Indeed-Id
OMNIKEY Provider

Руководство по установке и эксплуатации

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

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

ООО Индид
ИНН/КПП 7801540219/780601001, ОГРН 1117847053103

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 OMNIKEY Provider** и 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 OMNIKEY Provider

Indeed-Id OMNIKEY Provider предназначен для совместного использования с продуктами Indeed-Id Windows Logon и Indeed-Id Enterprise SSO. Компонент обеспечивает работу считывателей смарт-карт HID OMNIKEY с модулями программного комплекса Indeed-Id Access Management. Подробную информацию о считывателях и картах OMNIKEY Вы можете получить на сайте компании-производителя.

На данный момент поддерживается следующие модели сканеров HID OMNIKEY:

- OMNIKEY 5325
- OMNIKEY 6321
- OMNIKEY 5321 CLi
- OMNIKEY 6321 CLi
- OMNIKEY 5427 CK
- OMNIKEY 5421

Возможны варианты использования одного и того же устройства аутентификации как с запросом PIN-кода, так и без него. В случае использования **Indeed-Id OMNIKEY Provider** для аутентификации пользователю необходимо лишь приложить карту к считывателю, PIN-код запрашиваться не будет.

В случае использования **Indeed-Id OMNIKEY Provider with PIN** запрос PIN-кода будет происходить всякий раз, когда пользователь приложит карту к считывателю. PIN-код задается пользователем на этапе регистрации аутентификатора.

Работа с Indeed-Id OMNIKEY 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 OMNIKEY 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 войти в систему по доменному паролю и выполнить следующие действия:

