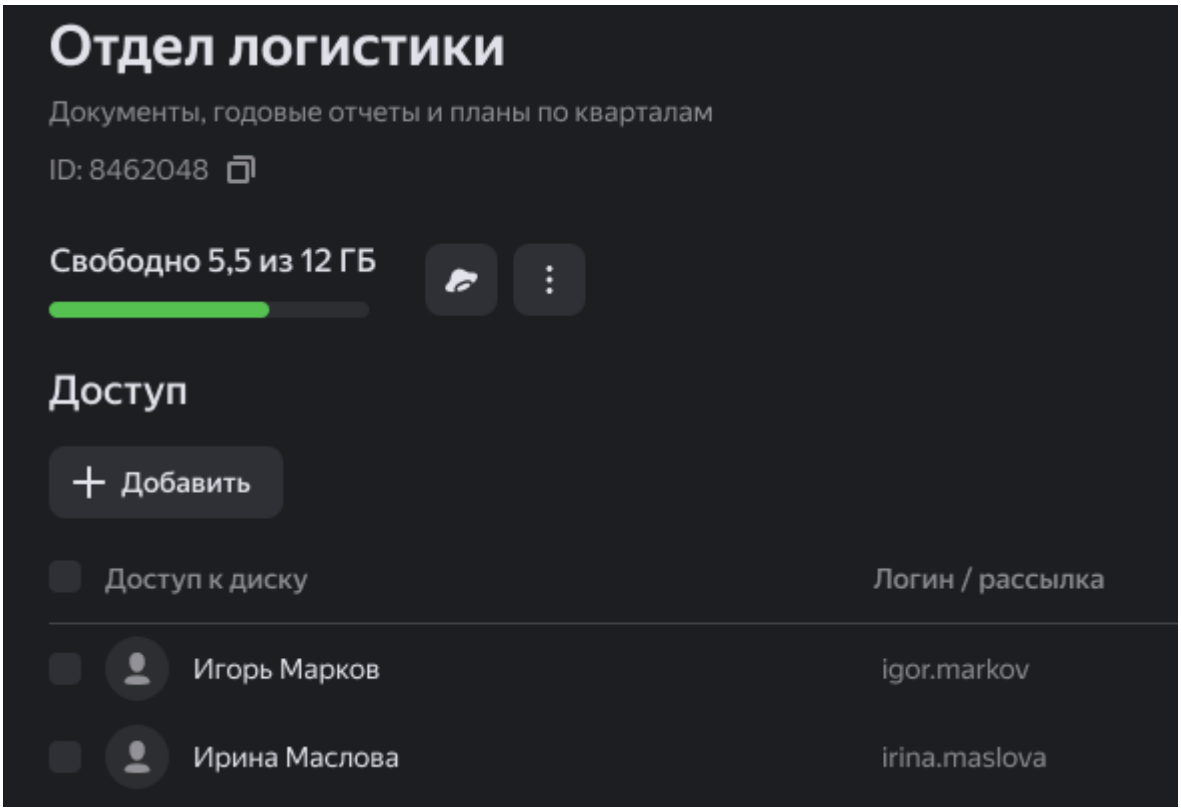
Прежде чем создавать общие диски, надо подключить возможность ими пользоваться. После подключения вы сможете создать необходимое количество общих дисков в пределах оплаченного лимита. Если достигнут лимит на количество общих дисков для организации, создать еще один диск не получится. Сначала удалите старые или увеличьте лимит. Подключение общих дисков и управление лимитом описано в Справке по тарифам и оплате.

Чтобы создать новый диск:

1. В кабинете организации перейдите в раздел **Диск** → **Общие диски**.
2. Нажмите кнопку **Создать**:
   - Если вы впервые добавляете общий диск, кнопка будет находиться в центре экрана.
   - Если у вашей организации уже есть общие диски, кнопка будет расположена над таблицей со списком дисков.
3. Укажите название (максимум 256 символов) и описание (максимум 512 символов) и подтвердите создание общего диска. После этого он появится в списке.

Настроить доступ

Для каждого общего диска в разделе **Доступ** отображается список тех, кто может с ним работать (пользователи, группы, подразделения). Чтобы открыть раздел, выберите нужный общий диск.



Особенности доступа сотрудников

> **Внимание**
>
> Открыть доступ можно только сотрудникам, аккаунты которых созданы на домене организации. Пользователям, приглашенным по ссылке, выдать доступ нельзя.

- Если вы откроете доступ группе, в которой есть приглашенные пользователи, общий диск будет доступен только сотрудникам, аккаунты которых были созданы на домене организации.
- Доступы для сотрудников работают по приоритетам: приоритет у доступа на редактирование выше. Если сотрудник состоит в двух группах, для одной из которых открыт доступ на редактирование, а для другой — на просмотр, сотрудник сможет редактировать файлы. То же касается ситуации, если у сотрудника имеется персональный доступ на редактирование.

Особенности доступа администраторов

- Администратор, аккаунт которого создан на домене организации:
  - в кабинете организации может перейти в любой Диск из раздела **Общие диски**, в том числе по прямой ссылке;
  - в своем Диске в разделе **Общий доступ** видит только те общие диски, к которым ему явно выдан доступ.
- Приглашенные пользователи с правами администратора могут создавать и удалять общие диски, просматривать информацию о них, управлять доступом и очищать корзину, но не могут переходить в общие диски и просматривать их содержимое.

Особенности доступа владельца

- У владельца организации с личным аккаунтом вида `login@yandex.ru` нет доступа к общим дискам.

Открыть доступ

1. Нажмите кнопку **Добавить**.
2. Введите в поле тех, кому хотите открыть доступ к общему диску.

   Вы можете искать по именам, логинам или названиям среди пользователей, групп, подразделений. Можно последовательно выбрать сразу несколько элементов, но добавить больше 100 элементов (пользователей, групп или подразделений) не получится.
3. Выберите уровень доступа:
   - **Просмотр**: пользователи могут просматривать, искать, скачивать и копировать файлы и папки на доступные диски. Файлы и папки нельзя скопировать или переместить на Диск, который доступен только в режиме просмотра.
   - **Редактирование**: пользователи имеют полный доступ к файлам и папкам и могут просматривать, перемещать, искать, скачивать, загружать, редактировать и удалять их.
   - **Управление доступом**: в веб-версии Диска позволяет видеть текущих пользователей общего диска, добавлять новых пользователей, назначать и изменять им уровни доступа, отключать доступ к общему диску.
4. Подтвердите добавление.

Изменить уровень доступа

Для одного пользователя

:

1. Напротив имени сотрудника в столбце **Уровень доступа** нажмите на название текущего уровня.
2. В выпадающем списке выберите нужный уровень доступа.

Для нескольких пользователей

1. Выберите пользователей, группы или подразделения, для которых хотите изменить доступ.
2. Нажмите кнопку **Настроить доступ**.
3. Выберите нужный и сохраните изменения.

Закрыть доступ

Одному пользователю

В строке с именем сотрудника нажмите ⋮ справа, а затем нажмите кнопку **Отключить**.

Нескольким пользователям

1. Выберите пользователей, группы или подразделения, которым хотите отключить доступ.
2. Нажмите кнопку **Отключить** и подтвердите действие.

Перейти в Диск

Переходить в общие диски может только администратор, аккаунт которого был создан на домене организации.

1. В кабинете организации откройте раздел **Диск** → **Общие диски** и найдите нужный диск.
2. Наведите указатель на строку с диском и нажмите ⋮ справа.
3. Выберите **Перейти в Диск**. В соседней вкладке браузера откроется содержимое Диска.

Действия, которые можно совершать в общем диске, описаны в Справке Яндекс Диска для бизнеса.

Очистить корзину

Когда пользователь удаляет файлы с общего диска, они попадают в корзину общего диска. Файлы можно восстановить из корзины в течение 30 дней, потом они удаляются окончательно. Пока файлы хранятся в корзине, они продолжают занимать место.

Администратор может очистить корзину и освободить место заранее:

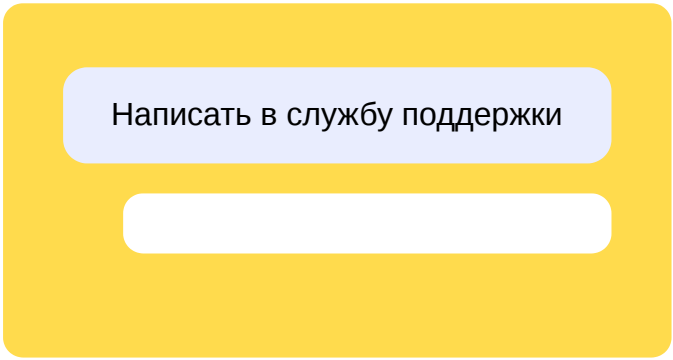
1. В кабинете организации перейдите в раздел **Диск** → **Общие диски** и найдите нужный диск.
2. Наведите указатель на строку с диском и нажмите ⋮ справа.
3. Выберите **Очистить корзину** и подтвердите действие.

Удалить

Администратор может удалить общий диск целиком со всем его содержимым:

1. В кабинете организации перейдите в раздел **Диск** → **Общие диски** и найдите нужный диск.
2. Наведите указатель на строку с диском и нажмите ⋮ справа.
3. Выберите **Удалить** и подтвердите действие.

После того как Диск удалится, вы не сможете восстановить файлы и назначенные права доступа.



Управление настройками персонального и общего доступов

Сотрудники могут совместно работать с файлами и папками на Диске и делиться ими. Например, настроить персональный или общий доступ к файлу, а затем отправить специальную ссылку на него коллегам или внешним контактам. По умолчанию сотрудники сами решают, кому будут доступны файлы и папки: только коллегам, конкретным людям, группам, подразделениям или всем, у кого есть ссылка. Как работают персональный и общий доступы

В кабинете организации администраторы могут управлять настройками этих доступов. Например, администратор может разрешить:

- делиться файлами и папками только с коллегами;
- настраивать к файлам и папкам только персональный доступ.

Сотрудники смогут настраивать доступы только с теми настройками, которые включил администратор. Это поможет предотвратить случайную утечку информации, которая хранится на личных или общих дисках.

Важно

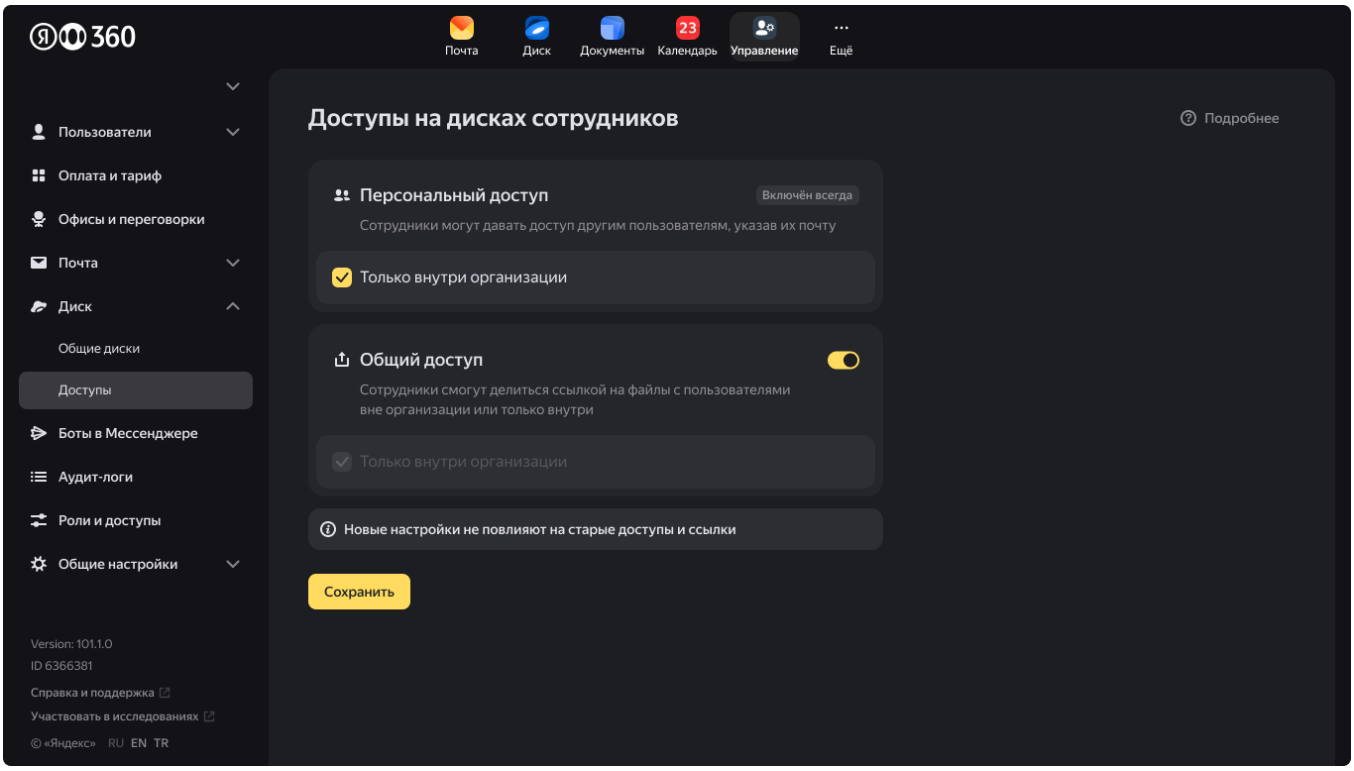
Доступы, которые сотрудники открыли **до включения настроек в кабинете организации**, продолжат действовать. Например, если у внешнего контакта уже есть персональный доступ к файлу, он не потеряет его, когда вы разрешите делиться файлами только внутри организации. Вы можете попросить сотрудников самостоятельно закрыть или перенастроить доступы, которые они успели выдать, — например, если в организации больше нельзя делиться файлами с внешними контактами.

Разрешить делиться файлами и папками только внутри организации

1. Откройте страницу admin.yandex.ru/virtual-disk-permissions.
2. В блоке **Персональный доступ** включите опцию **Только внутри организации**.
3. Нажмите **Сохранить**.

Опция **Только внутри организации** автоматически применится и к настройкам общего доступа. Это значит, что внешние контакты не получат доступ к файлу, даже если сотрудник отправит им ссылку на него.

Скриншот

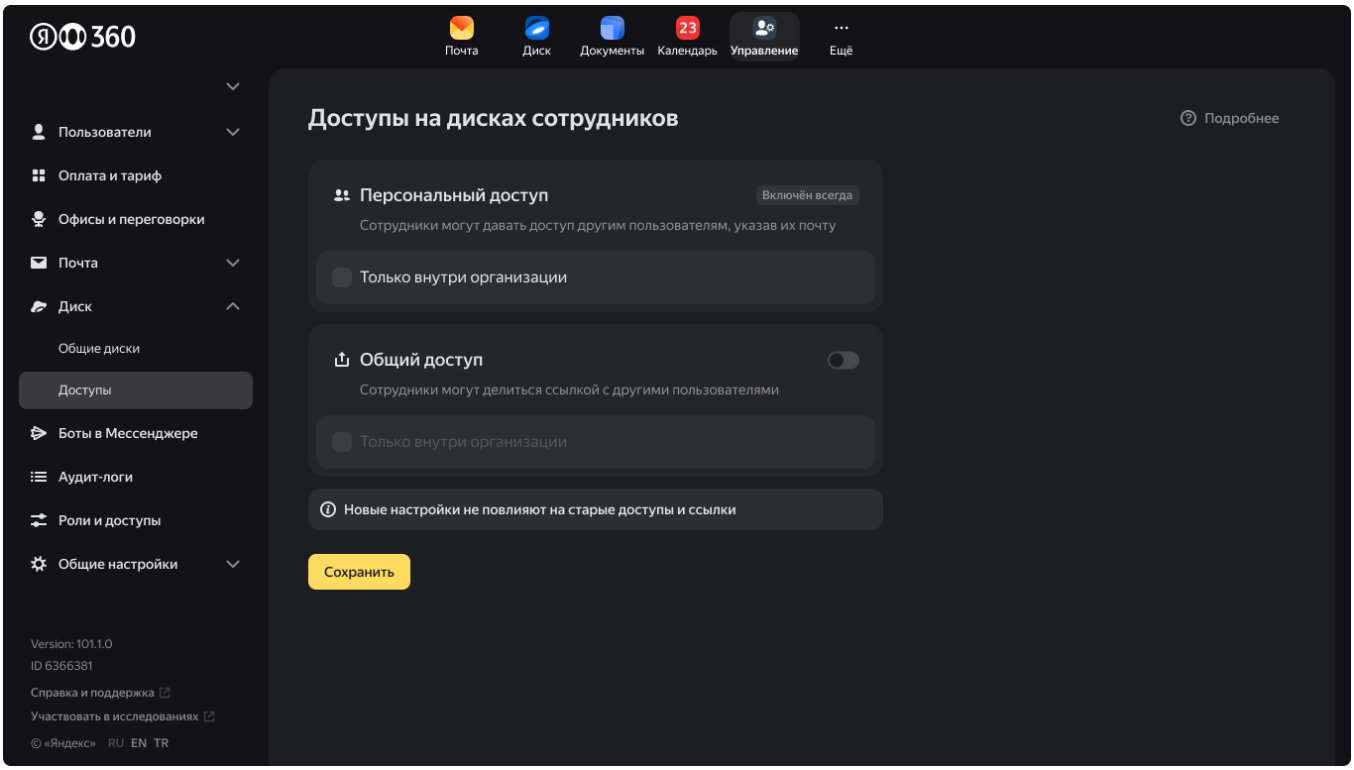


Разрешить настраивать только персональный доступ

1. Откройте страницу admin.yandex.ru/virtual-disk-permissions.
2. Выключите опцию **Общий доступ**.
3. Нажмите **Сохранить**.

Сотрудники смогут настраивать персональный доступ и для своих коллег, и для внешних контактов.

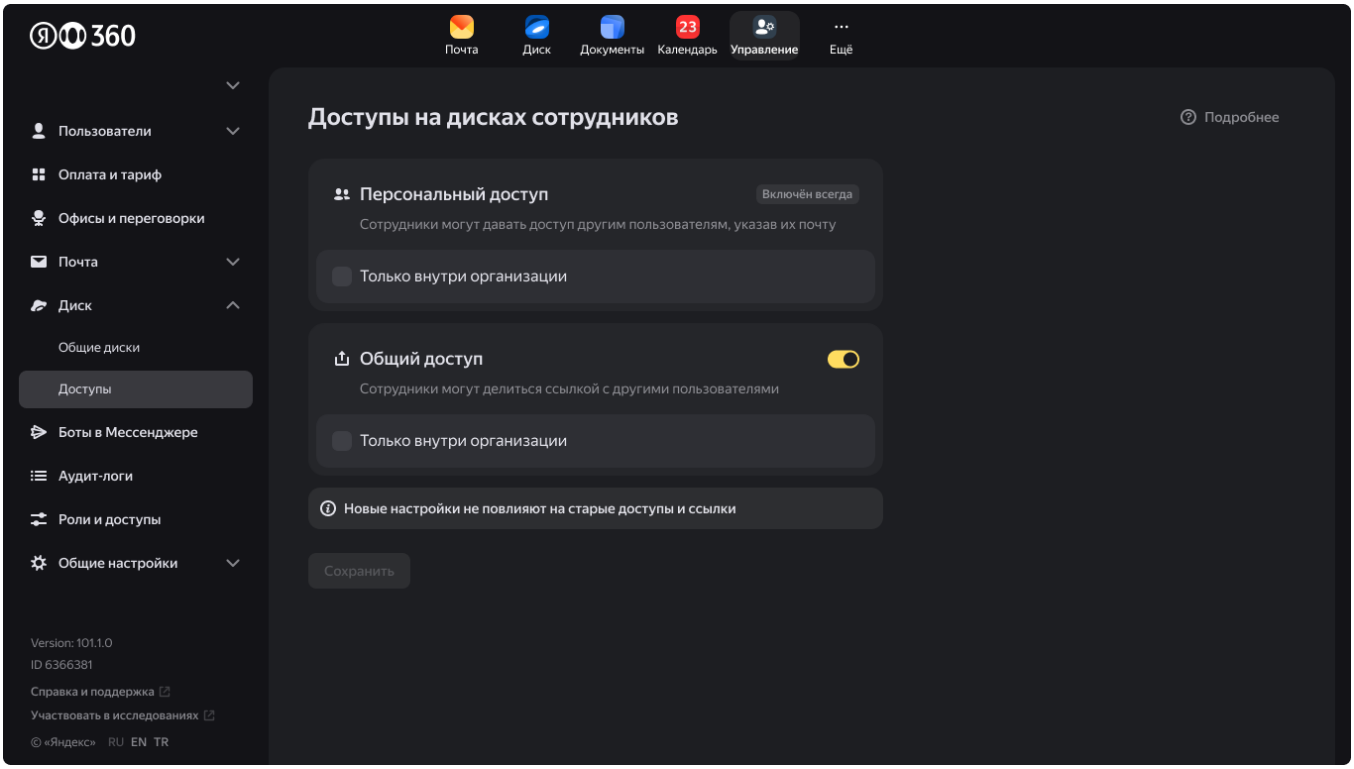
Скриншот



Разрешить делиться файлами и папками с любыми пользователями

1. Откройте страницу admin.yandex.ru/virtual-disk-permissions.
2. Включите опцию **Общий доступ**, если она отключена.
3. В блоках **Персональный доступ** и **Общий доступ** отключите опцию **Только внутри организации**, если она включена.
4. Нажмите **Сохранить**.

Скриншот



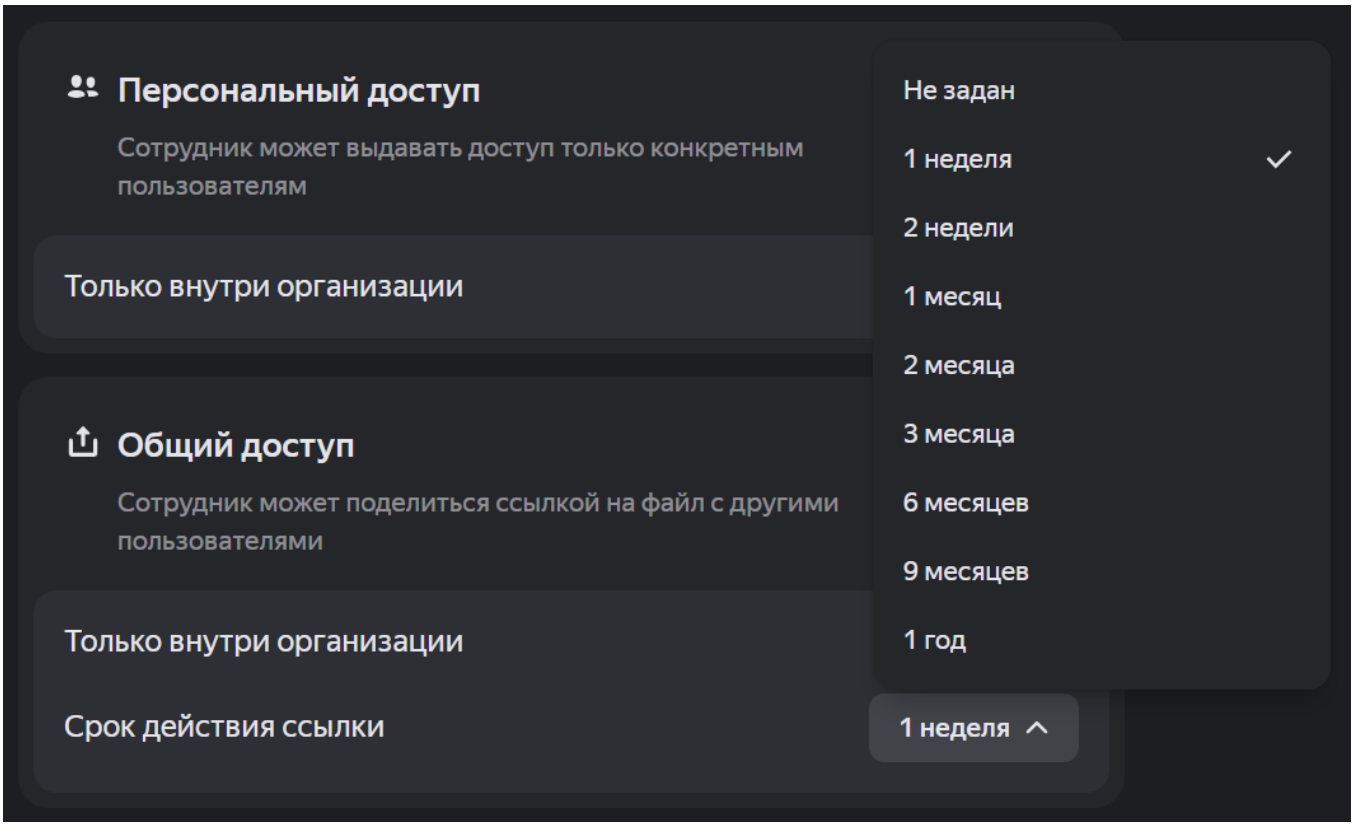
Установить максимальный срок действия ссылки

Эта настройка ограничивает время доступа к файлам и папкам, которыми сотрудники делятся с другими пользователями.

Например, ваши сотрудники работают с проектной документацией через облачное хранилище, предоставляя доступ по ссылкам внешним подрядчикам и клиентам. Вы можете ограничить срок действия таких ссылок, чтобы предотвратить несанкционированный доступ к диску после завершения проекта.

1. Откройте страницу admin.yandex.ru/virtual-disk-permissions.
2. Включите опцию **Общий доступ**, если она отключена.
3. В блоке **Общий доступ** выберите значение в выпадающем списке **Максимальный срок действия ссылки**.
4. Нажмите **Сохранить**.

Скриншот



После сохранения настройки сотрудники смогут выдавать доступы к файлам и папкам только на ограниченный срок, не превышающий установленного значения. К примеру, если установить ограничение **1 неделя**, сотрудник 1 июня в 9:00 сможет открыть доступ до 8 июня до 9:00 или выбрать более раннюю дату завершения доступа – например, 5 июня.

Написать в службу поддержки

Аудит-логи

Эта возможность доступна в тарифах **Основной**, **Продвинутый**, **Корпоративный + Безопасность** и **Корпоративный Максимум** из новой линейки, а также тарифах **Оптимальный** и **Расширенный** из старой.

Аудит-логи позволяют отслеживать основные события и активность сотрудников вашей организации. Это может быть полезно при инцидентах и нарушении безопасности.

С помощью аудит-логов администраторы и менеджеры аудит-логов могут посмотреть:

События в сервисах

- Как сотрудники входят в аккаунт. Например, можно увидеть когда и с какого устройства подключился сотрудник.
- Что сотрудники организации делают с письмами и файлами в Почте и Диске. Например, вы можете узнать, кто переместил письмо или файл.

События в кабинете организации

- Какие изменения вносились в кабинете организации. Например, можно узнать, кто добавил или пригласил нового пользователя.
- Что другие администраторы ищут в архиве писем и как настраивают правила для писем.

Как подключить

1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Аудит-логи**.
3. Нажмите кнопку **Подключить** и подтвердите подключение.

Уведомление пользователей

Согласно пункту 3.7 оферты, после подключения доступа администратор обязан уведомить об этом всех пользователей и при необходимости получить их письменное согласие (если они не давали его ранее).

Как посмотреть логи

Шаг 1. Укажите, какие логи нужно найти

События в сервисах

1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Аудит-логи** → **Логи в сервисах**.
3. Нажмите **Сервис** и выберите:

- **Почта** — Действия сотрудников с письмами.
- **Диск** — Действия сотрудников с файлами.
- **Мессенджер** — Действия сотрудников с чатами и каналами, а также отправка и удаление сообщений.
- **Авторизации** — События входа сотрудников в аккаунты.

События в кабинете организации

1. Откройте Яндекс 360 для бизнеса.
2. В меню слева выберите **Аудит-логи** → **Логи управления**.
3. Нажмите **Раздел** и выберите:
   - **Правила для писем** — Логи изменений в правилах для писем.
   - **Архив писем** — События поиска в архиве писем.
   - **Сотрудники** — Действия, связанные с аккаунтами сотрудников: добавление, изменение данных, удаление, блокировка, разблокировка, изменение алиаса, изменения групп и подразделений.
   - **Профиль организации** — Логи изменений в профиле организации: смена владельца организации, смена названия.
   - **Офисы и переговорки** — Добавление, изменение или удаление офисов и переговорок.
   - **Общие ящики** — Действия с общими почтовыми ящиками: добавление, изменение и удаление.
   - **Делегированные ящики** — Создание и удаление делегированных почтовых ящиков.
   - **Общие диски** — Создание и удаление общих дисков.
   - **Домены** — Логи изменения доменов: добавление, изменение и удаление.
   - **Единый вход (SSO)** — Логи изменения настроек SSO.
   - **Внешние контакты** — Добавление, изменение или удаление внешних контактов.

   Некоторые разделы можно выбрать одновременно, если рядом с ними можно поставить отметку. Чтобы выбрать несколько разделов, отметьте их и нажмите **Сохранить**.

Шаг 2. Уточните запрос с помощью фильтров

Фильтрация позволяет найти логи по заданным параметрам: например, конкретное событие за определенный период.

Чтобы добавить фильтр, нажмите на него и выберите необходимые параметры:

- **Сотрудник** или **Администратор** — Укажите одного или нескольких сотрудников и нажмите **Сохранить**.
- **Дата** — Выберите период или задайте свой.
- **Событие** — Укажите одно или несколько событий и нажмите **Сохранить**. При выборе одного события могут появиться дополнительные параметры фильтрации — можно выбрать не более трех.

Чтобы удалить фильтр, справа от него нажмите значок ×. Чтобы отменить выбранную фильтрацию и вернуться к предыдущему шагу, нажмите **Сбросить фильтры**.

Шаг 3. Соберите и просмотрите логи

1. Нажмите **Найти логи**.
2. Нажмите на событие в списке, чтобы узнать о нем подробнее: информация отобразится во всплывающем окне.

Если хотите посмотреть всю информацию о событии «Поиск» в архиве писем, подтвердите номер телефона, привязанный к вашему Яндекс ID. Или привяжите номер, если еще не сделали этого. Как привязать номер можно узнать в Справке Яндекс ID.

> **Дата и время событий**
>
> Логи отображаются в часовом поясе пользователя, который их запросил.

Сохранится ли результат поиска при обновлении страницы

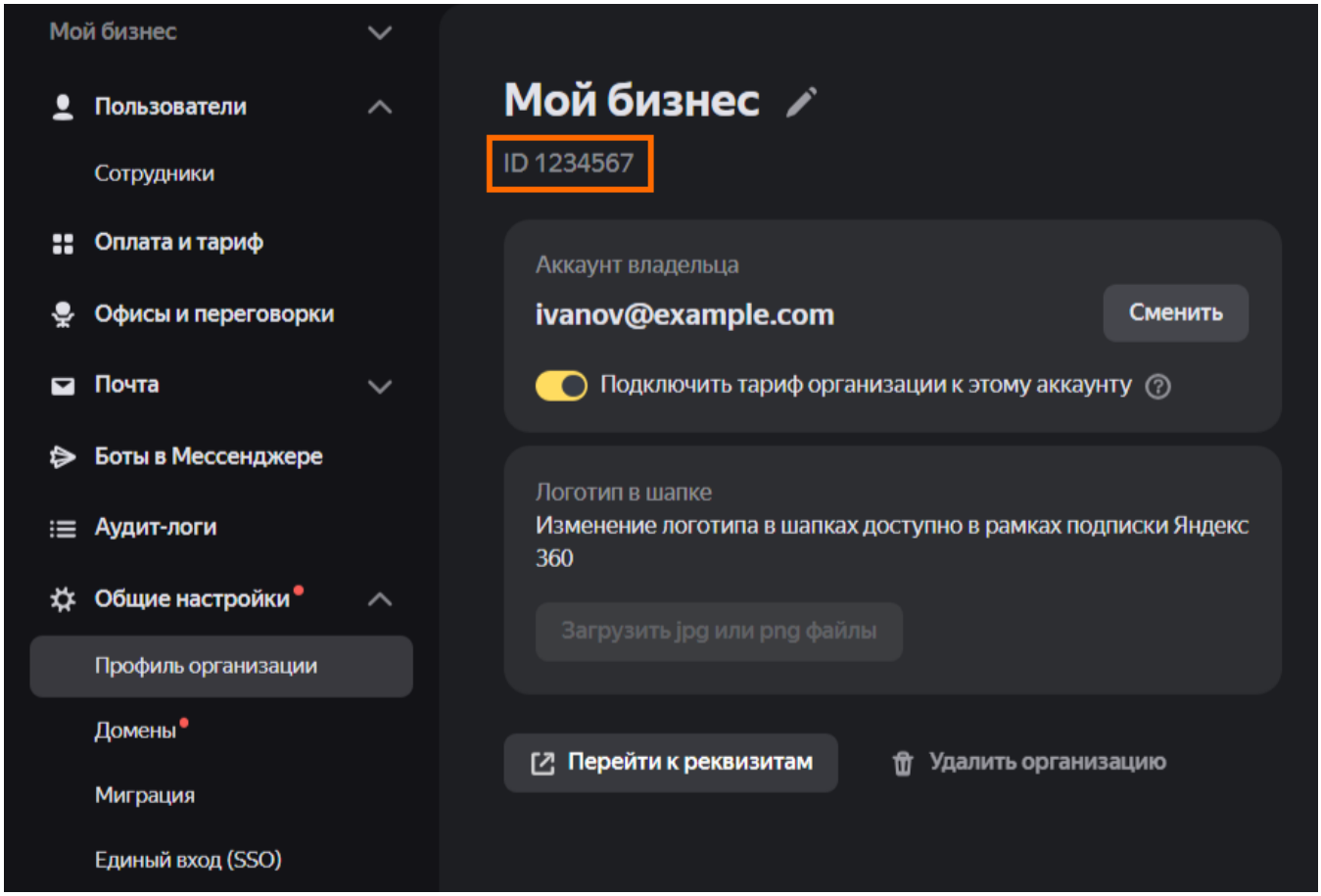
Результат поиска и выбранные фильтры сбросятся при обновлении страницы.

Если вы перейдете в другой раздел кабинета организации — результат поиска сбросится, но выбранные фильтры сохранятся. Вы сможете повторить поиск логов с теми же параметрами.

Работа с логами через API

Прежде чем начать

1. Для работы с API вам потребуется OAuth-токен, который можно получить после создания приложения в сервисе Яндекс OAuth.
   - Если у вас еще нет OAuth-приложения, то для его создания и получения токена воспользуйтесь инструкцией на странице Доступ к API. При создании приложения выберите права `ya360_security:read_auditlog`.
   - Если у вас уже есть OAuth-приложение для работы с API Яндекс 360 для бизнеса, то добавьте ему права доступа для чтение событий аудит-лога организации, а затем получите новый OAuth-токен по инструкции.
2. Определите идентификатор организации: откройте admin.yandex.ru и выберите **Общие настройки** → **Профиль организации**. Идентификатор будет написан под названием организации.



Как получить логи

1. Сформируйте GET-запрос:

   ```
   curl -X GET -H "Authorization: OAuth {oauth_token}" https://cloud-api.yandex.net/v1/auditlog/organizations/{org_id}/events?ended_at={ended_at}&count={count}
   ```

   В код подставьте обязательные значения:

   - `{orgId}` — идентификатор организации;
   - `{oauth_token}` — OAuth-токен;
   - `{ended_at}` — дата и время окончания аудит-лога в формате ISO 8601, например `2024-01-31T23:59:59`;
   - `{count}` — количество событий на одной странице результатов от 1 до 100.

2. Чтобы уточнить запрос, укажите в конце запроса дополнительные параметры через `&`, например:

   ```
   &started_at={started_at}&types={types}&include_uids={include_uids}&ip={ip}&service={service}
   ```

   В код подставьте значения:

- `{started_at}` — дата и время начала аудит-лога в формате ISO 8601, например `2024-01-01T00:00:00`;
- `{types}` — типы событий, которые должны быть включены в список. Можно указать несколько типов через запятую без пробела; Типы событий в документации API
- `{include_uids}` — список пользователей, действия которых должны быть включены в список событий. Можно указать нескольких пользователей через запятую без пробела, например `include_uids=1,2,3`;
- `{ip}` — IP-адрес, с которого было выполнено действие;
- `{service}` — платформа, с которой поступил запрос на действие, можно указать один из списка:
  - `Web` – веб-сайт;
  - `Desktop` – программа на компьютере;
  - `Mobile` – мобильное приложение;
  - `Api` – внешний HTTP API;
  - `Synchronization` – внешнее приложение для автоматической синхронизации данных (например, по стандарту SCIM);
  - `ID` – внутренний сервис авторизации пользователей;
  - `Internal` – другие внутренние сервисы;
  - `Unknown` – источник не указан.

3. Отправьте запрос. Ответ на запрос возвращает список событий по указанным параметрам.

   Пример ответа

```
{
   "iteration_key": "5",
   "items": [
     {
       "user_login": {логин},
       "user_name": {имя},
       "event": {
         "status": {статус},
         "idempotency_id": {идентификатор события},
         "uid": {идентификатор пользователя},
         "service": {сервис},
         "ip": {ip-адрес},
         "occurred_at": {дата},
         "org_id": {идентификатор организации},
         "is_system": false,
         "meta": {
           "device_id": null,
           "revision": "1"
         },
         "request_id": {идентификатор запроса},
         "type": {тип события}
       }
     }
```

```
    ]
  }
```

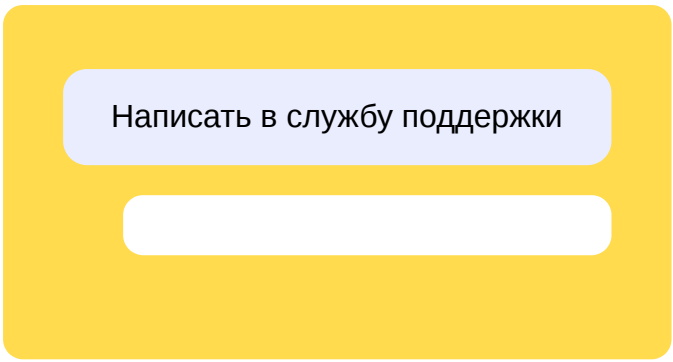
Здесь:
`{логин}`, `{имя}`, `{идентификатор пользователя}`, `{ip-адрес}` — данные инициатора события: логин и имя пользователя, идентификатор и IP-адрес;
`{статус}` — результат запроса: `Success` (успешно) или `Error` (ошибка – например, в событиях авторизации, где был неправильно введен логин или пароль);
`{сервис}` — платформа, с которой поступил запрос на действие, например `Web` – веб-сайт;
`{дата}` — дата и время события;
`{тип события}` — тип события, например `id_cookie.set` — вход через браузер. Типы событий в документации API

Я не понимаю, как отправлять запросы

1. Подготовьте запрос: скопируйте пример в любой редактор, вставьте в указанные места токен и идентификатор.
2. Откройте любую папку.
3. Нажмите на пустое место в адресной строке.
4. Напишите туда `cmd` и нажмите **Enter**.
5. Откроется окно «Командная строка». Вставьте в него готовый запрос и нажмите **Enter**.

Документация API

Полное описание всех методов для получения аудит-логов вы найдете в документации.



Рекомендации по безопасности

На этой странице мы собрали рекомендации по работе в Яндекс 360 для бизнеса, которые помогут повысить безопасность вашей организации.

Защита аккаунтов

Если злоумышленники получат доступ к аккаунту владельца или администратора, они также получат доступ к профилю вашей организации. Чтобы этого не случилось, воспользуйтесь нашими рекомендациями.

Используйте надежные пароли

Придумайте сложный пароль и не используйте его для других сайтов и приложений. Как придумать надежный пароль

Включите вход по паролю + одноразовому паролю

Вход с комбинацией постоянного и одноразового паролей — это один из самых надежных способов входа в аккаунт. Узнать больше о входе по паролю + одноразовому паролю

Если по каким-то причинам вы не готовы включить вход по комбинации паролей всем пользователям, то убедитесь, что он подключен для администраторов и других ключевых сотрудников.

Включить вход по комбинации паролей сразу для всех сотрудников можно с помощью запроса к API. Как это сделать

Добавьте телефонные номера и дополнительные адреса почты

Привязанный к Яндекс ID телефонный номер и дополнительный адрес почты помогают восстановить доступ к аккаунту. А еще на них Яндекс отправляет оповещения о подозрительной активности и других важных событиях. Защищенный номер также используется для подтверждения входа на Яндекс. Подробнее см. в разделах Привязка телефонных номеров и Дополнительные адреса почты.

Используйте единый вход (SSO)

С помощью технологии единого входа на базе стандарта SAML 2.0 вы можете организовать вход в сервисы Яндекс 360 через вашу систему управления доступом (например, Active Directory или Keycloak). Так сотрудникам не придется запоминать новые логин и пароль, а вам — заводить для них отдельные аккаунты в Яндекс 360 для бизнеса. Как настроить единый вход (SSO)

Синхронизируйте пользователей из Active Directory

Если в вашей компании развернута служба федерации Active Directory, вы можете настроить автоматическую синхронизацию сотрудников и групп с Яндекс 360 для бизнеса. Если сотрудник уволится или злоумышленники получат доступ к его аккаунту, вы сможете отключить аккаунт в Active Directory, и он заблокируется в Яндексе. Как синхронизировать пользователей с каталогом LDAP

Установите периодичность смены пароля

Если вы не используете SSO, ограничьте срок действия паролей пользователей. Когда срок действия закончится, Яндекс предложит сотруднику изменить пароль. Настроить

периодичность смены пароля можно с помощью запроса к API. Как изменить параметры парольной политики

Настройте время жизни cookie-сессии

Вы можете выбрать время, спустя которое сотрудникам нужно будет повторно входить в аккаунт. По умолчанию время жизни cookie-сессий не ограничено. Настройте это значение в соответствии с политикой информационной безопасности вашей организации. Это можно сделать с помощью запроса к API. Как изменить время жизни cookie-сессии

Выдавайте только необходимые права

Минимизируйте количество администраторов. Выдавайте пользователям только те права, которые им нужны. Как назначить сотрудника на роль менеджера

Администраторам организации можно создать вторые аккаунты с правами обычных пользователей. Это снизит вероятность того, что злоумышленники получат доступ к аккаунту с расширенными правами.

Не используйте один аккаунт администратора для нескольких сотрудников

Если несколько сотрудников используют один аккаунт администратора, у злоумышленников появляется больше шансов получить к нему доступ. Если аккаунт один, невозможно отследить, кто и когда выполнял в нем действия.

Если потеряли доступ к аккаунту владельца, восстановите его

Доступ к аккаунту владельца организации можно потерять: например, когда сотрудник увольняется или забывает пароль. Попробуйте восстановить доступ самостоятельно. Как это сделать

Защита корпоративной почты

Настройте DKIM-подпись

Вы можете установить DKIM-подпись для писем, которые сотрудники отправляют с вашего домена. Тогда получатель сможет удостовериться в том, что письмо действительно пришло от вас. Как настроить DKIM-подпись

Настройте SPF-запись

SPF-запись помогает снизить риск того, что письмо, отправленное с адреса на вашем домене, попадет в спам у получателя. Как настроить SPF-запись

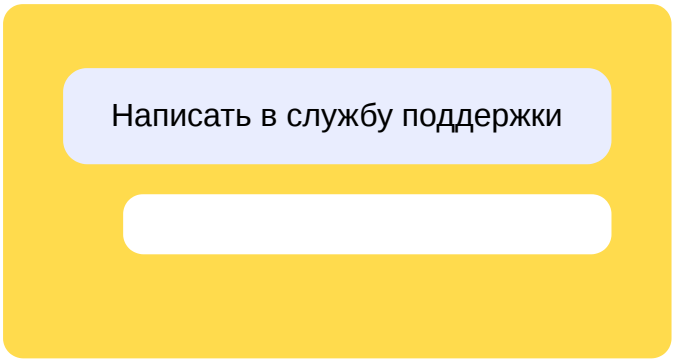
Ограничьте получение нежелательных писем

Вы можете управлять письмами, которые получают сотрудники, с помощью правил обработки. Например, ограничьте получение писем с определенного адреса. Как настроить правила обработки писем

Полезные ссылки

Также советуем ознакомиться с другими рекомендациями по защите данных:

- Защита личных данных
- Мошенничество в сети
- Защита от вирусов
- Защита компьютера


Написать в службу поддержки

Подтверждение входа в сервисы Яндекс 360

Этот инструмент доступен в тарифах для крупных организаций **Корпоративный + Безопасность** и **Корпоративный Максимум** из новой линейки, а также тарифе **Оптимальный** из старой линейки.

На остальных тарифах подтверждение входа можно включить через API без возможности его персональной настройки для отдельных сотрудников. Как это сделать

Вы можете настроить для пользователей дополнительное подтверждение входа в сервисы Яндекс 360 для бизнеса. В этом случае для авторизации надо будет вводить не только обычный пароль, но и одноразовый код: последние цифры номера, с которого поступит звонок на зарегистрированный в системе телефон, или числовую комбинацию из смс. Такой способ называется двухфакторной аутентификацией (2FA) — он надежнее, чем просто пароль.

Подтверждение входа в Яндекс 360 доступно пользователям, чьи аккаунты созданы на домене организации. Подтверждение входа можно настроить сразу всем таким сотрудникам или персонально — только некоторым из них.

