Indeed-Id
eTokenPASS Provider (Demo)

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 eToken PASS Provider** и параметрами его установки.

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 eTokenPASS Provider

Автономный генератор одноразовых паролей eToken PASS можно использовать для аутентификации в любых приложениях и службах, поддерживающих протокол аутентификации RADIUS – VPN, Microsoft ISA, Microsoft IIS, Outlook Web Access и др. В eToken PASS реализован алгоритм генерации одноразовых паролей (One-Time Password – OTP). Этот алгоритм основан на алгоритме HMAC и хэш-функции SHA-1. Для расчета значения OTP принимаются два входных параметра – секретный ключ (начальное значение для генератора) и текущее значение счетчика (количество необходимых циклов генерации). Начальное значение хранится как в самом устройстве, так и на сервере в системе Indeed-Id TMS. Счетчик в устройстве увеличивается при каждой генерации OTP, на сервере – при каждой удачной аутентификации по OTP. Подробную информацию об устройстве eToken PASS Вы можете получить на официальном сайте компании Aladdin: **http://www.aladdin-rd.ru**.

В состав демонстрационной версии **Indeed-Id eToken PASS Provider** входят следующие компоненты:

- **Indeed-Id eToken PASS Provider** – компонент, обеспечивающий работу устройства Aladdin eToken PASS с модулями решения Indeed-Id.
- **Indeed-Id TMS** – компонент, обеспечивающий возможность управления токенами.
- **Indeed-Id TMS Manager** – консоль администрирования, предназначенная для управления токенами.

В демонстрационной версии Indeed-Id eToken PASS Provider поддерживает работу только с одним экземпляром Indeed-Id Enterprise Server.

Работа с Indeed-Id eTokenPASS 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 eToken PASS 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).

