??????????????

Доступ к разделу "Безопасность" предоставляется должностным лицам с правами доступа "Безопасность"

- События
- 2ФА
- Ограничение доступа
- Пароль
- УНЭП EasyDocs
- Single sign-on (SSO)
  - ADFS
  - Authentik

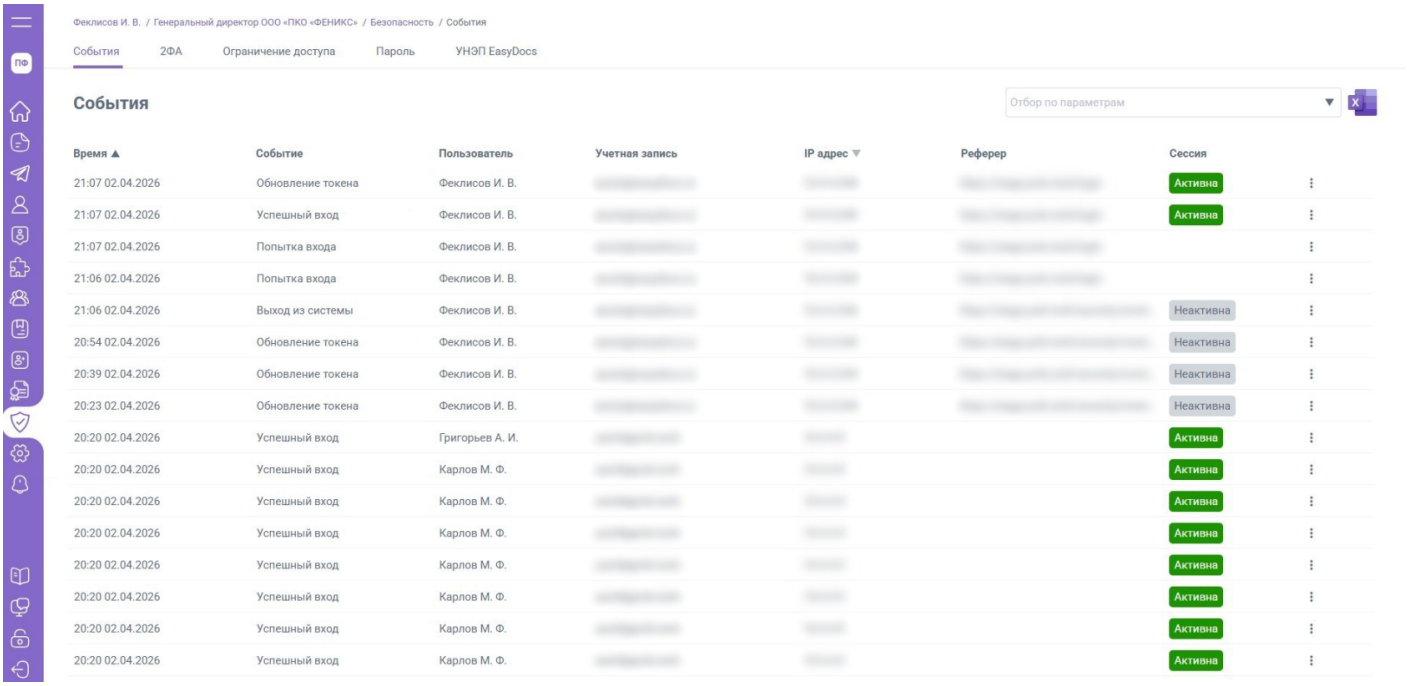
???????

Вкладка «События» предназначена для просмотра истории по всем значимым действиям, выполненным внутри сервиса (вход в личный кабинет, подписание документов и др.), что позволяет:

- Контролировать безопасность личных кабинетов пользователей
- Расследовать подозрительные действия
- Отслеживать, кто, когда и откуда работал внутри сервиса

Вкладка состоит из следующих столбцов:

- **Время** – дата и время события
- **Событие** – тип выполненного действия (вход, подписание, смена пароля и тд.)
- **Пользователь** – ФИО пользователя, который выполнил действие
- **Учетная запись** – e-mail, на который зарегистрирован личный кабинет пользователя
- **IP адрес** – IP адрес устройства, с которого пользователь выполнил действие
- **Референр** – ссылка на страницу, откуда пользователем выполненено действие из столбца «События» (например, страница входа)
- **Сессия** – статус сессии (активна / неактивна)