Включить

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Безопасность** → **Подтверждение входа**.
3. Задайте необходимые настройки:
   - **Кому включить** — укажите **Всем сотрудникам**, если включаете подтверждение сразу на всю организацию, или **Выбранным сотрудникам**, если хотите настроить его персонально.
   - **Срок предупреждения** — время, которое отводится пользователям для настройки подтверждения входа. Когда этот период закончится, сотрудники больше не смогут отложить настройку.

   Метод проверки недоступен для редактирования. Приоритет отдается получению кода через звонок на телефон. Смс используется системой, только если звонок недоступен.
4. Нажмите кнопку **Включить**.
5. Если вы включаете подтверждение входа отдельным пользователям, выберите нужных сотрудников. Про выбор сотрудников
6. Если вы включаете подтверждение входа всем сотрудникам организации, вы можете принудительно выйти из аккаунтов всех пользователей.

Выйти из всех аккаунтов

Вы можете принудительно закрыть все сессии пользователей, если подтверждение входа распространяется на всех сотрудников организации: в разделе **Подтверждение входа** нажмите **Выйти из всех аккаунтов** и подтвердите выход. Обычно это делается сразу после того, как вы

включили подтверждение — так для продолжения работы сотрудникам потребуется заново войти в Яндекс 360 уже с окном настройки подтверждения входа.

> **Выход из сервисов выполняется для всех сотрудников с аккаунтами на домене организации**
>
> Если ваш аккаунт администратора создан на домене организации, то после выхода из всех аккаунтов вам также придется войти в кабинет организации заново.

В случае, когда подтверждение входа включено отдельным сотрудникам, кнопка **Выйти из всех аккаунтов** недоступна.

Выбрать сотрудников

Когда вы включаете подтверждение входа с настройкой **Выбранным сотрудникам**, код подтверждения будет запрашиваться только у пользователей из раздела **Сотрудники** внизу страницы. Просто отметьте нужных людей в этом списке. Вы можете пользоваться поиском по имени, фамилии или логину либо фильтрами:

- **Только администраторы**, чтобы видеть в списке только администраторов организации и сотрудников с ролями менеджеров.
- **Включено подтверждение входа**, чтобы видеть только тех, на кого подтверждение уже включено.

> **При включении персонального подтверждения входа для администратора действует правило «второй руки»**
>
> Включить себя в список сотрудников или исключить из него вы не можете. При наличии такой необходимости попросите другого администратора вашей организации сделать это.

Если подтверждение входа включено **Всем сотрудникам**, раздел **Сотрудники** игнорируется — код будет запрашиваться у всех.

Изменить

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Безопасность** → **Подтверждение входа**.
3. Нажмите **Редактировать**.
4. Измените необходимые настройки:
   - **Кому включить**. Если вы меняете настройку с **Всем сотрудникам** на **Выбранным сотрудникам**, то выбрать сотрудников вы сможете после сохранения. Про выбор сотрудников
   - **Срок предупреждения**. Когда этот период закончится, сотрудники не смогут отложить настройку подтверждения входа.
5. Нажмите кнопку **Сохранить**.

Отключить

После отключения подтверждения входа сотрудники смогут заходить в аккаунты, используя только пароль.

1. Откройте кабинет организации **admin.yandex.ru**.
2. Выберите в меню **Безопасность** → **Подтверждение входа**.
3. Если подтверждение входа включено только выбранным сотрудникам:
   3.1. Выключите подтверждение входа у каждого сотрудника, которому оно было настроено персонально.
   3.2. Задайте настройке **Кому включить** значение **Всем сотрудникам**.
4. Нажмите кнопку **Отключить** и подтвердите действие.

Управление авторизацией на устройствах сотрудника

Администраторы и менеджеры безопасности могут:

- Посмотреть, с каких устройств сотрудники организации вошли в сервисы Яндекс 360 для бизнеса.
- Самостоятельно выйти из аккаунта сотрудника на любом устройстве из списка.
- Завершить все сессии сотрудника сразу во всех сервисах Яндекс 360 для бизнеса.

Это может быть полезно, например, если есть подозрение на несанкционированный доступ к сервисам или когда вам нужно удалить активные сессии пользователя на устройстве, которое больше не используется.

> Этот инструмент доступен в тарифах для крупных организаций **Корпоративный** + **Безопасность** и **Корпоративный Максимум**. Чтобы узнать подробности, оставьте заявку: менеджер Яндекс 360 свяжется с вами, ответит на все вопросы и поможет с подключением. Оставить заявку

Просмотреть устройства с активной авторизацией

1. Откройте кабинет организации.
2. В меню слева выберите **Безопасность** → **Устройства и активность**.
3. В окне поиска начните вводить имя, фамилию или логин сотрудника, для которого хотите посмотреть информацию, и выберите нужного пользователя из выпадающего списка.

На экране появится список устройств с активной авторизацией сотрудника в программах, приложениях и веб-версиях сервисов Яндекс 360.

Выйти из аккаунта сотрудника

1. Откройте список устройств с активной авторизацией сотрудника по инструкции выше.
2. Выполните одно из действий:
   - Чтобы выйти из аккаунта сотрудника только на одном устройстве из списка, нажмите ✕ напротив названия этого устройства и подтвердите выход.
   - Чтобы завершить все активные сессии сотрудника, нажмите кнопку **Выйти на всех устройствах** внизу окна и подтвердите действие. В этом случае завершатся все без исключения сессии пользователя, в том числе и в веб-версиях сервисов.

После выхода компьютеры, телефоны или планшеты пользователя с завершенными сессиями исчезнут из списка авторизованных устройств. Чтобы снова войти в рабочий аккаунт, сотруднику нужно будет заново ввести логин и пароль на этих устройствах.

Интеграция Почты с внешними системами защиты от утечек

Эта возможность доступна в тарифах **Основной**, **Продвинутый** и всех версиях тарифа **Корпоративный** из новой линейки, а также тарифах **Оптимальный** и **Расширенный** из старой.

Для защиты исходящей почты от утечек в Яндекс 360 для бизнеса можно использовать внешние DLP-системы. DLP (Data Loss Prevention) — это технология, которая помогает обнаружить и предотвратить передачу сотрудниками конфиденциальной информации, такой как персональные данные, коммерческая тайна, интеллектуальная собственность и т. д.

Как это работает

После настройки интеграции вся исходящая почта сотрудников попадает в DLP-систему. DLP на основе заданных правил определяет, есть ли в отправляемых письмах данные, которые считаются конфиденциальными. Если нарушение обнаружено, система действует в соответствии со своими настройками: отправляет уведомления администратору безопасности, записывает событие во внутренний журнал аудита и т. д.

Также через DLP-систему при необходимости можно проверять входящую почту на наличие запрещенной информации, фишинга или спама.

Внимание

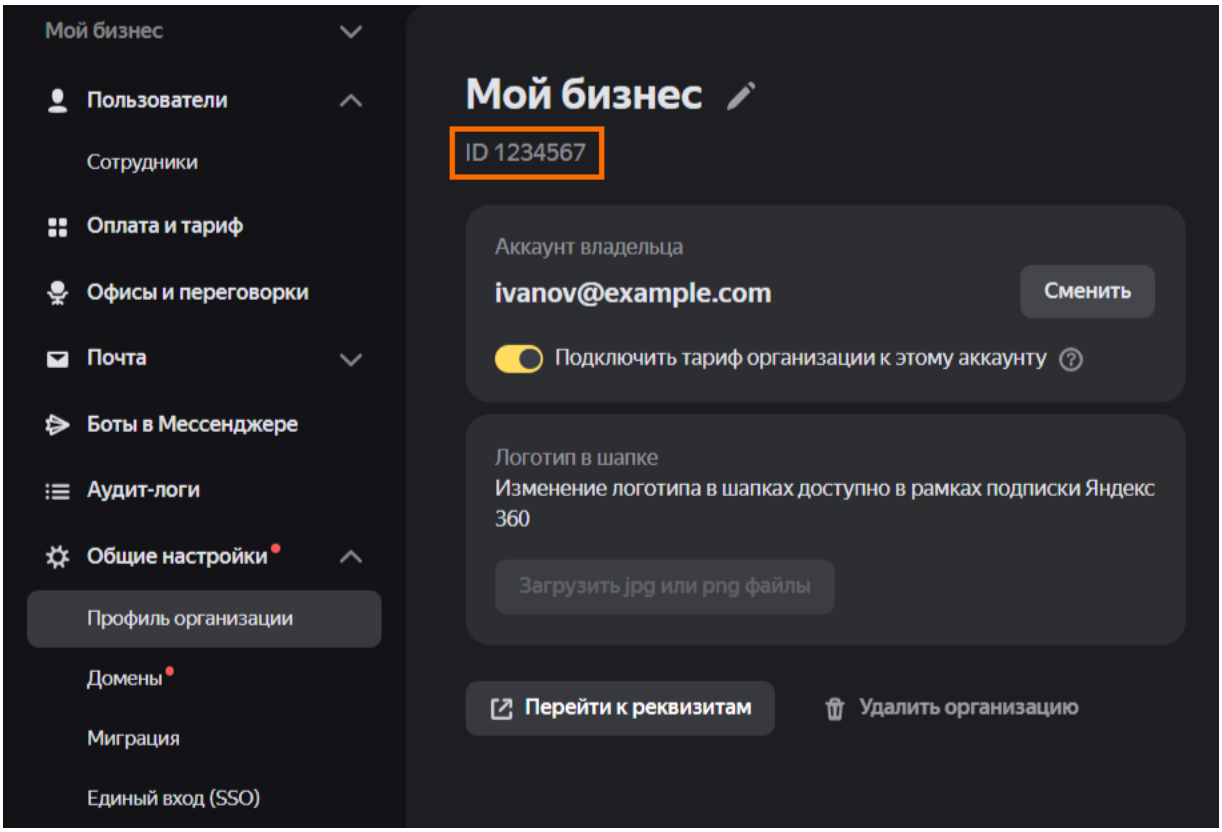
По умолчанию максимальное количество писем, которое может проходить в час через DLP-систему, — 10 000. Лимит действует на все письма в совокупности: и на исходящие, и на входящие. Чтобы увеличить лимит, обратитесь к вашему аккаунт-менеджеру.

Настройка взаимодействия с DLP

1. В вашей организации в Яндекс 360 для бизнеса создайте отдельного пользователя для работы с DLP-системой (например, с логином dlp). Как это сделать
2. Настройте пересылку *исходящей почты* всех сотрудников на ящик созданного dlp-пользователя. Для этого потребуется работа с API.
   2.1. Воспользуйтесь инструкцией на странице Доступ к API, чтобы получить OAuth-токен. При создании приложения выберите доступы `ya360_admin:mail_read_routing_rules` и `ya360_admin:mail_write_routing_rules`.

   Если OAuth-приложение уже создано, но у него нет нужных прав доступа, добавьте их. После сохранения изменений система предложит выпустить новый токен.
   2.2. Определите идентификатор вашей организации: откройте admin.yandex.ru и выберите **Общие настройки** → **Профиль организации**. Идентификатор будет указан под названием организации.

Скриншот



2.3. Получите список правил обработки писем, настроенных в вашей организации, чтобы обновить его.

2.3.1. Сформируйте и отправьте API-запрос на получение списка правил:

- HTTP-метод: `GET`
- URL запроса:

```
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mail/routing/rules
```

где `{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.2.

Пример

```
https://api360.yandex.net/admin/v1/org/1234567/mail/routing/rules
```

- Заголовок:

```
Authorization: OAuth {OAUTH-TOKEN}
```

где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 2.1.

Если вы работаете на Windows, то отправить запрос на получение списка правил обработки писем можно с помощью команды `curl` такого вида:

```
curl -X GET -H "Authorization: OAuth {OAUTH-TOKEN}"
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mail/routing/rules
```

где

`{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 2.1;
`{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.2.

Я не понимаю, как это сделать

4. Подготовьте команду: скопируйте пример в любой редактор, вставьте в указанные места токен и идентификатор организации.
5. Нажмите кнопку поиска на панели задач Windows, напишите в поисковой строке `cmd` и нажмите клавишу Enter.
6. Откроется окно «Командная строка». Вставьте в него готовую команду и нажмите Enter.

2.3.2. Проанализируйте полученный ответ:

- Если в списке нет ни одного правила обработки, переходите к следующему шагу.
- Если список непустой, скопируйте полученный ответ, в любом текстовом редакторе создайте файл, вставьте в него полученный код и сохраните его в формате JSON (например, с именем `rules-list.json`).

2.4. Подготовьте новый список правил. Порядок действий зависит от полученного ответа на предыдущий запрос.

В списке уже есть правила

Добавьте в начало списка правило пересылки исходящей почты на ящик dlp-пользователя:

6. В текстовом редакторе откройте файл `rules-list.json`.
7. После текста `{"rules":[` добавьте следующий код:

```
{"terminal":false,"condition":{},"actions":[{"data":
{"email":"dlp@domain.ru"},"action":"forward"}],"scope":
{"direction":"outbound"}},
```

где `dlp@domain.ru` — электронный адрес пользователя, созданного на шаге 1.

8. Сохраните файл с именем `rules-list-new.json`.

В списке пока нет правил

Создайте файл с именем `rules-list-new.json` со следующим содержимым:

```
{
  "rules": [
    {
```

```
      "terminal": false,
      "condition": {},
      "actions": [
        {
          "data": {
            "email": "dlp@domain.ru"
          },
          "action": "forward"
        }
      ],
      "scope": {
        "direction": "outbound"
      }
    }
  ]
}
```

где `dlp@domain.ru` — электронный адрес пользователя, созданного на шаге 1.

2.5. Сформируйте и отправьте API-запрос, который создает правило пересылки исходящей почты.

- HTTP-метод: `PUT`
- URL запроса:

```
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mail/routing/rules
```

где `{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.2.

- Заголовки:

  ```
  Authorization: OAuth {OAUTH-TOKEN}
  Content-Type: application/json
  ```

  где `{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 2.1.
- Тело запроса: содержится в файле `rules-list-new.json`, созданном на шаге 2.4.

Если вы работаете на Windows, то отправить запрос на создание правила пересылки можно с помощью команды `curl` такого вида:

```
curl -X PUT -H "Authorization: OAuth {OAUTH-TOKEN}" -H "Content-Type:
application/json" -d "@rules-list-new.json"
https://api360.yandex.net/admin/v1/org/{ОРГАНИЗАЦИЯ}/mail/routing/rules
```

где

`{OAUTH-TOKEN}` — OAuth-токен, полученный на шаге 2.1;

`rules-list-new.json` — файл с телом запроса, созданный на шаге 2.4;

`{ОРГАНИЗАЦИЯ}` — идентификатор организации, полученный на шаге 2.2.

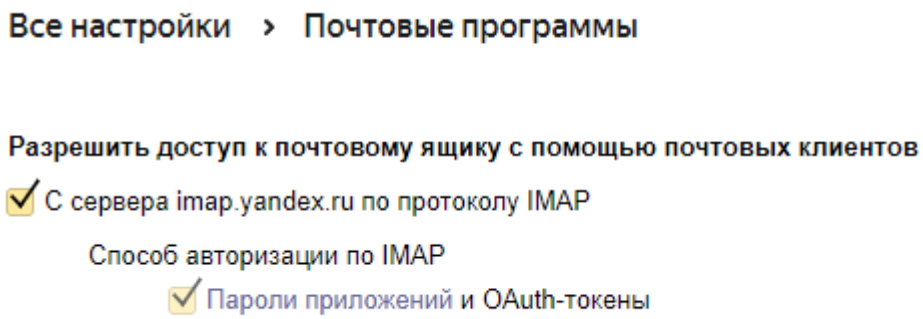
Я не понимаю, как это сделать

1. Подготовьте команду: скопируйте пример в любой редактор, вставьте в указанные места токен и идентификатор организации.
2. Откройте папку, в которой лежит файл `rules-list-new.json`.
3. Нажмите на пустое место в адресной строке.
4. Напишите туда `cmd` и нажмите клавишу Enter.
5. Откроется окно «Командная строка». Вставьте в него готовую команду и нажмите Enter.

2.6. Проверить, что правило создалось, можно, отправив API-запрос на просмотр правил обработки писем по инструкции из шага 2.3.

3. Чтобы проверять *входящую почту* на конфиденциальную информацию, для нее также настройте правила пересылки на ящик dlp-пользователя. Это можно сделать в интерфейсе Яндекс 360 для бизнеса по инструкции.
4. Настройте ящик dlp-пользователя для работы по протоколу IMAP:
   4.2. Откройте раздел Почтовые программы в настройках Яндекс Почты dlp-пользователя.
   4.3. В разделе **Разрешить доступ к почтовому ящику с помощью почтовых клиентов** выберите опции:
   - **С сервера imap.yandex.ru по протоколу IMAP**
   - **Способ авторизации по IMAP → Пароли приложений и OAuth-токены**

   Скриншот

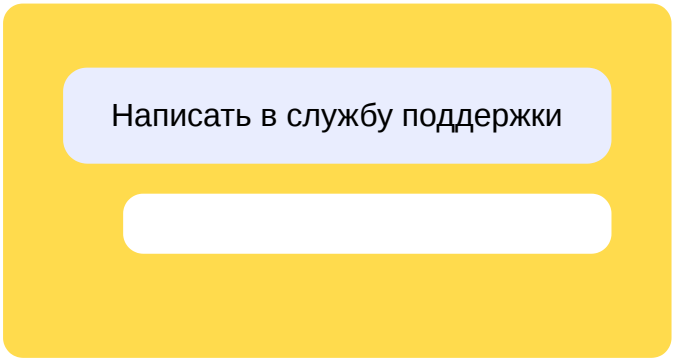


   4.4. Сохраните изменения.
5. Создайте пароль приложения для доступа к почтовому ящику dlp-пользователя:
   5.2. Откройте страницу Пароли приложений Яндекс ID dlp-пользователя.
   5.3. В разделе **Создать пароль приложения** нажмите ＋ в строке **Почта**.
   5.4. Придумайте название пароля, например dlp-access. С этим названием пароль будет отображаться в списке.
   5.5. Нажмите кнопку **Далее** — на экране появится созданный пароль. Скопируйте и сохраните его.

> **Внимание**
>
> Пароль можно увидеть только один раз. Если вы не сохранили его и закрыли окно, удалите текущий пароль и создайте новый.

6. Во внешней DLP-системе настройте подключение к ящику dlp-пользователя по IMAP с использованием полученного пароля приложений. Общие параметры настройки:
   - Адрес почтового сервера — `imap.yandex.ru`.
   - Защита соединения — `SSL`.
   - Порт — `993`.

За подробной инструкцией по настройке обратитесь к документации или поддержке производителя DLP-системы.



Сервисные приложения

Эта возможность доступна в тарифах **Основной**, **Продвинутый** и всех версиях тарифа **Корпоративный** из новой линейки, а также тарифах **Оптимальный** и **Расширенный** из старой.

При переходе на **Минимальный** или **Базовый** тариф управлять приложениями не получится — в течение месяца можно будет только очистить их список. Когда месяц закончится, приложения будут удалены из организации.

Сервисные приложения используются, чтобы управлять ресурсами пользователей в организации по API. Например, с их помощью вы сможете создать резервную копию писем или управлять событиями в Календаре пользователя. Всего можно создать до 20 сервисных приложений.

Внимание

Согласно пункту 3.7 оферты, после подключения доступа администратор обязан уведомить об этом всех пользователей и при необходимости получить их письменное согласие (если они не давали его ранее).

Подключение сервисных приложений

1. Войдите в аккаунт владельца организации.
2. Зарегистрируйте приложение, которое будет управлять списком сервисных приложений в организации.
   2.1. Откройте страницу создания OAuth-приложения.
   2.2. Укажите название вашего сервиса и при необходимости прикрепите иконку.
   2.3. В блоке **Платформы приложения** выберите **Веб-сервисы**. В поле **Redirect URI** нажмите ссылку **Подставить URL для отладки**.
   2.4. В разделе **Доступ к данным** укажите права доступа, которые необходимы для управления сервисными приложениями в организации:
      - `ya360_security:service_applications_read` — чтение списка сервисных приложений;
      - `ya360_security:service_applications_write` — управление списком сервисных приложений (чтение и запись).
   2.5. Добавьте электронную почту для связи. Внизу страницы нажмите **Создать приложение**. На экране появятся его описание.
   2.6. Скопируйте идентификатор приложения из поля **ClientID** — он потребуется для получения OAuth-токена. В дальнейшем открыть страницу со всеми вашими приложениями вы сможете по ссылке oauth.yandex.ru/.
3. Запросите OAuth-токен любым подходящим способом. Он понадобится для дальнейшей регистрации всех сервисных приложений в организации.

Отладочный OAuth-токен можно получить вручную:

3.1. Перейдите по ссылке

```
https://oauth.yandex.ru/authorize?response_type=token&client_id=
<main_app_client_id>
```

Вместо `<main_app_client_id>` подставьте значение **ClientID** из п. 2.6.

3.2. Если OAuth-токен вашему приложению выдается впервые, откроется экран авторизации. После входа Яндекс OAuth перенаправит вас на страницу с токеном. Подробнее об отладочных токенах.

4. Уведомите пользователей и получите от них согласие, если они не давали его ранее, на доступ администратора к управлению их ресурсами согласно пункту 3.7 оферты.
5. Активируйте функцию сервисных приложений с помощью запроса:

```
POST
https://api360.yandex.net/security/v1/org/<org_id>/service_applications/activate
```

Вместо `<org_id>` подставьте идентификатор вашей организации.

6. Зарегистрируйте сервисное приложение. С его помощью можно будет получать временные OAuth-токены пользователей. Срок действия временного токена — 1 час.

6.1. Создайте отдельное OAuth-приложение по аналогии с созданием основного приложения (п. 2). В качестве прав доступа этого приложения укажите те, которые будут использоваться в API-запросах .

6.2. Сделайте приложение из предыдущего шага сервисным для организации.

Пример

```
curl --location \
--request POST
'https://api360.yandex.net/security/v1/org/<org_id>/service_applications'
\
--header 'Authorization: OAuth <owner_token_to_manage_service_app>' \
--header 'Content-Type: application/json' \
--data-raw '{ \
  "applications": [ \
    { \
      "id": "<OAuth_service_app_client_id>", \
      "scopes": [ \
        "cloud_api:disk.app_folder", \
        "cloud_api:disk.read", \
        "cloud_api:disk.write", \
        "cloud_api:disk.info" \
      ] \
    } \
  ] \
}'
```

В код подставьте значения:

- `<org_id>` — идентификатор вашей организации;
- `<owner_token_to_manage_service_app>` — OAuth-токен из п. 3;
- `<OAuth_service_app_client_id>` — **ClientID** сервисного приложения из п. 6.1.

6.3. Проверьте, что приложение добавилось как сервисное корректно.

Пример

```
curl --location  \
--request GET
'https://api360.yandex.net/security/v1/org/<org_id>/service_applications'
\
--header 'Authorization: OAuth <owner_token_to_manage_service_app>'
```

Чтобы подключить другие сервисные приложения, повторите шаги п. 6.

7. Получите временный токен пользователя. Это можно сделать с помощью API-запроса:

```
POST /token HTTP/1.1
   Host: http://oauth.yandex.ru
   Content-type: application/x-www-form-urlencoded
```

Пример

```
curl --location \
--request POST 'https://oauth.yandex.ru/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'grant_type=urn:ietf:params:oauth:grant-type:token-exchange'
\
--data-urlencode 'client_id=<OAuth_service_app_client_id>' \
--data-urlencode 'client_secret=<OAuth_service_app_client_secret>' \
--data-urlencode 'subject_token=<user_id>' \
--data-urlencode 'subject_token_type=urn:yandex:params:oauth:token-type:uid'
```

или

```
curl --location
--request POST 'https://oauth.yandex.ru/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'grant_type=urn:ietf:params:oauth:grant-type:token-exchange'
\
--data-urlencode 'client_id=<OAuth_service_app_client_id>' \
--data-urlencode 'client_secret=<OAuth_service_app_client_secret>' \
--data-urlencode 'subject_token=<user_email>' \
```

```
--data-urlencode 'subject_token_type=urn:yandex:params:oauth:token-
type:email'
```

В код подставьте значения:

- `<OAuth_service_app_client_id>` — **ClientID** сервисного приложения из п. 6.1.
- `<OAuth_service_app_client_secret>` — **Client secret** сервисного приложения;
- `<user_id>` — идентификатор пользователя, для которого необходимо получить токен;
- `<user_email>` — электронный адрес пользователя, для которого необходимо получить токен, вида `username@domain.ru`.

Ответ будет содержать токен, который надо использовать в запросах к API сервисов Яндекс 360.

Подробнее программная работа с сервисными приложениями описана в Справочнике API 360.

Примеры запросов для работы с ресурсами пользователей

Временные токены, полученные с помощью сервисных приложений, позволяют обращаться по API к некоторым ресурсам пользователей в организации, например для бэкапа данных, аудита или поиска информации.

Яндекс Диск

API Яндекс Диска предназначен для работы с файлами и управления доступом к ним. Вы можете направлять запросы к API Диска при помощи сервиса Полигон.

Пример

Запрос метаинформации о Диске сотрудника:

```
curl --request GET 'https://cloud-api.yandex.net/v1/disk' \
--header 'Accept: application/json' \
--header 'Authorization: OAuth <oauth_token>'
```

Вместо `<oauth_token>` подставьте значение временного токена пользователя из п. 7.

Подробнее о работе с REST-API Диска.

Яндекс Почта

Приложения могут получать доступ к ящикам Яндекс Почты по протоколу OAuth. OAuth-авторизацию поддерживают IMAP- и SMTP-серверы Яндекс Почты.

Пример

Скрипт Python для подсчета писем у пользователя по протоколу IMAP:

```
import imaplib

def generate_oauth2_string(username, access_token):
    auth_string = 'user=%s\1auth=Bearer %s\1\1' % (username, access_token)
    return auth_string

def get_imap_connector(username="<user_email>", token="<oauth_token>"):
    auth_string = generate_oauth2_string(username, token)
    imap_connector = imaplib.IMAP4_SSL("imap.yandex.com", 993)
    imap_connector.authenticate('XOAUTH2', lambda x: auth_string)
    return imap_connector

def get_total_emails(imap_connector):
    mailboxes = []
    ttl_emails = 0
    for mailbox in imap_connector.list()[1]:
        mailboxes.append(mailbox.decode("utf-8").split()[-1].replace('"',
''))
        for mailbox in mailboxes:
            try:
                imap_connector.select(mailbox)
                resp_code, mail_count =
imap_connector.select(mailbox=mailbox, readonly=True)
                ttl_emails += int(mail_count[0].decode("utf-8"))
            except imaplib.IMAP4.error:
                print(f"Folder: {folder} Error reading emails")
            except ValueError:
                print(f"Folder: {folder} Error reading emails")
    user_logout(imap_connector)
    return ttl_emails

get_total_emails(get_imap_connector())
```

В код подставьте значения:

- `<user_email>` — электронный адрес пользователя, для которого необходимо получить данные, вида `username@domain.ru`;
- `<oauth_token>` — временный токен пользователя из п. 7.

Подробнее о работе почтовых протоколов см. в описании IMAP и в спецификации SMTP.

Яндекс Календарь

С использованием OAuth-токенов можно взаимодействовать с Яндекс Календарем пользователей по протоколу CalDAV.

Пример 1

Скрипт Python для удаления выбранного Календаря пользователя:

```
import caldav

def get_principal(username, leg_token):
    client = caldav.DAVClient(url="https://caldav.yandex.ru/",
username=username, password=leg_token)
    principal = client.principal()
    return principal

my_principal = get_principal("<user_email>", "<oauth_token>")

def find_delete_calendar(my_principal, calendar_name="Мой календарь"):
    try:
        calendar = my_principal.calendar(name=calendar_name)
        assert calendar
        print(f"We found an existing calendar with name {calendar_name}, now
deleting it")
        calendar.delete()
    except caldav.error.NotFoundError:
        print("Calendar was not found")

find_delete_calendar(my_principal)
```

В код подставьте значения:

- `<user_email>` — электронный адрес пользователя вида `username@domain.ru`, для которого необходимо получить данные;
- `<oauth_token>` — временный токен пользователя из п. 7.

> **Примечание**
>
> Если администратор удалит календарь пользователя, восстановить его в дальнейшем не сможет ни администратор, ни сам пользователь.

Пример 2

Запросы создания встречи в Календаре со ссылкой на видеовстречу в Телемосте:

- Конференция для одиночного события.

  Создание

```
curl -v "https://caldav.yandex.ru/calendars/<user_email>/events-
default/<event_uid>.ics" \
-H "Authorization: OAuth <oauth_token>" \
-H "Content-type: text/ics" \
-X PUT \
--data-binary "
```

```
BEGIN:VCALENDAR
BEGIN:VEVENT
X-TELEMOST-REQUIRED:TRUE
DESCRIPTION:Single event
UID:<event_uid>
DTSTART:20230417T120000Z
END:VEVENT
END:VCALENDAR"
```

В код подставьте значения:

- `<user_email>` — электронный адрес пользователя, для которого необходимо получить данные, вида `username@domain.ru`;
- `<event_uid>` — идентификатор встречи и имени файла (например, `a5e3e7b0-dd11-11ed`);
- `<oauth_token>` — временный токен пользователя из п. 7.

Пример успешного ответа:

```
HTTP/1.1 201 Created
```

Получение

```
curl -v "https://caldav.yandex.ru/calendars/<user_email>/events-
default/<event_uid>.ics" \
  -H "Authorization: OAuth <oauth_token>"
```

В код подставьте значения:

- `<user_email>` — электронный адрес пользователя вида `username@domain.ru`, для которого необходимо получить данные;
- `<event_uid>` — идентификатор встречи и имени файла (например, `a5e3e7b0-dd11-11ed`);
- `<oauth_token>` — временный токен пользователя из п. 7.

Пример успешного ответа:

```
HTTP/1.1 200 OK
BEGIN:VCALENDAR
...
BEGIN:VEVENT
DTSTART:20230417T120000Z
DTEND:20230417T120000Z
SUMMARY:Без названия
UID:a5e3e7b0-dd11-11ed
DESCRIPTION:Link to video conference:
https://telemost.yandex.ru/j/78566269088286\n\nSingle event
X-TELEMOST-CONFERENCE:https://telemost.yandex.ru/j/78566269088286
```

```
...
END:VEVENT
END:VCALENDAR
```

- Конференция для повторяющегося события.

  Создание

  ```
  curl -v "https://caldav.yandex.ru/calendars/<user_email>/events-
  default/<event_uid>.ics" \
  -H "Authorization: OAuth <oauth_token>" \
  -H "Content-type: text/ics" \
  -X PUT \
  --data-binary "
  BEGIN:VCALENDAR
  BEGIN:VEVENT
  X-TELEMOST-REQUIRED:TRUE
  DESCRIPTION:Weekly event
  UID:<event_uid>
  DTSTART:20230411T200000Z
  RRULE:FREQ=WEEKLY
  END:VEVENT
  END:VCALENDAR"
  ```

  В код подставьте значения:

  - `<user_email>` — электронный адрес пользователя вида `username@domain.ru`, для которого необходимо получить данные;
  - `<event_uid>` — идентификатор встречи и имени файла (например, `a5e3e7b0-dd11-11ed`);
  - `<oauth_token>` — временный токен пользователя из п. 7.

  Пример успешного ответа:

  ```
  HTTP/1.1 201 Created
  ```

  Получение

  ```
  curl -v "https://caldav.yandex.ru/calendars/<user_email>/events-
  default/<event_uid>.ics" \
    -H "Authorization: OAuth <oauth_token>"
  ```

  В код подставьте значения:

  - `<user_email>` — электронный адрес пользователя вида `username@domain.ru`, для которого необходимо получить данные;

- `<event_uid>` — идентификатор встречи и имени файла (например, `a5e3e7b0-dd11-11ed`);
- `<oauth_token>` — временный токен пользователя из п. 7.

Пример успешного ответа:

```
BEGIN:VCALENDAR
...
BEGIN:VEVENT
RECURRENCE-ID:20230411T200000Z
X-TELEMOST-CONFERENCE:https://telemost.yandex.ru/j/39864310386563
DESCRIPTION:Ссылка на видеовстречу:
https://telemost.yandex.ru/j/39864310386563\n\nWeekly event
...
END:VEVENT
BEGIN:VEVENT
RRULE:FREQ=WEEKLY;BYDAY=TU;INTERVAL=1
DESCRIPTION:Ссылка на видеовстречу:
https://telemost.yandex.ru/j/39864310386563\n\nWeekly event
...
END:VEVENT
```

При отправке `PUT`-запроса для создания или изменения события в Календаре клиент добавляет внутрь компонентов `VEVENT` нестандартное свойство `X-TELEMOST-REQUIRED`. Сервер, получая такой запрос, генерирует ссылку на видеовстречу в Телемосте и добавляет ее в описание встречи в виде текста.

При чтении клиентом встреч сервер не указывает свойство `X-TELEMOST-REQUIRED`. Но, если ссылка на видеовстречу в Телемосте была сгенерирована, возвращает эту ссылку в нестандартном свойстве `X-TELEMOST-CONFERENCE`.

Подробнее о работе с протоколом CalDAV см. в его спецификации.

Написать в службу поддержки

Сценарии использования API для решения задач информационной безопасности

Администраторы Яндекс 360 для бизнеса могут управлять настройками, которые помогают решать задачи информационной безопасности в компании. Большинство таких настроек можно осуществлять в том числе через API.

Основные API-сценарии, которые могут использоваться подразделениями безопасности:

- Настройки антиспама: создать, изменить или удалить белый список отправителей, который содержит разрешенные IP-адреса и CIDR-подсети.
- Аудит-лог Диска: просмотреть список событий в аудит-логе Диска организации.
- Аудит-лог Почты: просмотреть список событий в аудит-логе Почты организации.
- Двухфакторная аутентификация: включить или выключить 2FA для всех пользователей домена.
- Сброс телефона для 2FA: удалить номер телефона, который используется сотрудником для проведения двухфакторной аутентификации.
- Выход из аккаунта: выйти из аккаунта определенного пользователя на всех устройствах, где есть незавершенные сеансы.
- Время жизни cookie: изменить время жизни cookie-сессий пользователей.
- Параметры парольной политики: просмотреть или настроить параметры парольной политики организации. Например, срок действия паролей и возможность их самостоятельной смены пользователями.
- Транспортные правила Почты: создать правила обработки входящих писем, имеющие приоритет над пользовательскими правилами. Например, возможность настроить пересылку копии писем, соответствующих определенному критерию, на заданный адрес или запретить доставку писем от определенных отправителей.
- Правила автоответа или пересылки: создать правила автоответа на письма, адресованные сотруднику, или правила их пересылки на другие ящики на домене организации.
- Информация о сотруднике: просмотреть данные о сотруднике (например, наличие роли администратора, статус аккаунта — активный или заблокированный) либо изменить их (например, сбросить пароль, установить признак необходимости смены пароля при первом входе).

Примечание

Полный перечень доступных операций содержится в документации API Яндекс 360 для разработчиков.

Реестр отечественного ПО

Каждый продукт Яндекс 360 для бизнеса занесен в Реестр отечественного программного обеспечения. Посмотреть записи о продуктах можно по ссылкам в таблице.

Продукт	Страна	Запись в реестре	Ссылка
Яндекс Почта	РФ	№ 13555 от 20.05.2022 г.	https://reestr.digital.gov.ru/reestr/745547
Приложение Яндекс Почта для Android	РФ	№ 6863 от 16.07.2020 г.	https://reestr.digital.gov.ru/reestr/308213
Приложение Яндекс Почта для iOS	РФ	№ 6862 от 16.07.2020 г.	https://reestr.digital.gov.ru/reestr/308212
Яндекс Диск	РФ	№ 13635 от 20.05.2022 г.	https://reestr.digital.gov.ru/reestr/745736
Программа Яндекс Диск для Windows	РФ	№ 12152 от 30.11.2021 г.	https://reestr.digital.gov.ru/reestr/469095
Программа Яндекс Диск для macOS	РФ	№ 12266 от 14.12.2021 г.	https://reestr.digital.gov.ru/reestr/478081
Приложение Яндекс Диск для Android	РФ	№ 6954 от 01.09.2020 г.	https://reestr.digital.gov.ru/reestr/308304

Приложение Яндекс Диск для iOS	РФ	№ 6953 от 01.09.2020 г.	https://reestr.digital.gov.ru/reestr/308303
Яндекс Документы	РФ	№ 13554 от 20.05.2022 г.	https://reestr.digital.gov.ru/reestr/745545
Яндекс Телемост	РФ	№ 13556 от 20.05.2022 г.	https://reestr.digital.gov.ru/reestr/745549
Программа Яндекс Телемост для Windows	РФ	№ 15241 от 21.10.2022 г.	https://reestr.digital.gov.ru/reestr/1081441
Программа Яндекс Телемост для macOS	РФ	№ 13300 от 15.04.2022 г.	https://reestr.digital.gov.ru/reestr/685400
Приложение Яндекс Телемост для Android	РФ	№ 12150 от 30.11.2021 г.	https://reestr.digital.gov.ru/reestr/469091
Приложение Яндекс Телемост для iOS	РФ	№ 13547 от 20.05.2022 г.	https://reestr.digital.gov.ru/reestr/745530
Яндекс Трекер	РФ	№ 5255 от 26.02.2019 г.	https://reestr.digital.gov.ru/reestr/306605
Приложение Яндекс Трекер для Android	РФ	№ 4789 от 26.11.2018 г.	https://reestr.digital.gov.ru/reestr/306139

Приложение Яндекс Трекер для iOS	РФ	№ 5115 от 10.01.2019 г.	https://reestr.digital.gov.ru/reestr/306465
Яндекс Календарь	РФ	№ 14087 от 01.07.2022 г.	https://reestr.digital.gov.ru/reestr/827607
Яндекс Мессенджер	РФ	№ 14033 от 28.06.2022 г.	https://reestr.digital.gov.ru/reestr/819108/
Программа Яндекс Мессенджер для Windows	РФ	№ 13672 от 01.06.2022 г.	https://reestr.digital.gov.ru/reestr/767866
Программа Яндекс Мессенджер для macOS	РФ	№ 14032 от 28.06.2022 г.	https://reestr.digital.gov.ru/reestr/819106
Приложение Яндекс Мессенджер для Android	РФ	№ 12151 от 30.11.2021 г.	https://reestr.digital.gov.ru/reestr/469093
Приложение Яндекс Мессенджер для iOS	РФ	№ 13557 от 20.05.2022 г.	https://reestr.digital.gov.ru/reestr/745551
Яндекс Рассылки	РФ	№ 13630 от 20.05.2022 г.	https://reestr.digital.gov.ru/reestr/745722

Обработка персональных данных в соответствии со 152-ФЗ

В России действует Федеральный закон «О персональных данных» (152-ФЗ). Он регламентирует, каким образом организации должны обрабатывать персональные данные своих сотрудников, клиентов, контрагентов и других лиц.

Яндекс 360 обрабатывает любые данные, полученные от клиентов, в строгом соответствии с этим законом:

- В дата-центрах используются современные и надежные технологии защиты данных.
- Внутренние регламенты и процессы в Яндексе устроены так, чтобы предотвратить любой несанкционированный доступ к клиентским данным.
- Яндекс 360 хранит данные в дата-центрах, расположенных на территории России. Использование сервисов Яндекс 360 не требует от клиентов никаких мер по локализации данных.

Внимание

Ваша организация остается **оператором персональных данных**, которые обрабатываются с использованием сервисов Яндекс 360. Использование сервисов Яндекс 360 не освобождает вас от обязанности соблюдать требования 152-ФЗ, которые могут применяться к вам как к самостоятельному оператору.

Памятка: что значит быть оператором персональных данных

Для соблюдения 152-ФЗ при внедрении продуктов Яндекс 360 в процессы компании мы рекомендуем принять следующие меры:

- Оцените бизнес-процессы, включающие обработку персональных данных, и наведите в них порядок: определите цели и порядок обработки, состав обрабатываемых данных, места и форму хранения. Убедитесь, что имеются законные основания для обработки персональных данных.
- Разработайте локальные документы, регулирующие обработку и защиту персональных данных, — публичную политику и внутренние инструкции. Политику разместите на сайтах и в приложениях организации.
- Оцените возможный ущерб субъектам персональных данных. Проведите моделирование угроз безопасности персональных данных в информационных системах.
- Назначьте ответственного за организацию обработки персональных данных.
- Подайте уведомление об обработке данных в Роскомнадзор, если еще этого не делали.

Подробности

Подробнее с условиями обработки персональных данных в сервисах Яндекс 360 вы можете ознакомиться в разделе 11 оферты и в Соглашении об обработке данных.

Субъект персональных данных — это человек, к которому они, собственно, относятся. Например, клиент или сотрудник.

Федеральная служба по техническому и экспортному контролю.

Стандарт безопасности ISO/IEC 27001

У Яндекс Почты, Диска, Мессенджера, Телемоста и Календаря есть сертификат соответствия стандарту ISO/IEC 27001:2022. Это международный стандарт обеспечения информационной безопасности. Он устанавливает требования к внедрению, поддержанию и непрерывному улучшению соответствующих процессов.

Согласно данным независимого аудита Почта, Диск, Мессенджер, Телемост и Календарь соответствуют требованиям стандарта. Например:

- заранее находят возможные проблемы и избегают их;
- достаточно финансируют направление информационной безопасности, чтобы поддерживать систему и оперативно защищаться от новых угроз;
- обучают сотрудников работать с конфиденциальными данными и проверяют, что знания применяются на практике;
- исключают несанкционированный доступ к данным, в том числе со стороны сотрудников;
- используют надежные технологии защиты данных.

Скачать сертификат на русском

Скачать сертификат на английском

Как подключить

Если у вас подключен и настроен поставщик удостоверений, вы можете подключить его к Яндекс 360. Для этого нужно настроить вашу федерацию удостоверений, а затем — сам Яндекс 360 для бизнеса.

Требования к организации

Эта возможность доступна в тарифах **Основной**, **Продвинутый** и всех версиях тарифа **Корпоративный** из новой линейки, а также тарифах **Оптимальный** и **Расширенный** из старой.

Прежде чем перейти к настройке единого входа (SSO), убедитесь, что в вашей организации:

- Подключен тариф, в котором доступен SSO.
- Подключен домен.
- Нет аккаунтов сотрудников, созданных на домене организации. Доменные аккаунты сотрудников — аккаунты с адресами вида `login@example.com`, где `@example.com` — имя вашей организации (домен). Такие аккаунты добавляются администратором организации вручную в разделе **Пользователи** → **Сотрудники**.

Шаг 1. Настройте федерацию удостоверений

Чтобы ваша федерация удостоверений смогла взаимодействовать с Яндекс 360, ее нужно настроить.

О том, как это сделать для разных поставщиков удостоверений, читайте в разделах:

- Настройка Active Directory
- Настройка Azure Active Directory
- Настройка Keycloak версии 18
- Настройка Keycloak версии 19 и выше
- Настройка Avanpost FAM
- Настройка Multifactor

Убедитесь, что ваш поставщик удостоверений совместим со службой каталога, которую вы используете. Совместимости приведены в таблице.

Служба каталога	Поставщик удостоверений

Microsoft Active Directory	• Microsoft AD FS • Keycloak • Avanpost FAM • Multifactor
Samba DC	• Keycloak • Avanpost FAM • Multifactor
Red ADM	• Keycloak • Avanpost FAM • Multifactor

ALD Pro	• Keycloak • Avanpost FAM • Multifactor
FreeIPA	• Keycloak • Avanpost FAM • Multifactor

документацией. Вы также можете
укажите следующие параметры:

`it` .

й чертой в конце).

русском языке, дополнительно
ых точек (Endpoints) с привязкой

ля английского;

я казахского;

я узбекского;

– для турецкого.

- `https://passport.yandex.co.il/auth/sso/commit`
- `https://passport.yandex.com/auth/sso/commit`
- `https://passport.yandex.com.am/auth/sso/commit`
- `https://passport.yandex.com.ge/auth/sso/commit`
- `https://passport.yandex.com.tr/auth/sso/commit`
- `https://passport.yandex.ee/auth/sso/commit`
- `https://passport.yandex.eu/auth/sso/commit`
- `https://passport.yandex.fi/auth/sso/commit`
- `https://passport.yandex.fr/auth/sso/commit`
- `https://passport.yandex.kg/auth/sso/commit`
- `https://passport.yandex.kz/auth/sso/commit`
- `https://passport.yandex.lt/auth/sso/commit`
- `https://passport.yandex.lv/auth/sso/commit`
- `https://passport.yandex.md/auth/sso/commit`
- `https://passport.yandex.pl/auth/sso/commit`
- `https://passport.yandex.ru/auth/sso/commit`
- `https://passport.yandex.tj/auth/sso/commit`
- `https://passport.yandex.tm/auth/sso/commit`
- `https://passport.yandex.uz/auth/sso/commit`

Также получите URL-адрес страницы входа, ID вашего поставщика удостоверений и проверочный сертификат X.509. Они пригодятся вам на следующем шаге.

Шаг 2. Настройте Яндекс 360 для бизнеса

1. Откройте Яндекс 360 для бизнеса.
2. Перейдите в раздел **Общие настройки → Единый вход (SSO)**.
3. Нажмите **Настроить**.
4. Заполните поля с обязательными параметрами:
   - **URL страницы входа** — URL-адрес конечной точки SAML 2.0.
   - **Издатель поставщика удостоверений** — ID субъекта IdP.
   - **Проверочный сертификат** — сертификат от поставщика удостоверений.

