# Indeed-Id

# Windows<sup>®</sup> Logon

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 http://indeed-id.ru/ служба поддержки пользователей

web-сайт компании

# Оглавление

Оглавление	2
Введение	5
Условные обозначения	5
Базовые термины и понятия	5
О программном комплексе Indeed Enterprise Authentication	6
Модули Indeed Enterprise Authentication	6
Возможности Indeed-Id Windows® Logon Дополнительные возможности Поддерживаемые технологии аутентификации	<b>7</b> 7 7
Функционирование Indeed-Id Windows® Logon Регистрация первого аутентификатора Доступ в систему по аутентификатору Кэширование аутентификаторов пользователя Смена пароля пользователем	<b>8</b> 8 9 9
Установка Indeed-Id Windows® Logon Аппаратные требования к рабочим станциям пользователей Поддерживаемые операционные системы Требования к окружению Требуемые административные права	<b>10</b> 10 10 10 10
Установка Indeed-Id Windows® Logon	11
Настройки межсетевого экрана	11
Удаление и обновление Indeed-Id Windows® Logon	12
Работа с Indeed-Id Windows® Logon	13
Первый вход в систему Работа в Microsoft Windows XP/Microsoft Windows Server 2003 Работа в Microsoft Windows Vista/Microsoft Windows 7 Работа в Microsoft Windows 8.1	<b>13</b> 14 18 18
Регистрация первого аутентификатора	19
Вход в систему с использованием аутентификатора Работа в Microsoft Windows XP/Windows Server 2003 Работа в Microsoft Windows Vista/Windows 7 Работа в Microsoft Windows 8.1	<b>22</b> 23 27 31
Доступ к удаленному рабочему столу с использованием аутентификатора	35
Вход в систему при отсутствии сети	35
Управление аутентификаторами	36
Добавление аутентификатора	38
Редактирование аутентификатора	42

Проверка аутентификатора	44
Удаление аутентификатора	47
Indeed-Id Paste	48
Run as administrator	49
Таблица сообщений журнала подключения	51
Сбор программных логов	56
Часто задаваемые вопросы	56

## Введение

Приветствуем вас и благодарим за приобретение программного комплекса Indeed Enterprise Authentication. Данное Руководство описывает способы аутентификации в операционной системе по технологии Indeed-Id, операции управления аутентификаторами и дополнительные возможности Indeed-Id Windows® Logon.

## 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.

#### Базовые термины и понятия

В рамках системы Indeed-Id используются следующие термины, связанные с продуктом Indeed-Id Windows® Logon:

- Indeed-Id Управление аутентификаторами приложение компонентов Indeed-Id Windows® Logon и Indeed-Id ESSO Agent. Приложение позволяет выполнять регистрацию, перерегистрацию, проверку и удаление аутентификаторов.
- Пользователь Indeed-Id доменный пользователь, для которого разрешено использование технологии аутентификации Indeed-Id.

# О программном комплексе Indeed Enterprise Authentication

Программный комплекс **Indeed Enterprise Authentication** обеспечивает безопасность вашей информации, предоставляя возможность отказаться от использования пароля и получать доступ к данным, подтверждая свою личность с помощью современных средств аутентификации.

Система **Indeed-Id** является модульным решением, состоящим из законченных продуктов и легко адаптируемым в соответствии с индивидуальными требованиями к информационной безопасности.

# Модули Indeed Enterprise Authentication

Основным модулем Indeed Enterprise Authentication является **Indeed-Id Enterprise Server**. Данный продукт обеспечивает:

- Централизованное хранение аутентификаторов, паролей и настроек пользователей.
- Централизованное управление и администрирование.
- Централизованный прием и обработку запросов от других модулей системы.
- Централизованный сбор и аудит событий.
- Координирование действий отдельных модулей и системы в целом.

Количество устанавливаемых серверов определяется в соответствии с индивидуальными требованиями к масштабируемости и отказоустойчивости системы. В среднем, рекомендуется устанавливать 1 сервер на ~400 пользователей. В качестве типового средства хранения данных и настроек используется Active Directory без расширения схемы.

К дополнительным компонентам системы относятся:

- Indeed Enterprise Management Console. WEB-приложение для управления системой.
- **Indeed Admin Pack**. Позволяет осуществлять централизованное администрирование параметрами системы Indeed при помощи набора специализированных утилит.
- Indeed Enterprise Authentication. Обеспечивает возможность доступа в систему с использованием аутентификаторов и выполняет синхронизацию паролей.
- Indeed-Id Providers (Провайдеры Indeed). Реализуют различные технологии аутентификации при доступе в систему и приложения и обеспечивают взаимодействие модулей Indeed EA/ESSO с используемыми устройствами аутентификации и пользователем.
- **Indeed-Id Enterprise SSO Агент**. Обеспечивает возможность единого доступа в приложения с использованием аутентификатора.
- **Indeed-Id Rule System**. Обеспечивает взаимодействие модуля Indeed Enterprise Authentication с системами контроля и управления доступом (СКУД).
- Indeed-Id Enterprise SSO TMS/SAM Connector. Обеспечивает взаимодействие Indeed Enterprise Authentication с системой централизованного управления Aladdin TMS/SAM.
- **Indeed IIS Extension**. Обеспечивает возможность аутентификации пользователей в webприложениях, развернутых на платформе Microsoft Internet Information Services (IIS) с использованием технологии аутентификации Indeed.

# Возможности Indeed-Id Windows® Logon

Продукт Indeed-Id Windows® Logon предоставляет пользователям следующие возможности:

- Доступ в операционную систему по паролю учетной записи
- Доступ в операционную систему с применением технологии аутентификации Indeed-Id
- Доступ к удаленному рабочему столу с применением технологии аутентификации Indeed-Id
- Доступ в операционную систему по кэшированному аутентификатору при отсутствии связи с сервером Indeed.

С целью обеспечения безопасности данных во время отсутствия пользователя на рабочем месте Indeed-Id Windows® Logon поддерживает как ручную блокировку рабочей станции, так и автоматическую блокировку (при извлечении устройства аутентификации или использовании экранной заставки). Независимо от способа блокировки для разблокирования рабочей станции всегда требуется повторное подтверждение личности пользователя с помощью аутентификатора.

#### Дополнительные возможности

Дополнительные возможности, предоставляемые продуктом Indeed-Id Windows® Logon, включают:

- Возможность самостоятельного регистрации аутентификаторов и управления ими с помощью приложения **Indeed-Id Управление аутентификаторами**.
- Функцию **Indeed-Id Paste** автоматическая подстановка пароля в скрытом виде в нужное поле при нажатии определенной комбинации "горячих клавиш".

#### Поддерживаемые технологии аутентификации

Продукт Indeed-Id Windows® Logon поддерживает более 20 современных технологий аутентификации. К ним относятся двухфакторная аутентификация, биометрическая аутентификация, сертификаты, бесконтактные карты, одноразовые пароли, sms-технологии и др.

Для каждой категории пользователей системы Indeed-Id Windows® Logon может быть подобрана собственная оптимальная технология аутентификации. Также пользователям может быть разрешено применение несколько технологий:

- технология аутентификации, адаптированная для работы в удаленном режиме;
- комбинация технологий аутентификации (мультифакторная аутентификация).

# Функционирование Indeed-Id Windows® Logon

Данный раздел содержит описание основных сценариев функционирования Indeed-Id Windows® Logon:

- Регистрация первого аутентификатора
- Доступ в систему по аутентификатору
- Кэширование аутентификаторов пользователя
- Смена пароля пользователем

#### Регистрация первого аутентификатора

Работа в системе Indeed-Id Windows® Logon начинается с регистрации первого аутентификатора. Для регистрации первого аутентификатора служит приложение **Indeed-Id – Управление аутентификаторами** (IndeedID.User.Enroller.exe). Ниже приведено краткое описание процесса регистрации:

- Пользователь проходит аутентификацию с использованием пароля. После успешной аутентификации пользователь может зарегистрировать один или более аутентификаторов.
- При добавлении пользователем первого аутентификатора сервер Indeed-Id выполняет проверку, разрешена ли для данного пользователя автоматическая генерация пароля учетной записи.
- Если генерация случайного пароля разрешена, сервер генерирует новый случайный пароль и устанавливает его для учетной записи пользователя. С этого момента пользователь не знает свой новый пароль и единственным способом входа в систему становится вход по аутентификатору.
- Если генерация случайного пароля не разрешена, то пароль учетной записи пользователя не изменяется и для входа в систему пользователь может использовать как пароль, так и обученные аутентификаторы.