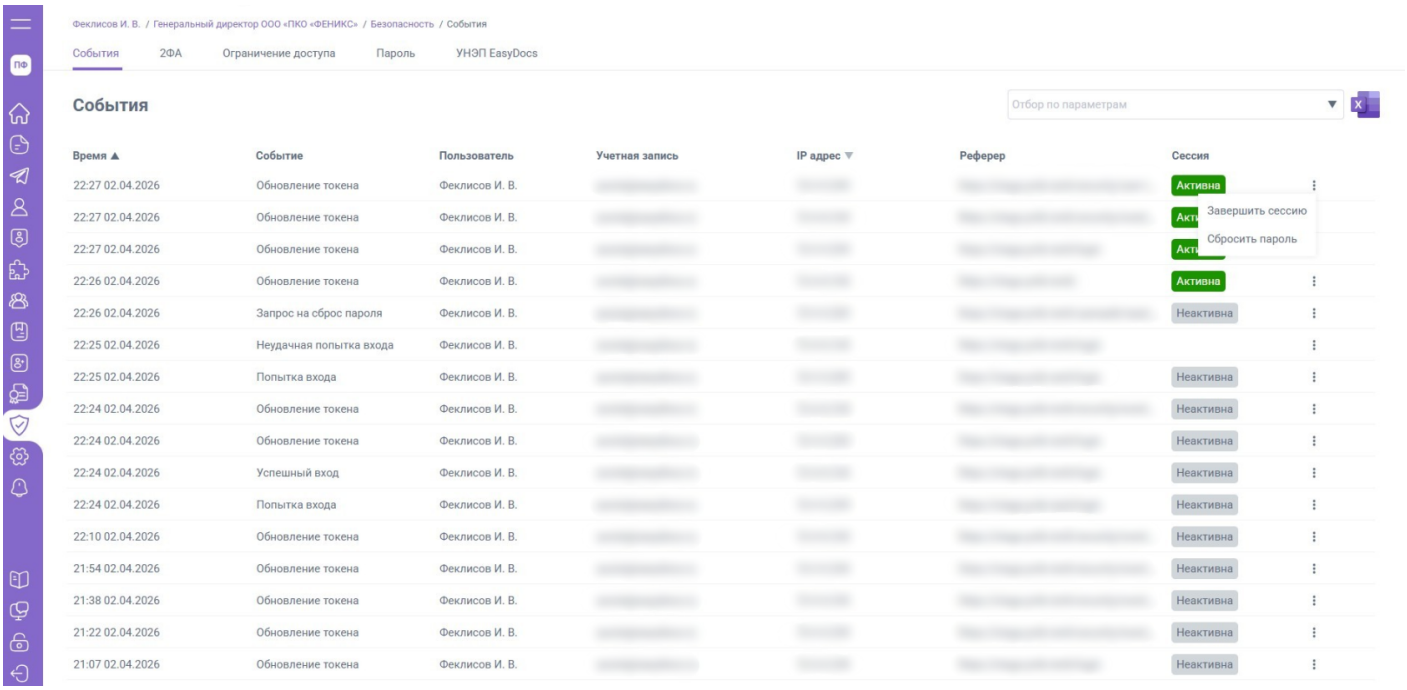
Каждая строка вкладки = одному действию пользователя – столбец «Событие» отображает, что именно произошло. Ниже приведен полный список событий с описанием, которое поможет определить, какое именно действие было выполнено внутри сервиса.

- **Попытка входа** - Пользователем был введен e-mail учетной записи, но вход еще не завершен
- **Успешный вход** - Пользователь успешно вошел в личный кабинет
- **Неудачная попытка входа** - Пользователь ввел неправильный e-mail учетной записи или пароль
- **Выход из системы** — Пользователь нажал «Выйти»
- **Запрос 2ФА кода** — От пользователя ожидается ввод кода подтверждения (направленного на email, в СМС, мессенджер или приложение аутентификатор) при двухфакторной аутентификации
- **Успешная 2ФА верификация** — При двухфакторной аутентификации пользователь корректно ввел код подтверждения (направленный на e-mail, в СМС, мессенджер или приложение аутентификатор)
- **Неудачная 2ФА верификация** — При двухфакторной аутентификации пользователь некорректно ввел код подтверждения (направленный на e-mail, в СМС, мессенджер или приложение аутентификатор) или истекло время ввода кода
- **Обновление токена** — Обновление токена доступа пользователя (каждые 15 минут при активной сессии, при обновлении страницы и при входе в личный кабинет)
- **Запрос на сброс пароля** — Пользователем запрошено восстановление пароля
- **Запрос на смену email** — Пользователем начат процесс изменения e-mail учетной записи
- **Успешная смена email** — Пользователь изменил email учетной записи
- **Запрос на смену контакта** — Пользователь начал процесс изменения контактного e-mail и (или) контактного номера
- **Успешная смена контакта** — Пользователь изменил контактный e-mail и (или) контактный номер
- **Запрос на смену типа 2ФА** — Пользователь начал процесс изменения способа доставки кода, направляемого при двухфакторной аутентификации
- **Успешная смена типа 2ФА** — Пользователь завершил процесс изменения способа доставки кода, направляемого при двухфакторной аутентификации
- **Попытка подписания** — Пользователь начал процесс подписания (процесс не завершен)
- **Запрос 2ФА для подписания** — От пользователя ожидается ввод кода подтверждения (направленного на email, в СМС, мессенджер или приложение аутентификатор) при подписании
- **Успешная 2ФА для подписания** — При подписании пользователь корректно ввел направленный код подтверждения
- **Неудачная 2ФА для подписания** — При подписании пользователь некорректно ввел направленный код подтверждения или истекло время ввода кода
- **Успешное подписание ПЭП** — Пользователь подписал документ простой электронной подписью
- **Неудачное подписание ПЭП** — Пользователем получена ошибка при попытке подписания документа простой электронной подписью
- **Успешное подписание Госключ** — Пользователь подтвердил подписание, Госключ передал ответное событие о подписании документа

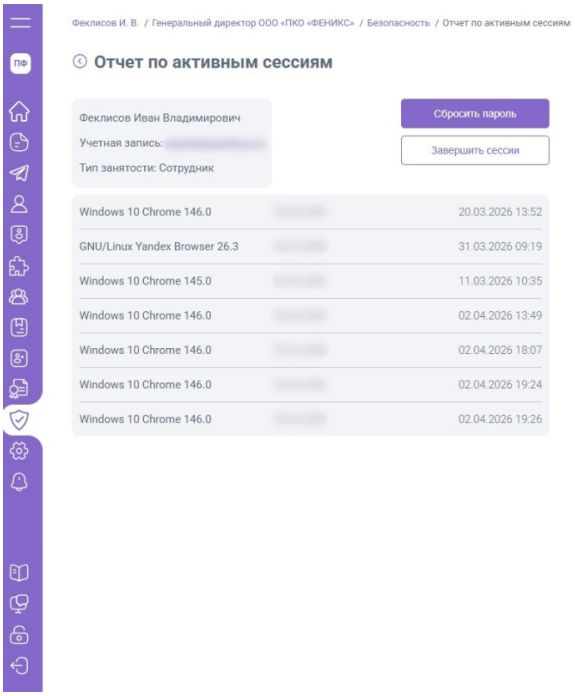
- **Неудачное подписание Госключ** — Пользователем получена ошибка при попытке подписания документа в Госключе
- **Успешное подписание УКЭП** — Пользователь успешно завершил подписание мобильной УКЭП или УКЭП на usb носителе
- **Неудачное подписание УКЭП** — Пользователем получена ошибка при попытке подписания мобильной УКЭП или УКЭП на usb носителе
- **Документ отклонен** — Пользователь отклонил поступивший документ
- **Документ создан** — Пользователь создал документ, но не завершил его отправку в сторону контрагента (ЮЛ / ИП)
- **Документ просмотрен** — Пользователь открыл документ для чтения
- **Начало редактирования** — Пользователь начал процесс редактирования документа по кнопке «Редактировать»
- **Документ обновлен** — Пользователь завершил процесс редактирования документа
- **Ознакомление с документом** — Пользователь ознакомился с поступившим документом
- **Документ отправлен в архив** — По документу завершен маршрут документооборота или на одном из этапов документ был принудительно отправлен в архив (отклонить / отозвать / в архив)
- **Запрос смены 2ФА для сертификата** — Пользователь начал процесс изменения способа доставки кода подтверждения 2ФА
- **Успешная 2ФА для сертификата** — Пользователь завершил процесс изменения способа доставки кода подтверждения 2ФА