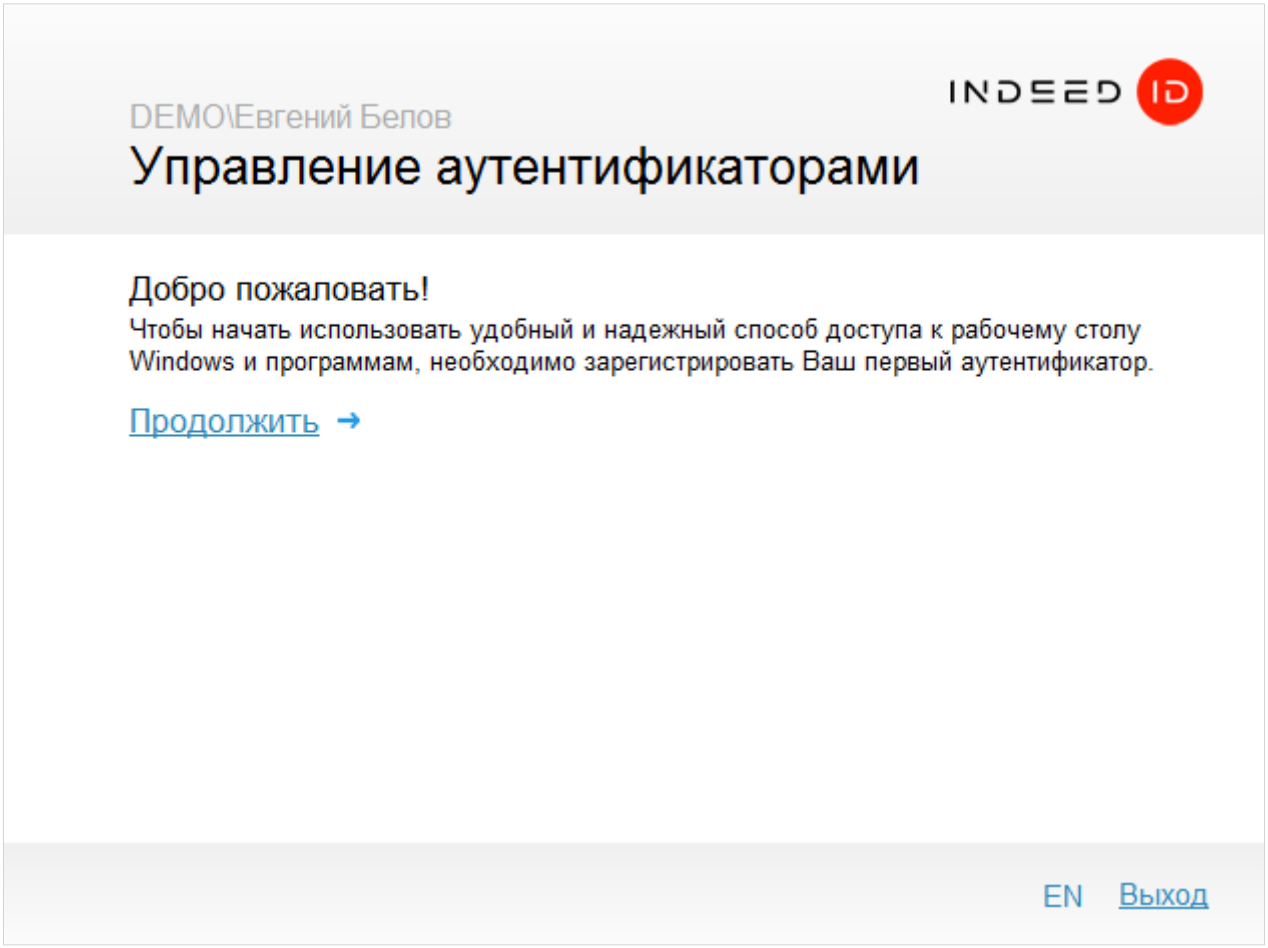

Рисунок 1a.

Если на рабочей станции пользователя установлено несколько провайдеров аутентификации, то необходимо выбрать **Одноразовый пароль (Aladdin eToken PASS)** из списка (Рисунок 1b). Если на компьютере установлен только один провайдер, окно выбора не отображается. Введите серийный номер устройства eToken PASS и нажмите кнопку **Обучить** (Рисунок 1c).