Управление аутентификаторами (регистрация, перерегистрация, удаление) при входе в систему по паролю возможно только в том случае, если в момент аутентификации по паролю у пользователя не было ни одного ранее зарегистрированного аутентификатора.

Если у пользователя уже имеются ранее обученные аутентификаторы, для управления аутентификаторами ему необходимо аутентифицироваться, используя один из них.

При аутентификации пользователя по паролю, функция генерации случайного пароля не срабатывает.

#### Доступ в систему по аутентификатору

После регистрации первого аутентификатора пользователь получает возможность использовать аутентификаторы для доступа в систему. Доступ в систему по аутентификатору обеспечивается компонентом Indeed-Id Windows® Logon. После установки на рабочую станцию пользователя Indeed-Id Windows® Logon выполняет функции стандартного клиента Windows, дополняя их возможностью применения технологии аутентификации Indeed-Id. Процедура получения доступа в систему выглядит следующим образом:

- Пользователь проходит аутентификацию по одному из обученных аутентификаторов.
- После успешной аутентификации компонент Indeed-Id Windows® Logon запрашивает у модуля Indeed-Id Server пароль учетной записи и использует его для стандартной (парольной) аутентификации пользователя на Контроллере Домена. Таким образом, процедура аутентификации происходит без явного для пользователя запроса пароля учетной записи.

#### Кэширование аутентификаторов пользователя

Для обеспечения возможности работы пользователей при отсутствии доступа к сети в составе программного комплекса Indeed Enterprise Authentication предусмотрена возможность кэширования данных пользователя на локальной рабочей станции. Возможность кэширования включается для каждого пользователя администратором системы. Ниже приведено краткое описание процесса доступа в систему при разрешенном и запрещенном кэшировании аутентификаторов:

- Если для пользователя разрешено кэширование данных, при каждом входе в систему по аутентификатору происходит явное для пользователя сохранение данных в локальном кэше (предлагается выполнить кэширование аутентификаторов). Если пользователю было запрещено кэширование, происходит очистка локального кэша.
- При попытке входа в систему при отсутствии связи с серверами Indeed выполняется поиск данных пользователя в локальном кэше. Если эти данные найдены (ранее было разрешено и выполнено кэширование), у пользователя запрашивается аутентификатор и происходит аутентификация на локальной рабочей станции. Если данные не обнаружены (кэширование аутентификаторов запрещено), пользователь не может выполнить вход в систему по аутентификатору. При этом генерируется сообщение об ошибке: "Ошибка при входе в систему. Сервер не найден. Кэширование данных пользователя запрещено" или "Сервер не найден".

При включении кэширования в свойствах пользователя и последующем входе/разблокировке по аутентификатору отображается сообщение о том, что аутентификатор сохранен в кэше. Также это сообщение должно отображаться при добавлении нового аутентификатора и при изменении аутентификатора.

При отключении кэширования в свойствах пользователя и последующем входе/разблокировке по аутентификатору отображается сообщение о том, что кэширование отключено.

#### Смена пароля пользователем

Если текущее значение пароля известно пользователю, а генерация случайного пароля для его учетной записи не разрешена, пользователь может самостоятельно сменить пароль (например, если заканчивается срок действия текущего пароля). Синхронизацию пароля при его смене пользователем осуществляет компонент Indeed-Id Windows® Logon. Ниже приведено краткое описание процесса смены пароля:

- Пользователь выполняет смену пароля учетной записи обычным способом (например, через Диспетчер задач).
- Компонент Indeed-Id Windows® Logon фиксирует событие смены пароля и передает запрос на смену пароля серверу Indeed-Id.
- Сервер Indeed-Id обновляет пароль учетной записи в хранилище данных.

# Установка Indeed-Id Windows® Logon

Базовая конфигурация системы Indeed EA включает основной модуль программного комплекса **Indeed-Id Server**, модули **Indeed-Id Windows® Logon**, **Indeed-Id Admin Pack**, **Indeed EMC** и компонент **Indeed-Id Provider**, соответствующий выбранному типу аутентификации. При необходимости конфигурация системы может быть расширена дополнительными модулями программного комплекса Indeed Enterprise Authentication.

#### Аппаратные требования к рабочим станциям пользователей

- Не менее 50 МБ свободного дискового пространства
- Аппаратные требования совпадают с требованиями, предъявляемыми к операционным системам, на которых функционирует ПО

#### Поддерживаемые операционные системы

- Windows XP SP2 64 bit, SP3 32bit
- Windows Vista SP2 32/64bit
- Windows 7 SP1 32/64bit
- Windows 8.1 32/64bit
- Windows 10 32/64bit
- Windows Server 2003/2003 R2 SP2 32/64bit
- Windows Server 2008 SP2 32/64bit
- Windows Server 2008 R2 SP1
- Windows Server 2012/2012 R2
- Windows Server 2016

#### Требования к окружению

Для корректной работы Indeed-Id Windows® Logon необходимо следующее окружение:

• Настроенный DNS сервер (необходимо добавление Reverse lookup zones). Параметры DNS сервера необходимо указать в настройках сетевого подключения на каждой рабочей станции.

#### Требуемые административные права

Для установки Indeed-Id Windows® Logon требуются права **Локального Администратора** (Adminstrator).

# Установка Indeed-Id Windows® Logon



Для развертывания Indeed-Id Windows® Logon 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 компонента Indeed-Id Windows® Logon запустите программу установки **IndeedID.WindowsLogon.msi**<sup>1</sup> и следуйте указаниям Мастера установки.

После завершения установки компонента необходима перезагрузка системы. Нажмите **Да**, чтобы выполнить перезагрузку сразу, или **Нет**, чтобы сделать это позднее вручную.

## Настройки межсетевого экрана

Для корректной работы системы Indeed-Id необходимо изменить следующие настройки межсетевого экрана на Indeed-Id Server и на рабочих станциях, на которых установлен компонент Indeed-Id Windows® Logon:

- 1. Открыть порт 53 (DNS) (TCP и UDP) для всех процессов в обоих направлениях. Этот порт используется системой Indeed-Id для определения наличия сети.
- 2. Открыть порт 3268 (Microsoft Global Catalog) (TCP) для всех процессов в обоих направлениях. Этот порт используется системой Indeed-Id для поиска серверов Indeed.
- 3. Если при установке Indeed-Id Server была выбрана опция **Использовать статический порт**, необходимо **открыть заданный порт** (по умолчанию **23809**) **(TCP)** для всех процессов в обоих направлениях. Этот порт используется системой Indeed-Id для коммуникации между рабочими станциями пользователей и Indeed-Id Server.
- 4. Запретить **IPS (Intrusion Prevention System)**. При разрешенном IPS межсетевым экраном блокируется исходящий запрос на неизвестный DCOM интерфейс. В этом случае соединение с сервером Indeed-Id не будет установлено.
- 5. Открыть порт 135 (RPC) для всех процессов в обоих направлениях. Этот порт используется системой для коммуникации между рабочими станциями пользователей и Indeed-Id Server.
- 6. **Открыть порт 389 (LDAP)** для всех процессов в обоих направлениях. Этот порт используется системой для получения доступа в Active Directory (в т.ч. при поиске Indeed-Id Server).

<sup>&</sup>lt;sup>1</sup> Для установки на 64-битных ОС следует использовать инсталлятор IndeedID.WindowsLogon.x64.msi

# Удаление и обновление Indeed-Id Windows® Logon

Удаление/восстановление продукта осуществляется стандартным для поддерживаемых ОС способом, через меню Панель управления.



Для удаления Indeed-Id Windows® Logon требуются права локального администратора. После удаления пакета **Indeed-Id Windows® Logon** требуется перезагрузка системы.

Для обновления не требуется удалять текущую версию. При установке новой версии ранее установленные компоненты заменяются новыми.



Для обновления Indeed-Id Windows® Logon на рабочих станциях пользователей в автоматическом режиме удобно использовать механизм групповых политик (Microsoft Group Policy) или использовать для этих целей развернутый в организации Microsoft System Center Configuration Manager.

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

# Работа с Indeed-Id Windows® Logon

Для обеспечения доступа в систему с использованием технологии аутентификации Indeed-Id на вашем рабочем месте должны быть установлены:

- Модуль Indeed-Id Windows® Logon, обеспечивающий возможность доступа в систему по аутентификатору.
- Модуль Indeed-Id Provider, соответствующий выбранной технологии аутентификации.
- Аппаратное устройство аутентификации (в случае необходимости).

Возможности входа в систему по аутентификатору и управления аутентификаторами доступны только при наличии разрешения, установленного администратором системы.