     Если текущий сертификат скоро истекает, вы можете добавить второй ему на замену — для этого нажмите **Добавить второй сертификат для обновления**.
5. Для синхронизации учетных записей из каталогов LDAP: чтобы обновлять список сотрудников в Яндекс 360 автоматически, настройте синхронизацию и укажите ID вашего приложения в блоке **Синхронизация SCIM**.
6. Сохраните изменения.
7. Нажмите **Включить**.

Шаг 3. Проверьте аутентификацию

1. Откройте браузер в режиме гостя или инкогнито.
2. Перейдите на страницу passport.yandex.ru/auth, введите логин учетной записи из поставщика удостоверений и нажмите **Войти**. Если все настроено верно, вы будете перенаправлены на страницу входа, которую указали на шаге 2.

Отладка и устранение проблем

Если в процессе настройки поставщика удостоверений заданы неверные значения, то при попытке входа через SSO вы увидите сообщение «Авторизация не удалась» и код ошибки:

email.no_in_response

Указывайте имена атрибутов в формате `User.Firstname`, `User.Surname`, `User.EmailAddress`. Если задать другой формат, например `Firstname`, авторизоваться не получится.

request_your_admin

Ошибка появляется, если администратор каталога пользователей вашей организации ограничил для аккаунта доступ к Яндекс 360. За подробной информацией обратитесь к специалистам технической поддержки вашей организации.

samlresponse.invalid

Ошибка возникает, если неверно указаны URL страницы входа, издатель поставщика удостоверений или проверочный сертификат. Также она может возникнуть в течение 14 дней до истечения проверочного сертификата или после его истечения. Проверьте корректность настроек SSO в Яндекс 360 для бизнеса.

unsupportable_domain

Проверьте, что домен из почтового атрибута `User.EmailAddress` в SAML response такой же, как и основной домен или один из доменов-алиасов организации Яндекс 360.

SAML-tracer для устранения неполадок

SAML-tracer — это расширение браузера, которое отслеживает SAML-события, помогает найти и исправить ошибки при настройке единого входа (SSO). Отчет о проверке можно экспортировать в файл `JSON`.

Установка и запуск

Установите расширение по ссылке:

- SAML-tracer — для Яндекс Браузера, Google Chrome и Microsoft Edge;
- SAML-tracer — для Mozilla Firefox.

Чтобы запустить SAML-tracer, нажмите на значок на панели расширений браузера или комбинацию `Alt` + `Shift` + `S` на клавиатуре.

Отслеживание SAML-событий

1. Откройте браузер в режиме гостя или инкогнито и запустите SAML-tracer. Если значок отсутствует или окно SAML-tracer не открылось, в настройках расширения включите **Разрешить использование в режиме инкогнито**.
2. Перейдите на страницу passport.yandex.ru/auth, введите логин учетной записи из поставщика удостоверений и нажмите **Войти**. В окне SAML-tracer появятся записи `GET` и `POST`, SAML-события будут выделены оранжевым цветом и меткой.
3. Чтобы проверить атрибуты и их значения, выберите запись с SAML-событием и перейдите на вкладку **SAML** на панели предварительного просмотра.

Экспорт отчета в файл

1. Выберите запись с SAML-событием.
2. Нажмите **Export** на панели инструментов SAML-tracer.
3. Чтобы скрыть конфиденциальную информацию, выберите **Mask values**.
4. Нажмите **Export**. Файл в формате `JSON` скачается на ваш компьютер.

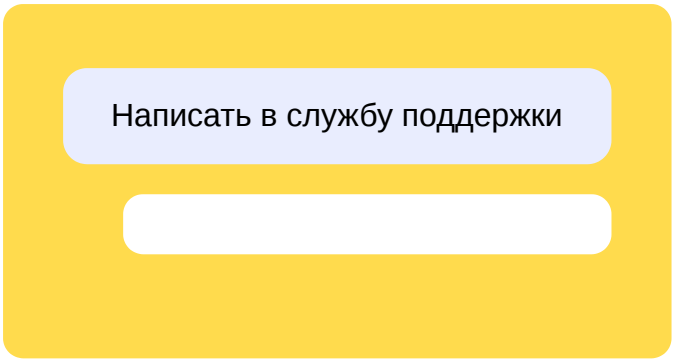
Ограничения при включенном едином входе (SSO)

После того как вы включите единый вход (SSO), для организации станут недоступны импорт сотрудников и перемещение отделов.

Если вы также подключили утилиту ADSCIM, будет отключено управление почтовыми алиасами через интерфейс Яндекс 360 для бизнеса.

Если в Яндекс 360 для бизнеса вы используете несколько организаций и решили подключить единый вход (SSO), то он включится одновременно для всех организаций.

Выключение единого входа (SSO) работает аналогично. Если в одной из организаций вы перейдете на Минимальный или Базовый тариф, единый вход отключится в этой организации и в других.


Написать в службу поддержки

Настройка Active Directory

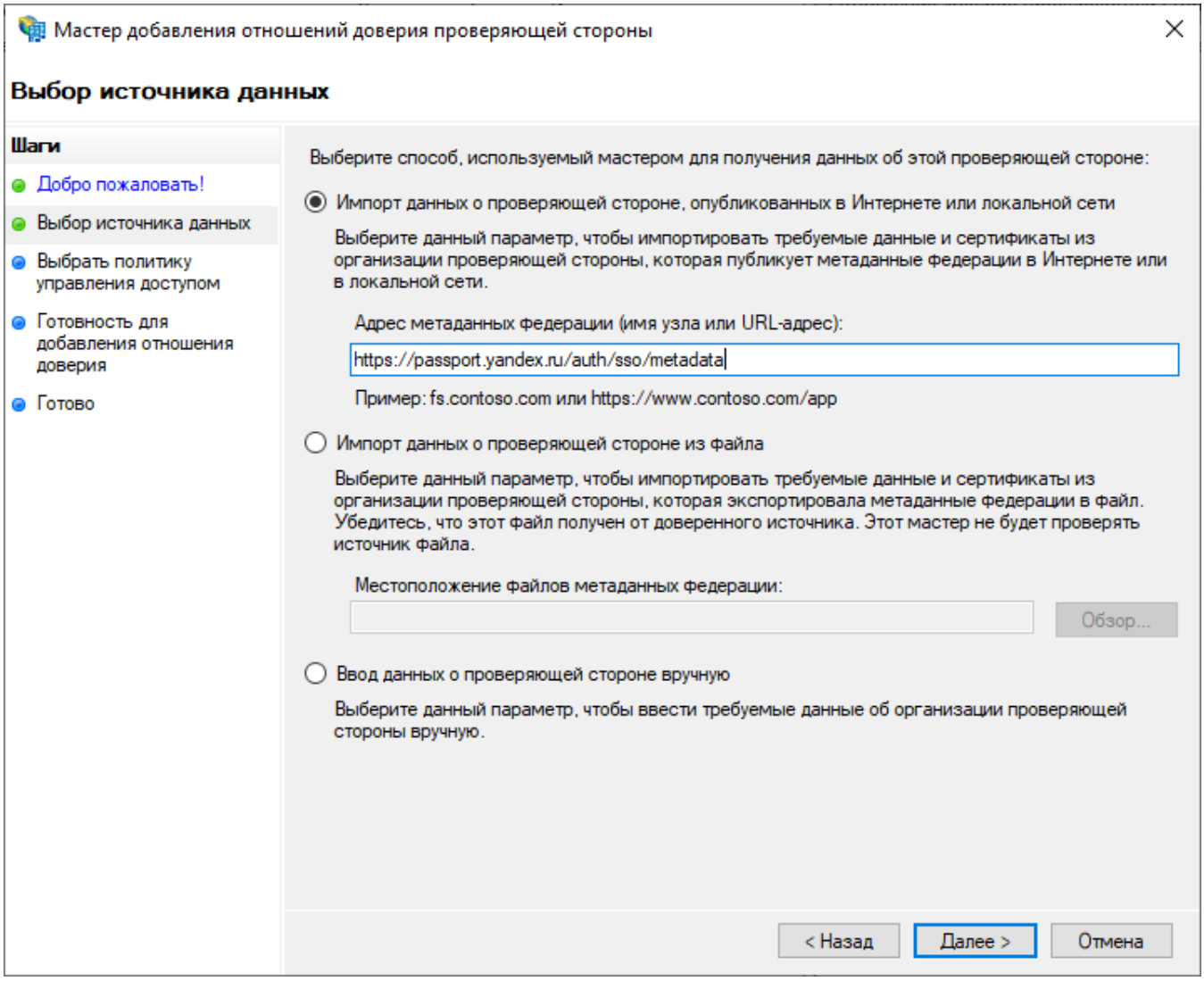
Если вы используете интерфейс Active Directory на английском языке, воспользуйтесь этой инструкцией.

Чтобы организовать единый вход (SSO) в сервисы Яндекс 360 через службу федерации Active Directory, нужно предварительно настроить сервер.

Шаг 1. Создайте отношение доверия с проверяющей стороной

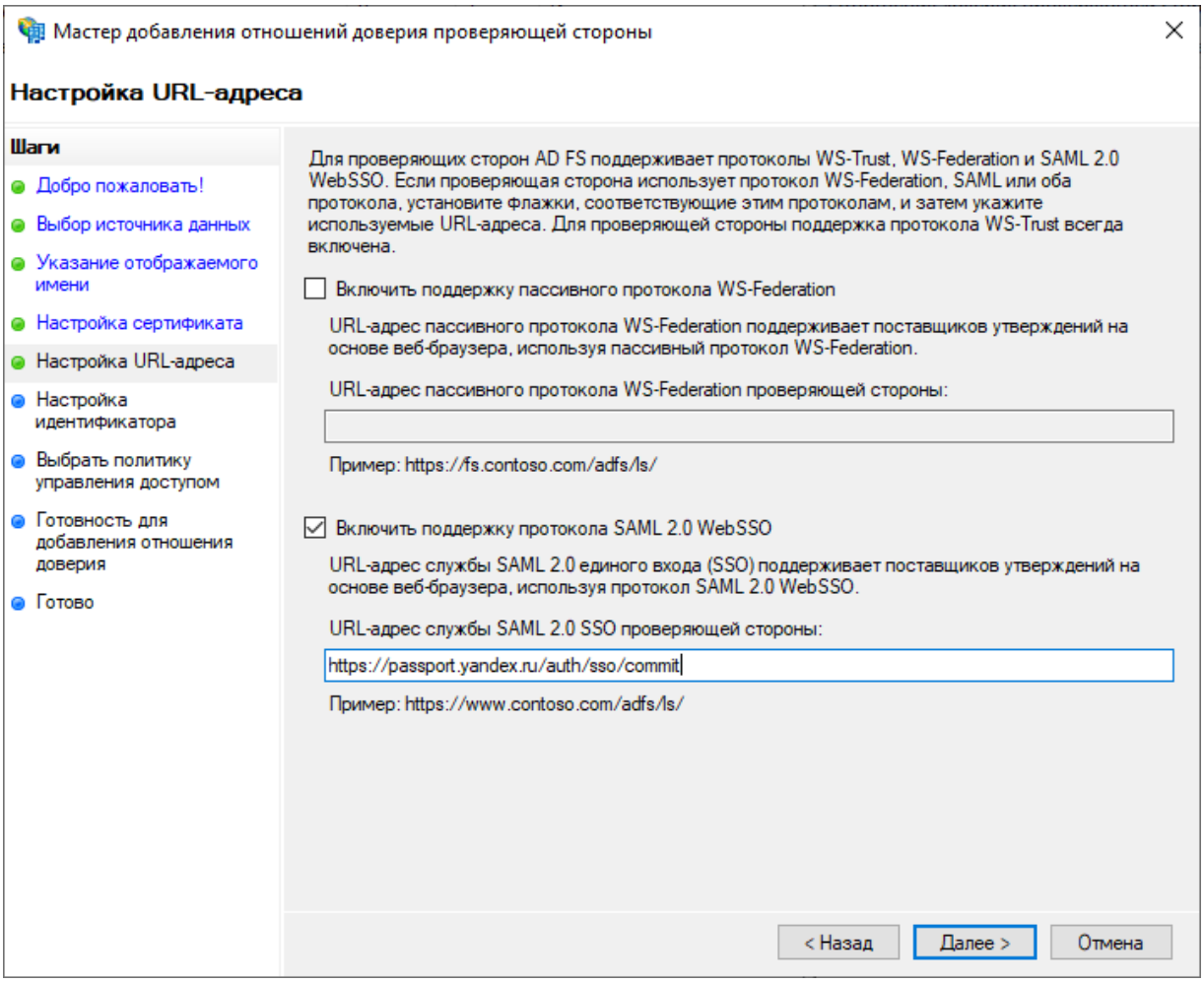
1. Войдите на ваш сервер AD FS и откройте **Диспетчер серверов**.
2. Откройте консоль управления: нажмите **Средства** → **Управление AD FS**.
3. В списке действий выберите **Добавить отношение доверия проверяющей стороны**.
4. Выберите **Поддерживающие утверждения** и нажмите **Старт**.
5. Для автоматической настройки отношения на шаге **Выбор источника данных** выберите **Импорт данных о проверяющей стороне, опубликованных в интернете или локальной сети** и введите URL: `https://passport.yandex.ru/auth/sso/metadata`.

   Нажмите **Далее**.

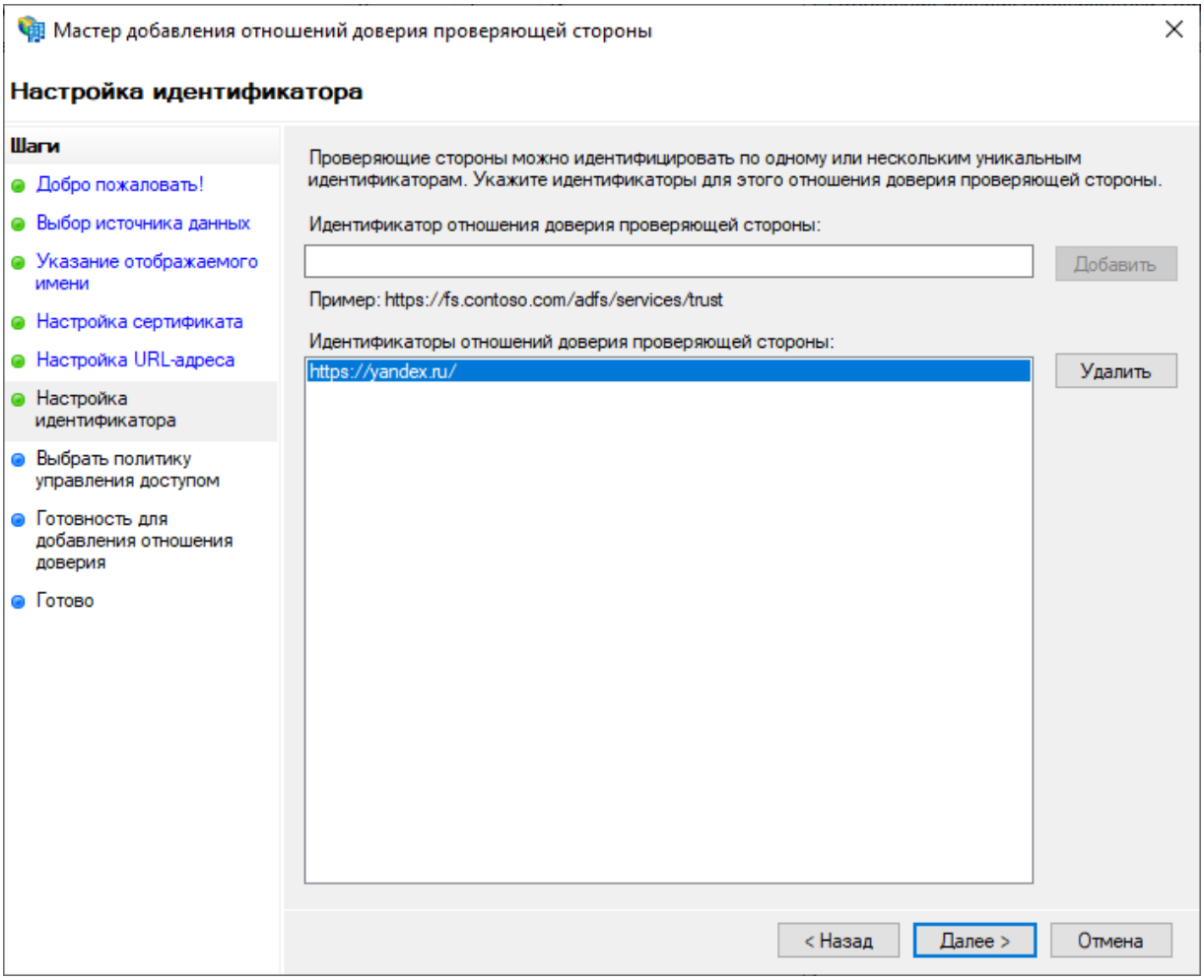


Как настроить отношение вручную

1. На шаге **Выбор источника данных** выберите **Ввод данных о проверяющей стороне вручную**. Затем нажмите **Далее**.
2. Задайте любое название отношения, например «Яндекс 360». Нажмите **Далее**.
3. Пропустите шаг **Настройка сертификата** — для этого нажмите **Далее**.
4. Отметьте **Включить поддержку протокола SAML 2.0 WebSSO** и укажите URL: `https://passport.yandex.ru/auth/sso/commit`. Нажмите **Далее**.

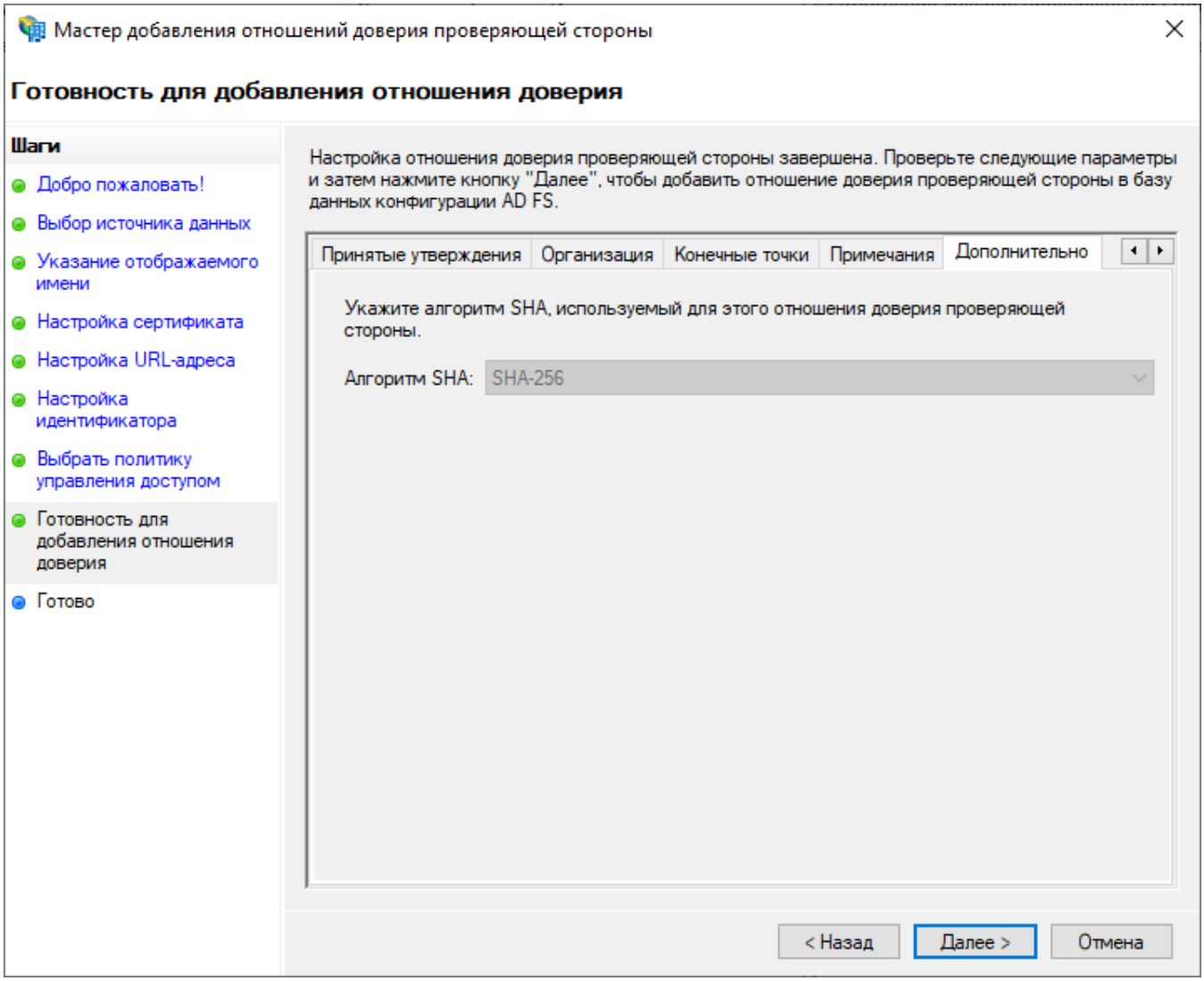


5. Добавьте идентификатор `https://yandex.ru/` (обязательно с косой чертой в конце) — вставьте его в поле и нажмите **Добавить**. Затем нажмите **Далее**.



6. Пропустите шаг **Выбрать политику управления доступом**.

6. Проверьте данные. Убедитесь, что на вкладке **Дополнительно** выбран алгоритм хеширования `SHA-256`. Если все в порядке, нажмите **Далее** → **Закрыть**.



Если вы воспользовались автоматической настройкой отношения, переходите сразу к шагу 3. При ручном создании отношения выполните шаг 2.

Шаг 2. Добавьте конечные точки для языковых доменов

Внимание

Пропустите этот шаг, если вы выбрали автоматическую настройку отношения в пункте 5 шага 1.

Если ваши сотрудники пользуются сервисами Яндекс 360 не только на русском домене, дополнительно добавьте URL языковых доменов в качестве конечных точек:

1. В консоли управления нажмите **Отношения доверия проверяющей стороны**.
2. Откройте настройки отношения, созданного на шаге 1, — для этого нажмите на него два раза.
3. Перейдите на вкладку **Конечные точки**.
4. Добавьте нужные вам конечные точки.

   Чтобы добавить конечную точку для языкового домена, нажмите **Добавить SAML**, в значении **Привязка** выберите `POST` и укажите URL:

- `https://passport.yandex.com/auth/sso/commit` — для английского;
- `https://passport.yandex.kz/auth/sso/commit` — для казахского;
- `https://passport.yandex.uz/auth/sso/commit` — для узбекского;
- `https://passport.yandex.com.tr/auth/sso/commit` — для турецкого.

Полный список

- `https://passport.yandex.com/auth/sso/commit`
- `https://passport.yandex.az/auth/sso/commit`
- `https://passport.yandex.by/auth/sso/commit`
- `https://passport.yandex.co.il/auth/sso/commit`
- `https://passport.yandex.com/auth/sso/commit`
- `https://passport.yandex.com.am/auth/sso/commit`
- `https://passport.yandex.com.ge/auth/sso/commit`
- `https://passport.yandex.com.tr/auth/sso/commit`
- `https://passport.yandex.ee/auth/sso/commit`
- `https://passport.yandex.eu/auth/sso/commit`
- `https://passport.yandex.fi/auth/sso/commit`
- `https://passport.yandex.fr/auth/sso/commit`
- `https://passport.yandex.kg/auth/sso/commit`
- `https://passport.yandex.kz/auth/sso/commit`
- `https://passport.yandex.lt/auth/sso/commit`
- `https://passport.yandex.lv/auth/sso/commit`
- `https://passport.yandex.md/auth/sso/commit`
- `https://passport.yandex.pl/auth/sso/commit`
- `https://passport.yandex.ru/auth/sso/commit`
- `https://passport.yandex.tj/auth/sso/commit`
- `https://passport.yandex.tm/auth/sso/commit`
- `https://passport.yandex.uz/auth/sso/commit`

Затем нажмите **OK**.

Шаг 3. Настройте сопоставление утверждений

Чтобы настроить сопоставление утверждений, нужно указать атрибут. Он будет использоваться для идентификации пользователя в Яндекс ID. После того как вы выберете атрибут, поменять его будет нельзя.

- Если имена для входа пользователей не будут меняться, укажите атрибут «UPN».
- Если же в вашей организации запланированы изменения домена или бизнес-процессов, которые могут привести к изменению UPN пользователей, нужно будет выбрать другой атрибут: «objectSID», «objectGUID» или другой.

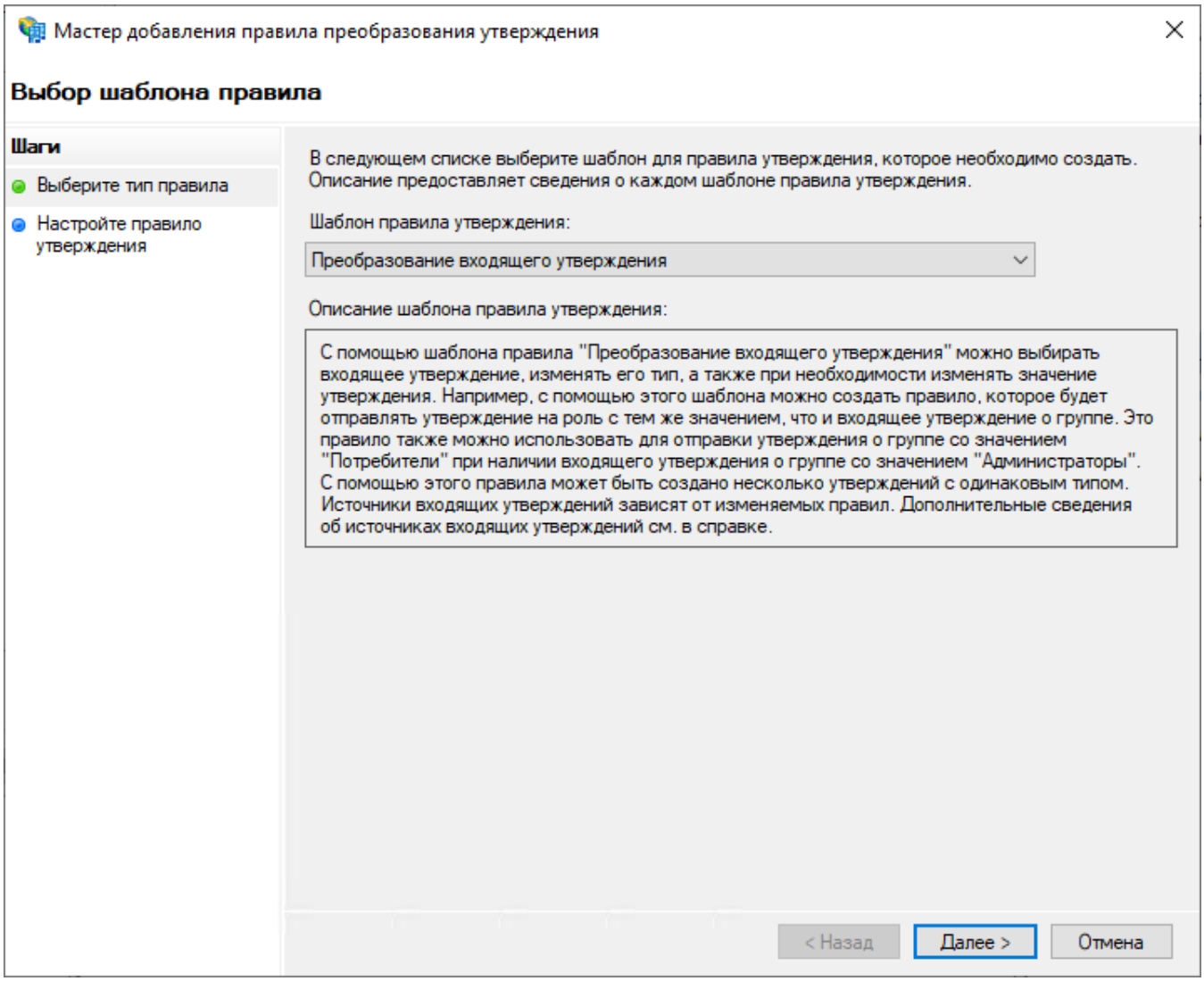
Совет

Атрибут ObjectGUID по умолчанию не работает. Чтобы он заработал, необходимо преобразовать формат его передачи с помощью скрипта.

Как указать атрибут:

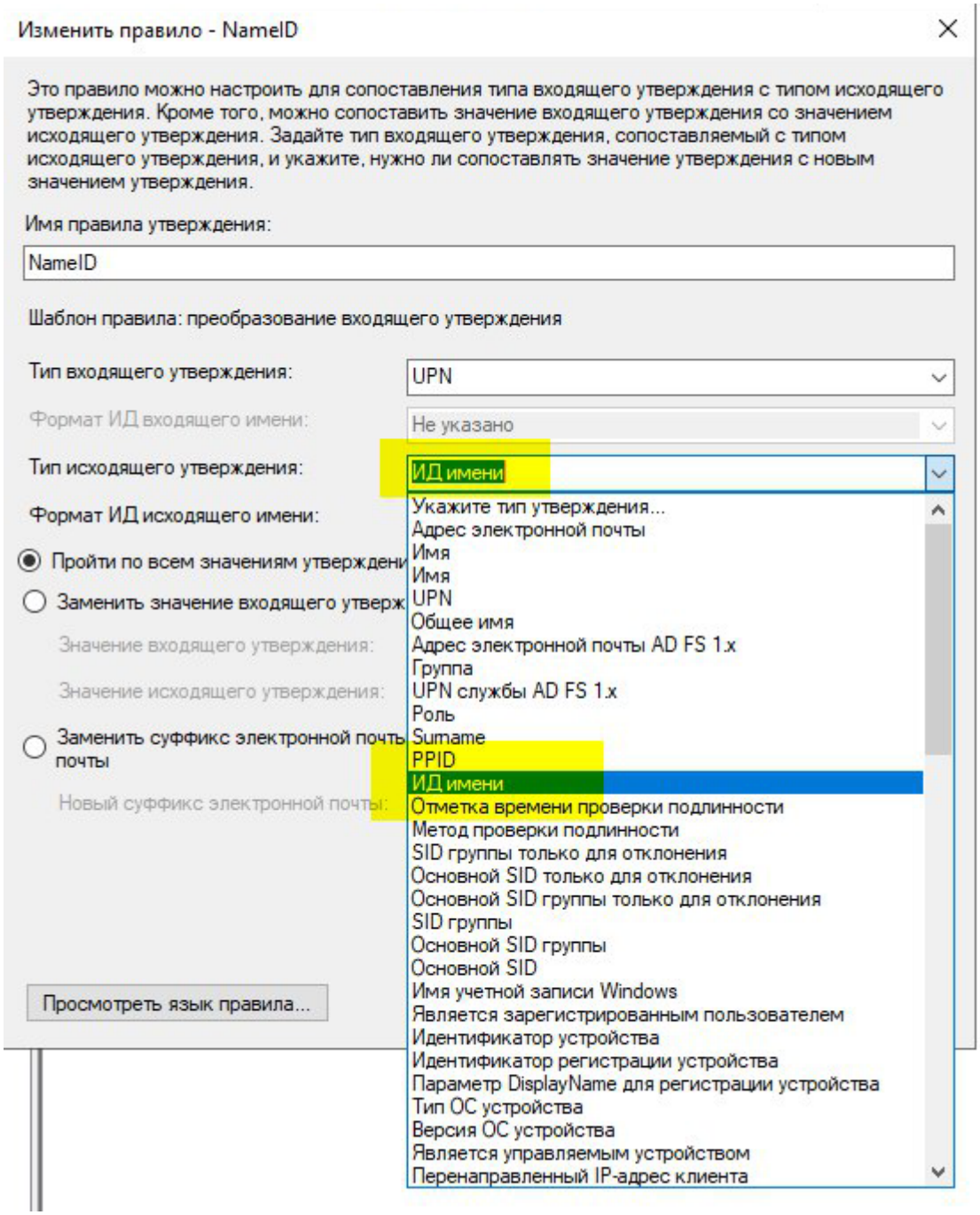
UPN

1. В блоке **Отношения доверия проверяющей стороны** правой кнопкой мыши нажмите на отношение, созданное на шаге 1, и выберите **Изменить политику подачи запросов**.
2. Нажмите **Добавить правило**.
3. В поле **Шаблон правила утверждения** выберите **Преобразование входящего утверждения** и нажмите **Далее**.

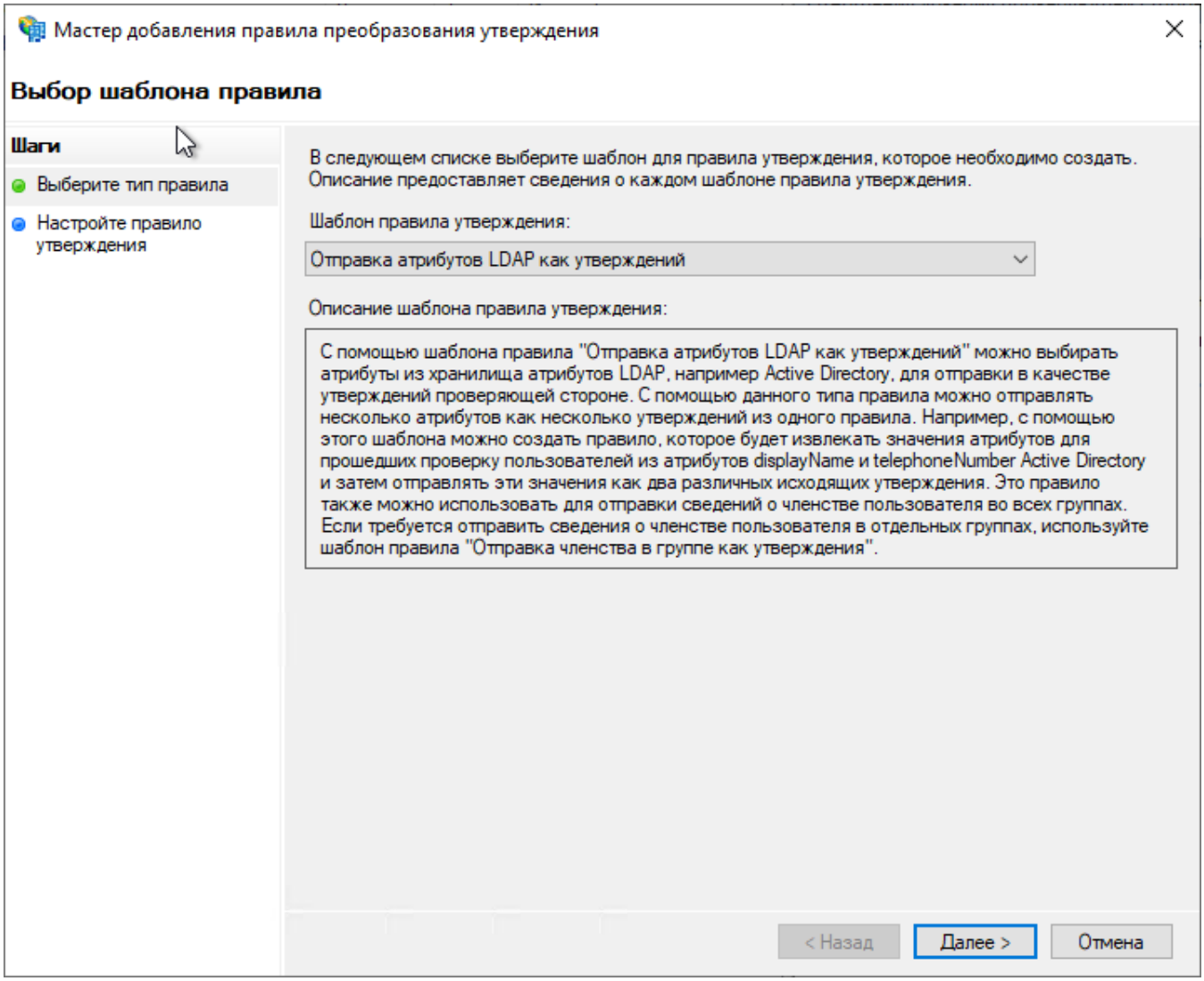


4. Придумайте название правила. При работе с русифицированными атрибутами используйте **ИД имени** вместо **NameID**. Укажите **ИД имени** в поле **Имя правила утверждения**. Это предотвратит проблемы аутентификации.

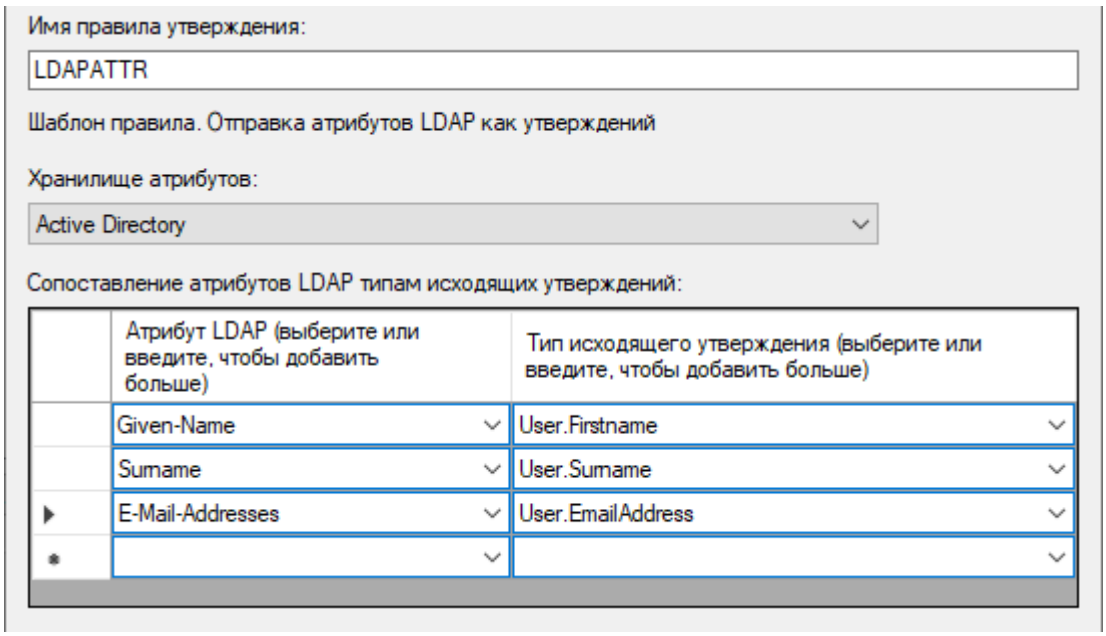
   В поле **Тип исходящего утверждения** выберите `ИД имени`. Нажмите **Готово**.



5. Создайте еще одно правило: снова нажмите **Добавить правило**. Выберите шаблон **Отправка атрибутов LDAP как утверждений** и нажмите **Далее**.



6. Задайте правилу название, например «LDAPATTR». Заполните остальные поля, как указано ниже:

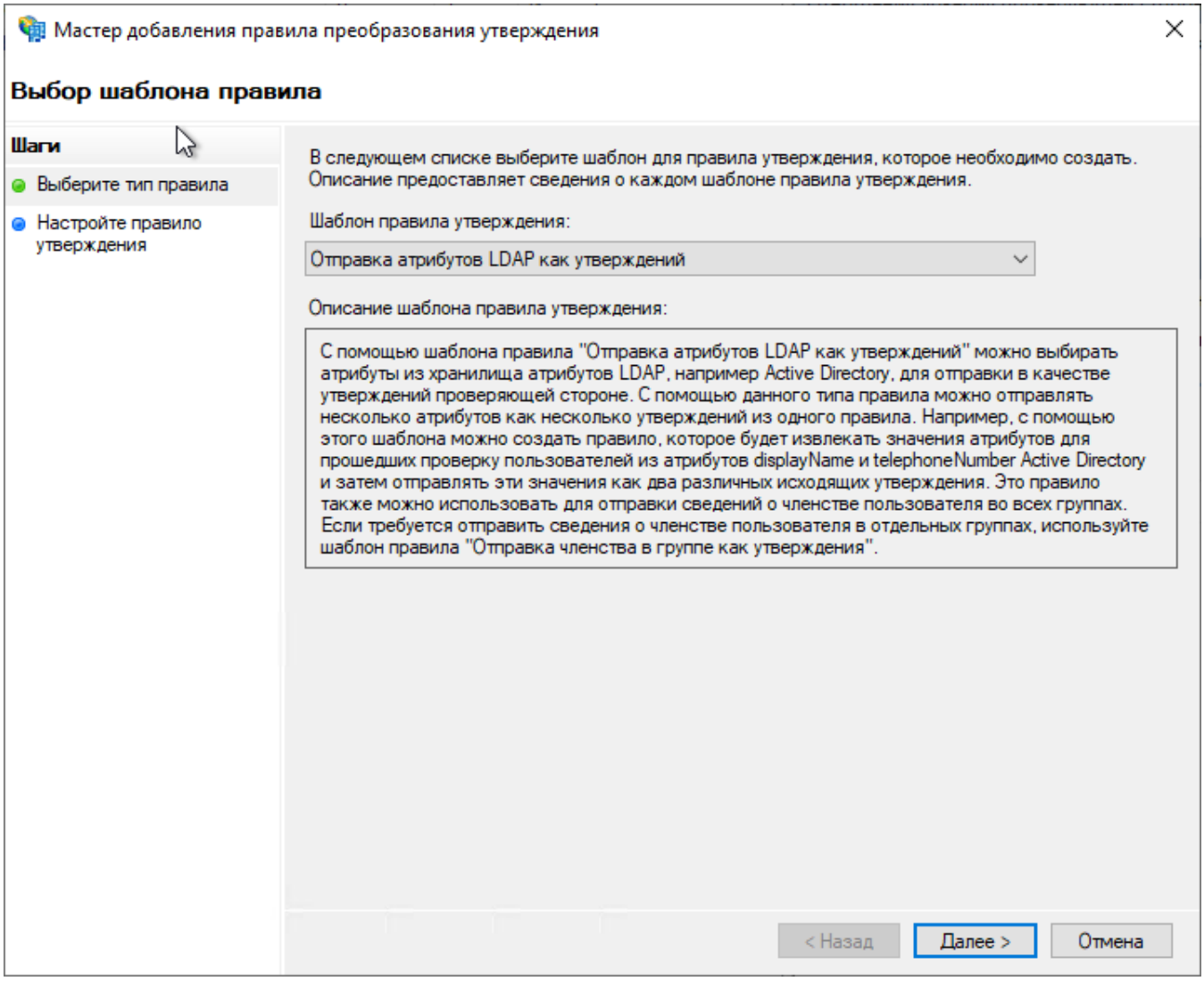


Затем нажмите **Готово**.

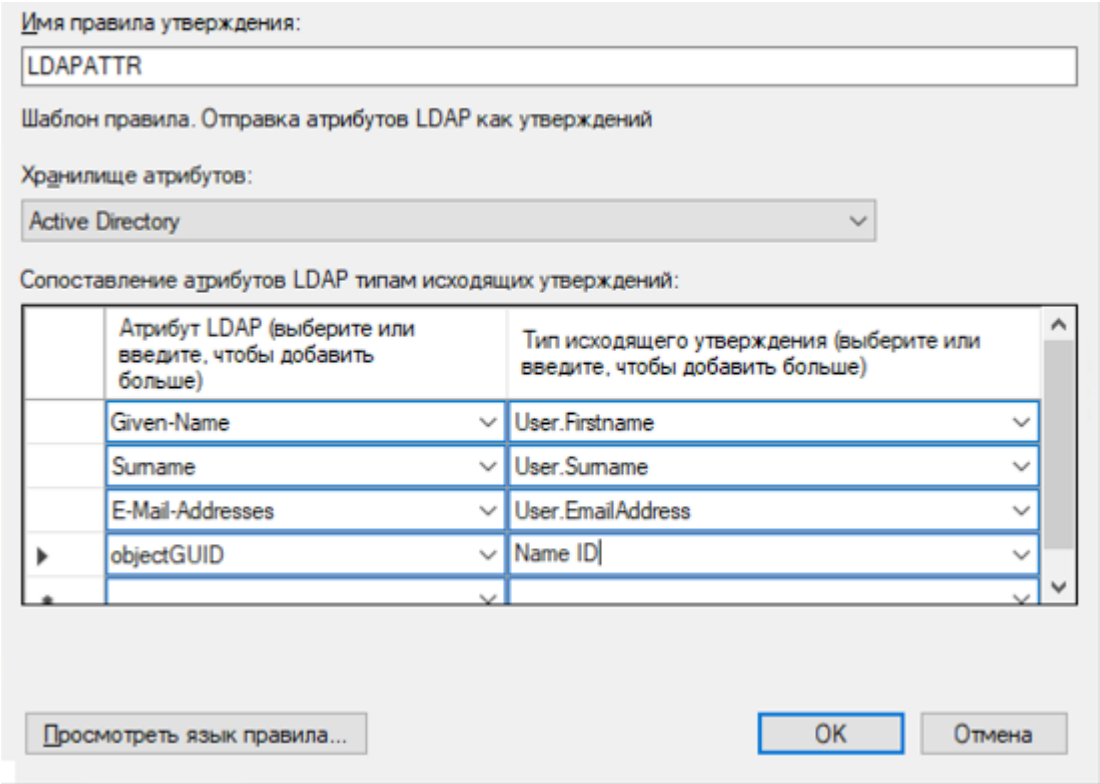
Названия атрибутов чувствительны к формату и регистру. Укажите названия именно так, как показано на картинке: `User.Firstname`, `User.Surname`, `User.EmailAddress`. Иначе при авторизации могут возникнуть ошибки, например email.no_in_response.

objectGUID, objectSID или другой

1. В блоке **Отношения доверия проверяющей стороны** правой кнопкой мыши нажмите на отношение, созданное на шаге 1, и выберите **Изменить политику подачи запросов**.
2. Нажмите **Добавить правило**. Выберите шаблон **Отправка атрибутов LDAP как утверждений** и нажмите **Далее**.