К каждой строке вкладки «События» доступно меню с действиями:

- **Завершить сессию** – сессия пользователя будет завершена, потребуется повторный вход в личный кабинет
- **Сбросить пароль** – текущий пароль будет сброшен, пользователю потребуется восстановить пароль для доступа к личному кабинету



При нажатии на одно из событий списка, откроется отчет по активным сессиям пользователя, где удастся сбросить пароль и (или) завершить все активные сессии.

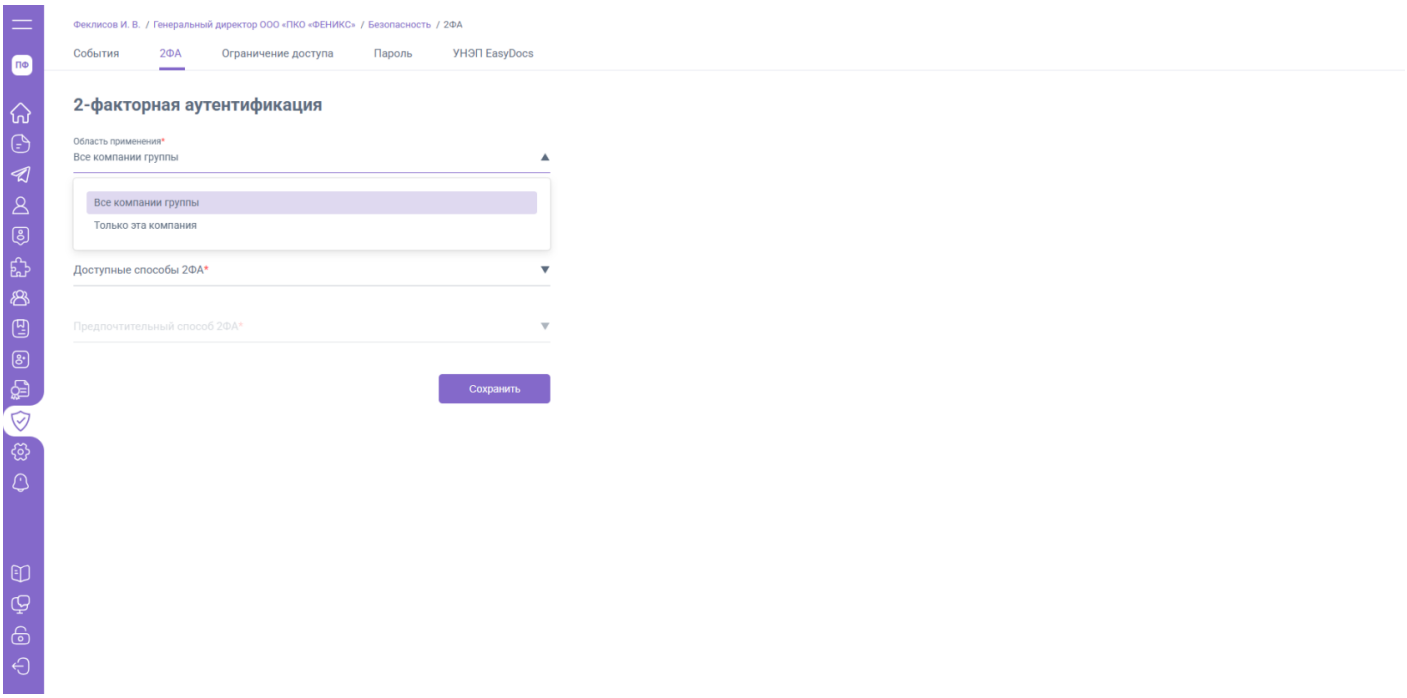


2??

