# 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				2
	Путь	ind.loc/Users/Admin Indeed				
	E-mail	Admin-Indeed@ind.loc				
	Телефон	+789524855904				
Аутентификаторы	Лицензи	и Настройки				
Windows Pas	SWORD Des per	истрации	0 -	Software TOTP		0
Passcode			0 -	Дата регистрации	Комментарий	
				12.11.2010 12.21.45	≺пс задаñ∕	**

#### Отключение аутентификатора

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

Software TOTP		0 -
-		Отключить
Дата регистрации	Комментарий	+ Зарегистрировать
14.02.2019 9:58:57	<Не задан>	0 <del>-</del>

Passcode		0.
Дата регистрации	Комментарий	
14.03.2019 10:41:07	<Не задан>	0 -
		Изменить
		× Удалить

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 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 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".

8	Блокировка сг	юсобов входа		_ <b>□</b> X	
📆 Блокировка способов входа	Пре	цыдущий параметр	<u>С</u> ледующий параметр		
<ul> <li><u>Н</u>е задано</li> <li><u>В</u>ключено</li> <li><u>О</u>тключено</li> <li>Требования к версии:</li> </ul>	Windows XP и более поздние	версии		~	
Параметры:	Справк	a:		~	
Параметры: Количество попыток аутентификации до блокировки 1		ойка задает время тайл будет заблокирован. П атически разблокиров а входа установлено з сированным до тех пор истратором. ество попыток аутенти ровки способа входа. З упным для использов истратором или до ис вить это значение рав сирован. счетчика блокировки араметр определяет, с ной порытки входа, п ее в 0. Этот параметр Если количество поп елено, то данный инте етра "Таймаут до разб	иаута в минутах, на которо lo истечению таймаута спо ан. Если для длительности значение 0, способ входа о p, пока не будет явно разбл ификации до блокировки чество неудачных попыток Заблокированный способ ания до момента разблоки течения таймаута до разбл ным 0, то способ входа ни через колько минут должно про режде чем счетчик неудач может принимать значени ыток аутентификации до б рвал сброса не должен бы локировки способа входа"	е заданный способ особ входа будет в блокировки останется покирован с аутентификации до входа становится ировки юкировки. Если когда не будет и после ных попыток будет ия от 1 до 99 999 олокировки ть больше	
			ОК От	мена Применить	·]

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

	Software TOTP		≜ ≎-
Дата	регистрации	Комментарий	
14.03	3.2019 11:22:21	<Не задан>	0 -

Для разблокировки необходимо:

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

Software TOTP		🔒 💇
_		Разблокировать
Дата регистрации	Комментарий	<ul> <li>Отключить</li> <li>Зарегистрировать</li> </ul>
14.03.2019 11:22:21	<Не задан>	sapanaiphpobalb

## Регистрация аутентификаторов

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

Windows Password Без регистрации	0 -
Passcode	0-
	• Отключить
	+ Зарегистрировать

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

# 🛆 Примечание

Для различных аутентификаторов будут отличаться окна и действия для обучения.

# Passcode

~		
$\sim$		
20		
-		

×

#### 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		0 -
Дата регистрации	Комментарий	
13.12.2018 15:13:29	My Passcode	0 -

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

Software TOTP		8 0 -
Дата регистрации	Комментарий	
12.03.2019 12:48:30	<Не задан>	0 -

7. Провайдеры **Email** и **SMS** регистрируются автоматически, если у пользователя задан **email** или **номер телефона** соответственно.

**а.** 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		0
Дата регистрации	Комментарий	
13.12.2018 15:13:29	My Passcode	0-
		Изменить
		Заблокировать
		🗙 Удалить

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

Passcode	
Пароль	
•••••	
Подтвердите пароль	
•••••	

# b. Удаление аутентификатора.

• Для удаления аутентификатора выберите "Удалить".

Passcode		0
Дата регистрации	Комментарий	
13.12.2018 15:13:29	My Passcode	0
		Изменить
		Заблокировать
		🗙 Удалить

• В окне подтверждения нажмите "Удалить".

Vлапецие	аутентификатора
удаление	аутентификатора

Вы уверены, что хотите удалить аутентификатор?



×