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

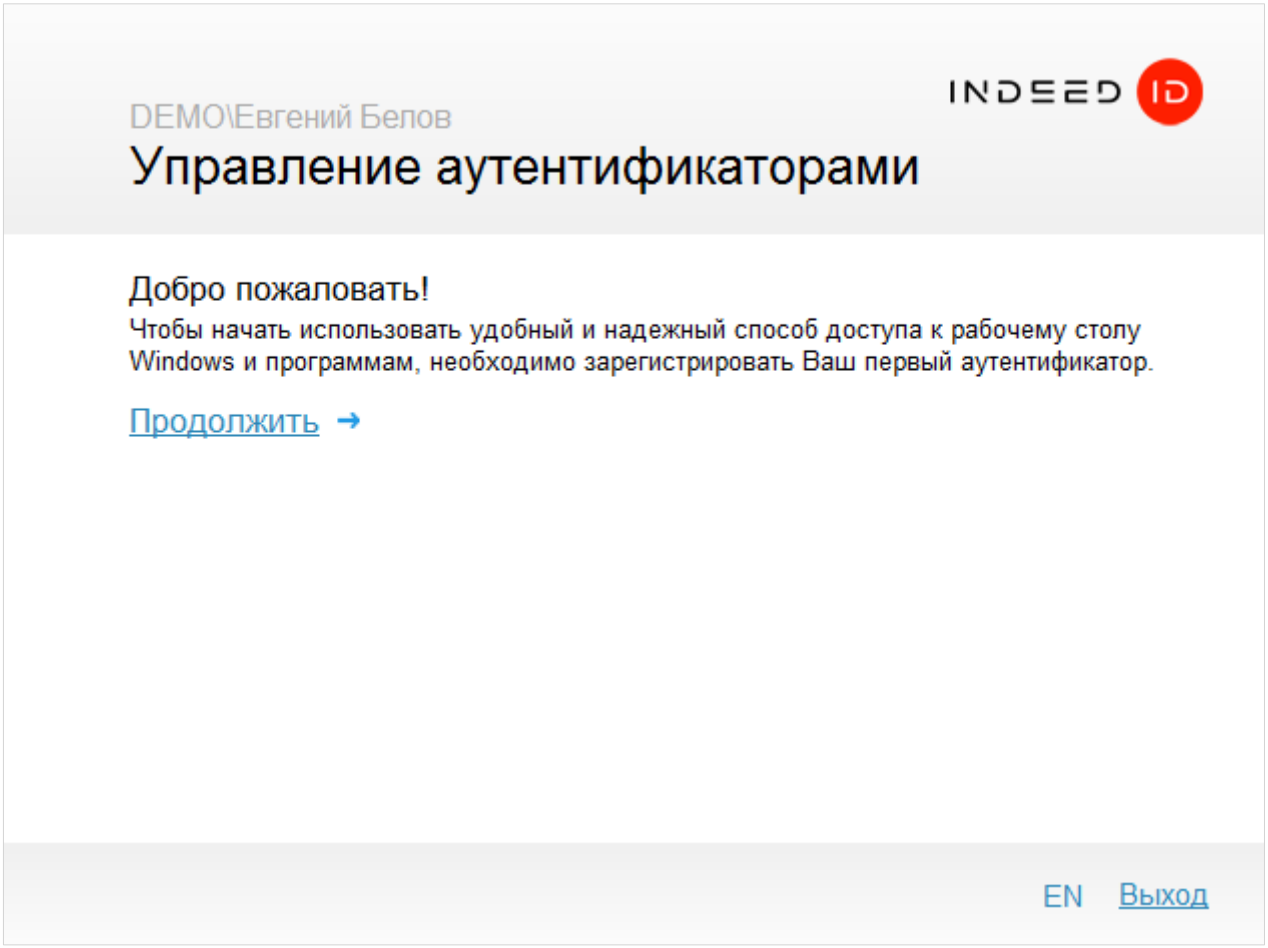

Рисунок 1a.

Если на рабочей станции пользователя установлено несколько провайдеров аутентификации, то необходимо выбрать **Карта (HID OMNIKEY Smart Card Reader)** из списка (Рисунок 1b).