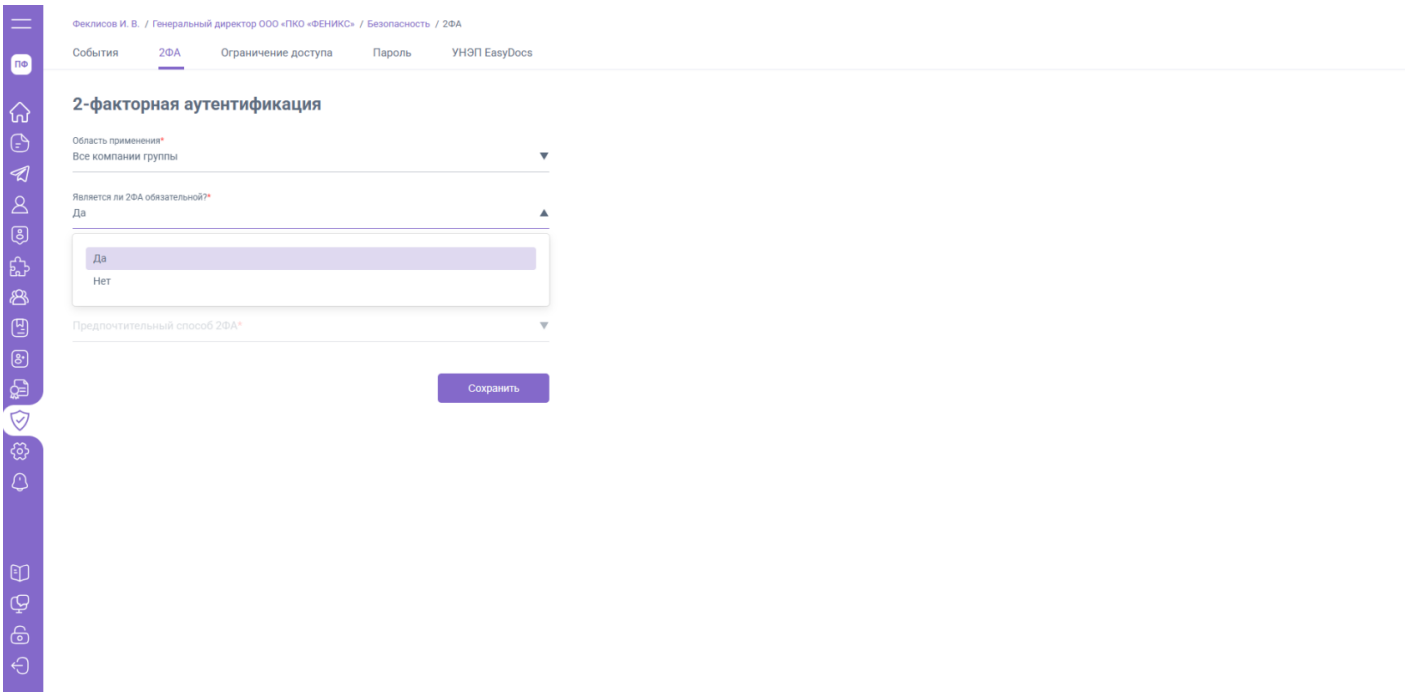
Вкладка «2ФА» предназначена для управления двухфакторной аутентификацией пользователей в EasyDocs.

1. Область применения – доступна только главной компании группы и определяет, на какие компании (только эта компания или все компании группы) распространяются настройки 2ФА

- Если выбран вариант «Только эта компания» – другие компании группы смогут самостоятельно настраивать требования к 2ФА
- Если выбран вариант «Все компании группы» – другие компании группы не смогут самостоятельно настраивать требования к 2ФА



2. Является ли 2ФА обязательной? – включает (да) и отключает (нет) требование подтверждения через 2ФА при каждом входе пользователя в EasyDocs

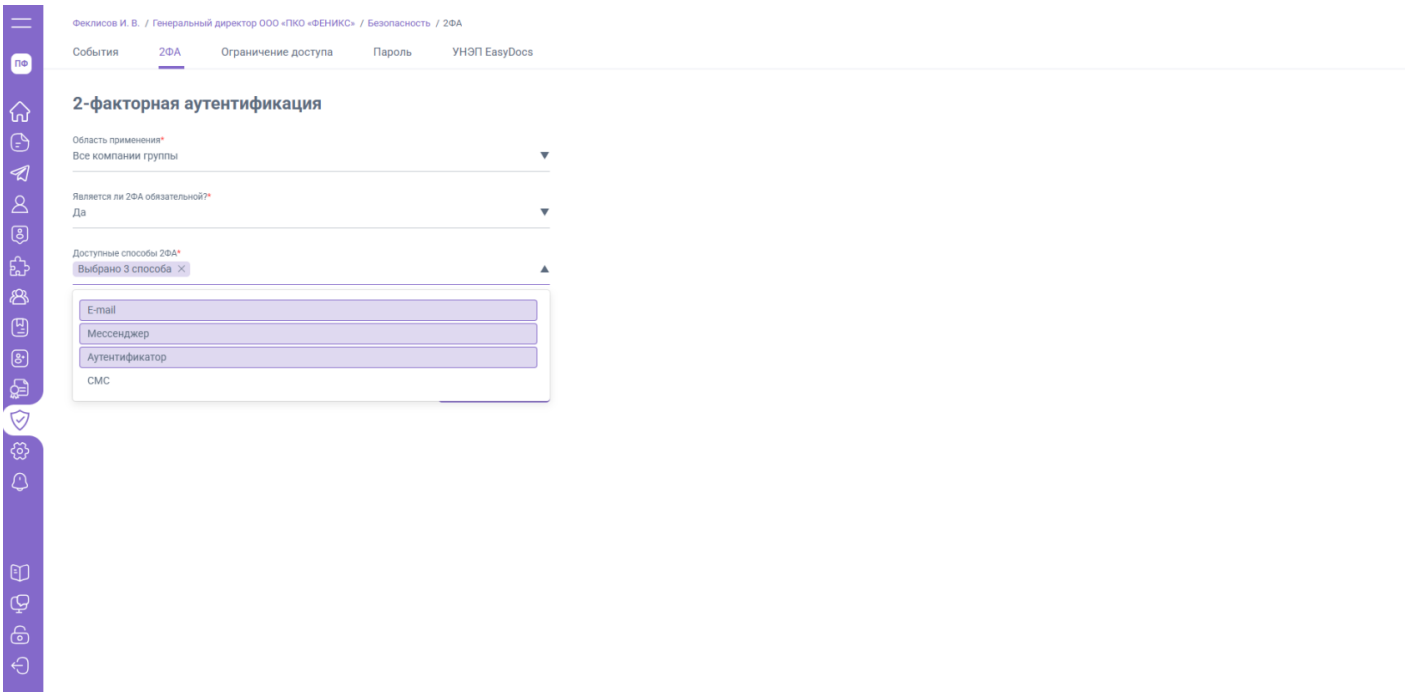


3. Доступные способы 2ФА – определяет каким способом пользователи будут получать код подтверждения