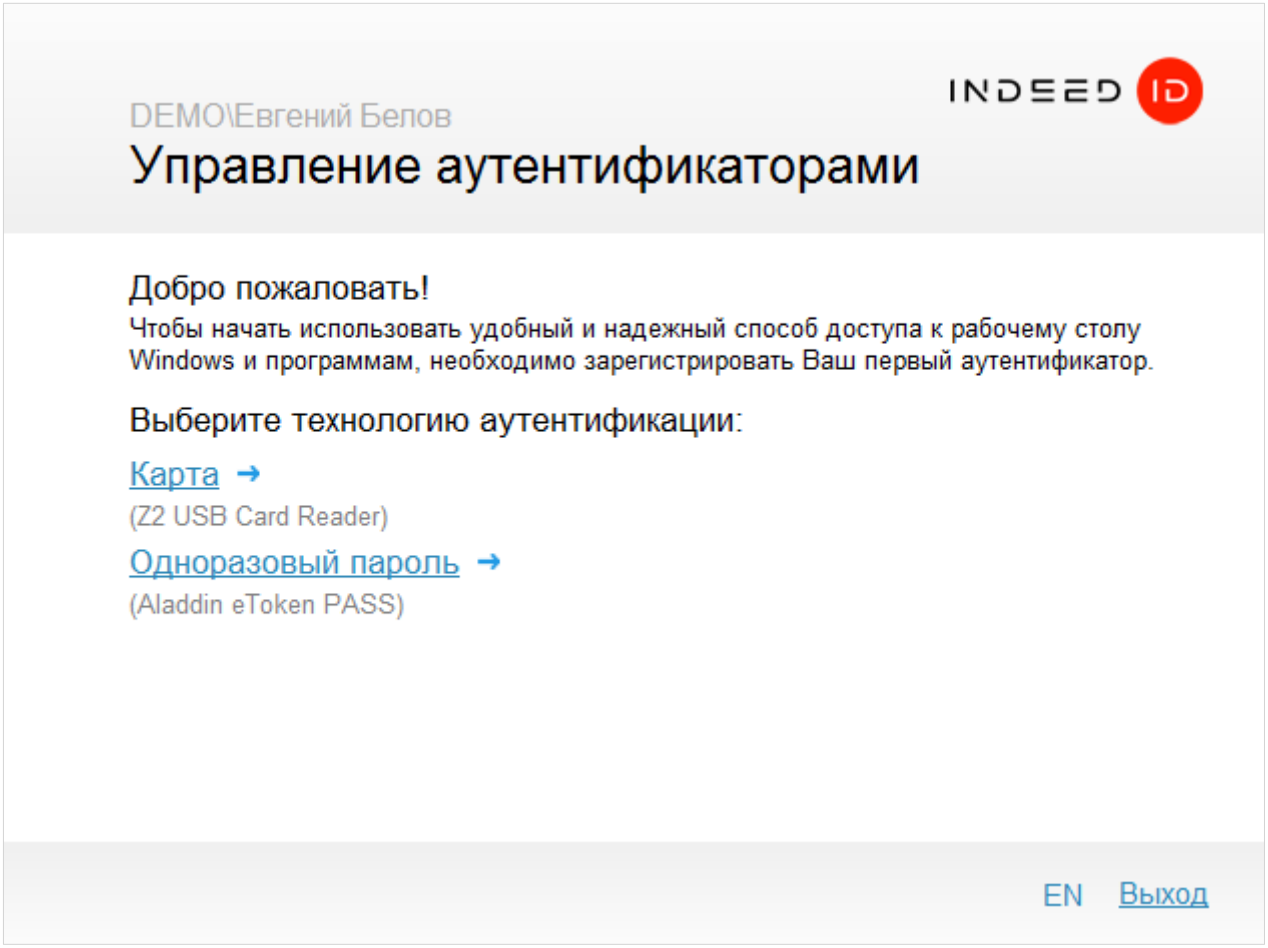

Рисунок 1b.