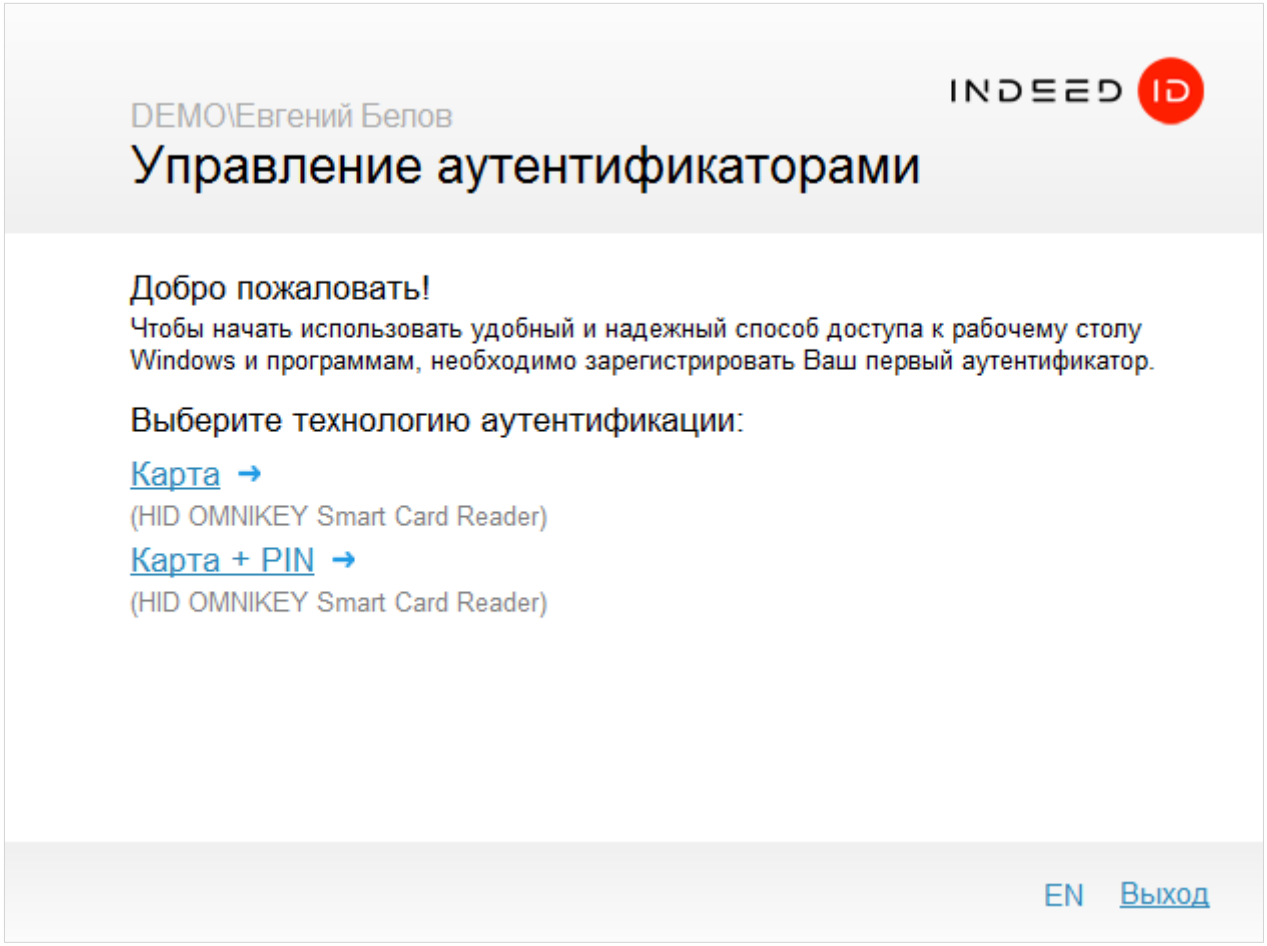

Рисунок 1b.

В случае использования провайдера Indeed-Id OMNIKEY with PIN Provider выберите **Карта + PIN (HID OMNIKEY Smart Card Reader)**. Если на компьютере установлен только один провайдер, окно выбора не отображается. Подключите считыватель карт OMNIKEY и положите на него карту (Рисунок 1c).

Во время процесса регистрации аутентификатора карта должна находиться на считывателе. В случае использования провайдера **Indeed-Id OMNIKEY with PIN Provider** потребуется придумать PIN-код и ввести его. Минимальное количество символов – три (Рисунок 1d). Данный PIN-код необходимо будет вводить каждый раз после прикладывания карты к считывателю. Задайте PIN-код и нажмите кнопку **Обучить**.

