Indeed-Id
Google Authenticator Provider

Руководство по установке и эксплуатации

8 (800) 333-09-06
телефон бесплатной горячей линии

ООО Индид
ИНН/КПП 7801540219/780601001, ОГРН 1117847053103

8 (800) 333-09-06 или support@indeed-id.com
служба поддержки пользователей

http://indeed-id.ru/
web-сайт компании

Версия 1.0.2

Оглавление

Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed. Данное руководство, предназначенное для администраторов и пользователей продуктов Indeed-Id, поможет ознакомиться с принципом работы компонента **Indeed-Id Google Authenticator Provider**, параметрами его установки и настройки.

Условные обозначения

В Руководстве используются следующие условные обозначения:

Важная информация. Разделы, содержащие важную информацию, необходимую для успешной работы.

Дополнительная информация. Разделы, содержащие дополнительную информацию.

О компоненте Indeed-Id Google Authenticator Provider

Google Authenticator – это двухфакторная аутентификация, основанная на программном обеспечении, разработанном компанией Google. Аутентификатор представляет собой шестизначный одноразовый пароль, который пользователь должен предоставить в дополнение к своему логину и паролю, чтобы получить доступ к приложению.

Одноразовый пароль генерируется автономно на мобильном устройстве (телефон, смартфон, планшет) с использованием специализированного приложения. Генерация одноразового пароля производится на основе двух параметров: секретного ключа, задаваемого на этапе регистрации аутентификатора и текущего времени.

Технология аутентификации основана на системе, где для заданного секретного ключа пользователя в каждый момент времени существует единственный верный одноразовый пароль. Таким образом, имея информацию о секретном ключе, сервер может проверить переданный пользователем одноразовый пароль. Для правильного функционирования технологии время на мобильном устройстве и сервере аутентификации должно совпадать (при этом допускается погрешность, величина которой может регулироваться администратором).

Технология доступа Google Authenticator проста, удобна и может быть успешно освоена любым пользователем. Преимуществом Google Authenticator является экономичность: не требуются приобретение и установка дополнительного оборудования, бесплатное приложение для генерирования паролей существует на всех популярных платформах.

Google Authenticator может быть дополнен PIN-кодом (**Indeed-Id Google Authenticator with PIN Provider**). В этом случае для аутентификации пользователю необходимо будет помимо одноразового пароля ввести известный ему PIN-код. Получить доступ по одному лишь одноразовому паролю или PIN-коду невозможно.

Работа с Indeed-Id Google Authenticator Provider

Регистрация аутентификатора

Аутентификатор – набор данных, создаваемый для каждого пользователя системы Indeed-Id, необходимый для прохождения процедуры аутентификации. Каждый новый пользователь системы Indeed-Id должен пройти процедуру регистрации одного (или нескольких) аутентификаторов.

Регистрация аутентификатора осуществляется после установки на рабочую станцию пользователя необходимых компонентов системы Indeed-Id: Indeed-Id Windows Logon/Indeed-Id ESSO Agent (в зависимости от используемой конфигурации системы) и провайдера Indeed-Id Google Authenticator Provider.

Пользователь выполняет вход в систему по доменному паролю и, следуя указаниям приложения **Indeed-Id Управление аутентификаторами**, регистрирует аутентификатор.

Для успешной регистрации аутентификатора необходимо, чтобы пользователю, от имени которого осуществляется регистрация, было разрешено использовать технологию аутентификации Indeed-Id. Соответствующая настройка **выполняется администратором системы в свойствах пользователя на вкладке Настройки в консоли управления Indeed EMC.**

Подробные сведения по настройке свойств пользователя содержатся в документе *Indeed Enterprise Management Console. Руководство по установке и администрированию.pdf*.

Если аутентификатор не был зарегистрирован при первом входе пользователя в систему, регистрацию можно выполнить в любой удобный момент, запустив приложение **Indeed-Id Управление аутентификаторами** из меню Пуск – Все программы – Indeed-Id.

Для регистрации аутентификатора необходимо установить на мобильное устройство приложение Google Authenticator[1], связать устройство с вашей доменной учетной записью и сгенерировать одноразовый пароль. Для генерации пароля необходимо провести сканирование[2] QR-кода, отображаемого в мастере регистрации первого аутентификатора Indeed-Id.

Для регистрации аутентификатора необходимо войти в систему по доменному паролю и выполнить следующие действия:

В окне **Управление ауентификаторами** нажмите **Продолжить** (Рисунок 1a).

