Этот документ входит в комплект поставки продукта.
Информация, содержащаяся в этом документе, может быть изменена разработчиком без уведомления пользователя.

Контактная информация:

+7 (495) 640-06-09
Москва
+7 (812) 640-06-09
Санкт-Петербург

inbox@indeed-id.com
почта

8 800 333-09-06
support@indeed-id.com
техническая поддержка

Indeed-Id Smart Card Provider

Руководство по установке и эксплуатации

версия 1.7.1

Содержание

Введение

Приветствуем вас и благодарим за приобретение программных продуктов компании Indeed ID. Это руководство поможет вам ознакомиться с принципом работы компонента **Indeed-Id Smart Card Provider**, параметрами его установки и настройки.

Условные обозначения

В Руководстве используются следующие условные обозначения:

Важная информация
Указания, требующие особого внимания при развертывании, настройке, работе или обновлении продукта.

Дополнительная информация
Указания, способные упростить развертывание, настройку, работу или обновление продукта.

О компоненте Indeed-Id Smart Card Provider

Компонент Indeed-Id Smart Card Provider предназначен для аутентификации пользователей по персональным устройствам (смарт-картам, usb-ключами) и совместного использования с продуктами Indeed Enterprise Authentication и Indeed Enterprise Single Sign-On.
Возможны варианты использования одного и того же устройства аутентификации как с запросом PIN-кода, так и без него. В случае использования **Indeed-Id Smart Card Provider** для аутентификации пользователю потребуется приложить карту к считывателю, PIN-код запрашиваться не будет. При использовании **Indeed-Id Smart Card Provider with PIN** ввод PIN-кода потребуется при каждой аутентификации пользователя.

Indeed-Id Smart Card Provider with PIN не позволяет задавать, изменять или удалять PIN-коды устройств аутентификации. Для изменения или удаления PIN-кодов используйте специализированное программное обеспечение от производителей устройств аутентификации.

Таблица 1 – Поддерживаемые устройства аутентификации

Рутокен	eToken	ESMART	Avest	SafeNet	JaCarta	Gemalto	Indeed
Рутокен S Рутокен ЭЦП Рутокен ЭЦП 2.0 Рутокен Lite	eToken Pro 32k eToken Pro 64k eToken Pro Java 72k	Token 64K Token SC 64K Token USB 64K	Avest Key-256A	iKey 1000 iKey 1032	JaCarta PKI	IDPrime MD	AirKey Enterprise

Работа с Indeed-Id Smart Card 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 компонентов системы Indeed EA(ESSO): Indeed-Id Windows Logon или Indeed-Id ESSO Агент (в зависимости от используемой конфигурации системы) и провайдера Indeed-Id Smart Card Provider. Пользователь выполняет вход в операционную систему или приложение ESSO по доменному паролю и, следуя указаниям приложения **Indeed-Id Управление аутентификаторами**, регистрирует аутентификатор.

Для регистрации аутентификатора пользователю должно быть разрешено использовать технологию аутентификации Indeed-Id. Разрешение выдается **администратором Indeed EA(ESSO) 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 операционную систему или приложение ESSO, то регистрацию можно выполнить в любой удобный момент, запустив приложение **Indeed-Id Управление аутентификаторами** из меню *Пуск – Все программы – Indeed-Id*.

Для регистрации аутентификатора войдите в операционную систему или приложение **Управление аутентификаторами** по доменному паролю и выполнить следующие действия:

В окне **Управление аутентификаторами** нажмите **Продолжить** (Рисунок 1).