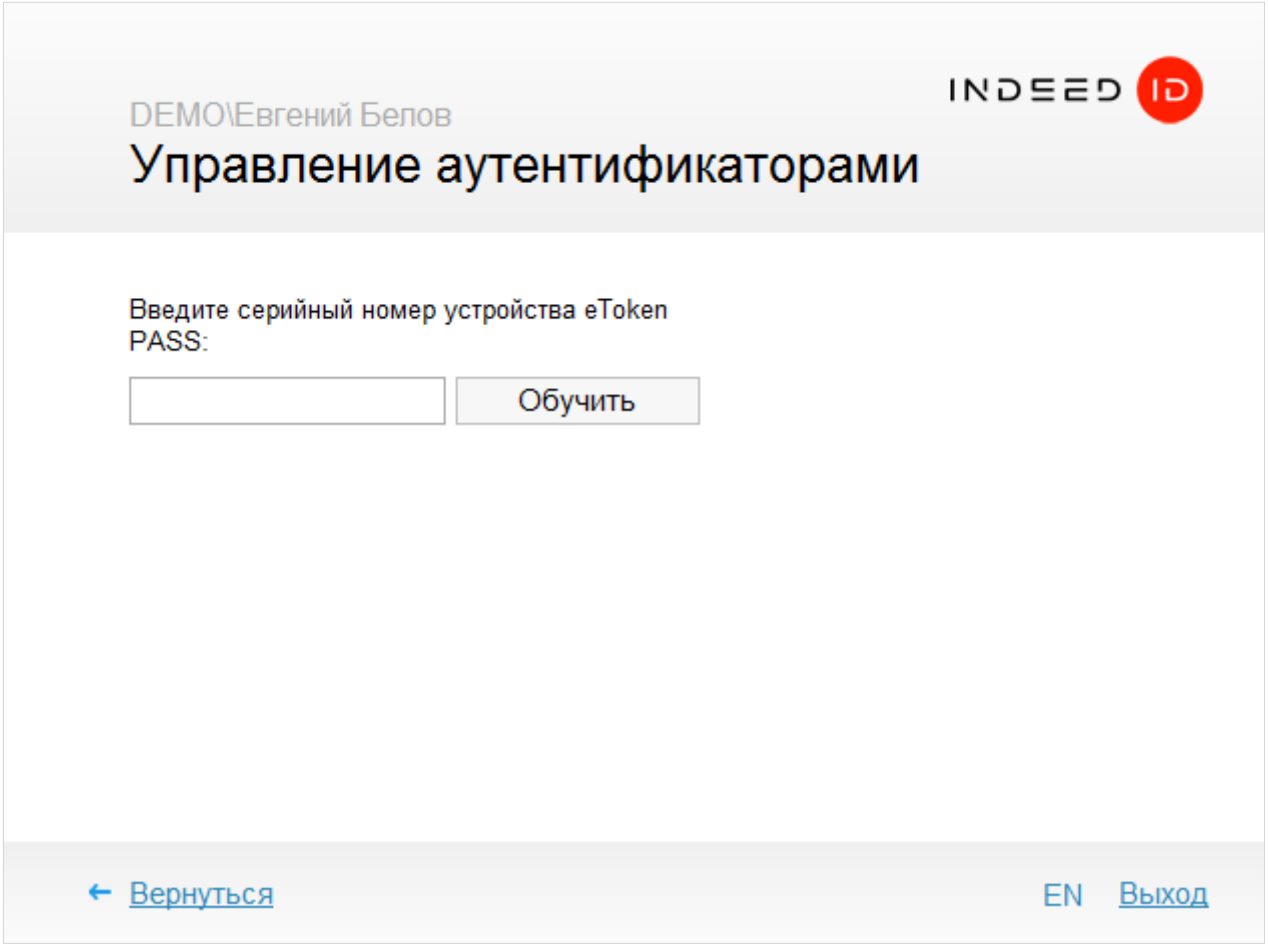

Рисунок 1c.

