

Indeed-Id Futronic Provider

Руководство по установке и эксплуатации



© Компания «Индид», 2009 – 2018. Все права защищены.

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

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

Оглавление

Введение	4
Условные обозначения	4
О компоненте Indeed-Id Futronic Provider	4
Работа с Indeed-Id Futronic Provider	5
Регистрация аутентификатора	5
Аутентификация при помощи Indeed-Id Futronic Provider	10
Управление аутентификаторами	11
Установка и настройка Indeed-Id Futronic Provider	12
Установка компонента	12
Настройка параметров аутентификации	13

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 Futronic 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 Futronic Provider

Indeed-Id Futronic Provider предназначен для совместного использования с продуктами Indeed-Id Windows Logon и Indeed-Id Enterprise SSO.

Компонент Indeed-Id Futronic Provider необходим для аутентификации пользователей с применением биометрического сканера Futronic FS80. Получить подробную информацию об устройствах Futronic вы можете на официальном сайте компании [Futronic Technologies](https://www.futronic.com).

Работа с Indeed-Id Futronic 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 Futronic 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 аутентификаторами** нажмите **Продолжить** (Рисунок 1а).

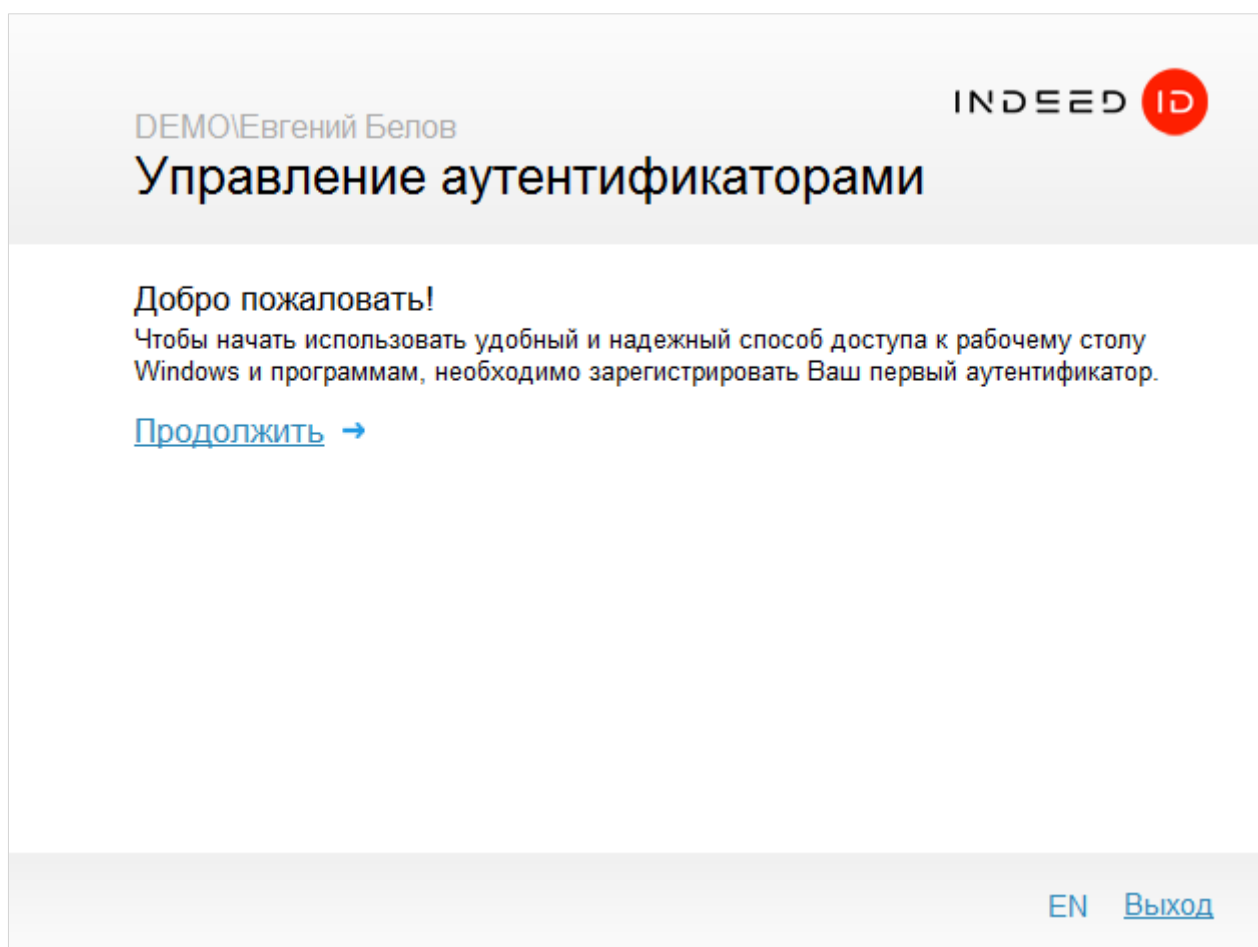


Рисунок 1а.