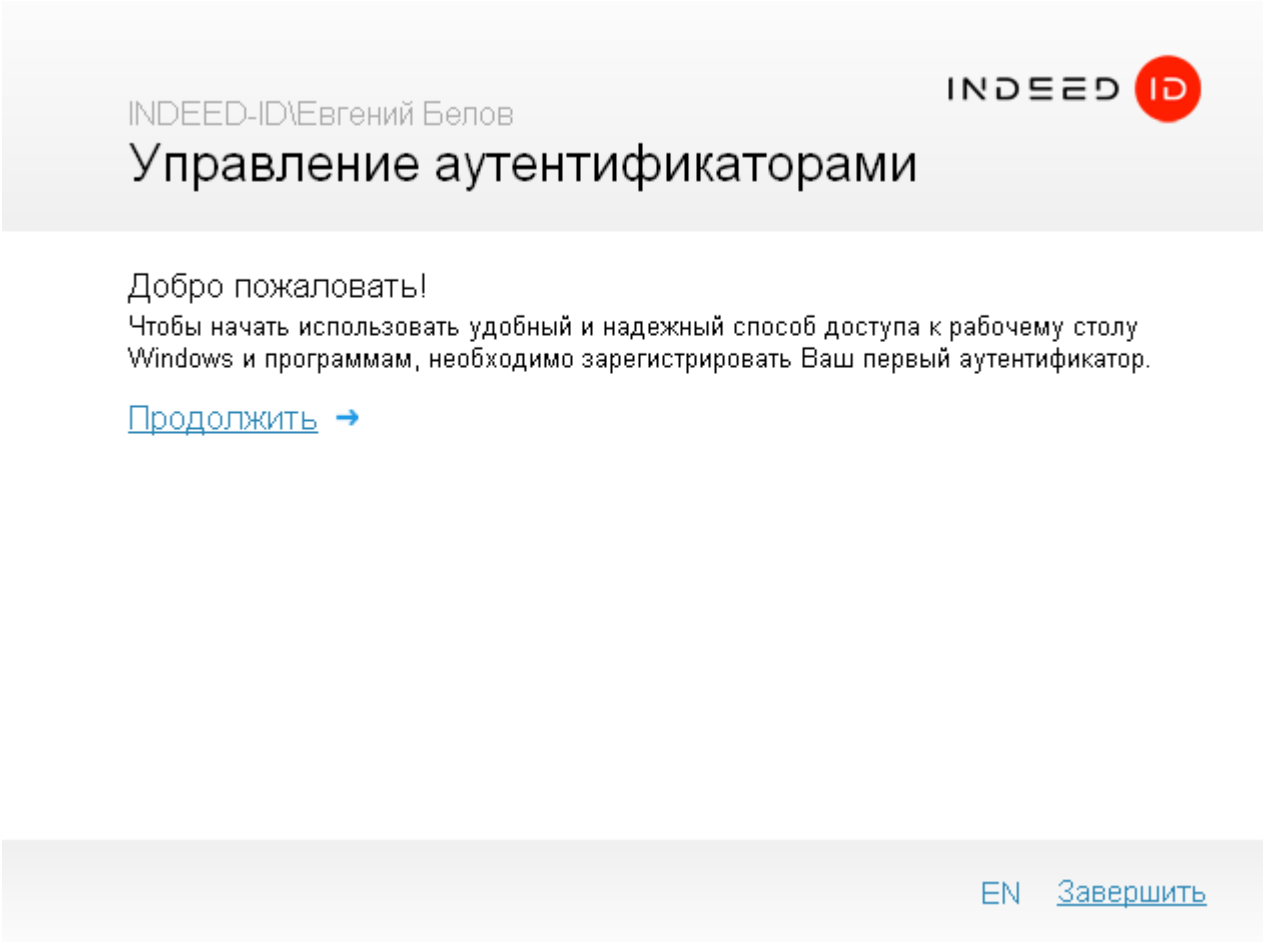

Рисунок 1 – Регистрация аутентификатора.

Если на рабочей станции пользователя установлено несколько провайдеров аутентификации, то необходимо выбрать **Смарт-карта или USB-ключ** из списка (Рисунок 2). Если установлен только один провайдер, окно выбора не отображается. В случае использования провайдера Indeed-Id Smart Card Providerwith PIN Provider выберите **Смарт-карта или USB-ключ** + **PIN**).