3. Задайте правилу название, например «LDAPATTR». Заполните остальные поля, как указано ниже. Напротив типа «Name ID» укажите атрибут: «objectGUID», «objectSID» или другой.



Затем нажмите **Готово**.

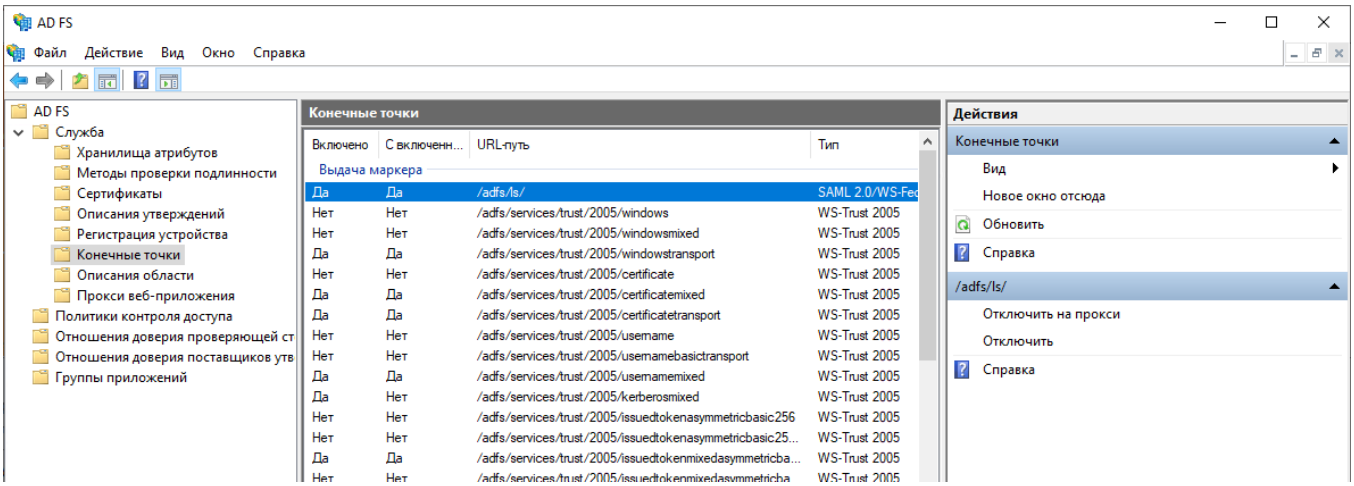
Названия атрибутов чувствительны к формату и регистру. Укажите названия именно так, как показано на картинке: `User.Firstname`, `User.Surname`, `User.EmailAddress`. Иначе при авторизации могут возникнуть ошибки, например email.no_in_response.

Шаг 4. Соберите данные, которые нужно будет передать Яндекс 360

URL страницы входа

Адрес точки входа. Как правило, это `https://домен/adfs/ls`.

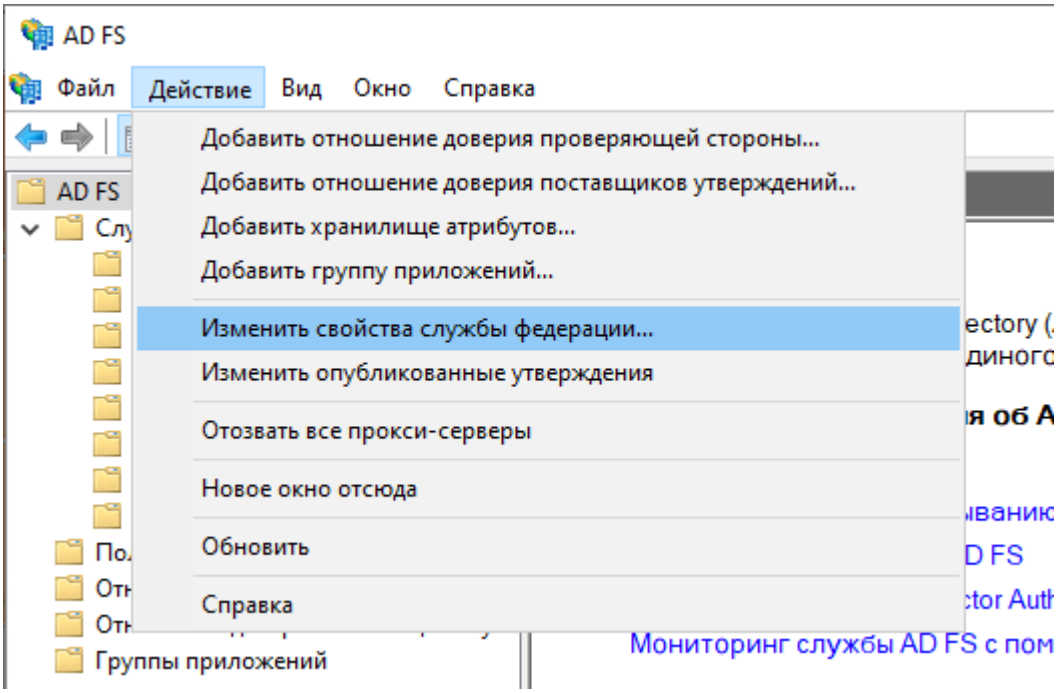
В консоли управления откройте **Конечные точки** и убедитесь, что для параметра **С включенным прокси** у `/adfs/ls/` установлено значение `Да`. Этот параметр отвечает за активацию страницы аутентификации в AD FS, которая должна быть доступна извне, — адрес вида `https://домен_ADFS/adfs/ls/idpinitiatedsignon.aspx`.



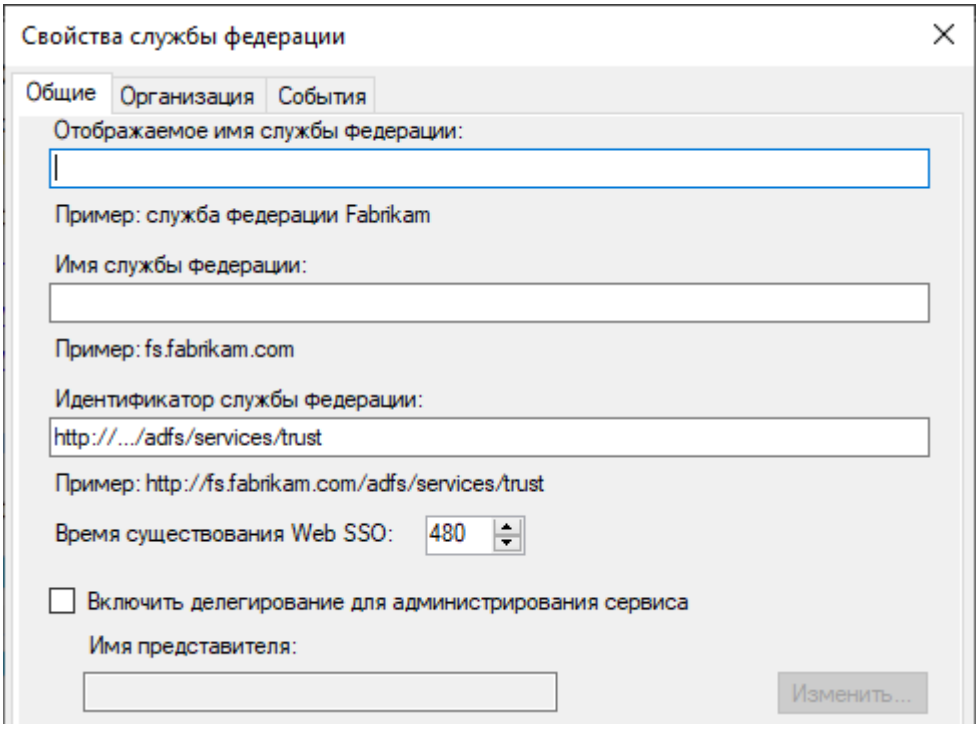
Издатель поставщика удостоверений

Entity ID домена. Как правило, это `http://домен/adfs/services/trust`.

Чтобы получить его, в консоли управления перейдите на вкладку **Действие** и выберите **Изменить свойства службы федерации**.



Нужное значение находится в поле **Идентификатор службы федерации**.



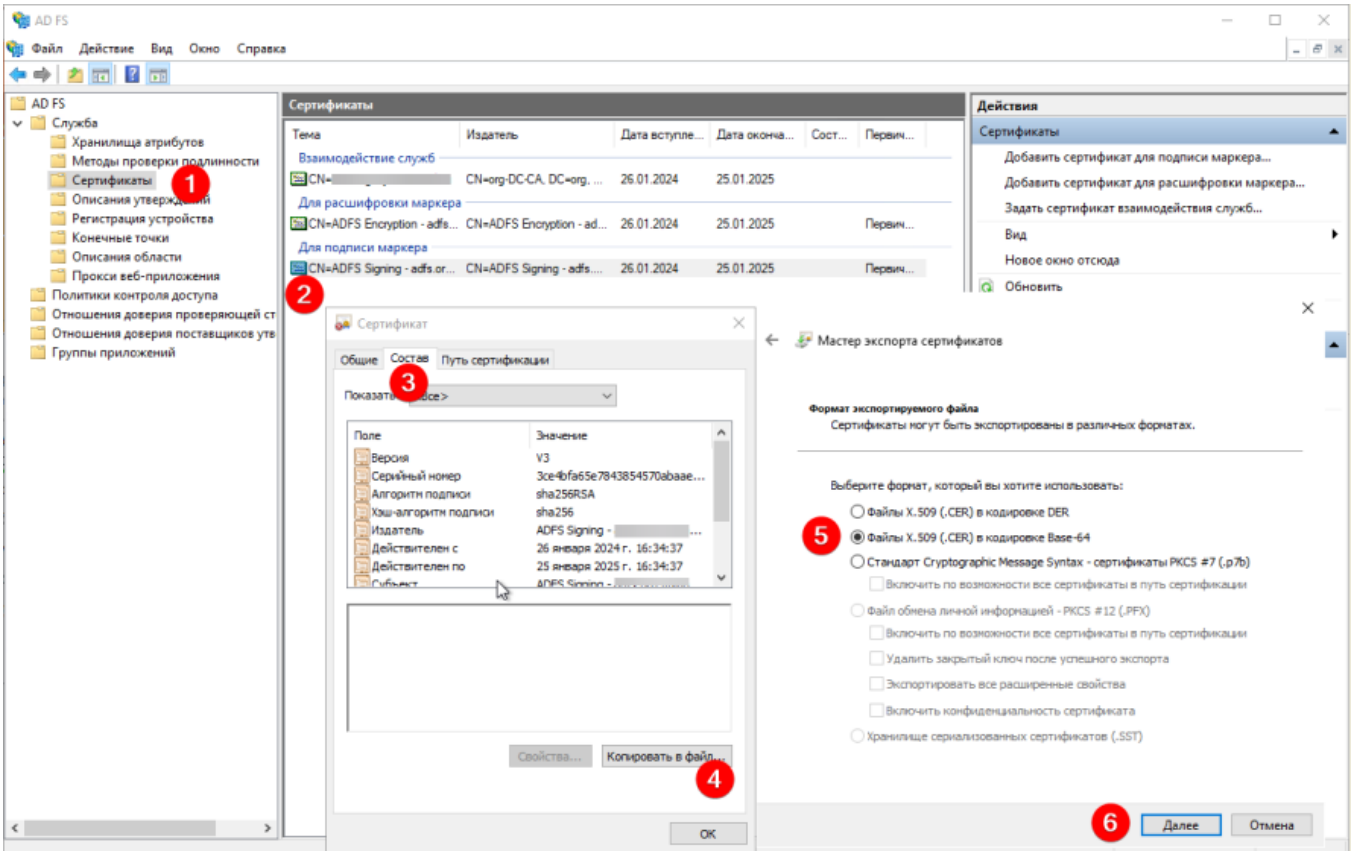
Проверочный сертификат

Сертификат подписи токенов формата X.509 в Base64. Чтобы получить:

1. В консоли управления откройте **Сертификаты**.
2. Нажмите два раза на ваш сертификат **Для подписи маркера**.
3. Перейдите на вкладку **Состав** и нажмите **Копировать в файл**.

4. Выберите тип сертификата **Файлы X.509 (.CER) в кодировке Base-64** и нажмите **Далее**.

5. Сохраните файл на жесткий диск.



Если у вас два активных сертификата подписи токенов и вы не уверены, какой сертификат используется сейчас, повторите аналогичные действия для второго сертификата.

Шаг 5. Настройте синхронизацию сотрудников SCIM

По умолчанию новые сотрудники появляются в Яндекс 360 только после первой авторизации, а бывших сотрудников нужно удалять вручную. Если вы хотите автоматически синхронизировать список сотрудников из AD FS с Яндекс 360 для бизнеса, подключите синхронизацию SCIM.

Решение проблем с настройкой

Если в процессе настройки поставщика удостоверений заданы неверные значения, то при попытке входа через SSO вы увидите сообщение «Авторизация не удалась» и код ошибки:

email.no_in_response

Указывайте имена атрибутов в формате `User.Firstname`, `User.Surname`, `User.EmailAddress`. Если задать другой формат, например `Firstname`, авторизоваться не получится.

request_your_admin

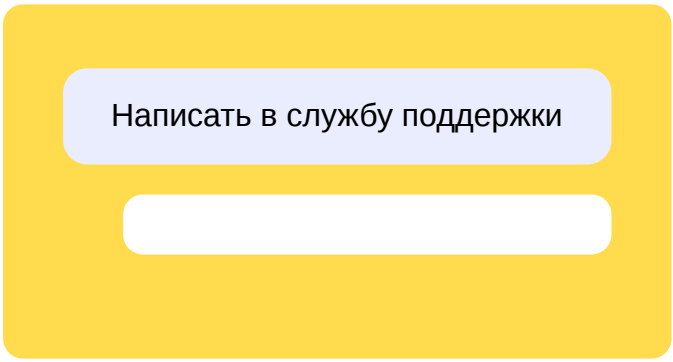
Ошибка появляется, если администратор каталога пользователей вашей организации ограничил для аккаунта доступ к Яндекс 360. За подробной информацией обратитесь к специалистам технической поддержки вашей организации.

samlresponse.invalid

Ошибка возникает, если неверно указаны URL страницы входа, издатель поставщика удостоверений или проверочный сертификат. Также она может возникнуть в течение 14 дней до истечения проверочного сертификата или после его истечения. Проверьте корректность настроек SSO в Яндекс 360 для бизнеса.

unsupportable_domain

Проверьте, что домен из почтового атрибута `User.EmailAddress` в SAML response такой же, как и основной домен или один из доменов-алиасов организации Яндекс 360.



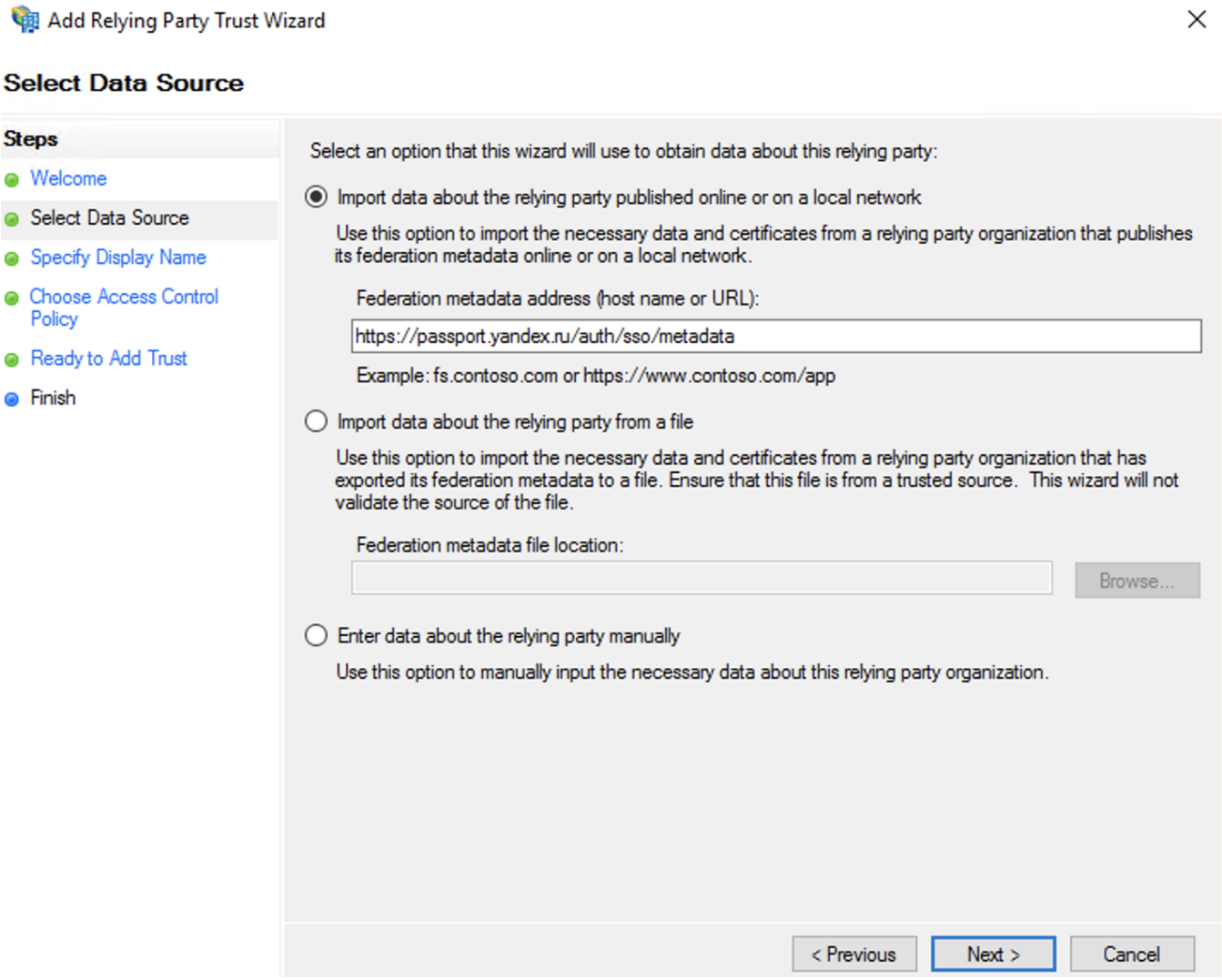
Настройка Active Directory (английский интерфейс)

Чтобы организовать единый вход (SSO) в сервисы Яндекс 360 через службу федерации Active Directory, нужно предварительно настроить сервер.

Шаг 1. Создайте отношение доверия с проверяющей стороной

1. Войдите на ваш сервер AD FS и откройте **Server Manager**.
2. Откройте консоль управления: нажмите **Tools** → **AD FS Management**.
3. В списке действий выберите **Add Relying Party Trust**.
4. Выберите **Claims aware** и нажмите **Start**.
5. Для автоматической настройки отношения на шаге **Select Data Source** выберите **Import data about the relying party published online or on a local network** и введите URL: `https://passport.yandex.ru/auth/sso/metadata`.

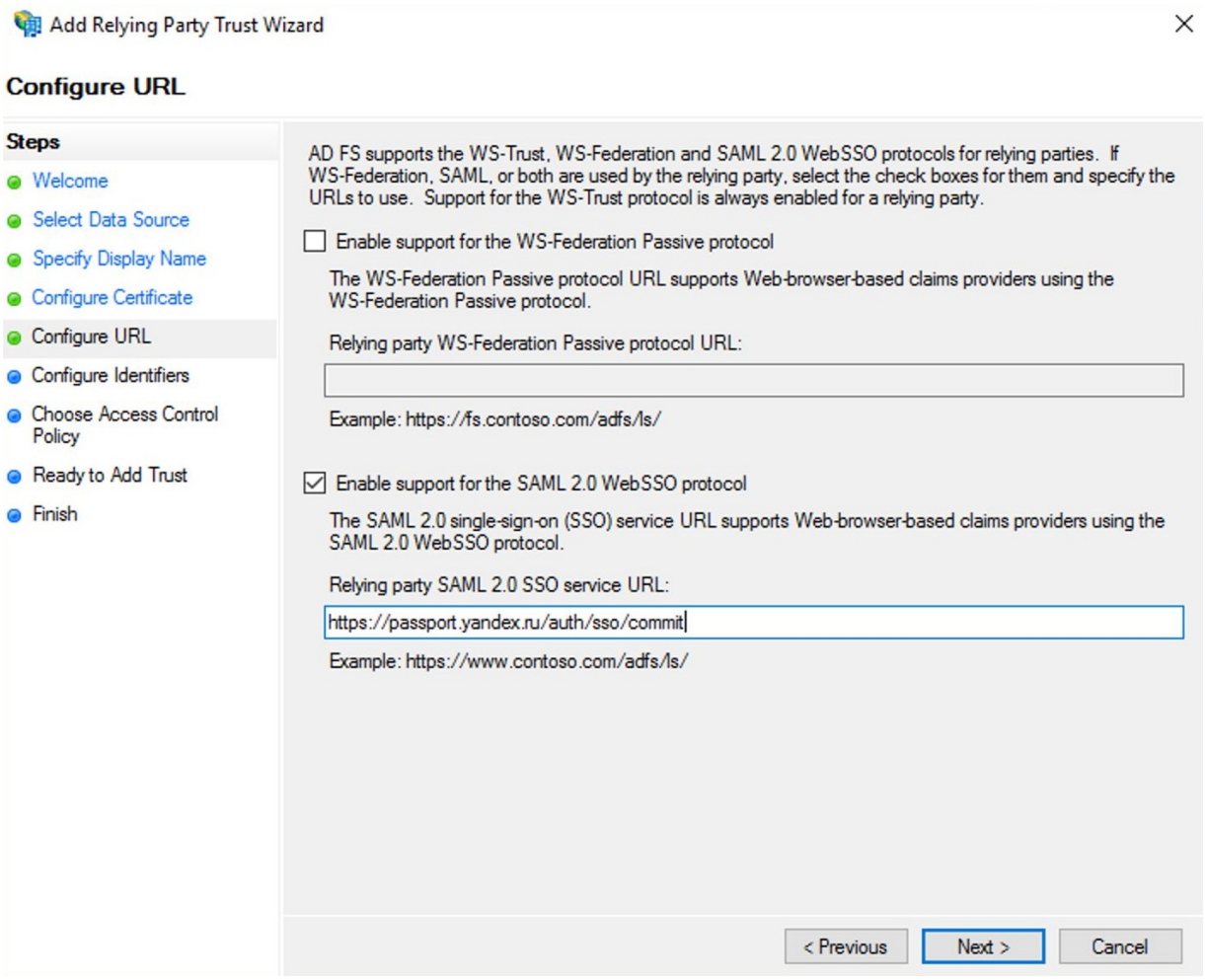
   Нажмите **Next**.



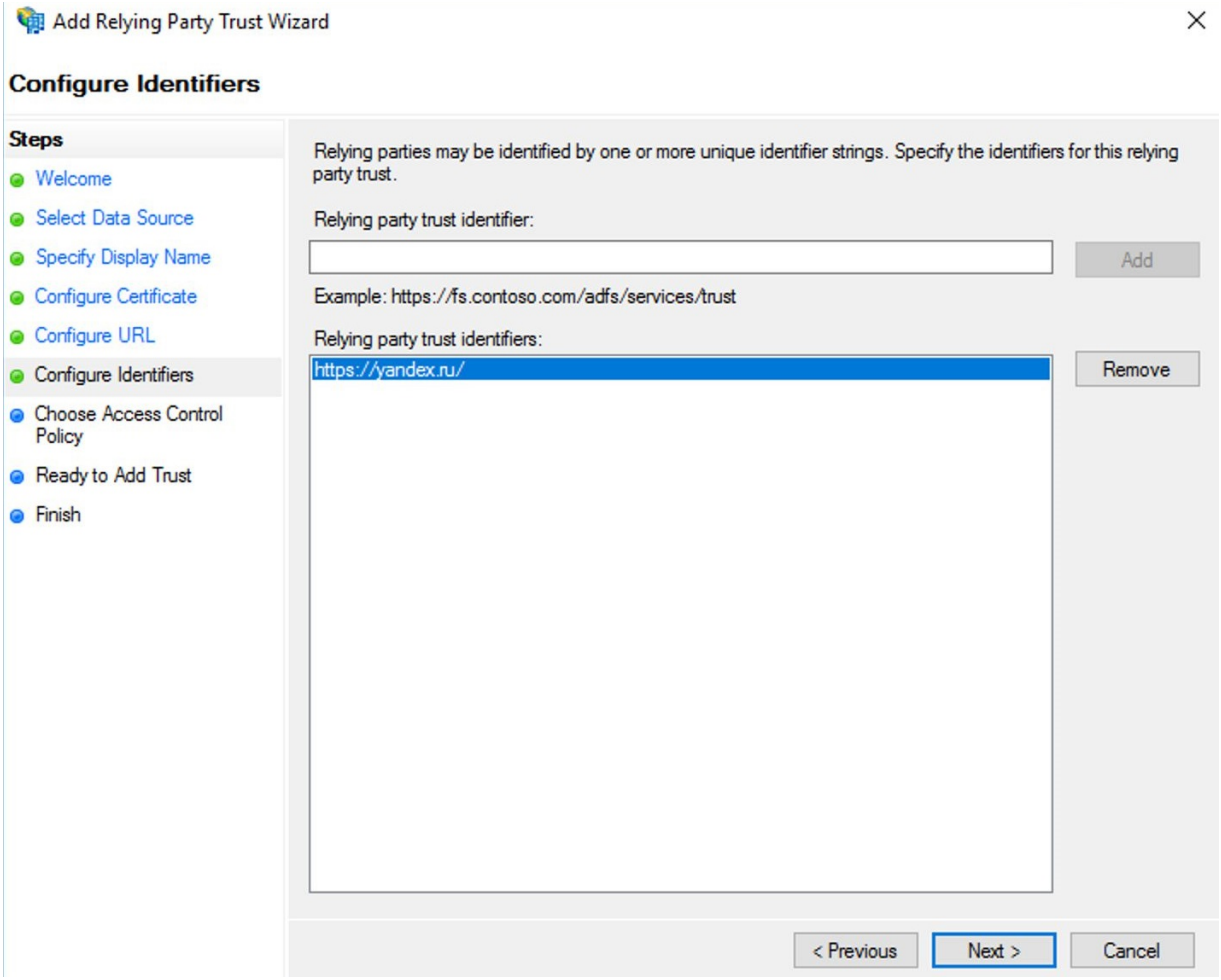
Как настроить отношение вручную

1. На шаге **Select Data Source** выберите **Enter data about the relying party manually**. Затем нажмите **Next**.
2. Задайте любое название отношения, например «Яндекс 360». Нажмите **Next**.

3. Пропустите шаг **Configure Certificate** — для этого нажмите **Next**.
4. Отметьте **Enable support for the SAML 2.0 WebSSO protocol** и укажите Service URL: `https://passport.yandex.ru/auth/sso/commit`. Нажмите **Next**.

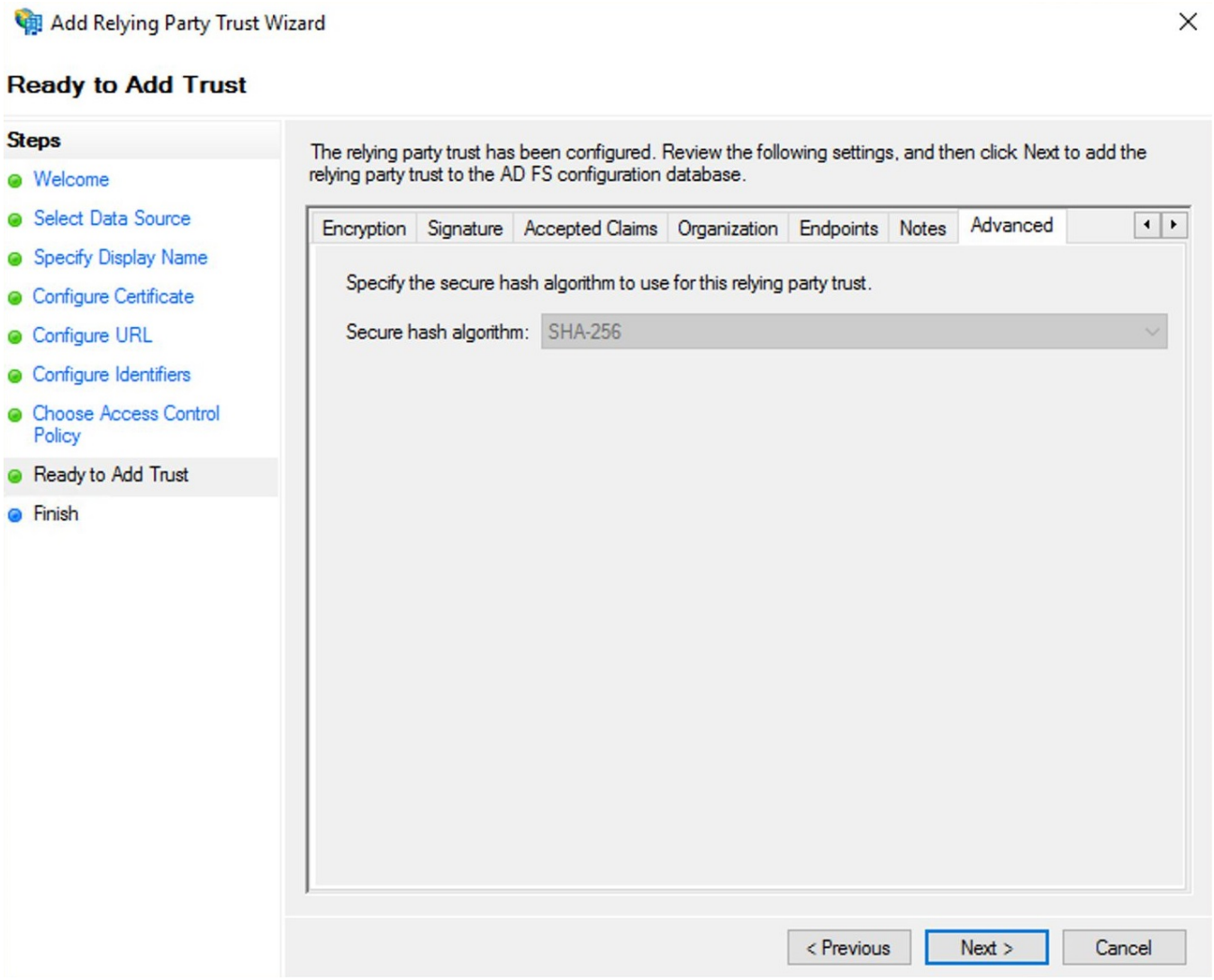


5. Добавьте идентификатор `https://yandex.ru/` (обязательно с косой чертой в конце) — вставьте его в поле и нажмите **Add**. Затем нажмите **Next**.



6. Пропустите шаг **Choose Access Control Policy**.

6. Проверьте данные. Убедитесь, что на вкладке **Advanced** выбран алгоритм хеширования `SHA-256`. Если все в порядке, нажмите **Next** → **Close**.



Если вы воспользовались автоматической настройкой отношения, переходите сразу к шагу 3. При ручном создании отношения выполните шаг 2.

Шаг 2. Добавьте конечные точки для языковых доменов

Внимание

Пропустите этот шаг, если вы выбрали автоматическую настройку отношения в пункте 5 шага 1.

Если ваши сотрудники пользуются сервисами Яндекс 360 не только на русском домене, дополнительно добавьте URL языковых доменов в качестве конечных точек:

1. В консоли управления нажмите **Trust Relationships** → **Relying Party Trusts**.
2. Откройте настройки отношения, созданного на шаге 1, — для этого нажмите на него два раза.
3. Перейдите на вкладку **Endpoints**.
4. Добавьте нужные вам конечные точки.

   Чтобы добавить конечную точку для языкового домена, нажмите **Add SAML**, в значении **Binding** выберите `POST` и укажите URL:

- `https://passport.yandex.com/auth/sso/commit` — для английского;
- `https://passport.yandex.kz/auth/sso/commit` — для казахского;
- `https://passport.yandex.uz/auth/sso/commit` — для узбекского;
- `https://passport.yandex.com.tr/auth/sso/commit` — для турецкого.

Полный список

- `https://passport.yandex.com/auth/sso/commit`
- `https://passport.yandex.az/auth/sso/commit`
- `https://passport.yandex.by/auth/sso/commit`
- `https://passport.yandex.co.il/auth/sso/commit`
- `https://passport.yandex.com/auth/sso/commit`
- `https://passport.yandex.com.am/auth/sso/commit`
- `https://passport.yandex.com.ge/auth/sso/commit`
- `https://passport.yandex.com.tr/auth/sso/commit`
- `https://passport.yandex.ee/auth/sso/commit`
- `https://passport.yandex.eu/auth/sso/commit`
- `https://passport.yandex.fi/auth/sso/commit`
- `https://passport.yandex.fr/auth/sso/commit`
- `https://passport.yandex.kg/auth/sso/commit`
- `https://passport.yandex.kz/auth/sso/commit`
- `https://passport.yandex.lt/auth/sso/commit`
- `https://passport.yandex.lv/auth/sso/commit`
- `https://passport.yandex.md/auth/sso/commit`
- `https://passport.yandex.pl/auth/sso/commit`
- `https://passport.yandex.ru/auth/sso/commit`
- `https://passport.yandex.tj/auth/sso/commit`
- `https://passport.yandex.tm/auth/sso/commit`
- `https://passport.yandex.uz/auth/sso/commit`

Затем нажмите **OK**.

Шаг 3. Настройте Claims Mapping

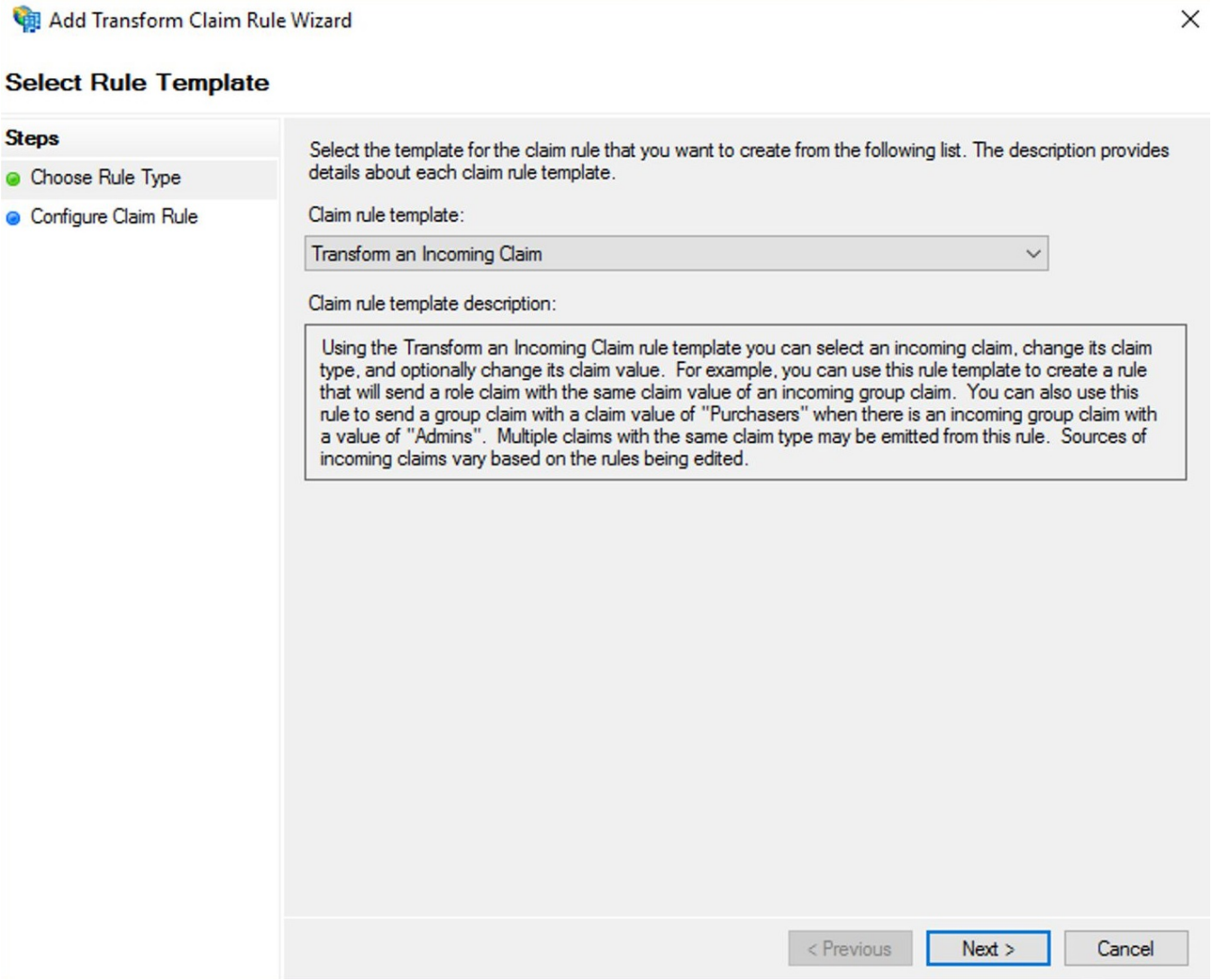
Чтобы настроить сопоставление утверждений, нужно указать атрибут. Он будет использоваться для идентификации пользователя в Яндекс ID. После того как вы выберете атрибут, поменять его будет нельзя.

- Если имена для входа пользователей не будут меняться, укажите атрибут «UPN».
- Если же в вашей организации запланированы изменения домена или бизнес-процессов, которые могут привести к изменению UPN пользователей, нужно будет выбрать другой атрибут: «objectSID», «objectGUID» или другой.

Как указать атрибут:

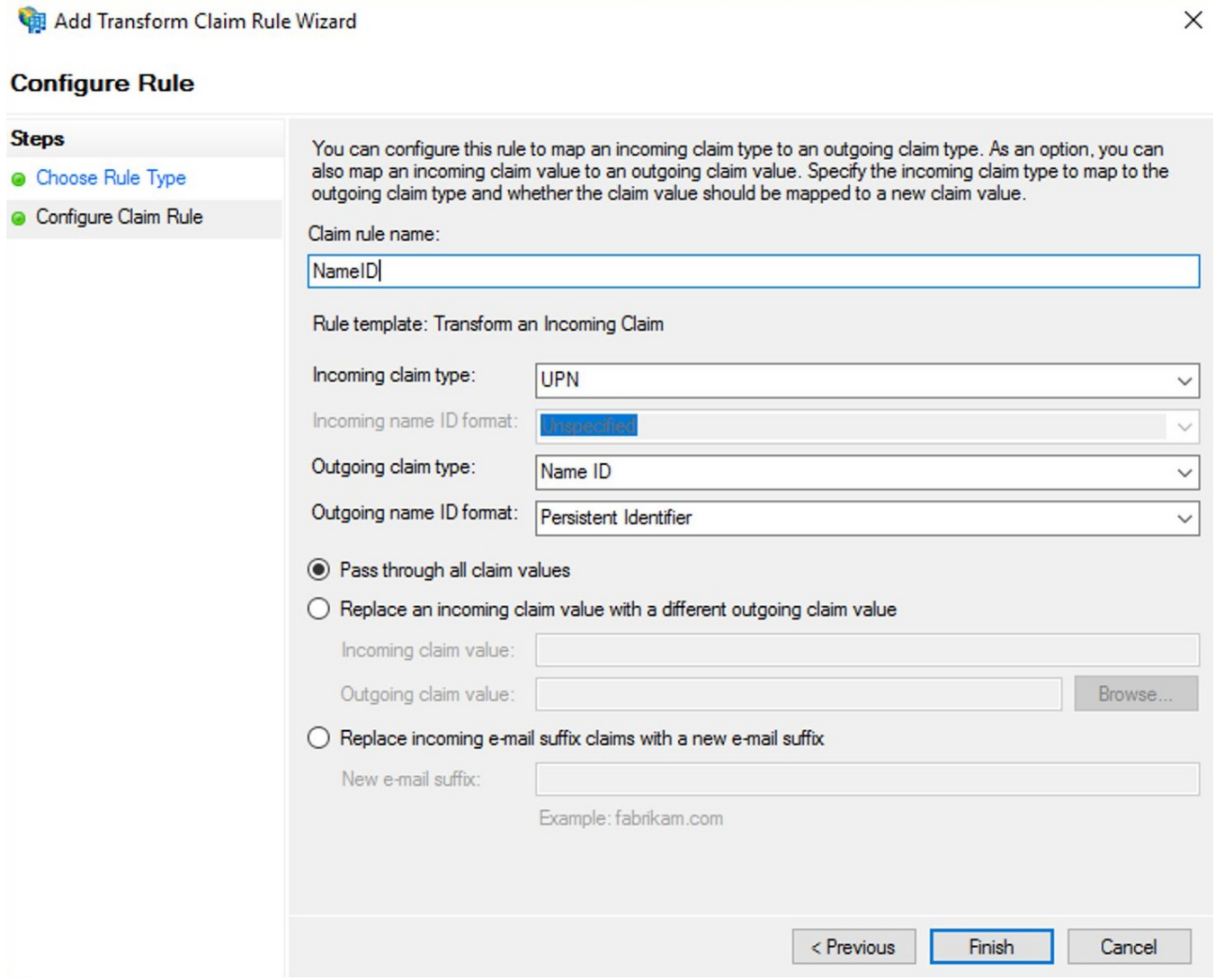
UPN

1. В блоке **Trust Relationships** правой кнопкой мыши нажмите на отношение, созданное на шаге 1, и выберите **Edit Claim Issuance Policy**.
2. Нажмите **Add Rule**.
3. В качестве **Claim rule template** выберите **Transform an Incoming Claim** и нажмите **Next**.

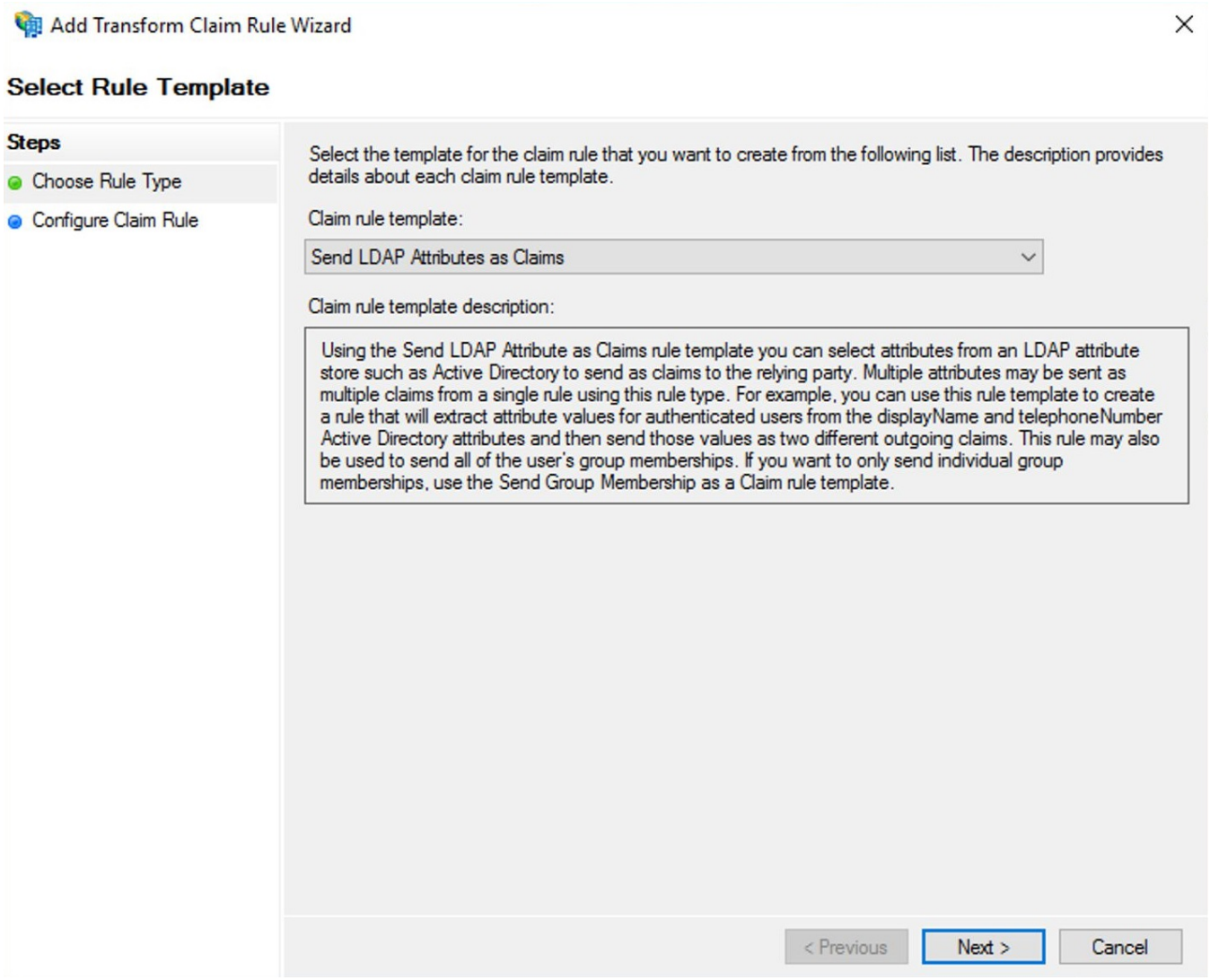


4. Придумайте любое название правила, например «NameID», и укажите его в поле **Claim rule name**.