# Первый вход в систему

После установки необходимого программного обеспечения на ваш компьютер первый вход в систему осуществляется по паролю учетной записи.

Смотрите далее:

- Работа в Microsoft Windows XP/Microsoft Windows Server 2003
- Работа в Microsoft Windows Vista/Microsoft Windows 7
- Работа в Microsoft Windows 8.1

## Работа в Microsoft Windows XP/Microsoft Windows Server 2003

После загрузки операционной системы отображается окно приветствия Windows. Нажмите комбинацию клавиш **Ctrl+Alt+Del** (Рисунок 1).



Рисунок 1 – Окно входа в операционную систему Windows XP.

В открывшемся окне **Bxog в Windows** отображается имя пользователя, выполнявшего вход в систему последним, и используемый им способ входа. Выполните одно из следующих действий:

1. В окне **Вход в Windows** выберите способ входа **Пароль**, затем введите свой пароль и нажмите **Вход** (Рисунок 2).

Bход в Windows	
<b>Евгений Белов</b> (DEMO\Евгений Белов) Введите свой пароль	
<ul> <li>→ Выбрать другого пользователя</li> <li>→ Сменить способ входа</li> </ul>	
Завершить работу системы	RU <u>Отмена</u>

Рисунок 2 – Окно «Вход в Windows» компонента Indeed-Id Windows® Logon.

2. Если необходимо изменить имя учетной записи, нажмите **Выбрать другого** пользователя (Рисунок 3), затем выберите имя учетной записи, введите пароль и нажмите **Вход**.

Bход в Windows	
<ul> <li>→ <u>Аdministrator</u> (DEMO\Administrator)</li> <li>→ <u>Евгений Белов</u> (DEMO\Eвгений Белов)</li> <li>→ <u>Irina Stepanova</u> (DEMO\Stepanova.Irina)</li> <li>→ <u>Другой пользователь</u></li> </ul>	
Завершить работу системы	RU <u>Отмена</u>

Рисунок 3 – Выбор пользователя для входа в операционную систему.

Если для вашей учетной записи разрешена регистрация аутентификаторов, то при входе в систему запустится «Мастер первого входа» (Рисунок 4) и предложит зарегистрировать аутентификатор.



Мастер первого входа отображается только при условии, что вы являетесь лицензированным пользователем Indeed-Id и имеете разрешение на использование технологии аутентификации Indeed-Id. Для получения подробной информации обратитесь к администратору системы.

DEMO\Евгений Белов 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:	
<u>Карта</u> → (HID OMNIKEY Smart Card Reader) <u>Карта</u> → (Z2 USB Card Reader)	* II
<u>Карта + PIN</u> → (HID OMNIKEY Smart Card Reader) <u>Карта + PIN</u> → (Z2 USB Card Reader) <u>Одноразовая матрица</u> →	Ŧ
RU <u>Выхо</u>	<u>ם</u>

Рисунок 4 – «Мастер первого входа» компонента Indeed-Id Windows® Logon.

Вы можете зарегистрировать аутентификатор сразу или позднее в любое удобное время.

- Чтобы перейти к регистрации аутентификатора, в окне Управление аутентификаторами выберите один из доступных способов аутентификации (например, «Одноразовая матрица»).
- Чтобы выполнить вход в систему без регистрации аутентификатора, нажмите **Выход**. В этом случае Мастер первого входа будет отображаться при каждом следующем входе в систему до регистрации первого аутентификатора.

Смотрите также: Регистрация первого аутентификатора.

Если на рабочей станции не найдены необходимые провайдеры Indeed-Id, регистрация аутентификаторов невозможна (Рисунок 5). При отображении данного сообщения обратитесь к администратору системы.



## Работа в Microsoft Windows Vista/Microsoft Windows 7

После загрузки операционной системы отображается экран приветствия Windows. Нажмите комбинацию клавиш **Ctrl+Alt+Del**.

Выберите вашу учетную запись. Если необходимо выполнить вход от имени другой учетной записи, нажмите **Другой пользователь** (Рисунок 6).

DEMO\Ivanova.Maria	7X64CLIENT\Administrator	DEMO\livanov.livan	Другой пользователь
	Отме	на	

Рисунок 6 – Окно входа в операционную систему Windows 7.

Далее следуйте инструкциям в пп. 1-2 раздела Работа в Microsoft Windows XP/Microsoft Windows Server 2003.

#### Работа в Microsoft Windows 8.1

После загрузки операционной системы перейдите на экран выбора пользователя.

Выберите вашу учетную запись. Если необходимо изменить имя учетной записи, нажмите **Другой** пользователь (Рисунок 7).



Рисунок 7 – Окно входа в операционную систему Windows 8.1.

Далее следуйте инструкциям в пп. 1-2 раздела Работа в Microsoft Windows XP/Microsoft Windows Server 2003.

## Регистрация первого аутентификатора

Если пользователю разрешено использовать технологию аутентификации Indeed-Id, то после входа на рабочую станцию по доменному паролю ему будет предложено зарегистрировать свой первый аутентификатор. Для этого необходимо выбрать способ аутентификации и следовать инструкциям Мастера регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного способа аутентификации (Рисунок 8).

- Выполните необходимые действия следуя подсказкам в окне **Управление** аутентификаторами.
- Если вы хотите вернуться на предыдущую страницу и выбрать другой способ входа, нажмите **Вернуться**.



Рисунок 8 – Пример регистрации аутентификатора One Time Matrix.

После выполнения необходимых действий по регистрации в окне **Управление** аутентификаторами отображается сообщение **"Новый аутентификатор успешно обучен"** (Рисунок 9).

Вы можете добавить произвольный текстовый комментарий к зарегистрированному аутентификатору (если данное действие разрешено администратором системы). Для завершения регистрации аутентификатора нажмите **Сохранить**.

DEMO\Евген Управле	ий Белов ение аутентификаторами	
	Новый аутентификатор успешно обуч Все готово для регистрации аутентификатора в с Перед сохранением вы можете задать коммента к аутентификатору: Сохранить	НӨН системе. арий
		EN <u>Выход</u>

Рисунок 9 – Сохранение аутентификатора и комментария к нему.

Тип зарегистрированного аутентификатора и комментарий к нему отображаются в окне Управление аутентификаторами. Если для учетной записи пользователя разрешено добавление нескольких аутентификаторов, то вы можете перейти к их регистрации, нажав на ссылку **Добавить способ входа**. Также вы можете изменить, проверить или удалить зарегистрированный аутентификатор (если данные действия разрешены администратором системы).

 $\bigcirc$ 

При использовании определенных моделей биометрических устройств (например, сканеров отпечатков пальцев Digent IZZIX FD 2000, FD/FM 1000) возможны ошибки при регистрации и распознавании аутентификатора, связанные с уровнем чувствительности сканера и индивидуальными особенностями человека (температура тела, уровень влажности кожи, способ прикладывания пальца). Во избежание таких ошибок рекомендуется проверять аутентификатор сразу после регистрации.

При следующем входе в систему будет доступен способ входа по зарегистрированному аутентификатору.

Если для вашей учетной записи разрешена генерация случайного пароля, то после регистрации первого аутентификатора в окне **Управление аутентификаторами** отображается сообщение (Рисунок 10):

DEM Уп	Ю\Евгений Белов равление аутентификато	овеемі рами
<b></b>	Вашей учетной записи был автоматически сген Старый пароль более не действителен. Для вхо обученный аутентификатор.	ерирован случайный пароль. Эда в домен используйте
← <u>Верн</u>	<u>іуться</u>	Выход

Случайный пароль для учетной записи будет сгенерирован по истечении срока действия текущего пароля. Если для вашей учетной записи был сгенерирован случайный пароль, то

текущего пароля. Если для вашеи учетной записи был сгенерирован случайный пароль, то следующий вход в систему возможен только с использованием аутентификатора.

Если для учетной записи разрешено кэширование аутентификаторов, то при последующем входе в систему по аутентификатору будет выполнено сохранение аутентификатора в локальную память компьютера. В дальнейшем вы сможете выполнять доступ в систему по кэшированному аутентификатору при отсутствии подключения к серверам Indeed.

## Вход в систему с использованием аутентификатора



Этот способ входа доступен при условии, что вы являетесь лицензированным пользователем Indeed-Id, для вашей учетной записи разрешено регистрация аутентификаторов и вы уже зарегистрировали хотя бы один аутентификатор.