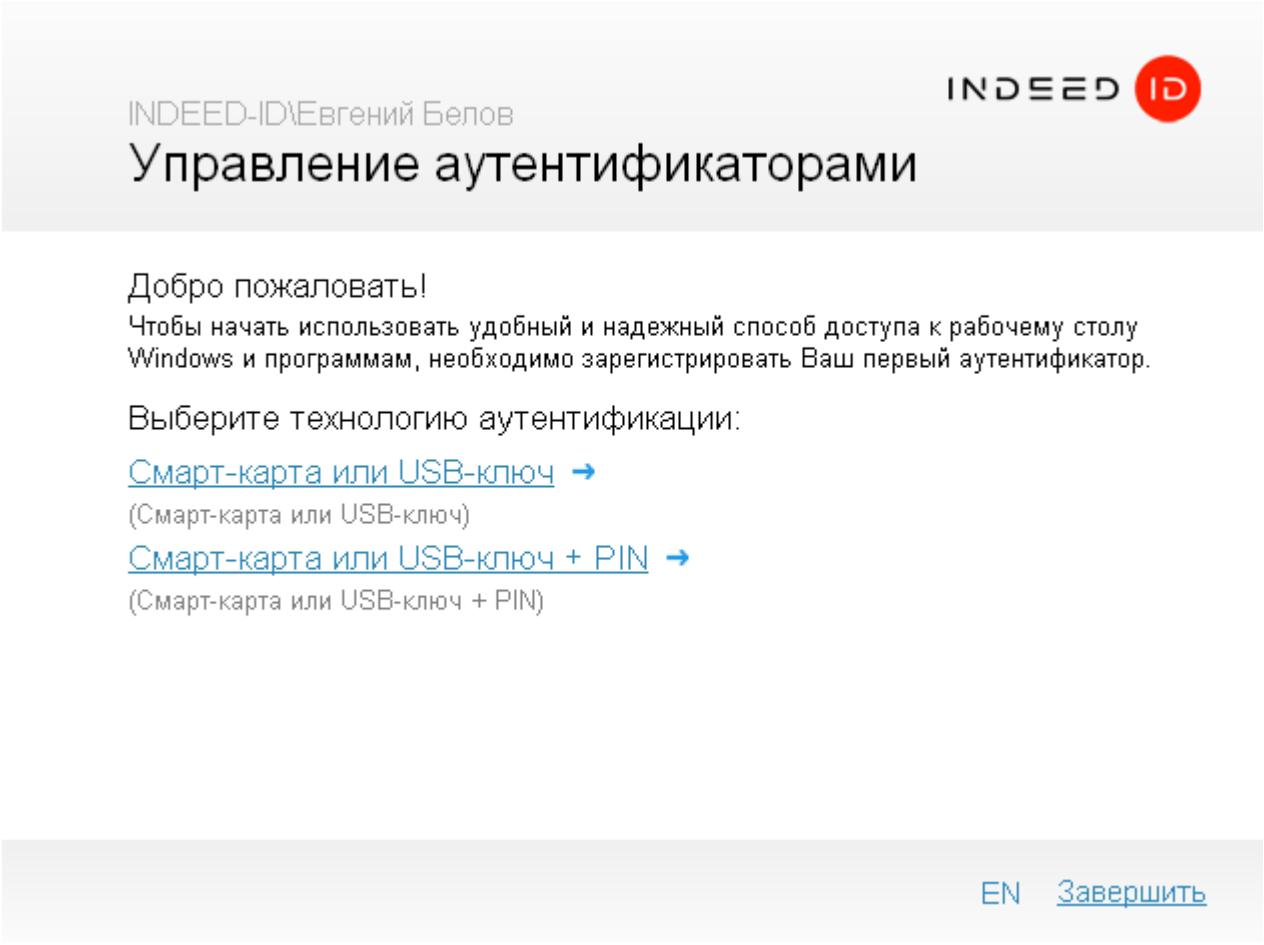

Рисунок 2 – Выбор аутентификатора.

Подключите смарт-карту или USB-ключ к компьютеру (Рисунок 3). Если к компьютеру подключено несколько устройств, выберите нужное и нажмите **ОК** (Рисунок 4).