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

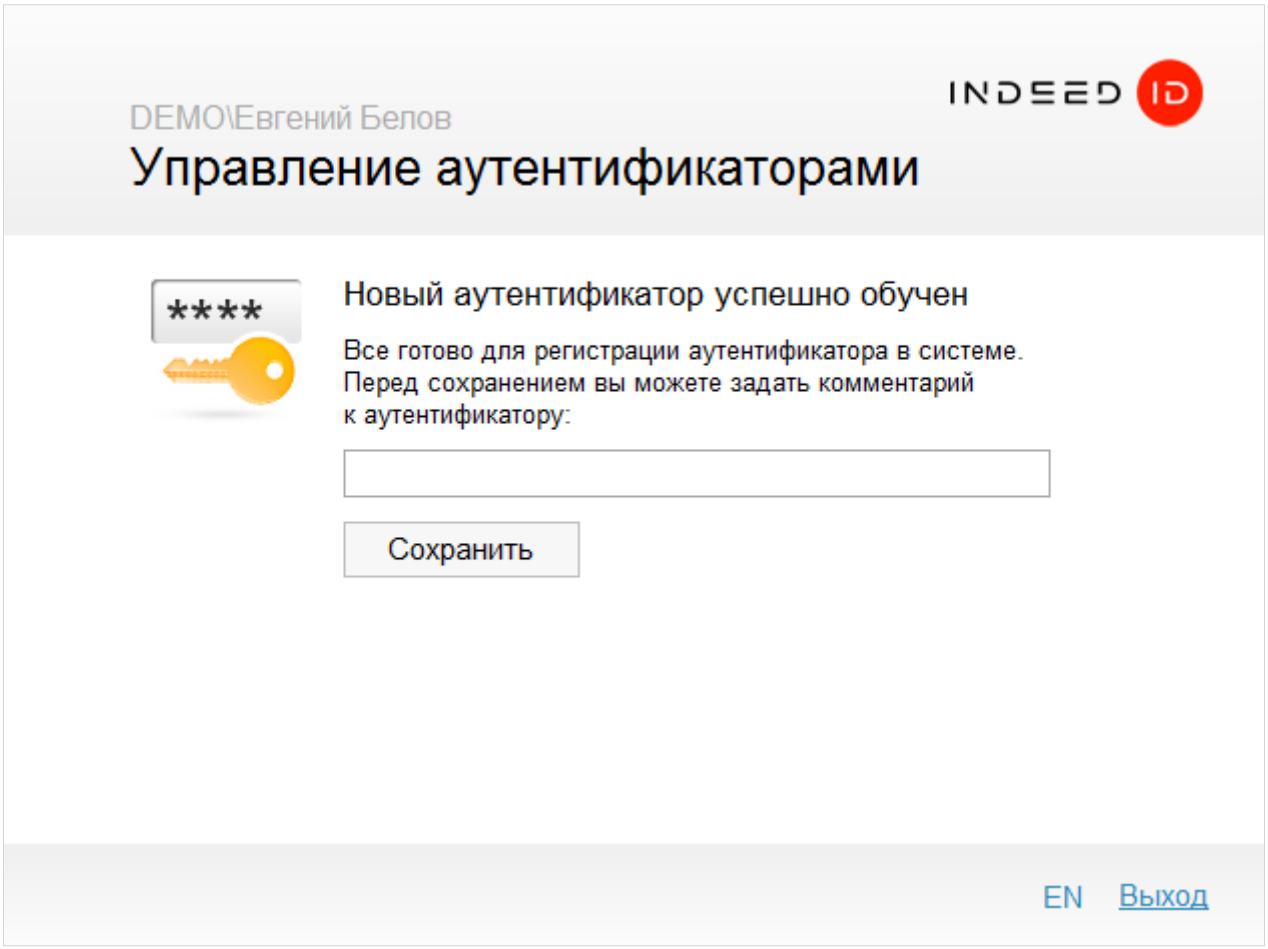

Рисунок 1d.

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 eToken PASS 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**.