- Email
- Мессенджер
- СМС
- Приложение аутентификатор

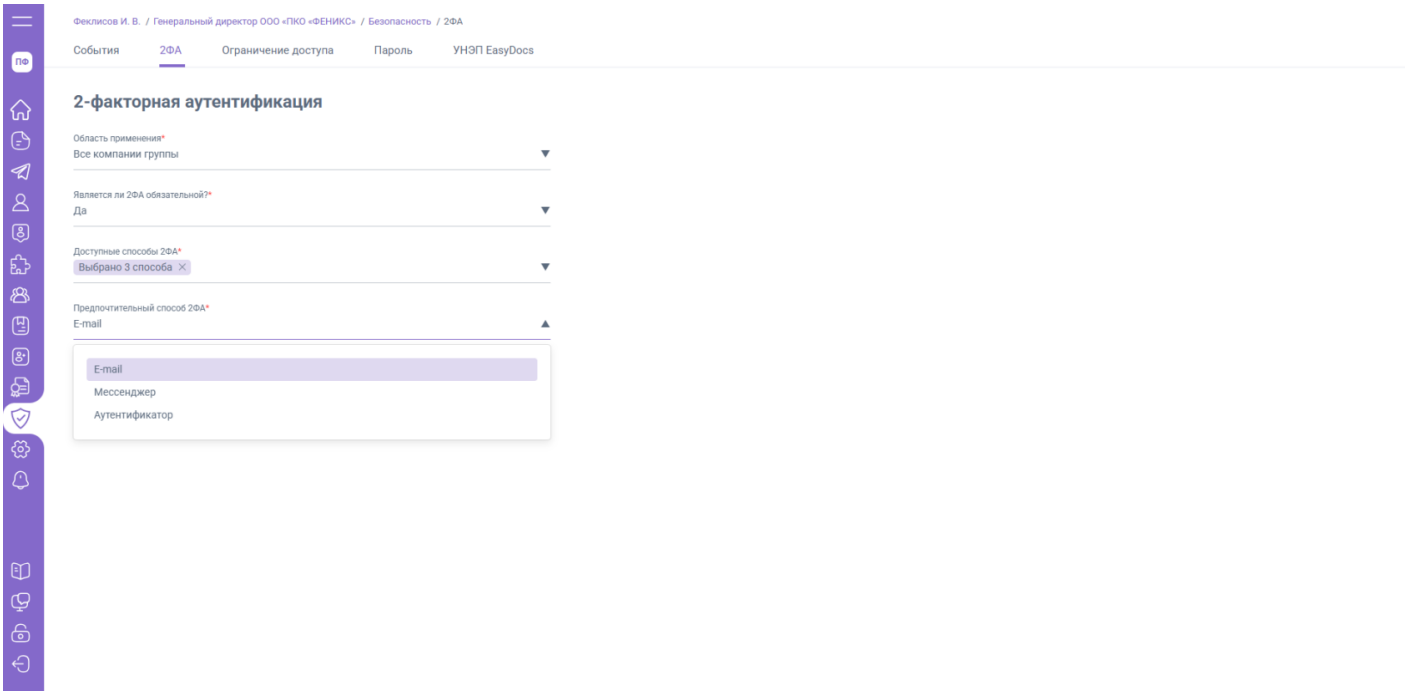
Важно!

- **Вы можете выбрать один или несколько способов одновременно**
- **Выбранные способы будут доступны пользователям в личном кабинете**
- **Если способ не выбран – пользователь не сможет его использовать**



4. Предпочтительный способ 2ФА – задает предпочтительный способ доставки кода подтверждения

- Если в «Доступные способы 2ФА» выбран только один способ – только этот способ будет доступен в «Предпочтительный способ 2ФА»
- Если в «Доступные способы 2ФА» выбрано несколько способов – потребуется выбрать предпочтительный способ (например, email). Выбранный способ будет устанавливаться пользователям автоматически, но если в «Доступные способы 2ФА» выбрано несколько способов, пользователь сможет обновить данные



?????????? ???????

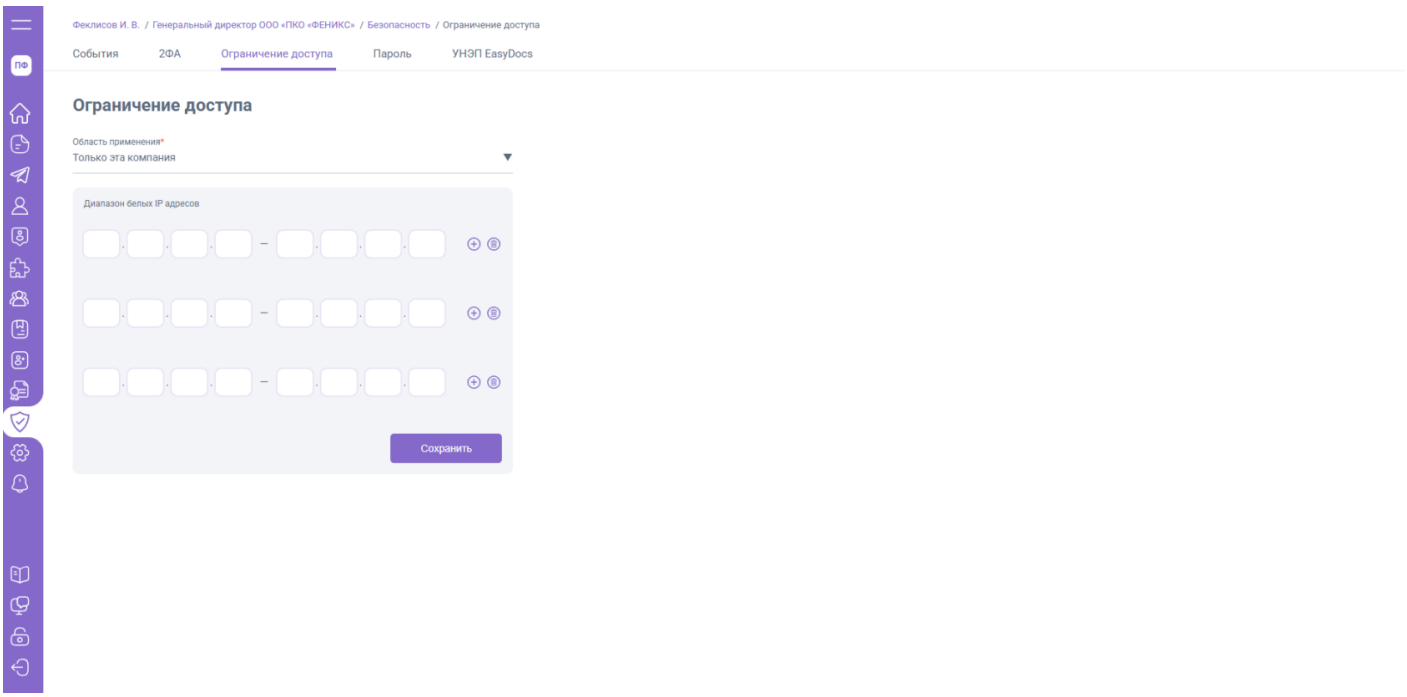
Вкладка «Ограничение доступа» предназначена для настройки подключений по IP адресам (например, вы можете разрешить доступ к личным кабинетам пользователей только по офисным IP адресам).

