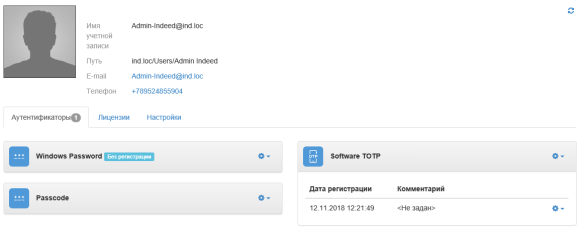
Управление аутентификаторами (SelfService)

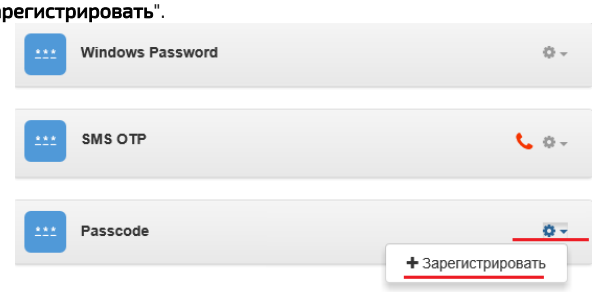
> **Информация**
>
> Для управления аутентификаторами у пользователя должны быть выданы необходимые права доступа. Права по умолчанию позволяют **только зарегистрировать** аутентификатор.

На странице пользователя сосредоточена информация по количеству зарегистрированных аутентификаторов пользователя и их параметры.



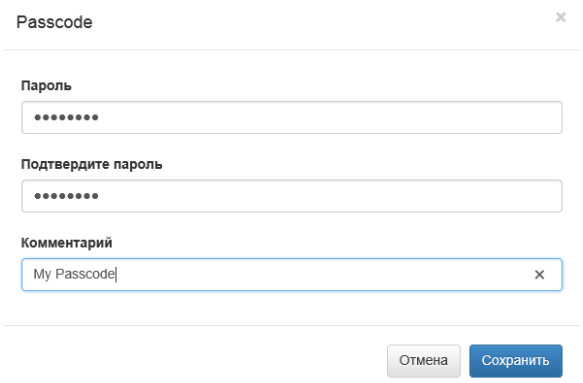
Регистрация аутентификаторов

1. Выберите необходимый аутентификатор.
2. Нажмите на значок шестеренки.
3. Выберите "**Зарегистрировать**".



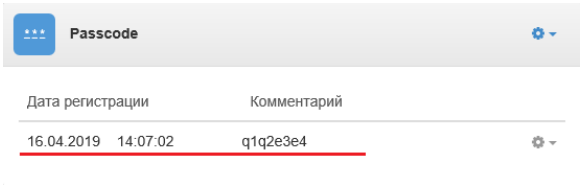
4. Введите данные для обучения выбранного аутентификатора и нажмите "**Сохранить**".

> **Примечание**
>
> Для различных аутентификаторов будут отличаться окна и действия для обучения.

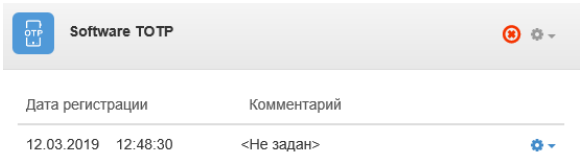


5. После успешной регистрации аутентификатор отобразится как зарегистрированный.

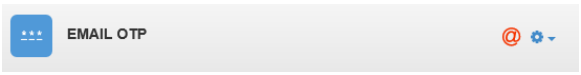
> **Информация**
>
> Если у пользователя зарегистрировано максимальное количество аутентификаторов, то регистрация завершится ошибкой: "**Доступ запрещен: Достигнуто максимальное количество аутентификаторов.**"



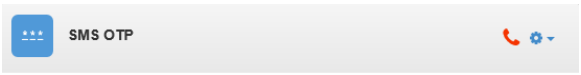
6. Если был удален провайдер, имеющий зарегистрированные аутентификаторы, то в правой части панели аутентификатора будет отображаться значок "**Недоступно**".



7. Провайдеры **Email** и **SMS** регистрируются автоматически, если у пользователя задан **email** или **номер телефона** соответственно.
    a. Если у пользователя после установки **Email** провайдера не был задан email, то аутентификатор не будет использоваться. В правой части панели аутентификатора будет отображаться значок "**@**".