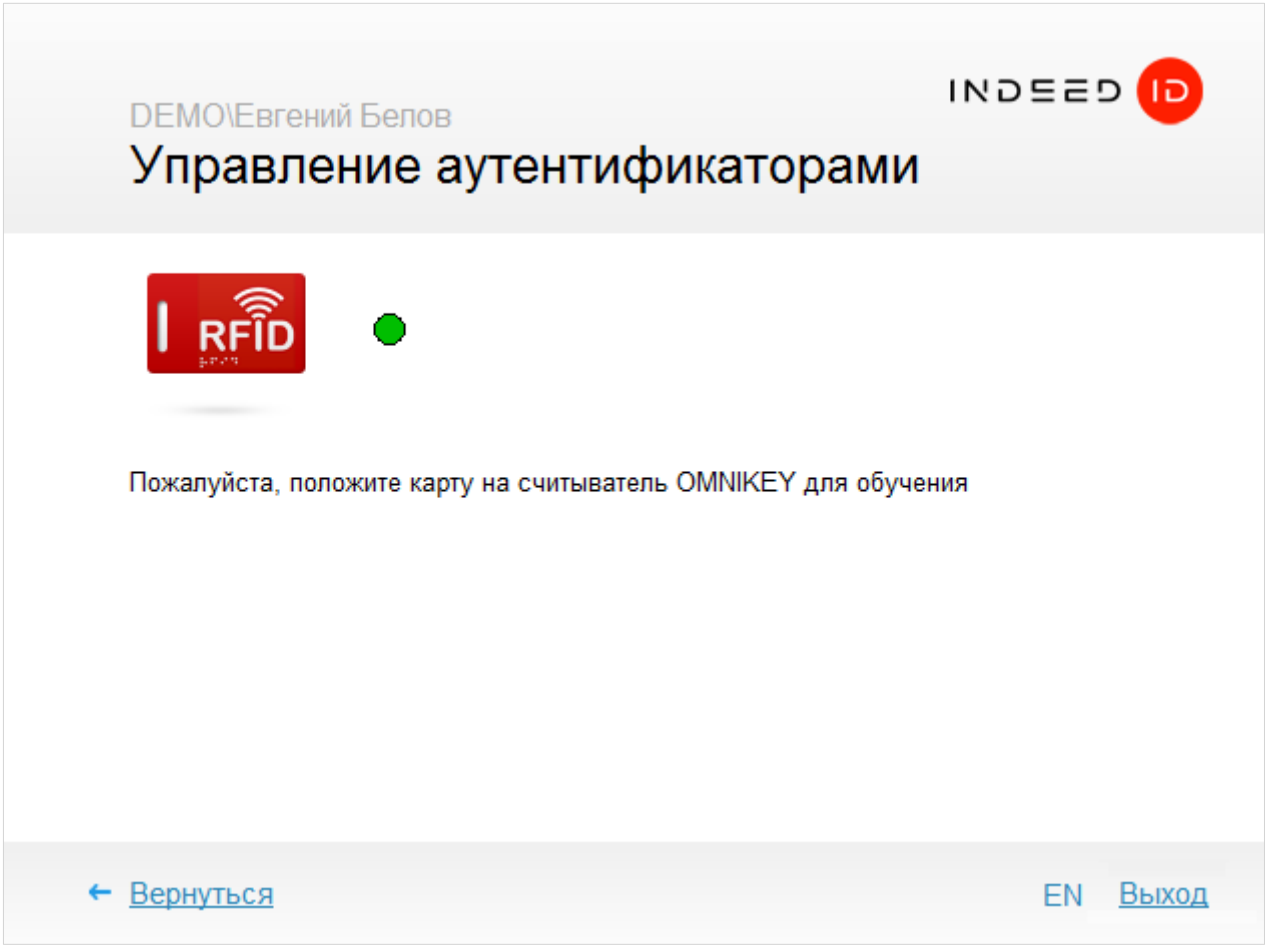

Рисунок 1c.