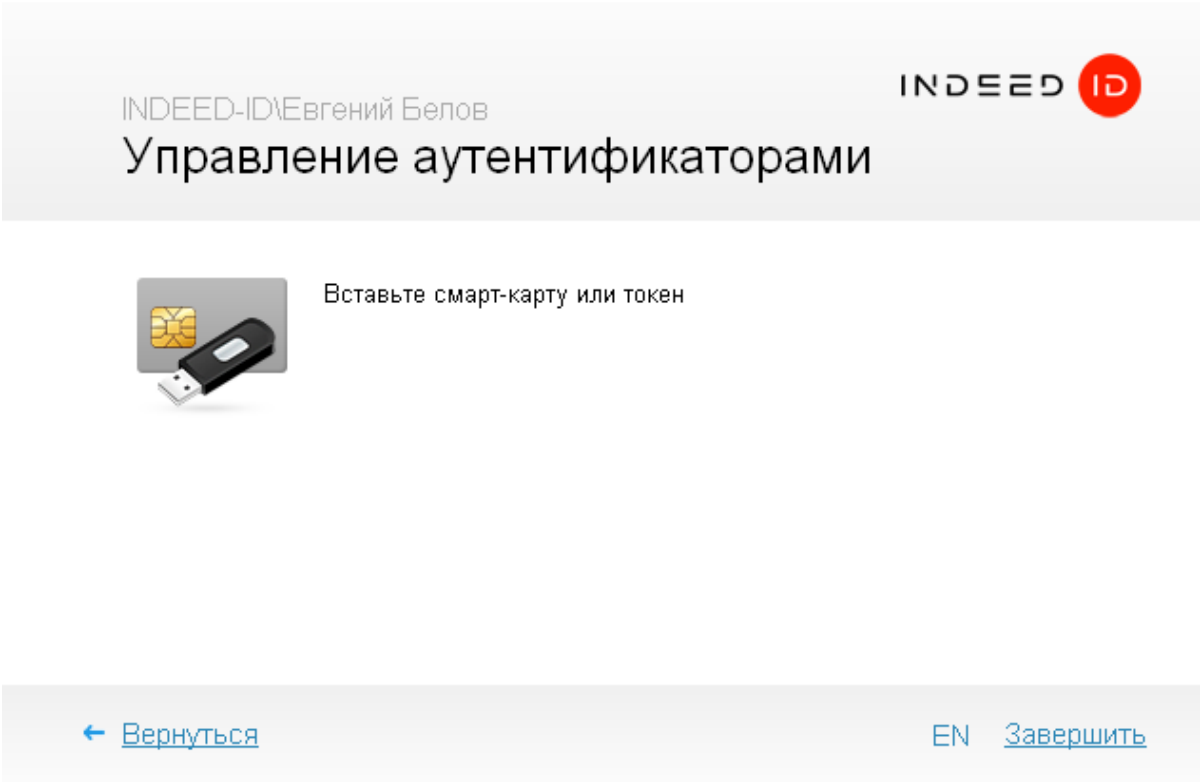

Рисунок 3 – Подключение смарт-карты.