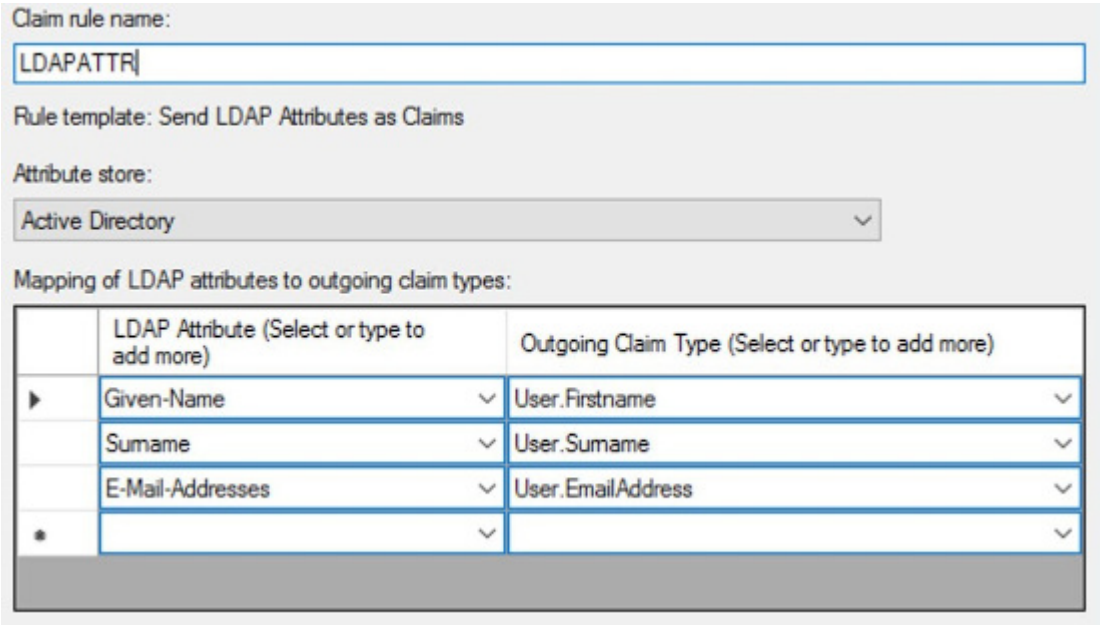
   В поле **Outgoing claim type** выберите `Name ID`. Нажмите **Finish**.



5. Создайте еще одно правило: снова нажмите **Add Rule**. Выберите шаблон **Send LDAP Attributes as Claims** и нажмите **Next**.



6. Задайте правилу название, например «LDAPATTR». Заполните остальные поля, как указано ниже:

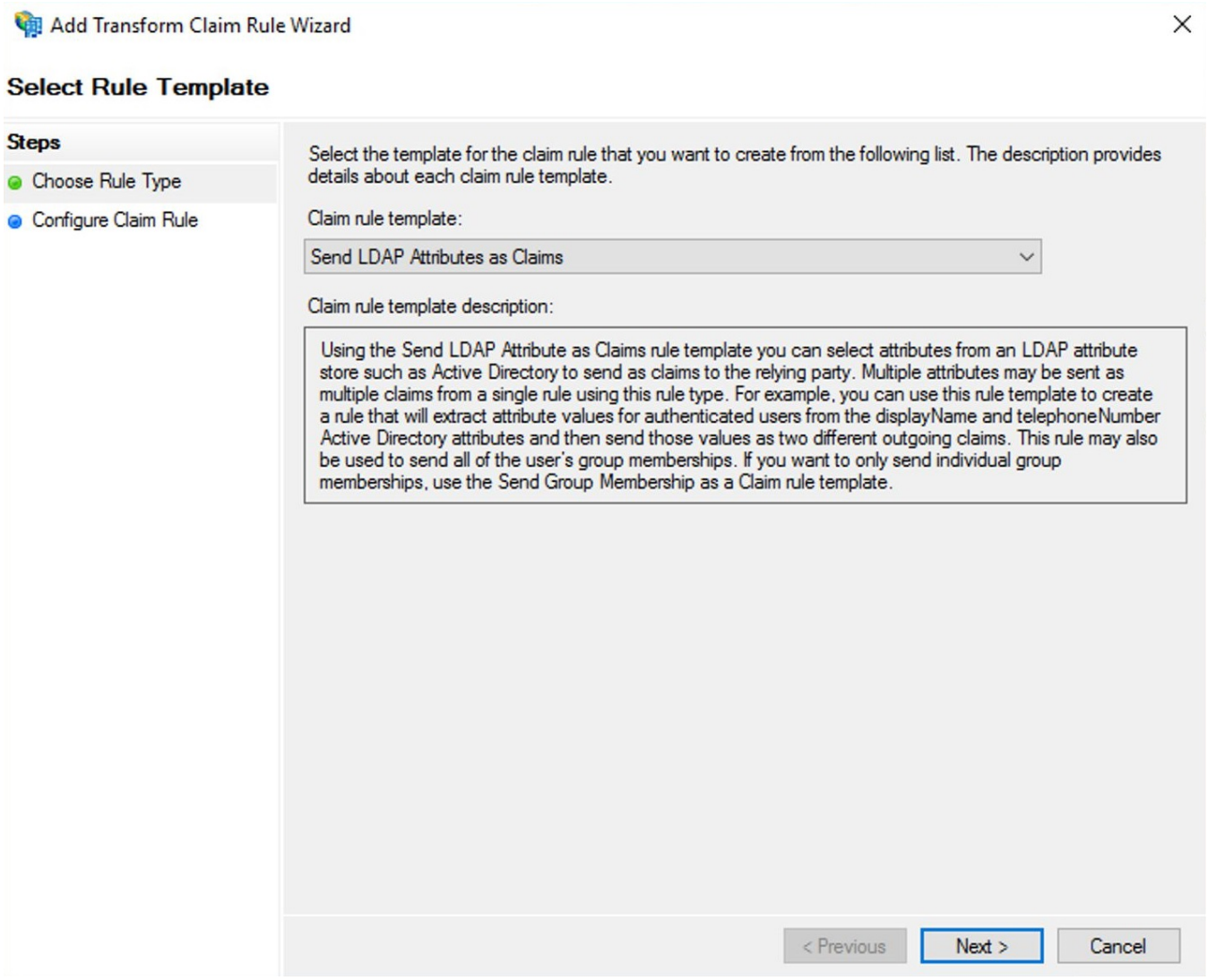


Затем нажмите **Finish**.

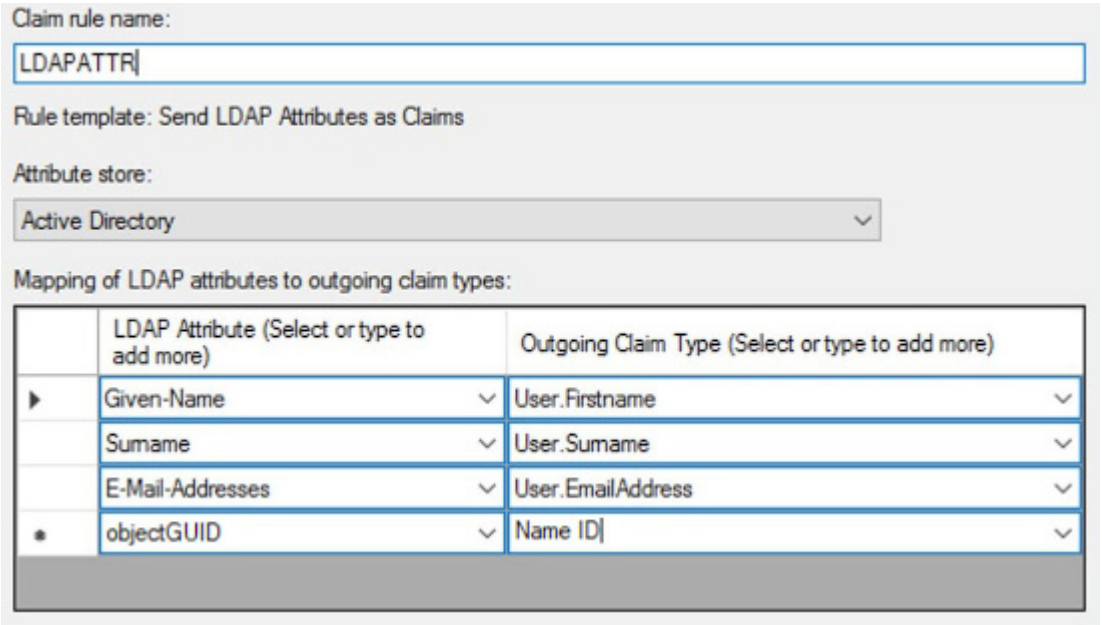
Названия атрибутов чувствительны к формату и регистру. Укажите названия именно так, как показано на картинке: User.Firstname, User.Surname, User.EmailAddress. Иначе при авторизации могут возникнуть ошибки, например email.no_in_response.

objectGUID, objectSID или другой

1. В блоке **Trust Relationships** правой кнопкой мыши нажмите на отношение, созданное на шаге 1, и выберите **Edit Claim Issuance Policy**.
2. Нажмите **Add Rule**. Выберите шаблон **Send LDAP Attributes as Claims** и нажмите **Next**.



3. Задайте правилу название, например «LDAPATTR». Заполните остальные поля, как указано ниже. Напротив типа «Name ID» укажите атрибут: «objectGUID», «objectSID» или другой.



Затем нажмите **Finish**.

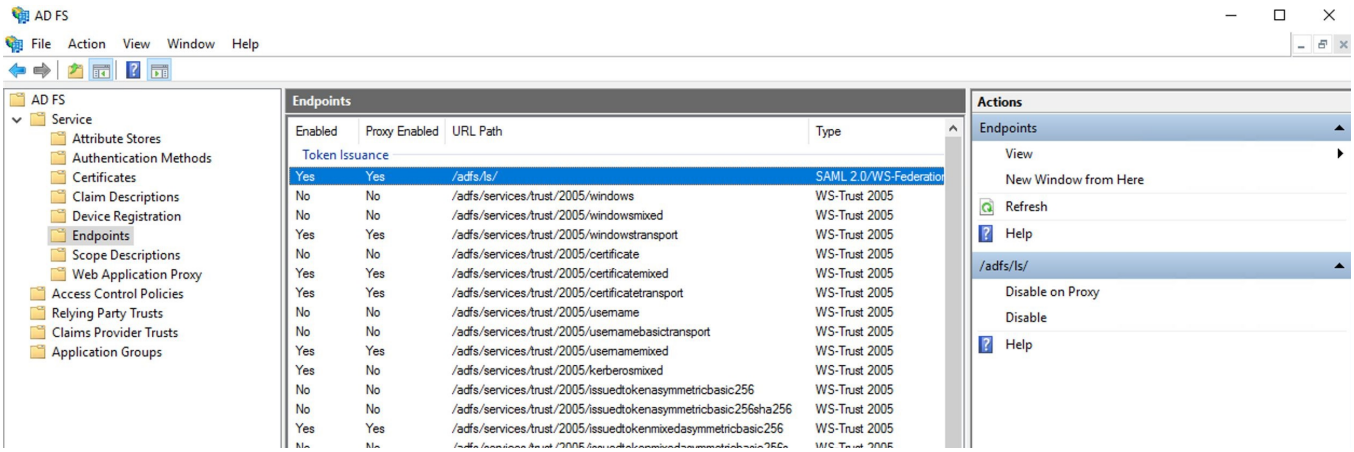
Названия атрибутов чувствительны к формату и регистру. Укажите названия именно так, как показано на картинке: `User.Firstname`, `User.Surname`, `User.EmailAddress`. Иначе при авторизации могут возникнуть ошибки, например email.no_in_response.

Шаг 4. Соберите данные, которые нужно будет передать Яндекс 360

URL страницы входа

Адрес точки входа. Как правило, это `https://домен/adfs/ls`.

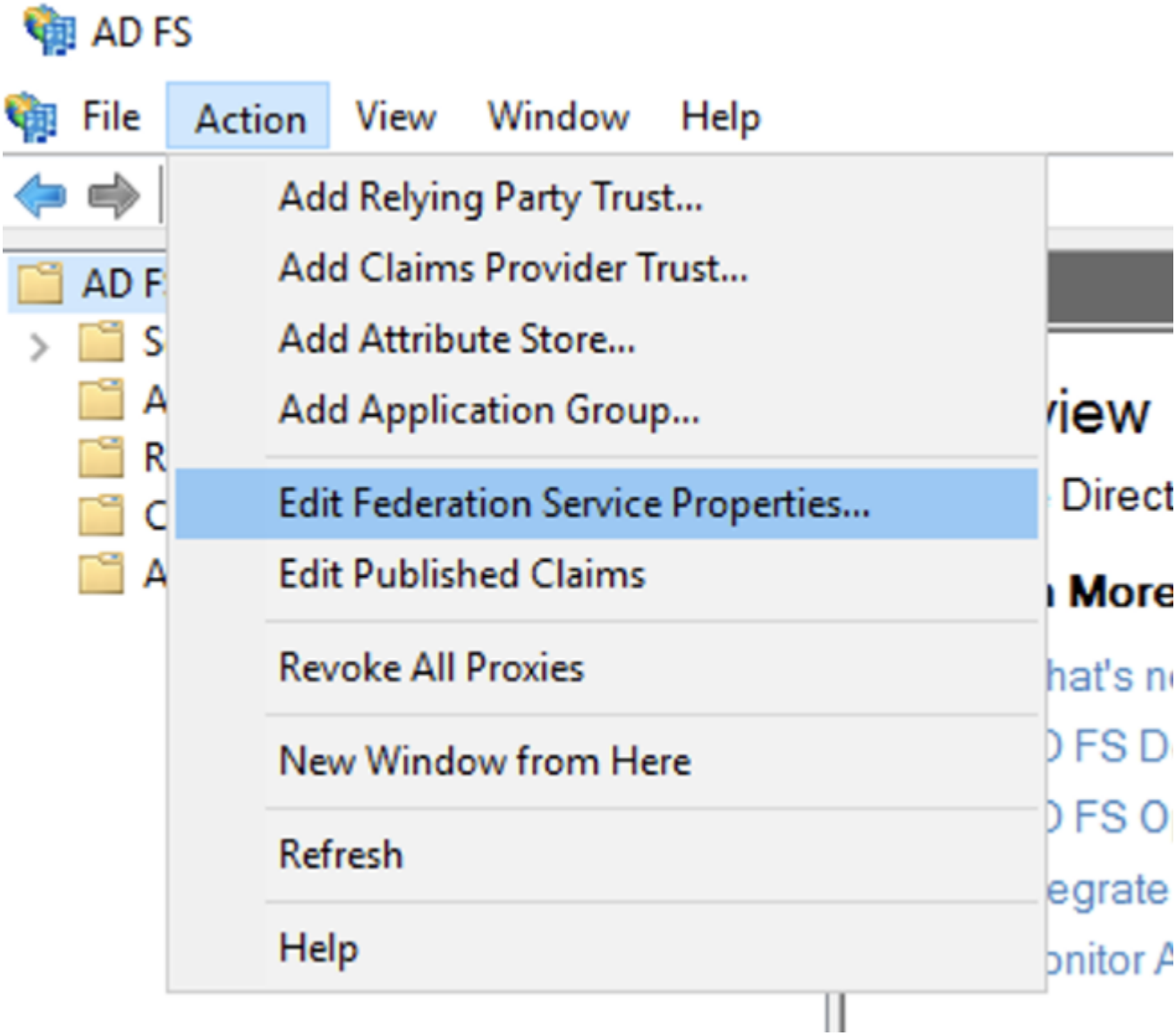
В консоли управления откройте **Endpoints** и убедитесь, что для параметра **Proxy Enabled** у `/adfs/ls/` установлено значение `Yes`. Этот параметр отвечает за активацию страницы аутентификации в AD FS, которая должна быть доступна извне, — адрес вида `https://домен_ADFS/adfs/ls/idpinitiatedsignon.aspx`.



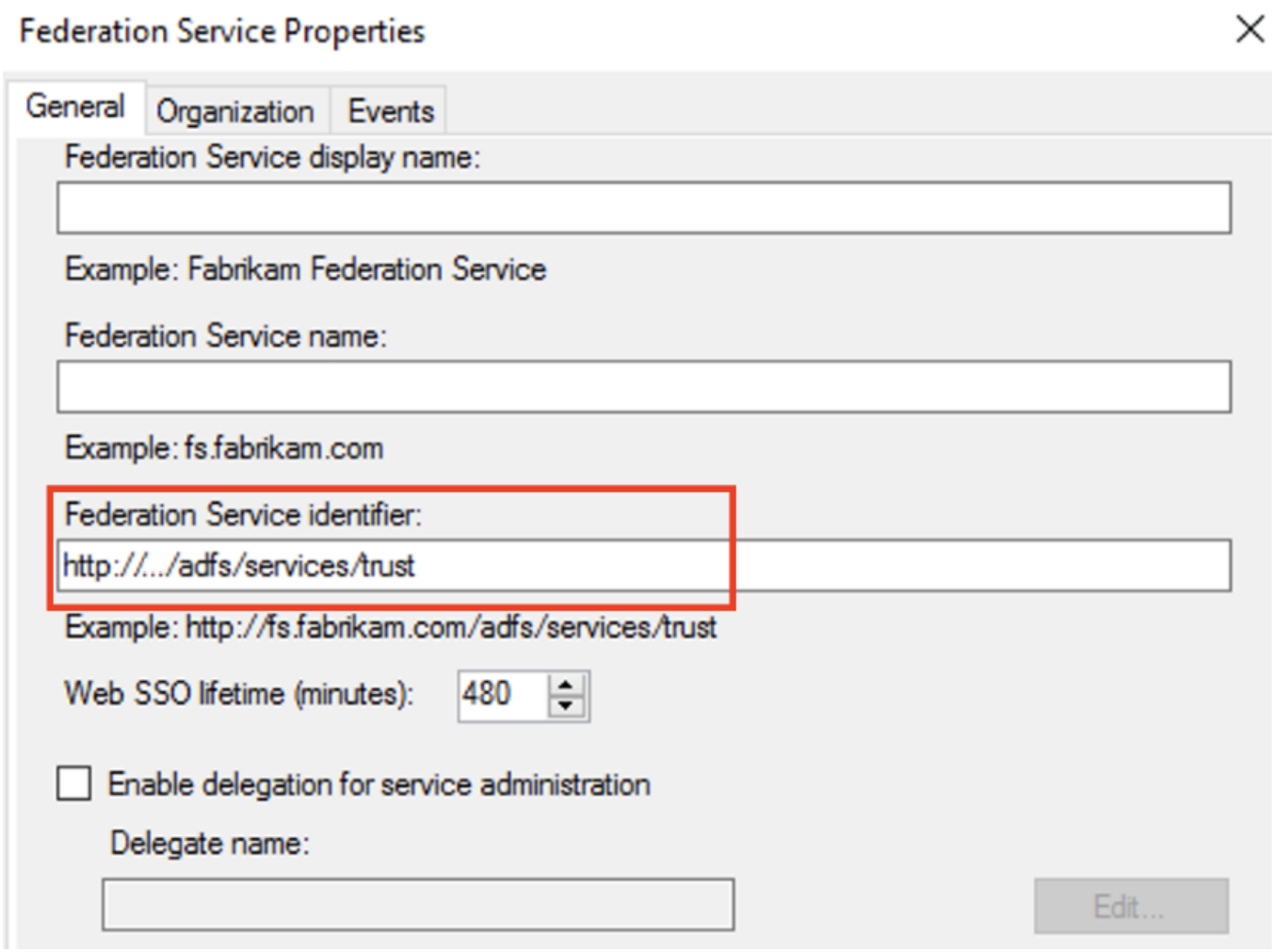
Издатель поставщика удостоверений

Entity ID домена. Как правило, это `http://домен/adfs/services/trust`.

Чтобы получить его, в консоли управления перейдите на вкладку **Action** и выберите **Edit Federation Service Properties**.



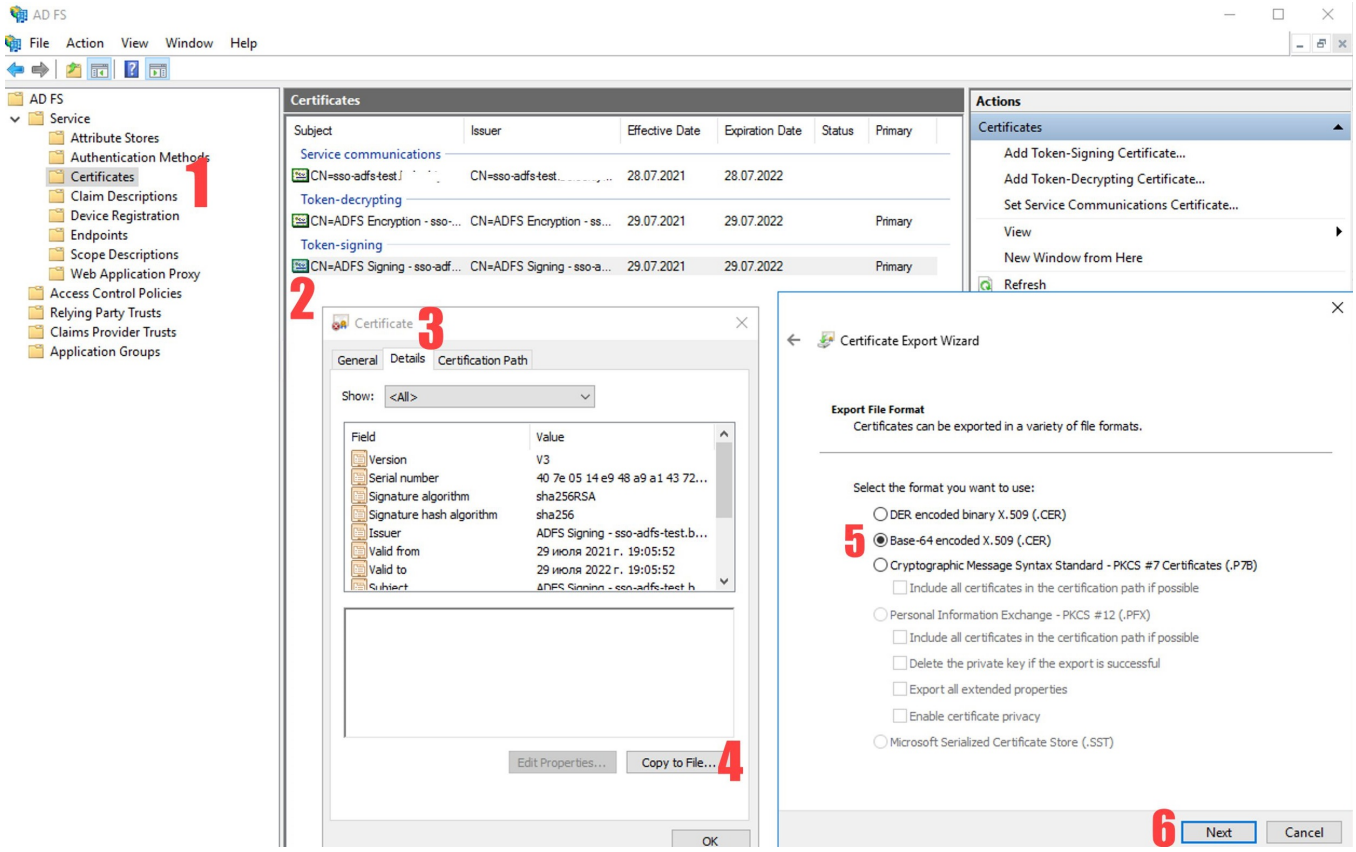
Нужное значение находится в поле **Federation Service identifier**.



Проверочный сертификат

Сертификат подписи токенов формата X.509 в Base64. Чтобы получить:

1. В консоли управления откройте **Certificates**.
2. Нажмите два раза на ваш сертификат **Token-signing**.
3. Перейдите на вкладку **Details** и нажмите **Copy to File**.
4. Выберите тип сертификата **Base-64 encoded X.509 (.CER)** и нажмите **Next**.
5. Сохраните файл на жесткий диск.



Если у вас два активных сертификата подписи токенов и вы не уверены, какой сертификат используется сейчас, повторите аналогичные действия для второго сертификата.

Шаг 5. Настройте синхронизацию сотрудников SCIM

По умолчанию новые сотрудники появляются в Яндекс 360 только после первой авторизации, а бывших сотрудников нужно удалять вручную. Если вы хотите автоматически синхронизировать список сотрудников из AD FS с Яндекс 360 для бизнеса, подключите синхронизацию SCIM.

Проблемы с настройкой

Если заданы неверные значения атрибутов, при входе через SSO вы увидите сообщение «Авторизация не удалась» и код ошибки:

email.no_in_response

Указывайте имена атрибутов в формате `User.Firstname`, `User.Surname`, `User.EmailAddress`. Если задать другой формат, например `Firstname`, авторизоваться не получится.

request_your_admin

Ошибка появляется, если администратор каталога пользователей вашей организации, например Active Directory или Keycloak, ограничил для аккаунта доступ к Яндекс 360. За подробной информацией обратитесь к специалистам технической поддержки вашей организации.

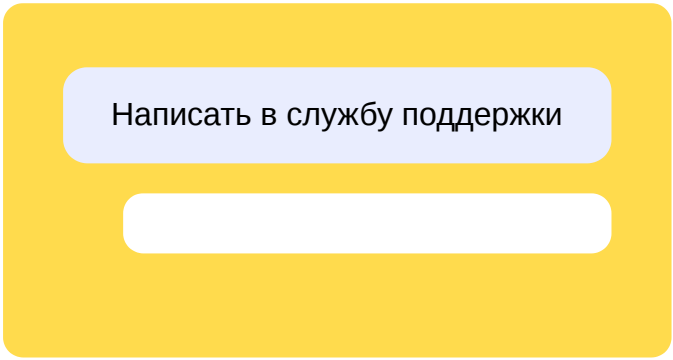
samlresponse.invalid

Ошибка возникает, если неверно указаны URL страницы входа, издатель поставщика удостоверений или проверочный сертификат. Также она может возникнуть в течение 14 дней

до истечения проверочного сертификата или после его истечения. Проверьте корректность настроек SSO в Яндекс 360 для бизнеса.

unsupportable_domain

Проверьте, что домен из почтового атрибута `User.EmailAddress` в SAML response такой же, как и основной домен или один из доменов-алиасов организации Яндекс 360.



Настройка Azure Active Directory

Если вы используете интерфейс центра администрирования Azure Active Directory на английском языке, воспользуйтесь этой инструкцией.

Чтобы организовать единый вход (SSO) в сервисы Яндекс 360 через Azure Active Directory, нужно предварительно создать и настроить SAML-приложение.

Шаг 1. Создайте и настройте SAML-приложение

1. Войдите в центр администрирования Azure Active Directory.
2. В разделе **Azure Active Directory** на панели слева перейдите на вкладку **Корпоративные приложения**.
3. Создайте SAML-приложение:
   3.1. Нажмите кнопку **Новое приложение**.
   3.2. На вкладке **Обзор коллекции Azure AD** нажмите кнопку **Создайте собственное приложение**.
   3.3. В правой части открывшегося окна введите название приложения, например `yandexsso`.
   3.4. Выберите вариант приложения: **Интеграция с любыми другими приложениями, которых нет в коллекции (вне коллекции)**.
   3.5. Нажмите кнопку **Создать**.

   На вкладке **Корпоративные приложения** в списке **Все приложения** добавится созданное приложение.
4. Выберите ваше приложение в списке.

   Если вы не хотите специально назначать пользователей, которые могут пользоваться единым входом (SSO), на вкладке **Свойства** для параметра **Назначение обязательно** выберите значение **Нет**. Чтобы сохранить настройки, наверху вкладки нажмите кнопку **Сохранить**.

   Чтобы назначить отдельных пользователей для использования единого входа (SSO), на вкладке **Свойства** для параметра **Назначение обязательно** выберите значение **Да**. Затем перейдите на вкладку **Пользователи и группы**, нажмите **Добавить пользователя или группу** и укажите нужных пользователей.
5. Перейдите на вкладку **Единый вход** и выберите способ единого входа **SAML**.
6. В окне **Настройка единого входа с помощью SAML** в разделе **Базовая конфигурация SAML** нажмите кнопку **Изменить** и установите параметры:
   6.1. **Идентификатор (сущности)**: `https://yandex.ru/` (обязательно с косой чертой в конце).
   6.2. **URL-адрес ответа (URL-адрес службы обработчика утверждений)**: `https://passport.yandex.ru/auth/sso/commit`.
   6.3. **URL-адрес для входа** (необязательный параметр): `https://passport.yandex.ru/auth/sso/commit`.
   6.4. Если ваши сотрудники пользуются сервисами не только на русском языке, в полях **URL-адрес ответа (URL-адрес службы обработчика утверждений)** и **URL-адрес для входа** дополнительно добавьте URL других языковых доменов. Например:

   `https://passport.yandex.com/auth/sso/commit` — для английского;

`https://passport.yandex.kz/auth/sso/commit` — для казахского;

`https://passport.yandex.uz/auth/sso/commit` — для узбекского;

`https://passport.yandex.com.tr/auth/sso/commit` — для турецкого.

Полный список

`https://passport.yandex.com/auth/sso/commit`

`https://passport.yandex.az/auth/sso/commit`

`https://passport.yandex.by/auth/sso/commit`

`https://passport.yandex.co.il/auth/sso/commit`

`https://passport.yandex.com/auth/sso/commit`

`https://passport.yandex.com.am/auth/sso/commit`

`https://passport.yandex.com.ge/auth/sso/commit`

`https://passport.yandex.com.tr/auth/sso/commit`

`https://passport.yandex.ee/auth/sso/commit`

`https://passport.yandex.eu/auth/sso/commit`

`https://passport.yandex.fi/auth/sso/commit`

`https://passport.yandex.fr/auth/sso/commit`

`https://passport.yandex.kg/auth/sso/commit`

`https://passport.yandex.kz/auth/sso/commit`

`https://passport.yandex.lt/auth/sso/commit`

`https://passport.yandex.lv/auth/sso/commit`

`https://passport.yandex.md/auth/sso/commit`

`https://passport.yandex.pl/auth/sso/commit`

`https://passport.yandex.ru/auth/sso/commit`

`https://passport.yandex.tj/auth/sso/commit`

`https://passport.yandex.tm/auth/sso/commit`

`https://passport.yandex.ua/auth/sso/commit`

`https://passport.yandex.uz/auth/sso/commit`

6.5. Нажмите **Сохранить**.

Шаг 2. Настройте сопоставление атрибутов пользователей

1. Перейдите в **Корпоративные приложения** → **Все приложения** → <ваше приложение> → **Единый вход**, чтобы синхронизировать атрибуты пользователей в Azure Active Directory и Яндекс 360.
2. В разделе **Атрибуты и утверждения** выберите **Уникальный идентификатор пользователя**.
3. Чтобы имя и фамилия пользователя корректно отображались в Яндекс 360, в группе настроек **Обязательные утверждения** в поле **Источник** выберите **Атрибут**, а в поле **Атрибут источника** введите `user.mail`, затем нажмите **Сохранить**. Убедитесь, что поле **Пространство имен** везде осталось пустым.
4. В группе настроек **Дополнительные утверждения** измените существующие утверждения или удалите и создайте их заново:

Имя утверждения	Значение
User.EmailAddress	user.mail
User.Firstname	user.givenname
User.Surname	user.surname

Убедитесь, что поле **Пространство имен** осталось пустым.

Пример SAML-запроса:

```
<Attribute Name="User.EmailAddress">
   <AttributeValue>email@test.com</AttributeValue>
</Attribute>
<Attribute Name="User.Surname">
   <AttributeValue>Surname</AttributeValue>
</Attribute>
<Attribute Name="User.Firstname">
   <AttributeValue>Firstname</AttributeValue>
</Attribute>
```

Шаг 3. Сохраните сертификат

1. Перейдите в **Корпоративные приложения** → **Все приложения** → <ваше приложение> → **Единый вход**.
2. В разделе **Сертификаты SAML** рядом с параметром **Сертификат (Base64)** нажмите **Скачать**. Сохраните файл на жесткий диск.

Сохраненный файл с расширением `.cer` можно открыть в любом текстовом редакторе.

Шаг 4. Соберите данные, которые нужно будет передать Яндекс 360

Для дальнейшей настройки в Яндекс 360 вам понадобится сертификат, полученный на шаге 3, и значения параметров конфигурации:

- **URL-адрес входа**
- **Идентификатор Azure AD**

Чтобы сохранить значения параметров:

1. На вкладке **Корпоративные приложения** → **Все приложения** → <ваше приложение> → **Единый вход** перейдите в раздел **Настройка** <название приложения>.
2. Скопируйте значения полей **URL-адрес входа** и **Идентификатор Azure AD** в любое удобное место.

После этого переходите к настройке Яндекс 360 для бизнеса.

Решение проблем с настройкой

Если в процессе настройки поставщика удостоверений заданы неверные значения, то при попытке входа через SSO вы увидите сообщение «Авторизация не удалась» и код ошибки:

email.no_in_response

Указывайте имена атрибутов в формате `User.Firstname`, `User.Surname`, `User.EmailAddress`. Если задать другой формат, например `Firstname`, авторизоваться не получится.

request_your_admin

Ошибка появляется, если администратор каталога пользователей вашей организации ограничил для аккаунта доступ к Яндекс 360. За подробной информацией обратитесь к специалистам технической поддержки вашей организации.

samlresponse.invalid

Ошибка возникает, если неверно указаны URL страницы входа, издатель поставщика удостоверений или проверочный сертификат. Также она может возникнуть в течение 14 дней до истечения проверочного сертификата или после его истечения. Проверьте корректность настроек SSO в Яндекс 360 для бизнеса.

unsupportable_domain

Проверьте, что домен из почтового атрибута `User.EmailAddress` в SAML response такой же, как и основной домен или один из доменов-алиасов организации Яндекс 360. Если они не совпадают, вы увидите сообщение об ошибке.

Написать в службу поддержки

Настройка Azure Active Directory (английский интерфейс)

Чтобы организовать единый вход (SSO) в сервисы Яндекс 360 через Azure Active Directory, нужно предварительно создать и настроить SAML-приложение.

Шаг 1. Создайте и настройте SAML-приложение

1. Войдите в центр администрирования Azure Active Directory.
2. В разделе **Azure Active Directory** на панели слева перейдите на вкладку **Enterprise applications**.
3. Создайте SAML-приложение:
   3.1. Нажмите кнопку **New application**.
   3.2. На вкладке **Browse Azure AD Gallery** нажмите кнопку **Create your own application**.
   3.3. В правой части открывшегося окна введите название приложения, например `yandexsso`.
   3.4. Выберите вариант приложения: **Integrate any other application you don't find in the gallery (Non-gallery)**.
   3.5. Нажмите кнопку **Create**.

   На вкладке **Enterprise applications** в списке **All applications** добавится созданное приложение.
4. Выберите ваше приложение в списке.

   Если вы не хотите специально назначать пользователей, которые могут пользоваться единым входом (SSO), на вкладке **Properties** для параметра **Assign Required** выберите значение **No**. Чтобы сохранить настройки, наверху вкладки нажмите кнопку **Save**.

   Чтобы назначить отдельных пользователей для использования единого входа (SSO), на вкладке **Properties** для параметра **Assign Required** выберите значение **Yes**. Затем перейдите на вкладку **Пользователи и группы**, нажмите **Добавить пользователя или группу** и укажите нужных пользователей.
5. Перейдите на вкладку **Single sign-on** и выберите способ единого входа **SAML**.
6. В окне **Set up Single Sign-On with SAML** в разделе **Basic SAML Configuration** нажмите кнопку **Edit** и установите параметры:
   6.1. **Identifier (Entity ID)**: `https://yandex.ru/` (обязательно с косой чертой в конце).
   6.2. **Reply URL (Assertion Consumer Service URL)**: `https://passport.yandex.ru/auth/sso/commit`.
   6.3. **Sign on URL** (необязательный параметр): `https://passport.yandex.ru/auth/sso/commit`.
   6.4. Если ваши сотрудники пользуются сервисами не только на русском языке, в полях **Reply URL (Assertion Consumer Service URL)** и **Sign on URL** дополнительно добавьте URL других языковых доменов. Например:

   `https://passport.yandex.com/auth/sso/commit` — для английского;

   `https://passport.yandex.kz/auth/sso/commit` — для казахского;

   `https://passport.yandex.uz/auth/sso/commit` — для узбекского;

`https://passport.yandex.com.tr/auth/sso/commit` — для турецкого.

Полный список

`https://passport.yandex.com/auth/sso/commit`

`https://passport.yandex.az/auth/sso/commit`

`https://passport.yandex.by/auth/sso/commit`

`https://passport.yandex.co.il/auth/sso/commit`

`https://passport.yandex.com/auth/sso/commit`

`https://passport.yandex.com.am/auth/sso/commit`

`https://passport.yandex.com.ge/auth/sso/commit`

`https://passport.yandex.com.tr/auth/sso/commit`

`https://passport.yandex.ee/auth/sso/commit`

`https://passport.yandex.eu/auth/sso/commit`

`https://passport.yandex.fi/auth/sso/commit`

`https://passport.yandex.fr/auth/sso/commit`

`https://passport.yandex.kg/auth/sso/commit`

`https://passport.yandex.kz/auth/sso/commit`

`https://passport.yandex.lt/auth/sso/commit`

`https://passport.yandex.lv/auth/sso/commit`

`https://passport.yandex.md/auth/sso/commit`

`https://passport.yandex.pl/auth/sso/commit`

`https://passport.yandex.ru/auth/sso/commit`

`https://passport.yandex.tj/auth/sso/commit`

`https://passport.yandex.tm/auth/sso/commit`

`https://passport.yandex.ua/auth/sso/commit`

`https://passport.yandex.uz/auth/sso/commit`

6.5. Нажмите **Save**.

Шаг 2. Настройте сопоставление атрибутов пользователей

1. Перейдите в **Enterprise applications** → **All applications** → <ваше приложение> → **SAML-based Sign-on**, чтобы синхронизировать атрибуты пользователей в Azure Active Directory и Яндекс 360.
2. В разделе **Attributes & Claims** выберите **Unique User Identifier (Name ID)**.
3. Чтобы имя и фамилия пользователя корректно отображались в Яндекс 360, в поле **Source attribute** группы настроек **Required claim** введите `user.mail`, а затем нажмите **Save**.
4. В группе настроек **Additional claims** измените существующие утверждения или удалите и создайте их заново:

Claim name	Value
User.EmailAddress	user.mail
User.Firstname	user.givenname
User.Surname	user.surname

Пример SAML-запроса:

```
<Attribute Name="User.EmailAddress">
   <AttributeValue>email@test.com</AttributeValue>
</Attribute>
<Attribute Name="User.Surname">
   <AttributeValue>Surname</AttributeValue>
</Attribute>
<Attribute Name="User.Firstname">
   <AttributeValue>Firstname</AttributeValue>
</Attribute>
```

Шаг 3. Сохраните сертификат

1. Перейдите в **Enterprise applications** → **All applications** → <ваше приложение> → **SAML-based Sign-on**.
2. В разделе **SAML Signing Certificate** рядом с параметром **Certificate (Base64)** нажмите **Download**. Сохраните файл на жесткий диск.
   Сохраненный файл с расширением `.cer` можно открыть в любом текстовом редакторе.

Шаг 4. Соберите данные, которые нужно будет передать Яндекс 360

Для дальнейшей настройки в Яндекс 360 вам понадобится сертификат, полученный на шаге 3, и значения параметров конфигурации:

- **Login URL**
- **Azure AD Identifier**

Чтобы сохранить значения параметров:

1. **Enterprise applications** → **All applications** → <ваше приложение> → **SAML-based Sign-on** → перейдите в раздел **Set up** <название приложения>.
2. Скопируйте значения полей **Login URL** и **Azure AD Identifier** в любое удобное место.

После этого переходите к настройке Яндекс 360 для бизнеса.

Решение проблем с настройкой

Если в процессе настройки поставщика удостоверений заданы неверные значения, то при попытке входа через SSO вы увидите сообщение «Авторизация не удалась» и код ошибки:

email.no_in_response

Указывайте имена атрибутов в формате `User.Firstname`, `User.Surname`, `User.EmailAddress`. Если задать другой формат, например `Firstname`, авторизоваться не получится.

request_your_admin

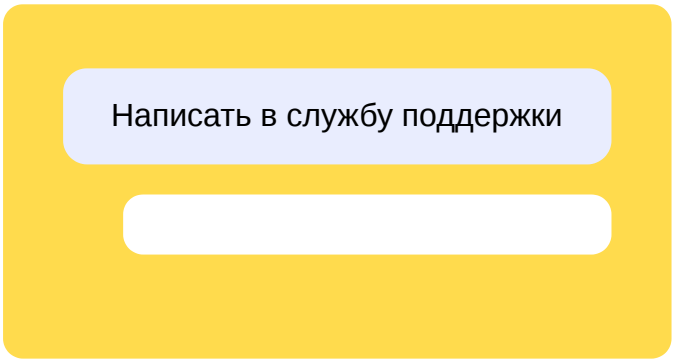
Ошибка появляется, если администратор каталога пользователей вашей организации ограничил для аккаунта доступ к Яндекс 360. За подробной информацией обратитесь к специалистам технической поддержки вашей организации.

samlresponse.invalid

Ошибка возникает, если неверно указаны URL страницы входа, издатель поставщика удостоверений или проверочный сертификат. Также она может возникнуть в течение 14 дней до истечения проверочного сертификата или после его истечения. Проверьте корректность настроек SSO в Яндекс 360 для бизнеса.

unsupportable_domain

Проверьте, что домен из почтового атрибута `User.EmailAddress` в SAML response такой же, как и основной домен или один из доменов-алиасов организации Яндекс 360. Если они не совпадают, вы увидите сообщение об ошибке.



Настройка Keycloak версии 18

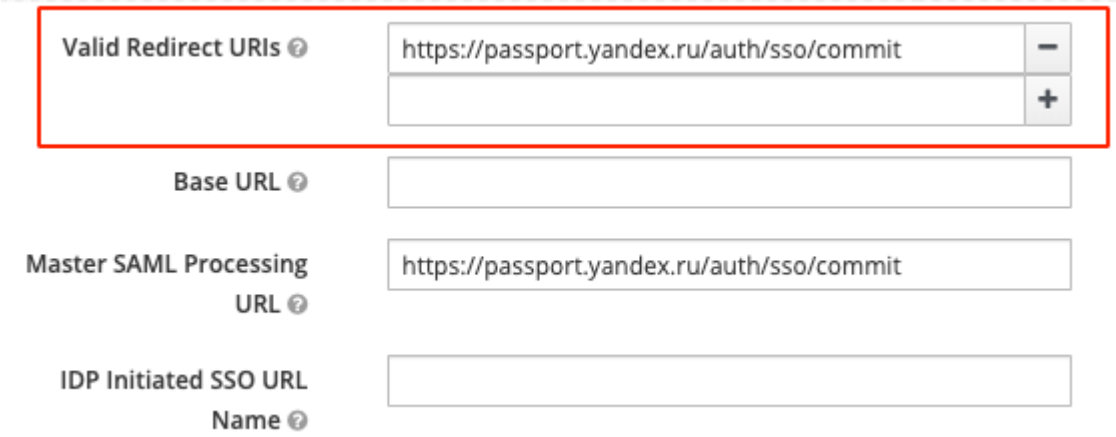
Чтобы организовать единый вход (SSO) в сервисы Яндекс 360 через Keycloak, нужно предварительно создать и настроить SAML-приложение.

Шаг 1. Создайте и настройте SAML-приложение

1. Войдите в аккаунт администратора Keycloak.
2. Откройте консоль управления — нажмите **Administration Console**.
3. Создайте SAML-приложение:
   3.1. На панели слева выберите **Clients** и нажмите кнопку **Create**.
   3.2. В поле **Client ID** введите `https://yandex.ru/` (обязательно с косой чертой в конце).
   3.3. В поле **Client Protocol** укажите **saml**.
   3.4. В поле **Client SAML Endpoint** введите Service URL: `https://passport.yandex.ru/auth/sso/commit`. Нажмите **Save**.
4. На вкладке **Settings** настройте параметры SAML-приложения:
   4.1. В поле **Name** укажите имя приложения, например `yandex360`.
   4.2. Выключите опцию **Client Signature Required**, если она включена.
   4.3. Опции, заполненные по умолчанию (**Enabled**, **Include AuthnStatement**, **Sign Documents** и др.), оставьте без изменений.
   4.4. В качестве **Name ID Format** выберите email. Чтобы выбранный вариант передавался вне зависимости от настроек Яндекс 360, включите опцию **Force Name ID format**.