Смотрите далее:

- Работа в Microsoft Windows XP/Windows Server 2003
- Работа в Microsoft Windows Vista/Windows 7
- Работа в Microsoft Windows 8.1

## Работа в Microsoft Windows XP/Windows Server 2003

Для входа в систему по аутентификатору выполните следующие действия:

Нажмите комбинацию клавиш **Ctrl+Alt+Del** после загрузки операционной системы (Рисунок 11):



Рисунок 11 – Окно входа в операционную систему Windows XP.

В открывшемся окне **Вход в Windows** отображается имя пользователя, выполнявшего вход в систему последним и используемый им способ входа (Рисунок 12).

Вход в Windows	
<b>Евгений Белов</b> (DEMO\Евгений Белов) Введите свой пароль Вход	
<ul> <li>→ Выбрать другого пользователя</li> <li>→ Сменить способ входа</li> </ul>	
Завершить работу системы	RU <u>Отмена</u>

Рисунок 12 – Окно «Вход в Windows» компонента Indeed-Id Windows® Logon.

Если вы хотите сменить учетную запись, нажмите **Выбрать другого пользователя** и выберите нужную учетную запись.

Если вы хотите выбрать другой способ входа, нажмите **Сменить способ входа** и выберите один из способов входа, соответствующий зарегистрированному ранее аутентификатору (Рисунок 13).

Bход в Windows	
<b>Евгений Белов</b> (DEMO\Евгений Белов)	
→ <u>Пароль</u>	×
→ Смарт-карта или USB-ключ (Смарт-карта или USB-клю	94)
→ <u>Смарт-карта или USB-ключ + PIN</u> (Смарт-карта или U	JSB-ключ + PIN)
→ <u>Электронный ключ</u> (iButton Reader)	E
Электронный ключ + PIN (iButton Reader + PIN)	
→ Выбрать другого пользователя	•
Завершить работу системы	RU <u>Отмена</u>

Рисунок 13 – Выбор способа аутентификации из числа установленных провайдеров Indeed-Id.

Чтобы выполнить вход в систему, необходимо предоставить зарегистрированный аутентификатор. Внешний вид окна аутентификации и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.



Если администратором установлено требование на смену пароля и разрешена генерация случайного пароля, при входе в систему будет автоматически сгенерирован случайный пароль. При этом отображается сообщение об успешной автоматической смене пароля (Рисунок 14а):

Change	Password 🛛 🔀
٩	Пароль был автоматически изменен.
	ок

Рисунок 14а – Сообщение об автоматическом изменении пароля в Windows XP.

Если доменный пароль был сброшен администратором системы при хотя бы одном зарегистрированном аутентификаторе, то при входе в систему по этому аутентификатору

отобразится предупреждение о рассинхронизации пароля. Пользователю потребуется ввести и подтвердить новый доменный пароль (Рисунок 14b).

Синхронизация п	ароля	×
Ошибка при входе Произошла нешта	е в систему. тная ситуация: рассинхронизация пароля.	
Для исправления про администратором ил	облемы введите пароль, установленный системным и обратитесь к администратору Indeed-ID.	
Новый пароль:		
Подтверждение:		
	ОК Отмена	

Рисунок 14b – Сообщение о рассинхронизации пароля в Windows XP.

Если запрос на изменение пароля произойдет в момент, когда ни один из серверов Indeed не будет доступен (но при этом будет доступен хотябы один контроллер домена), то после ввода нового пароля пользователем также появится сообщение о рассинхронизации пароля, т.к. новый пароль, установленный пользователем, невозможно будет синхронихировать с хранилищем данных Indeed (Рисунок 14с).

Сменаг	ароля 🔀
2	Ошибка связи с сервером.
	Если Вы продолжите, произойдет рассинхронизация пароля. Хотите продолжить?
	OK Cancel

Рисунок 14с – Предупреждение о рассинхронизации пароля в Windows XP.

В этом случае новый доменный пароль необходимо будет синхронизировать с хранилищем данных Indeed при следующем входе в систему с использованием аутентификатора при хотя бы одном доступном сервере Indeed. После успешной синхронизации пароля будет выполнен вход в систему.

#### Автоматическая идентификация

Если на сервере Indeed-Id и на вашей рабочей станции настроена автоматическая идентификация, то для входа в систему указывать пользователя не нужно.



Автоматическая идентификация пользователей поддерживается только провайдерами Автоматическая идентификация пользователей поддерживается следующими провайдерами:

- Indeed-Id Z2USB (+PIN)
- Indeed-Id OMNIKEY (+PIN)
- Indeed-Id OMNIKEY+PalmSecure
- Indeed-Id Smart Card (+PIN)

Для использования автоматической идентификации необходимо зарегистрировать аутентификатор после того, как будет выполнена настройка автоматической идентификации на всех серверах Indeed-Id и рабочей станции пользователя.



Функция автоматической идентификации может быть использована вместе с функцией автоматического завершения сеанса пользователя, если другой пользователь предоставит свой аутентификатор. Для настройки автоматической идентификации и автоматического завершения сеанса пользователя обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf.* 

Выберите **Автоматическая идентификация** и приложите ранее зарегистрированный аутентификатор к считывателю (Рисунок 15).



## Работа в Microsoft Windows Vista/Windows 7

Для доступа в систему по аутентификатору выполните следующие действия:

После загрузки операционной системы отображается экран приветствия Windows. Нажмите комбинацию клавиш **Ctrl+Alt+Del**. Выберите вашу учетную запись. Если необходимо изменить имя учетной записи, нажмите **Другой пользователь** (Рисунок 16).

DEMO\Ivanova.Maria	7X64CLIENT\Administrator	DEMO\Ivanov.Ivan	Другой пользователь
	Отме	на	

Рисунок 16 – Окно входа в операционную систему Windows 7.

В открывшемся окне **Вход в Windows** отображается имя пользователя, выполнявшего вход в систему последним и используемый им способ входа (Рисунок 17).

Bход в Windows	
<b>Евгений Белов</b> (DEMO\Евгений Белов) Введите свой пароль Вход	
→ <u>Сменить способ входа</u>	RU <u>Отмена</u>

Рисунок 17 – Окно «Вход в Windows» компонента Indeed-Id Windows® Logon.

Если вы хотите сменить учетную запись, нажмите **Отмена** и выберите учетную запись нужного пользователя.

Если вы хотите выбрать другой способ входа, нажмите **Сменить способ входа** и выберите один из способов входа, соответствующий зарегистрированному ранее аутентификатору (Рисунок 18).

<ul> <li>Вгений Белов (DEMO\Евгений Белов)</li> <li> Пароль </li> <li> Смарт-карта или USB-ключ (Смарт-карта или USB-ключ) </li> <li> Смарт-карта или USB-ключ + PIN (Смарт-карта или USB-ключ + PIN) </li> <li> Электронный ключ + PIN (Button Reader) </li> <li> Электронный ключ + PIN (Button Reader + PIN)</li></ul>	Bход в Windows	
<ul> <li>→ Пароль</li> <li>→ Смарт-карта или USB-ключ (Смарт-карта или USB-ключ)</li> <li>→ Смарт-карта или USB-ключ + PIN (Смарт-карта или USB-ключ + PIN)</li> <li>→ Электронный ключ (iButton Reader)</li> <li>→ Электронный ключ + PIN (iButton Reader + PIN)</li> </ul>	<b>Евгений Белов</b> (DEMO\Евгений Белов)	
<ul> <li>→ <u>Смарт-карта или USB-ключ</u> (Смарт-карта или USB-ключ)</li> <li>→ <u>Смарт-карта или USB-ключ + PIN</u> (Смарт-карта или USB-ключ + PIN)</li> <li>→ <u>Электронный ключ</u> (iButton Reader)</li> <li>→ <u>Электронный ключ + PIN</u> (iButton Reader + PIN)</li> </ul>	→ <u>Пароль</u>	^
<ul> <li>→ <u>Смарт-карта или USB-ключ + PIN</u> (Смарт-карта или USB-ключ + PIN)</li> <li>→ <u>Электронный ключ + PIN</u> (iButton Reader)</li> <li>→ <u>Электронный ключ + PIN</u> (iButton Reader + PIN)</li> </ul>	→ <u>Смарт-карта или USB-ключ</u> (Смарт-карта или	USB-ключ)
<ul> <li>Электронный ключ (iButton Reader)</li> <li>Электронный ключ + PIN (iButton Reader + PIN)</li> </ul>	→ <u>Смарт-карта или USB-ключ + PIN</u> (Смарт-кар	рта или USB-ключ + PIN)
→ Электронный ключ + PIN (iButton Reader + PIN)	⇒ <u>Электронный ключ</u> (iButton Reader)	E
	Электронный ключ + PIN (iButton Reader + PIN)	D
		RU Отмена
RU Otmen:		Tto <u>omicia</u>

Рисунок 18 – Выбор способа аутентификации из числа установленных провайдеров Indeed-Id.