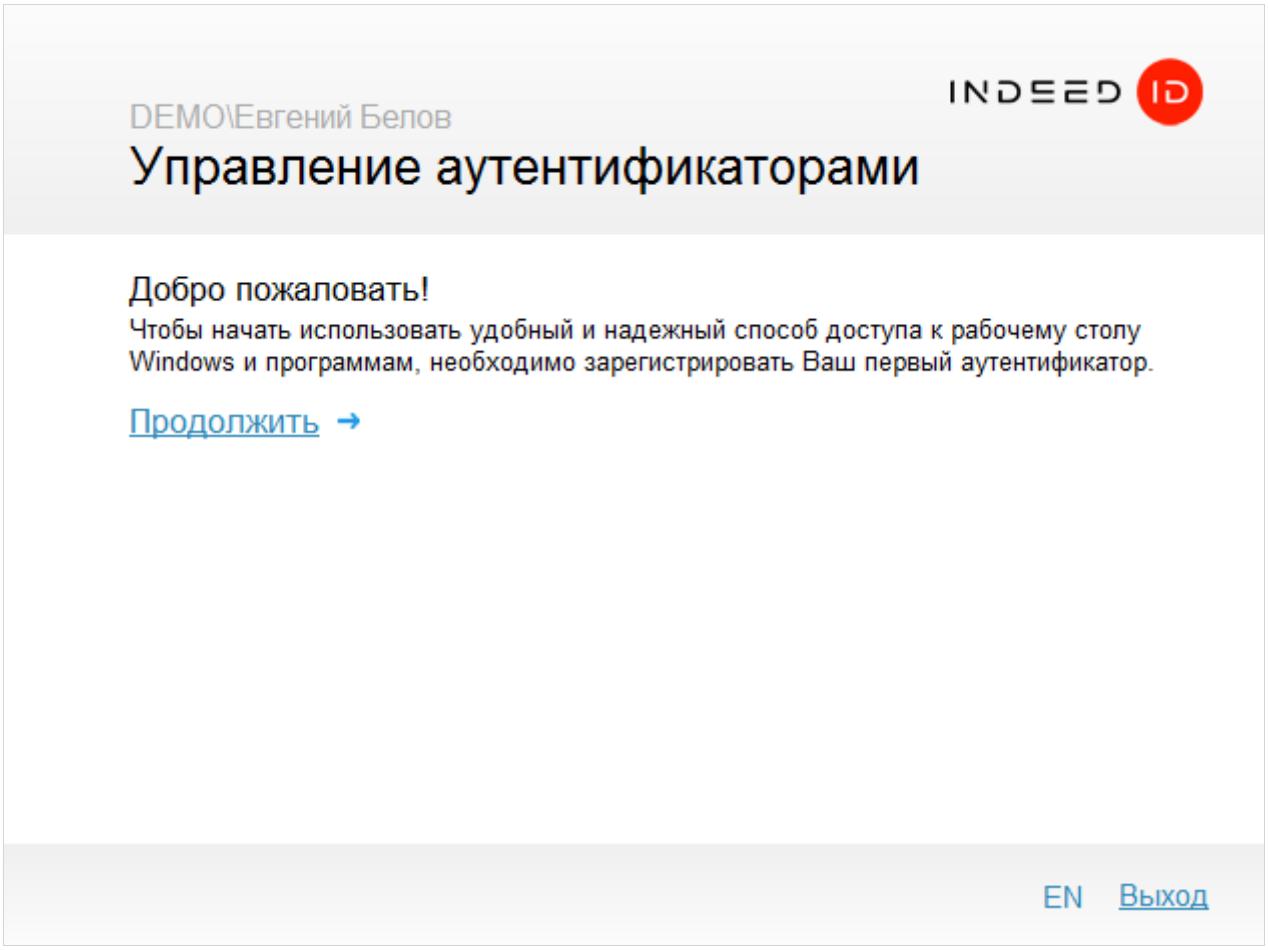

Рисунок 1a.

Если на рабочей станции пользователя установлено несколько провайдеров аутентификации, то необходимо выбрать **Одноразовый пароль (Google Authenticator)** из списка (Рисунок 1b).

В случае использования провайдера Indeed-Id Google Authenticator with PIN Provider выберите **Одноразовый пароль (Google Authenticator + PIN)**. Если на компьютере установлен только один провайдер, окно выбора не отображается.

[1] Доступно для iOS, Android и BlackBerry

[2] Может потребоваться стороннее приложение для распознавания QR-кода.