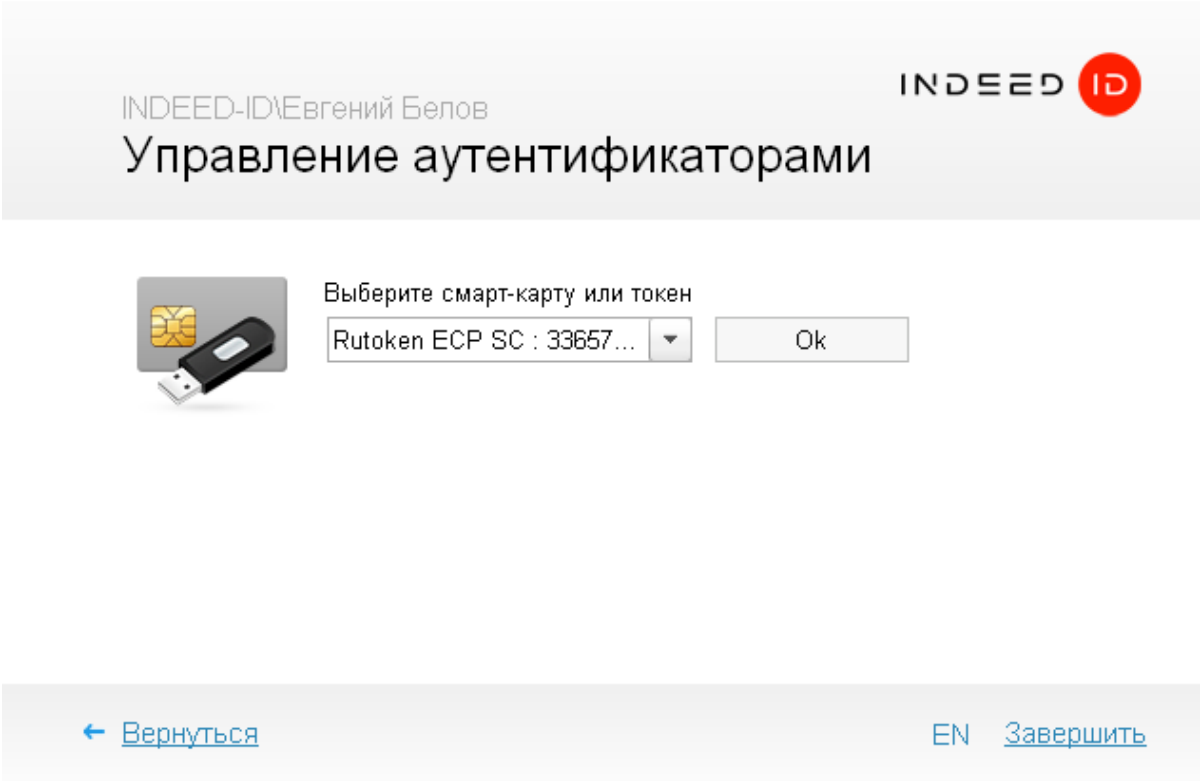

Рисунок 4 – Выбор смарт-карты.

В случае использования провайдера Indeed-Id Smart Card Provider with PIN потребуется ввести PIN-код смарт-карты (USB-ключа). PIN-код необходимо будет вводить каждый раз при прохождении процедуры аутентификации. Введите PIN-код и нажмите **OK** (Рисунок 5).

