

Управление аутентификаторами

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.



Имя
учетной
записи

Admin-Indeed@ind.loc

Путь

ind.loc/Users/Admin Indeed

E-mail

Admin-Indeed@ind.loc

Телефон

[+789524855904](tel:+789524855904)

Аутентификаторы 1

[Лицензии](#)

[Настройки](#)

Windows Password

Без регистрации

⚙

Passcode

⚙

ОТР

Software TOTP

⚙

Дата регистрации	Комментарий
12.11.2018 12:21:49	<Не задан>

⚙

Отключение аутентификатора

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

 **Software TOTP** 

↓ Отключить

+ Зарегистрировать

Дата регистрации		Комментарий	
14.02.2019	9:58:57	<Не задан>	

 **Passcode** 

Дата регистрации		Комментарий	
14.03.2019	10:41:07	<Не задан>	

 Изменить

 Отключить

 Удалить

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

 **Software TOTP**  

Дата регистрации		Комментарий	
14.02.2019	9:58:57	<Не задан>	

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 AM. Файлы шаблонов политик входят в состав дистрибутива провайдера и расположены в каталоге: *Indeed Enterprise Server\<Homep 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 таймута до разблокировки. Если установить это значение равным 0, то способ входа никогда не будет заблокирован.

- **Таймаут до разблокировки способа входа.**

Настройка задает время таймута в минутах, на которое заданный способ входа будет заблокирован. По истечению таймута 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".

Блокировка способов входа

☐ Не задано
 ☒ Включено
 ☐ Отключено

Комментарий:

Требования к версии: Windows XP и более поздние версии

Параметры:

 Количество попыток аутентификации до блокировки: 1

 Таймаут до разблокировки способа входа (минут): 0

 Сброс счетчика блокировки через (минут): 1

Справка:

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.

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.

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".

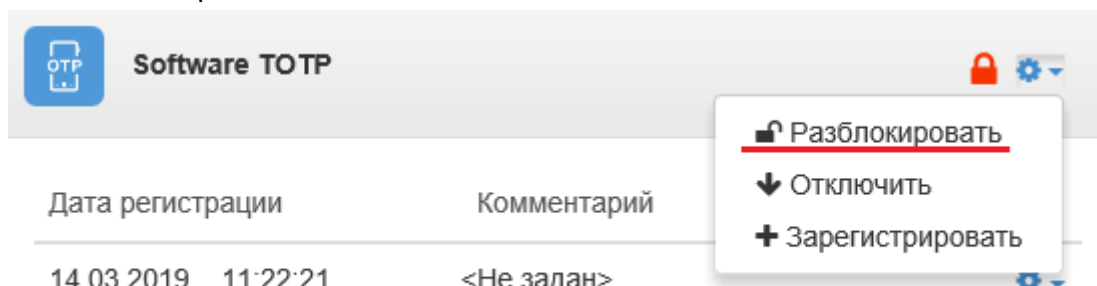
OK
 Отмена
 Применить

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

Software TOTP		
ОТР Software TOTP		
Дата регистрации		Комментарий
14.03.2019	11:22:21	<Не задан>

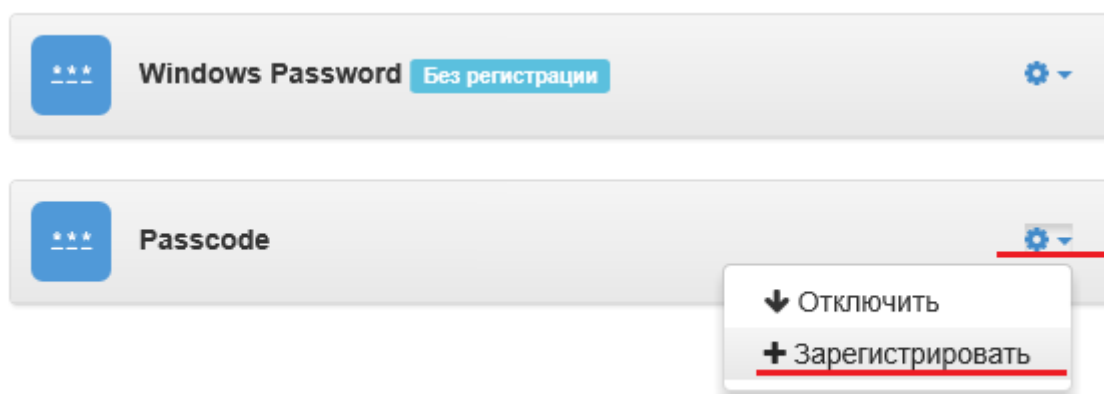
Для разблокировки необходимо:

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



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.