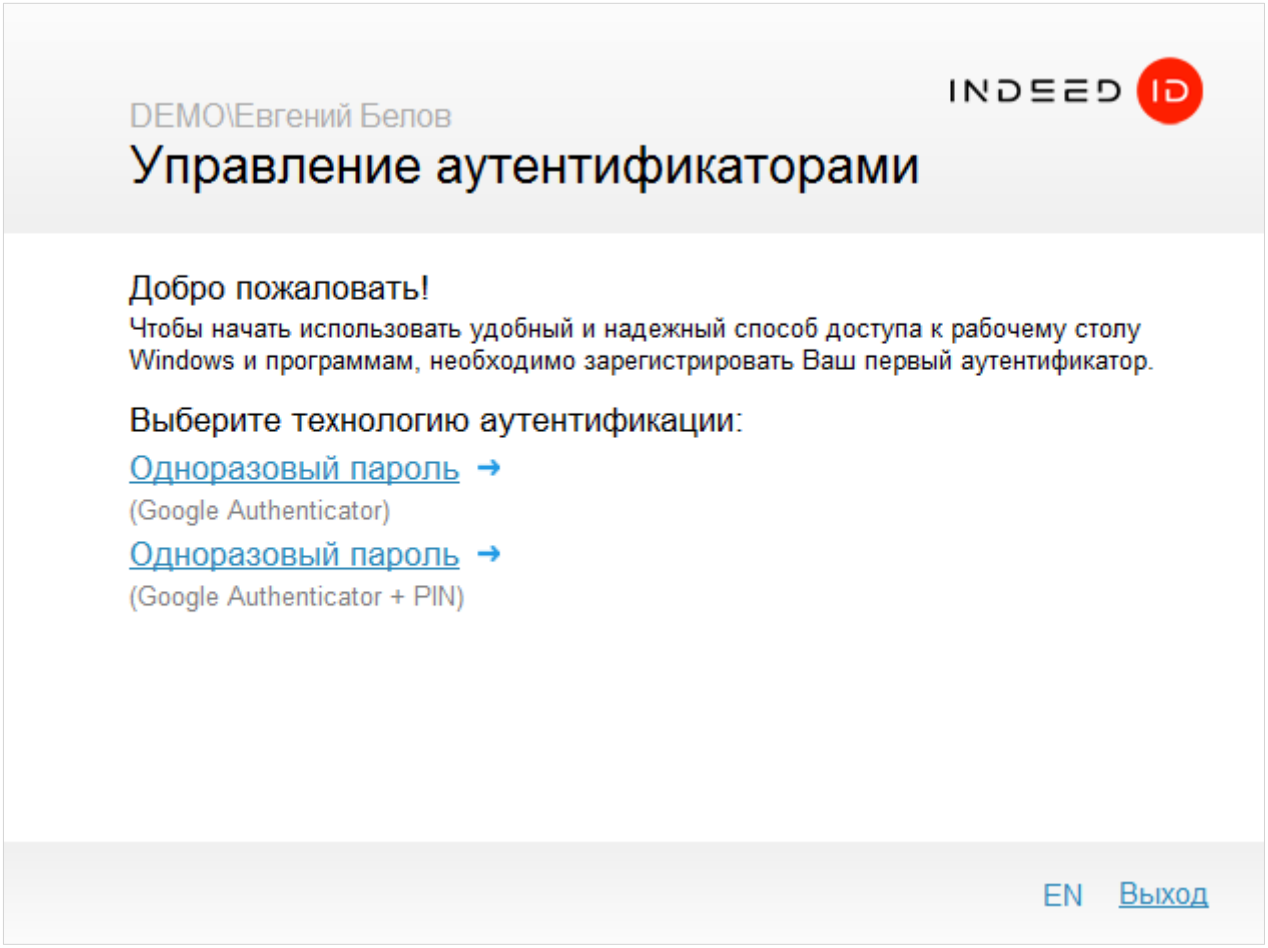

Рисунок 1b.

Выберите **Сканировать штрих-код** в приложении Google Authenticator на вашем устройстве и направьте камеру на QR-код, отображенный на мониторе компьютера (Рисунок 1c). После сканирования в приложении появится одноразовый пароль для вашей учетной записи. Нажмите кнопку **Обучить.**

В случае использования провайдера **Indeed-Id Google Authenticator with PIN Provider** потребуется не только отсканировать QR-код, но и задать PIN-код. Минимальное количество символов PIN-кода – 4. Использовать можно кириллические и латинские символы, знаки и цифры. (Рисунок 1d). Данный PIN-код необходимо будет вводить каждый раз при прохождении аутентификации в дополнение к одноразовому паролю. Задайте PIN-код и нажмите кнопку **Ok**.