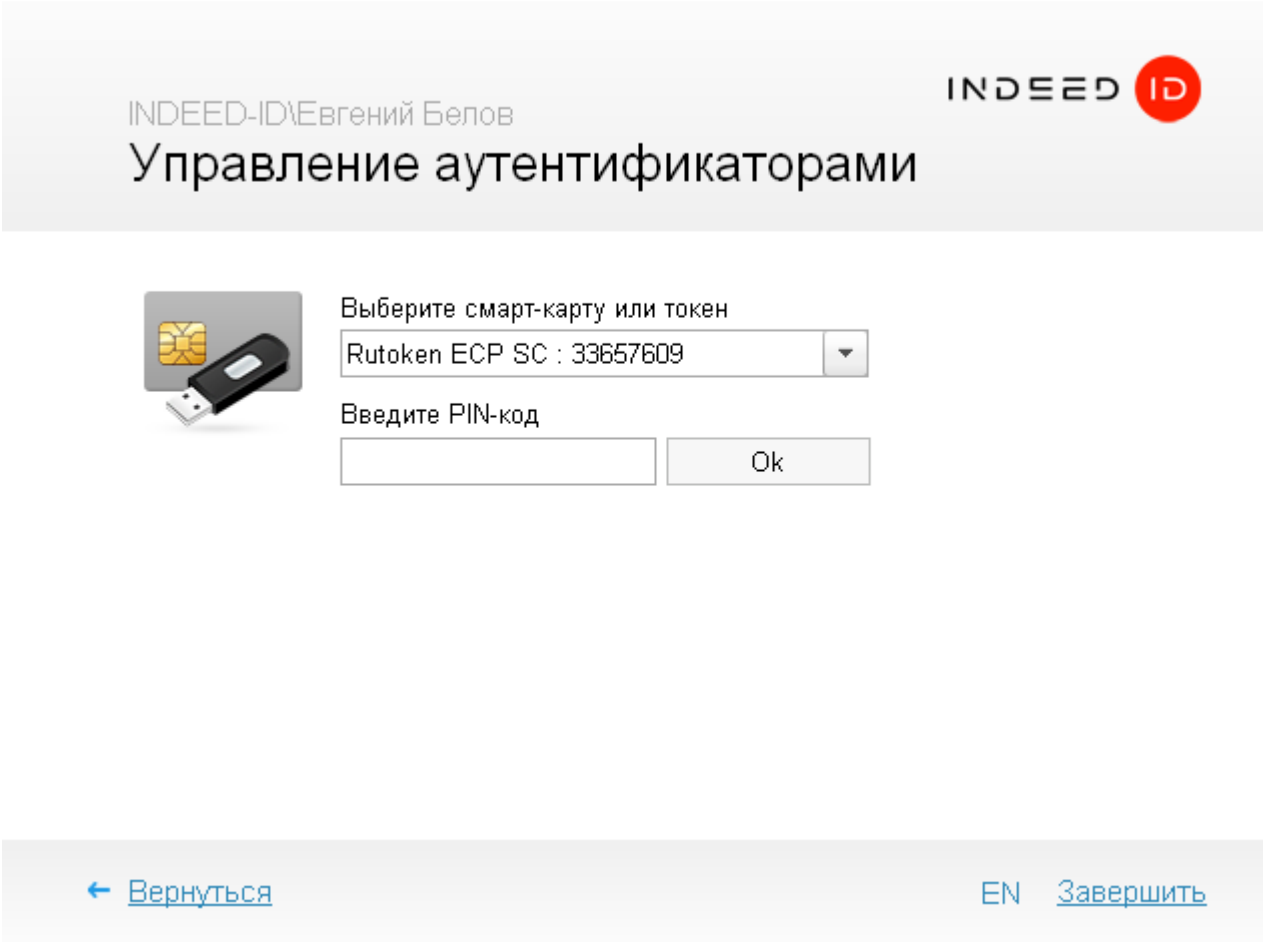

Рисунок 5 – Ввод PIN-кода пользователя.

При необходимости, введите комментарий к заданному способу входа и нажмите **Сохранить** (Рисунок 6).

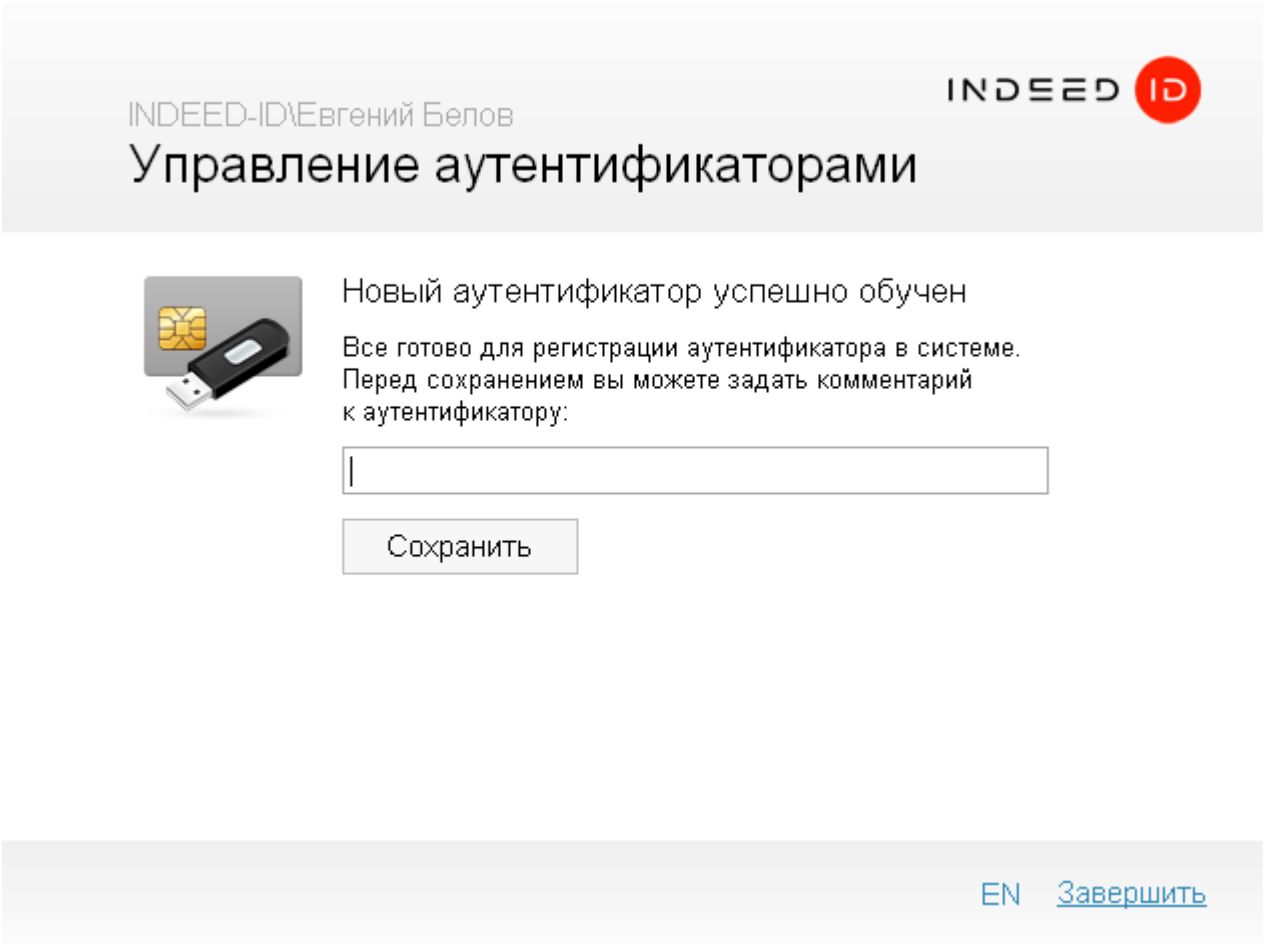

Рисунок 6 – Комментарий к аутентификатору.