1. Область применения – список доступен главной компании группы и определяет, на какие компании (только эта компания или все компании группы) распространяются настройки

- Если выбран вариант «Только эта компания» – другие компании группы смогут самостоятельно добавлять диапазоны IP адресов
- Если выбран вариант «Все компании группы» – другие компании группы не смогут самостоятельно добавлять диапазоны IP адресов

2. Диапазон белых IP адресов – задает список IP адресов, с которых разрешен доступ в EasyDocs

- Если диапазон не задан – доступ будет разрешен со всех IP адресов
- Количество задаваемых диапазонов не ограничено
- Для добавления нового диапазона нажмите «+»
- Для удаления добавленного диапазона нажмите кнопку в виде мусорного ведра



??????

Вкладка «Пароль» предназначена для управления требованиями к задаваемым пользователями паролям.

1. Область применения – список доступен главной компании группы и определяет, на какие компании (только эта компания или все компании группы) распространяются настройки

- Если выбран вариант «Только эта компания» – другие компании группы смогут самостоятельно настраивать требования к паролям
- Если выбран вариант «Все компании группы» – другие компании группы не смогут самостоятельно настраивать требования к паролям

2. Длина пароля – определяет допустимое количество символов в пароле пользователя

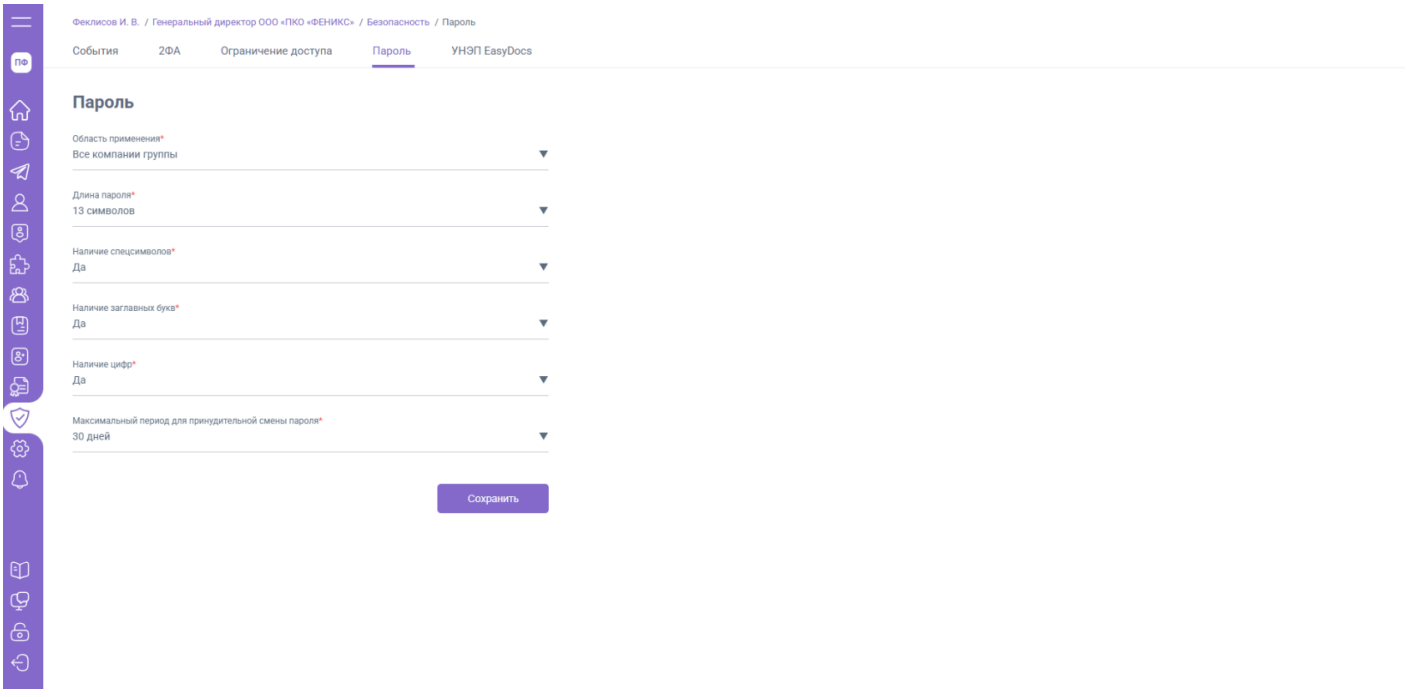
- Минимальное количество символов – 8
- Максимальное количество символов – 20

3. Наличие спецсимволов (!, @, # и др.)

4. Наличие заглавных букв

5. Наличие цифр

6. Максимальный период для принудительной смены пароля – количество дней, через которое пользователь будет обязан сменить пароль



???? EasyDocs

Вкладка «УНЭП EasyDocs» предназначена для управления способами доставки кодов подтверждения УНЭП EasyDocs.