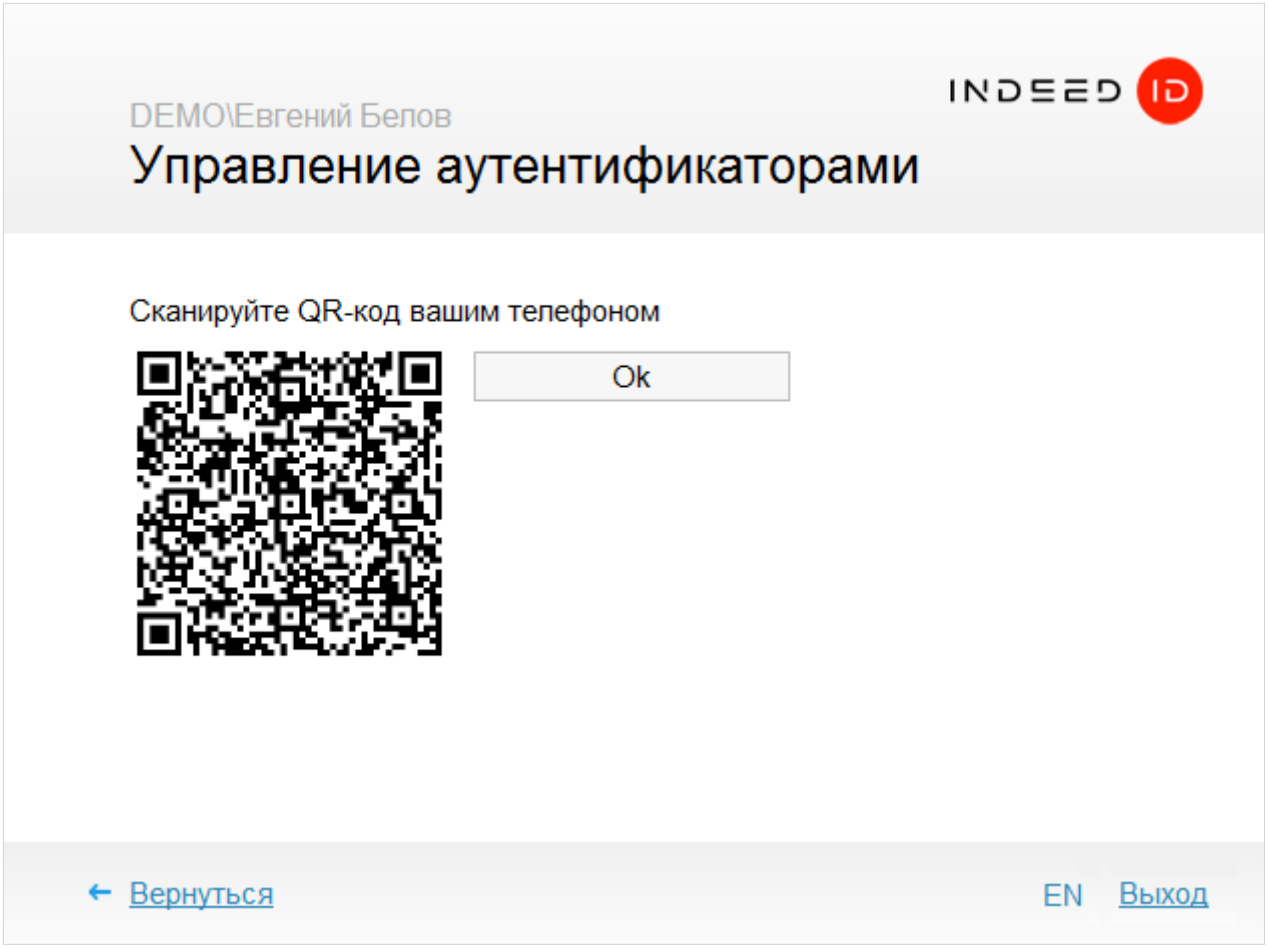

Рисунок 1c.