Чтобы выполнить вход в систему, необходимо предоставить зарегистрированный аутентификатор. Внешний вид окна аутентификации и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.



Если администратором системы установлено требование на смену пароля и разрешена генерация случайного пароля, при входе в систему будет автоматически сгенерирован случайный пароль. При этом отображается сообщение об успешной автоматической смене пароля (Рисунок 19а):



Рисунок 19а – Сообщение об автоматическом изменении пароля в Windows 7.

Если доменный пароль был сброшен администратором системы при хотя бы одном зарегистрированном аутентификаторе, то при входе в систему по этому аутентификатору отобразится предупреждение о рассинхронизации пароля. Пользователю потребуется ввести и подтвердить новый доменный пароль (Рисунок 19b).



Рисунок 19b – Сообщение о рассинхронизации пароля в Windows 7.

Если запрос на изменение пароля произойдет в момент, когда ни один из серверов Indeed не будет доступен (но при этом будет доступен хотябы один контроллер домена), то после ввода нового пароля пользователем также появится сообщение о рассинхронизации пароля, т.к. новый пароль, установленный пользователем, невозможно будет синхронихировать с хранилищем данных Indeed (Рисунок 19с).



Рисунок 19с – Предупреждение о рассинхронизации пароля в Windows 7.

В этом случае новый доменный пароль необходимо будет синхронизировать с хранилищем данных Indeed при следующем входе в систему с использованием аутентификатора при хотя бы одном доступном сервере Indeed. После успешной синхронизации пароля будет выполнен вход в систему.

#### Автоматическая идентификация

Если на сервере Indeed-Id и на вашей рабочей станции настроена автоматическая идентификация, то для входа в систему указывать пользователя не нужно. выберите **Автоидентификация** (Рисунок 20) и приложите ранее зарегистрированный аутентификатор к считывателю.



Рисунок 20 – Автоматическая идентификация в Windows 7.

Автоматическая идентификация пользователей поддерживается только провайдерами Indeed-Id Z2USB(+PIN) и Indeed-Id OMNIKEY(+PIN).

Для использования автоматической идентификации необходимо зарегистрировать аутентификатор после того, как будет выполнена настройка автоматической идентификации на всех серверах Indeed-Id и рабочей станции пользователя.



Функция автоматической идентификации может быть использована вместе с функцией автоматического завершения сеанса пользователя, если другой пользователь предоставит свой аутентификатор. Для настройки автоматической идентификации и автоматического завершения сеанса пользователя обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf.* 

## Работа в Microsoft Windows 8.1

Для входа в систему по паролю выполните следующие действия:

После загрузки операционной системы перейдите на экран выбора пользователя. Выберите вашу учетную запись. Если необходимо изменить имя учетной записи, нажмите **Другой пользователь** (Рисунок 21).



Рисунок 21 – Окно входа в операционную систему Windows 8.1.

В открывшемся окне **Вход в Windows** отображается имя пользователя, выполнявшего вход в систему последним и используемый им способ входа (Рисунок 22).

Bход в Windows	
<b>Евгений Белов</b> (DEMO\Евгений Белов) Введите свой пароль Вход	
→ Сменить способ входа	RU <u>Отмена</u>

Рисунок 22 – Окно «Вход в Windows» компонента Indeed-Id Windows® Logon.

Если вы хотите сменить учетную запись, нажмите **Отмена** и выберите учетную запись нужного пользователя.

Если вы хотите выбрать другой способ входа, нажмите **Сменить способ входа** и выберите один из способов входа, соответствующий зарегистрированному ранее аутентификатору (Рисунок 23).

<ul> <li>Вгений Белов (DEMO\Евгений Белов)</li> <li>→ Пароль</li> <li>→ Смарт-карта или USB-ключ (Смарт-карта или USB-ключ)</li> <li>→ Смарт-карта или USB-ключ + PIN (Смарт-карта или USB-ключ + PIN)</li> <li>→ Электронный ключ (iButton Reader)</li> <li>→ Электронный ключ + PIN (iButton Reader + PIN)</li> </ul>	<ul> <li>ВЕГЕНИЙ БЕЛОВ (DEMO\Евгений Белов)</li> <li> Пароль </li> <li> Смарт-карта или USB-ключ (Смарт-карта или USB-ключ) </li> <li> Смарт-карта или USB-ключ + PIN (Смарт-карта или USB-ключ + PIN) </li> <li> Электронный ключ (iButton Reader) </li> <li> Электронный ключ + PIN (iButton Reader + PIN) </li> </ul>	Вход в Windows	
<ul> <li>→ Пароль</li> <li>→ Смарт-карта или USB-ключ (Смарт-карта или USB-ключ)</li> <li>→ Смарт-карта или USB-ключ + PIN (Смарт-карта или USB-ключ + PIN)</li> <li>→ Электронный ключ (iButton Reader)</li> <li>→ Электронный ключ + PIN (iButton Reader + PIN)</li> </ul>	<ul> <li>Пароль</li> <li>Смарт-карта или USB-ключ (Смарт-карта или USB-ключ)</li> <li>Смарт-карта или USB-ключ + PIN (Смарт-карта или USB-ключ + PIN)</li> <li>Электронный ключ (iButton Reader)</li> <li>Электронный ключ + PIN (iButton Reader + PIN)</li> </ul>	<b>Евгений Белов</b> (DEMO\Евгений Белов)	
<ul> <li>→ Смарт-карта или USB-ключ (Смарт-карта или USB-ключ)</li> <li>→ Смарт-карта или USB-ключ + PIN (Смарт-карта или USB-ключ + PIN)</li> <li>→ Электронный ключ (iButton Reader)</li> <li>→ Электронный ключ + PIN (iButton Reader + PIN)</li> </ul>	<ul> <li>→ <u>Смарт-карта или USB-ключ</u> (Смарт-карта или USB-ключ)</li> <li>→ <u>Смарт-карта или USB-ключ + PIN</u> (Смарт-карта или USB-ключ + PIN)</li> <li>→ <u>Электронный ключ</u> (iButton Reader)</li> <li>→ <u>Электронный ключ + PIN</u> (iButton Reader + PIN)</li> </ul>	→ <u>Пароль</u>	
<ul> <li>→ <u>Смарт-карта или USB-ключ + PIN</u> (Смарт-карта или USB-ключ + PIN)</li> <li>→ <u>Электронный ключ + PIN</u> (iButton Reader)</li> <li>→ <u>Электронный ключ + PIN</u> (iButton Reader + PIN)</li> </ul>	<ul> <li>→ <u>Смарт-карта или USB-ключ + PIN</u> (Смарт-карта или USB-ключ + PIN)</li> <li>→ <u>Электронный ключ + PIN</u> (iButton Reader)</li> <li>→ <u>Электронный ключ + PIN</u> (iButton Reader + PIN)</li> </ul>	→ <u>Смарт-карта или USB-ключ</u> (Смарт-карта или	USB-ключ)
<ul> <li>Электронный ключ (iButton Reader)</li> <li>Электронный ключ + PIN (iButton Reader + PIN)</li> </ul>	<ul> <li>Электронный ключ (iButton Reader)</li> <li>Электронный ключ + PIN (iButton Reader + PIN)</li> </ul>	→ <u>Смарт-карта или USB-ключ + PIN</u> (Смарт-ка	рта или USB-ключ + PIN)
→ <u>Электронный ключ + PIN</u> (iButton Reader + PIN)	→ <u>Электронный ключ + PIN</u> (iButton Reader + PIN)	→ <u>Электронный ключ</u> (iButton Reader)	E
		→ <u>Электронный ключ + PIN</u> (iButton Reader + PIN	۹)
			RU <u>Отмена</u>

Рисунок 23 – Выбор способа аутентификации из числа установленных провайдеров Indeed-Id.

Чтобы выполнить вход в систему, необходимо предоставить зарегистрированный аутентификатор. Внешний вид окна аутентификации и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.



Если администратором системы установлено требование на смену пароля и разрешена генерация случайного пароля, при входе в систему будет автоматически сгенерирован случайный пароль. При этом отображается сообщение об успешной автоматической смене пароля (Рисунок 24а):

Ваш пароль был автоматически изменен. ОК

Рисунок 24а – Сообщение об автоматическом изменении пароля в Windows 8.1.