1. Область применения – список доступен главной компании группы и определяет, на какие компании (только эта компания или все компании группы) распространяются настройки

- Если выбран вариант «Только эта компания» – другие компании группы смогут самостоятельно настраивать требования к способам доставки кодов подтверждения УНЭП EasyDocs
- Если выбран вариант «Все компании группы» – другие компании группы не смогут самостоятельно настраивать требования к способам доставки кодов подтверждения УНЭП EasyDocs

2. Доступные способы доставки кодов подтверждения – определяет каким способом пользователи будут получать код подтверждения

- E-mail
- Мессенджер
- СМС
- Приложение аутентификатор

Важно!

- Вы можете выбрать один или несколько способов одновременно
- Выбранные способы будут доступны пользователям в личном кабинете
- Если способ не выбран – пользователь не сможет его использовать

4. Предпочтительный способ доставки кодов подтверждения – задает способ доставки кода подтверждения

- Если в «Доступные способы доставки кодов подтверждения» выбран только один способ – только этот способ будет доступен в «Предпочтительный способ доставки кодов подтверждения»
- Если в «Доступные способы доставки кодов подтверждения» выбрано несколько способов – потребуется выбрать предпочтительный способ (например, e-mail). Выбранный способ будет устанавливаться пользователям автоматически, но если в «Доступные способы доставки кодов подтверждения» выбрано несколько способов, пользователь сможет обновить данные.



УНЭП EasyDocs

Область применения*
Все компании группы

Доступные способы доставки кодов подтверждения*
E-mail

Предпочитаемый способ доставки кодов подтверждения*
E-mail

Сохранить

Single sign-on (SSO)

Функция, которая позволяет входить в систему **через один аккаунт**, без необходимости вводить логин и пароль отдельно для EasyDocs.

Single sign-on (SSO)

ADFS

Работодатель может выбрать для авторизации собственную базу пользователей Active Directory. Для интеграции EasyDocs с Active Directory необходимо направить в службу заботы о клиентах запрос о подключении ADFS с указанием следующих параметров:

- Client Identifier
- Адрес сервера ADFS
- Домен адреса электронной почты

Для корректной авторизации пользователей EasyDocs через ADFS необходимо выполнить следующие настройки:

Шаг 1 — Настройка группы приложений

На экране управления AD FS перейдите в **раздел ADFS «Группы приложений» (Application Groups)**и нажмите «**Добавить группу приложений» (Add Application Group)**



Введите **имя** для группы приложений, например «**EasyDocs**», выберите **Веб-браузер, подключающийся к веб-приложению (Web browser accessing a web application)** и нажмите **«Далее»**.



Сохраните значение **Идентификатор клиента (Client Identifier)**, оно потребуется для на стороне EasyDocs для настройки интеграции.

В значении **Redirect URI** укажите Веб-сервер EasyDocs: **https://my.easydocs.ru/oauth-callback**и нажмите «**Добавить».**

Выберите **Разрешение для каждого (Permit everyone)**и нажмите «**Далее**».



Проверьте настройки и нажмите **«Далее».**



Закройте мастер, нажав «**Закрыть**». Теперь приложение EasyDocs зарегистрировано в ADFS.



Шаг 2 — Настройка утверждений (claims)

Откройте **свойства** для группы приложений, которую мы только что создали. Выберите запись **Веб-приложение (Web application)**и нажмите **«Изменить»**





На вкладке **Правила Преобразования выдачи (Issuance Transform Rules)** нажмите кнопку **Добавить правило (Add Rule).**



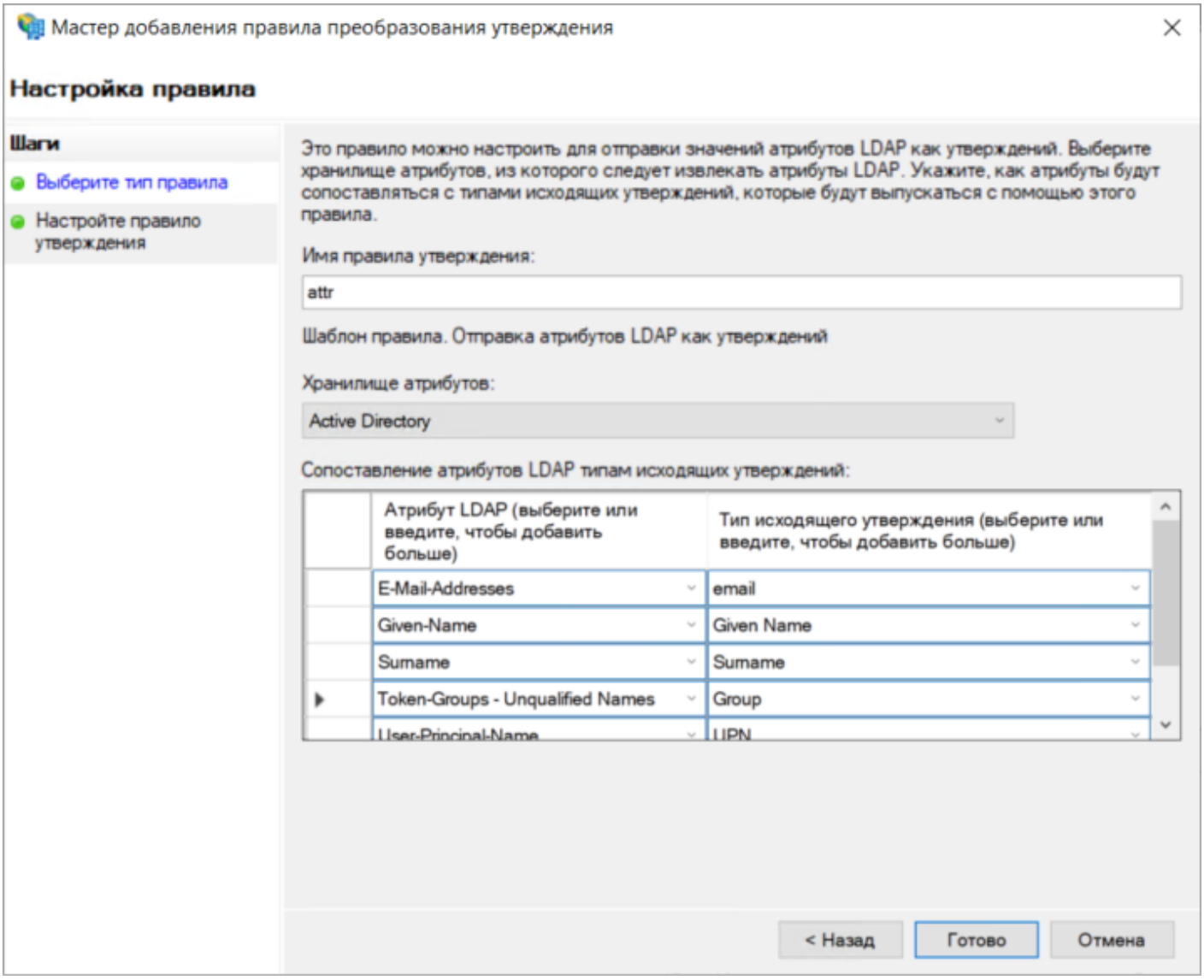
Выберите **Отправка атрибутов LDAP как утверждений (Send LDAP Attributesas Claims)** и нажмите **«Далее».**