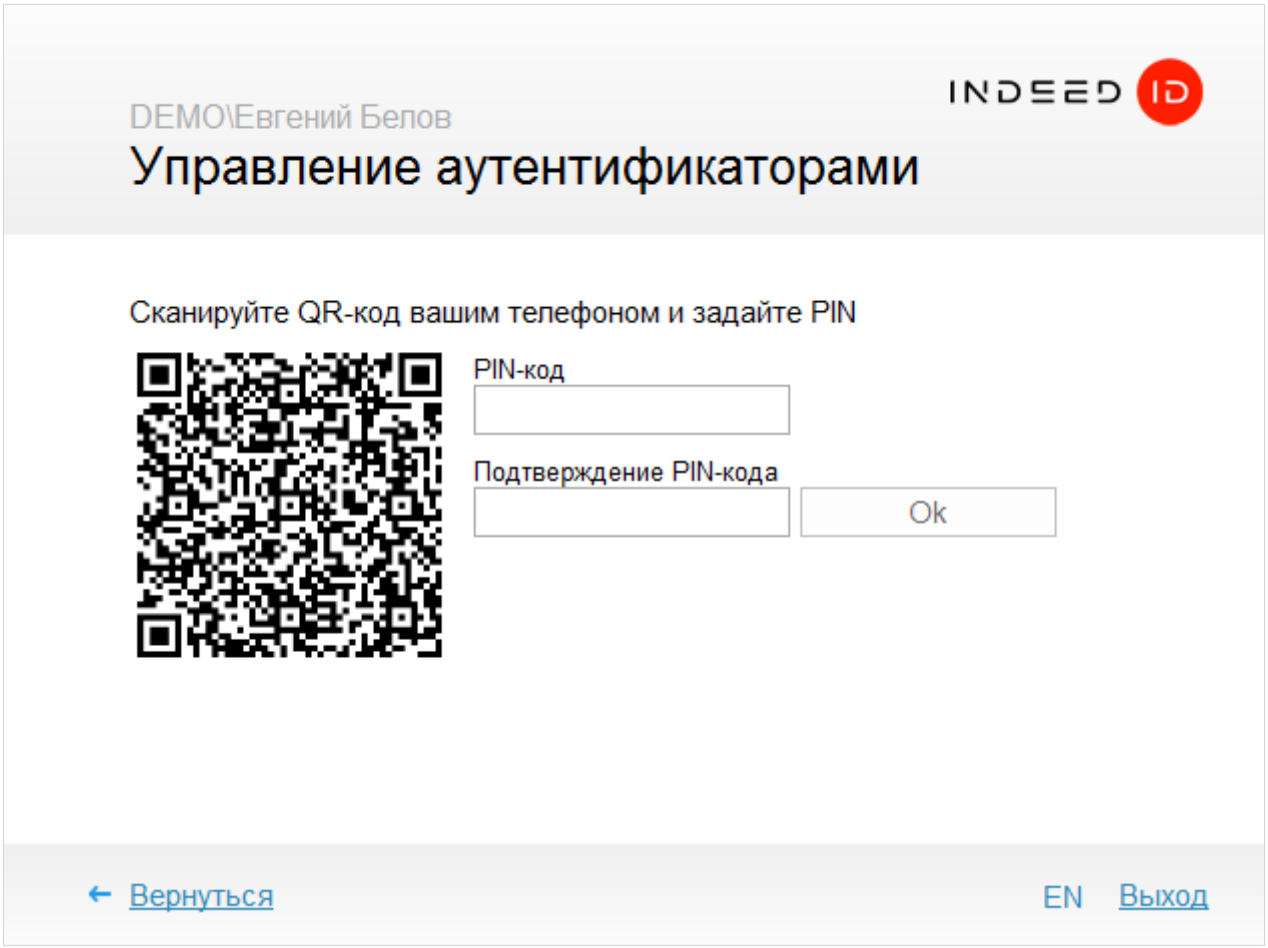

Рисунок 1d.

При необходимости введите комментарий к заданному способу входа и нажмите кнопку **Сохранить** (Рисунок 1e).