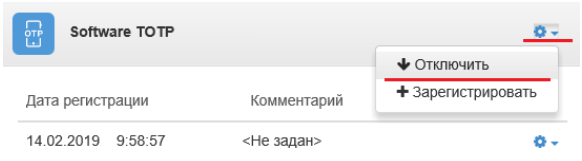


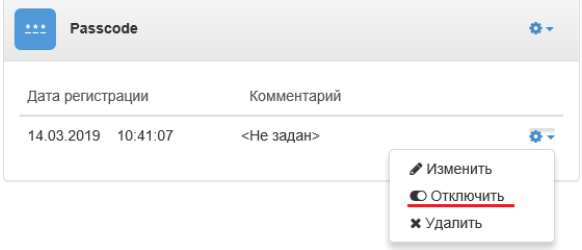
    b. Если у пользователя после установки **SMS** провайдера не был задан номер телефона, то аутентификатор не будет использоваться. В правой части панели аутентификатора будет отображаться значок телефонной трубки.



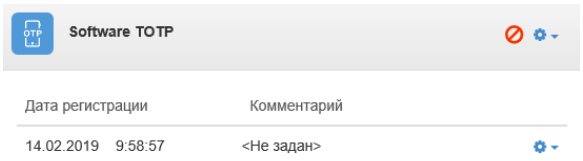
Отключение аутентификатора

1. Выберите необходимый аутентификатор.
2. Нажмите на значок шестеренки.
3. Выберите "Отключить".





4. После отключения аутентификатора пользователь не сможет использовать данный способ входа. Отключенный аутентификатор отмечается значком красного цвета "**Запрещено**".



Автоматическая блокировка и разблокировка аутентификаторов

> **Информация**
>
> Автоматическая блокировка/разблокировка настраивается через групповые политики. Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed-Id. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге: ***Indeed Enterprise Server\<Номер версии>\Misc\Templates***.

Для настройки необходимо открыть политику "**Блокировка способов входа**" (Конфигурация компьютера/Политики/Административные шаблоны/Indeed ID/Server).

Политика применяется к серверам Indeed и позволяет настроить автоматическую блокировку/разблокировку аутентификаторов.

Не задан (Not Configured) или Отключен (Disabled)

Если политика не задана или отключена, то блокировка аутентификаторов не будет осуществляться.

Включен (Enabled)

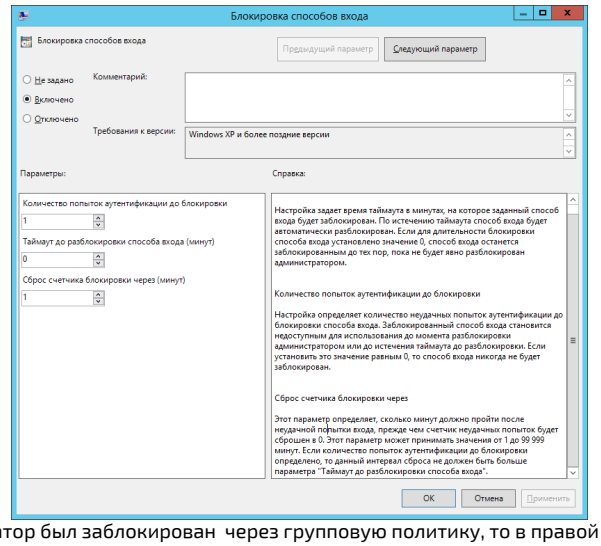
Блокировка/Разблокировка аутентификаторов будет осуществляться согласно заданным в политике параметрам.

Параметры:

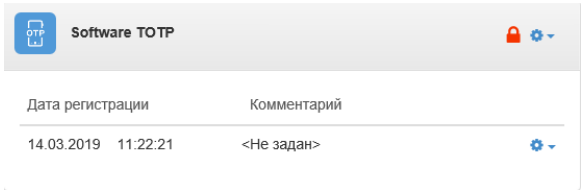
- **Количество попыток аутентификации до блокировки.**
  Настройка определяет количество неудачных попыток аутентификации до блокировки способа входа. Заблокированный способ входа становится недоступным для использования до момента разблокировки администратором или до истечения таймаута до разблокировки. Если установить это значение равным 0, то способ входа никогда не будет заблокирован.

- **Таймаут до разблокировки способа входа.**
  Настройка задает время таймаута в минутах, на которое заданный способ входа будет заблокирован. По истечению таймаута способ входа будет автоматически разблокирован. Если для длительности блокировки способа входа установлено значение 0, способ входа останется заблокированным до тех пор, пока не будет явно разблокирован администратором.

- **Сброс счетчика блокировки через.**
  Этот параметр определяет, сколько минут должно пройти после неудачной попытки входа, прежде чем счетчик неудачных попыток будет сброшен в 0. Этот параметр может принимать значения от 1 до 99 999 минут. Если количество попыток аутентификации до блокировки определено, то данный интервал сброса не должен быть больше параметра "Таймаут до разблокировки способа входа".