> **Примечание**
>
> Значение атрибута **NameID** нельзя изменить — он используется для идентификации пользователя в Яндекс ID. Если вы меняете UPN, в качестве **NameID** укажите один из неизменяемых атрибутов пользователей в вашем каталоге LDAP.
>
> Если нужен настраиваемый **NameID**, задайте его по умолчанию в настройках сопоставления атрибутов пользователя: в меню **Mappers** создайте новый **User Attribute Mapper For NameID**.

   4.5. В полях **Valid Redirect URIs**, **Base URL**, **Master SAML Processing URL** введите Service URL: `https://passport.yandex.ru/auth/sso/commit`. Нажмите **Save**.
   4.6. Если ваши сотрудники пользуются сервисами Яндекс 360 не только на русском домене, в поле **Valid Redirect URIs** дополнительно добавьте URL языковых доменов в качестве конечных точек.



Конечные точки для языковых доменов:

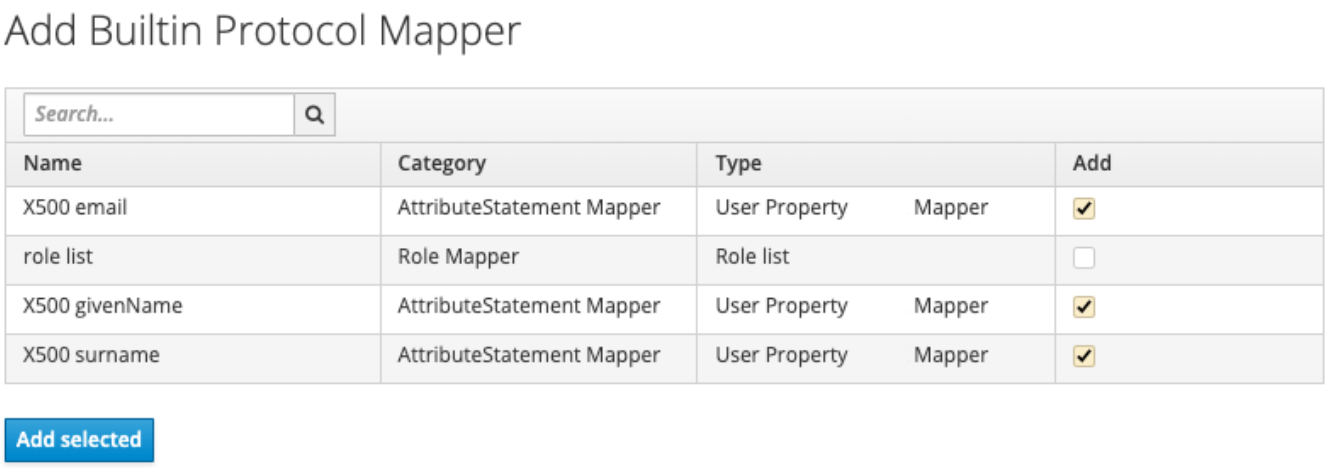
- `https://passport.yandex.com/auth/sso/commit` — для английского;
- `https://passport.yandex.kz/auth/sso/commit` — для казахского;
- `https://passport.yandex.uz/auth/sso/commit` — для узбекского;
- `https://passport.yandex.com.tr/auth/sso/commit` — для турецкого.

Полный список

- `https://passport.yandex.com/auth/sso/commit`
- `https://passport.yandex.az/auth/sso/commit`
- `https://passport.yandex.by/auth/sso/commit`
- `https://passport.yandex.co.il/auth/sso/commit`
- `https://passport.yandex.com/auth/sso/commit`
- `https://passport.yandex.com.am/auth/sso/commit`
- `https://passport.yandex.com.ge/auth/sso/commit`
- `https://passport.yandex.com.tr/auth/sso/commit`
- `https://passport.yandex.ee/auth/sso/commit`
- `https://passport.yandex.eu/auth/sso/commit`
- `https://passport.yandex.fi/auth/sso/commit`
- `https://passport.yandex.fr/auth/sso/commit`
- `https://passport.yandex.kg/auth/sso/commit`
- `https://passport.yandex.kz/auth/sso/commit`
- `https://passport.yandex.lt/auth/sso/commit`
- `https://passport.yandex.lv/auth/sso/commit`
- `https://passport.yandex.md/auth/sso/commit`
- `https://passport.yandex.pl/auth/sso/commit`
- `https://passport.yandex.ru/auth/sso/commit`
- `https://passport.yandex.tj/auth/sso/commit`
- `https://passport.yandex.tm/auth/sso/commit`
- `https://passport.yandex.uz/auth/sso/commit`

Шаг 2. Настройте сопоставление атрибутов пользователей

1. На вкладке **Scope** отключите опцию **Full Scope Allowed**.
2. Перейдите на вкладку **Mappers** и нажмите кнопку **Add Builtin**.
3. Отметьте атрибуты в списке и нажмите **Add selected**:
   - `X500 email` — адрес электронной почты;
   - `X500 surname` — фамилия;
   - `X500 givenName` — имя.



4. Настройте синхронизацию атрибутов Keycloak и Яндекс 360: откройте каждый атрибут и измените значение SAML Attribute Name. Значения SAML Attribute Name, которые поддерживаются в Яндекс 360, приведены ниже.

SAML Attribute Name	Value
User.EmailAddress	X500 email
User.Firstname	X500 givenName
User.Surname	X500 surname

В итоге сопоставление атрибутов будет выглядеть так:

Clients > https://yandex.ru/ > Mappers > X500 email

X500 Email

Protocol	saml
ID	d00eb0c3-44af-4737-87ae-87a6c20720b1
Name	X500 email
Mapper Type	User Property
Property	email
Friendly Name	
SAML Attribute Name	User.EmailAddress
SAML Attribute NameFormat	

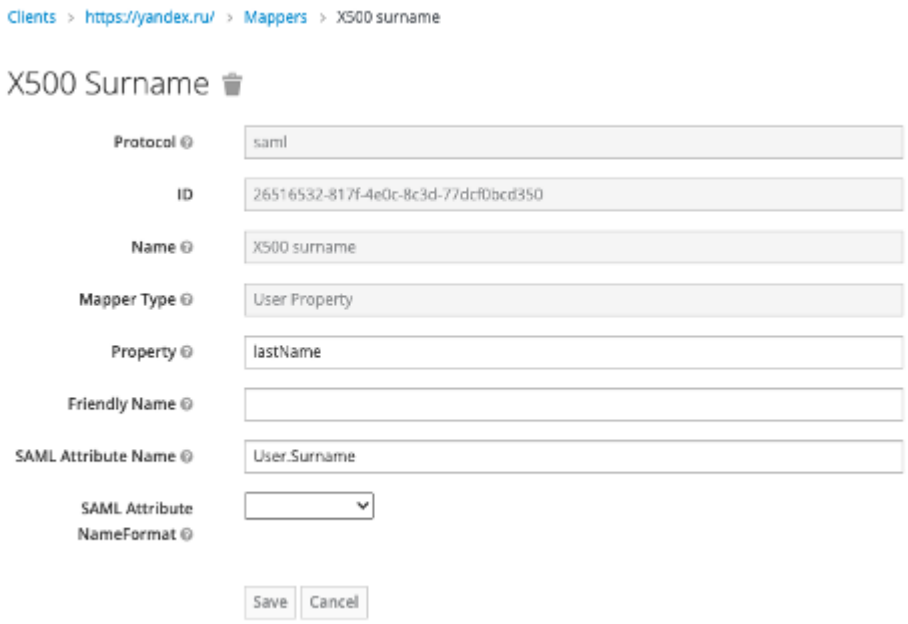
Save Cancel

Clients > https://yandex.ru/ > Mappers > X500 givenName

X500 GivenName

Protocol	saml
ID	3156de84-726c-4558-8671-02372e61fe5b
Name	X500 givenName
Mapper Type	User Property
Property	firstName
Friendly Name	
SAML Attribute Name	User.Firstname
SAML Attribute NameFormat	

Save Cancel



Ответ SAML должен иметь вид:

```
<Attribute Name="User.EmailAddress">
    <AttributeValue>email@test.com</AttributeValue>
</Attribute>
<Attribute Name="User.Surname">
    <AttributeValue>Surname</AttributeValue>
</Attribute>
<Attribute Name="User.Firstname">
    <AttributeValue>Firstname</AttributeValue>
</Attribute>
```

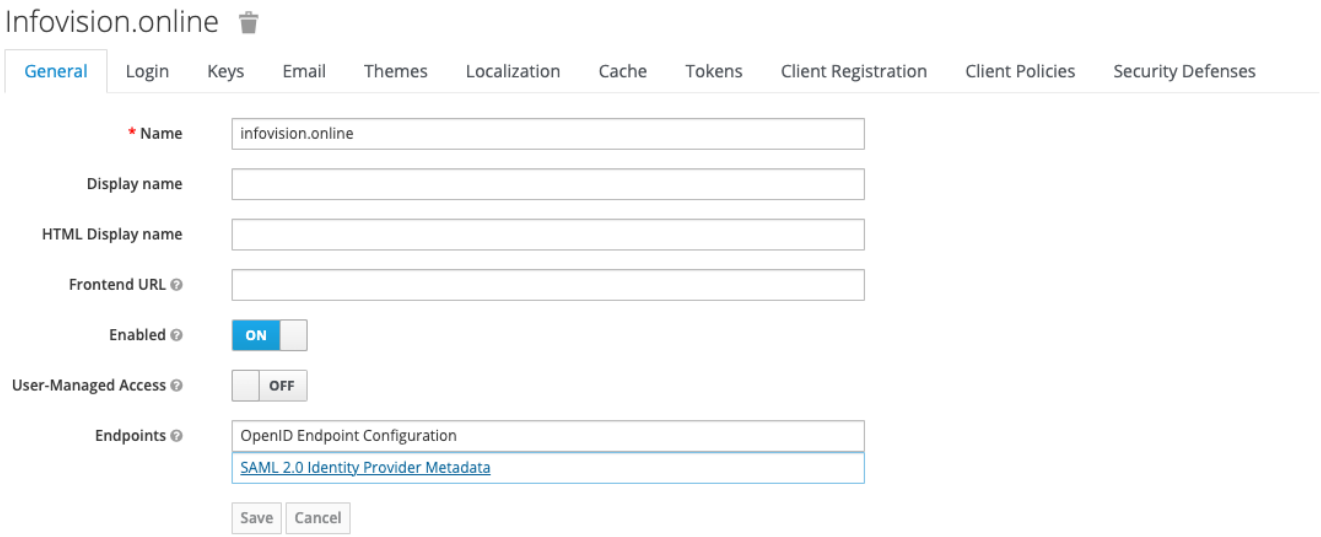
Шаг 3. Соберите данные, которые нужно будет передать Яндекс 360

URL страницы входа

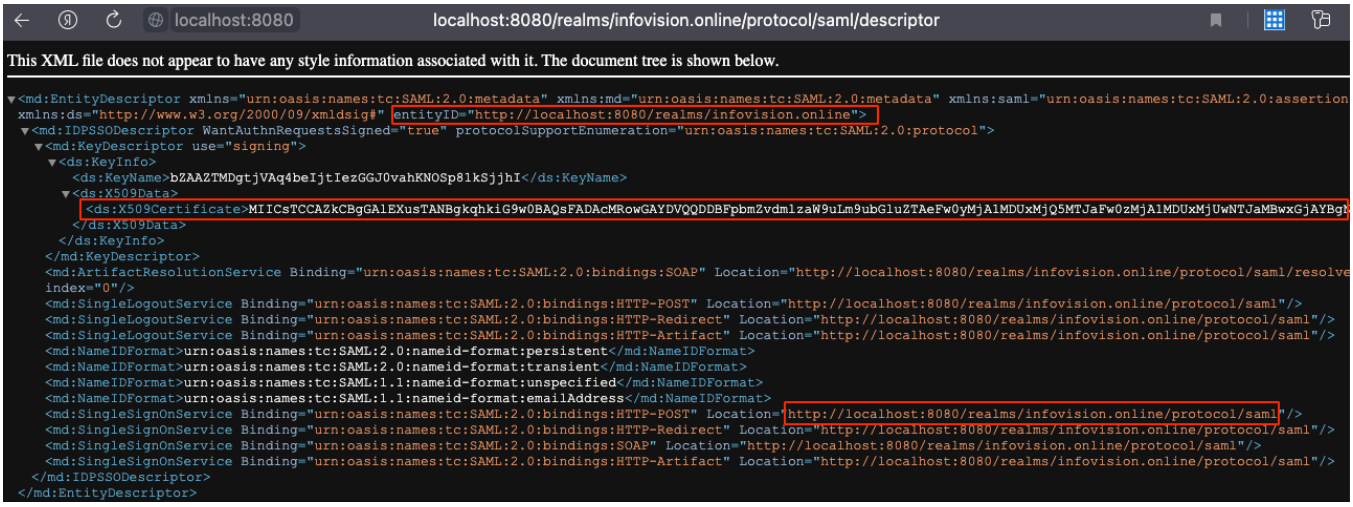
Адрес точки входа.

Чтобы получить:

1. В консоли управления на панели слева выберите **Realm Settings** и нажмите ссылку **SAML 2.0 Identity Provider Metadata**.



2. Нужное значение находится в поле **Location**, скопируйте его.



Издатель поставщика удостоверений

Entity ID домена.

Получить можно так же, как и **URL страницы входа**. Нужное значение находится в поле **entityID**.

Проверочный сертификат

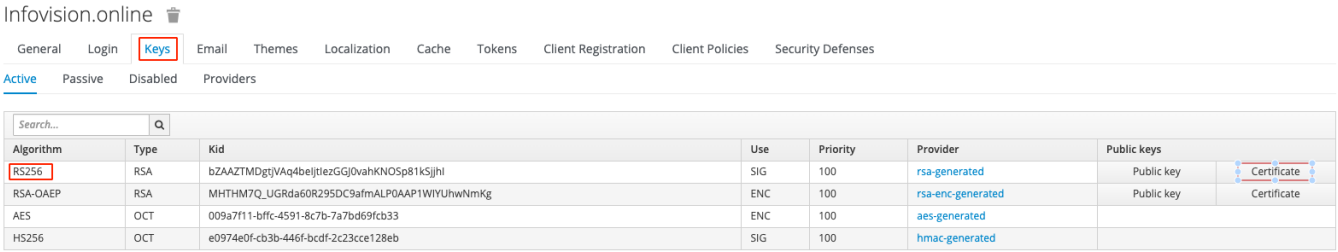
Сертификат подписи токенов формата X.509.

Получить можно так же, как и **URL страницы входа**. Нужное значение находится в поле **X509Certificate**.

Также сертификат можно скопировать со вкладки **Keys**:

1. Перейдите к строке RS256.

2. Скопируйте содержимое **Certificate**.



Если у вас два активных сертификата подписи токенов и вы не уверены, какой сертификат используется сейчас, повторите аналогичные действия для второго сертификата.

После этого переходите к настройке Яндекс 360 для бизнеса.

Решение проблем с настройкой

Если в процессе настройки поставщика удостоверений заданы неверные значения, то при попытке входа через SSO вы увидите сообщение «Авторизация не удалась» и код ошибки:

email.no_in_response

Указывайте имена атрибутов в формате `User.Firstname`, `User.Surname`, `User.EmailAddress`. Если задать другой формат, например `Firstname`, авторизоваться не получится.

request_your_admin

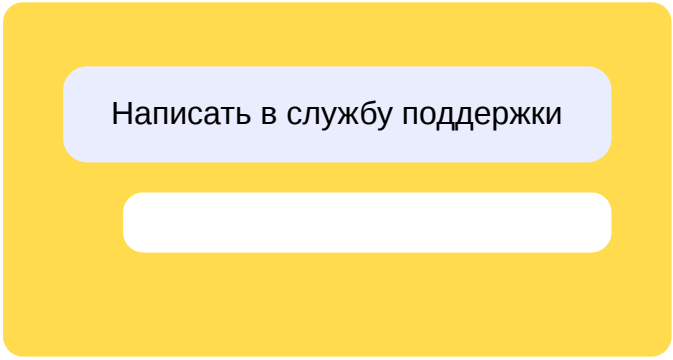
Ошибка появляется, если администратор каталога пользователей вашей организации ограничил для аккаунта доступ к Яндекс 360. За подробной информацией обратитесь к специалистам технической поддержки вашей организации.

samlresponse.invalid

Ошибка возникает, если неверно указаны URL страницы входа, издатель поставщика удостоверений или проверочный сертификат. Также она может возникнуть в течение 14 дней до истечения проверочного сертификата или после его истечения. Проверьте корректность настроек SSO в Яндекс 360 для бизнеса.

unsupportable_domain

Проверьте, что домен из почтового атрибута `User.EmailAddress` в SAML response такой же, как и основной домен или один из доменов-алиасов организации Яндекс 360. Если они не совпадают, вы увидите сообщение об ошибке.

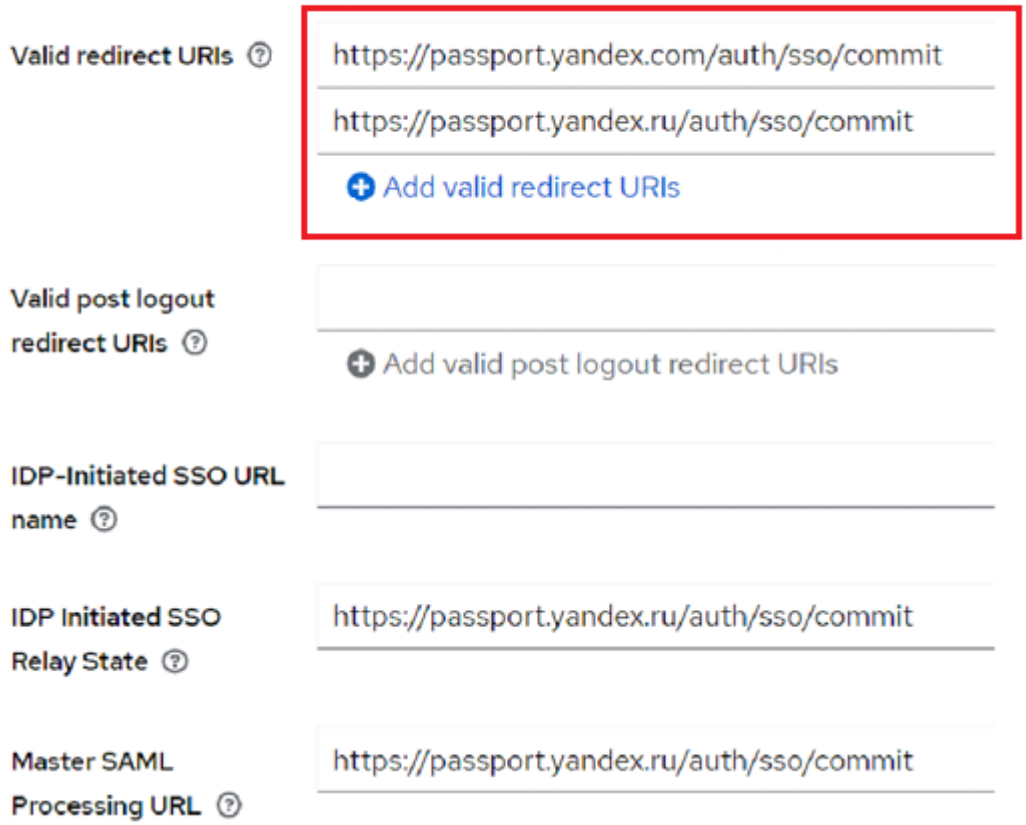


Настройка Keycloak версии 19 и выше

Чтобы организовать единый вход (SSO) в сервисы Яндекс 360 через Keycloak, нужно предварительно создать и настроить SAML-приложение.

Шаг 1. Создайте и настройте SAML-приложение

1. Войдите в аккаунт администратора Keycloak.
2. Откройте консоль управления — нажмите **Administration Console**.
3. Создайте SAML-приложение и настройте его:
   3.1. На панели слева выберите **Clients** и нажмите кнопку **Create Client**.
   3.2. В поле **Client ID** введите `https://yandex.ru/` (обязательно с косой чертой в конце).
   3.3. В поле **Client type** укажите **SAML** и нажмите **Save**.
   3.4. В поле **Name** укажите имя приложения, например `yandex360`.
   3.5. В поле **Root URL** введите Service URL: `https://passport.yandex.ru/auth/sso/commit`.
   3.6. В поле **Valid Redirect URIs** введите Service URL: `https://passport.yandex.ru/auth/sso/commit` и `https://passport.yandex.com/auth/sso/commit`. Если ваши сотрудники пользуются сервисами Яндекс 360 на языковых доменах, дополнительно добавьте их URL в качестве конечных точек.



Конечные точки для языковых доменов:

- `https://passport.yandex.com/auth/sso/commit` — для английского;
- `https://passport.yandex.kz/auth/sso/commit` — для казахского;

- `https://passport.yandex.uz/auth/sso/commit` — для узбекского;
- `https://passport.yandex.com.tr/auth/sso/commit` — для турецкого.

Полный список

- `https://passport.yandex.com/auth/sso/commit`
- `https://passport.yandex.az/auth/sso/commit`
- `https://passport.yandex.by/auth/sso/commit`
- `https://passport.yandex.co.il/auth/sso/commit`
- `https://passport.yandex.com/auth/sso/commit`
- `https://passport.yandex.com.am/auth/sso/commit`
- `https://passport.yandex.com.ge/auth/sso/commit`
- `https://passport.yandex.com.tr/auth/sso/commit`
- `https://passport.yandex.ee/auth/sso/commit`
- `https://passport.yandex.eu/auth/sso/commit`
- `https://passport.yandex.fi/auth/sso/commit`
- `https://passport.yandex.fr/auth/sso/commit`
- `https://passport.yandex.kg/auth/sso/commit`
- `https://passport.yandex.kz/auth/sso/commit`
- `https://passport.yandex.lt/auth/sso/commit`
- `https://passport.yandex.lv/auth/sso/commit`
- `https://passport.yandex.md/auth/sso/commit`
- `https://passport.yandex.pl/auth/sso/commit`
- `https://passport.yandex.ru/auth/sso/commit`
- `https://passport.yandex.tj/auth/sso/commit`
- `https://passport.yandex.tm/auth/sso/commit`
- `https://passport.yandex.uz/auth/sso/commit`

3.7. В полях **IDP Initiated SSO Relay State** и **Master SAML Processing URL** введите Service URL: `https://passport.yandex.ru/auth/sso/commit`.

3.8. Опции, заполненные по умолчанию (**Enabled**, **Include AuthnStatement**, **Sign Documents** и др.), оставьте без изменений.

3.9. В качестве **Name ID Format** можно использовать email или другой атрибут пользователя в вашем каталоге LDAP.

> **Примечание**
>
> **NameID** используется для идентификации пользователя в Яндекс ID. Выбрав его формат, вы не сможете позже его изменить. Если UPN может измениться (например, предстоит смена домена электронной почты), выбирайте в качестве **NameID** другой, неизменяемый атрибут.

Email

Если в качестве **Name ID Format** выберан email, то для идентификации пользователя в системе и в Яндекс ID будет использоваться его адрес электронной почты. Чтобы выбранный вариант передавался вне зависимости от настроек Яндекс 360, включите опцию **Force Name ID format**.

Другой атрибут

Если вы планируете использовать в LDAP-каталоге в качестве **NameID** не email, а другой атрибут, например, **objectGUID**, укажите его в LDAP-каталоге:

1. Отключите опцию **Force Name ID format**.
2. Откройте LDAP-каталог.
3. Перейдите в раздел **User Federation**.
4. Нажмите карточку LDAP-провайдера.
5. Перейдите в раздел **LDAP searching and updating**.
6. В поле **UUID LDAP attribute** укажите `objectGUID`.

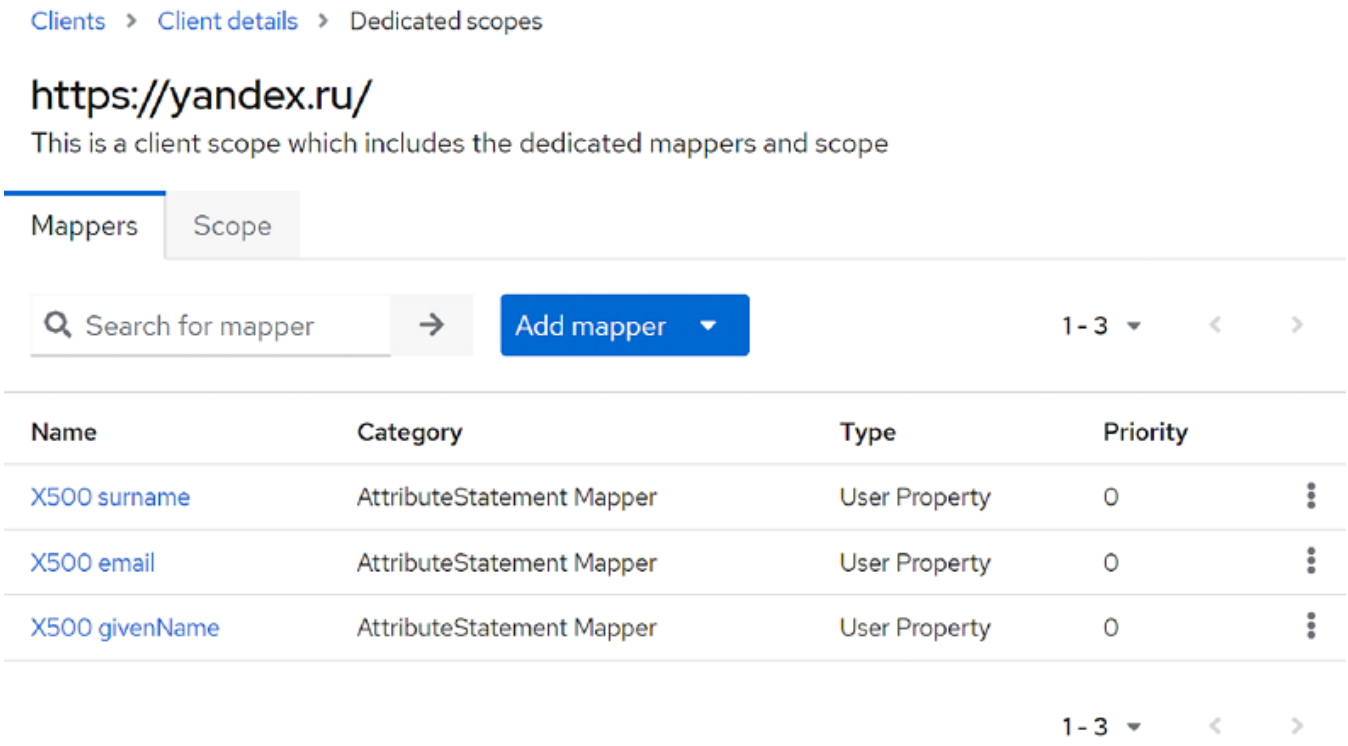
После этого атрибут **objectGUID** будет использоваться в качестве уникального идентификатора пользователя в LDAP-каталоге, а на стороне Keycloak он будет храниться в поле **LDAP_ID**.

3.10. Нажмите **Save**.

3.11. На вкладке **Keys** в разделе **Signing keys config** выключите опцию **Client Signature Required**, если она включена, и еще раз нажмите **Save**.

Шаг 2. Настройте сопоставление атрибутов пользователей

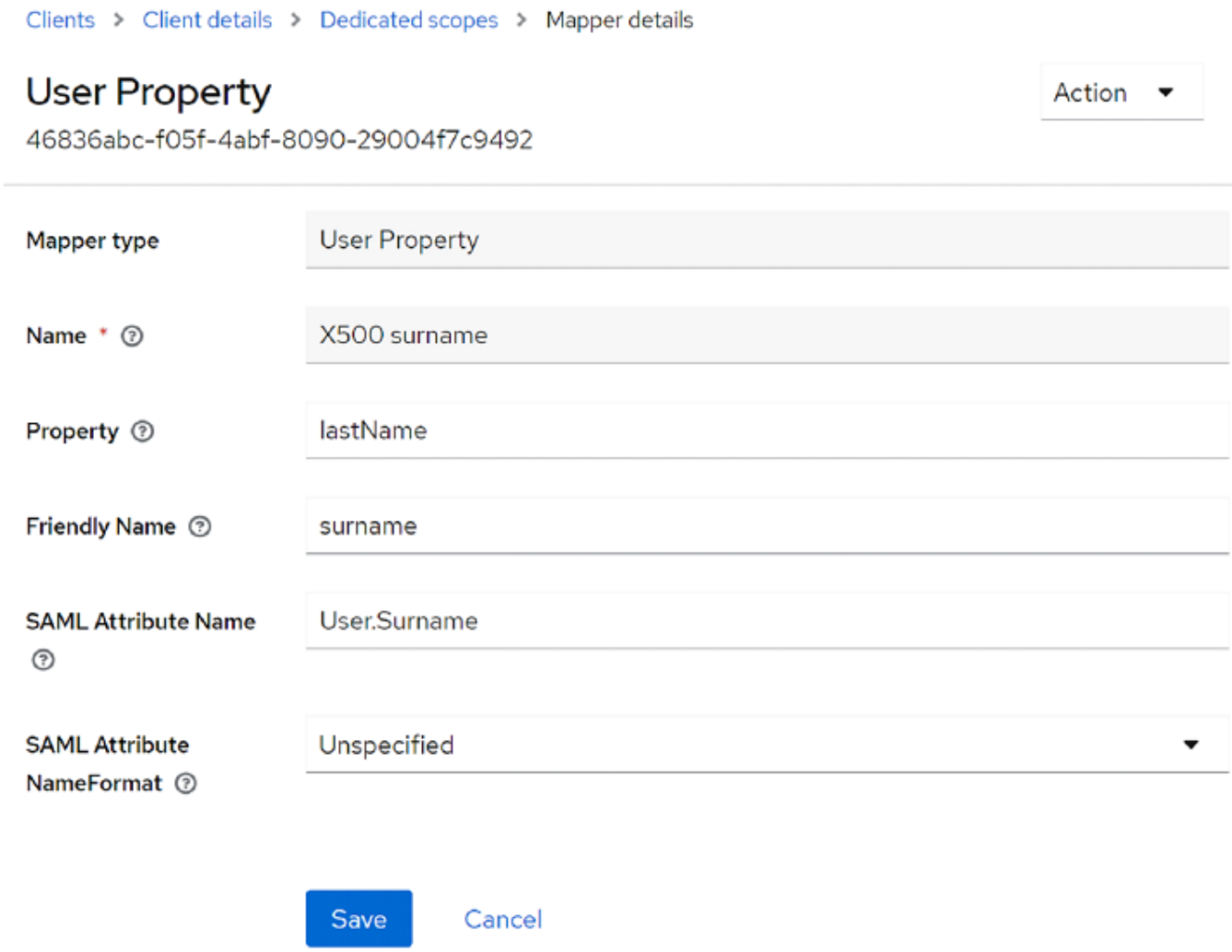
1. На вкладке **Client scopes** откройте **Client scope**, который соответствует создаваемому клиенту, например `https://yandex.ru/-dedicated`.
2. На вкладке **Scope** отключите опцию **Full Scope Allowed**.
3. Перейдите на вкладку **Mappers**, нажмите кнопку **Add Mapper** и выберите пункт **By Configuration**.
4. В открывшемся окне выберите пункт **User Property**.
5. Создайте поочередно необходимые атрибуты:
   - `X500 email` — адрес электронной почты;
   - `X500 surname` — фамилия;
   - `X500 givenName` — имя.

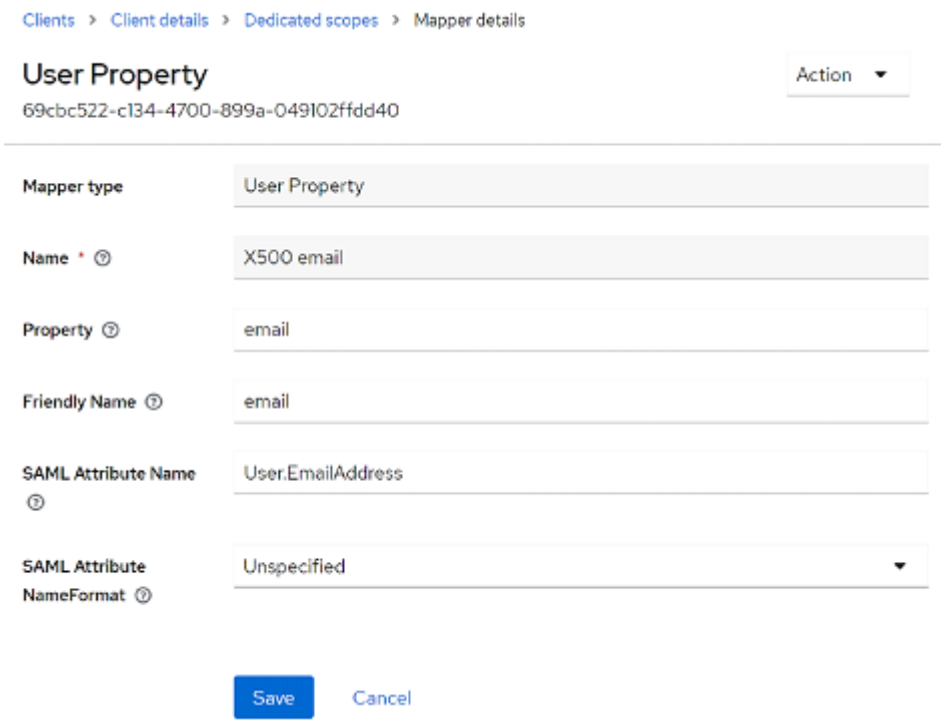


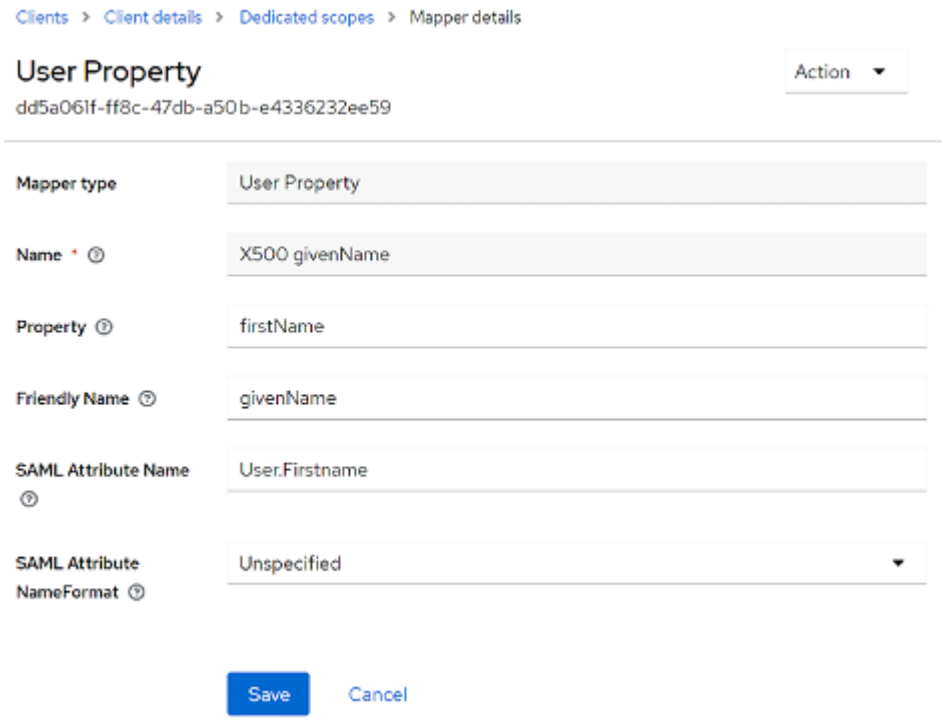
6. Настройте синхронизацию атрибутов Keycloak и Яндекс 360: откройте каждый атрибут и измените значение SAML Attribute Name. Значения SAML Attribute Name, которые поддерживаются в Яндекс 360, приведены ниже.

SAML Attribute Name	Value
User.EmailAddress	X500 email
User.Firstname	X500 givenName
User.Surname	X500 surname

В итоге сопоставление атрибутов будет выглядеть так:


Clients > Client details > Dedicated scopes > Mapper details
User Property
46836abc-f05f-4abf-8090-29004f7c9492
Action
Mapper type
User Property
Name *
X500 surname
Property
lastName
Friendly Name
surname
SAML Attribute Name
User.Surname
SAML Attribute NameFormat
Unspecified
Save
Cancel

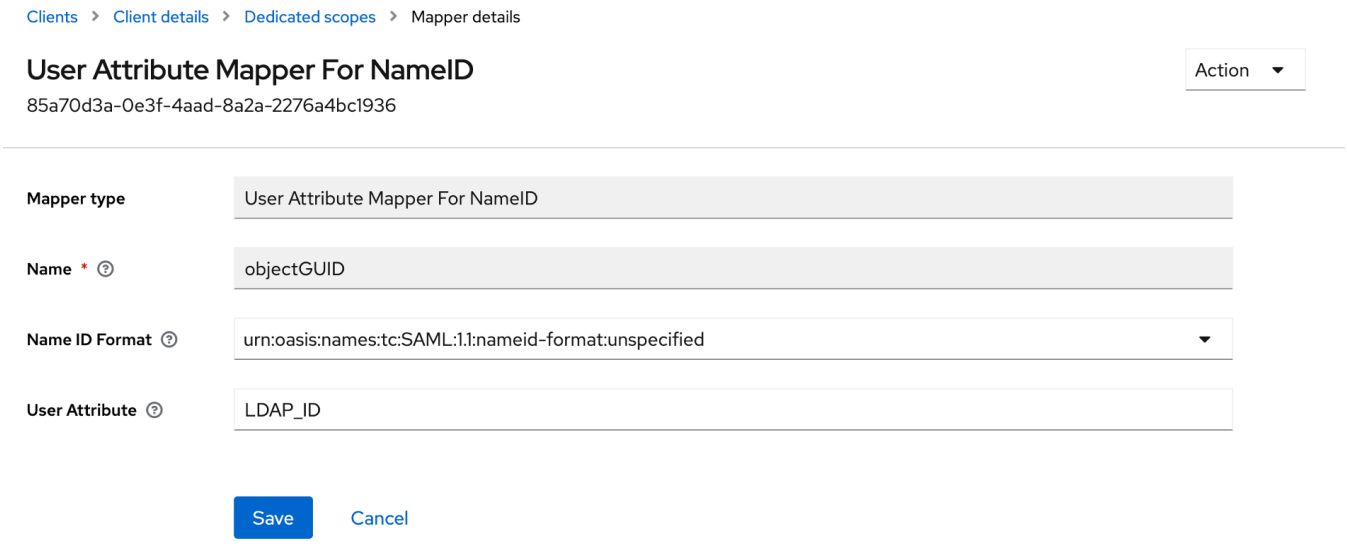

Clients > Client details > Dedicated scopes > Mapper details
User Property
69cbc522-c134-4700-899a-049102ffdd40
Action
Mapper type
User Property
Name *
X500 email
Property
email
Friendly Name
email
SAML Attribute Name
User.EmailAddress
SAML Attribute NameFormat
Unspecified
Save
Cancel



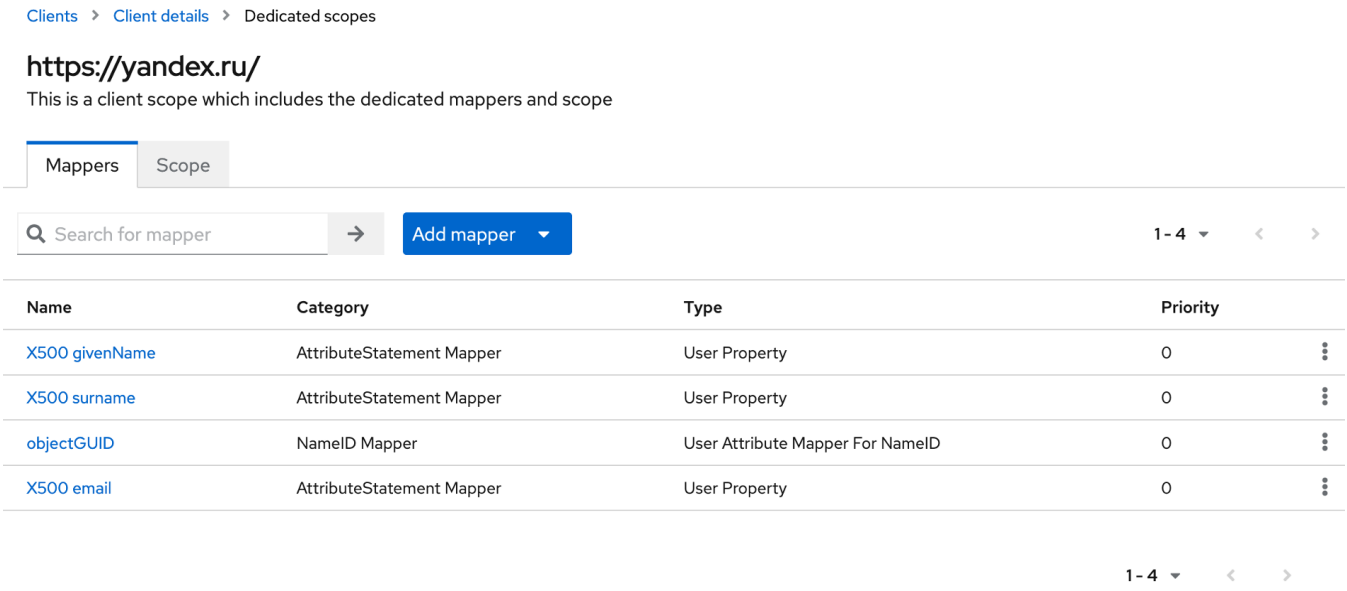
Ответ SAML должен иметь вид:

```
<Attribute Name="User.EmailAddress">
    <AttributeValue>email@test.com</AttributeValue>
</Attribute>
<Attribute Name="User.Surname">
    <AttributeValue>Surname</AttributeValue>
</Attribute>
<Attribute Name="User.Firstname">
    <AttributeValue>Firstname</AttributeValue>
</Attribute>
```

7. Если вы используете для **NameID** настраиваемый атрибут, добавьте для него сопоставление атрибутов:
   7.1. Перейдите на вкладку **Mappers** и выберите **Add Mapper** → **By Configuration**.
   7.2. В открывшемся окне выберите **User Attribute Mapper For NameID**.
   7.3. В поле **User Attribute** укажите `LDAP_ID`.



Итоговый набор сопоставленных атрибутов должен выглядеть так:



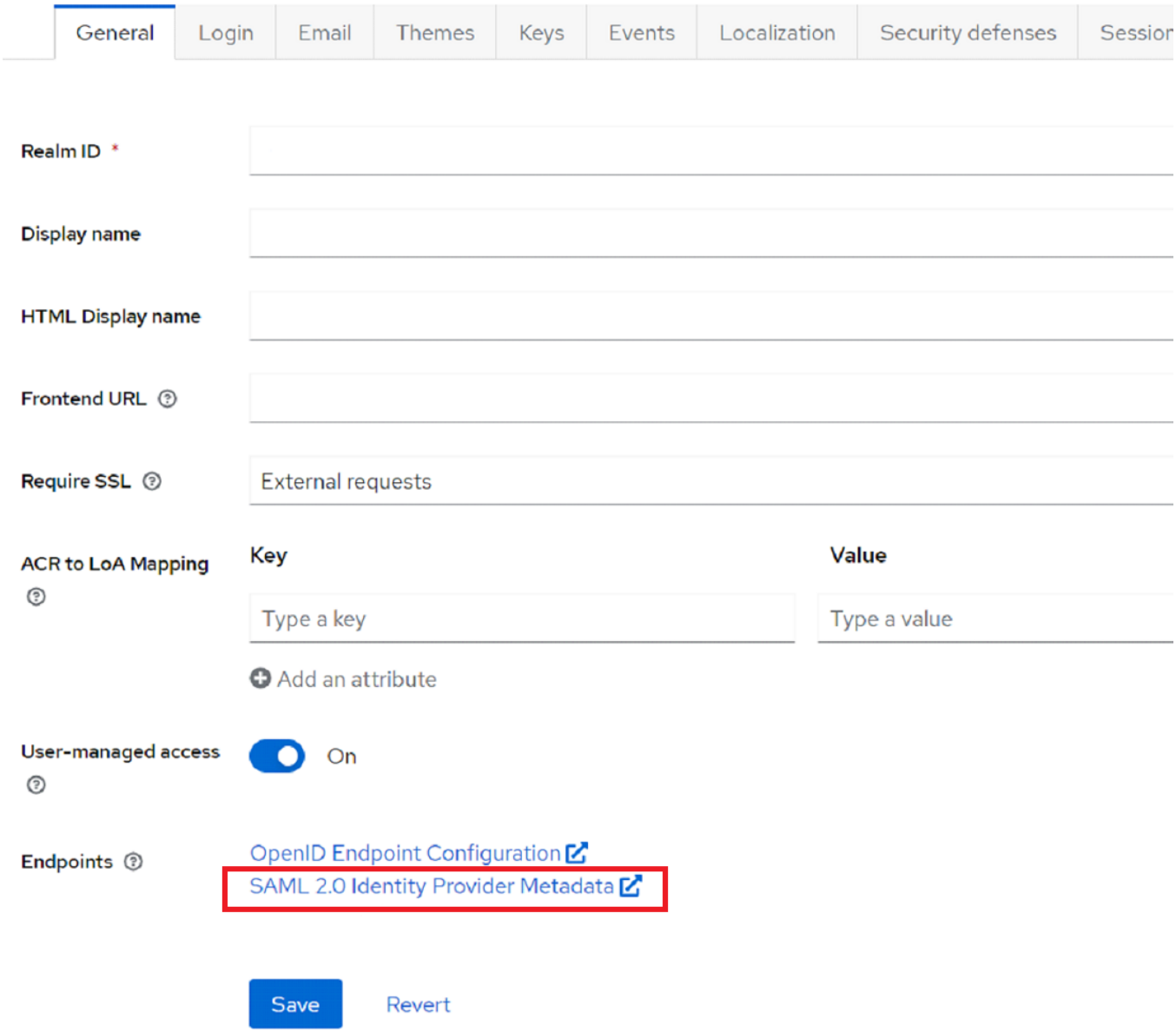
Шаг 3. Соберите данные, которые нужно будет передать Яндекс 360

URL страницы входа

Адрес точки входа.