Если на рабочей станции пользователя установлено несколько провайдеров аутентификации, то необходимо выбрать **Палец (Futronic)** из списка (Рисунок 1b). Если на компьютере установлен только один провайдер, окно выбора не отображается.

Управление аутентификаторами

Добро пожаловать!

Чтобы начать использовать удобный и надежный способ доступа к рабочему столу Windows и программам, необходимо зарегистрировать Ваш первый аутентификатор.

Выберите технологию аутентификации:

[Одноразовая матрица](#) →

(Indeed-Id OTM)

[Палец](#) →

(Futronic)

EN [Выход](#)

Рисунок 1b.

Подключите считыватель к компьютеру и приложите к нему палец (Рисунок 1c). Регистрация аутентификатора производится по трем отпечаткам одного пальца для более точного формирования шаблона. Следуя подсказкам мастера обучения, уберите палец со сканера и затем приложите его еще 2 раза (Рисунок 1d).

Управление аутентификаторами



Приложите палец к сканеру

[← Вернуться](#)

EN [Выход](#)

Рисунок 1с.

Управление аутентификаторами



Приложите тот же палец к сканеру еще раз

[← Вернуться](#)

EN [Выход](#)

Рисунок 1d

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

DEMO\Евгений Белов

INDEED ID

Управление аутентификаторами



Новый аутентификатор успешно обучен

Все готово для регистрации аутентификатора в системе.
Перед сохранением вы можете задать комментарий к аутентификатору:

Сохранить

[EN](#) [Выход](#)

Рисунок 1е

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 Futronic 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 **Палец**.



Рисунок 2.

Подключите биометрический сканер к компьютеру и приложите к нему палец (Рисунок 2). В случае успешного входа по аутентификатору, способ входа **Палец** 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 Futronic Provider

Установка компонента

В этом разделе содержатся сведения по установке и настройке Indeed-Id Futronic Provider. Установку Indeed-Id Futronic 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 сканера



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



Для развертывания Indeed-Id Futronic 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 Futronic Provider

1. Запустите файл IndeedID.Futronic.Provider.msi¹ 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 инсталлятор IndeedID.Futronic.Providerx64.msi.

Настройка параметров аутентификации

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



Перед настройкой групповой политики необходимо добавить в список административных шаблонов шаблоны политик Indeed-Id. Административный файл шаблона политики IndeedID.Futronic.Provider_1049.adm входит в состав дистрибутива и расположен в каталоге Misc.

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

Политика **Минимально допустимое качество шаблона при обучении** определяет, каким должно быть минимально приемлемое качество шаблона отпечатка пальца при обучении. Качество шаблона задается целым числом от 1 до 10, где 10 соответствует максимально возможному качеству шаблона.

Для достижения максимального качества шаблона при обучении необходимо прикладывать палец к сканеру аккуратно и не меняя положения пальца относительно сканера. Политика должна быть определена на клиентах системы, где происходит обучение аутентификаторов, то есть на рабочих станциях пользователей, на которых установлены клиентские компоненты системы. Если политика не определена, по умолчанию используется значение 3.

Политика **Максимально допустимый FAR** определяет максимально допустимое значение FAR (False Acceptance Rate) при сравнении шаблонов отпечатков. Задается целым числом от 1 до 1000. Значение 1 соответствует самому «мягкому» сравнению, когда вероятность сравнить разные шаблоны и получить положительный результат максимальна. Значение 1000 соответствует самому «жесткому» сравнению, когда такая вероятность минимальна. Если задано слишком большое значение параметра, это может привести к частым ошибкам, связанным с отказом легитимным пользователям. Политика должна быть определена на всех серверах Indeed-Id. Если политика не определена, значением по умолчанию является 250.



Значение FRR (False Rejection Rate – отказ в доступе легитимному пользователю) не регулируется политикой. На этот параметр влияют значения FAR и качества шаблона. Если будет слишком высокий порог FAR и слишком низкое качество шаблона при регистрации аутентификатора, то FRR при этом будет очень высоким. Это приведет к тому, что с очень большой вероятностью такого пользователя система не аутентифицирует по верному отпечатку.

Для распространения данных групповых политик на рабочие станции пользователей и на серверы Indeed-Id, рекомендуется создать два отдельных объекта групповых политик, один из которых будет распространяться на рабочие станции и содержать в себе настройки политики **Минимально допустимое качество шаблона при обучении**, а второй будет распространять свое действие на все серверы Indeed-Id и содержать в себе настройки политики **Максимально допустимый FAR**.



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