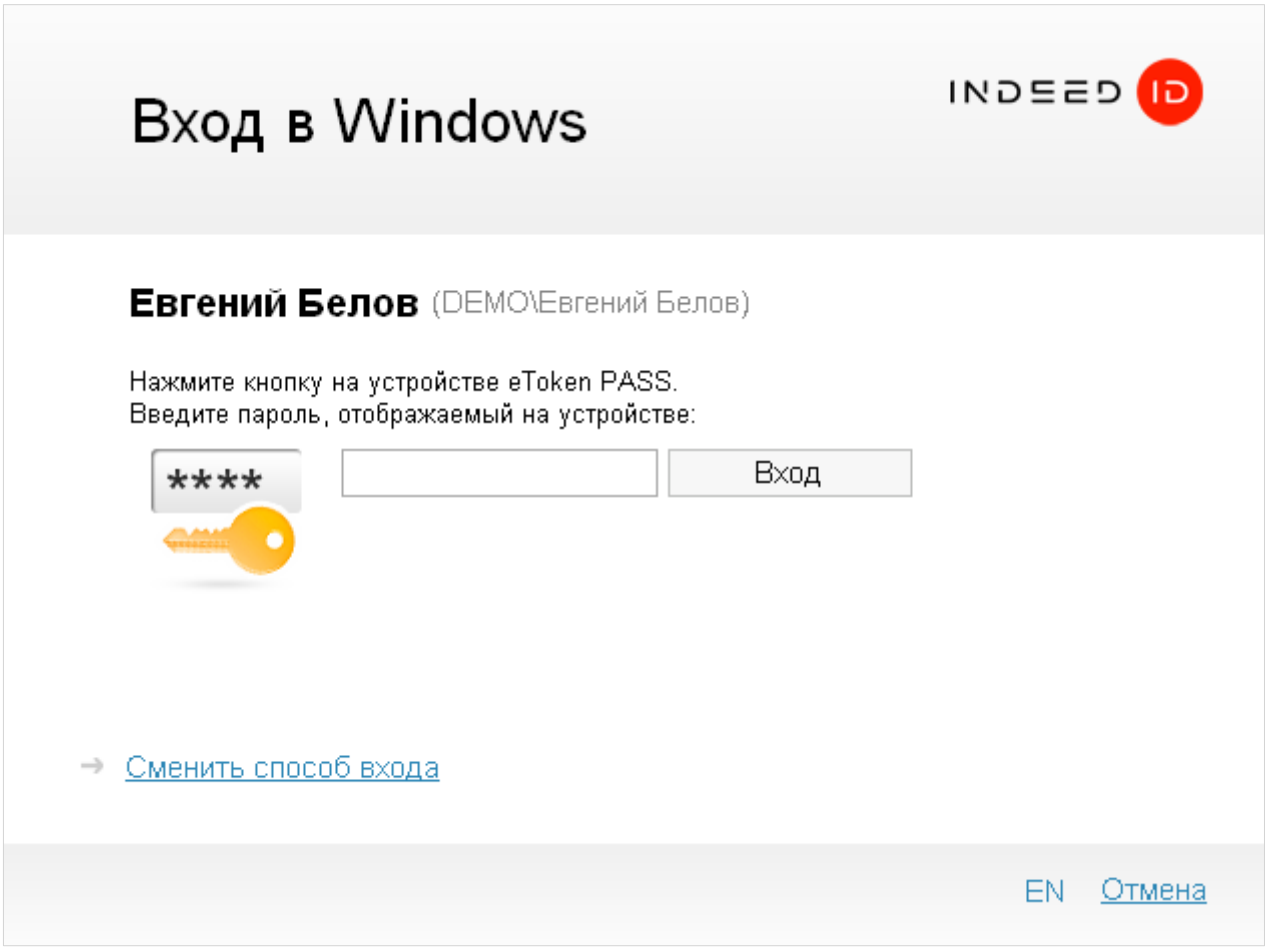

Рисунок 2.

Введите одноразовый пароль, сгенерированный устройством eToken PASS (Рисунок 2). В случае успешного входа по аутентификатору, способ входа **Одноразовый пароль** 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 eToken PASS Provider

В этом разделе содержатся сведения по установке и настройке Indeed-Id eToken PASS Provider. Установку Indeed-Id eToken PASS 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
- Aladdin eToken PKI Client версии не ниже 5.1 SP1[1]

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

Для развертывания Indeed-Id eToken PASS 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 eToken PASS Provider

1. Запустите файл IndeedID.eToken.PASS.Provider.msi 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] Установка необходима только на рабочую станцию с Indeed-Id Enterprise Server.

Установка компонентов Indeed-Id TMS

1. Установка компонент **Indeed-Id TMS** выполняется на сервере Indeed-Id. Скопируйте файлы IndeedID.TMS.exe и IndeedID.TMS.Manager.exe из дистрибутива Indeed-Id в каталог %Program Files% на сервере Indeed-Id.
2. Выполните регистрацию компонента IndeedID.TMS.exe командой **IndeedID.TMS.exe /RegServer**.
3. Скопируйте на сервер Indeed-Id файлы .xml, входящие в комплект поставки устройства eToken PASS.