Чтобы получить:

1. В консоли управления на панели слева выберите **Realm Settings** и нажмите ссылку **SAML 2.0 Identity Provider Metadata**.



2. Нужное значение находится в поле **Location**, скопируйте его.

Издатель поставщика удостоверений

Entity ID домена.

Получить можно так же, как и **URL страницы входа**. Нужное значение находится в поле **entityID**.

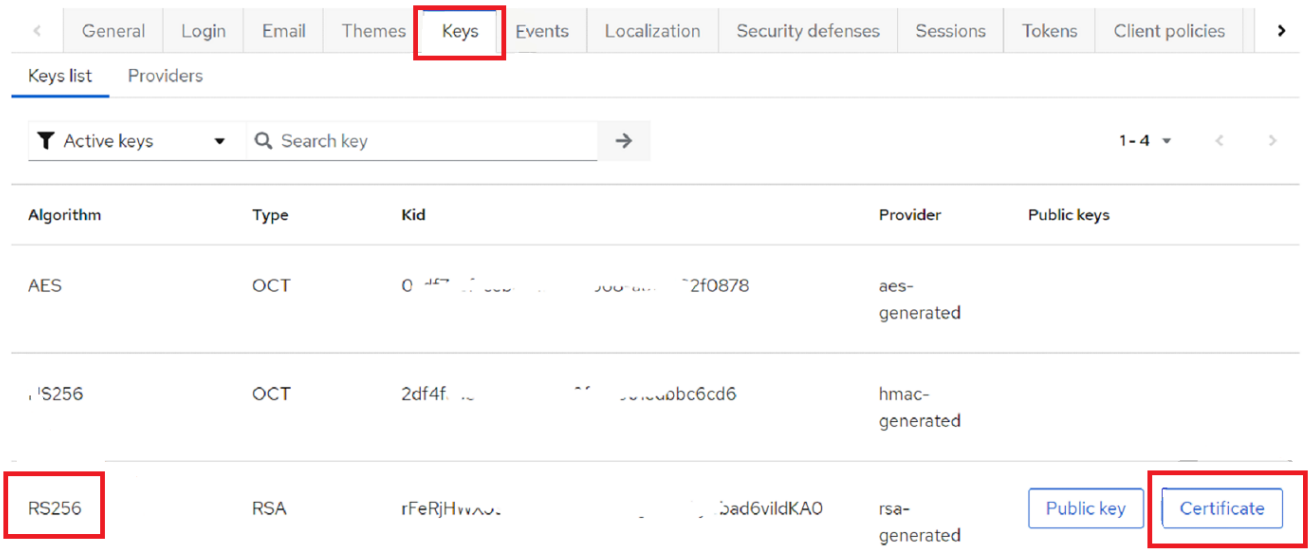
Проверочный сертификат

Сертификат подписи токенов формата X.509.

Получить можно так же, как и **URL страницы входа**. Нужное значение находится в поле **X509Certificate**.

Также сертификат можно скопировать со вкладки **Keys**:

1. Перейдите к строке RS256.
2. Скопируйте содержимое **Certificate**.



Если у вас два активных сертификата подписи токенов и вы не уверены, какой сертификат используется сейчас, повторите аналогичные действия для второго сертификата.

После этого переходите к настройке Яндекс 360 для бизнеса.

Решение проблем с настройкой

Если в процессе настройки поставщика удостоверений заданы неверные значения, то при попытке входа через SSO вы увидите сообщение «Авторизация не удалась» и код ошибки:

email.no_in_response

Указывайте имена атрибутов в формате `User.Firstname`, `User.Surname`, `User.EmailAddress`. Если задать другой формат, например `Firstname`, авторизоваться не получится.

request_your_admin

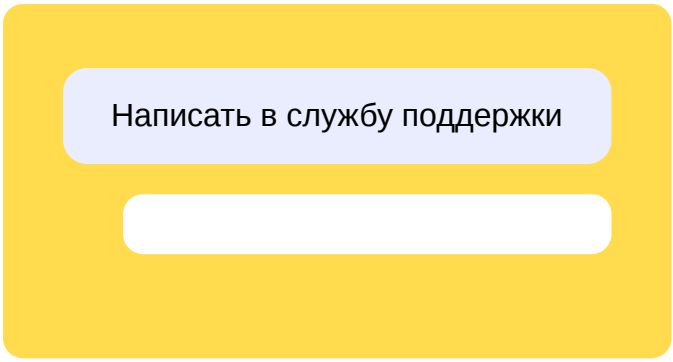
Ошибка появляется, если администратор каталога пользователей вашей организации ограничил для аккаунта доступ к Яндекс 360. За подробной информацией обратитесь к специалистам технической поддержки вашей организации.

samlresponse.invalid

Ошибка возникает, если неверно указаны URL страницы входа, издатель поставщика удостоверений или проверочный сертификат. Также она может возникнуть в течение 14 дней до истечения проверочного сертификата или после его истечения. Проверьте корректность настроек SSO в Яндекс 360 для бизнеса.

unsupportable_domain

Проверьте, что домен из почтового атрибута `User.EmailAddress` в SAML response такой же, как и основной домен или один из доменов-алиасов организации Яндекс 360. Если они не совпадают, вы увидите сообщение об ошибке.

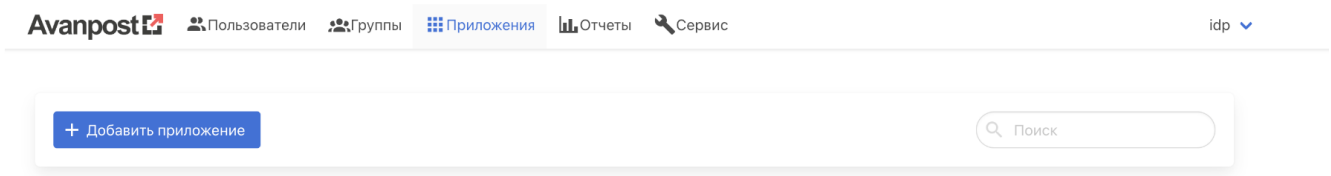

Написать в службу поддержки

Настройка Avanpost FAM

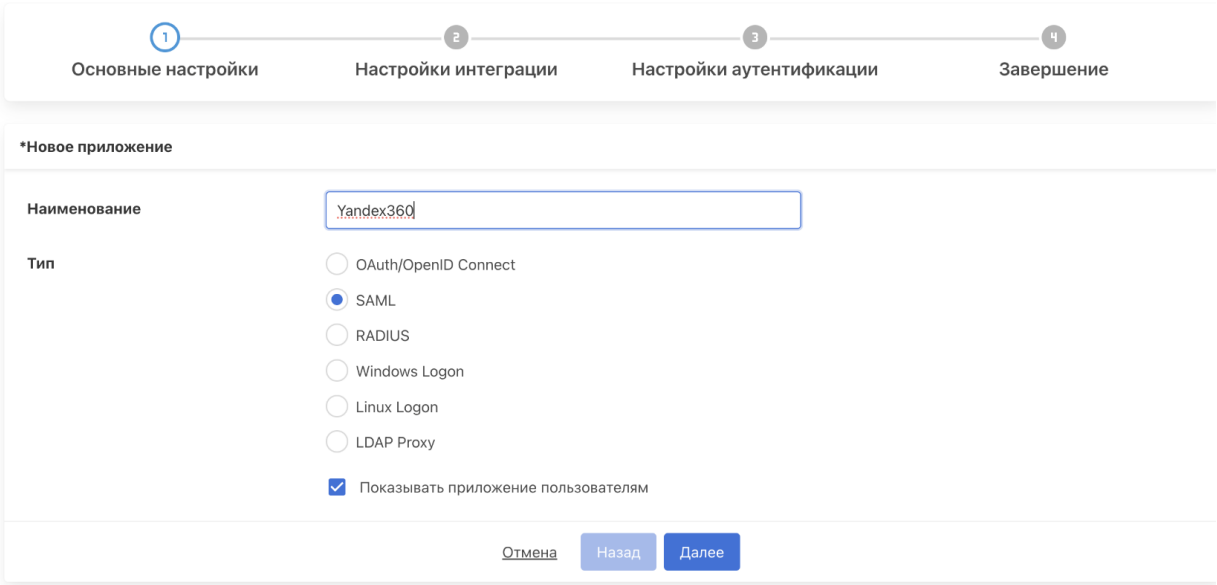
Чтобы организовать единый вход (SSO) в сервисы Яндекс 360 через систему единой аутентификации Avanpost FAM, нужно предварительно создать и настроить SAML-приложение.

Шаг 1. Создайте и настройте SAML-приложение

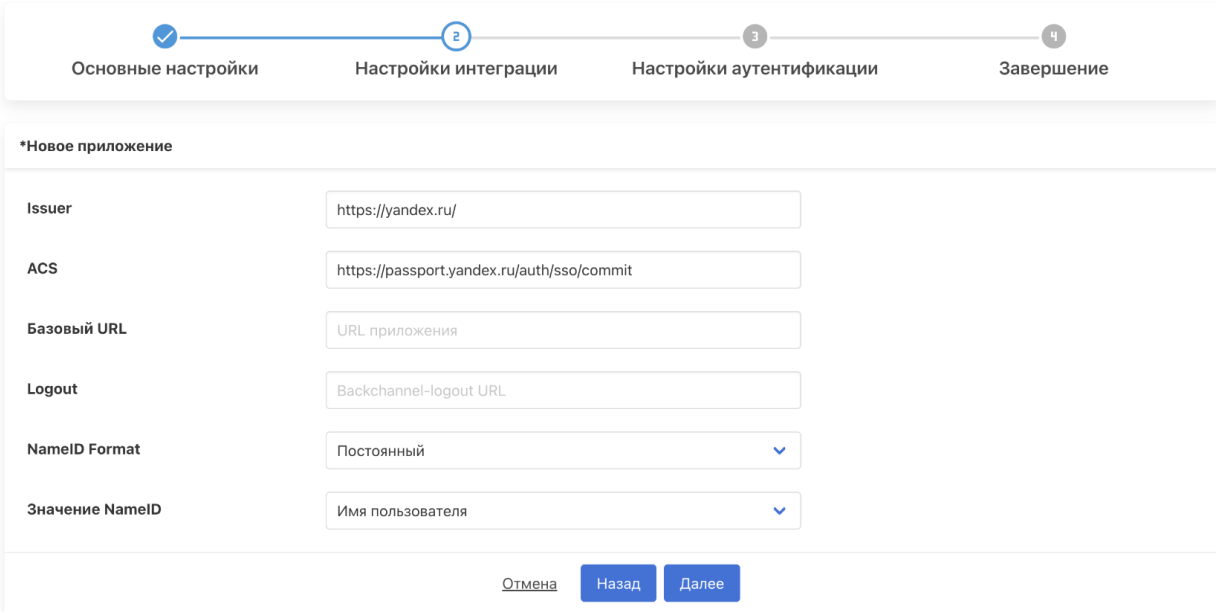
1. Авторизуйтесь в Avanpost.
2. Откройте веб-интерфейс Avanpost FAM.
3. Создайте SAML-приложение — перейдите в раздел **Приложения** и нажмите **Добавить приложение**.



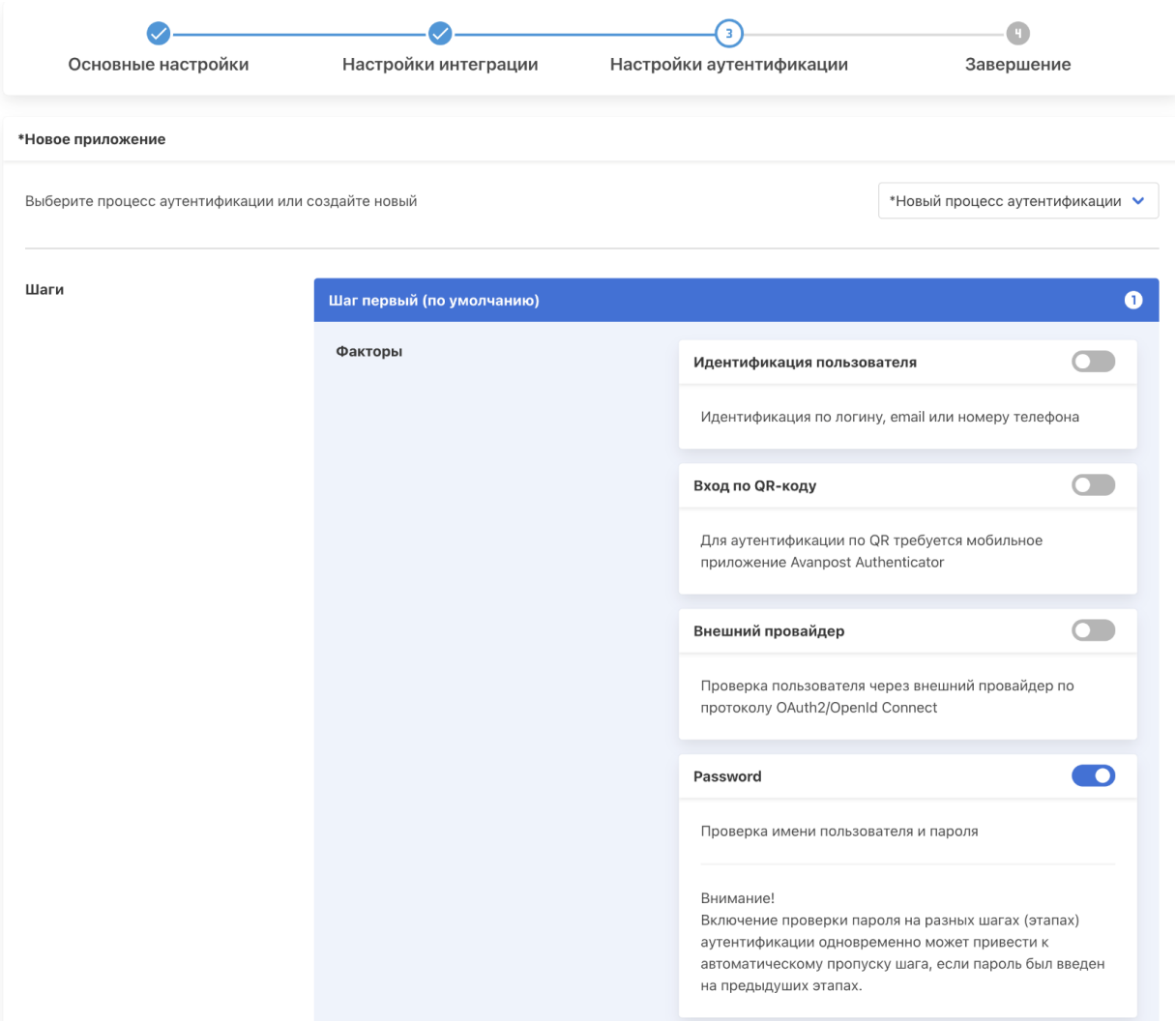
4. Задайте **Основные настройки** приложения:
   4.1. **Наименование** — укажите произвольное название приложения, например «Yandex360».
   4.2. **Тип** — выберите **SAML**.
   4.3. Проверьте, что опция **Показывать приложение пользователям** включена.
   4.4. Нажмите **Далее**.



5. Задайте **Настройки интеграции**:
   5.1. В поле **Issuer** введите `https://yandex.ru/` (обязательно с косой чертой в конце).
   5.2. В поле **ACS** введите Service URL: `https://passport.yandex.ru/auth/sso/commit`.
   5.3. Поля **Базовый URL** и **Logout** оставьте пустыми.
   5.4. Задайте **NameID Format** — выберите из списка **Постоянный**.
   5.5. В поле **Значение NameID** выберите идентификатор, который вы будете использовать в качестве NameID при SAML SSO: **Имя пользователя** или **Адрес электронной почты**.
   5.6. Нажмите **Далее**.

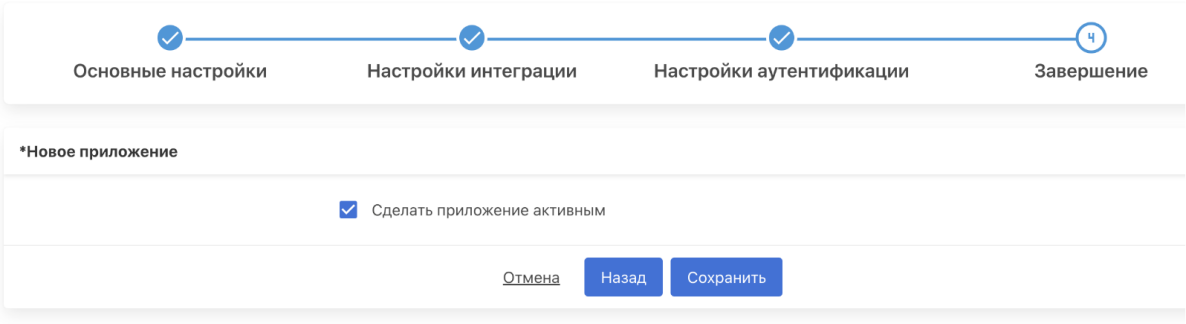


6. Задайте **Настройки аутентификации**:
   6.1. Для нового процесса аутентификации задайте проверку по имени пользователя и паролю — включите метод **Password** в предлагаемом списке факторов.
   6.2. Остальные методы оставьте выключенными.
   6.3. Нажмите **Далее**.



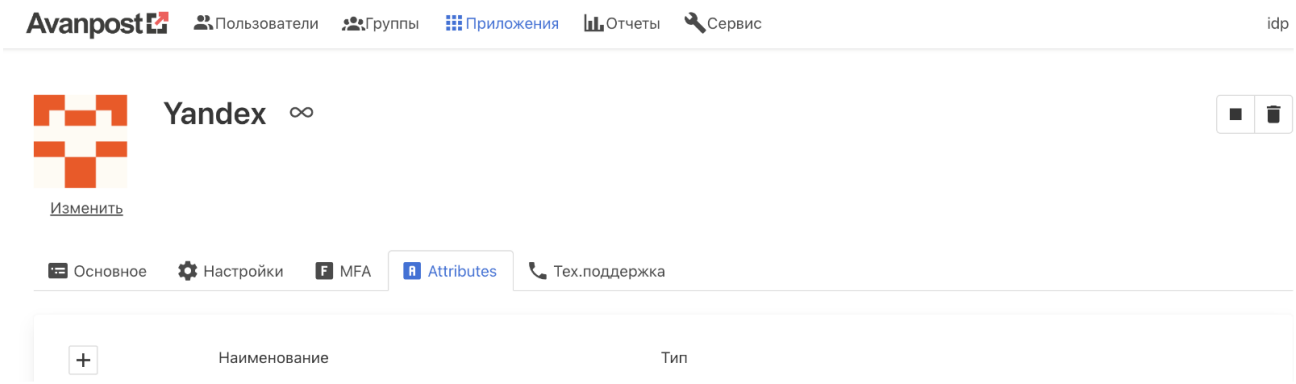
7. Активируйте приложение:
   7.1. Отметьте опцию **Сделать приложение активным**.

7.2. Нажмите **Сохранить**.

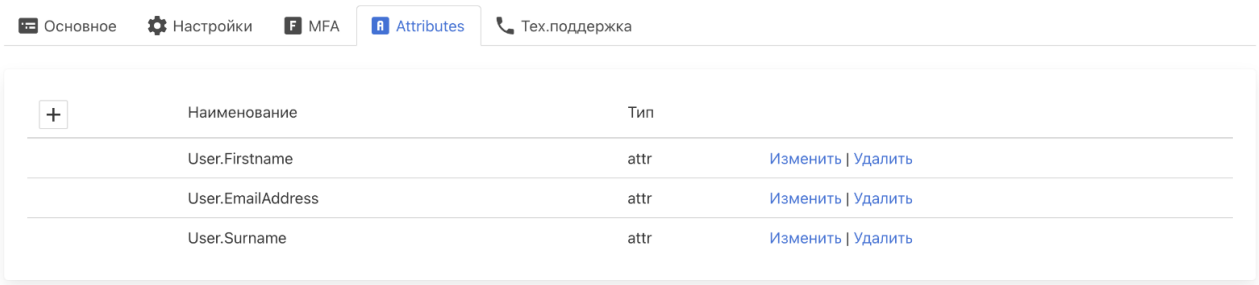


Шаг 2. Настройте сопоставление атрибутов пользователей

1. В разделе **Приложения** веб-интерфейса Avanpost FAM выберите созданное на шаге 1 SAML-приложение.
2. В открывшемся окне перейдите на вкладку **Attributes**.



3. Нажимая значок `+`, добавьте поочередно три атрибута:
   - `User.EmailAddress` — адрес электронной почты;
   - `User.Surname` — фамилия;
   - `User.Firstname` — имя.



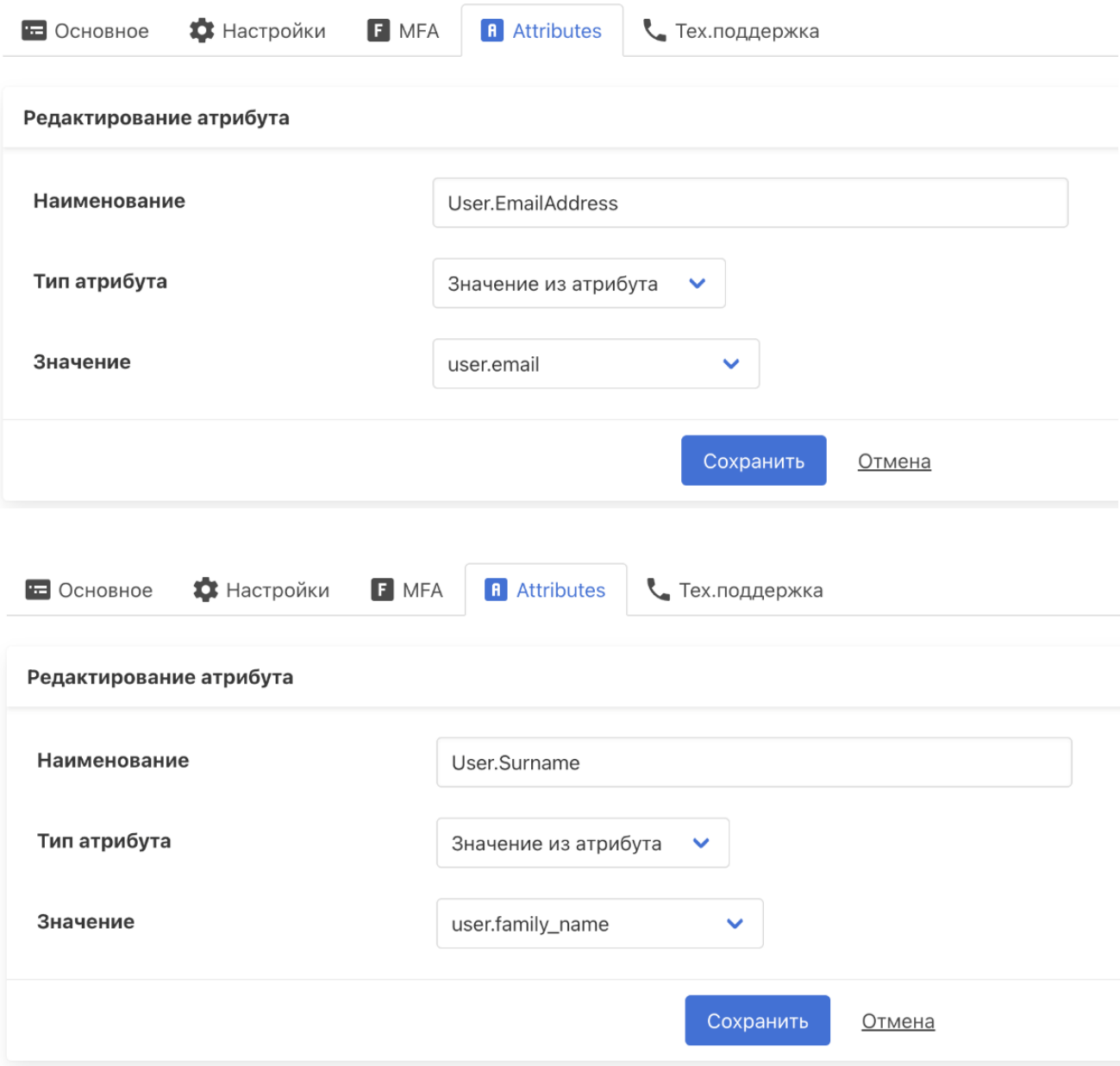
4. Настройте синхронизацию атрибутов Avanpost FAM и Яндекс 360 — откройте каждый атрибут и измените параметры источников значений.

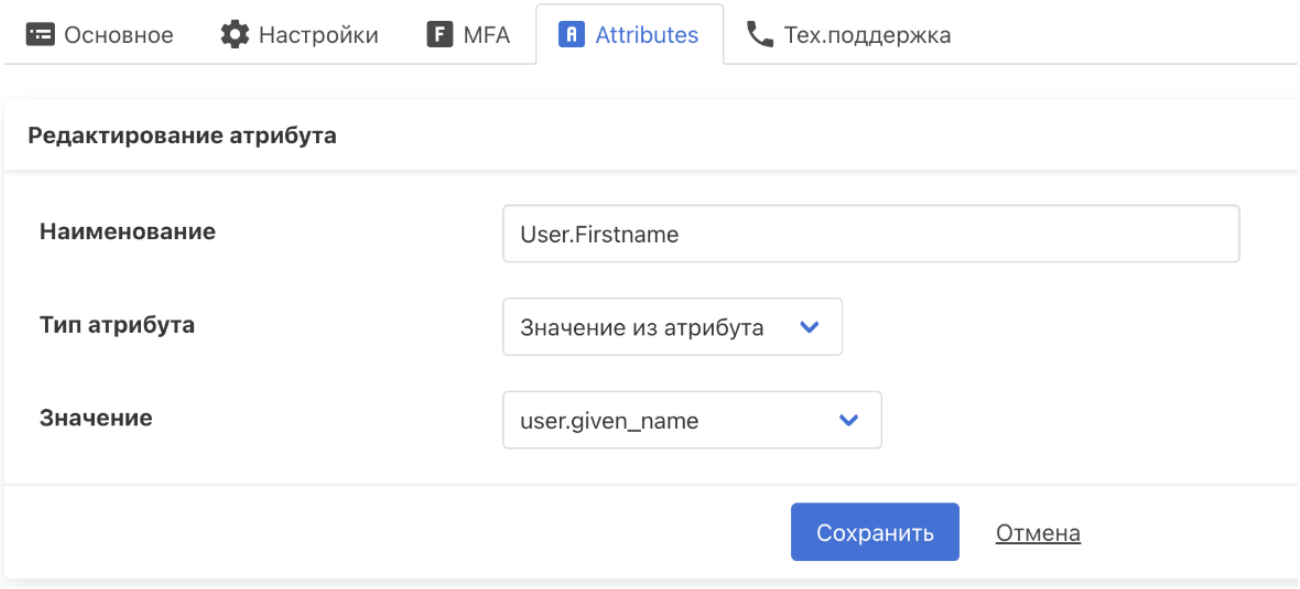
   Значения SAML Attribute Name, которые поддерживаются в Яндекс 360 для бизнеса, приведены в таблице.

SAML Attribute Name	Значение

User.EmailAddress	user.email
User.Firstname	user.family_name
User.Surname	user.given_name

В итоге сопоставление атрибутов будет выглядеть так:





Шаг 3. Соберите данные для передачи в Яндекс 360 для бизнеса

Основные параметры для настройки единого входа можно получить по ссылке вида

```
http://<avanpost hostmane/IP>/.well-known/samlidp.xml
```

где `<avanpost hostmane/IP>` — имя хоста или IP-адрес, по которому доступен сервис.

Для SSO вам потребуются следующие данные:

- **URL страницы входа** — адрес точки входа. Значение указано в поле `Location`.
- **Издатель поставщика удостоверений** — Entity ID домена. Значение указано в поле `entityID`.
- **Проверочный сертификат** — сертификат подписи токенов формата X.509. Значение указано в поле `X509Certificate`.

Решение проблем с настройкой

Если в процессе настройки поставщика удостоверений заданы неверные значения, то при попытке входа через SSO вы увидите сообщение «Авторизация не удалась» и код ошибки:

email.no_in_response

Указывайте имена атрибутов в формате `User.Firstname`, `User.Surname`, `User.EmailAddress`. Если задать другой формат, например `Firstname`, авторизоваться не получится.

request_your_admin

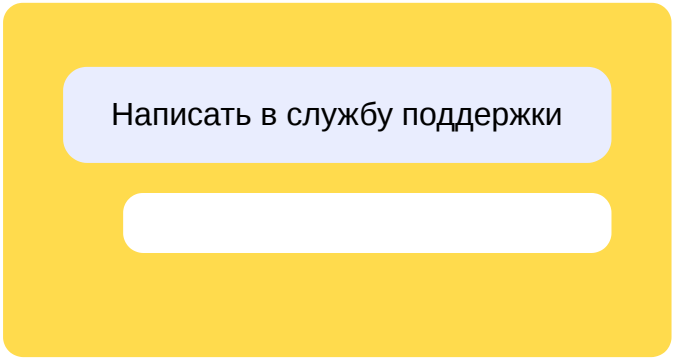
Ошибка появляется, если администратор каталога пользователей вашей организации ограничил для аккаунта доступ к Яндекс 360. За подробной информацией обратитесь к специалистам технической поддержки вашей организации.

samlresponse.invalid

Ошибка возникает, если неверно указаны URL страницы входа, издатель поставщика удостоверений или проверочный сертификат. Также она может возникнуть в течение 14 дней до истечения проверочного сертификата или после его истечения. Проверьте корректность настроек SSO в Яндекс 360 для бизнеса.

unsupportable_domain

Проверьте, что домен из почтового атрибута `User.EmailAddress` в SAML response такой же, как и основной домен или один из доменов-алиасов организации Яндекс 360. Если они не совпадают, вы увидите сообщение об ошибке.



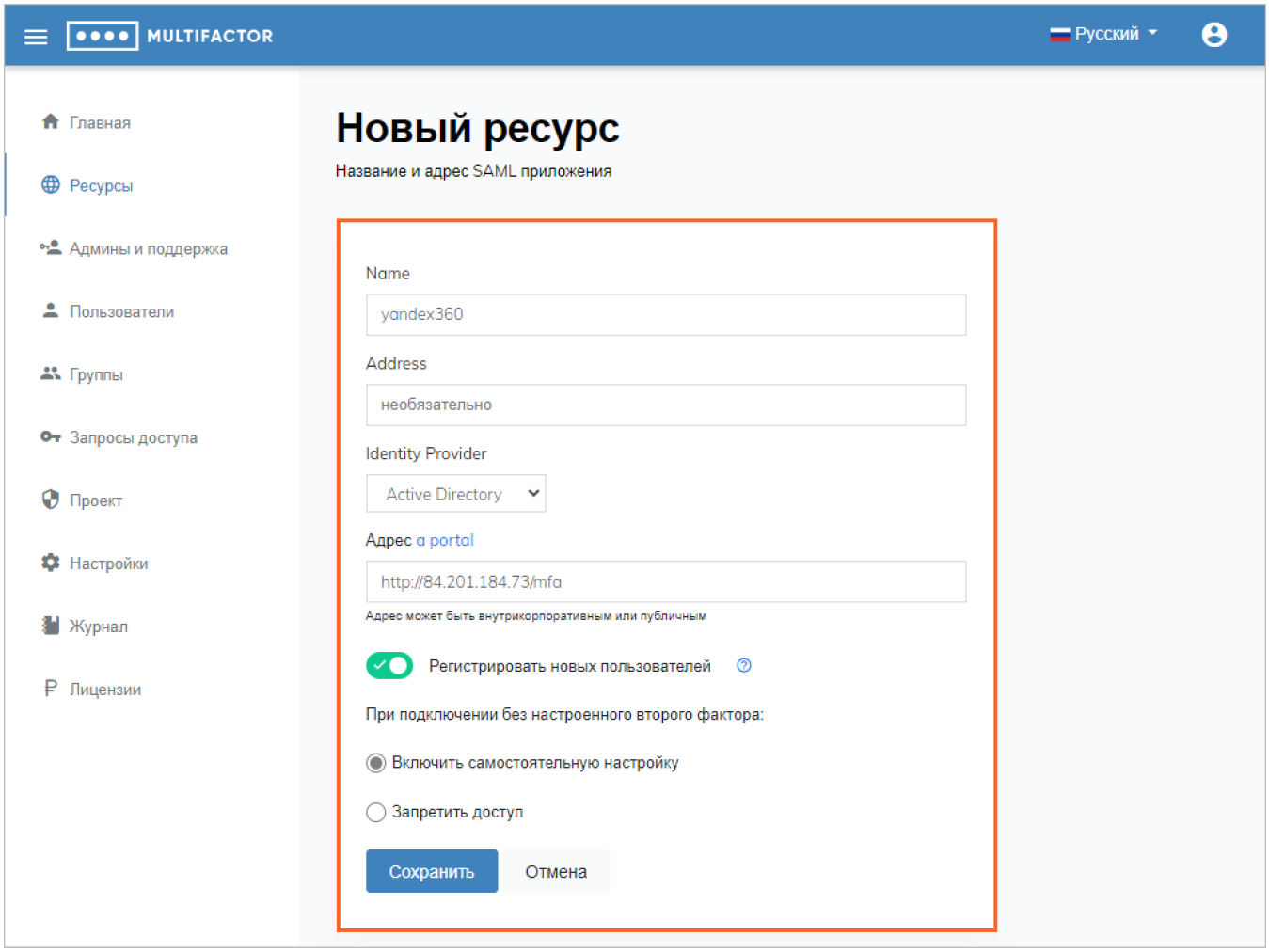
Настройка Multifactor

Чтобы организовать единый вход (SSO) в сервисы Яндекс 360 через Multifactor, нужно предварительно настроить портал самообслуживания Multifactor и создать SAML-приложение.

Пользователи должны быть созданы заранее с помощью утилиты YandexADSCIM, при этом в качестве `NameID` может быть использовано только UPN с указанием домена.

Шаг 1. Создайте и настройте SAML-приложение

1. Войдите в аккаунт администратора Multifactor.
2. Создайте SAML-приложение:
   2.1. На панели слева выберите **Ресурсы** и нажмите **Добавить ресурс** → **SAML-приложение**.
   2.2. В поле **Name** укажите произвольное название приложения, например `yandex360`.
   2.3. Поле **Address** оставьте пустым.
   2.4. В поле **Identity Provider** выберите **Active Directory**.
   2.5. В поле **Адрес a portal** введите адрес (внешний или внутренний) предварительно настроенного портала самообслуживания Multifactor.
   2.6. Включите опцию **Регистрировать новых пользователей**.
   2.7. Нажмите **Сохранить**, откроется страница настройки SAML-приложения.



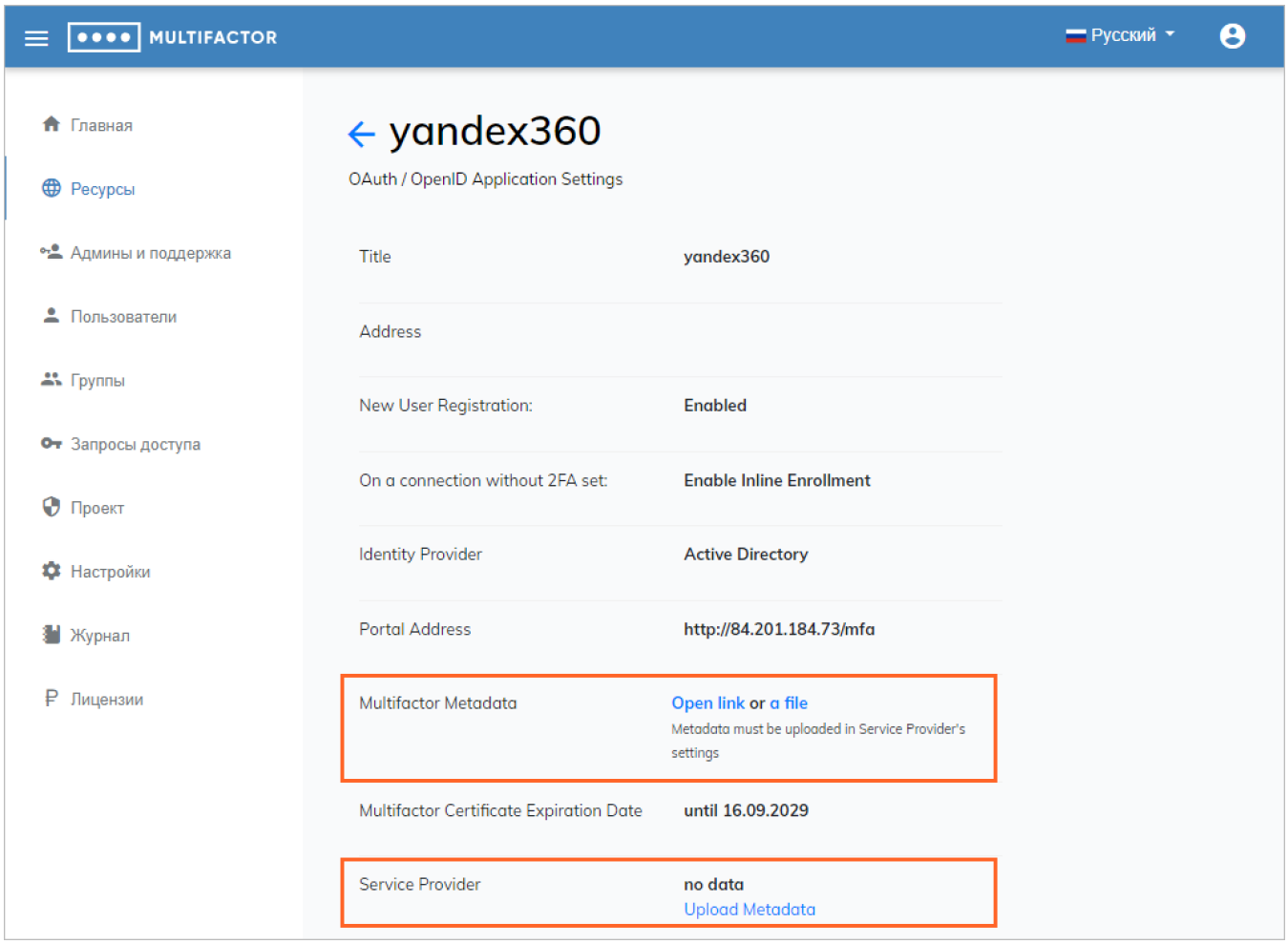
3. Настройте параметры SAML-приложения:
   3.1. Создайте XML-файл с названием `sp_metadata.xml`, добавьте в него следующий код:

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                     entityID="https://yandex.ru/">
    <md:SPSSODescriptor AuthnRequestsSigned="false"
WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat>
        <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                     Location="https://passport.yandex.ru/auth/sso/commit"
index="1" />
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

3.2. Укажите параметры и сохраните файл:

- **entityID** — `https://yandex.ru/` (обязательно с косой чертой в конце).
- **Location** — `https://passport.yandex.ru/auth/sso/commit`.

3.3. На странице настройки SAML-приложения в блоке **Service Provider** нажмите **Upload Metadata** и загрузите созданный файл `sp_metadata.xml`.



Шаг 2. Соберите данные, которые нужно будет передать Яндекс 360

1. На странице настройки SAML-приложения в блоке **Multifactor Metadata** нажмите **Open Link**.

2. Откроется XML-файл, для SSO вам потребуются следующие данные:
   - **URL страницы входа** — адрес точки входа. Значение указано в поле `Location` в строке с `SingleSignOnService`.
   - **Издатель поставщика удостоверений** — Entity ID домена. Значение указано в поле `entityID`.
   - **Проверочный сертификат** — сертификат подписи токенов формата X.509. Значение указано в поле `X509Certificate`.

После этого переходите к настройке Яндекс 360 для бизнеса.

Решение проблем с настройкой

Если в процессе настройки поставщика удостоверений заданы неверные значения, то при попытке входа через SSO вы увидите сообщение «Авторизация не удалась» и код ошибки:

email.no_in_response

Указывайте имена атрибутов в формате `User.Firstname`, `User.Surname`, `User.EmailAddress`. Если задать другой формат, например `Firstname`, авторизоваться не получится.

request_your_admin

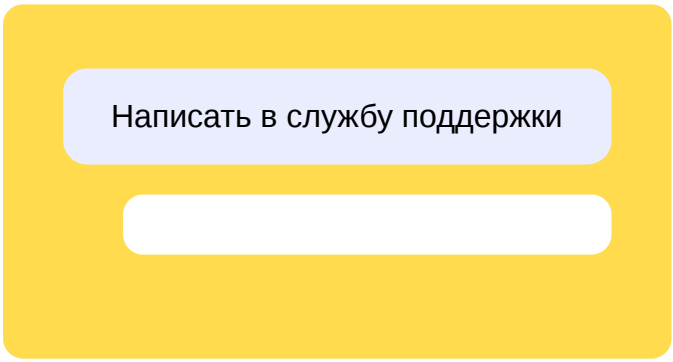
Ошибка появляется, если администратор каталога пользователей вашей организации ограничил для аккаунта доступ к Яндекс 360. За подробной информацией обратитесь к специалистам технической поддержки вашей организации.

samlresponse.invalid

Ошибка возникает, если неверно указаны URL страницы входа, издатель поставщика удостоверений или проверочный сертификат. Также она может возникнуть в течение 14 дней до истечения проверочного сертификата или после его истечения. Проверьте корректность настроек SSO в Яндекс 360 для бизнеса.

unsupportable_domain

Проверьте, что домен из почтового атрибута `User.EmailAddress` в SAML response такой же, как и основной домен или один из доменов-алиасов организации Яндекс 360. Если они не совпадают, вы увидите сообщение об ошибке.



Синхронизация пользователей и групп с каталогом LDAP с помощью утилиты ADSCIM

Если в вашей компании развернута служба федерации Active Directory, вы можете настроить автоматическую синхронизацию сотрудников и групп с Яндекс 360 для бизнеса — для этого нужно установить и настроить специальную службу Windows.

Если вы хотите подключить синхронизацию пользователей из Active Directory, установите **YandexADSCIM** (утилита в виде службы Windows на компьютере) по инструкции ниже и запустите программу от имени пользователя с правами чтения из каталога LDAP. YandexADSCIM управляется через оснастку **Сервисы**. Настройки меняются в конфигурационном файле.

Сейчас полноценно поддерживаются каталоги Active Directory, Samba DC и Red ADM. Другие каталоги LDAP будут полноценно поддержаны в будущем, когда утилита YandexADSCIM будет портирована на *nix-платформы. Сейчас ее можно использовать для настройки работы с другими каталогами LDAP, но запускать нужно на устройстве с ОС Windows.

Подключение и первоначальная настройка ADSCIM

Шаг 1. Начните настройку

1. Проверьте, что единый вход (SSO) подключен и правильно работает. Как подключить единый вход
2. Задайте уникальный идентификатор пользователя:
   - Выберите атрибут Active Directory для передачи в параметр утилиты ADSCIM **PropertyLoginName**, чтобы внести его в каталог Яндекса:
     - **UPN** (**userPrincipalName** в ADSCIM) – если имена для входа пользователей не будут меняться;
     - **objectSID**, **objectGUID** или другой — если запланированы изменения домена или бизнес-процессов, которые могут привести к изменению UPN пользователей.

     Внимание

     Атрибут, который вы зададите в качестве основного идентификатора, не должен меняться. Пользователь с другим атрибутом при входе будет считаться новым пользователем.

   - Если ваши пользователи уже используют сервисы Яндекс 360 и проходят аутентификацию с помощью протокола SAML 2.0, проверьте совпадение атрибутов: значение атрибута **NameID**, которое указано в Active Directory, должно соответствовать основному идентификатору утилиты ADSCIM **PropertyLoginName**.