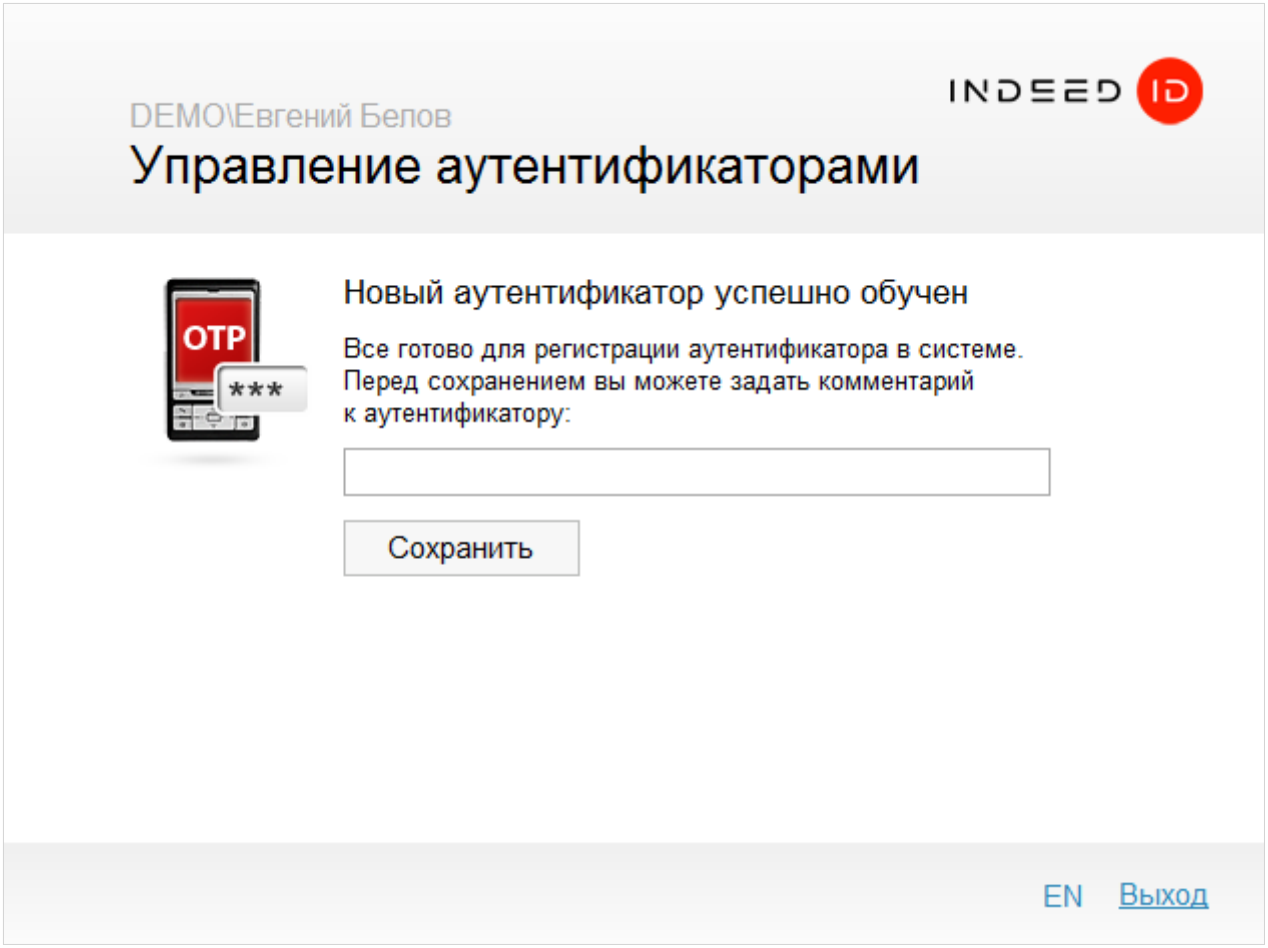

Рисунок 1e.

После нажатия на кнопку **Сохранить** аутентификатор будет сохранен в системе и его можно будет использовать для аутентификации. Нажмите **Выход** для завершения работы приложения **Indeed-Id Управление аутентификаторами**.

Аутентификация при помощи Google Authenticator Provider

При первом входе в систему или приложение с использованием технологии аутентификации Indeed-Id необходимо выбрать способ входа. Для этого нажмите **Сменить способ входа** (Рисунок 2) окне **Вход в Windows** (окно **Аутентификация** для Enterprise SSO). Выберите способ входа **Одноразовый пароль (Google Authenticator)** или **Одноразовый пароль (Google Authenticator + PIN)**.