Если доменный пароль был сброшен администратором системы при хотя бы одном зарегистрированном аутентификаторе, то при входе в систему по этому аутентификатору отобразится предупреждение о рассинхронизации пароля. Пользователю потребуется ввести и подтвердить новый доменный пароль (Рисунок 24b).



Рисунок 24b – Сообщение о рассинхронизации пароля в Windows 8.1.

Если запрос на изменение пароля произойдет в момент, когда ни один из серверов Indeed не будет доступен (но при этом будет доступен хотябы один контроллер домена), то после ввода нового пароля пользователем также появится сообщение о рассинхронизации пароля, т.к. новый пароль, установленный пользователем, невозможно будет синхронихировать с хранилищем данных Indeed (Рисунок 24с).

	Смена пароля	×
?	Ошибка связи с сервером. Сервер не найден. Если Вы продолжите, произойдет рассинхронизация пароля. Хотите продолжить?	
	ОК Отмена	

Рисунок 24с – Предупреждение о рассинхронизации пароля в Windows 8.1.

В этом случае новый доменный пароль необходимо будет синхронизировать с хранилищем данных Indeed при следующем входе в систему с использованием аутентификатора при хотя бы одном доступном сервере Indeed. После успешной синхронизации пароля будет выполнен вход в систему.

#### Автоматическая идентификация

Если на сервере Indeed-Id и на вашей рабочей станции настроена автоматическая идентификация, то для входа в систему указывать пользователя не нужно. выберите **Автоидентификация** (Рисунок 25) и приложите ранее зарегистрированный аутентификатор к считывателю.



Рисунок 25 – Автоматическая идентификация в Windows 8.1.

Aвтоматическая идентификация пользователей поддерживается только провайдерами Indeed-Id Z2USB и Indeed-Id OMNIKEY.

Для использования автоматической идентификации необходимо зарегистрировать аутентификатор после того, как будет выполнена настройка автоматической идентификации на всех серверах Indeed-Id и рабочей станции пользователя.

Функция автоматической идентификации может быть использована вместе с функцией автоматического завершения сеанса пользователя, если другой пользователь предоставит свой аутентификатор. Для настройки автоматической идентификации и автоматического завершения сеанса пользователя обратитесь к документу *Indeed-Id Admin Pack. Руководство по установке и использованию.pdf.* 

# Доступ к удаленному рабочему столу с использованием аутентификатора

Для доступа к удаленному рабочему столу по аутентификатору требуются:

- Стандартная утилита Windows mstsc.exe (Подключение к удаленному рабочему столу/Remote Desktop) на терминальном клиенте.
- Модуль Indeed-Id Windows® Logon, установленный на терминальном сервере.
- Модуль **Indeed-Id Provider**, соответствующий используемой технологии аутентификации, установленный на терминальном клиенте и терминальном сервере.
- Аппаратное устройство аутентификации, подключенное к терминальному клиенту (не требуется при использовании провайдеров Indeed OTM Provider, Indeed Google Authenticator Provider, Indeed Passcode Provider).

Для доступа к удаленному рабочему столу по аутентификатору выполните следующие действия:

#### 1. Запустите Подключение к удаленному рабочему столу.

- 2. Введите имя/адрес терминального сервера и установите подключение.
- 3. В отобразившемся окне **Вход в Windows** выберите вашу учетную запись, способ входа (тип аутентификатора) и пройдите аутентификацию.



Если для вашей учетной записи не сгенерирован случайный пароль, вы можете получить доступ к удаленному рабочему столу по паролю.

#### Вход в систему при отсутствии сети

Вход в систему по аутентификатору может быть выполнен даже при отсутствии физического подключения к сети. Действия при входе в систему в отсутствие сети по кэшированному аутентификатору аналогичны действиям при входе в систему по аутентификатору при доступной сети.

Данный способ входа доступен, если:

- Для вашей учетной записи было установлено разрешение на кэширование аутентификаторов.
- Было выполнено кэширование аутентификаторов (при первом входе в систему по аутентификатору).

Был выполнен вход в систему по кэшированному аутентификатору при доступной сети



Срок действия кэшированных аутентификаторов может быть ограничен администратором системы. По умолчанию этот срок составляет 10 дней, отсчитывается с даты последнего входа в и не зависит от того, будет ли выполнен вход в систему в дальнейшем в течение этого срока. Например, при установленном сроке 10 дней и выполнении входа в систему 12.04.2010 кэшированные аутентификаторы будут действительны с 00 ч 00 мин 13.04.2010 до 00ч 00 мин 23.04.2010. Если для вашей учетной записи разрешено кэширование аутентификаторов, то уточните у администратора наличие возможных ограничений. Если срок действия кэшированных аутентификаторов истек и серверы Indeed недоступны, при попытке входа в систему отображается сообщение об ошибке: "Ошибка при входе в систему. Сервер не найден. Кэширование данных пользователя запрещено".

# Управление аутентификаторами

Вы можете управлять аутентификаторами с помощью приложения **Indeed-Id Управление** аутентификаторами. Данное приложение позволяет добавлять новые аутентификаторы, редактировать, проверять и удалять имеющиеся.



Возможности управления аутентификаторами доступны при наличии разрешения, установленного администратором системы.

Для перехода к управлению аутентификаторами выполните следующие действия:

- 1. Откройте приложение Indeed-Id Управление аутентификаторами (Программы > Indeed-Id > Indeed-Id Управление аутентификаторами).
- 2. В окне **Аутентификация** выберите свою учетную запись и способ входа (тип аутентификатора). По умолчанию автоматически выбирается последний использованный способ входа (Рисунок 26).



Для входа в приложение «Управление аутентификаторами» следует использовать ранее зарегистрированный аутентификатор. При использовании пароля для доступа к приложению часть функций будет недоступна.

A	ут	e⊦	ITI	∕ı¢	эи	кация	INT	∍≘⋷	:D 🕞
Ев	ген	ий	Б	эло	в (	DEMO\Евгений Белов)			
9	6	3	7	7	0	Используя клавиатуру, вве находящиеся в ячейках ва	едите цифры, ашего шаблона		
3	1	8	6	2	0	•••••	Вхол		
9	8	1	1	4	2		Блод		
5	4	6	5	5	8				
4	3	2	0	7	9				
а 5 4 <u>Выб</u>	4 3 <u>5рат</u>	6 2 ъдр	5 0 0 0 0 0 0 0 0 0 0 0	4 5 7 <u>то пс</u> <u>6 вх</u>	2 8 9 ольз	ователя			

Выполните требуемые действия (в зависимости от выбранного способа входа).



Возможности добавления, редактирования и удаления аутентификаторов доступны после авторизации с использованием аутентификатора. Возможность проверки аутентификаторов доступна как после авторизации с использованием аутентификатора, так и после авторизации с использованием пароля.

- 3. После успешной аутентификации отображается окно Управление аутентификаторами.
  - Для перехода к добавлению аутентификатора нажмите **Добавить аутентификатор**.
  - Для перехода к редактированию выбранного аутентификатора нажмите Изменить.
  - Для перехода к проверке выбранного аутентификатора нажмите Проверить.
  - Для перехода к удалению выбранного аутентификатора нажмите Удалить.

Смотрите также:

- Добавление аутентификатора
- Редактирование аутентификатора
- Проверка аутентификатора
- Удаление аутентификатора

# Добавление аутентификатора

Количество аутентификаторов, которое вы можете добавить, устанавливается администратором системы. После достижения максимального количества аутентификаторов кнопка **Добавить способ входа** в окне **Управление аутентификаторами** становится неактивна.

Для добавления аутентификатора выполните следующие действия:

В окне Управление аутентификаторами нажмите Добавить способ входа (Рисунок 27).



Рисунок 27 – Окно «Управление аутентификаторами» компонента Indeed-Id Windows® Logon.



Следуйте инструкциям по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора (Рисунок 28b).



Рисунок 28b – Пример регистрации аутентификатора.

После успешной регистрации аутентификатора в окне **Управление аутентификаторами** отображается сообщение **"Новый аутентификатор успешно обучен"** (Рисунок 28с).

DEMO\Евген Управле	ий Белов ение аутентификаторами	INDEE	ם וס
	Новый аутентификатор успешно обуч Все готово для регистрации аутентификатора в с Перед сохранением вы можете задать коммента к аутентификатору: Сохранить	ӨН истеме. рий	
← Вернуться		RU	Выход

Рисунок 28с – Сохранение аутентификатора.

Вы можете добавить произвольный текстовый комментарий к зарегистрированному аутентификатору (если данное действие разрешено администратором системы). Для завершения регистрации аутентификатора нажмите **Сохранить**.