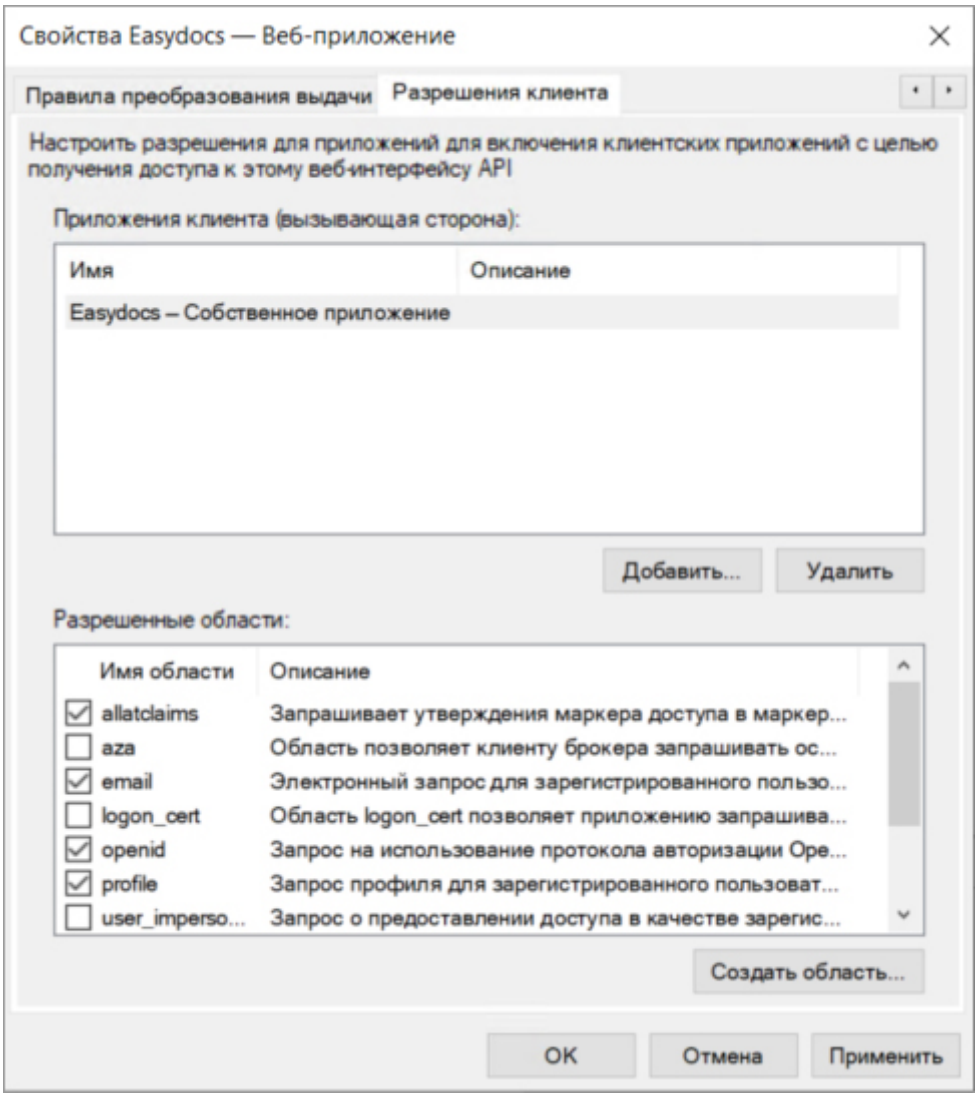
Дайте правилу имя и выберите **Active Directory** в качестве хранилища атрибутов. Если хранилища нет - закройте окно и заново добавьте правило. Затем настройте следующие утверждения и нажмите **Готово**.

Атрибут LDAP	Outgoing Claim Type
E-Mail-Addresses	email
Given-Name	Given Name

Атрибут LDAP	Outgoing Claim Type
Surname	Surname
Token-Groups - Unqualified Names	Group
User-Principal-Name	UPN



Перейдите во вкладку **Разрешения клиента** (Client Permissions) выберите как на скриншоте **Разрешенные области** (Permitted scopes):



Нажмите **Ок**
Настройка Active Directory завершена

Authentik

Authentik может выступать в роли единого способа входа в сервис. В этом случае при попытке входа в личный кабинет EasyDocs пользователь автоматически перенаправляется на страницу Authentik, где проходит аутентификацию.

Для настройки интеграции необходимо предоставить технической поддержке EasyDocs следующие данные:

- Домен адреса электронной почты
- Client ID
- Client Secret
- Auth URL
- Token URL

После настройки все пользователи, личные кабинеты которых зарегистрированы на email с указанным доменом, будут перенаправляться на страницу аутентификации Authentik.