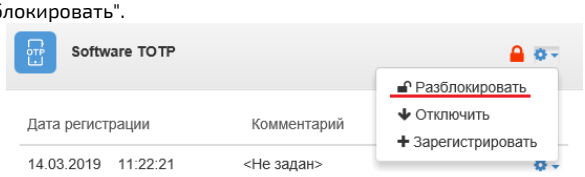


Если аутентификатор был заблокирован через групповую политику, то в правой части панели аутентификатора будет отображаться значок "**Блокировки**".



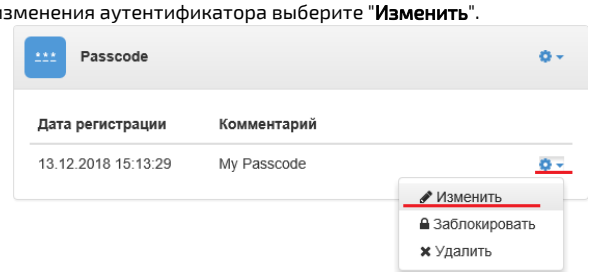
Для разблокировки необходимо:

1. Выбрать необходимый аутентификатор.
2. Нажать на значок шестеренки.
3. Выбрать "Разблокировать".

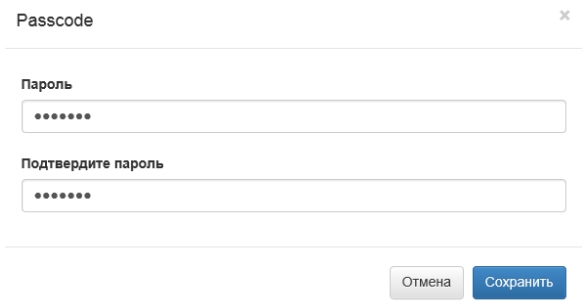


Изменение и удаление аутентификатора

1. Выберите необходимый аутентификатор.
2. Нажмите на значок шестеренки.
    a. **Изменение аутентификатора**.
        - Для изменения аутентификатора выберите "**Изменить**".

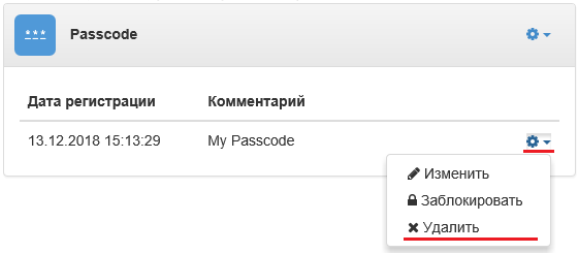


        - Введите новые данные для аутентификатора и нажмите **"Сохранить"**.

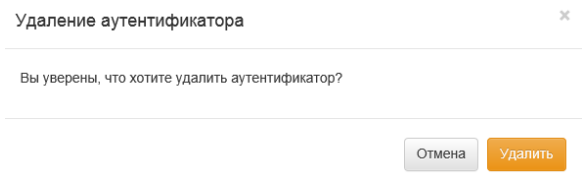


b. Удаление аутентификатора.

- Для удаления аутентификатора выберите "**Удалить**".



- В окне подтверждения нажмите "**Удалить**".

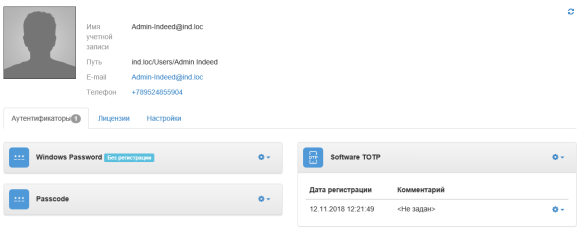


Информация

Для управления аутентификаторами у пользователя должны быть выданы необходимые права доступа.

Для управления аутентификаторами откройте вкладку "**Аутентификаторы**" в карточке пользователя.

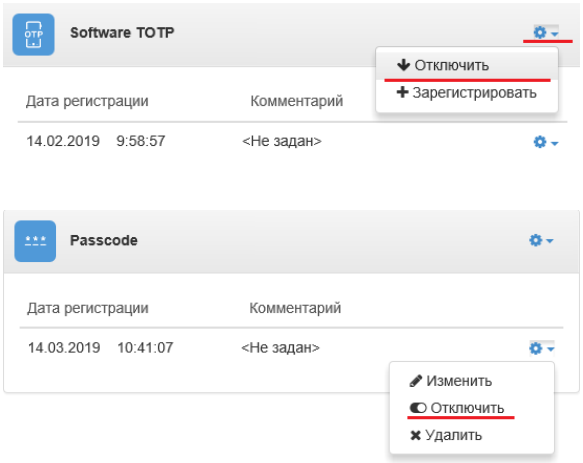
На вкладке сосредоточена информация по количеству зарегистрированных аутентификаторов пользователя и их параметры.