   Больше информации про **PropertyLoginName** см. в шаге 4, п. 2.5.
3. Проверьте, что у пользователей в Active Directory заполнены атрибуты:
   - идентификатор, выбранный в качестве основного;
   - User SamAccountName;

- E-mail.

Шаг 2. Получите Client ID и OAuth-токен

1. Перейдите на страницу создания приложения. Перейти
2. Введите название сервиса и прикрепите его иконку.
3. В блоке **Платформы приложения** выберите **Веб-сервисы**. В поле **Redirect URI** нажмите ссылку **Подставить URL для отладки**.
4. В блоке **Доступ к данным** в начале строки введите название доступа **Управление федерациями**.
5. Укажите почту для связи. Внизу страницы нажмите **Создать приложение**.
6. Отправьте POST-запрос, чтобы получить OAuth-токен. Например, через cURL это можно сделать при помощи следующей команды:

   ```
   curl -X POST https://oauth.yandex.ru/token -d
   "grant_type=client_credentials&client_id=значение1&client_secret=значение2"
   ```

   где значение параметра `client_id` — это **ID** созданного приложения, а `client_secret` — его **секретный ключ**.
7. Сохраните полученные ID и OAuth-токен. Они пригодятся на следующих шагах.

Шаг 3. Укажите Client ID в Яндекс 360 и получите Domain ID

1. Откройте кабинет организации в Яндекс 360 для бизнеса. Перейти
2. Перейдите в раздел **Общие настройки → Единый вход (SSO)**.
3. Нажмите **Настроить**.
4. В блоке **Синхронизация SCIM** вставьте ID вашего приложения, полученный на шаге 2.
5. Скопируйте ваш **Domain ID**, он пригодится на следующем шаге.
6. Сохраните изменения.

Шаг 4. Установите и настройте службу Windows для синхронизации

1. Скачайте и установите службу YandexADSCIM. Скачать установочный файл
2. Найдите конфигурационный файл `%ProgramData%\Yandex\YandexADSCIM\AD_Users.config` и откройте его в любом текстовом редакторе.

   > **Совет**
   >
   > Если найти папку `%ProgramData%` не получается, включите отображение скрытых файлов. Как это сделать

   Каждая настройка в конфигурационном файле записывается отдельной строкой в формате `ключ=значение`. Строки, которые начинаются с символа `#`, служба игнорирует.

Настройте конфигурационный файл:

2.1. Проверьте, что в значении параметра **LDAP** указан правильный путь для подключения к Active Directory. Если нет, исправьте его. Подставьте в поисковые параметры собственные значения.

Для поискового запроса используйте путь из структуры `DIT = Directory Information Tree` (читается справа налево):

```
LDAP = LDAP://CN=Users,OU=DomainGroup,DC=YourCompanyName,DC=com
```

где

- `DC` – domainComponent, собственный домен и доменная зона;
- `OU` – OrganizationUnit, компания, департамент или отдел, из которого вы хотите получить пользователей;
- `CN` – commonName, наименование объекта, который хотите получить из каталога.

2.2. В значении параметра **BearerToken** укажите OAuth-токен, полученный на шаге 2.

2.3. В значении параметра **DomainID** укажите ID домена, полученный на шаге 3.

2.4. Значение параметра **DryRun** изначально установлено в значение `true`. Если оставить это значение, то на данном этапе служба будет работать в тестовом режиме. Запросы будут фиксироваться в логах, но синхронизация производиться не будет. Чтобы включить синхронизацию SCIM уже сейчас, поменяйте значение параметра на `false`.

2.5. Синхронизируйте пользовательские данные из Active Directory. Переназначить атрибуты при создании или синхронизации пользователей в Яндекс 360 позволяют параметры, которые начинаются с **Property**.

Параметр **PropertyLoginName**, который соответствует идентификатору пользователя, может принимать одно из трех значений:

- `userPrincipalName` — UPN, значение по умолчанию;
- `objectSID`;
- `objectGUID`.

Значение параметра должно соответствовать значению атрибута **NameID**.

Если вы используете атрибут вида `username`, а не `username@domain.com`, то дополнительно укажите параметр **IgnoreUsernameDomain** со значением `true`.

Для остальных пользовательских атрибутов:

Название параметра утилиты YandexADSCIM	Название атрибута (рус.)	Значение по умолчанию из Active Directory	Пример

PropertyFirstName	Имя	givenName	Иван
PropertyMiddleName	Отчество	middleName	Иванович
PropertyLastName	Фамилия	sn (SurName)	Иванов
PropertyDisplayName	Выводимое имя	displayName	Иванов И. И.
PropertyWorkMail	Основная почта	mail	I_ivanov@domain.ru
PropertyTitle	Должность	title	Разработчик
PropertyMobilePhoneNumber	Мобильный телефон	mobile	+7 012 345-67-89
PropertyWorkPhoneNumber	Рабочий телефон	telephoneNumber	+7 495 123-45-67
PropertyIpPhoneNumber	IP-телефон	ipPhone	7495 012-34-56

случае значением параметра будет список. Порядок атрибутов при этом важен. Например, для получения фамилии пользователя можно задать атрибуты: `PropertyLastName = surName`, `PropertyLastName = sn`, `PropertyLastName = lastName`. Если существует атрибут `surName`, будет использовано его значение. Если этого атрибута нет, будет использовано значение атрибута `sn`. Если он также отсутствует — значение атрибута `lastName`.

2.6. Чтобы ограничить выгрузку пользователей, можно воспользоваться фильтром **UsersFilter** и применить стандартный синтаксис запросов LDAP.

- Чтобы выбрать пользователей по их членству в определенной группе, используйте фильтр:

```
UsersFilter =(memberOf=CN=groupname,CN=Users,DC=domainname,DC=com)
```

- Если нужно дополнительно исключить из выборки заблокированных в Active Directory пользователей, используйте фильтр:

  ```
  UsersFilter =(&(memberOf=CN=groupname,CN=Users,DC=domainname,DC=com) (!
  (userAccountControl:1.2.840.113556.1.4.803:=2)))
  ```

  В результате синхронизации пользователи, которые зарегистрированы на почтовом домене вашей организации, но не попали в фильтр, будут заблокированы.

2.7. Если нужно, чтобы алиасы почтовых ящиков из Active Directory синхронизировались с Яндекс 360 для бизнеса, добавьте параметр **EnableAliases** со значением `true`. Доменные почтовые алиасы, которые указаны в Active Directory в атрибуте пользователя `proxyAdresses` с типом SMTP, добавятся в аккаунт сотрудника в Яндекс 360 для бизнеса автоматически.

> **Важно**
>
> Для корректной синхронизации алиасов версия утилиты YandexADSCIM должна быть 1.1.0.144 или выше. Скачать установочный файл

2.8. Синхронизируйте группы из Active Directory — добавьте параметр **EnableGroups** со значением `true`.

Чтобы ограничить список групп, можно воспользоваться фильтром **GroupsFilter** и применить стандартный синтаксис запросов LDAP. Например, чтобы выгрузить все списки рассылок, используйте фильтр:

```
GroupsFilter =(&(objectClass=group)(!
(groupType:1.2.840.113556.1.4.803:=2147483648)))
```

2.9. Синхронизируйте атрибуты групп из Active Directory. Переназначить атрибуты при создании или синхронизации групп в Яндекс 360 позволяют параметры, которые начинаются с **PropertyGroup**.

Название параметра утилиты YandexADSCIM	Название атрибута (рус.)	Значение по умолчанию из Active Directory	Пример
PropertyGroupDisplayName	Название	name	Проект интеграции

PropertyGroupDescription	Описание	description	Сотрудники, участвующие в проекте интеграции
PropertyGroupEmail	Рассылка	mail	int@domain.ru

В таком случае значением параметра будет список. Порядок атрибутов при этом важен. Например, для получения названия группы можно задать атрибуты: `PropertyGroupDisplayName = name`, `PropertyGroupDisplayName = cn`. Если существует атрибут `name`, будет использовано его значение. Если этого атрибута нет, будет использовано значение атрибута `cn`.

2.10. Синхронизируйте внешние контакты, если вы используете их в Яндекс 360. Для этого добавьте параметр **EnableContacts** со значением `true`.

> **Важно**
>
> Для корректной синхронизации контактов версия утилиты YandexADSCIM должна быть 1.1.0.156 или выше. Скачать установочный файл

По умолчанию в качестве контактов из Active Directory будут синхронизироваться все объекты, удовлетворяющие LDAP-запросу `(&(objectClass=contact))`. Чтобы ограничить список контактов, можно воспользоваться фильтром **ContactsFilter** и применить стандартный синтаксис запросов LDAP. Например, чтобы выгрузить только контакты из группы `groupname`, используйте фильтр:

```
ContactsFilter = (&(objectClass=contact)
(memberOf=CN=groupname,CN=Users,DC=domainname,DC=com))
```

2.11. Синхронизируйте атрибуты контактов из Active Directory. Переназначить атрибуты при создании или синхронизации контактов в Яндекс 360 позволяют параметры, которые начинаются с **PropertyContact**.

Название параметра утилиты YandexADSCIM	Название атрибута (рус.)	Значение по умолчанию из Active Directory	Пример
PropertyContactFirstName	Имя	givenName	Иван

PropertyContactMiddleName	Отчество	middleName	Иванович
PropertyContactLastName	Фамилия	sn (SurName)	Иванов
PropertyContactTitle	Должность	title	Разработчик
PropertyContactDepartment	Отдел	department	Отдел разработки
PropertyContactCompany	Компания	company	ООО «Страна чудес»
PropertyContactMail	Основной email*	mail	I_ivanov@domain.ru
PropertyContactWorkPhone	Основной рабочий телефон	telephoneNumber	+7 495 123-45-67
PropertyContactOtherWorkPhone	Другие рабочие телефоны	otherTelephone	+7 495 765-43-21
PropertyContactMobile	Основной мобильный телефон	mobile	+7 012 345-67-89
PropertyContactOtherMobile	Другие мобильные телефоны	otherMobile	+7 987 654-32-10

PropertyContactIpPhone	Основной IP-телефон	ipPhone	7495 012-34-56
PropertyContactOtherIpPhone	Другие IP-телефоны	otherIpPhone	7495 987-65-43
PropertyContactAddress1	Адрес - Улица	streetAddress	Юбилейная
PropertyContactAddress2	Адрес - Город	l	Подольск
PropertyContactAddress3	Адрес - Регион	st	Московская область
PropertyContactAddress4	Адрес - Индекс	postalCode	142121

символ `-` (минус). Например, чтобы отключить синхронизацию атрибута «Должность», нужно указать `PropertyContactTitle = -`.

2.12. Поменяйте значение параметра **DryRun** на `true` перед первым запуском сервиса, если ранее (п. 2.4) вы изменяли его на `false`. Периодичность запуска сервиса определяется параметром **UpdateEveryMins = N**, где N — интервал в минутах. Запустите сервис через оснастку и проанализируйте файл лога.

Системные сообщения в логах

Уведомление	Результат
CORE Update user: user@domain.ru (Active:true -> false)	Пользователь будет заблокирован.
SCIM Update user	Изменение атрибутов пользователя в каталоге Яндекса.

SCIM Add user	Добавление пользователя в каталог Яндекса.
CORE Users: added 0, removed 3 237, modified 0	Добавлено — 0, заблокировано — 3 237, изменено — 0.
SCIM GET Users: Response is successful	Пользователи успешно зачитаны из каталога Яндекса.
AD Received user count: N	Из Active Directory загружено N пользователей.
AD Received groups count: N	Из Active Directory загружено N групп.
AD_CONFIG Wrong line N	Ошибка в строке N конфигурационного файла.
AD Received contacts count: N	Из Active Directory загружено N контактов.
SCIM Add SharedContact:	Добавление контакта в каталог Яндекса.

3. Остановите службу и запустите снова, чтобы применить изменения из конфигурационного файла. Как это сделать

Изменение настроек

Если вы хотите изменить настройки, внесите изменения в конфигурационный файл, а затем перезапустите службу **YandexADSCIM** через командную строку или диспетчер задач по инструкции.

Просмотр логов

Все логи службы сохраняются в папке `%ProgramData%\Yandex\YandexADSCIM`.

Обновление ADSCIM

Приложение обновляется автоматически: по умолчанию в конфигурационном файле указано значение `AutoUpdate = True` либо этого параметра нет, так как значение `True` является для него значением по умолчанию.

Если вы хотите обновлять приложение вручную, укажите `AutoUpdate = False`. Теперь, чтобы обновить приложение, вам нужно будет скачать последнюю версию YandexADSCIM (скачать) и запустить установочный файл.

Остановка и перезапуск ADSCIM

YandexADSCIM — это служба Windows, поэтому исполняется автоматически при запуске системы и не зависит от статуса пользователя. Но вы можете отключить ее вручную — для этого в командной строке (`cmd.exe`) введите `sc stop yandexadscim` или в диспетчере задач нажмите **Остановить**.

Для повторного запуска службы в командной строке введите `sc start yandexadscim`. Также вы можете перезапустить ADSCIM в диспетчере задач на вкладке **Службы**.

Удаление ADSCIM

Если же вы хотите удалить службу насовсем, используйте команду `sc delete yandexadscim`.

Возможные ситуации при работе с ADSCIM

Ситуация	Результат
У пользователя изменились атрибуты в Active Directory, но при этом уникальный идентификатор не изменился	Система обновит атрибуты в каталоге Яндекса (кроме основной почты и NameID).
У пользователя изменился уникальный идентификатор	Система не сможет найти объект с исходным идентификатором и заблокирует предыдущего пользователя. Далее система попытается добавить пользователя с новым идентификатором, но не сможет этого сделать, так как логин пользователя уже занят предыдущим. Если удалить заблокированного пользователя, система добавит нового без переноса каких-либо данных со старого.

Пользователь удален в Active Directory	Пользователь будет заблокирован в каталоге Яндекса.
Новый пользователь в Active Directory	Пользователь будет добавлен в каталог Яндекса с соответствующими атрибутами.
Все пользователи в каталоге Яндекса заблокированы	Это могло произойти, если: • изменилось поле основного идентификатора; • по какой-то причине приложение не смогло прочитать пользователей в каталоге Active Directory.

Написать в службу поддержки

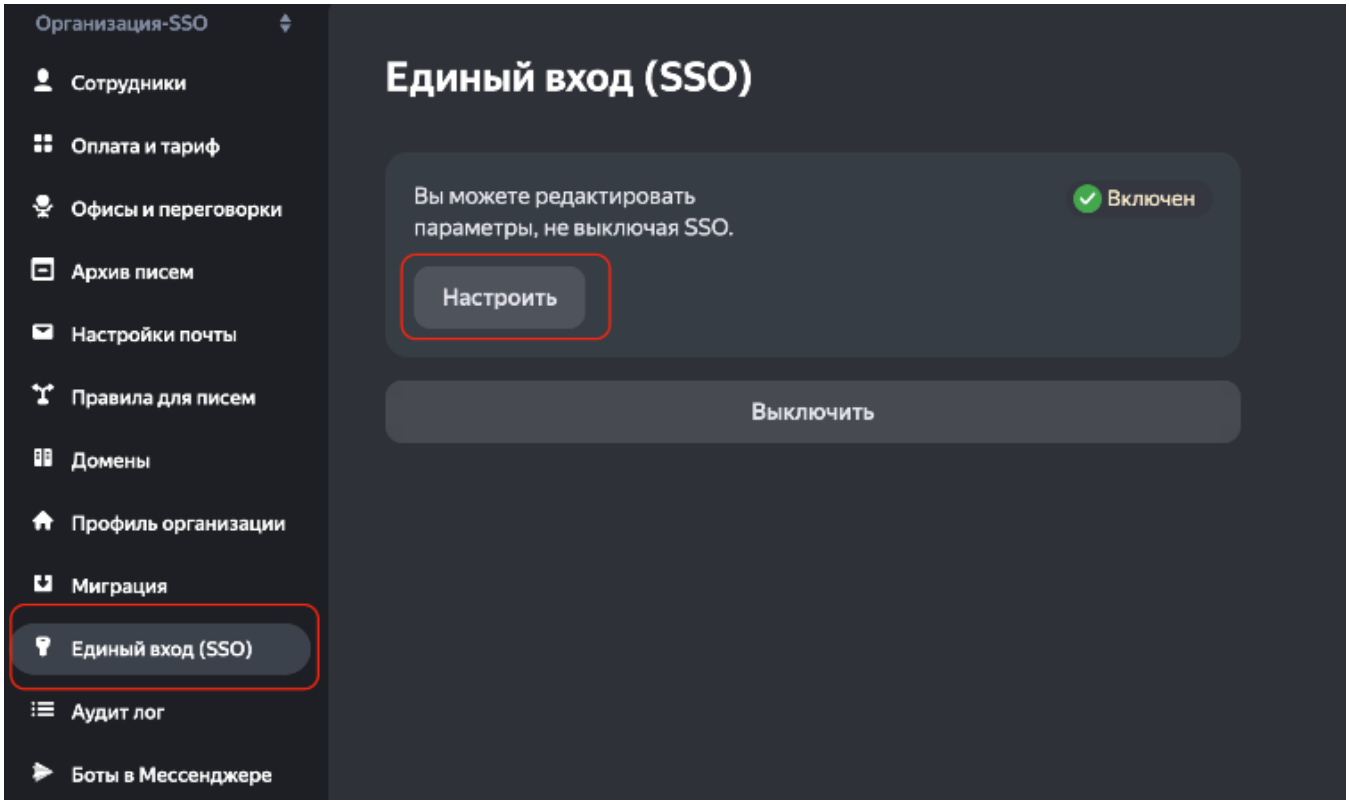
Смена поставщика удостоверений (IdP)

Если в вашей организации изменился поставщик удостоверений, вы можете организовать единый вход в Яндекс 360 для бизнеса через нового поставщика.

> **Важно**
>
> Значения атрибутов пользователей в новой и старой IdP должны совпадать.

Для смены IdP отредактируйте настройки SSO:

1. Откройте Яндекс 360 для бизнеса.
2. Перейдите в раздел **Общие настройки → Единый вход (SSO)**.
3. Нажмите **Настроить**.

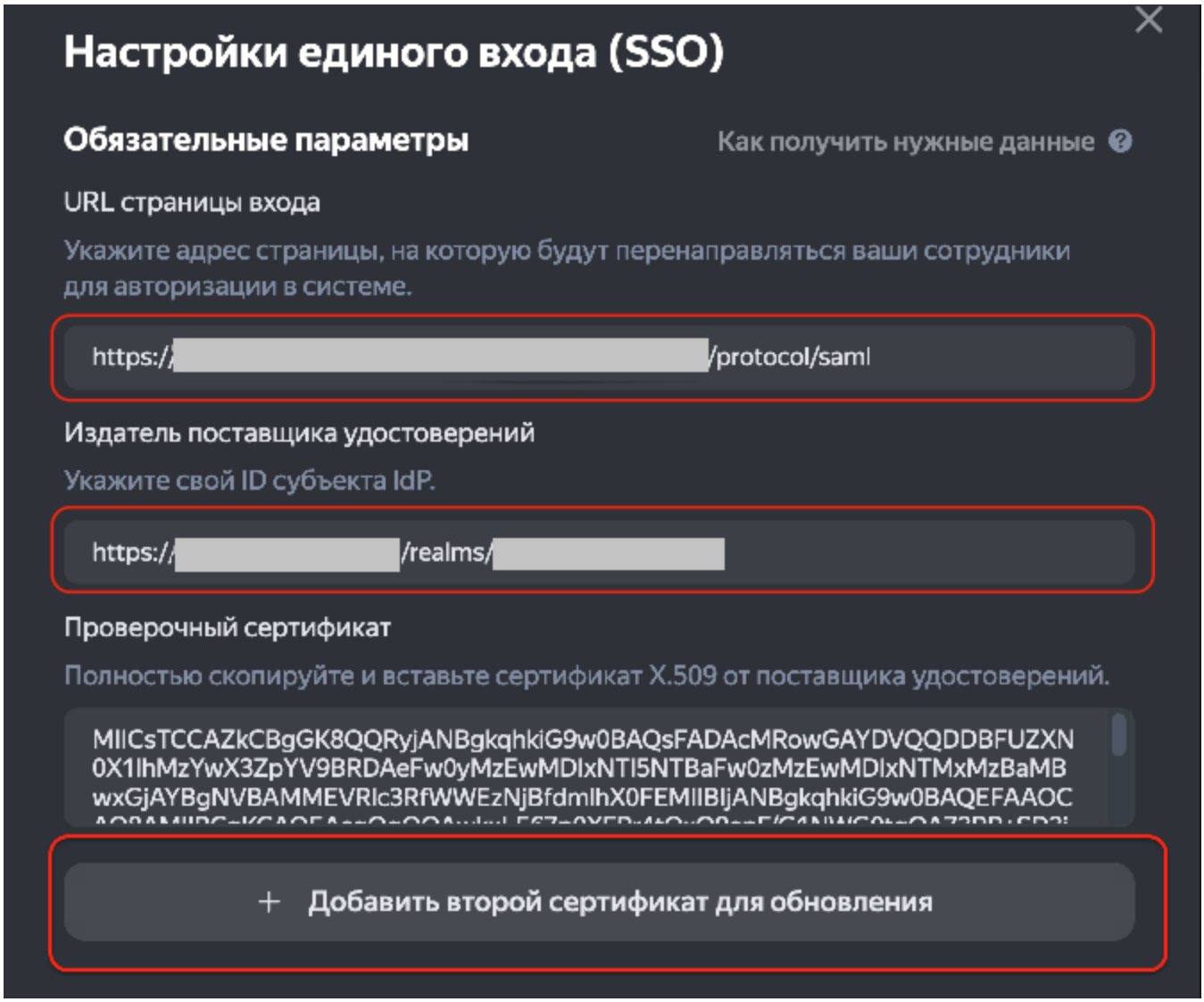


> **Примечание**
>
> Не выключайте SSO. Тогда при смене IdP пароли приложений и сессии пользователей, которые получили доступ через предыдущего поставщика удостоверений, не будут сброшены.

4. Замените параметры SSO на актуальные для текущего IdP. Данные можно получить при настройке новой федерации удостоверений:
   - URL страницы входа;
   - издатель поставщика удостоверений;

- проверочный сертификат.

> **Примечание**
>
> Если вы планируете возвращаться к работе с предыдущим поставщиком удостоверений, то не изменяйте проверочный сертификат, а добавьте новый, нажав кнопку **Добавить второй сертификат для обновления**. Тогда для возврата к предыдущему IdP потребуется заменить только два поля: URL страницы входа и издателя.



После изменения параметров аутентификация пользователей при входе в Яндекс 360 для бизнеса будет осуществляться через того поставщика удостоверений, ID которого указано в настройках в текущий момент.

Написать в службу поддержки

SAML

SAML 2.0 (Security Assertion Markup Language) — стандарт безопасности, который позволяет обмениваться аутентификационными и авторизационными данными в интернете. С его помощью пользователи могут получить доступ в несколько приложений с помощью единой учетной записи без необходимости каждый раз вводить свои логин и пароль. Это называется SSO (Single Sign-On) — система единого входа.

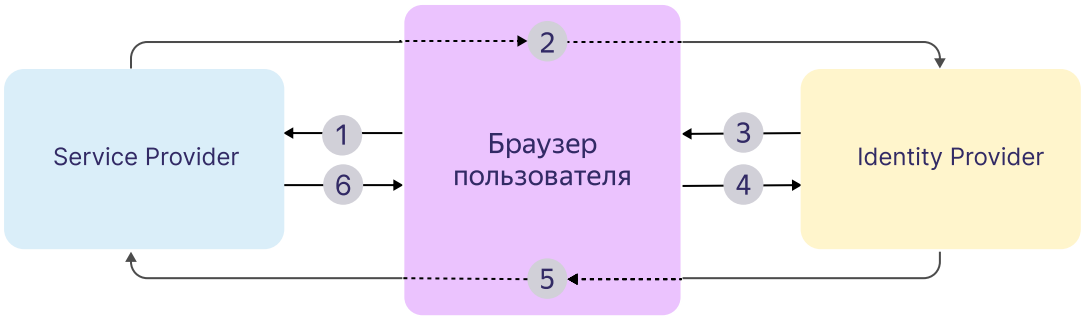
SAML SSO используется для интеграции систем управления доступом (Active Directory, Azure Active Directory, Keycloak, Avanpost FAM) с веб-приложениями и сервисами.

Как работает SSO на базе SAML 2.0

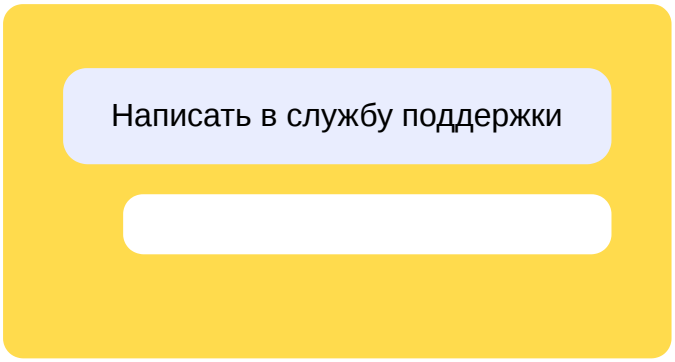
- Вся информация о логинах и паролях пользователей хранится у доверенного поставщика удостоверений (Identity Provider, IdP). В роли IdP может выступать любая система управления доступами, например Active Directory, Azure Active Directory, Keycloak, Avanpost FAM.
- Вторая сторона процесса — поставщик услуг (Service Provider, SP), например Яндекс 360 для бизнеса. В момент авторизации Service Provider отправляет пользователя проходить аутентификацию на сервере поставщика удостоверений.
- SP не взаимодействует с IdP напрямую, это происходит через браузер пользователя.

Такой подход называется федерацией удостоверений.

Обмен пользовательской информацией (логинами, состоянием аутентификации, идентификаторами и другими данными) между системой управления доступами и поставщиком услуг происходит следующим образом:



1. Пользователь открывает браузер и заходит в приложение поставщика услуг (Service Provider).
2. Приложение отвечает SAML-запросом, который браузер перенаправляет системе управления доступами (IdP).
3. Сервер IdP обрабатывает SAML-запрос и предлагает пользователю пройти аутентификацию, например ввести логин и пароль. Если пользователь уже был аутентифицирован, этот и следующий шаги пропускаются.
4. Пользователь вводит на сервере IdP данные, необходимые для аутентификации.
5. В случае успешной аутентификации система управления доступами генерирует SAML-ответ и отправляет его через браузер пользователя в приложение поставщика услуг на проверку.
6. Если проверка прошла успешно, веб-приложение предоставляет доступ пользователю.


Написать в службу поддержки

Как отключить

Если вы больше не хотите, чтобы сотрудники входили в сервисы Яндекс 360 через вашу систему аутентификации, отключите единый вход (SSO). После этого вам нужно будет завести для них новые аккаунты.

Вы также можете выключить единый вход (SSO) временно — например, чтобы изменить домен. При этом изменять настройки SSO можно и во включенном состоянии.

1. Откройте Яндекс 360 для бизнеса.
2. Перейдите в раздел **Общие настройки → Единый вход (SSO)**.
3. Нажмите **Выключить**.

Спустя некоторое время после отключения все сотрудники, которые были созданы с помощью SSO, заблокируются, но не удалятся. Вы сможете разблокировать их, если решите вернуть единый вход (SSO), или удалить вручную.

Внимание

Данные сотрудников в Почте, Диске и других сервисах перенести на новые аккаунты не получится.

Написать в службу поддержки

Меры безопасности, принимаемые Яндекс 360

На этой странице рассказывается о технических и организационных мерах, которые Яндекс реализует для защиты данных клиентов Яндекс 360 для бизнеса.

Организация информационной безопасности

Система управления информационной безопасностью

Яндекс поддерживает систему управления информационной безопасностью, принимает и применяет внутренние политики и процедуры, чтобы минимизировать риски нарушения информационной безопасности для данных клиентов.

Ответственность за безопасность

В Яндексе есть команда, ответственная за внедрение и мониторинг процедур безопасности.

Управление рисками

У Яндекса есть программа управления рисками, которая включает в себя регулярную оценку рисков и выполнение планов их обработки.

Безопасность человеческих ресурсов

Обучение

- Яндекс требует от сотрудников и подрядчиков применять меры информационной безопасности в соответствии с правилами и процедурами компании.
- Яндекс обучает сотрудников надлежащему обращению с данными клиентов.

Прекращение или смена работы

Яндекс определяет и доводит до сведения своих сотрудников и подрядчиков их обязанности по обеспечению информационной безопасности, а также добивается выполнения тех из них, которые остаются в силе после увольнения или смены места работы.

Управление активами

Допустимое использование

Яндекс документирует и соблюдает правила допустимого использования информации и активов, связанных с информацией и средствами обработки информации.

Возвращение активов

Предусмотрено, что после прекращения трудового договора сотрудники Яндекса должны вернуть организационные активы, которые были в их распоряжении.

Классификация информации

Яндекс классифицирует информацию с точки зрения требований законодательства, ценности, критичности и чувствительности к несанкционированному раскрытию или изменению.

Обращение с активами

Яндекс разрабатывает и внедряет процедуры обращения с активами в соответствии с принятой схемой классификации информации.

Управление доступом

Политика доступа к данным клиентов

Регламенты Яндекс 360 запрещают доступ сотрудников к данным клиентов, если иное не предусмотрено договором или законодательством.

Политика управления доступом

У Яндекса есть политика, которая предусматривает, что только авторизованные лица имеют доступ к объектам, защищенным зонам, вычислительным и сетевым ресурсам.

Доступ к сетям и системам

- Доступ к сетям и системам Яндекса предоставляется уполномоченным сотрудникам.
- Руководители сотрудников Яндекса утверждают доступ подчиненных к объектам, защищенным зонам, вычислительным и сетевым ресурсам.
- Яндекс ограничивает права доступа пользователя минимальным набором прав, необходимым для выполнения его работы и на необходимое время.
- Яндекс размещает интерфейсы управления аппаратным обеспечением в сегрегированных сетях с ограниченным доступом авторизованного персонала.
- Яндекс предоставляет доступ к исходному коду уполномоченным лицам в соответствии с политикой безопасности.

Проверка прав доступа пользователей

Яндекс ежегодно пересматривает все права доступа сотрудников.

Отзыв или корректировка прав доступа

Яндекс отзывает права доступа к информации и системам для сотрудников, которые прекращают работу в компании, и корректирует при изменениях круга их ответственности.

Качество паролей

Яндекс обеспечивает качественные пароли во внутренних системах управления паролями. Проверки учитывают минимальную длину пароля, количество классов символов и максимальный срок действия.

Физическая безопасность и безопасность среды

Контроль физического доступа

У Яндекса есть надлежащие средства контроля физического доступа, которые нацелены на обеспечение доступа в офисы и дата-центры только авторизованному персоналу.

Безопасная утилизация или повторное использование оборудования

Конфиденциальные данные на носителях информации удаляются или надежно перезаписываются перед повторным использованием носителей. Если носители становятся непригодны, Яндекс утилизирует их, следуя формальным процедурам.

Безопасность данных и управление жизненным циклом информации

Безопасность передачи данных

Яндекс защищает с использованием протокола TLS информацию клиентов, которая передается по общедоступным сетям и во внутренней сети.

Управление инцидентами

Реагирование на инциденты. Отчетность

- В Яндексе есть формальный процесс мониторинга, отчетности и реагирования в случае угроз безопасности, чтобы их идентифицировать, регистрировать и соответственно реагировать на известные или предполагаемые инциденты.
- В Яндексе есть процедуры уведомления клиентов без неоправданных задержек об утечках данных клиентов.

Разработка и обслуживание информационных систем

Жизненный цикл разработки систем

В Яндексе есть жизненный цикл разработки систем, который регулирует разработку и развертывание систем и приложений.

Требования информационной безопасности

Связанные с информационной безопасностью требования Яндекс применяет к новым информационным системам и усовершенствованию уже существующих.

Безопасная разработка

- В Яндексе постоянно развиваются ключевые компоненты процесса безопасной разработки: Security Development Lifecycle, SDLC.
- Яндекс контролирует изменения в системах в рамках жизненного цикла разработки с помощью формальных процедур контроля изменений. Они включают в себя обзор архитектуры безопасности и аудит безопасности продуктов.
- Яндекс создает и надлежащим образом защищает среды для разработки и интеграции систем во всем жизненном цикле разработки систем.
- Яндекс разделяет среды разработки, тестирования и продакшн-среду.
- У Яндекса есть процедуры, предусматривающие, что производственные данные никогда не реплицируются в средах разработки или тестирования.

Управление уязвимостями

- Яндекс регулярно тестирует облачную платформу на проникновение и сканирует на уязвимости, чтобы обнаруживать, смягчать и решать проблемы безопасности.
- Яндекс устраняет обнаруженные уязвимости до перехода систем в производство.
- У Яндекса есть политика управления исправлениями. Она документирует максимальное время между моментом поставки критического патча безопасности и моментом его применения.
- Яндекс проводит программу «Охота за ошибками», которая поощряет этичных хакеров находить уязвимости в продуктах и сообщать об этом компании за награду.

Криптографические стандарты

В Яндексе утверждена политика, которая устанавливает минимальные криптографические стандарты. Им должны соответствовать все приложения, а также сетевые и вычислительные ресурсы.

Непрерывность работы и аварийное восстановление

Избыточность

- Яндекс использует механизмы резервирования для всех критических сервисов.
- Яндекс работает в нескольких территориально распределенных дата-центрах, предназначенных для круглосуточной работы без выходных и защищенных от угроз окружающей среды.
- Яндекс использует избыточность хранилищ данных, которая нацелена сохранить данные клиентов на случай выхода оборудования из строя.

Тесты

Яндекс регулярно тестирует свои планы обеспечения непрерывности работы и аварийного восстановления.

Обзор информационной безопасности

Самостоятельная оценка

- Яндекс регулярно проверяет свои информационные системы на соответствие политике и стандартам информационной безопасности компании.
- Яндекс оценивает и пересматривает свой подход к управлению и реализации информационной безопасности с запланированной регулярностью или при существенных изменениях.

Яндекс 360 и Браузер для организаций: как получить идентификаторы

Чтобы подключить тариф Яндекс 360 с Браузером для организаций, понадобятся два идентификатора:

- **user_id** — идентификатор сотрудника, который станет администратором Браузера;
- **company_id** — идентификатор организации, который будет указан в лицензиях Браузера.

Получить идентификаторы нужно только один раз при подключении тарифа.

Кто может получить идентификаторы

Идентификаторы должен получить сотрудник, который станет администратором Браузера.

Можно ли сделать так, чтобы администраторов Браузера было несколько?

Аккаунт администратора Браузера может быть только один. Но можно сделать так, чтобы этим аккаунтом пользовались несколько сотрудников, например системные администраторы, технические специалисты, менеджеры.

Для этого:

1. Владелец организации или ее администратор должен создать отдельный аккаунт для совместного использования, а затем передать нужным сотрудникам почтовый адрес и пароль для входа в этот аккаунт. Как создать аккаунт.
2. Сотрудник, который будет выполнять роль администратора Браузера, должен войти в общий аккаунт и получить идентификаторы по инструкции.

Как получить идентификаторы

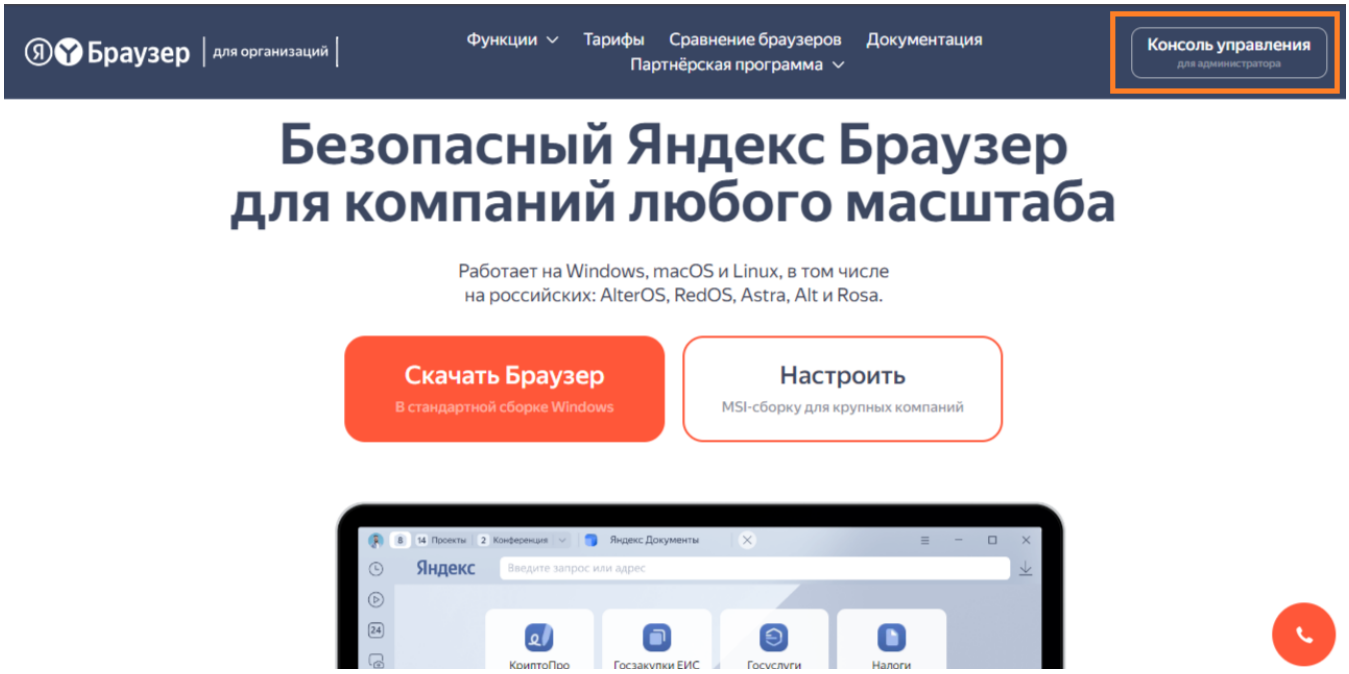
1. Откройте страницу id.yandex.ru.
2. Убедитесь, что вы вошли в аккаунт сотрудника, который должен стать администратором Браузера. Если в вашей организации будет использоваться общий аккаунт, войдите в него.

   Если вы вошли не в тот аккаунт, смените его:

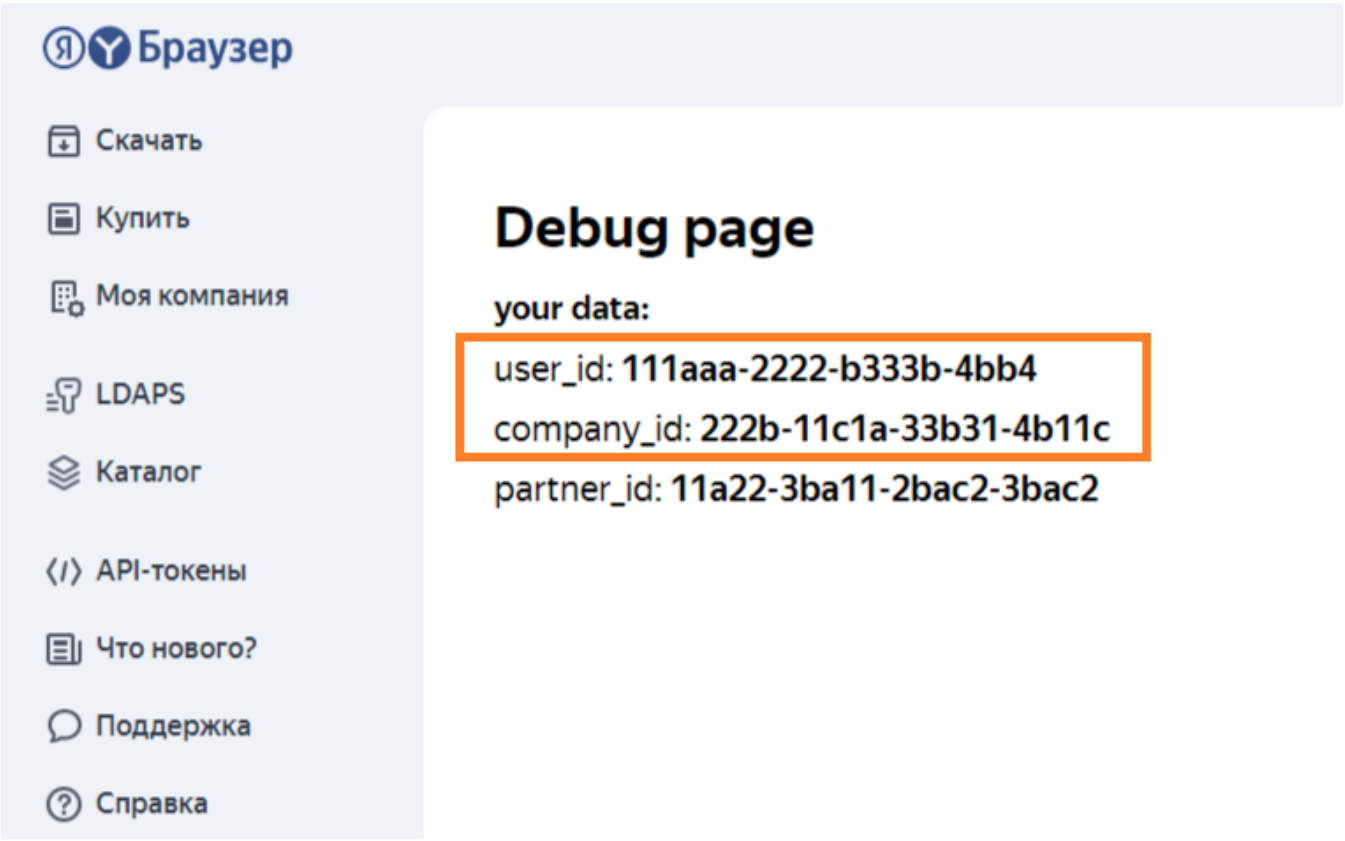
   2.1. Нажмите на портрет в правом верхнем углу.

   2.2. Пролистайте меню вниз до списка аккаунтов.

   2.3. Выберите нужный аккаунт. Если его еще нет в списке, нажмите **Добавить аккаунт**. Для входа используйте полный почтовый адрес (например, browser-admin-login@your-domain.ru) и пароль.
3. Откройте страницу browser.yandex.ru/corp/. Нажмите кнопку **Консоль управления** в правом верхнем углу.



4. Откройте страницу browser.yandex.ru/corp/debug.
5. Скопируйте строки **user_id** и **company_id** и отправьте ответом на письмо, в котором у вас их запрашивали.



Документация программы «Рассылки»

Название документа	Ссылка на скачивание
Инструкция по установке экземпляра ПО	Скачать документ
Документация, содержащая описание функциональных характеристик экземпляра ПО	Скачать документ
Документация, содержащая описание процессов, обеспечивающих поддержание жизненного цикла ПО, в том числе устранение неисправностей и совершенствование, а также информацию о персонале, необходимом для обеспечения такой поддержки	Скачать документ
Документация, содержащая информацию, необходимую для эксплуатации экземпляра ПО	Скачать документ

Как работает служба поддержки Яндекс 360 для бизнеса

Если у вас возник вопрос о Яндекс 360 для бизнеса и вы не нашли ответа в Справке, напишите в службу поддержки. Специалисты проконсультируют вас и помогут разобраться со сложностями.

Как связаться со службой поддержки

- Через форму обратной связи
- По электронной почте support-team@360.yandex.ru
- Через чат в аккаунте администратора организации

С чем поможет поддержка

Вы можете узнать:

- о возможностях сервисов Яндекс 360 для бизнеса;
- о доступных тарифах;
- о подключении и настройке;
- о миграции в Яндекс 360 для бизнеса с других платформ;
- об оплате, оформлении документов и заполнении реквизитов;
- об управлении организацией;
- о решении технических проблем.

Если у вас есть идеи и предложения по улучшению сервисов Яндекс 360 для бизнеса, расскажите о них в своем обращении.

Примечание

Служба поддержки Яндекс 360 для бизнеса не сможет помочь вам с вопросами по настройке и отладке стороннего программного обеспечения — в этом случае вам лучше обратиться к его производителю.

Как быстро вы получите ответ

Служба поддержки Яндекс 360 для бизнеса работает круглосуточно, 7 дней в неделю. Номер вашего обращения поступит на адрес электронной почты, который вы указали в своем сообщении.

Первый ответ от службы поддержки обычно приходит в течение 3 часов. Срок полного решения проблемы зависит от ее тематики и сложности.

Переезд в Яндекс 360 для бизнеса

Мы собрали ответы на частые вопросы о том, как перенести данные вашей организации в Яндекс 360 для бизнеса из Google Workspace, Microsoft 365 и других платформ. Смотреть >

Связаться со службой поддержки

Если вопрос про Яндекс Доски — заполните отдельную форму

О том, как перенести данные из Miro, настроить доступы и начать работу, читайте в Справке Яндекс Досок.

Если там нет ответа на ваш вопрос, заполните отдельную форму — мы ответим вам на почту.

Если вы не нашли ответ на свой вопрос в Справке, напишите нам.