Тип зарегистрированного аутентификатора и комментарий к нему отображаются в окне **Управление аутентификаторами**. Если для вашей учетной записи разрешено добавление нескольких аутентификаторов, вы можете перейти к их регистрации, нажав на кнопку **Добавить** аутентификатор.

![](_page_40_Picture_5.jpeg)

При использовании определенных моделей биометрических устройств (например, сканеров отпечатков пальцев Digent IZZIX FD 2000, FD/FM 1000) возможны ошибки при регистрации и распознавании аутентификатора, связанные с уровнем чувствительности сканера и индивидуальными особенностями человека (температура тела, уровень влажности кожи, способ прикладывания пальца). Во избежание таких ошибок рекомендуется проверять аутентификатор сразу после регистрации.

# Редактирование аутентификатора

![](_page_41_Picture_1.jpeg)

Вы можете отредактировать (повторно зарегистрировать) аутентификатор или изменить только комментарий к аутентификатору (если это действие разрешено администратором системы).

Для редактирования аутентификатора выполните следующие действия:

В окне **Управление аутентификаторами** выберите аутентификатор и нажмите **Изменить** (Рисунок 29а).

![](_page_41_Picture_5.jpeg)

Рисунок 29а – Окно «Управление аутентификаторами» компонента Indeed-Id Windows® Logon.

Выполните одно из указанных действий:

• Чтобы отредактировать только комментарий к аутентификатору, введите его в соответствующее поле и нажмите **Сохранить** (Рисунок 29b).

DEMO\Евген Управле	ий Белов ение аутентификаторами	) = = !	D (D)
	<u>Задать заново</u> → Вы можете изменить комментарий к аутентификатору: [ Сохранить		
← <u>Вернуться</u>		RU	<u>Выход</u>

Рисунок 29b – Редактирование комментария зарегистрированного аутентификатора.

• Чтобы перейти к редактированию самого аутентификатора, нажмите **Задать заново**. После нажатия на ссылку **Задать заново** в окне отобразятся инструкции по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора. выполните требуемые действия.

После успешной регистрации аутентификатора в окне нажмите Сохранить.

# Проверка аутентификатора

Для проверки аутентификатора выполните следующие действия:

В окне **Управление аутентификаторами** выберите аутентификатор и нажмите **Проверить** (Рисунок 30а).

![](_page_43_Picture_3.jpeg)

Рисунок 30а – Проверка зарегистрированного аутентификатора.

После нажатия на ссылку **Проверить** в окне **Управление аутентификаторами** отображаются инструкции по регистрации аутентификатора. Внешний вид окна и текст подсказок зависят от выбранного типа аутентификатора. Выполните требуемые действия.

После завершения проверки в окне **Управление аутентификаторами** отображается сообщение о результате.

• Если аутентификаторы совпадают (Рисунок 30b):

![](_page_44_Picture_2.jpeg)

Рисунок 30b – Проверка аутентификатора: аутентификаторы совпадают.

• Если аутентификаторы не совпадают (Рисунок 30с):

![](_page_45_Picture_1.jpeg)

Рисунок 30с – Проверка аутентификатора: аутентификаторы не совпадают.

Если аутентификаторы не совпадают, нажмите **Вернуться** и повторите процедуру проверки или заново обучите аутентификатор.

# Удаление аутентификатора

Для удаления аутентификатора выполните следующие действия:

В окне **Управление аутентификаторами** выберите аутентификатор и нажмите **Удалить**. Для подтверждения действия нажмите **Да** (Рисунок 31а).

DEM0\Евге Управл	ний Белов ение аутентификаторами	INDEE	כן ס
→ <u>Карта</u> <b>→ Одноразов</b> Изменить   При	ая матрица рверить   Удалить		
	Подтверждение		
	😢 Вы действительно хотите удалить этот спос	соб входа? <u>Да Нет</u>	
+ <u>Добавить сп</u>	<u>эсоб входа</u>	RU	Выход

Рисунок 31а – Подтверждение удаления аутентификатора.

Если для вашей учетной записи был сгенерирован случайный пароль, при попытке удалить единственный имеющийся аутентификатор система отображает диалог-предупреждение (Рисунок 31b):

![](_page_46_Picture_6.jpeg)

Рисунок 31b – Подтверждение удаления последнего аутентификатора.

Если вы удалили все аутентификаторы и не можете выполнить вход в систему по паролю, обратитесь к администратору системы. После сброса пароля вы снова сможете выполнить вход в систему и зарегистрировать новые аутентификаторы.

После удаления всех аутентификаторов вход в систему может быть выполнен только по паролю. Если для вашей учетной записи был сгенерирован случайный пароль, вход в систему станет невозможен.

# **Indeed-Id Paste**

В случаях, когда ввод пароля требуется для доступа в приложения, программный комплекс Indeed-Id делает его использование максимально безопасным. С помощью **Indeed-Id Paste** вы можете автоматически подставлять скрытый пароль в поле ввода при нажатии определенной комбинации «горячих клавиш» (по умолчанию **[Ctrl] [Alt] [V]**). Включить и отключить функцию Indeed-Id Paste вы можете из приложения Indeed-Id Paste Tray. Щелкните на значке

🥴 в области уведомлений Windows и выберите нужный пункт контекстного меню:

- **Разрешить Indeed-Id Paste** (включение функции, выбрано по умолчанию)
- Запускать при загрузке (запуск Indeed-Id Paste Tray при загрузке Windows, выбран по умолчанию)
- Выход (выход из приложения)

Чтобы воспользоваться функцией Indeed-Id Paste, выполните следующие действия:

- 1. В окне приложения установите фокус мыши в поле ввода пароля.
- 2. Нажмите комбинацию «горячих клавиш».
- 3. Отображается окно **Аутентификация**. Подтвердите свою личность любым доступным способом (**Аутентификатор**/**Пароль**).

После успешной аутентификации в поле ввода отображается скрытый пароль.

# **Run as administrator**

Для систем Microsoft Windows Vista и более поздних версий реализован запрос на аутентификацию по технологии Indeed-Id для стандартной команды **Run as administrator**. После запуска данной команды отображается диалог выбора учетной записи, затем окно **Аутентификация** системы Indeed-Id. В зависимости от версии операционной системы окно выбора учетной записи может иметь разный вид. На Рисунках 32a и 32b приведены примеры для операционных систем Windows 7 и Windows 8.1 соответственно.

😚 Контроль учетных записей пользователей 🗾			
Разрешить следующей программе внести изменения на этом компьютере?			
8	Имя программы: Проверенный издатель: Источник файла:	Калькулятор Windows <b>Microsoft Windows</b> Жесткий диск компьютера	
Чтобы продолжить, введите пароль администратора и нажмите кнопку "Да".			
	Евгений Белов		
	DEMO\Administrator		
D	Другой пользовател	<b>b</b>	
D	Автоидентификация		
🕑 Показать п	одробности	Да Нет	

Рисунок 32а – Контроль учетных записей пользователей Windows 7.

![](_page_49_Figure_0.jpeg)

Рисунок 32b – Контроль учетных записей пользователей Windows 8.1.

## Таблица сообщений журнала подключения

Журнал подключения используется для отображения системной информации о процессе поиска и подключения компонентов системы Indeed к серверу Indeed-Id. При возникновении ошибки подключения к серверу, Windows® Logon отображает сообщение «Ошибка при соединении с сервером. Сервер не найден. Подробное описание ошибки в журнале подключения». При нажатии на «журнал подключения» отобразится информация о подключении к серверу (Рисунок 33). Текст сообщения может меняться в зависимости от возникшей проблемной ситуации.

📩 Информация об ошибке подключения	
Connecting to remote server.[*** Searching for Global Catalog server name from server cache.WIN-EUMHASQJIDG.demo.local[*** Searching for Indeed-Id server ***]Acquiring servers IP addresses.192.168.12.1 DNS server answer: WIN-EUMHASQJIDG.demo.local - 192.168.12.1.Pinging the servers.Server WIN-EUMHASQJIDG.demo.local is available.[*** Connecting to Indeed-Id server: WIN-EUMHASQJIDG.demo.local ***]Creating remote IndeedIDHostEnterprise instance.Acquiring Server object.Error: spHost->GetServer (hr=0xc100006b Cepвер остановлен.)Error: wIN-EUMHASQJIDG.demo.local is unavailable (hr=0x8007274d Подключение неустановлено, т.к. конечный компьютер отверг запрос на подключение.)Connection to Indeed-Id server failed.Acquiring DirectorySearch object from Global Catalog.Searching for Global Catalog server on current site.Acquiring DNS name of current site.Acquiring DNS name.	4
Копировать в буфер обмена Закрыти	Ъ

Рисунок 33 – Журнал подключения компонента Indeed-Id Windows® Logon.