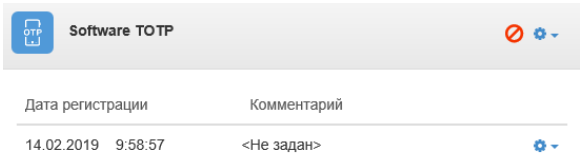
Отключение аутентификатора

1. Выберите необходимый аутентификатор.

2. Нажмите на значок шестеренки.
3. Выберите "Отключить".



4. После отключения аутентификатора пользователь не сможет использовать данный способ входа. Отключенный аутентификатор отмечается значком красного цвета "**Запрещено**".



Автоматическая блокировка и разблокировка аутентификатора

> **Информация**
>
> Автоматическая блокировка/разблокировка настраивается через групповые политики. Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed-Id. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге: ***Indeed Enterprise Server\<Номер версии>\Misc\Templates***.

- Откройте политику "**Блокировка способов входа**": Конфигурация компьютера/Политики /Административные шаблоны/Indeed ID/Server.

  Политика применяется к серверам Indeed и позволяет настроить автоматическую блокировку

  ## аутентификатора

  .

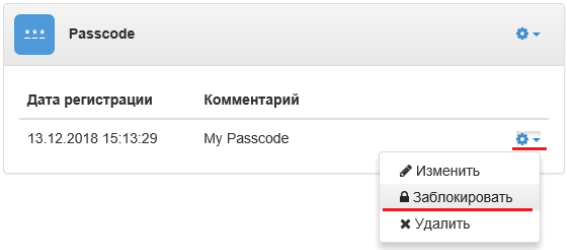
  Не задан (Not Configured) или Отключен (Disabled)

  Если политика не задана или отключена, то пароль будет состоять из цифр и иметь длину 4 символов.

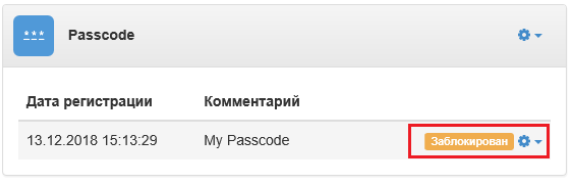
  Включен (Enabled)

  Одноразовый пароль будет генерироваться согласно заданным в политике правилам. Если политика не определена или выключена, то пароль будет состоять из цифр, строчных латинских букв и иметь длину 6 символов.

1. Выберите необходимый аутентификатор.
2. Нажмите на значок шестеренки.
3. Выберите "**Заблокировать**". Для разблокировки выберите "**Разблокировать**".

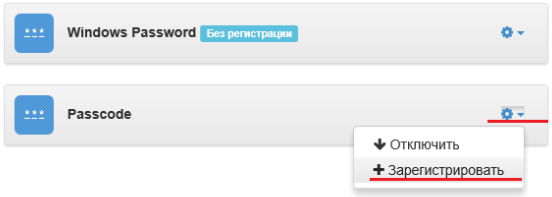


4. После в правой части панели аутентификатора будет отображаться значок "**блокировки**".



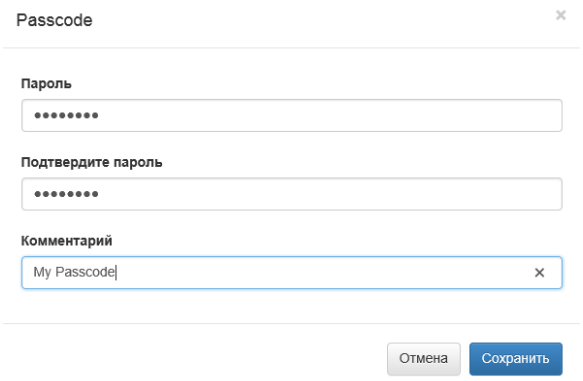
Регистрация аутентификаторов

1. Выберите необходимый аутентификатор.
2. Нажмите на значок шестеренки.
3. Выберите "Зарегистрировать".