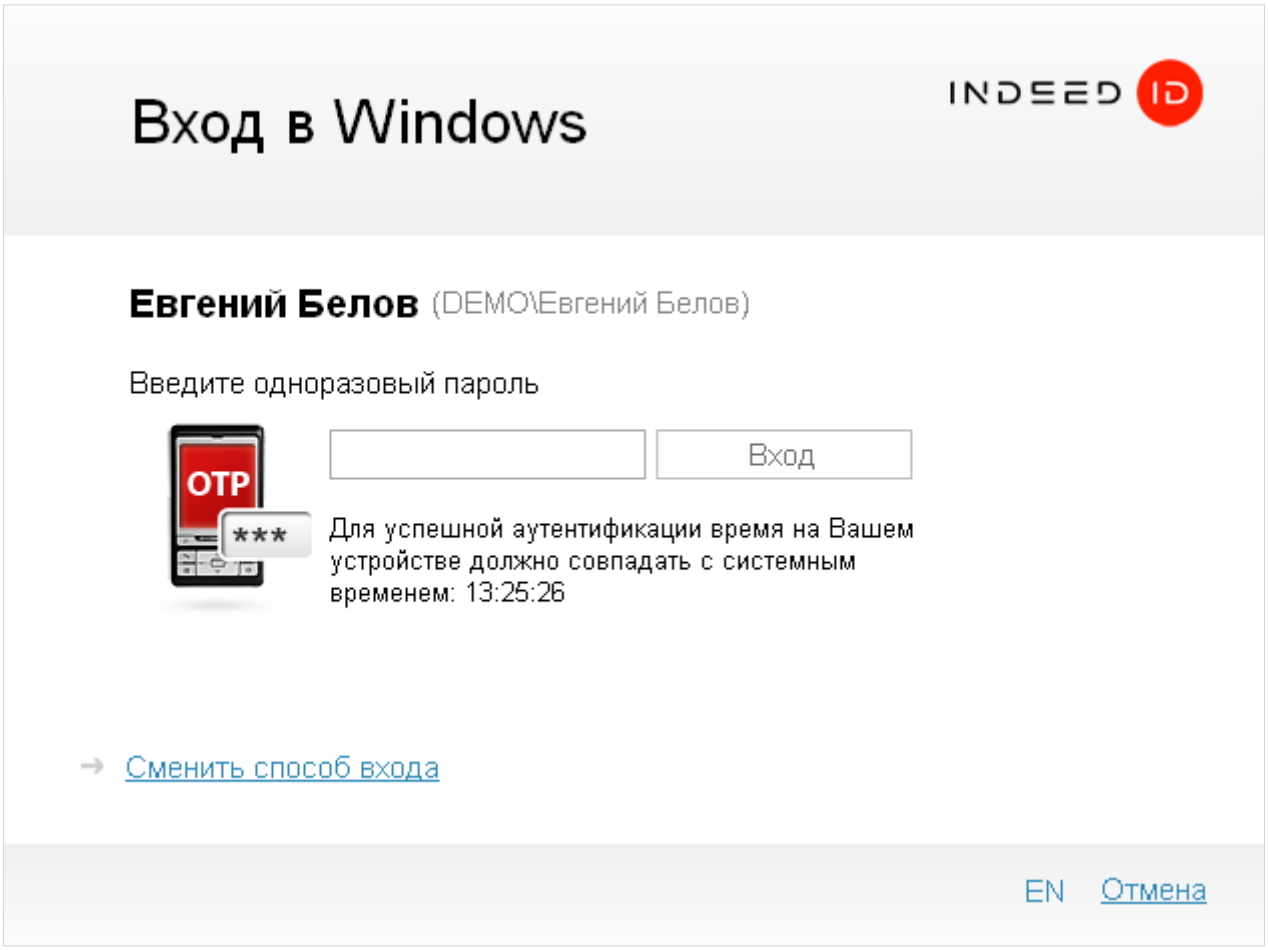

Рисунок 2.

Убедитесь, что время на мобильном устройстве синхронизировано со временем на вашем ПК (текущее время отображается ниже поля ввода одноразового пароля).

Введите одноразовый пароль, отображаемый в приложении Google Authenticator на вашем мобильном устройстве и нажмите кнопку **Вход** в окне аутентификации Indeed-Id.

Если используется провайдер **Indeed-Id Google Authenticator Provider with PIN**, то кроме одноразового пароля следует ввести PIN-код и затем нажать **Вход**.

В случае успешного входа по аутентификатору, способ входа **Одноразовый пароль (Google Authenticator)** или **Одноразовый пароль (Google Authenticator + PIN)** запоминается как предпочтительный и будет автоматически предложен пользователю при следующем входе в систему или приложение.

Управление аутентификаторами

Управление аутентификаторами пользователя осуществляется при помощи приложения **Indeed-Id Управление аутентификаторами**. Приложение позволяет пользователю выполнять следующие действия с аутентификаторами:

- обучать
- переобучать
- удалять
- редактировать комментарий

Перечень действий, которые пользователь может выполнять над аутентификаторами, **задается администратором системы в свойствах пользователя на вкладке Аутентификаторы консоли управления Indeed EMC**.