Passcode



Пароль

••••••••

Подтвердите пароль

••••••••

Комментарий

My Passcode|



Отмена

Сохранить

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."**

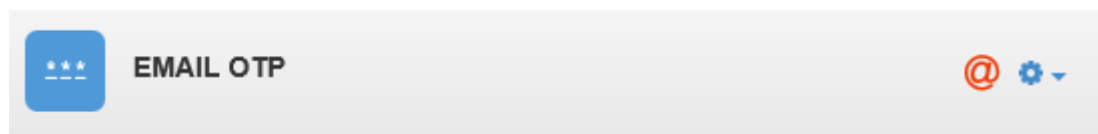
Passcode		
Дата регистрации	Комментарий	
13.12.2018 15:13:29	My Passcode	

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

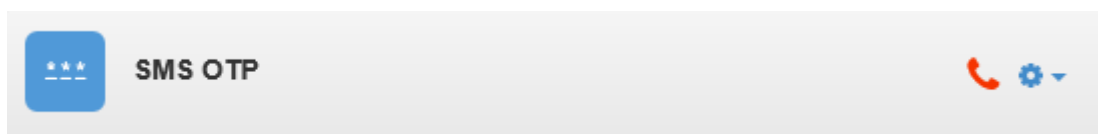
Software TOTP		
Дата регистрации	Комментарий	
12.03.2019 12:48:30	<Не задан>	 

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.



Изменение и удаление аутентификатора

1. Выберите необходимый аутентификатор.
2. Нажмите на значок шестеренки.

а. Изменение аутентификатора.

- Для изменения аутентификатора выберите "Изменить".

*** Passcode

Дата регистрации	Комментарий
13.12.2018 15:13:29	My Passcode

Изменить

Заблокировать

Удалить

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

Passcode

Пароль

.....

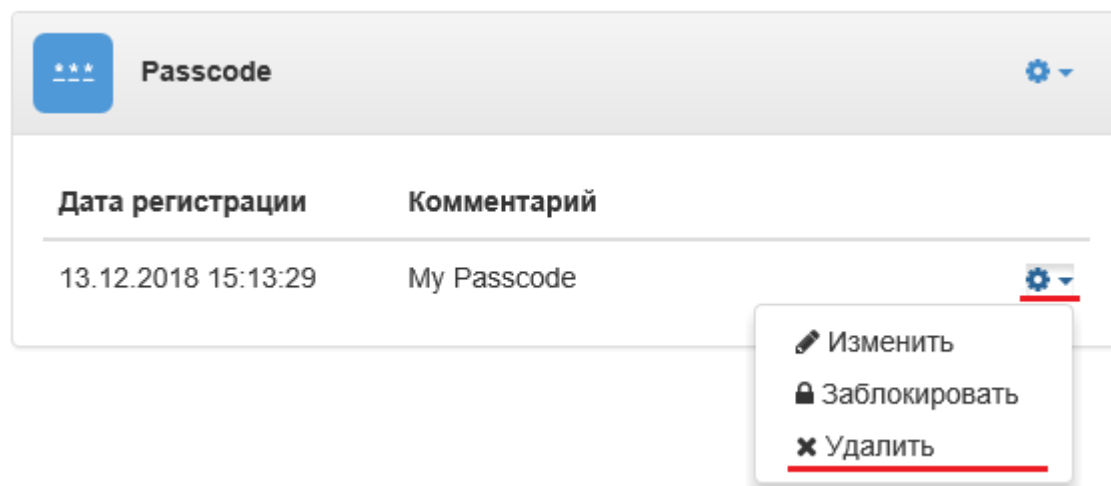
Подтвердите пароль

.....

Отмена Сохранить

в. Удаление аутентификатора.

- Для удаления аутентификатора выберите "Удалить".



- В окне подтверждения нажмите "Удалить".