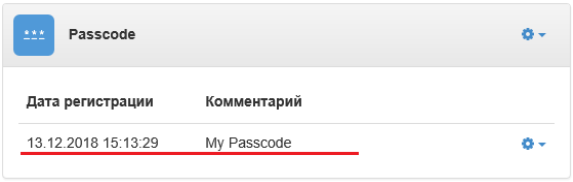
4. Введите данные для обучения выбранного аутентификатора и нажмите "Сохранить".

> **Примечание**
>
> Для различных аутентификаторов будут отличаться окна и действия для обучения.

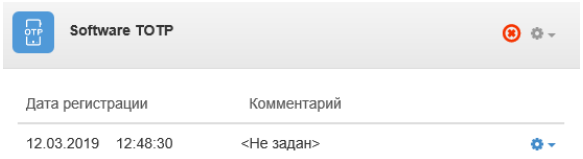


5. После успешной регистрации, аутентификатор отобразится как зарегистрированный.

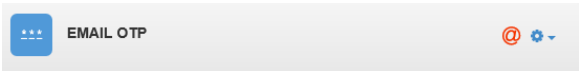
> **Информация**
>
> Если у пользователя зарегистрировано максимальное количество аутентификаторов, то регистрация завершится ошибкой: "**Доступ запрещен: Достигнуто максимальное количество аутентификаторов.**"



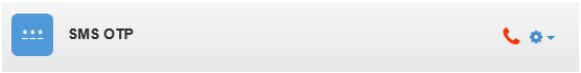
6. Если был удален провайдер, имеющий зарегистрированные аутентификаторы, то в правой части панели аутентификатора будет отображаться значок "**Недоступно**".



7. Провайдеры **Email** и **SMS** регистрируются автоматически, если у пользователя задан **email** или **номер телефона** соответственно.
    a. Если у пользователя после установки **Email** провайдера не был задан email, то ау тентификатор не будет использоваться. В правой части панели аутентификатора будет отображаться значок "**@**".

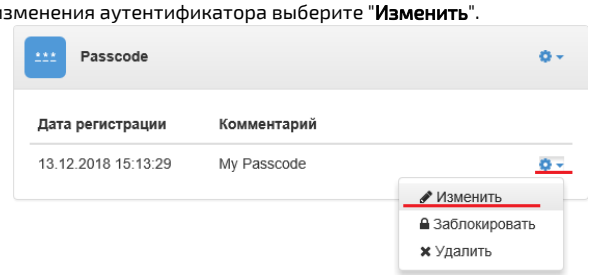


    b. Если у пользователя после установки **SMS** провайдера не был задан номер телефона, то аутентификатор не будет использоваться. В правой части панели ау тентификатора будет отображаться значок телефонной трубки.

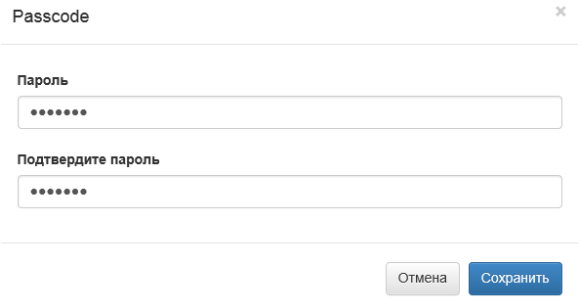


Изменение и удаление аутентификатора

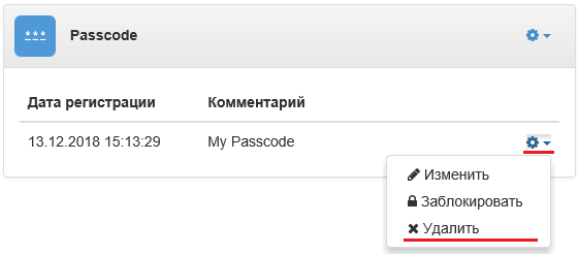
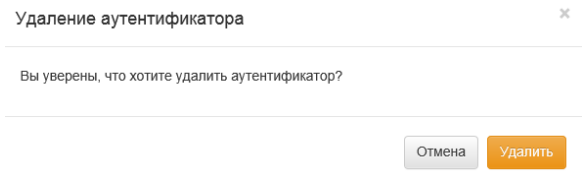
1. Выберите необходимый аутентификатор.
2. Нажмите на значок шестеренки.
    a. **Изменение аутентификатора**.
        - Для изменения аутентификатора выберите "**Изменить**".



        - Введите новые данные для аутентификатора и нажмите **"Сохранить"**.



    b. **Удаление аутентификатора.**
        - Для удаления аутентификатора выберите "**Удалить**".



- В окне подтверждения нажмите "**Удалить**".