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

Аутентификация при помощи Indeed-Id Smart Card Provider

При первом входе в операционную систему или приложение с использованием технологии аутентификации Indeed-Id выберите способ входа. Для этого нажмите **Сменить способ входа** (Рисунок 7) в окне **Вход в Windows** (окно **Аутентификация** для Enterprise SSO). Выберите способ входа **Смарт-карта или USB-ключ** или **Смарт-карта или USB-ключ + PIN**.

Рисунок 7 – Вход в Windows с помощью Indeed-Id Smart Card Provider.

Подключите USB-ключ или смарт-карту к компьютеру. Если используется **Indeed-Id Smart Card Providerwith PIN**, введите PIN-код и нажмите **Вход**. В случае успешного входа по аутентификатору, способ входа **Смарт-карта или USB-ключ** (Смарт-карта или USB-ключ + PIN) запоминается, как предпочтительный и будет автоматически предложен пользователю при следующем входе в операционную систему или приложение ESSO.

Управление аутентификаторами

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

- Регистрировать
- Перерегистрировать
- 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 Indeed-Id Smart Card Provider

Установка Indeed-Id Smart Card Provider выполняется на всех серверах Indeed-Id и затем на рабочих станциях пользователей.

Предварительные условия для установки:

- Минимум 30 Мб свободного места на жестком диске компьютера
- USB-порт для подключения считывателя
- Установленные драйверы считывателей смарт-карт и драйверы самих смарт-карт, если таковые предоставляются производителем карт.

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

Для развертывания Indeed-Id Smart Card 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*.

Для установки Indeed-Id Smart Card Provider выполните следующие действия:

1. Запустите файл IndeedID.Smartcard.Provider.msi[1] 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.

[1] IndeedID.Smartcard.PIN.Provider.msi если необходимо установить версию провайдера с PIN-кодом.

Настройка параметров аутентификации

Изменение параметров работы провайдера осуществляется через механизм групповых политик Active Directory.

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

Настройка политик необходима для повышения уровня безопасности. Однако полноценная работа Indeed-Id Smart Card 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.

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** предотвращает автоматическую блокировку компьютера при случайном извлечении устройства аутентификации.

Наличие **сервисного таймаута** предотвращает автоматическую блокировку компьютера в случаях, когда извлечение используемого устройства аутентификации необходимо (зарегистрировать дополнительный аутентификатор, получить доступ в операционную систему или приложение под другой учетной записью и аутентификатором). Для активации сервисного таймаута перед извлечением устройства нажмите и удерживайте комбинацию клавиш **[Ctrl]+[L]**.

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

Для настройки политики добавьте файл политики **IndeedID.Client.admx** 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 раздела **Providers – Использовать дополнительные данные** позволяет настроить режим повышенной безопасности с возможностью записи дополнительных данных на устройство и чтения этих данных. Режим использования дополнительных данных предотвращает повторную инициализацию устройства и последующее несанкционированное использование аутентификатора от имени учетной записи настоящего владельца.

Перед настройкой групповой политики добавьте в список административных шаблонов шаблоны политик Indeed-Id. Административный файл шаблона политики **IndeedID.Smartcard.Provider.admx** 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.

Дополнительные данные – последовательность из 64 случайных байт, которая записывается на смарт-карту (usb-ключ) и включается в состав аутентификатора вместе с серийным номером средства аутентификации. Дополнительные данные считываются устройства и проходят проверку одновременно с серийным номером при аутентификации пользователя.

Режим использования дополнительных данных включен, если настройка политики установлена в значение **Включен** (Enabled) или **Не задан** (Not Configured).

Разрешить работу без дополнительных данных – разрешение работы провайдера без использования дополнительных данных (при включенной политике). Опция может использоваться для работы с устройствами, зарегистрированными в старых версиях Indeed-Id Smart Card Provider (без поддержки дополнительных данных).

Выполните обновление групповых политик для применения настроек. Для немедленного обновления групповой политики используйте команду **gpupdate /force**.