Убедитесь в том, что файлы .xml соответствуют имеющимся у вас устройствам eToken PASS. Перед копированием файлов рекомендуется проверить их корректность. Для этого:

- Сверьте серийный номер устройства с серийным номером, указанным в файле. Серийный номер устройства нанесен на задней поверхности корпуса:

- Откройте файл .xml в web-браузере. Ниже приведен фрагмент файла .xml, содержащий серийный номер устройства (выделен цветом):

```
<?xml version="1.0" encoding="utf-8"?>
<Tokens xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:js="js"
 xmlns:msxsl="urn:schemas-microsoft-com:xslt">
  <Token serial="00020007145B">
<CaseModel>5</CaseModel>
    <Model>109</Model>
    <ProductionDate>11/4/2008</ProductionDate>
    <ProductName>Aladdin OTPO v1.0</ProductName>
    <Applications>
```

Регистрация устройств eToken PASS

Для регистрации информации об устройствах Indeed-Id eToken PASS в командной строке введите команду вида:

IndeedID.TMS.Manager.exe /register --file <имя файла xml>.

Пример:

IndeedID.TMS.Manager.exe /register --file f000001254.xml

При успешной регистрации в строке результата отображается сообщение "The operation completed successfully":

```
C:\Program Files\Indeed-ID\TMS>.TMS.Manager.exe /register --file f000001254.xml

Registration results:

Token serial     Registration result
00020007145B     0x0 (The operation completed successfully.)
00020009AF1D     0x0 (The operation completed successfully.)
```

Проверка регистрации

Для проверки регистрации в командной строке введите команду **IndeedID.TMS.Manager.exe /info**. Если регистрация устройств была выполнена успешно, в строке результата отображается информация о зарегистрированных устройствах. Информация включает серийный номер устройства, дату регистрации, статус (включено/отключено), дату принудительной синхронизации, дату последней успешной проверки OTP и дату последней неуспешной проверки OTP:

```
C:\Program Files\Indeed-ID\TMS>IndeedID.TMS.Manager.exe /info
Registered tokens count: 2

Serial          :  00020007145B
Registered on   :  10/26/2010 12:53:31 PM
Enabled         :  yes
Forcibly synchronized on          :  Never
Last successfull OTP validation on :  Never
Last failed OTP validation on     :  Never
-----------------------------------------

Serial          :  00020009AF1D
Registered on   :  10/26/2010 12:53:31 PM
Enabled         :  yes
Forcibly synchronized on          :  Never
Last successfull OTP validation on :  Never
Last failed OTP validation on     :  Never
-----------------------------------------
```

Синхронизация счетчиков устройства eToken PASS с Indeed-Id TMS

Для синхронизации счетчиков устройства необходим Aladdin eToken PKI Client версии не ниже 5.1 SP1, установленный на сервере Indeed-Id.

Для синхронизации счетчиков устройства eToken PASS с Indeed-Id TMS необходимо ввести команду вида:

IndeedID.TMS.Manager.exe /synchronize --serial <номер> --otp <значение 1> --otp2 <значение 2> --window <значение>

Пример:

IndeedID.TMS.Manager.exe /synchronize --serial 0002-0007145B --otp 249300 --otp2 485554 --window 1000

Параметры:

- **serial** – серийный номер устройства, нанесенный на задней поверхности корпуса (может быть указан как без разделителя «-», так и с разделителем «-»)
- **otp и otp2** – значения одноразового пароля

Для получения значения **otp** необходимо однократно нажать на кнопку, расположенную на корпусе устройства:

Для получения значения **otp2** необходимо нажать на кнопку спустя 20 секунд после первого нажатия.

- **window** – интервал значения счетчика (от 0 до 10000)

При успешной синхронизации в строке результата отображается сообщение, содержащее точную дату и время синхронизации:

```
C:\Program Files\Indeed-ID\IMS>IndeedID.IMS.Manager.exe /info
Registered tokens count: 2

Serial          :  00020007145B
Registered on   :  10/26/2010 12:53:31 PM
Enabled         :  yes
Forcibly synchronized on           :  10/26/2010 1:01:06 PM
Last successfull OTP validation on :  Never
Last failed OTP validation on      :  Never
-----------------------------------------------

Serial          :  00020009AF1D
Registered on   :  10/26/2010 12:53:31 PM
Enabled         :  yes
Forcibly synchronized on           :  Never
Last successfull OTP validation on :  Never
Last failed OTP validation on      :  Never
-----------------------------------------------
```