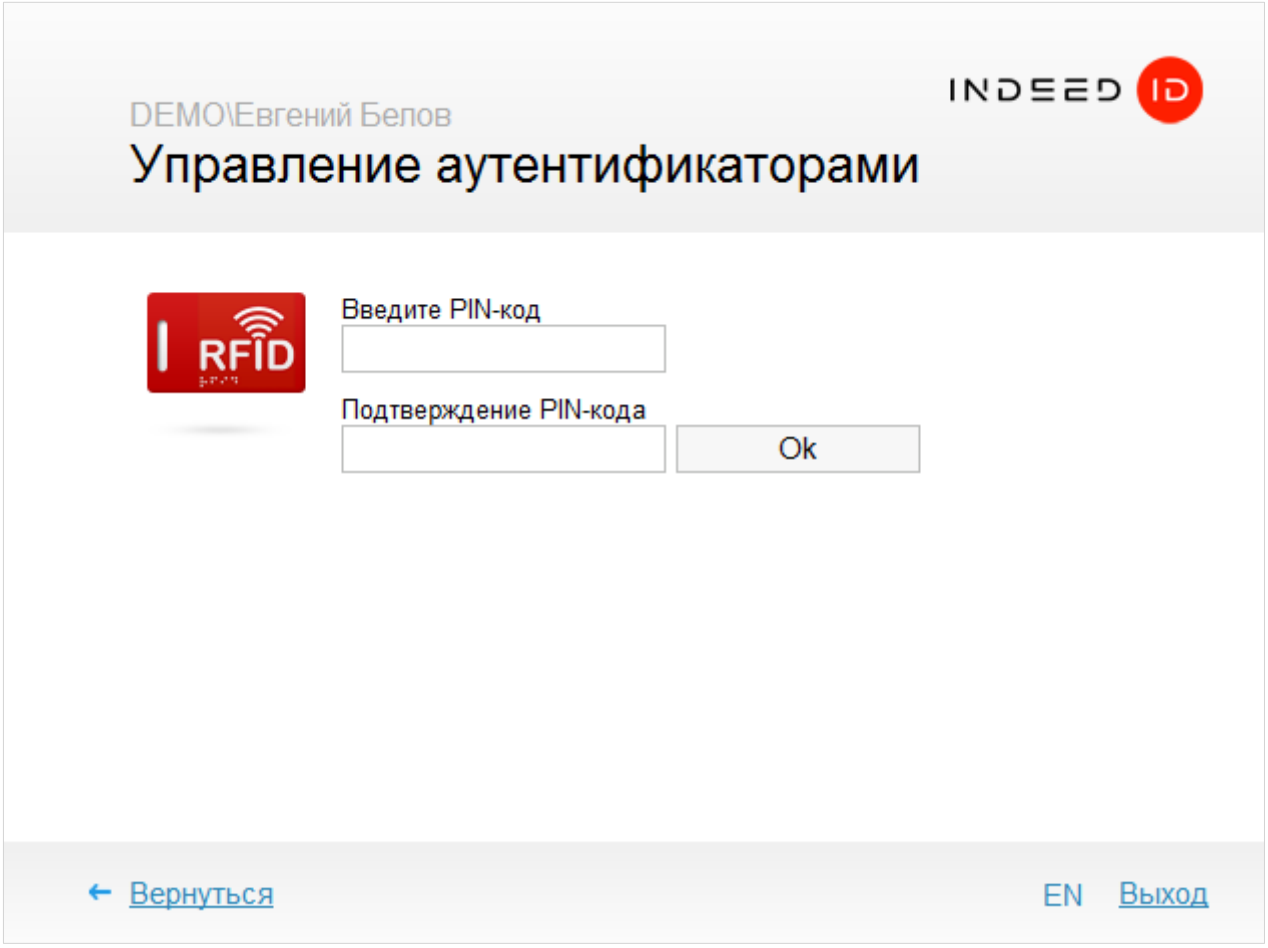

Рисунок 1d.