Подробные сведения по настройке свойств пользователя содержатся в документе *Indeed Enterprise Management Console. Руководство по установке и администрированию.pdf*.

Запустите приложение **Indeed-Id Управление аутентификаторами** из меню Пуск – Все программы – Indeed-Id.

Для работы с приложением Indeed-Id Управление аутентификаторами необходимо выполнить вход в приложение с использованием любого из зарегистрированных аутентификаторов Indeed-Id или по доменному паролю. Если зарегистрированных аутентификаторов нет, то после аутентификации по доменному паролю пользователю будет предложено зарегистрировать аутентификатор.

В случае аутентификации по доменному паролю при наличии как минимум одного зарегистрированного аутентификатора Indeed-Id, независимо от настроек, выставленных в свойствах пользователя администратором системы, пользователю будет доступен только просмотр списка зарегистрированных аутентификаторов и проверка каждого из них.

Только пользователи, прошедшие аутентификацию по одному из обученных аутентификаторов Indeed-Id, имеют возможность управлять своими аутентификаторами (в соответствии с настройками, заданными администратором системы для пользователя).

Подробнее об управлении аутентификаторами смотрите в документах *Indeed-Id Enterprise SSO. Руководство пользователя.pdf* и *Indeed-Id Windows Logon. Руководство по установке и использованию.pdf*.

Установка и настройка Indeed-Id Google Authenticator Provider

Установка компонента

В этом разделе содержатся сведения по установке и настройке Indeed-Id Google Authenticator Provider.

Установку Indeed-Id Google Authenticator Provider необходимо выполнить на всех серверах Indeed-Id и затем на рабочих станциях пользователей. Для установки компонента потребуется минимум 10Мб свободного места на жестком диске компьютера.

Для установки Indeed-Id Google Authenticator Provider, пользователь, от имени которого выполняется установка, должен обладать правами администратора (быть членом локальной группы «Администраторы»).

Для развертывания Indeed-Id Google Authenticator Provider на рабочих станциях пользователей в автоматическом режиме удобно использовать механизм групповых политик (Microsoft Group Policy). Или любой другой инструмент, позволяющий массово распространять и устанавливать msi-пакеты на рабочие станции пользователей (например, Microsoft System Center Configuration Manager).

Подробнее со способами распространения компонентов системы Indeed-Id в автоматическом режиме можно ознакомиться в документе *Indeed-Id. Руководство по развертыванию системы.pdf.*

Установка Indeed-Id Google Authenticator Provider

1. Запустите файл IndeedID.GoogleAuthenticator.Provider.msi (или IndeedID.GoogleAuthenticator.PIN.Provider.msi если необходимо установить версию провайдера с PIN-кодом) из дистрибутива провайдера и выполните установку, следуя указаниям мастера.
2. После завершения установки может потребоваться перезагрузка системы. Если программа установки предлагает выполнить перезагрузку, подтвердите данное действие.
3. Удаление/Восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.

Настройка параметров аутентификации

В этом разделе содержится описание настраиваемых параметров работы Indeed-Id Google Authenticator Provider и способах их изменения. Изменение параметров работы Indeed-Id Google Authenticator Provider осуществляется через механизм групповых политик Active Directory.

Настройка политик необходима для повышения уровня безопасности. Однако полноценная работа Indeed-Id Google Authenticator Provider возможна и со значениями политик, определенными по умолчанию.

Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed-Id. Административный файл шаблона политики IndeedID.GoogleAuthenticator.BSP.adm входит в состав дистрибутива и расположен в каталоге Misc.

Для получения подробной информации обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf.*

Политика **Время действия одноразового пароля** определяет, каким должен быть минимальный период действия одноразового пароля при обучении. Период задается целым числом от 3 до 18, где 3 соответствует временному промежутку в 30 секунд (+/- 15 секунд). Политика должна быть определена на клиентах системы, где происходит обучение аутентификаторов, то есть на рабочих станциях пользователей. Если политика не определена, по умолчанию используется значение 6.

Политика **Минимальная длина PIN-кода** позволяет задать минимальное количество символов, из которых должен состоять PIN-код. Допустимый диапазон от 4 до 25 символов.

Для того чтобы изменения в настройках политик вступили в силу, необходимо выполнить обновление групповой политики. Для немедленного обновления групповой политики используйте команду **gpupdate /force**.