Ниже приведены основные сообщения журнала подключения:

Сервер выключен	Connecting to remote server.	
или не развернут	[*** Searching for Global Catalog server ***]	
	Acquiring Global Catalog server name from server cache.	
	Server name not found.	
	Acquiring DirectorySearch object from Global Catalog.	
Searching for closest Global Catalog server. Searching for Global Catalog server on current site.		
	Global Catalog servers list: w2003dc.test.local,	
	Opening the Global Catalog.	
	Opening an ActiveDirectory object(GC://w2003dc.test.local).	
	Global Catalog has been opened on w2003dc.test.local	
	Acquiring list of Indeed-Id servers from the Global Catalog.	
	Indeed-Id servers: WS2003SERVER.test.local,	
	Sorting servers by distance.	
	WS2003SERVER.test.local.	

	Close servers:
	no hosts.
	Far servers:
	WS2003SERVER.test.local.
Сервер отключен от	Connecting to remote server.
сети	[*** Searching for Global Catalog server ***]
	Acquiring Global Catalog server name from server cache.
	Server name not found.
	Acquiring DirectorySearch object from Global Catalog.
	Searching for closest Global Catalog server
	Searching for Global Catalog server on current site
	Acquiring DNS name of current site
	Acquiring forest DNS name
	Opening an ActiveDirectory object(IDAP://RootDSE)
	Acquiring servers list by DNS( ac_trn Default-First-Site-Name_sites test local)
	Clobal Catalog convers list: w2003dc tect local
	Opening the Clebal Catalog
	Opening an ActiveDirectory object(CC://w2002dc tect local)
	Clobal Catalog has been enough an w2003dc test local.
	Acquiring list of Indeed Id convers from the Clebal Catalog
	Acquiring list of Indeed-10 servers from the Global Catalog.
	Indeed-Id Servers: WS2003SERVER.lest.local,
	Sorung servers by distance.
	WS2003SERVER.test.local.
	Close servers: no nosts.
	Far servers: wS2003SERVER.test.local.
	Searching for server in the list of close servers.
	[*** Searching for Indeed-Id server ***]
	Acquiring servers IP addresses.
	Connection to Indeed-Id server failed.
	Searching for server in the list of far servers.
	[*** Searching for Indeed-Id server ***]
	Acquiring servers IP addresses.
	192.168.0.1 DNS server answer: WS2003SERVER.test.local - 192.168.0.2.
	Pinging the servers.
	Connection to Indeed-Id server failed.
Рабочая станция	Checking adapters.
клиента отключена	Testing DNS availability.
от сети	Test DNS query.
	Network unavailable, retrying
	Checking adapters.
	Testing DNS availability.
	Test DNS query.
	Network unavailable, retrying
	Checking adapters.
	Testing DNS availability.
	Test DNS query.
	Network unavailable, retrying
	Network unavailable

	Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Network unavailable, retrying
Контроллер домена недоступен	Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Network unavailable, retrying
Служба DNS отключена на контроллере домена	Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Network unavailable, retrying
Неправильный DNS сервер в настройках сетевого подключения	Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Checking adapters. Testing DNS availability. Test DNS query. Network unavailable, retrying Network unavailable, retrying

Ha сервере Connecting to remote server.

отключена служба «Indeed-Id Local BSP Broker»	[*** Searching for Global Catalog server ***] Acquiring Global Catalog server name from server cache. Server name not found. Acquiring DirectorySearch object from Global Catalog. Searching for Global Catalog server on current site. Acquiring DNS name of current site. Acquiring forest DNS name. Opening an ActiveDirectory object(LDAP://RootDSE). Acquiring servers list by DNS(_gc_ttp.Default-First-Site-Name_sites.test.local). Global Catalog servers u2003dc.test.local, Opening an ActiveDirectory object(GC://w2003dc.test.local). Global Catalog servers list: w2003dc.test.local, Opening an ActiveDirectory object(GC://w2003dc.test.local). Global Catalog has been opened on w2003dc.test.local Acquiring list of Indeed-Id servers from the Global Catalog. Indeed-Id servers: WS2003SERVER.test.local, Sorting servers by distance. WS2003SERVER.test.local. Close servers: no hosts. Far servers: WS2003SERVER.test.local. Searching for server in the list of close servers. [*** Searching for Indeed-Id server ***] Acquiring servers IP addresses. Connection to Indeed-Id server failed. Searching for server in the list of far servers. [*** Searching for Indeed-Id server ***] Acquiring servers IP addresses. I92.168.0.1 DNS server answer: WS2003SERVER.test.local - 192.168.0.2. Pinging the servers. Server WS2003SERVER.test.local is available. [*** Connecting to Indeed-Id server: WS2003SERVER.test.local - 192.168.0.2. Pinging the servers. Server WS2003SERVER.test.local is available. [*** Connecting to Indeed-Id server: WS2003SERVER.test.local ***] Creating remote IndeedDHostEnterprise instance. Acquiring Server object. Error: spServer>>ISSupportMode (hr=0x80070422 Yka3anHaas cnyxKå не может быть запущена, поскольку она отключена или все связанные с ней ycrpoйства отключены.) Error: WS2003SERVER.test.local is unavailable (hr=0x8007274d Подключение не ycrahobaneho, т.к. конечный компьютер отверг запрос на подключение.) Connection to Indeed-Id server failed.
Компьютер	Checking adapters. Testing DNS availability.
расположен в	The computer is NOT a member of a domain
домене	Checking adapters. Testing DNS availability.
	The computer is NOT a member of a domain
	Network unavailable, retrying
	Testing DNS availability.
	The computer is NOT a member of a domain
	Network unavailable, retrying Network unavailable.
Неправильные	Connecting to remote server.
настройки	[*** Searching for Global Catalog server ***]
межсетевого экрана	Acquiring Global Catalog server name from server cache.
	Server name not found. Acquiring DirectorySearch object from Global Catalog
	הכינטו אסרמי אסרמי לא מיני אסרמי לא אסרמי אסר

Searching for closest Global Catalog server. Searching for Global Catalog server on current site. Aquiring DNS name of current site. Aquiring forest DNS name. Opening an ActiveDirectory object(LDAP://RootDSE). Error: ADsOpenObject() failed (hr=0x8007054b Указанный домен не существует или к нему невозможно подключиться.) Searching for Global Catalog server in the domain. Aquiring forest DNS name. Opening an ActiveDirectory object(LDAP://RootDSE). Error: ADsOpenObject() failed (hr=0x8007054b Указанный домен не существует или к нему невозможно подключиться.) Opening an ActiveDirectory object(GC:). Error: After ADsEnumerateNext (hr=0x8007054b Указанный домен не существует или к нему невозможно подключиться.) Sorting servers by distance. WS2003SERVER.test.local. Error: ADsGetObject(Root) (hr=0x8007054b Указанный домен не существует или к нему невозможно подключиться.) Close servers: no hosts. Far servers: WS2003SERVER.test.local. Searching for server in the list of close servers. [\*\*\* Searching for Indeed-Id server \*\*\*] Acquiring servers IP addresses. Connection to Indeed-Id server failed. Searching for server in the list of far servers. [\*\*\* Searching for Indeed-Id server \*\*\*] Acquiring servers IP addresses. 192.168.0.1 DNS server answer: WS2003SERVER.test.local - 192.168.0.2. Pinging the servers. Server WS2003SERVER.test.local is available. [\*\*\* Connecting to Indeed-Id server: WS2003SERVER.test.local \*\*\*] Creating remote IndeedIDHostEnterprise instance. Error: CoCreateInstanceEx (hr=0x80070005 Отказано в доступе.) Error: WS2003SERVER.test.local is unavailable (hr=0x8007274d Подключение не установлено, т.к. конечный компьютер отверг запрос на подключение.) Connection to Indeed-Id server failed.

## Сбор программных логов

Наличие программных логов Indeed-Id позволяет специалистам службы поддержки оперативно локализовать причины возможных проблемных ситуаций и принять меры к их устранению. Сбор программных логов осуществляется с помощью утилиты Indeed-Id GetLog, поставляемой в составе программного комплекса Indeed Enterprise Authentication. Для получения подробной информации обратитесь к документу *Indeed-Id GetLog. Руководство по эксплуатации.pdf*.

### Часто задаваемые вопросы

Ознакомиться со списком часто задаваемых вопросов и ответов на них можно в **Базе знаний** по продуктам компании Indeed.