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

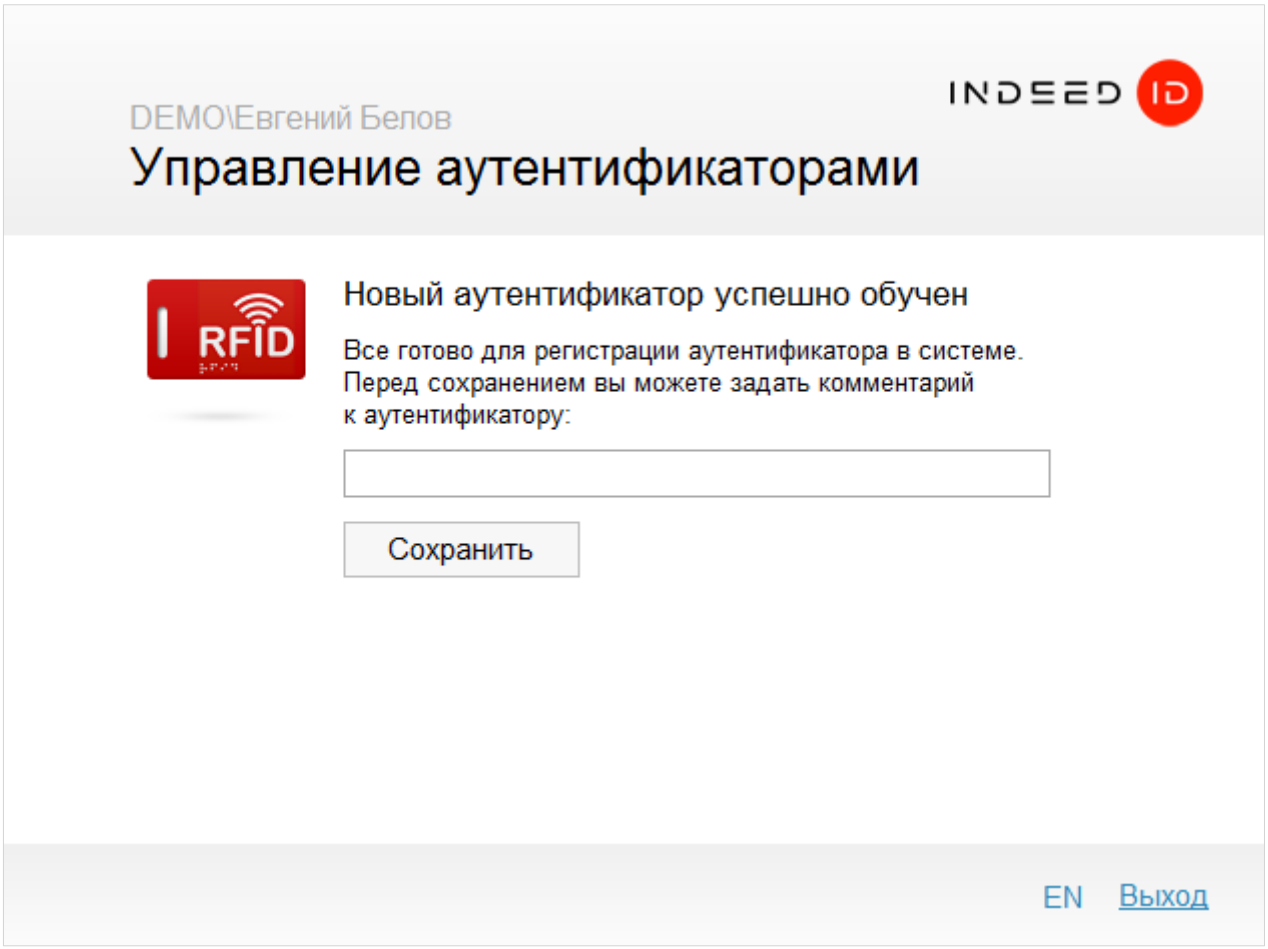

Рисунок 1e.

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 Indeed-Id OMNIKEY 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 **Карта** или **Карта + PIN**.

Рисунок 2.

Подключите считыватель карт OMNIKEY и положите на него карту (Рисунок 2). Если используется провайдер **Indeed-Id OMNIKEY Provider with PIN**, то следует ввести PIN-код и затем нажать **Вход**.

В случае успешного входа по аутентификатору, способ входа **Карта** или **Карта + 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 OMNIKEY Provider

Установка компонента

В этом разделе содержатся сведения по установке и настройке Indeed-Id OMNIKEY Provider. Установку Indeed-Id OMNIKEY Provider необходимо выполнить на всех серверах Indeed-Id и затем на рабочих станциях пользователей.

Предварительные условия для установки

Для корректной установки компонента должны выполняться следующие условия:

- Минимум 30 Мб свободного места на жестком диске компьютера
- USB-порт для подключения считывателя

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

Для развертывания Indeed-Id OMNIKEY 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 OMNIKEY Provider

1. Запустите файл IndeedID.OMNIKEY.Provider.msi[1] (или IndeedID.OMNIKEY.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 – Программы и компоненты (Установка и удаление программ).

[1] Для установки на 64-битных ОС следует использовать инсталляторы IndeedID.OMNIKEY.Provider.x64.msi и IndeedID.OMNIKEY.PIN.Provider.x64.msi

Настройка параметров аутентификации

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

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

Политика раздела **Windows Logon®** – **Таймаут выполнения действия при извлечении смарт–карты** определяет продолжительность стандартного и сервисного таймаута после извлечения устройства аутентификации.

Для настройки политики необходимо добавить файл политики **IndeedID.Client.adm** в список административных шаблонов политик Indeed-Id. Для получения подробной информации обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf.*

Политика задает интервал времени в секундах между извлечением смарт–карты и действием, выполняемым согласно политике Windows **Интерактивный вход: поведение при извлечении смарт–карты** (Interactive logon: Smart–card enhanced removal behavior).

Наличие **стандартного таймаута** позволяет предотвратить автоматическую блокировку компьютера при случайном извлечении устройства аутентификации.

Наличие **сервисного таймаута** позволяет предотвратить автоматическую блокировку компьютера в случаях, когда извлечение используемого устройства аутентификации необходимо (обучение дополнительного аутентификатора, получение доступа в систему от имени другой учетной записи по другому аутентификатору и т. п.). Для активации сервисного таймаута перед извлечением устройства необходимо нажать и удерживать комбинацию клавиш **[Ctrl]+[L]**.

Если политика не задана или отключена, то таймаут перед автоматической блокировкой рабочей станции не предоставляется.

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